Cisco Wide Area Application Services Configuration Guide (Software Version 6.4.3x)

Last Modified: 2021-01-22

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

CONTENTS

PREFACE

CHAPTER 1

Preface

This preface describes who should read the *Cisco Wide Area Application Services Configuration Guide*, how it is organized, and its document conventions. It contains the following sections:

Audience

This guide is for experienced network administrators who are responsible for configuring and maintaining the Cisco Wide Area Application Services (WAAS) network.

You should be familiar with the basic concepts and terminology used in internetworking, and understand your network topology and the protocols that the devices in your network can use. You should also have a working knowledge of the operating systems on which you are running your WAAS network, such as Microsoft Windows, Linux, or Solaris.

Document Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	Introduction to Cisco WAAS, on page 1	Provides an overview of the Cisco WAAS product and its features.
Chapter 2	Planning Your Cisco WAAS Network, on page 23	Provides general guidelines and preparation information you should read before installing the Cisco WAAS product in your network.
Chapter 3	Using Device Groups and Device Locations, on page 53	Describes how to create groups that make it easier to manage and configure multiple devices at the same time This chapter also covers device locations.

Chapter	Title	Description
Chapter 4	Configuring Cisco AppNav, on page 67	Describes how to configure your Cisco WAAS network using the AppNav deployment model.
Chapter 5	Configuring Traffic Interception, on page 127	Describes the Cisco WAAS software support for intercepting all TCP traffic in an IP-based network.
Chapter 6	Configuring Network Settings, on page 187	Describes how to configure interfaces and basic network settings like DNS and CDP.
Chapter 7	Configuring Administrative Login Authentication, Authorization, and Accounting, on page 219	Describes how to centrally configure administrative login authentication, authorization, and accounting for WAEs in your Cisco WAAS network.
Chapter 8	Creating and Managing Administrator User Accounts and Groups, on page 255	Describes how to create device-based CLI accounts and roles-based accounts from the Cisco WAAS Central Manager GUI.
Chapter 9	Creating and Managing IP Access Control Lists for WAAS Devices, on page 277	Describes how to centrally create and manage Internet Protocol (IP) access control lists (ACLs) for your WAEs.
Chapter 10	Configuring Other System Settings, on page 289	Describes how to perform various other system configuration tasks such as specifying an NTP server and setting the time zone on a device.
Chapter 11	Configuring File Services, on page 343	Describes how to configure Common Internet File System (CIFS) acceleration, which allows branch office users to more efficiently access data stored at centralized data centers.
Chapter 12	Configuring Application Acceleration, on page 371	Describes how to configure the application policies on your Cisco WAAS system that determine the types of application traffic that is accelerated over your WAN.
Chapter 13	Configuring WAAS with Akamai Connect, on page 467	Describes how to configure Cisco WAAS with Akamai Connect, to reduce latency for HTTP/HTTPS traffic for business and web applications and improve performance for many applications.
Chapter 14	Maintaining Your Cisco WAAS System, on page 513	Describes the tasks you may need to perform to maintain your Cisco WAAS system.
Chapter 15	Monitoring Your Cisco WAAS Network, on page 553	Describes the monitoring tools available in the Cisco WAAS Central Manager GUI that provide detailed status information on your WAAS network.
Chapter 16	Troubleshooting Your Cisco WAAS Network, on page 619	Describes the troubleshooting tools available in the Cisco WAAS Central Manager GUI that can help you identify and resolve issues with your Cisco WAAS network.

Chapter	Title	Description
Chapter 17	Configuring SNMP Monitoring, on page 647	Describes how to configure SNMP traps, recipients, community strings and group associations, user security model groups, and user access permissions.
Appendix A	Predefined Application Policies, on page 697	Lists the predefined applications and classifiers that WAAS will either optimize or pass through based on the policies that are provided with the system.
Appendix B	Transaction Log Format, on page 709	Describes the transaction log format.

Document Conventions

Command descriptions use these conventions:

boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.

Screen examples use these conventions:

screen font	Terminal sessions and information the switch displays are in screen font.
boldface screen font	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

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

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

Tip Means the following information will help you solve a problem. Tips might not be troubleshooting or even an action, but could help you save time.

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

  (this manual)
- 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
- Cisco Wide Area Application Services vWAAS Installation and Configuration Guide
- Configuring WAAS Express
- 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
- Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series
- Installing the Cisco WAE Inline Network Adapter

Obtaining Documentation and Submitting a Service Request

For information on 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

Introduction to Cisco WAAS

This chapter provides an overview of the Cisco Wide Area Applications Services (Cisco WAAS) solution and describes the main features that enable Cisco WAAS to overcome the most common challenges in transporting data over a wide area network.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco WAAS Central Managers and Cisco Wide Area Application Engines (Cisco WAEs) in your network. The term Cisco WAE refers to Cisco WAE and Cisco Wide Area Virtualization Engine (Cisco WAVE) appliances, and Cisco Virtual WAAS (Cisco vWAAS) instances.

This chapter contains the following sections:

About Cisco WAAS

The Cisco WAAS system consists of a set of devices called Cisco WAEs that work together to optimize TCP traffic over your network. When client and server applications attempt to communicate with each other, the network intercepts and redirects this traffic to the WAEs so that they can act on behalf of the client application and the destination server. The WAEs examine the traffic and use built-in optimization policies to determine whether to optimize the traffic or allow it to pass through your network unoptimized.

Cisco WAAS Version 5.0 introduced a new AppNav deployment model that greatly reduces dependency on the intercepting switch or router by taking on the responsibility of distributing traffic among Cisco WAAS devices for optimization. Cisco WAAS appliances with AppNav Controller Interface Modules operate in a special AppNav Controller mode, with AppNav policies controlling traffic flow to Cisco WAAS devices performing optimization. The AppNav model is well suited for data center deployments and addresses many of the WAN optimization challenges in this environment.

Note You can deploy Cisco WAAS in either the AppNav model, or in the traditional model without using AppNav Controllers.

Use the Cisco WAAS Central Manager GUI to centrally configure and monitor the Cisco WAEs and optimization policies in your network. You can also use the Cisco WAAS Central Manager GUI to create new optimization policy rules so that the Cisco WAAS system can optimize both custom applications and less common applications.

Cisco WAAS helps enterprises meet the following objectives:

- Provide branch office employees with LAN-like access to information and applications across a geographically distributed network.
- Migrate application and file servers from branch offices into centrally managed data centers.
- Minimize unnecessary WAN bandwidth consumption through the use of advanced compression algorithms.
- Improve application performance over the WAN by addressing the following common issues:
    - Low data rates (constrained bandwidth)
    - Slow delivery of frames (high network latency)
    - Higher rates of packet loss (low reliability)

Note A Cisco WAAS Express device, which is a Cisco router with Cisco WAAS Express functionality enabled, can interoperate with other Cisco WAAS devices. A Cisco WAAS Express device provides basic WAN optimization and some application optimization, but no virtualization. For more information on Cisco WAAS Express, see *Configuring WAAS Express*.

A device having the AppNav-XE component, typically, a Cisco router or virtual Cisco Cloud Services Router with virtual AppNav functionality, can interoperate with other Cisco WAAS devices that are acting as WAAS nodes. Such a device acts as an AppNav Controller that distributes traffic to other Cisco WAAS devices acting as WAAS nodes that optimize the traffic. However, a device with the AppNav-XE component cannot interoperate with other AppNav Controller hardware appliances. For more information on AppNav-XE, see the AppNav-XE documentation. For more information on AppNav, see the chapter Configuring Cisco AppNav, on page 67.

A Cisco vWAAS instance is a virtual Cisco WAAS appliance running on a VMware virtual machine and providing all of the same features as a Cisco WAAS appliance. A Cisco WAAS Central Manager can manage Cisco WAEs, Cisco WAAS Express devices, and Cisco vWAAS instances all in the same Cisco WAAS network. For more information on Cisco vWAAS, see the *Cisco Virtual Wide Area Application Services Configuration Guide* .

Cisco ISR-WAAS is a virtualized Cisco WAAS instance running on a Cisco ISR router. It provides added optimization without the need for additional hardware or external appliances. A Cisco WAAS Central Manager can monitor and configure Cisco ISR-WAAS.

The following table shows how Cisco WAAS uses a combination of TCP optimization techniques and application acceleration features to overcome the most common challenges associated with transporting traffic over a WAN.

Table 1: Cisco WAAS Solutions for WAN Issues

WAN Issue	Cisco WAAS Solution
High network latency	Intelligent protocol adapters reduce the number of round-trip responses common with chatty application protocols.
Constrained bandwidth	Data caching provided with the file services feature and data compression reduce the amount of data sent over the WAN, which in turn, increases data transfer rates. These solutions improve application response time on congested links by reducing the amount of data sent across the WAN.
Poor link utilization	TCP optimization features improve network throughput by reducing the number of TCP errors sent over the WAN and maximizing the TCP window size that determines the amount of data that a client can receive at one time.
Packet loss	Optimized TCP stack in Cisco WAAS overcomes the issues associated with high packet loss and protects communicating end points from the state of the WAN.

Key Services of Cisco WAAS

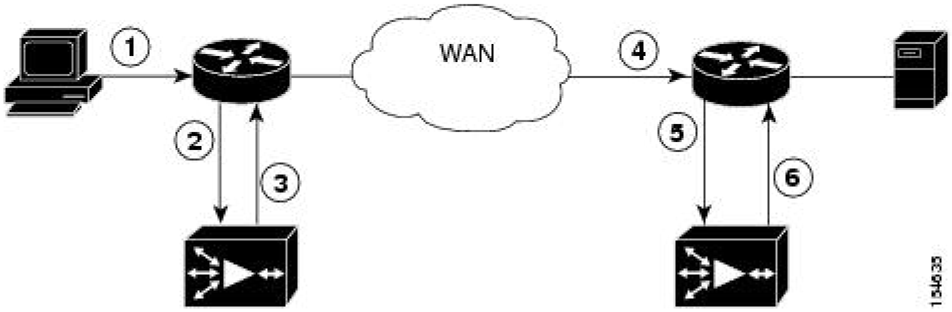
This section contains the following topics:

Note Cisco WAAS Express devices provide basic optimization and compression services and some application acceleration.

Traffic Optimization Process

The following figure shows the process that Cisco WAAS follows to optimize application traffic.

Figure 1: Traffic Optimization Process



The following steps describe how your Cisco WAAS network optimizes a connection between a branch office client and a destination server:

1. A branch office client attempts to connect to the destination server over the native application port.

2. The Cisco WAAS network uses Web Cache Communication Protocol (WCCP) or Policy-Based Routing (PBR) to intercept the client request, or if deployed on an inline Cisco WAE, Cisco WAAS can intercept

the request directly, using inline mode. For more information on inline mode, see Using Inline Mode Interception, on page 171 in the Chapter "Configuring Traffic Interception."

3. The branch WAE performs the following actions:
    - Examines the parameters in the traffic's TCP headers and then refers to the optimization policies to determine if the intercepted traffic should be optimized. Information in the TCP header, such as the source and destination IP address and port, allows the branch WAE to match the traffic to an optimization policy rule. For a list of predefined policy rules, see Appendix A, "Predefined Optimization Policy."
    - If the branch WAE determines that the traffic should be optimized, it adds information to the TCP header informs the next WAE in the network path to optimize the traffic.
4. The branch WAE passes along the client request through the network to its original destination server.
5. The data center WAE performs the following actions:
    - Intercepts the traffic going to the destination server.
    - Establishes an optimized connection with the branch WAE. If the data center WAE has optimization disabled, an optimized connection is not established, and the traffic passes over the network unoptimized.

      In an AppNav deployment, an AppNav Controller intercepts the traffic in the data center and distributes it to a WAAS node that establishes an optimized connection with the branch WAE. For more information on AppNav deployment, see the chapter Configuring Cisco AppNav, on page 67.
6. Cisco WAAS optimizes subsequent traffic between the branch WAE and data center WAE for this connection.

   Cisco WAAS does not optimize traffic in the following situations:
    - The WAE intercepts non-TCP traffic (such as UDP or ICMP).
    - The WAE is overloaded and does not have the resources to optimize traffic.
    - The intercepted traffic matches an optimization or AppNav policy rule that specifies that traffic can be passed through unoptimized.

Note If unoptimized traffic reaches a WAE, the WAE forwards the traffic in pass-through mode without affecting the performance of the application using the passed-through connection.

Transport Flow Optimization

Cisco WAAS uses a variety of transport flow optimization (TFO) features to optimize TCP traffic intercepted by the Cisco WAAS devices. TFO protects communicating clients and servers from negative WAN conditions, such as bandwidth constraints, packet loss, congestion, and retransmission.

TFO includes the following optimization features:

Window Scaling

Window scaling allows the receiver of a TCP packet to advertise that its TCP receive window can exceed 64 KB. The receive window size determines the amount of space that the receiver has available for unacknowledged data. By default, TCP headers limit the receive window size to 64 KB, but Windows scaling allows the TCP header to specify receive windows of up to 1 GB.

Window scaling allows TCP endpoints to take advantage of available bandwidth in your network and not be limited to the default window size specified in the TCP header.

For more information about Window scaling, see RFC 1323 .

TCP Initial Window Size Maximization

Cisco WAAS increases the upper bound limit for TCP's initial window from one or two segments to two to four segments (approximately 4 KB). Increasing TCP's initial window size provides the following advantages:

- When the initial TCP window is only one segment, a receiver that uses delayed ACKs is forced to wait for a timeout before generating an ACK response. With an initial window of at least two segments, the receiver generates an ACK response after the second data segment arrives, eliminating the wait on the timeout.
- For connections that transmit only a small amount of data, a larger initial window reduces the transmission time. For many e-mail (SMTP) and web page (HTTP) transfers that are less than 4 KB, the larger initial window reduces the data transfer time to a single round-trip time (RTT).
- For connections that use large congestion windows, the larger initial window eliminates up to three RTTs and a delayed ACK timeout during the initial slow-start phase.

For more information about this optimization feature, see RFC 3390.

Increased Buffering

Cisco WAAS enhances the buffering algorithm used by the TCP kernel so that WAEs can pull data from branch office clients and remote servers more aggressively. This increased buffer helps the two WAEs participating in the connection keep the link between them full, thus increasing link utilization.

Selective Acknowledgment

Selective Acknowledgment (SACK) is an efficient packet loss recovery and retransmission feature that allows clients to recover from packet losses more quickly, compared to the default recovery mechanism used by TCP.

By default, TCP uses a cumulative acknowledgment scheme that forces a sender to either wait for a round-trip to learn if packets were not received by a recipient, or to unnecessarily retransmit segments that may have been correctly received.

SACK allows the receiver to inform the sender about all the segments that have arrived successfully, so that the sender needs to retransmit only the segments that have actually been lost.

For more information, see RFC 2018 .

Binary Increase Congestion TCP

Binary Increase Congestion (BIC) TCP is a congestion management protocol that allows your network to recover more quickly from packet loss events.

When your network experiences a packet loss event, BIC TCP reduces the receiver's window size and sets that reduced size as the new value for the minimum window. BIC TCP then sets the maximum window size value to the size of the window just before the packet loss event occurred. Because packet loss occurred at the maximum window size, the network can transfer traffic without dropping packets whose size falls within the minimum and maximum window size values.

If BIC TCP does not register a packet loss event at the updated maximum window size, that window size becomes the new minimum. If a packet loss event does occur, that window size becomes the new maximum. This process continues until BIC TCP determines the new optimum minimum and maximum window size values.

Compression Technologies in Cisco WAAS

Cisco WAAS uses the following compression technologies to help reduce the size of data transmitted over your WAN:

- Data Redundancy Elimination (DRE)
- Lempel-Ziv (LZ) compression

These compression technologies reduce the size of transmitted data by removing redundant information before sending the shortened data stream over the WAN. By reducing the amount of transferred data, Cisco WAAS compression helps reduce network utilization and application response times.

When a WAE uses compression to optimize TCP traffic, it replaces repeated data in the stream with a much shorter reference, and then sends the shortened data stream out across the WAN. The receiving WAE uses its local redundancy library to reconstruct the data stream before passing it along to the destination client or server.

The Cisco WAAS compression scheme is based on a shared cache architecture where each WAE involved in compression and decompression shares the same redundancy library. When the cache that stores the redundancy library on a WAE becomes full, Cisco WAAS uses a FIFO algorithm to discard old data and make room for new.

LZ compression operates on smaller data streams and maintains limited compression history. DRE operates on significantly larger streams (typically tens to hundreds of bytes or more) and maintains a much larger compression history. Large chunks of redundant data is common in file system operations when files are incrementally changed from one version to another or when certain elements are common to many files, such as file headers and logos.

Application-Specific Acceleration Features in Cisco WAAS

In addition to the TCP optimization features that speed the flow of traffic over a WAN, Cisco WAAS includes these application acceleration features:

- Operation prediction and batching: Allows a Cisco WAAS device to transform a command sequence into a shorter sequence over the WAN to reduce roundtrips.
- Intelligent message suppression: Decreases the response time of remote applications. Even though TFO optimizes traffic over a WAN, protocol messages between branch office clients and remote servers can still cause slow application response time. To resolve this issue, each Cisco WAAS device contains application proxies that can respond to messages locally so that the client does not have to wait for a response from the remote server. The application proxies use a variety of techniques, including caching, command batching, prediction, and resource prefetch to decrease the response time of remote applications.

Cisco WAAS uses application-intelligent software modules to apply these acceleration features.

File Services for Desktop Applications

The file services (SMB accelerators) feature allows a WAE to fulfill a client's requests more quickly instead of sending every request over the WAN to the file server. By fulfilling a client's requests locally, the WAE minimizes the traffic sent over the WAN and reduces the time it takes branch office users to access files and many desktop applications, allowing enterprises to consolidate their important information in data centers. For more information, see the chapter Configuring File Services, on page 343.

Note Legacy-mode Wide Area File Services (WAFS) are no longer supported. Legacy WAFS users must migrate to the SMB accelerator.

This section contains the following topics:

Cisco WAAS Print Services

The Cisco WAAS software includes the following print services options:

- Microsoft Windows print accelerator: Use this option when you have a print server in a data center and branch clients are printing to local or remote printers. This service accelerates print traffic between clients and a Windows print server located in the data center. This option requires no configuration, but does require that both the SMB application accelerator and Microsoft Windows print acceleration be enabled. For more information, see Enabling and Disabling the Global Optimization Features, on page 373 in the chapter "Configuring Application Acceleration."

Note The **Legacy Print Services** feature is no longer supported. Users of **Legacy Print Services** must migrate to another print services option.

These services eliminate the need for a separate hardware print server in the branch office. Cisco WAAS print services are available for Microsoft Windows clients and work with any IP-based network printer.

Cisco WAAS Interfaces

The Cisco WAAS software provides the following interfaces to help you manage, configure, and monitor the various elements of your Cisco WAAS network:

Cisco WAAS Central Manager

This section contains the following topics:

About the Cisco WAAS Central Manager

Every Cisco WAAS network must have one primary Cisco WAAS Central Manager device that is responsible for managing the other Cisco WAAS devices in your network. The Cisco WAAS Central Manager device hosts the Cisco WAAS Central Manager GUI, a Web-based interface that allows you to configure, manage, and monitor the Cisco WAAS devices in your network. The Cisco WAAS Central Manager resides on a dedicated Cisco WAE device.

The Cisco WAAS Central Manager GUI allows administrators to perform the following tasks:

- Configure system and network settings for an individual Cisco WAAS device, Cisco vWAAS device, Cisco WAAS Express device, device group, AppNav Controller, and AppNav Cluster.
- Create and edit optimization policies that determine the action that a Cisco WAAS device performs when it intercepts specific types of traffic.
- Create and edit AppNav policies that determine how AppNav Controllers distribute traffic to optimizing Cisco WAAS nodes.
- Configure file services.
- Create device groups that help you manage and configure multiple Cisco WAEs at the same time.
- View detailed reports about the optimized traffic in your Cisco WAAS network.

Note You cannot enable optimization and application acceleration services on a WAE that has been configured as a Cisco WAAS Central Manager. The purpose of the Cisco WAAS Central Manager is to configure, monitor, and manage the Cisco WAEs in your network.

This section contains the following topics:

Accessing and Using the Cisco WAAS Central Manager

You can access the Cisco WAAS Central Manager with an IPv4 address, with an IPv6 address, or with a web browser.

Accessing the Cisco WAAS Central Manager with an IPv4 Address

To access the Cisco WAAS Central Manager with an IPv4 address, enter the following URL in your web browser:

https://*WAE_Address*:8443/

The *WAE_Address* value is the IP address or hostname of the WAAS Central Manager device.

The default administrator username is *admin* and the password is *default*. For information on creating accounts and changing passwords, see the Chapter Configuring Administrative Login Authentication, Authorization, and Accounting, on page 219 .

Accessing the Cisco WAAS Central Manager with an IPv6 Address

If the Cisco WAAS Central Manager has been configured with an IPV6 address, you can access it using https://[*CM ipv6 address*]:8443/

The default administrator username is *admin* and the password is *default*. For information on creating accounts and changing passwords, see the Chapter Configuring Administrative Login Authentication, Authorization, and Accounting, on page 219.

Ensure that your web browser is set to use Unicode (UTF-8) character encoding.

Accessing the Cisco WAAS Central Manager with Microsoft Internet Explorer

When using Microsoft Internet Explorer to access the Cisco WAAS Central Manager GUI, you may see a **Choose a digital certificate** dialog box. Click **Cancel** to proceed to the Cisco WAAS Central Manager login screen.You may also see a browser security warning that there is a problem with the website's security certificate. This happens because the Cisco WAAS Central Manager uses a self-signed certificate. Click **Continue to this website (not recommended)**. To avoid this error message in the future, you can permanently install the certificate. The certification installation procedure differs depending on the browser used.

To install the certificate in Internet Explorer 8:

1. Click the red **Certificate Error** button in the address bar.
2. Choose **View Certificates**.
3. Click **Install Certificate**.
4. Click **Next**.
5. Choose **Automatically select the certificate store based on the type of certificate**.
6. Click **Next**.
7. Click **Finish**.
8. At the **Security Warning**, at the **Acknowledgment**, click **OK**.
9. At the **Certificate** dialog box, click **OK**.

   The certificate installation procedure differs depending on the browser.

Operating Guidelines for the Cisco WAAS Central Manager

Consider the following operating guidelines for Cisco WAAS Central Manager user sessions:

- After an upgrade, downgrade, or new installation of Cisco WAAS: You must first clear the cache in your browser, close the browser, and restart the browser session to the Cisco WAAS Central Manager.
- If you are using Internet Explorer to access the Cisco WAAS Central Manager GUI, we strongly recommend that you install the Google Chrome Frame plug-in for better performance. When you log in to the Cisco WAAS Central Manager the first time, you are prompted to install Google Chrome Frame. Choose a language, click **Get Google Chrome Frame**, and follow the prompts to download and install the plug-in. If you do not want to install the plug-in, click the link to continue without installing Google Chrome Frame.

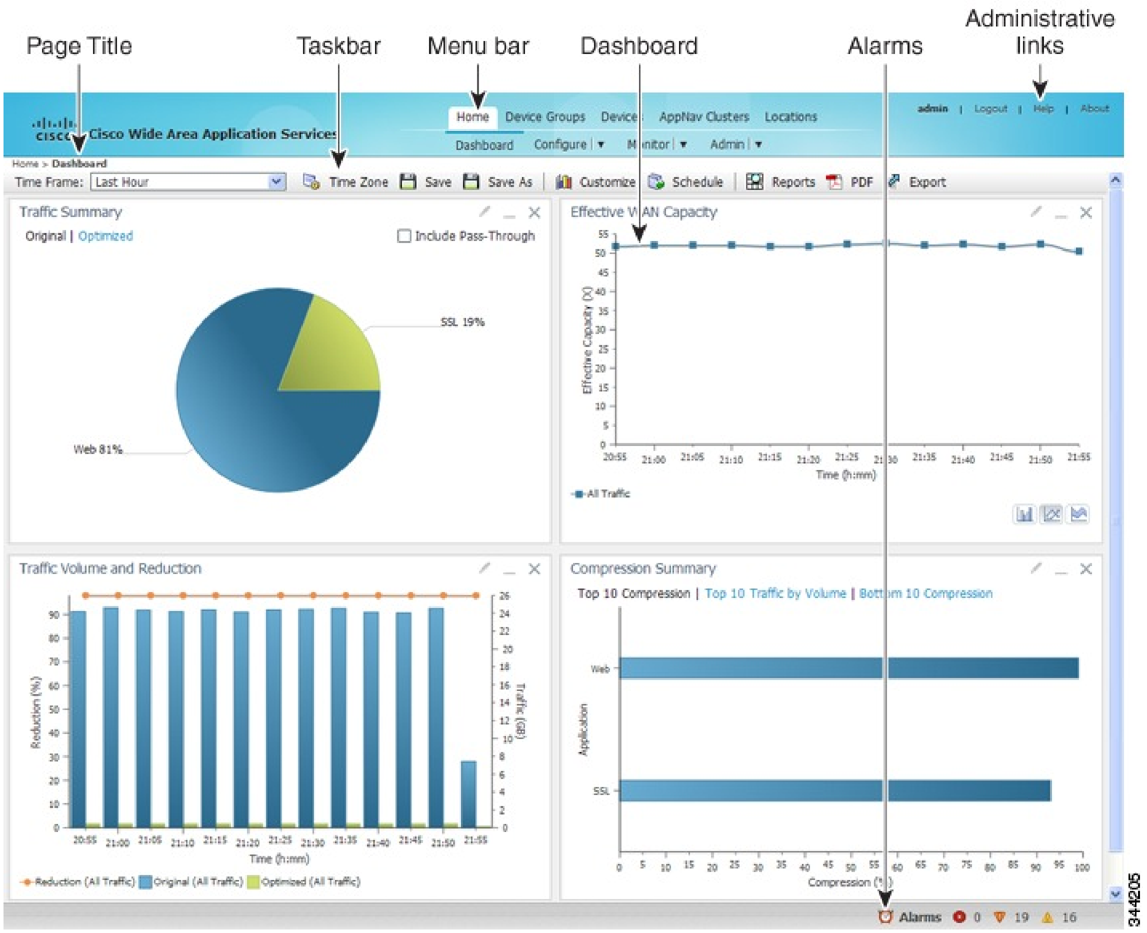
Note In Microsoft Internet Explorer Version 8 and Version 9, bookmarks to Cisco WAAS Central Manager pages other than the home page also go to the home page. In Microsoft Internet Explorer Version 10 and Version 11, bookmarks work as expected.

- For Cisco WAAS Version 5.4.1 and later, you are no longer prompted to install the Google Frame plug-in when you access the Cisco WAAS Central Manager GUI using Microsoft Internet Explorer. However, if the Google Frame plug-in has already been installed, Microsoft Internet Explorer will continue to use it.
- You can configure the Cisco WAAS Central Manager to limit the number of concurrent sessions permitted for a user. The number of concurrent sessions is unlimited by default. To change the number of permitted concurrent sessions, set the **System.security.maxSimultaneousLogins** property, as described in Modifying Default System Properties in the chapter "Configuring Other System Settings."
- To end a session, a user must log out of the Cisco WAAS Central Manager. If a user closes the browser or connection without logging off, the session is not closed until after it times out (in 10 minutes by default, up to a possible maximum of 1440 minutes). If the number of concurrent sessions permitted is also exceeded for that user, there is no way for that user to gain access to the Cisco WAAS Central Manager until after the timeout expires.

Components of the Cisco WAAS Central Manager GUI

The following figure shows the main components of the Cisco WAAS Central Manager GUI.

Figure 2: Components of the Cisco WAAS Central Manager GUI



The Cisco WAAS Central Manager GUI includes the following main components:

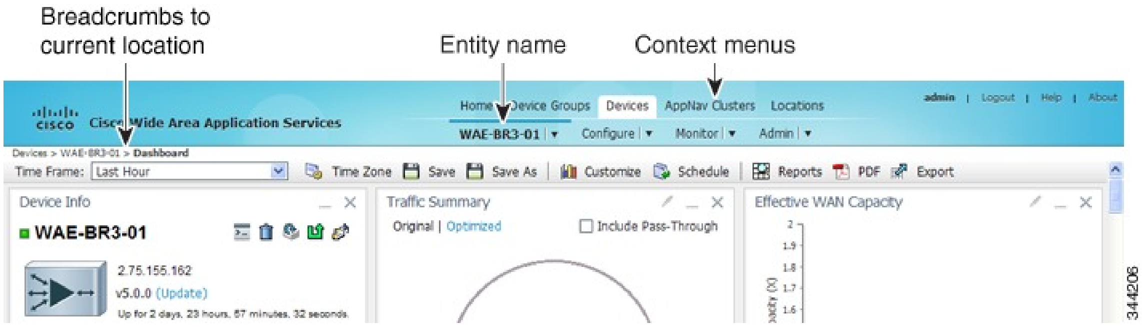
- Page title: Displays the title of the page being viewed and breadcrumb links to ease navigation back to previous levels in the hierarchy. (Breadcrumb links as shown in the following figure.)
- Menu bar: The upper level of the menu bar contains menu options that allow you to choose the context. The lower level of the menu bar contains menu options that group the Cisco WAAS Central Manager functions available within the chosen context. For more information, see Cisco WAAS Central Manager Menus, on page 12.
- Taskbar: Contains labeled icons that perform various functions depending on the content shown in the dashboard. For more information, see Cisco WAAS Central Manager Taskbar Icons, on page 13.
- Dashboard: Displays the main content, which changes depending on the option that is chosen in the menu.
- Administrative links: Includes these navigation links:
    - Logout: Logs out the current user from the Cisco WAAS Central Manager.
    - Help: Opens a separate window displaying Cisco WAAS context-sensitive help

      .
    - About: Displays the Cisco WAAS **About** window that shows the Cisco WAAS Central Manager version number.
- Alarms: Opens the alarm panel, which displays alarms in your Cisco WAAS network.

The upper level of the menu bar allows you to choose one of the five contexts available in the Cisco WAAS Central Manager GUI:

- Home: Click this to go to the global context, with no particular device group, device, AppNav Cluster, or location chosen.
- Device Groups: Choose a device group from this menu option to enter the device group context. The page title and the first menu on the lower level display the name of the chosen device group.
- Devices: Choose a device from this menu option to enter the device context. The page title and the first menu on the lower level display the name of the chosen device, as shown in the following figure.
- AppNav Clusters: Choose an AppNav Cluster from this menu option to enter the AppNav Cluster context. The page title and the first menu on the lower level display the name of the chosen AppNav Cluster.
- Locations: Choose a location from this menu option to enter the location context. The page title and the first menu on the lower level display the name of the chosen location.

Figure 3: Cisco WAAS Central Manager Device Context



Time Frame: Last Hour

WAE-BR3-01

2.75.155.162

v5.0.0 (Update)

Up for 2 days, 23 hours, 57 minutes, 32 seconds.

The Cisco WAAS Central Manager GUI includes the following items to help you navigate:

- Breadcrumbs to current location: Displays the path to your current location in the menu structure. You can click the **Devices** link to return to the **All Devices** page.

  If you are in the device group context, this link is named **Device Groups** and it returns you to the **All Device Groups** page. If you are in the AppNav Cluster context, this link is named **AppNav Clusters** and it returns you to the **All AppNav Clusters** page.

  If you are in the location context, this link is named **Locations** and it returns you to the **All Locations** page.

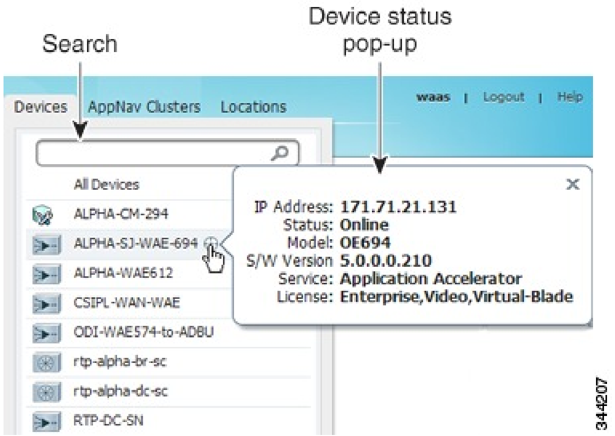
- Entity name: The first menu option in the lower level of the menu bar shows the name of the chosen device group, device, AppNav Cluster, or location.

- Context menu options: The top level of the menu bar contains menu options that allow you to switch easily to any entity in any context. You can search for an item by entering a part of its name in the search box at the top and clicking the magnifying glass icon or by pressing **Enter**. The list is filtered to include only entities that contain the search string.

  The top entry in each menu is **All Entities**, which takes you to a window that lists all the entities of the selected type, has more advanced search functions, and has taskbar icons that perform functions that are appropriate to the entity group. You can also click the context menu name to go to the corresponding listing window.

  In the **Devices** and **AppNav Clusters** menu bar options, a small target icon appears when you hover your mouse over a device or cluster name. Place your cursor over the target icon to open a dialog box that shows the device or cluster status (as shown in the following figure).

Figure 4: Devices Context Menu



IP Address: 171.71.21.131
Status: Online
Model: OE694
S/W Version 5.0.0.0.210
Service: Application Accelerator
License: Enterprise,Video,Virtual-Blade

Cisco WAAS Central Manager Menus

The Cisco WAAS Central Manager menu bar contains two levels of menus:

- Upper level: Contains menu options that allow you to switch to any entity in any context.

- Lower level: Contains menu options that group the Cisco WAAS Central Manager functions available within the chosen context. The following table describes the menu options in the lower menu bar.

Menus contain different functions when a particular device, device group, AppNav cluster, or location is selected than when you are in the global context.

Some menu options contain submenus. Hover the mouse over the triangle to the right of the menu option name to open the submenu.

Note The functions available for Cisco WAAS Express devices are a subset of those available for other Cisco WAAS devices. However, some functions are not available on Cisco WAAS Express devices.

Table 2: Cisco WAAS Central Manager Lower Menu Bar Descriptions

Menu	Description
Dashboard or Device, Device Group, AppNav Cluster, or Location Name	In the global context, allows you to go to the dashboard pertaining to your WAAS network. In a context other than global, this menu is named with the corresponding entity name and allows you to activate devices, view users, assign groups or devices, or view the dashboard or home screen of the entity.
Configure	Allows you to configure Cisco WAAS services and settings.
Monitor	Allows you to see network traffic and other charts and reports to monitor the health and performance of your Cisco WAAS network. Allows you to manage and schedule reports for your Cisco WAAS network. Contains troubleshooting tools.
Admin	Allows you to manage user accounts, passwords, secure store, licenses, update the Cisco WAAS software, and view system logs and messages.

Cisco WAAS Central Manager Taskbar Icons

The following table describes the taskbar icons in the Cisco WAAS Central Manager GUI.

Table 3: Cisco WAAS Central Manager Taskbar Icon Descriptions

Taskbar Icon	Function
Common Icons	
	Refreshes the current page of the Cisco WAAS Central Manager GUI.
	Deletes a Cisco WAAS element, such as a device or device group.
	Creates a new Cisco WAAS element, such as a report.
	Edits a Cisco WAAS element, such as interface settings.
	Filters the information in a table to make it easier to locate a specific item.
	Displays all the items in a table on a single page instead of displaying them over multiple pages.

Taskbar Icon	Function
	Prints the information.
	Creates a PDF of the information.
	Selects all the valid items in a table. For example, if you are distributing print drivers to a Cisco WAAS print server, you can click this icon to select all the drivers in the list that the print server should download.
	Deselects all the selected items in a table.
Devices and Device Group Icons	
	Activates all the inactive Cisco WAAS and Cisco WAAS Express devices in your Cisco WAAS network.
	Reapplies the device configuration as seen in the Cisco WAAS Central Manager GUI to the device. Normally, changes made in the Cisco WAAS Central Manager GUI are applied to the device as soon as the configuration is submitted. From time to time, however, a CLI error or some other error on the device may cause the configuration on the device to differ from what is seen in the Cisco WAAS Central Manager GUI. The **Force Full Database Update** icon applies the full configuration that the Cisco WAAS Central Manager has for the device to be updated, to the device, and the configuration is reapplied. When using the **Request FullUpdate** icon from the device group window, the full device configuration is reapplied to each device in the device group. Group settings do not overwrite device-specific settings. You can view device CLI errors in the **System Message** window described in Viewing the System Message Log in the chapter "Troubleshooting Your WAAS Network." The **Force Full Database Update** icon appears on the **Device Dashboard** window, described in Device Dashboard Window in the chapter "Monitoring Your Cisco WAAS Network." The **Request FullUpdate** icon appears in the **Modifying Device Group** window. **Note** These functions do not apply to Cisco WAAS Express devices.
	Reboots a WAE or device group depending on the location in the Cisco WAAS Central Manager GUI. Reload is not available for Cisco WAAS Express devices.
	Forces the device group configuration across all the devices in that group. For more information, see Forcing Device Group Settings on All Devices in the Group in the chapter "Using Device Groups and Device Locations."
	Applies the default settings to the fields in the window.
	Exports table information into a CSV file.
	Allows you to specify device-specific settings that override the group settings for the device. For more information, see Overriding the Device Group Settings on a Device in the chapter "Using Device Groups and Device Locations."
	Deactivates a Cisco WAAS or Cisco WAAS Express device.

Taskbar Icon	Function
	Updates the application statistics.
	Deletes all the Cisco WAAS elements of a particular type, such as IP ACL conditions.
	Displays all WAE devices or device groups.
	Allows you choose which charts to display in the **Device Dashboard** window.
	Copies interception settings to other devices (not available for inline interception).
Acceleration Icons	
	Restores the default predefined optimization policy rules on the device or device group. For more information, Restoring Optimization Policies and Class Maps in the chapter "Configuring Application Acceleration."
	Displays the topology map that shows all the TFO connections among your WAE devices. For more information, see the Topology Report in the chapter "Monitoring Your Cisco WAAS Network."
	Displays the configuration page used to create applications. For more information, see Viewing a List of Applications in the chapter "Configuring Application Acceleration."
System Message Log Icons	
	Allows you to truncate the system message log based on size, date, or message content. For more information, see Viewing the System Message Log in the chapter "Troubleshooting Your Cisco WAAS Network."

Cisco WAAS Central Manager Monitoring API

The Cisco WAAS Central Manager monitoring application programming interface (API), provides a programmable interface for system developers to integrate with customized or third-party monitoring and management applications. The Cisco WAAS Central Manager Monitoring API communicates with the Cisco WAAS Central Manager to retrieve status information and monitoring statistics.

The Cisco WAAS Central Manager Monitoring API is a Web Service implementation. Web Service is defined by the W3C standard as a software system designed to support interoperable machine-to-machine (client and server) interaction over the network. The client and server communication follows the Simple Object Access Protocol or Service Oriented Architecture Protocol (SOAP) standard.

Cisco WAAS CLI

The Cisco WAAS CLI allows you to configure, manage, and monitor WAEs on a per-device basis through a console connection or a terminal emulation program. The Cisco WAAS CLI also allows you to configure certain features that are supported only through the Cisco WAAS CLI (for example, configuring the Lightweight Directory Access Protocol [LDAP] signing on a WAE). We strongly recommend that you use the Cisco WAAS Central Manager GUI instead of the Cisco WAAS CLI, whenever possible.

Note You must wait for approximately 10 minutes (two data feed poll cycles) after registering a WAE with the Cisco WAAS Central Manager before making any CLI configuration changes on the WAE. Any CLI configuration changes made sooner may be overwritten when the Cisco WAAS Central Manager updates the WAE. We strongly recommend making all configuration changes by using the Cisco WAAS Central Manager GUI.

The Cisco WAAS CLI is organized into four command modes. Each command mode has its own set of commands to use for the configuration, maintenance, and monitoring of a WAE. The commands that are available to you depend on the mode you are in. When you enter a question mark (?) at the system prompt, you can obtain a list of commands available for each command mode.

The four Cisco WAAS command modes are as follows:

- EXEC mode: For setting, viewing, and testing system operations. This mode is divided into two access levels: user and privileged. To use the privileged access level, enter the **enable** command at the user access level prompt, then enter the privileged EXEC password when you see the password prompt.
- Global configuration mode: For setting, viewing, and testing the configuration of WAAS software features for the entire device. To use this mode, enter the **configure** command from the privileged EXEC mode.
- Interface configuration mode: For setting, viewing, and testing the configuration of a specific interface. To use this mode, enter the **interface** command from the global configuration mode.
- Feature-specific configuration mode: Some configuration modes are available from the global configuration mode for managing specific features.

For information about using the Cisco WAAS CLI to configure a Cisco WAAS device, see the *Cisco Wide Area Application Services Command Reference* and the *Cisco Wide Area Application Services Quick Configuration Guide*.

Benefits of Cisco WAAS

This section contains the following topics:

Preservation of Source TCP/IP Information

Many optimization products create tunnels through routers and other networking devices, which result in a loss of source TCP/IP information in the optimized data. This loss of TCP/IP information often disrupts important network services (such as QoS and NBAR), and can disrupt proper operation of traffic analysis tools such as NetFlow and security products and features such as ACLs and IP-based firewalls.

Unlike other optimization products, Cisco WAAS seamlessly integrates into your network and preserves all TCP/IP header information in the traffic that it optimizes, so that your existing analysis tools and security products are not compromised.

Autodiscovery of Cisco WAAS Devices

Cisco WAAS includes an autodiscovery feature that enables WAEs to automatically locate peer WAEs on your network. After autodiscovering a peer device, the WAEs can terminate and separate the LAN-to-WAN

TCP connections and add a buffering layer to resolve the differing speeds. Once a WAE establishes a connection to a peer WAE, the two devices can establish an optimized link for TCP traffic, or pass the traffic through as unoptimized.

The autodiscovery of peer Cisco WAAS devices is achieved using proprietary TCP options. These TCP options are only recognized and understood by Cisco WAAS devices and are ignored by non-Cisco-WAAS devices.

Centralized Network Monitoring and Management

Cisco WAAS Web-based management tools (Cisco WAAS Central Manager GUI) enable IT administrators to centrally define, monitor, and manage policies for each Cisco WAAS device, such as usage quota, backups, disaster recovery, restores, access control, and security policies. IT administrators can also perform the following tasks:

- Remotely provision, configure, and monitor each Cisco WAAS device or device group.
- Optimize system performance and utilization with comprehensive statistics, logs, and reporting.
- Perform troubleshooting tasks using tools such as SNMP-based monitoring, traps and alerts, and debug modes.

IT administrators benefit from the following features of Cisco WAAS:

- **Native protocol support**: Provides complete end-to-end support for the underlying file system protocol (Windows) used by the enterprise. Security, concurrency, and coherency are preserved between each client and file server.
- **Transparency**: Is fully transparent to applications, file systems, and protocols, enabling seamless integration with existing network infrastructures, including mixed environments. Cisco WAAS also has no impact on any security technology currently deployed.
- **Branch office data protection**: Increases data protection at branch offices. Its file cache appears on the office’s LAN in the same way as a local file server. End users can map their personal document folders onto the file cache using Windows or UNIX utilities. A cached copy of user data is stored locally in the branch WAE for fast access. The primary copy is stored centrally in the well-protected data center.
- **Centralized backup**: Consolidates data across the extended enterprise into a data center, which makes it easy to apply centralized storage management procedures to branch office data. Backup and restore operations become simpler, faster, and more reliable than when the data was decentralized.

In the event of data loss, backup files exist in the data center and can be quickly accessed for recovery purposes. The amount of data loss is reduced because of the increased frequency of backups performed on the centralized storage in the data center. This centralized storage backup makes disaster recovery much more efficient and economical than working with standalone file servers or NAS appliances.

- **Simplified storage management**: Migrates storage from remote locations to a central data facility, which reduces costs and simplifies storage management for the extended enterprise.
- **WAN adaptation**: Provides remote users with near-LAN access to files located at the data center. Cisco WAAS uses a proprietary protocol that optimizes the way traffic is forwarded between the WAEs.

Optimized Read and Write Caching

The common file services feature in Cisco WAAS maintains files locally, close to the clients. Changes made to files are immediately stored in the local branch WAE, and then streamed to the central file server. Files stored centrally appear as local files to branch users, which improves access performance. SMB caching includes the following features:

- Local metadata handling and caching: Allows metadata such as file attributes and directory information to be cached and served locally, optimizing user access.
- Partial file caching: Propagates only the segments of the file that have been updated on write requests rather than the entire file.
- Write-back caching: Facilitates efficient write operations by allowing the data center WAE to buffer writes from the branch WAE and to stream updates asynchronously to the file server without risking data integrity.
- Advance file read: Increases performance by allowing a WAE to read the file in advance of user requests when an application is conducting a sequential file read.
- Negative caching: Allows a WAE to store information about missing files to reduce round-trips across the WAN.
- Microsoft Remote Procedure Call (MSRPC) optimization: Uses local request and response caching to reduce the round-trips across the WAN.
- Signaling messages prediction and reduction: Uses algorithms that reduce round-trips over the WAN without loss of semantics.

WCCP Support

The Web Cache Communication Protocol (WCCP) developed by Cisco Systems specifies interactions between one or more routers (or Layer 3 switches) and one or more application appliances, web caches, and caches of other application protocols. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic flowing through a group of routers. The selected traffic is redirected to a group of appliances. Any type of TCP traffic can be redirected.

The WCCP v2 protocol has a built-in set of beneficial features, for example, automatic failover and load balancing. The router monitors the liveness of each WAE attached to it through the WCCP keepalive messages, and if a WAE goes down, the router stops redirecting packets to the WAE. By using WCCP, the branch WAE avoids becoming a single point of failure. The router can also load balance the traffic among a number of branch WAEs.

Cisco WAAS supports transparent interception of TCP sessions through WCCP. After WCCP is turned on at both the router and the branch WAE, only new sessions are intercepted. Existing sessions are not affected.

PBR Support

Policy-based routing (PBR) allows IT organizations to configure their network devices (a router or a Layer 4 to Layer 6 switch) to selectively route traffic to the next hop based on the classification of the traffic. Cisco WAAS administrators can use PBR to transparently integrate a WAE into their existing branch office network and data centers. PBR can be used to establish a route that goes through a WAE for some or all packets based on the defined policies.

For more information about PBR, see the chapter Configuring Traffic Interception, on page 127.

Inline Interception Support

Direct inline traffic interception is supported on WAEs with a Cisco WAE Inline Network Adapter or Interface Module installed. Inline interception of traffic simplifies deployment and avoids the complexity of configuring WCCP or PBR on the routers.

An inline WAE transparently intercepts traffic flowing through it or bridges traffic that does not need to be optimized. It also uses a mechanical fail-safe design that automatically bridges traffic if a power, hardware, or unrecoverable software failure occurs.

Note AppNav Controller Interface Modules do not support automatic bypass mode to continue traffic flow in the event of a failure. For high availability, two or more AppNav Controller Interface Modules should be deployed in an AppNav cluster. For more information on using inline mode with the AppNav solution, see the chapter Configuring Cisco AppNav, on page 67.

You can configure the inline WAE to accept traffic only from certain VLANs; for all other VLANs, traffic is bridged and not processed.

You can serially cluster inline WAE devices to provide higher availability in the event of a device failure. If the current optimizing device fails, the second inline WAE device in the cluster provides the optimization services. Deploying WAE devices in a serial inline cluster for the purposes of scaling or load balancing is not supported.

For more information about inline mode, see Using Inline Mode Interception in the chapter "Configuring Traffic Interception."

Failure Resiliency and Protection

Cisco WAAS provides a high-availability failover (and load-balancing) function that minimizes the probability and duration of SMB downtime.

If a WAE configured for SMB fails, all peer WAEs configured to operate with it are redirected to work with an alternate WAE. This operation maintains high availability without service interruption.

This change may not be transparent to users, which means that client connections are closed and require SMB clients to reestablish their connection. Whether such changes impact currently running applications depends on the behavior of the application being used, and on the behavior of the specific SMB client. Typically, however, the transition is transparent to the client.

RAID Compatibility

Cisco WAAS provides the following Redundant Array of Independent Disks (RAID) capability for increased storage capacity or increased reliability:

- Logical Disk Handling with RAID-5–Logical disk handling with Redundant Array of Independent Disks-5 (RAID-5) is implemented in Cisco WAAS as a hardware feature. RAID-5 devices can create a single logical disk drive that may contain up to six physical hard disk drives, providing increased logical disk capacity.

Systems with RAID-5 can continue operating if one of the physical drives fails or goes offline.

Note RAID Controller Firmware 12.12.0(0060) or later version is required for Toshiba SSD to work on Cisco WAVE 8541 model. Else it is unable to create a RAID.

- Logical Disk Handling with RAID-1: Logical disk handling with RAID-1 is implemented in Cisco WAAS as a software feature. RAID-1 uses disk mirroring to write data redundantly to two or more drives, providing increased reliability. Because the software must perform each disk write operation against two disk drives, the filesystem **write** performance may be affected.

- Disk Hot-Swap Support: Cisco WAAS for RAID-1 allows you to hot-swap the disk hardware. RAID-5 also allows you to hot-swap the disk hardware after the RAID array is shut down. For the disk removal and replacement procedures for RAID systems, see the Chapter Maintaining Your Cisco WAAS System, on page 513.

Streamlined Security

Cisco WAAS supports disk encryption, which addresses the need to securely protect sensitive information that flows through deployed Cisco WAAS systems and that is stored in WAAS persistent storage.

Cisco WAAS does not introduce any additional maintenance overhead on already overburdened IT staffs. Cisco WAAS avoids adding its own proprietary user management layer, and instead makes use of the users, user credentials, and access control lists maintained by the file servers. All security-related protocol commands are delegated directly to the source file servers and the source domain controllers. Any user recognized on the domain and source file server are automatically recognized by Cisco WAAS with the same security level, and all without additional configuration or management.

Cisco WAAS delegates access control and authentication decisions to the origin file server.

SNMP Support

Cisco WAAS supports Simple Network Management Protocol (SNMP) including SNMPv1, SNMPv2, and SNMPv3. Cisco WAAS supports many of the most commonly used SNMP managers, such as HP OpenView and IBM Tivoli NetView.

Most Cisco WAAS traps are also recorded in the logs displayed in the Cisco WAAS Central Manager GUI, although some (such as exceeding the maximum number of sessions) are reported only to the SNMP manager.

Cisco WAAS supports parameters based on SNMPv2, enabling it to integrate into a common SNMP management system. These parameters enable system administrators to monitor the current state of the Cisco WAAS network and its level of performance.

Exported parameters are divided into the following categories:

- General parameters: Includes the version and build numbers and license information.

- Management parameters: Includes the location of the Cisco WAAS Central Manager.

- Data center WAE parameters: Includes the general parameters, network connectivity parameters, and file servers being exported.

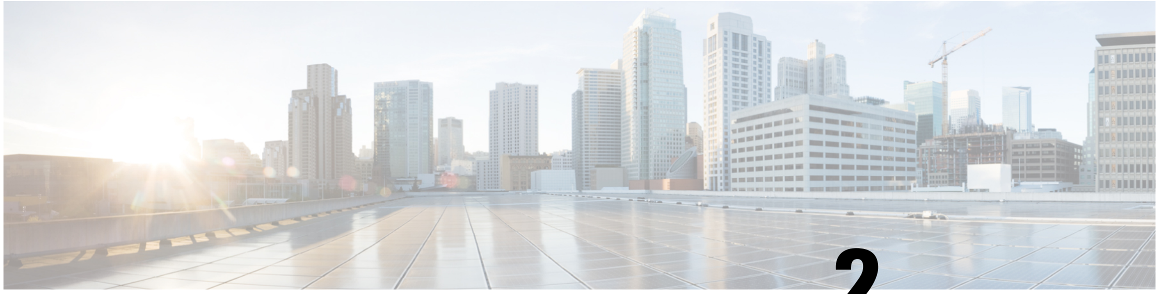
- Branch WAE parameters: Includes the general parameters, network connectivity parameters, and cache statistics.

For more information about SNMP and supported MIBs, see the chapter Configuring SNMP Monitoring, on page 647.

IPv6 Support

For Cisco WAAS Version 6.0 and later, IPv6 support is implemented for management access to Cisco WAAS devices. Basic IPv6 connectivity can be enabled on the Cisco WAAS interfaces by assigning IPv6 addresses, configuring default gateway and static IP routes. This can be further enhanced by configuring support for AAAA record types in the Domain Name System (DNS) name-to-address and address-to-name lookup processes and by managing IPv6 neighbour discovery

All devices in the Cisco WAAS network can communicate in the IPv6 network using Telnet, SSH, FTP, TFTP, in IPv6 addresses. The management plane can configure IPv6 address for **syslog**, AAA servers, NTP servers, SNMP servers and name servers to communicate with Cisco WAAS devices.



CHAPTER 2

Planning Your Cisco WAAS Network

This chapter describes general guidelines, restrictions, and limitations that you should be aware of before you set up your Cisco Wide Area Application Services (Cisco WAAS) network.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco WAAS Central Managers and Cisco Wide Area Application Engines (Cisco WAEs) in your network. The term WAE refers to Cisco WAE and Cisco Wide Area Virtual Engine (Cisco WAVE) appliances, and Cisco Virtual WAAS (Cisco vWAAS) instances.

This chapter contains the following sections:

Checklist for Planning Your Cisco WAAS Network

This section contains the following topics:

Network Topologies

Cisco Wide Area Application Engines (Cisco WAEs) that are running the Cisco WAAS software can be used by enterprises or service providers to optimize the application traffic flows between their branch offices and data centers. You should deploy WAE nodes at the WAN endpoints near the networked application clients and their servers, where they intercept WAN-bounded application traffic and optimize it. You must insert WAE nodes into the network flow at defined processing points.

Cisco WAAS software supports the following three typical network topologies:

- **Hub and spoke deployments**: In a hub and spoke deployment, servers are centralized, and branch offices host clients and a few local services only, for example, Cisco WAAS printing services.
- **Mesh deployments**: In a mesh deployment, a location can host both clients and servers, and the clients can access any number of local or remote servers.
- **Hierarchical deployments**: In a hierarchical deployment, servers are located in multiple regional and national data centers, and can be accessed by different clients. The connections between the data centers are of higher bandwidth than the connections to the branch offices.

The deployments are characterized according to the Cisco WAAS element connections, which follow the client-server access pattern and may differ from the physical network links. For more information, see the chapter "Introduction to Cisco WAAS."

Planning Checklist

When you are planning your Cisco WAAS network, use the following checklist as a guideline. As the following checklist indicates, you can break the planning phase into the following three main categories of planning activities:

- Sizing phase
- Planning for management
- Planning for application optimization

Note Although there are some interdependencies, you do not have to complete all of the steps in a particular planning phase before you start the next step.

To plan your network, follow these guidelines:

1. Complete the sizing phase that includes the following tasks:
    - Determine which locations in your existing network require Cisco WAAS optimization, for example, branch offices and data centers.
    - Determine if you are going to use a traditional Cisco WAAS deployment model or the AppNav deployment model. For more information on AppNav, see the chapter Configuring Cisco AppNav, on page 67.
    - Determine the number and models of the Cisco WAAS devices that are required for each location. Some key factors in this selection process is the WAN bandwidth, the number of users, and the expected use. Various hardware configurations are possible, for example, different hard disk models and RAM size. Consider running a cluster of WAEs where additional scalability and or failover is required. For more information, see Calculating the Number of Cisco WAAS Devices Required, on page 41
    - Verify that you have purchased sufficient licenses to cover your requirements.
2. Plan for management as follows:

- Complete site and network planning, for example, obtain the IP and routing information, including IP addresses and subnets, routers and default gateway IP addresses, and hostnames for devices. See the "Checklist of Cisco WAAS Network System Parameters" table in the *Cisco Wide Area Application Services Quick Configuration Guide*.

- Determine the login authentication and login authorization methods, for example, external RADIUS, TACACS+, Windows domain servers, and accounting policies that you want your Cisco WAAS Central Managers and WAEs to use. For more information, see the chapter .

- For security purposes, plan to change the predefined password for Configuring Administrative Login Authentication, Authorization, and Accounting, on page 219the predefined superuser account immediately after you have completed the initial configuration of a WAE. For more information, see Cisco WAAS Login Authentication and Authorization, on page 49.

- Determine if you need to create any additional administrative accounts for a Cisco WAAS device. For more information, see the chapter Creating and Managing Administrator User Accounts and Groups, on page 255

- Determine if you should group your WAEs into logical groups. For more information, see Logically Grouping Your WAEs, on page 50.

- Determine which management access method to use. By default, Telnet is used, but SSH may be the preferred method in certain deployments. For more information, see Configuring Login Access Control Settings for Cisco WAAS Devices in the chapter "Configuring Administrative Login Authentication, Authorization, and Accounting."

3. **3.** Plan for application optimization as follows:

   - Determine and resolve router interoperability issues, for example, the supported hardware and software versions, router performance with interception enabled. For more information, see Site and Network Planning, on page 26

   - Determine the appropriate interception location when the data center or branch office is complex, for example, if your existing network uses a hierarchical topology.

   - Determine which Cisco WAAS services to deploy. For more information about the different Cisco WAAS services, see the chapter "Introduction to Cisco WAAS."

   - Determine which Cisco WAAS software licenses to install. Software licenses enable specific Cisco WAAS services. For more information about installing software licenses, see the Managing Cisco WAAS Software Licenses, on page 291 in the chapter "Configuring Other System Settings."

   - Determine which traffic interception methods to use in your Cisco WAAS network, for example, AppNav, inline mode, WCCP Version 2, or policy-based routing (PBR).

   - For more information on the advantages and disadvantages of using WCCP, see Supported Methods of Traffic Redirection, on page 42

   - For more information on WCCP traffic interception and redirection, see About Traffic Interception Methods in the chapter "Configuring Traffic Interception."

   Note WCCP works only with IPv4 networks.

- If you plan to use the WCCP TCP promiscuous mode service as a traffic interception method, determine whether you should use IP Access Control Lists (ACLs) on your routers.

Note IP ACLs that are defined on a router take precedence over the ACLs that are defined on the WAE. For more information, see Access Lists on Routers and WAEs, on page 48.

- Determine whether you have to define IP ACLs or interception ACLs on the WAEs. For more information, see Access Lists on Routers and WAEs, on page 48

Note ACLs that are defined on a WAE take precedence over the Cisco WAAS application definition policies that are defined on the WAE.

- If PBR is to be used, determine which PBR method to use to verify PBR next-hop availability for your WAEs. For more information, see Methods of Verifying PBR Next-Hop Availability in the chapter "Configuring Traffic Interception."
- Determine the major applications for your Cisco WAAS network. Verify whether the predefined application definition policies cover these applications and whether you should add policies if your applications are not covered by these predefined policies. For a list of the predefined application definition policies, see Appendix A, Predefined Optimization Policy, on page 697.
- Consider day zero migration of file systems if file servers are to be centralized in the process. For more information, see Data Migration Process, on page 51

After you complete the planning tasks, you are ready to perform a basic configuration of a Cisco WAAS network, as described in the Cisco Wide Area Application Services Quick Configuration Guide.

Site and Network Planning

This section contains the following topics:

About Site and Network Planning

Before you install and deploy Cisco WAAS devices in your network, collect information about your network to accommodate the integration of the Cisco WAAS devices.

In a typical distributed organizational layout, there are two types of networks where Cisco WAAS devices are installed:

- The data center (central office): One or more colocated data center WAEs provide access to the resident file and application servers. In data centers, you can deploy a WAE as a single device or a pair of WAEs as a high-availability or load-sharing pair. High availability pairs are supported if either WCCP Version 2 or PBR is being used for traffic redirection to the data center; load-sharing pairs are supported only if WCCP Version 2 is being used for traffic redirection to the data center.

- The branch offices: Branch WAEs enable users to access the file and application servers over the WAN. In branch offices, you can deploy a WAE as a single device or a pair of WAEs as a high-availability or load-sharing pairs. High-availability pairs are supported if either WCCP Version 2 or PBR is being used for traffic redirection in the branch office; load-sharing pairs are only supported if WCCP Version 2 is being used for traffic redirection in the branch office.

In collaborative networks, colocated data center WAEs and branch WAEs are deployed throughout the network. These colocated WAEs are configured to share data in opposite directions (two cross-linked servers).

The WAE attaches to the LAN as an appliance. A WAE relies on packet interception and redirection to enable application acceleration and WAN optimization. Consequently, traffic interception and redirection to a WAE must occur at each site where a WAE is deployed. Traffic interception and redirection occurs in both directions of the packet flow. Because Layer 3 and Layer 4 headers are preserved, you should ensure that you always connect a WAE to a tertiary interface (or a subinterface) on the router to avoid routing loops between the WAE and the WCCP or PBR-enabled router that is redirecting traffic to it. For more information on this topic, see Using Tertiary Interfaces or Subinterfaces to Connect WAEs to Routers, on page 47.

Note We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices because half duplex impedes performance. Check each Cisco WAE interface and port configuration on the adjacent device (router, switch, firewall, or WAE) to verify that full duplex is configured.

Note The data center WAE and branch WAE communicate with each other only if the firewall is open.

Microsoft Windows Network Integration

To successfully integrate Cisco WAAS devices into the Microsoft Windows environment, you may have to perform certain tasks on both the data center WAE and branch WAE sides of the Cisco WAAS network. This section contains the following topics:

Data Center WAE Integration

Before the initial configuration of the data center WAE, verify the following parameters:

- WINS server (if applicable).
- DNS server and DNS domain (if applicable).
- A browsing user with file-server directory traversal (read-only) privileges. This user, who is usually set up as a domain or service user, is required for running preposition policies.

To successfully integrate Cisco WAAS into the Microsoft Windows environment on the data center WAE side of a network where DHCP is not being used, you must manually add the name and IP address of the data center WAE to the DNS server. You should take this action before installing and deploying the Cisco WAAS devices.

Note User permissions are determined by the existing security infrastructure.

Branch WAE Integration

Before the initial configuration of the branch WAE, verify the following parameters:

- DNS server and DNS domain
- Windows Domain Name
- WINS server (if applicable)

To successfully integrate Cisco WAAS into the Microsoft Windows environment on the branch WAE side of the network, you should take the following preliminary actions before installing and deploying the Cisco WAAS devices in your network:

- To enable all branch WAEs in the specified domain to appear in the **Network Neighborhood** of users within the same domain, ensure that a **Domain Primary Browser** or **local Primary Browser** is active.
- If DHCP is not used, you must manually add the name and IP address of the branch WAE to the DNS server.

UNIX Network Integration

Before the initial configuration of a Cisco WAAS device, verify the following parameters:

- DNS server and DNS domain.
- NIS server parameters (if applicable).
- On the data center WAE side, a browsing UID or GID with file-server directory traversal (read-only) privileges. This UID or GID, which is usually set up as a domain or service user, is required for browsing when defining coherency policies.

To successfully integrate Cisco WAAS into the UNIX environment, you should perform these actions on both the data center WAE and branch WAE sides of the network:

- Manually add the name and IP address of both the data center WAE and the branch WAE to the DNS server.
- When separate domains are used, UNIX users may be defined at the remote (branch) offices or on the central servers. This situation may result in the same user name being defined in different domains. A user may be defined differently in the branch and center or may be defined only on one end and not on the other. You can ensure consistency in such cases by using NIS or by mapping between the different domains, either manually or automatically. That is, users can be mapped from the remote server to the central servers by translating their identities from the central office to the remote offices.

Note To map users using automatic management, you must first configure the NIS server in both the data center WAE (primary) and branch WAE (secondary).

SMB-Related Ports in a Cisco WAAS Environment

SMB-related ports used betwwen your clients are Cisco WAEs that are accelerating SMB traffic, and SMB file servers. Most SMB communication occurs between the branches and the central office. This communication is encrypted and delivered through the organization's VPN. No ports on the firewall have to be opened because all communication is tunneled internally.

You only have to change the firewall setup if administrative or other maintenance work has to be done from a location outside the organization.

Here are two sets of SMB-related ports used with Cisco WAAS: ports 139 and 445 to connect clients to a branch WAE, and ports 88 and 464 to authenticate clients with the domain controller.

- **Ports 139 and 445**: If you have deployed SMB acceleration services in your Cisco WAAS network, your Cisco WAAS network uses ports 139 and 445 to connect clients to a branch WAE and to connect a data center WAE to the associated file servers. The port that is used depends on the configuration of your Cisco WAAS network.

  If WCCP is enabled or inline mode is used, the branch WAE accepts client connections on ports 139 or 445. If WCCP or inline is not enabled, the branch WAE accepts connections only over port 139.

  Your Cisco WAAS network always tries to use the same port to communicate end-to-end. Consequently, if a client uses port 445 to connect to a branch WAE, the associated data center WAE will try to use the same port to connect to the file server. If port 445 is unavailable, the data center WAE will try to use port 139.

  Some organizations close port 139 on their networks to minimize the security risks associated with this port. If your organization has closed port 139 for security reasons, you can configure your Cisco WAAS network to bypass port 139.

  To bypass port 139 and use port 445 in its place if you use the SMB application accelerator, running on CIFS policy, for these ports: Enable WCCP Version 2 on your routers and branch WAE, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*. Alternatively, you can use inline mode on a branch WAE with a Cisco WAE Inline Network Adapter or Cisco Interface Module installed.

  Note The CIFS application accelerator is removed from Cisco WAAS Version 6.0 and later, but the CIFS policy is continued for two ports: port 139 and port 445. For these ports only, the SMB application accelerator runs on CIFS policy. Therefore, an alarm generated by SMB on port 139 or port 445 is seen as a CIFS alarm.

- **Ports 88 and 464**: If you are using Windows Domain authentication with Kerberos enabled, the WAE uses ports 88 and 464 to authenticate clients with the domain controller.

Firewalls and Standby Cisco WAAS Central Managers

Primary and standby Cisco WAAS Central Managers communicate on port 8443. If your network includes a firewall between primary and standby Cisco WAAS Central Managers, you must configure the firewall to allow traffic on port 8443 so that the Cisco WAAS Central Managers can communicate and stay synchronized.

Performance Tuning for High WAN Bandwidth Branch Offices

Cisco WAAS combines Layer 4 TCP optimizations with Layer 7 application accelerators for various protocols. For some branch offices with high WAN bandwidth, for example, above 50 Mbps, if the native latency is low, for example, below 20 ms RTT, depending on the number of user sessions and data patterns, applying Layer 4 optimizations alone may provide optimal levels of performance. In such cases, we recommend that you measure end-user response times under production load to determine the appropriate operational state for the application accelerators and sizing.

Autoregistration and WAEs

This section contains the following topics:

About Autoregistration and WAEs

Autoregistration automatically configures primary network settings and registers a WAE with the Cisco WAAS Central Manager device. On startup, a Cisco WAAS device (except for the Cisco WAAS Central Manager) that does not have an existing network configuration on its primary interface can automatically discover the Cisco WAAS Central Manager device and register with it. You do not have to manually configure the network settings of the primary interface on the Cisco WAAS device. This feature is useful for large-scale automated deployments of devices. After a WAE is registered, configure other interfaces and settings on the device remotely by using the Cisco WAAS Central Manager GUI.

In the example configuration provided in the *Cisco Wide Area Application Services Quick Configuration Guide*, the autoregistration feature is disabled on the WAEs when the setup utility is used to perform the initial configuration of the device and manually configure the interface settings.

Autoregistration and DHCP

Autoregistration uses a form of the Dynamic Host Configuration Protocol (DHCP). For autoregistration to function, you must have a DHCP server that is configured with basic settings.

Note The WAE sends CISCOCDN as the vendor-class identifier in option 60 of the DHCP DISCOVER message to facilitate your grouping of WAEs into device groups.

Autoregistration DHCP requires that the following options be present in the DHCP server's offer:

- Subnet mask **(Option 1)**
- Router (default gateway) **(Option 3)**
- Domain name **(Option 15)**
- Domain name servers **(Option 6)**

Additionally, the DHCP offer can contain the WAE hostname (**Option 12**), but it is not required. If the hostname option is not supplied, the WAE hostname is automatically set to NO-HOSTNAME-*a.b.c.d* , where *a.b.c.d* is the IP address that is assigned to the WAE by the DHCP server.

All of the above options, with the exception of domain name servers (**Option 6**), replace the existing configuration on the system. The domain name servers option is added to the existing list of name servers with a restriction of a maximum of eight name servers.

After the WAE configures its network settings from DHCP, it requires the Cisco WAAS Central Manager hostname so that it can register with the Cisco WAAS Central Manager. The WAE queries the configured DNS server to obtain the Cisco WAAS Central Manager hostname. For autoregistration to work, you must configure the DNS server with the Cisco WAAS Central Manager hostname by configuring a DNS SRV (Service Location) record. This record is easy to configure and does not affect normal DNS operation. The DNS SRV record must be configured as follows:

- Service is **_waascms**.
- Protocol is **_tcp**.
- Host offering this service is the Fully Qualified Domain Name (FQDN) of the Cisco WAAS Central Manager.

To create an SRV record in Windows Server 2008, open the DNS Manager, navigate to **Forward Lookup Zones**, and select the correct DNS zone. Right click the zone, choose **Other New Records** and then choose **Service Location (SRV)**.

If the DNS request fails or if the domain is not configured, the WAE tries an alternative DNS query for an SRV record to the ciscowaas.local domain. If this alternative request also fails, the WAE cannot register with the Cisco WAAS Central Manager. However, the network configuration remains and allows you to connect through Telnet to perform additional configuration from the Cisco WAAS CLI.

Autoregistration is enabled by default on the first interface of the device. On a Cisco NME-WAE module, autoregistration is enabled on the configured interface. On an SRE-SM module (for Cisco WAAS versions earlier than 6.4.x), autoregistration is disabled by default.

Note You must disable autoregistration when both device interfaces are configured as port-channel interfaces.

If you do not have a DHCP server, the device is unable to complete autoregistration and eventually times out. You can disable autoregistration at any time after the device has booted, and proceed with manual setup and registration.

To disable autoregistration, or to configure autoregistration on a different interface, use the **no auto-register enable** global configuration command. If you want to preserve the dynamically configured IP address on the interface as a static IP address when you disable autoregistration, use the **preserve-ip** command option. This option prevents the WAE from losing network connectivity because its IP address has been removed.

Note Autoregistration is automatically disabled if a static IP address is configured or if you configure interface-level DHCP on the same interface that autoregistration uses. (See Selecting Static IP Addresses or Using Interface-Level DHCP, on page 32.)

The following example shows how to disable autoregistration on the interface GigabitEthernet 1/0:

```
WAE(config)# no auto-register enable GigabitEthernet 1/0 preserve-ip
```

Autoregistration status can be obtained by using the following **show** EXEC command:

```
WAE# show auto-register
```

For Cisco WAAS Release 6.0 and later, autoregistration is possible for a dual-stack Cisco WAAS device. In a dual-stack network, the Cisco WAAS device should be able to get a IPv6 DHCP address and an IPv6 Cisco WAAS Central Manager address through DNS entry or in the DHCP pool and then register with the Cisco WAAS Central Manager using IPv6. If IPv6 DHCP fails and IPv4 is also configured on the auto-registration interface, then the device should fall back to getting IPv4 address and proceed as it would in a IPv4-only network.

Selecting Static IP Addresses or Using Interface-Level DHCP

During the initial configuration, you have the option of configuring a static IP address for the device or choosing DHCP.

DHCP is a communications protocol that allows network administrators to manage their networks centrally and automate the assignment of IP addresses in an organization’s network. When an organization sets up its computer users with a connection to the network, an IP address must be assigned to each device. Without DHCP, the IP address must be entered manually for each computer, and if computers move to another location in another part of the network, the IP address must be changed accordingly. DHCP automatically sends a new IP address when a computer is connected to a different site in the network.

If you have a DHCP server configured, autoregistration automatically configures the network settings and registers WAEs with the Cisco WAAS Central Manager device upon bootup.

If you do not have a DHCP server configured, or you have a DCHP server, but do not want to use the autoregistration feature, manually configure the following network settings with the interactive setup utility or Cisco WAAS CLI, and then register the WAEs with the Cisco WAAS Central Manager. Configure these settings:

- Interface IP address and subnet mask
- IP domain name
- Hostname
- IP name server
- Default gateway
- Primary interface

When a Cisco WAAS device boots, you are prompted to run the first-time setup utility (enter basic configuration), which you use to set up the basic device network settings for the WAE.

Interoperability and Support

This section describes Cisco WAAS interoperability with and support for how to identify and resolve interoperability issues. It contains the following topics:

Unicode Support for Cisco WAAS GUI Interfaces

The Cisco WAAS software supports Unicode in the Cisco WAAS Central Manager and the Cisco WAE Device Manager GUI interfaces.

- In the Cisco WAAS Central Manager, you can create preposition policies that include Unicode characters. For example, you can define a preposition policy for a directory that contains Unicode characters in its name.

  Specifically, the root directory and file pattern fields in the preposition policies in the Cisco WAAS Central Manager GUI support Unicode.

- In the Cisco WAE Device Manager GUI, you can include Unicode characters in the name of the backup configuration file. In addition, the logs included in the Cisco WAE Device Manager GUI can display Unicode characters.

Note the following about Unicode support limitations:

- Usernames cannot contain Unicode characters.
- When defining policies for coherency, and so on, you cannot use Unicode characters in the Description field.
- File server names cannot contain Unicode characters.

For a list of the hardware, SMB clients, and web browsers supported by the Cisco WAAS software, see the Release Note for Cisco Wide Area Application Services.

Cisco WAAS and Cisco IOS Interoperability

This section contains the following topics about the interoperability of the Cisco WAAS software with the Cisco IOS features for a basic Cisco WAAS deployment that uses WCCP-based interception and transparent transport:

Note The Cisco WAAS software does not support Mobile IP.

We recommend that you use Cisco IOS Software Release 12.2 or later.

Cisco WAAS and the Cisco IOS QoS Classification Feature

Classify packets by using a policy filter, for example, QPM, which is defined on the packets. You can use the following policy filter properties:

- Source IP address or hostname: Supported by Cisco WAAS because the source IP address is preserved by the Cisco WAAS device.
- Source TCP/UDP port (or port range): Supported by Cisco WAAS because the source port is preserved by the Cisco WAAS device.
- Destination IP address or hostname: Supported by Cisco WAAS because the destination IP is preserved by Cisco WAAS. Cisco WAAS relies on interception at the data center for redirecting traffic to the peer Cisco WAAS device.
- Destination TCP/UDP port (or port range): Supported by Cisco WAAS because the destination IP is preserved by Cisco WAAS. Cisco WAAS relies on interception at the data center for redirecting traffic to the peer Cisco WAAS device.

- DSCP/IP precedence (TOS): Supported by Cisco WAAS because Cisco WAAS copies the settings of incoming packets on to the outgoing packets from Cisco WAAS back to the router. If the packets are not colored at connection establishment time (for TCP packets), there might be a delay in propagating the settings because Cisco WAAS does not poll these settings periodically. The packets are eventually colored properly. When packets are not colored, they are left uncolored by the Cisco WAAS software.

Note Cisco WAAS software does not support QoS, MPLS QoS, ATM QoS, Frame Relay QoS, and Layer 2 (VLAN) QoS.

Cisco WAAS and the Cisco IOS NBAR Feature

Unlike a traditional type of classification that is specified through a policy filter, as listed in Cisco WAAS and the Cisco IOS QoS Classification Feature, on page 33, Network-Based Application Recognition (NBAR) classification needs to consider payload. The classification keeps track of any interceptor that modifies the payload because this modification might cause NBAR to not be able to classify the packets. However, the Cisco WAAS software does support NBAR.

The following is an example flow of how the Cisco WAAS software supports NBAR:

1. A packet, P1, which is a part of a TCP stream, S1, enters the router and is classified by NBAR on the LAN interface of the router as belonging to class C1. If the classification of P1 does not involve payload inspection, for example, only TCP/IP headers, no action is to be taken because the Cisco WAAS software preserves this information.

2. If P1 classification requires payload inspection, P1 should be marked using the TOS/DSCP bits in the packet (as opposed to using other internal marking mechanisms).

3. P1 is then intercepted through WCCP Version 2 (still on the LAN interface, WCCP is processed after NBAR) and is redirected to a WAE.

4. Cisco WAAS applies optimizations, if any, on the payload and copies the DCSP bits settings from the incoming TCP stream, S1, onto the outgoing stream, S2 (which is established between the local Cisco WAAS appliance and the remote Cisco WAAS appliance over the WAN). Because NBAR usually has to see some payload before performing the classification, it is unlikely that Cisco WAAS will have the proper bit settings at connection-establishment time. Consequently, the Cisco WAAS software uses polling to inspect the DSCP bits on the incoming TCP stream, and then copies it over to the stream from the Cisco WAAS device back to the router.

5. When S2 re-enters the router, NBAR will not classify S2 as belonging to C1 because the payload has been changed or compressed. However, the DSCP settings have already marked these packets as belonging to C1. Consequently, these packets will be treated appropriately as if they were classified through NBAR.

   As long as the flow is not identified, NBAR will continue to search for classification in the packets. Because compressed packets will not be classified, this situation can unnecessarily burden the CPU (performing packet inspection). Because of the potential degradation in performance and the slight possibility of correctness issues, we strongly recommend that you use a subinterface or a separate physical interface to connect the WAE to the router (as described in Using Tertiary Interfaces or Subinterfaces to Connect WAEs to Routers, on page 47). When you use a tertiary interface or subinterface to connect the WAE to the router, both the performance and correctness issues are addressed because each packet is processed only once.

6. For dynamic classifications, NBAR maintains a per-flow state. After certain flows are classified, NBAR does not continue to perform deep-packet inspection anymore. However, for other flows, for example, Citrix, NBAR does look at packets continuously because the classification may change dynamically in a flow. Therefore, in order to support all NBAR classifications, it is not sufficient to only poll the DSCP settings of packets coming in to Cisco WAAS once per flow; you should also poll periodically to identify flow changes. However, the Cisco WAAS system expects packets to appear in the sequence of packets belonging to the class C1, followed by a sequence of C2, and so forth, so that a polling method is sufficient to track such dynamic changes.

Note This dynamic classification support requires support for marking DSCP/ToS settings, as specified in Cisco WAAS and the Cisco IOS QoS Classification Feature, on page 33, as well as the tracking of dynamic changes through polling.

Several router configurations should be followed in order to ensure NBAR-Cisco WAAS compliance, and you must ensure that the following router configurations are adhered to:

- Ensure that classification is followed by proper DSCP marking.
- Ensure that the router in general (IP access lists that are configured on the router) does not scrub DSCP/TOS settings that are already marked on the packets on entry, and that NBAR does not unmark marked packets.

Cisco WAAS and Cisco IOS Marking

The Cisco IOS marking feature is supported by the Cisco WAAS software.

Cisco WAAS and Cisco IOS Queuing

The Cisco IOS queuing feature for congestion management is supported by the Cisco WAAS software.

Cisco WAAS and Cisco IOS Congestion Avoidance

The Cisco IOS congestion avoidance feature is supported by the Cisco WAAS software.

Cisco WAAS and Cisco IOS Traffic Policing and Rate Limiting

The Cisco IOS traffic policing and rate-limiting feature is only partially supported by the Cisco WAAS software. This Cisco IOS feature will work properly when enabled on an outbound interface. However, when this feature is enabled on an inbound interface, it will see both compressed and uncompressed traffic, and will result in inaccurate rate limiting.

Cisco WAAS and Cisco IOS Signaling

The Cisco IOS signaling (RSVP) feature is typically implemented in Multiprotocol Label Switching (MPLS) networks. Because the Cisco WAAS software does not interact with MPLS RSVP messages, the RSVP feature is supported.

Cisco WAAS and Cisco IOS Link-Efficiency Operations

The Cisco IOS link-efficiency operations are supported by the Cisco WAAS software.

Cisco WAAS and Cisco IOS Provisioning, Monitoring, and Management

The Cisco IOS AutoQoS feature is supported by the Cisco WAAS software, but requires additional configuration. This feature is closely connected with NBAR support because the AutoQoS feature uses NBAR to discover the various flows on the network. However, because the Cisco IOS AutoQoS feature is strictly on an outbound feature, for example, it cannot be enabled on the inbound side of an interface, this situation could create a potential problem because enabling NBAR on the outbound interface is not supported.

To avoid this potential problem, enable the trust option of the AutoQoS feature on the following interfaces so that classification and queuing are performed based on the marked value (NBAR is not enabled on the outbound interface using this solution):

- On the LAN interface on which the input policy is created and on which the marking of the packets should be performed according to the AutoQoS marking, for example, interactive video mark to **af41**.
- On the WAN outbound interface.

Cisco WAAS and Management Instrumentation

For management instrumentation use with the Cisco WAAS software, consider the following guidelines:

- When deployed in native (transparent) mode, Cisco WAAS maintains packet header information vital to technologies, such as NetFlow. NetFlow can be configured on adjacent devices and exports flow record information in accordance with where NetFlow is configured in relation to the Cisco WAAS device. For NetFlow configurations on the LAN side of a Cisco WAAS device, NetFlow exports records containing information about original flows. For NetFlow configurations on the WAN side of a Cisco WAAS device, NetFlow exports records containing information about optimized and pass-through flows.
- You may see statistics on optimized and unoptimized traffic.
- IP Service-Level Agreements (SLAs) are supported.
- Full support of policies based on Layer 3 and Layer 4 is provided. Policies based on Layer 7 are partially supported because the first few messages are unoptimized.
- Intrusion Detection System (IDS) is partially supported. The first few messages are unoptimized to allow IDS to detect intrusive strings.
- Cisco IOS security is partially supported with the exception of features that rely on Layer 5 and above visibility.
- IPsec and SSL VPN are supported.
- ACLs are supported. IP ACLs on the router take precedence over ACLs that are defined on the WAE. For more information, see Access Lists on Routers and WAEs.
- VPN is supported if the VPN is deployed after WCCP interception occurs.

Note A Cisco WAAS device does not encrypt WAN traffic. If you require additional security measures, you should use a VPN. However, the VPN appliances must encrypt and decrypt traffic after and before the Cisco WAAS devices so that the Cisco WAAS device sees only unencrypted traffic. The Cisco WAAS device is unable to compress encrypted traffic and provides only limited TCP optimization to it.

- Network Address Translation (NAT) is supported. However, payload-based NAT is not supported.

Cisco WAAS and MPLS

MPLS is partially supported by the Cisco WAAS software. WCCP does not know how to operate with packets that are tagged with MPLS labels. Consequently, inside the cloud, WCCP redirection will not function, for example, WCCP redirection will not work for intermediate WAEs. However, as long as redirection occurs on interfaces that are outside the MPLS cloud, Cisco WAAS is supported.

Cisco WAAS Application Accelerators Interoperability with Third-Party Load Balancers

A load balancer is used to balance network and application traffic across a set of servers. The resulting evenly-distributed traffic improves the response rate of network traffic, increases the availability of applications, and minimizes the risk of a single server becoming overloaded.

The following table shows the interoperability between Cisco WAAS application accelerators and the F5 load balancer. For more information about Cisco WAAS load balancing, see About Traffic Interception Methods and Configuring Policy-Based Routing in the chapter "Configuring Traffic Interception" of this Configuration Guide, and also see the Server Load-Balancing Guide vA5(1.0), Cisco ACE Application Control Engine .

Table 4: Cisco WAAS AOs Interoperability with Load Balancers

Cisco WAAS Status	Load Balancer Status	Authentication Method	Cisco WAAS Application Accelerator Supported or Not Supported
Cisco WAAS enabled	F5 enabled	Kerberos	• EMAPI not supported • SSL not supported
Cisco WAAS disabled	F5 enabled	Kerberos	• EMAPI supported • SSL supported
Cisco WAAS enabled	F5 disabled	Kerberos	• EMAPI supported • SSL supported
Cisco WAAS enabled	F5 enabled	NTLM	• EMAPI supported • SSL not supported

Cisco WAAS Compatibility with Other Cisco Appliances and Software

If a firewall is placed between the clients and the WAE on one side, and the router on the other side of the firewall, default WCCP redirection does not work. However, if there is a router inside the firewall and another router outside the firewall, the default WCCP-based redirection does work and Cisco WAAS is supported.

Note Cisco Application and Content Networking Software (Cisco ACNS) devices, used with earlier Cisco WAAS versions to optimize web protocols, is End of Life and End of Sale. For more information, including migration options, see the End-of-Sale and End-of-Life Announcement for the Cisco Application and Content Networking System (ANCS) Software Version 5.5 .

Cisco WAAS Devices and Device Modes

This section contains the following topics:

About Cisco WAAS Devices and Device Modes

You must deploy the Cisco WAAS Central Manager on a dedicated appliance. Although the Cisco WAAS Central Manager device runs the Cisco WAAS software, its only purpose is to provide management functions. The Cisco WAAS Central Manager communicates with the WAEs, which are registered with it in the network. Through the Cisco WAAS Central Manager GUI, you can centrally manage the configuration of the WAEs individually or in groups. The Cisco WAAS Central Manager also gathers management statistics and logs for its registered WAEs.

A WAE also runs the Cisco WAAS software, but its role is to act as an accelerator in the Cisco WAAS network.

In a Cisco WAAS network, you must deploy a Cisco WAAS device in one of the following device modes:

- **WAAS Central Manager mode**: Mode that the Cisco WAAS Central Manager uses.
- **WAAS application accelerator mode**: Mode that a Cisco WAAS Accelerator (data center WAEs and branch WAEs that run the Cisco WAAS software) uses to optimize and accelerate traffic.
- **WAAS AppNav Controller mode**: Mode for a Cisco WAAS device that is operating as an AppNav Controller that is intercepting and distributing traffic to other Cisco WAAS devices operating in application accelerator mode.

  The default device mode for a Cisco WAAS device is WAAS accelerator mode. The **device mode** global configuration command allows you to change the device mode of a Cisco WAAS device.

  For example, after you use the Cisco WAAS CLI to specify the basic network parameters for the designated Cisco WAAS Central Manager (the Cisco WAAS device named **waas-cm**) and assign it a primary interface, you can use the **device mode** global configuration command to specify its device mode as WAAS Central Manager mode. You can also specify it to be set up as an IPv4 or an IPv6 interface during basic configuration. The following example shows the configuration of an IPv6 interface.

```
waas-cm# configure
waas-cm(config)# primary-interface gigabitEthernet 1/0 IPv6
waas-cm(config)# device mode central-manager
waas-cm(config)# exit
waas-cm(config)# copy run start
waas-cm(config)# reload
Proceed with reload? [confirm] yes
Shutting down all services, will timeout in 15 minutes.
reload in progress...
```

- Cisco WAAS Version 6.1.1 and later supports IPv6. If you are configuring the Cisco WAAS Central Manager as part of a dual-stack network, and you are using an IPv6 interface on the Cisco WAAS Central Manager, you must specify the virtual interface as the primary interface for IPv6 traffic, using the global configuration command primary-interface virtual 1/0 ipv6. Specifying the virtual interface as the primary interface for IPv6 traffic ensures that a device configured with IPv6 address only will be in Online state after registration to the Cisco WAAS Central Manager. Otherwise, the device may go into Offline state when it is registered to the Cisco WAAS Central Manager. For more information on the primary-interface global configuration command, see the *Cisco Wide Area Application Services Command Reference*

  For more information about how to initially configure a Cisco WAAS device, see the *Cisco Wide Area Application Services Quick Configuration Guide*.

Note You cannot configure a WAE network module in the NME-WAE family of devices or SRE-SM (Cisco WAAS versions earlier than Cisco WAAS Version 6.4.x) family of devices to operate in WAAS Central Manager mode.

You can configure a WAE with a Cisco WAE Inline Network Adapter to operate in WAAS Central Manager mode, but the inline interception functionality is not available.

Changing Device Mode

Before you begin

If you want to change the device mode of a device that is already registered with a Cisco WAAS Central Manager, you must first deregister the device from the Cisco WAAS Central Manager, change the device mode, reload the device, and then re-enable CMS services.

Procedure

Step 1 Deregister the device from the Cisco WAAS Central Manager:

```
wae# cms deregister
Deregistering WAE device from Central Manager will result in loss of data on encrypted file
 systems.
imported certificate/private keys for SSL service.If secure store is initialized and open,
 clear secure store.
If encrypted MAPI is enabled, windows-domain encryption-service identities will be disabled.
 The passwords must be re-entered again the next time the WAE joins a central manager.
Do you really want to continue (yes|no) [no]? yes
Disabling management service.
management services stopped
Sending de-registration request to CM
SSMGR RETURNING: 7 (Success)
Removing cms database tables.
Re-initializing SSL managed store and restarting SSL accelerator.
Deregistration complete. Save current cli configuration using 'copy running-config
startup-config' command because CMS service has been disabled.
```

Step 2 Change the device mode to **appnav-controller**:

```
wae# configure
wae(config)# device mode appnav-controller
The new configuration will take effect after reload.
```

Step 3 Save the configuration and reload:

```
wae(config)# exit
wae# copy run start
wae# reload
Proceed with reload?[confirm] yes
Proceed with clean WCCP shutdown?[confirm] yes
WCCP clean shutdown initiated
Waiting for shutdown ok (1 seconds) . Press ^C to skip waiting
WCCP clean shutdown wait time expired
Shutting down all services, will timeout in 15 minutes.
reload in progress ..
```

Step 4 Log in to the WAE after it has finished rebooting:

```
AppNav Controller
wae login: admin
Password:
System Initialization Finished.
wae#
```

Step 5 Re-enable CMS services:

```
wae# config
wae(config)# cms enable
Registering WAAS AppNav Controller...
Sending  device registration request to Central Manager with address 10.43.65.50
Please wait, initializing CMS tables
Successfully initialized CMS tables
Registration complete.
Please preserve running configuration using 'copy running-config startup-config'.
Otherwise management service will not be started on reload and node will be shown
'offline' in WAAS Central Manager UI.
management services enabled
```

Step 6 Save the configuration:

```
wae(config)# exit
wae# copy run start
```

What to do next

Note As shown in the following table, for Cisco WAVE-7571 and Cisco WAVE-8541, if the device mode is changed to **appnav-controller**, the connection limit is reduced for certain accelerators.

Cisco Platform	Application Accelerator	Appnav-mode
WAVE-7571	60,000	50,000
WAVE-8541	1,50,000	1,40,000

Calculating the Number of Cisco WAAS Devices Required

When the threshold value of an operational system aspect is exceeded, Cisco WAAS may not meet its expected service level. This situation might result in degraded performance.

The source of the limitation might originate from a specific Cisco WAAS device (Cisco WAAS Central Manager, branch WAE, or data center WAE), the entire Cisco WAAS system, a hardware constraint, or the network connecting the distributed software entities. In some cases, the limitation might be resolved by adding more resources or by upgrading the hardware or software.

When planning your network, consider the operational capacity, such as the number of users it should support, how many files it should support, and how much data it should cache.

When planning your Cisco WAAS network, refer to the following additional guidelines:

- **Number of Cisco WAAS Central Managers**: All networks must have at least one Cisco WAAS Central Manager. For larger networks, you should consider deploying two Cisco WAAS Central Managers for active and standby backup, high availability, and failover. A Cisco WAAS Central Manager is deployed on a dedicated appliance.
- **Number of WAEs**: A minimum of two WAEs are required for traffic optimization; one WAE is required on either side of a network link, for example, one in the branch office and one in the data center. A single site can have more than one WAE for redundancy purposes.
- **Number of branch WAEs**: At least one branch WAE is required in each remote office. Larger offices usually have multiple departments whose users work with different servers in the central office. In such a scenario, you can manage your system better by following the organizational structure with a branch WAE for each department. In certain situations, multiple branch WAEs can be clustered and configured using WCCP to provide failover capabilities. WCCP is the recommended method for larger user populations.
- **Number of data center WAEs**: Each organization must have at least one data center WAE.
- **Number of AppNav Controllers**: If you are using the AppNav deployment model, at least one AppNav Controller is required.

When determining the number of the component types required by your organization, consider the following factors:

- **Number of users connecting to the system**: This number depends on the static and dynamic capacities defined for the system:
    - **Static capacities**: Defines the number of user sessions that can connect to the system before it reaches its capacity.
    - **Dynamic capacities**: Defines the amount of traffic handled by the servers, which means the amount of work being performed on the network. For example, consider whether the users currently connected to the system place a heavy or light load on it.

Note Calculate dynamic limits based on the specific load assumptions that are particular to each customer.

- **Total number of users in all the branches that connect to the file servers through the data center WAE**: When the number of users is more than what one data center WAE can support, you must add one or more additional data center WAEs to the network.

Supported Methods of Traffic Redirection

In a Cisco WAAS network, traffic between the clients in the branch offices and the servers in the data center can be redirected to WAEs for optimization, redundancy elimination, and compression. Traffic is intercepted and redirected to WAEs based on the policies that have been configured on the routers. The network elements that transparently redirect requests to a local WAE can be a router using WCCP version 2 or PBR to transparently redirect traffic to the local WAE or a Layer 4 to Layer 7 switch, for example, the Cisco Catalyst 6500 Series Content Switching Module (Cisco Catalyst 6500 Series CSM) or Cisco Application Control Engine (Cisco ACE).

Alternatively, a WAE that has the Cisco WAE Inline Network Adapter or Cisco Interface Module installed can operate in inline mode and receive and optimize traffic directly before it passes through the router.

In an AppNav deployment, an AppNav Controller in the data center receives intercepted traffic through WCCP, PBR, or inline mode, and distributes it to WAAS nodes that optimize the traffic. For more information on an AppNav deployment, see the chapter "Configuring Cisco AppNav, on page 67."

This section contains the following topics:

For how to configure traffic interception for your Cisco WAAS network, see the chapter "Configuring Traffic Interception, on page 127."

Advantages and Disadvantages of Using Inline Interception

Inline interception requires usage of a WAE appliance that has the Cisco WAE Inline Network Adapter, Cisco Interface Module, or Cisco AppNav Controller Interface Module installed. In inline mode, the WAE can physically and transparently intercept traffic between the clients and the router. When using this mode, you physically position the WAE device in the path of the traffic that you want to optimize, typically between a switch and a router.

Because redirection of traffic is not necessary, inline interception simplifies deployment and avoids the complexity of configuring WCCP or PBR on the routers.

The inline adapter or module contains one or more pairs of LAN/WAN Ethernet ports, each grouped into an inline or bridge group interface. If the inline adapter or module has multiple pairs of ports, it can connect to multiple routers if the network topology requires it.

The inline or bridge group interface transparently intercepts the traffic flowing through it or bridges traffic that does not have to be optimized. It also uses a mechanical fail-safe design that automatically bridges traffic if a power, hardware, or unrecoverable software failure occurs.

Note The AppNav Controller Interface Modules do not support automatic bypass mode to continue traffic flow in the event of a failure. For high availability, two or more AppNav Controller Interface Modules should be deployed in an AppNav cluster. For more information on using inline mode with the AppNav solution, see the chapter Configuring Cisco AppNav, on page 67.

You can configure the inline or bridge group interface to accept traffic only from certain VLANs; for all other VLANs, traffic is bridged, and not processed. You can serially cluster WAE devices (not AppNav Controllers) in inline mode to provide higher availability in the event of a device failure. If the current optimizing device fails, the second WAE device in the cluster provides the optimization services. Deploying WAE devices in a serial inline cluster for the purposes of scaling or load balancing is not supported.

Any combination of traffic interception mechanisms on peer WAEs is supported. For example, you can use inline interception on the branch WAE and WCCP on the data center WAE. For complex data center deployments, we recommend that you use hardware-accelerated WCCP interception or load balancing with the Cisco Application Control Engine (Cisco ACE) and a Cisco WAAS AppNav deployment.

For more information on inline interception, see Using Inline Mode Interception, on page 171 in the chapter "Configuring Traffic Interception."

Three elements can help ease traffic interception in data centers without using a WCCP-based approach:

- Multiple pairs of inline interfaces are available on certain WAE models:
- The WAVE-294, WAVE-594, WAVE-694, WAVE-7541, and WAVE-8541 models support one installed Cisco Interface Module, which can be configured with up to 16 inline ports in 8 inline groups, or one installed AppNav Controller Interface Module, which can be configured with up to 12 inline ports in 5 bridge groups.Serial inline clustering of two WAEs (not AppNav Controllers) to support high availability.
- Interception ACLs to control the traffic that is intercepted and what is passed through. For more information on interception ACLs, see Configuring Interception Access Control Lists in the chapter "Configuring Traffic Interception."

Advantages and Disadvantages of Using WCCP

WCCP (Web Cache Communication Protocol) specifies interactions between one or more routers (or Layer 3 switches) and one or more application appliances, web caches, and caches of other application protocols. The purpose of the interaction is to establish and maintain the transparent redirection of selected types of traffic flowing through a group of routers. The selected traffic is redirected to a group of appliances.

WCCP allows you to transparently redirect client requests to a WAE for processing. The Cisco WAAS software supports transparent intercept of all TCP traffic.

To configure basic WCCP, enable **WCCP** as the **interception method** on the router and WAE or ANC in the data center, and the router or WAE in the branch office. By default, WCCP Version 2 is used with Cisco WAAS. You do not have to configure all of the available WCCP features or services in order to get a WAE up and running.

Note You must configure the routers and WAEs to use WCCP Version 2 instead of WCCP Version 1, because WCCP Version 1 supports only web traffic (port 80). The routers must be running a version of Cisco IOS software that also supports WCCP Version 2.

WCCP is much simpler to configure than PBR. However, you should have write access to the router in order to configure WCCP on the router, which typically resides in the data center and on the edge of the branch office. Another advantage of using WCCP is that you have to perform only a basic configuration of WCCP on your routers and WAEs in order to get your WAE up and running.

The WCCP Version 2 protocol also has a set of useful features built-in, for example, automatic failover and load balancing between multiple devices. The WCCP-enabled router monitors the liveliness of each WAE or

ANC that is attached to it through the WCCP keepalive messages. If a WAE goes down, the router stops redirecting packets to the WAE. When you use WCCP Version 2, the branch WAE is not made a single point of failure for the WAAS services. The router or ANC can also load balance the traffic among a number of branch WAEs.

You can use CLI commands to configure basic WCCP on both the routers and the WAEs, or you can use CLI commands to configure the router for WCCP and use the Cisco WAAS Central Manager GUI to configure basic WCCP on the WAEs.

We recommend that you use the Cisco WAAS CLI to complete the initial basic configuration of WCCP on your first branch WAE and data center WAE, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*. After you have verified that WCCP transparent redirection is working properly, you can use the Cisco WAAS Central Manager GUI to centrally modify this basic WCCP configuration or configure additional WCCP settings, for example, load balancing, for a WAE (or group of WAEs). For more information, see Configuring WCCP on Cisco WAEs in the chapter "Configuring Traffic Interception." After you have configured basic WCCP on the router, you can configure advanced WCCP features on the router, as described in Configuring Advanced WCCP Features on Routers in the chapter "Configuring Traffic Interception."

Advantages and Disadvantages of Using PBR

PBR allows IT organizations to configure their network devices (a router or a Layer 4 to Layer 6 switch) to selectively route traffic to the next hop, based on the classification of the traffic. Cisco WAAS administrators can use PBR to transparently integrate a WAE into their existing branch office network and data centers. PBR can be used to establish a route that goes through a WAE for some or all packets, based on the defined policies.

To configure PBR, you must create a route map and then apply the route map to the router interface on which you want the transparent traffic redirection to occur. Route maps reference access lists that contain explicit permit or deny criteria. The access lists define the traffic that is interesting to the WAE, that is, traffic that the network device should transparently intercept and redirect to the local WAE. Route maps define how the network device should handle interesting traffic, for example, send the packet to the next hop, which is the local WAE.

The following list summarizes the main advantages of using PBR instead of WCCP Version 2 to transparently redirect IP/TCP traffic to a WAE:

- PBR provides higher performance than WCCP Version 2 because there is no GRE overhead.
- By default PBR uses CEF when CEF is enabled on the router. (PBR uses CEF for fast switching of packets.)
- PBR can be implemented on any Cisco IOS-capable router or a switch that is running an appropriate version of the Cisco IOS software. We recommend that you use Cisco IOS Software Release 12.2 or later.
- PBR provides failover if multiple next-hop addresses are defined.

The following list summarizes the main disadvantages of using PBR instead of WCCP Version 2 to transparently redirect IP/TCP traffic to a WAE:

- PBR does not support load balancing between equal cost routes. Consequently, PBR does not provide scalability for the deployment location.
- PBR is more difficult to configure than WCCP Version 2. For an example of how to configure PBR for WAAS traffic, see the Using Policy-Based Routing Interception in the chapter "Configuring Traffic Interception."

Configuring WCCP or PBR Routing for Cisco WAAS Traffic

This section contains the following topics:

About Configuring WCCP or PBR Routing for Cisco WAAS Traffic

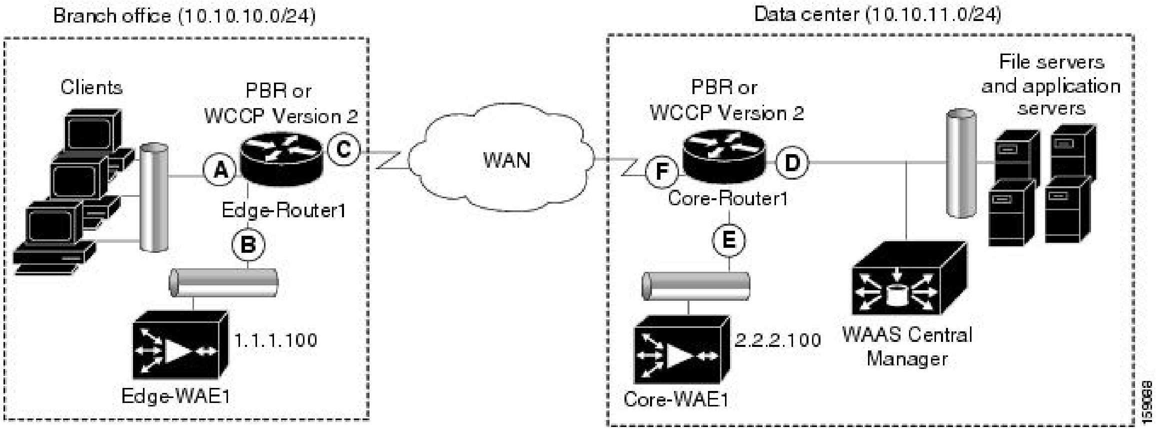
The primary function of Cisco WAAS is to accelerate WAN traffic. In general, Cisco WAAS accelerates TCP traffic, and uses a symmetric approach for application optimization. A WAE that has application-specific and network-specific intelligence is placed on each side of the WAN. These WAEs are deployed out of the data path in both the branch office and the data center.

Traffic between the clients in the branch offices and the servers at the data center is transparently redirected through the WAEs based on a set of configured policies with no tunneling. The routers use WCCP Version 2 or PBR to transparently intercept and redirect traffic to the local WAE for optimization, redundancy elimination, and compression. For example, Edge-Router1 uses PBR or WCCP Version 2 to transparently redirect traffic to Edge-WAE1, the local WAE in the branch office. Core-Router1 uses PBR or WCCP Version 2 to transparently redirect traffic to the Core-WAE1, the local WAE in the data center.

Note In this sample deployment, Edge-Router1 and Core-Router1 can be replaced with Layer 4 to Layer 7 switches, which are capable of redirecting traffic to the local WAE.

The following figure shows that the WAEs (Edge-WAE1 and Core-WAE1) must reside in an out-of-band network that is separate from the traffic's destination and source. For example, Edge-WAE1 is on a subnet that is separate from the clients (the traffic source), and Core-WAE1 is on a subnet that is separate from the file servers and application servers (the traffic destination). Additionally, you may have to use a tertiary interface (a separate physical interface) or a subinterface to attach a WAE to the router, which redirects traffic to it, in order to avoid an infinite routing loop between the WAE and the router. For more information about this, see Using Tertiary Interfaces or Subinterfaces to Connect WAEs to Routers, on page 47.

Figure 5: Using PBR or WCCP Version 2 for Transparent Redirection of All TCP Traffic to WAEs



The following table provides a summary of the router interfaces that you must configure to use PBR or WCCP Version 2 to transparently redirect traffic to a WAE.

Table 5: Router Interfaces for WCCP or PBR Traffic Redirection to WAEs

Router interface	Description
Edge-Router1	
A	Edge LAN interface (ingress interface) that performs redirection on the outbound traffic.
B	Tertiary interface (separate physical interface) or a subinterface off of the LAN port on Edge-Router1. Used to attach Edge-WAE1 to Edge-Router1 in the branch office.
C	Edge WAN interface (egress interface) on Edge-Router1 that performs redirection on the inbound traffic.
Core-Router1	
D	Core LAN interface (ingress interface) that performs redirection on outbound traffic.
E	Tertiary interface or subinterface off of the LAN port on Core-Router1. Used to attach Core-WAE1 to Core-Router1 in the data center.
F	Core WAN interface (egress interface) on Core-Router1 that performs redirection on the inbound traffic.

This traffic redirection does not use tunneling; the full original quadruple (source IP address, source port number, destination IP address, and destination port number) of the TCP traffic is preserved end to end. The original payload of the TCP traffic is not preserved end to end because the primary function of Cisco WAAS is to accelerate WAN traffic by reducing the data that is transferred across the WAN. This change in payload can potentially impact features on the router that is performing the WCCP or PBR redirection, and that needs to see the actual payload to perform its operation, for example, NBAR. For more information on this topic, see Cisco WAAS and Cisco IOS Interoperability, on page 33.

Using WCCP or PBR at both ends with no tunneling requires that traffic is intercepted and redirected not only in the near-end router but also at the far-end router, which requires four interception points, as opposed to two interception points in a tunnel-based mode.

You can enable packet redirection on either an outbound interface or inbound interface of a WCCP-enabled router. The terms **outbound** and **inbound** are defined from the perspective of the interface. Inbound redirection specifies that traffic should be redirected as it is being received on a given interface. Outbound redirection specifies that traffic should be redirected as it is leaving a given interface.

If you are deploying WAN optimization in your Cisco WAAS network, you must configure the router and WAE for WCCP Version 2 and the TCP promiscuous mode service (WCCP Version 2 services 61 and 62 by default).

Note Services 61 and 62 are always enabled together when configuring TCP promiscuous mode on the WAE. Services 61 and 62 must be defined and configured separately when configuring TCP promiscuous mode on the network device (router, switch, or other). Service 61 distributes traffic by source IP address, and service 62 distributes traffic by destination IP address. The service IDs are configurable; 61 and 62 are the defaults.

The TCP promiscuous mode service intercepts all the TCP traffic that is destined for any TCP port and transparently redirects it to the WAE. The WCCP-enabled router uses service IDs 61 and 62 to access this service. The service IDs used on the router must match those on the WAE if service IDs that are different from the defaults are configured.

By default, IP Protocol 6 is specified for the TCP promiscuous mode service. Consequently, the routers that have been configured to the TCP promiscuous mode service will intercept all the TCP traffic destined for any TCP port to the local WAE. Because the TCP promiscuous mode service is configured on the WAE, the WAE will accept all of the TCP traffic that is transparently redirected to it by specified WCCP routers, for example, Edge-WAE1 will accept all TCP traffic that Edge-Router1 redirects to it. In the branch office, you can intercept packets at the edge LAN and WAN interfaces on the Edge routers and redirect the TCP traffic to the local WAE (the branch WAE). In the data center, you can intercept packets at the core LAN and WAN interfaces on the core routers and redirect the TCP traffic to the local WAE (the data center WAE). For more information, see Configuring WAEs as Promiscuous TCP Devices in a Cisco WAAS Network, on page 47.

Configure packet redirection on inbound interfaces of branch software routers whenever possible. Inbound traffic can be configured to use Cisco Express Forwarding (CEF), distributed Cisco Express Forwarding (dCEF), fast forwarding, or process forwarding.

Note CEF is required for WCCP, and must be enabled on the router.

To enable packet redirection on a router’s outbound or inbound interface using WCCP, use the **ip wccp redirect** interface configuration command.

Caution The **ip wccp redirect** interface conifguration command has the potential to affect the **ip wccp redirect exclude in** command. If you have **ip wccp redirect exclude in** set on an interface and you subsequently configure the **ip wccp redirect in** command, the **ip wccp redirect exclude in** command is overridden. If you configure the **exclude in** command, the **redirect in** command is overridden.

Configuring WAEs as Promiscuous TCP Devices in a Cisco WAAS Network

For a Cisco WAE to function as a promiscuous TCP device for the TCP traffic that is transparently redirected to it by the specified WCCP Version 2 routers, the WAE uses WCCP Version 2 services 61 and 62 by default, though the service IDs are configurable. The WCCP services are represented by the canonical name **tcp-promiscuous** on the WAE CLI and **TCP Promiscuous** in the Cisco WAAS Central Manager GUI.

For instructions on how to perform a basic WCCP configuration for a Cisco WAAS network, see the *Cisco Wide Area Application Services Quick Configuration Guide*. For how to use the Cisco WAAS Central Manager GUI to modify the basic WCCP configuration on a Cisco WAE, see Configuring WCCP on Cisco WAEs in the chapter "Configuring Traffic Interception."

Using Tertiary Interfaces or Subinterfaces to Connect WAEs to Routers

If you plan to use WCCP Version 2 or PBR to transparently redirect TCP traffic to a WAE, make sure that the WAE is not attached to the same segment as the router interface on which the traffic redirection is to occur. Otherwise, an infinite routing loop between the router and the WAE will occur. These infinite routing loops occur because there is no way to notify the router to bypass the interception and redirection after it has redirected the traffic to the WAE the first time; the router will continuously redirect the same intercepted traffic to the local WAE, creating the infinite routing loop.

Note The WCCP GRE return and generic GRE egress methods allow you to place WAEs on the same VLAN or subnet as clients and servers. For how to configure these egress methods, see Configuring Egress Methods for WCCP-Intercepted Connections in the chapter "Configuring Traffic Interception."

For example, if you attach Edge-WAE 1 to the same segment (subnet) as the LAN router interface on which the PBR or WCCP traffic redirection occurs in the branch office, there will be an infinite routing loop between Edge-Router1 and Edge-WAE1. If you attach Core-WAE1 to the same segment (subnet) as the LAN router interface on which the PBR or WCCP traffic redirection occurs in the data center, there will be an infinite routing loop between Core-Router1 and Core-WAE1.

To avoid an infinite routing loop between the router and its local WAE, connect the WAE to the router through a tertiary interface (a separate physical interface) or a subinterface (a different virtual subinterface) from the router’s LAN port. By using a tertiary interface or a subinterface to connect a WAE to the router that is performing the PBR or WCCP redirection, the WAE has its own separate processing path that has no Cisco IOS features enabled on it. In addition, this approach simplifies the process of integrating WAEs into an existing network. Because the WAEs are being connected to the routers through a tertiary interface or subinterface that has no Cisco IOS features enabled on it, the Cisco IOS features that are already enabled on your existing Cisco-enabled network elements, for example, Edge-Router1 or Core-Router1, will generally not be affected when you connect WAEs to these routers. For more information about Cisco WAAS and Cisco IOS interoperability, see Cisco WAAS and Cisco IOS Interoperability, on page 33.

See the *Cisco Wide Area Application Services Quick Configuration Guide* for an example of how to use a subinterface to properly attach a local WAE to the router that is redirecting TCP traffic to it.

Access Lists on Routers and WAEs

You can optionally configure the router to redirect traffic from your WAE based on the access lists that you define on the router. These access lists are also referred to as redirect lists. For how to configure access lists on routers that will be configured to transparently redirect traffic to a WAE, see Configuring IP Access Lists on a Router in the chapter "Configuring Traffic Interception."

Note IP access lists on routers have the highest priority, followed by IP ACLs that are defined on the WAEs, and then interception ACLs that are defined on the WAEs.

This section contains the following topics:

- IP ACLs on WAEs, on page 48
- Interception ACLs on WAEs, on page 49

IP ACLs on WAEs

In a centrally managed Cisco WAAS network environment, administrators need to be able to prevent unauthorized access to various devices and services. The Cisco WAAS software supports standard and extended IP access control lists (ACLs) that allow you to restrict access to or through particular interfaces on a Cisco

WAAS device. For more information, see the chapter Creating and Managing IP Access Control Lists for WAAS Devices, on page 277.

Note IP ACLs that are applied on interfaces, and WCCP ACLs, always take precedence over any interception ACLs and Cisco WAAS application definitions, if any, that have been defined on the WAE.

Interception ACLs on WAEs

You can configure an interception ACL to control what incoming traffic across all interfaces should be intercepted by a Cisco WAE device. Packets that are permitted by the ACL are intercepted by the WAE and packets that are denied by the ACL are passed through the WAE without processing. By configuring interception ACLs on the WAE, you can control traffic interception without modifying the router configuration.

An interception ACL can be used both with WCCP and inline interception.

Interception ACLs that are defined on a WAE always take precedence over any Cisco WAAS application definitions that have been defined on the WAE, but they are applied after interface ACLs and WCCP ACLs.

For information about how to configure an interception ACL for a WAE, see Configuring Interception Access Control Lists in the chapter "Configuring Traffic Interception."

Cisco WAAS Login Authentication and Authorization

This section contains the following topics:

About Cisco WAAS Login Authentication and Authorization

In the Cisco WAAS network, administrative login authentication and authorization are used to control login requests from administrators who want to access a Cisco WAAS device for configuring, monitoring, or troubleshooting purposes.

Login authentication is the process by which Cisco WAAS devices verify whether the administrator who is attempting to log in to the device has a valid username and password. The administrator who is logging in must have a user account registered with the device. User account information serves to authorize the user for administrative login and configuration privileges. The user account information is stored in an authentication, authorization, and accounting (AAA) database, and the Cisco WAAS devices must be configured to access the particular authentication server (or servers) where the AAA database is located. When the user attempts to log in to a device, the device compares the person’s username, password, and privilege level to the user account information that is stored in the database.

The Cisco WAAS software provides the following AAA support for users who have external access servers, for example, RADIUS, TACACS+, or Windows domain servers, and for users who need a local access database with AAA features:

- **Authentication** (or **login authentication**): The action of determining who the user is. It checks the username and password.
- **Authorization** (or **configuration**): The action of determining what a user is allowed to do. It permits or denies privileges for authenticated users in the network. Generally, authentication precedes authorization. Both authentication and authorization are required for a user log in.

- **Accounting**: The action of keeping track of administrative user activities for system accounting purposes. In the Cisco WAAS software, AAA accounting through TACACS+ is supported.

For more information, see Configuring AAA Accounting for Cisco WAAS Devices in the chapter "Configuring Administrative Login Authentication, Authorization, and Accounting."

Cisco WAAS Administrator Accounts

In a centrally managed Cisco WAAS network, administrator accounts can be created for access to the Cisco WAAS Central Manager and, independently, for access to the WAEs that are registered with the Cisco WAAS Central Manager. There are two distinct types of accounts for Cisco WAAS administrators:

- Role-based accounts: Allows users to access the Cisco WAAS Central Manager GUI, the Cisco WAAS Central Manager CLI, and the Cisco WAE Device Manager GUI. The Cisco WAAS software has a default Cisco WAAS system user account (username is admin and password is default) that is assigned the role of administrator.
- Device-based Cisco WAAS CLI accounts: Allows users to access the Cisco WAAS CLI on a Cisco WAAS device. These accounts are also referred to as local user accounts.

Note An administrator can log in to the Cisco WAAS Central Manager device through the console port or the Cisco WAAS Central Manager GUI. An administrator can log in to a Cisco WAAS device that is functioning as a data center or branch WAE through the console port or the Cisco WAE Device Manager GUI.

A Cisco WAAS device that is running Cisco WAAS software comes with a predefined superuser account that can be used initially to access the device. When the system administrator logs in to a Cisco WAAS device before authentication and authorization have been configured, the administrator can access the Cisco WAAS device by using the predefined superuser account (the predefined username is admin and the predefined password is default). When you log in to a Cisco WAAS device using this predefined superuser account, you are granted access to all the Cisco WAAS services and entities in the Cisco WAAS system.

After you have initially configured your Cisco WAAS devices, we strongly recommend that you immediately change the password for the predefined superuser account (the predefined username is **admin**, the password is **default**, and the privilege level is **superuser, privilege level 15**) on each Cisco WAAS device. For how to use the Cisco WAAS Central Manager GUI to change the password, see Changing the Password for Your Own Account in the chapter "Creating and Managing Administrative User Accounts and Groups."

Logically Grouping Your WAEs

To streamline the configuration and maintenance of WAEs that are registered with a Cisco WAAS Central Manager, you can create a logical group and then assign one or more of your WAEs to the group. Groups not only save you time when configuring multiple WAEs, but they also ensure that configuration settings are applied consistently across your Cisco WAAS network. For example, you can set up a **WinAuth** group that defines the standard Windows authentication configuration that is wanted for all of the WAEs in that group. After you define the **WinAuth** settings once, you can centrally apply those values to all of the WAEs in the WinAuth group instead of defining these same settings individually on each WAE.

With the Cisco WAAS Central Manager GUI, you can easily organize your branch and data center WAEs into device groups, which are a collection of WAEs that share common qualities and capabilities. Setting up groups based on their authentication settings is an example of a device group.

When you create a device group, you should identify the unique characteristics that distinguish that group of WAEs from others in your network. For example, in larger Cisco WAAS deployments, one set of WAEs may have to be configured with authentication settings that are different from another set of WAEs in your WAAS network. In such a scenario, you should create two device groups, each of which contain different authentication settings, and then assign your WAEs to the most appropriate group.

If you have WAEs that reside in different time zones, you can also create device groups based on geographic regions so that the WAEs in one group can have a different time zone setting from the WAEs in another group.

In smaller Cisco WAAS deployments where all WAEs can be configured with the same settings, you may only have to create one general device group. This practice allows you to configure settings for the group, and then apply those settings consistently across all your WAEs.

Note The **AllWAASGroup** and **AllWAASExpressGroup** are default device groups that automatically contain all Cisco WAAS and Cisco WAAS Express devices. In these or any other device groups, you should configure only the settings that you want to be consistent across all the devices in the group. Settings that apply to a single device should be configured on that device only and not on the device group.

By default, Cisco WAAS Central Manager allows you to assign a device to multiple device groups. Before you create a device group, make sure you understand the unique properties that you want the group to contain.

The Cisco WAAS Central Manager allows you to create locations that you can associate with a Cisco WAAS device. You assign a device to a location when you first activate the device. The main purpose of assigning a Cisco WAAS device to a location is to help you identify a Cisco WAAS device by the physical region in which it resides. Locations are different from device groups because devices do not inherit settings from locations.

You assign a device to a location when you activate the device, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*. For how to logically group your Cisco WAEs, see the chapter Using Device Groups and Device Locations, on page 53.

Data Migration Process

If you have an existing network, you must perform some tasks before setting up your Cisco WAAS network. The first step in the data migration process is to back up the data at the branch offices and restore it to the data center.

After you back up data to the data center, you should preload the cache (called preposition) with the files for which you want to provide the fastest access. Set up the files from your branch office file server to the WAEs that are also located in the same branch office. You can then remove the file servers from the branch offices and point to the data center file server.

The final step in the data migration process is to set the SMB policies.

When performing the data migration process, note the following restrictions:

- The topology for the file server at the data center must be identical to the topology that exists on the branch file server.

- Resource credentials such as ACLs are not automatically migrated. Two options are available:
    - You can use backup or restore software to restore an initial backup of the tree to the target server. This practice allows both the creation of ACLs as well as the creation of the initial file set that Rsync can take as an input for diff calculations. The replication inherits the existing ACLs in that tree.
    - The other option is to perform a first run of Robocopy (including data and permissions), and then continue with sync iterations using Rsync.

After replicating, use one of Microsoft’s tools for copying only ACLs (no data) onto the replicated tree. You can use **Robocopy.exe** for copying the directory tree or file ACLs, and **Permcopy.exe** to copy share permissions.

- The migration size must be less than the cache size of the branch WAE.

CHAPTER 3

Using Device Groups and Device Locations

This chapter describes the types of device groups supported by the Cisco WAAS software and how to create groups that make it easier to manage and configure multiple devices at the same time. This chapter also discusses how to use device locations.

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

This chapter contains the following sections:

About Device Groups

When you create a device group, you need to identify the unique characteristics that distinguish that group of devices from others in your network. For example, in larger Cisco WAAS deployments, one set of devices may need to be configured with authentication settings that are different from another set of devices in your Cisco WAAS network. In this situation, you would create two device groups that each contain different authentication settings, and then assign your devices to the most appropriate group.

If you have devices that reside in different time zones, you can also create device groups based on geographic regions so that the devices in one group can have a different time zone setting from the devices in another group.

In smaller Cisco WAAS deployments where all devices can be configured with the same settings, you may only need to create one general device group. This setup allows you to configure settings for the group, and then apply those settings consistently across all your Cisco WAAS devices.

Groups not only save you time when configuring multiple devices, but they also ensure that configuration settings are applied consistently across your Cisco WAAS network.

There are two types of device groups: **WAAS Device Groups** and **WAAS Express Device Groups**. These groups are explained in more detail in Creating a New Device Group, on page 54.

When you register a Cisco WAAS device with the Cisco WAAS Central Manager, that device automatically joins the **AllWAASGroup**, which is the default device group on the system for Cisco WAAS devices. If you create additional device groups, you need to decide if you want your devices to belong to more than one group (the default **AllWAASGroup** and the new device group you create). If you only want a device to belong to a device group that you create, make sure that you remove the device from the default **AllWAASGroup**. WAAS Express devices automatically join the default **AllWAASExpressGroup** device group when they are registered with the Central Manager.

Cisco WAAS devices and Cisco WAAS Express devices cannot be mixed in the same device group. You choose the device group type when you create the group and it cannot be changed. When you create a Cisco WAAS Express type of device group, you can copy policies from an existing Cisco WAAS or Cisco WAAS Express group, but policies cannot be copied after creation.

Working with Device Groups

This section contains the following topics:

Creating a Device Group

This section contains the following topics:

The following table provides a checklist for creating a new device group.

Table 6: Checklist for Creating a Device Group

Task	Additional Information and Instructions
1. Create a new device group.	Defines general information about the new group, such as the group name, group type, and whether all newly activated devices are assigned to this group. For more information, see Creating a New Device Group, on page 54.
2. Configure the settings of the new device group.	Specifies the settings that are unique to this device group. All devices that are a member of this group will automatically inherit these settings. For more information, see Configuring the Settings for a Device Group, on page 56.
3. Assign devices to the device group.	Assigns devices to the group so they can inherit the group settings. For more information, see Assigning Devices to a Configuration Device Group, on page 57.

Creating a New Device Group

Before you begin

Before you create a device group, make sure you understand the unique properties that you want the group to contain. For example, you may want to set up two device groups that have different authentication settings or different time zone settings.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups > All Device Groups**.

The **Device Group** window appears. From this window you can perform the following tasks:

- Click the **Edit** icon next to the device group that you want to modify.
- Create a new device group as described in the steps that follow.

Step 2 Click the **Create New Device Group** icon in the taskbar. The **Creating New Device Group** window appears.

Step 3 In the **Name** field, enter the name of the device group.

The name must be unique and should be a name that is useful in distinguishing the device group from others/other groups on your system. Otherwise, an error message stating that the name already exists is displayed. The name cannot contain characters other than letters, numbers, period, hyphen, underscore, and space.

Step 4 For the **Configuration Group Type**, choose either **WAAS** or **WAAS Express** . This sets the type of devices that the group can contain. A WAAS Express group can contain only WAAS Express devices. A WAAS group can contain all types of devices *except for* WAAS Express devices.

Step 5 Check the **Automatically assign all newly activated device to this group** check box to set this device group as the default device group for all newly activated devices.

Step 6 If you chose the **WAAS Express** group type, you can copy policies from another existing group by choosing the group in the Copy Policies from the device group drop-down list. If you copy policies from a WAAS group, only basic optimization policies are copied, not application acceleration policies.

If you chose the WAAS device group type, you can copy policies from another existing WAAS device group by choosing the WAAS device group in the Copy Configuration from the device group drop-down list. This copies only the WAAS policy configurations from the selected device group. Note that only those WAAS device groups that have configured policies are listed here.

Step 7 (Optional) Enter comments about the group in the **Comments** field. The comments that you enter will appear in the **Device Group** window.

Step 8 Click **Submit**.

The window refreshes with additional options.

Note The **Pages** configured for this device group arrow lists the configuration windows in the Cisco WAAS Central Manager GUI that have been configured for this device group. Because this is a new device group, no pages will appear in this list.

Step 9 (Optional) Customize the menu options for this device group by completing the following steps. Use this feature to remove from view any configuration windows that you do not need for that particular device group:

a) Click **Select pages to hide from table contents for this device group** arrow.

A list of windows in the Cisco WAAS Central Manager GUI appears.

b) Check the windows that you want to hide for this device group. You can click the folder icon next to a window to display its child windows.

c) Click **Submit**.

Step 10 Configure the settings for this device group as described in Configuring the Settings for a Device Group, on page 56.

Configuring the Settings for a Device Group

Before you begin

After creating a device group, you need to configure the settings that you want to be unique to this group.

Consider the following guidelines when you configure device group settings:

- If you have a general device group that contains all your Cisco WAAS devices of a specific type, configure only the settings that you want to be consistent across all the devices of that type.
- Settings that apply to a single device should be configured on that device only and not on the device group.
- When a device group is created, no policies are assigned to that group unless the admin adds them.
- Note the following about the class-default policy and creating or changing device group settings:
  - After policies are added to a device group (either custom or the default set), a class-default policy is also created.
  - All of the policies in a default policy set or custom policy set except the class-default policy can be modified or deleted.
  - The class-default policy cannot be modified or deleted. To change the class-default policy, you must delete the device group, and then create a new device group with a new class-default policy.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** > *device-group-name*.

The **Modifying Device Group** window appears.

Step 2 Click the **Pages configured for this device group** arrow button to view which configuration windows have already been configured for the group.

A list of pages that are configured for that device group appears. If this is a new device group or if there are no pages configured for this device group, the list displays **Null**.

Step 3 Customize the menu options for this device group by completing the following steps:

a) Click the **Select pages to hide from table of contents of this device group** arrow button.

   A list of windows in the Cisco WAAS Central Manager GUI appears.

b) Place a check next to the windows that you want to hide for this device group. Use this feature to remove from view any configuration windows that you do not need for this particular device group.

Step 4 Use the menu bar to choose each configuration option that you want to modify for this device group.

If the configuration option has not been configured for this device group, the message **There are currently no settings for this group** appears at the top of the window.

Step 5 Make the necessary changes on the configuration option window and, after finished, click **Submit**.

After a particular setting is configured, the configuration window is listed under **Pages** configured for this device group in the **Modifying Device Group** window.

Step 6 Assign devices to this new group as described in Assigning Devices to a Configuration Device Group, on page 57.

Assigning Devices to a Configuration Device Group

Before you begin

After you create a configuration device group, you need to assign devices to the group. The Cisco WAAS Central Manager GUI provides two methods to assign devices to a configuration group:

- Select the device first, and then assign a device group to the device.
- Select the device group first, and then assign devices to the device group.

Consider the following guidelines for assigning devices to a configuration device group.

- To assign a device group to a device, choose **Devices** > *device-name* and choose **Assign Device Groups** from the *device-name* menu. You can then assign a device group to the device using the same method described in **Step 4** and **Step 5** below.
- You cannot assign the Cisco WAAS Central Manager to a device group. You must configure the Cisco WAAS Central Manager separately from other devices.
- You cannot assign WAAS Express devices to a WAAS group, and you cannot assign WAAS devices to a WAAS Express group. When you assign devices to device groups, invalid devices are not shown in the device list.
- By default, all devices when they are activated automatically join either the **AllWAASGroup** or the **AllWAASExpressGroup**. If you do not want a device to belong to one of the default device groups: unassign that device from the default device group, and then assign that device to a custom device group. Generally, when assigning a device to two different Device Groups, have the same page configured in it: either have the page configured in single Device Group or it is expected to have **Force Device Group (FDG)** settings enabled in the other Device Group. The Cisco WAAS Central Manager pushes the latest changed Device Group's configuration to the device.
- When a device is moved from a Device level to Device Group level, the configurations of the **Current applied settings from Device** are applied to the Device Group. In such conditions, the **Force** device group icon appears in the respective device group configuration pages for that device.

  This **Force** device group icon depicts that there is difference between Device and Device group configurations and can be resolved using the Procedure for Forcing Device Group Settings, on page 61.

  Additionally, they show up in the **Force Device Group Detection** window. This **Force** device group icon depicts that there is a difference between Device and Device group configurations. The Cisco WAAS Central Manager provides an easy way to identify, view and resolve these configuration conflicts.
- When you assign devices that have different Cisco WAAS software versions to a device group, some features configured for a device group may not be supported by all devices in the group. In some cases, devices may be prevented from joining the group if the group is configured with policies that they cannot

support. In such cases, we recommend that you upgrade all devices to the same software version, or create different device groups for devices with incompatible versions.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** *device-group-name* .

The **Modifying Device Group** window appears.

Step 2 Choose *device-group-name* **Assign Devices**.

The **WAE/WAAS Express Assignments** window appears, displaying the devices assigned to various locations. If you are editing a WAAS group, only WAAS devices are shown. If you are editing a WAAS Express group, only WAAS Express devices are shown.

The **WAE/WAAS Express Assignments** window allows you to filter your view of the items in the list. Filtering allows you to find items in the list that match the criteria that you set.

Step 3 Assign all available devices, or specific devices, to the device group:

- To assign all available devices to the device group, click the **Select All** icon (blue "x" overlaid with green arrow)
- To assign specific devices to the device group, click the **Select** icon (blue "x") next to each device that you want to assign to the device group.

Step 4 Click **Submit**.

A green check mark appears next to the assigned devices.

Step 5 Click the **Unassign** icon (green check mark) next to the name of the device that you want to remove from the device group. Alternatively, you can click the **Remove all** icon in the taskbar to remove all devices from the selected device group. Click **Submit**.

If there is any mismatch in the configuration between a Device and Device group configured pages, the **Force Device Group** icon will appear in the respective device group configuration page after assigning the device to the device group.

To correct this, use the Force Group Settings, described in Procedure for Forcing Device Group Settings, on page 61 to ensure that all devices in the specified group have the same configuration.

Deleting a Device Group

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** > *device-group-name*.

The **Modifying Device Group** window appears.

Step 2 In the taskbar, click the **Delete Device Group** icon. You are prompted to confirm your decision to delete the device group.

Step 3 To confirm your decision, click **OK**.

Viewing the Groups Assigned to a Device

Before you begin

The Cisco WAAS Central Manager GUI allows you to view the groups that a device belongs to, as well as the devices that belong to a specific group. This section describes both of these procedures.

Procedure

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

The **Device Dashboard** window appears.

Step 2 In the **Assignments** field on the **Device Dashboard** window, click the link that displays the groups to which the device is assigned.

The **Device Group Assignments** window appears, which shows all the device groups in your Cisco WAAS network that match the device type (Cisco WAAS or Cisco WAAS Express). The device is assigned to the device groups with a green check mark next to them.

You can also go to the **Device Group Assignments** window by choosing the **Assign Device Groups** option in the menu bar.

Viewing the Devices Assigned to a Group

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** *device-group-name* .

The **Modifying Device Group** window appears.

Step 2 Choose *device-group-name* **Assign Devices**.

The **WAE/WAAS Express Assignments** window appears, which shows all the Cisco WAAS or Cisco WAAS Express devices on your Cisco WAAS network. The devices with a green check mark next to them are assigned to this group.

Viewing the Device Groups List

The **Device Groups** window lists all the device groups that have been created in your Cisco WAAS network. To view this list, from the Cisco WAAS Central Manager menu bar, choose **Device Groups** > **All Device Groups**.

The **Device Groups** window appears; this window displays the following information about each device group:

- Type of device group (WAAS Configuration Group or WAAS Express Configuration Group).
- Any comments that were entered when the device group was created.

From the **Device Groups** window, you can perform the following tasks:

- Create a new device group. For more information, see Creating a New Device Group, on page 54.
- Modify the settings of a device group: click the **Edit** icon next to the group that you want to edit.

Enabling or Disabling Device Group Overlap

Before you begin

By default, you can assign a device to multiple device groups. You can disable this functionality so a device can only belong to one device group, which eliminates the possibility of a device inheriting settings from more than one group.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **Global** > **System Properties**.

The **Config Properties** window appears.

Step 2 Click the **Edit** icon next to the property name **DeviceGroup.overlap**.

The **Modifying Config Property, DeviceGroup.overlap** window appears.

Step 3 From the **Value** drop-down list, choose either **true** or **false**. The default is **true**.

When you disable Device Group Overlap (set to **false**), existing overlapping device groups are retained and continue to be handled as though overlap were enabled. However, any newly added groups do not allow overlapping, and new devices cannot be added to the existing overlapping groups.

Step 4 Click **Submit**.

Overriding Group Configuration Settings

The Cisco WAAS Central Manager GUI provides the following methods to override the current group configuration on a device:

Forcing Device Group Settings on All Devices in the Group

This section contains the following topics:

Operating Considerations for Force Group Settings

The **Device Groups** > *device-group-name* > **Force Group Settings** applies all settings configured for a specified device group to all the WAEs and WAAS Express assigned to it.

When you register a WAE to the Cisco WAAS Central Manager, consider the following uses of **Force Group Settings**:

- Because all devices in a device group have the same configuration, the configuration you apply at the device group level gets assigned to all the devices in the group. However, if a device in a device group has local settings that were either configured manually using the Cisco WAAS CLI or automatically during upgrade, its device settings may be out of sync with the rest of the device group. To remedy this:
    - To ensure that all devices in the specified group have the same configuration, use **Force Group Settings**, as described in Procedure for Forcing Device Group Settings, on page 61.
    - To avoid the need to use **Force Group Settings** after a device is registered to the Cisco WAAS Central Manager, restore the device's default factory settings before registering it to the Cisco WAAS Central Manager.

Procedure for Forcing Device Group Settings

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** > *device-group-name*.

The **Modifying Device Group** window appears.

Step 2 In the **Taskbar**, click the **Force Group Settings** icon.

The Cisco WAAS Central Manager GUI displays the following message:

The action will apply all settings configured for this device group to all the WAEs/WAAS Express assigned to it. Do you wish to continue?

Step 3 To force group settings across all devices in the device group, click **OK**.

Step 4 Click **Submit**.

Selecting Device Group Precedence

Before you begin

When a device belongs to multiple device groups that have conflicting settings, the device automatically inherits the settings from the device group that was most recently changed. For a more detailed description of how a device inherits settings when it belongs to multiple device groups, see Understanding the Impact of Assigning a Device to Multiple Device Groups , on page 63.

When a configuration conflict occurs, you can edit a device's configuration on a page-by-page basis and select which device group's settings should take precedence.

Procedure

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

The **Device Dashboard** window appears.

Step 2 From the Cisco WAAS Central Manager menu bar, choose the configuration option that contains the conflicting settings.

A drop-down list appears in the taskbar at the top of the window. This drop-down list allows you to select the device group that you want this configuration window to inherit settings from. The device group that is currently selected is the device group that has precedence.

Step 3 From the drop-down list, choose the device group that you want this configuration page to inherit settings from, and click **Submit**.

The selected configuration window changes to reflect the settings associated with the selected device group.

Overriding the Device Group Settings on a Device

Before you begin

The Cisco WAAS Central Manager GUI allows you to override the device group settings and specify new settings that are unique to that device.

Procedure

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

The **Device Dashboard** window appears.

Step 2 From the menu bar, choose the configuration option that contains the device group settings you want to override.

Step 3 In the Taskbar, click the **Override Group Settings** icon.

The settings in the selected configuration window are enabled.

Note The **Override Group Settings** icon only appears on configuration windows that have been modified on the associated device group.

Step 4 Make the necessary changes to the configuration window and click **Submit**.

The device is now configured with settings that are different from the device group it belongs to.

Note The **Force Settings on all Devices in Group** icon appears in the device group view of an overridden configuration window. To reapply the device group settings to all devices in the device group, click this icon.

Step 5 To reapply the device groups settings to this configuration window, choose the device group from the drop-down list in the Taskbar and click **Submit**.

Understanding the Impact of Assigning a Device to Multiple Device Groups

If a device belongs to multiple device groups, a configuration conflict might occur if the groups are not configured exactly the same. In this case, the device will inherit the settings from the device group that was most recently changed. In some cases, however, a device can retain settings from more than one device group depending on how the changes were implemented.

The following scenario describes how a device can retain settings from multiple device groups:

Action 1: Device A is assigned to Device Group 1 (DG1).

Result: Device A automatically inherits all the configuration settings of DG1.

Action 2: Device A is assigned to Device Group 2 (DG2) so it now belongs to two device groups (DG1 and DG2).

Result: Device A inherits all the settings from DG2, but it remains a member of DG1.

Action 3: The standard time zone setting on DG1 is changed to America New York.

Result: The time zone of Device A changes to America New York, but the device maintains all its other configuration settings from DG2.

In this scenario, Device A's configuration is a hybrid of DG1 and DG2. To specify which device group settings a device should inherit, use the override features described in Overriding Group Configuration Settings, on page 60.

Methods of Moving a Device Between Device Groups

The Cisco WAAS Central Manager GUI provides two methods to move a device from one device group to another device group.

- Select the device first: From the Cisco WAAS Central Manager menu, select the device and choose **Devices** > *device-name* > **Assign Device Groups** and use the green check mark icon next to each Devcie Group to assign a Device Group to the specified device. Similarly you can also unassign the device from the group and assign to a new device group.
- Select the Device Group first: From the Cisco WAAS Central Manager menu, select the Device Group and choose **Device Groups** > *device-group-name* > **Assign Devices** and use the green check mark icon next to each device you want to assign to the specified Device Group. You can also unassign the device from one device group and assign to a new device group.

However, when you do any of the above, configuration conflicts can occur. These are available in the configuration page for the device as a **Force Device Group** icon and can be resolved using the Procedure for Forcing Device Group Settings, on page 61.

Additionally they show up in the **Force Device Group Detection** page. This **Force Device Group** icon indicates that there is a difference between Device and Device Group configurations. The Cisco WAAS Central Manager provides an easy way to identify, view and resolve these configuration conflicts.

To move a Cisco WAAS device between two device groups that have different optimization policies, you must reassign the device to a different device group and then force the device group settings on the device.

Moving a Device Between Device Groups

Before you begin

To move a Cisco WAAS device between two device groups that have different optimization policies, you must reassign the device to a different device group and then force the device group settings on the device.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** > *old-device-group-name*.

Step 2 Choose *DeviceGroup* > **Assign Devices**.

Step 3 Click the green check icon next to the device that you want to reassign. The icon changes to a red arrow pointing left.

Step 4 Click **Submit**.

Step 5 From the Cisco WAAS Central Manager menu, choose **Device Groups** > *new-device-group-name*.

Step 6 Click the blue **X** icon next to the device that you want to reassign. The icon changes to a green arrow pointing right.

Step 7 Click **Submit**.

Step 8 Choose **Configure** > **Acceleration** > **Optimization Policies**.

Step 9 In the Taskbar, click the **Force Settings on all Devices in Group** icon.

Working with Device Locations

The Cisco WAAS Central Manager GUI allows you to create locations that you can associate with a Cisco WAAS device. You assign a device to a location when you first activate the device. The main purpose of assigning a device to a location is to help you identify a Cisco WAAS device by the physical region in which it resides. Locations are different from device groups because devices do not inherit settings from the location to which they belong.

You can view reports that aggregate data from all the devices in a particular location. For more information, see Location-Level Reports in the chapter "Monitoring Your Cisco WAAS Network."

You assign a device to a location when you activate the device as described in the Modifying Device Properties in the chapter "Configuring Other System Settings."

This section contains the following topics:

Creating Locations

Procedure

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

The **Location** window appears.

Step 2 In the Taskbar, click the **Create New Location** icon.

The **Creating New Location** window appears.

Step 3 In the **Name** field, enter a location name.

The name can contain letters, numbers, period, hyphen, underscore, and space.

Step 4 From the **Parent Location** drop-down list, choose a parent location, or choose **None**.

A location with no parent is a Level 1 location. A location with a Level 1 parent becomes a Level 2 location, and so forth. The location level is displayed after you choose a parent location, or choose None.

Step 5 To save the configuration, click **Submit**.

Step 6 (Optional) In the **Comments** field, enter comments about the location.

Step 7 Click **Submit**.

Step 8 To modify a location, choose the **Locations** window and click the **Edit** icon next to the name of the location that you want to modify.

Step 9 Assign a device to this location. For more information, see Modifying Device Properties in the chapter "Configuring Other System Settings."

Deleting Locations

Before you begin

You can delete locations as needed, as long as they are not the root locations of activated Cisco WAAS devices.

Note If a location has a device assigned to it, you can first assign the device to another location and then delete the original location.

Procedure

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

The **Modifying Location** window appears.

Step 2 In the Taskbar, click the **Delete Location** icon. You are asked to confirm your decision to delete the location.

Step 3 To confirm the action and delete the location, click **OK**.

Viewing the Location Tree

The location tree represents the network topology you configured when you assigned a parent to each location. The Cisco WAAS Central Manager GUI graphically displays the relationships between the locations configured in your Cisco WAAS network.

To view the location tree, choose **Locations > All Locations**. In the Taskbar, click the **Location Trees** icon. The location tree shows an expandable list. For each tree node, the corresponding icons show the location or device name.

CHAPTER 4

Configuring Cisco AppNav

This chapter describes how to configure Cisco AppNav, which is a hardware and software solution that simplifies network integration of WAN optimization and overcomes challenges with provisioning, visibility, scalability, asymmetry, and high availability.

This chapter includes the following topics:

About Cisco AppNav

Cisco AppNav greatly reduces dependency on the intercepting switch or router by distributing traffic among Cisco WAAS devices for optimization, by using a powerful class-and-policy mechanism. You can use Cisco WAAS nodes to optimize traffic based on sites, or applications, or both.

The Cisco AppNav solution has the ability to scale up to available capacity by taking into account Cisco WAAS device utilization because it distributes traffic among nodes. Also, the solution provides for high availability of optimization capacity by monitoring node overload and liveliness, and by providing configurable failure and overload policies.

This section contains the following topics:

Benefits of Cisco AppNav

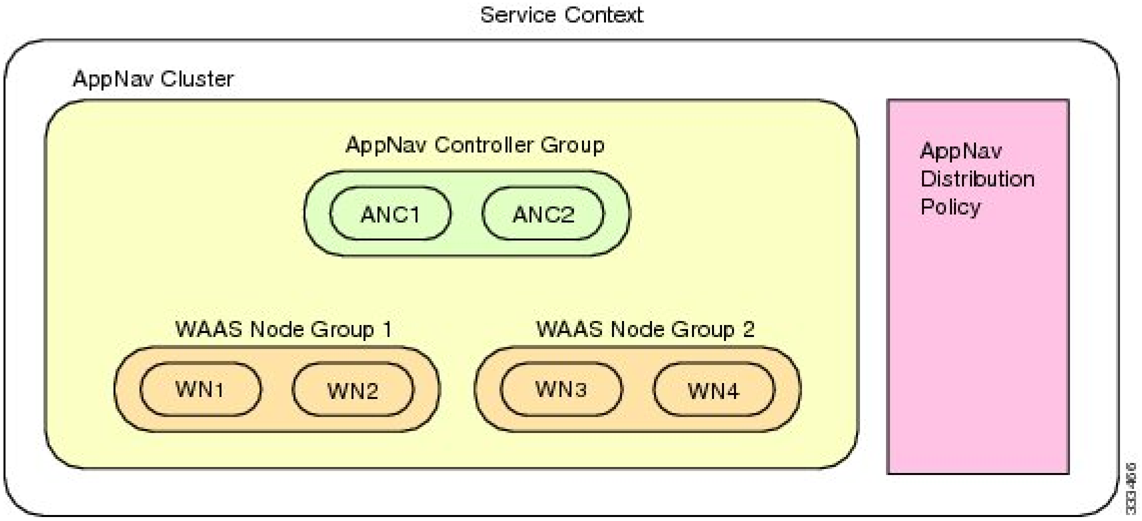
Cisco AppNav greatly reduces dependency on the intercepting switch or router by distributing traffic among Cisco WAAS devices for optimization, by using a powerful class-and-policy mechanism. You can use Cisco WAAS nodes to optimize traffic based on sites, or applications, or both.

The AppNav solution has the ability to scale up to available capacity by taking into account Cisco WAAS device utilization because it distributes traffic among nodes. Also, the solution provides for high availability of optimization capacity by monitoring node overload and liveliness, and by providing configurable failure and overload policies.

AppNav System Components

The Cisco AppNav solution consists of the following components, shown in the following figure and described in this section.

Figure 6: Cisco AppNav Solution Components



- **AppNav Controller** (ANC, or AC on the router): A device that intercepts network traffic and, based on an AppNav policy, distributes that traffic to one or more Cisco WAAS nodes (WNs) for optimization. The device can be one of the following:
  - A Cisco WAAS appliance with a Cisco AppNav Controller Interface Module
  - A Cisco router with Cisco IOS XE Release 3.9 or later, running AppNav-XE (known as an AppNav-XE device in this document).

You cannot mix the ANCs on different platforms in the same AppNav cluster.

- **AppNav Controller Group** (ANCG, or ACG on the router): A group of AppNav Controllers that together provide the necessary intelligence for handling asymmetric flows and high availability. The ANCG is configured on the ANC. An ANCG can have up to eight Cisco WAAS appliance-based ANCs or four AppNav-XE-based ANCs, which must be on the same router platform with the same memory configuration.
- **WAAS Node** (WN, or SN on the router): A Cisco WAAS optimization engine (Cisco WAE or Cisco WAVE appliance, Cisco NME-WAE or Cisco SM-SRE network module (for Cisco WAAS versions earlier than 6.4.x), or Cisco vWAAS instance, but not a Cisco WAAS Express device) that optimizes and accelerates traffic according to the optimization policies configured on the device. You can have up to 32 WNs in the cluster. (In the Cisco WAAS CLI and on the router, a Cisco WAAS node is also known as a service node.)
- **WAAS Node Group** (WNG, or SNG on the router): A group of Cisco WAAS nodes that services a particular set of traffic flows identified by AppNav policies. The WNG is configured on the ANC. You can have up to 32 WNGs in the cluster. (In the Cisco WAAS CLI and on the router, a Cisco WAAS node group is also known as a service node group.)
- **AppNav Cluster**: A group of all the ANC and WN devices within a cluster.

- **AppNav Context**: The topmost entity that groups together one AppNav Controller Group (ANCG), one or more Cisco WAAS node groups (WNGs), and an associated AppNav policy. The AppNav context is configured on the ANC. When using a Cisco WAAS appliance ANC, there is only one AppNav context. However, when using an AppNav-XE ANC, you can define up to 32 AppNav contexts that are associated with different Virtual Routing and Forwarding (VRF) instances defined on the router.

Within a service context, Cisco WAAS devices can operate in one of two modes:

- **Application accelerator**: The device serves only as a WN within the service context. It receives traffic from the ANC, optimizes the traffic, and returns the traffic to the ANC to be delivered to its destination. The WN can be any kind of WAAS device or Cisco vWAAS instance.
- **AppNav Controller**: The device operates as an ANC that intercepts network traffic, and, based on a flow policy, distributes that traffic to one or more Cisco WAAS nodes for optimization. Only a Cisco WAVE appliance that contains an AppNav Controller Interface Module, or an AppNav-XE device, can operate as an ANC. A Cisco WAAS appliance ANC can also operate as a Cisco WAAS node and optimize traffic as part of a WNG.

AppNav Controller Deployment Models and Modes

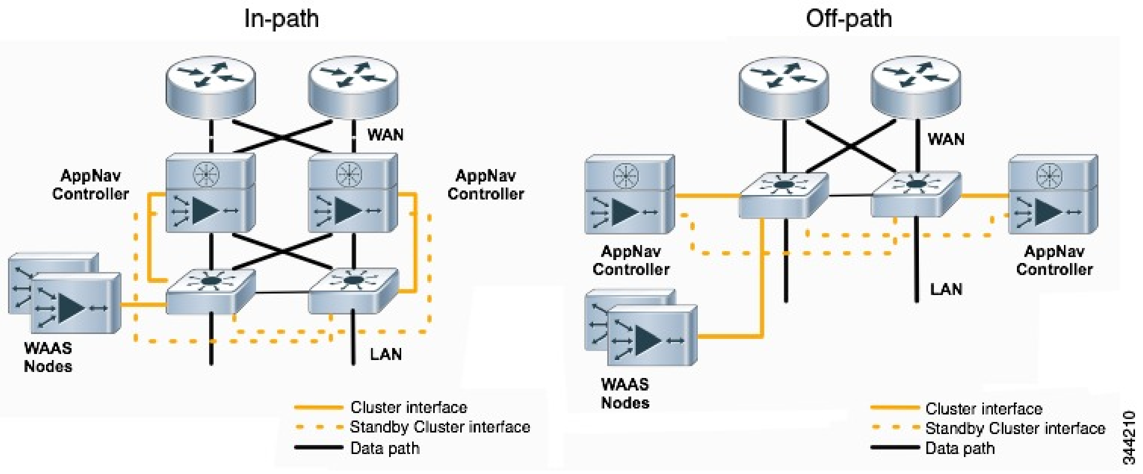
As shown in the following figure, you can deploy Cisco WAAS appliance AppNav Controllers (ANCs) in your network in two ways, in-path or off-path:

- **In-Path deployment**: The ANC is physically placed between one or more network elements, enabling traffic to traverse a bridge group configured on the device in inline mode.
- **Off-Path deployment**: The ANC works with the network infrastructure to intercept traffic through the Web Cache Communication Protocol (WCCP).

The ANC provides the same features in both in-path and off-path deployments. In either case, only ANCs participate in interception from the switch or router. The ANCs then distribute flows to WNs using a consistent and predictable algorithm that considers configured policies and Cisco WAAS node utilization.

The following figure shows that Cisco WAAS Nodes can be attached to either or both switches in the diagrams.

Figure 7: Cisco WAAS Appliance AppNav Deployment Models

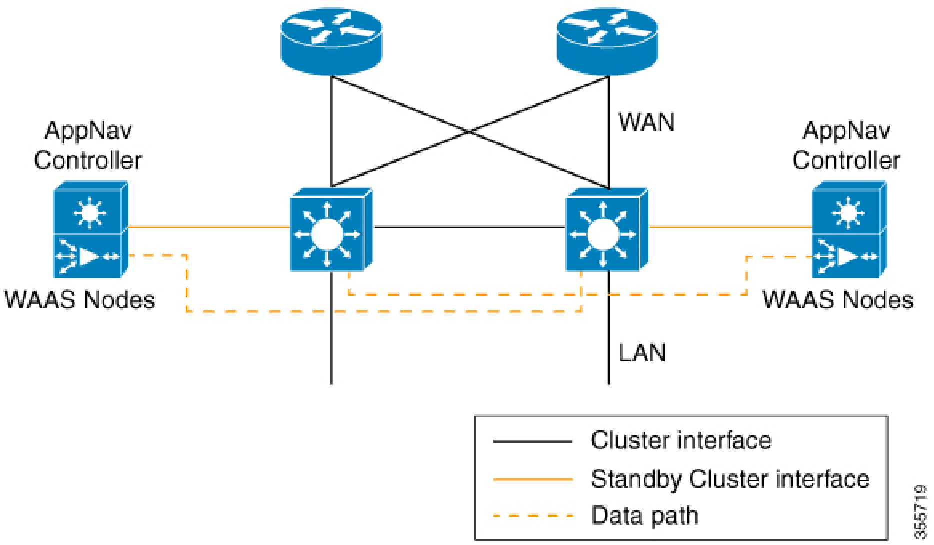


AppNav-XE ANCs have deployment models similar to the in-path diagram shown in the following figure. You can see the specific deployment diagrams in the Cisco WAAS Central Manager cluster wizard when you choose a platform.

Combination Mode

A Cisco WAAS device, which has an AppNav IOM card installed, can be configured to perform traffic interception using the AppNav module, and perform optimization as a single device. This is **Combination mode**, an example of which is shown in the following figure.

Figure 8: Devices in Combination Mode (Off-Path Deployment)



A combination mode deployment is not recommended due the limitation of single point failure as explained below.

Limitation

In a combination deployment, a single AppNav IOM module failure impacts both the AppNav and Cisco WAAS functionality. All the traffic to a WAAS node is blocked leading to a loss of active sessions in Cisco WAAS. The WAAS node on the combination device becomes unreachable and is removed from the distribution list as shown below. Note that this is applicable for both In-path and Off-path deployments.

Figure 9: Devices Failure in Combination Mode (Off-Path Deployment)

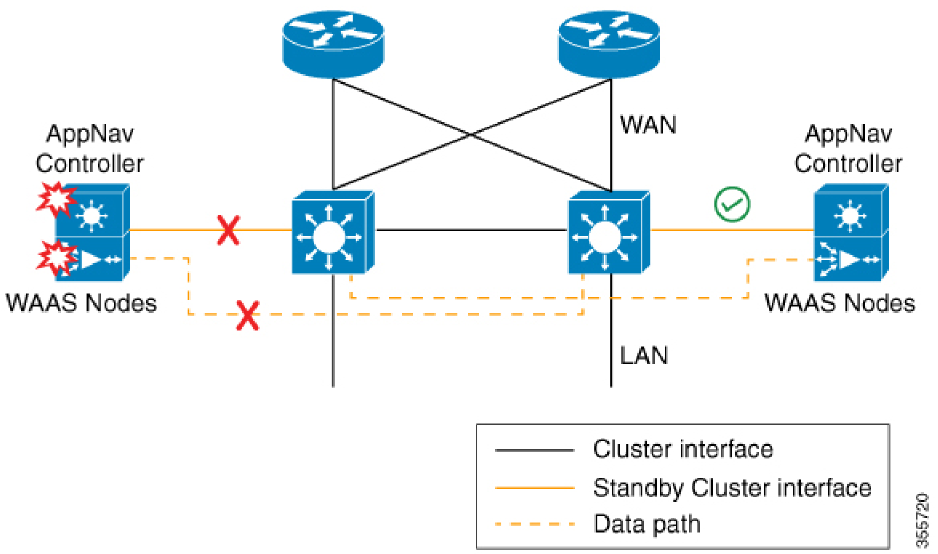
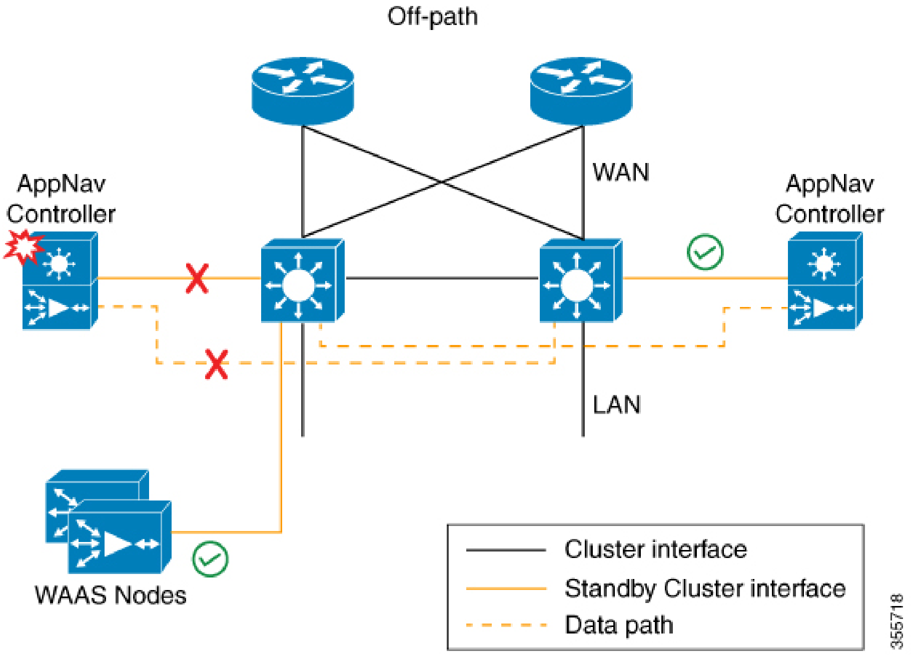


Figure 10: AppNav IOM and WAAS Nodes in Separate Devices (Off-Path Deployment)



You may experience some delay during cluster convergence when the AppNav IOM module comes back on line. Until then, other devices in the cluster will handle the new flows.

Recommendation

Considering the technical limitation in the combination mode, we strongly recommend to use separate devices for AppNav IOM and WAAS node to avoid a single point failure.

AppNav Controller Interface Modules

A Cisco WAAS appliance operating as an ANC requires a Cisco AppNav Controller Interface Module. A Cisco AppNav Controller Interface Module is similar to a standard Cisco WAVE appliance interface module, but contains additional hardware, including a network processor and high-speed Ternary Content Addressable Memory (TCAM), to provide intelligent and accelerated flow handling. The following AppNav Controller Interface Modules are supported:

- 1-GB copper 12-port AppNav Controller Interface Module
- 1-GB SFP 12-port AppNav Controller Interface Module
- 10-GB SFP+ 4-port AppNav Controller Interface Module

AppNav Controller Interface Module interfaces are configured differently to support either in-path or off-path models of deployment:

- **In-path**: The ANC operates in inline interception mode with at least one inline bridge group configured on the AppNav Controller Interface Module. A bridge group consists of two or more physical or logical (port channel) interfaces.
- **Off-path**: The ANC operates in WCCP interception mode with one physical or logical (standby or port channel) interface configured with an IP address.

Interfaces on the AppNav Controller Interface Module can have three functions:

- **Interception**: Used to receive traffic intercepted from the network and egress traffic to the network. The interception interface is implied based on the AppNav Controller placement and does not require explicit configuration for this function.
- **Distribution**: Used to distribute traffic to the WNs and receive egressed traffic from the WNs. The distribution interface is explicitly configured as the cluster interface for intracluster traffic and must be assigned an IP address.
- **Management**: A management interface can be optionally and exclusively designated for management traffic and isolated from the normal data path. We recommend that you use one of the appliance's built-in interfaces for management traffic and reserve the high-performance interfaces on the AppNav Controller Interface Module for interception and distribution.

For best performance, use separate interfaces for interception and distribution. However, you can use the same interface for both functions.

AppNav Controller Interface Modules support port channel and standby logical interfaces. A port channel allows you to increase the bandwidth of a link by combining multiple physical interfaces into a single logical interface. A standby interface allows you to designate a backup interface in case of a failure.

Interfaces on the AppNav Controller Interface Module support the following:

- A maximum of seven port channels with up to eight physical interfaces combined into a single port channel group.
- A maximum of five bridge groups configured over the physical or logical interfaces.

Interfaces on the AppNav Controller Interface Module do not support the following:

- Fail-to-wire capability

- Bridge Virtual Interfaces (BVIs)

AppNav Policy

The AppNav policy is a flow distribution policy that allows you to control how ANCs distribute traffic to the available WNs.

The AppNav policy consists of class maps that classify traffic according to one or more match conditions and a policy that contains rules that specify distribution actions to WNGs for each of the classes.

This section contains the following topics:

Class Maps

AppNav class maps classify traffic according to one or more of the following match conditions:

- Peer device ID: Matches traffic from one peer Cisco WAAS device, which could be handling traffic from a single site or a group of sites.

  You can use this kind of matching to classify all traffic from a peer device that serves one branch office.

- 3-tuple of source IP, or destination IP, or destination port (matches traffic from a specific application).

  For example, you can use this kind of matching to classify all HTTP traffic that uses port 80.

- A mix of one peer device ID and the source IP, or destination IP, or destination port (matches application-specific traffic from one site).

  For example, you can use this kind of matching to classify all HTTP traffic that is from a peer device that serves the branch office.

The **class-default** class map (or **APPNAV-class-default** on AppNav-XE clusters) is a system-defined default class map that is defined to match any traffic. By default, it is placed in the last rule in each policy to handle traffic that is not matched by other classes.

Policies

An AppNav Controller matches incoming flows to class maps and the policy rules in a policy associate class maps with actions, such as distributing a flow to a particular WNG for optimization. The order in which rules are listed in the policy is important. Starting at the top of the policy, the first rule that matches a flow determines to which WNG it is distributed.

A policy rule can specify four kinds of actions to take on a flow:

- Specify the primary WNG to which to distribute the flow (required).
- Specify a backup WNG for distribution if the primary WNG is unavailable or overloaded (optional; not supported on AppNav-XE clusters).

Note Even though a new WNG or SNG can become operational without having an AppNav policy attached, in order to have your Cisco WAAS system work successfully, configure and attach an AppNav policy to each new WNG or SNG.

The primary WNG receives all traffic until all WNs within the group become overloaded (reach 95 percent of the maximum number of connections) or are otherwise unavailable, and then traffic is distributed to the backup WNG. If a WN in the first WNG becomes available, traffic is again distributed there. If all WNs in both the WNGs become overloaded, traffic is passed through unoptimized.

- Monitor the load on the application accelerator that corresponds to the application traffic matched by the class (optional).

If the monitored application accelerator on one WN in a WNG becomes overloaded (reaches 95 percent of its maximum number of connections), the WN is considered overloaded and traffic is directed to another WN in the group. If all WNs become overloaded, traffic is distributed to the backup WNG. This application accelerator monitoring feature is useful for ensuring optimization for critical applications and is recommended for the MAPI and SMB accelerators.

- Specify a nested policy to apply to the flow (optional; not supported on AppNav-XE clusters).

For more information, see Nested Policies, on page 74.

Within a WNG, flows are distributed among WNs using a hash. If a WN reaches its maximum capacity or becomes unavailable, it is not sent new flows. New flows are sent to other available WNs in the WNG so that they can be optimized successfully. If an unavailable WN later becomes available again, the same client/server pairs will hash to this WN as before.

Note If a WAAS Node that is doing MAPI or ICA application acceleration becomes overloaded, flows associated with existing MAPI and ICA sessions continue to be sent to the same WN due to the requirement that the same WN handles these types of flows. New MAPI and ICA flows, however, are distributed to other WNs.

The AppNav policy is specific to each ANC, though typically, all the ANCs in a cluster have the same policy. Each ANC consults its AppNav policy to determine which WNG to use for a given flow. Different ANCs in a cluster can have different AppNav policies, which allows you to customize distribution in certain cases. For example, when a cluster contains ANCs and WNs that are in different locations, it may be more desirable for an ANC to distribute traffic to WNs that are closer to it.

Note On AppNav-XE clusters, the AppNav policy must be the same on all the ANCs in a context.

Nested Policies

A policy rule can specify one nested policy, which allows traffic identified in a class to be subdivided and handled differently. Nested policies provide two advantages:

- They allow another policy to be used as a common subclassification tool.

  For example, you can define a policy that contains monitoring actions and apply it as a subpolicy to multiple classes in the primary policy.

- They provide a method of including class maps with both match-any and match-all characteristics into a single subclass.

The nested policy feature is designed for use with site-based classes (matched by peer ID) at the first-level and application-based subclasses (matched by IP address/port) at the second level. Only the first level policy can contain classes that use match peer conditions.

Note AppNav-XE clusters do not support nested policies.

Site and Application Affinity

This section contains the following topics:

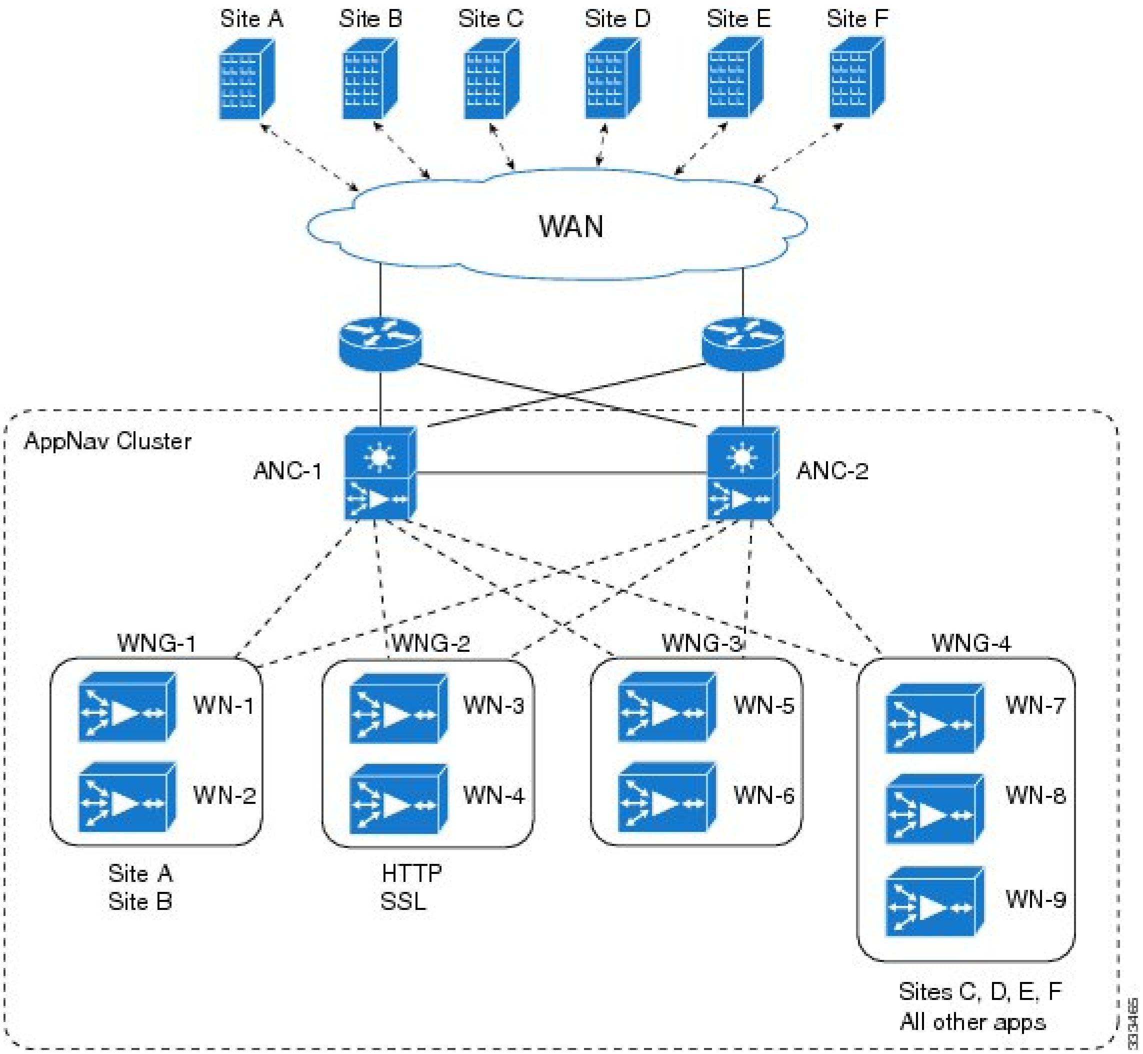
About Site and Application Affinity

You can provision a WNG to serve specific peer locations (site affinity) or applications (application affinity) or a combination of the two. Using a WNG for site or application affinity provides the following advantages:

- **Provisioning**: Localize a class of traffic to achieve control over provisioning and performance monitoring. For example, a business-critical application such as Sharepoint or a business-critical site can be given assured capacity and monitored closely for performance.
- **Enhanced application performance**: Better compression performance is achieved by limiting data that belongs to a site, to one or a few WNs, which results in better utilization of the Data Redundancy Elimination (DRE) cache.

The following figure shows how sites and applications can be associated with node groups. In this figure, the following WNGs are defined:

Figure 11: Flow Distribution Using Site and Application Affinity



- **WNG-1**: Consists of two WNs that process flows coming only from Site A and Site B.
- **WNG-2**: Consists of two WNs that process HTTP and SSL flows from any site. Whether HTTP and SSL flows from Site A and Site B should be processed by WNG-2 or WNG-1 is determined by the order of rules in the policy.
- **WNG-3**: Consists of two WNs that process MAPI flows coming from any site. Whether MAPI flows from Site A and Site B should be processed by WNG-3 or WNG-1 is determined by the order of rules in the policy.
- **WNG-4**: Consists of three WNs. The class-default class is applied to this WNG so that it all the flows that do not match any other class map are sent to it.

Site Affinity Operating Guidelines

Consider the following site affinity operating guidelines:

- Site affinity provides you with the ability to always send all the traffic from one site to a specific WNG, which allows you to reserve optimization capacity for critical sites and to improve compression performance through better utilization of the DRE cache.
- Traffic from any location, not just a single site, can be matched in a class map and associated with a WNG.
- You can implement site affinity by configuring a class map that matches the device ID of the WAE in the site. If a site has more than one WAE in a WCCP farm or a serial inline cluster, specify multiple device IDs in the class map. Next, associate the class map with a distribution action to a WNG in a policy rule. You can also identify sites using source IP addresses or subnets in the class map, if you know what IP addresses are used in the site and keep the policy configuration consistent with site IP addresses. However, we recommend that you use peer device IDs when configuring site affinity.
- A peer ID-based class map works only for matching flows that carry the Cisco WAAS autodiscovery TCP options. If you configure a class to match a site peer ID at the data center, the same class does not match flows that originate in the other direction, such as those flows that originate from the data center and go back to the same site. Such flows are usually small in number compared to the site-to-data center flows.
    - If you want flows in both directions to go to the same WNG, you must configure two class maps: one to match in the site-to-data center direction, typically using the site device ID; and another to match the data center-to-site direction, using destination IP subnets belonging to the site. Both class maps can be configured to distribute traffic to the same WNG. A mesh network is a specific use case where flows can originate in either direction.
    - If the site WAE is in overload or does not mark the SYN packet with autodiscovery options for any other reason, the ANC cannot match it to the peer match class map.

Application Affinity Operating Guidelines

Consider the following application affinity operating guidelines:

- Application affinity gives you the ability to always send certain application traffic to a specific WNG, which allows you to reserve optimization capacity for different applications depending on business priorities.
- In the context of AppNav flow distribution, an application is defined using a three-tuple of source IP, destination IP, and destination TCP port. The actual type of traffic does not matter for flow distribution. For example, you can use separate WNGs for HTTP traffic that is addressed to different destination ports or different server IP addresses. Destination IP and ports are most useful in using application affinity, but having the source IP also helps you to define the traffic of interest.
- A small number of protocols, such as FTP, use dynamic destination ports. An FTP server in active mode originates a data connection back to the FTP client using a dynamic destination port. This port is exchanged over the control channel from client to server using the well-defined destination **port 21**. Consider trying to define a class map for FTP. Because the destination port is not known in advance, you cannot map both control and data connections to the same class.

  In this case, we recommend that you use the client IP addresses or subnets to match the destination IP addresses for the data connections. You must configure two class maps: one for the control channel, using destination **port 21**, and another for the data channel, using destination IP addresses. You can configure policy rules so that both class maps distribute traffic to the same WNG.

- You can further classify traffic from a site into applications by combining the peer matches with three-tuple matches in a match-all class map, called a Custom class map type, in the Cisco WAAS Central Manager.

Default Policy Behavior

The following default class maps are provided:

- **Citrix**: Matches traffic for destination port 1494 and 2598
- **epmap**: Matches traffic for destination port 135
- **HTTP**: Matches traffic for destination ports 80, 3128, 8000, 8080, and 8088
- **HTTPS**: Matches traffic for destination port 443
- **MAPI**: Matches traffic for the MS RPC MAPI application (dynamic port assignment)
- **RTSP**: Matches traffic for destination ports 554 and 8554
- **class-default** or **APPNAV-class-default**: Matches any TCP traffic. This class map cannot be edited or deleted.

If you use the Cisco WAAS Central Manager AppNav Cluster wizard to create an AppNav Cluster, the wizard creates a default policy. This policy is assigned by default to all the ANCs in a cluster and contains only the class-default policy rule (APPNAV-class-default on AppNav-XE clusters) that has the following characteristics:

- Matches class-default (any TCP) traffic (APPNAV-class-default on AppNav-XE clusters).
- Distributes class-default traffic to the default WNG, which includes all the WNs created by the wizard, with no backup WNG specified.
- Contains the **waas_app_default** nested policy, which provides application monitoring for each of the default class maps. (Not used on AppNav-XE clusters, which do not support nested policies.)

  When you use the Cisco WAAS Central Manager to define a policy rule for any class that uses peer matching or source or destination IP address matching (but not port matching), it automatically adds the waas_app_default policy as a nested policy. The **waas_app_default** policy is created by the system and monitors all application accelerators, so you do not need to manually add application accelerator monitoring to your policy rules.

If you do not use the Cisco WAAS Central Manager AppNav Cluster Wizard to create a cluster, there is no default flow distribution. Therefore, if an incoming flow does not match any class in the AppNav policy, it is not distributed to any WNG; instead, it is passed through.

If a WNG is defined, but is not used in any policy rule, it does not receive any flows. If a policy is defined, but not applied to an ANC, it does not take effect.

The default action for a policy rule is none, which is context dependent: in a top-level policy, it means pass-through, and if the policy is nested, it means inherit-the-parent-policy-rule action.

Prerequisites for AppNav Deployment

Consider the following prerequisites for AppNav deployment:

- Each Cisco WAAS appliance to be used as an AppNav Controller must contain a Cisco AppNav Controller Interface Module.
- Each Cisco WAAS appliance AppNav Controller must be configured in appnav-controller device mode.
- If you are using AppNav-XE devices, they must be registered and activated in the Cisco WAAS Central Manager before the Cisco WAAS Central Manager can manage them. For more information on registering AppNav-XE devices, see Managing Cisco IOS Router Devices in the chapter "Configuring Other System Settings."

Note You can use an AppNav-XE device in a small deployment without a Cisco WAAS Central Manager by configuring the cluster from the AppNav-XE device CLI. For more information, see the corresponding router documentation on www.cisco.com.

Guidelines for AppNav Deployment

This section contains the following topics:

General Deployment Guidelines

Consider the following general deployment guidelines:

- AppNav class maps and policies can be configured only at the cluster level, not at the device level, from the Cisco WAAS Central Manager. At the device level, class maps and policies can only be viewed.
- There is no fail-to-wire capability on AppNav Controller Interface Module interfaces configured in bridge groups for inline mode, which would allow traffic to bypass the interface if the device fails or loses power. Therefore, if you are using inline mode, we recommend that you deploy two or more AppNav Controller appliances to provide high availability.
- When configuring a nested class map as a match condition from the CLI you can nest up to four layers. This configuration does not show up as a **Force Device Group** conflict on the Cisco WAAS Central Manager page but is listed as an exception in the error logs of the CLI.

Guidelines for AppNav Devices and Clusters

Consider the following configuration guidelines for AppNav devices and clusters:

- An AppNav Cluster can contain a maximum of:
  - 8 ANCs if you are using Cisco WAAS appliances, or 4 ANCs if you are using AppNav-XE devices.
  - 32 WNs, or 64 WNs if you are configuring an AppNav-XE cluster.
  - 32 WNGs
  - A service context if you are using Cisco WAAS appliances or 32 service contexts if you are using AppNav-XE devices.

- You cannot mix ANCs on different platforms in an AppNav Cluster.
- All the ANCs in an ANCG must have the same set of ANCs and WNGs in their configuration.
- All the WNs in a WNG must have identical optimization policies configured.
- You can define the following maximum policy entities within a service context on a Cisco WAAS appliance cluster:
    - 1024 match conditions
    - 512 AppNav class maps
    - 64 rules per AppNav policy
    - 64 AppNav policies, though only one policy is actively bound to the service context and used for flow distribution on a given ANC

Guidelines for AppNav-XE Devices and Clusters

Consider the following configuration guidelines for AppNav-XE devices and clusters:

- On AppNav-XE devices, all the ANCs in the cluster must have an identical AppNav configuration (such as class maps, policy maps, VRFs). In an AppNav- XE cluster, all AppNav-XE devices must be of the same hardware model.
- You can define the following maximum policy entities for an AppNav-XE cluster:
    - 32 match conditions per class map
    - 16384 AppNav class maps
    - 1000 rules per AppNav policy
    - 1024 AppNav policies
- On AppNav-XE devices, do not use VRF to access the WNs from the ANCs.
- On AppNav-XE devices, do not use a port channel between the ANCs and the WNs because traffic is transmitted over a GRE tunnel and all traffic is switched on one link.
- An AppNav-XE device cannot intercept Overlay Transport Virtualization (OTV) traffic that is configured on the interception interface.
- If you have configured an AppNav-XE device by using the EZConfig CLI utility on the router, you cannot manage the AppNav-XE device with the Cisco WAAS Central Manager. To switch between managing the AppNav-XE device with the EZConfig utility on the router and the Cisco WAAS Central Manager, either delete the AppNav-XE cluster and contexts by using the router CLI or register the devices with the Cisco WAAS Central Manager and wait for the device configuration to synchronize (about 10 minutes). Then re-create the cluster and contexts by using the Cisco WAAS Central Manager. To switch from using the Cisco WAAS Central Manager to manage the AppNav-XE configuration to using the router CLI, delete the cluster and contexts from the Cisco WAAS Central Manager and then re-create the cluster and contexts by using the router CLI or EZConfig utility.

Configuring an AppNav Cluster

This section contains the following topics:

Workflow for Configuring an AppNav Cluster

You must complete the following steps to configure an AppNav Cluster:

1. Install and configure the individual ANC and WN devices with basic network settings.

   For Cisco WAAS appliances, see Configuring Cisco WAAS Device Interfaces, on page 82.

   For AppNav-XE devices, see the router documentation.

2. Create an AppNav cluster with the Cisco WAAS Central Manager AppNav Cluster Wizard.

   Use the Cisco WAAS Central Manager AppNav Cluster Wizard to create a cluster and configure the interception mode, configure cluster settings, choose cluster devices, configure VRFs (for AppNav-XE), configure traffic interfaces, and configure WCCP settings if you are using WCCP. AppNav-XE. See Creating a New AppNav-XE Cluster with the AppNav Cluster Wizard, on page 88.

   Use the Cisco WAAS Central Manager, only, to create AppNav cluster. Do not use the Cisco WAAS CLI to create the AppNav cluster.

   In addition to this: adding, modifying or deleting a Service Node or Service Context must also be done from WCM GUI. We do not recommend using the Cisco WAAS CLI for any of these operations.

   If cluster configuration changes are done from the Cisco WAAS CLI, then the cluster configuration between the device and the Cisco WAAS Central Manager will go out of sync, which will result in incorrect cluster-configuration information displayed in the Cisco WAAS Central Manager GUI.

3. (Optional) Configure AppNav class maps.

   This step is necessary only if you want to customize the default class map configuration. The system adds several default class maps that match traffic corresponding to most of the application accelerators and a class-default class map that matches all traffic. See Configuring Class Maps, on page 92.

4. (Optional) Configure an AppNav policy.

   This step is necessary only if you want to customize the default policy. The system adds a default policy that distributes all traffic to the WNG-Default WNG, which is the node group into which all WNs are grouped by default. See Configuring AppNav Policies, on page 92.

5. (Optional) Configure Cisco WAAS node optimization class maps and policy rules.

   This step is necessary only if you want to customize the default optimization policy that is listed in Appendix A, "Predefined Application Policies."

6. (Optional) Configure an interception ACL on Cisco WAAS appliance ANCs.

   See Configuring AppNav Controller ACLs, on page 108

Operating Guidelines for AppNav Clusters and Service Nodes

- Use the Cisco WAAS Central Manager, only, to create AppNav cluster. Do not use the Cisco WAAS CLI to create the AppNav cluster.

- Use the Cisco WAAS Central Manager, only, to add, modify, or delete a Service Node or Service Context. Do not use the Cisco WAAS CLI for any of these operations.

Note If cluster configuration changes are done using the Cisco WAAS CLI, then the cluster configuration between the device and the Cisco WAAS Central Manager will go out of sync, which will result in incorrect cluster-configuration information displayed in the Cisco WAAS Central Manager GUI.

Configuring Cisco WAAS Device Interfaces

Before using the AppNav Cluster wizard to create an AppNav Cluster, connect the Cisco WAAS device interfaces and configure the management interfaces. Configuration differs depending on whether management traffic uses a separate interface or shares the traffic handling interface.

For more information on device interface configuration, see the chapter Configuring Network Settings, on page 187. For more information about configuring a bridge group for inline interception mode, see Configuring Inline Operation on ANCs in the chapter "Configuring Traffic Interception."

For information on configuring interfaces on AppNav-XE devices, see your Cisco router documentation.

This section contains the following topics:

Interface Configuration with a Separate Management Interface

This section contains the following topics:

Configuring an AppNav Controller as a Separate Management Interface

Procedure

Step 1 Connect the last AppNav Controller Interface Module port to the switch/router port for the cluster traffic.

For example, this port is GigabitEthernet 1/11 on a 12-port module or TenGigabitEthernet 1/3 on a 4-port module.

Step 2 Connect a built-in Ethernet port to the switch/router port for the management interface.

Step 3 For an in-path (inline) deployment, connect the first pair of ports on the AppNav Controller Interface Module, for example, GigabitEthernet 1/0 (LAN) and GigabitEthernet 1/1 (WAN) for bridge 1, to the corresponding switch/router ports.

If the ANC is connected to a second router for a dual inline deployment, connect the second pair of ports on the AppNav Controller Interface Module, for example, GigabitEthernet 1/2 (LAN) and GigabitEthernet 1/3 (WAN) for bridge 2, to corresponding switch/router ports.

Step 4 Use the device **setup** command to configure the following settings:

- Configure the device mode as **AppNav Controller**.
- Configure the IP address and netmask of the built-in management port.
- Configure the built-in management port as the primary interface.

- Configure the other network and basic settings (such as default gateway, DNS, and NTP server).
- Register the device with the Cisco WAAS Central Manager by entering the Cisco WAAS Central Manager IP address.

Step 5 Configure the IP address and netmask of the last AppNav Controller Interface Module port, and do *not* use DHCP. You can also configure these settings through the AppNav Cluster wizard.

Configuring a WAAS Node as a Separate Management Interface

Procedure

Step 1 Connect a built-in Ethernet port to the switch/router port for management interface.

Step 2 Use the device setup command to configure the following settings:

- Configure the device mode as **Application Accelerator**.
- Configure the IP address and netmask of the built-in management port.
- Configure the built-in management port as the primary interface.
- Configure the other network and basic settings (such as default gateway, DNS, and NTP server).
- Register the device with the Cisco WAAS Central Manager by entering the Cisco WAAS Central Manager IP address.

Interface Configuration with a Shared Management Interface

This section contains the following topics:

Configuring an AppNav Controller as a Shared Management Interface

Procedure

Step 1 Connect the last AppNav Controller Interface Module port to the switch/router port for cluster traffic. For example, this port is GigabitEthernet 1/11 on a 12-port module or TenGigabitEthernet 1/3 on a 4-port module.

Step 2 For an in-path (inline) deployment, connect the first pair of ports on the AppNav Controller Interface Module, for example, GigabitEthernet 1/0 (LAN) and GigabitEthernet 1/1 (WAN) for bridge 1, to corresponding switch/router ports.

If the ANC is connected to a second router for a dual inline deployment, connect the second pair of ports on the AppNav Controller Interface Module, for example, GigabitEthernet 1/2 (LAN) and GigabitEthernet 1/3 (WAN) for bridge 2, to corresponding switch/router ports.

Step 3 Use the device **setup** command to configure the following settings:

- Configure the device mode as **AppNav Controller**.

- Configure the IP address and netmask of the last AppNav Controller Interface Module port. Do not use DHCP.
- Configure the last AppNav Controller Interface Module port as the primary interface.
- Configure the other network and basic settings (such as default gateway, DNS, and NTP server).
- Register the device with the Cisco WAAS Central Manager by entering the Cisco WAAS Central Manager IP address.

Configuring a WAAS Node as a Shared Management Interface

Procedure

Step 1 Connect a built-in Ethernet port to the switch/router port for management interface.

Step 2 Use the device **setup** command to configure the following settings

- Configure the device mode as **Application Accelerator**.
- Configure the IP address and netmask of the built-in management port.
- Configure the built-in management port as the primary interface.
- Configure the other network and basic settings (such as default gateway, DNS, and NTP server).
- Register the device with the Cisco WAAS Central Manager by entering the Cisco WAAS Central Manager IP address.

Interface Configuration Guidelines

Consider the following guidelines for Cisco WAAS device interface configuration:

- On an ANC, the intercepted traffic must go through an interface on the AppNav Controller Interface Module.
- On an ANC that also serves as a WN, the cluster interface is the same as the interception interface.
- On a WN, cluster traffic can be handled on any interface, either built-in or on an interface module.
- To simplify AppNav deployment, the AppNav Cluster Wizard uses the following conventions for configuring the AppNav Controller Interface Module ports on an ANC:
    - The default port for cluster traffic is the last port on the module, for example, GigabitEthernet 1/11 on a 12-port module or TenGigabitEthernet 1/3 on a 4-port module.
    - For an in-path (inline) deployment, the default interception bridge is the first pair of ports on the module, for example, GigabitEthernet 1/0 (LAN) and GigabitEthernet 1/1 (WAN) for bridge 1. If the ANC is connected to a second router for a dual inline deployment, the default second interception bridge is the second pair of ports on the module, for example, GigabitEthernet 1/2 (LAN) and GigabitEthernet 1/3 (WAN) for bridge 2.

The AppNav Cluster Wizard uses four predefined deployment models to help simplify configuration on a Cisco WAAS appliance. Each deployment model expects interfaces to be connected and configured in a particular way, except for the **Custom** option, which allows you to configure interfaces in any way. Before you run the wizard with one of the four predefined models, the required interfaces must be in either of these states:

- Not configured with an IP address and netmask and not used as part of another logical interface. (However, the last port on the AppNav Controller Interface Module can be configured with an IP address because it is the default port for cluster traffic.)

  The **AppNav Cluster Wizard** configures all required traffic interface settings.

- Configured as expected by the AppNav Cluster Wizard according to the following predefined deployment model expectations:

  Single AppNav Controller WCCP Interception with a 12-port AppNav Controller Interface Module

  - Port channel 1: Contains ports GigabitEthernet 1/10 and 1/11
  - Cluster interface: Port channel 1

  Single AppNav Controller WCCP Interception with a 4-port AppNav Controller Interface Module

  - Cluster interface: GigabitEthernet 1/3

  Dual AppNav Controllers WCCP Interception with a 12-port AppNav Controller Interface Module

  - Port channel 1: Contains ports GigabitEthernet 1/10 and 1/11
  - Port channel 2: Contains ports GigabitEthernet 1/8 and 1/9
  - Standby group 1: Contains interfaces Port channel 1 (primary) and Port channel 2
  - Cluster interface: Standby Group

  Dual AppNav Controllers WCCP Interception with a 4-port AppNav Controller Interface Module

  - Standby group 1: Contains ports GigabitEtherne 1/2 and 1/3 (primary)
  - Cluster interface: Standby Group

  Single AppNav Controller Inline Interception

  - Interception Bridge 1: Contains ports GigabitEthernet 1/0 (LAN) and 1/1 (WAN)
  - Cluster Interface: GigabitEthernet 1/11

  Dual AppNav Controllers WCCP Interception

  - Interception Bridge 1: Contains ports GigabitEthernet 1/0 (LAN) and 1/1 (WAN)
  - Interception Bridge 2: Contains ports GigabitEthernet 1/2 (LAN) and 1/3 (WAN)
  - Standby Group 1: Contains ports GigabitEthernet 1/10 and 1/11 (primary)
  - Cluster Interface: Standby Group 1

Creating a WAAS Appliance AppNav Cluster with the AppNav Cluster Wizard

Before you begin

- Set up the individual ANC and WN devices as described in Configuring Cisco WAAS Device Interfaces.
- Ensure that all ANCs are configured for AppNav Controller device mode. If you need to change the device mode, see Changing Device Mode in the chapter "Planning Your Cisco WAAS Network."
- Use the Cisco WAAS Central Manager to configure basic settings for all devices such as NTP server, AAA, and logging.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters > All AppNav Clusters**.

The **Manage AppNav Clusters** window appears.

Step 2 Click the **AppNav Cluster Wizard** icon in the taskbar of the **Manage AppNav Clusters** area.

The **AppNav Cluster Wizard** window appears.

Step 3 From the **AppNav platform** drop-down list, choose **WAVE Appliance**.

Step 4 From the **Deployment model** drop-down list, choose one of the following deployment models that matches your deployment:

- **Single AppNav Controller WCCP interception**
- **Dual AppNav Controllers WCCP interception**
- **Single AppNav Controller Inline interception**
- **Dual AppNav Controllers Inline interception**
- **Custom**: For a deployment that does not match one of the above choices. To select a deployment model other than custom, go through the Interface Configuration Guidelines, on page 84.

Click **Next**.

Step 5 If you chose the **Custom** deployment model, from the **Interception method** drop-down list, choose the WCCP or **Inline interception** method and click **Next**.

Step 6 Define the cluster settings by entering the following information:

- In the **Name** field, enter a unique name for the cluster. This name should be different from the name used for a Device Group. Otherwise, an error message stating that the name already exists is displayed. Use only letters, numbers, hyphen, and underscore, up to a maximum of 32 characters and beginning with a letter.
- (Optional) In the **Description** field, enter a description of the cluster. Use only letters and numbers, up to a maximum of 200 characters.
- Check the **Disable Distribution** check box if you want make the cluster operate in monitoring mode, otherwise, it is activated when the wizard finishes. In monitoring mode, all traffic is passed through instead of being distributed to WNs.

Step 7 Click **Next**.

Step 8 Choose the ANC and WN devices that you want to be part of the cluster:

a) Choose up to eight ANCs in the AppNav Controller device list by clicking the check box next to the device names. You can use the filter settings in the taskbar to filter the device list.
b) (Optional) To enable optimization on the ANC devices, check the **Enable WAN optimization on selected AppNav Controllers** check box (it may be enabled or disabled by default, depending on the deployment model you chose).
c) Choose up to 32 WNs in the **WAAS Nodes** device list by clicking the check box next to the device names. You can use the filter settings in the taskbar to filter the device list.

   If there are devices that are ineligible to join the cluster, click **Show Ineligible Devices** to see them and the reasons why they are ineligible. You can use the filter settings to filter the list.

Step 9 Click **Next**.

Step 10 Verify the cluster interface, IP address, and netmask for each device in the cluster. The wizard automatically selects recommended cluster interfaces that should be configured. To edit the IP address and netmask settings for a device, choose the device and click the **Edit** taskbar icon.

Note This window does not appear if you are configuring a custom cluster.

Step 11 Click **Finish** if you are using inline interception (and you are done) or click **Next** if you are using WCCP interception (and continue with the following steps for WCCP).

Step 12 (Optional) Configure the WCCP settings for the ANC. This window does not appear if you are configuring an inline cluster.

For more information on configuring WCCP, see Configuring WCCP on Cisco WAEs in the chapter "Configuring Traffic Interception."

a) Ensure that the **Enable WCCP Service** check box is checked if you want to enable WCCP. This item appears only if you are defining a custom cluster.
b) Verify the single WCCP service ID of 61 (default), or change it if desired.

   Configure only this single WCCP service on both the ingress and egress ports of the router doing WCCP redirection to this ANC.

c) (Optional) If you want to enable two WCCP services, uncheck the **Enable Single Service Mode** check box (it is checked by default because two WCCP services are not required). The automatically assigned second service ID number is shown in the **Service ID2** field.
d) From the **Redirect Method** drop-down list, choose the WCCP L2 or WCCP GRE redirect method. For details on the redirect method, see Configuring or Viewing the WCCP Settings on ANCs in the chapter "Configuring Traffic Interception." This item appears only if you are defining a custom cluster.
e) (Optional) If you do not want to use the default gateway defined on the device, uncheck the **Use Default Gateway as WCCP Router** check box. Enter the address of one or more WCCP routers, separated by commas, in the **WCCP Routers** field.
f) Click **Advanced WCCP Settings** to configure additional settings, as needed. For more information on these fields, see Configuring or Viewing the WCCP Settings on ANCs in the chapter "Configuring Traffic Interception." This item appears only if you are defining a custom cluster.

Step 13 Click **Next**. If you are configuring multiple ANCs, a similar window is shown for each ANC.

Step 14 Configure the interception and cluster interface settings for each device. The **Cluster Interface** wizard only appears if you are defining a custom cluster, with one window for each device in the cluster:

a) Configure individual interception interfaces, port channels, standby interfaces, and bridge interfaces (for inline only), as needed, on the device by using the graphical interface wizard. If you are configuring an inline ANC, you must define a bridge interface with two physical or port-channel interfaces (or one of each) for interception. For more information, see Configuring Interfaces with the Graphical Interface Wizard, on page 90.

b) From the **Cluster Interface** drop-down list, choose the interface to be used for intracluster traffic.

Step 15 Click **Next**. If you are configuring multiple devices, a similar screen is shown for each device.

Step 16 Click **Finish** to save the cluster configuration.

By default, the **Cluster Interface** wizard assigns all the WNs to a default WNG named WNG-Default. You can create additional WNGs, as described in Adding a New WAAS Node to the Cluster. You can reassign WNs to different WNGs, as described in Configuring WAAS Node Settings

Note After you create an AppNav Cluster, it is shown in the **Manage AppNav Clusters** list. For more information, see Monitoring an AppNav Cluster.

Creating a New AppNav-XE Cluster with the AppNav Cluster Wizard

This section contains the following topics:

Creating an AppNav-XE Cluster with the AppNav Cluster Wizard

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters > All AppNav Clusters**.

The **Manage AppNav Clusters** window appears.

Step 2 Click the **AppNav Cluster Wizard** icon in the taskbar of the **Manage AppNav Clusters** pane.

The **Cluster Wizard** window appears.

Step 3 From the **AppNav platform** drop-down list, choose one of the following AppNav-XE platforms to use for your deployment. All ANCs must use the same platform type with identical memory configurations.

- **ASR 1000 Series**: AppNav-XE on the Cisco ASR 1000 Series Aggregation Services Router
- **CSR 1000V Series**: AppNav-XE on the Cisco Cloud Services Router 1000V Series
- **ISR 4451X**: AppNav-XE on the Cisco 4451-X Integrated Services Router

Step 4 Click **Next**.

Step 5 Define the cluster settings by entering the following information:

- In the **Cluster Name** field, enter a name for the cluster. Use only letters, numbers, hyphen, and underscore. A maximum of 32 characters, beginning with a letter, can be entered.
- (Optional) In the **Description** field, enter a description of the cluster. Use only letters and numbers. A maximum of 200 characters can be entered.
- From the **WAAS Cluster ID** drop-down list, choose a cluster ID that is unique for this cluster in your Cisco WAAS network. Only unused cluster IDs are shown.

Click **Next**.

Step 6 Choose the ANC and WN devices that you want to be part of the cluster:

a) Choose up to four AppNav-XE devices of the same platform type in the AppNav Controller device list by clicking the check box next to the device names. You can use the filter settings in the taskbar to filter the device list.

b) Choose up to 64 WNs in the **WAAS Nodes** device list by clicking the check box next to the device names. You can use the filter settings in the taskbar to filter the device list.

If there are devices that are ineligible to join the cluster, click **Show Ineligible Devices** to see them and the reasons why they are ineligible. You can use the filter settings to filter the list.

Step 7 Click **Next**.

Step 8 Choose the VRF instances to associate with the service context by checking the box next to each VRT instance that you want to use. If you choose the VRF default, you cannot choose other VRFs. If you choose multiple they must not have overlapping source IP addresses. Only VRFs that are available on all the ANCs are listed in the top table. Ineligible VRFs are listed in the lower table.

Step 9 Click **Next**.

Step 10 Configure the interception and cluster interface settings for each ANC device in the cluster:

a) Choose the WAN interfaces on which traffic interception is to be enabled. Interfaces must already be configured on the AppNav-XE devices and only those on which service insertion can be enabled are listed.

b) Choose the local interface to be used for intra-cluster traffic.

Step 11 Click **Next**. If you are configuring multiple ANCs, a similar screen is shown for each device.

Step 12 Configure the cluster interface settings for each WN device in the cluster. The Cluster Interface wizard appears, with one screen for each WN in the cluster:

a) Configure individual interfaces, as needed, on the device by using the graphical interface wizard. For more information, see Configuring Interfaces with the Graphical Interface Wizard, on page 90.

b) From the **Cluster Interface** drop-down list, choose the interface to be used for intra-cluster traffic.

Step 13 Click **Next**. If you are configuring multiple WNs, a similar screen is shown for each device.

Step 14 To save the cluster configuration, click **Finish**.

What to do next

By default, the wizard assigns all the WNs to a default WNG named WNG-Default. You can create additional WNGs, as described in Adding a New WAAS Node to the Cluster, on page 119. You can reassign WNs to different WNGs, as described in Configuring WAAS Node Settings, on page 114.

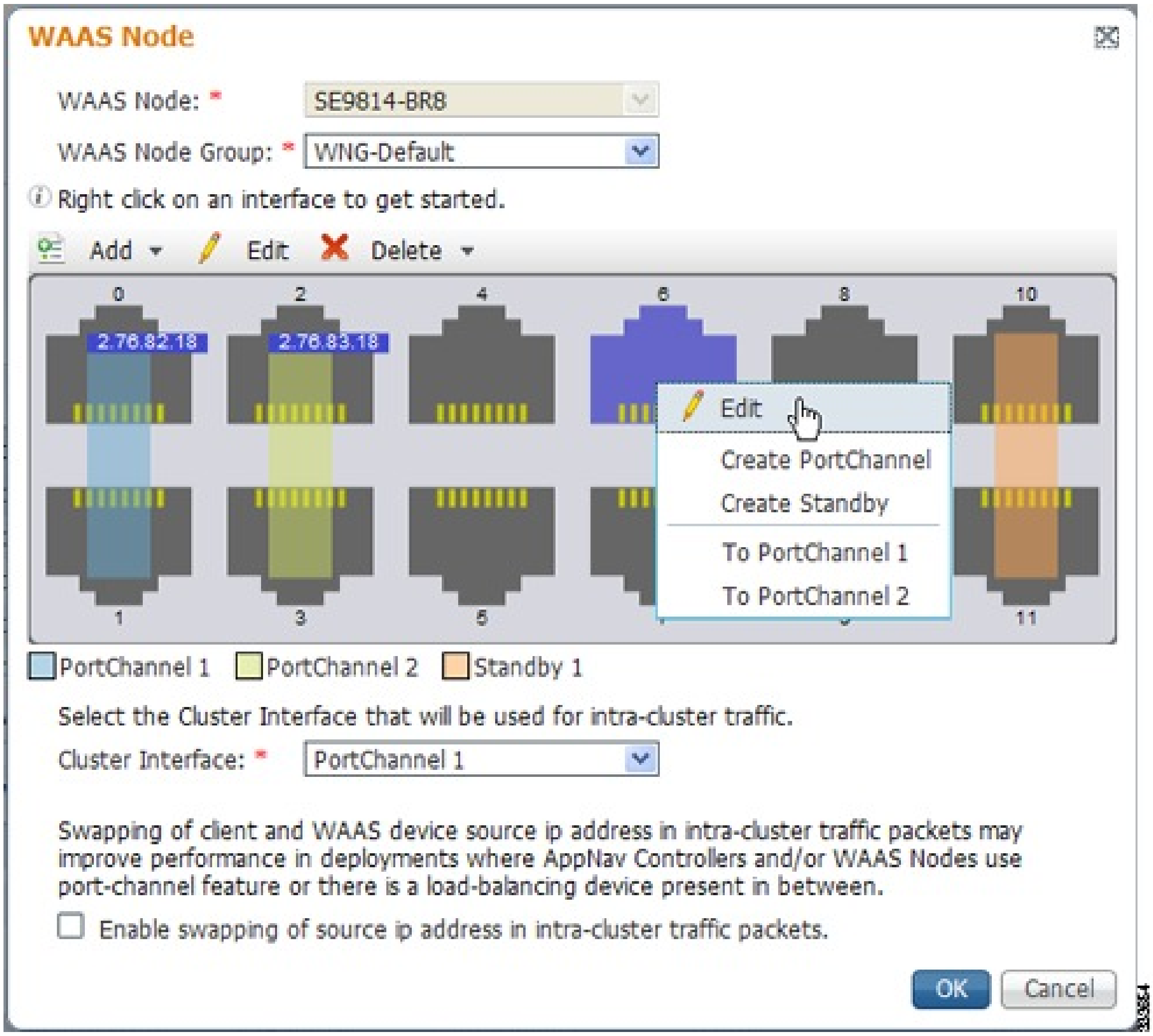
To begin traffic optimization with AppNav-XE, enable WAAS service insertion on the AppNav-XE device interfaces on which you chose to intercept traffic. For more information, see Enabling WAAS Service Insertion on AppNav-XE Device Interfaces in the chapter "Configuring Network Settings."

After you create an AppNav Cluster, it is displayed in the **Manage AppNav Clusters** list. For more information, see Monitoring an AppNav Cluster, on page 121.

Configuring Interfaces with the Graphical Interface Wizard

You can easily configure interfaces on the AppNav Controller Interface Modules that are installed in devices that are a part of an AppNav Cluster by using the Graphical Interface Wizard. Additionally, you can configure WN interfaces.

Figure 12: Graphical Interface Wizard



WAAS Node

WAAS Node: * SE9814-BR8

WAAS Node Group: * WNG-Default

Right click on an interface to get started.

□ PortChannel 1 □ PortChannel 2 □ Standby 1

Select the Cluster Interface that will be used for intra-cluster traffic.

Cluster Interface: * PortChannel 1

Swapping of client and WAAS device source ip address in intra-cluster traffic packets may improve performance in deployments where AppNav Controllers and/or WAAS Nodes use port-channel feature or there is a load-balancing device present in between.

□ Enable swapping of source ip address in intra-cluster traffic packets.

Note The Graphical Interface Wizard is not used to configure interfaces on AppNav-XE ANCs.

The Graphical Interface Wizard appears when you are editing the settings for a WN or ANC in the AppNav Cluster context.

Note The top two fields, **WAAS Node** and **WAAS Node Group**, do not appear when configuring ANC interfaces.

In the **Graphical Interface** view, hover your mouse over a physical or logical interface to see its identifier, for example, GigabitEthernet 1/0. Port channels, bridge groups, and standby groups are indicated by colored blocks or dotted outlines. The IP address of each configured physical or logical interface is shown with a small blue highlight. The legend below the table indicates port channel, bridge group, and standby interfaces.

Right-click an interface to choose, from the following options (available actions are dependent on the device and cluster type):

- **Edit**: Displays a pane where you can edit the interface description, IP address, netmask, and shutdown status.
- **Create PortChannel**: Creates a new port channel with this interface. This choice displays a pane where you can configure the port channel number, description, IP address, netmask, and shutdown status.
- **Create Bridge**: To create a new bridge group with this interface. This choice displays a pane where you can configure the bridge group number and description and enable link state propagation. This choice appears only when configuring a device for inline interception. A bridge interface consists of two physical or port-channel interfaces (or one of each).
- **Create Standby**: Creates a new standby group with this interface. This choice displays a pane where you can configure the standby group number, description, IP address, netmask, and shutdown status.
- **To PortChannel** *n*: Adds this interface to an existing port channel, where *n* is the port channel number.
- **To Standby** *n*: Adds this interface to an existing standby group, where *n* is the standby group number.
- **To Bridge** *n*: Adds this interface to an existing bridge group, where *n* is the bridge group number.
- For standby interfaces (right-click within the standby interface group indicator):
    - **Edit**: Edits the standby group settings, such as the description, IP address, netmask, primary interface, and shutdown status.
    - **Delete Standby** *n*: Deletes the standby group.
- For port channel interfaces (right-click within the port channel indicator):
    - **Edit**: To edit the port channel settings such as the port channel number, description, IP address, netmask, and shutdown status.
    - **Remove from Standby** *n*: To remove the port channel from standby group *n*.
    - **Delete PortChannel** *n*: To delete the port channel.
- For bridge group interfaces (right-click within the bridge group indicator):
    - **Edit**: Edits the bridge group settings, such as the bridge group number, description, and link state propagation status.
    - **Delete Bridge** *n*: Deletes the standby group.

To select an interface:

- **Individual interface**: Click-and-selection is indicated by a blue color.
- **Standby group**: Click the colored or dotted line indicator (the selection is indicated by a thick dotted blue outline around all the interfaces in the standby group).

- **Port channel or bridge group**: Click the colored indicator (the selection is indicated by a thick dotted blue outline around all the interfaces in the port channel or bridge group).

You can also perform actions by selecting an interface and clicking the following taskbar icons:

- Add (choices differ depending on the selected entity):
    - **Create PortChannel**: Creates a new port channel with this interface.
    - **Create Bridge**: Creates a new bridge group with this interface.
    - **Create Standby**: Creates a new standby group with this interface.
    - **To PortChannel** *n*: Adds this interface to an existing port channel, where *n* is the port channel number.
    - **To Standby** *n*: Adds this interface to an existing port channel, where *n* is the port channel number.
- **Edit**: Edits the selected interface.
- **Delete** (choices differ depending on the selected entity):
    - **Remove from Standby** *n*: Removes the port channel from standby group *n* .
    - **Delete PortChannel** *n*: Deletes the port channel.
    - **Delete Standby** *n*: Deletes the standby group.
    - **Delete Bridge** *n*: Deletes the bridge group.

From the **Cluster Interface** drop-down list, select the interface to be used for intra-cluster traffic, between the ANCs and WNs.

To enable swapping of client and Cisco WAAS device source IP address fields in intra-cluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box. Consider enabling this option if you are using a port channel for the cluster interface, or there is a load-balancing device between the ANC and WN. This option can improve load balancing of traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.) This option is not available for AppNav-XE clusters.

Note If you are using WCCP, the WCCP control messages must pass through the ANC interface that receives intercepted traffic from the routers. If WCCP control messages are routed to the ANC management interface, the cluster does not operate.

Configuring AppNav Policies

This section contains the following topics:

Configuring Class Maps

This section contains the following topics:

Configuring a Class Map for a Cisco WAAS Appliance AppNav Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Configure** > **AppNav Cluster** > **AppNav Class-Map**.

The **AppNav Class-Maps** window appears, listing the existing class maps.

From this window, you can perform the following tasks:

- To filter the class map list as needed, from the **Show** drop-down list, use **Quick Filter** or **Show All Class Maps**.
- To edit a class map, select it and then click the **Edit** Taskbar icon.
- To delete one or more class maps, select them and then click the **Delete** Taskbar icon.
- To add a new class map, use the following steps.

Step 3 Click the **Add Class-Map** Taskbar icon.

Step 4 In the **Name** field, enter a name for the class map. The **Name** can contain a maximum of 40 alphanumeric characters and an underscore.

Step 5 (Optional) In the **Description** field, enter a description for the class map. The Description can contain a maximum of 200 alphanumeric characters, underscore, and a space.

Step 6 From the **Type** drop-down list, choose the class map type:

- **Application**: Matches traffic for a particular application based on source or destination IP addresses or ports, or all of them, or the Microsoft RPC application identifier (for applications that use dynamic port allocation). If you choose this option, continue to Step 7.
- **Site**: Matches traffic from particular WAAS peer devices, for site affinity. If you choose this option, continue to Step 8.
- **Custom**: Mixes application and site affinity. Matches traffic for a particular application from one specific peer WAAS device. If you choose this option, continue to Step 9.
- **Any TCP**: Matches any TCP traffic as a catch-all classifier. If you choose this type, there are no other fields to set.

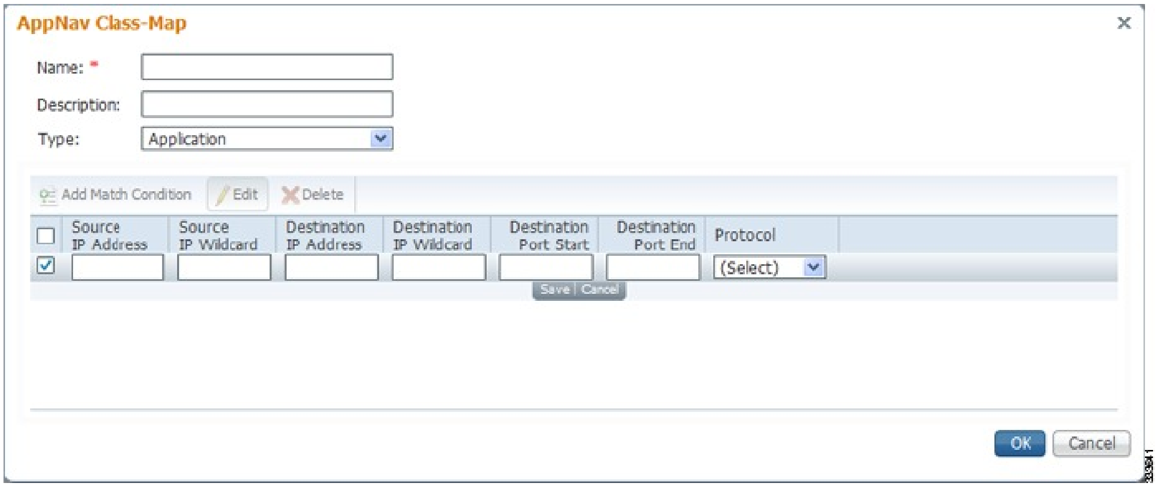
Step 7 To finish and return to the class maps list, click **OK**.

The match conditions shown in the lower part of the pane change depending on the class map type.

Step 8 (Optional) For an **Application** class map type, enter one or more match conditions. You can perform the following tasks in this pane:

- To edit a match condition, select it and then click the **Edit** Taskbar icon.
- To delete one or more match conditions, select them and then click the **Delete** Taskbar icon.
- To add a new match condition, use the following steps to enter information in the **AppNav Class-Map** dialog box, shown in the following figure.

Figure 13: AppNav Class Map Dialog Box



a) Click the **Add Match Condition** Taskbar icon.

b) To create a condition for a specific type of traffic, enter values in one or more fields. For example, to match all the traffic going to ports 5405 to 5407, in the **Destination Port Start** field enter **5405**, and in the **Destination Port End** field, enter **5407**. To specify a range of IP addresses using a wildcard subnet mask in dotted decimal notation, for example, 0.0.0.255 for /24, use the **IP address wildcard fields**.

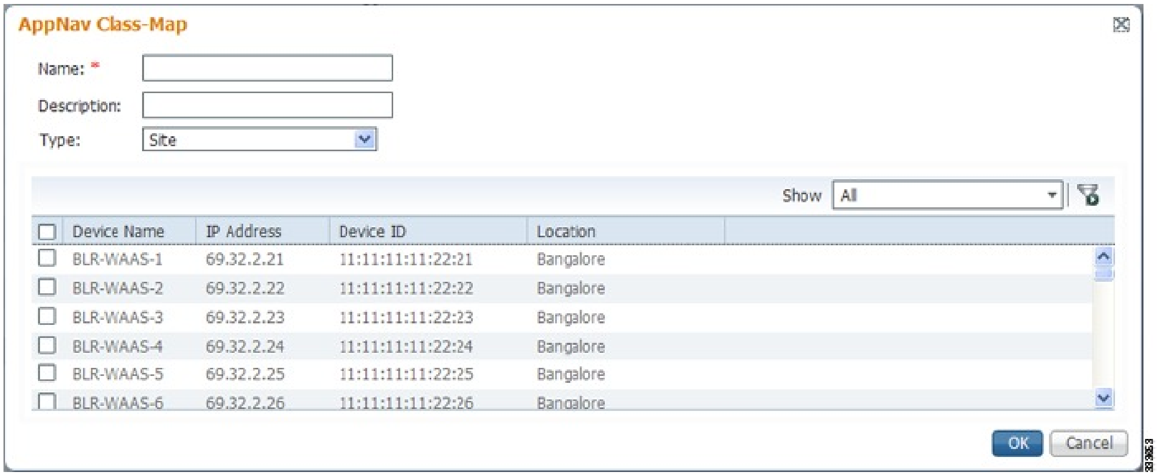
c) To match Microsoft RPC traffic that uses dynamic port allocation: From the **Protocol** drop-down list, choose the **RPC application identifier**. For example, to match Microsoft Exchange Server traffic that uses the MAPI protocol, choose **mapi**.

d) To save the match condition, click **Save**.

e) Add additional match conditions, as needed. To save the class map and return to the class maps list, click **OK**. If any of the conditions is matched, the class is considered matched.

Step 9 (Optional) For a **Site** class map type, select one or more peer devices. To create the class map, use the following steps to enter information in the **AppNav Class-Map** dialog box, shown in the following figure.

Figure 14: AppNav Class Map Dialog Box with Add Match Condition List



□	Device Name	IP Address	Device ID	Location
□	BLR-WAAS-1	69.32.2.21	11:11:11:11:22:21	Bangalore
□	BLR-WAAS-2	69.32.2.22	11:11:11:11:22:22	Bangalore
□	BLR-WAAS-3	69.32.2.23	11:11:11:11:22:23	Bangalore
□	BLR-WAAS-4	69.32.2.24	11:11:11:11:22:24	Bangalore
□	BLR-WAAS-5	69.32.2.25	11:11:11:11:22:25	Bangalore
□	BLR-WAAS-6	69.32.2.26	11:11:11:11:22:26	Bangalore

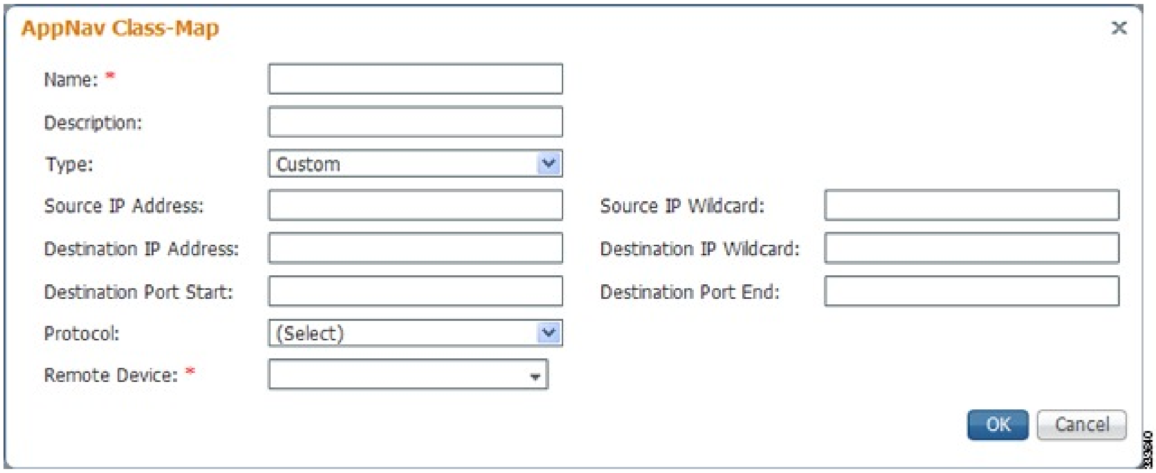
a) From the **Show** drop-down list, filter the device list as required, using: **Quick Filter**, **Show All Devices**, or **Show All Assigned Devices**.

b) Check the box next to each device you want to match traffic from. Check the box next to the column title to select all the devices and uncheck it to deselect all the devices. If any of the selected devices is matched, the class is considered matched.

c) To save the class map and return to the class maps list, click **OK**.

Step 10 (Optional) For a **Custom** class map type, enter a match condition based on IP address/port or Microsoft RPC application ID, and choose a WAAS peer device. All the specified matching criteria must be met for the class to be considered matched. To create the class map, use the following steps to enter information in the **AppNav Class-Map** dialog box, shown in the following figure.

Figure 15: AppNav Class Map with Match Conditions



AppNav Class-Map

Name: *

Description:

Type: Custom

Source IP Address:

Source IP Wildcard:

Destination IP Address:

Destination IP Wildcard:

Destination Port Start:

Destination Port End:

Protocol: (Select)

Remote Device: *

a) Enter values in one or more **IP Address** fields or **Port** fields, or both, to create a condition for a specific type of traffic. For example, to match all traffic going to ports 5405 to 5407, in the **Destination Port Start** field enter **5405**, and in the **Destination Port End** field enter **5407**. To specify a range of IP addresses using a wildcard subnet mask in dotted decimal notation, for example, 0.0.0.255 for /24, use the **IP address wildcard fields**.

Note We strongly recommend that you use the Cisco WAAS Central Manager GUI to centrally configure class maps for your Cisco WAAS devices. However, there is one exception to this recommendation. Use the Cisco WAAS CLI to create an AppNav class map with a type of **Application** or **Custom**, and whose source or destination address has one of the following: an IP address ending in **0.0.0** or a non-Class A IP address ending in **0.0**.

b) (Optional) To match Microsoft RPC traffic that uses dynamic port allocation, from the **Protocol** drop-down list, choose the **RPC application identifier**. For example, to match Microsoft Exchange Server traffic that uses the MAPI protocol, choose **mapi**.

c) From the **Remote Device** drop-down list, choose a WAAS peer device.

d) To save the class map and return to the **Class Maps Configuration** window, click **OK**.

Configuring a Class Map for an AppNav-XE Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Configure** > **AppNav Cluster** > **AppNav Class-Map**.

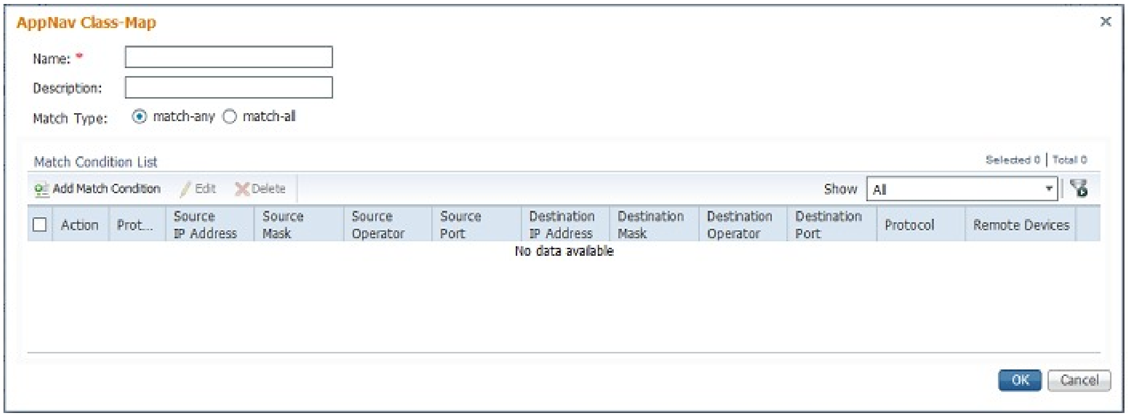
The **AppNav Class-Maps** window appears, listing the existing class maps.

From this window, you can perform the following tasks:

- From the **Show** drop-down list, choose a filter setting to filter the class map list as needed. You can use **Quick Filter** or **Show All Class Maps**.
- Edit a class map by selecting it and clicking the **Edit** taskbar icon.
- Delete one or more class maps by selecting them and clicking the **Delete** taskbar icon.
- Add a new class map as described in the steps that follow.

Step 3 Click the **Add Class-Map** taskbar icon.

Figure 16: AppNav Class Map with Match Condition List



AppNav Class-Map

Name: *

Description:

Match Type: ● match-any ○ match-all

Match Condition List

Selected 0 | Total 0

Show: All

□	Action	Prot...	Source IP Address	Source Mask	Source Operator	Source Port	Destination IP Address	Destination Mask	Destination Operator	Destination Port	Protocol	Remote Devices

No data available

Step 4 In the **Name** field, enter a name for the class map. A maximum of 221 characters, excluding space or question mark (**?**), can be entered.

Step 5 (Optional) In the **Description** field, enter a description for the class map. A maximum of 200 characters, excluding a question mark (**?**), can be entered.

Step 6 From the **Match Type** radio buttons, choose **match-any** or **match-all**. Match-any means that if any one of the match conditions is matched, the class is considered matched. Match-all means that all the match conditions must be matched for the class to be matched.

Step 7 Click the **Add Match Condition** taskbar icon.

The **Match Condition** pane appears.

Step 8 From the **Match Condition** drop-down list, choose the type of match condition you want to create:

- **Source/Destination IP**: Matches traffic for a particular application based on an access list of source and/or destination IP addresses and/or ports. Continue with Step 9 .
- **Protocol**: Matches traffic for a particular Microsoft RPC application identifier (for applications that use dynamic port allocation). Continue with Step 10 .
- **Peer**: Matches traffic from particular WAAS peer devices, for site affinity. Continue with Step 11.
- **NBAR Protocol**: Matches traffic based on application id using the lowest NBAR version protocol pack library that has an evolved application recognition capability. Continue with Step 12.

The match conditions shown in the lower part of the pane change depending on the condition type.

Supported Application Accelerators	Application Accelerators Not Supported
SSL/SSLv2 Dual Sided	ICA
HTTP and AKC Dual Sided	MAPI
SMB	Single Sided App-ID Traffic with SSLv2/AKC

- **Nested Class Maps**: Matches traffic from WAAS devices based on multiple traffic classes. Continue with Step 13.

Consider the following guidelines:

- If the AppNav cluster runs with more than one router, all the routers software version needs to be greater than or equal to 16.10 for NBAR Protocol or Nested Class Map configuration from the Cisco WAAS Central Manager.
- The lowest NBAR protocol version is taken from among all AppNav-XE routers (running software version 16.10 and later) that are registered with the Cisco WAAS Central Manager.

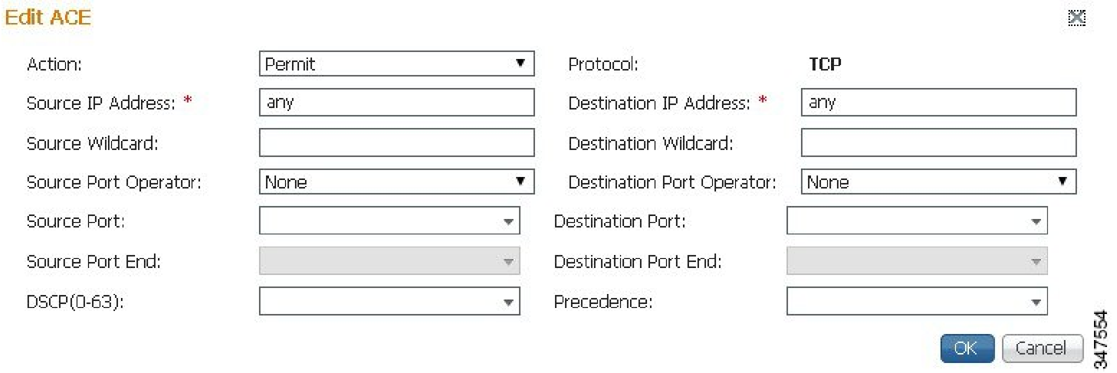
The match conditions shown in the lower part of the pane change depending on the condition type.

Step 9 (Optional) For a Source/Destination IP match condition type, enter one or more access control entries (ACEs). You can perform the following tasks in this pane:

- Edit an ACE by selecting it and clicking the **Edit** taskbar icon.
- Delete one or more ACEs by selecting them and clicking the **Delete** taskbar icon.
- Move one or more selected ACEs to a new position by clicking the **Move To** taskbar icon. After moving the ACEs, click **Save Moved Rows** to save the change.
- Move one or more selected ACEs up or down one position by clicking the **Up** or **Down Arrow** taskbar icons, and then click **Save Moved Rows** to save the change.
- Save the ACEs that you have moved with the Move To or Up and Down Arrow functions by clicking the **Save Moved Rows** taskbar icon.
- Insert a new ACE before the selected row by clicking the **Insert** taskbar icon. The workflow for inserting is the same as for adding (described in the following steps).
- Add a new ACE, as described in the steps that follow.

a) Click the **Add ACE** taskbar icon.

Figure 17: Edit ACE Pane



Edit ACE

Action:	Permit	Protocol:	TCP
Source IP Address: *	any	Destination IP Address: *	any
Source Wildcard:		Destination Wildcard:	
Source Port Operator:	None	Destination Port Operator:	None
Source Port:		Destination Port:	
Source Port End:		Destination Port End:	
DSCP(0-63):		Precedence:	

b) From the **Action** drop-down list, choose **Permit** or **Deny**, to determine whether this ACE permits or denies matched traffic.

c) Enter values in one or more fields to create an ACE for a specific type of traffic. Enter any in the IP address fields to specify any IP address.

d) Use the IP address wildcard fields to specify a range of IP addresses using a wildcard subnet mask in dotted decimal notation, for example, 0.0.0.255 for /24.

e) Use the **Source/Destination Port Operator** drop-down lists to choose an operator and behavior for the port fields:

- **None**: Port field is not used.
- **eq**: Match requires traffic port to be equal to the **Port** field.
- **gt**: Match requires traffic port to be greater than the **Port** field.
- **lt**: Match requires traffic port to be less than the **Port** field.
- **neq**: Match requires traffic port to be not equal to the **Port** field.
- **Range**: Match requires traffic port to be within the range of ports from the **Start Port** field through the **Port End** field.

In the port fields, you can choose the port from a drop-down list or enter a numeric value.

f) Set the differentiated services code point (DSCP) value. Alternatively, select a Precedence value from the **Precedence** drop-down list to set the priority.

The DSCP value must be between 0 and 63. Additionally, DSCP names are also allowed.

g) Click **OK** to save the ACE.

h) Add additional ACEs. Click **OK** to save the match condition and return to the Match Conditions list.

Step 10 (Optional) For a **Protocol** match condition type, follow these steps:

a) From the **Select Protocol** drop-down list, choose the Microsoft RPC application identifier that identifies the traffic you want to match. For example, to match Microsoft Exchange Server traffic that uses the MAPI protocol, choose **mapi**.

b) Click **OK** to save the match condition and return to the match conditions list.

Step 11 (Optional) For a **Peer** match condition type, select one or more peer devices. Follow these steps to create the match condition:

a) From the **Show** drop-down list, choose a filter to filter the device list as needed. You can use **Quick Filter**, **Show All Devices**, or **Show All Assigned Devices**.
b) Check the check box next to each device you want to match traffic from. You can check the check box next to the column title to select all the devices and uncheck it to deselect all devices.
c) Click **OK** to save the match condition and return to the match conditions list.

Step 12 (Optional) For a NBAR Protocol match condition type, follow these steps:

a) From the **NBAR Protocol Type** drop-down list, choose **Protocol**.

- Select the NBAR Protocol from the drop-down list to match traffic based on the protocol. Note that when you use the Cisco WAAS Central Manager to create a class map and match condition with the NBAR protocol, you can match condition to the protocol on the router running only the lowest NBAR version protocol pack.

- After you create a class map from the Cisco WAAS Central Manager, if you use the Cisco WAAS CLI to create a class map and match condition with the router that has the greater NBAR protocols, the Cisco WAAS Central Manager page detects a configuration conflict and the device goes into the Force Device Settings (FDG) mode.

- When the router version is upgraded or downgraded from the Cisco WAAS CLI, and if the router does not support the NBAR Protocol, the devices configured with the class map to use the NBAR match condition protocol go into the FDG mode as there is a configuration conflict.

- When the Cisco WAAS Central Manager is downgraded to a version that does not support NBAR Protocol or nested class maps, an error message guides you to remove the App ID configuration before downgrading the Cisco WAAS Central Manager.

- Select the **NBAR Attribute** and the **NBAR Sub-Attribute** from the respective drop-down to set the traffic to match the **Attribute**. The **Attributes** feature provides the mechanism to match applications based on certain attributes. This helps with performing group actions on them. Attributes are statically assigned to each protocol or application, and they are not dependent on the traffic.

  The data is visible in the **Match Condition List** table.

b) Click **OK** to save the class map and return to the **Class Maps Configuration** window.

Step 13 (Optional) For a **Nested Class Map** match condition type, follow these steps:

a) Select the **Nested Class Maps** drop-down list and click **OK**.

   All the existing class maps from the Cisco WAAS Central Manager database are listed in the **AppNav Class-Map** drop down list.

b) Select the class map and click **OK**.

   An entry is created in the first dialog box, i.e, the **AppNav Class Map** dialog box. Consider the following guidelines for nested class maps:

- You can nest up to two levels from the Cisco WAAS Central Manager. Any further configuration from the Cisco WAAS Central Manager shows a warning.

- Although you can use the Cisco WAAS CLI for this configuration, we recommend that you do not configure more than two layers from the Cisco WAAS CLI, because the configurations are incorrect.

Step 14 Click **OK** to save the class map and return to the **Class Maps Configuration** window.

Configuring AppNav Policy Rules

This section contains the following topics:

Note Even though a new WNG or SNG can become operational without having an AppNav policy attached, in order to have your Cisco WAAS system work successfully, configure and attach an AppNav policy to each new WNG or SNG.

Configuring AppNav Policy Rules for a WAAS Appliance AppNav Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Configure** > **AppNav** > **AppNav Policies**.

The **AppNav Policy** window appears.

Step 3 From the **AppNav Policy** drop-down list at the top, choose the policy to configure.

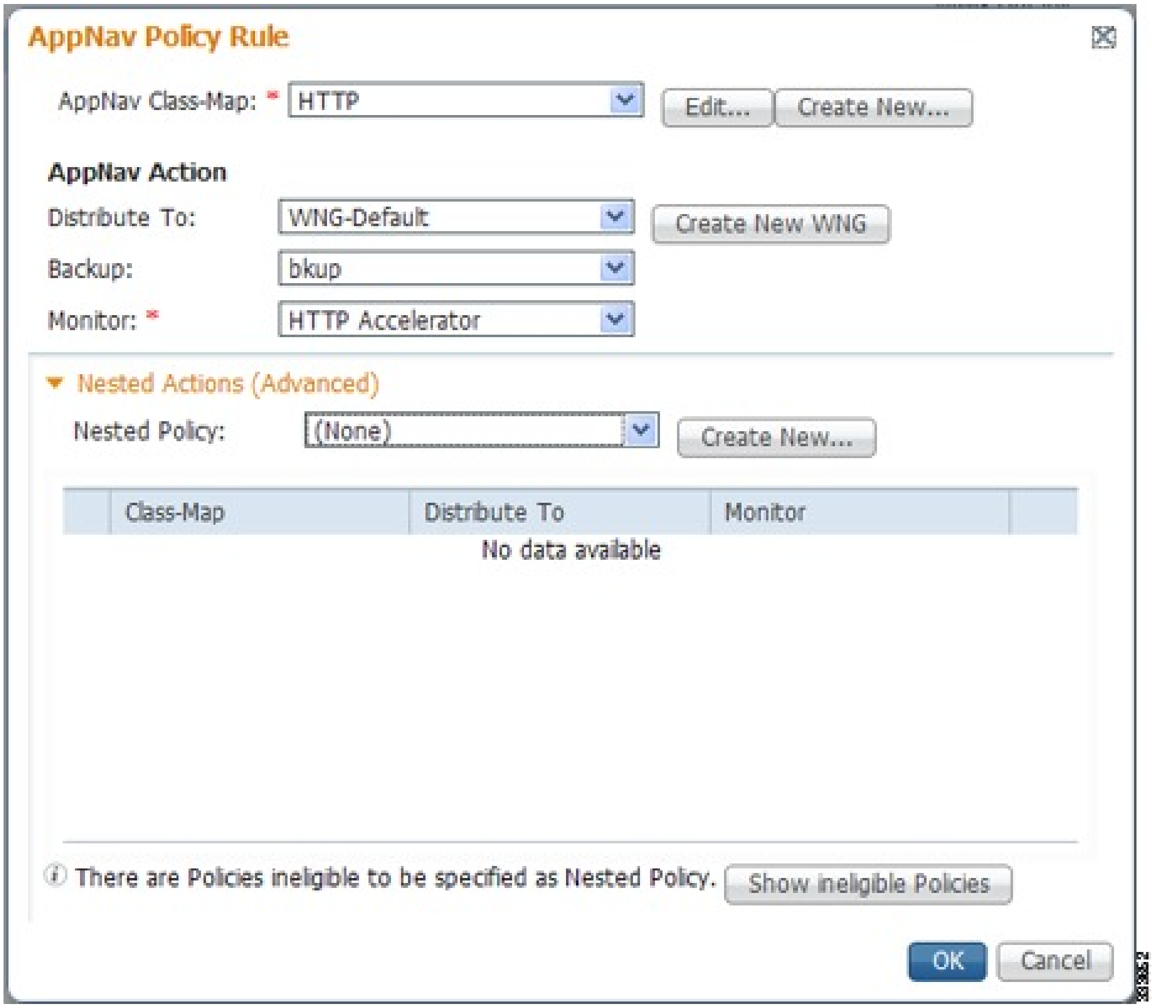
To create or delete a policy or configure the ANCs to which a policy is applied, click **Manage**. For more information, see Managing AppNav Policies and ANCs for a WAAS Appliance AppNav Cluster, on page 104.

From the **AppNav Policy Rules** pane, you can perform the following tasks:

- From the **Show** drop-down list, choose the filter to filter the rule list as needed. You can use a **Quick Filter** or **Show All Rules**.
- Edit a rule by selecting it and clicking the **Edit** taskbar icon.
- Delete one or more rules by selecting them and clicking the **Delete** taskbar icon.
- Move one or more selected rules to a new position by clicking the **Move To** taskbar icon. After moving the rows, click **Save Moved Rows** to save the change.
- Move one or more selected rules up or down one position by clicking the **Up Arrow** or **Down Arrow** taskbar icons, and then click **Save Moved Rows** to save the change.
- Insert a new rule before the selected row by clicking the **Insert** Taskbar icon. The workflow for inserting is the same as for adding (described in the following steps).
- Add a new rule at the end of the list, as described in the steps that follow. (The class-default rule is always pushed to the last position.)

Step 4 Click the **Add Police Rule** Taskbar icon.

Figure 18: AppNav Policy Rule Pane



AppNav Policy Rule

AppNav Class-Map: * HTTP

AppNav Action

Distribute To: WNG-Default

Backup: bkup

Monitor: * HTTP Accelerator

Nested Actions (Advanced)

Nested Policy: (None)

Class-Map	Distribute To	Monitor

No data available

There are Policies ineligible to be specified as Nested Policy.

Step 5 From the **AppNav Class-Map** drop-down list, choose the class map to which this policy rule applies.

To edit the class map, click **Edit**. To create a new class map, click **Create New**. The workflow is the same, as described in Configuring a Class Map for a Cisco WAAS Appliance AppNav Cluster, on page 93.

Step 6 From the **Distribute To** drop-down list, choose the distribution action to apply to the class map. The list includes all the defined WNGs and the various options: **None**, for no action, and **Passthrough**, to pass through this type of traffic. The meaning of None is context dependent: in a top-level policy it means pass-through, if this policy is nested, it means inherit the parent policy rule action.

a) When you choose a WNG, other settings appear.

b) To create a new WNG, click **Create New**.

The workflow is the same as that described in Adding a New WAAS Node to the Cluster.

The newly created WNG appears in both the **Distribute To** and **Backup** drop-down lists.

Step 7 (Optional) From the **Backup** drop-down list, choose the backup WNG to use for distribution if the primary WNG is unavailable.

Step 8 (Optional) From the **Monitor** drop-down list, choose the application accelerator to monitor. When you monitor an application accelerator, the ANC checks for overload on that application accelerator and does not send new flows to a WN that is overloaded. If you choose **None**, a specific application accelerator is not monitored, only the maximum connection limit of the device is monitored.

Step 9 (Optional) To apply a nested policy within this rule, click **Nested Actions (Advanced)** to expand this area.

Step 10 (Optional) From the **Nested Policy** drop-down list, choose the policy to nest, or choose **None** to select no policy. When you choose a policy, the policy rules are displayed in a table.

If there are policies that are ineligible to be specified as a nested policy, click **Show Ineligible Policies** to display them and the reasons they are ineligible. A policy is ineligible if it already has a nested policy, because only one level of nesting is allowed.

To edit the chosen policy, click **Edit**. To create a new policy for nesting, click **Create New**. The workflow for both editing and creating is the same.

a) In the **Name** field, enter the policy name.

Note This field is not editable for the **waas_app_default** policy.

b) Click the **Add Policy Rule** Taskbar icon.

A new row is added, showing fields for configuring the rule.

c) From the **Class-Map** drop-down list, choose the class map to which this rule applies.
d) From the **Distribute To** drop-down list, choose the distribution action to apply to the class map. The list includes all the defined WNGs and the choices, Inherit, to inherit this action from the parent policy, and Passthrough, to pass through this type of traffic.
e) (Optional) From the **Backup** drop-down list, choose the backup WNG to use for distribution if the primary WNG is unavailable.
f) (Optional) From the **Monitor** drop-down list, choose the application accelerator to monitor.
g) Click **OK** to save the policy rule and return to the AppNav Policy Rule pane for the primary policy rule you are creating.

Step 11 Click **OK** to create the policy rule and return to the **Policy Configuration** window.

Note If all the AppNav policies have been deleted and you add a new policy rule, the policy rule is added to a new **appnav_default** policy, which is created automatically.

Configuring AppNav Policy Rules for an AppNav-XE Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name* .

Step 2 Choose **Configure** > **AppNav Clusters** > **AppNav Policies**.

The **AppNav Policy** window appears.

Step 3 Click the radio button next to the policy you want to configure in the **AppNav Policies** table at the top of the window.

In the **AppNav Policies** table, you can perform the following tasks:

- Use the filter settings in the **Show** drop-down list to filter the rule list as needed. You can use **Quick Filter** or **Show All Rules**.
- Edit a policy by selecting it and clicking the **Edit** taskbar icon.
- Delete a policy by selecting it and clicking the **Delete** taskbar icon.
- Unassign a policy by selecting it and clicking the **Unassign Policy** taskbar icon.
- Add a policy by clicking the **Add Policy** taskbar icon.

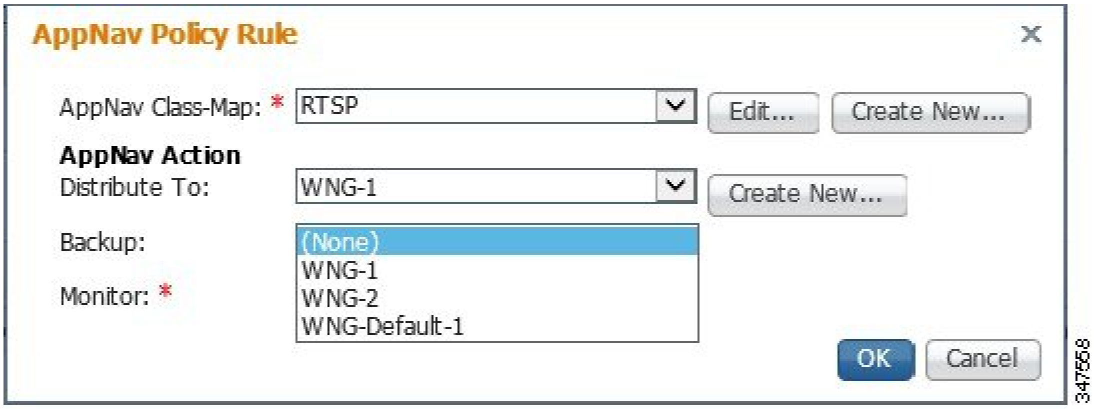
For details on these tasks see Managing AppNav Policies for an AppNav-XE Cluster, on page 107.

The **AppNav Policy Rules** table in the lower part of the window shows the selected rules in the **AppNav Policies** table. From this table, you can perform the following tasks:

- From the **Show** drop-down list, choose a filter to filter the rule list as needed. You can use **Quick Filter** or **Show All Rules**.
- Edit a rule by selecting it and clicking the **Edit** taskbar icon.
- Delete one or more rules by selecting them and clicking the **Delete** taskbar icon.
- Move one or more selected rules to a new position by clicking the **Move To** taskbar icon. After moving the rows, click **Save Moved Rows** to save the change.
- Move one or more selected rules up or down one position by clicking the **Up** or **Down Arrow** taskbar icons, and then click **Save Moved Rows** to save the change.
- Insert a new rule before the selected row by clicking the **Insert** Taskbar icon. The workflow for inserting is the same as for adding (described in the following steps).
- Add a new rule at the end of the list, as described in the steps that follow. (The class-default rule is always pushed to the last position.)

Step 4 Click the **Add Policy Rule** Taskbar icon.

Figure 19: AppNav Policy Rule Pane



AppNav Policy Rule

AppNav Class-Map: * RTSP

AppNav Action

Distribute To: WNG-1

Backup: (None)

Monitor: *

Step 5 From the **AppNav Class-Map** drop-down list, choose the class map to which this policy rule applies.

- To edit the class map, click **Edit**.
- To create a new class map, click **Create New**.

The workflow is the same as described in Configuring a Class Map for an AppNav-XE Cluster, on page 95.

Step 6 From the **Distribute To** drop-down list, choose the distribution action to apply to the class map. The list includes WNGs and the choices **None**, for no action, and Passthrough, to pass through this type of traffic. Here, the meaning of **None** is the same as **Passthrough**.

For the default policy map, the WNG list includes the default WNG and any custom WNG that is a part of the assigned context. For a custom policy map, the WNG list includes default and custom WNGs that are not already assigned to another context.

When you choose a WNG, other settings appear. To create a new WNG, click **Create New**. The workflow is the same as described in Adding a New WAAS Node Group to the Cluster, on page 120. The newly created WNG appears in the Distribute To drop-down list.

Step 7 (Optional) From the **Backup** drop-down list, choose the backup WNG to use for distribution if the primary WNG is unavailable or overloaded.

Consider the following guidelines for the backup WNG:

- The **Backup WNG** option is available only for cluster/s that have XE3.13 devices or later. It is recommended that prior to downgrading the Cisco WAAS Central Manager to a version of Cisco WAAS Version 5.2.1 or earlier, the Backup WNG must be removed from the AppNav-XE cluster and make sure the Cisco WAAS Central Manager and AppNav-XE device configurations are in sync.
- PreXE3.13 controllers cannot be added to the cluster policy that has been configured with a backup WNG. A validation message is displayed while adding preXE3.13 controller to a cluster with backup WNG policy.A cluster having pre 3.13 devices cannot be configured with backup WNG. The option for backup WNG will not be visible if the cluster has at least one pre-3.13 XE device.
- We recommend that, prior to downgrading XE to a Pre XE3.13 release, the **Backup WNG** be removed from the AppNav-XE cluster. Ensure that the Cisco WAAS Central Manager and AppNav-XE device configuration are in sync.

Step 8 (Optional) From the **Monitor** drop-down list, choose the application accelerator to monitor. When you monitor an application accelerator, the ANC checks for overload on that application accelerator and does not send new flows to a WN that is overloaded. If you choose None, a specific application accelerator is not monitored, only the maximum connection limit of the device is monitored.

Step 9 Click **OK** to create the policy rule and return to the policy configuration window.

Managing AppNav Policies

This section contains the following topics:

Managing AppNav Policies and ANCs for a WAAS Appliance AppNav Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Configure** > **AppNav Cluster** > **AppNav Policies**.

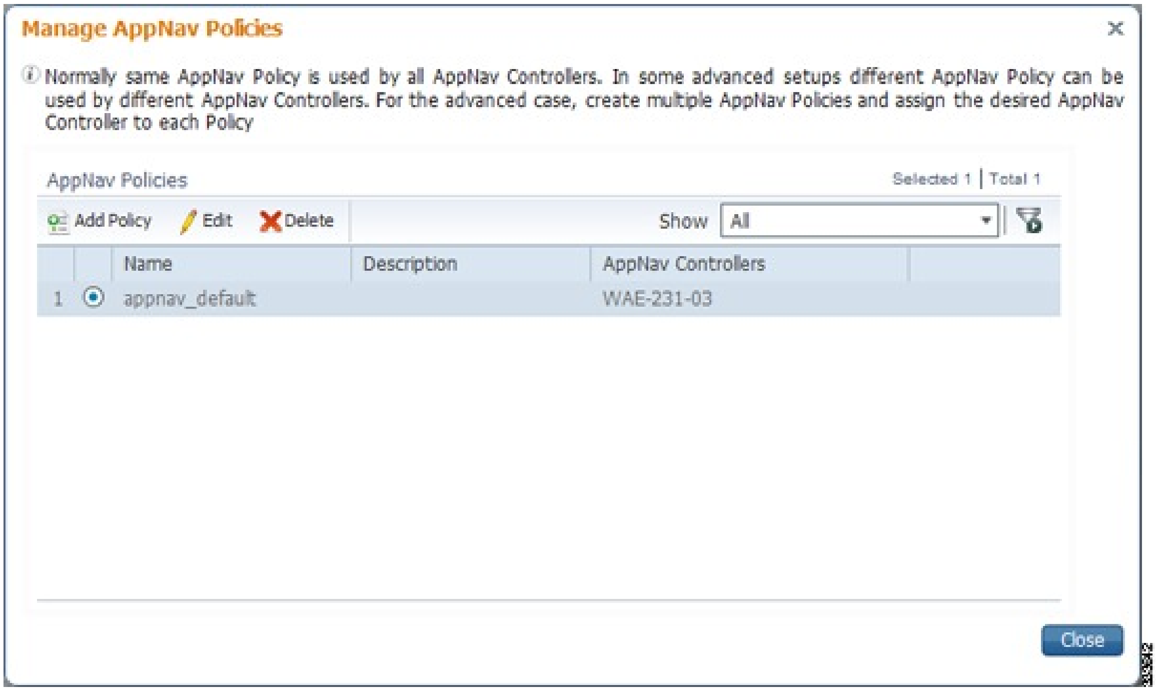
The **AppNav Policy** window appears.

Step 3 Choose the policy to view from the **AppNav Policy** drop-down list at the top.

For more information on the **AppNav Policy Rules** pane see Configuring AppNav Policy Rules for a WAAS Appliance AppNav Cluster, on page 100.

Step 4 Click **Manage**.

Figure 20: Manage AppNav Policies Pane



Manage AppNav Policies

Normally same AppNav Policy is used by all AppNav Controllers. In some advanced setups different AppNav Policy can be used by different AppNav Controllers. For the advanced case, create multiple AppNav Policies and assign the desired AppNav Controller to each Policy

AppNav Policies — Selected 1 | Total 1

Show: All

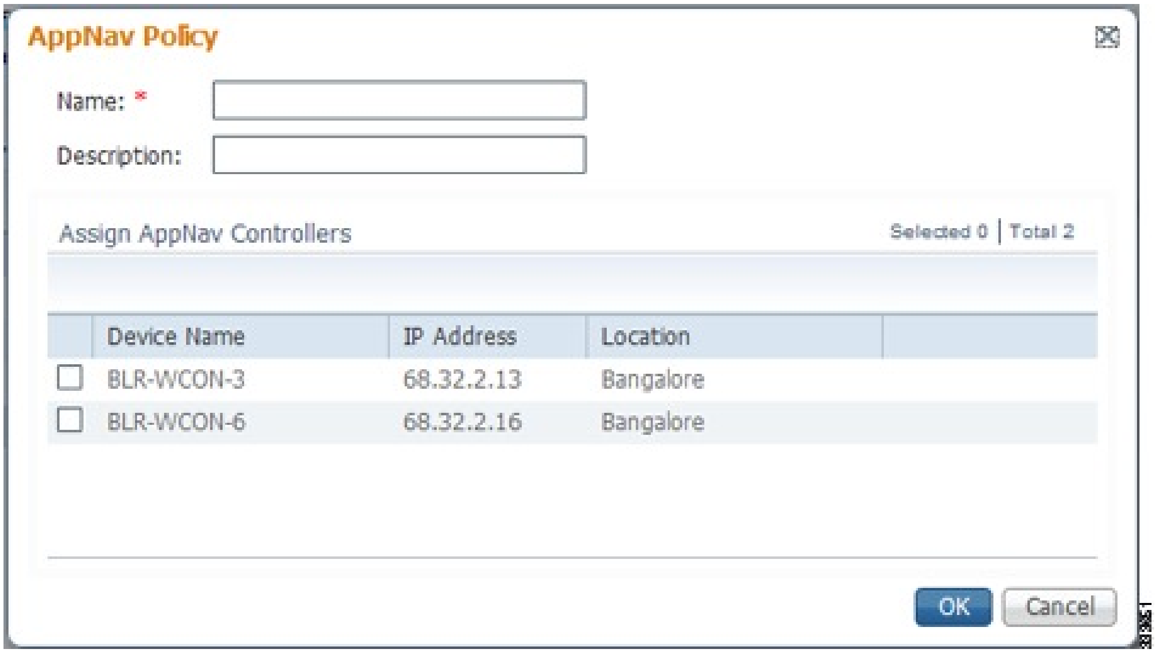
		Name	Description	AppNav Controllers
1	●	appnav_default		WAE-231-03

From the **Manage AppNav Policies** pane, you can perform the following tasks:

- From the **Show** drop-down list, choose a filter to filter the policy list as needed. You can use a **Quick Filter** or **Show All Policies**.
- Edit a policy and configure the ANCs to which it applies by selecting it and clicking the **Edit** taskbar icon.
- Delete a policy by selecting it and clicking the **Delete** taskbar icon.
- Add a new policy, as described in the following steps.

Step 5 Click the **Add Policy** taskbar icon.

Figure 21: AppNav Policy Pane



AppNav Policy

Name: *

Description:

Assign AppNav Controllers

Selected 0 | Total 2

	Device Name	IP Address	Location
□	BLR-WCON-3	68.32.2.13	Bangalore
□	BLR-WCON-6	68.32.2.16	Bangalore

Step 6 In the **Name** field, enter a name for the policy. A maximum of 40 alphanumeric characters, including an underscore, can be entered.

Step 7 (Optional) In the **Description** field, enter a description for the policy. A maximum of 200 alphanumeric characters, including underscore and space, can be entered.

Step 8 (Optional) Check the check box next to each ANC that you want to assign to this policy. To unassign any assigned devices, uncheck the check box.

Assigning a policy to an ANC makes the policy active on that ANC (only one policy can be active on an ANC) and removes the association of any previously active policy on that ANC. It is not necessary to assign a policy to an ANC if you want to create the policy as an alternative. You can assign it to ANCs later, as required.

Step 9 To save the policy and return to the **Manage AppNav Policies** pane, click **OK**.

Step 10 To return to the **Policy Configuration** window, click **Close**.

Step 11 Add policy rules to the new policy as described in Configuring AppNav Policy Rules for a WAAS Appliance AppNav Cluster, on page 100.

What to do next

To restore the default class maps and policy maps to your cluster, click the **Restore Default** taskbar icon at the top of the **AppNav Policies** window. This action removes all the existing class and policy map configurations and restores the default class and policy maps. All the WAAS nodes assigned to WNGs are moved to the default WNG, and other WNGs are removed.

Managing AppNav Policies for an AppNav-XE Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Configure** > **AppNav Clusters** > **AppNav Policies**.

The **AppNav Policy** window appears.

Step 3 Click the radio button next to the policy to modify, in the **AppNav Policies** table at the top of the window.

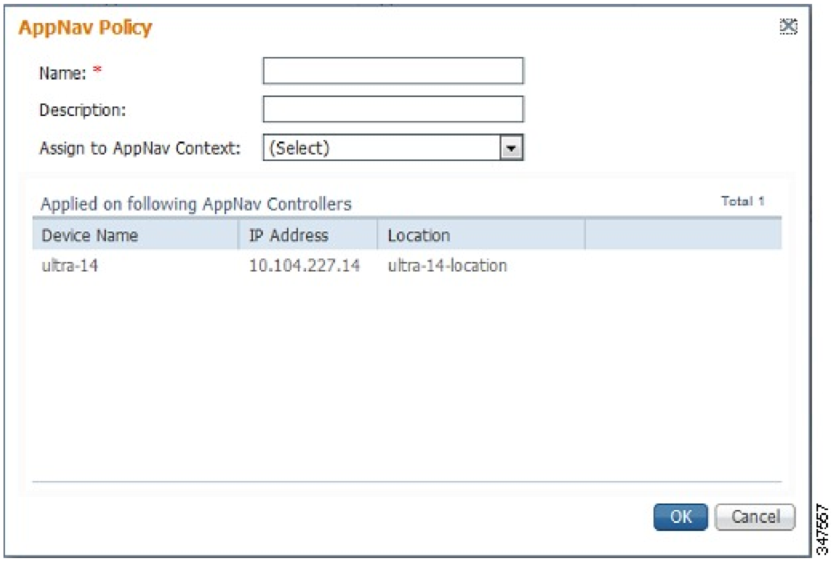
From the **AppNav** Policies table, you can perform the following tasks:

- From the **Show** drop-down list, choose a filter to the rule list as required. You can use **Quick Filter** or **Show All Rules**.
- Edit a policy by selecting it and clicking the **Edit** taskbar icon.
- Delete a policy by selecting it and clicking the **Delete** taskbar icon.
- Unassign a policy from a context by selecting it and clicking the **Unassign Policy** taskbar icon. Unassigning a policy from a context also disables the context and unassigns all the WNGs from the context. Click **OK** again to confirm that you want to proceed.
- Add a new policy, as described in the steps that follow.

For details on using the AppNav Policy Rules area, see Configuring AppNav Policy Rules for an AppNav-XE Cluster, on page 102.

Step 4 Click the **Add Policy** taskbar icon.

Figure 22: AppNav Policy Pane



AppNav Policy

Name: *

Description:

Assign to AppNav Context: (Select)

Applied on following AppNav Controllers

Total 1

Device Name	IP Address	Location
ultra-14	10.104.227.14	ultra-14-location

Step 5 In the **Name** field enter a name for the policy. A maximum of up to 227 characters, excluding a space or question mark (**?**), can be entered. Do not use a name of the format **APPNAV-*n*-PMAP**, which is used for default policy maps.

Step 6 (Optional) In the **Description** field, enter a description for the policy. A maximum of up to 200 characters, not including a question mark (**?**), can be entered.

Step 7 From the **Assign to AppNav Context** drop-down list, choose the context to which to assign the new policy.

Assigning the policy to a context makes the policy active on all the ANCs that are a part of the context. Only contexts that do not already have an assigned policy are listed.

For default policy maps, only one context is displayed, based on the context ID. For example, for APPNAV-4-PMAP, only waas/4 is displayed (in case it is not already assigned).

Step 8 Click **OK** to save the policy and return to the AppNav Policies window.

Step 9 Add policy rules to the new policy as described in Configuring AppNav Policy Rules for an AppNav-XE Cluster, on page 102.

What to do next

To restore the default class maps and policy maps to your cluster, click the **Restore Default** taskbar icon at the top of the **AppNav Policies** window. This action removes all the existing class and policy map configurations and restores the default class and policy maps. All the WAAS nodes assigned to each context are moved to their respective default WNGs and all the unassigned WNGs are removed.

Configuring WAAS Node Optimization Policy

The WAAS node optimization policy controls how traffic that is distributed to the WAAS nodes is optimized. The optimization policy is configured on the WNs and the ANCs that are also acting as optimizing nodes.

All the WNs in one WNG must have an identical optimization policy configured on them. Otherwise, optimization of flows is not predictable. The optimization policy can be different for different WNGs.

For information on how to configure the optimization policy, see the chapter "Configuring Application Acceleration."

The default optimization policy is listed in Appendix A, "Predefined Optimization Policy."

Configuring AppNav Controller ACLs

An AppNav Controller ACL controls what traffic is intercepted by a Cisco WAAS appliance ANC. You may want to configure an ANC interception ACL for each WAAS appliance ANC in an AppNav Cluster.

For information on how to configure an ANC interception ACL, see Configuring Interception Access Control Lists in the chapter "Configuring Traffic Interception."

Configuring AppNav Cluster Settings for an AppNav Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Cluster** > **All AppNav Clusters**.

The **Manage AppNav Clusters** window showing the status of each cluster appears.

From this window, you can perform the following tasks:

- Create a new AppNav Cluster. The workflow is the same as described in Creating a New AppNav-XE Cluster with the AppNav Cluster Wizard, on page 88.
- Delete an AppNav Cluster by selecting an AppNav Cluster and clicking the **Delete** icon in the taskbar of the **Manage AppNav Clusters** area.
- View an AppNav Cluster topology and edit its settings as described in the following steps.

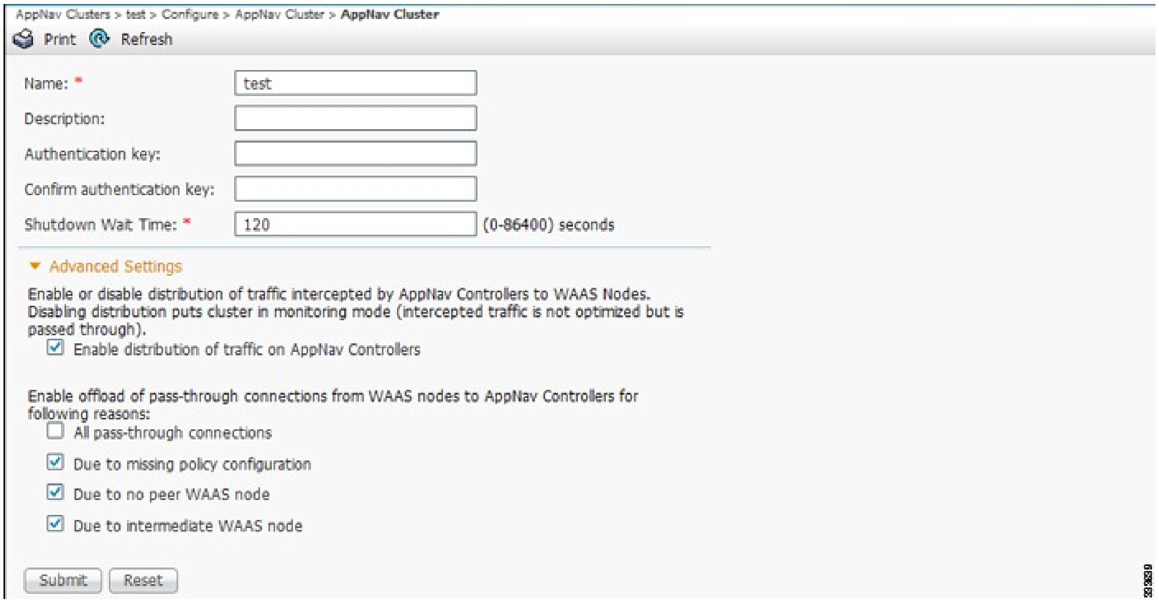
Step 2 Click the name of the cluster whose settings you want to edit.

The cluster topology diagram appears.

Step 3 Choose **Configure** > **AppNav Cluster** > **AppNav Cluster**.

The **Cluster Configuration** window appears.

Figure 23: Cluster Configuration Window



AppNav Clusters > test > Configure > AppNav Cluster > AppNav Cluster

Print Refresh

Name: * test

Description:

Authentication key:

Confirm authentication key:

Shutdown Wait Time: * 120 (0-86400) seconds

▾ Advanced Settings

Enable or disable distribution of traffic intercepted by AppNav Controllers to WAAS Nodes. Disabling distribution puts cluster in monitoring mode (intercepted traffic is not optimized but is passed through).

☑ Enable distribution of traffic on AppNav Controllers

Enable offload of pass-through connections from WAAS nodes to AppNav Controllers for following reasons:

☐ All pass-through connections

☑ Due to missing policy configuration

☑ Due to no peer WAAS node

☑ Due to intermediate WAAS node

Submit Reset

Step 4 In the **Name** field, enter a new name for the cluster if you want to rename it. (This feature is not available on AppNav-XE clusters.)

Step 5 (Optional) In the **Description** field, enter the cluster description. Use only letters and numbers, up to a maximum of 200 characters. (This feature is not available on AppNav-XE clusters.)

Step 6 (Optional) In the **Authentication Key** and **Confirm Authentication Key** fields, enter an authentication key that is used to authenticate communications between the Cisco WAAS devices in the cluster. Use only letters and numbers, up to a maximum of 64 characters.

Step 7 (Optional) In the **Shutdown Wait Time** field, enter the number of seconds that the WNs in the cluster should wait for all the connections to get terminated before shutting down. The default is 120 seconds.

Step 8 (Optional) To configure cluster distribution and off-loading of pass-through connections, expand the **Advanced Settings** section by clicking it.

Step 9 (Optional) To enable distribution of traffic from the ANCs in the cluster to WNs, ensure that the **Enable distribution of traffic on AppNav Controllers** check box is checked. To disable distribution of traffic, uncheck this box. When distribution is disabled, the cluster operates in monitoring mode where it continues to intercept traffic and, instead of distributing it to WNs, passes it through. This mode can be useful for monitoring traffic statistics without optimizing the traffic. (Not available on AppNav-XE clusters.)

Step 10 (Optional) To configure offloading of pass-through connections from WNs to ANCs, check the check boxes in the **Enable offload of pass-through connections from WAAS nodes to AppNav Controllers for following reasons** section. This feature allows pass-through connections to be passed through at the ANC instead of being distributed to the WN and then passed through. Configure pass-through offload as follows:

a) To offload all pass-through connections, which includes connections passed through due to error conditions, check the **All pass-through connections** check box. Check this check box only if you do not require application visibility on the WNs into pass-through traffic due to error conditions. The default is unchecked.

b) To offload connections passed through due to missing policy configuration, check the **Due to missing policy configuration** check box. By default, it is checked.

c) To offload connections passed through due to the absence of peer WN, check the **Due to no peer WAAS node** check box. By default, it is checked.

d) To offload connections passed through due to an intermediate WN, check the **Due to intermediate WAAS node** check box. By default, it is checked.

e) If some of the WNs use different pass-through offload settings, you can synchronize the settings on all the WNs to match the configuration shown here by checking the **Synchronize settings on all devices** check box. This check box is shown only if the settings on some WNs are different. The default is unchecked.

Step 11 Click **Submit**.

The lower part of this window includes tabs that show lists of the ANCs, WNs, and WNGs that are a part of the cluster. On AppNav-XE devices, there is an additional AppNav Contexts tab that displays contexts. The controls in these parts of this window work are described in the following sections:

- AppNav Controllers: Configuring AppNav Controller Settings, on page 110
- AppNav Contexts: Configuring AppNav Contexts, on page 112
- WAAS Nodes: Configuring WAAS Node Settings, on page 114
- WAAS Node Groups: Configuring WAAS Node Group Settings, on page 115

To configure AppNav Cluster settings for an individual WN, see Configuring AppNav Cluster Settings for a WAAS Node, on page 116. If you are using an authentication key to authenticate communications, you must configure the cluster and each WN with the same key.

Configuring AppNav Controller Settings

This section contains the following topics:

Configuring AppNav Controller Settings for a WAAS Appliance

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **AppNav Controllers** tab below the topology diagram.

All the ANCs in the cluster are listed, along with the name, location, IP address, and interface used for intracluster traffic, and enabled status.

From this list, you can perform the following tasks:

- Edit the interface settings for an ANC by choosing the ANC and clicking the **Edit** taskbar icon, as described in the following steps.
- Delete an ANC by choosing the ANC and clicking the **Delete** taskbar icon.
- Add a new ANC to the cluster by clicking the **Add AppNav Controller** taskbar icon. See Adding an ANC to a Cluster, on page 117.
- Enable a disabled ANC by choosing the cluster and clicking the **Enable** taskbar icon.
- Disable an ANC by choosing the ANC and clicking the **Disable** taskbar icon.

Step 3 Click the radio button next to the ANC that you want to edit and click the **Edit** taskbar icon.

The **Edit AppNav Controller** pane appears.

Step 4 Configure the internal WAAS node settings:

a) To enable optimization on the ANC, check the **Enable WAN optimization (Internal WAAS Node)** check box.
b) If you enabled WAN optimization, from the **WAAS Node Group** drop-down list, choose the WNG to which the internal WN should belong.
c) Click **Next**.

Step 5 (Optional) Configure the WCCP settings for the ANC. This window does not appear if the ANC is configured for inline interception. For more information on the WCCP fields, see Configuring or Viewing the WCCP Settings on ANCs.

When finished with the WCCP settings, click **Next**.

The Graphical Interface Wizard appears.

Step 6 Configure the interception and cluster interface settings:

a) In the Graphical Interface view, configure interception interfaces on the AppNav Controller Interface Module, as required. For details on how to use the wizard, see Configuring Interfaces with the Graphical Interface Wizard, on page 90.
b) From the **Cluster Interface** drop-down list, choose the interface to be used for intracluster traffic.
c) (Optional) To enable swapping of client and WAAS device source IP address fields in intra-cluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box.

   You may want to enable this option if you are using a port channel for the cluster interface or there is a load-balancing device between the ANC and WN. This option can improve the load balancing of the traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.) The Cisco WAAS Central Manager enables this feature automatically if any existing ANCs have port channel cluster interfaces.

Step 7 Click **Finish**.

Configuring ANC Settings for an AppNav-XE Device

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **AppNav Controllers** tab below the topology diagram.

All the ANCs in the cluster are listed, along with the name, location, IP address, interface used for intracluster traffic, and enabled status.

From this list, you can perform the following tasks:

- Edit the interface settings for an ANC by choosing the ANC and clicking the **Edit** taskbar icon, as described in the following steps.
- Delete an ANC by choosing the ANC and clicking the **Edit** taskbar icon.
- Add a new ANC to the cluster by clicking the **Add AppNav Controller** taskbar icon. See Adding an ANC to a Cluster, on page 117.

Step 3 Click the radio button next to the ANC that you want to edit and click the **Edit** taskbar icon.

The **Edit AppNav Controller** pane appears.

Step 4 On an AppNav-XE cluster, configure the interception and cluster interface settings:

a) Choose the WAN interfaces on which traffic interception is to be enabled. Interfaces must already be configured on the AppNav-XE devices; only those on which service insertion can be enabled are listed.
b) From the **Cluster Interface** drop-down list, choose the interface to be used for intra-cluster traffic.

Step 5 Click **Finish**.

Configuring AppNav Contexts

Before you begin

An AppNav-XE cluster can have up to 32 contexts. A WAAS appliance AppNav cluster can have only one context, which is defined by the cluster settings; the ability to add contexts is not available.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **AppNav Contexts** tab below the topology diagram.

All the AppNav contexts in the cluster are listed, along with the name, associated WNGs, VRFs, the AppNav policy, and enabled status.

From this list, you can perform the following tasks:

- Edit a context by choosing the context and clicking the **Edit** taskbar icon.

- Delete a context by choosing the context and clicking the **Delete** taskbar icon.
- Enable a disabled context by choosing the context and clicking the **Enable** taskbar icon.
- Disable a context by choosing the context and clicking the **Disable** taskbar icon.
- Add a new context as described in the steps that follow. (This feature is not allowed for Cisco WAAS appliance clusters.)

Step 3 Click the **Add AppNav Context** taskbar icon.

Step 4 From the **WAAS Cluster ID** drop-down list, choose the cluster ID to assign to this context. The first available ID is initially selected.

Step 5 (Optional) In the **AppNav Policy Name** field, specify the name of the AppNav policy to associate with the cluster. A default suggested policy name initially appears in the field, which you can change if you want to. If you enter the name of a policy that does not exist, it is created.

Note You cannot specify a name that uses the same form as the default name but with a number that is different from the context ID, because such names are reserved for the default policy maps associated with contexts.

Step 6 (Optional) In the **WAAS Node Group** field, specify the name of the WNG to associate with the context. A default suggested WNG name initially appears in the field, which you can change if desired. If you enter the name of a WNG that does not exist, it is created. To associate a WNG with a context, the WNG must be used in policy rules that are used in the context.

You cannot specify a name that uses the same form as the default name but with a number different than the context ID, because such names are reserved for the default WNGs associated with contexts.

Step 7 (Optional) Select the **Disable PassThrough FlowSync** check box if you do not want the passthrough flow information to be synchronized between all the AppNav-XE devices in the cluster. By default, when more than one AppNav-XE device is configured in a cluster, the passthrough and redirect flow information is synchronized between all the AppNav-XE devices in the cluster.

Step 8 Click **Next**.

Step 9 Select one or more VRFs to associate with the context. Follow these steps:

a) From the **Show** drop-down list, choose a filter the VRF list, as required. You can use Quick Filter or Show All VRFs. The lower part of the pane lists ineligible VRFs, along with the reason why each is ineligible.
b) Check the check box next to each VRF that you want to associate with the context.
c) Click **Next**.

Step 10 Choose the WN devices that you want to be a part of the WNG associated with the context:

a) Choose WNs in the WAAS Nodes device list by checking the check box next to the device names. You can use the filter settings in the taskbar to filter the device list.

   If there are devices that are ineligible to join the cluster, click **Show Ineligible Devices** to see them and the reasons why they are ineligible. You can use the filter settings to filter the list.

b) Click **Next**.

Step 11 Configure the cluster interface settings for each WN device in the context.

The Cluster Interface Wizard appears, with one window for each WN in the context:

a) Configure individual interfaces, as required, on the device by using the Graphical Interface Wizard. For details on how to use the wizard, see Configuring Interfaces with the Graphical Interface Wizard, on page 90.

b) From the **Cluster Interface** drop-down list, choose the interface to be used for intra-cluster traffic.

c) Click **Next**.

If you are configuring multiple WNs, a similar screen is shown for each device.

Step 12 Click **Finish** to save the context configuration.

Configuring WAAS Node Settings

Before you begin

All the WNs in a Cisco WAAS appliance cluster must be configured with application-accelerator device mode and appnav-controller interception mode. If you created the cluster with the Cisco WAAS Central Manager AppNav Wizard, both of these settings are already in place. (The wizard sets the interception, and the device mode would have been set before the wizard is run.)

From within the AppNav Cluster, you can configure the following settings for a WN:

- WNG to which a WN belongs
- AppNav Controller Interface Module interface settings (including configuring port channel, standby, and bridge group interfaces)
- Cluster interface used for intracluster traffic

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** *cluster-name*.

Step 2 Click the **WAAS Nodes** tab below the topology diagram.

All the WNs in the cluster are listed, along with the name, location, IP address, interface in use, WNG to which the node belongs, and enabled status.

From this list, you can perform the following tasks:

- Edit the settings for a WN by choosing the WN and clicking the **Edit** taskbar icon.
- Delete a WN by choosing the WN and clicking the **Delete** taskbar icon.
- Add a new WN to the cluster by clicking the **Add WAAS Node** taskbar icon. See Adding a New WAAS Node to the Cluster, on page 119.
- Enable a disabled WN by choosing the node and clicking the **Enable** taskbar icon.
- Disable a WN by choosing the node and clicking the **Disable** taskbar icon.

Step 3 Click the radio button next to the WN that you want to edit and click the **Edit** taskbar icon.

The **WAAS Node** pane appears.

Step 4 From the **WAAS Node Group** drop-down list, choose the WNG to which you want to assign the node.

Step 5 In the graphical interface view, configure interfaces on the device, as required. For more information, see Configuring Interfaces with the Graphical Interface Wizard, on page 90.

Step 6 From the **Cluster Interface** drop-down list, select the interface to be used for intra-cluster traffic.

Step 7 (Optional) To enable swapping of client and WAAS device source IP address fields in intra-cluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box. (This option is not available for WNs used in an AppNav-XE cluster.)

Enable this option if you are using a port channel for the cluster interface or there is a load-balancing device between the ANC and WN. This option can improve load balancing of the traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.) The Central Manager enables this feature automatically if any existing ANCs have port channel cluster interfaces.

Step 8 To save the settings, click **OK**.

Configuring WAAS Node Group Settings

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **WAAS Node Groups** tab below the topology diagram.

All the WNGs in the cluster are listed, along with the name, description, and the WNs contained in the group. In an AppNav-XE cluster, the list also shows the WAAS cluster ID.

From this list, you can perform the following tasks:

- Edit the settings for a WNG by choosing the WNG and clicking the **Edit** taskbar icon.
- Delete a WNG by choosing the WNG and clicking the **Delete** taskbar icon.
- Add a new WNG to the cluster by clicking the **Add WAAS Node Group** taskbar icon. See Adding a New WAAS Node Group to the Cluster, on page 120.

Step 3 Click the radio button next to the WNG that you want to edit and click the **Edit** taskbar icon.

Step 4 (Optional) In the **Description** field, enter a description of the WNG, with up to 32 alphanumeric characters on a WAAS appliance cluster. For an AppNav-XE cluster, you can enter up to 241 characters, not including a space.

Step 5 Click **OK** to save the settings.

To associate a newly created WNG with the desired context in an AppNav-XE cluster, you must use it in the AppNav policy rules of the context. For one or more rules, choose the WNG for the **Distribute To** action of the policy rule.

Configuring AppNav Cluster Settings for a WAAS Node

Before you begin

The **WAAS Node Configuration** window is available for a WN only if the device mode is configured as appnav-controller. This window is editable only if the WN is running Cisco WAAS Version 5.2.1 or later, and is not a part of an AppNav cluster.

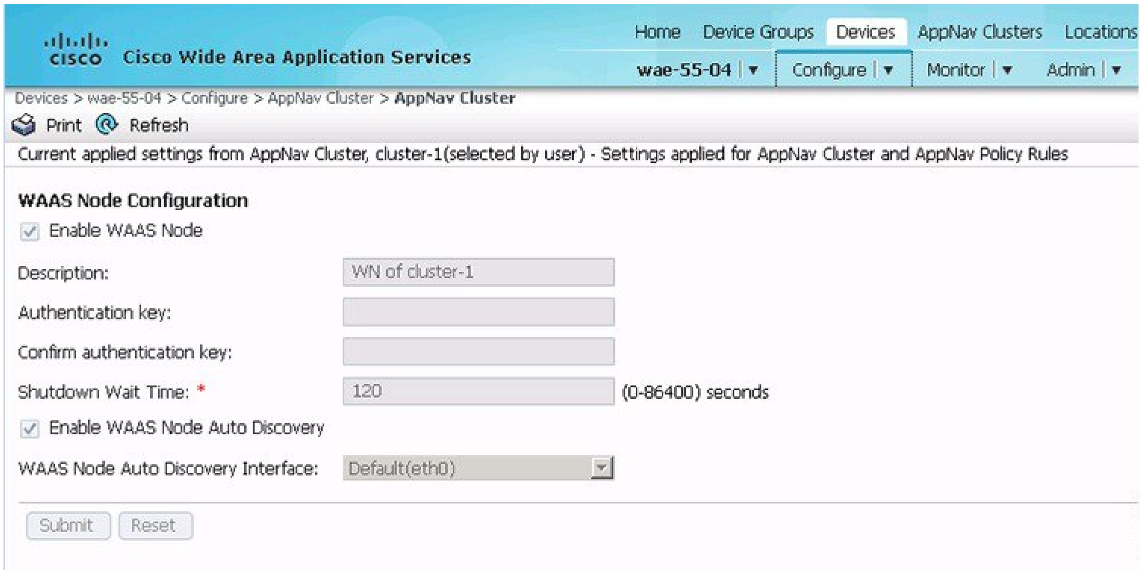
Procedure

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

Step 2 Choose **Configure** > **AppNav Cluster** > **AppNav Cluster**.

The **WAAS Node Configuration** window appears.

Figure 24: WAAS Node Configuration Window



Current applied settings from AppNav Cluster, cluster-1(selected by user) - Settings applied for AppNav Cluster and AppNav Policy Rules

WAAS Node Configuration

☑ Enable WAAS Node

Description: WN of cluster-1

Authentication key:

Confirm authentication key:

Shutdown Wait Time: * 120 (0-86400) seconds

☑ Enable WAAS Node Auto Discovery

WAAS Node Auto Discovery Interface: Default(eth0)

Step 3 (Optional) To enable this WN to handle traffic distributed by the ANC, check the **Enable WAAS Node** check box.

Step 4 (Optional) In the **Description** field, enter the WN description. Use only letters and numbers, up to a maximum of 200 characters are allowed.

Step 5 (Optional) In the Authentication Key and Confirm Authentication Key fields, enter an authentication key that is used to authenticate communications between the WN and the ANC. Use only letters and numbers, up to a maximum of 64 characters.

Step 6 (Optional) In the Shutdown Wait Time field, enter the number of seconds that the WN should wait for all the connections to be terminated before shutting down. The default is 120 seconds.

Step 7 (Optional) To enable automatic discovery of this WN by the ANC, check the **Enable WAAS Node Auto Discovery** check box. (This feature is not used on WNs with Cisco WAAS Version 5.1 and earlier.)

This setting is intended to allow an AppNav-XE ANC to discover WNs that are to participate in a cluster that is created by the CLI and not configured by the Cisco WAAS Central Manager.

Step 8 From the **WAAS Node Auto Discovery Interface** drop-down list, choose the WN interface that is to be used for auto discovery. (This feature is not used on WNs with Cisco WAAS version 5.1 and earlier.)

Step 9 Click **Submit**.

What to do next

To configure AppNav Cluster settings at the cluster level, see Configuring AppNav Cluster Settings for an AppNav Cluster, on page 108. If you are using an authentication key to authenticate communications, you must configure the cluster and each WN with the same key.

Note Do not use both automatic node discovery and the Cisco WAAS Central Manager to add a WN to an AppNav-XE cluster. We recommend that you disable automatic node discovery in AppNav-XE and then register the device and add it to the cluster with the Cisco WAAS Central Manager.

Adding or Removing Devices from the AppNav Cluster

This section contains the following topics:

Adding an ANC to a Cluster

Procedure

Step 1 Configure the basic device and network settings on each new ANC, and ensure that the device mode is set to appnav-controller on a WAAS appliance.

Step 2 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 3 Click the **AppNav Controllers** tab below the topology diagram.

Step 4 Click the **Add AppNav Controller** taskbar icon.

The **Add AppNav Controllers** pane appears.

Step 5 Select the ANC devices to add:

a) Select one or more ANCs in the AppNav Controller device list by checking the check boxes next to the device names. You can use the filter settings in the taskbar to filter the device list.

   If there are devices that are ineligible to join the cluster, click **Show Ineligible Devices** to see them and the reasons why they are ineligible. You can use the filter settings to filter the list.

b) Click **Next**.

Step 6 Configure the interception method, policy, WCCP settings (if using WCCP interception), VRFs, and interfaces for each ANC device you are adding (different screens and options appear for WAAS appliance and AppNav-XE clusters):

a) From the **Interception Method** drop-down list, choose **WCCP** or **Inline**. (This feature is not used on AppNav-XE clusters.)

b) From the **AppNav Policy-Map** drop-down list, choose the AppNav policy to apply to the ANC. (Not used on AppNav-XE clusters.)

c) (Optional) To enable optimization on the ANC devices, check the **Enable WAN optimization (Internal WAAS Node)** check box. (This feature is not used on AppNav-XE clusters.)

d) (Optional) If you enabled WAN optimization, from the **WAAS Node Group** drop-down list, choose the WNG to which the internal WN should belong. (This feature is not used on AppNav-XE clusters.)

e) Click **Next**.

f) (Optional) If you chose WCCP interception, configure the WCCP settings on the WCCP settings pane that appears. For details on WCCP settings, see Configuring or Viewing the WCCP Settings on ANCs in the chapter, "Configuring Traffic Interception."

Note Remember to check the **Enable WCCP Service** check box to enable WCCP.

g) If you configured WCCP settings, click **Next**.

h) On an AppNav-XE cluster, choose the VRF instances to associate with the service context by checking the check box next to each VRF instance that you want to use. If you choose the VRF default, you cannot choose other VRFs. If you choose multiple VRFs, they must not have overlapping source IP addresses. Only VRFs that are available on all the ANCs are listed.

i) Click **Next**.

j) Configure the ANC interception interfaces. On a WAAS appliance cluster, you use the Cluster Interface Wizard graphical interface and on an AppNav-XE cluster, choose from a list of router interfaces. If you chose inline interception on a WAAS appliance, you must configure a bridge group interface. For details on using the wizard, see the Configuring Interfaces with the Graphical Interface Wizard, on page 90.

k) From the Cluster Interface drop-down list, select the interface to be used for intracluster traffic.

l) (Optional) To enable swapping of client and WAAS device source IP address fields in intracluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box. (Not available on AppNav-XE clusters.)

Enable this option if you are using a port channel for the cluster interface or there is a load-balancing device between the ANC and WN. This option can improve load balancing of the traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.) The Central Manager enables this feature automatically if any existing ANCs have port channel cluster interfaces.

m) Click **Next** to save the settings and continue with the next ANC you are adding. If this is the last ANC being added, click **Finish**.

After a convergence waiting period of up to two minutes, the new ANCs are available in the cluster for traffic interception and distribution. Traffic interception on the new ANCs is prevented until the devices have fully joined the cluster. You can monitor the ANC status as described in Monitoring an AppNav Cluster, on page 121.

Removing or Disabling an ANC from a Cluster

Procedure

Step 1 Disable the traffic interception path on the ANC. For an inline ANC, shut down the in-path interfaces, and for an ANC using WCCP, disable WCCP.

Traffic that was previously routed to this ANC is rerouted to other ANCs in the cluster.

Step 2 Disable the ANC (not necessary on an AppNav-XE cluster):

a) From the Cisco WAAS Central Manager menu, choose **AppNav Cluster** > *cluster-name*.

b) Click the **AppNav Controllers** tab below the topology diagram.

c) Click the radio button next to the ANC that you want to disable and then click the **Disable** taskbar icon.

The ANC is disabled and the service unreachable alarm is raised on the other ANCs in the cluster.

To permanently remove the ANC, click the radio button next to the ANC that you want to remove and then click the **Delete** taskbar icon.

This action removes the ANC from the ANCG on all the other ANCs and clears the service unreachable alarm on the other ANCs.

- If the ANC is configured for WCCP interception, all the WCCP settings on the device are removed.
- If the ANC is also configured as a WN, the WN is removed from the cluster.

Step 3 (Optional) Power down the ANC.

Adding a New WAAS Node to the Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** *cluster-name*.

Step 2 Click the **WAAS Nodes** tab below the topology diagram.

Step 3 Click the **Add WAAS Node** taskbar icon.

The **Add WAAS Nodes** pane appears.

Step 4 Select one or more WNs in the **WAAS Nodes** device list by checking the check boxes next to the device names. You can use the filter settings in the taskbar to filter the device list.

If there are devices that are ineligible to join the cluster, click **Show Ineligible Devices** to see them and the reasons why they are ineligible. You can use the filter settings to filter the list.

Step 5 Click **Next**.

Step 6 Configure the WNG and interfaces for each WN device you are adding:

a) From the **WAAS Node Group** drop-down list, choose the WNG to which you want to add the new WNs. The list shows only the defined WNGs.

b) Click **Next**.

c) Use the Cluster Interface Wizard graphical interface to configure the WN interfaces. For details on using this wizard, see Configuring Interfaces with the Graphical Interface Wizard, on page 90.

d) From the **Cluster Interface** drop-down list, select the interface to be used for intra-cluster traffic.

e) (Optional) To enable swapping of client and **WAAS device source IP address** fields in intra-cluster traffic, check the **Enable swapping of source IP address in intra-cluster traffic** check box. (Not available for AppNav-XE clusters.)

Enable this option if you are using a port channel for the cluster interface, or there is a load-balancing device between the ANC and WN. This option can improve load balancing of the traffic that the ANC distributes to WNs for optimization because it load balances based on the client IP address rather than the

ANC IP address. (For traffic from the server to the client, it swaps the server IP address with the ANC IP address.) The Central Manager enables this feature automatically if any existing ANCs have port channel cluster interfaces.

f) To save the settings and continue with the next WN you are adding, click **Next**. If this is the last WN being added, click **Finish**.

Step 7 Configure and enable optimization on the WNs. For more information, see the chapter Configuring Application Acceleration, on page 371.

After a convergence waiting period of up to two minutes, the new WNs are available on all the ANCs for optimization.

Removing a WAAS Node from a Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **WAAS Nodes** tab below the topology diagram.

Step 3 Choose the node and click the **Disable** taskbar icon.

This causes a graceful exit of the WN from the cluster. The ANCs stop sending new flows to the WN but continue to distribute existing flows to it until the connection count reaches zero, or the maximum shutdown wait time expires.

Note The default shutdown wait time is 120 seconds. You can configure it from the **Shutdown Wait Time** field in the AppNav Cluster tab.

Step 4 (Optional) When the graceful exit process on the WN is complete (all existing connections have terminated), remove the WN from the WNG on the ANCs by choosing the node and clicking the **Delete** taskbar icon.

You can monitor the node status in the topology diagram in the upper part of the window. The colored status light indicator on the device turns gray when the node is no longer processing connections.

Step 5 (Optional) Power down the WN.

Adding a New WAAS Node Group to the Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Click the **WAAS Node Groups** tab below the topology diagram.

Step 3 Click the **Add WAAS Node Group** taskbar icon.

The **Add WAAS Node Group** pane appears.

Step 4 In the **Name** field, enter the name of the WNG. On a WAAS appliance cluster, you can enter up to 32 alphanumeric characters, and on an AppNav-XE cluster, you can enter up to 64 characters, excluding a space.

Step 5 (Optional) In the **Description** field, enter a description of the WNG. You can enter up to 200 alphanumeric characters, including ' | \ ;' on a WAAS appliance cluster. In an AppNav-XE cluster, you can enter up to 241 characters, excluding a space.

Step 6 To save the settings, click **OK**.

Step 7 Add one or more WNs to the new WNG. To add a new WN, see Adding a New WAAS Node to the Cluster, on page 119, or to reassign an existing WN to the new WNG, see Configuring WAAS Node Settings, on page 114.

After a convergence waiting period of up to two minutes, the new WNG is available on all the ANCs for optimization.

Removing a WAAS Node Group from a Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name* .

Step 2 Click the **WAAS Nodes** tab below the topology diagram.

Step 3 Click the radio button next to the node name you want to disable and click the **Disable** taskbar icon. This causes a graceful exit of each WN from the cluster.

Step 4 After all WNs have completed a graceful exit from the cluster, click the **WAAS Node Groups** tab.

You can monitor the node status in the topology diagram in the upper part of the window. The colored status light indicator on the device turns gray when the node is no longer processing connections.

Step 5 (Optional) Choose the WNG you want to remove, and click the **Delete** taskbar icon.

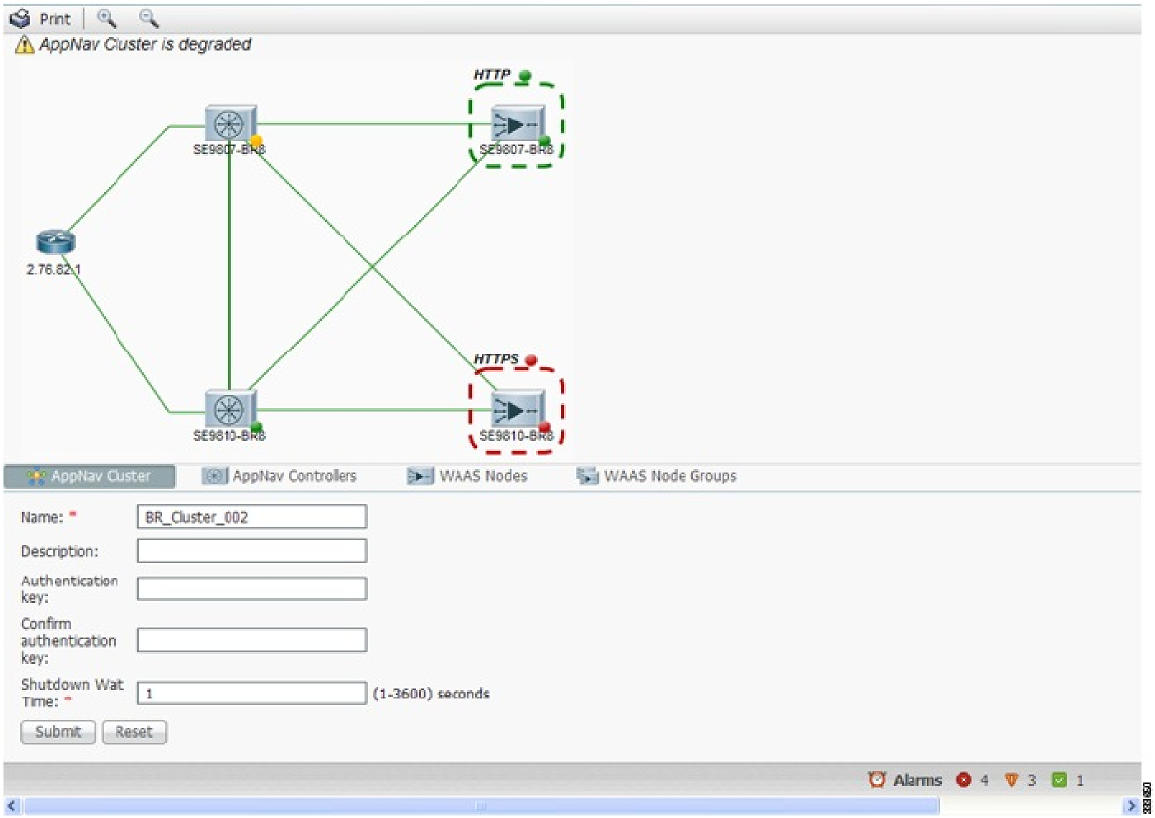
Monitoring an AppNav Cluster

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Cluster** *cluster-name*.

The **Cluster** home window displays the cluster topology and device status.

Figure 25: AppNav Cluster Topology and Status



AppNav Cluster is degraded

Name: * BR_Cluster_002

Description:

Authentication key:

Confirm authentication key:

Shutdown Wat Time: * 1 (1-3600) seconds

Submit Reset

Step 2 Consider the following guidelines for the using the **AppNav Cluster** window:

- To zoom in or out on the topology diagram, click the + or - magnifying glass icons in the taskbar. You can also click on the diagram and drag it within the window to reposition it.
- To change the cluster settings, edit any of the fields in the **Cluster Settings** tab below the topology diagram and click **Submit**.
- On AppNav-XE clusters, the **Name** and **Description** fields are not shown.
- To see all the AppNav contexts, click the **AppNav Contexts** tab below the diagram. From this tab, you can edit, delete, add, enable, or disable an AppNav context. This tab is not shown on WAAS appliance clusters.
- To see all the ANCs, click the **AppNav Controllers** tab below the diagram. From this tab, you can edit, delete, add, enable, or disable an ANC in the cluster.
- To see all the WNs, click the **WAAS Nodes** tab below the diagram. From this tab, you can edit, delete, add, enable, or disable a WN in the cluster.
- To see all the WNGs, click the **WAAS Node Groups** tab below the diagram. From this tab, you can edit, delete, or add a WNG in the cluster.
- The overall cluster status is shown in the top left corner of the diagram, as follows:
    - **Green**: All the ANCs are operational with no error conditions.

    - **Yellow**: Degraded because one or more ANCs have operational issues. This is also the initial state before all the nodes have sent status updates.
    - **Red**: Cluster is down because all the ANCs are down, or indicates a split cluster where there is no connectivity between one or more ANCs.

- The overall cluster status does not include administratively disabled ANCs.
- The status light indicators on each device and dotted lines around each WNG show the status of the device or group:
    - **Green**: Operational with no error conditions
    - **Yellow**: Degraded (overloaded, joining cluster, or has other noncritical operational issues)
    - **Red**: Critical (one or more processes is in a critical state)
    - **Gray**: Disabled
    - **Black**: Unknown status
- The lines between each device show the status of the link between devices:
    - **Green**: Operational with no error conditions
    - **Red**: Link is down
    - **Black**: Unknown status
- A red plus symbol is shown on the upper right corner of any device that is added to an AppNav-XE cluster by automatic node discovery. The cluster configuration of such a device is not being managed by the Cisco WAAS Central Manager, and you should verify that its configuration is correct.

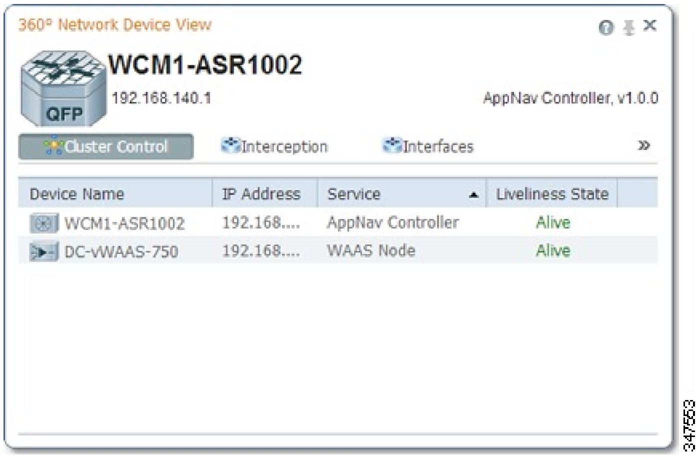
  Additionally, statistics from the device are not aggregated in any Central Manager reports if the device is not registered to the Cisco WAAS Central Manager; if the device is registered to the Central Manager, its optimization (but not AppNav) statistics are included in Central Manager reports.

Step 3 Consider these general guidelines for using and monitoring an AppNav cluster:

- Do not use both automatic node discovery and the Central Manager to add a WN to an AppNav-XE cluster. We recommend that you disable automatic node discovery in AppNav-XE and then register the device and add it to the cluster with the Cisco WAAS Central Manager. For details on configuring auto discovery, see Configuring AppNav Cluster Settings for a WAAS Node, on page 116.
- An orange triangle warning indicator is shown on any device for which the Cisco WAAS Central Manager may not have current information because the device has not responded within the last 60 seconds (the device could be offline or unreachable).
- A recently removed device still appears in the topology diagram for a few minutes until all the devices agree on the new cluster topology.

Step 4 To view a more comprehensive device status display, hover your cursor over a device icon to see the **360-degree Network Device View** dialog box. (The dialog box for a WN device is similar.)

Figure 26: ANC 360-Degree Network Device View



360° Network Device View

WCM1-ASR1002

192.168.140.1

AppNav Controller, v1.0.0

Device Name	IP Address	Service ▲	Liveliness State
WCM1-ASR1002	192.168....	AppNav Controller	Alive
DC-vWAAS-750	192.168....	WAAS Node	Alive

The **360-degree Network Device View** dialog box shows the following status information:

- Device name and IP address.
- Device type and software version.
- (ANC only) Interception tab that displays the interception method for a WAAS appliance (Inline or WCCP). For inline, this tab shows the bridge groups defined for interception, their member interfaces, and their status. For WCCP, this tab lists the defined WCCP service IDs, their associated client IP addresses, router IP address, and notes about problems. For an AppNav-XE device, this tab shows the router interfaces on which interception is enabled and their status.
- (ANC only) **Overloaded Policies** tab that lists monitored AppNav policies that are overloaded. (Not shown on AppNav-XE devices.)
- (ANC only) **Cluster Control** tab that lists all the devices in the cluster, along with device name, IP address, service type, liveliness state, and reason for any error condition.
- (WN only) **Optimization** tab that lists the application accelerators and their status.
- Alarms tab that lists pending alarms on the device. (Not shown on AppNav-XE devices.)
- Interfaces tab that lists the device interfaces and status. You can filter the list by choosing a filter type from the drop-down list above the interface list, entering filter criteria, and clicking the filter icon.

Step 5 Consider the following guidelines for displaying AppNav cluster status:

- You can pin the status dialog box so it stays open by clicking the pin icon in the upper right corner. You can also drag the dialog box to any location within your browser window.
- For additional cluster status, you can view the **Monitor** > **AppNav** > **AppNav Report** as described in AppNav Report in the chapter "Monitoring Your Cisco WAAS Network."
- If you have multiple AppNav Clusters, you can see the brief status for all of them at once by choosing **AppNav Clusters** > **All AppNav Clusters** from the menu.

Step 6 Consider the following guidelines to display connection statistics:

- To trace connections in a Cisco WAAS appliance cluster, see AppNav Connection Tracing, on page 125.

- To view connection statistics in an AppNav-XE cluster, see AppNav Connection Statistics, on page 126.

Step 7 Consider the following guidelines about the **Force Settings** feature:

- You may see a taskbar icon named **Force Settings on all the Devices in a Group** if the configuration across all the ANCs in the cluster becomes unsynchronized. If you see the icon, it means that the cluster settings, ANC configuration, WN configuration, and WNG configuration do not match on all the ANCs in the cluster. This scenario may occur if you configure a device outside the Cisco WAAS Central Manager by using the Cisco WAAS CLI.

  To update all the devices with the configuration that is currently shown in the Cisco WAAS Central Manager for the cluster, click the **Force Settings** Taskbar icon.

- You may also see a Taskbar icon named **Force Settings** in the AppNav XE Cluster page when you downgrade the router (that is part of this cluster) from a **PassThrough FlowSync** supported software version, such as Cisco IOS XE 17.2 to a non-supported software version, lower than Cisco IOS XE 17.2.x.

  To prevent this from happening, uncheck the **Disable PassThrough FlowSync** check box before performing the downgrade.

AppNav Connection Tracing

Before you begin

To assist in troubleshooting AppNav flows in a Cisco WAAS appliance cluster, use the **Connection Trace** tool in the Cisco WAAS Central Manager. This tool shows the following information for a particular connection:

- Whether the connection was passed through or distributed to a WNG
- Pass-through reason, if applicable
- The WNG and WN to which the connection was distributed
- Accelerator monitored for the connection
- Class-map applied

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Monitor** > **Tools** > **Connection Trace**.

Step 3 From the **AppNav Controller** drop-down list, choose the ANC that has the connection that you want to trace.

Step 4 From the **Site (Remote Device)** drop-down list, choose the peer WAAS device at the remote site.

Step 5 In one or more of the **Source IP**, **Source Port**, **Destination IP**, and **Destination Port** fields, enter matching criteria for one or more connections.

Step 6 Click **Trace** to display the connections that match the IP address and port criteria.

Connections are displayed in the **Connection Tracing Results** table below the fields. Use the filter settings in the **Show** drop-down list to filter the connections, as required. You can use **Quick Filter** to filter on any value or use **Show All Connections**.

Step 7 To display flow distribution information from the Cisco WAAS CLI, run the show **appnav-controller flow-distribution** EXEC command.

Another troubleshooting tool that you can use to trace connections on a WAAS appliance AppNav cluster is the Cisco WAAS **TCPtraceroute** tool. For more information, see Using WAAS TCP Traceroute in the chapter "Troubleshooting Your Cisco WAAS Network."

AppNav Connection Statistics

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **AppNav Clusters** > *cluster-name*.

Step 2 Choose **Monitor** > **Tools** > **Connection Statistics**.

Step 3 From the **AppNav Controller** drop-down list, choose the ANC from which you want to view statistics.

Step 4 In the **Source IP Address**, **Source Port**, **Destination IP Address**, **Destination Port**, and **Vrf Name** fields, enter matching criteria for one or more connections.

Step 5 Click **Submit** to display the connection statistics that match the IP address and port criteria.

Connections are displayed in the **Connection Statistics** table below the fields. Use the filter settings in the **Show** drop-down list to filter the connections, as required. You can use **Quick Filter** to filter on any value or **Show All Connections**.

You can display connection statistics from the Cisco WAAS CLI by running using the **show service-insertion statistics connection** EXEC command.

CHAPTER 5

Configuring Traffic Interception

This chapter describes how to configure interception of TCP traffic in an IP-based network, based on the IP and TCP header information, and how to redirect the traffic to Cisco Wide Area Application Services (WAAS) devices. This chapter describes the use of the Web Cache Communication Protocol (WCCP), policy-based routing (PBR), inline mode for transparent redirection of traffic to Cisco Wide Area Application Engines (WAEs), appnav-controller mode for use with an AppNav Controller.

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

Before you perform the procedures in this chapter:

This chapter contains the following sections:

Traffic Interception Methods

This section contains the following topics:

About Traffic Interception Methods

Prerequisities for configuring traffic interception for Cisco WAAS

- Complete a basic initial installation and configuration of your Cisco WAAS network, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.
- For detailed command syntax information for any of the Cisco WAAS CLI commands in this chapter, see *Cisco Wide Area Application Services Command Reference*.
- For more information about WCCP see the Cisco IOS documentation.

In a Cisco WAAS network, traffic between clients in the branch offices and the servers in the data center can be redirected to WAEs for optimization, redundancy elimination, and compression. Traffic is transparently intercepted and redirected to WAEs based on policies that have been configured on the routers or on an AppNav Controller (ANC). The network elements that transparently redirect requests to a local WAE can be a router using WCCP Version 2 or PBR to redirect traffic to the local WAE or a Layer 4 to Layer 7 switch, for example, the Catalyst 6500 series Content Switching Module (CSM) or Application Control Engine (ACE).

Alternately, you can intercept traffic directly by using the inline mode with a WAE that has a Cisco WAE Inline Network Adapter or Interface Module. When equipped with a Cisco AppNav Controller Interface Module, a WAVE appliance or cluster can intercept network traffic through WCCP or inline mode, and based on flow policies, distribute that traffic to one or more WAEs (WAAS nodes) for optimization.

The following table summarizes the transparent traffic interception methods that are supported in your Cisco WAAS network.

Table 7: Supported Methods of Transparent Traffic Interception

Method	Description
WCCP Version 2	Used for transparent interception of application traffic and Common Internet File System (SMB) traffic. Used in branch offices and data centers to transparently redirect traffic to the Cisco WAAS devices. The traffic is transparently intercepted and redirected to the local WAE or ANC by a WCCP-enabled router or a Layer 3 switch. You must configure WCCP on the router and WAE in the branch office and the router and WAE in the data center. For more information, see the following sections: • WCCP Interception, on page 129 • Configuring Advanced WCCP Features on Routers, on page 133 • Configuring WCCP on Cisco WAEs, on page 137
PBR	Used in branch offices used for wide area application optimization. The branch office router is configured to use PBR to transparently intercept and route both client and server traffic to the WAE that resides in the same branch office. In data centers, used for data center application optimization. The data center router or Layer 3 switch can be configured to use PBR to transparently intercept and route client and server traffic to WAEs within the data center. PBR, however, does not support load balancing across multiple WAEs, such as WCCP does. PBR does not support load balancing when you use a hardware load balancer, such as the Cisco CSM or Cisco ACE. See Using Policy-Based Routing Interception, on page 161.

Method	Description
Inline	The WAE physically and transparently intercepts traffic between the clients and the router. To use this mode, you must use a Cisco WAAS device with the Cisco WAE Inline Network Adapter, Cisco Interface Module, or Cisco AppNav Controller Interface Module. See Using Inline Mode Interception, on page 171.
vPATH	**Note** Cisco WAAS versions 6.0 and later use either the WCCP or AppNav traffic interception methods. Cisco WAAS versions 5.5.1 and earlier use WCCP, AppNav, or vPATH traffic interception methods.
AppNav Controller	For WAEs that are part of an AppNav deployment and are configured as WAAS nodes in an AppNav Cluster, you must configure them to use the appnav-controller interception method. This configuration allows WAEs to receive and optimize traffic that is intercepted and distributed by the AppNav Controllers. See Configuring AppNav Interception, on page 185.
ACE or CSM	Cisco Application Control Engine (ACE) or Catalyst 6500 series Content Switching Module (CSM) installed in the data center for data center application optimization. The ACE or CSM allows for both traffic interception and load balancing across multiple WAEs within the data center.

Guidelines for Configuring Traffic Interception

Note these guidelines when configuration traffic interception for your Cisco WAAS network:

- ISR-WAAS devices support only the AppNav Controller interception method.
- For Cisco vWAAS in Azure, the supported traffic interception method is PBR (Police-Based Routing); vWAAS in Azure does not support WCCP or AppNav interception methods.
- Pass-through traffic does not benefit from optimization. For example, SSH port 22 has minimal traffic volume, so would not benefit by optimizing TCP flows.
- If you use Microsoft System Center Configuration Manager with Preboot Execution Environment (SCCM/PXE), we recommend the following configurations for the ports that carry SCCM/PXE traffic: port 80, port 443, and port 445.
    - **port 80**: Communicates with the distribution point. Configure for pass-through traffic.
    - **port 443**: Communicates with the distribution point. Configure for pass-through traffic.
    - **port 445**: Used for software package distribution data transfer. Configure for traffic optimization.

    Without these configurations you may see the error message **PXE error code 80070056**.

WCCP Interception

The Cisco WAAS software uses the WCCP standard, Version 2, for redirection. The main features of WCCP Version 2 include support for the following:

- Up to 32 WAEs per WCCP service
- Up to 32 routers per WCCP service
- Authentication of protocol packets
- Redirection of non-HTTP traffic
- Packet return (including generic routing encapsulation [GRE], allowing a WAE to reject a redirected packet and to return it to the router to be forwarded)
- Masking for improved load balancing
- Multiple forwarding methods
- Packet distribution method negotiation within a service group
- Command and status interaction between the WAE and a service group

Note WCCP works only with IPv4 networks.

Cisco WAAS software supports the WCCP TCP promiscuous mode service (services 61 and 62 by default, though these service IDs are configurable). This WCCP service requires that WCCP Version 2 is running on the router and the WAE.

The TCP promiscuous mode service is a WCCP service that intercepts all TCP traffic and redirects it to the local WAE.

The Cisco WAAS software also supports service passwords, WAE failover, and interception ACLs.

Many Cisco routers and switches can be configured and enabled with WCCP Version 2 support for use with Cisco WAAS devices.

Many legacy Cisco routers, including the 2500, 2600, and 3600 routers, have far less processing power and memory than newer routing platforms, such as the Integrated Services Router (ISR) models 2800 and 3800. As such, the use of WCCPv2 or PBR may cause a high level of CPU utilization on the router and cause erratic behavior. WAAS can be configured to work with these routers, but not to the same levels of performance or scalability as can be found with newer routing platforms. The Cisco ISR is the routing platform of choice for the branch office.

If you are experiencing erratic behavior, such as the WAE being ejected from the service group, enable fair queuing, weighted fair queuing, or rate limiting on all physical interfaces on the router that connect to users, servers, WAEs, and the WAN. Fair queuing cannot be configured on subinterfaces, and should be configured on both ingress and egress physical interfaces. If another form of queuing is already configured on the LAN or WAN interfaces other than fair queuing, and provides similar fairness, it should be sufficient.

Additionally, limit the amount of bandwidth that can be received on the LAN-side interface of the router, to help the router keep its interface queues less congested and provide better performance and lower CPU utilization. Set the maximum interface bandwidth on the router to no more than 10 times the WAN bandwidth capacity. For instance, if the WAN link is a T1, the LAN interface and WAE LAN interface bandwidth should be throttled to 10 * T1 = 10 * 1.544 Mbps, or approximately 15 Mbps. See the Cisco IOS documentation for more information.

This section contains the following topics:

- Guidelines for Configuring WCCP Version 2, on page 131

- Guidelines for File Server Access Methods, on page 133

Configuring WCCP Version 2

This section contains the following topics:

- Guidelines for Configuring WCCP Version 2, on page 131
- Guidelines for File Server Access Methods, on page 133

Guidelines for Configuring WCCP Version 2

When you configure transparent redirection on a WAE using WCCP Version 2, follow these guidelines:

- **Creating WCCP Passwords**

  Use WCCP passwords to avoid denial-of-service attacks. For more information, see Setting a Service Group Password on a Router.

- **Configuring WCCP and Routers and WAEs**

  Configure the routers and WAEs to use WCCP Version 2 instead of WCCP Version 1 because WCCP Version 1 supports only web traffic (port 80).

  To configure basic WCCP, enable the WCCP service on at least one router in your network and on the WAE or ANC that you want the traffic redirected to. It is not necessary to configure all the available WCCP features or services to get your WAE up and running. For an example of how to complete a basic WCCP configuration on routers and WAEs in a branch office and data center, see the *Cisco Wide Area Application Services Quick Configuration Guide*.

  Cisco Express Forwarding (CEF) is required for WCCP and must be enabled on the router.

  Use Cisco WAAS CLI commands to configure basic WCCP on both the routers and the WAEs or ANCs. Alternatively, you can use CLI commands to configure the router for WCCP and use the Cisco WAAS Central Manager to configure basic WCCP on the Cisco WAEs or Cisco ANCs. In the configuration example provided in the *Cisco Wide Area Application Services Quick Configuration Guide*, the wccp global configuration command is used to configure basic WCCP on the Cisco WAEs or ANCs.

  We recommend that you use the Cisco WAAS CLI to complete the initial basic configuration of WCCP on your first branch WAE and data center WAE, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*. After you have verified that WCCP transparent redirection is working properly, you can use the Cisco WAAS Central Manager to modify this basic WCCP configuration or configure additional WCCP settings, for example, load balancing, for a WAE. For more information, see Configuring WCCP on WAEs. After you have configured basic WCCP on the router, you can configure advanced WCCP features on the router, as described in Configuring Advanced WCCP Features on Routers.

- **Configuring WCCP and Branch WAEs**

  Branch WAEs must not have their packets encrypted or compressed and should be part of the inside Network Address Translation (NAT) firewall if one is present.

  Place branch WAEs on the client side of the network to minimize client-side packets through the router.

- **Configuring WCCP Interception and Redirection**

  Intercept and redirect packets on the inbound interface whenever possible.

Use Layer 2 redirection as the packet forwarding method if you are using Catalyst 6500 series switches or Cisco 7600 Series Routers. Use Layer 3 GRE packet redirection if you are using any other Cisco router.

Use WCCP redirect lists for new implementations to limit client or server populations. For more information, see Configuring IP Access Lists on a Router .

Configure the WAE to accept redirected packets from one or more WCCP-enabled routers.

When you add a new router to an existing WCCP router farm or WCCP service group, the new router will reset existing connections. Until WCCP re-establishes path redirections and assignments, packets are sent directly to the client (as expected).

The router must support the redirect and return methods configured on the WAE. If the router does not support the configured methods, the WAE will not join the WCCP router farm. If you have a mix of routers in the farm, only those routers that support the configured methods will join the farm.

- **Configuring WCCP GRE and Generic GRE**

  Use WCCP GRE or generic GRE as the egress method to place WAEs on the same VLAN or subnet as clients and servers. This topology is not allowed when using the IP forwarding egress method.

- **Configuring WCCP Service Farms**

  To ensure consistency among WAEs, we recommend that you configure WCCP settings on one device and then use the Copy Settings taskbar icon from within the WCCP configuration window to copy the settings to other devices in your network. You should copy the settings only to the WAEs in the same WCCP service farm, AppNav Controller group (ANCG), or WAAS node group (WNG), because WCCP settings may have to be different in different farms or service groups.

  The WAE joins the WCCP farm only if the assignment method configured on the WAE is supported by the router. (The strict assignment method is always enforced with Version 4.4.1 and later.)

  A WAE joins a WCCP farm only if it is seen by all the configured routers in the farm. If there is a link failure in any one of the routers, the farm reconfigures, and the WAE is removed from the farm.

  All the WAEs in a WCCP farm must use the same pair of WCCP service IDs (the default is 61 and 62), and these IDs must match all the routers that are supporting the farm. A WAE with different WCCP service IDs is not allowed to join the farm, and an alarm is raised. Likewise, all the WAEs in a farm must use the same value for failure detection timeout. A WAE raises an alarm if you configure it with a mismatching value.

- **Configuring WCCP and TCP Promiscuous Mode**

  After enabling WCCP on the router, configure the TCP promiscuous mode service on the router and the WAE, as described in the Cisco Wide Area Application Services Quick Configuration Guide. The service IDs are configurable on the WAE; you choose a pair of numbers that are different from the default of 61 and 62 to allow the router to support multiple WCCP farms because the WAEs in different farms can use different service IDs. The router configuration must use WCCP service IDs that match those configured on the WAEs in each farm it is supporting.

  For the WAE to function in TCP promiscuous mode, the WAE uses WCCP Version 2 services 61 and 62 (the service IDs are configurable). These two WCCP services are represented by the canonical name tcp-promiscuous on the Cisco WAE.

- **Configuring WCCP, HSRP, and VRRP**

  When you configure WCCP for use with the Hot Standby Router Protocol (HSRP), you must configure the WAE with the HSRP or the Virtual Router Redundancy Protocol (VRRP) virtual router address as its default gateway, and the WAE WCCP router list with the primary address of the routers in the HSRP group.

- **WCCP Scalability**

  Virtual routing and forwarding-aware (VRF) WCCP scalability is as follows:

  - The maximum number of WAEs supported by a single VRF instance is 32.
  - The maximum number of VRF instances supported by the router is router dependent.
  - VRF-aware WCCP is supported only on specific releases of Cisco IOS software. Ensure that the router is running a release of Cisco IOS software that supports VRF-aware WCCP.
  - Each VRF instance has independent assignment, redirection, and return methods.

- **WCCP and Cisco WAAS Appnav Deployment**

  In a WAAS AppNav deployment, enable WCCP only on the ANC devices that are intercepting traffic and distributing it to the optimizing WAAS nodes (WNs). Configure WNs that are a part of the AppNav Cluster, with the appnav-controller interception method.

- **WCCP and MSS**

  To reduce the number of dropped packets in a network where WCCP L2 is deployed, we recommend that you configure the maximum segment size (MSS) to 1406 bytes on the WAAS nodes using the Cisco WAAS Central Manager. For more information on modifying MSS, see Modifying the Acceleration TCP Settings in the chapter "Configuring Application Acceleration."

Guidelines for File Server Access Methods

Some file servers have several network interfaces and can be reached through multiple IP addresses. For these server types, you must add all the available IP addresses to the branch WAE's WCCP accept list. This situation prevents a client from bypassing the branch WAE by using an unregistered IP address.

Some file servers have several NetBIOS names and only one IP address. Cisco WAAS uses that name to perform NetBIOS negotiations between the data center WAE and the file server, and to create resources in the cache. If a file server uses multiple NetBIOS names to represent virtual servers (possibly with different configurations) and has one NetBIOS name that is identified as the primary server name, put that name in the server list before the other names.

Configuring Advanced WCCP Features on Routers

This section describes how to configure the advanced WCCP Version 2 features on a WCCP-enabled router that is transparently redirecting requests to WAEs in your Cisco WAAS network and contains the following topics:

- Configuring a Router to Support WCCP Service Groups, on page 134
- Configuring IP Access Lists on a Router , on page 135
- Setting a Service Group Password on a Router, on page 136
- Configuring a Loopback Interface on the Router, on page 137
- Configuring Router QoS for WCCP Control Packets, on page 137

Note Before you perform the procedures in this section, you should have configured your router for basic WCCP as described in the *Cisco Wide Area Application Services Quick Configuration Guide* .

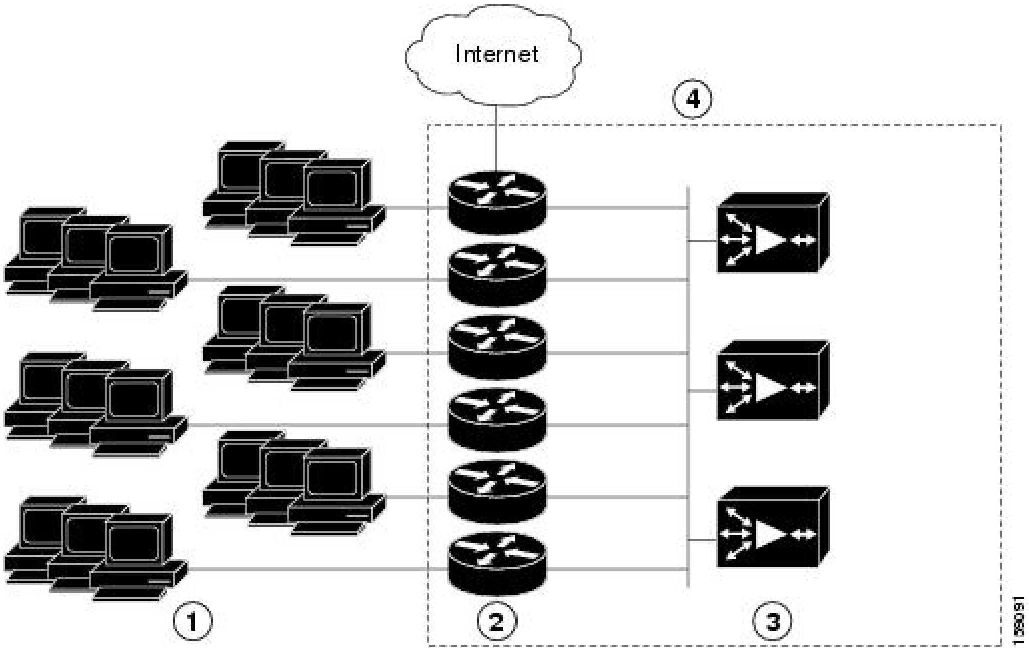
Configuring a Router to Support WCCP Service Groups

WCCP Version 2 enables a set of branch WAEs in a WAE or ANC group to connect to multiple routers. The WAEs in a group and the WCCP Version 2-enabled routers connected to the WAE group that are running the same WCCP service are known as a **service group**.

Through communication with the branch WAEs, the WCCP Version 2-enabled routers are aware of the available branch WAEs. Routers and branch WAEs become aware of one another and form a service group using WCCP Version 2 (Service Groups with WCCP Version 2).

In a Cisco WAAS AppNav deployment, only the ANCs are included in the service group. The routers do not send traffic directly to the optimizing WAEs (WNs); instead, ANCs distribute traffic within the WAAS network to the optimizing WNs.

Figure 27: Service Groups with WCCP Version 2



1	Clients requesting file services	3	Branch WAEs
2	Cisco routers	4	WAE service group

If you have a group of branch WAEs, the WAE that is seen by all the WCCP Version 2-enabled routers, and that has the lowest IP address, becomes the lead branch WAE.

The following procedure describes how a branch WAE in a service group is designated as the lead:

1. Each branch WAE is configured with a list of WCCP-enabled routers.

Multiple WCCP-enabled routers can service a group (up to 32 routers can be specified). Any of the available routers in a service group can redirect packets to each of the branch WAEs in the group.

2. Each branch WAE announces its presence to each router on the router list. The routers reply with their view of branch WAEs in the service group.
3. After the view is consistent across all of the branch WAEs in the group, one branch WAE is designated as the lead branch WAE and sets the policy that the WCCP-enabled routers need to deploy in redirecting packets.

The lead branch WAE determines how traffic should be allocated across the branch WAEs in the group. The assignment information is passed to the entire service group from the designated lead branch WAE so that the WCCP-enabled routers of the group can redirect the packets, and the branch WAEs in the group can better manage their load.

WCCP uses service groups to define WAAS services for a WCCP Version 2-enabled router and branch WAEs in a group. WCCP also redirects client requests to these groups in real time.

All the ports receiving redirected traffic that are configured as members of the same WCCP service group share the following characteristics:

- They have the same hash or mask parameters, as configured with the Cisco WAAS Central Manager (Configuring or Viewing the WCCP Settings on WAEs, on page 143) or the Cisco WAAS CLI (the **wccp service-number mask** global configuration command).
- The WCCP Version 2 service on individual ports cannot be stopped or started individually (a WCCP Version 2 restriction).

Configuring IP Access Lists on a Router

You can optionally configure the router to redirect traffic from your WAE based on access control lists (ACLs) that you define on the router. These access lists are also referred to as redirect lists.

Note We recommend that you use redirect lists on the WCCP-enabled router where possible, because that is the most efficient method to control traffic interception. However, you can also configure static bypass lists or interception ACLs on the WAEs, and of these two, we recommend that you use interception ACLs because they are more flexible and give better statistics about passed-through connections. For information about how to configure an interception ACL for a WAE, see Configuring Interception Access Control Lists, on page 155. For information about how to configure a static bypass list, see Configuring Static Bypass Lists for WAEs, on page 154. You can also configure interface ACLs on WAEs to control access to the WAE, as described in the chapter Creating and Managing IP Access Control Lists for WAAS Devices, on page 277 Redirect lists that are configured on the routers have the highest priority, followed by static bypass lists or interception ACLs on WAEs. Interception ACLs that are configured on WAEs take precedence over application definition policies that have been defined on the WAE.

A WCCP Version 2-enabled router can be configured with access lists to permit or deny redirection of TCP traffic to a WAE. The following example shows that traffic conforming to the following criteria are not redirected by the router to the WAE:

- Originating from the host 10.1.1.1 destined for any other host
- Originating from any host destined for the host 10.255.1.1

```
Router(config)# ip wccp 61 redirect-list 120
Router(config)# ip wccp 62 redirect-list 120
Router(config)# access-list 120 deny ip host 10.1.1.1 any
Router(config)# access-list 120 deny ip any host 10.1.1.1
Router(config)# access-list 120 deny ip any host 10.255.1.1
Router(config)# access-list 120 deny ip host 10.255.1.1 any
Router(config)# access-list 120 permit ip any
```

Traffic that is not explicitly permitted is implicitly denied redirection. The **access-list 120 permit ip any** command explicitly permits all traffic (from any source on the way to any destination) to be redirected to the WAE. Because criteria matching occurs in the order in which the commands are entered, the global **permit** command is the last command entered.

To limit the redirection of packets to those packets matching an access list, use the ip wccp redirect-list global configuration command. Use this command to specify which packets should be redirected to the WAE.

When WCCP is enabled, but the ip wccp redirect-list command is not used, all the packets matching the criteria of a WCCP service are redirected to the WAE. When you specify the ip wccp redirect-list command, only packets that match the access list are redirected.

The ip wccp global configuration command and the ip wccp redirect interface configuration command are the only commands required to start redirecting requests to the WAE using WCCP. To instruct an interface on the WCCP-enabled router to check for appropriate outgoing packets and redirect them to a WAE, use the **ip wccp redirect** interface configuration command. If the ip wccp command is enabled, but the ip wccp redirect command is disabled, the WCCP-enabled router is aware of the WAE, but does not use it.

To specify the access list by name or number, use the **ip wccp group-list** global configuration command, which defines criteria for group membership. In the following example, the **access-list 1 permit 10.10.10.1** command is used to define the IP address of the WAE that is allowed to join the WCCP service group:

```
Router(config)# ip wccp 61 group-list 1
Router(config)# ip wccp 62 group-list 1
Router(config)# access-list 1 permit 10.10.10.1
```

Tip If you have a WCCP service farm with multiple WAEs, the load-balancing assignment may cause packets that are sent to the WAE devices themselves (such as management traffic) to be redirected to a different WAE in the farm, negatively impacting performance. To avoid this situation, we recommend that you configure a WCCP redirect list that excludes traffic that is sent to the WAE IP addresses from being redirected.

For more information on access lists, see the Cisco IOS IP addressing and services documentation.

Setting a Service Group Password on a Router

For security purposes, you can set a service password for your WCCP Version 2-enabled router and the WAEs that access it. Only devices configured with the correct password are allowed to participate in the WCCP service group.

From the global configuration mode of your WCCP-enabled router, enter the following commands to specify the service group password for the TCP promiscuous mode service on the router (the service IDs must match the service IDs configured on the WAE):

```
Router(config)# ip wccp 61 password [0-7] password
Router(config)# ip wccp 62 password [0-7] password
```

The required *password* argument is the string that directs the WCCP Version 2-enabled router to apply MD5 authentication to messages received from the specified service group. Messages that are not accepted by the authentication are discarded. *0-7* is the optional value that indicates the HMAC MD5 algorithm used to encrypt the password. This value is generated when an encrypted password is created for the WAE. 7 is the recommended value. The optional *password* argument is the optional password name that is combined with the HMAC MD5 value to create security for the connection between the router and the WAE.

For information on using the Cisco WAAS Central Manager to specify the service group password on a WAE, see Configuring or Viewing the WCCP Settings on WAEs, on page 143.

Configuring a Loopback Interface on the Router

The highest IP address among the router's loopback interfaces is used to identify the router to the WAEs.

The following example configures the loopback interface, exits configuration mode, and saves the running configuration to the startup configuration:

```
Router(config)# interface Loopback0
Router(config-if)# ip address 111.111.111.111 255.255.255.0
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

Configuring Router QoS for WCCP Control Packets

Cisco WAAS sends WCCP control packets marked with a differentiated services code point (DSCP) value of 192. (In Cisco WAAS versions earlier than 4.2, packets were unmarked.) For a router to honor this priority value, you must configure the router's multilayer switching (MLS) quality of service (QoS) port trust state and classify traffic by examining the DSCP value. To configure the router appropriately, run the **mls qos trust dscp** command in interface configuration mode on the interface connected to the WAE.

Configuring WCCP on Cisco WAEs

This section contains the following topics:

- About Load Balancing and Cisco WAEs, on page 138
- About Packet-Forwarding Methods, on page 140
- Configuring or Viewing the WCCP Settings on WAEs, on page 143
- Configuring or Viewing the WCCP Settings on ANCs, on page 149
- Configuring and Viewing WCCP Router Lists for WAEs, on page 153
- Configuring WAEs for a Graceful Shutdown of WCCP, on page 153
- Configuring Static Bypass Lists for WAEs, on page 154
- Configuring Interception Access Control Lists, on page 155
- Configuring Egress Methods for WCCP-Intercepted Connections, on page 157

Note Before you perform the procedures in this section, you should have completed an initial configuration of your Cisco WAAS network, which includes the basic configuration of WCCP Version 2 and the TCP promiscuous mode service on your routers and WAEs, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.

About Load Balancing and Cisco WAEs

Multiple WAEs with WCCP support can be deployed for dynamic load balancing to enable adjustments to the loads being forwarded to the individual WAEs in a service group. IP packets received by a WCCP-enabled router are examined to determine if it is a request that should be directed to a WAE. Packet examination involves matching the request to a defined service criteria. These packets are passed to the processing routine on the router to determine which WAE, if any, should receive the redirected packets.

Note In a Cisco WAAS AppNav deployment, only ANCs are included in the service group and are load balanced by the routers. The routers do not send traffic to the optimizing WAEs (WNGs); instead, ANCs distribute traffic to the optimizing WNGs.

You can use load balancing to balance the traffic load across multiple WAEs. Load balancing allows the set of hash address buckets assigned to a WAE to be adjusted, shifting the load from an overwhelmed WAE to other WAEs that have available capacity. Two assignment methods are used by this technique: hashing and masking.

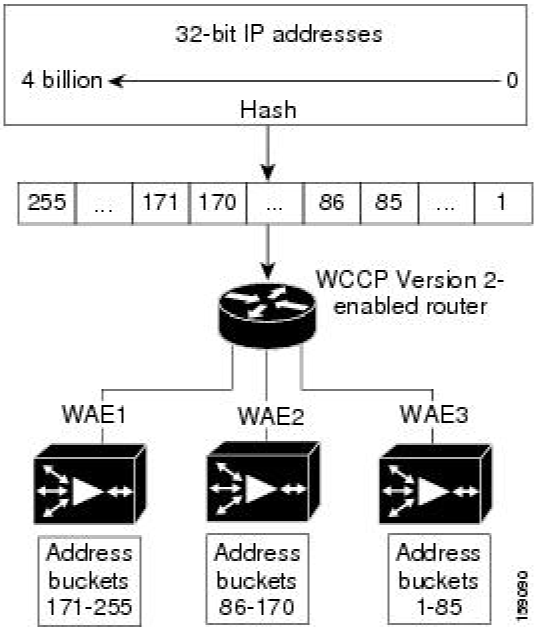
Assignment method denotes the method used by WCCP to perform load distribution across WAEs. The two possible load-balancing assignment methods are hashing and masking. If the mask load-balancing method is not specified, then the hash load-balancing method, which is the default method, is used.

Note In a Cisco WAAS AppNav deployment, only the mask assignment method is supported and is the default.

WCCP supports redirection based on a hash function. The hash key may be based on the source or destination IP address of the packet. For Cisco WAAS, load-balancing hashing is based on a source IP address (default), a destination IP address, or both.

The hash function uses the source IP address to obtain an address bucket to which the packet is assigned. These source address buckets are then mapped to a particular WAE depending on how many WAEs are present and how busy they are.

Figure 28: Load Balancing Through Hashing of IP Addresses



Note Packets that the WAEs do not service are tunneled back to the same router from which they were received. When a router receives a formerly redirected packet, it knows that it should not redirect it again.

Destination IP address hashing guarantees that a single WAE caches a given file server. This method, which allows a local coherency directive to be safely applied to the file server content (provided that no other collaboration on the content occurs), improves performance and WAN link and disk utilization. This method may distribute the load unevenly because of uneven activity on a file server.

Source IP address hashing has better potential for session distribution between the caches on branch WAEs. This method may impact performance and WAN link and disk utilization (see the previous description of factors to be aware of when load balancing is applied). Also, any change in the IP address of a client (which can happen when working in DHCP environments) may cause the client to switch to another branch WAE, which can cause the client to experience reduced performance until the client's working set is retrieved into the new cache.

Hashing that is based on a client IP address does not guarantee any locality of the hash key. For example, clients from the same subnet (which are likely to share and collaborate on the same content) may be assigned two different hash numbers and may be redirected to different branch WAEs, while clients from different subnets may be assigned the same hash number and may be redirected to the same branch WAE. Hashing that is based on a client IP address does guarantee consistency. For example, a client using the same IP address is redirected to the same branch WAE.

In the service farm, a lead WAE is chosen to build the hash table that distributes the load between the available WAEs. The lead WAE distributes the buckets evenly. The source IP address is hashed and the resulting bucket determines the WAE that will handle the packet.

WCCP supports redirection by mask value assignments. This method relies on masking to make redirection decisions. The decisions are made using special hardware support in the WCCP-enabled router. This method can be very efficient because packets are switched by the hardware.

Note The masking method can only be used for load balancing with the Catalyst 3750, Catalyst 4500, and Catalyst 6500 Series Switches, Cisco 7600 Series Routers, and Cisco ASR 1000 Aggregation Series Routers. And, the masking method can be used with the Cisco 2800, 3800, and 7200 Series Routers when they are running Cisco IOS Release 12.4(20)T or later releases.

You must explicitly specify masking. You can specify two mask values based on the source or destination IP address of the packet. For Cisco WAAS, the default mask value is based on the source IP address. You can enable masks by using the default values or specifying a particular mask. The default mask values, specified in hexadecimal notation, are as follows:

- dst-ip-mask= 0x0
- src-ip-mask= 0xF00

You can specify the mask value with a maximum of seven bits. The WAE creates a table of the 27 (or 128) combinations, assigns the WAE IP addresses to them, and sends this table to a WCCP-enabled router. The router uses this table to distribute the traffic among all the WAEs that are in the service group. Each packet that matches the WCCP service parameters is compared to this table and the packets are sent to the matching WAE.

In a service farm where the WAEs have different masks, the first WAE to establish two-way communication with the routers determines the farm's mask. All the other WAEs cannot join the farm unless they are configured with the same mask.

Masking is typically used at the data center, where you can take advantage of the hardware-accelerated WCCP redirection capabilities of switches, such as the Catalyst 6500 Series Switches. At the data center, the load balancing goal should be to have all the connections originating from a given client subnet (typically equivalent to a branch) go to one data center WAE, in order to improve data redundancy elimination (DRE) compression performance. Also, mask assignment on the Catalyst 6500 series switches uses the ACL Ternary Content Adjustable Memory (TCAM). When combined with WCCP redirect lists, mask assignment can use a large portion of the TCAM. To minimize TCAM usage, use a mask with fewer care bits.

Given these considerations, beginning with Cisco WAAS Version 4.2.1, the default mask has been changed from src-ip-mask 0x1741 and dst-ip-mask 0x0 (in Cisco WAAS 4.1x versions) to src-ip-mask 0xF00 and dst-ip-mask 0x0 (in 4.2.1 and later versions). The current source IP mask uses only four care bits rather than the six care bits used by the old mask.

With a typical data center WCCP interception configuration (ingress interception with service 61 on the WAN, ingress interception with service 62 on the LAN), this mask load balances /24 branch subnets (it extracts the last 4 bits of /24 subnets). Connections from one branch subnet will be pinned to one data center WAE. If your network has a different distribution of IP addresses, for example, /16 subnets, you should configure a mask that extracts bits from the /16 network part of the address, for example, src-ip-mask 0xF0000. Similarly, if some branches generate more traffic than others, you may want to create a mask that also extracts bits from the host part of the address, for example, 0xF03.

About Packet-Forwarding Methods

A WCCP-enabled router redirects intercepted TCP segments to a WAE using one of the following two packet-forwarding methods:

- Generic routing encapsulation (GRE): Allows packets to reach the WAE, irrespective of the number of routers in the path to the WAE.

- Layer 2 redirection: Allows packets to be switched at Layer 2 (MAC layer) and reach the WAE.

The following table describes the packet-forwarding methods.

Table 8: Packet-Forwarding Methods

Packet-Forwarding Method	Load-Balancing Method: Hashing	Load-Balancing Method: Masking
GRE (Layer 3)	Packet redirection is completely handled by the router software.	Packet redirection is handled by the router software. We do not recommend the use of mask assignment when GRE is being used as the packet-forwarding method.
Layer 2 redirection	First redirected packet is handled by the router software; all subsequent redirected packets are handled by the router hardware.	All the packets are handled by the router hardware (currently supported only on the Catalyst 6500 Series Switches or Cisco 7600 Series Routers because special hardware is required).

The redirection mode is controlled by the branch WAE. The first branch WAE that joins the WCCP service group decides the forwarding method (GRE or Layer 2 redirection) and the assignment method (hashing or masking). The term *mask assignment* refers to WCCP Layer 2 Policy Feature Card 2 (PFC2) input redirection.

If masking is selected with WCCP output redirection, the branch WAE falls back to the original hardware acceleration that is used with the Multilayer Switch Feature Card (MSFC) and the Policy Feature Card (PFC).

For example, WCCP filters the packets to determine which redirected packets have been returned from the branch WAE and which ones have not. WCCP does not redirect the ones that have been returned because the branch WAE has determined that the packets should not be processed. WCCP Version 2 returns the packets that the branch WAE does not service to the same router from which they were transmitted.

This section contains the following topics:

Reasons for Packet Rejection and Return

A branch WAE rejects packets and initiates packet return for the following reasons:

- The WAE is filtering out certain conditions that make processing packets unproductive, for example, when IP authentication has been turned on.
- You have configured a static bypass list or interception ACL on the branch WAE.

Note The packets are redirected to the source of the connection between the WCCP-enabled router and the branch WAE. Depending on the Cisco IOS software version used, this source could be either the address of the outgoing interface or the router IP address. In the latter case, it is important that the branch WAE has the IP address of the WCCP-enabled router stored in the router list. For more information, see Configuring and Viewing WCCP Router Lists for WAEs, on page 153.

Cisco Express Forwarding (CEF) is required for WCCP and must be enabled on the router.

WCCP also allows you to configure multiple routers in a router list to support a particular WCCP service (for example, SMB redirection).

Layer 3 GRE as a Packet-Forwarding Method

A WCCP-enabled router redirects intercepted requests to a WAE, and can encapsulate packets using GRE. This method of forwarding packets allows packets to reach the WAE even if there are routers in the path to the WAE. Packet redirection is handled entirely by the router software.

GRE allows datagrams to be encapsulated into IP packets at the WCCP-enabled router and then redirected to a WAE (the transparent proxy server). At this intermediate destination, the datagrams are decapsulated and then handled by the WAAS software. If the request cannot be handled locally, the origin server may be contacted by the associated WAE to complete the request. In doing so, the trip to the origin server appears to the inner datagrams as one hop. The redirected traffic using GRE is usually referred to as GRE tunnel traffic. With GRE, all redirection is handled by the router software.

With WCCP redirection, a Cisco router does not forward the TCP SYN packet to the destination because the router has WCCP enabled on the destination port of the connection. Instead, the WCCP-enabled router encapsulates the packet using GRE tunneling and sends it to the WAE that has been configured to accept redirected packets from this WCCP-enabled router.

After receiving the redirected packet, the WAE performs the following tasks:

1. Strips the GRE layer from the packet.
2. Decides whether it should accept this redirected packet and process the request for content or deny the redirected packet as follows:
   - If the WAE decides to accept the request, it sends a TCP SYN ACK packet to the client. In this response packet, the WAE uses the IP address of the original destination (origin server) that was specified as the source address so that the WAE can be invisible (transparent) to the client; it pretends to be the destination that the TCP SYN packet from the client was trying to reach.
   - If the WAE decides not to accept the request, it re-encapsulates the TCP SYN packet in GRE, and sends it back to the WCCP-enabled router. The router understands that the WAE is not interested in this connection and forwards the packet to its original destination (that is, the origin server).

Layer 2 Redirection as a Packet-Forwarding Method

Layer 2 redirection is accomplished when a WCCP-enabled router or switch takes advantage of internal switching hardware that either partially or fully implements the WCCP traffic interception and redirection functions at Layer 2. This type of redirection is currently supported only with the Cisco Catalyst 6500 Series Switches and Cisco 7200 and 7600 Series Routers. With Layer 2 redirection, the first redirected traffic packet is handled by the router software. The rest of the traffic is handled by the router hardware. The branch WAE instructs the router or switch to apply a bit mask to certain packet fields, which in turn provides a mask result or index mapped to the branch WAE in the service group in the form of a mask index address table. The redirection process is accelerated in the switching hardware, making Layer 2 redirection more efficient than Layer 3 GRE.

Note WCCP is licensed only on the WAE and not on the redirecting router. WCCP does not interfere with normal router or switch operations.

Configuring or Viewing the WCCP Settings on WAEs

Before you begin

This section describes how to configure or view WCCP settings on WAEs that are configured as application accelerators and are not part of an AppNav Cluster (WAEs that are part of an AppNav Cluster use only the appnav-controller interception method). To configure or view the WCCP settings on WAEs configured as AppNav Controllers, see Configuring or Viewing the WCCP Settings on ANCs, on page 149.

Device group configuration is not possible beginning with Cisco WAAS version 5.0. However, you can use the **Copy Settings** taskbar icon in the configuration window to copy the settings to other devices in your network. To ensure consistency, we recommend that you copy the same WCCP settings to all devices in the same WCCP service farm.

Note Before you perform the procedure in this section, you should have already completed a basic WCCP configuration for your Cisco WAAS network that includes the configuration of the TCP promiscuous mode service, as described in the *Cisco Wide Area Application Services Quick Configuration Guide* .

Procedure

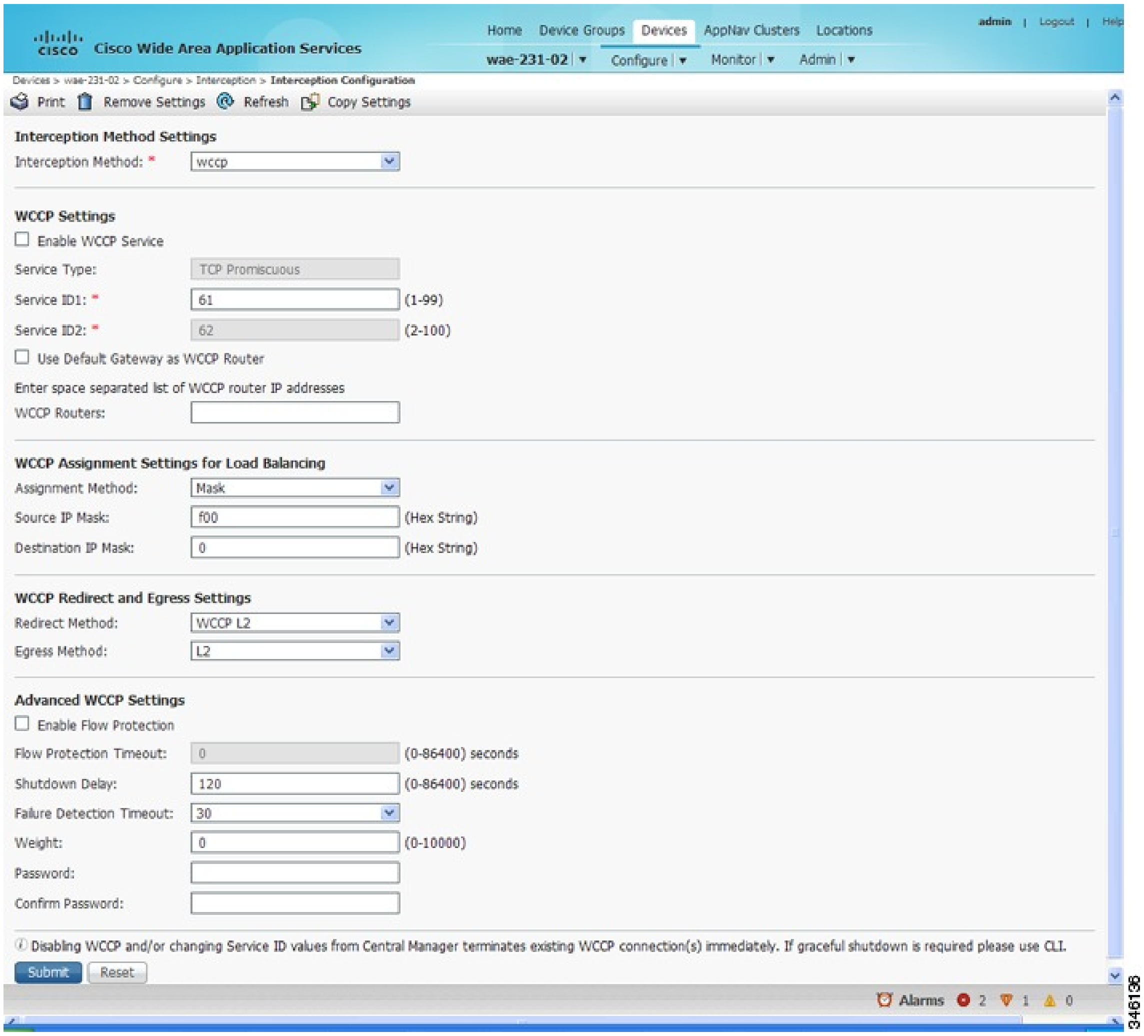
Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**.

The **Interception Configuration** window appears.

Note If you are configuring a device running a Cisco WAAS version earlier than Cisco WAAS Version 5.0, choose **Configure** > **Interception** > **WCCP** > **Settings** to configure WCCP settings. The **Configuration** window looks different, but has similar settings.

Figure 29: Interception Configuration Window for WAE



Interception Method Settings

Interception Method: * wccp

WCCP Settings

□ Enable WCCP Service

Service Type: TCP Promiscuous

Service ID1: * 61 (1-99)

Service ID2: * 62 (2-100)

□ Use Default Gateway as WCCP Router

Enter space separated list of WCCP router IP addresses

WCCP Routers:

WCCP Assignment Settings for Load Balancing

Assignment Method: Mask

Source IP Mask: f00 (Hex String)

Destination IP Mask: 0 (Hex String)

WCCP Redirect and Egress Settings

Redirect Method: WCCP L2

Egress Method: L2

Advanced WCCP Settings

□ Enable Flow Protection

Flow Protection Timeout: 0 (0-86400) seconds

Shutdown Delay: 120 (0-86400) seconds

Failure Detection Timeout: 30

Weight: 0 (0-10000)

Password:

Confirm Password:

Disabling WCCP and/or changing Service ID values from Central Manager terminates existing WCCP connection(s) immediately. If graceful shutdown is required please use CLI.

Step 3 Check the current settings for the chosen device:

- To keep the current settings and to close the window, click **Reset**.
- To remove the current settings, click the **Remove Settings** taskbar icon.
- To modify the current settings, change the current setting, as described in the rest of this procedure.
- To copy the settings to other WAEs in your network, click the **Copy Settings** taskbar icon.

  The **Copy Interception Settings** window opens, where you can select other WAEs to which the interception settings can be copied. You can copy all the settings or you can exclude the router list and enable the WCCP service.

Step 4 To copy the settings to the selected WAEs devices, click **OK**.

By default, WCCP is disabled on a WAE. However, as part of the initial configuration of WCCP in your Cisco WAAS network, you should have enabled WCCP Version 2 on your WAEs (the branch WAE and the data center WAE) as well as on the routers in the data center and branch office that will be transparently redirecting requests to these WAEs. For information about how to perform a basic WCCP configuration in your Cisco WAAS network, see the *Cisco Wide Area Application Services Quick Configuration Guide*.

Step 5 From the **Interception Method** drop-down list, choose **WCCP** to enable the WCCP interception method. If you change this setting from any setting other than None, click **Submit** to update the window with the proper fields for configuring WCCP. (The **Interception Method** drop-down list is not displayed for devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0.)

Step 6 Check the **Enable WCCP Service** check box to enable WCCP Version 2 on the chosen device, or uncheck the check box to disable WCCP on the chosen device.

Note Ensure that the routers used in the WCCP environment are running a version of the Cisco IOS software that also supports the WCCP Version 2.

Note If you use the Cisco WAAS Central Manager to disable WCCP on a WAAS device, the Cisco WAAS Central Manager immediately shuts down WCCP and closes any existing connections, ignoring the setting configured by the **wccp shutdown max-wait** global configuration command. To gracefully shut down WCCP connections, run the **no enable wccp** configuration command on the Cisco WAAS device.

Step 7 In the **Service ID1** field, specify the first service ID of the WCCP service pair. After you submit, the **Service ID2** field is filled in with the second service ID of the pair, which is one greater than Service ID1.

For WAEs with Cisco WAAS Version 4.4.1 or later, you can change the WCCP service IDs from the default of 61/62 to a different pair of numbers, which allows a router to support multiple WCCP farms because the WAEs in different farms can use different service IDs. (The Service ID fields are not shown for devices running Cisco WAAS versions earlier than Cisco WAAS Version 4.4 and the service IDs are fixed at 61/21.)

The router service priority varies inversely with the service ID. The service priority of the default service IDs 61/62 is 34. If you specify a lower service ID, the service priority is higher than 34; if you specify a higher service ID, the service priority is lower than 34.

Step 8 Check the **Use Default Gateway as WCCP Router** check box to use the default gateway of the WAE device as the router to associate with the WCCP TCP promiscuous mode service.

- Alternatively, uncheck this check box and specify a list of one or more routers by their IP addresses, separated by spaces.

  The Cisco WAAS Central Manager assigns the router list number, which is displayed next to the router list field after the page is submitted. As part of the initial configuration of your Cisco WAAS network, you may have already created a WCCP router list with the setup utility, as described in the *Cisco Wide Area Application Services Quick Configuration Guide* . For more information about WCCP router lists, see Configuring and Viewing WCCP Router Lists for WAEs, on page 153.

Note Checking or unchecking the Use Default Gateway as WCCP Router check box, changing the router list, or submitting the WCCP page removes existing router lists, if any, that are not assigned to the WCCP service, including router lists configured by the setup utility or through the CLI.

Step 9 (Optional) To force WCCP to use only the configured assignment method, check the **Only Use Selected Assignment Method** check box. You can specify only one load-balancing method (hashing or masking) per WCCP service in a branch WAE service group. (This check box is shown only for devices using Cisco WAAS versions earlier than Cisco WAAS Version 4.4.)

Note If you check the **Only Use Selected Assignment Method** check box, the WAE only joins a WCCP farm if the assignment method configured on the WAE is supported by the router. If you do not check the Only Use Selected Assignment Method check box, the WAE uses the assignment method that the router supports, even if the WAE is configured differently from the router.

Step 10 (Optional) From the **Assignment Method** drop-down list, choose the type of WAE load-balancing assignment method to use:

- Choose **Hash** to use the hash method (the default for devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0). Perform Step 10 and Step 11 to define how the hash works, and skip to Step 13 because the mask settings are not used.
- Choose **Mask** to use the mask method (the default for devices using Cisco WAAS Version 5.0 or later). Skip to Step 12 to define the service mask.

For more information, see About Load Balancing and Cisco WAEs.

Step 11 (Optional) To define the load-balancing hash for WCCP service ID1 on the source IP address, check the **Hash on Source IP** check box. This check box is shown only if the hash assignment method is used.

Step 12 (Optional) To define the load-balancing hash for WCCP service ID1 on the destination IP address, check the **Hash on Destination IP** check box. This check box is shown only if the hash assignment method is used.

Step 13 (Optional) To use a custom service mask, enter different mask values in the **WCCP Assignment Settings for Load Balancing** pane, overwriting the default mask settings. If you do not change these settings, the defaults are used. Define the custom mask as follows:

- In the **Source IP Mask** field, specify the IP address mask defined by a hexadecimal number, for example, FE000000, used to match the packet source IP address. The range is **00000000** to **FE000000**. The default is **F00**.
- In the **Destination IP Mask** field, specify the IP address mask defined by a hexadecimal number, for example, FE000000, used to match the packet destination IP address. The range is **0000000** to **FE000000**. The default is **0**.

Note If you apply the default mask to a WAE running Cisco WAAS Version 4.1.x or earlier, the mask is different from the default mask (0x1741) set under WAAS Version 4.1.x and earlier.

If the WAE detects that its configured mask is not the same as that advertised by one or more routers in the farm, it is not allowed to join the farm, and a major alarm is raised (**Configured mask mismatch for WCCP**). This alarm can occur when a WAE is trying to join a farm that already has other WAEs, and these other WAEs are configured with a different mask. The routers do not allow other WAEs to join the farm unless they advertise the same mask. To correct this alarm, ensure that all the WAEs in the farm are configured with the same mask. This alarm is cleared when the WAE's configured mask matches the mask of all the routers in the farm.

Step 14 From the **Redirect Method** drop-down list, choose the type of packet redirection (forwarding) method to use:

- **WCCP GRE** (the default for devices using WAAS versions earlier than 5.0) to use Layer 3 GRE packet redirection.
- **WCCP L2** (the default for devices using WAAS versions 5.0 or later) to permit the WAE to receive transparently redirected traffic from a WCCP Version 2-enabled switch or router if the WAE has a Layer 2 connection with the device and the device is configured for Layer 2 redirection. For more information, see About Packet-Forwarding Methods.

Note Do not use WCCP L2 redirection on an ISR-WAAS device when ip unnumbered is configured on the host router VirtualPortGroup interface. The device will not be able to join the WCCP farm and the missing_assignment alarm will be raised.

Step 15 From the **Return Method** drop-down list, choose the type of method to use to return nonoptimized (bypassed) packets to the router:

- **WCCP GRE** (the default) to use GRE packet return.
- **WCCP L2** to use Layer 2 rewriting for packet return.

The **Return Method** drop-down list is shown only for devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0.

- For Cisco WAAS Version 5.1, the return method is set the same as the redirect method.
- For Cisco WAAS Version 5.2 and later, the return method is automatically negotiated with router to the same as the redirect method if the router supports it.
- If the router does not support the return method that matches the redirect method, then the return method is set to the return method supported by the router. For example, if the redirect method is set to WCCP L2, but the router supports only the GRE return method, then the return method is set to WCCP GRE.

Step 16 (Optional) From the **Egress Method** drop-down list, choose the method to use to return optimized packets to the router or switch:

- **Generic GRE** (available and set as the default only if Redirect Method is WCCP GRE)
- **IP Forwarding**
- **L2** (available and set as the default only if Redirect Method is WCCP L2)
- **WCCP GRE** (available only if Redirect Method is WCCP GRE)

For devices using Cisco WAAS versions earlier than Cisco WAAS Versoin 5.0, the choices are as follows: **IP Forwarding** (the default), **WCCP Negotiated Return**, or **Generic GRE**. For more information, see Configuring Egress Methods for WCCP-Intercepted Connections, on page 157.

Step 17 (Optional) Modify the current advanced settings in the **Advanced WCCP Settings** pane as follows:

- Check the **Enable Flow Protection** check box to keep the TCP flow intact and to avoid overwhelming the device when it comes up or is reassigned new traffic. Flow protection is disabled by default.
- In the **Flow Protection Timeout** field, specify the amount of time (in seconds) that flow protection should be enabled. The default is 0, which means it stays enabled with no timeout. (The **Flow Protection Timeout** field is not shown for devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0.)

Note The **Enable Flow Protection** check box and the **Flow Protection Timeout** field are not enabled on Cisco WAAS Version 6.0.1.

- In the **Shutdown Delay** field, specify the maximum amount of time (in seconds) that the chosen device waits to perform a clean shutdown of WCCP. The default is 120 seconds.

The WAE does not reboot until either all connections have been serviced or the maximum wait time (specified through this **Shutdown Delay** field) has elapsed for WCCP.

- From the **Failure Detection Timeout** drop-down list, choose the failure detection timeout value (9, 15, or 30 seconds). The default is 30 seconds and is the only value supported on WAAS versions prior to 4.4.1. This failure detection value determines how long it takes the router to detect a WAE failure. (The Failure Detection Timeout field is not shown for devices using WAAS versions earlier than 4.4.)

The failure detection timeout value is negotiated with the router and takes effect only if the router also has the variable timeout capability. If the router has a fixed timeout of 30 seconds and you have configured a failure detection value on the WAE other than the default 30 seconds, the WAE is not able to join the farm and an alarm is raised (**Router unusable** with a reason of **Timer interval mismatch with router**).

- In the **Weight** field, specify the weight value that is used for load balancing. The weight value ranges from 0 to 10000. If the total of all the weight values of the WAEs in a service group is less than or equal to 100, then the weight value represents a literal percentage of the total load redirected to the device for load-balancing purposes. For example, a WAE with a weight of 10 receives 10 percent of the total load in a service group where the total of all the weight values is 50. If a WAE in such a service group fails, the other WAEs still receive the same load percentages as before the failure; they will not receive the load allocated to the failed WAE.

If the total of all the weight values of the WAEs in a service group is between 101 and 10000, then the weight value is treated as a fraction of the total weight of all the active WAEs in the service group. For example, a WAE with a weight of 200 receives 25 percent of the total load in a service group where the total of all the weight values is 800. If a WAE in such a service group fails, the other WAEs will receive the load previously allocated to the failed WAE. The failover handling is different than if the total weights are less than or equal to 100.

By default, weights are not assigned and the traffic load is distributed evenly between the WAEs in a service group.

- In the **Password** field:
    - Specify the password to be used for secure traffic between the WAEs within a cluster and the router for a specified service.

      Passwords must not exceed eight characters in length. Do not use the following characters: space, backwards single quote ('), double quote ("), pipe (|), or question mark (?). – Be sure to enable all other WAEs and routers within the cluster with the same password.

      Be sure to enable all other WAEs and routers within the cluster with the same password.

    - Re-enter the password in the **Confirm Password** field.

Note For information about how to use the CLI to specify the service group password on a router, see Setting a Service Group Password on a Router, on page 136.

Step 18 To save the settings, click **Submit**.

To configure WCCP settings from the Cisco WAAS CLI, you must first set the interception method to WCCP by running the **interception-method** global configuration command, after which you can run the **wccp router-list**, **wccp shutdown**, and **wccp tcp-promiscuous** global configuration commands.

For more information, see Configuring WAEs for a Graceful Shutdown of WCCP, on page 153.

Configuring or Viewing the WCCP Settings on ANCs

Before you begin

This section describes how to configure or view WCCP settings on WAAS devices configured as AppNav Controllers (ANCs). Typically, you configure ANCs and their settings through the AppNav Clusters window in the Central Manager, which includes WCCP settings. Therefore, you do not have to configure the WCCP settings outside the AppNav Cluster context, as described in this section.

To configure or view the WCCP settings on WAEs configured as application accelerators, see Configuring or Viewing the WCCP Settings on WAEs, on page 143. To configure interception settings on WAEs operating as WAAS nodes for an AppNav Controller, see Configuring AppNav Interception, on page 185.

Device group configuration is not possible beginning with Cisco WAAS Version 5.0. However, you can use the **Copy Settings** taskbar icon in the **Interception Configuration** window to copy the settings to other devices in your network. To ensure consistency, we recommend that you copy the same WCCP settings to all the devices in the same WCCP service farm.

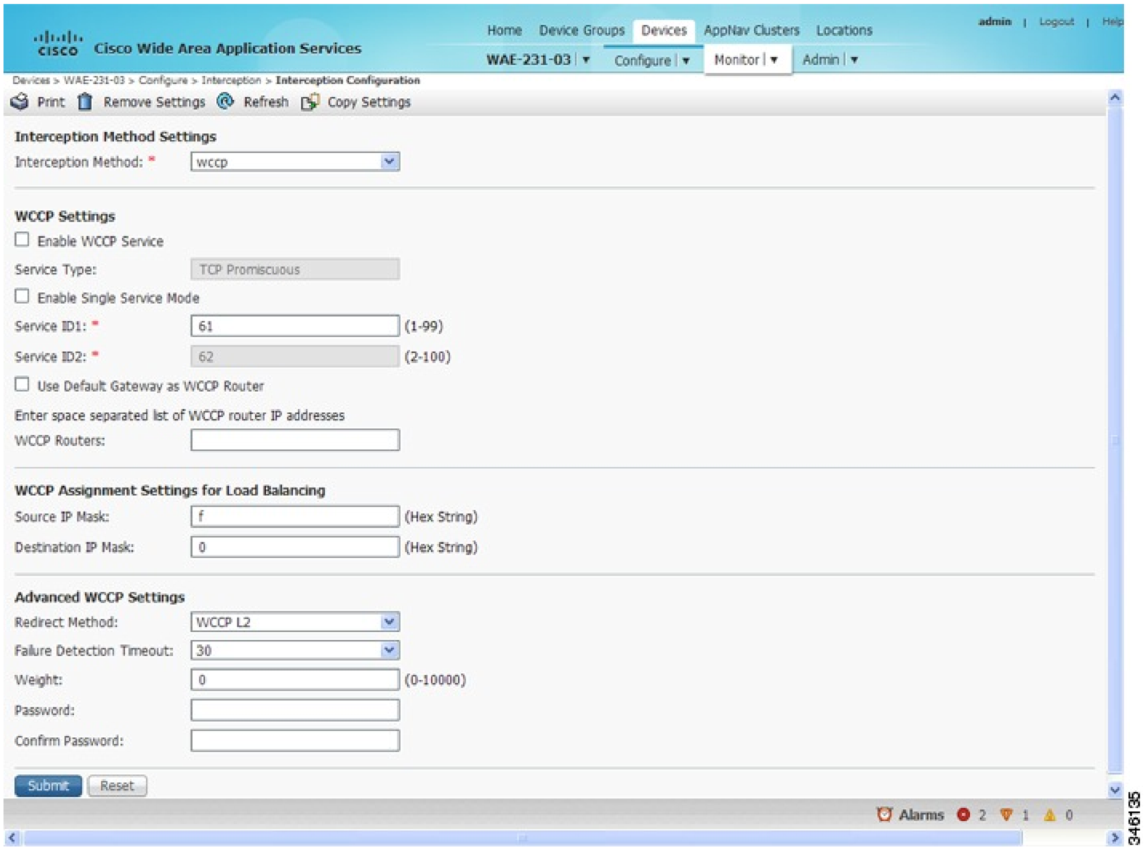
Procedure

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

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**.

The **Interception Configuration** window appears.

Figure 30: Interception Configuration Window for ANC


Cisco Wide Area Application Services
Home | Device Groups | Devices | AppNav Clusters | Locations
admin | Logout | Help
WAE-231-03 | Configure | Monitor | Admin
Devices > WAE-231-03 > Configure > Interception > Interception Configuration
Print | Remove Settings | Refresh | Copy Settings
Submit | Reset
Alarms 2 1 0
346135

Interception Method Settings

Interception Method: * wccp

WCCP Settings

□ Enable WCCP Service

Service Type: TCP Promiscuous

□ Enable Single Service Mode

Service ID1: * 61 (1-99)

Service ID2: * 62 (2-100)

□ Use Default Gateway as WCCP Router

Enter space separated list of WCCP router IP addresses

WCCP Routers:

WCCP Assignment Settings for Load Balancing

Source IP Mask: f (Hex String)

Destination IP Mask: 0 (Hex String)

Advanced WCCP Settings

Redirect Method: WCCP L2

Failure Detection Timeout: 30

Weight: 0 (0-10000)

Password:

Confirm Password:

Step 3 Check the current settings for the chosen device:

- To keep the current settings and to close the window, click **Reset**.
- To remove the current settings, click the **Remove Settings** taskbar icon.
- To modify the current settings, change the current setting, as described in the rest of this procedure.
- To copy the settings to other WAEs in your network, click the **Copy Settings** taskbar icon.

  The **Copy Interception Settings** window opens, where you can select other WAEs to which the interception settings can be copied. You can copy all the settings or you can exclude the router list and enable the WCCP service.

  To copy the settings to the selected WAEs, click **OK**.

By default, WCCP is disabled on a WAE. However, as part of the initial configuration of WCCP in your Cisco WAAS network, you should have enabled WCCP Version 2 on your WAEs (the branch WAE and the data center WAE) as well as on the routers in the data center and branch office that will be transparently redirecting requests to these WAEs. For information about how to perform a basic WCCP configuration in your Cisco WAAS network, see the *Cisco Wide Area Application Services Quick Configuration Guide*.

Step 4 From the **Interception Method** drop-down list, choose **wccp** to enable the WCCP interception method. If you change this setting from any setting other than None, click **Submit** to update the window with the proper fields for configuring WCCP.

Step 5 Check the **Enable WCCP Service** check box to enable WCCP Version 2 on the chosen device, or uncheck the check box to disable WCCP on the chosen device.

Note Ensure that the routers used in the WCCP environment are running a version of the Cisco IOS software that also supports WCCP Version 2.

Note If you use the Cisco WAAS Central Manager to disable WCCP on a Cisco WAAS device, the Central Manager immediately shuts down WCCP and closes existing connections, if any, ignoring the setting configured by the **wccp shutdown max-wait** global configuration command. To gracefully shut down WCCP connections, run the **no enable wccp** configuration command on the Cisco WAAS device.

Step 6 (Optional) Enable single service mode by checking the **Enable Single Service Mode** check box (the default). Single service mode simplifies configuration by using the same service ID for incoming and outgoing traffic, which is possible only with an AppNav deployment because it can handle asymmetric traffic flows.

Step 7 In the **Service ID1** field, specify the service ID of the WCCP service.

If the **Enable Single Service Mode** check box is unchecked, a pair of WCCP service IDs are required, and the **Service ID2** field is filled in with the second service ID of the pair, which is one greater than **Service ID1**. The default service IDs are **61** and **62**. You can change the WCCP service IDs from the default of **61** and **62** to a different pair of numbers, which allows a router to support multiple WCCP farms because the ANCs in different farms can use different service IDs.

The router service priority varies inversely with the service ID. The service priority of the default service IDs 61 and 62 is **34**. If you specify a lower service ID, the service priority is higher than 34; if you specify a higher service ID, the service priority is lower than 34.

Step 8 Check the **Use Default Gateway as WCCP Router** check box to use the default gateway of the WAE device as the router to associate with the WCCP TCP promiscuous mode service. Alternatively, you can uncheck this check box and specify a list of one more routers by their IP addresses, separated by spaces. The Cisco WAAS Central Manager assigns the router list number, which is displayed next to the router list field after the page is submitted. As part of the initial configuration of your Cisco WAAS network, you may have already created a WCCP router list with the setup utility, as described in the *Cisco Wide Area Application Services Quick Configuration Guide* . For more information about WCCP router lists, see Configuring and Viewing WCCP Router Lists for WAEs, on page 153.

Note Checking or unchecking the **Use Default Gateway as WCCP Router** check box, changing the router list, or submitting the WCCP page removes existing router lists, if any, that are not assigned to the WCCP service, including router lists configured by the setup utility or through the CLI.

Step 9 (Optional) To use a custom service mask, enter different mask values in the WCCP Assignment **Settings for Load Balancing** pane, overwriting the default mask settings. If you do not change these settings, the defaults are used. Define the custom mask as follows:

- In the **Source IP Mask** field, specify the IP address mask defined by a hexadecimal number, for example, FE000000, used to match the packet source IP address. The range is **00000000** to **FE000000**. The default is **F**.

- In the **Destination IP Mask** field, specify the IP address mask defined by a hexadecimal number, for example, FE000000, used to match the packet destination IP address. The range is **0000000** to **FE000000**. The default is **0**.

For more information, see About Load Balancing and Cisco WAEs, on page 138.

If the WAE detects that its configured mask is not the same as advertised by one or more routers in the farm, it is not allowed to join the farm and a major alarm is raised (**Configured mask mismatch for WCCP**). This alarm can occur when a WAE is trying to join a farm that already has other WAEs, and these other WAEs are configured with a different mask. The routers do not allow other WAEs to join the farm unless they advertise the same mask. To correct this alarm, ensure that all the WAEs in the farm are configured with the same mask. This alarm is cleared when the WAE's configured mask matches the mask of all the routers in the farm.

Step 10 (Optional) Modify the current advanced settings in the **Advanced WCCP Settings** pane as follows:

a) From the **Redirect Method** drop-down list, choose the type of packet redirection (forwarding) method to use:

- **WCCP GRE** to use Layer 3 GRE packet redirection.
- **WCCP L2** (the default) to permit the WAE to receive transparently redirected traffic from a WCCP Version 2-enabled switch or router if the WAE has a Layer 2 connection with the device and the device is configured for Layer 2 redirection. For more information, see About Packet-Forwarding Methods, on page 140.

The return method is set the same as the redirect method. The return method is generic GRE when the WCCP GRE redirect method is chosen or WCCP L2 return when the WCCP L2 redirect method is chosen.

b) In the **Failure Detection Timeout** drop-down list, choose the failure detection timeout value (**3**, **6**, **9**, **15**, or **30 seconds**). The default is **30 seconds** and is the only value supported on Cisco WAAS versions earlier than Cisco WAAS Version 4.4.1. This failure detection value determines how long it takes the router to detect a WAE failure.

The failure detection timeout value is negotiated with the router and takes effect only if the router also has the variable timeout capability. If the router has a fixed timeout of 30 seconds and you have configured a failure detection value on the WAE other than the default 30 seconds, the WAE is not able to join the farm and an alarm is raised (**Router unusable** with a reason of **Timer interval mismatch with router**).

c) In the **Weight** field, specify the weight value that is used for load balancing. The weight value ranges from 0 to 10000. If the total of all the weight values of the WAEs in a service group is less than or equal to 100, then the weight value represents a literal percentage of the total load redirected to the device for load-balancing purposes. For example, a WAE with a weight of 10 receives 10 percent of the total load in a service group where the total of all weight values is 50. If a WAE in such a service group fails, the other WAEs still receive the same load percentages as before the failure; they will not receive the load allocated to the failed WAE.

If the total of all the weight values of the WAEs in a service group is between **101** and **10000**, then the weight value is treated as a fraction of the total weight of all the active WAEs in the service group. For example, a WAE with a weight of 200 receives 25 percent of the total load in a service group where the total of all the weight values is 800. If a WAE in such a service group fails, the other WAEs will receive the load previously allocated to the failed WAE. The failover handling is different than if the total weights are less than or equal to 100.

By default, weights are not assigned and the traffic load is distributed evenly between the WAEs in a service group.

d) In the **Password** field, specify the password to be used for secure traffic between the WAEs within a cluster and the router for a specified service. Be sure to enable all the other WAEs and routers within the cluster with the same password. Passwords must not exceed eight characters in length. Do not use the following characters: space, backwards single quote ('), double quote ("), pipe (|), or question mark (?). Re-enter the password in the **Confirm Password** field.

Note For information about how to use the CLI to specify the service group password on a router, see Setting a Service Group Password on a Router, on page 136.

Step 11 To save the settings, click **Submit**.

To configure WCCP settings from the Cisco WAAS CLI, you must first set the interception method to WCCP by running the **interception-method** global configuration command, and then you can run the **wccp router-list** and **wccp tcp-promiscuous** global configuration commands.

Configuring and Viewing WCCP Router Lists for WAEs

You can configure and view one router list from the Central Manager through the WCCP settings (see Configuring or Viewing the WCCP Settings on WAEs, on page 143). The Central Manager supports only a single router list assigned to the WCCP service and removes existing router lists, if any, that can be configured through the CLI if you use the Central Manager to configure a router list, check or uncheck the Use Default Gateway check box in the WCCP settings page, or submit the WCCP settings page. To configure a router list through the CLI, use the **wccp router-list** global configuration command.

Note WCCP must be enabled before you can use the WCCP global configuration commands.

To delete a router list, use the **no wccp router-list** global configuration command.

To view an unassigned router list configured by the **wccp router-list** command, use the **show running-config wccp** EXEC command.

Configuring WAEs for a Graceful Shutdown of WCCP

To prevent broken TCP connections, the WAE performs a clean shutdown of WCCP after you disable WCCP Version 2 on a WAE, or reload the WAE from the CLI. You can perform this task locally through the CLI on a device by running the **no enable wccp** configuration command.

The Cisco WAAS Central Manager also allows you to disable WCCP Version 2 on a WAE, but this does not perform a graceful shutdown of WCCP connections. To disable WCCP immediately for a chosen device, uncheck the Enable WCCP check box in the WAAS Central Manager Interception Configuration window.

Note If you use the Cisco WAAS Central Manager to disable WCCP on a WAAS device, the Cisco WAAS Central Manager immediately shuts down WCCP and closes existing connections, if any, ignoring the setting configured by the **wccp shutdown max-wait** global configuration command. To gracefully shut down WCCP connections, run the **no enable wccp** configuration command on the Cisco WAAS device.

During a graceful shutdown, the WAE does not reboot until one of the following occurs:

- All the connections have been serviced.
- The maximum wait time (specified in the **Shutdown Delay** field in the WCCP Configuration Settings window, or with the **wccp shutdown max-wait** command [by default, 120 seconds]) has elapsed for WCCP Version 2.

During a clean shutdown of WCCP, the WAE continues to service the flows that it is handling, but it starts to bypass new flows. When the number of flows goes down to zero, the WAE takes itself out of the group by having its buckets reassigned to other WAEs by the lead WAE. TCP connections can still be broken if the WAE crashes or is rebooted without WCCP being cleanly shut down.

You cannot shut down an individual WCCP service on a particular port on a WAE; you must shut down WCCP on the WAE. After WCCP is shut down on the WAE, the WAE preserves its WCCP configuration settings.

Configuring Static Bypass Lists for WAEs

Before you begin

Consider the following guidelines for configuring static bypass lists:

- Static bypass lists are supported only for devices (but not device groups) using Cisco WAAS versions earlier than Cisco WAAS Version 5.0, and are deprecated for such devices. Interception ACLs are recommended instead.
- Using a static bypass allows traffic flows between a configurable set of clients and servers to bypass handling by the WAE. By configuring static bypass entries on the branch WAE, you can control traffic interception without modifying the router configuration.

  IP access lists can be configured separately on the router to bypass traffic without first redirecting it to the branch WAE. Typically, the WCCP accept list defines the group of servers that are accelerated (and the servers that are not).

  Static bypass can be used occasionally when you want to prevent Cisco WAAS from accelerating a connection from a specific client to a specific server (or from a specific client to all servers).
-
- We recommend that you use ACLs on the WCCP-enabled router where possible, rather than using static bypass lists or interception ACLs on the WAEs, because that is the most efficient method to control traffic interception.

  If you decide to use static bypass lists or interception ACLs, we recommend that you use interception ACLs because they are more flexible and give better statistics about passed-through connections. For information about how to configure ACLs on a router, see Configuring IP Access Lists on a Router , on page 135. For information about how to configure an interception ACL for a WAE, see Configuring Interception Access Control Lists, on page 155.

Procedure

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

Step 2 Choose **Configure** > **Interception** > **Bypass Lists**.

Step 3 In the taskbar, click the **Create New WCCP/Inline Bypass List** icon. The **Creating new WCCP/Inline Bypass List** window appears.

Step 4 In the **Client Address** field, enter the IP address for the client.

Step 5 In the **Server Address** field, enter the IP address for the server.

Step 6 Check **Submit** to save the settings.

To configure a static bypass list from the Cisco WAAS CLI, run the **bypass static** global configuration command.

Configuring Interception Access Control Lists

Before you begin

You can configure an interception ACL to control what incoming traffic across all interfaces is to be intercepted by an ANC or WAE device (on an ANC, the interception ACL is called an AppNav Controller interception ACL). Packets that are permitted by the ACL are intercepted by the device, and packets that are denied by the ACL are passed through without processing.

Cisco WAAS allows or denies optimization based on how the interception ACL processes a TCP SYN packet at the start of a TCP connection, and allows or denies optimization based on the SYN packet matching or not matching a permit statement in the ACL.

- You do not need to configure a **symmetric ACL entry** to allow a connection to be optimized when the SYN packet is matching.
- You do need to configure the **symmetric ACL entry** if you want to allow optimization for a connection established in the opposite direction (**from server to client**).

The following is an example of how the **ip access-list** global configuration command marks connections for optimization:

```
WAE(config)# ip access-list extended optimized_traffic permit ip host 1.1.1.1 host 2.2.2.2
WAE(config)# interception access-list optimized_traffic
```

- In this example, if a SYN packet with **source IP 1.1.1.1** and **destination IP 2.2.2.2** hits the Cisco WAAS device, the Cisco WAAS device would mark the connection for optimization.
- In this example, if a SYN packet with **source IP 2.2.2.2** and **destination IP 1.1.1.1** hits the Cisco WAAS device, the connection will be put in **PT Interception ACL**. If you want both types of connections to be optimized, add **permit IP host 2.2.2.2 host 1.1.1.1** to the access list.

Note If Interception ACLs are applied to peer Cisco WAAS devices, the ACL entries must be specular on the two devices to allow a connection to be marked for optimization on both sides.

By configuring an interception ACL on a Cisco WAAS device, you can control traffic interception without modifying the router configuration. IP ACLs can be configured separately on the router to bypass traffic without first redirecting it to the Cisco WAAS device. Typically, the WCCP accept list defines the group of servers that are accelerated (and the servers that are not). Using an interception ACL allows you to easily bypass uninteresting traffic, for example, in a pilot deployment where you do not want to modify the router configuration. Additionally, it allows you to more easily transition from a pilot to a production deployment by allowing and accelerating different kinds of traffic in phases.

An interception ACL can be used both with WCCP and inline interception.

When used with interface ACLs and WCCP ACLs, the interface ACL is applied first, the WCCP ACL is applied second, and then the interception ACL is applied last. Application policies defined on the Cisco WAE are applied after all ACLs have filtered the traffic.

An ANC that is also operating as a WAAS node can have both an AppNav Controller interception ACL to control what is intercepted by the ANC and an interception ACL to control what is accepted by the optimizing engine. A flow may be permitted by the AppNav Controller interception ACL, but subsequently rejected by the WAAS node interception ACL.

Note The interception ACL feature is mutually exclusive with static bypass lists. You cannot use both types of lists at the same time. We recommend that you use interception ACLs instead of static bypass lists. Static bypass lists are supported only for devices using a Cisco WAAS version earlier than 5.0.

To use an interception ACL, first define an ACL (for more information, see the chapter Creating and Managing IP Access Control Lists for WAAS Devices, on page 277) and then apply it to a device. Interception ACLs are configured only for individual devices and not for device groups.

Procedure

Step 1 Follow the instructions in the chapter Creating and Managing IP Access Control Lists for WAAS Devices, on page 277 to create an ACL that you want to use for interception, but do not apply it to an interface.

Step 2 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.

Step 3 Choose **Configure** > **Interception** > **Interception Access List**.

Step 4 To configure a WAE interception ACL, click the arrow next to the Interception Access List field to display a drop-down list of ACLs you have defined, and choose an ACL to apply to WAE interception. Alternatively, you can enter an ACL name directly in the field and create it after you submit this page. If you enter information, drop-down list of displayed ACLs is filtered to show only the entries that match the beginning of the entered text.

To create or edit an ACL, click the **Go to IP ACL** link next to the field to take you to the IP ACL configuration window (**Configure** > **Network** > **TCP/IP Settings** > **IP ACL**).

Step 5 To configure an ANC interception ACL, click the arrow next to the **AppNav Controller Interception Access List** field to display a drop-down list of ACLs you have defined and choose an ACL to apply to ANC interception. Alternatively, you can enter an ACL name directly in the field and create it after you submit this page. If you enter information, drop-down list of displayed ACLs is filtered to show only entries that match the beginning of the entered text. This field is displayed only on devices configured in appnav-controller mode.

To create or edit an ACL, click the **Go to IP ACL** link to take you to the IP ACL configuration window (**Configure** > **Network** > **TCP/IP Settings** > **IP ACL**).

Step 6 To save the settings, click **Submit**.

Note In AppNav Controller interception ACLs, the **TCP … established** extended ACL condition is not supported and is ignored if encountered.

Step 7 (Optional) To configure an interception ACL from the CLI, run the **ip access-list** and **interception access-list** global configuration commands. To configure an AppNav Controller interception ACL, run the **interception appnav-controller access-list** global configuration command.

To verify that a connection was passed through by an interception ACL, run the **show statistics connection** EXEC command. Flows passed through by an interception ACL are identified with the connection type PT Interception ACL.

Additionally, the **show statistics pass-through** command **Interception ACL** counter reports the number of active and completed pass-through flows due to an interception ACL.

To view the individual ACL rules that are being matched, run the **show ip access-list** command.

Configuring Egress Methods for WCCP-Intercepted Connections

This section contains the following topics:

- About Egress Methods, on page 157
- Configuring the Egress Method, on page 159
- Configuring a GRE Tunnel Interface on a Router, on page 159

About Egress Methods

The following list describes types of egress methods, the Layer 2 egress method, the

Types of egress methods supported by Cisco WAAS for WCCP-intercepted connections:

- IP forwarding
- WCCP GRE return (available only if the redirect method is WCCP GRE; called WCCP-negotiated return for devices earlier than Version 5.0)
- Generic GRE (available only if the redirect method is WCCP GRE)
- Layer 2 (available only if the redirect method is WCCP L2)

Note For ANCs, the egress method is not configurable. The egress method that is used depends on the redirect method. The ANC uses generic GRE when the WCCP GRE redirect method is chosen, or Layer 2 when the WCCP L2 redirect method is chosen.

Layer 2 Egress Method:

For devices running Cisco WAAS Version 5.0 and later, the default egress method is L2. This egress method sends out optimized data through a Layer 2 connection to the router. This method is available only if the redirect method is also set to WCCP L2, and is not available on devices running a Cisco WAAS version earlier than Cisco WAAS Version 5.0. The router must also support Layer 2 redirect. If you configure the WCCP GRE redirect method or switch between WCCP GRE and L2, the default egress method is set to IP Forwarding.

IP Forwarding Egress Method:

For devices with a Cisco WAAS version earlier than Cisco WAAS Version 5.0, the default egress method is IP forwarding. The IP forwarding egress method does not allow you to place WAEs on the same VLAN or subnet as the clients and servers, and it does not ensure that packets are returned to the intercepting router.

WCCP GRE Return and Generic GRE Egress Methods:

The WCCP GRE Return and Generic GRE egress methods allow you to place WAEs on the same VLAN or subnet as clients and servers.

Consider the following guidelines for Cisco WAAS versions and the WCCP GRE Return and Generic GRE egress methods:

- For devices with a Cisco WAAS version earlier than Cisco WAAS Version 5.0, WCCP Version 2 is capable of negotiating the redirect method and the return method for intercepted connections. The WAAS software supports WCCP GRE and WCCP Layer 2 as WCCP-negotiated return methods. If WCCP negotiates a WCCP Layer 2 return, the WAE defaults to using IP forwarding as the egress method.

  The WAE also defaults to IP forwarding if the interception method is set to WCCP Layer 2 and you configure generic GRE as the egress method, both of which are not compatible. When the WAE defaults to IP forwarding, the WAE logs a minor alarm that is cleared when you correct the configuration so that the interception and egress methods are consistent. The output of the show egress methods EXEC command also displays a warning if the interception and egress methods are not consistent.

- For devices with Cisco WAAS Version 5.0, you must explicitly configure the egress method.

- Repeating redirection is prevented by encapsulating the outgoing frames in the GRE frames. Routers using Cisco IOS software handle these GRE frames as bypass frames, and do not apply WCCP redirection. With the WCCP GRE return method, Cisco WAAS uses the router ID address as the destination for GRE frames; with the generic GRE method, Cisco WAAS uses the address of the router configured in the WAE router list.

  This technique makes it possible to support redundant routers and router load balancing; Cisco WAAS makes a best effort to return frames back to the router from which they arrived, though this is not guaranteed.

  To use this functionality with multiple routers connected to the Cisco WAAS network segment, ensure connectivity to the router ID address, for example, by configuring static routes. The router ID is the address of the first loopback interface or highest active physical interface. This address can be found in the output of the show wccp routers EXEC command.

- Cisco WAAS applies the following logic in its router selection for WCCP GRE and generic GRE:

  - When the Cisco WAAS software applies data redundancy elimination (DRE) and compression to a TCP flow, the number of packets that are sent out may be fewer. A single packet that carries optimized data may represent original data that was received in multiple packets redirected from different routers. That optimized data-carrying packet will egress from the WAE to the router that last redirected a packet to the WAE for that flow direction.

  - When the WAE receives optimized data, the data may arrive in multiple packets from different routers. The Cisco WAAS software expands the optimized data back to the original data, which will be sent out as several packets. Those original data-carrying packets will egress from the WAE to the router that last redirected a packet to the WAE for that flow direction.

  - The WCCP GRE return and generic GRE egress methods are similar, but the generic GRE egress method is designed specifically to be used in deployments where the router or switch performs hardware-accelerated processing of GRE packets, such as with a Cisco 7600 Series router or a Catalyst 6500 Series switch with the Supervisor Engine 32 or 720. Additionally, the generic GRE egress method returns packets to the intercepting router by using a GRE tunnel that you must configure on the router (the WAE end of the tunnel is configured automatically). The generic GRE egress method is supported only when the WCCP GRE interception method is used.

- To use the generic GRE egress method, you must create an intercepting router list on the WAE (multicast addresses are not supported) and configure a GRE tunnel interface on each router. For details on configuring GRE tunnel interfaces on the routers, see Configuring a GRE Tunnel Interface on a Router.

Configuring the Egress Method

To configure the egress method for WCCP-intercepted connections from the Central Manager, see Configuring or Viewing the WCCP Settings on WAEs, on page 143.

To configure the egress method for WCCP GRE packet return from the CLI, use the **egress-method** WCCP configuration command:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# egress-method wccp-gre
```

To configure the egress method for L2 return from the CLI, use the **egress-method** WCCP configuration command:

```
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# egress-method L2
```

To configure the generic GRE egress method from the CLI, configure an intercepting router list and configure the egress method, as follows:

```
WAE(config)# wccp router-list 1 192.168.68.98
WAE(config)# wccp tcp-promiscuous service-pair 61 62
WAE(config-wccp-service)# router-list-num 1
WAE(config-wccp-service)# egress-method generic-gre
```

The router list must contain the IP address of each intercepting router. Multicast addresses are not supported. Additionally, you must configure a GRE tunnel interface on each router. For details on configuring GRE tunnel interfaces on the routers, see Configuring a GRE Tunnel Interface on a Router, on page 159.

To view the egress method that is configured and that is being used on a particular WAE, use the **show wccp egress** EXEC command. To view information about the egress method for each connection segment, use the **show statistics connection egress-methods** EXEC command.

To view the generic GRE tunnel statistics for each intercepting router, use the **show statistics generic-gre** EXEC command. To clear statistics information for the generic GRE egress method, use the **clear statistics generic-gre** EXEC command.

Configuring a GRE Tunnel Interface on a Router

Consider the following guidelines for configuring a GRE tunnel interface on a router:

- If you plan to use the generic GRE egress method on the WAE, configure a GRE tunnel interface on each intercepting router. For ease of configuration, we recommend that you create a single multipoint tunnel on the router, instead of one point-to-point tunnel per WAE in the farm.
- If you have only one WAE in the farm, you can use a point-to-point tunnel. However, ensure that the router is configured with no other tunnel that has the same tunnel source as the WAE tunnel.

  On a Catalyst 6500 Series switch with the Supervisor Engine 32 or 720, do not configure more than one GRE tunnel (multipoint or point-to-point) with the same tunnel source interface, because this may result in high switch CPU load.

- The tunnel interface must have a Layer 3 source interface to which it is attached, and this source interface must be the interface whose IP address is configured in the WAE's intercepting router list.
- The tunnel interface must be excluded from WCCP interception to avoid routing loops when outbound interception is used. Use the **ip wccp redirect exclude in** command. You can always use this command because it does not cause any impact even when it is not required, such as for inbound interception.
- To configure WCCP to work with WAEs with the generic GRE egress method, you must configure keepalives on the tunnel interface used on the Cisco WCCP router. The following is a sample configuration:

```
interface Tunnel1
ip address 12.12.12.12 255.255.255.0
no ip redirects
ip wccp redirects exclude in
keepalive 20 3 <<<<<<<<<<<<
tunnel source FastEthernet0/.130
tunnel mode gre multipoint
```

Multipoint Tunnel Configuration

Consider a deployment in which there are two intercepting routers and two WAEs in the farm. Each WAE configuration will look like the following example:

```
wccp router-list 1 192.168.1.1 192.168.2.1
wccp tcp-promiscuous service-pair 61 62
  router-list-num-1
  egress-method generic-gre
  redirect-method gre
  enable
```

Each router can configure a single multipoint GRE tunnel to the WAE farm.

Router 1 configuration will look like the following example:

```
interface gigabitEthernet 1/1
ip address 192.168.1.1 255.255.255.0
...
interface Tunnel1
ip address 12.12.12.1 255.255.255.0
tunnel source GigabitEthernet1/1
tunnel mode gre multipoint
ip wccp redirect exclude in
end
```

Router 2 configuration will look like the following:

```
interface Vlan815 1/0
ip address 192.168.2.1 255.255.255.0
...
interface Tunnel1
ip address 13.13.13.1 255.255.255.0
tunnel source vlan815
tunnel mode gre multipoint
ip wccp redirect exclude in
end
```

Note The tunnel interface is enabled for IP by provisioning an IP address, which allows it to process and forward transit packets. If you do not want to provision an IP address, the tunnel must be IP enabled by making it an IP unnumbered interface. This restricts the tunnel; it can only be a point-to-point tunnel.

Point-To-Point Tunnel Configuration

This section describes how to configure a point-to-point tunnel for a single WAE instead of a multipoint tunnel on the router. A point-to-point tunnel is enabled for IP either by making it unnumbered or by giving it an IP address. The unnumbered method is shown in the following example router configuration:

```
interface gigabitEthernet 1/1
ip address 192.168.1.1 255.255.255.0
...
! Tunnel1 is an unnumbered point-to-point tunnel towards WAE1
interface Tunnel1
ip unnumbered GigabitEthernet1/1
tunnel source GigabitEthernet1/1
! tunnel destination is the IP address of WAE1
tunnel destination 10.10.10.10
ip wccp redirect exclude in
end
```

Using Policy-Based Routing Interception

This section contains the following topics:

- About Policy-Based Routing, on page 161
- Configuring Policy-Based Routing, on page 163
- Methods of Verifying PBR Next-Hop Availability, on page 167

About Policy-Based Routing

Policy-based routing (PBR), introduced in Cisco IOS Release 11.0, allows you to implement policies that selectively cause packets to take specific paths in the network.

PBR also provides a method to mark packets so that certain kinds of traffic receive differentiated, preferential service when used in combination with queuing techniques enabled through the Cisco IOS software. These queuing techniques provide an extremely powerful, simple, and flexible tool to network managers who implement routing policies in their networks.

PBR enables a router to put packets through a route map before routing them. When configuring PBR, you must create a route map that specifies the match criteria, and the resulting action, if all the match clauses are met. You must enable PBR for that route map on a particular interface. All the packets arriving on the specified interface matching the match clauses will be subject to PBR.

One interface can have only one route map tag; but you can have several route map entries, each with its own sequence number. Entries are evaluated in the order of their sequence numbers until the first match occurs. If no match occurs, packets are routed as usual.

```
Router(config-if)# ip policy route--tag
```

The route map determines which packets are routed next.

You can enable PBR to establish a route that goes through Cisco WAAS for some or all packets. Cisco WAAS proxy applications receive PBR-redirected traffic in the same manner as WCCP redirected traffic.

To enable PBR to establish a route that goes through Cisco WAAS for some or all packets, follow these steps:

1. In the branch office, define traffic of interest on the branch office router (Edge-Router1) as follows:
   1. Specify which traffic is of interest to the LAN interface (ingress interface) on Edge-Router1.

      Use extended IP access lists to define traffic of interest (traffic from all or filtered local source addresses to any or filtered destination address).
   2. Specify which traffic is of interest to the WAN interface (egress interface) on Edge-Router1.

      Use extended IP access lists to define traffic of interest (traffic from all or filtered local source addresses from any or filtered remote addresses).
2. In the data center, specify which traffic is of interest to the data center router (Core-Router1) as follows:
   1. Specify which traffic is of interest to the LAN interface (ingress interface) on Core-Router1.

      Use extended IP access lists to define traffic of interest (traffic from all or filtered local source addresses to any or filtered destination address).
   2. Specify which traffic is of interest to the WAN interface (egress interface) on Core-Router1.

      Use extended IP access lists to define traffic of interest (traffic from all or filtered local source addresses from any or filtered remote addresses).
3. In the branch office, create route maps on Edge-Router1, as follows:
   1. Create a PBR route map on the LAN interface of Edge-Router1.
   2. Create a PBR route map on the WAN interface of Edge-Router1.
4. In the data center, create route maps on Core-Router1, as follows:
   1. Create a PBR route map on the LAN interface of Core-Router1.
   2. Create a PBR route map on the WAN interface of Core-Router1.
5. In the data center, apply the PBR route maps to Edge-Router1.
6. In the data center, apply the PBR route maps to Core-Router1.
7. Determine which PBR method to use to verify PBR next-hop availability of a WAE. For more information, see Methods of Verifying PBR Next-Hop Availability, on page 167.

Note For a description of the PBR commands that are referenced in this section, see *Cisco Quality of Service Solutions Command Reference*.

WAEs (Edge-WAE1 and Core-WAE1) must reside in an out-of-band network that is separate from the traffic's destination and source. For example, Edge-WAE1 is on a subnet that is separate from the clients (the traffic source), and Core-WAE that is on a subnet separate from the file servers and application servers (the traffic destination). Additionally, the WAE may have to be connected to the router that is redirecting traffic to it through a tertiary interface (a separate physical interface) or a subinterface to avoid a routing loop. For more information, see Using Tertiary Interfaces or Subinterfaces to Connect WAEs to Routers in the chapter Planning Your Cisco WAAS Network."

The following table provides a summary of the router interfaces that you must configure to use PBR or WCCP Version 2 to transparently redirect traffic to a WAE.

Table 9: Router Interfaces for WCCP or PBR Traffic Redirection to WAEs

Router interface	Comment
Edge-Router1	
A	Edge LAN interface (ingress interface) that performs redirection on outbound traffic.
B	Tertiary interface (separate physical interface) or a subinterface off of the LAN port on Edge-Router1. Used to attach Edge-WAE1 to Edge-Router1 in the branch office.
C	Edge WAN interface (egress interface) on Edge-Router1 that performs redirection on inbound traffic.
Core-Router1	
D	Core LAN interface (ingress interface) that performs redirection on outbound traffic.
E	Tertiary interface or subinterface off of the LAN port on Core-Router1. Used to attach Core-WAE1 to Core-Router1 in the data center.
F	Core WAN interface (egress interface) on Core-Router1 that performs redirection on inbound traffic.

The example provided in Configuring Policy-Based Routing, on page 163 shows how to configure PBR as the traffic redirection method in a WAAS network that has one WAE in a branch office and one WAE in the data center.

Note The commands that are used to configure PBR on a router, can vary based on the Cisco IOS release installed on the router. For information about the commands that are used to configure PBR for the Cisco IOS release that you are running on your routers, see the appropriate Cisco IOS configuration guide.

Configuring Policy-Based Routing

The example provided in this section shows how to configure PBR as the traffic redirection method in a WAAS network that has one WAE in a branch office and one WAE in the data center.

Procedure

Step 1 In the branch office, use extended IP access lists to specify which traffic is of interest to the LAN interface (ingress interface-A) on **Edge-Router1**:

a) On **Edge-Router1**, define an extended IP access list within the range of 100 to 199. For example, create access list 100 on Edge-Router1:

```
Edge-Router1(config)# ip access-list extended 100
```

b) On Edge-Router1, specify which traffic is of interest to this particular interface. For example, mark any IP/TCP traffic from any local source addresses (traffic for any branch office clients) on any TCP port to any destination, as interesting:

```
Edge-Router1(config-ext-nacl)# permit tcp 10.10.10.0 0.0.0.255 any
```

- Alternatively, you can selectively mark interesting traffic by defining the source IP subnet, destination IP address, and TCP port numbers. For example, mark IP/TCP traffic from any local source address on TCP ports 135 and 80 to any destination as interesting:

```
Edge-Router1(config-ext-nacl)# permit tcp 10.10.10.0 0.0.0.255 any eq 135
Edge-Router1(config-ext-nacl)# permit tcp 10.10.10.0 0.0.0.255 any eq 80
```

Step 2 In the branch office, use extended IP access lists to specify which traffic is of interest to the WAN interface (egress interface-C) on Edge-Router1:

a) On Edge-Router1, define an extended IP access list within the range of 100 to 199, for example, create access list 101 on Edge-Router1:

```
Edge-Router1(config)# ip access-list extended 101
```

b) On **Edge-Router1**, specify which traffic is of interest to its WAN interface:

- For example, mark any IP/TCP traffic to a local device, as interesting:

```
Edge-Router1(config-ext-nacl)# permit tcp any 10.10.10.0 0.0.0.255
```

- Alternatively, you can selectively mark interesting traffic by defining the source IP subnet, destination IP address, and TCP port numbers. For example, mark IP/TCP traffic to any local source addresses on TCP ports 135 and 80 to any destination, as interesting:

```
Edge-Router1(config-ext-nacl)# permit tcp any 10.10.10.0 0.0.0.255 eq 135
Edge-Router1(config-ext-nacl)# permit tcp any 10.10.10.0 0.0.0.255 eq 80
```

Step 3 In the data center, use extended IP access lists to specify which traffic is of interest to the LAN interface (ingress interface-D) on Core-Router1:

a) On Core-Router1, define an extended IP access list within the range of 100 to 199, for example, create access list 102 on Core-Router1:

```
Core-Router1(config)# ip access-list extended 102
```

b) On Core-Router1, specify which traffic is of interest to its LAN interface:

- For example, mark any IP/TCP traffic sourced from any local device, for example, traffic sourced from any file server or application server in the data center, on any TCP port to any destination, as interesting:

```
Core-Router1(config-ext-nacl)# permit tcp 10.10.11.0 0.0.0.255 any
```

- Alternatively, you can selectively mark traffic as interesting by defining the source IP subnet, destination IP address, and TCP port numbers. For example, selectively mark IP/TCP traffic sourced from any local device on TCP ports 135 and 80 to any destination, as interesting:

```
Core-Router1(config-ext-nacl)# permit tcp 10.10.11.0 0.0.0.255 any eq 135
Core-Router1(config-ext-nacl)# permit tcp 10.10.11.0 0.0.0.255 any eq 80
```

Step 4 In the data center, use extended IP access lists to mark traffic of interest for the WAN interface (egress interface-F) on Core-Router1:

a) On Core-Router1, define an extended access list within the range of 100 to 199, for example, create access list 103 on Core-Router1:

```
Core-Router1(config)# ip access-list extended 103
```

b) On Core-Router1, mark interesting traffic for the WAN interface:

- For example, mark any IP/TCP traffic destined to any local device (for example, traffic destined to any file server or application server in the data center) as interesting:

```
Core-Router1(config-ext-nacl)# permit tcp any 10.10.11.0 0.0.0.255
```

- Alternatively, you can selectively mark traffic as interesting by defining the source IP subnet, destination IP address, and TCP port numbers. For example, mark IP/TCP traffic on ports 135 and 80 to any local source addresses, as interesting:

```
Core-Router1(config-ext-nacl)# permit tcp any 10.10.11.0 0.0.0.255 eq 135
Core-Router1(config-ext-nacl)# permit tcp any 10.10.11.0 0.0.0.255 eq 80
```

Step 5 In the branch office, define PBR route maps on Edge-Router1:

a) Define a route map for the LAN interface (ingress interface). The following example shows how to create a WAAS-EDGE-LAN route map:

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

b) Define a route map for the WAN interface (egress interface).

The following example shows how to create a WAAS-EDGE-WAN route map:

```
Edge-Router1(config)# route-map WAAS-EDGE-WAN permit
```

c) Specify the match criteria.

Run the **match** command to specify the extended IP access list that Edge-Router1 should use to determine which traffic is of interest to its WAN interface. If you do not specify a **match** command, the route map applies to all packets.

The following example shows how to configure Edge-Router1 to use the access list 101 as the criteria for determining which traffic is of interest to its WAN interface:

```
Edge-Router1(config-route-map)# match ip address 101
```

Note The **ip address** command option matches the source or destination IP address that is permitted by one or more standard or extended access lists.

d) Specify how the matched traffic should be handled.

The following example shows how to configure Edge-Router1 to send the packets that match the specified criteria to the next hop, which is Edge-WAE1 that has an IP address of 1.1.1.100:

```
Edge-Router1(config-route-map)# set ip next-hop 1.1.1.100
```

Note If you have more than one branch WAE, you can specify the IP address of a second branch WAE for failover purposes, for example, run the **set ip next-hop 1.1.1.101** command on Edge-Router1, to specify a next-hop address of 1.1.1.101 (the IP address of Edge-WAE2) for failover purposes. Run the **next-hop** command for failover purposes and not for load-balancing purposes.

Step 6 In the data center, create route maps on Core-Router1:

a) Define a route map on the LAN interface (ingress interface).

The following example shows how to create a WAAS-CORE-LAN route map:

```
Core-Router1(config)# route-map WAAS-CORE-LAN permit
```

b) Define a route map on the WAN interface (egress interface).

The following example shows how to create a WAAS-CORE-WAN route map:

```
Core-Router1(config)# route-map WAAS-CORE-WAN permit
```

c) Specify the match criteria.

Use the **match** command to specify the extended IP access list that Core-Router 1 should use to determine which traffic is of interest to its WAN interface. If you do not enter a **match** command, the route map applies to all the packets. The following example shows how to configure Core-Router1to use access list 103 as the criteria for determining which traffic is of interest to its WAN interface:

```
Core-Router1(config-route-map)# match ip address 103
```

d) Specify how the matched traffic is to be handled.

The following example shows how to configure Core-Router1 to send packets that match the specified criteria to the next hop, which is Core-WAE1 that has an IP address of 2.2.2.100:

```
Core-Router1(config-route-map)# set ip next-hop 2.2.2.100
```

Note If you have more than one data center WAE, specify the IP address of a second data center WAE for failover purposes, for example, run the **set ip next-hop 2.2.2.101** command on Core-Router1, to specify a next-hop address of 2.2.2.101 (the IP address of Core-WAE2) for failover purposes. Run the **next-hop** command for failover purposes and not for load-balancing purposes.

Step 7 In the branch office, apply the route maps to the LAN interface (ingress interface) and the WAN interface (egress interface) on Edge-Router1:

a) On Edge-Router1, enter interface configuration mode:

```
Edge-Router1(config)# interface FastEthernet0/0.10
```

b) Specify that the LAN router interface should use the WAAS-EDGE-LAN route map for PBR:

```
Edge-Router1(config-if)# ip policy route-map WAAS-EDGE-LAN
```

c) Enter interface configuration mode:

```
Edge-Router1(config-if)# interface Serial0
```

d) Specify that the WAN router interface should use the WAAS-EDGE-WAN route map for PBR:

```
Edge-Router1(config-if)# ip policy route-map WAAS-EDGE-WAN
```

Step 8 In the data center, apply the route maps to the LAN interface (ingress interface) and the WAN interface (egress interface) on Core-Router1:

a) On Core-Router1, enter interface configuration mode:

```
Core-Router1(config)# interface FastEthernet0/0.10
```

b) Specify that for PBR, the LAN router interface should use the WAAS-CORE-LAN route map:

```
Core-Router1(config-if)# ip policy route-map WAAS-CORE-LAN
```

c) Enter interface configuration mode:

```
Core-Router1(config-if)# interface Serial0
```

d) Specify that for PBR, the WAN router interface should use the WAAS-CORE-WAN route map:

```
Core-Router1(config-if)# ip policy route-map WAAS-CORE-WAN
```

Methods of Verifying PBR Next-Hop Availability

When using PBR to transparently redirect traffic to WAEs, we recommend that you use one of the following methods to verify the PBR next-hop availability of a WAE. The method that you choose should be based on the version of the Cisco IOS software that is running on the routers and the placement of your WAEs. However, Method 2 is the preferred method whenever possible:

- **Method 1**: If the device sees the WAEs as a CDP neighbor (directly connected), it can use CDP and ICMP to verify that the WAE is operational. For more information, see Method 1: Using CDP to Verify Operability of WAEs, on page 167.
- **Method 2 (Recommended method)**: If the device is running Cisco IOS software Release 12.4 or later and the device does not see the WAE as a CDP neighbor, use the IP service level agreements (SLAs) can be used to verify that the WAE is operational using ICMP echoes. For more information, see Method 2: Using IP SLAs to Verify WAE Operability Using ICMP Echo Verification, on page 168.
- **Method 3**: If the device is running the Cisco IOS software Release 12.4 or later and does not see the WAE as a CDP neighbor, use IP SLAs to verify that the WAE is operational using TCP connection attempts. For more information, see Method 3: Using IP SLAs to Verify WAE Operability Using TCP Connection Attempts, on page 169.

Note In this section, device is used to refer to the router or switch that has been configured to use PBR to transparently redirect traffic to a WAE.

To verify whether the WAE is CDP visible to a device that has been configured to use PBR, run the **show cdp neighbors** command on the device. If the WAE is CDP visible to the device, the WAE will be listed in the output of the **show cdp neighbors** command.

Method 1: Using CDP to Verify Operability of WAEs

Before you begin

If the device that is configured to use PBR views the WAEs as a CDP neighbor (the WAE is directly connected to the device), you can configure CDP and ICMP to verify the availability of a WAE as a PBR next hop.

The following example shows how to use this method to verify PBR next-hop availability of a WAE. You must complete the following configuration process for each of the LAN and WAN route maps that are configured when CDP should be used.

Procedure

Step 1 On the router where PBR is configured, for example, on the branch office router named Edge-Router1, enter configuration mode and enable CDP on the router:

```
Edge-Router1(config)# cdp run
```

Step 2 Enable route-map configuration mode for the route map, WAAS-EGDE-LAN, which has already been created on the router:

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

Step 3 Configure the router to use CDP to verify the availability of the configured next-hop addresses:

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability
```

Step 4 Enable CDP on the WAE, for example, on the branch office WAE named Edge-WAE1, that you want the router to redirect traffic to using PBR:

```
Edge-WAE1(config)# cdp enable
```

Note If you are configuring PBR and have multiple WAEs, and are using Method 1 to verify the PBR next-hop availability of a WAE, no additional configuration is necessary after you have completed the preceding process.

Method 2: Using IP SLAs to Verify WAE Operability Using ICMP Echo Verification

Procedure

Step 1 On the branch office router named Edge-Router1, enter the route-map configuration mode for the route map named WAAS-EDGE-LAN, which has been previously configured on this router:

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

Step 2 Specify a match condition for the traffic. In the following example, the match condition specifies access list number 105:

```
Edge-Router1(config)# match ip address 105
```

Step 3 Configure the route map to use IP SLA tracking instance number 1 to verify the availability of the next-hop WAE, for example, the branch WAE named Edge-WAE1 that has an IP address of 1.1.1.100:

Edge-Router1(config-route-map)# **`set ip next-hop verify-availability 1.1.1.100 track 1`**

Note Enter the set ip next-hop verify-availability command for each route map that has been configured on this branch office edge router and on the data center’s core router that has also been configured to use PBR to redirect traffic to WAEs.

Step 4 Configure IP SLA tracking instance 1:

```
Edge-Router1(config-route-map)# exit
Edge-Router1(config)# ip sla 1
Edge-Router1(config-ip-sla)#
```

Step 5 Configure the router to echo Edge-WAE1 using the specified source interface:

```
Edge-Router1(config-ip-sla)# icmp-echo 1.1.1.100 source-interface FastEthernet 0/0.20
```

Step 6 Configure the router to perform the echo every 20 seconds:

```
Edge-Router1(config-ip-sla)# frequency 20
Edge-Router1(config-ip-sla)# exit
```

Step 7 Schedule IP SLA tracking instance 1 to start immediately and to run continuously:

```
Edge-Router1(config)# ip sla schedule 1 life forever start-time now
```

Step 8 Configure IP SLA tracking instance 1 to track the device, which is defined in the IP SLA tracking instance 1:

```
Edge-Router1(config)# track 1 rtr 1
```

Note If you are configuring PBR and have multiple WAEs, and you are using Method 2 to verify PBR next-hop availability of a WAE, you must configure a separate IP SLA per WAE, and then run the track command for each IP SLA.

Method 3: Using IP SLAs to Verify WAE Operability Using TCP Connection Attempts

Before you begin

If the device that is configured for PBR is running the Cisco IOS software Release 12.4 or later, and does not see the WAE as a CDP neighbor, use IP SLAs to verify that the WAE is alive using TCP connection attempts. Use IP SLAs to monitor a WAE's availability as the PBR next hop using TCP connection attempts at a fixed interval of 60 seconds.

Procedure

Step 1 On the branch office router named Edge-Router1, enter route-map configuration mode for the route map named WAAS-EDGE-LAN, which has been previously configured on this router:

```
Edge-Router1(config)# route-map WAAS-EDGE-LAN permit
```

Step 2 Configure the route map to use IP SLA tracking instance number 1 to verify the availability of the next-hop WAE (the Edge WAE that has an IP address of 1.1.1.100):

```
Edge-Router1(config-route-map)# set ip next-hop verify-availability 1.1.1.100 track 1
```

Note Enter the set ip next-hop verify-availability command for each route map that is configured on this branch office edge router and on the data center's core router that has also been configured to use PBR to transparently redirect traffic to WAEs.

Step 3 Configure the IP SLA tracking instance 1:

```
Edge-Router1(config-route-map)# exit
Edge-Router1(config)# ip sla 1
```

Step 4 Configure the router to use the specified source and destination ports to use TCP connection attempts at a fixed interval of 60 seconds to monitor the WAE availability:

```
Edge-Router1(config-ip-sla)# tcp-connect 1.1.1.100 80 source-port 51883 control disable
Edge-Router1(config-ip-sla)# exit
```

Step 5 Schedule the IP SLA tracking instance 1 to start immediately and to run forever:

```
Edge-Router1(config)# ip sla schedule 1 life forever start-time now
```

Step 6 Configure the IP SLA tracking instance 1 to track the device, that is defined in the IP SLA tracking instance 1:

```
Edge-Router1(config)# track 1 rtr 1
```

Note If you are configuring PBR and have multiple WAEs, and you are using Method 3 to verify PBR next-hop availability of a WAE, you must configure a separate IP SLA per WAE, and then run the track command per IP SLA.

Cisco ITD Support

This section contains the following topics:

About Cisco ITD

For Cisco WAAS Version 6.4.3 and later, Cisco Intelligent Traffic Director (ITD) supports Cisco WAAS.is an intelligent, hardware-based, multi-terabit solution that allows you to build a scalable architecture for Layer 3 and Layer 4 traffic distribution, load balancing, and traffic redirection. Cisco ITD provides adaptive load balancing to distribute traffic to an application cluster. For more information on how to configure Cisco ITD for Cisco WAAS, see Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide.

Cisco ITD has reduced complexities and architecture scaling for alternative features like Web Cache Communication Protocol (WCCP) and policy-based routing (PBR). Unlike WCCP, ITD is not CPU intensive and has less ternary content-addressable memory (TCAM) utilization.

Cisco ITD is used in the following scenarios.

- **Server Load balancing**: Server farms, Application servers, Web Servers.
- **Services Load balancing, clustering**: Firewall, IDS, IPS, L7 Server LB, WAF, VDS -TC (Transparent Caching), WAE.
- **Traffic Steering, Redirection**: Web accelerator Engine (WAE), Web Caches.

Cisco ITD can be used in single-sided or double-sided deployments:

- Single-sided deployment: For Cisco WAAS with single-sided ITD interception, Cisco ITD supports an end-to-end topology. Cisco ITD configured in the branch will be interoperable with WAN side interception methods supported by Cisco WAAS like WCCP, Inline and Appnav redirection and vice versa.
- Double-sided deployment: Cisco ITD can be used on both sides of the WAN.

Configuring Cisco ITD

The following example shows how to configure Cisco ITD as the traffic redirection method in a Nexus switch that has one or more WAEs connected as nodes.

Procedure

Step 1 Enable the Cisco ITD feature in the switch. It is disabled by default.

```
switch# configure terminal
switch(config)# feature itd
switch(config)# feature pbr
switch(config)# feature sla sender
```

Step 2 Create an Access list, one for allowing client to server and other for allowing server to client networks.

```
switch(config)# ip access-list <Client-Server>
switch(config-acl)# 10 permit tcp <source address /mask><destination address /mask>
switch(config)# ip access-list <Server-Client>
switch(config-acl)# 20 permit tcp <source address /mask><destination address /mask>
```

Cisco Catena Support

Cisco Catena allows you to create several chains with multiple elements in each chain. You can configure security policies to specify segments of traffic through a particular chain. Cisco Catena support is available for Cisco WAAS in a routed mode beginning with Cisco Version 6.4.3. For more information, see the *Cisco Nexus 9000 Series NX-OS Catena Configuration Guide*.

Using Inline Mode Interception

This section contains the following topics:

- About Inline Interception, on page 171
- Enabling Inline Operation on WAEs, on page 173
- Configuring Inline Interface Settings on WAEs, on page 175
- Configuring Inline Operation on ANCs, on page 178
- Configuring an IP Address on an Inline Interface, on page 180
- Configuring VLANs for Inline Support, on page 182
- About Clustering Inline Cisco WAEs, on page 182
- Disabling Peer Optimization Between Serial Inline WAEs, on page 183

About Inline Interception

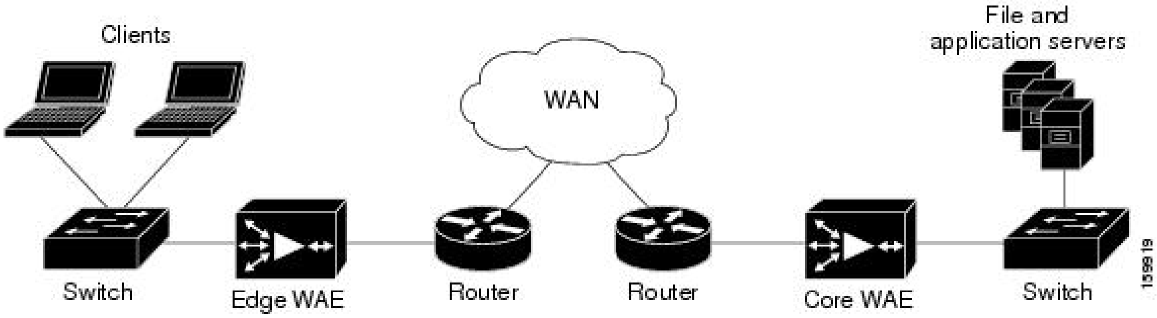
A WAE can physically and transparently intercept traffic between clients and a router by using inline mode.

Consider the following operating guidelines for inline interception:

- To use inline mode, use a WAE with the Cisco WAE Inline Network Adapter or Interface Module installed. In this mode, you physically position the WAE device in the path of the traffic that you want to optimize, typically between a switch and a router, as shown in the following figure. Redirection of traffic is not necessary.

- When you install an inline WAE device, you must follow the cabling requirements described in the appropriate platform hardware guide.
- Any combination of traffic interception mechanisms on peer WAEs is supported. For example, you can use inline interception on the branch WAE and WCCP on the data center WAE. For complex data center deployments, we recommend that you use hardware-accelerated WCCP interception with the Cisco WAAS AppNav solution (see the chapter "Configuring Cisco AppNav") or load balancing with the Cisco Application Control Engine (ACE).

Figure 31: Inline Interception



Note Inline mode and WCCP redirection are exclusive. You cannot configure inline mode if the WAE is configured for WCCP operation. Inline mode is the default mode when a Cisco WAE Inline Network Adapter is installed in a WAE device, but you must configure inline mode explicitly on a device with a Cisco Interface Module.

- An inline WAE can be configured as a Central Manager, but the inline interception functionality is not be available.
- The Cisco WAE Inline Network Adapter contains two or four Ethernet ports, the Cisco Interface Module contains two to eight Ethernet ports, and the Cisco AppNav Controller Interface Module contains four to 12 Ethernet ports. Ports on the Cisco WAE Inline Network Adapter are always configured as inline ports, while ports on the Interface Modules are configured as normal standalone ports by default, and you must explicitly configure these ports as inline ports. Each pair of inline ports is grouped into a logical inline group.
- Each inline group has one LAN-facing port and one WAN-facing port. Typically, you use just one inline group, and connect the LAN-facing port to a switch and the WAN-facing port to a router. On adapters or interface modules with additional ports, additional groups of interfaces are provided if you are using a network topology where you have to connect a WAE to multiple routers. Traffic that enters into one interface in a group, exits the device via another interface in the same group.
- The following are hardware platforms supported for inline ports:
    - Cisco WAVE-294: Supports one installed Cisco Interface Module with 2, 4, or 8 ports.
    - Cisco WAVE-594, 694, 7541, 7571, and 8541: Support one installed Cisco Interface Module with 2, 4, or 8 ports or a Cisco AppNav Controller Interface Module with 4 or 12 ports.

- The two-port 10-Gigabit Cisco Interface Module cannot be used in inline mode. The four-port 10-Gigabit Cisco AppNav Controller Interface Module is supported only on the Cisco WAVE-594.
- You have the option of assigning an IP address to an inline interface, but it is not required. For more information, see Configuring an IP Address on an Inline Interface.
- Traffic that flows through an inline group is transparently intercepted for optimization. Traffic that does not have to be optimized is bridged across the LAN/WAN interfaces. If a power, hardware, or unrecoverable software failure occurs, the network adapter automatically begins operating in bypass mode (fail-close), where all traffic is mechanically bridged between the LAN and WAN interfaces in each group. The Cisco WAE Inline Network Adapter and Cisco Interface Module also operate in bypass mode when the WAE is powered off or starting up. Additionally, you can manually put an inline group into bypass mode.
- AppNav Controller Interface Modules do not support automatic bypass mode to continue traffic flow in the event of a failure. For high availability, two or more AppNav Controller Interface Modules should be deployed in an AppNav cluster. For more information on using inline mode with the AppNav solution, see the chapter "Configuring Cisco AppNav."
- Inline mode is configured by default to accept all TCP traffic. If the network segment in which the WAE is inserted is carrying 802.1Q tagged (VLAN) traffic, initially, traffic on all VLANs is accepted. Inline interception can be enabled or disabled for each VLAN. However, optimization policies cannot be customized based on the VLAN.
- You can serially cluster WAE devices operating in inline mode to provide higher availability if a device fails. For details, see About Clustering Inline Cisco WAEs.
- When a WAE inline group enters bypass mode, the switch and router ports to which it is connected may have to reinitialize, which may cause an interruption of several seconds in the traffic flow through the WAE.

  If the WAE is deployed in a configuration where the creation of a loop is not possible, that is, if it is deployed in a standard fashion between a switch and a router, configure **PortFast** on the switch port to which the WAE is connected. **PortFast** allows the port to skip the first few stages of the Spanning Tree Algorithm (STA) and move more quickly into a packet forwarding mode.

Enabling Inline Operation on WAEs

Before you begin

This section describes how to enable and configure inline settings on WAEs configured as application accelerators and that are not part of an AppNav Cluster (WAEs that are part of an AppNav Cluster use only the appnav-controller interception method). To configure the inline settings on WAEs configured as AppNav Controllers, see Configuring Inline Operation on ANCs, on page 178.

On WAVE-294/594/694/7541/7571/8541 devices that use Cisco Interface Modules, the Interface Module ports are configured by default for normal standalone operation. If you want to use the device in inline mode, you must configure the ports for inline operation. Enabling inline mode configures all the ports for inline operation and converts each pair of ports to an inline group.

On other WAE devices that use the Cisco WAE Inline Network Adapter, the ports on the adapter always operate in inline mode. You can use this configuration window to enable or disable VLAN ID connection verification, which is the only setting that appears for such WAE devices.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*. (You cannot enable inline operation from device groups.)

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**.

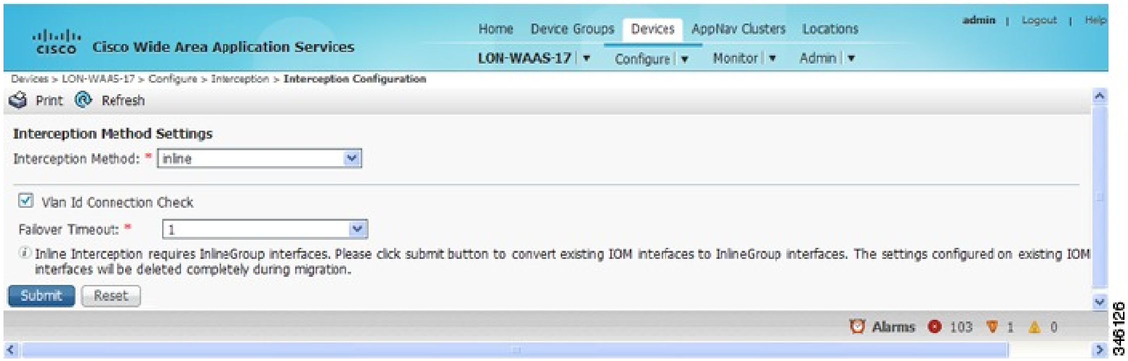
Note If you are configuring a device using a Cisco WAAS version earlier than Cisco WAAS Version 5.0, choose **Configure** > **Interception** > **Inline** > **General Settings** to configure inline general settings. The **Configuration** window looks different, but has similar settings.

The **Interception Configuration** window appears.

Step 3 From the **Interception Method** drop-down list, choose **Inline** to enable inline mode. The **Interception Method** drop-down list is not displayed for devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0.

The **Interception Configuration** window refreshes with the inline settings.

Figure 32: Inline Interception Settings Window



Devices > LON-WAAS-17 > Configure > Interception > Interception Configuration

Interception Method Settings

Interception Method: * inline

☑ Vlan Id Connection Check

Failover Timeout: * 1

Inline Interception requires InlineGroup interfaces. Please click submit button to convert existing IOM interfaces to InlineGroup interfaces. The settings configured on existing IOM interfaces will be deleted completely during migration.

Step 4 Check the **Inline Enable** check box to enable inline operation.

The **Inline Enable** check box is displayed only for Cisco WAVE devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0 and that have a Cisco Interface Module installed.

Step 5 Check the **VLAN ID Connection Check** check box to enable VLAN ID connection checking. Uncheck the check box to disable it. The default setting is enabled.

Cisco WAAS uses the VLAN ID to intercept or bridge VLAN traffic on the inline interface for a TCP flow. The VLAN ID of all the packets sent in a particular TCP connection must match; packets with a different VLAN ID will be bridged and not optimized. If your system has an asymmetric routing topology, in which the traffic flow in one direction uses a different VLAN ID than the traffic flow from the other direction, you may have to disable VLAN ID checking to ensure that the traffic is optimized.

Step 6 From the **Failover Timeout** drop-down list, choose the failover timeout (1, 5, or 25 seconds), which is the number of seconds that the interface should wait for before going into bypass mode, after a device or power failure. The default is 1 second.

This item appears only for Cisco WAVE devices that use Cisco Interface Modules, but not for AppNav Controller Interface Modules. For devices that use Cisco WAE Inline Network Adapters, the failover timeout is configured in the **Inline Interface Settings** window. This item is named **Time Out for WAAS versions earlier than 5.0** and appears before the **VLAN ID Connection Check** item.

Step 7 Click **Submit**. A message appears, for you to confirm that all the Interface Module interfaces are to be converted to inline group interfaces, and the existing Interface Module interface configurations are to be removed.

Step 8 To confirm, click **OK**.

Consider the following inline mode configuration guidelines:

- The inline groups are configured with basic default settings. To configure inline group settings, see Configuring Inline Interface Settings on WAEs, on page 175.
- For devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0, after enabling Inline mode, it takes about two data feed poll cycles (about 10 minutes by default) for the inline groups to appear in the Inline Interfaces list in the lower part of the window.
- Inline mode cannot be enabled if any of the Interface Module ports are configured as the primary interface. Change the primary interface and return to this window to enable inline mode.

  For devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0, if you configure any of the interfaces on an Interface Module with nondefault settings (standby group, port channel, BVI, speed, duplex, IP address, ACLs, and so on), inline mode cannot be enabled, and a warning message appears, asking you to check all the interfaces for configuration settings. You must remove all the configuration settings from all the interface module interfaces (slot 1) and then return to this window to enable inline mode.
- To enable inline operation from the CLI, run the **interception-method inline** global configuration command.
- To configure VLAN ID checking from the CLI, use the **inline vlan-id-connection-check** global configuration command after inline operation is enabled.

Configuring Inline Interface Settings on WAEs

Before you begin

This section describes how to configure inline settings on WAEs configured as application accelerators, and that are not a part of an AppNav Cluster (WAEs that are a part of an AppNav Cluster use only the appnav-controller interception method). To configure inline settings on WAEs configured as AppNav Controllers, see Configuring Inline Operation on ANCs, on page 178.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*. (You cannot configure inline interface settings from device groups.)

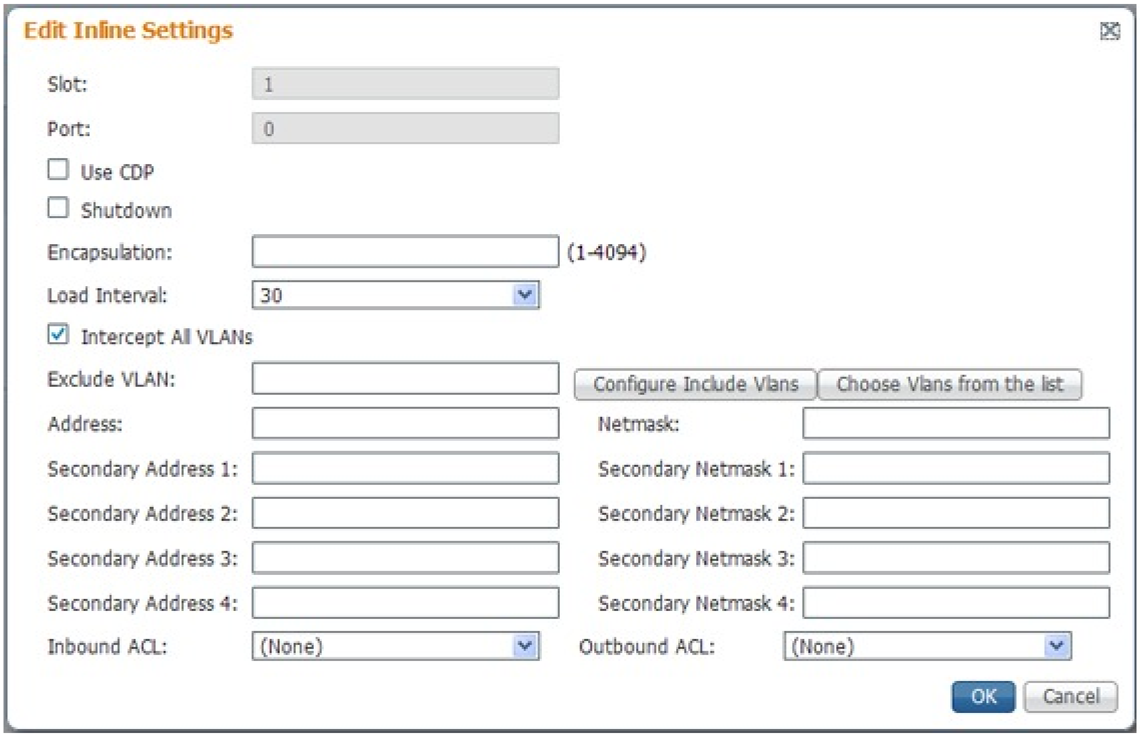
Step 2 Choose **Configure** > **Interception** > **Interception Configuration**.

Note If you are configuring a device using a Cisco WAAS version earlier than Cisco WAAS Version 5.0, choose **Configure** > **Interception** > **Inline** > **Inline Interfaces** to configure inline interface settings. The **Configuration** window looks different, but has similar settings.

The **Inline Interfaces** window appears, listing the inline interface groups available on the device.

Step 3 Choose an inline group to configure and click the **Edit** taskbar icon. (For devices using Cisco WAAS Versions earlier than Cisco WAAS Version 5.0, click the **Edit** icon next to the interface.)

The **Edit Inline Settings** window appears, displaying the inline interface configurations for a particular slot and port group.



Edit Inline Settings

Slot: 1

Port: 0

☐ Use CDP

☐ Shutdown

Encapsulation: (1-4094)

Load Interval: 30

☑ Intercept All VLANs

Exclude VLAN:

Address: Netmask:

Secondary Address 1: Secondary Netmask 1:

Secondary Address 2: Secondary Netmask 2:

Secondary Address 3: Secondary Netmask 3:

Secondary Address 4: Secondary Netmask 4:

Inbound ACL: (None) Outbound ACL: (None)

Step 4 Check the **Use CDP** check box to enable Cisco Discovery Protocol (CDP) on the inline group interfaces. The **Use CDP** check box is not shown for devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0.

When enabled, CDP obtains protocol addresses of neighboring devices and discovers the platform of those devices. It also shows information about the interfaces used by your router.

Configuring CDP from the CDP Settings window enables CDP globally on all the interfaces. For information on configuring CDP settings, see Configuring CDP Settings in the chapter "Configuring Network Settings."

Step 5 Check the **Shutdown** check box to shut down the inline group. This setting bridges traffic across the LAN/WAN interfaces without any processing.

Step 6 In the **Encapsulation** field, enter the VLAN ID that is to be assigned to traffic that leaves the WAE. The VLAN ID should be set to match the VLAN ID expected by the router.

For more information about the VLAN ID, see Configuring an IP Address on an Inline Interface, on page 180.

Step 7 From the **Load Interval** drop-down list, choose the interval, in seconds, at which to poll the interface for statistics and calculate throughput. The default is 30 seconds. (The **Load Interval** item is not shown for devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0.)

Step 8 Check the **Intercept all VLANs** check box to enable inline interception on the interface group. Inline interception is enabled by default when the WAE contains a Cisco WAE Inline Network Adapter, but must be explicitly enabled on devices with a Cisco Interface Module (see Enabling Inline Operation on WAEs, on page 173).

Step 9 In the **Exclude VLAN** field, enter a list of one or more VLAN ranges to exclude from optimization. You can enter the word native to exclude the native VLAN. Separate each VLAN range from the next with a comma. Alternatively, you can select VLAN ranges from a list by following these steps:

a) Click **Configure Include VLANs** when you know the list of VLANs that you want to include in inline interception. This button runs a script that prompts you for a comma-separated list of VLANs that you want to include. The script generates an inverse list of all the VLANs that should be excluded and then updates the window and puts the list into the **Exclude VLAN** field.

b) Click **Choose VLANs from the list** to choose VLAN ranges. The VLAN Range Assignments window appears, displaying the VLAN ranges that are defined. Defining VLAN ranges is described in Configuring VLANs for Inline Support, on page 182.

c) Choose the VLAN ranges to include or exclude:

d) Click **OK**. For devices using WAAS versions earlier than 5.0, click **Submit**.

Step 10 From the **Failover Timeout** drop-down list, choose **1**, **3**, **5**, or **10 seconds**. The default is **1 second**. This value sets the number of seconds after a failure event that the WAE waits for before beginning to operate in bypass mode. In Bypass mode, all the traffic received on either port of the interface group is forwarded out to the other port in the group.

This check box applies only to devices that use Cisco WAE Inline Network Adapters. For devices that use Cisco Interface Modules, the failover timeout is configured in the Inline Interception Settings window and does not appear in this window.

Step 11 Configure the **Speed** and **Mode** port settings as follows (these settings are not used for the interfaces on the Cisco Interface Module on a device using Cisco WAAS Version 5.0 or later, which uses auto sensing):

a) Uncheck the **AutoSense** check box, which is enabled by default.

b) From the **Speed** drop-down list, choose a transmission speed (10, 100, 1000, or 10000 Mbps). Choose 1000 Mbps for fiber Gigabit Ethernet interfaces on a Cisco Interface Module for devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0.

c) From the **Mode** drop-down list, choose a transmission mode (full-duplex or half-duplex). Choose full-duplex for fiber Gigabit Ethernet interfaces on a Cisco Interface Module for devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0.

Note We strongly recommend that you do not use half-duplex connections on WAEs or on routers, switches, or other devices. Half duplex impedes performance and should not be used. Check each Cisco WAE interface and port configuration on the adjacent device (router, switch, firewall, and WAE) to verify that full duplex is configured.

Step 12 In the **Address** field, enter an IP address for the inline interface, if you want to assign an IP address.

Step 13 In the **Netmask** field, enter a subnet mask for the inline interface.

Step 14 Enter up to four secondary IP addresses and corresponding subnet masks in the **Secondary Address** and **Secondary Netmask** fields.

Configuring multiple IP addresses allows the device to be present in more than one subnet and can be used to optimize response time because it allows the data to go directly from the Cisco WAAS device to the client that is requesting the information without being redirected through a router. The Cisco WAAS device becomes visible to the client because both are configured on the same subnet.

Step 15 In the **Default Gateway** field, enter the default gateway IP address. The **Default Gateway** field is not shown for devices running Cisco WAAS version 5.0 or later.

Step 16 (Optional) From the **Inbound ACL** drop-down list, choose an IP ACL to apply to inbound packets.

The drop-down list contains all the IP ACLs that you configured in the system.

Step 17 (Optional) From the **Outbound ACL** drop-down list, choose an IP ACL to apply to outbound packets.

Step 18 Under **IPv6 Settings**, you can manually assign an IPv6 address to the inline interface or select from the following options. If you select one of the following options, the IPv6 address field and subsequent secondary IPv6 address fields are not available.

- **Use Single Link Local**: A unicast address that is automatically configured on an interface using the link-local prefix FE80::/10 and the interface identifier in the modified EUI-64 format. Using this address configuration option is sufficient for nodes on a link to communicate.
- **Use Auto Config**: To auto-configure an IPv6 global unicast address on the interface as per RFC 4862.

Step 19 Enter up to four secondary IP addresses and corresponding subnet masks in the **Secondary Address** and **Secondary Netmask** fields.Configuring multiple IP addresses allows the device to be present in more than one subnet and can be used to optimize response time because it allows the data to go directly from the WAAS device to the client that is requesting the information without being redirected through a router. The Cisco WAAS device becomes visible to the client because both are configured on the same subnet.

Step 20 In the **Duplicate Address Detection Attempts** field enter a number between 0-600 to specify the number of attempts by which the duplicate address should be detected.

Step 21 Click **OK**. (For devices running Cisco WAAS versions earlier than 5.0, click **Submit**.)

Step 22 For Cisco WAAS Version 5.0 and later, choose **Configure** > **Network** > **Default Gateway** to configure the default gateway for an inline interface:

a) In the **Default Gateway** field, enter the default gateway IP address.

b) Click **Submit**.

To configure inline interception from the CLI, run the **interface InlineGroup** global configuration command.

Configuring Inline Operation on ANCs

Before you begin

This section describes how to enable and configure inline settings on WAAS devices configured as AppNav Controllers (ANCs). You can also use the AppNav Cluster wizard to configure an inline ANC and create an inline bridge interface, as described in Creating a New AppNav-XE Cluster with the AppNav Cluster Wizard in the chapter "Configuring Cisco AppNav."

To configure the inline settings on WAEs configured as application accelerators, see Enabling Inline Operation on WAEs, on page 173.

On WAVE-594/694/7541/7571/8541 devices that use Cisco AppNav Controller Interface Modules, the AppNav Controller Interface Module ports are configured by default for normal standalone operation. To use the device in inline mode, you must configure the ports for inline operation and create an inline bridge group. Enabling inline mode configures all the ports for inline operation.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*. (You cannot enable inline operation from device groups.)

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**.

The **Interception Configuration** window appears.

Step 3 To enable **Inline** mode, from the **Interception Method** drop-down list, choose **Inline**.

Step 4 To enable **Inline** mode and refresh the window with additional settings, click **Submit**.

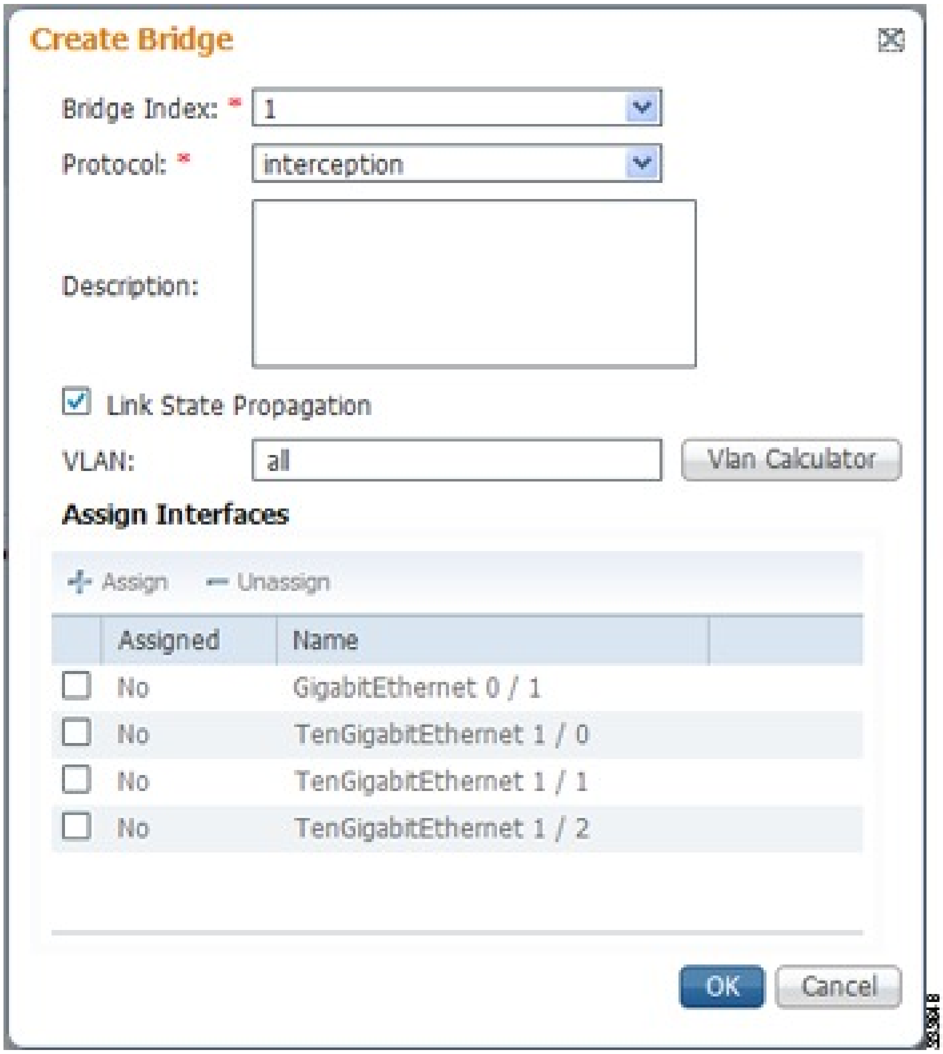
All the existing bridge groups are listed, showing the bridge group number, protocol, link state propagation setting, VLAN ranges, and included interfaces.

From this list, you can perform the following tasks:

- Edit the settings for a bridge group by choosing it, and clicking the **Edit** taskbar icon.
- Delete a bridge group by choosing it, and clicking the **Delete** taskbar icon.
- Create a new bridge group as described in the following steps.

Step 5 Click the **Create Bridge** taskbar icon.

Figure 33: Create Bridge window



Create Bridge

Bridge Index: * 1

Protocol: * interception

Description:

☑ Link State Propagation

VLAN: all

Assign Interfaces

	Assigned	Name
□	No	GigabitEthernet 0 / 1
□	No	TenGigabitEthernet 1 / 0
□	No	TenGigabitEthernet 1 / 1
□	No	TenGigabitEthernet 1 / 2

Step 6 From the **Bridge Index** drop-down list, choose the bridge group number.

Step 7 (Optional) In the **Description** field, enter a bridge group description.

Step 8 (Optional) Check the **Link State Propagation** check box to enable link state propagation. It is enabled by default.

Link state propagation means that if one interface in the inline bridge group is down, the system automatically shuts down the other interface to ensure that a network failover scheme is triggered.

Step 9 (Optional) Configure VLANs to include in interception. Initially, all the VLANS are included. To include or exclude specific VLAN ranges, follow these steps:

a) Click **Vlan Calculator**.

b) For each VLAN range that you want to include in interception, from the **Select Operation Type** drop-down list, choose **Add/Include**. In the **Vlan Range** field, enter a comma-separated list of one or more VLAN ranges to include. You can enter the word **native** to include the native VLAN.

c) For each VLAN range that you want to exclude from interception, from the **Select Operation Type** drop-down list, choose **Except/Exclude**. In the **Vlan Range** field, enter a comma-separated list of one or more VLAN ranges to exclude. You can enter the word native to exclude the native VLAN.

d) To save the your settings, click **OK**.

Step 10 In the **Assign Interfaces** pane, check the check box next to two interfaces that you want to assign to this bridge group, and then click the **Assign** taskbar icon. To unassign assigned interfaces, check each interface that you want to unassign, and click the **Unassign** taskbar icon. The bridge group can contain two physical or two port-channel interfaces, or a combination.

Step 11 To create the bridge group, click **OK**.

Configuring an IP Address on an Inline Interface

You can assign IP addresses to the inline group interfaces, but it is not required. You can assign a primary IP address and up to four secondary IP addresses, using the procedure described in Configuring Inline Interface Settings on WAEs, on page 175.

You can set an inline group interface as the primary interface on the WAE by using the Configure > Network > Network Interfaces window, in the **Primary Interface** drop-down list.

In scenarios where the primary interface for a WAE is set to an inline group interface and management traffic is configured on a separate IP address (either on a secondary IP address on the same inline group interface or on a built-in interface), configure the WAAS Central Manager to communicate with the WAE on the IP address designated for management traffic. Configure the WAE management interface settings with the **Configure > Network > Management Interface Settings** menu item. For Cisco WAAS versions earlier than Cisco WAAS Version 5.0, configure the WAE management traffic IP address in the *device-name* > **Activation** window, in the **Management IP** field.

If a WAE operating in inline mode is present in an 802.1Q VLAN trunk line between a switch and a router, and you are configuring the inline interface with an IP address, you must set the VLAN ID that is to be assigned to the traffic that leaves the WAE. The VLAN ID should be set to match the VLAN ID expected by the router.

Run the **encapsulation dot1Q interface** command to assign a VLAN ID, as follows:

```
(config)# interface inlineGroup 1/0
(config-if)# encapsulation dot1Q 100
```

This example shows how to assign VLAN ID 100 to the traffic leaving the WAE. The VLAN ID can range from 1 to 4094.

You can set the VLAN ID of the inline traffic by using the **encapsulation dot1Q** interface command or by using the Cisco WAAS Central Manager menu item **Configure > Interception > Interception Configuration** (see Configuring Inline Interface Settings on WAEs, on page 175).

If the VLAN ID that you set does not match the VLAN ID expected by the router subinterface, you may not be able to connect to the inline interface IP address.

The inline adapter supports only a single VLAN ID for each inline group interface. If you have configured a secondary address from a different subnet on an inline interface, you must have the same secondary address assigned on the router subinterface for the VLAN.

Using IEEE 802.1Q tunneling increases the frame size by 4 bytes when the tag is added. Therefore, you must configure all the switches through which the tunneled packet traverses to be able to process larger frames by increasing the device MTU to at least 1504 bytes.

Note When an Inline interface on a WAE configured with IPv6 address and dot1 q encapsulation, tries to communicate with an IPv6 default gateway, the communication fails. If the same device, configured with IPv4 address and dot1 Q encapsulation, tries to communicate with an IPv4 default gateway, the communication is successful. Note that when dot1Q encapsulation is disabled, the WAE (configured with either IPv6 or IPv4) can successfully reach the default gateway of the relevant IP type.

The following operating considerations apply to configuring IP addresses on the inline interfaces:

- This feature provides basic routable interface support and does not support the following additional features associated with the built-in interfaces: standby and port channel.
- If you have configured a WAE to use inline interfaces for all traffic, inline interception must be enabled; otherwise, the WAE will not receive any traffic.
- If you have configured a WAE to use the inline interfaces for all traffic, and it goes into mechanical bypass mode, the WAE become inaccessible through the inline interface IP address. Console access is required for device management when an inline interface is in bypass mode.
- If you have configured a WAE with an IP address on an inline interface, the interface can accept only traffic addressed to it and ARP broadcasts, and the interface cannot accept multicast traffic.
- In a deployment using the Hot Standby Router Protocol (HSRP) where two routers that participate in an HSRP group are directly connected through two inline groups, HSRP works for all the clients if the active router fails. However, this redundancy does not apply to the IP address of the WAE itself for management traffic, if management traffic is also configured to use the inline interface.

  If the active router fails, you will not be able to connect to the WAE inline IP address because the inline interface is physically connected to the failed router interface. You will be able to connect to the WAE through the second inline group interface that is connected to the standby router. If redundancy is needed for the IP address of the WAE itself for management traffic, we recommend that you use the IP addresses of the built-in interfaces rather than the inline interfaces.

Configuring VLANs for Inline Support

Before you begin

Initially, the WAE accepts traffic from all VLANs. You can configure the WAE to include or exclude traffic from certain VLANs; for excluded VLANs, traffic is bridged across the LAN/WAN interfaces in a group and is not processed.

Procedure

Step 1 From the WAAS Central Manager menu, choose **Configure** > **Platform** > **Vlans**.

The **Vlans** window appears, which lists the VLANs that are defined. From this list, you can perform the following tasks:

- Edit a VLAN by choosing it and clicking the **Edit** taskbar icon.
- Delete a VLAN by choosing it and clicking the **Delete** taskbar icon.
- Create a new VLAN as described in the following steps.

Step 2 Click the **Add VLAN** taskbar icon. The VLAN pane appears.

Step 3 In the **Name** field, enter a name for the VLAN list.

Step 4 In the **Ranges** field, enter a list of one or more VLAN ranges. Separate each VLAN range from the next with a comma (but no space). This list of VLAN ranges can be included or excluded from optimization when you configure the inline interface group, as described in Configuring Inline Interface Settings on WAEs, on page 175. You cannot specify the term native in this field.

Step 5 Click **OK**.

What to do next

This facility for creating VLAN lists is provided so that you can configure VLAN lists globally. You do not have to use this facility to configure VLANs for an inline interface. You can configure VLANs directly in the inline interface settings window, as described in Configuring Inline Interface Settings on WAEs, on page 175.

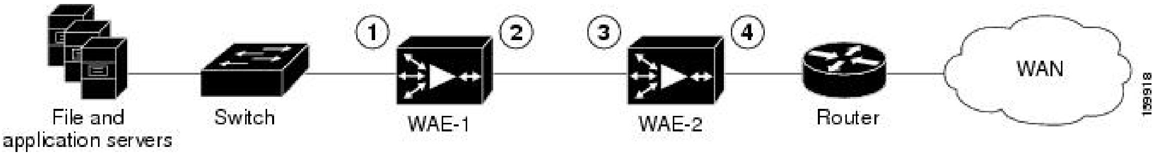
About Clustering Inline Cisco WAEs

You can serially cluster two WAE devices that are operating in inline mode to provide higher availability in the data center if a device fails. If the current optimizing device fails, the inline group shuts down, or the device becomes overloaded, the second WAE device in the cluster provides the optimization services. Deploying WAE devices in a serial inline cluster for scaling or load balancing is not supported.

Note Overload failover occurs on TFO overload, not overload of individual application accelerators, and it is intended for temporary overload protection. We do not recommend that you continually run a WAE in an overloaded state, frequently triggering overload failover.

A serial cluster consists of two WAE devices connected together sequentially in the traffic path. The WAN port of one device is connected to the LAN port of the next device, as shown in the following figure.

Figure 34: Inline Cluster



1	Inline LAN port on WAE-1	3	Inline LAN port on WAE-2
2	Inline WAN port on WAE-1	4	Inline WAN port on WAE-2

In a serial cluster, all the traffic between a switch and router passes through all the inline WAEs. In the above figure, connections are optimized by WAE-1. If WAE-1 fails, it bypasses the traffic and connections are then optimized by WAE-2.

The policy configuration of serially clustered WAEs should be the same. Additionally, we recommend that you use the same device for both the WAEs in the cluster.

When serially clustering inline WAEs, on each WAE, you must configure the address of the other WAE in the cluster as a nonoptimizing peer. This disables optimization between the two peer WAEs in the serial cluster, since you want optimization only between the WAE peers on each side of the WAN link. For information on how to disable optimization between peers, see Disabling Peer Optimization Between Serial Inline WAEs, on page 183.

Disabling Peer Optimization Between Serial Inline WAEs

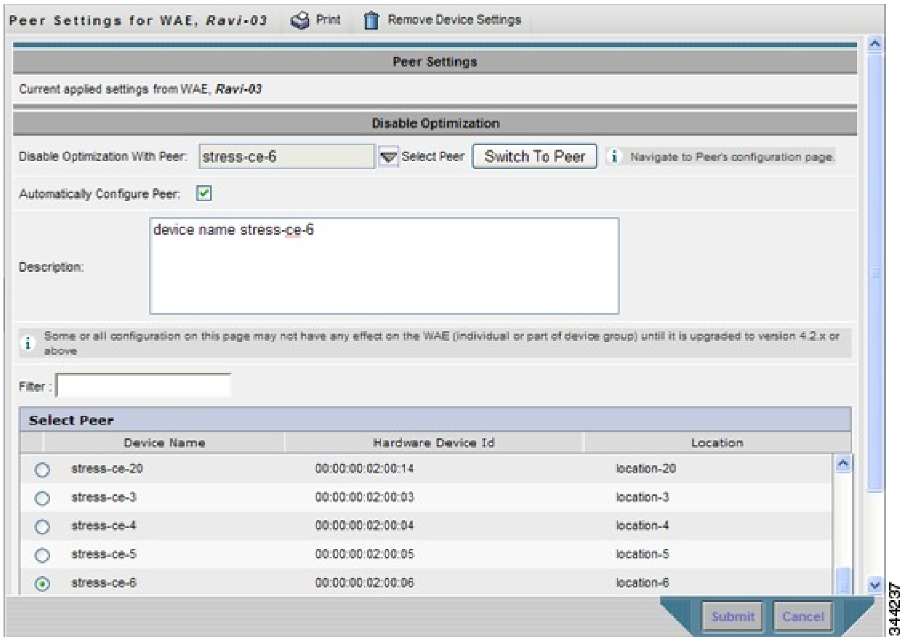
Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*. (You cannot configure peer settings from device groups.)

Step 2 Choose **Configure** > **Peers** > **Peer Settings**.

The **Peer Settings** window appears.

Figure 35: Peer Settings Window



Current applied settings from WAE, *Ravi-03*

Disable Optimization With Peer: stress-ce-6

Automatically Configure Peer: ☑

Description: device name stress-ce-6

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 4.2.x or above

Filter :

Select Peer

	Device Name	Hardware Device Id	Location
○	stress-ce-20	00:00:00:02:00:14	location-20
○	stress-ce-3	00:00:00:02:00:03	location-3
○	stress-ce-4	00:00:00:02:00:04	location-4
○	stress-ce-5	00:00:00:02:00:05	location-5
●	stress-ce-6	00:00:00:02:00:06	location-6

Step 3 Click the **Select Peer** triangle control to display the other WAEs that are registered with this Cisco WAAS Central Manager, in the lower part of the window (see the **Select Peer** pane).

Step 4 In the **Select Peer** area, click the radio button next to the serial peer of the current device. The peer device name appears in the **Disable Optimization With Peer** field.

To filter the device list, enter a string in the **Filter** field. As you enter characters, the device list is dynamically filtered to include only devices that have the filter string in their name or hardware device ID.

Step 5 Check the **Automatically Configure Peer** check box to allow the Cisco WAAS Central Manager to configure the other peer with a similar setting to disable optimization with the current device.

If you do not check this check box, you must manually configure the other peer to disable optimization with the current device. After you submit your changes, you can click **Switch to Peer** to go to this same configuration page for the peer device.

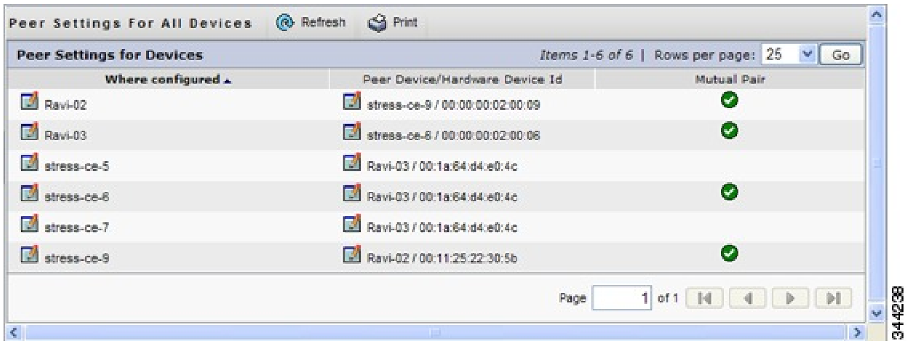
Step 6 In the **Description** field, enter a description for the peer. The default description is the device name of the peer.

Step 7 Click **Submit**.

Step 8 (Optional) To disable serial peer optimization from the CLI, run the **no peer device-id** global configuration command. To re-enable serial peer optimization, use the **peer device-id** global configuration command.

To view the status of all the serial cluster pairs registered with the Cisco WAAS Central Manager, from the Cisco WAAS Central Manager menu, choose **Configure** > **Global** > **Peer Settings**. The **Peer Settings** status window appears, as shown in the following figure.

Figure 36: Peer Settings For All Devices Window


Peer Settings For All Devices
Refresh
Print
Peer Settings for Devices
Items 1-6 of 6 | Rows per page: 25 Go
Page 1 of 1
344238

Where configured ▲	Peer Device/Hardware Device Id	Mutual Pair
Ravi-02	stress-ce-9 / 00:00:00:02:00:09	✓
Ravi-03	stress-ce-6 / 00:00:00:02:00:06	✓
stress-ce-5	Ravi-03 / 00:1a:64:d4:e0:4c	
stress-ce-6	Ravi-03 / 00:1a:64:d4:e0:4c	✓
stress-ce-7	Ravi-03 / 00:1a:64:d4:e0:4c	
stress-ce-9	Ravi-02 / 00:11:25:22:30:5b	✓

The **Peer Settings** window lists each WAE for which you have configured peer optimization settings. Verify that there are two entries for each serial cluster pair, both with a check mark in the **Mutual Pair** column. There should be an entry for each WAE in the pair, for example, the first and last entries in the figure.

If you see an entry without a check mark in the **Mutual Pair** column (like the third one in the figure), it indicates a WAE on which a serial peer is configured, but the peer is not similarly configured with the first device as its serial peer.

Configuring AppNav Interception

Before you begin

For WAEs that are a part of an AppNav deployment and are configured as WAAS nodes (WNs) in an AppNav Cluster, you must configure them to use the appnav-controller interception method. These WNs receive traffic only from the ANCs, not directly from routers. It is on the ANC devices that you configure an interception method, such as WCCP, PBR, or inline to intercept network traffic. For more information about an AppNav deployment, see the chapter "Configuring Cisco AppNav."

Note ISR-WAAS devices support only the AppNav Controller interception method.

If you create an AppNav Cluster by using the Central Manager wizard, or you add WNs to a cluster through the AppNav Clusters window, the Cisco WAAS Central Manager automatically configures WNs with the appnav-controller interception method. After the WN is added to a cluster, its interception method cannot be changed.

Procedure

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

Step 2 Choose **Configure** > **Interception** > **Interception Configuration**. The **Interception Configuration** window appears.

Step 3 From the **Interception Method** drop-down list, choose **appnav-controller** to enable the appnav-controller interception method.

Step 4 Click **Submit**.

CHAPTER 6

Configuring Network Settings

This chapter describes how to configure basic network settings such as configuring additional network interfaces to support network traffic, creating port channel and standby interfaces, configuring optimization on Cisco Wide Area Application Services (WAAS) Express interfaces, specifying a default gateway and Domain Name System (DNS) servers, enabling the Cisco Discovery Protocol (CDP).

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the WAAS Central Managers and Cisco Wide Area Application Engines (WAEs) in your network. The term WAE refers to WAE and WAVE appliances, and Cisco Virtual WAAS (vWAAS) instances.

For information on configuring a bridge group for inline interfaces on an AppNav Controller Interface Module, see Configuring Inline Operation on ANCs in the chapter "Configuring Traffic Interception," or use the AppNav Cluster wizard, as described in Creating a New AppNav-XE Cluster with the AppNav Cluster Wizard in the chapter "Configuring Cisco AppNav."

This chapter contains the following sections:

Configuring Network Interfaces

During initial setup, you choose an initial interface and either configure it for DHCP or gave it a static IP address, as described in the *Cisco Wide Area Application Services Quick Configuration Guide*.

The following devices support IPv4 only, IPv6 only and dual stack configuration.

- Cisco ENCS-5406/K9, ENCS-5406/K9, ENCS-5408/K9, ENCS-5412/K9
- Cisco vWAAS on VMware ESX and ESXi hypervisor, Cisco vWAAS on ISR-4451(kWAAS)
- Cisco WAAS Express

This section describes how to configure additional interfaces using options for redundancy, load balancing, and performance optimization and also to modify previously configured settings on interfaces.

This section contains the following topics:

We recommend that you use the Cisco WAAS Central Manager instead of the Cisco WAAS CLI to configure network settings. If you want to use the CLI, see the following commands in the *Cisco Wide Area Application Services Command Reference*: **interface**, **ip address**, **port-channel**, and **primary-interface** commands.

Network interfaces are named as follows on Cisco WAAS devices:

- ENCS-5406/K9, ENCS-5408/K9, ENCS-5412/K9: Have two inbuilt Ethernet interfaces named GigabitEthernet 1/0 and GigabitEthernet 2/0.
- ENCS-5406/K9, ENCS-5408/K9, ENCS-5412/K9: Have two inbuilt Ethernet interfaces named GigabitEthernet 0/0 and GigabitEthernet 0/1. Additional interfaces on the Cisco Interface Module and AppNav Controller Interface Module are named GigabitEthernet 1/0 to 1/11 or TenGigabitEthernet 1/0 to 1/3, depending on the number and type of ports.
- NME-WAE devices: Have an internal interface to the router that is designated 1/0, and an external interface that is designated 2/0.SM-SRE devices (Cisco WAAS versions earlier than Cisco WAAS Version 6.4.x).

Note We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Half duplex impedes performance and should not be used. Check each Cisco WAE interface and the port configuration on the adjacent device (router, switch, firewall, and WAE) to verify that full duplex is configured. When connecting an AppNav Controller to a Cisco Nexus 7000 Series switch, the interfaces on both devices must be set to the same autonegotiate setting: either both on or both off. If they are set differently, switch-link flapping may occur.

Note On Cisco ISR-WAAS devices, you cannot configure the following from the Cisco WAAS Central Manager: network interfaces, ip addresses (IPv4 or IPv6), routes, default gateway, DNS servers, and jumbo maximum transmission unit (MTU). Use the router CLI to configure these.

Note Layer 3 interfaces may drop bridge protocol data unit (BPDU) packets. However, this does not affect data traffic.

Note When a Cisco WAAS Central Manager and WAE are part of a dual stack configuration, the primary interface on the Cisco WAAS Central Manager must be configured with an IPv6 address. If this is not configured, then a device (configured with only an IPv6 address) fails to communicate with the Cisco WAAS Central Manager when it is registered to the Cisco WAAS Central Manager; and goes into the offline state.

Configuring a Standby Interface

Using this procedure, you can configure a logical interface called a standby interface. After you configure this standby interface, you must associate physical or port-channel interfaces with the standby interface in order to create a standby group. In the Cisco WAAS Central Manager, you can create a standby group by assigning two interfaces to the standby group and assigning one as primary.

Standby interfaces remain unused unless a member interface that is in use fails. When an in-use network interface fails (because of cable trouble, Layer 2 switch failure, or other failure), the other member interface of the standby group changes its state to in use and starts to carry traffic and take the load off the failed interface. With the standby interface configuration, only one interface is in use at a given time.

To configure standby interfaces, you must assign two physical or two port-channel interface members to a standby group. The following operating considerations apply to standby groups:

- A standby group consists of two physical or two port-channel interfaces. (If you are configuring a WAAS device running a version earlier than 5.0, both interfaces must be physical interfaces.)
- The maximum number of standby groups on a Cisco WAAS device is two. When using a Cisco AppNav Controller Interface Module, you can have up to three standby groups.
- A standby group is assigned a unique standby IP address, shared by all members of the group.
- Configuring the duplex and speed settings of the standby group member interfaces provides better reliability.
- IP ACLs can be configured on physical interfaces that are members of a standby group.
- One interface in a standby group is designated as the primary standby interface. Only the primary interface uses the group IP address.
- If the in-use interface fails, another interface in its standby group takes over and carries the traffic.
- If all the members of a standby group fail, and then one recovers, the WAAS software brings up the standby group on the operational interface.
- The primary interface in a standby group can be changed at runtime. (The default action is to pre-empt the currently in-use interface if a different interface is made primary.)
- If a physical interface is a member of a standby group, it cannot also be a member of a port channel.
- If a device has only two interfaces, you cannot assign an IP address to both a standby group and a port channel. On such a device, only one logical interface can be configured with an IP address.
- The member interfaces of a standby group can be connected to different switches if you use a VLAN tagging protocol and assign the same VLAN tag to each interface.
- You cannot include a built-in Ethernet port and a port on a Cisco Interface Module in the same standby group.

Configuring a standby interface differs, depending on the version of the Cisco WAAS device that you are configuring. See one of the following topics:

- Configuring a Standby Interface on a Device with Version 5.0 or Later, on page 190
- Configuring a Standby Interface on a Device Earlier than Version 5.0, on page 191

Configuring a Standby Interface on a Device with Version 5.0 or Later

To configure a standby interface for devices with Cisco WAAS Version 5.0 or later, follow these steps:

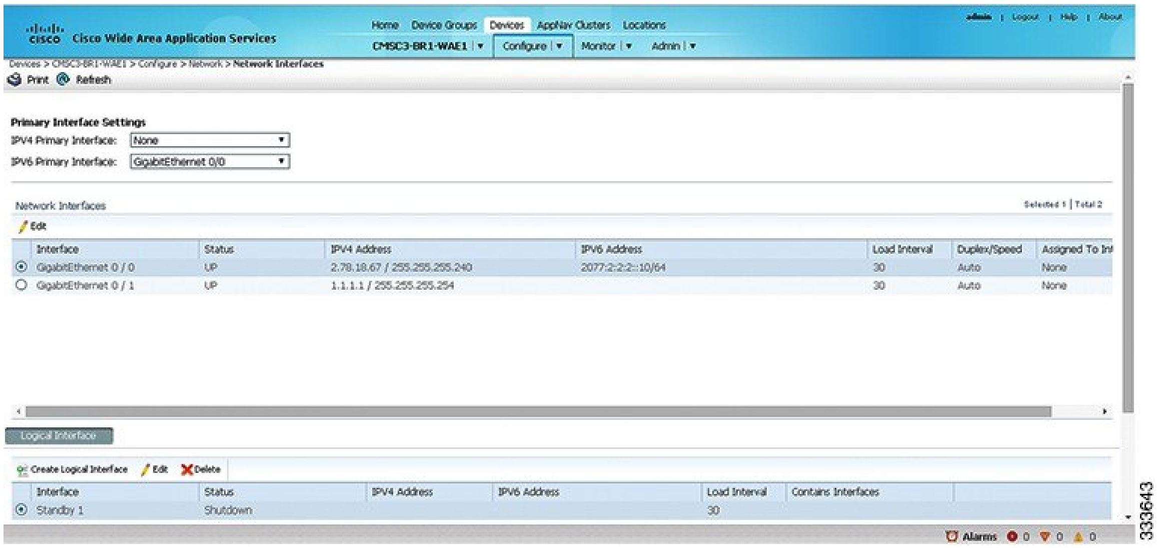
Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The **Network Interfaces** window for the device appears.

Figure 37: Network Interfaces for Device Window



Primary Interface Settings

IPV4 Primary Interface: None

IPV6 Primary Interface: GigabitEthernet 0/0

Network Interfaces — Selected 1 | Total 2

	Interface	Status	IPV4 Address	IPV6 Address	Load Interval	Duplex/Speed	Assigned To Int
●	GigabitEthernet 0 / 0	UP	2.78.18.67 / 255.255.255.240	2077:2:2:2::10/64	30	Auto	None
○	GigabitEthernet 0 / 1	UP	1.1.1.1 / 255.255.255.254		30	Auto	None

	Interface	Status	IPV4 Address	IPV6 Address	Load Interval	Contains Interfaces
●	Standby 1	Shutdown			30	

Step 3 In the taskbar of the lower area, click the **Create Logical Interface** icon.

The **Create Logical Interface** window appears.

Step 4 From the **Logical Interface Type** drop-down list, choose **Standby** and click **OK**.

The window refreshes with fields for configuring the standby group settings.

Step 5 From the **Standby Group Number** drop-down list, choose a group number for the interface.

Step 6 (Optional) From the **Bridge Group Number** drop-down list, choose a bridge virtual interface (BVI) group number with which to associate this standby interface, or **None**. For more information on BVI, see Configuring the Management Interface Settings, on page 208.

Note This configuration item is not supported on AppNav Controller Interface Module ports.

Step 7 (Optional) In the **Description** field, enter a description for the standby group.

Step 8 (Optional) Check the **Shutdown** check box to shut down the hardware interface. By default, this option is disabled.

Step 9 (Optional) From the **Load Interval** drop-down list, choose the interval, in seconds, at which to poll the interface for statistics and calculate throughput. The default is 30 seconds.

Step 10 In the **Address** field, specify the IP address of the standby group.

Step 11 In the **Netmask** field, specify the netmask of the standby group.

Step 12 Under **IPv6 Settings**, manually assign an IPv6 address to the primary interface or select from the following options. If you select one of the following options, the IPv6 address field and subsequent secondary IPv6 address fields are not available.

- **Use Link Local**: A unicast address that is automatically configured on an interface using the link-local prefix FE80::/10 and the interface identifier in the modified EUI-64 format. Using this address configuration option is sufficient for nodes on a link to communicate.
- **Use Auto Config**: To auto-configure an IPv6 global unicast address on the interface as per RFC 4862.

Step 13 In the **Duplicate Address Detection Attempts** field enter a number between 0-600 to specify the number of attempts by which the duplicate address should be detected.

Step 14 In the **Assign Interfaces** area, check the check boxes next to the two interfaces that you want to assign to this standby group and click the **Assign** taskbar icon. (To unassign any assigned interfaces, check the check box next to each interface that you want to unassign and click the **Unassign** taskbar icon.)

If you want to have two port-channel interfaces as members of the standby group, do not assign any interfaces here. When you create the port-channel interfaces, you assign the standby group number in that window.

Step 15 To assign one physical interface as the primary (active) interface in the standby group, ensure that it is the only interface that is checked, and then click the **Enable Primary** taskbar icon.

Step 16 Click **OK**.

Configuring a Standby Interface on a Device Earlier than Version 5.0

To configure a standby interface for devices with Cisco WAAS versions earlier than Cisco WAAS Version 5.0, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The **Network Interfaces** window for the device appears.

Step 3 In the taskbar, click the **Create New Interface** icon.

The **Creating New Network Interface** window appears.

Step 4 From the **Port Type** drop-down list, choose **Standby**.

The window refreshes with fields for configuring the standby group settings.

Step 5 From the **Standby Group Number** drop-down list, choose a group number for the interface.

Step 6 (Optional) In the **Description** field, enter a description for the standby group.

Step 7 In the **Address** field, specify the IP address of the standby group.

Step 8 In the **Netmask** field, specify the netmask of the standby group.

Step 9 (Optional) Check the **Shutdown** check box to shut down the hardware interface. By default, this option is disabled.

Step 10 In the **Default Gateway** field, enter the default gateway IP address. If an interface is configured for DHCP, then this field is read only.

Step 11 (Optional) From the **Bridge Group Number** drop-down list, choose a bridge virtual interface (BVI) group number with which to associate this standby interface, or choose **None**. For more information on BVI, see Configuring the Management Interface Settings, on page 208.

Step 12 Click **Submit**.

Step 13 Configure the physical interface members, as described in Assigning Physical Interfaces to a Standby Group, on page 192.

What to do next

Note After you create the standby interface, assign two physical interfaces to the standby group.

Assigning Physical Interfaces to a Standby Group

After you configure a logical standby interface for a device with a Cisco WAAS version earlier than 5.0, configure the standby group by assigning physical interfaces to the standby group and setting one physical interface as the primary standby interface. The primary interface in the standby group uses the standby group IP address. You must have a standby interface configured before you can set it as primary. (See Configuring a Standby Interface, on page 189.)

You can assign an interface to a standby group only if the interface does not have an IP address assigned, and uses the IP address of the standby group.

Note Removing a physical interface from standby group 2 on all Cisco WAAS device models may cause network disruption for up to 30 seconds. Additionally, removing a physical interface from standby group 1 on device model WAE-612 may cause network disruption for up to 30 seconds. The best practice is to make such changes when traffic interception is disabled, or at a time when traffic disruption is acceptable.

To associate an interface with a standby group and set it as the primary standby interface, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**. The **Network Interfaces** window for the device appears.

Step 3 Click the **Edit** icon next to the physical interface that you want to assign to a standby group. The **Interface Settings** window appears.

Note Choose a physical interface, not a logical interface (standby, port channel, or BVI), in this step.

Step 4 Complete the following steps to assign the interface to a standby group and specify it as the primary standby interface:

a) In the **Port Type To Assign** drop-down list, choose **Standby**.

b) Check either the **Join Standby Group 1** or the **Join Standby Group 2** check box. (Only one check box is shown if only one standby interface has been defined.)

c) (Optional) Check the **Standby Primary** check box if you want this physical interface to be the primary (active) interface in the standby group.

Step 5 Click **Submit**.

Configuring Multiple IP Addresses on a Single Interface

You can configure up to four secondary IP addresses on a single interface. This configuration allows the device to be present in more than one subnet and can be used to optimize the response time because it allows the data to go directly from the Cisco WAAS device to the client that is requesting the information without being redirected through a router. The Cisco WAAS device becomes visible to the client because both are configured on the same subnet.

Configuring multiple IP addresses is not supported on AppNav Controller Interface Module ports.

To configure multiple IP addresses on a single interface, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**. The **Network Interfaces** listing window appears.

Step 3 Choose the physical interface that you want to modify and click the **Edit** taskbar icon. (For devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0, click the **Edit** icon next to the interface.)

The **Interface Settings** window appears.

Note Do not choose a standby or port-channel interface in this step. You cannot configure multiple IP addresses on these types of interfaces.

Step 4 In the **Secondary Address** and **Secondary Netmask** fields 1 through 4, enter up to four different IP addresses and secondary netmasks for the interface.

Step 5 Click **OK**. (For devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0, click **Submit**).

Modifying Ethernet Interface Settings

This section contains the following topics:

Modifying Physical Ethernet Interface Settings

To modify the settings of a physical Ethernet interface, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The **Network Interfaces** window appears, listing the configured network interfaces.

Note On NME-WAE devices, the internal interface to the router is designated slot 1, port 0, and the external interface is designated slot 2, port 0. For NME-WAE configuration details, see the document Configuring Cisco WAAS Network Modules for Cisco Access Routers. On ISR-WAAS devices you cannot configure the network interfaces from the Cisco WAAS Central Manager.

Step 3 Choose the physical interface that you want to modify, and click the **Edit** taskbar icon. (For devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0, click the **Edit** icon next to the interface.)

The **Interface Settings** window appears, displaying the interface configurations on a particular slot and port. The interface type, slot, and port are determined by the hardware.

Note When configuring the internal interface (GigabitEthernet 1/0) on an NME-WAE device, you cannot change the following fields or check boxes: Port Channel Number, AutoSense, Speed, Mode, Address, Netmask, Use DHCP, and Standby Group. If you attempt to change these values, the Central Manager displays an error when you click OK. These settings for the internal interface can be configured only through the host router CLI. For NME-WAE details, see the document Configuring Cisco WAAS Network Modules for Cisco Access Routers .

Step 4 (Optional) In the **Description** field, enter a description for the interface.

Step 5 (Optional) Check the **Use CDP** check box to enable the Cisco Discovery Protocol (CDP) on an interface.

When enabled, CDP obtains protocol addresses of neighboring devices and discovers the platform of those devices. It also shows information about the interfaces used by your router.

Configuring CDP from the CDP Settings window enables CDP globally on all the interfaces. For information on configuring CDP settings, see Configuring CDP Settings, on page 214.

Step 6 (Optional) Check the **Shutdown** check box to shut down the hardware interface.

Step 7 (Optional) From the **Load Interval** drop-down list, choose the interval, in seconds, at which to poll the interface for statistics and calculate throughput. The default is 30 seconds. (The **Load Interval** item is not shown for devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0.)

Step 8 (Optional) Check the **AutoSense** check box to set the interface to autonegotiate the speed and mode. (This setting is not available on interfaces on some Cisco Interface Modules.)

Checking this check box disables the manual **Speed** and **Mode** drop-down list settings.

Note When autosense is on, manual configurations are overridden. You must reboot the Cisco WAAS device to start autosensing.

Step 9 (Optional) Manually configure the interface transmission speed and mode settings as follows (these settings are not available on interfaces on some Cisco Interface Modules):

a) Uncheck the **AutoSense** check box.
b) From the **Speed** drop-down list, choose a transmission speed (10, 100, 1000, or 10000 Mbps). You must choose 1000 Mbps for fiber Gigabit Ethernet interfaces on a Cisco Interface Module.
c) From the **Mode** drop-down list, choose a transmission mode (**full-duplex** or **half-duplex**). You must choose full-duplex for fiber Gigabit Ethernet interfaces on a Cisco Interface Module. This configuration item is not supported on AppNav Controller Interface Module ports.

   Full-duplex transmission allows data to travel in both directions at the same time through an interface or a cable. A half-duplex setting ensures that data travels only in one direction at any given time. Although full duplex is faster, the interfaces sometimes cannot operate effectively in this mode. If you encounter excessive collisions or network errors, you may configure the interface for half duplex rather than full duplex.

Note We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Half duplex impedes performance and should not be used. Check each Cisco WAE interface and the port configuration on the adjacent device (router, switch, firewall, and WAE) to verify that full duplex is configured.

Step 10 Specify a value (in bytes) in the MTU field to set the interface MTU size.

Consider the following guidelines for specifying the MTU size:

- The range is 576 to 1500 bytes. The MTU is the largest size of IP datagram that can be transferred using a specific data link connection.
- If the interface has an IPv6 configuration, the MTU range is between 1280-1500 bytes.
- The Cisco WAAS system automatically adjusts the maximum segment size (MSS) to match the advertised MSS of the client or server for each connection. The Cisco WAAS system uses the lower of 1432 or the MSS value advertised by the client or server.

Note A WN may go offline from the Cisco WAAS Central Manager if there is an MTU change in the packet path. To remedy this scenario, change the MSS to 1314.

- The MTU field is not editable if the interface is assigned to a standby or port-channel group, or if a system jumbo MTU is configured.

Step 11 (Optional) Check the Use DHCP check box to obtain an interface IP address through DHCP. Checking this box hides the IP address and Netmask fields. (For devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0, these fields are not hidden, but are disabled.) This configuration item is not supported on AppNav Controller Interface Module ports.

Optionally, supply a hostname in the Hostname field and a client ID in the **Client Id** field.

Step 12 In the **Address** field, enter a new IP address to change the interface IP address.

Step 13 In the **Netmask** field, enter a new netmask to change the interface netmask.

Step 14 (Optional) Enter up to four secondary IP addresses and corresponding subnet masks in the **Secondary Address** and **Secondary Netmask** fields. These fields are not supported on AppNav Controller Interface Module ports.

Configuring multiple IP addresses allows the device to be present in more than one subnet and can be used to optimize the response time because it allows the data to go directly from the Cisco WAAS device to the client that is requesting the information without being redirected through a router. The Cisco WAAS device becomes visible to the client because both are configured on the same subnet.

Step 15 In the **Default Gateway** field, enter the default gateway IP address. If an interface is configured for DHCP, this field is read only. (The **Default Gateway** field is not shown for devices running Cisco WAAS versions 5.0 or later; configure it as described in Configuring the Default Gateway, on page 198.)

Step 16 (Optional) From the **Inbound ACL** drop-down list, choose an IP ACL to apply to inbound packets.

The drop-down list contains all the IP ACLs that you configured in the system.

Step 17 (Optional) From the **Outbound ACL** drop-down list, choose an IP ACL to apply to outbound packets.

Step 18 Under **IPv6 Settings**, manually assign an IPv6 address to the primary interface or select from the following options. If you select one of the following options, the IPv6 address field and subsequent secondary IPv6 address fields are not available.

- **Use Link Local**: A unicast address that is automatically configured on an interface using the link-local prefix FE80::/10 and the interface identifier in the modified EUI-64 format. Using this address configuration option is sufficient for nodes on a link to communicate.
- **Use Auto Config**: To auto-configure an IPv6 global unicast address on the interface as per RFC 4862.
- **Use DHCP**: To obtain an interface IP address through DHCP.

Step 19 In the **Duplicate Address Detection Attempts** field enter a number between 0-600 to specify the number of attempts by which the duplicate address should be detected.

Step 20 Click **OK**. (For devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0, click **Submit**.)

Changing the interface transmission speed, duplex mode, or MTU may cause network disruption for up to 30 seconds. The best practice is to make such changes when traffic interception is disabled or at a time when traffic disruption is acceptable.

Configuring Flow Control on 1 GB/s and Faster Ethernet Ports

To configure flow control for 1 GB/s and faster Ethernet ports, follow these steps:

Before you begin

For Ethernet ports that run at 1 Gb/s or faster, you can enable or disable the port's ability to send and receive flow-control pause frames. For Ethernet ports that run slower than 1 Gb/s, you can enable or disable only the port's ability to receive flow-control pause frames.

Note We recommend that you enable flow control on the Nexus 7000 and 6500 Series models when WAAS IOM onboard NIC are directly attached to the Nexus 7000 and 6500 Series models, and input packet drops are seen.

There are three options for enabling flow control for the local port:

- Fully enable the local port to send or receive frames regardless of the flow-control setting of the remote port.
- Set the local port to use the same setting you have specified for the remote port.
- Set a combination of the two states for the local and remote ports.

Note If you enable flow control on both the local and the remote Ethernet port, or you set a specified flow control of the remote port only, or set a combination of these states, flow control is enabled for those ports.

Note For Ethernet ports that run at 10 GB/s or faster, you cannot used the specified state for the send/receive parameter.

Before you configure flow control, verify these conditions:

- Verify that the remote port that has the corresponding setting for the local port has the flow control that you need.
- If you want the local port to send flow-control pause frames, verify that the remote port has a **Receive** parameter set to **On** or **Desired**.
- If you want the local port to receive flow-control frames, verify that the remote port has a **Send** parameter set to **On** or **Desired**.
- If you do not want to use flow control, set the remote port's **Send** and **Receive** parameters to **Off**.

Procedure

Step 1 Enter **Configuration** mode for the terminal, using the config terminal command.

Step 2 Specify an Ethernet interface to configure, using the interface ethernet slot/port command.

The interface ethernet slot/port command enters the terminal into **Interface Configuration** mode.

Step 3 Specify the flow-control setting for ports, using the flowcontrol command.

Parameters for this command are send/receive and desired/on/off.

- You can set the **Send** parameter only for ports running at 1000 MB/s or faster.
- You can set the **Receive** parameter for ports running at any speed.

Step 4 Display the interface status, using the show interface gigabitEthernet slot/port command.

The interface status includes the flow-control parameters.

The following is sample output from the show interface gigabitEthernet slot/port command:

```
#show interface gigabitEthernet 0/1
Ethernet Address                    : 50:3d:e5:9d:1c:ef
Internet Address                     : --
Netmask                             : --
Admin State                         : Up
Operation State                     : Running
Maximum Transfer Unit Size          : 1500
Input Errors                        : 2
Input Packets Dropped               : 41967568
Packets Received                    : 218840605830
Output Errors                       : 0
Output Packets Dropped              : 0
Load Interval                       : 30
Input Throughput                    : 364402648 bits/sec, 45090 packets/sec
Output Throughput                   : 191939420 bits/sec, 23974 packets/sec
Packets Sent                        : 161861463575
```

Step 5 To display the flow control status for all Ethernet ports, run the **show interface flowcontrol** command.

Step 6 To exit **Interface** mode, run the **exit** command.

Step 7 (Optional) To copy the running configuration to the startup configuration, run the **copy running-config startup-config** command.

Configuring the Default Gateway

Before you begin

Configuring the default gateway is used for Cisco WAAS devices running Cisco WAAS Version 5.0 or later.

Procedure

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

Step 2 Choose **Configure** > **Network** > **Default Gateway**.

The **Default Gateway** window appears with fields for IPv4 and IPv6.

Step 3 In the **Default Gateway** field, enter the default gateway IP address, either IPv4 or IPv6 address.

Step 4 Click **Submit**.

To configure a default gateway from the CLI, run the **ip default-gateway** global configuration or the ipv6 default-gateway address command.

On Cisco WAAS devices running versions earlier than Cisco WAAS versions earlier than 5.0, the default gateway should be configured within the interface settings for each interface.

Note On ISR-WAAS devices, you cannot configure the default gateway from the Cisco WAAS Central Manager.

Configuring Port-Channel Settings

The Cisco WAAS software supports grouping of up to four (eight on AppNav Controller Interface Modules) physical network interfaces into one logical interface called a port channel. After you configure this port-channel interface, you must associate physical interfaces with the port channel.

You can configure up to four port-channel interfaces (seven on AppNav Controller Interface Modules). This capability also provides interoperability with Cisco routers, switches, and other networking devices or hosts supporting EtherChannel, load balancing, automatic failure detection, and recovery based on each interface's current link status. EtherChannel is also referred to as a port channel.

You can use a port channel in standby interface, or as a member of an inline bridge group on an AppNav Controller Interface Module. For more information on configuring a BVI, see Configuring the Management Interface Settings, on page 208. The following operating considerations apply to a port-channel virtual interface:

- A physical interface can be a member of a port channel or a standby group, but not both.
- You cannot assign an IP address to both a port channel and a standby group. Only one logical interface can be configured with an IP address.
- All port-channel member interfaces must have the same port bandwidth.

- Port-channel settings are not applicable to vWAAS devices.
- You cannot include a built-in Ethernet port and a port on a Cisco Interface Module in the same port-channel interface.

Note You must disable autoregistration if the device has only two interfaces and both device interfaces are configured as port-channel interfaces.

Configuring a port-channel interface differs, depending on the version of the WAAS device that you are configuring. See one of the following topics:

- Configuring a Port-Channel Interface on a Device with Cisco WAAS Version 5.0 or Later, on page 199
- Configuring a Port-Channel Interface on a Device Earlier than Cisco WAAS Version 5.0, on page 200

Configuring a Port-Channel Interface on a Device with Cisco WAAS Version 5.0 or Later

To configure a port-channel interface for devices with Cisco WAAS Version 5.0 or later, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The **Network Interfaces** window for the device appears.

Step 3 In the taskbar of the lower area, click the **Create Logical Interface** icon.

The **Create Logical Interface** window appears.

Step 4 From the **Logical Interface Type** drop-down list, choose **PortChannel** and click **OK**. The window refreshes with fields for configuring the port-channel interface settings.

Step 5 From the **Port Channel Number** drop-down list, choose a number for the interface.

Step 6 (Optional) From the **Bridge Group Number** drop-down list, choose a bridge group number with which to associate this interface, or choose **None**. The bridge group number can be associated with a BVI or an inline bridge group defined on an AppNav Controller.

Step 7 (Optional) From the **Standby Group Number** drop-down list, choose a standby group number with which to associate this interface, or choose **None**.

You must create the standby group with no assigned interfaces before it appears as a choice in this list.

Step 8 (Optional) In the **Description** field, enter a description for the interface.

Step 9 (Optional) Check the **Shutdown** check box to shut down the hardware interface. By default, this option is disabled.

If you plan to assign this port-channel interface to a standby interface, check this check box.

Step 10 (Optional) From the **Load Interval** drop-down list, choose the interval, in seconds, at which to poll the interface for statistics and calculate throughput. The default is 30 seconds.

Step 11 In the **Address** field, specify the IP address of the interface.

If you are assigning this port-channel interface to a standby group, do not configure an IP address or netmask. The standby group supplies the IP address and netmask.

Step 12 In the **Netmask** field, specify the netmask of the interface.

Step 13 (Optional) From the **Inbound ACL** drop-down list, choose an IP ACL to apply to inbound packets.

The drop-down list contains all the IP ACLs that you configured in the system.

Step 14 (Optional) From the **Outbound ACL** drop-down list, choose an IP ACL to apply to outbound packets.

Step 15 Under **IPv6 Settings**, manually assign an IPv6 address to the primary interface or select from the following options. If you select one of the following options, the IPv6 address field and subsequent secondary IPv6 address fields are not available.

- **Use Link Local**: A unicast address that is automatically configured on an interface using the link-local prefix FE80::/10 and the interface identifier in the modified EUI-64 format. Using this address configuration option is sufficient for nodes on a link to communicate.
- **Use Auto Config**: To auto-configure an IPv6 global unicast address on the interface as per RFC 4862.

Step 16 In the **Duplicate Address Detection Attempts** field enter a number between 0-600 to specify the number of attempts by which the duplicate address should be detected.

Step 17 In the **Assign Interfaces** area, click the check box next to the interfaces that you want to assign to this port channel and click the **Assign** taskbar icon. To unassign assigned interfaces, check the check box next to each interface that you want to unassign and click the **Unassign** taskbar icon.

If you plan to assign this port-channel interface to a standby interface, do not assign interfaces until after the port channel is assigned to the standby interface.

Step 18 Click **OK**.

Configuring a Port-Channel Interface on a Device Earlier than Cisco WAAS Version 5.0

To configure a port-channel interface for devices running Cisco WAAS versions earlier than 5.0, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The **Network Interfaces** window appears, listing all the interfaces for the chosen device.

Step 3 In the taskbar, click the **Create New Interface** icon.

The **Creating New Network Interface** window appears.

Step 4 From the **Port Type** drop-down list, choose **PortChannel**.

The window refreshes and provides fields for configuring the network interface settings.

Step 5 From the **Port Channel Number** drop-down list, choose the number of the port-channel interface. Up to four port channels are supported, depending on the Cisco WAAS device model and installed interface module.

Step 6 (Optional) In the **Description** field, enter a description for the port channel.

Step 7 (Optional) Check the **Shutdown** check box to shut down this interface. By default, this option is disabled.

Step 8 In the **Default Gateway** field, enter the default gateway IP address.

Step 9 In the **Address** field, specify the IP address of the interface.

Step 10 In the **Netmask** field, specify the netmask of the interface.

Step 11 (Optional) From the **Inbound ACL** drop-down list, choose an IP ACL to apply to inbound packets.

The drop-down list contains all the IP ACLs that you configured in the system.

Step 12 (Optional) From the **Outbound ACL** drop-down list, choose an IP ACL to apply to outbound packets.

Step 13 Click **Submit**.

Step 14 Configure the physical interface members as described in Assigning Physical Interfaces to a Port Channel, on page 201.

What to do next

Note After you create the port-channel interface, assign physical interfaces to the port channel.

Assigning Physical Interfaces to a Port Channel

To add an interface to a port channel, follow these steps:

Before you begin

After you have configured a logical port-channel interface, you must assign multiple physical interfaces to the port channel. You can assign up to four physical interfaces to one port-channel interface, depending on the Cisco WAAS device.

You can assign an interface to a port channel only if the interface does not have an IP address assigned, and uses the IP address of the port channel.

You cannot combine built-in Ethernet ports with ports on a Cisco Interface Module into the same port-channel interface.

Note Removing a physical interface from a port channel on device model WAE-612 may cause network disruption for up to 30 seconds. The best practice is to make such changes when traffic interception is disabled or at a time when traffic disruption is acceptable.

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The **Network Interfaces** window for the device appears.

Step 3 Click the **Edit** icon next to the physical interface that you want to assign to a port channel. The Modifying Network Interface window appears.

Choose a physical interface, not a logical interface (standby, port channel, or BVI), in this step.

Step 4 Complete the following steps to assign the interface to a port channel:

a) From the **Port Type To Assign** drop-down list, choose **PortChannel**.

b) From the **Port Channel Number** drop-down list, choose the number of the port channel to which you want to add the physical interface.

Step 5 Click **Submit**.

Configuring a Load-Balancing Method for Port-Channel Interfaces

Before you begin

Before you configure load balancing, ensure that you have configured the port-channel settings described in Configuring Port-Channel Settings, on page 198.

Procedure

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

Step 2 Choose **Configure** > **Network** > **Port Channel**.

Step 3 From the **Load Balancing Method** drop-down list, choose a load-balancing method:

- **src-dst-ip-port**: The distribution function is based on a combination of source and destination IP addresses and ports. This load-balancing method is available only on devices running Version 4.4.1 and later.
- **src-dst-ip**: The distribution function is based on a combination of source and destination IP addresses. This load-balancing method is available only on devices running Cisco WAAS Version 5.0.1 and later.
- **round-robin**: Round robin allows traffic to be distributed evenly among all the interfaces in the channel group. This load-balancing method is available only on devices running Cisco WAAS versions earlier than Cisco WAAS Version 4.4.1.

Step 4 Click **Submit**.

Step 5 (Optional) To configure a load-balancing method from the Cisco WAAS CLI, run the **port-channel** global configuration command.

To configure devices running previous versions of Cisco WAAS, you can configure a device group with a load-balancing method supported only by previous WAAS software versions.

When viewing the **Port Channel Settings** window for Cisco WAAS Version 4.4.1 or later for a device that gets its settings from such a device group, you may see an unsupported load-balancing method listed. However, a Cisco WAAS device running Cisco WAAS Version 4.4.1 or later device supports *only* the load-balancing methods as described above, regardless of what the device group or device configuration window shows for the setting.

Configuring Interfaces for DHCP

To enable an interface for DHCP, follow these steps:

Before you begin

Consider the following guidelines for configuring interfaces for DHCP:

- You must disable autoregistration before you can manually configure an interface for DHCP.
- A Cisco WAAS device sends its configured client identifier and hostname to the DHCP server when requesting network information. You can configure DHCP servers to identify the client identifier information and the hostname information that the Cisco WAAS device is sending and then to send back the specific network settings that are assigned to the Cisco WAAS device.

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The **Network Interfaces** listing window appears.

Step 3 Choose the physical interface that you want to modify and click the **Edit** taskbar icon. (For devices running Cisco WAAS version earlier than Cisco WAAS Version 5.0, click the **Edit** icon next to the interface.)

The **Interface Settings** window appears.

Note Do not choose a logical interface (standby, port channel, or BVI) in this step, because you cannot configure DHCP on a logical interface. In addition, do not choose the internal interface (GigabitEthernet 1/0) on an NME-WAE module, because this interface can be configured only through the host router CLI. For NME-WAE details, see the document Configuring Cisco WAAS Network Modules for Cisco Access Routers.

Step 4 Check the **Use DHCP** check box.

When this check box is checked, the IP address and netmask fields are disabled.

Step 5 In the **Hostname** field, specify the hostname for the Cisco WAAS device or other device.

Step 6 In the **Client ID** field, specify the configured client identifier for the device.

The DHCP server uses this identifier when the Cisco WAAS device requests the network information for the device.

Step 7 Click **Submit**.

Modifying Virtual Interface Settings for a vWAAS Device

To modify the settings of an existing Cisco vWAAS interface, follow these steps:

Procedure

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

Note On Cisco ISR-WAAS devices, you cannot configure the virtual interface settings from the Cisco WAAS Central Manager.

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The Network Interfaces window appears, listing the network interfaces configured.

Note Certain values (including autosense) are not applicable to a Cisco vWAAS interface.

Step 3 Choose the interface that you want to modify and click the **Edit** taskbar icon. (For devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0, click the **Edit** icon next to the interface.)

The **Interface Settings** window appears, displaying the interface configurations on a particular slot and port.

Note Interface configurations for slot, port, and port type are set for virtual interfaces during initial startup, or by using the Cisco WAAS CLI. Some of the fields in the window (port-channel number, autosense, speed, mode, and standby-related fields) are not available because they are not applicable.

Step 4 (Optional) In the **Description** field, enter a description for the interface.

Step 5 (Optional) Check the **Use CDP** check box to enable the Cisco Discovery Protocol (CDP) on an interface.

When enabled, CDP obtains protocol addresses of neighboring devices and discovers the platform of those devices. It also shows information about the interfaces used by your router.

Configuring CDP from the **CDP Settings** window enables CDP globally on all the interfaces. For information on configuring CDP settings, see Configuring CDP Settings, on page 214.

Step 6 (Optional) Check the **Shutdown** check box to shut down the virtual interface.

Step 7 (Optional) From the **Load Interval** drop-down list, choose the interval, in seconds, at which to poll the interface for statistics and calculate throughput. The default is **30 seconds**. (The **Load Interval** item is not shown for devices using Cisco WAAS versions earlier than Cisco WAAS Version 5.0.)

Step 8 Specify a value (in bytes) in the **MTU** field to set the interface MTU size.

The range is **576** to **1500** bytes. The MTU is the largest size of IP datagram that can be transferred using a specific data link connection.

If the interface has a IPv6 configuration, the MTU range is between **1280** to **1500** bytes.

Note The MTU field is not editable if a system jumbo MTU is configured.

Step 9 Check the **Use DHCP** check box to obtain an interface IP address through DHCP. Checking this check box hides the IP address and Netmask fields. (For devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0, these fields are not hidden but are disabled.)

a) (Optional) In the **Hostname** field, specify the hostname for the Cisco WAAS device or other device.
b) (Optional) In the **Client Id** field, specify the configured client identifier for the device. The DHCP server uses this identifier when the Cisco WAAS device requests the network information for the device.

Step 10 In the **Address** field, enter a new IP address to change the interface IP address.

Step 11 In the **Netmask** field, enter a new netmask to change the interface netmask.

Step 12 In the **Default Gateway** field, enter the default gateway IP address. The gateway interface IP address should be in the same network as one of the device's network interfaces. If an interface is configured for DHCP, this field is read only. (The Default Gateway field is not shown for devices running Cisco WAAS Version 5.0 or later; instead, configure it, as described in Configuring the Default Gateway, on page 198.)

Step 13 (Optional) From the **Inbound ACL** drop-down list, choose an IP ACL to apply to inbound packets.

The drop-down list contains all the IP ACLs that you configured in the system.

Step 14 (Optional) From the **Outbound ACL** drop-down list, choose an IP ACL to apply to outbound packets.

Step 15 Under **IPv6 Settings**, manually assign an IPv6 address to the primary interface or select from the following options.

- **Use Link Local**: A unicast address that is automatically configured on an interface using the link-local prefix FE80::/10 and the interface identifier in the modified EUI-64 format. Using this address configuration option is sufficient for nodes on a link to communicate.
- **Use Auto Config**: To auto-configure an IPv6 global unicast address on the interface as per RFC 4862.
- **Use DHCP**: To obtain an interface IP address through DHCP.

Step 16 In the **Duplicate Address Detection Attempts** field enter a number between **0** to **600** to specify the number of attempts by which the duplicate address should be detected.

Step 17 Click **OK**. (For devices running Cisco WAAS versions earlier than Cisco WAAS Version 5.0, click **Submit**.)

Enabling or Disabling Optimization on Cisco WAAS Express Interfaces

Before you begin

Cisco WAAS Express device interfaces are configured by using the router CLI, not through the Cisco WAAS Central Manager. However, you can enable or disable WAAS optimization on the available interfaces on the router.

Procedure

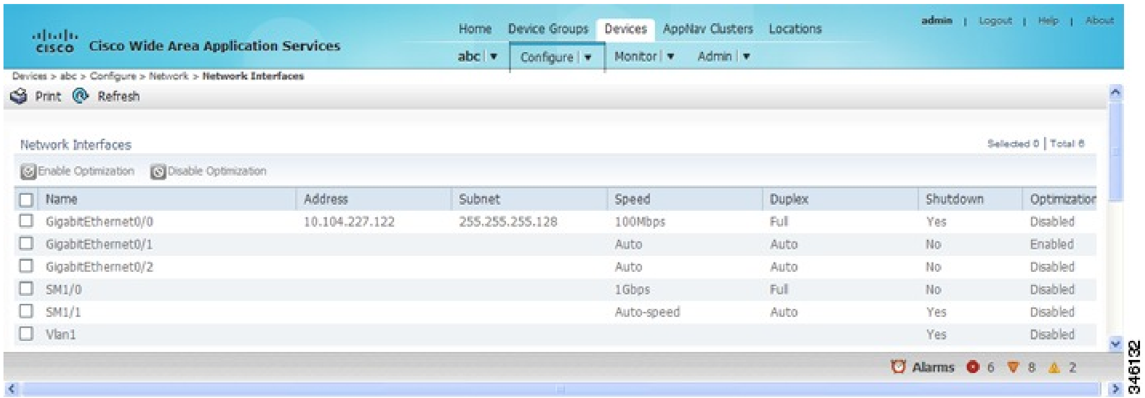
Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *WAAS-Express-device-name* or **Device Groups** > *WAAS-Express-device-group-name*.

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The **Network Interfaces** window appears and lists the available interfaces.

Note Loopback interfaces are not included because they are not valid interfaces for optimization. Null, Virtual-Access, NVI, and Embedded-Service interfaces are also not supported.

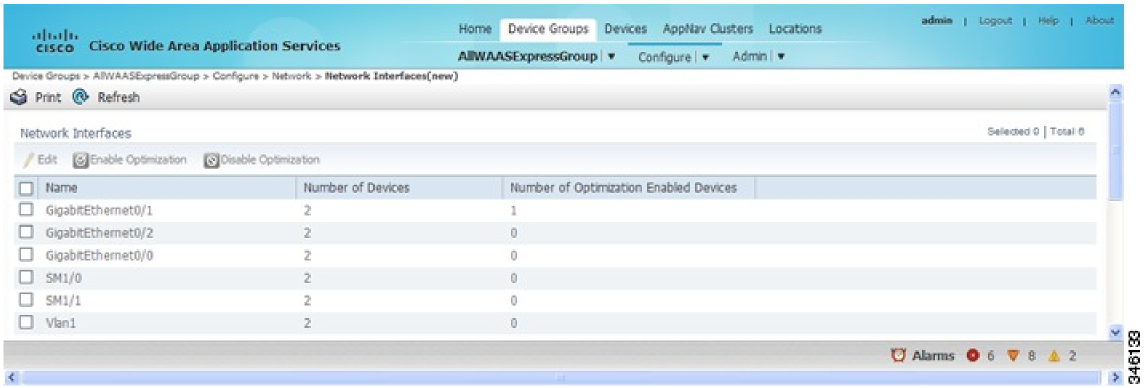
Figure 38: Cisco WAAS Express Network Interfaces Device Window


Cisco Wide Area Application Services
Home | Device Groups | Devices | AppNav Clusters | Locations
admin | Logout | Help | About
abc | Configure | Monitor | Admin
Devices > abc > Configure > Network > Network Interfaces
Print
Refresh
Network Interfaces
Selected 0 | Total 6
Enable Optimization
Disable Optimization
Alarms 6 8 2
346132

□	Name	Address	Subnet	Speed	Duplex	Shutdown	Optimizatior
□	GigabitEthernet0/0	10.104.227.122	255.255.255.128	100Mbps	Full	Yes	Disabled
□	GigabitEthernet0/1			Auto	Auto	No	Enabled
□	GigabitEthernet0/2			Auto	Auto	No	Disabled
□	SM1/0			1Gbps	Full	No	Disabled
□	SM1/1			Auto-speed	Auto	Yes	Disabled
□	Vlan1					Yes	Disabled

For a device group, the **Network Interfaces** window is different and displays an interface name, the number of devices that contain that interface, and the number of devices in the group that have optimization enabled on the interface.

Figure 39: Cisco WAAS Express Network Interfaces Device Group Interfaces Window

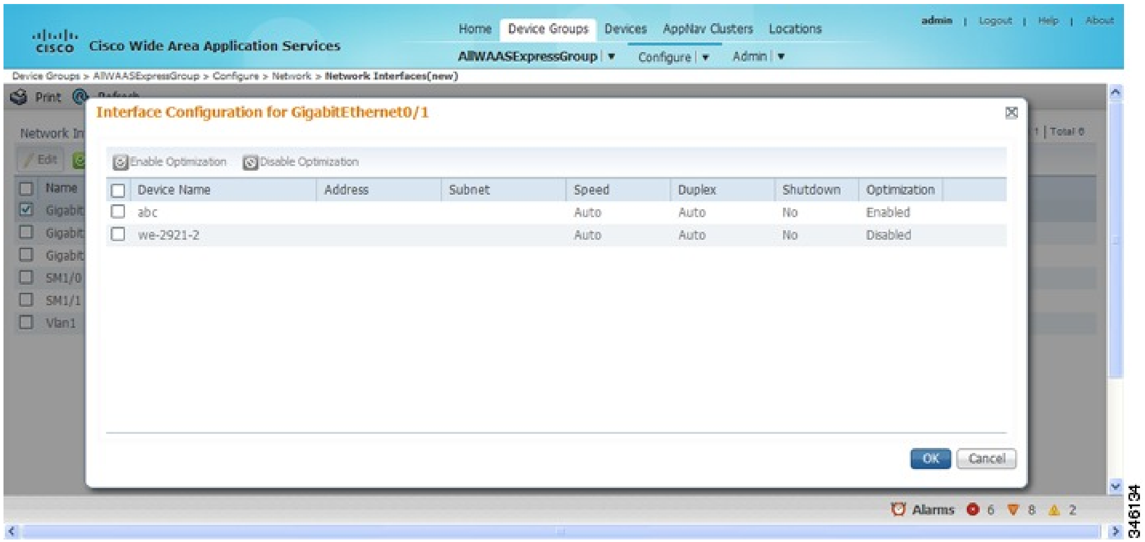

Cisco Wide Area Application Services
Home | Device Groups | Devices | AppNav Clusters | Locations
admin | Logout | Help | About
AllWAASExpressGroup | Configure | Admin
Device Groups > AllWAASExpressGroup > Configure > Network > Network Interfaces(new)
Print
Refresh
Network Interfaces
Selected 0 | Total 6
Edit
Enable Optimization
Disable Optimization
Alarms 6 8 2
346133

□	Name	Number of Devices	Number of Optimization Enabled Devices
□	GigabitEthernet0/1	2	1
□	GigabitEthernet0/2	2	0
□	GigabitEthernet0/0	2	0
□	SM1/0	2	0
□	SM1/1	2	0
□	Vlan1	2	0

Step 3 Check the check box next to each interface on which you want to enable Cisco WAAS optimization, and click the **Enable Optimization** taskbar icon; or, to disable optimization, click the **Disable Optimization** taskbar icon.

Note Enable Cisco WAAS optimization only on WAN interfaces, not LAN interfaces.

For a device group, enabling optimization for an interface enables optimization on that interface for all the devices in the group that have the interface. You can check the check box next to a single device and click the **Edit** taskbar icon to display a list of devices on which an interface is available and individually configure optimization on those devices.



Interface Configuration for GigabitEthernet0/1

□	Device Name	Address	Subnet	Speed	Duplex	Shutdown	Optimization
□	abc			Auto	Auto	No	Enabled
□	we-2921-2			Auto	Auto	No	Disabled

Enabling WAAS Service Insertion on AppNav-XE Device Interfaces

Before you begin

AppNav-XE device interfaces are configured by using the router CLI, not through the Cisco WAAS Central Manager. However, you can use the Cisco WAAS Central Manager to enable or disable the WAAS service insertion on the available interfaces on the router.

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Interfaces**.

The **Network Interfaces** window appears and lists the available interfaces.

Step 3 Check the check box next to an interface on which you want to enable WAAS service insertion and click the **Edit** taskbar icon.

Step 4 Check the **Enable WAAS Service Insertion** check box; or, to disable optimization, uncheck the check box.

Enable WAAS service insertion only on WAN interfaces, not LAN interfaces.

Step 5 Click **OK**.

Step 6 Repeat Step 3 through Step 5 for each interface on which you want to enable WAAS service insertion.

Configuring the Management Interface Settings

Before you begin

On devices running Cisco WAAS Version 5.0 or later, you can designate a specific interface to be used as the management interface for communicating with the Central Manager, Telnet, SSH, and so on. This configuration separates management traffic from data traffic.

If you designate a management interface, you must have another active interface to handle data traffic. In addition to management interface for IPv4 traffic, a separate management interface can be configured for IPV6 traffic. This interface will use the management features with IPV6 support.

Procedure

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

Step 2 Choose **Configure > Network > Management Interface Settings**.

The **Management Interface Settings** window appears with tabs for IPv4 and IPv6 settings. Select the appropriate one for your network before you proceed.

Step 3 From the **Management Interface** drop-down list, choose the interface that you want to use as the management interface.

Step 4 In the **Management Default Gateway** field, enter the default gateway IP address for management traffic.

- To use the designated management interface for FTP traffic, check the **Use Management Interface for FTP Traffic** check box.
- To use the designated management interface for TFTP traffic, check the **Use Management Interface for TFTP Traffic** check box.
- To use the designated management interface for TACACS traffic, check the **Use Management Interface for TACACS Traffic** check box.
- To use the designated management interface for Radius traffic, check the **Use Management Interface for Radius Traffic** check box.
- To use the designated management interface for DNS traffic, check the **Use Management Interface for DNS Traffic** check box.
- To use the designated management interface for NTP traffic, check the **Use Management Interface for NTP Traffic** check box.

Step 5 Click **Submit**. A confirmation message appears.

Step 6 Click **OK**.

To configure a different default gateway for management traffic from the CLI, run the **ip default-gateway management** global configuration command.

Step 7 After you have designated a management interface, create static IP routes for management traffic so that an IP packet that is designated for the specified destination uses the configured route. To configure a static route for management traffic, follow these steps:

a) In the **Management Interface Settings** window, in the Management IP Routes area of this window, click the **Create Management IP Route** taskbar button.

The **Management IP Routes** window appears.

b) In the **Destination Network Address** field, enter the destination network IP address.
c) In the **Netmask** field, enter the destination host netmask. This field is not available when you create a IPv6 Management IP Route.
d) In the Gateway's **IP Address** field, enter the IP address of the gateway interface.

The gateway interface IP address should be in the same network as the device's management interface.

e) Click **Submit**.

To configure a static route for management traffic from the CLI, run the **ip route management** global configuration command.

Configuring a Jumbo MTU

Before you begin

A jumbo MTU can be configured on the following devices: Cisco WAVE-294, WAVE-594, WAVE-694, WAVE-7541, WAVE-7571, WAVE-8541, and Cisco vWAAS.

Note To enable Jumbo MTU on ISR-WAAS devices, you must first upgrade the ISR-WAAS to Version 6.0 using the **.ova** files. The default MTU size for the virtual interface of the ISR-WAAS devices is 9000, and cannot be changed.

If configured, a jumbo MTU applies to all the device interfaces, including logical interfaces with at least one member physical interface. The MTU for individual interfaces cannot be changed while the jumbo MTU is configured. If the jumbo MTU is disabled, all the interfaces are configured with an MTU of 1500.

Procedure

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

Step 2 Choose **Configure** > **Network** > **Jumbo MTU**.

The **Jumbo MTU Settings** window appears.

Step 3 In the **System Jumbo MTU** field, enter the jumbo MTU size, in bytes (maximum size varies by platform).

Step 4 Click **Submit**.

Consider the following guidelines:

- If the original and optimized maximum segment sizes are set to their default values and you configure a jumbo MTU setting, the segment sizes are changed to the jumbo MTU setting minus 68 bytes. If you have configured custom maximum segment sizes, their values are not changed if you configure a jumbo MTU. For more information on configuring maximum segment sizes, see Modifying the Acceleration TCP Settings in the chapter "Configuring Application Acceleration."

- To configure a jumbo MTU from the CLI, run the **system jumbomtu** global configuration command.

Configuring TCP Settings

This section contains the following topics:

Configuring the TCP and IP Settings

To configure TCP and IP settings, follow these steps:

Before you begin

For data transactions and queries between client and servers, the size of windows and buffers is important. Therefore, fine-tuning the TCP stack parameters becomes the key to maximizing cache performance.

Note Because of the complexities involved in TCP parameters, be careful when tuning these parameters. In nearly all environments, the default TCP settings are adequate. Fine-tuning TCP settings is for network administrators with adequate experience and full understanding of TCP operation details.

Procedure

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

Step 2 Choose **Configure** > **Network** > **TCP/IP Settings** > **TCP/IP**.

The **TCP/IP Settings** window appears.

Step 3 Make the necessary changes to the TCP settings.

See the following table for a description of each TCP field in this window.

Table 10: TCP Settings

TCP Setting	Description
TCP General Settings	
Enable Explicit Congestion Notification	Enables reduction of delay and packet loss in data transmissions. Provides TCP support for RFC 2581. From software version 6.4.3d, this option is no longer enabled by default. For more information, see Explicit Congestion Notification, on page 212.
Initial Send Congestion Window Size	Initial congestion window size value, in segments. The range is 0 to 10 segments. The default is 0 segment. For more information, see Congestion Windows, on page 212.

TCP Setting	Description
ReTransmit Time Multiplier	Factor used to modify the length of the retransmit timer by 1 to 3 times the base value determined by the TCP algorithm. The default is 1, which leaves the times unchanged. The range is 1 to 3. For more information, see Retransmit Time Multiplier, on page 212. **Note** Modify this factor with caution. It can improve throughput when TCP is used over slow reliable connections, but should never be changed in an unreliable packet delivery environment.
Keepalive Probe Count	Number of times that the WAAS device can retry a connection before the connection is considered unsuccessful. The range is 1 to 120 attempts. The default is 4 attempts.
Keepalive Probe Interval	Length of time that the WAAS device keeps an idle connection open. The default is 75 seconds.
Keepalive Timeout	Length of time that the Cisco WAAS device keeps a connection open before disconnecting. The range is 1 to 120 seconds. The default is 90 seconds.
Enable Path MTU Discovery	Enables discovery of the largest IP packet size allowable between the various links along the forwarding path and automatically sets the correct value for the packet size. By default, this option is disabled. For more information, see Path MTU Discovery, on page 213.
Enable Satellite Optimization	Enables traffic optimization for better throughput in high latency, low bandwidth, satellite networks that are used by Cisco WAAS peer devices on the Satellite WAN link.This feature is disabled by default. You can enable it at the device level. If your device is part of a device group, you can enable and disable it globally from the group level. If you use the CLI to enable/disable this feature for a device managed by the Cisco WAAS Central Manager, the change is reflected in the Cisco WAAS Central Manager within two data feed cycles.

Step 4 Click **Submit**.

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

To use the CLI for configuration:

- To configure TCP settings from the CLI, use the **tcp** global configuration command.
- To configure TCP satellite settings from the CLI, use the **tcp satellite** global configuration command.
- To enable the MTU discovery utility from the CLI, use the **ip path-mtu-discovery enable** global configuration command.

Explicit Congestion Notification

The TCP Explicit Congestion Notification (ECN) feature allows an intermediate router to notify the end hosts of impending network congestion. It also provides enhanced support for TCP sessions associated with applications that are sensitive to delay or packet loss. The major issue with ECN is that the operation of both the routers and the TCP software stacks needs to be changed to accommodate the operation of ECN.

Congestion Windows

The congestion window (**cwnd**) is a TCP state variable that limits the amount of data that a TCP sender can transmit to the network before receiving an acknowledgment (ACK) from the receiving side of the TCP transmission. The TCP **cwnd** variable is implemented by the TCP congestion avoidance algorithm. The goal of the congestion avoidance algorithm is to continually modify the sending rate so that the sender automatically senses any increase or decrease in available network capacity during the entire data flow. When congestion occurs (manifested as packet loss), the sending rate is first lowered, and then gradually increased as the sender continues to probe the network for additional capacity.

Retransmit Time Multiplier

A TCP sender uses a timer to measure the time that has elapsed between sending a data segment and receiving the corresponding ACK from the receiving side of the TCP transmission. When this retransmit timer expires, the sender (according to the RFC standards for TCP congestion control) must reduce its sending rate. However, because the sender is not reducing its sending rate in response to network congestion, the sender is not able to make any valid assumptions about the current state of the network. Therefore, in order to avoid congesting the network with an inappropriately large burst of data, the sender implements the slow start algorithm, which reduces the sending rate to one segment per transmission. (See TCP Slow Start, on page 212.)

You can modify the sender's retransmit timer by using the **Retransmit Time Multiplier** field in the Cisco WAAS Central Manager. The retransmit time multiplier modifies the length of the retransmit timer by one to three times the base value, as determined by the TCP algorithm that is being used for congestion control.

Note When making adjustments to the retransmit timer, be aware that they affect performance and efficiency. If the retransmit timer is triggered too early, the sender pushes duplicate data onto the network unnecessarily; if the timer is triggered too slowly, the sender remains idle for too long, unnecessarily slowing data flow.

TCP Slow Start

Slow start is one of four congestion-control algorithms used by TCP. The slow-start algorithm controls the amount of data being inserted into the network at the beginning of a TCP session when the capacity of the network is not known.

For example, if a TCP session began with an insertion of a large amount of data into the network, much of the initial burst of data is likely be lost. Instead, TCP should initially transmit a modest amount of data, which has a high probability of successful transmission. Next, TCP can probe the network by sending increasing amounts of data as long as the network does not show signs of congestion.

The slow-start algorithm begins by sending packets at a rate that is determined by the congestion window, or **cwnd** variable. (See Congestion Windows, on page 212.) The algorithm continues to increase the sending rate until it reaches the limit set by the slow-start threshold (**ssthresh**) variable. Initially, the value of the **ssthresh** variable is adjusted to the receiver's maximum segment size (RMSS). However, when congestion occurs, the **ssthresh** variable is set to half the current value of the **cwnd** variable, marking the point of the onset of network congestion for future reference.

The starting value of the **cwnd** variable is set to that of the sender maximum segment size (SMSS), which is the size of the largest segment that a sender can transmit. The sender sends a single data segment, and because the congestion window is equal to the size of one segment, the congestion window is full. The sender then waits for the corresponding ACK from the receiving side of the transmission. When the ACK is received, the sender increases the congestion window size by increasing the value of the **cwnd** variable by the value of one SMSS. Now the sender can transmit two segments before the congestion window is again full and the sender is once more required to wait for the corresponding ACKs for these segments. The slow-start algorithm continues to increase the value of the **cwnd** variable, and thus increases the size of the congestion window by one SMSS for every ACK received. If the value of the **cwnd** variable increases beyond the value of the **ssthresh** variable, the TCP flow-control algorithm changes from the slow-start algorithm to the congestion-avoidance algorithm.

Path MTU Discovery

The Cisco WAAS software supports the IP Path Maximum Transmission Unit (MTU) Discovery method, as defined in RFC 1191. When enabled, the Path MTU Discovery feature discovers the largest IP packet size allowable between the various links along the forwarding path and automatically sets the correct value for the packet size. By using the largest MTU that the links can handle, the sending device can minimize the number of packets it must send.

IP Path MTU Discovery is useful when a link in a network goes down, which forces the use of another, different MTU-sized link. IP Path MTU Discovery is also useful when a connection is first being established, and the sender has no information about the intervening links.

Note IP Path MTU Discovery is a process initiated by the sending device. If a server does not support IP Path MTU Discovery, the receiving device will have no available means to avoid fragmenting datagrams generated by the server.

By default, this feature is disabled. With the feature disabled, the sending device uses a packet size that is the lesser of 576 bytes and the next hop MTU. Existing connections are not affected when this feature is turned on or off.

Configuring a Static IP Route

Before you begin

The Cisco WAAS software allows you to configure a static route for a network or host. Any IP packet designated for the specified destination uses the configured route.

Procedure

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

Step 2 Choose **Configure > Network > TCP/IP Settings > Static Routes**.

The **IP Route Entries** window appears.

Step 3 In the taskbar, click the **Create New IP Route Entry** icon.

The **Creating New IP Route** window appears.

Step 4 In the **Destination Network Address** field, enter the destination network IP address.

Step 5 In the **Netmask** field, enter the destination host netmask.

Step 6 In the Gateway's **IP Address** field, enter the IP address of the gateway interface.

The gateway interface IP address should be in the same network as that of one of the device's network interfaces.

Step 7 Alternately, if you select the check box for IPv6 Address, you need to specify the details only for the **Destination Network Address** and the Gateway's **IP Address** field.

Step 8 Click **OK**.

To configure a static route from the CLI, run the **ip route** global configuration command or run the **ipv6 route** global configuration command.

Aggregating IP Routes

An individual WAE device can have IP routes defined and can belong to device groups that have other IP routes defined.

In the **IP Route Entries** window, the Aggregate Settings radio button controls how IP routes are aggregated for an individual device, as follows:

- Choose **Yes** to configure the device with all the IP routes that are defined for itself and for the device groups to which it belongs.
- Choose **No** to limit the device to just the IP routes that are defined for itself.

When you change the setting, you get the following confirmation message: **This option will take effect immediately and will affect the device configuration. Do you wish to continue?** Click **OK** to continue.

Configuring CDP Settings

Before you begin

Consider the following guidelines for configuring CDP settings:

- The Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured devices. With CDP, each device in a network sends periodic messages to all the other devices in the network. All the devices listen to periodic messages that are sent by others to learn about neighboring devices and determine the status of their interfaces.
- With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices. Applications are able to send SNMP queries within the network. CiscoWorks2000 also discovers the Cisco WAAS devices by using the CDP packets that are sent by the Cisco WAAS device after booting.
- To perform device-related tasks, the Cisco WAAS device platform must support CDP to be able to notify the system manager of the existence, type, and version of the Cisco WAAS device platform.

Procedure

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

Step 2 Choose **Configure** > **Network** > **CDP**.

The **CDP Settings** window appears.

Step 3 Check the **Enable** check box to enable CDP support. By default, this option is enabled.

Step 4 In the **Hold Time** field, enter the time (in seconds) to specify the length of time that a receiver is to keep the CDP packets.

The range is 10 to 255 seconds. The default is 180 seconds.

Step 5 In the **Packet Send Rate** field, enter a value (in seconds) for the interval between CDP advertisements.

The range is 5 to 254 seconds. The default is 60 seconds.

Step 6 Click **Submit**.

To configure CDP settings from the CLI, run the **cdp** global configuration command.

Configuring the DNS Server

To configure DNS server settings for a Cisco WAAS device, follow these steps:

Before you begin

DNS allows the network to translate the domain names entered in requests into their associated IP addresses. To configure DNS on a Cisco WAAS device, you must complete the following tasks:

- Specify the list of DNS servers that are used by the network to translate requested domain names into IP addresses (both IPv4 and IPv6) that the Cisco WAAS device should use for domain name resolution.
- Enable DNS on the Cisco WAAS device.

Procedure

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

Step 2 Choose **Configure** > **Network** > **DNS**. The DNS Settings window appears.

Step 3 In the **Local Domain Name** field, enter the name of the local domain. You can configure up to three local domain names. Separate items in the list with a space.

Step 4 In the **List of DNS Servers** field, enter a list of DNS servers used by the network to resolve hostnames to IP addresses.

You can configure up to three DNS servers. Separate items in the list with a space.

Step 5 Click **Submit**.

A **Click Submit to Save** message appears in red next to the Current Settings line when there are pending changes to be saved after you have applied default and device group settings. To revert to the previously configured window settings, click **Reset**, which appears only when you have applied default or group settings to change the current device settings, but the settings have not yet been submitted.

To configure DNS name servers from the CLI, run the **ip name-server** global configuration command.

Note On ISR-WAAS devices you cannot configure the DNS server from the Cisco WAAS Central Manager.

Configuring Windows Name Services

Procedure

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

Step 2 Choose **Configure** > **Network** > **WINS**.

The **Windows Name Services Settings** window appears.

Step 3 In the **Workgroup** or **Domain Name** field, enter the name of the workgroup (or domain) in which the chosen device or device group resides.

This name must be entered in shortname format and cannot exceed 15 characters. Valid characters include alphanumeric characters, a forward slash (\), an underscore (_), and a dash (-).

For example, if your domain name is cisco.com, the short name format is cisco.

Step 4 Check the **NT** check box if the workgroup or domain is a Windows NT 4 domain. For example, if your domain name is cisco.com, the short name format is cisco. If your workgroup or domain is a Windows 2000 or Windows 2003 domain, do not check the NT check box. By default, this option is disabled.

Step 5 In the **WINS Server** field, enter the hostname or IP address of the Windows Internet Naming Service (WINS) server.

Step 6 Click **Submit**.

Step 7 (Optional) To configure Windows name services from the Cisco WAAS CLI, run the **windows-domain** global configuration command.

Configuring NAT Settings

Before you begin

When the Cisco WAAS Central Manager manages Microsoft Azure devices, it is important to configure the NAT settings on the Central Manager because the Microsoft Azure devices are in the public network and cannot communicate with the Cisco WAAS Central Manager using the internal ip address. The NAT settings can only be configured when the device is in the **Central Manager** mode, whether primary or secondary.

Procedure

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

Step 2 Choose **Configure** > **Network** > **NAT Settings**.

The **NAT Settings** window appears.

Step 3 In the **NAT IP** field, enter the external IP of the Cisco WAAS Central Manager and click **Submit**.

The external ip configuration (routed through NAT) is pushed to the Microsoft Azure devices. This IP is used by the Microsoft Azure devices to communicate with the Cisco WAAS Central Manager.

CHAPTER 7

Configuring Administrative Login Authentication, Authorization, and Accounting

This chapter describes how to configure administrative login authentication, authorization, and accounting for Cisco Wide Area Application Services (WAAS) devices.

Use the WAAS Central Manager GUI to centrally create and manage two different types of administrator user accounts (device-based CLI accounts and roles-based accounts) for your Cisco WAAS devices. For more information, see Creating and Managing Administrator User Accounts and Groups, on page 255.

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

This chapter contains the following sections:

About Administrative Login Authentication and Authorization

In the Cisco WAAS network, administrative login authentication and authorization are used to control login requests from administrators who want to access a WAAS device for configuring, monitoring, or troubleshooting purposes.

Login authentication is the process by which Cisco WAAS devices verify whether an administrator who is attempting to log in to the device has a valid username and password. An administrator who is logging in must have a user account registered with the device. User account information serves to authorize a user for administrative login and configuration privileges. The user account information is stored in an authentication, authorization and accounting (AAA) database, and the WAAS devices must be configured to access the particular authentication server (or servers) where the AAA database is located. When a user attempts to log in to a device, the device compares the person's username, password, and privilege level to the user account information that is stored in the database.

The Cisco WAAS software provides the following AAA support for users who have external access servers, for example, RADIUS or TACACS+ servers, and for users who require a local access database with AAA features:

- Authentication (or login authentication) is the action of determining who a user is. It checks the username and password.
- Authorization (or configuration) is the action of determining what a user is allowed to do. It permits or denies privileges for authenticated users in the network. Generally, authentication precedes authorization. Both authentication and authorization are required for a user login.
- Accounting is the action of keeping track of administrative user activities for system accounting purposes. In the WAAS software, AAA accounting through TACACS+ is supported. For more information, see Configuring AAA Accounting for Cisco WAAS Devices, on page 252.

Note An administrator can log in to the Cisco WAAS Central Manager device through the console port or the Cisco WAAS Central Manager GUI. An administrator can also log in to a Cisco WAAS device that is functioning as a data center or branch WAE through the console port.

When the system administrator logs in to a Cisco WAAS device before authentication and authorization have been configured, the administrator can access the Cisco WAAS device by using the predefined superuser account (the predefined username is admin and the predefined password is default). When you log in to a Cisco WAAS device using this predefined superuser account, you are granted access to all the Cisco WAAS services and entities in the Cisco WAAS system.

Note Each Cisco WAAS device must have one administrator account with the username admin. You cannot change the username of the predefined superuser account. The predefined superuser account must have the username admin.

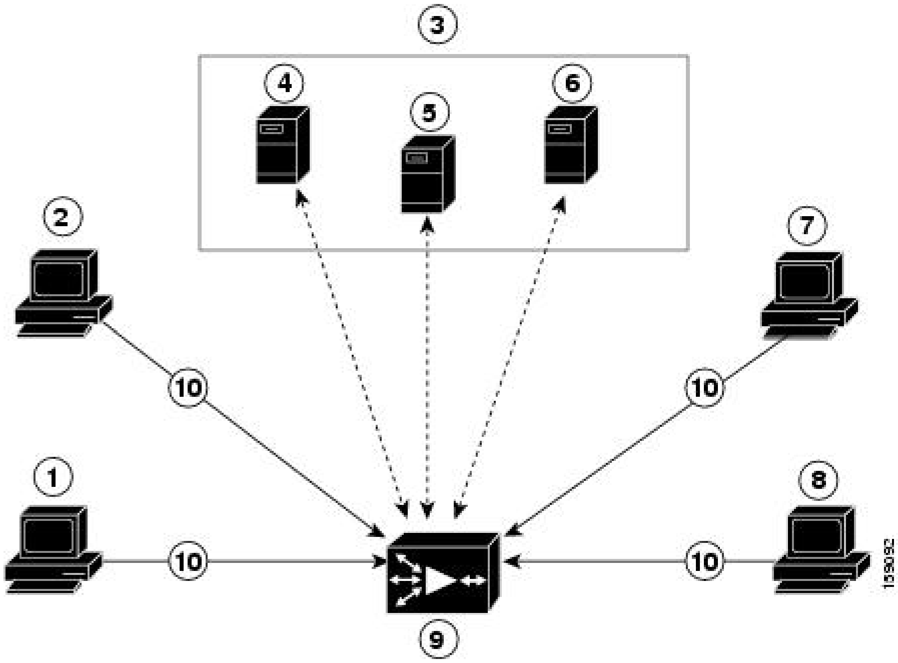
All AAA interfaces support IPv6 configurations.

After you have initially configured your Cisco WAAS devices, we strongly recommend that you immediately change the password for the predefined superuser account (the predefined username is **admin**, the password is **default**, and the privilege level is **superuser**, privilege level **15**) on each Cisco WAAS device.

For instructions on using the Cisco WAAS Central Manager GUI to change the password for a predefined superuser account, see Changing the Password for Your Own Account, on page 261 in the chapter "Creating and Managing Administrative Groups."

The following figure shows how an administrator can log in to a WAE through the console port or the Cisco WAAS Central Manager GUIs. When the Cisco WAAS device receives an administrative login request, the WAE can check its local database or a remote third-party database (TACACS+, RADIUS, or Windows domain database) to verify the username with the password and to determine the access privileges of the administrator.

Figure 40: Authentication Databases and a WAE



1	FTP/SFTP client	6	Windows domain server
2	Cisco WAAS Central Manager GUI	7	Console or Telnet clients
3	Third-party AAA servers	8	SSH client
4	RADIUS server	9	WAE that contains a local database and the default primary authentication database
5	TACACS+ server	10	Administrative login requests

The user account information is stored in an AAA database, and the Cisco WAAS devices must be configured to access the particular authentication server (or servers) that contains the AAA database. You can configure any combination of these authentication and authorization methods to control administrative login access to a Cisco WAAS device:

- Local authentication and authorization
- RADIUS
- TACACS+
- Windows domain authentication

Note Even if you configure authentication using an external authentication server, you must create a role-based user or user group account in the Cisco WAAS Central Manager, as described in the chapter "Creating and Managing Administrator User Accounts and Groups, on page 255."

For more information on the default AAA configuration, see Default Administrative Login Authentication and Authorization Configuration, on page 222. For more information on configuring AAA, see Configuring Administrative Login Authentication and Authorization, on page 223.

Default Administrative Login Authentication and Authorization Configuration

By default, a Cisco WAAS device uses the local database to obtain login authentication and authorization privileges for administrative users.

The following table lists the default configuration for administrative login authentication and authorization.

Table 11: Default Configuration for Administrative Login Authentication and Authorization

Feature	Default Value
Administrative login authentication	Enabled
Administrative configuration authorization	Enabled
Authentication server failover because the authentication server is unreachable	Disabled
TACACS+ port	Port 49
TACACS+ login authentication (console and Telnet)	Disabled
TACACS+ login authorization (console and Telnet)	Disabled
TACACS+ key	None specified
TACACS+ server timeout	5 seconds
TACACS+ retransmit attempts	2 times
RADIUS login authentication (console and Telnet)	Disabled
RADIUS login authorization (console and Telnet)	Disabled
RADIUS server IP address	None specified
RADIUS server UDP authorization port	Port 1645
RADIUS key	None specified
RADIUS server timeout	5 seconds
RADIUS retransmit attempts	2 times
Windows domain login authentication	Disabled
Windows domain login authorization	Disabled
Windows domain password server	None specified

Feature	Default Value
Windows domain realm (Kerberos realm used for authentication when Kerberos authentication is used). **Note** When Kerberos authentication is enabled, the default realm is DOMAIN.COM and security is the Active Directory Service (ADS).	Null string
Hostname or IP address of the Windows Internet Naming Service (WIN) server for Windows domain	None specified
Window domain administrative group	There are no predefined administrative groups.
Windows domain NETBIOS name	None specified
Kerberos authentication	Disabled
Kerberos server hostname or IP address (host that is running the Key Distribution Center (KDC) for the given Kerberos realm	None specified
Kerberos server port number (port number on the KDC server)	Port 88
Kerberos local realm (default realm for WAAS)	kerberos-realm: null string
Kerberos realm (maps a hostname or DNS domain name to a Kerberos realm)	Null string

Note If you configure a RADIUS or TACACS+ key on a Cisco WAAS device (the RADIUS and or TACACS+ client), make sure that you configure an identical key on the external RADIUS or TACACS+ server.

Change these defaults through the Cisco WAAS Central Manager GUI, as described in Configuring Administrative Login Authentication and Authorization, on page 223.

Multiple Windows domain utilities are included in the Cisco WAAS software to assist with Windows domain authentication configuration. You can access these utilities through the Cisco WAAS CLI by running the **windows-domain diagnostics** EXEC command.

Configuring Login Authentication and Authorization

This section contains the following topics:

Configuring Administrative Login Authentication and Authorization

To centrally configure administrative login authentication and authorization for a Cisco WAAS device or a device group (a group of WAEs), follow these steps:

Procedure

Step 1 Determine the login authentication scheme that you want to configure for the Cisco WAAS device to use when authenticating administrative login requests, for example, use the local database as the primary login database and your RADIUS server as the secondary authentication database.

Step 2 Configure the login access control settings for the Cisco WAAS device, as described in Configuring Login Access Control Settings for Cisco WAAS Devices, on page 225.

Step 3 Configure the administrative login authentication server settings on the WAAS device (if a remote authentication database is to be used). For example, specify the IP address(IPv4/IPv6) of the remote RADIUS servers, TACACS+ servers, or Windows domain server that the Cisco WAAS device should use to authenticate administrative login requests, as described in the following sections:

- Configuring RADIUS Server Authentication Settings, on page 231
- About TACACS+ Server Authentication Settings, on page 233
- Configuring Windows Domain Server Authentication Settings, on page 235

Step 4 Specify one or all of the following login authentication configuration schemes that the Cisco WAAS device should use to process administrative login requests:

- Specify the administrative login authentication scheme.
- Specify the administrative login authorization scheme.
- (Optional) Specify the failover scheme for the administrative login authentication server.

For example, specify which authentication database the Cisco WAAS device should check to process an administrative login request. For more information, see Enabling Administrative Login Authentication and Authorization Schemes for Cisco WAAS Devices, on page 245.

What to do next

Considering the following guidelines:

Caution Make sure that the RADIUS, TACACS+, or Windows domain authentication server is configured and operating correctly before disabling local authentication and authorization. If you disable local authentication, and RADIUS, TACACS+, or Windows domain settings are not configured correctly, or if the RADIUS, TACACS+, or Windows domain server is not online, you may be unable to log in to the WAAS device.

- You can enable or disable the local and the remote databases (TACACS+, RADIUS, and Windows domain) through the Cisco WAAS Central Manager GUI or the Cisco WAAS CLI. The Cisco WAAS device verifies whether all the databases are disabled, and, if so, sets the system to the default state.

  If you have configured the Cisco WAAS device to use one or more of the external third-party databases (TACACS+, RADIUS, or Windows domain authentication) for administrative authentication and authorization, make sure that you have also enabled the local authentication and authorization method on the Cisco WAAS device, and that the local method is specified as the last option. Otherwise, the Cisco

WAAS device will not go to the local authentication and authorization method by default if the specified external third-party databases are not reachable.

- By default, local login authentication is enabled first. Local authentication and authorization uses locally configured login names and passwords to authenticate administrative login attempts. The login names and passwords are local to each Cisco WAAS device and are not mapped to individual usernames. When local authentication is disabled, if you disable all the other authentication methods, local authentication is re-enabled automatically.
- You can disable local login authentication only after enabling one or more of the other administrative login authentication methods. However, when local login authentication is disabled, if you disable all other administrative login authentication methods, local login authentication is re-enabled automatically. You cannot specify different administrative login authentication methods for console and Telnet connections.
- We strongly recommend that you set the administrative login authentication and authorization methods in the same order. For example, configure the Cisco WAAS device to use RADIUS as the primary login method, TACACS+ as the secondary login method, Windows as the tertiary method, and the local method as the quaternary method for both administrative login authentication and authorization.

  A TACACS+ server will *not* authorize a user who is authenticated by a different method. For example, if you configure Windows as the primary authentication method, but use TACACS+ as the primary authorization method, TACACS+ authorization will fail.
- We strongly recommend that you specify the local method as the last method in your prioritized list of login authentication and authorization methods. By adhering to this practice, if the specified external third-party servers (TACACS+, RADIUS, or Windows domain servers) are not reachable, a Cisco WAAS administrator can still log in to a WAAS device through the local authentication and authorization method.

Configuring Login Access Control Settings for Cisco WAAS Devices

This section describes how to centrally configure remote login and access control settings for a Cisco WAAS device or device group, and contains the following topics:

Configuring Secure Shell Settings for Cisco WAAS Devices

This section contains the following topics:

About SSH

Secure Shell (SSH) consists of a server and a client program. Like Telnet, you can use the client program to remotely log in to a machine that is running the SSH server, but unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

The SSH management window in the Cisco WAAS Central Manager GUI allows you to specify the key length, login grace time, and maximum number of password guesses allowed when logging in to a specific Cisco WAAS device or device group for configuration, monitoring, or troubleshooting purposes.

Operating Guidelines for SSH and Cisco WAAS Versions

Note these operational guidelines when enabling or disabling SSH for different Cisco WAAS versions:

Table 12: SSH Default Status and Cisco WAAS Versions

Cisco WAAS Version	SSH Default Value
6.2.3x and later	• SSH is enabled by default. To disable SSH, check the **Disable** check box on the SSH screen (displayed on the **SSH Configuration** window for Cisco WAAS Version 6.2.3x and later). • If you click **Reset** to remove features that you have enabled, after reset, the SSH feature will remain enabled by default. • If you downgrade to a version earlier than Cisco WAAS Versoin 6.2.3x, the SSH default status will remain as enabled.
6.2.1x and earlier	• SSH is disabled by default. To enable SSH, check the **Enable** check box in the SSH screen (displayed on the SSH screen for Cisco WAAS versions earlier than 6.2.3x). • If you click **Reset** to remove features that you have enabled, after reset, the SSH feature will remain disabled by default. • If you upgrade to Cisco WAAS version 6.2.3x and later, the SSH default status will remain as disabled.

Procedure for Configuring SSH for Cisco WAAS Devices

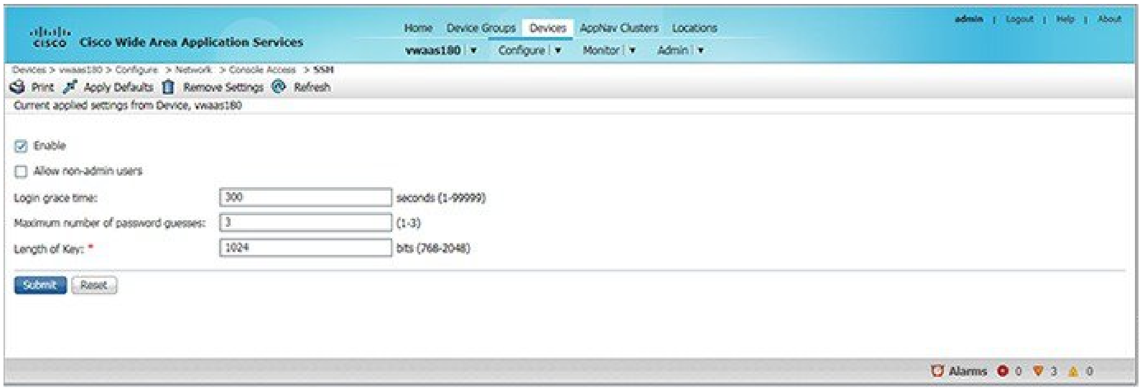
Procedure

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

Step 2 Choose **Configure** > **Network** > **Console Access** > **SSH**.

The **SSH Configuration** window appears.

Note The SSH Version 1 protocol is no longer supported. Only the SSH Version 2 protocol is supported by the WAAS device.



Current applied settings from Device, vwaas180

☑ Enable

☐ Allow non-admin users

Login grace time: 300 seconds (1-99999)

Maximum number of password guesses: 3 (1-3)

Length of Key: * 1024 bits (768-2048)

Step 3 SSH enables login access to the chosen Cisco WAAS device (or the device group) through a secure and encrypted channel. The SSH default status is determined by your Cisco WAAS version. Depending on your Cisco WAAS version, an **Enable** or **Disable** check box is displayed in the **SSH Configuration** window for you to change the default status, if needed.

You can also use the CLI to enable or disable SSH, running the **sshd enable** global configuration command, or the **no sshd enable** command.

Step 4 Check the **Allow non-admin users** check box to allow nonadministrative users to gain SSH access to the chosen device (or device group). By default, this option is disabled.

Note Nonadministrative users are nonsuperuser administrators. All nonsuperuser administrators have only restricted access to a Cisco WAAS device because their login accounts have a privilege level of 0. Superuser administrators have full access to a Cisco WAAS device because their login accounts have the highest level of privileges, a privilege level of **15**.

Step 5 In the **Login grace time** field, specify the number of seconds for which an SSH session will be active during the negotiation (authentication) phase between the client and the server before it times out. The default is **300 seconds**.

Step 6 In the **Maximum number of password guesses** field, specify the maximum number of incorrect password guesses allowed per connection. The default is **3**.

Although the value in the **Maximum number of password guesses** field specifies the number of password guesses allowed from the SSH server side, the actual number of password guesses for an SSH login session is determined by the combined number of allowed password guesses of the SSH server and the SSH client.

Some SSH clients limit the maximum number of allowed password guesses to three (or to one in some cases), even though the SSH server allows more than this number of guesses. When you specify *n* password guesses allowed, certain SSH clients interpret this number as *n* + 1. For example, when configuring the number of guesses to two for a particular device, SSH sessions from some SSH clients will allow three password guesses.

Step 7 In the **Length of key** field, specify the number of bits required to create an SSH key. The default is **1024**.

When you enable SSH, be sure to generate both a private and a public host key, which client programs can use to verify the server's identity. When you use an SSH client and log in to a Cisco WAAS device, the public key for the SSH daemon running on the device is recorded in the client machine known_hosts file in your home directory.

If the Cisco WAAS administrator subsequently regenerates the host key by specifying the number of bits in the Length of key field, you must delete the old public key entry associated with the Cisco WAAS device in the known_hosts file before running the SSH client program to log in to the Cisco WAAS device. When you run the SSH client program after deleting the old entry, the **known_hosts** file is updated with the new SSH public key for the Cisco WAAS device.

Step 8 Click **Submit** to save the settings.

- A **Click Submit to Save** message appears in red in the **Current Settings** line when there are pending changes to be saved after you have applied the default or device group settings. You can also revert to the previously configured settings by clicking **Reset** button, which is visible only if you have applied default or group settings to change the current device settings, but have not yet submitted the changes.
- If you try to exit this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box appears only if you are using the Internet Explorer browser.

- To configure SSH settings from the CLI, run the **sshd** and **ssh-key-generate** global configuration commands.

Disabling and Re-enabling the Telnet Service for WAAS Devices

By default, the Telnet service is enabled on a WAAS device. You must use a console connection instead of a Telnet session to define device network settings on a WAAS device. However, after you have used a console connection to define the device network settings, you can use a Telnet session to perform subsequent configuration tasks.

You must enable the Telnet service before you can use the Telnet button in the Device Dashboard window to use Telnet to connect to a device.

Note Telnet is not supported in Internet Explorer. If you want to use the Telnet button from the Device Dashboard, use a different web browser.

To centrally disable the Telnet service on a WAAS device or a device group, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Network** > **Console Access** > **Telnet**.

The Telnet Settings window appears.

Step 3 Uncheck the **Telnet Enable** check box to disable the terminal emulation protocol for remote terminal connection for the chosen device (or device group).

Step 4 Click **Submit** to save the settings.

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

If you try to exit this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box appears only if you are using the Internet Explorer browser.

What to do next

To centrally re-enable the Telnet service on the device (or device group) at a later time, check the **Telnet Enable** check box in the Telnet Settings window, and click **Submit**.

From the CLI, use the **no telnet enable** global configuration command to disable Telnet, or the **telnet enable** global configuration command to enable it.

Configuring Message-of-the-Day Settings for Cisco WAAS Devices

The Message of the Day (MOTD) feature enables you to provide information bits to the users when they log in to a device that is a part of your Cisco WAAS network. There are three types of messages that you can set up:

- MOTD banner
- EXEC process creation banner
- Login banner

To configure the MOTD settings, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Network** > **Console Access** > **Message of the day**.

The **MOTD Configuration** window for the chosen device appears.

Step 3 To enable the MOTD settings, check the **Enable** check box. The **Message of the Day (MOTD) banner**, **EXEC process creation banner**, and **Login banner** fields become enabled.

Step 4 In the **Message of the Day (MOTD) Banner** field, enter a string that you want displayed as the MOTD banner after a user logs in to the device.

In the **Message of the Day (MOTD) Banner**, **EXEC Process Creation Banner**, and **Login Banner** fields, you can enter a maximum of **1024** characters. A new line character (or Enter) is counted as two characters, as it is interpreted as *n* by the system. You cannot use special characters such as `, % ,^ , and " in the MOTD text. If your text contains any of these special characters, Cisco WAAS software removes it from the MOTD output.

Step 5 In the **EXEC Process Creation Banner** field, enter a string to be displayed as the EXEC process creation banner when a user enters into the EXEC shell of the device.

Step 6 In the **Login Banner** field, enter a string to be displayed after the MOTD banner, when a user attempts to log in to the device.

Step 7 To save the configuration, click **Submit**.

Configuring EXEC Timeout Settings for Cisco WAAS Devices

To centrally configure the length of time for which an inactive Telnet session remains open on a WAAS device or device group, follow these steps:

Procedure

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

Step 2 Click the **Edit** icon next to the device (or device group) for which you want to configure the EXEC timeout.

Step 3 Choose **Configure** > **Network** > **Console Access** > **Exec Timeout**.

Step 4 In the **Exec Timeout** field, specify the number of minutes after which an active session times out. The default is 15 minutes.

A Telnet session with a Cisco WAAS device can remain open and inactive for the period specified in this field. When the EXEC timeout period elapses, the Cisco WAAS device automatically closes the Telnet session.

Step 5 To save the settings, click **Submit**.

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

If you try to exit this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box appears only if you are using the Internet Explorer browser.

To configure the Telnet session timeout from the CLI, run the **exec-timeout** global configuration command.

Configuring Line Console Carrier Detection for WAAS Devices

You should enable carrier detection if you plan to connect the WAAS device to a modem for receiving calls.

Note By default, this feature is disabled on a WAAS device.

To centrally enable Console Line Carrier Detection for a WAAS device or device group, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Network** > **Console Access** > **Console Carrier Detect**.

The Console Carrier Detect Settings window appears.

Step 3 Check the **Enable console line carrier detection before writing to the console** check box to enable the window for configuration.

Step 4 Click **Submit** to save the settings.

A message appears that explains that if a null-modem cable that does not have a carrier detect pin wired is being used, the WAE may appear unresponsive on the console until the carrier detect signal is asserted. To recover from a misconfiguration, the WAE should be rebooted and the 0x2000 bootflag should be set to ignore the carrier detect setting.

Step 5 Click **OK** to continue.

What to do next

To configure console line carrier detection from the CLI, you can use the **line console carrier-detect** global configuration command.

Configuring Remote Authentication Server Settings for Cisco WAAS Devices

If you have determined that your login authentication scheme should include one or more external authentication servers, you must configure these server settings before you can configure the authentication scheme in the Cisco WAAS Central Manager GUI. The section contains the following topics:

Configuring RADIUS Server Authentication Settings

RADIUS is a client/server authentication and authorization-access protocol used by a network access server (NAS) to authenticate users attempting to connect to a network device. The NAS functions as a client, passing user information to one or more RADIUS servers. The NAS permits or denies network access to a user based on the response that it receives from one or more RADIUS servers. RADIUS uses the User Datagram Protocol (UDP) for transport between the RADIUS client and server.

RADIUS authentication clients reside on devices that are running WAAS software. When enabled, these clients send authentication requests to a central RADIUS server, which contains user authentication and network service access information.

You can configure a RADIUS key on the client and server. If you configure a key on the client, it must be the same as the one configured on the RADIUS servers. The RADIUS clients and servers use the key to encrypt all the RADIUS packets transmitted. If you do not configure a RADIUS key, packets are not encrypted. The key itself is never transmitted over the network.

Note For more information about how the RADIUS protocol operates, see RFC 2138, *Remote Authentication Dial In User Service (RADIUS)* .

RADIUS authentication usually occurs when an administrator first logs in to the WAAS device to configure the device for monitoring, configuration, or troubleshooting purposes. RADIUS authentication is disabled by default. You can enable RADIUS authentication and other authentication methods at the same time. You can also specify which method to use first.

You can configure multiple RADIUS servers; authentication is attempted on the servers in order. If the first server is unreachable, then authentication is attempted on the other servers in the farm, in order. If authentication fails for any reason other than a server being unreachable, authentication is not attempted on the other servers in the farm.

Tip The WAAS Central Manager does not cache user authentication information. Therefore, the user is reauthenticated against the RADIUS server for every request. To prevent performance degradation caused by many authentication requests, install the WAAS Central Manager device in the same location as the RADIUS server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

To centrally configure RADIUS server settings for a WAAS device or device group, follow these steps:

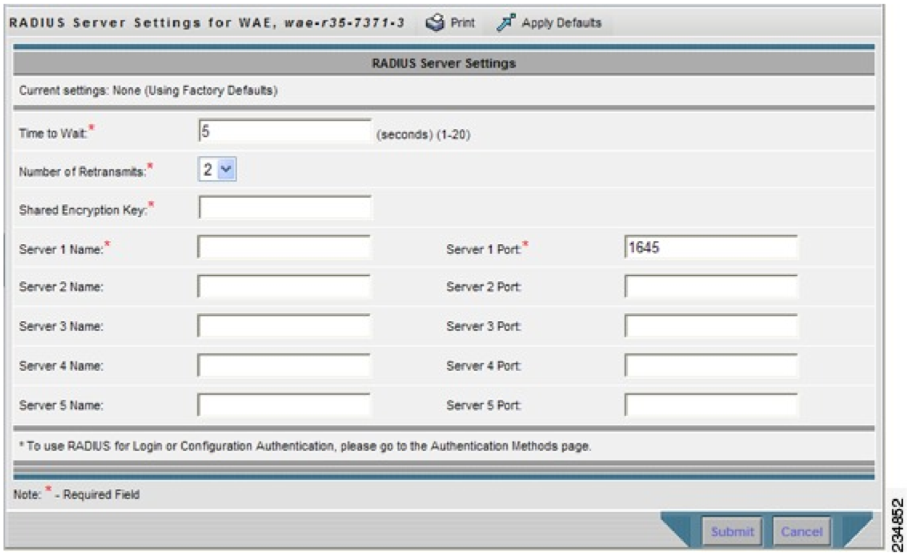
Procedure

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

Step 2 Choose **Configure** > **Security** > **AAA** > **RADIUS**.

The RADIUS Server Settings window appears. (See Figure 7-3 .)

Figure 41: RADIUS Server Settings Window



RADIUS Server Settings for WAE, wae-r35-7371-3

RADIUS Server Settings

Current settings: None (Using Factory Defaults)

Time to Wait:*	5 (seconds) (1-20)		
Number of Retransmits:*	2		
Shared Encryption Key:*			
Server 1 Name:*		Server 1 Port:*	1645
Server 2 Name:		Server 2 Port:	
Server 3 Name:		Server 3 Port:	
Server 4 Name:		Server 4 Port:	
Server 5 Name:		Server 5 Port:	

* To use RADIUS for Login or Configuration Authentication, please go to the Authentication Methods page.

Note: * - Required Field

Step 3 In the Time to Wait field, specify how long the device or device group should wait for a response from the RADIUS server before timing out. The range is from 1 to 20 seconds. The default value is 5 seconds.

Step 4 In the Number of Retransmits field, specify the number of attempts allowed to connect to a RADIUS server. The default value is 2 times.

Step 5 In the Shared Encryption Key field, enter the secret key that is used to communicate with the RADIUS server.

Note If you configure a RADIUS key on the WAAS device (the RADIUS client), make sure that you configure an identical key on the external RADIUS server. Do not use the following characters: space, backwards single quote (`), double quote ("), pipe (|), or question mark (?).

Step 6 In the Server Name field, enter an IP address (IPv4/IPv6) or hostname of the RADIUS server. Five different hosts are allowed.

Step 7 In the Server Port field, enter a UDP port number on which the RADIUS server is listening. You must specify at least one port. Five different ports are allowed.

Step 8 Click **Submit** to save the settings.

What to do next

You can now enable RADIUS as an administrative login authentication and authorization method for this WAAS device or device group, as described in Enabling Administrative Login Authentication and Authorization Schemes for Cisco WAAS Devices, on page 245.

To configure RADIUS settings from the CLI, you can use the **radius-server** global configuration command.

About TACACS+ Server Authentication Settings

TACACS+ controls access to network devices by exchanging network access server (NAS) information between a network device and a centralized database to determine the identity of a user or an entity. TACACS+ is an enhanced version of TACACS, a UDP-based access-control protocol specified by RFC 1492. TACACS+ uses TCP to ensure reliable delivery and encrypt all the traffic between the TACACS+ server and the TACACS+ daemon on a network device.

TACACS+ works with many authentication types, including fixed password, one-time password, and challenge-response authentication. TACACS+ authentication usually occurs when an administrator first logs in to the WAAS device to configure the WAE for monitoring, configuring, or troubleshooting.

When a user requests restricted services, TACACS+ encrypts the user password information using the MD5 encryption algorithm and adds a TACACS+ packet header. This header information identifies the packet type being sent, for example, an authentication packet, the packet sequence number, the encryption type used, and the total packet length. The TACACS+ protocol then forwards the packet to the TACACS+ server.

A TACACS+ server can provide authentication, authorization, and accounting functions. These services, while are all part of TACACS+, are independent of one another. Therefore a given TACACS+ configuration can use any or all of the three services.

When the TACACS+ server receives a packet, it does the following:

- Authenticates the user information and notifies the client that the login authentication has either succeeded or failed.
- Notifies the client that authentication will continue and that the client must provide additional information. This challenge-response process can continue through multiple iterations until login authentication either succeeds or fails.

You can configure a TACACS+ key on the client and server. If you configure a key on a WAAS device, it must be the same as the one configured on the TACACS+ servers. The TACACS+ clients and servers use the key to encrypt all the TACACS+ packets transmitted. If you do not configure a TACACS+ key, packets are not encrypted.

TACACS+ authentication is disabled by default. You can enable TACACS+ authentication and local authentication at the same time.

You can configure one primary and two backup TACACS+ servers; authentication is attempted on the primary server first. If the primary server is unreachable, authentication is attempted on the other servers in the farm, in order. If authentication fails for any reason other than a server being unreachable, authentication is not attempted on the other servers in the farm.

The TACACS+ database validates users before they gain access to a WAAS device. TACACS+ is derived from the United States Department of Defense (RFC 1492) and is used by Cisco Systems as an additional control of nonprivileged and privileged mode access. The Cisco WAAS software supports TACACS+ only and not TACACS or Extended TACACS.

If you are using TACACS+ for user authentication, you can create WAAS user group names that match the user groups that you have defined on the TACACS+ server. Cisco WAAS can then dynamically assign roles and domains to users based on their membership in the groups defined on the TACACS+ server. (See Working with Accounts in the chapter "Creating and Managing Administrative Groups.") You must specify associated group names for each user in the TACACS+ configuration file, as follows:

```
user = tacusr1 {
 default service = permit
 service = exec
 {
   waas_rbac_groups = admin,groupname1,groupname2
   priv-lvl = 15
 }
 global = cleartext "tac"
}
```

For each user, list the groups they belong to in the **waas_rbac_groups** attribute, separating each group from the next with a comma.

The dynamic assignment of roles and domains based on external user groups requires a TACACS+ server that supports shell custom attributes. For example, these are supported in Cisco ACS Version 4.x and 5.1 and later.

Tip The Cisco WAAS Central Manager does not cache user authentication information. Therefore a user is reauthenticated against the TACACS+ server for every request. To prevent performance degradation caused by many authentication requests, install the WAAS Central Manager device in the same location as the TACACS+ server, or as close as possible to it, to ensure that authentication requests can occur as quickly as possible.

Configuring TACACS+ Server Settings

The WAAS software CLI EXEC mode allows you to set, view, and test system operations. The mode is divided into two access levels: user and privileged. To access privileged-level EXEC mode, enter the enable EXEC command at the user access-level prompt and specify the admin password when prompted for a password.

In TACACS+, the enable password feature allows an administrator to define a different enable password per administrative-level user. If an administrative-level user logs in to the WAAS device with a normal-level user account (privilege level of 0) instead of an admin or admin-equivalent user account (privilege level of 15), that user must enter the admin password to access privileged EXEC mode.

```
WAE> enable
Password:
```

Note This caveat applies even if the WAAS users are using TACACS+ for login authentication.

To centrally configure TACACS+ server settings on a WAAS device or device group, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Security** > **AAA** > **TACACS+**.

The **TACACS+ Server Settings** window appears.

Note The TACACS+ server configuration cannot be modified or deleted when AAA Command Authorization is enabled.

Step 3 Check the **Use ASCII Password Authentication** check box to use the ASCII password type for authentication.

The default password type is PAP (Password Authentication Protocol). However, you can change the password type to ASCII when the authentication packets are to be sent in ASCII cleartext format.

Step 4 In the **Time to Wait** field, specify how long the device should wait before timing out. The range is from 1 to 20 seconds. The default value is 5 seconds.

Step 5 In the **Number of Retransmits** field, specify the number of attempts allowed to connect to a TACACS+ server. The range is 1 to 3 times. The default value is 2 times.

Step 6 In the **Security Word** field enter the secret key that is used to communicate with the TACACS+ server. The secret key value can contain a maximum of 32 alphanumeric characters. The following characters are not allowed: space, backwards single quote (`), double quote ("), pipe (|), number sign (#), question mark (?), or backslash (\).

Note The **Security Word** field is a mandatory field.

- When you configure a TACACS+ key on the WAAS device (the TACACS+ client), you must also configure an identical key on the external TACACS+ server.

Step 7 In the **Primary Server** field, enter an IP address (IPv4/IPv6) or hostname for the primary TACACS+ server.

To change the default port (49), enter the port in the Primary Server Port field.

Step 8 In the **Secondary Server** field, enter an IP address (IPv4/IPv6) or hostname for a secondary TACACS+ server.

To change the default port (49), enter the port in the **Secondary Server Port** field.

Step 9 In the **Tertiary Server** field, enter an IP address (IPv4/IPv6) or hostname for a tertiary TACACS+ server.

To change the default port (49), enter the port in the **Tertiary Server Port** field.

Note You can specify up to two backup TACACS+ servers.

Step 10 Click **Submit** to save the settings.

What to do next

You can now enable TACACS+ as an administrative login authentication and authorization method for this WAAS device or device group, as described in Enabling Administrative Login Authentication and Authorization Schemes for Cisco WAAS Devices, on page 245.

To configure TACACS+ settings from the CLI, run the **tacacs** global configuration command.

Configuring Windows Domain Server Authentication Settings

A Microsoft Windows domain controller can be configured to control access to the Cisco WAAS software services using either a challenge/response or shared secret authentication method. The system administrator can log in to the Cisco WAAS device by using an FTP, SSH, or Telnet session, the console, or the Cisco WAAS Central Manager GUI with a single user account (username/password/privilege). RADIUS and TACACS+ authentication schemes can be configured simultaneously with Windows domain authentication. Logging of a variety of authentication login statistics can be configured when Windows domain authentication is enabled. The log files and the statistical counters and related information can be cleared at any time.

In a Cisco WAAS network, Microsoft Windows domain authentication is used in the following scenarios:

- Logging in to the WAAS Central Manager GUI
- CLI configuration on any WAAS device

You can configure Windows authentication for the Cisco WAAS Central Manager device, a single Cisco WAAS device, or a group of devices. To configure Windows domain authentication on a Cisco WAAS device, configure a set of Windows domain authentication settings.

Note Windows domain authentication is not performed unless a Windows domain server is configured on the WAAS device. If the device is not successfully registered, authentication and authorization do not occur. WAAS supports authentication by a Windows domain controller running only on Windows Server 2000, Windows Server 2003, or Windows Server 2008.

This section contains the following topics:

Configuring Windows Domain Server Settings on a Cisco WAAS Device

To configure Windows Domain server settings on a Cisco WAAS device or device group, follow these steps:

Before you begin

You should know the name and IP address, or hostname, of the Windows domain controller that will be used for authentication.

Procedure

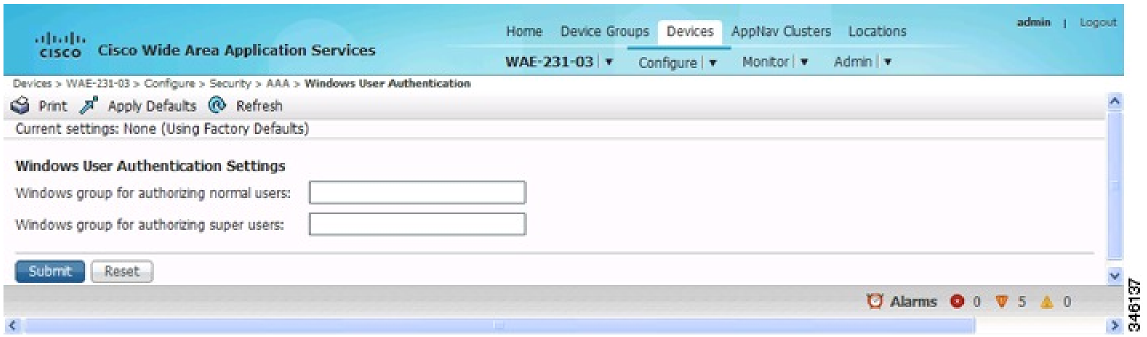
Step 1 From the WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 2 Choose **Configure** > **Security** > **AAA** > **Windows User Authentication**.

The **Windows User Authentication** window appears.

Note Workgroup settings are only required for Windows domain authentication, not for a domain join. You can skip to workgroup settings if you are only performing a domain join.

Figure 42: Windows User Authentication



Devices > WAE-231-03 > Configure > Security > AAA > Windows User Authentication

Current settings: None (Using Factory Defaults)

Windows User Authentication Settings

Windows group for authorizing normal users:

Windows group for authorizing super users:

Step 3 In the **Windows group for authorizing normal users** field, specify an administrative group for normal users (nonsuperuser administrators), who only have restricted access to the chosen device (or device group) because their administrator user account has a privilege level of **0**.

Note By default, there are no predefined user groups for Windows domain authorization configured on a WAE.

Step 4 In the Windows group for authorizing super users field, specify an administrative group for superusers (superuser administrators), who have unrestricted access to the chosen device (or device group) because their administrator user account has a privilege level of **15**.

Note In addition to configuring Windows domain administrative group on a WAE, you must configure the Windows domain administrative group on your Microsoft Windows 2000, 2003, or 2008 server. You must create a Windows Domain administrative superuser group and a normal user group. Make sure that the group scope for the superuser group is set to global, assign user member to newly created administrative group, and add the user account, for example, the winsuper user, to the Windows domain superuser group. For more information about how to configure the Windows domain administrative group on your Windows server, see the corresponding Microsoft documentation.

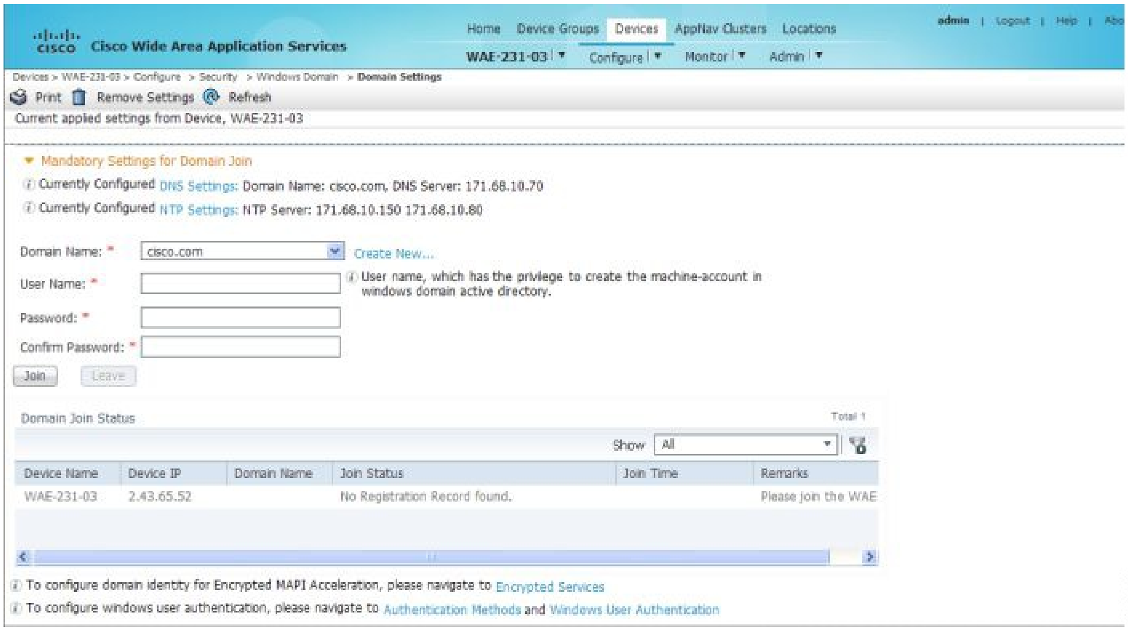
When a user attempts to access this WAE through a Telnet session, FTP, or SSH session, the WAE is configured to use the Active Directory user database to authenticate a request for administrative access.

Step 5 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 6 Choose **Configure** > **Security** > **Windows Domain** > **Domain Settings**.

The **Domain Settings** window appears.

Figure 43: Domain Settings



Current applied settings from Device, WAE-231-03

Currently Configured DNS Settings: Domain Name: cisco.com, DNS Server: 171.68.10.70

Currently Configured NTP Settings: NTP Server: 171.68.10.150 171.68.10.80

Domain Name: * cisco.com

User Name: *

Password: *

Confirm Password: *

User name, which has the privlege to create the machine-account in windows domain active directory.

Domain Join Status

Total 1

Show: All

Device Name	Device IP	Domain Name	Join Status	Join Time	Remarks
WAE-231-03	2.43.65.52		No Registration Record found.		Please join the WAE

To configure domain identity for Encrypted MAPI Acceleration, please navigate to Encrypted Services

To configure windows user authentication, please navigate to Authentication Methods and Windows User Authentication

Consider the following guidelines:

- In Cisco WAAS versions earlier than 5.1.1, if the related WINS server and the workgroup or domain name have not been defined for the chosen device (or device group), an informational message is displayed at the top of this window to inform you that these related settings are currently not defined.
- To define these settings, choose **Configure > Network > WINS**. Domain name, DNS server, and NTP configuration are mandatory prerequisites for the Windows domain join. The Windows domain controller and the Cisco WAAS device must be in time sync for Kerberos authentication to succeed. For full AAA functionality, workgroup and WINS server must also be configured.
- In Cisco WAAS versions earlier than 5.1.1, NetBIOS name does not have to be configured for Windows domain join. If left unconfigured, the first 15 characters of the hostname are automatically assigned as the NetBIOS name during the join. For WAAS versions later than 5.1.1, NetBIOS name, WINS server, and workgroup configuration settings are not required for Windows domain authentication configuration.

Step 7 From the **Domain Name** drop-down list, choose a name or click **Create New** to create a new Local Domain Name.

Step 8 If your Cisco WAAS device (or device group) is a previous version of the software.

a) Choose Kerberos, NTLM1 plus ESS (Extended Session Security), or NTLM2 as a shared secure authentication method for administrative logins to the chosen device (or device group). The default authentication protocol is kerberos.

Note In Cisco WAAS Version 5.0.1 and later, Windows domain user login authentication using NTLM protocol is deprecated. We recommend that you use Kerberos protocol for Windows domain user login authentication.

Note In Cisco WAAS Version 5.1.1 and later, Windows domain user authentication using NTLM protocol is not supported.You can use the Kerberos protocol, NTLMv1 plus ESS (Extended Session Security), or NTLMv2 for encrypted MAPI acceleration.

Click **Auto Detect the Parameters** when using Kerberos to automatically obtain the kerberos realm, kerberos server, and domain controller. Domain, DNS, and NTP parameters must be configured first. This option is not supported with NTLM.

After the device is queried for the parameters, a status message is displayed on the screen indicating either success or failure. The process may not be immediate and the status message will not appear until the auto detection process is completed.

When successful, the parameters can be reviewed and edited, if required. After the parameters are reviewed, the values can be submitted.

If auto detection fails, check the configured domain/DNS configuration and enter them manually. The values can then be submitted.

Note Kerberos Version 5 is used for Windows systems running Windows 2000 or later, with users logging in to domain accounts. For Windows domain join using Kerberos authentication, you must have the following ports open on the firewall for outgoing traffic: 53 UDP/TCP, 88 UDP/TCP, 123 UDP, 135 TCP, 137 UDP, 139 TCP, 389 UDP/TCP, 445 TCP, 464 UDP/TCP, and 3268 TCP.

b) (Skip this step for Kerberos) For NTLM, choose version 1 or version 2 from the drop-down list. NTLM Version 1 is selected by default.

Note For Cisco WAAS Version 5.3.1, NTLM is also supported for encrypted MAPI (EMAPI). Note the following about NTLM for EMAPI:NTLM for EMAPI does not require any additional configuration other than what is required for Kerberos. However, the client must be joined to the domain.NTLM with EMAPI uses a key for each NTLM user. These keys are stored in memory and removed after a reload. If, for example, a core WAE is rebooted during the night, all NTLM keys need to be gathered again at startup, which may cause an increase in latency in establishing the client-server connection.

- NTLM Version 1 is used for all Windows systems, including legacy systems such as Windows 98 with Active Directory, Windows NT, and more recent Windows systems, such as Windows 2000, Windows XP, and Windows 2003. We recommend the use of Kerberos if you are using a Windows 2000 SP4 or Windows 2003 domain controller.
- NTLM Version 2 is used for Windows systems running Windows 98 with Active Directory, Windows NT 4.0 (Service Pack 4 or later), Windows XP, Windows 2000, and Windows 2003. Enabling NTLM Version 2 support on the WAAS print server will not allow access to clients who use NTLM or LM.

Caution Enable NTLM Version 2 support in the print server only if all the clients' security policy has been set to Send NTLMv2 responses only/Refuse LM and NTLM.

c) (Skip this step for NTLM) In the **Kerberos Realm** field, enter the fully qualified name of the realm in which the WAAS device resides. In the Key Distribution center, enter the fully qualified name or the IP address of the distribution center for the Kerberos key. If you clicked Auto Detect The Parameters when you selected the Kerberos authentication method, these fields will already be populated.

All Windows 2000 domains are also Kerberos realms. Because the Windows 2000 domain name is also a DNS domain name, the Kerberos realm name for the Windows 2000 domain name is always in uppercase letters. This capitalization follows the recommendation for using DNS names as realm names in the Kerberos Version 5 protocol document (RFC-4120) and affects only interoperability with other Kerberos-based environments.

d) In the **Domain Controller** field, enter the name of the Windows Domain Controller.

When you click **Submit**, the Cisco WAAS Central Manager validates this name by requesting the Cisco WAAS device to resolve the domain controller name. If the domain controller is not resolvable, you are asked to submit a valid name. If the device is offline, you are asked to verify device connectivity. If you are configuring a device group, the domain controller name is not validated on each device before this page is accepted and if it is not resolvable on a device, the configuration changes on this page are not applied to that device.

e) Click **Submit**.

Note Make sure that you click **Submit** now so that the specified changes are committed to the Cisco WAAS Central Manager database. The Domain Administrator's username and password, which you will enter in Step 9 , are not stored in the Cisco WAAS Central Manager's database.

Step 9 To register the chosen device (or device group) with the Windows Domain Controller, follow these steps:

a) In the **User Name** field, enter a username (the domain\username or the domain name plus the username) for the specified Windows Domain Controller. This must be the username and password of a user who has administrative privileges in Active Directory (permission to add a computer to a domain).

If your Cisco WAAS device (or device group) is running a previous version of the software, click the **Domain Join** tab. For NTLM, the user credentials can be any normal user that belongs to the Domain Users group. For Kerberos, the user credentials must be a user that belongs to the **Domain Admins** group, but does not need to be the system default Administrator user.

Note To use Windows domain server authentication, the Cisco WAAS device must join the Windows domain. For registration, you will require a user credential with permission to join a machine to the Windows domain. The user credential used for registration is not shown in clear text anywhere, including log files. Cisco WAAS does not modify the structure or schema of the Windows Active Directory.

Note A domain join is required for encrypted MAPI acceleration using a machine account.

b) In the **Password** field, enter the password of the specified Windows Domain Controller account.
c) In the **Confirm password** field, re-enter the password of the specified Windows Domain Controller.
d) (Optional, if your Cisco WAAS device or device group is running a previous version of the software) If necessary, enter the name of the organizational unit in the **Organizational Unit** field (for Kerberos authentication only).
e) Click **Join**.

Note When you click **Join**, the Cisco WAAS Central Manager immediately sends a registration request to the Cisco WAAS device (or all of the devices in the device group) using SSH (the specified domain administrator password is encrypted by SSH). The registration request instructs the device to perform domain registration with the specified Windows Domain Controller using the specified domain username and password. If the device is accessible (if it is behind a NAT and has an external IP address), the registration request is performed by the device (or device group).

The status of the registration request is shown in the **Domain Join Status** table.

f) If your Cisco WAAS device or device group is running a version of the software that is earlier than latest version of Cisco WAAS, click the **Show Join Status** button to view the status of the registration request.

It may take a few moments for the results to be updated. You can also click the **Refresh** button on the **Domain Join Status** table to see the status of the device. If the join request fails, the result is shown in the table.

g) Wait for a few more minutes and try again to see the updated authentication status.

If the request succeeds, the domain registration status is shown in the **Domain Join Status** table.

What to do next

After configuring the Windows domain settings, to complete the process of enabling Windows authentication, you must set Windows as the authentication and authorization method for the device by using the Authentication Methods window, as described in the Enabling Administrative Login Authentication and Authorization Schemes for Cisco WAAS Devices, on page 245.

We recommend that you use the Cisco WAAS Central Manager GUI instead of the Cisco WAAS CLI to configure the Windows Domain server settings, but if you want to use the CLI, see the following commands in the *Cisco Wide Area Application Services Command Reference*: **windows-domain join** and **kerberos** (if you are using Kerberos as a shared secure authentication method).

You must first configure the IP domain name and IP name server by running the **ip** global configuration command.

Next, configure the appropriate NTP server by running the **ntp** global configuration command.

Next, configure the windows domain administrative supergroup and normal group running the following global configuration commands:

```
WAE(config)# windows-domain administrative group super-user group_name
WAE(config)# windows-domain administrative group normal-user group_name
```

Next, register the Cisco WAAS device with the Windows domain server that you configured, by running the following command:

```
WAE# windows-domain join domain-name DomainName
 user UserName
```

To create a machine account in a specific organizational unit, run following command:

```
WAE# windows-domain join domain-name DomainName organization-unit OUName user UserName
```

Finally, enable Windows Domain as the administrative login authentication and authorization configuration by running the following commands:

```
WAE(config)# authentication login windows-domain enable primary
WAE(config)# authentication configuration windows-domain enable primary
```

Unregistering a WAE from a Windows Domain Controller

Before you begin

If you want to unregister a WAE device from a Windows domain controller, you can do that directly from the WAAS Central Manager, as long as you have used the Kerberos shared secure authentication method. If you have used the NTLM method, you cannot unregister the WAE by using the WAAS Central Manager; you must log in to the domain controller and remove the device registration manually.

Note Before you can unregister a device, you must disable Windows authentication for the device. Also, if Encrypted MAPI is utilizing the machine account domain identity, you must remove it before performing a domain leave.

Procedure

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

Step 2 Choose **Configure** > **Security** > **AAA** > **Authentication Methods**.

The **Authentication and Authorization Methods** window appears.

Step 3 Under both the Authentication Login Methods and the Authorization Methods sections, change the value WINDOWS that is already chosen by choosing another value from the drop-down lists. For more information about changing these settings, see Enabling Administrative Login Authentication and Authorization Schemes for Cisco WAAS Devices, on page 245.

Step 4 To save the settings, click **Submit**.

Step 5 Choose **Configure** > **Security** > **Windows Domain** > **Domain Settings**. If your WAAS device (or device group) is running a previous version of the software, click the **Domain Join** tab.

Step 6 (Optional) Enter the administrative username and password in the Administrator Username, Password, and Confirm Password fields. The domain controller requires the username and password to perform the unregistration.

Step 7 Click **Leave**.

Note When you click **Leave**, the Cisco WAAS Central Manager immediately sends an unregistration request to the WAAS device (or device group) using SSH. The unregistration request instructs the device to unregister from the specified Windows Domain Controller. Request to unregister the device is not allowed when encrypted MAPI is configured to use machine accounts. You must delete the machine account identity before proceeding with the leave.

The status of the unregistration request is shown in the Domain Join Status table.

Step 8 If your WAAS device (or device group) is running a previous version of the software, check the status of the unregistration request by waiting a few minutes and click **Show Join Status**.

What to do next

If you want to use the CLI to unregister a WAE device, you must first use the following commands to disable windows authentication:

```
WAE(config)# no authentication login windows-domain enable
WAE(config)# no authentication configuration windows-domain enable
```

Note If an Encrypted MAPI machine account identity has been configured, then it has to be removed first. Use the no windows-domain encryption-service global configuration command to remove a machine account identity.

Next, unregister the WAAS device from the Windows domain server by using the following command (for Kerberos authentication):

```
WAE# windows-domain leave user UserName
 password Password
```

There is no CLI command to unregister the Cisco WAAS device if it is using NTLM authentication.

LDAP Server Signing

This section contains the following topics:

About LDAP Server Signing

Lightweight Directory Access Protocol (LDAP) server signing is a configuration option of the Microsoft Windows Server's Network security settings. This option controls the signing requirements for LDAP clients. LDAP signing is used to verify that an intermediate party did not tamper with the LDAP packets on the network and to guarantee that the packaged data comes from a known source. Windows Server 2003 administration tools use LDAP signing to secure communications between running instances of these tools and the servers that they administer.

By using the Transport Layer Security (TLS, RFC 2830) protocol to provide communications privacy over the Internet, client/server applications can communicate in a way that prevents eavesdropping, tampering, or message forging. TLS v1 is similar to Secure Sockets Layer (SSL). TLS offers the same encryption on regular LDAP connections (ldap://:389) as SSL, while operating on a secure connection (ldaps://:636). A server certificate is used by the TLS protocol to provide a secure, encrypted connection to the LDAP server. A client certificate and key pair are required for client authentication.

In the Cisco WAAS software, login authentication with Windows 2003 domains is supported when the **LDAP server signing requirements** option for the Domain Security Policy is set to **Require signing**. The LDAP server signing feature allows the WAE to join the domain and authenticate users securely.

Note When you configure your Windows domain controller to require an LDAP signature, you must also configure LDAP signing on the client WAE. By not configuring the client to use LDAP signatures, communication with the server is affected, and user authentication, group policy settings, and login scripts might fail. Install the Certification Authority service on the Microsoft server with the server's certificate (**Programs** > **Administrative Tools** > **Certification Authority**). Enable the LDAP server signing requirements property on the Microsoft server (**Start** > **Programs** > **Administrative Tools** > **Domain Controller Security Policy**). In the window that is displayed, choose **Require signing** from the drop-down list, and click **OK**. For information about how to configure your Windows domain controller to require an LDAP signature, see your Microsoft documentation.

Configuring LDAP Signing on the Client WAEs

You can configure a security setting on Windows 2003 domain controllers to require clients (such as WAEs) to sign LDAP requests. Because unsigned network traffic can be intercepted and manipulated by outside parties, some organizations require LDAP server signing to prevent man-in-the-middle attacks on their LDAP servers. You configure LDAP signing only on a single WAE; it cannot be configured at a system level. In addition, you must configure LDAP signing on a WAE through the WAAS CLI; you cannot configure LDAP signing through any of the WAAS GUI.

By default, LDAP server signing is disabled on a WAE. To enable this feature on a WAE, follow these steps:

Procedure

Step 1 Enable LDAP server signing on the WAE:

```
WAE# configure
WAE(config)# smb-conf section "global" name "ldap ssl" value "yes"
```

Step 2 Save the configuration on the WAE:

```
WAE(config)# exit
WAE# copy run start
```

Step 3 Verify the current running LDAP client configuration on the WAE:

```
WAE# show smb-conf
```

Step 4 Register the WAE with the Windows domain:

```
WAE# windows-domain diagnostics net "ads join -U username%password"
```

Step 5 Enable user login authentication on the WAE:

```
WAE# configure
WAE(config)# authentication login windows-domain enable primary
```

Step 6 Enable user login authorization on the WAE:

```
WAE(config)# authentication configuration windows-domain enable primary
```

Step 7 Check the current configuration for login authentication and authorization on the WAE:

```
WAE# show authentication user
Login Authentication:    Console/Telnet/Ftp/SSH Session
----------------------------- ------------------------------
local                                enabled (secondary)
Windows domain           enabled (primary)
```

```
Radius                            disabled
Tacacs+                          disabled
Configuration Authentication: Console/Telnet/Ftp/SSH Session
----------------------------- ------------------------------
local                                 enabled (primary)
Windows domain           enabled (primary)
Radius                             disabled
Tacacs+                           disabled
```

The WAE is now configured to authenticate Active Directory users, who can use Telnet, FTP, or SSH to connect to the WAE. Alternatively, they can access the WAE through the Cisco WAAS GUI.

Step 8 View statistics that are related to Windows domain user authentication. Statistics increment after each user authentication attempt:

```
WAE# show statistics windows-domain
Windows Domain Statistics
  -----------------------------------------------
  Authentication:
    Number of access requests:                      9
    Number of access deny responses:                3
    Number of access allow responses:               6
  Authorization:
    Number of authorization requests:                9
    Number of authorization failure responses:       3
    Number of authorization success responses:       6
  Accounting:
    Number of accounting requests:                   0
    Number of accounting failure responses:          0
    Number of accounting success responses:          0
WAE# show statistics authentication

    Authentication  Statistics
    --------------------------------------
    Number of access requests:        9
    Number of access deny responses:  3
    Number of access allow responses: 6
```

Step 9 To clear statistics on the WAE, run the **clear statistics** EXEC command:

- To clear all the login authentication statistics, enter the **clear statistics authentication** EXEC command.
- To clear only the statistics that are related to Windows domain authentication, run the **clear statistics windows-domain** EXEC command.
- To clear all the statistics, run the **clear statistics** all EXEC command.

Disabling LDAP Server Signing on a Client WAE

To disable LDAP server signing on a WAE, follow these steps:

Procedure

Step 1 Unregister the WAE from the Windows domain:

```
WAE# windows-domain diagnostics net "ads leave -U Administrator"
```

Step 2 Disable user login authentication:

```
WAE# configure
WAE(config)# no authentication login windows-domain enable primary
```

Step 3 Disable LDAP signing on the WAE:

```
WAE(config)# no smb-conf section "global" name "ldap ssl" value "yes"
```

Enabling Administrative Login Authentication and Authorization Schemes for Cisco WAAS Devices

This section describes how to centrally enable the various administrative login authentication and authorization schemes (the authentication configuration) for a WAAS device or device group.

Caution Make sure that RADIUS, TACACS+, or Windows domain authentication is configured and operating correctly before disabling local authentication and authorization. If you disable local authentication, and if RADIUS, TACACS+, or Windows domain authentication is not configured correctly, or if the RADIUS, TACACS+, or Windows domain server is not online, you will be unable to log in to the WAAS device.

By default, a WAAS device uses the local database to authenticate and authorize administrative login requests. The WAAS device verifies whether all the authentication databases are disabled, and if so, sets the system to the default state. For information on this default state, see Default Administrative Login Authentication and Authorization Configuration, on page 222.

Note You must configure the TACACS+, RADIUS, or Windows server settings for the WAAS device (or device group) before you configure and submit these settings. For information on how to configure these server settings on a WAAS device or device group, see About TACACS+ Server Authentication Settings, on page 233, and Configuring RADIUS Server Authentication Settings, on page 231, and Configuring Windows Domain Server Authentication Settings, on page 235.

By default, WAAS devices fail over to the secondary method of administrative login authentication whenever the primary administrative login authentication method fails for any reason. Change this default login authentication failover method through the WAAS Central Manager GUI, as follows:

- To change the default for a Cisco WAAS device, choose **Devices** > *device-name* and then choose **Configure** > **Security** > **AAA** > **Authentication Methods** from the menu. Check the **Failover to next available authentication method** box in the displayed window and click **Submit**.
- To change the default for a device group, choose **Device Groups** > *device-group-name* and then choose **Configure** > **Security** > **AAA** > **Authentication Methods** from the menu. Check the **Failover to next available authentication method** box in the displayed window and click **Submit**.

After you enable the failover to next available authentication method option, the Cisco WAAS device (or the devices in the device group) queries the next authentication method only if the administrative login authentication server is unreachable, not if authentication fails for some other reason. The authentication server could be unreachable due to an incorrect key in the RADIUS or TACACS+ settings on the WAAS device.

You can configure multiple TACACS+ or RADIUS servers; authentication is attempted on the primary server first. If the primary server is unreachable, then authentication is attempted on the other servers in the TACACS+ or RADIUS farm, in order. If authentication fails for any reason other than a server being unreachable, authentication is not attempted on the other servers in the farm. This process applies regardless of the setting of the **Failover to next available authentication method** check box.

Note To use the login authentication failover feature, you must set TACACS+, RADIUS, or Windows domain as the primary login authentication method, and local as the secondary login authentication method.

If the failover to the next available authentication method option is **enabled**, follow these guidelines:

- You can configure only two login authentication schemes (a primary and secondary scheme) on the WAAS device.
- Note that the WAAS device (or the devices in the device group) fails over from the primary authentication scheme to the secondary authentication scheme only if the specified authentication server is unreachable.
- Configure the local database scheme as the secondary scheme for both authentication and authorization (configuration).

For example, if the failover to next available authentication method option is enabled and RADIUS is set as the primary login authentication scheme and local is set as the secondary login authentication scheme, the following events occur:

1. When the Cisco WAAS device (or the devices in the device group) receives an administrative login request, it queries the external RADIUS authentication server.
2. One of the following occurs:
    a. If the RADIUS server is reachable, the Cisco WAAS device (or the devices in the device group) uses this RADIUS database to authenticate the administrator.
    b. If the RADIUS server is not reachable, the Cisco WAAS device (or the devices in the device group) tries the secondary authentication scheme (that is, it queries its local authentication database) to authenticate the administrator.

Note The local database is contacted for authentication only if this RADIUS server is not available. In any other situation, for example, if the authentication fails in the RADIUS server, the local database is not contacted for authentication.

Conversely, if the failover to the next available authentication method option is **disabled**, the Cisco WAAS device (or the devices in the device group) contacts the secondary authentication database regardless of the reason why the authentication failed with the primary authentication database.

If all the authentication databases are enabled for use, then all the databases are queried in the order of priority selected and based on the failover reason. If no failover reason is specified, then all the databases are queried in the order of their priority. For example, first the primary authentication database is queried, then the secondary authentication database is queried, then the tertiary database is queried, and finally the quaternary authentication database is queried.

To specify the login authentication and authorization scheme for a Cisco WAAS device or device group, follow these steps:

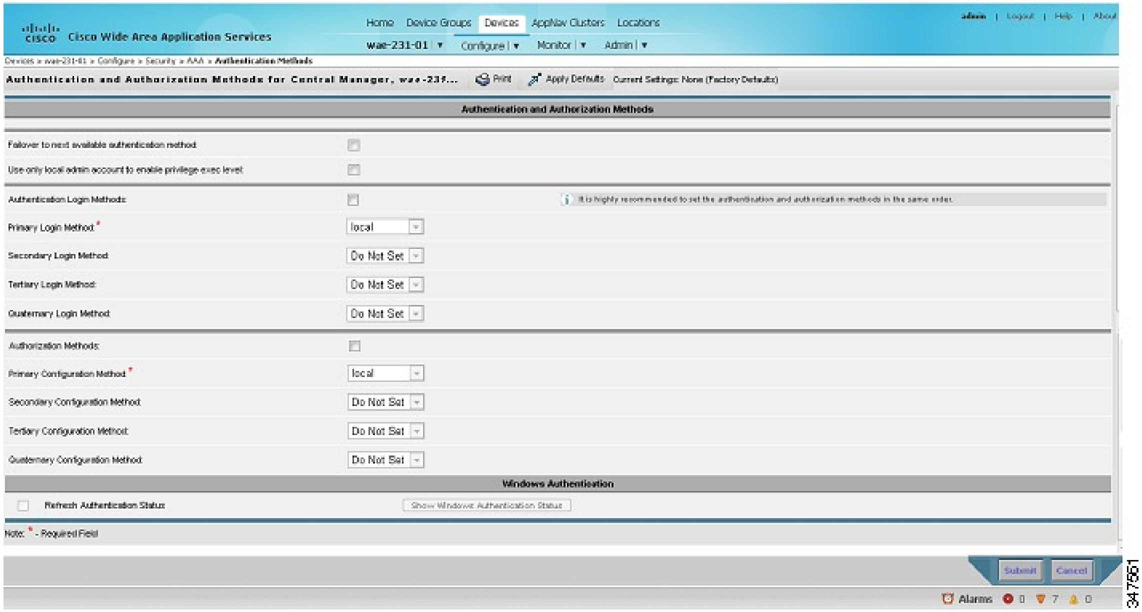
Procedure

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

Step 2 Choose **Configure** > **Security** > **AAA** > **Authentication Methods**.

The Authentication and Authorization Methods window appears.

Figure 44: Authentication and Authorization Methods Window


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
admin | Logout | Help | About
wae-231-01 ▾
Configure ▾
Monitor ▾
Admin ▾
Devices > wae-231-01 > Configure > Security > AAA > Authentication Methods
Print
Apply Defaults
Submit
Cancel
Alarms 0 7 0
347561

Authentication and Authorization Methods for Central Manager, wae-231...

Current Settings: None (Factory Defaults)

Authentication and Authorization Methods

Failover to next available authentication method: □

Use only local admin account to enable privilege exec level: □

Authentication Login Methods: □

It is highly recommended to set the authentication and authorization methods in the same order.

Primary Login Method:* local

Secondary Login Method: Do Not Set

Tertiary Login Method: Do Not Set

Quaternary Login Method: Do Not Set

Authorization Methods: □

Primary Configuration Method:* local

Secondary Configuration Method: Do Not Set

Tertiary Configuration Method: Do Not Set

Quaternary Configuration Method: Do Not Set

Windows Authentication

□ Refresh Authentication Status   Show Windows Authentication Status

Note: * - Required Field

Step 3 Check the **Failover to next available authentication method** check box to query the secondary authentication database only if the primary authentication server is unreachable. When the check box is unchecked, the other authentication methods are tried if the primary method fails for any reason.

To use this feature, you must set TACACS+, RADIUS, or Windows domain as the primary authentication method, and local as a secondary authentication method. Make sure that you configure the local method as a secondary scheme for both authentication and authorization (configuration).

Check the Use only local admin account to enable privilege exec level check box to configure enable authentication by using the local admin user account password. In this case, the request for enable access is not sent to the external authentication servers, but is processed on the WAE. It uses only the local “admin” user account password to verify the given password, and to provide access.

Step 4 Check the **Authentication Login Methods** check box to enable authentication privileges using the local, TACACS+, RADIUS, or WINDOWS databases.

Step 5 Specify the order of the login authentication methods that the chosen device or device group are to use:

a) From the Primary Login Method drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **Windows**. This option specifies the first method that the chosen device (or the device group) should use for administrative login authentication.

b) From the **Secondary Login Method** drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **Windows**. This option specifies the method that the chosen device (or the device group) should use for administrative login authentication if the primary method fails.

c) From the **Tertiary Login Method** drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **Windows**. This option specifies the method that the chosen device (or the device group) should use for administrative login authentication if both the primary and the secondary methods fail.

d) From the **Quaternary Login Method** drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **Windows**. This option specifies the method that the chosen device (or device group) should use for administrative login authentication if the primary, secondary, and tertiary methods all fail.

Note We strongly recommend that you specify the local method as the last method in your prioritized list of login authentication and authorization methods. By adhering to this practice, the WAAS administrator will be able to log in to a Cisco WAAS device (or the devices in the device groups) through the local authentication and authorization method if the specified external third-party servers (TACACS+, RADIUS, or Windows domain servers) are not reachable.

Step 6 Check the **Authorization Methods** check box to enable authorization privileges using the local, **TACACS+**, **RADIUS**, or **Windows** databases.

Note Authorization privileges apply to console and Telnet connection attempts, secure FTP (SFTP) sessions, and Secure Shell (SSH Version 2) sessions.

Step 7 Specify the order of the login authorization (configuration) methods that the chosen device (or the device group) should use:

Note We strongly recommend that you set the administrative login authentication and authorization methods in the same order. For example, configure the Cisco WAAS device (or device group) to use RADIUS as the primary login method, TACACS+ as the secondary login method, Windows as the tertiary method, and the local method as the quaternary method for both administrative login authentication and authorization.

a) From the **Primary Configuration Method** drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **Windows**. This option specifies the first method that the chosen device (or the device group) should use to determine authorization privileges.

Note If you have checked the **Failover to next available authentication method** check box (Step 3), make sure that you choose **TACACS+** or **RADIUS** from the **Primary Configuration Method** drop-down list to configure either the TACACS+ or RADIUS method as the primary scheme for authorization (configuration).

b) From the **Secondary Configuration Method** drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **Windows**. This option specifies the method that the chosen device (or the device group) should use to determine authorization privileges if the primary method fails.

Note If you have checked the **Failover to next available authentication method** check box (Step 3), make sure that you choose **local** from the **Secondary Configuration Method** drop-down list to configure the local method as the secondary scheme for authorization (configuration).

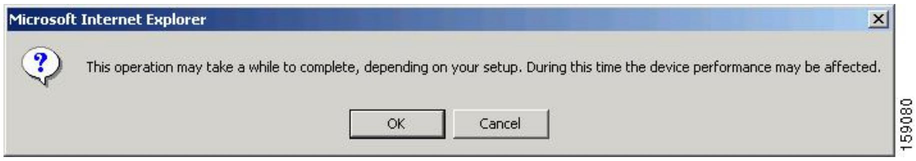
c) From the **Tertiary Configuration Method** drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **Windows**. This option specifies the method that the chosen device (or the device group) should use to determine authorization privileges if both the primary and secondary methods fail.

d) From the **Quaternary Configuration Method** drop-down list, choose **local**, **TACACS+**, **RADIUS**, or **Windows**. This option specifies the method that the chosen device (or device group) should use to determine authorization privileges if the primary, secondary, and tertiary methods all fail.

Step 8 To refresh the authentication status, check the check box and click **Show Windows Authentication Status**. This option is only available when Windows is set as the authentication and authorization methods.

A dialog box prompts you about whether or not you want to continue with this request to refresh the status of the authentication request.

Figure 45: Confirmation Dialog Box



Microsoft Internet Explorer

This operation may take a while to complete, depending on your setup. During this time the device performance may be affected.

Step 9 Click **OK** to continue or click **Cancel** to cancel the request.

If the request fails, an error dialog box is displayed. Wait for a few more minutes and try again to see the updated authentication status.

Step 10 Click **Submit** to save the settings.

Note If you have enabled the Windows authentication or authorization method, the Central Manager queries the WAE (of Cisco WAAS Version 4.2.1 or later) to ensure that it is registered to a Windows domain. This can take up to one minute after you click **Submit**. You will see a message asking you to confirm this process. Click **OK** to proceed. If you are configuring a WAE of Version 4.1.x or earlier, or a device group, the Central Manager does not query the WAEs and you must ensure that each WAE is properly registered. You will see a message informing you that system behavior is unknown (if a WAE is unregistered). Click **OK** to proceed.

Note If you have enabled the Windows authentication method, it takes about 15 seconds to activate it. Wait for at least 15 seconds before verifying the Windows authentication status or performing any operation that requires Windows authentication.

To configure the login authentication and authorization scheme from the CLI, run the **authentication** global configuration command. Before you enable Windows domain authentication or authorization for a device, the device must be registered with the Windows domain controller.

Configuring AAA Command Authorization

Command authorization enforces authorization through an external AAA server for each command executed by the CLI user. All the commands executed by a CLI user are authorized before they are executed. RADIUS, Windows domain, and local users are not affected.

Note Only commands executed through the CLI interface are subject to command authorization. When command authorization is enabled, you must specify "permit null" on the TACACS+ server to allow authorized commands with no arguments to be executed.

To configure command authorization for a WAAS device or device group, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Security** > **AAA** > **Command Authorization Settings**.

The **Command Authorization** window appears.

Step 3 Check the **Command Authorization Level** check box to mark the desired level:

- **Level 0**: Only EXEC commands are authorized by the TACACS+ server before they are executed, regardless of user level (normal or super). Global configuration commands are not allowed.
- **Level 15**: Both EXEC and global configuration level commands are authorized by the TACACS+ server before they are executed, regardless of user level (normal or super).

Note You must have a TACACS+ server configured before you can configure command authorization.

Step 4 To save the settings, click **Submit**.

Configuring Cisco Prime Network Control System Single Sign-On

New IOS/WAAS features, such as AppNav and kWAAS, require the use of both WAAS and Cisco Prime Network Control System (NCS) management systems at the same time. Lack of integration between the NCS and WAAS CM impairs user experience. NCS Single Sign-On (SSO) functionality provides a way to integrate these two systems and seamlessly launch the WAAS CM from NCS.

The NCS integration has the following prerequisites:

- The NCS device is running the 2.x code.
- The Cisco IOS-XE device must be running 3.10 code.
- The Cisco WAAS 5.3.0 or later Central Manager is installed and configured.
- The IOS-XE device with kWAAS instance is configured.
- The vWAAS instance is registered with the Cisco WAAS Central Manager.

To configure the NCS, follow the steps below:

Procedure

Step 1 Configure the NCS device. For more information, see Configuring the NCS Device, on page 251.

Step 2 Configure the Cisco WAAS Central Manager. For more information, see Configuring the Cisco WAAS Central Manager to Use SSO.

Step 3 Use the **Single Sign-on** feature. For more information, see Launching Cisco WAAS Central Manager from NCS, on page 252.

Configuring the NCS Device

To configure the NCS Server follow these steps:

Procedure

Step 1 Log in to Prime NCS to add the SSO server:

a) Choose **Administration** > **Users, Roles & AAA** > **SSO servers.**
b) Enter the SSO server information, then click **Save**.

Note If you use an external Cisco Prime host for SSO, specify the IP address of that host. If you do not currently use the SSO functionality to log in to Cisco Prime, use the IP address of the Cisco Prime device itself.

Step 2 To enable SSO authentication:

a) Choose **Administration** > **Users, Roles & AAA** > **AAA mode**.
b) Click the **SSO mode** radio button. Click Save.

Step 3 To configure WAAS CM address:

a) Choose **Administration** > **System Settings** > **Service Container Management** and enter the WAAS CM Ip address in the WCM IP Address field.
b) Click Save.

Configuring the Cisco WAAS Central Manager to Use SSO

To configure the Cisco WAAS Central Manager to use SSO follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose **Admin > AAA > Users** to configure a NCS user account. The **User Accounts** window displays all the user accounts on the system.

Step 2 Click the **Create New User Accounts** icon.

The **Creating New User Account** window appears.Create a new non-local (remote) user account with the name matching exactly the name of the NCS SSO user. Assign needed roles and domains in the **Role Management** and **Domain Management** windows.

Step 3 To configure the NCS server from the Cisco WAAS Central Manager:

a) From the WAAS Central Manager menu, choose **Devices > WAAS CM> Configure AAA> Cisco Prime SSO**.

b) Check the **Enable NCS Single Sign-on** check box, enter the NCS SSO server URL to configure the SSO server.
c) Click **Submit**.
d) Verify the Server Certificate and click **Submit**.

The SSO feature is now ready for use.

Launching Cisco WAAS Central Manager from NCS

To launch Cisco WAAS Central Manager from NCS, follow these steps:

Procedure

Step 1 Go to Cisco Prime Server and select the appropriate device from the Service Container.

Step 2 Click the **WAAS CM UI** tab to launch the Cisco WAAS Central Manager GUI.

Alternatively, select the device to launch the device instance homepage in the Cisco WAAS Central Manager GUI.

Configuring AAA Accounting for Cisco WAAS Devices

Accounting tracks all user actions and when the actions occurred. It can be used for an audit trail or for billing connection time or resources used (bytes transferred). Accounting is disabled by default.

The Cisco WAAS accounting feature uses TACACS+ server logging. Accounting information is sent only to the TACACS+ server, not to the console or any other device. The syslog file on the WAAS device logs accounting events locally. The format of events stored in the syslog is different from the format of accounting messages.

The TACACS+ protocol allows effective communication of AAA information between WAAS devices and a central server. It uses TCP for reliable connections between clients and servers. WAAS devices send authentication and authorization requests, as well as accounting information to the TACACS+ server.

Note Before you can configure the AAA accounting settings for a WAAS device, you must first configure the TACACS+ server settings for the WAAS device. (See About TACACS+ Server Authentication Settings, on page 233.)

Note If you enable AAA accounting for a device, we strongly recommended that you create an IP ACL condition in the first entry position permitting access to the TACACS+ servers to avoid delay while processing the commands. For information on IP ACLs, see the chapter Creating and Managing IP Access Control Lists for WAAS Devices, on page 277.

To centrally configure AAA accounting settings for a Cisco WAAS device or device group, follow these steps:

Procedure

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

Step 2 Choose **Configure** > **Security** > **AAA** > **AAA Accounting**.

The **AAA Accounting Settings** window appears.

Step 3 From the **System Events** drop-down list, choose a keyword to specify when the chosen device (or the device group) should track system-level events that are not associated with users, such as reloads, and to activate accounting for system events.

Step 4 From the **Exec Shell and Login/Logout Events** drop-down list, choose a keyword to specify when the chosen device (or the device group) should track EXEC shell and user login and logout events and to activate accounting for EXEC mode processes. Reports include username, date, start and stop times, and the Cisco WAAS device IP address.

Step 5 From the **Normal User Commands** drop-down list, choose a keyword to specify when the chosen device (or the device group) should track all the commands at the normal user privilege level (privilege level 0) and to activate accounting for all the commands at the nonsuperuser administrative (normal user) level.

Step 6 From the **Administrative User Commands** drop-down list, choose a keyword to specify when the chosen device (or the device group) should track all commands at the superuser privilege level (privilege level 15) and to activate accounting for all the commands at the superuser administrative user level.

Caution Before using the **wait-start** option, ensure that the Cisco WAAS device is configured with the TACACS+ server and is able to successfully contact the server. If the Cisco WAAS device cannot contact a configured TACACS+ server, it might become unresponsive.

The following table describes the event type options.

Table 13: Event Types for AAA Accounting

GUI Parameter	Function
Event Type Options	
stop-only	The Cisco WAAS device sends a stop record accounting notice at the end of the specified activity or event to the TACACS+ accounting server.
start-stop	The Cisco WAAS device sends a start record accounting notice at the beginning of an event and a stop record at the end of the event to the TACACS+ accounting server. The start accounting record is sent in the background. The requested user service begins regardless of whether or not the start accounting record was acknowledged by the TACACS+ accounting server.

GUI Parameter	Function
wait-start	The Cisco WAAS device sends both a start and a stop accounting record to the TACACS+ accounting server. However, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.
Do Not Set	Accounting is disabled for the specified event.

Step 7 Check the **Enable CMS CLI Accounting** check box to enable AAA accounting to TACACS+ server.

Step 8 To save the settings, click **Submit**.

To configure AAA accounting settings from the CLI, run the **aaa accounting** global configuration command.

Viewing Audit Trail Logs

The Cisco WAAS Central Manager device logs user activity in the system. The only activities that are logged are those activities that change the Cisco WAAS network. For more information on viewing a record of user activity on your Cisco WAAS system, see Viewing the Audit Trail Log in the chapter "Troubleshooting Your WAAS Network."

CHAPTER 8

Creating and Managing Administrator User Accounts and Groups

This chapter describes how to create user accounts and groups from the Cisco Wide Area Applications Services Central Manager GUI (Cisco WAAS Central Manager GUI).

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

This chapter contains the following sections:

About Administrator User Accounts

Your Cisco WAAS system comes with an administrator account already created, which you can use to access the Cisco WAAS Central Manager GUI as well as the Cisco WAAS CLI. This account has the username of **admin** and the password **default**. You can use the Cisco WAAS Central Manager GUI to change the password of this account.

If you want to create additional administrator user accounts, see the following list for a description of the two types of accounts you can create from the Cisoc WAAS Central Manager GUI.

- **Roles-based account**
  - Allows you to create accounts that manage and configure specific Cisco WAAS services. For example, you may want to delegate the configuration of application acceleration to a specific administrator. In this case, you could create a roles-based account that only has access to the **Acceleration** windows in the Cisco WAAS Central Manager GUI.
  - You can create a role-based account that also is a local user account.
  - You create roles-based accounts from the **Admin** menu in the Cisco WAAS Central Manager GUI.

- **Local account**
    - Provides CLI access to Cisco WAE devices. A user with this account type can log in to the Cisco WAAS Central Manager but they have the access rights assigned to the default account, which initially has no access to GUI functionality.
    - We recommend that you create a local account if there is an administrator that only needs CLI access to Cisco WAE devices.
    - You should create local accounts the same way as roles-based accounts, but you should check the **Local User** check box when creating the account.

Administrator Account User Name and Strong Password Guidelines

The Cisco WAAS administrator account username is **admin** and the password is initially set to **default**.

Note For how to change the devices administrator account username and password for Cisco vWAAS, see the chapter "Cisco vWAAS on Cisco ENCS 5400-W Series" in the Cisco Virtual Wide Area Application Services Configuration Guide.

For Cisco WAAS Version 6.4.3d and earlier: Changing the password of the administrator account is recommended but *optional* after your initial login.

For Cisco WAAS Version 6.4.3e and later: Changing the password of the administrator account to a strong password is *required* after your initial login, regardless of device mode (Application Accelerator, Appnav or Central Manager).

Consider the following operating guidelines for the **strong password** feature for Cisco WAAS Version 6.4.3e and later:

- **Strong password and Administrator account**: Strong password enforcement is applicable *only* to the Administrator account with the username **admin**. For more information on creating a strong password, see Working with Passwords, on page 263.
- **Strong password and registered Cisco vWAAS devices in upgrade from Cisco WAAS Version 6.4.1b to Cisco WAAS Version 6.4.3e or later**: to ensure that a new strong password is reflected in both the Cisco WAAS Central Manager and the Cisco vWAAS, follow these steps:
    1. Use the Cisco WAAS Central Manager GUI to upgrade the Cisco WAAS Central Manager from Cisco WAAS Version 6.4.1b to 6.4.3e or later.
    2. Change the strong password.
    3. Login with the new strong password.
    4. Choose **Home** > **Security** > **Password** and submit the new strong password.
    5. Verify that the new strong password is reflected in the Cisco vWAAS as well as the Cisco WAAS Central Manager.

6. Upgrade the Cisco vWAAS from Cisco WAAS Version 6.4.1b to 6.4.3e or later.

To update the password on the Cisco Wide Area Virtualization Engine Console:

1. In the **Username** field, enter admin or a username of your choice.
2. In the **Password** field, enter a password that contains the following parameters:
    - At least one lowercase character (a-z)
    - At least one uppercase character (A-Z)
    - At least one number (0-9)
    - At least one special character
    - A password length of 8 to 31 characters

To update the password using the CLI:

NO-HOSTNAME(config)# **username** *username* **passwd**

The following message will be displayed:

```
Warning: User configuration performed via CLI may be overwritten
by the central manager. Please use the central manager to configure
user accounts.
New WAAS password:
Retype new WAAS password:
NO-HOSTNAME#
```

Note To ensure the new password gets reflected to all devices, after you change the password using the Cisco WAAS Central Manager CLI, you must then change the password in **Home** > **Admin** > **Security**. This new password should not be the same password used in the Cisco WAAS CLI.

Creating and Managing User Accounts

This section contains the following topics:

Workflow for Creating and Managing a User Account

The following list provides a workflow of the steps you must complete to create a new roles-based administrator account.

1. Create a new account.

    Creates an account on the system with a specific username, password, and privilege level. For more information, see Creating a New Account .

2. Create a role for the new account.

Creates a role that specifies the services that an account can configure in your WAAS network. For more information, see Creating a New Role. If you are using an external authentication server, you can define matching user groups that automatically assign roles to users.

3. **3.** Assign the role to the new account.

   Assigns the new role to the new account. For more information, see Assigning a Role to a User Account. If you are using an external authentication server, you can define matching user groups that automatically assign roles to users.

4. **4.** Create a domain.

   Creates a domain that will specify the WAEs, device groups, or AppNav Clusters that the new account can manage. For more information, see Creating a New Domain.

5. **5.** Add an entity to the domain.

   Adds one or more WAEs, device groups, or AppNav Clusters to the domain. For more information, see Adding an Entity to a Domain.

6. **6.** Assign a domain to a user account.

   Assigns the domain to the new user account. For more information, see Assigning a Domain to a User Account. If you are using an external authentication server, you can define matching user groups that automatically assign domains to users.

Working with Accounts

When you create a user account, you enter information about the user, such as the username, the name of the individual who owns the account, contact information, job title, and department. All user account information is stored in an internal database on the Cisco WAAS Central Manager.

Each user account can then be assigned to a role. A *role* defines which Cisco WAAS Central Manager GUI configuration pages the user can access and which services the user has authority to configure or modify. The Cisco WAAS Central Manager provides one predefined role, known as the admin role. The admin role has access to all services. A *domain* defines the entities in the network that the user can access, configure, or modify. You can assign a user account to zero or more roles and to zero or more domains.

In addition to user accounts, you can create user groups if you are using external authentication of users on a TACACS+ or Windows domain server (not a RADIUS server). By creating user group names that match the user groups that you have defined on the external authentication server, WAAS can dynamically assign roles and domains to users based on their membership in a group as defined on the external authentication server. You do not have to define a role or domain for each user individually.

Two default user accounts are preconfigured in the Cisco WAAS Central Manager. The first account, called *admin* , is assigned the administrator role that allows access to all services, and access to all entities in the system. This account cannot be deleted from the system, but it can be modified. Only the username and the role for this account are unchangeable. Only an account that has been assigned the admin role can create other admin-level accounts.

The second preconfigured user account is called *default* . Any user account that is authenticated but has not been registered in the Cisco WAAS Central Manager obtains the access rights (role) assigned to the default account. This account is configurable by an administrator, but it cannot be deleted nor its username changed. Initially, the default account has no access to GUI functionality because it has no roles defined, although you can use the default account to log in to the Cisco WAAS Central Manager GUI.

This section contains the following topics:

Creating a New Account

Before you begin

The first step in setting up an account is to create the account by specifying a username and selecting whether a local CLI account is created at the same time. After the account is created, you can assign roles to the account, which determine the WAAS services and devices that the account can manage and configure.

The following table describes the outcome of creating a local CLI user when setting up an account.

Table 14: Outcome of Creating a Local User

Action	Result
Creating a Local User	• The account can be used to access the Cisco WAAS CLI and the Cisco WAAS Central Manager GUI (with the default role). • Users can change their own passwords, and the password change will propagate to standby Cisco WAAS Central Managers. • The account is stored in the Cisco WAAS Central Manager database and is also propagated to the standby Cisco WAAS Central Managers.
Not Creating a Local User	• The user account is created in the primary and standby Cisco WAAS Central Manager management databases. • No user account is created in the CLI. Users will have to use another account to access the CLI. • The new account can be used to log in to the Cisco WAAS Central Manager GUI if an external authentication server is set. The user is assigned the roles defined for the default user (initially none). • Local users can change their passwords using the Cisco WAAS Central Manager GUI only if they have roles that allow access to the Admin > AAA section.

Note If a user account has been created from the CLI only, when you log in to the Cisco WAAS Central Manager GUI for the first time, the Centralized Management System (CMS) automatically creates a user account (with the same username as that configured in the CLI) with default authorization and access control. An account created from the CLI will initially be unable to access any configuration pages in the Cisco WAAS Central Manager GUI. You must use an admin account to give the account created from the CLI the roles it requires to perform configuration tasks from the WAAS Central Manager GUI.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **AAA** > **Users**.

The **User Accounts** window displays all the user accounts on the system.

Step 2 Click the **Create New User Accounts** icon.

The **Creating New User Account** window appears.

Note This window can be accessed only by users with **administrator**-level privileges.

Step 3 In the **Username** field, enter the user account name.

Step 4 Usernames are case sensitive and cannot contain characters other than letters, numbers, period, hyphen, and underscore. Complete the following steps to create a local CLI user account:

a) Check the **Local User** check box. See the above table for information about the benefits of creating a local CLI user. A local user is created on all Cisco WAE devices.

Note Do not create a local user with a username that is identical to a username defined in an external authentication server that is authorizing access to the Cisco WAAS device.

b) In the **Password** field, enter a password for the local user account, and re-enter the same password in the Confirm Password field. Passwords are case-sensitive, must be 1 to 31 characters in length, and cannot contain the characters ', ", | (apostrophe, double quote, or pipe) or any control characters.

c) From the **CLI Privilege Level** drop-down list, select one of the following options for the local user account:

- 0 (normal user): Limits the CLI commands this user can use to only user-level EXEC commands. This is the default value.
- 15 (super user): Allows this user to use privileged EXEC-level CLI commands, similar to the functions that a Cisco WAAS Central Manager GUI user with the **admin** role can perform.

Note Use the Cisco WAAS CLI EXEC mode for setting, viewing, and testing system operations. It is divided into two access levels: user and privileged. A local user who has normal privileges can only access the user-level EXEC CLI mode. A local user who has superuser privileges can access the privileged EXEC mode as well as all other modes, for example, configuration mode and interface mode, to perform any administrative task. For more information, see the Cisco Wide Area Application Services Command Reference .

Step 5 (Optional) In the **User Information** fields, enter the following information about the user in the appropriate fields: first name, last name, phone number, e-mail address, job title, and department.

Step 6 (Optional) In the **Comments** field, enter any additional information about this account.

Step 7 Click **Submit**.

A **Changes Submitted** message appears at the bottom of the window.

Step 8 Assign roles to this new account, as described in Working with Roles, on page 265 and assign domains, as described in Working with Domains, on page 269.

Modifying and Deleting a User Account

Note Modifying a user account from the CLI does not update the Centralized Management System (CMS) database and the change will not be reflected in the Central Manager GUI.

To modify an existing user account, follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose **Admin** > **AAA** > **Users**.

The User Accounts window appears.

Step 2 Click the Edit icon next to the user account that you want to modify.

Note This window can only be accessed by users with administrator-level privileges.

The Modifying User Account window appears. You can delete or edit user accounts as follows:

- To delete the user account, click the **Delete** icon in the taskbar, and then click **OK** to confirm the deletion.

  If the local user account was created using the WAAS Central Manager GUI, the corresponding user account is removed from the CLI and is also deleted from all standby WAAS Central Managers.

Note Deleting a user account from the CLI does *not* disable the corresponding user account in the CMS database. Consequently, the user account remains active in the CMS database. User accounts created in the WAAS Central Manager GUI should always be deleted from the WAAS Central Manager GUI.

- To edit the user account, make the necessary changes to the username and account information, and click **Submit**.

Changing the Password for Your Own Account

Before you begin

If you are logged in to the Cisco WAAS Central Manager GUI, you can change your own account's password if you meet the following requirements:

- Your account and password were created in the Cisco WAAS Central Manager GUI and not in the CLI.
- You are authorized to access the **Password** window.

Note We do not recommend changing the local CLI user password from the CLI. Any changes to local CLI user passwords from the CLI are *not* updated in the management database and are not propagated to the standby Cisco WAAS Central Manager. Therefore, passwords in the management database will not match a new password configured in the CLI.

Note The advantage of initially setting passwords from the Cisco WAAS Central Manager GUI is that both the primary and the standby Cisco WAAS Central Managers will be synchronized, and GUI users will not have to access the CLI to change their password.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **Security** > **Password**.

The **Changing Password for User Account** window appears.

Step 2 In the **New Password** field, enter the changed password. Passwords are case sensitive, and must be 1 to 31 characters in length, and cannot contain the characters ', ", | (apostrophe, double quote, or pipe) or any control characters.

Step 3 In the **Confirm New Password** field, re-enter the password for confirmation.

Step 4 Click **Submit**.

The message **Changes Submitted** appears at the bottom of the window, confirming that your password has been changed.

When you change the password of an account by using the Cisco WAAS Central Manager GUI, it changes the password for all Cisco WAE devices managed by the Cisco WAAS Central Manager.

Changing the Password for Another Account

If you log in to the Cisco WAAS Central Manager GUI using an account with **admin** privileges, you can change the password of any other account.

Note If you change a user password from the CLI, the password change applies only to the local device, will not be reflected in the Central Manager GUI, and is not propagated to any other devices.

To change the password for another account, follow these steps:

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **AAA** > **Users**.

A list of roles-based user accounts appears.

Step 2 Click the **Edit** icon next to the account that needs a new password.

The **Modifying User Account** window appears.

Step 3 In the **Password** field, enter the changed password. Passwords are case-sensitive, must be 1 to 31 characters in length, and cannot contain the characters ', ", | (apostrophe, double quote, or pipe) or any control characters.

Step 4 In the **Confirm Password** field, reenter the password for confirmation.

Step 5 Click **Submit**.

The message **Changes Submitted** appears at the bottom of the window confirming that your password has been changed.

Viewing a User Account

To view all user accounts, choose **Admin** > **AAA> Users** from the Cisco WAAS Central Manager GUI. The **User Accounts** window displays all the user accounts in the management database. From this window, you can also create new accounts, as described in Creating a New Account .

To view user accounts for a specific device, choose **Devices** > *device-name* and then choose *device-name* > **Device Users** or **CM Users**, depending on the device mode. The **Users for Device** window displays all the user accounts defined for the device.

To view the details of an account, click the **View** icon next to the account.

Unlocking a User Account

Before you begin

When a user account is locked out, the user cannot log in to the WAAS device until an administrator unlocks the account. A user account will be locked out if the user unsuccessfully tries to log in three consecutive times.

Procedure

Step 1 From the Cisco WAAS Central Manager GUI, choose **Admin** > **AAA** > **Users**.

The **User Accounts** listing window appears and displays the status of each user account.

Note This window can only be accessed by users with **administrator**-level privileges.

Step 2 Click the **Edit** icon next to the user account that you want to modify.

The **Modifying User Account** window appears and displays a list of devices on which this account is locked out.

Step 3 Choose the device in which you want to unlock the account.

The list of device users appears.

Step 4 Choose the user or users to unlock, and click **unlock**.

Working with Passwords

Before you begin

The Cisco WAAS system features two levels of password policy: **Standard** and **Strong**. By default, the **Standard** password policy is enabled.

Procedure

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

Step 2 Choose **Configure** > **Security** > **Password Policy Settings**.

Step 3 To enable the strong password policy, check the **Enforce stringent password** check box.

Step 4 In the **Maximum login retries** field, enter the maximum number of login attempts to be allowed before a user is locked out. The user remains locked out until cleared by the administrator. For more information, see Unlocking a User Account, on page 263.

Step 5 To save your changes, click **Submit**.

Note The MAPI process terminates abruptly when you try to upgrade to version 6.4.3e and higher. This happens when the **admin** user uses the **default**password and enforces password checking using the **Enforce stringent password** checkbox. To avoid this, either change the password or disable stringent password checking while upgrading the device.

Step 6 (Optional) To configure a password policy from the CLI, run the **authentication strict-password-policy** global configuration command.

When the **Standard password** policy is enabled, user passwords must meet the following requirements:

- The password must be 1 to 31 characters long.
- The password can include both uppercase and lowercase letters (A-Z and a-z) and numbers (0 to 9).
- The password cannot contain the characters ', ", | (apostrophe, double quote, or pipe) or any control characters.

When the **Strong password** policy is enabled, user passwords must meet the following requirements:

- The password must be 8 to 31 characters long. However, the minimum password length can vary depending on the following conditions:
  - The minimum password length must be 10 characters if all characters are the same type of characters: all lowercase letters. all uppercase letters, all numbers, or all special characters.
  - The minimum password length must be 9 characters if you use any two different types of characters.
  - The minimum password length must be 8 characters if you use any three different types of characters.
  - The minimum password length must be 7 if you use any four different types of characters.
- The password can include both uppercase and lowercase letters (A-Z and a-z), numbers (0 to 9), and special characters including ~,`,!,@,#,$,%,^,&,*,(,),_,+,-,=,[,],\,{,},;,:,,,<,/,>.
- The password cannot contain the characters ' ? | (apostrophe, double quote, or pipe) or any control characters.
- The password cannot contain all the same characters (for example, 99999).
- The password cannot contain consecutive characters (for example, 12345).
- The password cannot be the same as the username.
- Each new password must be different from the previous 12 passwords. User passwords expire within 90 days.
- The password cannot contain dictionary words.

Note When you enable the strong password policy, existing standard-policy passwords will still work. However, these passwords are subject to expiration under the strong password policy.

A user account will be locked out after the configured number of failed login attempts (the default is **3**). The user remains locked out until cleared by the administrator. For more information, see Unlocking a User Account, on page 263.

Working with Roles

The WAAS Central Manager GUI allows you to create roles for your WAAS system administrators so that each administrator can focus on configuring and managing a specific WAAS service. For example, you can set up a role that allows an administrator to create and modify application policies, but does not allow the administrator to make any other changes to the system.

You can think of a role as a set of enabled services. Make sure you have a clear idea of the services that you want the role to be responsible for because you will select these services when you create the role. After you create a role, you can assign the role to existing accounts, as described later in this chapter.

A role can give read and write or read-only access to each enabled service.

Each user account or group can be assigned to zero or more roles. Roles are not inherited or embedded. The WAAS Central Manager provides a predefined role, known as the admin role. The admin role has access to all services, similar to a CLI user having privilege level 15. Without the admin role, a user will not be able to perform all the administrative tasks.

Note Assigning the admin role to a user does not change the user privilege level to 15. The user must also have privilege level 15 in order to perform administrative tasks.

WAAS can dynamically assign a role to users based on their membership in a group as defined on an external TACACS+ or Windows domain authentication server. To take advantage of this feature, you must define user group names on the WAAS Central Manager that match the user groups defined on the external authentication server, and assign a role to the user groups on the WAAS Central Manager. For more information on user groups, see Working with User Groups, on page 273.

This section contains the following topics:

Creating a New Role

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **AAA** > **Roles**.

The **Roles** listing window appears.

Step 2 Click the **Create New Role** icon from the taskbar.

The **Creating New Role** window appears.

Step 3 In the **Name** field, enter the name of the role.

The name cannot contain characters other than letters, numbers, period, hyphen, underscore, and space.

Step 4 Check the check box next to the services you want this role to manage.

- The check boxes in this window are tri-state check boxes. When there is a check in a check box, it means that the user will have read and write access to the listed service.
- Click the check box again to change the indicator to a square partially filling the check box. This indicator means that the user will have read-only access to the service.
- To expand the listing of services under a category, click the **folder** icon, and then check the check box next to the services you want to enable for this role.

  To choose all the services under one category simultaneously, check the check box next to the top-level folder for those services.
- The following table lists the services that you can enable for a role.

Table 15: Description of Cisco WAAS Services

Service	Description
Home	Allows a role to view, configure, and manage the system dashboard and settings in the **Configure**, **Monitor**, and **Admin** menus of the Cisco WAAS Central Manager GUI in the **Home** (global) context. Under each folder you can select the subpages that you want this role to manage.
Device Groups	Allows a role to view, configure, and manage the settings and subpages for the various device groups in the Cisco WAAS Central Manager GUI in the device group context.
Devices	Allows a role to view, configure, and manage the settings and subpages for various kinds of devices in the Cisco WAAS Central Manager GUI in the device context.
AppNav Clusters	Allows a role to view, configure, and manage the settings and subpages in the Cisco WAAS Central Manager GUI in the AppNav Cluster context.
Locations	Allows a role to view, configure, and manage the settings and subpages in the Cisco WAAS Central Manager GUI in the Location context.
All Devices	Allows a role to access all the devices in your Cisco WAAS network. If this service is not enabled, the user account will only have access to the devices associated with the domain that you assign to the account. Selecting this service allows you to skip the following tasks when setting up a roles-based account: • Creating and maintaining a domain that contains all the devices in your network. • Assigning to the account the domain that contains all the devices.

Service	Description
All Device Groups	Allows a role to access all the device groups in your Cisco WAAS network. If this service is not enabled, the user account will only have access to the device groups associated with the domain that you assigned to the account. Selecting this service allows you to skip the following tasks when setting up a roles-based account: • Creating and maintaining a domain that contains all the device groups in your network. • Assigning to the account the domain that contains all the device groups.
All AppNav Clusters	Allows a role to access all the AppNav clusters in your Cisco WAAS network. If this service is not enabled, the user account will only have access to the AppNav clusters associated with the domain that you assign to the account. Selecting this service allows you to skip the following tasks when setting up a roles-based account: • Creating and maintaining a domain that contains all the AppNav clusters in your network. • Assigning to the account the domain that contains all the AppNav clusters.
Monitoring API	Allows a role to access monitoring APIs through HTTPS requests. For more information, see Cisco Wide Area Application Services API Reference.
System Status	Allows a role to access the device Alarms panel. For more information about device alarms, see the chapter Monitoring Your Cisco WAAS Network, on page 553.

Step 5 (Optional) Enter comments, if any, about this role in the Comments field.

Step 6 Click **Submit** to save your settings.

Assigning a Role to a User Account

Before you begin

After you create a role, you must assign the role to an account (or a user group). If you create an account, but do not assign a role to the account, the user for that account can log in to the Cisco WAAS Central Manager GUI but no data will be displayed and the configuration pages will not be available.

Note The **admin** user account, by default, is assigned to the role that allows access to all entities in the system. It is not possible to change the role for this user account.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin > AAA > Users** or **Admin > AAA > User Groups**.

The **User Accounts** or **User Groups** window appears with all the configured user accounts listed.

Step 2 Click the **Edit** icon next to the user account or group for which you want to assign roles.

The **Modifying User Account** or **Modifying User Group** window appears.

Step 3 Click the **Role Management** tab.

The **Role Management** window appears with all the configured role names listed.

Step 4 Click the **Assign** icon (blue cross mark) that appears next to the role name you want to assign to the selected user account or group.

Step 5 Click the **Unassign** icon (green tick mark) next to the role name to unassign a previously assigned role.

Note Click the **Assign all Roles** icon in the taskbar to assign all the roles in the current window to a user account or group. Alternatively, click the **Remove all Roles** icon to unassign all the roles associated with a user account or group.

Step 6 Click **Submit**.

The roles assigned to a user account or group will be listed in the **Roles** section in the **Modifying User Account** or **Modifying User Group** window.

Modifying and Deleting a Role

Note The admin user account, by default, is allowed access to all the services, and cannot be modified.

To modify or delete a role, follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose **Admin** > AAA > Roles.

The Roles window appears.

Step 2 Click the Edit icon next to the name of the role you want to change or delete.

The Modifying Role window appears. You can modify the role as follows:

- To delete this role, click the **Delete** icon in the taskbar.
- To edit this role, make the necessary changes to the fields, and click **Submit**.

- To enable a service for this role, check the check box next to the corresponding service. To disable a previously selected service, uncheck the check box next to the service you want to disable. To choose all the services under one category simultaneously, check the check box next to the top-level service.

Viewing Role Settings

You might want to view role settings before assigning a role to a particular user account or group.

To view role settings, follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose **Admin > AAA > Users** (or **Admin** > AAA > User Groups).

The User Accounts (or User Groups) window appears with all the configured user accounts or groups listed.

Step 2 Click the **Edit** icon next to the user account or group that you want to view.

The Modifying User Account (or Modifying User Group) window appears.

Step 3 Click the **Role Management** tab.

The Role Management window appears.

Step 4 Click the **View** icon next to the role that you want to view.

The Viewing Role window appears, which displays the role name, comments about this role, and the services that are enabled for this role.

Step 5 After you have finished viewing the settings, click **Close**.

Working with Domains

A Cisco WAAS **domain** is a collection of device groups or Cisco WAEs that make up the Cisco WAAS network. A role defines which services a user can manage in the Cisco WAAS network, but a domain defines the device groups, Cisco WAEs, or file server dynamic shares that are accessible and configurable by the user.

Note A Cisco WAAS domain is not the same as a DNS domain or Windows domain.

When you create a domain, you choose the type of entities that can be associated with the domain. Entity types include Devices, Device Groups, or None (for file server dynamic shares). For file server dynamic shares, the dynamic shares are assigned in the dynamic shares configuration.

Cisco WAAS can dynamically assign a domain to a user based on their membership in a group as defined on an external TACACS+ or Windows domain authentication server. To take advantage of this feature, you must define user group names on the Cisco WAAS Central Manager that match the user groups defined on the external authentication server and you must assign a domain to the user groups on the Cisco WAAS Central Manager. For more information on user groups, see Working with User Groups, on page 273.

This section contains the following topics:

Creating a New Domain

To create a new domain, follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose **Admin** > **AAA** > **Domains**.

The Domains listing window appears.

Step 2 Click the **Create New Domain** icon in the taskbar.

The Creating New Domain window appears.

Step 3 In the Name field, enter the name of the domain.

Step 4 From the Entity Type drop-down list, choose the entity type (Devices, Device Groups, or None) that you want to assign to the domain.

Note Choose **None** if this domain is used for a file server dynamic share.

Step 5 (Optional) In the Comments field, enter comments, if any, about this domain.

Step 6 Click **Submit**.

If the entity type you chose has not been assigned to the domain, then a message indicating that the entity type has not been assigned appears.

Step 7 Assign an entity to this domain, as described in Adding an Entity to a Domain, on page 270. If you chose None for the Entity Type, do not assign an entity to the domain, instead, the entity is used in a dynamic share configuration.

For a domain used in a dynamic share configuration, assign the domain to each user having to edit the dynamic share configuration, as described in Assigning a Domain to a User Account, on page 271. Only users assigned to the domain will be able to edit the dynamic share configuration.

Adding an Entity to a Domain

After you have created a domain, you can assign an entity to the domain. An entity is either a collection of devices or a collection of device groups. You do not have to assign an entity to a domain that is used for a file server dynamic share, where the entity type is None.

To add an entity to a domain, follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose **Admin** > **AAA** > **Domains**.

Step 2 Click the **Edit** icon next to the domain that you want to modify.

Step 3 Click the **Entity Management** tab.

The *Entity_name* Assignments for Domain window for the current domain appears.

You can add or remove entities from the domain as follows:

- To add an entity to the current domain, click the Assign icon (blue cross mark) next to the entity that you want to add. A green tick mark appears next to the selected entity when you submit the settings.

Alternatively, to add all the entities to the selected domain, click the Assign all icon in the taskbar.

- To remove an entity from the current domain, click the Unassign icon (green tick mark) next to the name of the entity that you want to remove from the domain. A blue cross mark appears next to the unassigned entity after you submit the settings.

Alternatively, to remove all the entities from the domain, click the Remove all icon in the taskbar.

Step 4 Click **Submit**.

Green check marks appear next to the entities that you assigned to the domain.

Step 5 Assign the domain to an account, as described in Assigning a Domain to a User Account, on page 271.

Assigning a Domain to a User Account

Before you begin

Assigning a domain to an account or user group specifies the entities (devices or device groups) or file server dynamic shares that the account or user group can access.

When working with a domain of type **None** that is used for dynamic file shares, you will need a user account for every user having to edit the dynamic share configuration. If you are using external authentication of users on TACACS+ or Windows domain servers, you can use user groups to more easily assign Cisco WAAS domains to users. For more information, see Working with User Groups, on page 273.

Note If the role that you assigned to an account or group has the **All Devices** or **All Device Groups** service enabled, you do not have to assign a domain to the account or group. The account or group can automatically access all the devices or device groups, or both, in the Cisco WAAS system. For more information, see Working with Passwords, on page 263.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **AAA** > **Users** or **Admin** > **AAA** > **User Groups**.

The **User Accounts** or **User Groups** window appears with all the configured user accounts or groups listed.

Step 2 Click the **Edit** icon next to the user account or group for which you want to assign domains.

The **Modifying User Account** or **Modifying User Group** window appears.

Step 3 Click the **Domain Management** tab.

The **Domain Management** window appears with all configured domains and their entity types listed.

Step 4 Click the **Assign** icon (blue cross mark) that appears next to the domain name that you want to assign to the selected user account or group.

To dissociate a domain from the user account or group, click the **Unassign** (green tick mark) next to the domain name.

Note To assign all the domains in the current window to a user account or group, click the **Assign all Domains** icon in the taskbar. Alternatively, to unassign all the domains associated with a user account or group, click the **Remove all Domains** icon.

Step 5 Click **Submit**.

The domains assigned to a user account or group are listed in the **Domains** section in the **Modifying User Account** or **Modifying User Group** window.

Modifying and Deleting a Domain

To modify or delete an existing domain, follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose **Admin** > **AAA** > **Domains**.

The Domains window appears.

Step 2 Click the **Edit** icon next to the domain that you want to modify.

The Modifying Domain window appears. You can modify the domain as follows:

- To delete the domain, click the **Delete** icon in the taskbar and then click **OK** to confirm the deletion.
- To modify a domain, make the necessary changes to the fields, and click **Submit**.

Viewing Domains

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin > AAA > Users** or **Admin > AAA > User Groups**.

The **User Accounts** or **User Groups** window appears, with all the configured user accounts or groups listed.

Step 2 Click the **Edit** icon next to the user account or group for which you want to view the domain configuration.

The **Modifying User Account** or **Modifying User Group** window appears.

Step 3 Click the **Domain Management** tab.

The **Domain Management** window appears.

Step 4 Click the **View** (eyeglass) icon next to the domain name to view details about the domain.

The **Viewing Domain** window appears and displays the domain name, entity type, comments about this domain, and entities assigned to this domain.

Step 5 After you have finished viewing the settings, click **Close**.

Working with User Groups

If you are using external authentication of users on TACACS+ or Windows domain servers (not RADIUS servers), you may want to create user groups. By creating user group names that match the user groups that you have defined on the external authentication server, WAAS can dynamically assign roles and WAAS domains to users, based on their membership in a group as defined on the external authentication server. You do not have to define a role or WAAS domain for each user individually; instead, you define roles and WAAS domains for the user groups, and a user is assigned the roles and WAAS domains that are defined for the groups to which they belong.

Note The dynamic assignment of roles and WAAS domains based on external user groups requires a TACACS+ server that supports shell custom attributes. For example, these are supported in Cisco ACS (Access Control Server) 4.x and 5.1 and later.

WAAS reads group membership information for each user from the external authentication server.

This section contains the following topics:

Creating a New User Group

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin > AAA > User Groups**.

The **User Groups** listing window appears.

Step 2 Click the **Create New User Groups** icon in the taskbar.

The **Creating New User Group** window appears.

Step 3 In the **Name** field, enter the name of the user group.

Ensure that the name matches the name of a user group defined on the external authentication server that you are using.

Name matching is case sensitive. A user group name cannot contain the following characters: # + " < > , (comma). A user group name cannot consist solely of numbers, periods (.), or spaces. Any leading periods, asterisks (*), or spaces are cropped.

Step 4 (Optional) In the Comments field, enter comments, if any, about this user group.

Step 5 Click **Submit**.

Step 6 Assign a role or Cisco WAAS domain to this user group, as described in Assigning Roles to a User Group, on page 274 and Assigning a Domain to a User Group, on page 274.

Assigning Roles to a User Group

After you create a user group, you have to assign a role to the group. If you create a user group but do not assign a role to the group, the users in that group can log in to the WAAS Central Manager GUI, but no data will be displayed and the configuration pages will not be available.

To assign one or more roles to a user group, follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose Admin > AAA > User Groups.

The User Groups window appears with all the configured user groups listed.

Step 2 Click the Edit icon next to the user group for which you want to assign roles.

The Modifying User Group window appears.

Step 3 Click the Role Management tab.

The Role Management for User Group window appears with all the configured role names listed.

Step 4 Click the Assign icon (blue cross mark) that appears next to the role name that you want to assign to the selected user group.

Step 5 Click the Unassign (green tick mark) next to the role name to unassign a previously assigned user group role.

Note Click the Assign all Roles icon in the taskbar to assign all the roles in the current window to a user group. Alternatively, click the Remove all Roles icon to unassign all the roles associated with a user group.

Step 6 Click **Submit**.

The roles assigned to a user group will be listed in the Roles section in the Modifying User Group window.

Assigning a Domain to a User Group

Assigning a WAAS domain to a user group specifies the entities (devices or device groups) that the users who are members of that user group can manage.

Note If the role that you assigned to a user group has the All Devices or All Device Groups service enabled, you do not have to assign a domain to the user group. The users in that group can automatically access all the devices, or device groups, or both, in the WAAS system. For more information, see Table 8-4 .

To assign a domain to a user group, follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose **Admin > AAA> User Groups**.

The User Groups window appears with all the configured user groups listed.

Step 2 Click the **Edit** icon next to the user group for which you want to assign domains.

The Modifying User Group window appears.

Step 3 Choose the **Domain Management** tab.

The Domain Management for User Group window appears with all the configured domains and their entity types listed.

Step 4 Click the **Assign** icon (blue cross mark) that appears next to the domain name that you want to assign to the selected user group.

To dissociate a domain from the user group, click the **Unassign** (green tick mark) next to the domain name.

Note To assign all the domains in the current window to a user group, click the **Assign all Domains** icon in the taskbar. Alternatively, to unassign all the domains associated with a user group, click the **Remove all Domains** icon.

Step 5 Click **Submit**.

The domains assigned to a user group are listed in the Domains section in the Modifying User Group window.

Modifying and Deleting a User Group

To modify an existing user group, follow these steps:

Procedure

Step 1 From the WAAS Central Manager menu, choose **Admin > AAA > User Groups**.

The User Groups window appears.

Step 2 Click the Edit icon next to the user group that you want to modify.

The Modifying User Group window appears. You can delete or edit user groups as follows:

Note This window can be accessed only by users with administrator-level privileges.

- To delete the user group, click the **Delete** icon in the taskbar, and then click **OK** to confirm the deletion.
- To edit the user group, make the necessary changes to the name and comment information, and click **Submit**.
- To change the roles assigned to the user group, click the **Role Management** tab, make the necessary changes to the roles, and click **Submit**.

- To change the domains assigned to the user group, click the **Domain Management** tab, make the necessary changes to the domains, and click **Submit**.

Viewing User Groups

To view all the user groups, choose **Admin > AAA > User Groups** from the Cisco WAAS Central Manager GUI. The **User Groups** window displays all the user groups in the management database. From this window, you can also create groups, as described in Creating a New User Group, on page 273.

CHAPTER 9

Creating and Managing IP Access Control Lists for WAAS Devices

This chapter describes how to use the Cisco Wide Area Application Services (Cisco WAAS) Central Manager GUI to centrally create and manage IP access control lists (ACLs) for your Cisco WAAS devices.

Note You must log in to the Cisco WAAS Central Manager GUI using an account with admin privileges to view, edit, or create IP ACL configurations.

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

This chapter contains the following sections:

About IP ACLs for Cisco WAAS Devices

In a centrally managed Cisco WAAS network environment, administrators should be able to prevent unauthorized access to various devices and services. IP ACLs can filter packets by allowing you to permit or deny IP packets destined for a Cisco WAAS device.

The Cisco WAAS software supports standard and extended ACLs that allow you to restrict access to a Cisco WAAS device. The Cisco WAAS software can use the following types of ACLs:

- Interface ACL: Applied on the built-in, port channel, standby, and inline group interfaces. This type of ACL is intended to control management traffic (Telnet, SSH, and Cisco WAAS Central Manager GUI). The ACL rules apply only to traffic that is destined for the WAE or originates from the WAE, not Web Cache Communication Protocol (WCCP) transit traffic. Use the **ip access-group interface** global configuration command to apply an interface ACL.

- Interception ACL: Applied globally to a Cisco WAAS device. This type of ACL defines what traffic is to be intercepted. Traffic that is permitted by the ACL is intercepted and traffic that is denied by the ACL is passed through the WAE. Use the **interception access-list** global configuration command to apply an interception ACL. For more information on using interception ACLs, see Configuring Interception Access Control Lists, on page 155 in the chapter "Configuring Traffic Interception."
- WCCP ACL: Applied on inbound WCCP-redirected traffic to control access between an external server and external clients. The WAE acts like a firewall. Use the **wccp access-list** global configuration command to apply a WCCP ACL.
- SNMP ACL: Applied on an SNMP agent to control access to the SNMP agent by an external SNMP server that is polling for SNMP MIBs or SNMP statistics. Use the **snmp-server access-list** global configuration command to apply an SNMP ACL.
- Transaction-logs-flow ACL: Applied on the transaction logging facility to restrict the transactions to be logged. Use the **transaction-logs flow access-list** global configuration command to apply a transaction log ACL.

The following examples show how interface ACLs can be used in environments that have Cisco WAAS devices:

- A Cisco WAAS device resides on the customer premises and is managed by a service provider, and the service provider wants to secure the device for its management only.
- A Cisco WAAS device is deployed anywhere within the enterprise. As with routers and switches, the administrator wants to limit access to Telnet, SSH, and the Cisco WAAS Central Manager GUI to the IT source subnets.

To use ACLs, you must first configure ACLs and then apply them to specific services or interfaces on the Cisco WAAS device. The following are some examples of how interface ACLs can be used in various enterprise deployments:

- An application layer proxy firewall with a hardened outside interface has no ports exposed. (Hardened means that the interface carefully restricts which ports are available for access, primarily for security reasons. Because the interface is outside, many types of attacks are possible.) The Cisco WAAS device's outside address is globally accessible from the Internet, while its inside address is private. The inside interface has an ACL to limit Telnet, SSH, and GUI access.
- A WAE that is using WCCP is positioned on a subnet off the Internet router. Both the WAE and the router must have IP ACLs. IP access lists on routers have the highest priority, followed by IP ACLs that are defined on the WAEs.

Note We strongly recommend that you use the Cisco WAAS Central Manager GUI instead of the Cisco WAAS CLI to centrally configure and apply ACLs to your Cisco WAAS devices. For more information, see Creating and Managing IP ACLs for Cisco WAAS Devices, on page 278.

Creating and Managing IP ACLs for Cisco WAAS Devices

This section provides guidelines and an example of how to use the Cisco WAAS Central Manager GUI to create and manage IP ACLs for your Cisco WAAS devices.

Consider the following guidelines to create an IP ACL:

- IP ACL names:

  Must be unique within the device.

  IP ACL names must be limited to 30 characters and contain no white space or special characters.

  When the IP ACL name is numeric, numbers 1 through 99 denote standard IP ACLs and numbers 100 through 199 denote extended IP ACLs. IP ACL names that begin with a number cannot contain nonnumeric characters.

- Each Cisco WAAS Central Manager device can manage up to 50 IP ACLs and a total of 500 conditions per device.

- When the IP ACL name is numeric, numbers 1 through 99 denote standard IP ACLs and numbers 100 through 199 denote extended IP ACLs. IP ACL names that begin with a number cannot contain nonnumeric characters.

- The Cisco WAAS Central Manager GUI allows the association of standard IP ACLs with SNMP and WCCP. Any device that attempts to access one of these applications associated with an ACL must be on the list of trusted devices to be allowed access.

- You can associate any previously configured standard IP ACL with SNMP and WCCP. However, you can associate an extended IP ACL only with the WCCP application.

- You can delete an IP ACL, including all conditions and associations with network interfaces and applications, or you can delete only the IP ACL conditions. Deleting all conditions allows you to change the IP ACL type if you choose to do so. The IP ACL entry continues to appear in the IP ACL listing. However, it is, in effect, nonexistent.

- If you specify an empty ACL for any of the ACL types used by Cisco WAAS, it permits all traffic.

To use the Cisco WAAS Central Manager GUI to create and modify an IP ACL for a single WAE, associate an IP ACL with an application, and then apply it to an interface on the WAE, follow these steps:

Procedure

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

Step 2 Choose **Configure Network TCP/IP Settings** > **IP ACL**.

The **IP ACL** window appears. By default, there are no IP ACLs defined for a WAE. The **IP ACL** window indicates if there are currently no IP ACLs configured for the WAE.

Step 3 In the Table Heading row, click **ADD IP ACL**.

The **IP ACL** window appears. Fill in the fields as follows:

- In the **Name** field, enter a name, for example, **test1**. IP ACL names must be unique within the device, must be limited to 30 characters, and cannot contain any white spaces or special characters.

  By default, this new IP ACL is created as a standard ACL.

- To change this default setting and create this new ACL as an extended ACL: from the **ACL Type** drop-down list, choose **Extended**.

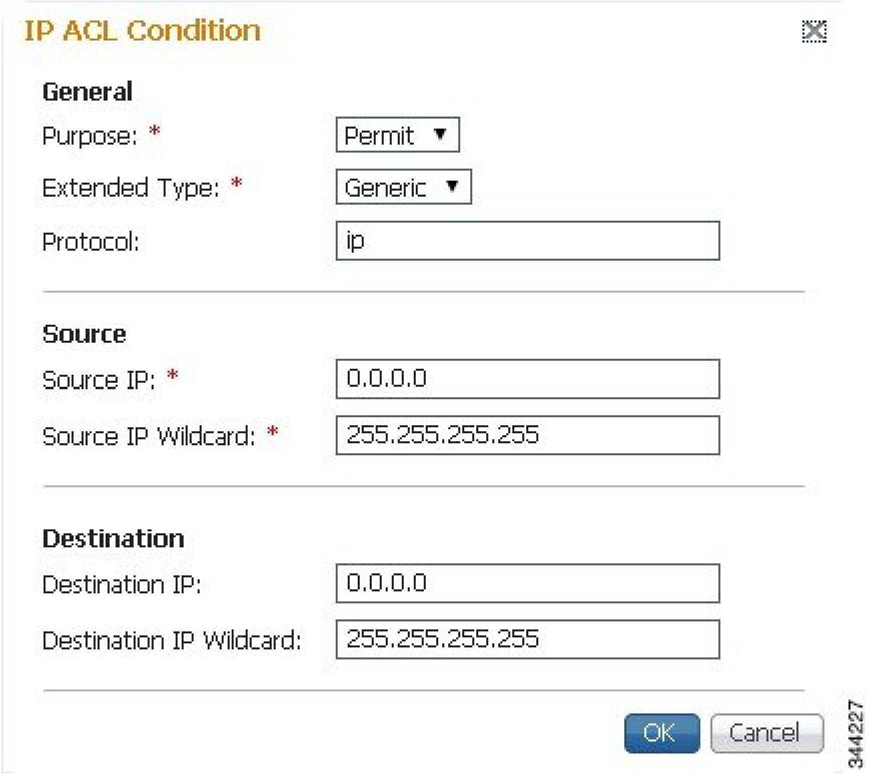
Step 4 To save the IP ACL named **test1**, click **OK**. IP ACLs without any conditions defined do not appear on the individual devices.

Step 5 Add conditions to the standard IP ACL named **test1** that you just created:

a) Click the **Add IP ACL Condition**.

The **IP ACL Condition** window appears, as shown in the following figure.

Figure 46: IP ACL Condition Window



Purpose: * Permit

Extended Type: * Generic

Protocol: ip

Source IP: * 0.0.0.0

Source IP Wildcard: * 255.255.255.255

Destination IP: 0.0.0.0

Destination IP Wildcard: 255.255.255.255

Note The number of available fields for creating IP ACL conditions depends on the type of IP ACL that you have created, either **Standard** or **Extended**.

b) Enter values for the properties that are enabled for the type of IP ACL that you are creating, as follows:

- To set up conditions for a standard IP ACL, go to Step 6 .
- To set up conditions for an extended IP ACL, go to Step 7 .

Step 6 Set up conditions for a standard IP ACL:

a) From the **Purpose** drop-down list, choose a purpose, **Permit** or **Deny**.
b) In the **Source IP** field, enter the source IP address.
c) In the **Source IP Wildcard** field, enter a source IP wildcard address.
d) To save the condition, click **OK**.

IP ACL conditions for the newly created IP ACL and its configured parameters are displayed in the following "Standard IP ACL Conditions" table.

e) To add another condition to the IP ACL, select it and click **Add IP ACL Condition**.

f) Enter the details of the condition, and click **OK** to save the additional condition.

g) For a newly created IP ACL condition to appear in a particular position, select the position and click **Insert**. The IP ACL condition is placed in the selected position.

h) To rearrange your list of conditions, select the condition (or multiple consecutive conditions), using the **Up** or **Down** arrows. To commit the changes, click **Save Moved Rows**. Alternatively, you can select one or multiple consecutive conditions and, to specify the row number in which the IP ACL condition should be positioned, click **Move to**. This is especially helpful when there are numerous conditions listed in the table. After you have verified that the entries and the new order in which the conditions are listed are appropriate, click **Save Moved Rows**.

Note The order of the conditions listed in the Cisco WAAS Central Manager GUI becomes the order in which IP ACLs are applied to the device.

Note Click a column heading to sort by a configured parameter.

The "Standard IP ACL Conditions" table describes the fields in a standard IP ACL.

Table 16: Standard IP ACL Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Source IP	0.0.0.0	The number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard	255.255.255.255	The wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.

Step 7 Set up conditions for an extended IP ACL:

a) From the **Purpose** drop-down list, choose a purpose: **Permit** or **Deny**.

b) From the **Extended Type** drop-down list, choose a value: **Generic**, **TCP**, **UDP**, or **ICMP**. Each value is described below in the "Extnded IP ACL Conditions" table.

Table 17: Extended IP ACL Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed or dropped. Choices are **Permit** or **Deny**.
Extended Type	Generic	Specifies the Internet protocol to be applied to the condition. When selected, the Cisc WAAS Central Manager GUI window refreshes with applicable field options enabled. The options are generic, TCP, UDP, or ICMP.

After you choose a type of extended IP ACL, various options become available in the GUI, depending on what type you choose.

c) In the fields that are enabled for the chosen type, enter the data. For more information, see List of Extended IP ACL Conditions, on page 284.

d) To save the condition, click **OK**.

   IP ACL conditions for the newly created IP ACL and its configured parameters are displayed above in the "Standard IP ACL Conditions" table.

e) To add another condition to the IP ACL, select it and click **Add IP ACL Condition**.

f) Enter the details of the condition in the window. To save the additional condition, click **OK**.

g) For a newly created IP ACL condition to appear in a particular position, select the position and click **Insert**. The IP ACL condition is placed in the selected position.

h) To rearrange your list of conditions, select the condition (or multiple consecutive conditions). using the **Up** and **Down** arrows. To commit the changes, click **Save Moved Rows**. Alternatively, you can select one or multiple consecutive conditions. To specify the row number in which the IP ACL condition should be positioned, click **Move to**. This is especially helpful when there are numerous conditions listed in the table. After you are satisfied with all your entries and the order in which the conditions are listed, click Save Moved Rows to commit the changes.

   Note The order of the conditions listed in the WAAS Central Manager GUI becomes the order in which IP ACLs are applied to the device.

   Note Click a column heading to sort by any configured parameter.

Step 8 Modify or delete an individual condition from an IP ACL:

a) Select the name of the IP ACL whose condition you want to modify.

b) A list of all the conditions that are currently applied to the IP ACL appears in the IP ACL Conditions, Table 9-1 . Select the condition and click Edit.

c) To modify the condition, change any corresponding field as necessary in the IP ACL Condition window and click OK to save the modifications.

d) To delete the condition, select it and click **Delete on the table** header.

e) To rearrange your list of conditions, use the Up or Down arrows or the Move to column outlined in Step 6f and 7f.

Step 9 Associate a standard IP ACL with SNMP or WCCP:

a) Click the **Edit** icon next to the name of the device for which you want to associate a standard IP ACL with SNMP or WCCP.

b) Choose **Configure** > **Network** > **TCP/IP Settings** > **IP ACL Feature Usage**.

   The IP ACL Feature Settings window appears.

c) From the SNMP or WCCP drop-down lists, choose the name of an IP ACL for SNMP or WCCP. (For more details, see Table 9-3 .) If you do not want to associate an IP ACL with one of the applications, choose **Do Not Set**.

Table 18: IP ACL Feature Settings

Cisco WAAS Central Manager GUI Parameter	Function
SNMP	Associates a standard IP ACL with SNMP. This option is supported for all WAAS devices.

Cisco WAAS Central Manager GUI Parameter	Function
WCCP	Associates any of the IP ACLs with WCCP Version 2. This option is supported only for WAAS devices that are operating in WCCP interception mode and not for WAAS Central Manager devices.

d) Click **Submit** to save the settings.

Step 10 Apply an IP ACL to an interface:

a) Click the **Edit** icon next to the name of the device for which you want to apply an IP ACL to an interface on the WAE.
b) Choose **Configure** > **Network** > **Network Interfaces**.

   The Network Interfaces window for the device appears. This window displays all the interfaces available on that device.

c) Click the **Edit** icon next to the name of the interface to which you want to apply an IP ACL.

   The Network Interface settings window appears.

d) From the Inbound ACL drop-down list at the bottom of the window, choose the name of an IP ACL.
e) From the Outbound ACL drop-down list, choose the name of an ACL.

   The only network interface properties that can be altered from the WAAS Central Manager GUI are the inbound and outbound IP ACLs. All other property values are populated from the device database and are read-only in the WAAS Central Manager GUI.

Step 11 Click **Submit** to save the settings.

Step 12

Step 13 (Optional) Delete an IP ACL:

a) Click the **Edit** icon next to the name of the device that has the IP ACL that you want to delete.
b) Choose **Configure** > **Network** > **TCP/IP Settings** > **IP ACL**.

   If you created conditions for the IP ACL, you have two options for deletion:

   - **Delete ACL**—Removes the IP ACL, including all the conditions and associations with network interfaces and applications.
   - **Delete All Conditions**—Removes all the conditions, while preserving the IP ACL name.

c) To delete the entire IP ACL and its conditions, select the corresponding IP ACL and click Delete. You are prompted to confirm your action. Click **OK**. The record is deleted.
d) To delete only the conditions, select the condition or multiple conditions (consecutive or nonconsecutive conditions) and click Delete. When you are prompted to confirm your action, click **OK**. The conditions are deleted.

What to do next

To define an IP ACL from the CLI, you can use the **ip access-list** global configuration command, and to apply the IP ACL to an interface on the WAAS device, you can use the **ip access-group** interface configuration command. To configure the use of an IP ACL for SNMP, you can use the **snmp-server access-list** global configuration command. To specify an IP ACL that the WAE applies to the inbound WCCP redirected traffic that it receives, you can use the **wccp access-list** global configuration command

List of Extended IP ACL Conditions

When you define a condition for an extended IP ACL, you can specify the Internet protocol to be applied to the condition (as described in Step 7 in the Creating and Managing IP ACLs for Cisco WAAS Devices, on page 278).

The list of extended IP ACL conditions are as follows:

- Generic
- TCP
- UDP
- ICMP

Table 19: Extended IP ACL Generic Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Extended Type	Generic	Matches any IP.
Protocol	ip	IP (**gre**, **icmp**, **ip**, **tcp**, or **udp)**. To match any IP, use the keyword **ip**.
Source IP 1	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard 1	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.

Table 20: Extended IP ACL TCP Conditions

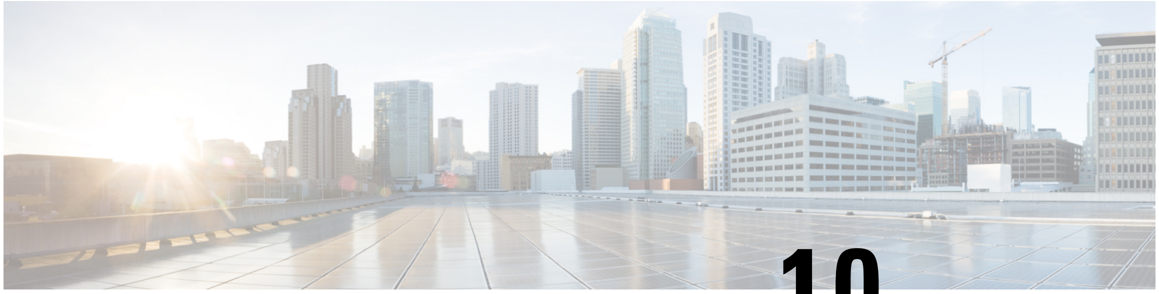
Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Extended Type	TCP	Matches the TCP IP.
Established	Unchecked (false)	When checked, a match with the ACL condition occurs if the TCP datagram has the ACK or RST bits set, indicating an established connection. Initial TCP datagrams used to form a connection are not matched.
Source IP	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Source Port 1	0	Decimal number or name of a TCP port. Valid port numbers are 0 to 65535. Valid TCP port names are as follows: ftp, ftp-data, https, mms, netbios-dgm, netbios-ns, netbios-ss, rtsp, ssh, telnet, and www.
Source Operator	range	Specifies how to compare the source ports against incoming packets. Choices are <, >, ==, !=, or range.
Source Port 2	65535	Decimal number or name of a TCP port. See Source Port 1, in this table.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Destination Port 1	0	Decimal number or name of a TCP port. Valid port numbers are 0-65535. Valid TCP port names are as follows: ftp, ftp-data, https, mms, netbios-dgm, netbios-ns, netbios-ss, rtsp, ssh, telnet, and www.
Destination Operator	range	Specifies how to compare the destination ports against incoming packets. Choices are <, >, ==, !=, or range.
Destination Port 2	65535	Decimal number or name of a TCP port. See Destination Port 1, in this table.

Table 21: Extended IP ACL UDP Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Extended Type	UDP	Matches the UDP IP.
Established	—	Not available for UDP.
Source IP	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Source Port 1	0	Decimal number or name of a UDP port. Valid port numbers are 0-65535. Valid UDP port names are as follows: bootpc, bootps, domain, mms, netbios-dgm, netbios-ns, netbios-ss, ntp, snmp, snmptrap, tacacs, tftp, and wccp.
Source Operator	range	Specifies how to compare the source ports against incoming packets. Choices are <, >, ==, !=, or range.
Source Port 2	65535	Decimal number or name of a UDP port. See Source Port 1, in this table.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Destination Port 1	0	Decimal number or name of a UDP port. Valid port numbers are 0-65535. Valid UDP port names are as follows: bootpc, bootps, domain, mms, netbios-dgm, netbios-ns, netbios-ss, ntp, snmp, snmptrap, tacacs, tftp, and wccp.
Destination Operator	range	Specifies how to compare the destination ports against incoming packets. Choices are <, >, ==, !=, or range.
Destination Port 2	65535	Decimal number or name of a UDP port. See Destination Port 1, in this table.

Table 22: Extended IP ACL ICMP Conditions

Field	Default Value	Description
Purpose	Permit	Specifies whether a packet is to be passed (**Permit**) or dropped (**Deny**).
Extended Type	ICMP	Matches the ICMP IP.
Source IP	0.0.0.0	Number of the network or host from which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Source IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
Destination IP	0.0.0.0	Number of the network or host to which the packet is being sent, specified as a 32-bit quantity in 4-part dotted decimal format.
Destination IP Wildcard	255.255.255.255	Wildcard bits to be applied to the source, specified as a 32-bit quantity in 4-part dotted decimal format. Place a 1 in the bit positions that you want to ignore and identify bits of interest with a 0.
ICMP Param Type	None	The ICMP parameter choices are **None**, **Type/Code**, or **Msg**. • **None** —Disables the ICMP Type, Code, and Message fields. • **Type/Code**—Allows ICMP messages to be filtered by ICMP message type and code. Also enables the ability to set an ICMP message code number. • **Msg**—Allows a combination of type and code to be specified using a keyword. Activates the ICMP message drop-down list. Disables the ICMP Type field.
ICMP Message	administratively-prohibited	Allows a combination of ICMP type and code to be specified using a keyword chosen from the drop-down list.
ICMP Type	0	Number from 0-255. This field is enabled when you choose **Type/Code**.
Use ICMP Code	Unchecked	When checked, enables the ICMP Code field.
ICMP Code	0	Number from 0-255. Message code option that allows ICMP messages of a particular type to be further filtered by an ICMP message code.



CHAPTER 10

Configuring Other System Settings

This chapter describes how to perform other system tasks such as setting the system clock, modifying the default system configuration settings, and enabling alarm overload detection, after you have done a basic configuration of your Cisco WAAS device. This chapter also describes how to register and manage Cisco IOS routers running Cisco AppNav-XE and Cisco WAAS Express.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco WAAS Central Managers and Cisco WAEs in your network. The term Cisco WAE refers to Cisco WAE and Cisco WAVE appliances, and Cisco vWAAS instances.

This chapter contains the following sections:

Modifying Device Properties

Before you begin

Use the Cisco WAAS Central Manager GUI to make the following changes to the properties of a Cisco WAE device:

- Rename the device.
- Assign a new location to the device.
- Assign an IP address to be used for management traffic to the device
- Deactivate or activate the device.

You can also use the Cisco WAAS Central Manager GUI to check the status of a device to determine if it is **Online**, **Pending**, or **Inactive**.

You can only rename a Cisco WAAS Central Manager device from the GUI.

To modify a device’s properties, follow these steps:

Procedure

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

Step 2 Choose *device-name* > **Activation**.

The **Device Activation** window appears, with fields for editing the properties of the selected device.

For a Cisco WAAS Central Manager device, the only fields that you can change in this window are the **Name** and **NetBIOS Name** of the device. In addition, the device IP address and role are displayed.

Step 3 Under the **General Configuration** heading, set or modify the following device properties:

- To change the hostname of the device, enter a new name in the **Name** field. This name must conform to the following rules:
  - The name must use only alphanumeric characters and hyphens (-).
  - The first and last character must be a letter or a digit.
  - Maximum length is 30 characters.
  - Names are case insensitive.
  - The following characters are considered illegal and cannot be used when naming a device:□ @, #, $,%, ^, &, *, (), |, \””/, <>.
- To activate or deactivate the device, check or uncheck the **Activate** check box.When this box is checked, the device is activated for centralized management through the Cisco WAAS Central Manager GUI.

  You can also click the **Deactivate** icon in the task bar to deactivate the device. Deactivating a device allows you to replace the device in the event of a hardware failure without losing all of its configuration settings.

- To change the NetBIOS name of the device, enter the new NetBIOS name for the device in the provided field. The NetBIOS name must not consist of only numbers; it must include some letters. This field is not displayed for Cisco WAAS Express devices.

Step 4 Under the **Locality** heading, set or change the location by choosing a new location from the Location drop-down list. To create a location for this device, see Creating Locations in the chapter "Using Device Groups and Device Locations."

Step 5 Under the **Management Interface Configuration with NAT** heading, configure the Network Address Translation (NAT) settings using the following fields:

a) To enable the Cisco WAAS Central Manager to use the IP address configured on the primary interface of the device to communicate with devices in the Cisco WAAS network that are behind a NAT firewall, check the **Use WAE's primary IP Address** check box.

This check box is not displayed for WAAS Express devices.

b) To allow the Cisco WAAS Central Manager to communicate with devices in the Cisco WAAS network that are behind the NAT firewall using an explicitly configured IP address, enter the IP address of the device in the **Management IP** field.

You also need to enter this address in scenarios where the primary interface for a Cisco WAE is set to an inline group interface and management traffic is configured on a separate IP address (either on a secondary IP address on the same inline group interface or on a built-in interface).

c) In the **Port** field, enter the port number for the management IP address. If the HTTPS server configured on a WAAS Express device is using a different port than the default of port 443, configure the same port here.

Note If the Cisco WAAS Central Manager cannot contact a device using the primary IP address, it attempts to communicate using the Management IP address.

Step 6 In the **Comments** field, enter comments that you want to display for this device.

Step 7 Click **Submit**.

Managing Cisco WAAS Software Licenses

This section contains the following topics:

About Managing Cisco WAAS Software Licenses

Cisco WAAS Version 4.1.1 and later provides software licenses that enable specific Cisco WAAS optimization and acceleration features. A software license must be installed and configured before the features that it enables will operate.

Table 23: Cisco WAAS Software Licenses lists the software licenses that may be purchased and the features that each license enables.

Table 23: Cisco WAAS Software Licenses

License	Description
Transport	Enables basic DRE, TFO, and LZ optimization. The Transport license cannot be configured if the Enterprise license is configured.
Enterprise	Enables the EPM, HTTP, MAPI, SSL, SMB, ICA, and Windows Print application accelerators, the Cisco WAAS Central Manager, and basic DRE, TFO, and LZ optimization. The Enterprise license cannot be configured if the Transport license is configured.

Consider the following operating guidelines for Cisco WAAS software licenses:

- Licenses are installed and managed only on individual Cisco WAE devices, not device groups. Not all licenses are supported on all devices.
- A Cisco WAAS Central Manager device requires only the Enterprise license and no other licenses can be configured.
- Cisco WAAS Express licenses cannot be managed via the Cisco WAAS Central Manager, because Cisco WAAS Express devices do not use the same kind of licenses as Cisco WAAS devices. Cisco WAAS Express licenses are managed via the router CLI only.

  The exact WAAS Express licensing process depends on the version of IOS running on your WAAS Express router:

  - Prior to Cisco IOS Version 15.3(3), the Cisco WAAS Express license is managed by using the router CLI command **license install**. This uses a single license that enables the Cisco WAAS Express optimization feature.
  - For Cisco IOS Version 15.3(3)M, the Cisco WAAS Express feature no longer requires a separate license, but is a **Right To Use** (RTU) feature included in the **AppxK9** license.
  - For Cisco IOS Version 15.4(1)T and later, Cisco WAAS Express is a **Right To Use** (RTU) feature that is included in the default license that is delivered with the router; no specific license needs to be installed.

- Regardless of the specific Cisco IOS version used, you must purchase the Cisco WAAS Express feature license.

Note If you are upgrading the Cisco WAAS Express devices to Cisco IOS Version 15.3(3)Mn, as part of the new **Appxk9** license support in Cisco WAAS Express IOS 15.3(3)M, you need to upgrade the Cisco WAAS Central Manager to Cisco WAAS Version 5.3.1 or later. or else the devices will go off offline.

Adding a Cisco WAAS Software License from the Cisco WAAS Central Manager

Procedure

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

Do not choose a Cisco WAAS Central Manager device to add a license, because you must use the Cisco WAAS CLI to manage licenses on Cisco WAAS Central Managers.

Step 2 Choose **Admin > History > License Management**.

Step 3 Check the check box next to each license that you want to add.

Step 4 Click **Submit**.

Adding and Managing Cisco WAAS Software Licenses from the Cisco WAAS CLI

Consider the following guidelines to add, remove, manage, or display Cisco WAAS software licenses:

- To add licenses from the Cisco WAAS CLI, run the **license add** EXEC command.
- To remove licenses from the Cisco WAAS CLI, run the **clear license** EXEC command.
- To display the status of all licenses from the Cisco WAAS CLI, run the **show license** EXEC command.
- To display the smart license status, run the **show license tech-support** EXEC command.
- You can also use the Cisco WAAS setup utility for basic Cisco WAE configuration when you set up a new Cisco WAAS device. Note that the Setup utility is only used for a new installation, because the running configuration of the existing system would not be reflected in the Setup tool.

  Consider the following recommendations, restrictions, and requirements when using the Cisco WAAS Setup utility:

  - For Cisco WAAS Version 6.0 and later, the Cisco WAAS Setup utility will accept IPv6 address for **Interface**, **Cisco WAAS Central Manager**, **Domain Name Server Entry** and **Network Time Protocol** settings. You can configure IPv4 only, IPv6 only or dual stack network using the Cisco WAAS setup utility.
  - The Cisco WAAS setup utility requires a minimum 25 row x 80 column terminal window for proper display (terminal length, if configured, must be 24).
  - For hyper terminal:

    - Set the emulation to **vt100**, so that all lines show up properly.

    - Set the **Input Translation** to **Shift-JIS** on the **File > Properties** menu.
  - When executing the Cisco WAAS setup utility from the Cisco WAAS CLI, disable console logging, to avoid system message flooding on the screen.
  - If you run the **restore factory-default** EXEC command, we recommend that you follow the system prompt to run the Cisco WAAS setup utility.

Enabling Smart Licensing

This section contains the following topics:

About Smart Licensing

Smart Licensing is a cloud-based, software license management solution that allows you to manage and track the status of your license, hardware and software usage trends. Smart Licensing enables you to automate time-consuming, manual licensing tasks by simplifying the three core functions of purchasing, managing and reporting of licenses. Smart Licensing on the device works with the Cisco Smart Software Manager (CSSM), the portal that enables you to manage all of your Cisco Smart software licenses from one centralized website.

Smart Licensing is available when you upgrade your Cisco WAAS Central Manager and all other devices registered with it to Cisco WAAS Version 6.4.3 and later. Table 24: Cisco Device Models Considered for Smart Licensing shows the models considered for smart licensing as part of this release.

Table 24: Cisco Device Models Considered for Smart Licensing

Cisco WAE and WAVE	Cisco ISR-WAAS	Cisco ENCS 5400-W	Cisco vWAAS	Cisco vCM
OE294 OE594 OE694 OE7541 OE7571 OE8541	OE-ISRWAAS-200 OE-ISRWAAS-750 OE-ISRWAAS-1300 OE-ISRWAAS-2500	WAAS-ENCS-W-200 WAAS-ENCS-W-750 WAAS-ENCS-W-1300 WAAS-ENCS-W-2500 WAAS-ENCS-W-6000	vWAAS-200 vWAAS-750 vWAAS-1300 vWAAS-2500 vWAAS-6000 vWAAS-12000 vWAAS-150000	vCM-100 vCM-500 vCM-1000 vCM-2000

Table 25: Checklist for Configuring Smart Licensing provides an overview of the steps to complete to set up and enable Smart Licensing.

Table 25: Checklist for Configuring Smart Licensing

Task	Description and Additional Information
1. Create a Smart Account.	Identify the information that you need to set up before configuring Smart licenses for your Cisco WAAS devices. For more information, see: • Creating a Smart Account, on page 295 • Adding Users to a Smart Account, on page 296 • Creating a New Token, on page 296

Task	Description and Additional Information
2. Enable Smart Licensing.	The steps required to enable smart licensing for the device. For more information, see Enabling Smart License on a Device, on page 296.
3. Obtain token from Cisco Smart Software Manager (CSSM).	The steps required to obtain a token to be used for registering your device. For more information, see Creating a New Token, on page 296.
4. Register or deregister the device with CSSM.	The steps required to register or deregister the device from the CSSM portal. For more information, see Registering a Device with Cisco Smart Manager, on page 297.

Creating a Smart Account

Before you begin

A **Smart Account** provides a single location for all Smart License-enabled products and entitlements. It assists in speed procurement, deployment and maintenance of Cisco Software. When creating a Smart Account, the submitter must have the authority to represent the requesting organization. After submitting, the request goes through a brief approval.

A **Virtual Account** exists as a sub-account within the Smart Account. Virtual Accounts are a customer defined structure based on organizational layout, business function, geography or any defined hierarchy. They are created and maintained by the Smart Account administrator(s).

The creation of a new Smart Account is a one-time event and subsequent management of users is a capability provided through the tool.

Procedure

Step 1 Log into the software.cisco.com and select **Administration** > **Request a Smart Account**.

Step 2 Select the type of Smart Account to create. There are two options:

- Individual Smart Account requiring agreement to represent your company. By creating this Smart Account you agree to authorization to create and manage product and service entitlements, users and roles on behalf of your organization.
- Create the account on someone else’s behalf.

Step 3 Provide the required domain identifier and the preferred account name.

The account request will be pending an approval of the **Account Domain Identifier**. A subsequent email will be sent to the requester to complete the setup process.

Adding Users to a Smart Account

Before you begin

Smart Account user management is available in the **Administration** section of software.cisco.com.

Procedure

Step 1 Log in to software.cisco.com and choose **Manage Smart Account> Administration**.

Step 2 From the **Administration** window, choose **Users** > **New User** and provide the required email address, Cisco ID and role. Roles may be defined to manage the entire Smart Account or specific Virtual Accounts.

Step 3 To complete this process, click **Continue**.

Creating a New Token

Before you begin

A token is required for registering a device to the Cisco Smart Software Manager (CSSM).

Procedure

Step 1 Log into the **CSSM**, select the appropriate **Virtual Account** and in the **General** tab, choose **New Token**.

Step 2 Follow the dialog box instructions to provide a name, duration and export compliance applicability before accepting the terms and responsibilities.

Step 3 To continue, choose **Create Token**.

Step 4 Copy the token ID. The Cisco Smart Software Manager will respond with a dialogue, indicating that the token has been copied to your clipboard.

Enabling Smart License on a Device

Before you begin

Cisco WAAS Version 6.4.3 and later, Cisco WAAS devices support both traditional licensing and smart software licensing. Eventually all devices in Cisco WAAS will support only the smart software licensing model in which case it will be enabled by default and the product instance will start in Evaluation Mode. Evaluation Mode means that a product instance has enabled Smart Licensing (either manually or by default and has not registered with Cisco Smart Software Manager or Cisco Smart Software Manager satellite).

Procedure

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

Step 2 Choose **Admin** > **Licenses**> **Smart License**.

The **Smart License Configuration** window appears.

Step 3 At the **Smart License Registration** pane, choose **Enable Smart License**.

Step 4 To see how your device communicates with the CSSM, see **View/Edit the Transport Settings**. The Transport methods are:

- **Direct**: The product communicates directly with Cisco's Licensing Servers. If you selected this the url is automatically populated.
- **HTTP Proxy**: The product communicates via an HTTP or HTTPS Proxy. Enter the **Proxy Host** and **Proxy Port** details in the respective fields and click **OK**.
- **Smart Software Satellite**: The product communicates via proxy via Transport Gateway or Smart Software Manager Satellite. Enter the URL of the gateway and click **OK**.

  The transport URL for satellite server version 5.0.1 is:

  http://satellite_server.ip/Transportgateway/services/DeviceRequestHandler

  The transport URL for satellite server version 7-202001 is:

  http://satellite_server.ip/SmartTransport

  Before configuring Smart Software Satellite, ensure that the Smart Software Manager Satellite is installed and is in running state. For more information, see the Smart Software Manager Satellite Enhanced Edition Installation Guide.

Step 5 Click **Submit**.

The product is in **Evaluation** mode after enabling Smart Software License and you can see the **Authorization Status** reflecting the same. The evaluation mode is for 90 days. You can continue to use the product in the **Evaluation** mode state.

Registering a Device with Cisco Smart Manager

Before you begin

A functioning Smart Account is required to complete the registration process. If you do not have a smart account, see Creating a Smart Account, on page 295.

During the registration process, three key elements are exchanged with the Cisco Smart Software Manager (CSSM) over HTTPS:

- **Trusted Unique Identifier**: The device ID (SUDI, SUVI, or ID).
- **Organizational Identifier**: In a numerical format to associate the product with a Smart Account or Virtual Account.
- **Licenses consumed**: Allows the CSSM to understand the license type and level of consumption.

Procedure

Step 1 Verify that you have completed steps 1-5 in Enabling Smart License on a Device.

Step 2 A token ID is required to register your device to CSSM. If you do not have a token, log into the Cisco Smart Software Manager and do the needful. For more information, see Creating a New Token.

Step 3 At the Cisco WAAS Central Manager GUI:

a) In the **Token ID** field, enter the token ID that you had obtained earlier.

b) From the drop-down list, to trigger the Smart License registration, choose **Register**.

- If you are initiating a fresh device registration, the license information is updated on the **CSSM** > **Smart Account Name** > **Virtual Account Name** > **Inventory** > **Licenses** tab.
- If your product instance is already registered, based on the license consumption, the following status is shown:
  - **Authorized**: If the license is available in the Cisco Smart Account.
  - **Out of Compliance**: If there is no license available in the Cisco Smart Virtual Account for that particular model. After license conversion process is complete the status changes to Authorized.

Note Conversion status and wait time for the next poll will be updated in Smart Agent after one hour and the same will be updated in the Cisco WAAS Central Manager GUI. This is because the Smart Agent running on the Cisco WAAS device takes one hour to check with the CSSM portal. *Do not perform any actions* such as re-register, reload, or restart, on the device when the conversion is in the **In Progress** state.

After completion of this process, the device is smart-enabled and accounted for. Smart License Status Field Details shows the refreshed details under the **Smart Licensing Status** after the registration is complete.

To see the latest device Smart License status in the Cisco WAAS Central Manager, click the **Refresh** button after each **Submit** action.

Table 26: Smart License Status Field Details

Field	Description
Registration Status	The registration status can be **Registered**, **Unregistered**, or **Registration Expired**: • **Registered**: The product is registered. The display shows **License Registered** and the registration date. • **Unregistered**: Smart Software Licensing is enabled but this Product Instance is not registered with CSSM. If any licenses are in use, it will run in Evaluation Mode until the evaluation period expires. • **Registration Expired**: Indicates that the device has been unable to communicate with the Cisco Smart Software Manager for an extended period of time. The device will attempt to contact the CSSM six months once in order to renew the ID certificate. If the Agent cannot communicate with the Cisco Smart Software Manager it will continue to try and renew the ID certificate until the expiration date (one year). Typically after one year this state will be present if failed to renew ID certificate.
Authorization Status	The Smart License authorization status can be **Unconfigured**, **Unidentified**, **Evaluation Mode**, **Authorized**, **Out-of-Compliance**, or **Authorization Expired**: • **Unconfigured**: Smart Software Licensing has not been configured. • **Unidentified**: Smart Software Licensing has been enabled but the registration has not taken place. • **Evaluation Mode**: Product is not registered with CSSM. If any licenses are in use, they are in Evaluation Mode and will run till the Evaluation period expires. • **Authorized**: Registration has been completed with a valid Smart Account and license consumption has begun.This is an indication of being in compliance. • **Out-Of-Compliance**: The virtual account containing your product instance has a license shortage for this type. You must buy additional licenses. • **Authorization Expired**: The device has been unable to communicate with the Cisco Smart Software Manager for an extended period of time. Typically after ninety days this state will be present. The device will attempt to contact the CSSM every hour in order to renew the authorization until the registration period expires.
Smart Account	A collection of virtual accounts that is accessible for you.
Virtual Account	A collection of licenses and product instances.

Field	Description
Product Instance	Unique Device Identifier used to identify an individual device registered with CSSM using a product instance registration token.
Transport Settings	Communication method with CSSM.

Step 4 In the case of **Registration** or **Authorization** failure: After viewing the failure message in the Cisco WAAS Central Manager GUI, click the **Force Register** button to register the product (in case there is an issue with the registration).

Step 5 Table 27: Registered State Actions displays the actions you can choose after the device is in **Registered** state.

Table 27: Registered State Actions

Action	Description
Renew ID Certificate	Smart Software Licensing registration certificate is renewed automatically by the agent every six months, so you may not need to use the **Renew ID Certificate** option in the page-level actions menu. • If you want to manually renew the Smart Software Licensing registration certificate, selecting the option that displays a progress dialog box as the product attempts to contact the Smart Software Manager or satellite. • After initiated, the operation runs in the background.
Renew Authorization	License authorization is renewed automatically by the agent every thirty days, so you may not need to use the Renew Authorization option in the page-level actions menu. • If you want to manually renew license authorization, selecting the option that displays a progress dialog box as the product attempts to contact the Smart Software Manager or satellite. • After initiated, the operation runs in the background.
Deregister	**Product Instance** no longer appears in the Smart Software Manager and the licenses being used will be made available (for use) to other products in the **Virtual Account**.
Disable	Disables the smart licensing for this product and deregisters from CSSM or satellite.

Step 6 To disable or to deregister the device from CSSM, from the **Action** drop-down list, choose **Deregister** or choose **Disable**, and click **Submit**. This will release the license from CSSM portal after successful deregistration.

Consider the following guidelines for viewing the status after you disable or deregister a device from the CSSM:

- After each action the details under the Smart Licensing Status are updated.
- Periodic synchronization between Cisco WAAS and CSSM every 24 hrs, ensures that the Smart Licensing status for the devices is up to date and in sync with the CSSM.

- You can monitor the smart license logs in the **smart-license.log** file under errorlog.
- To use the Cisco WAAS CLI to display the smart license status, run the **show license tech-support** EXEC command.

Enabling FTP Services

Before you begin

File Transfer Protocol (FTP) lets you download, upload, and copy configuration files between remote hosts and a switch. Unlike TFTP, which uses User Datagram Protocol (UDP), a connectionless protocol, FTP uses TCP, which is connection oriented. Inetd (an Internet daemon) is a program that listens for connection requests or messages for certain ports and starts server programs to perform the services associated with those ports. FTP copies files between devices.

FTP is a subset of the UNIX rshell service, which allows UNIX users to execute shell commands on remote UNIX systems. It is a UNIX built-in service. This service uses TCP as the transport protocol and listens for requests on TCP port 514. FTP service can be enabled on Cisco WAAS devices that use Cisco WAAS software.

Note For the FTP transfer to be successful, configure a Pass-Through policy for the FTP server. If an Optimized policy is configured for the FTP server, the FTP transfer will fail.

Procedure

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

Step 2 Choose **Configure** > **Network** > **Network Services**.

The **Network Services** window appears.

Step 3 To enable **Inetd FTP** services, check the **Enable FTP** check box. By default, this option is disabled.

Note The **Inetd** daemon listens for FTP and TFTP services. For **Inetd** to listen to FTP requests, it must be explicitly enabled for FTP service.

Step 4 To save your changes, click **Submit**.

Consider the following guidelines for saving these changes:

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

- If you try to leave this window without saving the modified settings, a **Warning** dialog box prompts you to submit the changes. The **Warning** dialog box appears only if you are using the Internet Explorer browser.

Configuring Date and Time Settings

This section explains how to configure date and time settings for your WAAS network devices and contains the following topics:

Configuring NTP Settings

Before you begin

The Cisco WAAS Central Manager GUI allows you to configure the time and date settings using a Network Time Protocol (NTP) host on your network. NTP allows the synchronization of time and date settings for the different geographical locations of the devices in your Cisco WAAS network, which is important for proper system operation and monitoring. On each Cisco WAAS device, be sure to set up an NTP server to keep the clocks synchronized.

Procedure

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

Step 2 Choose **Configure** > **Date/Time** > **NTP**.

The **NTP Settings** window appears.

Step 3 In the **NTP Server** field, enter up to four hostnames or IP addresses, separated by spaces.This field also accepts IPv6 addresses.

Step 4 Click **Submit**.

Note Unexpected time changes can result in unexpected system behavior. We recommend that you reload the system after configuring an NTP server or changing the system clock.

Configuring Time Zone Settings

Before you begin

If you have an outside source on your network that provides time services (such as an NTP server), you do not need to set the system clock manually. When manually setting the clock, enter the local time.

Note Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at startup to initialize the software clock.

Procedure

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

Step 2 Choose **Configure** > **Date/Time** > **Time Zone**. The **Time Zone Settings** window appears.

Step 3 To configure a standard time zone, follow these steps:

a) Under the **Time Zone Settings** section, click the **Standard Time Zone** radio button. The default is Universal Time Coordinated (UTC) (offset = 0) with no summer time configured. When you configure a standard time zone, the system is automatically adjusted for the UTC offset, and the UTC offset need not be specified.

   The standard convention for time zones uses a **Location/Area** format in which **Location** is a continent or a geographic region of the world and **Area** is a time zone region within that location.

b) From the **Standard Timezone** drop-down list, choose a location for the time zone. For an explanation of the abbreviations in this list, see Table 28: Timezone Location Abbreviations.

   The window refreshes, displaying all area time zones for the chosen location in the second drop-down list.

c) Choose an area for the time zone. The UTC offset is automatically set for standard time zones.

   Summer time is built-in for some standard time zones (mostly time zones within the United States), and will result an automatic change in the UTC offset during summer time. For a list of standard time zones that can be configured and their UTC offsets, see Table 29: Timezone - Offset from UTC.

Step 4 To configure a customized time zone on the device, follow these steps:

a) In the **Time Zone Settings** pane, click the **Customized Time Zone** radio button.
b) In the **Customized Time Zone** field, specify the name of the time zone. The time zone entry is case-sensitive and can contain up to 40 characters including spaces. If you specify any of the standard time zone names, an error message is displayed when you click **Submit**.
c) For UTC Offset, from the first drop-down list choose the plus sign (+) or minus sign (–) sign to specify whether the configured time zone is ahead or behind UTC. Also, choose the number of **hours** (**0 to 23**) and **minutes** (**0–59**) offset from UTC for the customized time zone. The range for the **UTC offset** is from **-23:59 to 23:59**, and the default is **0:0**.

Step 5 This step shows how to configure two types of customized summer time, **Absolute Summer Time** and **Recurring Summer Time**.

Note You can specify a customized summer time for both standard and customized time zones.

Configuring Absolute Summer Time

a) At the **Customized Summer Time Savings** pane, click the **Absolute Dates** radio button.

   You can configure a start date and end date for summer time in absolute dates or recurring dates. Absolute date settings apply only once and must be set every year. Recurring dates apply repeatedly for many years.

b) In the **Start Date** and **End Date** fields, specify the **month** (**January through December**), **day** (**1 to 31**), and **year** (**1993 to 2032**) on which summer time must start and end, in the **mm/dd/yyyy** format. Make sure that the end date is always later than the start date.

- Alternatively, click the **Calendar** icon next to the **Start Date** and **End Date** fields to display the **Date Time Picker** popup window. By default, the current date is highlighted in yellow.
- In the **Date Time Picker** popup window, use the left or right arrow icons to choose the previous or following years, if required. Choose a month from the drop-down list. Click a day of the month. The chosen date is highlighted in blue. Click **Apply**. Alternatively, click **Set Today** to revert to the current day. The chosen date will be displayed in the **Start Date** and **End Date** fields.

Configuring Recurring Summer Time

a) At the **Customized Summer Time Savings** pane, click the **Recurring Dates** radio button.
b) From the **Start Day** drop-down list, choose a day of the week to start (**Monday to Sunday**).
c) From the **Start Week** drop-down list, choose an option to set the starting week (**first, 2nd, 3rd, or last**).

For example, choose **first** to configure summer time to recur beginning the first week of the month or choose **last** to configure summer time to recur beginning the last week of the month.

d) From the **Start Month** drop-down list, choose a month to start (**January to December**).
e) From the **End Day** drop-down list, choose a day of the week to end (**Monday to Sunday**).
f) From the **End Week** drop-down list, choose an option to set the ending week (**first, 2nd, 3rd, or last**).

For example, choose first to configure summer time to end beginning the first week of the month or last to configure summer time to stop beginning the last week of the month.

g) From the **End Month** drop-down list, choose a month to end (**January to December**).

Step 6 **Start Time** and **End Time** fields for summer time are the times of the day when the clock is changed to reflect summer time. By default, both start time and end time are set to **00:00**.

To configure start time and end time:

a) From the **Start Time** drop-down lists, choose the **hour** (**0 to 23**) and **minute** (**0 to 59**) at which daylight saving time should start.
b) From the **End Time** drop-down lists, choose the **hour** (**0 to 23**) and **minute** (**0 to 59**) at which daylight saving time should end.

Step 7 In the **Offset** field, specify the minutes offset from UTC (**0–1439**). (See Table 29: Timezone - Offset from UTC.)

The summer time offset specifies the number of minutes that the system clock moves forward at the specified start time and backward at the end time.

Step 8 To not specify a summer or daylight saving time for the corresponding time zone, click the **No Customized Summer Time Configured** radio button .

Step 9 To save the settings, click **Submit**.

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

If you try to leave this window without saving the modified settings, a warning dialog box prompts you to submit the changes. This dialog box only appears if you are using the Internet Explorer browser.

Table 28: Timezone Location Abbreviations

Time Zone	Expansion
CET	Central European Time
CST/CDT	Central Standard/Daylight Time
EET	Eastern European Time
EST	Eastern Standard Time
EST/EDT	Eastern Standard/Daylight Time
GB	Great Britain
GB-Eire	Great Britain/Ireland
GMT	Greenwich Mean Time
HST	Hawaiian Standard Time
MET	Middle European Time
MST	Mountain Standard Time
MST/MDT	Mountain Standard/Daylight Time
NZ	New Zealand
NZ-CHAT	New Zealand, Chatham Islands
PRC	People’s Republic of China
PST/PDT	Pacific Standard/Daylight Time
ROC	Republic of China
ROK	Republic of Korea
UCT	Coordinated Universal Time
UTC	Coordinated Universal Time
WET	Western European Time
W-SU	Middle European Time

Table 29: Timezone - Offset from UTC

Time Zone	Offset from UTC (in hours)
Africa/Algiers	+1
Africa/Cairo	+2

Time Zone	Offset from UTC (in hours)
Africa/Casablanca	0
Africa/Harare	+2
Africa/Johannesburg	+2
Africa/Nairobi	+3
America/Buenos_Aires	-3
America/Caracas	-4
America/Mexico_City	-6
America/Lima	-5
America/Santiago	-4
Atlantic/Azores	-1
Atlantic/Cape_Verde	-1
Asia/Almaty	+6
Asia/Baghdad	+3
Asia/Baku	+4
Asia/Bangkok	+7
Asia/Colombo	+6
Asia/Dacca	+6
Asia/Hong_Kong	+8
Asia/Irkutsk	+8
Asia/Jerusalem	+2
Asia/Kabul	+4.30
Asia/Karachi	+5
Asia/Katmandu	+5.45
Asia/Krasnoyarsk	+7
Asia/Magadan	+11
Asia/Muscat	+4
Asia/New Delhi	+5.30
Asia/Rangoon	+6.30

Time Zone	Offset from UTC (in hours)
Asia/Riyadh	+3
Asia/Seoul	+9
Asia/Singapore	+8
Asia/Taipei	+8
Asia/Tehran	+3.30
Asia/Vladivostok	+10
Asia/Yekaterinburg	+5
Asia/Yakutsk	+9
Australia/Adelaide	+9.30
Australia/Brisbane	+10
Australia/Darwin	+9.30
Australia/Hobart	+10
Australia/Perth	+8
Australia/Sydney	+10
Canada/Atlantic	-4
Canada/Newfoundland	-3.30
Canada/Saskatchewan	-6
Europe/Athens	+2
Europe/Berlin	+1
Europe/Bucharest	+2
Europe/Helsinki	+2
Europe/London	0
Europe/Moscow	+3
Europe/Paris	+1
Europe/Prague	+1
Europe/Warsaw	+1
Japan	+9
Pacific/Auckland	+12

Time Zone	Offset from UTC (in hours)
Pacific/Fiji	+12
Pacific/Guam	+10
Pacific/Kwajalein	+12
Pacific/Samoa	-11
US/Alaska	-9
US/Central	-6
US/Eastern	-5
US/East-Indiana	-5
US/Hawaii	-10
US/Mountain	-7
US/Pacific	-8

UTC was formerly known as Greenwich Mean Time (GMT). The offset time (number of hours ahead or behind UTC) as displayed in Table 29: Timezone - Offset from UTC is in effect during winter time. During summer time or daylight saving time, the offset may be different from the values in the table and is calculated and displayed accordingly by the system clock.

Configuring Secure Store Encryption Settings

Secure Store encryption provides strong encryption and key management for your Cisco WAAS system. The Cisco WAAS Central Manager and Cisco WAE devices use secure store encryption for handling passwords, managing encryption keys, and for data encryption.

This section contains the following topics:

- About Secure Store Encryption, on page 309
- Workflow for Enabling Secure Store Encryption, on page 309
- Operating Guidelines for Secure Store Encryption, on page 310
- Enabling Secure Store Encryption on the Cisco WAAS Central Manager, on page 311
- Enabling Secure Store Encryption on a Standby Cisco WAAS Central Manager, on page 312
- Enabling Secure Store Encryption on a Cisco WAE Device, on page 313
- Changing the Secure Store Passphrase Mode, on page 313
- Changing the Secure Store Encryption Key and Password, on page 314
- Resetting Secure Store Encryption on a Cisco WAAS Central Manager, on page 316

- Disabling Secure Store Encryption on a Cisco WAE Device, on page 317

About Secure Store Encryption

With Secure Store encryption on the Cisco WAAS Central Manager or a Cisco WAE device, the Cisco WAAS system uses strong encryption algorithms and key management policies to protect certain data on the system. This data includes encryption keys used by applications in the Cisco WAAS system, user login passwords and certificate key files.

Secure Store encryption on the Cisco WAAS Central Manager is always enabled and uses a password that is auto-generated or user-provided. This password is used to generate the key encryption key according to secure standards. The Cisco WAAS system uses the key encryption key to encrypt and store other keys generated on the Cisco WAAS Central Manager or Cisco WAE devices. These other keys are used for Cisco WAAS functions including disk encryption, SSL acceleration, or to encrypt user passwords.

Data on the Cisco WAAS Central Manager is encrypted using a 256-bit key encryption key generated from the password and using SHA1 hashing and an AES 256-bit algorithm. When Secure Store is enabled on a WAE device the data is encrypted using a 256-bit key encryption key generated using SecureRandom, a cryptographically strong pseudo random number generator.

Secure Store encryption on a Cisco Central Manager uses one of the following modes:

- **Auto-generated passphrase mode**: The passphrase is automatically generated by the Cisco WAAS Central Manager and used to open the Secure Store after each system reboot. This is the default mode for new Cisco WAAS Central Manager devices or after the system has been reinstalled.
- **User-provided passphrase mode**: The passphrase is supplied by the user and must be entered after each system reboot to open the Secure Store. You can switch to this mode, and systems upgraded from Cisco WAAS versions earlier than Cisco WAAS Version 4.4.1, with Secure Store initialized, are configured in this mode after upgrading to Cisco WAAS Version 4.4.1 or later.

To implement Secure Store, your system must meet the following requirements:

- You must have a Cisco WAAS Central Manager configured for use in your network.
- Your Cisco WAE devices must be registered with the Cisco WAAS Central Manager.
- Your Cisco WAE devices must be online (have an active connection) with the Cisco WAAS Central Manager. This requirement applies only if you are enabling Secure Store on Cisco WAE devices.
- All Cisco WAAS Central Managers and Cisco WAE devices must be running Cisco WAAS Version 4.0.19 or later.

Workflow for Enabling Secure Store Encryption

Table 30: Workflow for Enabling Secure Store Encryption describes the steps and sections used to enable Secure Store encryption.

Table 30: Workflow for Enabling Secure Store Encryption

Task	Description or Section
1. Confirm that your system meets all requisite requirements listed in this table row.	• A Cisco WAAS Central Manager configured for use in your network. • Your Cisco WAE devices are registered with the Cisco WAAS Central Manager. • Your Cisco WAE devices are online (have an active connection) with the Cisco WAAS Central Manager. This requirement applies only if you are enabling Secure Store on Cisco WAE devices. • All Cisco WAAS Central Managers and Cisco WAE devices are running Cisco WAAS Version 4.0.19 or later.
2. Enable strong storage encryption on your Primary Cisco WAAS Central Manager.	• Enabling Secure Store Encryption on the Cisco WAAS Central Manager, on page 311 • You can enable Secure Store independently on the Cisco WAAS Central Manager and on the Cisco WAE devices. To ensure full protection of your encrypted data, enable Secure Store on both the Cisco WAAS Central Manager and the Cisco WAE devices. You must enable Secure Store on the Cisco WAAS Central Manager first.
3. Enable strong storage encryption on any Standby Cisco WAAS Central Managers.	Enabling Secure Store Encryption on a Standby Cisco WAAS Central Manager, on page 312
4. Enable strong storage encryption on Cisco WAE devices or Cisco WAE device groups.	Enabling Secure Store Encryption on a Cisco WAE Device, on page 313

Operating Guidelines for Secure Store Encryption

Note the following considerations regarding the Secure Store:

Note When you reboot the Cisco Central Manager, if Secure Store is in user-provided passphrase mode, you must manually open Secure Store encryption. All services that use the Secure Store (such as disk encryption, SSL acceleration, or AAA) on the remote Cisco WAE devices do not operate properly until you enter the Secure Store password on the Cisco WAAS Central Manager to open Secure Store encryption.

- Passwords stored in the Cisco WAAS Central Manager database are encrypted using strong encryption techniques.
- Certificate key files are encrypted using the strong encryption key on the Cisco WAAS Central Manager.

- If a primary Cisco WAAS Central Manager fails, Secure Store key management is handled by the standby Cisco WAAS Central Manager. (Secure Store mode must be enabled manually on the standby Cisco WAAS Central Manager.)
- Backup scripts back up the Secure Store passphrase mode (user-provided or auto-generated) of the device at the time of backup. Backup and restore are supported only on the Cisco WAAS Central Manager.
- If you have a backup made when the Secure Store was in **user-provided passphrase mode** and you restore it to a system where the Secure Store is in **auto-generated passphrase mode**, you must enter the user passphrase to proceed with the restore. After the restore, the system is in **user-provided passphrase mode**.

  If you have a backup made when the Secure Store was in **auto-generated passphrase mode** and you restore it to a system where the Secure Store is in **user-provided passphrase mode**, you do not need to enter a password. After the restore, the system is in **auto-generated passphrase mode**.
- When you enable Secure Store on a Cisco WAE device, the system initializes and retrieves a new encryption key from the Cisco WAAS Central Manager. The Cisco WAE uses this key to encrypt data credentials and information on the disk (if disk encryption is also enabled).
- When you reboot the Cisco WAE after enabling Secure Store, the Cisco WAE retrieves the key from the Cisco WAAS Central Manager automatically, allowing normal access to the data that is stored in Cisco WAAS persistent storage. If key retrieval fails, a critical alarm is raised and Secure Store should be reopened manually. Until Secure Store is reopened, the Cisco WAE rejects configuration updates from the Cisco WAAS Central Manager if the updates contain dynamic share, or user configuration. Also, the Cisco WAE does not include preposition configuration in the updates that it sends to the Cisco WAAS Central Manager.
- While Secure Store encrypts certain system information, it does not encrypt the data on the hard drives. To protect the data disks, you must enable disk encryption separately.

Enabling Secure Store Encryption on the Cisco WAAS Central Manager

Before you begin

Secure Store is enabled by default on a new Cisco WAAS Central Manager, with a system-generated password that opens the Secure Store after the system boots. You do not need to do anything to enable Secure Store.

If a Cisco WAAS Central Manager is configured in user-provided passphrase mode, you must manually open the Secure Store after the system boots.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin > Secure Store**.

The **Configure CM Secure Store** window appears.

Step 2 At the **Open Secure Store** pane, enter the **Secure Store passphrase** in the **Current passphrase** field.

Step 3 Click **Open**.

The Secure Store is opened. Data is encrypted using the key derived from the password.

Note When you enable Secure Store on the primary Cisco WAAS Central Manager in **user-provided passphrase mode**, you should also enable Secure Store on the Standby Cisco WAAS Central Manager. For more information, see Enabling Secure Store Encryption on a Standby Cisco WAAS Central Manager, on page 312.

Step 4 To use the Cisco WAAS CLI to enable and view status about Secure Store Encryption:

- To enable Secure Store Encryption, run the **cms secure-store open** EXEC command.
- To view the status of the Secure Store Encryption, run the **show cms secure-store** EXEC command.

Enabling Secure Store Encryption on a Standby Cisco WAAS Central Manager

Before you begin

Before you enable Secure Store Encryption on a Standby Cisco WAAS Central Manager, consider these guidelinse:

- **A Standby Cisco WAAS Central Manager provides limited encryption key management support**. If the Primary Cisco WAAS Central Manager fails, the Standby Cisco WAAS Central Manager provides only encryption key retrieval to the Cisco WAE devices but does *not* provide new encryption key initialization. Do *not* enable disk encryption or Secure Store on Cisco WAE devices when the primary Cisco WAAS Central Manager is not available.
- The Secure Store **passphrase mode** on the primary Cisco WAAS Central Manager is replicated to the Standby Cisco WAAS Central Manager (within the standard replication time). If the primary Cisco WAAS Central Manager is switched to **auto-generated passphrase mode**, the Standby Cisco WAAS Central Manager Secure Store changes to the **Open** state. If the Primary Cisco WAAS Central Manager is switched to **user-provided passphrase mode** or the passphrase is changed, the Standby Cisco WAAS Central Manager Secure Store changes to the **Initialized** but not open state and an alarm is raised. You must manually open the Secure Store on the Standby Cisco WAAS Central Manager.
- To enable Secure Store encryption on a Standby Cisco WAAS Central Manager when the Primary Cisco WAAS Central Manager is in **user-provided passphrase mode**, open the Secure Store on the Primary Cisco WAAS Central Manager and then use the Cisco WAAS CLI to run the **cms secure-store open** EXEC mode command on the Standby Cisco WAAS Central Manager.

Procedure

Step 1 Enable Secure Store encryption on the Primary Central Manager. For more information, see Enabling Secure Store Encryption on the Cisco WAAS Central Manager, on page 311.

Step 2 Wait until the standby Cisco WAAS Central Manager replicates the data from the primary Central Manager.

The replication should occur in 60 seconds (default) or as configured for your system.

Step 3 To activate Secure Store encryption, run the **cms secure-store open** EXEC command on the Standby Cisco WAAS Central Manager.

The Standby Cisco WAAS Central Manager displays the **Please enter passphrase** message.

Step 4 Type the password and click **Enter**.

The Standby Central Manager encrypts the data using Secure Store Encryption.

Note For each Standby Cisco WAAS Center Manager on your system, repeat Step 3 and Step 4.

Step 5 To use the Cisco WAAS CLI to view the status of the Secure Store Encryption, run the **show cms secure-store** EXEC command.

Enabling Secure Store Encryption on a Cisco WAE Device

Procedure

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

Note The Secure Store status must be the same for all Cisco WAE devices in a device group. Either all Cisco WAE devices in the group must have Secure Store enabled, or all must have Secure Store disabled. Before you add a Cisco WAE device to a device group, set its Secure Store status to match the others. See Working with Device Groups in the chapter "Using Device Groups and Device Locations."

Step 2 Choose **Configure** > **Security** > **Secure Store**.

The **Secure Store Settings** window appears.

Step 3 Check the **Initialize CMS Secure Store** box. (The **Open CMS Secure Store** check box will be checked automatically.)

Step 4 To activate Secure Store encryption, click **Submit**.

A new encryption key is initialized on the Cisco WAAS Central Manager, and the Cisco WAE encrypts the data using Secure Store encryption.

Note When you enable or disable Secure Store on a device group, the changes do not take effect on all Cisco WAE devices simultaneously. When you view the Cisco WAE devices, be sure to give the Cisco WAAS Central Manager enough time to update the status of each Cisco WAE device.

Step 5 To enable Secure Store from the Cisco WAAS CLI, run the **cms secure-store init** EXEC command.

Note If you have made any other Cisco WAAS CLI configuration changes on a Cisco WAE within the datafeed poll rate time interval (five minutes by default) *before* running the **cms secure-store** EXEC command, those prior configuration changes are lost and you must redo them.

Changing the Secure Store Passphrase Mode

Secure Store can operate either in **user-provided mode** or **auto-generated passphrase mode**, and you can switch between these modes.

To change Secure Store passphrase mode from the Cisco WAAS CLI, run the **cms secure-store mode** EXEC command.

Use the following **Step 1** to switch from **user-provided passphrase mode** to **auto-generated passphrase mode**. Use the following **Step 2** to switch from **auto-generated passphrase mode** to **user-provided passphrase mode**.

Procedure

Step 1 To switch from **user-provided passphrase mode** to **auto-generated passphrase mode**, follow these steps:

a) From the Cisco WAAS Central Manager menu, choose **Admin** > **Secure Store**.
b) In the **Switch to CM auto-generated passphrase mode** pane, enter the password in the **Current passphrase** field.
c) Click **Switch**.
d) In the **Confirmation** message that appears, click **OK**.

The Secure Store is changed to **auto-generated passphrase mode** and remains in the **Open** state.

Step 2 To switch from **auto-generated passphrase mode** to **user-provided passphrase mode**, follow these steps:

a) From the Cisco WAAS Central Manager menu, choose **Admin** > **Secure Store**.
b) In the **Switch to User-provided passphrase mode** pane, enter a password in the **New passphrase** field, and re-enter the password in the **Confirm passphrase** field.

   The password must conform to the following rules:

   - A length of 8 to 64 characters
   - Contain characters only from the allowed set: A-Za-z0-9~%'!#$^&*()|;:,"<>/
   - Contain at least one digit
   - Contain at least one lowercase and one uppercase letter

c) Click **Switch**.
d) In the **Confirmation** message that appears, click **OK**.

The Secure Store is changed to **user-provided passphrase mode** and remains in the **Open** state. If you have a Standby Cisco WAAS Central Manager, you must manually open its Secure Store. For more information, see Enabling Secure Store Encryption on a Standby Cisco WAAS Central Manager, on page 312.

Note When you reboot a Cisco WAAS Central Manager that is configured in **user-provided passphrase mode**, you must re-open the Secure Store manually. All services that use the Secure Store (such as disk encryption, SSL acceleration, or AAA) on the remote Cisco WAE devices do not operate properly until you enter the Secure Store password on the Cisco WAAS Central Manager to reopen the Secure Store. Switch to **auto-generated passphrase mode** to avoid having to re-open the Secure Store after each reboot.

Changing the Secure Store Encryption Key and Password

This section contains the following topics:

Changing the Secure Store Encryption Key and Password on the Cisco WAAS Central Manager

The Secure Store encryption password is used by the Cisco WAAS Central Manager to generate the encryption key for the encrypted data. If the Cisco WAAS Central Manager is configured for user-provided passphrase mode, you can change the password.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **Secure Store**.

Step 2 In the **Change Secure Store passphrase** pane, in the **Current passphrase** field, enter the current password.

Step 3 In the **New passphrase** field, enter the new password.

The password must conform to the following rules:

- Be 8 to 64 characters in length
- Contain characters only from the allowed set: A-Za-z0-9~%'!#$^&*()|;:,"<>/
- Contain at least one digit
- Contain at least one lowercase and one uppercase letter

Step 4 In the **Confirm passphrase** field, enter the new password again.

Step 5 Click **Change**.

The Cisco WAAS device re-encrypts the stored data using a new encryption key derived from the new password.

Note There may be a delay of a few minutes after you click **Change** before the changes take effect.

Step 6 To use the Cisco WAAS CLI to change the password and generate a new encryption key on the Central Manager, run the **cms secure-store change** EXEC command.

Changing the Secure Store Encryption Key and Password on a Cisco WAE Device

Procedure

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

Step 2 Choose **Configure** > **Security** > **Secure Store**.

Step 3 Check the **Change CMS Secure Store** check box and then click **Submit**.

A new encryption key is generated in the Cisco WAAS Central Manager. The Cisco WAAS Central Manager replaces the encryption key in the WAE with the new key. The WAE re-encrypts the stored data using the new encryption key.

Note There may be a delay of a few minutes after you click **Submit** before the changes take effect.

Step 4 To use the Cisco WAAS CLI to configure the Secure Store encryption key, run the **cms secure-store change** EXEC command.

Resetting Secure Store Encryption on a Cisco WAAS Central Manager

Before you begin

You can reset the Secure Store if you reload the Cisco WAAS Central Manager and you cannot open the Secure Store because it is configured in user-provided passphrase mode and you forget the Secure Store password. This procedure deletes all encrypted data, certificate and key files, and key manager keys. The Secure Store is reinitialized, configured in auto-generated passphrase mode, and opened.

Procedure

Step 1 To reset Secure Store encryption, at the primary Cisco WAAS Central Manager CLI, enter the **cms secure-store reset** EXEC command.

Step 2 Wait until the standby Cisco WAAS Central Manager replicates the data from the primary Central Manager.

The replication should occur in 60 seconds (default) or as configured for your system.

Step 3 If Secure Store is in the **Initialized** and **Open** state, enter the **cms secure-store reset** EXEC command on the standby Cisco WAAS Central Manager.

Step 4 From the primary Cisco WAAS Central Manager, reset all user account passwords.

For information on resetting user passwords, see the chapter "Creating and Managing Administrative User Accounts and Groups."

Step 5 On each Cisco WAE registered to the Cisco WAAS Central Manager, follow these steps:

a) If Secure Store is initialized and open, from the Cisco WAAS Central Manager, clear Secure Store (see Disabling Secure Store Encryption on a Cisco WAE Device). Or, from the Cisco WAAS CLI, run the **cms secure-store clear** EXEC command.
b) From the Cisco WAAS Central Manager, initialize Secure Store (see Enabling Secure Store Encryption on a Cisco WAE Device) or from the Cisco WAAS CLI, run the **cms secure-store init** EXEC command. (This step is needed only if you performed Step 5a.)
c) Enter the **crypto pki managed-store initialize** EXEC command and restart the SSL accelerator.
d) If disk encryption is enabled, from the Cisco WAAS Central Manager, disable disk encryption from the Cisco WAAS CLI: run the **no disk encrypt enable** global configuration command.
e) If you enabled disk encryption before, in Step 5, reload the device. After the reload, re-enable disk encryption and reload the device again.

Note If the Cisco WAE is reloaded before doing Step 5: disk encryption, SSL acceleration, and Secure Store do not function properly. In this case, you must restore the Cisco WAE to factory defaults.

Step 6 From the primary Cisco WAAS Central Manager, re-import all certificate and key files for all the accelerated and peering services which are configured on the Cisco WAEs.

Disabling Secure Store Encryption on a Cisco WAE Device

Procedure

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

Step 2 Choose **Configure** > **Security** > **Secure Store**.

The **Secure Store Settings** window appears

Step 3 To disable Secure Store encryption and return to Standard encryption, check the **Clear CMS Secure Store** box and then click **Submit**.

To disable Secure Store encryption and return to Standard encryption, you can also run the **cms secure-store clear** command.

Consider the following guidelines when you disable Secure Store in the Cisco WAAS Central Manager or by running the **cms secure-store clear** EXEC command:

- There may be a delay of a few minutes for the changes to take effect, after you either click **Submit** in the **Secure Store Settings** window, or run the **cms secure-store clear** EXEC command in the Cisco WAAS CLI.
- If a Windows Domain User account identity has been configured on the device or the device group for encrypted MAPI acceleration, you will not be able to clear the Secure Store on the device. You must remove the Microsoft Windows domain user account identity configuration from the device or device group before you can clear Secure Store.
- You cannot clear Secure Store on a device that contains an encrypted services user account domain identity. For more information on user account domain identities, see Configuring Encrypted MAPI Acceleration in the chapter "Configuring Application Acceleration."
- To disable Secure Store on a Cisco WAE from the Cisco WAAS CLI, run the **cms secure-store clear** EXEC command.
- Secure store cannot be disabled on a Cisco WAAS Central Manager.

Modifying Default System Properties

This section contains the following topics:

About Default System Properties

The Cisco WAAS software comes with default, preconfigured system properties that you can modify to alter the default behavior of the system.

The following list describes the default system properties that you can modify:

- **cdm.remoteuser.deletionDaysLimit**

Maximum number of days since their last login after which external users will be deleted from the Cisco WAAS Central Manager database.

For example, if **cdm.remoteuser.deletionDaysLimit** is set to **5**, external users will be deleted from the database if the difference between their last login time and the current time is more than 5 days. The default is 60 days.

External users are users that are defined in an external AAA server and not in the Cisco WAAS Central Manager. Any reports scheduled by such users are also deleted when the users are deleted.

- **cdm.session.timeout**

  Timeout in minutes of a Cisco WAAS Central Manager GUI session. The default is **10 minutes**. If the session is idle for this length of time, the user is automatically logged out.

- **DeviceGroup.overlap**

  Status of whether a device can belong to more than one device group. The default is **true** (devices can belong to more than one device group).

- **System.clusterStatus.collectRate**

  The rate (in seconds) at which AppNav Controller collects and sends **Cluster Status** to the Cisco WAAS Central Manager from the AppNav IOM. The default is **30 seconds**.

- **System.datafeed.pollRate**

  Poll rate between a Cisco WAAS (or Cisco WAAS Express) device and the Cisco WAAS Central Manager (in seconds). The default is **300 seconds**.

- **System.device.recovery.key**

  Device identity recovery key. This property enables a device to be replaced by another node in the Cisco WAAS network.

- **System.guiserver.fqdn**

  Scheme to use (IP address or FQDN) to launch the Device Manager GUI.

- **System.healthmonitor.collectRate**

  Collect and send rate in seconds for the CMS device health (or status) monitor. If the rate is set to **0**, the health monitor is disabled. The default is **120 seconds**.

- **System.IOS.clusterStatus.collectRate**

  Rate (in seconds) at which the Cisco WAAS Central Manager collects **Cluster Status** data from Cisco IOS Routers.

- **System.IOS.clusterTopologyView.collectRate**

  Rate (in seconds) at which the Cisco WAAS Central Manager collects **Cluster Status** data from Cisco IOS Routers for **Cluster Topology** view.

- **System.lcm.enable**

  Controls propagation of device CLI configuration changes back to the Cisco WAAS Central Manager. If disabled, configuration changes done in device's CLI will not be communicated to the Cisco WAAS Central Manager. This setting is system wide and applies to all managed Cisco WAAS devices. Note that disabling this setting may result in Cisco WAAS Central Manager and Cisco WAAS device(s) configuration to go out of sync.

To customize this setting for a specific device, choose the **Device** > **Admin** > **Config Synchronization UI** page.

- **System.pcm.enable**

  Controls whether Cisco WAAS devices accept or ignore configuration changes received from the Cisco WAAS Central Manager. It could be used in deployments where Cisco WAAS devices are not managed by the Cisco WAAS Central Manager but other entity (i.e., directly via CLI). Note that disabling this setting may result in Cisco WAAS Central Manager and Cisco WAAS device(s) configuration to go out of sync.

  To customize this setting for a specific device, choose the **Device** > **Admin** > **Config Synchronization UI** page.

- **System.monitoring.collectRate**

  Rate at which a Cisco WAE collects and sends the monitoring report to the Cisco WAAS Central Manager (in seconds). For a Cisco WAAS Express device, this is the rate at which the Cisco WAAS Central Manager collects the monitoring data from the Cisco WAAS Express device. The default is **300 seconds** (**5 minutes**). Reducing this interval impacts the performance of the Cisco WAAS Central Manager.

- **System.monitoring.dailyConsolidationHour**

  Hour at which the Cisco WAAS Central Manager consolidates hourly and daily monitoring records. The default is **1** (**1:00 a.m.**).

- **System.monitoring.enable**

  Cisco WAAS and Cisco WAAS Express statistics monitoring (enable or disable). The default is **true**.

- **System.monitoring.maxConsecutiveRpcErrorWaitCount**

  Maximum number of RPC failures after which statistics from Cisco WAE to Cisco WAAS Central Manager will not be transmitted.

- **System.monitoring.maxDevicePerLocation**

  Maximum number of devices for which monitoring is supported in location level reports. The default is **25**.

- **System.monitoring.maxReports**

- Maximum number of completed or failed report instances to store for each custom report. The default is **10** report instances.

- **System.monitoring.monthlyConsolidationFrequency**

  How often (in days) the Cisco WAAS Central Manager consolidates daily monitoring records into monthly records. If this setting is set to **1**, the Cisco WAAS Central Manager checks if consolidation needs to occur every day, but only performs consolidation if there is enough data for consolidation to occur. The default is **14 days**.

  When a monthly data record is created, the corresponding daily records are removed from the database. Consolidation occurs only if there is at least two calendar months of data plus the consolidation frequency days of data. This ensures that the Cisco WAAS Central Manager always maintains daily data records for the past month and can display data on a day level granularity for the last week.

  For example, if data collection starts on February 2nd, 2018 and **System.monitoring.monthlyConsolidationFrequency** is set to 14, then the Cisco WAAS Central Manager checks if there is data for the past two calendar months on the following days: Feb 16th, March

2nd, March 16th, and March 30th. No consolidation will occur because there is not enough data on these days.

On April 13th, however, two calendar months of data exists. The Cisco WAAS Central Manager then consolidates data for the month of February and deletes the daily data records for that month.

- **System.monitoring.recordLimitDays**

  Maximum number of days of monitoring data to maintain in the system. The default is **1825 days**.

- **System.monitoring.timeFrameSettings**

  Default time frame to be used for plotting all the charts. Settings saved by the user will not be changed. The default is **Last Hour**.

- **System.registration.autoActivation**

  Status of the automatic activation feature, which automatically activates Cisco WAAS and Cisco WAAS Express devices that are registered to the Cisco WAAS Central Manager. The default is **true** (devices are automatically registered).

- **System.rpc.timeout.syncGuiOperation**

  Timeout in seconds for the GUI synchronization operations for the Central Manager to WAE connection. The default is **50 seconds**.

- **System.security.maxSimultaneousLogins**

  Maximum number of concurrent Cisco WAAS Central Manager sessions permitted for a user. Specify **0** (**zero**, the default) for unlimited concurrent sessions. A user must log off the Cisco WAAS Central Manager to end a session. If a user closes the browser without logging off, the session is not closed until after it times out after **120 minutes** (the timeout is not configurable). If the number of concurrent sessions permitted also is exceeded for that user, there is no way for that user to regain access to the Cisco WAAS Central Manager GUI until after the timeout expires. This setting does not affect CLI access to the Cisco WAAS Central Manager device.

- **System.security.webApplicationFilter**

  Status of the web application filter, which rejects any javascript, SQL, or restricted special characters in input. The default is **false**.

- **System.standby.replication.maxCount**

  Maximum number of statistics data records (in thousands) that will be replicated to a Standby Cisco WAAS Central Manager. The range is **10 to 300**. The default is **200** (**200,000 records**). We do not recommend increasing this number.

- **System.standby.replicationTimeout**

  Maximum number of seconds to wait for replication to a Standby Cisco WAAS Central Manager. The range is **300 to 3600 seconds**. The default is **900 seconds**. We do not recommend decreasing this timeout.

- **System.WcmIosUser.enable**

  Enables creation of Cisco WAAS Central Manager user on the registered IOS device. Global, device level, device group level IOS Router credential pages will be hidden if this system property is enabled.

- System.clearedAlarm.purging.interval

Enables configuration of time interval for retaining alarm records. The default is **7 days** but can be configured for **365 days**.

Modifying a Default System Property

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure > Global > System Properties**. The **Config Properties** window appears.

Step 2 Click the **Edit** icon next to the system property that you want to change. The **Modifying Config Property** window appears.

Step 3 From a drop-down list, enter a new value or choose a new parameter, depending on the system property that you want to change.

Step 4 To save the settings, click **Submit**.

Configuring the Web Application Filter

This section contains the following topics:

Enabling the Web Application Filter

Before you begin

Web Application Filter is a security feature that protects the Cisco WAAS Central Manager GUI against Cross-Site Scripting (XSS) attacks. XSS security issues can occur when an application sends data that originates from a user to a web browser without first validating or encoding the content, which can allow malicious scripting to be executed in the client browser, potentially compromising database integrity.

This security feature verifies that all application parameters sent from Cisco WAAS users are validated and/or encoded before populating any HTML pages.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure > Global > System Properties**. The **Config Properties** window appears.

Note You cannot enable the **Web Application Filter** using the Cisco WAAS CLI. This feature is disabled by default.

Step 2 Click the **Edit** icon next to the **system.security.webApplicationFilter** entry.

The **Modifying Config Property** window appears.

Step 3 To enable the **Web Application Filter**, from the **Value** drop-down list, choose **True**.

A confirmation message appears to advise Cisco WAAS Central Manager users to log out and then back in after enabling this feature.

Step 4 Click **OK** and then click **Submit**.

Step 5 Log out and then back in again.

Web Application Filter Security Verification

The Web Application Filter verifies security using two methods, input verification and sanitization. Input validation validates all input data before accepting data. Sanitization prevents malicious configuration and scripts already present in the data from getting executed.

- **Web Application Filter Input Validation**: Scans all data that is input to the Cisco WAAS Central Manager database. It is only configurable by the **admin** user.

  Any input submitted using the Cisco WAAS Central Manager GUI that is suspicious of XSS is blocked. Blocked input results in a warning.

  Input data is checked against the following XSS filter rules:

  - Input is rejected if it contains a semicolon (;)
  - Input is rejected if it is enclosed in angle brackets (<>)
  - Input is rejected if it can be indirectly used to generate the above tags (&#60, &#62, %3c, %3e)

- **Web Application Filter sanitizer**: Prevents malicious configuration and scripts from getting executed in the browser when there is an XSS attack on the database. Sanitization is not configurable by the user.

  Configuration data coming from the Cisco WAAS Central Manager that is suspect for XSS is shown in red on the **Device Groups** > **All Device Groups** window.

Configuring Faster Detection of Offline Cisco WAAS Devices

This section contains the following topics:

About Faster Detection of Offline Cisco WAAS Devices

Communication between the Cisco WAAS device and Cisco WAAS Central Manager using User Datagram Protocol (UDP) allows faster detection of devices that have gone offline.

- UDP heartbeat packets are sent at a specified interval from each device to the primary Cisco WAAS Central Manager in a Cisco WAAS network.
  - The primary Cisco WAAS Central Manager tracks the last time that it received a UDP heartbeat packet from each device. If the Cisco WAAS Central Manager has not received the specified number of UDP packets, it displays the status of the nonresponsive devices as **offline**.
  - Because UDP heartbeats require less processing than a **getUpdate** request, they can be transmitted more frequently, and the Cisco WAAS Central Manager can detect offline devices much faster.

- You can enable or disable the UDP feature, specify the interval between two UDP packets, and configure the failed heartbeat count.
    - The default for the UDP feature is disabled.
    - Heartbeat packet rate is defined as the interval between two UDP packets. Using the specified heartbeat packet rate and failed heartbeat count values, the Cisco WAAS Central Manager GUI displays the resulting offline detection time as a product of heartbeat rate and failed heartbeat count.
    - If you enable the fast detection of offline devices, the Cisco WAAS Central Manager detects devices that are in network segments that do not support UDP and uses **getUpdate** (get configuration poll) request to detect offline devices.

Procedure for Configuring Faster Detection of Offline Cisco WAAS Devices

Before you begin

You can detect offline Cisco WAAS devices more quickly if you enable the fast detection of offline devices. A Cisco WAAS device is declared as offline when it has failed to contact the Cisco WAAS Central Manager for a getUpdate (get configuration poll) request for at least two polling periods.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **Global** > **Fast Device Offline Detection**.

The **Configure Fast Offline Detection** window appears.

Note The fast detection of offline devices feature is in effect only when the Cisco WAAS Central Manager receives the first UDP heartbeat packet and a **getUpdate** request from a device.

Step 2 To enable the Cisco WAAS Central Manager to detect the offline status of devices quickly, check the **Enable Fast Offline Detection** check box.

Step 3 In the **Heartbeat Rate** field, specify how often devices should transmit a UDP heartbeat packet to the Cisco WAAS Central Manager, in seconds. The default is **30 seconds**.

Step 4 In the **Heartbeat Fail Count** field, specify the number of UDP heartbeat packets that can be dropped during transmission from devices to the Cisco WAAS Central Manager before a device is declared offline. The default is **1 UDP heartbeat packet**.

Step 5 In the **Heartbeat UDP Port** field, specify the port number using which devices will send UDP heartbeat packets to the primary Cisco WAAS Central Manager. The default is **port 2000**.

The **Maximum Offline Detection Time** field displays the product of the failed heartbeat count and heartbeat rate.

Maximum Offline Detection Time = Failed heartbeat count * Heartbeat rate

If you have not enabled the fast detection of offline devices feature, then the Cisco WAAS Central Manager waits for at least two polling periods to be contacted by the device for a **getUpdate** request before declaring the device to be offline. However, if you enable the fast detection of offline devices feature, then the Cisco WAAS Central Manager waits until the value displayed in the **Maximum Offline Detection Time** field is exceeded.

If the Cisco WAAS Central Manager receives the Cisco Discovery Protocol (CDP) from a device, then the Cisco WAAS Central Manager GUI displays the device as offline after a time period of 2* (heartbeat rate) * (failed heartbeat count).

Step 6 Click **Submit**.

Note Any changes to the **Configure Fast WAE Offline Detection** window in the Cisco WAAS Central Manager could result in devices temporarily appearing to be offline. After the configuration changes are propagated to the devices, they again show as **online**.

Configuring Alarm Overload Detection

This section contains the following topics:

About Alarm Overload Detection

Cisco WAAS devices can track the rate of incoming alarms from the Node Health Manager. If the rate of incoming alarms exceeds the high-water mark (HWM), then the WAAS device enters an alarm overload state. This situation occurs when multiple applications raise alarms at the same time to report error conditions. When a Cisco WAAS device is in an alarm overload state, the following occurs:

- SNMP traps for subsequent alarm raise and clear operations are suspended. The trap for the raise alarm-overload alarm and the clear alarm-overload alarm are sent; however, traps related to alarm operations between the raise alarm-overload alarm and the clear alarm-overload alarm operations are suspended.
- Alarm overload raise and clear notifications are not blocked. The alarm overload state is communicated to SNMP and the Configuration Management System (CMS). However, in the alarm overload state, SNMP and the CMS are not notified of individual alarms. The information is only available by using the Cisco WAAS CLI.
- The Cisco WAAS device remains in an alarm overload state until the rate of incoming alarms decreases to the point that the alarm rate is less than the low-water mark (LWM).
- If the incoming alarm rate falls below the LWM, the Cisco WAAS device comes out of the alarm overload state and begins to report the alarm counts to SNMP and the CMS.

When the Cisco WAAS device is in an alarm overload state, the Node Health Manager continues to record the alarms being raised on the Cisco WAAS device and keeps a track of the incoming alarm rate. Alarms that have been raised on a Cisco WAAS device can be listed using the **show alarm** EXEC commands that are described in the **restore factory-default** EXEC command. For more information, see the *Cisco Wide Area Application Services Command Reference*.

Procedure for Configuring Alarm Overload Detection

Procedure

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

Step 2 Choose **Configure** > **Monitoring** > **Alarm Overload Detection**.

The **Alarm Overload Detection Settings** window appears.

Step 3 Uncheck the **Enable Alarm Overload Detection** check box if you do not want to configure the WAAS device (or device group) to suspend alarm raise and clear operations when multiple applications report error conditions. This check box is checked by default.

Step 4 In the **Alarm Overload Low Water Mark (Clear)** field, enter the number of incoming alarms per second below which the WAAS device comes out of the alarm overload state.

The low-water mark is the level up to which the number of alarms must drop before alarms can be restarted. The default value is **1**. The low-water mark value should be less than the high-water mark value.

Step 5 In the **Alarm Overload High Water Mark (Raise)** field, enter the number of incoming alarms per second above which the Cisco WAAS device enters the alarm overload state. The default value is **10**.

Step 6 To save the settings, click **Submit**.

Step 7 To configure alarm overload detection from the Cisco WAAS CLI, run the **alarm overload-detect** global configuration command.

Configuring the Email Notification Server

Before you begin

Consider the following guidelines for configuring the email notification server:

- You can schedule reports to be generated periodically, and when they are generated, a link to the report can be emailed to one or more recipients. (For more information, see Managing Reports in the chapter "Monitoring Your Cisco WAAS Network.")
- The **Enable Notification for Cleared Alarms** generates emails for cleared alarms *only if* you have cleared alarms after more than 24 hours of system time. If you clear alarms at 24 hours or less of system time, emails are not triggered for cleared alarms.
- The **Enable Notification for Raised Alarms** generates emails for raised alarms independent of when alarms are cleared.

Procedure

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

Step 2 Choose **Configure > Monitoring > Email Notification**.

The **Configure Email Server Details** window appears.

Step 3 In the **Mail Server Hostname** field, enter the hostname of the SMTP emmail server that is to be used to send email.

Note Only SMTP mail servers are supported. If any other type of mail server is configured, the email notification fails.

Step 4 In the **Mail Server Port** field, enter the port number. The default is **port 25**.

Step 5 In the **Server Username** field, enter a valid email account username.

Step 6 In the **Server Password** field, enter the password for the email account.

Step 7 In the **From Address** field, enter the email address shown as the sender of the email notification.

Step 8 Click **Submit**.

Using IPMI over LAN

This section contains the following topics:

About IPMI over LAN

Intelligent Platform Management Interface (IPMI) over LAN provides remote platform management service for Cisco WAVE-294, WAVE-594, WAVE-694, WAVE-7541, WAVE-7571, and WAVE-8541 appliances. IPMI is an open standard technology that defines how administrators monitor system hardware and sensors, control system components, and retrieve logs of important system events to conduct remote management and recovery.

IPMI runs on the Baseboard Management Controller (BMC) and operates independently of Cisco WAAS. After IPMI over LAN is set up and enabled on Cisco WAAS, authorized users can access BMC remotely even when Cisco WAAS becomes unresponsive or the device is powered down but connected to a power source. You can use an IPMI v2 compliant management utility, such as ipmitool or OSA SMbridge, to connect to the BMC remotely to perform IPMI operations.

The IPMI over LAN feature provides the following remote platform management services:

- Supports the power on, power off, and power cycle of the Cisco WAAS appliance.
- Monitors the health of the Cisco WAAS hardware components by examining Field Replaceable Unit (FRU) information and reading sensor values.
- Retrieves logs of important system events to conduct remote management and recovery.
- Provides serial console access to the Cisco WAAS appliance over the IPMI session.
- Support for IPMI Serial over LAN (SoL): IPMI SoL enables a remote user to access a Cisco WAAS appliance through a serial console through an IPMI session.

IPMI over LAN and IPMI SoL features can be configured using Cisco WAAS CLI commands and include the following:

- Configuring IPMI LAN interface

- Configuring IPMI LAN users
- Configuring security settings for remote IPMI access
- Enabling/disabling IPMI over LAN
- Enabling/disabling IPMI SoL
- Restoring the default settings for the BMC LAN channel
- Displaying the current IPMI over LAN and IPMI SoL configurations

For more information on configuring IPMI over LAN, see Configuring BMC for Remote Platform Management.

BMC Firmware Update for IPMI over LAN

IPMI over LAN requires that a specific BMC firmware version be installed on the device. The minimum supported BMC firmware versions are:

- Cisco WAVE-294, Cisco WAVE-594, or Cisco WAVE-694: **49**
- Cisco WAVE-7541, Cisco WAVE-7571, or Cisco WAVE-8541: **26a**

Cisco WAAS appliances shipped from the factory with Cisco WAAS Version 4.4.5 or later do have the correct firmware installed. If you are updating a device that was shipped with an earlier version of Cisco WAAS software, you must update the BMC firmware, unless it was updated previously.

To determine if you are running the correct firmware version, run the show bmc info EXEC command. The following example displays the latest BMC firmware version installed on the device (Version 49 in the following example):

```
wave# show bmc info
Device ID : 32
Device Revision : 1
Firmware Revision : 0.49 <<<<< version 49
IPMI Version : 2.0
Manufacturer ID : 5771
Manufacturer Name : Unknown (0x168B)
Product ID : 160 (0x00a0)
Product Name : Unknown (0xA0)
Device Available : yes
Provides Device SDRs : no
Additional Device Support :
Sensor Device
SDR Repository Device
SEL Device
FRU Inventory Device
Aux Firmware Rev Info :
0x0b
0x0c
0x08
0x0a <<<<< a
.
.
.
```

If a BMC firmware update is needed, you can download it from **cisco.com** at the Cisco Wide Area Application Service (Cisco WAAS) Software download page (registered customers only). The firmware binary image is named **waas-bmc-installer-49a-49a-27a-k9.bin**, or a newer version may be available. Use the latest firmware update that is available.

Run the following command to update the firmware from the image file that is available through FTP on your network:

copy ftp install *ip-address remotefiledir* **waas-bmc-installer-49a-49a-27a-k9.bin**

The update process automatically checks the health status of the BMC firmware. If BMC firmware corruption is detected, BMC is recovered during the BMC firmware update procedure. The complete update process can take several minutes and the device may appear unresponsive but do not interrupt the process or power cycle the device. After the update is complete, you must reload the device.

After the device reboots, you can verify the firmware version by running the **show bmc info** EXEC command.

BMC recovery and BMC firmware update restores the factory defaults on the BMC and all the current IPMI over LAN configurations are erased.

If BMC firmware corruption occurs, a critical alarm is raised.

Configuring BMC for Remote Platform Management

This section contains the following topics:

Enabling IPMI Over LAN

Procedure

Step 1 To enable IPMI over LAN, perform the following steps when running the **bmc lan** command.

Step 2 Change the default BMC LAN IP address.

Step 3 Change the password for the BMC default user, which is **User 2**.

Step 4 Enable IPMI over LAN.

Step 5 Access the BMC from a remote client over IPMI session v2.0 using the username and password for the **number 2 user**. The default cipher suite used to access the BMC is **3**, which specifies RAKP-HMAC-SHA1 authentication, HMAC-SHA1-96 integrity, and AES-CBC-128 encryption algorithms.

Step 6 To access the BMC over a IPMI session v1.5, change the **User 2** IPMI-session-version setting from v2.0 to **v1.5**.

Enabling IPMI SoL

Procedure

Step 1 On the Cisco WAAS device, configure and enable IPMI over Lan (IoL).

Step 2 On the remote client, make sure that the BMC user can do IoL operations successfully over IPMI session v2.0.

Step 3 On the remote client, change the baud-rate of the terminal to match the Cisco WAAS console baud rate of 9600 bps.

Step 4 On the Cisco WAAS device, enable IPMI SoL.

Step 5 On the remote client, if the IPMI management tool is ipmitool, check the SoL payload status of the specific BMC user with the following command:

ipmitool -I lanplus -H *bmc-ip-address -U bmc-user-name* **sol payload status 1** *bmc-user-userid*

For example:

```
# ipmitool -I lanplus -H 2.1.4.70 -U user3 sol payload status 1 3
Password:
User 3 on channel 1 is disabled
```

Step 6 If the SoL payload is disabled for this user, enable the SoL payload for this user with the following command:

ipmitool -I lanplus -H *bmc-ip-address* **-U** *bmc-user-name* **sol payload enable 1** *bmc-user-userid*

For example:

```
# ipmitool -I lanplus -H 2.1.4.70 -U user3 sol payload enable 1 3
Password:
# ipmitool -I lanplus -H 2.1.4.70 -U user3 sol payload status 1 3
Password:
User 3 on channel 1 is enabled
```

Step 7 On the remote client, use the following command to open the serial console to the Cisco WAAS device:

ipmitool -I lanplus -H *bmc-ip-address* **-U** *bmc-user-name* **sol activate**

Step 8 On the remote client, you have now entered the console session of the Cisco WAAS device. When you are done, use the ~. escape character to terminate the connection.

Managing Cisco IOS Router Devices

This section contains the following topics:

About Managing Cisco IOS Router Devices

You can use the Cisco WAAS Central Manager to manage Cisco WAAS Express and AppNav-XE devices, which are both Cisco IOS routers deployed with Cisco WAAS related software. The Cisco Central Manager menu displays a subset of the full menu when a Cisco WAAS Express or Cisco AppNav-XE is selected as the context, as these devices implement a subset of WAAS appliance functionality.

The Cisco WAAS Central Manager and a Cisco IOS device communicate using the HTTPS protocol. To establish communication between a Cisco WAAS Central Manager and a Cisco IOS router device, you must register the Cisco IOS router device with the Cisco WAAS Central Manager. Using the Cisco WAAS Central Manager GUI to register a Cisco IOS router device is the easiest method.

Registering a Cisco IOS Router Device Using the Central Manager GUI

Before you begin

Before you register a router with the Cisco WAAS Central Manager, remove all banner configurations (with keywords such as username, password, hostname), because these banner configurations interfere with the registration process, and will generate errors.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **Registration** > **Cisco IOS Routers**.

The **Cisco IOS Router Registration** window appears.

Note To register a Cisco IOS router device using the Central Manager GUI, SSH v1 or v2 must be enabled on the router.

Step 2 Select the type of IP address (IPv4 or IPv6) that the Router will use. The IPv6 option is available only when the Cisco WAAS Central Manager is configured with a valid IPv6 address.

Step 3 In the **IP Address(es)** field, enter the router IP addresses to register, separated by commas. The IP address, hostname, router type, and status are displayed in the **Registration Status** table.

Note Although a Cisco IOS router can have a dot (".") in the hostname, this special character is not allowed in a Cisco WAAS device hostname. If you try to import an AppNav-XE device that has a dot in the hostname, the import will fail and the following error message is displayed: **Registration failed for the device devicename ConstraintException; Invalid AppNav-XE name: X.X since name includes invalid character ".".**

You can also upload a CSV file that contains a list of IP addresses to register. To upload a list, click the **Import CSV file** radio button and then click **Choose File** to browse to the file, and then click **Open**. Each IP address must be on a separate line.

Step 4 Configure the router login credentials by entering the username and password. If you need to create a user on the router, see Registering a Cisco IOS Router Using the CLI, on page 332.

Step 5 Choose the **HTTP Authentication Type**, **local** or **AAA**.

Note Be sure to choose the HTTP authentication type that is currently configured on the router. If you choose an HTTP authentication type that differs from your current configuration, your existing configuration on the router will be overwritten and you may not be able to use HTTP to communicate with the router. Communications with routers with previously established authentication credentials will fail.

Step 6 In the **Central Manager IP Address** field, enter the IP address you want the router to use for the Cisco WAAS Central Manager. This field is initially filled in with the current Central Manager IP address, but you may need to change this in a NAT environment.

Step 7 Click the **Register** button and verify that the registration status was successful.

You can view the results in the log file: **/local/local1/errlog/waasx-audit.log**.

After you successfully register a Cisco IOS router device, the Cisco WAAS Central Manager displays it in the **Registration Status** table and in the **All Devices** list.

If you need to register additional devices, use the **Reset** button to clear data from all the fields, to enter the next configuration.

Step 8 You may need to install a software license on the Cisco IOS router device. For more information, see Registering a Cisco IOS Router Using the CLI, on page 332.

Configuring Cisco IOS Router Credentials

Before you begin

- For the Cisco WAAS Central Manager to access a Cisco IOS router device, you must configure the router credentials in the Cisco WAAS Central Manager.
- On the Cisco WAAS Central Manager, you can define global credentials that apply to all Cisco IOS router devices, or you can define credentials at the device group or individual device level by using the **Admin** > **Authentication** > **WAAS Express Credentials/AppNav-XE Credentials** menu item. To configure device group or individual device credentials, you must first complete the Cisco IOS router registration process and then configure credentials for a router device group or device. Device and device group credentials have precedence over global credentials.

This procedure describes how to configure global router credentials (**Step 1**) and how to configure router credentials at the device group or individual device level (**Step 2**). To configure router credentials, follow these steps:

Procedure

Step 1 **Configure global router credentials**:

a) From the Cisco WAAS Central Manager menu, choose **Admin** > **Security** > **Cisco IOS Router Global Credentials**.

   The **Cisco IOS Router Global Credential**s window appears.

b) In the **Username** field, enter a username that is defined on the Cisco IOS router. If you need to create a user on the router, see Registering a Cisco IOS Router Using the CLI, on page 332.

   Note The **Username** field is optional if you are not using **local** or **AAA** authentication for the HTTP server on the Cisco IOS router device; that is, if you use the default HTTP server configuration of the **ip http authentication enable** global configuration command. (For more information, see Registering a Cisco IOS Router Using the CLI, on page 332.)

c) In the **Password** field, enter the password for the specified username.

d) Click **Submit**.

Step 2 **Configure credentials at the device group or individual device level**:

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

   The **Device** or **Device Group** window appears.

b) Choose the **Admin** > **Authentication** > **WAAS Express Credentials/AppNav-XE Credentials** menu item.

c) In the **Username** field, enter a username that is defined on the Cisco IOS router. If you need to create a user on the router, seeRegistering a Cisco IOS Router Using the CLI, on page 332 .

   Note The Username field is optional if you are not using **local** or **AAA** authentication for the HTTP server on the Cisco IOS router device; that is, if you use the default HTTP server configuration of the **ip http authentication enable** global configuration command. (For more information, see Registering a Cisco IOS Router Using the CLI, on page 332.)

d) In the **Password** field, enter the password for the specified username.

e) Click **Submit**.

Note Changing the router credentials on the Cisco WAAS Central Manager does not change the configuration on the router device itself. It affects only the router credentials that are stored on the Cisco WAAS Central Manager.

Registering a Cisco IOS Router Using the CLI

Before you begin

Table 31: Checklist for Registering a Cisco IOS Router Using the CLI provides a checklist for using the CLI to register a Cisco IOS Router.

Table 31: Checklist for Registering a Cisco IOS Router Using the CLI

Step	Step Title	Description
1	Configure a username and password.	The same username and password are configured on the router and the Cisco WAAS Central Manager, so the Cisco WAAS Central Manager can log in to the router for management purposes.
2	Import the primary Central Manager administrative server certificate into the router.	The router requires the Cisco WAAS Central Manager certificate for secure HTTPS server communication.
3	Configure a Cisco IOS router certificate.	The Cisco WAAS Central Manager device requests this router certificate for secure HTTPS server communication.
4	Enable the secure HTTP server with user authentication.	Enables the Cisco WAAS Central Manager and router to communicate.
5	Install a permanent WAAS software license.	Allows the Cisco WAAS software to operate on the router.
6	Configure an NTP server.	Keeps the time synchronized between the router and the Cisco WAAS Central Manager.
7	Register the router with the Cisco WAAS Central Manager.	Registers the router with the Cisco WAAS Central Manager.

Procedure

Step 1 **Configure a user**.

The first step in setting up your router and Cisco WAAS Central Manager to communicate is to configure the same user on the router and the Cisco WAAS Central Manager.

a) Log in to the router Cisco WAAS CLI.

b) Configure a local user with **privilege level 15** on the router by using the username IOS configuration command:

```
router# config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# username cisco privilege 15 password 0 cisco
router(config)# exit
```

c) Alternatively, you can configure an external TACACS+ or RADIUS user.

Note The external authentication server for TACACS+ or RADIUS must be Cisco ACS 4.x or 5.x.

To configure an external **TACACS+ user** on the router, run the following configuration commands on the router:

```
router# config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# aaa new-model
router(config)# aaa authentication login default group tacacs+
router(config)# aaa authorization exec default group tacacs+
router(config)# tacacs-server host host-ip
router(config)# tacacs-server key keyword
```

To configure an external **RADIUS user** on the router, run the following configuration commands on the router:

```
router# config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# aaa new-model
router(config)# aaa authentication login default group radius
router(config)# aaa authorization exec default group radius
router(config)# radius-server host host-ip
router(config)# radius-server key keyword
```

Step 2 **Import the certificate from the Cisco WAAS Central Manager into the router**.

a) Log in to the Cisco WAAS Central Manager CLI.

b) To display the administrative certificate, run the **show crypto** EXEC command:

```
waas-cm# show crypto certificate-detail admin

...
-----BEGIN CERTIFICATE-----
TIICezCCAeSgAwIBAgIEVwMK8zANBgkqhkiG9w0BAQUFADCBgTELMAkGA1UEBhMC
VVMxEzARBgNVBAgTCkNhbGlmb3JuaWExETAPBgNVBAcTCFNhbiBKb3NlMQ0wCwYD
VQQLEwRDTkJVMRswGQYDVQQKExJDaXNjbyBTeXN0ZW1zLCBJbmMxHjAcBgNVBAMT
FWRvYy13YWFzLWNtLmNpc2NvLmNvbTAeFw0wODA3MjQxOTMwMjNaFw0xMzA3MjMx
OTMwMjNaMIGBMQswCQYDVQQGEwJVUzETMBEGA1UECBMKQ2FsaWZvcm5pYTERMA8G
A1UEBxMIU2FuIEpvc2UxDTALBgNVBAsTBENOQlUxGzAZBgNVBAoTEkNpc2NvIFN5
c3RlbXMsIEluYzEeMBwGA1UEAxMVZG9jLXdhYXMtY20uY2lzY28uY29tMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQCy10xBfsUDTh5imYwkkterx/IqkNQO7KB/
M0wqIK2j4zj4BpR1ztKaFyEtGjqGpxPBQ54V9EHGmGUljx/Um9PORk3AXyWoUsDf
o0T2Z94FL5UoVUGzUia6/xiUrPCLNf6BLBDGPQg970QtZSU+DYUqjYHzDgv6yXFt
viHARbhZdQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBADKF7aIeQ+Uh4Y2zZJwlaIF7
ON+RqDvtyy4DNerEN9iLI4EFO/QJ+uhChZZU8AKR8u3OnLPSNtNck33OWwMemcOd
QGhnsMtiUq2VuSh+A3Udm+sMLFguCw5RmJvqKTrj3ngAsmDBW3uaK0wkPGp+y3+0
2hUYMf+mCrCOwBEPfs/M
-----END CERTIFICATE-----
```

c) Copy the certificate text, which is the part in between the **BEGIN CERTIFICATE** and **END CERTIFICATE** lines in the output.

d) Log in to the router CLI.

e) Configure a certificate for the Cisco WAAS Central Manager:

```
router# config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# crypto pki trustpoint wcm

router(ca-trustpoint)# enrollment terminal pem
router(ca-trustpoint)# exit
router(config)# crypto pki authenticate wcm

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
```

f) Paste in the certificate that you copied from the Cisco WAAS Central Manager in Step 2c.

Step 3 **Configure a Cisco IOS Router certificate**.

The router needs a certificate that is requested by the Cisco WAAS Central Manager when establishing HTTPS communication. This procedure describes how to configure a persistent self-signed certificate on the router, but you can also use a CA signed certificate.

a) Log in to the router CLI.

Note Due to **CSCsy03412**, you must configure **ip domain name** *name* before enrolling the certificate. If you do not configure **ip domain name**, Cisco IOS regenerates the self-signed certificate upon reload and this affects the communication with the Cisco WAAS Central Manager.

```
router# config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# crypto pki trustpoint local
router(ca-trustpoint)# enrollment selfsigned
router(ca-trustpoint)# subject-alt-name routerFQDN
router(ca-trustpoint)# exit
router(config)# crypto pki enroll local
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 10.10.10.25
Generate Self Signed Router Certificate? [yes/no]: yes

Router Self Signed Certificate successfully created
```

For a Cisco AppNav XE device, if the self-signed certificate is generated with key label as hostname and if you change the hostname through the Cisco WAAS Central Manager GUI or router CLI, then there is a SSL handshake failure and the device goes offline. This is because the existing certificate is a valid only with respect to the old host name and the certificate needs to be validated against the hostname with which it was generated.

- To prevent this handshake failure, whenever you change the hostname, you need to re-generate the certificate for that hostname and reimport it.
- If the router certificate changes after the router is registered with the Central Manager, you must reimport the certificate into the Central Manager. For more information, see Reimporting a Cisco Router Device Certificate.

Step 4 **Enable the the HTTP secure server on the router**.

The Cisco WAAS Central Manager and a router communicate using the HTTPS protocol. You must enable the HTTP secure server on the router.

a) On the router, enable the HTTP secure server:

```
router# config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# ip http secure-server
```

Note Be sure to choose the HTTP authentication type that is currently configured on the router. If you choose an HTTP authentication type that differs from your current configuration, your existing configuration on the router will be overwritten and you will not be able to use HTTP to communicate with the router.

b) To configure authentication for the HTTP server, use the following options.

- To configure authentication for the HTTP server for a local user, use the following command:

  ```
  router(config)# ip http authentication local
  ```

- If you are using external TACACS+ or RADIUS user authentication, configure authentication for the HTTP server with the following command:

  ```
  router(config)# ip http authentication aaa
  ```

Note If you do not configure local or AAA authentication for the HTTP server, only the **enable password** global configuration command is used for authentication. (The default is the **ip http authentication enable** global configuration command, which uses only the enable password and no username.) If this default configuration is used, it is not necessary to define a username credential for the router on the Cisco WAAS Central Manager.

Step 5 **Install a license on the router**.

The router requires one or more licenses to operate the Cisco WAAS Express or Cisco AppNav-XE software. Refer to the router documentation for details.

a) Obtain and copy the appropriate license to a location accessible to the license command on the router.

b) On the router, install the license:

```
router# license install ftp://infra/licenses/FHH122500AZ_20100811190225615.lic
```

This example uses FTP to get and install the license, but there are various options available for this command. Choose one that best suits your deployment.

c) Save the running configuration:

```
router# write memory
Building configuration...
[OK]
```

Step 6 Configure an NTP Server.

It is important to keep the time synchronized between devices in your Cisco WAAS network. You should already have an NTP server configured for the Cisco WAAS Central Manager. For more information. see Configuring NTP Settings.

To configure an NTP server for the router, on the router, run the **ntp server** global configuration command, as follows:

```
router# config t
Enter configuration commands, one per line. End with CNTL/Z.
router(config)# ntp server 10.10.10.55
```

Step 7 **Register a router with the Cisco WAAS Central Manager**.

The final step in setting up a router with the Cisco WAAS Central Manager is to register the device. You will need to know the IP address of the Cisco WAAS Central Manager.

a) For a Cisco WAAS Express router, register with the Cisco WAAS Central Manager as follows:

```
router# waas cm-register https://CM_IP_Address:8443/wcm/register
```

b) If you want to register the Cisco WAAS Express router with an IPv6 address, register it with the following commands:

```
router# waas cm-register https://[CM_IPv6_Address]:8443/wcm/register
```

c) For a Cisco AppNav-XE router, register with the Cisco WAAS Central Manager as follows:

```
router# appnav cm-register https://CM_IP_Address:8443/wcm/register
```

```
router# appnav cm-register https://[CM_IPV6_Address]:8443/wcm/register
```

In the URL for this command, specify the Cisco WAAS Central Manager IP address as indicated. Be sure to include a colon and the port number of **8443**.

If a permanent Cisco WAAS license is not installed on the router, you must accept the terms of the evaluation license to continue. The evaluation license is valid for **60 days**.

d) Save the running configuration:

```
router#write memory
Building configuration...
[OK]
```

After the successful registration of the router with the Cisco WAAS Central Manager, the Cisco WAAS Central Manager initially shows the device on the **Manage Devices** screen with a management status of **Pending** and a license status of **Active**.

After the Cisco WAAS Central Manager retrieves the device configuration and status, the management status changes to **Online** and the license status changes to **Permanent** (or **Evaluation**, Expires in x weeks y days).

Reimporting a Cisco Router Device Certificate

Before you begin

If the router device certificate changes after you have registered the router device with the Cisco WAAS Central Manager, you must reimport a matching certificate into the Cisco WAAS Central Manager.

Procedure

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

Step 2 Choose **Admin** > **Authentication** > **Identity Certificate**.

The **Certificate** window appears.

- The **Certificate Info** tab shows the certificate information for the device.

- The **Certificate in PEM Encoded Format** tab shows the certificate in Privacy-Enhanced Mail (PEM) format. You can copy the certificate from this tab to use in the paste operation in the next step.

Step 3 Import this certificate into the Cisco WAAS Central Manager by selecting one of the following radio buttons that are shown above the tabs:

- **Upload PEM file**: Click **Choose File** and locate the PEM file containing the certificate.
- **Manual**: Paste the PEM-encoded certificate in the text field that appears.

Step 4 Click **Submit**.

Creating a New Cisco WAAS Central Manager IOS User on Preregistered Cisco IOS Devices

Before you begin

Consider the following guidelines for creating a new Cisco WAAS Central Manager IOS user on preregistered Cisco IOS devices:

- A router that has already been registered with the Cisco WAAS Central Manager before the system property was enabled needs to be migrated to communicate with the Cisco WAAS Central Manager. To enable this communication, you need to create a new Cisco WAAS Central Manager IOS user so that the ongoing communication uses the same to communicate with the Cisco WAAS Central Manager.
- The **WAAS Express User Creation Tool** window is visible only when the **System.WcmIosUser.enable** is enabled on the **Home** > **Configure** > **System Properties** > **WcmIosUser** window.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Home** > **Admin** > **Security** > **WCM Cisco IOS User Creation Tool**.

The **WAAS Express User Creation Tool** window appears.

Step 2 Configure the router login credentials by entering the **username**, **password**, and **enable**.

Step 3 Select the Router IP address type: **IPv4** or **IPv6**.

Step 4 Select the Router IP Address entry method.

Step 5 In the **IP Address(es)** field, enter the Cisco WAAS Express router IP addresses to migrate, separated by commas. The IP address, hostname and status are displayed in the **Status** table.

You can also upload a CSV file that contains a list of IP addresses to migrate:

a) To upload a list, click the **Upload File** check box.
b) To browse to the file, click **Choose File**.
c) Click **Open**.

Each IP address must be on a separate line.

Step 6 To create a new Cisco WAAS Central Manager IOS user on the router, click **Update**.

- Verify that the user creation status was successful.
- If you want to migrate additional preregistered routers, use the **Reset** button to clear data from all the fields, to enter the next configuration.

Step 7 **Note** that if you create a Cisco IOS WCM user using the **Home** > **Admin** > **Security** > **WCM Cisco IOS User Creation Tool** by specifying the Cisco IOS username, password and enable:

a) You must manually log in to the Cisco IOS router.
b) Save the running configuration by running the **write memory** EXEC command.

Note If you do not save the running configuration and reload the device, the Cisco IOS router goes off line in the Cisco WAAS Central Manager.

Cisco WAAS, ISR-WAAS, and IOS-XE Interoperability

Consider the following operating guidelines for Cisco WAAS, Cisco ISR-WAAS, and Cisco IOS-XE interoperability:

- The following table shows interoperability for Cisco WAAS, Cisco ISR, and Cisco IOS-XE versions:

Table 32: Cisco WAAS, ISR and IOS-XE Interoperability

Cisco ISR- Platform	Cisco WAAS Version Supported	Cisco IOS-XE Version Supported
ISR-4321, ISR-4331, ISR-4351, ISR-4431, ISR-4451	6.4.3e	16.6.8, 16.9.5*, 16.12.03s
	6.4.3d	16.3.9, 16.6.7, 16.9.4*, 16.12.2, 17.1.1
	6.4.3c	16.3.8, 16.6.6, 16.9.3, 16.11.1, 16.11.2
	6.4.3b	16.3.8, 16.6.5, 16.6.6, 16.9.3, 16.11.1
	6.4.3a	16.9.2, 16.9.3
	6.4.3	3.16.4a, 3.16.7b, and 16.3.6, 16.3.7, 16.6.3, 16.6.4, 16.5.2, 16.8.1, 16.3.5, 16.6.2, 16.9.1

  - *****In the table column "Cisco IOS-XE Version Supported," the starred version is the recommended release version.
  - For interoperability information for Cisco WAAS versions earlier than 6.4.x, see the particular version of the Release Note for Cisco Wide Area Application Services.

- Cisco ISR4321-B/K9 is not supported for Cisco ISR-WAAS installation.
- Activating Cisco ISR-WAAS after formatting the Cisco 4000 Series ISR-router bootflash:

After you format the Cisco 4000 Series ISR-router bootflash, you must reload the router to ensure a successful activation of Cisco ISR-WAAS. If you do not reload the Cisco ISR router after formatting the bootflash, you will be unable to activate Cisco ISR-WAAS. For more information on formatting the Cisco 4000 Series ISR router bootflash, see the *Configuration Guide for Integrated AppNav/AppNav-XE and ISR-WAAS on Cisco 4000 Series ISRs*.

- For Cisco ISR-4321 with Cisco IOS-XE, used with Cisco WAAS Version 6.2.3c or 6.3.1

  You must complete a new OVA deployment of Cisco WAAS version 6.2.3c or 6.3.1 for this configuration to work successfully. This configuration will not automatically work after an upgrade to Cisco WAAS Version 6.2.3c or 6.3.1 from Cisco WAAS Version 5.x or 6.x.

- Using Snort with Cisco ISR-WAAS and Cisco ISR-4000 Series, with a hard disk less than or equal to 200 GB

  To ensure a successful WAAS installation of ISR-WAAS and the intrusion detection and prevention system Snort on an ISR router, you must install ISR-WAAS before you install Snort. If you do not follow this installation order, ISR-WAAS will not install and a disk error will be displayed.

- VRF restriction for VirtualPortGroup31 on Cisco ISR-WAAS

  When you configure Cisco ISR-WAAS with EZConfig: **VirtualPortGroup31**, the Cisco WAAS service and router interface, is automatically created, and you can then add or modify specific parameters for it.

  Do *not* add Virtual Routing and Forwarding (VRF) to **VirtualPortGroup31**, because VRF causes VirtualPortGroup31 to lose its IP address and to disable Cisco AppNav. To re-establish these, you must uninstall and reinstall Cisco ISR-WAAS without VRF.

  For more information on **VirtualPortGroup31**, see the *Configuration Guide for Integrated AppNav/AppNav-XE and ISR-WAAS on Cisco 4000 Series ISRs*.

Configuring the Hostname for Cisco ISR-WAAS

This section contains the following topics:

About Cisco ISR-WAAS and Cisco ISR-WAAS Hostname

For Cisco WAAS Version 5.5.5 and later, you can configure the Cisco ISR-WAAS hostname. For Cisco WAAS versions earlier than Cisco WAAS Version 5.5.1, Cisco ISR-WAAS receives a system-generated hostname from the Cisco ISR router, which cannot be edited.

Cisco ISR-WAAS is the specific implementation of Cisco vWAAS running in a Cisco IOS-XE Software container (the hypervisor that runs virtualized applications on a Cisco ISR 4000 Series router). Table 33: Cisco ISR-WAAS Models Supported for Cisco vWAAS shows the ISR-WAAS models and associated Cisco WAAS versions supported for Cisco vWAAS.

Table 33: Cisco ISR-WAAS Models Supported for Cisco vWAAS

Cisco vWAAS Model	Cisco vWAAS Model Memory	Supported Cisco ISR-WAAS Model	Cisco WAAS Version Supported
ISR-WAAS-200	3 GB	ISR-4321	5.2.1 and later
	4 GB	ISR-4321	6.2.3 and later
ISR-WAAS-750	4 GB	ISR-4351 ISR-4331 ISR-4431 ISR-4451	5.2.1 and later
		ISR-4461	6.4.1b and later
ISR-WAAS-1300	6 GB	ISR-4431 ISR-4451	5.2.1 and later
		ISR-4461	6.4.1b and later
ISR-WAAS-2500	8 GB	ISR-4451	5.2.1 and later
		ISR-4461	6.4.1b and later

Consider the following guidelines for the Cisco ISR-WAAS hostname:

- The Cisco ISR-WAAS hostname is independent of the Cisco ISR router hostname. Changing the Cisco ISR router hostname does not change the Cisco ISR-WAAS hostname.
- Hostname configuration is not supported on the Cisco ISR-WAAS device when it is downgraded from Cisco WAAS Version 6.x to a Cisco WAAS version earlier than Cisco WAAS Version 5.5.5.
- Each Cisco ISR-WAAS image is shipped with multiple profiles; each profile dictates the resources used by the Cisco ISR-WAAS virtual instance and the number of connections supported. The default is the profile with the highest number of connections; you can select the profile that meets the requirements of your system.

Note To change the Cisco ISR-WAAS profile of an active Cisco ISR-WAAS, you must first uninstall and then reinstall the Cisco ISR-WAAS.□

If you only deactivate the existing Cisco ISR-WAAS instance and then change the Cisco ISR-WAAS profile, the Cisco ISR-WAAS will become unstable and the TFO limit will show Zero on the Cisco ISR-WAAS console.

For information on how to deploy and register a Cisco ISR-WAAS on the Cisco ISR-4451-X, see the *Configuration Guide for Integrated AppNav/AppNav-XE and ISR-WAAS on Cisco ISR-4451-X*.

Configuring the Cisco ISR-WAAS Hostname with the Cisco WAAS Central Manager

Procedure

Step 1 Verify that the Cisco ISR-WAAS device is online by choosing **Devices** > *device-name*.

The **Device Dashboard** window appears, and displays information including device status: Pending, Installed, Online, or Inactive.

Note During a fresh OVA deployment of a Cisco ISR-WAAS instance, the Cisco ISR-WAAS default hostname is *router-name* **isr-waas**. After the hostname is changed on the **vwaas** instance, the **vwaas** instance does not get an update from the router until you change it in the **vwaas** instance with the Cisco WAAS CLI **no-hostname** command.

Step 2 To change the Cisco ISR WAAS hostname, choose **Devices** > **ISR WAAS Device** > **Activation**.

The **Device Activation** window appears, with fields for editing properties of the selected device. The **Name** field initially has the default Cisco ISR-WAAS hostname, *router-hostname*-**isr-waas**.

Step 3 In the **Name** field of the **Activation** window, enter the new name of the Cisco ISR-WAAS hostname. A maximum of 30 alphanumeric characters, including a hyphen, can be entered. The hostname is case sensitive. Special characters such as $, #, or * are not allowed.

Step 4 Click **Submit**.

Step 5 To verify that the new hostname is saved, click the Cisco WAAS CLI **show hosts** EXEC command.

Configuring the Cisco ISR-WAAS Hostname with the IRS Router CLI

Procedure

Step 1 To verify that the Cisco ISR-WAAS device is online, run the router CLI command **show virtual-service list**. The **show virtual-service list** command displays the status for each device, such as Initializing, Installing, Installed, Install Failed, Activating, Activated, Activated Failed, Deactivating, Deactivated, and Error.

Step 2 Log in to the Cisco ISR-WAAS device.

Step 3 Enter **Configuration** mode and run the router global configuration command **hostname** *hostname* to specify a new hostname. A maximum of 30 alphanumeric characters, including a hyphen, can be entered. Special characters such as $, #, or * are not allowed.

```
Router# config
Router (config)# hostname isr-waas-rs4a
```

Step 4 To verify that the new Cisco ISR-WAAS hostname has been saved, run the **show hosts** command.

Resetting a Cisco ISR-WAAS Hostname

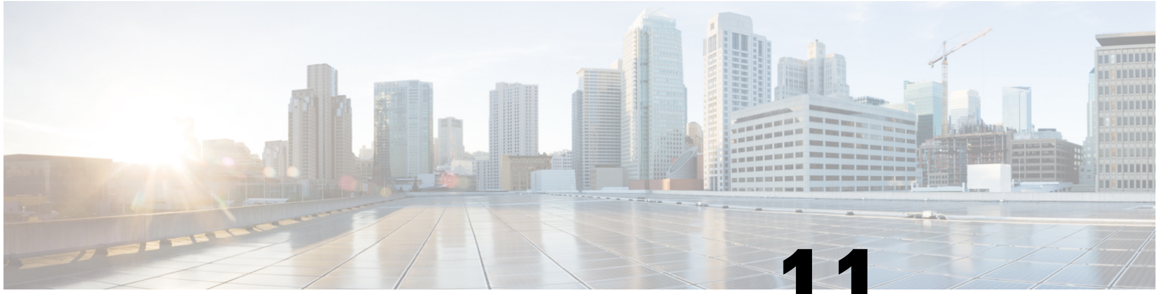
To reset a Cisco ISR-WAAS hostname, run the **restore factory default** command.

Consider the different results generated by the restore factory default command and its parameters:

- To reset the Cisco ISR-WAAS hostname to its factory default (-IRS-WAAS): Run the **restore factory-default** command. This version of the command resets the entire device configuration and all data back to the manufacture factory status.
- To retain the Cisco ISR-WAAS hostname but reset other parts of the device configuration and data: Run the **restore factory-default preserve basic-config** command.

  The **restore factory-default preserve basic-config** version of the command resets all device configuration and all data back to the manufacture factory status but preserves the Cisco ISR-WAAS hostname, as well as domain name, name server, and network interfaces.

For more information on using the **restore factory-default** command, see the *Cisco Wide Area Application Services Command Reference Guide* .



CHAPTER 11

Configuring File Services

This chapter describes how to configure Cisco WAAS File Services. This feature allows branch office users to access data stored at centralized data centers more efficiently. The file services feature overcomes the WAN latency and bandwidth limitations by caching data on Cisco Edge Wide Area Application Engines (Cisco WAEs) near branch office users. Cisco Wide Area Application Services (WAAS) file services use Server Message Block (SMB) application accelerators.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco WAAS Central Managers and WAEs in your network. The term WAE refers to WAE and Cisco Wide Area Virtualization Engine (Cisco WAVE) appliances, and Cisco Virtual WAAS (Cisco vWAAS) instances.

This chapter contains the following sections:

About Cisco WAAS File Services

Enterprises today have remote offices in different parts of the country and around the world, often with remote offices having their own file servers to store and manage the data needed by local users. This method of operation can be costly to purchase, manage, and upgrade file servers at each remote office, and to protect data in case of server failure. To achieve the required level of data assurance, the remote office must devote resources to back up the data at the remote site and physically move it to a secure location, often at a considerable distance from the site. When this scenario is multiplied by tens, hundreds, and thousands of remote offices, the enterprise data management costs can rise exponentially, along with the increased risks to critical data.

The logical solution is to move all of the enterprise’s important data to a central location containing the facilities, trained personnel, and storage mass required to manage the data properly. By having a data center provide backup and other storage-management facilities, the enterprise can achieve better utilization of both personnel and storage, as well as a higher level of data assurance and security.

However, the WAN between the enterprise's data center and its remote offices can be unreliable and slow, with limited bandwidth and high latency. The WAN can also create other obstacles to the implementation of the data center solution, including file server protocols that operate over the WAN. Every file operation generates several exchanges of protocol messages between the client and the file server. While often not noticeable on the LAN, this can quickly cause high latency over the WAN, which sometimes can break the file server protocol altogether. Even when the file server protocol functions correctly over the WAN, there can be long delays between each transaction, which can cause timeouts in user applications such as word-processing programs, image-editing programs, and design tools, or which stop the applications from functioning correctly.

The problems of unreliable WANs, file system protocol compatibility, and user application compatibility diminish productivity, and overall, negatively affect the user experience.

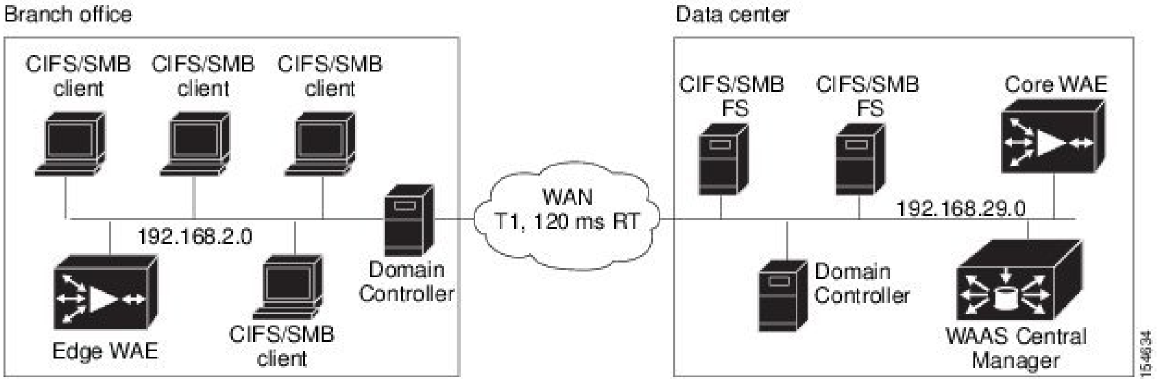
Cisco WAAS File Services overcomes WAN latency and bandwidth limitations by caching data on Edge WAEs near the user. This data caching method allows branch office users to access centralized data at LAN-like speeds over the WAN. The solution is based on several key concepts:

- Use the WAN as little as possible: By minimizing the number of operations that need to traverse the WAN, Cisco WAAS effectively shields users from many of the obstacles that WANs create.
- Use the WAN optimally: Cisco WAAS File Services uses sophisticated caching, compression, and network optimization technologies, which enable the system to use the WAN optimally.
- Preserve file system protocol semantics: Although Cisco WAAS software uses its own proprietary protocol over the WAN, it leaves intact the complete semantics of the standard file system protocol commands. This is essential to preserve the correctness and coherency of the data in the network.
- Make the solution transparent to users: The best solutions are the ones that do their jobs unnoticed, without interfering with end users' operations or forcing users to change their ways of doing business. The Cisco WAAS File Services solution does not require any software installations, either on the server side or at the client-side, and does not require a user to learn anything new. Users derive all the benefits of having a secure data center without needing to change any of their work habits.

By using Cisco WAAS File Services, enterprises can consolidate their file servers to a data center that provides the facilities, IT personnel, and storage devices required to manage the data properly.

The following figure shows a typical deployment scenario after Cisco WAAS File Services have been set up.

Figure 47: Cisco WAAS File Services Solution



Cisco WAAS File Services Features

This section contains the following topics:

Note To accelerate SMB traffic, use the SMB application accelerator, which handles optimizations of file server operations. These optimizations apply to SMBv1, SMBv2 and SMBv3. For information on how to use the SMB application accelerator to perform specific file server optimizations, see Configuring SMB Acceleration in the chapter "Configuring Application Acceleration." Legacy-mode Cisco Wide Area File Services (Cisco WAFS) is not supported for Cisco WAAS Version 4.4.1 and later. Before upgrading, legacy Cisco WAFS users must migrate to the SMB accelerator.

Automatic Discovery

The Automatic Discovery feature allows you to enable SMB without having to register individual file servers in the Cisco WAAS Central Manager. With the Automatic Discovery feature, Cisco WAAS attempts to automatically discover and connect to a new file server when a SMB request is received.

Data Coherency and Data Concurrency

Cisco WAAS software ensures data integrity across the system by using two interrelated features: **data coherency**, which manages the freshness of data, and **data concurrency**, which controls the access to data by multiple clients.

This section contains the following topics:

- Data Coherency, on page 345
- Data Concurrency, on page 346

Data Coherency

Maintaining multiple copies of data files in multiple locations increases the likelihood that one or more of these copies will be changed, which can cause the changed copy to lose consistency or coherency with the other copies. To address this scenario, data coherency manages the freshness of data.

Coherency semantics are used to provide guarantees of freshness (whether the copy is up-to-date or not) and the propagation of updates to and from the origin file server.

The Cisco WAAS software applies the following coherency semantics to its built-in coherency policies:

- **Strict SMB behavior for intra-site**: Users of the same cache are always guaranteed standard, strict SMB coherency semantics.
- **Cache validation on SMB open**: In SMB, the **File Open** operation is passed through to the file server. For data coherency purposes, the Cisco WAAS software validates the freshness of the file on every file that is open, and invalidates the cached file if a new version exists on the file server.

Cisco WAAS software validates data by comparing the time stamp of a file in the cache to the time stamp of the file on the file server. If the time stamps are identical, the cached copy in the Cisco Edge WAE is considered valid, and the user is permitted to open the file from the Cisco Edge WAE cache.

If the time stamps are different, the Cisco Edge WAE removes the file from its cache and requests a fresh copy from the file server.

- **Proactive cache updating**: Cisco WAAS software supports the use of change notifications in SMB environments as a way to keep cached data on the Cisco Edge WAEs up-to-date.

  When a client makes a change to a directory or file, the Cisco Edge WAE sends a change notification to the file server. The file server then sends a change notification to all the Cisco Edge WAEs, which includes a list of the modified directories and files. Upon receiving the change notification, each Cisco Edge WAE checks its cache and invalidates the directories and files listed in the notification, and then updates its cache with the latest versions.

  Example:

  If a user edits an existing Microsoft Word document and saves the changes to the Cisco Edge WAE cache, the Cisco Edge WAE sends a change notification to the file server so that it knows that the file has been modified. The Cisco Edge WAE then sends the changed sections to the file server, and the file server proactively sends change notifications to the other Cisco Edge WAEs in the network. These Cisco Edge WAEs then update their cache so that the file is consistent across all access points.

  This process is also applicable when you rename a directory, add a new subdirectory, rename a file, or create a new file in a cached directory.

- **Flush on SMB close**: In SMB, the **File Close** operation forces all the write buffers to be flushed to the file server, and the Close request is only granted after all the updates have been propagated to the file server. From a data coherency standpoint, the combination of **Validate on File Open** and **Flush on File Close** ensures that well-behaved applications, such as Microsoft Office, operate in session semantics. The SMB commands **Open**, **Lock**, **Edit**, **Unlock**, and **Close**, are guaranteed to work correctly on the Cisco WAAS network.

  This authorization process prevents users from accessing directories and files in the cache that they do not have permission to access on the file server.

Data Concurrency

Data concurrency control is important when multiple users access the same cached data to read, or write, or both. Data concurrency control synchronizes this access by establishing and removing file system locks. This file-locking feature ensures data integrity and provides the following benefits:

- Enables a client to aggressively cache file data so that it does not have to rely on retrieving data from the remote file server.
- Provides a performance boost in many applications running on existing CIFS client implementations.
- Preserves data integrity because only one user at a time can make changes to a section of a file.

Cisco WAAS software supports the CIFS OpLock feature, which allows a user to lock a file so that the user can safely read and write data to its local cache instead of using network bandwidth to perform these functions over the WAN on the file server. By using OpLock, a user can proactively cache read-ahead 11-5 Cisco Wide Area Application Services Configuration Guide Chapter 11 Configuring Cisco WAAS File Services Cisco WAAS File Services Features data because it knows that no other user is accessing the file, and therefore, there is no chance of the cached data becoming stale. The user can also write data to its local cache and does not have to update the file server until it closes the file or until another user requests that the same file be opened.

Oplock applies to files only. The file server does not grant OpLock requests on directories and named pipes.

File-Locking Process:

When a user opens a file, it sends a lock request to the file server. The Cisco Edge WAE intercepts and forwards all lock requests from the user to the file server as well as all the responses from the file server to the user. If no other user has a lock on the file, the file server grants an exclusive lock request so that the user can safely cache the file.

If a second user requests that the same file be opened, the following actions occur:

- The file server revokes the exclusive file lock obtained by the first user.
- The first user performs the following actions:
    - Flushes any file changes stored in its cache to the file server. This action ensures that the second user opening the file receives the latest information from the file server.
    - Deletes any of its read-ahead buffers for the file because that data is no longer guaranteed to remain up-to-date since a second user will open the file.
- The file server allows the second user to open the file.

Prepositioning

The prepositioning feature allows system administrators to proactively push frequently-used files from the central storage into the cache of selected Cisco Edge WAEs. This operation provides users with faster first-time file access, and makes more efficient use of available bandwidth.

- When an end user attempts to open a file that is not found in the Cisco Edge WAE cache, the Cisco Edge WAE retrieves it across the WAN from the file server where it is stored.
- The prepositioning feature allows administrators to push large, frequently-accessed files from file servers to selected Cisco Edge WAE caches according to a predefined schedule. Through the appropriate use of prepositioning, administrators can enable users to benefit from cache-level performance even during first-time access of these files.
- Prepositioning improves WAN bandwidth utilization by transferring heavy content when the network is otherwise idle, for example, at night, which frees up bandwidth for other applications during the day.
- The Cisco WAAS Central Manager GUI allows administrators to create multiple, overlapping preposition policies (each with its own schedule), a list of target Cisco Edge WAEs, and defined time and size constraints.

  Create preposition directives from the Cisco WAAS Central Manager GUI.
- Prepositioning includes the ability to configure multiple roots. For more information, see Creating a Preposition Directive for CIFS Files and Creating a Preposition Directive for SMB Files.

Prerequisites for Configuring Cisco WAAS File Services

This section describes the prerequisites for configuring Cisco WAAS Files Services on Cisco WAEs and for configuring Cisco WAAS File Services on a Cisco ISR Router with a Cisco NME-WAE.

- **Prerequisites for enabling file services on Cisco WAEs**:
  - If you want to configure multiple devices with the same settings, ensure that you have created a device group that contains all the devices you want to enable with file services. For information on creating device groups, see the chapter "Using Device Groups and Device Locations."
  - Identify the file servers that you want to export, and refer to Checklist for Configuring the CIFS Accelerator to verify that these file servers can operate with Cisco WAAS software.
  - Other file servers may operate with Cisco WAAS, but only those listed in the table were tested. The file server must support opportunistic locking (OpLock) and CIFS notifications.
  - The CIFS application accelerator does not support file servers that use the FAT32 file system. You can use the policy rules to exclude FAT32 file servers, if any, from CIFS accelerator optimization.
  - Certain combinations of operating systems and file systems on a file server can result in the server responding with different timestamp precisions for different SMB commands. In such a situation, you may not get the highest possible CIFS optimization if the CIFS application accelerator avoids using cached files with mismatched timestamps in favor of preserving data coherency.
- **Prerequisites for configuring Cisco WAAS File Services on a Cisco ISR Router with a Cisco NME-WAE**:
  - If you are running the Cisco WAAS on a network module that is installed in a Cisco ISR router, there are specific memory requirements for supporting file services. The Cisco WAAS NME-WAE must contain at least 1 GB of RAM to support file services.
  - If you try to enable file services and the device does not contain enough memory, the Cisco WAAS Central Manager displays an error message.
  - You can check the amount of memory that a device contains in the Device Dashboard window. For details, see Device Dashboard Window in the chapter "Monitoring Your Cisco WAAS Network."

Configuring the CIFS Accelerator

This section containst the follow topics:

Checklist for Configuring the CIFS Accelerator

To accelerate CIFS traffic, enable and configure the CIFS accelerator.

The CIFS accelerator relies on automatic discovery and transparently accelerates CIFS traffic with no configuration needed.

The following table provides a checklist for steps that you must complete to configure the CIFS accelerator.

Table 34: Checklist for Configuring CIFS Accelerator

Task	Additional Information and Instructions
1. Prepare for Cisco WAAS file services.	The tasks that you need to complete before enabling and configuring file services on your WAAS devices.For more information, see Prerequisites for Configuring Cisco WAAS File Services.
2. Enable CIFS acceleration.	Enables and configures the CIFS accelerator. For more information, see Enabling and Disabling the Global Optimization Features in the chapter "Configuring Application Acceleration."
3. (Optional) Identify dynamic shares.	Identifies the dynamic shares on an exported file server. If your file server uses Access Based Enumeration (ABE) to give users different views of the share, you must configure the dynamic shares on the Cisco WAAS Central Manager. For more information, see Creating Dynamic Shares for the CIFS Accelerator.
4. (Optional) Create a preposition directive.	Defines which files are proactively copied from an exported file server to the Edge WAE cache. For more information, see Preposition Directives for CIFS Files.

Creating Dynamic Shares for the CIFS Accelerator

Before you begin

Many file servers use dynamic shares, that is, multiple users can access the same share, but the share is then automatically mapped to a different directory based on a user’s credentials. Dynamic shares are most commonly used on file servers to set up user home directories. For example, a directory named Home can be set up as a dynamic share on a file server so that each user accessing that share is automatically redirected to their own personal directory.

If a file server contains a dynamic share or is using Access Based Enumeration (ABE), you must register that dynamic share with the Cisco WAAS Central Manager, as described in this section.

Defining a dynamic share in the Cisco WAAS Central Manager allows each user to see a different view of the share and allows the operation of ABE if it is configured on the Microsoft Windows Server.

Note Dynamic share configuration on the Cisco WAAS Central Manager overrides any dynamic share configuration set up directly on the Cisco WAE device using the Cisco WAAS CLI.

Before configuring a dynamic share, consider the following limitations:

- Each dynamic share on a file server must be unique.
- You cannot configure a dynamic share if that share has a preposition directive. You must remove the preposition policy before you can configure the dynamic share.
- You can use the Cisco WAAS Central Manager GUI to define any directory as a dynamic share. However, if a directory is not set up as a dynamic share on the file server, all the users will read or write the same content from the same directory and will not be redirected to different directories based on their credentials.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure > CIFS File Services > Dynamic Shares**.

A list of dynamic shares appears. The **Dynamic Shares** window shows all the dynamic shares that are configured. From this window, you can perform the following tasks:

- To edit the configuration of an existing dynamic share, click the **Edit** icon next to the share. You can delete a dynamic share, or modify any of the dynamic share settings.
- Add a new dynamic share definition.

Step 2 To add a new dynamic share, click the **Create New Dynamic Share** icon in the taskbar.

The **Creating a New Dynamic Share** window appears.

Step 3 In the **Name** field, enter a name for the dynamic share.

The following characters are not supported in the dynamic share name: /, \, :, *, ?, ", <, >, |. From the **Assigned Domain** drop-down list, choose the Cisco WAAS domain that you want to assign to the dynamic share. Only administrators who are also assigned to this Cisco WAAS domain have permission to edit the dynamic share configuration. The domain does not affect a client's access to the dynamic share.

Note A Cisco WAAS domain is not the same as a DNS domain or Microsoft Windows domain. For more information, see Working with Domains in the chapter "Creating and Managing Administrator User Accounts and Groups."

The Cisco WAAS domain does not use entities. When defining the Cisco WAAS domain, choose **None** for the **Entity Type**. The Cisco WAAS domain must be assigned to each Cisco WAAS administrative user who needs to edit the dynamic share configuration. For more information, see Assigning a Domain to a User Account in the chapter "Creating and Managing Administrator User Accounts and Groups."

Step 4 In the **File Server** field, enter the name or IP address of the file server with the dynamic share.

If you specify the file server name, the Edge WAE resolves it to an IP address.

The registered file servers are displayed in a drop-down list.

Step 5 In the **User name**, **Password**, and **Confirm Password** fields, enter the username and password credentials for the file server. If the username is in a Microsoft Windows domain, specify the domain name as part of the **User name** field, as follows: **domain\username**.

These credentials are used only to access the file server when you click **Browse**.

Step 6 In the **Share Name** field, specify the location of the dynamic share by doing one of the following tasks:

- Enter the name of the dynamic share on the file server. The following characters cannot be used in the share name: \, /, :, *, ?, “, <, >, |.
- To navigate to the correct root directory, click **Browse** next to the **Share Name** field.

Note The **Browse** button appears only if you have at least one Cisco WAE device with the CIFS accelerator enabled and registered to the Cisco WAAS Central Manager.

Step 7 Ensure that the status of the share is set to **Enabled**. If you change the status to **Disabled**, the share will not be set up as a dynamic share in your Cisco WAAS environment.

Step 8 Click **Submit**.

The specified directory now functions as a dynamic share on the Cisco Edge WAE cache.

Preposition Directives for CIFS Files

This section contains the following topics:

About Preposition Directives for CIFS Files

A preposition directive allows you to determine which files should be proactively copied from CIFS file servers to the cache of selected Cisco Edge WAEs. Prepositioning enables you to take advantage of the idle time on the WAN to transfer frequently-accessed files to selected WAEs, where users can benefit from cache-level performance even during first-time access of these files.

Consider the following operating guidelines for preposition directives for CIFS files:

- You can start or stop a preposition task from the Cisco WAAS Device Manager.
- Prepositioning is supported on automatically discovered file servers in the transparent CIFS accelerator.
- When defining a preposition directive, select the Cisco Edge WAEs that you want to be prepositioned with content from the file server, and then specify the root directories on the file server to be prepositioned. Initially, the preposition directive is in the unscheduled state. You must create a schedule that determines when and how often the content is prepositioned. Because content can be prepositioned on a regular basis, you can specify whether each new iteration of the task should copy all designated files, or only those files that have changed over a specified time interval.
- In addition, you can specify time and size limits to prevent a preposition task from consuming too much bandwidth on the WAN or too much space on the Cisco Edge WAE cache. We strongly recommend that you use these limits to optimize network efficiency and prevent misuse of this feature.
- When the activation time of a preposition directive arrives, a preposition task starts on the Cisco Edge WAE. Each preposition task can be monitored in the Cisco WAAS Central Manager GUI during and after processing. You can also terminate active preposition tasks, if required.
- Prepositioning requires that the username and password needed to access the file server be specified. These items are specified directly in the **Creating New Preposition Directive** window, as described in Creating a Preposition Directive for CIFS Files.

Note When preposition updates are sent to the Cisco WAAS Central Manager, if any preposition file server credentials cannot be decrypted, all further preposition updates are not sent from the Cisco WAE to the Cisco WAAS Central Manager, and decryption failure error messages are logged in **errorlog/cms_log.current**. You must reconfigure the preposition credentials from the Cisco WAAS CLI.

- Prepositioning includes the ability to configure multiple roots. For more information, see Creating a Preposition Directive for CIFS Files.
- When using prepositioning, both branch and data center WAEs are required (the same as for any other accelerated traffic). The branch WAE retrieves prepositioned files through an optimized connection. Verify that you have connectivity between the following network entities:

  - Client to branch WAE
  - Branch WAE to data center WAE
  - Branch WAE to file server
  - Data center WAE to file server

- You will need to change any ACLs that might be blocking prepositioning traffic.

Note Although preposition directives can be created and managed by using the Cisco WAAS CLI, we recommend that you use the Cisco WAAS Central Manager GUI because you can manage prepositioning for groups of Cisco WAEs from the Cisco WAAS Central Manager. If you mix Cisco WAAS Central Manager and Cisco WAAS CLI configuration, unpredictable results may occur because changes on one device can affect other devices.

Creating a Preposition Directive for CIFS Files

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure > CIFS File Services > Preposition**.

The **Preposition Directive** window appears. This window displays the following information about preposition directives that exist on the system:

- **Preposition Directive**: Name of the preposition directive.
- **Type**: **Full**, **Differential**, or **Since**
  - **Full**: All the files that match the other filters of the task and that are found on the file server are sent to the Edge to be compared with the cache.
  - **Differential**: Only the files that are found as changed since the last successful preposition are sent to the Edge cache. The time of the last successful preposition is taken from the Edge device, so ensure that the clock is synchronized with the file server. The first scan is always a full scan. If you change the preposition task, the last successful scan time is reset.
  - **Since**: Only the files that are found as changed within a specified time period are sent to the Edge cache.
- **Status**: Whether the preposition directive is enabled or disabled.
- **File Server**: Name of the exported file server.

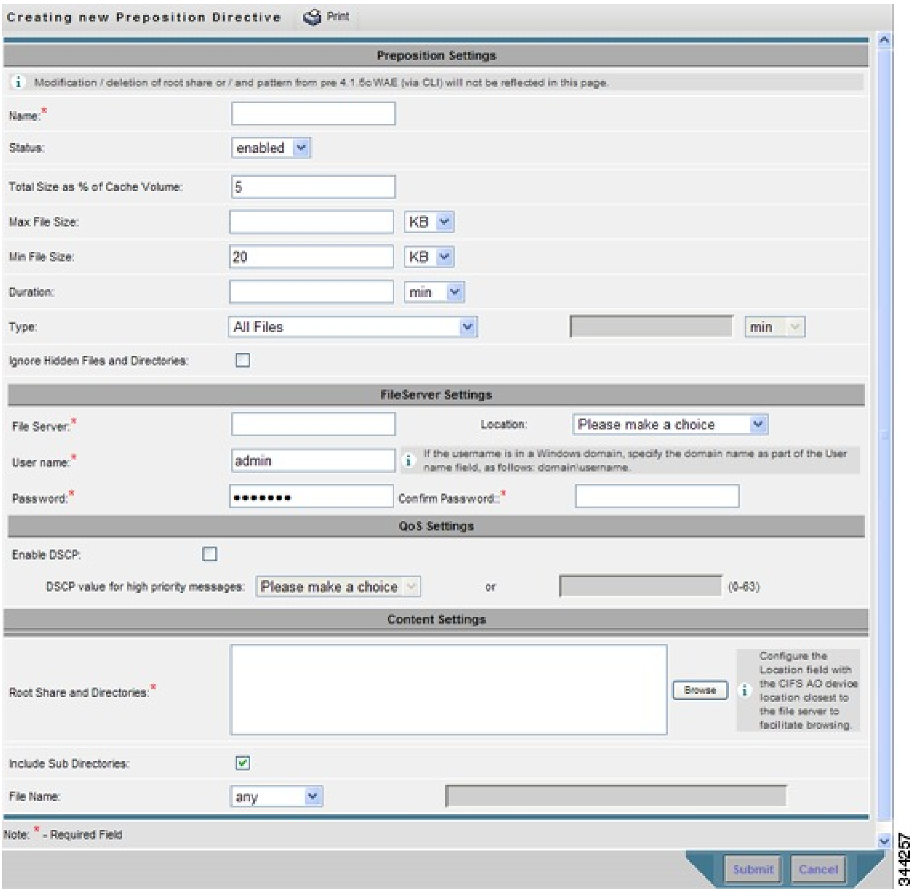
The following tasks are available from the **Preposition Directive** window:

- To edit the configuration of an existing preposition directive, click the **Edit** icon next to the corresponding directive. You can then delete the preposition directive, or modify any of the settings.
- To add a new preposition directive, follow the Step 2 and later steps.

Step 2 To create a new preposition directive, click the **Create New Preposition Directive** icon in the taskbar.

The **Creating New Preposition Directive** window appears.

Figure 48: Creating a New Preposition Directive Window



Creating new Preposition Directive   Print

Preposition Settings

Modification / deletion of root share or / and pattern from pre 4.1.5c WAE (via CLI) will not be reflected in this page.

Name:*
Status: enabled
Total Size as % of Cache Volume: 5
Max File Size: KB
Min File Size: 20 KB
Duration: min
Type: All Files   min
Ignore Hidden Files and Directories: □

FileServer Settings

File Server:*   Location: Please make a choice
User name:* admin   If the username is in a Windows domain, specify the domain name as part of the User name field, as follows: domain\username.
Password:* •••••••   Confirm Password::*

QoS Settings

Enable DSCP: □
DSCP value for high priority messages: Please make a choice   or   (0-63)

Content Settings

Root Share and Directories:*   Browse   Configure the Location field with the CIFS AO device location closest to the file server to facilitate browsing.
Include Sub Directories: ☑
File Name: any

Note: * - Required Field

Step 3 Enter a unique name for the directive. The name cannot contain characters other than letters, numbers, period, hyphen, and underscore; the double quote (") character is not allowed in the name.

Step 4 From the **Status** drop-down list, choose **enabled** or **disabled**. (Disabled directives are not put into effect.)

Step 5 (Optional) Define the time and size limitations using the provided fields.

> **Note** The table Table 39: Preposition Time and Size Limitations , on page 364 describes the time and size limitation fields. If one of these limits is exceeded during a prepositioning task, the task is terminated and a message is sent to the **Administrator** log. Any remaining files are exported the next time the task is run. If a user requests one of the missing files before this happens, it is fetched over the WAN through Cisco WAAS software as usual.

Step 6 (Optional) To prevent hidden directories on the file server from being prepositioned, check the **Ignore Hidden Directories** check box. This check box is unchecked by default. If you leave this box unchecked, hidden directories are prepositioned.

Step 7 In the **File Server** field, enter the unique name of a file server to export. The name cannot contain characters other than letters, numbers, period, hyphen, and underscore; the double quote (") or forward slash (/) characters are not allowed in the name.

Step 8 From the **Location** drop-down list, choose the device location that will provide browsing services for the file server. Regularly, this is the data center WAE. For the best browsing performance, specify a location that is close to the file server. The location is used only for browsing; each edge WAE will retrieve prepositioned files directly from the file server, not from this location. For more information on defining locations, see Working with Device Locations, on page 64.

Step 9 In the **User name**, **Password**, and **Confirm Password** fields, enter the username and password credentials for the file server. If the username is in a Windows domain, specify the domain name as part of the **User name** field, as follows: **domain\username**.

The access credentials that you enter must allow read access to the prepositioned root directories and to their parent directories.

Step 10 (Optional) Check the **DSCP value for high priority messages** check box if you want to assign a DSCP marking value to the prepositioning traffic. Choose a DSCP value from the drop-down list or enter a number from **0** to **63** in the text field.

DSCP is a field in an IP packet that enables different levels of service to be assigned to the network traffic. Levels of service are assigned by marking each packet on the network with a DSCP code and associating a corresponding level of service. DSCP is the combination of **IP Precedence** and **Type of Service (ToS)** fields. For more information, see RFC 2474.

Step 11 In the **Root Share and Directories** field, enter the directories on the file server that you want to export. Use any of the following methods to identify a directory:

- Manually enter one or more directory paths in the following format: **protocol://server/share** or **server\share**, for example, **cifs://win12srv/home** or **win12srv\home**. You can enter multiple lines for multiple directories, with each full directory path on its own line. You cannot specify the root directory (/) as a root share.
- When you define multiple root shares, the preposition sequence that is performed for a single root configuration is repeated for each root serially.
- To browse the directories on the file server, click **Browse**.
    - To navigate to a directory, click the **File Folder** icon to the left of the directory name.
    - Check the check box next to the directory that you want to export and then click **Select Directory**.

      The **Browse** window allows you to choose multiple directories.
    - The **Browse** function operates best when you choose the location of the nearest CIFS accelerator to the file server, from the Location drop-down list. If you do not choose a location, the browse request is sent to all the devices that have the CIFS accelerator enabled, and the request may time out.
- To include all the subdirectories under the specified root directory, check the **Include Sub Directories** check box. If this option is not selected, only the files in the specified root directory are prepositioned and you cannot select subdirectories when you are browsing.
- To narrow the policy definition to a particular type of file, choose a pattern operator from the **File Name** drop-down list and enter the text that describes the pattern in the adjacent text box. For example, enter ends with .doc. Do not use a space or the following special characters: |, :, >, <, ", ?, *, /, \.

Step 12 Click **Submit**.

The directive is saved and additional tabs appear at the top of the window.

Assigning Edge Devices to a Preposition Directive for CIFS Files

Before you begin

- After you create a preposition directive, you need to assign Cisco Edge WAEs or device groups to the directive. This task determines which Cisco Edge WAEs will store preposition content in their cache.
- Prepositioning includes the ability to configure multiple roots. See Creating a Preposition Directive for CIFS Files.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **CIFS File Services** > **Preposition**.

The **Preposition Directives** window appears, which lists the preposition directives that exist on the system.

Step 2 Click the **Edit** icon next to the preposition directive that you want to assign to an Edge WAE or device group.

Step 3 Click one of the following tabs at the top of the window:

- **Assign Edge Devices**: Allows you to select one or more Cisco Edge WAEs to assign to this directive.
- **Assign Edge Groups**: Allows you to select a device group to assign to this directive.

The **Edge Device Assignments** window or the **Device Groups Assignments** window appears, depending on the selected option.

For either view, the assignments window lets you filter your view of the items in the list. Filtering enables you to find items in the list that match the criteria that you set.

Step 4 Choose the Edge WAEs or device groups to assign to this preposition directive by doing either of the following:

- To assign all the available Cisco Edge WAEs or device groups to this directive, click the **Assign All** icon in the taskbar.
- To assign individual devices or device groups, click the blue "X" next to each Cisco Edge WAE or device group that you want to assign to this directive.

Note If a device or device group is offline (identified by a red "X"), then you cannot assign that device or group to this directive. The preposition directive, when assigned to a device group, is applied only to connected Edge devices in the assigned device group.

When assigning a CIFS accelerator preposition directive to a device group, the directive is applied only to those devices enabled for CIFS acceleration in the assigned device group.

Step 5 Click **Submit**.

The icon next to each edge device or device group you selected changes to a white checkmark inside a green circle.

Note If the CIFS accelerator is disabled on a Cisco WAE, the Cisco WAE is removed from any preposition directives to which it is assigned. Also, the preposition directive is removed from the device's running configuration.

Creating a Preposition Schedule for CIFS Files

Before you begin

After you create a preposition directive and assign Cisco WAEs to the directive, create a schedule that determines when and how often prepositioning occurs.

Example:

You want to schedule prepositioning to occur at night to minimize the amount of traffic during business hours, or, you may want to schedule prepositioning to occur on a recurring basis if the exported data changes often. This will help ensure that the Cisco WAEs assigned to this directive have the latest file updates in their cache.

Note When a preposition task is scheduled to begin at the same time for multiple Cisco Edge WAEs that are located in different timezones, the task will begin on the Cisco Edge WAEs based on the Cisco Core WAE timezone. If the clocks of the Cisco Edge WAE and the Cisco Core WAE are not synchronized, the task will *not* start on time.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **CIFS File Services** > **Preposition**.

The **Preposition Directives** window appears, which lists the preposition directives that exist on the system.

Step 2 Click the **Edit** icon next to the preposition directive for which you want to create a schedule.

Step 3 Click the **Schedule** tab at the top of the window.

The **Creating New Preposition Schedule** window appears. By default, no schedule is configured.

Step 4 Choose one of the following scheduling options:

- **Not Scheduled**: Prepositioning is not scheduled at this time.
- **Now**: Prepositioning occurs within a few minutes after you submit this schedule.

A **Now** schedule begins again each time you make a change to the preposition directive and click **Submit**. A **Now** schedule also begins again as soon as a Cisco Edge device that has been reloaded comes back online.

- **Daily**: Prepositioning occurs daily at the defined time.
- **Date**: Prepositioning occurs at the defined time and date.
- **Weekly**: Prepositioning occurs on the selected days of the week at the defined time.
- **Monthly Days**: Prepositioning occurs on the selected days of the month at the defined time.

- **Monthly Weekdays**: Prepositioning occurs on the defined day (as opposed to a defined date) and time during the month. For example, you can schedule prepositioning to occur on the second Tuesday of every month.

Step 5 Specify a start time for the prepositioning task.

Consider the following guidelines for specifying a start time:

- The time is expressed in 24-hour format with **00:00** representing midnight. The time refers to the local time of the Cisco Edge WAE where the data is to be prepositioned.
- If there are multiple Cisco Edge WAEs in different time zones, the time refers to the local time of the Cisco Core WAE.
- You cannot schedule a start time for the **Now** option.

Step 6 Click **Submit**.

The message **Changes Submitted** appears at the bottom of the window confirming that your schedule was saved.

Step 7 Verify that the preposition directive has completed successfully by checking the preposition status. For more information, see Checking the Preposition Task Status of CIFS Files, on page 357.

Checking the Preposition Task Status of CIFS Files

Before you begin

After you create one or more preposition directives, you can verify the status of all the preposition tasks to ensure that they are completed successfully. If a task does not complete successfully, then some of the prepositioned files may have not been copied to the Cisco Edge WAE cache.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **CIFS File Services** > **Preposition**.

The **Preposition Directives** window, which lists the preposition directives that exist on the system, appears.

Step 2 Click the **Edit** icon next to the preposition directive that you want to check.

Step 3 Click the **Preposition Status** tab at the top of the window.

The **Preposition Status** window displays the following information:

- **WAE**: The name of each Edge WAE that received the prepositioned files in its cache.
- **Start Time**: The time the preposition task started.
- **Duration**: The amount of time it took the preposition task to be completed.
- **Amount Copied**: The amount of data copied to the WAE cache, in bytes.
- **Status**: Whether the preposition task is completed successfully.
- **Reason**: The reason a preposition task failed.

Step 4 Ensure that the **Status** column shows **Completed**.

If this column shows **Failure**, look in the **Reason** column for an explanation that can help you troubleshoot why the preposition task failed. After resolving the issue, you can schedule the preposition task to run again now, or wait until the scheduled start time and verify the status again later.

Configuring the SMB Accelerator

This section contains the following topics:

Checklist for Configuring the SMB Accelerator

To accelerate SMB traffic, enable and configure the SMB accelerator.

The following table provides a checklist for steps that you must complete to configure the SMB accelerator.

Table 35: Checklist for Configuring SMB Accelerator

Task	Additional Information and Instructions
1. Prepare for Cisco WAAS file services.	The tasks that you need to complete before enabling and configuring file services on your WAAS devices.For more information, see Prerequisites for Configuring Cisco WAAS File Services.
2. Enable SMB acceleration.	Enables and configures the SMB accelerator. For more information, see Enabling and Disabling the Global Optimization Features in the chapter "Configuring Application Acceleration."
3. (Optional) Identify dynamic shares.	Identifies the dynamic shares on an exported file server. If your file server uses Access Based Enumeration (ABE) to give users different views of the share, you must configure the dynamic shares on the Cisco WAAS Central Manager. For more information, see Creating Dynamic Shares for the SMB Accelerator, on page 358.
4. (Optional) Create a preposition directive.	Defines which files are proactively copied from an exported file server to the Edge WAE cache. For more information, see Creating a Preposition Directive for SMB Files, on page 362.

Creating Dynamic Shares for the SMB Accelerator

Before you begin

Many file servers use dynamic shares, that is, multiple users can access the same share, but the share is then automatically mapped to a different directory based on a user’s credentials. Dynamic shares are most commonly used on file servers to set up user home directories. For example, a directory named Home can be set up as a dynamic share on a file server so that each user accessing that share is automatically redirected to their own personal directory.

If a file server contains a dynamic share or is using Access Based Enumeration (ABE), you must register that dynamic share with the Cisco WAAS Central Manager, as described in this section.

Defining a dynamic share in the Cisco WAAS Central Manager allows each user to see a different view of the share and allows the operation of ABE if it is configured on the Microsoft Windows Server.

Note Dynamic share configuration on the Cisco WAAS Central Manager overrides any dynamic share configuration set up directly on the Cisco WAE device using the Cisco WAAS CLI.

Before configuring a dynamic share, consider the following limitations:

- Each dynamic share on a file server must be unique.
- You cannot configure a dynamic share if that share has a preposition directive. You must remove the preposition policy before you can configure the dynamic share.
- You can use the Cisco WAAS Central Manager GUI to define any directory as a dynamic share. However, if a directory is not set up as a dynamic share on the file server, all the users will read or write the same content from the same directory and will not be redirected to different directories based on their credentials.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure > SMB File Services > Dynamic Shares**.

A list of dynamic shares appears. The **Dynamic Shares** window shows all the dynamic shares that are configured. From this window, you can perform the following tasks:

- To edit the configuration of an existing dynamic share, click the **Edit** icon next to the share. You can delete a dynamic share, or modify any of the dynamic share settings.
- Add a new dynamic share definition.

Step 2 To add a new dynamic share, click the **Add Dynamic Share** icon in the taskbar.

The **Creating a New Dynamic Share** window appears.

Step 3 In the **File server** field, enter the name or IP address of the file server with the dynamic share

If you specify the file server name, the Cisco Edge WAE resolves it to an IP address.

The registered file servers are displayed in a drop-down list.

Step 4 In the **Share name** field, specify the location of the dynamic share by doing one of the following tasks:

Enter the name of the dynamic share on the file server. The following characters cannot be used in the share name: \ / : * ? “ < > |

To navigate to the correct root directory, click Browse next to the Share Name field

The **Browse** button appears only if you have at least one Cisco WAE device with the SMB accelerator enabled and registered to the Cisco WAAS Central Manager.

Step 5 To submit the changes, click **OK**.

The specified directory now functions as a dynamic share in the Cisco Edge WAE cache.

Preposition Directives for SMB Files

This section contains the following topics:

About Preposition Directives for SMB Files

A preposition directive allows you to determine which files should be proactively copied from SMB file servers to the cache of selected Cisco Edge WAEs. Prepositioning enables you to take advantage of the idle time on the WAN to transfer frequently accessed files to selected WAEs, where users can benefit from cache-level performance even during first-time access of these files.

Considering the following guidelines for creating and using preposition directives for SMB files:

Note When preposition updates are sent to the Cisco WAAS Central Manager, if any preposition file server credentials cannot be decrypted, all further preposition updates are not sent from the Cisco WAE to the Cisco WAAS Central Manager, and decryption failure error messages are logged in **errorlog/cms_log.current**. You must reconfigure the preposition credentials from the Cisco WAAS CLI.

Note Although preposition directives can be created and managed by using the Cisco WAAS CLI, we recommend that you use the Cisco WAAS Central Manager GUI because you can manage prepositioning for groups of Cisco WAEs from the Cisco WAAS Central Manager. If you mix Cisco WAAS Central Manager and Cisco WAAS CLI configuration, unpredictable results may occur because changes on one device can affect other devices.

- You can start or stop a preposition task from the Cisco WAAS Device Manager.
- Cisco SMB AO supports accelerating client connections to Microsoft Distributed File System (DFS) shares.
- Prepositioning is supported on automatically discovered file servers in the SMB accelerator.
- When defining a preposition directive, select the Cisco Edge WAEs that you want to be prepositioned with content from the file server, and then specify the root directories on the file server to be prepositioned. Initially, the preposition directive is in the unscheduled state. You must create a schedule that determines when and how often the content is prepositioned.

  In addition, you can specify time and size limits to prevent a preposition task from consuming too much bandwidth on the WAN or too much space on the Cisco Edge WAE cache. We strongly recommend that you use these limits to optimize network efficiency and prevent misuse of this feature.
- When the activation time of a preposition directive arrives, a preposition task starts on the Cisco Edge WAE. Each preposition task can be monitored in the Cisco WAAS Central Manager GUI during and after processing. You can also terminate active preposition tasks, if required.

- Prepositioning requires that the username and password needed to access the file server be specified. These items are specified directly in the **Creating New Preposition Directive** window, as described in Creating a Preposition Directive for SMB Files.
- Prepositioning includes the ability to configure multiple roots. For more information, see Creating a Preposition Directive for SMB Files.
- When using prepositioning, both branch and data center WAEs are required (the same as for any other accelerated traffic). The branch WAE retrieves prepositioned files through an optimized connection. Verify that you have connectivity between the following network entities:
  - Client to branch WAE
  - Branch WAE to data center WAE
  - Branch WAE to file server
  - Data center WAE to file server

  You will need to change any ACLs that might be blocking prepositioning traffic.
- Do not configure more than 25 preposition directives per device.
- DRE is disabled by default. To enable DRE, choose **Device> Configure** > **Acceleration** > **SMB Preposition Settings**, and then select the SMB Preposition DRE settings check box.
  - When DRE is enabled for the all prepositioning tasks, files are cached in Object Cache and DRE cache, particularly when the size of the prepositioned files is huge and this could affect the normal traffic. Otherwise, the files will be cached only in Object Cache.
  - The following table shows the DRE disk capacity, default object cache capacity, and default Akamai Connect Cache capacity by WAVE model.

Table 36: DRE Disk, Default OC, and Default Akamai Connect Cache by Cisco WAVE Model

Cisco WAVE Model	DRE Disk Capacity	Default Object Cache Capacity	Default Akamai Connect Cache Capacity
WAVE 294-4G	40	102	59
WAVE 294-4G-SSD	40	57	55
WAVE 294-8G	55	77	65
WAVE 294-8G-SSD	55	46	47
WAVE 594-8G	80	143	200
WAVE 594-8G-SSD	80	125	125

  - The following table shows the default and resized DRE disk capacity, object cache capacity, and Akamai Connect Cache capacity by Cisco vWAAS model.

Table 37: Default and Resized DRE, OC, and Akamai Connect Cache, by Cisco vWAAS Model

Cisco vWAAS Model	DRE Disk Capacity	Default Object Cache Capacity	Default Akamai Connect Cache Capacity
vWAAS-150	52.3	52	30
vWAAS-150 Resized	51.25	52	30
vWAAS-200	52.23	82	100
vWAAS-200 Resized	52.23	82	100
vWAAS-750	96.75	122	250
vWAAS-750 Resized	96.75	122	250

- The following table shows the DRE disk capacity, default object cache capacity, and default Akamai Connect Cache capacity by Cisco ISR-WAAS model.

Table 38: DRE Disk, Object Cache, and Akamai Connect Cache by Cisco ISR-WAAS Model

Cisco ISR-WAAS Model	DRE Disk Capacity	Default Object Cache Capacity	Default Akamai Connect Cache Capacity
ISR-WAAS-200	75	32	30
ISR-WAAS-750	73	32	30
ISR-WAAS-1300	71	32	30
ISR-WAAS-2500	210	52	50

Creating a Preposition Directive for SMB Files

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure > SMB File Services > Preposition**.

The **Preposition Directives** window appears. This window displays the following information about preposition directives that exist on the system:

- **Preposition Directive**: Name of the preposition directive.
- **Status**: Whether the preposition directive is enabled or disabled.
- **File Server**: Name of the exported file server.
- **Schedule Details**: Schedule to determine how often content is prepositioned.

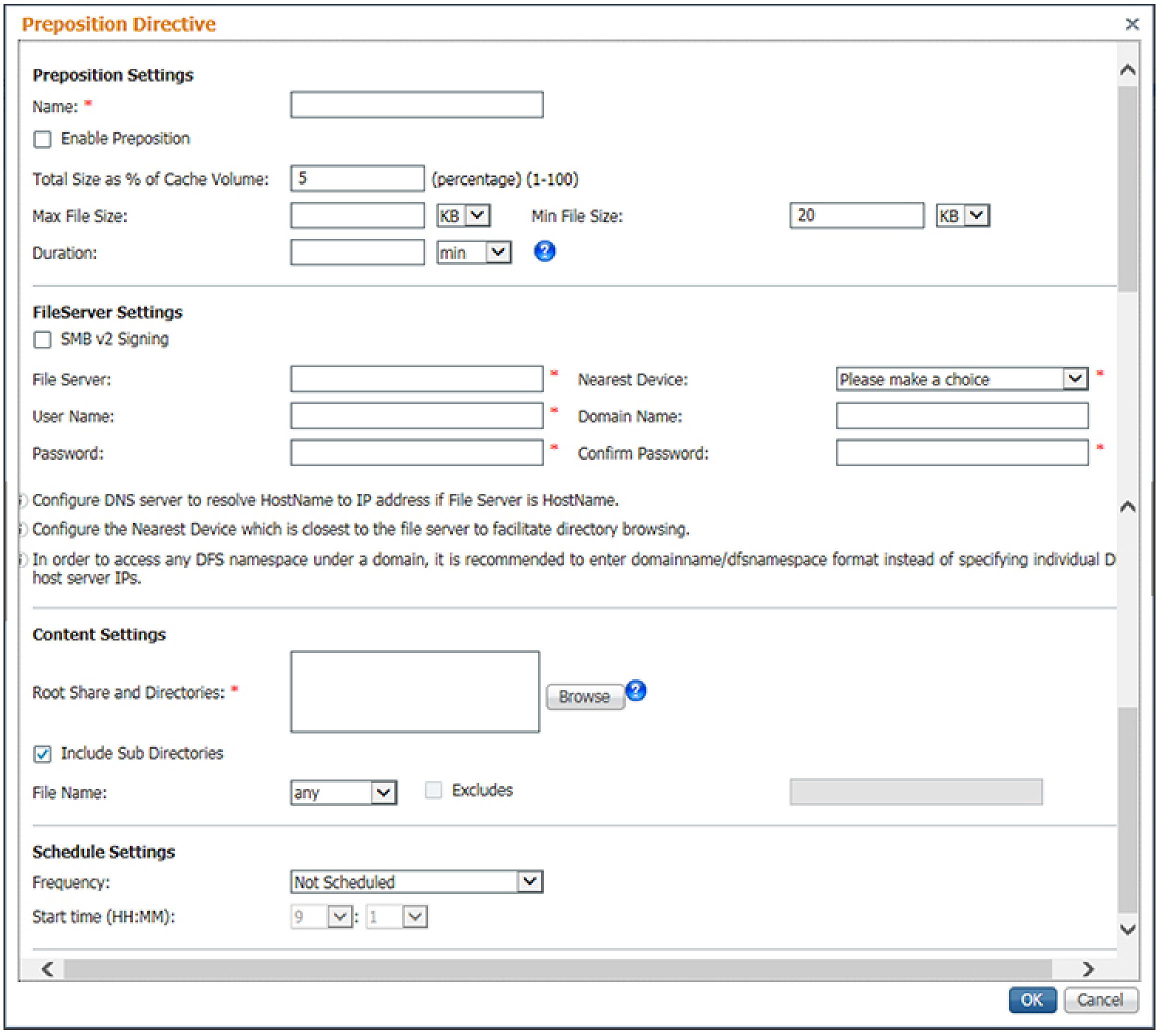
From the **Preposition Directives** window, you can perform the following tasks:

- Edit the configuration of an existing preposition directive by clicking the **Edit** icon next to the corresponding directive. You can then delete the preposition directive, or modify any of the settings.
- To assign the Device or Device Group (s) to the preposition operation, click the **Assign Device/DeviceGroup(s)** icon and select the appropriate one.
- To collect preposition status, click the **Collect Preposition Status** link.
- Add a new preposition directive, as described in the following steps.

Step 2 To create a new preposition directive, click the **Create New Preposition** icon in the taskbar.

The **Creating a New Preposition Directive** window appears.

Figure 49: Creating a New Preposition Directive Window



Preposition Directive

Preposition Settings

Name: *

□ Enable Preposition

Total Size as % of Cache Volume: 5 (percentage) (1-100)

Max File Size: KB Min File Size: 20 KB

Duration: min

FileServer Settings

□ SMB v2 Signing

File Server: * Nearest Device: Please make a choice *

User Name: * Domain Name:

Password: * Confirm Password: *

Configure DNS server to resolve HostName to IP address if File Server is HostName.

Configure the Nearest Device which is closest to the file server to facilitate directory browsing.

In order to access any DFS namespace under a domain, it is recommended to enter domainname/dfsnamespace format instead of specifying individual D host server IPs.

Content Settings

Root Share and Directories: *

Browse

☑ Include Sub Directories

File Name: any □ Excludes

Schedule Settings

Frequency: Not Scheduled

Start time (HH:MM): 9 : 1

OK Cancel

Step 3 At the **Preposition Settings** pane, in the **Name** field, enter a unique name for the directive. The name cannot contain characters other than letters, numbers, period, hyphen, and underscore; the double quote (") character is not allowed in the name.

Step 4 Click the **Enable Preposition** check box. This denotes status of preposition. This is unchecked by default. If you disable it, preposition is not possible.

Step 5 (Optional) Define the time and size limitations using the provided fields.

The following table describes the **Time** and **Size Limitation** fields.

Table 39: Preposition Time and Size Limitations

Field	Description
Total Size as % of Cache Volume	Percentage of the overall Edge WAE cache that prepositioned files can consume. For example, if you do not want this prepositioning directive to consume more than 30 percent of a WAE's cache, enter 30 in this field. The default value is **5 percent**. The percentage of the cache defined for a preposition task defines the maximum size that can be prepositioned in a single iteration of the task regardless of how much is already in the cache. The total size of the files to be prepositioned will always be less than or equal to the total percentage of object cache size specified. Example: • If the user has specified max-cache directive as 10% and total object-cache size is 100 GB, then the maximum size of the total files to be prepositioned for the task is 10 GB (10% of 100 GB). • If there are 100 files in the configured shares and first 50 files size up to 10 GB, the rest of the files will not be prepositioned. When the cache is full, regardless of the reason, prepositioning operates like on-demand caching: an eviction process begins and the files with the oldest time-last-accessed values are removed from the cache.
Max File Size	Maximum file size that can be exported. Files that are larger than this value are not exported to the WAE cache.
Min File Size	Minimum file size that can be exported. Files that are smaller than this value are not exported to the WAE cache. It is inefficient to preposition files smaller than 20 KB because these files can be retrieved quickly over the WAN through normal WAAS. The default value is **20 KB**.
Duration	Maximum amount of time it should take WAAS to export the file server. If it takes WAAS longer than this amount of time to export the file server, WAAS stops the exporting process before all files are copied to the Edge WAE cache. If the preposition task does not start at the scheduled start time, for example, because the Edge and the Core have no connection, the start retries are counted in the duration. If you do not specify a value for this field, WAAS takes as much time as needed to export this file server.

> **Note** If one of these limits is exceeded during a prepositioning task, the task is terminated and a message is sent to the **Administrator log**. Any remaining files are exported the next time the task is run. If a user requests one of the missing files before this happens, it is fetched over the WAN through Cisco WAAS software as usual.

Step 6 To enable prepositioning of this traffic, at the **File Server Settings** pane, check the **SMBv2** check box. The **SMBv2** check box is unchecked (disabled) by default.

Step 7 In the **File Server** field, enter the unique name of a file server to export. The name cannot contain characters other than letters, numbers, period, hyphen, and underscore; the double quote (") is not allowed in the name.

To preposition a DFS share, enter the DFS workspace name and the file server name. The DFS share can be either a domain name or a domain IP address and can accept a maximum of one forward slash (/) character (/) and one period, for example, **google.com/namespace**.

> **Note** The configuration of one forward slash character (/) and one period is only for devices for Cisco WAAS Software Version 6.4.3 and later. The Cisco WAAS Central Manager Device Group lists only the devices that have the appropriate software version.

Step 8 From the **Nearest Device** drop-down list, choose the device location that will provide browsing services for the file server. Normally, this is the Cisco data center WAE. For optimum browsing performance, specify a location that is close to the file server.

The location is used only for browsing; each Cisco Edge WAE retrieves prepositioned files directly from the file server, not from this location. For more information on defining locations, see Working with Device Locations in the chapter "Using Device Groups and Device Locations."

Step 9 In the **User name**, **Password**, and **Confirm Password** fields, enter the username and password credentials for the file server.

Consider the following naming guidelines:

- If the username is in a Microsoft Windows domain, specify the domain name in the **Domain name** field.
- The access credentials that you enter must allow read access to the prepositioned root directories and to their parent directories.
- The following characters cannot be used in **usernames** ; | && || : \ / * ? < > + = , [ ] “ ` !.
- The following characters cannot be used in **server names** ; | && || , ~ : ! ` @ # $ % ^ & ‘ { } ( ) _ “
- The following characters cannot be used in **domain names** ; | && || : \ / * ? < > “ ` !

Step 10 Under **Content Settings**, in the **Root Share and Directories** field, enter the directories on the file server that you want to export. Use any of the following methods to identify a directory:

- Manually enter one or more directory paths in the following format: **protocol://server/share** or **server\share**, for example, **smb://win12srv/home** or **win12srv\home**. You can enter multiple lines for multiple directories, with each full directory path on its own line. You cannot specify the root directory (/) as a root share. Special characters like ; | && || : * ? < > " ` ! [ ] + = , are not allowed for top level shares. Additionally, when you create subdirectories inside the shares, the following special characters are not allowed: ; | && || : * ? < > " ` !

  > **Note** Do not use the special character ";" in files and directory names, because it will generate errors. Additionally, Cisco WAAS Version 6.2.1 does not support extended Unicode characters in files and directories. These files or directories will skipped and not prepositioned.

When you define multiple root shares, the preposition sequence that is performed for a single root configuration is repeated for each root serially.

- Click **Browse** to browse the directories on the file server. To navigate to a directory, click the File Folder icon to the left of the directory name. Check the check box next to the directory that you want to export and then click **Select Directory**. The **Browse** window allows you to choose multiple directories.

  The **Browse** function operates best when you choose the location of the nearest SMB accelerator to the file server from the **Location** drop-down list. If you do not choose a location, the browse request is sent to all the devices that have the SMB accelerator enabled, and the request may time out.

- To include all the subdirectories under the specified root directory, check the **Include Sub Directories** check box. If this option is not selected, only the files in the specified root directory are prepositioned and you cannot select subdirectories when you are browsing.

- To narrow the policy definition to a particular type of file, choose a pattern operator from the **File Name** drop-down list, and enter the text that describes the pattern in the adjacent text box, for example, enter: ends with .doc. Do not use a space or the following special characters: ; | && || : * ? < > \ / " ` !

Step 11 By default, a **Now** schedule begins (if the status is enabled) each time you make a change to the **Preposition Directives** window. A new schedule also begins as soon as a Cisco Edge device that has been reloaded comes back online.

- **Not-Scheduled**: This option is displayed by default.
- **Immediate**: Prepositioning occurs within a few minutes after you click **OK** in the **Schedule** dialog box.
- **Date**: Prepositioning occurs at the defined time and date.
- **Daily**: Prepositioning occurs daily at the defined time.
- **Weekly**: Prepositioning occurs on the selected days of the week at the defined time.
- **Monthly Days**: Prepositioning occurs on the selected days of the month at the defined time.
- **Monthly WeekDays**: Prepositioning occurs on the selected month weekdays at the defined time.

Step 12 Specify the preposition start time from the **Start Time** drop-down list.

- The time is expressed in 24-hour format with **00:00** representing midnight.
- The time refers to the local time of the Cisco Edge WAE where the data is to be prepositioned.
- If there are multiple Cisco Edge WAEs in different time zones, the time refers to the local time of the Cisco Core WAE.

Step 13 Click **OK**.

The directive is saved and is added to the **Preposition Directive** table.

Assigning Edge Devices to a Preposition Directive for SMB Files

Before you begin

- After you create a preposition directive, you need to assign Cisco Edge WAEs or device groups to the directive. This task determines which Cisco Edge WAEs will store preposition content in their cache.
- Prepositioning includes the ability to configure multiple roots. For more information, see .Creating a Preposition Directive for SMB Files, on page 362
- After you create a preposition directive, you need to assign Edge WAEs or device groups to the directive. This task determines which Edge WAEs will store-preposition content in their cache.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **SMB File Services** > **Preposition**.

The **Preposition Directives** window appears, which lists the preposition directives that exist on the system.

Step 2 Select the appropriate Preposition Directive to assign it to the Device or Device Group, and click the **Assign Devices/ Device Groups** icon.

The **Assign Device/Device Groups Assignments** window appears. This window lets you filter your view of the items in the list. Filtering enables you to find items in the list that match the criteria that you set.

Step 3 Choose the Cisco Edge WAEs or device groups to assign to this preposition directive, and then click **Assign**.

The **Assigned Status** column changes to **Assigned** next to the selected device or device group. You can also un-assign a device or device group by clicking **Unassign**. The **Assigned Status** column changes to **Not Assigned**.

Step 4 If there is a delay in sending the preposition details to the device, the **Assigned Status** column displays **Notify Updates In-Progress** for the device or device group.

Step 5 To see a change in status after the preposition changes have been made to the device, click **Refresh**.

Step 6 Consider the following operating guidelines:

- If a device or device group is offline (identified by a red "X"), then you cannot assign that device or group to this directive. The preposition directive, when assigned to a device group, is applied only to connected Cisco Edge devices in the assigned device group.
- When assigning a SMB accelerator preposition directive to a device group, the directive is applied only to those devices enabled for SMB acceleration in the assigned device group.
- If the SMB accelerator is disabled on a Cisco WAE, the SMB accelerator preposition task will fail with error that SMB accelerator is not enabled on the Cisco WAE.

Step 7 Click **OK**.

Creating a Preposition Schedule for SMB Files

Before you begin

After you create a preposition directive and assign Cisco WAEs to the directive, create a schedule that determines when and how often prepositioning occurs.

Example:

You may want to schedule prepositioning to occur at night to minimize the amount of traffic during business hours, or, you may want to schedule prepositioning to occur on a recurring basis if the exported data changes often. This will help ensure that the Cisco WAEs assigned to this directive have the latest file updates in their cache.

Consider the following guidelines for specifying a start time:

- The time is expressed in 24-hour format with **00:00** representing midnight.
- The time refers to the local time of the Cisco Edge WAE where the data is to be prepositioned.
- When a preposition task is scheduled to begin at the same time for multiple Cisco Edge WAEs that are located in different timezones, the task will begin on the Cisco Edge WAEs based on the Cisco Core WAE timezone.
- If the clocks of the Cisco Edge WAE and the Cisco Core WAE are not synchronized, the task will not start on time.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure > SMB File Services > Preposition**.

The **Preposition Directives** window appears, which lists the preposition directives that exist on the system.

Step 2 Click the **Edit** icon next to the preposition directive for which you want to create a schedule.

Step 3 Click the **Schedule** tab at the top of the window.

The **Creating New Preposition Schedule** window appears. By default, no schedule is configured.

Step 4 Choose one of the following scheduling options:

- **Not Scheduled**: Prepositioning is not scheduled at this time.
- **Now**: Prepositioning occurs within a few minutes after you submit this schedule.

  A **Now** schedule begins again each time you make a change to the preposition directive and click **Submit**.

  A **Now** schedule also begins again as soon as a Cisco Edge device that has been reloaded comes back online.
- **Daily**: Prepositioning occurs daily at the defined time.
- **Date**: Prepositioning occurs at the defined time and date.
- **Weekly**: Prepositioning occurs on the selected days of the week at the defined time.
- **Monthly Days**: Prepositioning occurs on the selected days of the month at the defined time.

- **Monthly Weekdays**: Prepositioning occurs on the defined day (as opposed to a defined date) and time during the month. For example, you can schedule prepositioning to occur on the second Tuesday of every month.

Step 5 Specify a start time for the prepositioning task.

Consider the following guidelines for specifying a start time:

- The time is expressed in 24-hour format with 00:00 representing midnight.
- The time refers to the local time of the Cisco Edge WAE where the data is to be prepositioned.
- If there are multiple Cisco Edge WAEs in different time zones, the time refers to the local time of the Cisco Core WAE.
- You cannot schedule a start time for the **Now** option.

Step 6 Click **Submit**.

To confirm that your schedule has been saved, the **Changes Submitted** message is displayed at the bottom of the window.

Step 7 Verify that the preposition directive has completed successfully by checking the preposition status. For more information, see Checking the Preposition Task Status of SMB Files, on page 369.

Checking the Preposition Task Status of SMB Files

Before you begin

After you create one or more preposition directives, you can verify the status of all the preposition tasks to ensure that they are completed successfully. If a task does not complete successfully, then some of the prepositioned files may have not been copied to the Cisco Edge WAE cache.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **SMB File Services** > **Preposition**.

The **Preposition Directives** window, which lists the preposition directives that exist on the system, appears.

Step 2 Select the SMB preposition directive that you want to check and click the **Collect Preposition Status** tab at the top of the window.

The **Preposition Status** window displays the following information:

- **WAE**: The name of each Edge WAE that received the prepositioned files in its cache.
- **Start Time**: The time the preposition task started.
- **Duration**: The amount of time it took the preposition task to be completed.
- **Amount Copied**: The amount of data copied to the WAE cache, in bytes.
- **Status**: Whether the preposition task is completed successfully.

- **Error Reason**: The reason a preposition task failed.

Verify that the **Status** column shows **Completed**.

If this column shows **Failure**, look in the **Reason** column for an explanation that can help you troubleshoot why the preposition task failed. After resolving the issue, you can schedule the preposition task to run again now, or wait until the scheduled start time and verify the status again later.

Step 3 Click **OK**.

You can also export this data and save it to your local machine.

CHAPTER 12

Configuring Application Acceleration

This chapter describes how to configure the optimization policies, which determine the types of application traffic that is accelerated over your WAN on your Cisco WAAS system.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco Wide Area Application Services (Cisco WAAS) Central Managers and Cisco Wide Area Application Engines (WAEs) in your network. The term WAE refers to WAE and Cisco Wide Area Virtualization Engine (WAVE) appliances, and Cisco Virtual WAAS (vWAAS) instances.

This chapter contains the following sections:

About Application Acceleration

The Cisco WAAS software comes with more than 150 predefined optimization policies that determine the type of application traffic your Cisco WAAS system optimizes and accelerates. These predefined policies cover the most common type of application traffic on your network. For a list of the predefined policies, see Appendix A, "Predefined Optimization Policy."

Each optimization policy contains the elements shown in the following table:

Table 40: Optimization Policy Elements

Optmization Policy Element	Description
Application Definition	Identifies general information about a specific application, such as the application name and whether the Cisco WAAS Central Manager collects statistics about this application.

Optmization Policy Element	Description
Class Map	Contains a matching condition that identifies specific types of traffic. For example, the default HTTP class map matches all the traffic going to ports 80, 8080, 8000, 8001, and 3128. You can create up to 512 class maps and 800 matching conditions.
Policy	Combines the application definition and class map into a single policy. This policy also determines the optimization and acceleration features, if any, that a Cisco WAAS device applies to the defined traffic. You can create up to 512 policies. A policy can also contain a Differentiated Services Code Point (DSCP) marking value that is applied to the traffic and that overrides a DSCP value set at the application or global level.

You can use the Cisco WAAS Central Manager GUI to modify the predefined policies and to create additional policies for other applications. For more information on creating optimization policies, see Creating a New Traffic Optimization Policy. For more information on viewing reports, restoring policies, monitoring applications, and other functions, see Managing Application Acceleration.

Note All application definitions configured in the Cisco WAAS Central Manager are globally applied to all the Cisco WAAS devices that register with the Cisco WAAS Central Manager, regardless of the device group membership configuration.

Cisco WAAS policies can apply two kinds of optimizations to matched traffic:

- Layer 4 optimizations that include Transport Flow Optimization (TFO), Data Redundancy Elimination (DRE), and Lempel-Ziv (LZ) compression. These features can be applied to all types of TCP traffic.
- Layer 7 optimizations that accelerate application-specific protocols. The application accelerators control these kinds of optimizations.

For a specified optimization policy, for Cisco WAAS Version 4.4.1 and later, the DRE feature can use different caching modes, shown in the following table.

Table 41: DRE Caching Modes

DRE Caching Mode	Description
Bidirectional	The peer Cisco WAEs maintain identical caches for inbound and outbound traffic. This caching mode is best suited for scenarios where a significant portion of the traffic seen in one direction between the peers is also seen in the reverse direction. For Cisco WAAS versions earlier than Cisco WAAS Version 4.4.1, bidirectional mode is the only supported caching mode.

DRE Caching Mode	Description
Unidirectional	The peer Cisco WAEs maintain different caches for inbound and outbound traffic. This caching mode is best suited for scenarios where a significant portion of the traffic seen in one direction between the peers is not seen in the reverse direction.
Adaptive	The peer Cisco WAEs negotiate either bidirectional or unidirectional caching based on the characteristics of the traffic seen between the peers.

The predefined optimization policies are configured to use the optimal DRE caching mode, depending on the typical application traffic, although you can change the mode if you want.

Enabling and Disabling the Global Optimization Features

This section contains the following topics:

About Global Optimization Features

The global optimization features determine if traffic flow optimization (TFO), data redundancy elimination (DRE), and persistent compression are enabled on a device or device group. By default, all of these features are enabled. If you choose to disable one of these features, the device will be unable to apply the full Cisco WAAS optimization techniques to the traffic that it intercepts.

In addition, the global optimization features include each of the following application accelerators:

- Microsoft End Port Mapper (EPM)
- HyperText Transfer Protocol (HTTP)
- Independent Computing Architecture (ICA)
- Messaging Application Programming Interface (MAPI)
- Server Message Block (SMB)
- Secure Sockets Layer (SSL)
- SSL Interposer

By default, all of the application accelerators are enabled except SMB, SSL Interposer and Encrypted MAPI.

Note The application accelerators require specific types of licenses to operate: a Transport license for TFO, DRE, and LZ optimization, and an Enterprise license for all other application accelerators. For more information on installing and managing licenses, see the chapter "Configuring Other System Settings, on page 289".

Procedure for Enabling and Disabling the Global Optimization Features

Before you begin

- You must enable the accelerator on both of the peer Cisco WAEs at either end of a WAN link for all application accelerators to operate, except for single-sided SMART-SSL acceleration.
- In the case of single-sided SMART-SSL acceleration, you do not need a peer Cisco WAE to exist or for both Cisco WAEs to have the SSL Interposer accelerator enabled.

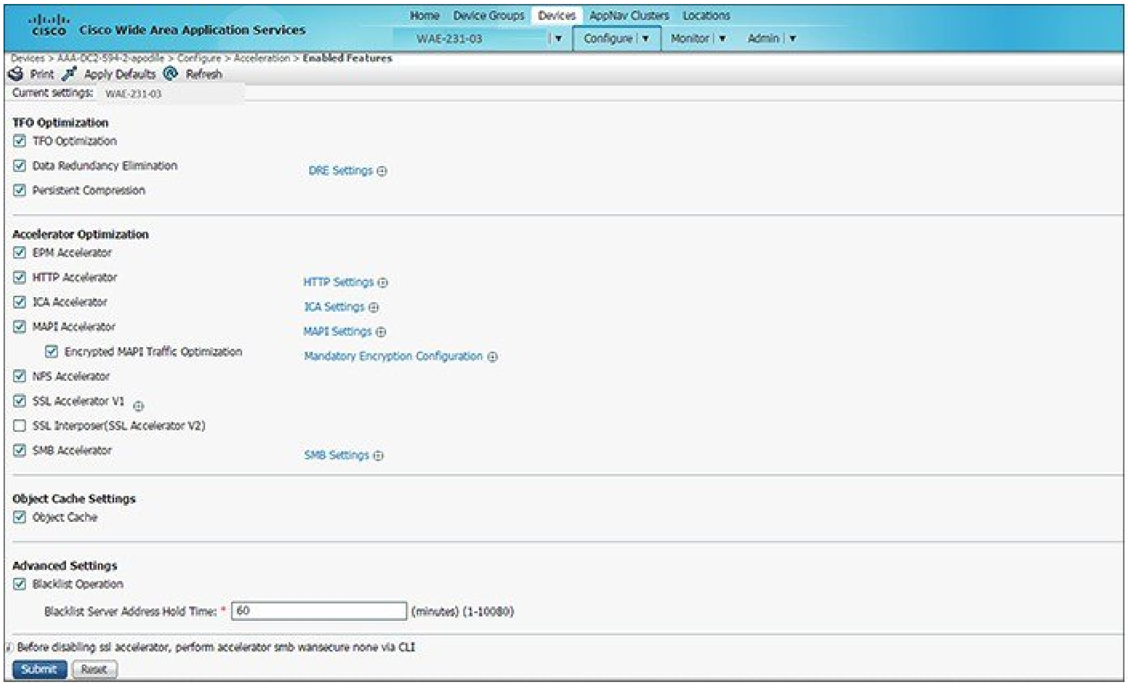
Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **Enabled Features**.

The **Enabled Features** window appears.

Figure 50: Enabled Features Window



Current settings: WAE-231-03

TFO Optimization

☑ TFO Optimization

☑ Data Redundancy Elimination — DRE Settings

☑ Persistent Compression

Accelerator Optimization

☑ EPM Accelerator

☑ HTTP Accelerator — HTTP Settings

☑ ICA Accelerator — ICA Settings

☑ MAPI Accelerator — MAPI Settings

☑ Encrypted MAPI Traffic Optimization — Mandatory Encryption Configuration

☑ NFS Accelerator

☑ SSL Accelerator V1

□ SSL Interposer(SSL Accelerator V2)

☑ SMB Accelerator — SMB Settings

Object Cache Settings

☑ Object Cache

Advanced Settings

☑ Blacklist Operation

Blacklist Server Address Hold Time: * 60 (minutes) (1-10080)

Before disabling ssl accelerator, perform accelerator smb wansecure none via CLI

For Cisco WAAS Express Devices:

- On Cisco WAAS Express devices, only a subset of the standard features are available. On Cisco ISR-WAAS devices, the SMB application accelerator is enabled by default.

  In the **Enabled Features** window for a device group, two SMB Accelerator options are shown, one for Cisco ISR-WAAS devices and one for all other kinds of Cisco WAEs.

- Not all of the properties in the standard Cisco WAAS device are available in the Cisco WAAS Express version of the application accelerators, including SMART-SSL acceleration.

- For Cisco WAAS Express, the following Express versions of application accelerators are supported:
  - HTTP accelerator express (see Configuring HTTP Acceleration)
  - SSL accelerator express (see Configuring SSL Acceleration)
- For a Cisco WAAS device running Cisco WAAS Version 6.x and a Cisco WAAS Express peer device running Cisco IOS Release 15.6(3)M, 15.6(2)T1 or later, TLS1 is supported, but SSL3 is removed. Before upgrading Cisco WAAS Express to one of these Cisco IOS releases, configure TLS1 in the Cisco WAAS Express Device Group:

  a. Navigate to **Device Groups** > *DeviceGroupName* > **Configure** > **Enabled Features**.

  b. Select the **SSL Accelerator Express Peering Service**.

  c. From the **SSL Version:** dropdown list, choose **TLS1**.

  d. Click **Submit**.

  e. Upgrade the Cisco WAAS Express.
- For information on upgrading and interoperability, see the Release Note for Cisco Wide Area Application Services.
- If you try to enable DRE on a Cisco WAAS Express device on which it is not supported, a message stating that it is not supported is displayed.
- The **Restore Predefined Settings** icon for Cisco WAAS Express applies the predefined settings for HTTP/HTTPS, and SSL cipher list and peering service.

Step 3 Check the check boxes adjacent to the optimization features that you want to enable, and uncheck the check boxes adjacent to the features that you want to disable.

For a description of each of the optimization features, see Key Services of Cisco WAAS in the chapter "Introduction to Cisco WAAS."

Some features have additional settings that you can configure by clicking the link next to the setting name. Hover your cursor over the small target icon next to the link to see a dialog box that shows the current settings.

- If you check the **Data Redundancy Elimination** check box, you can click the DRE Settings link as a shortcut to the **DRE Settings Configuration** window. For more information, see Configuring DRE Settings, on page 379.
- If you check the **HTTP Accelerator** check box, you can click the HTTP Settings link as a shortcut to the **HTTP/HTTPS Settings** window. For more information, see Procedure for Configuring HTTP Acceleration, on page 380.
- If you check the **ICA Accelerator** check box, you can click the ICA Settings link as a shortcut to the **ICA Acceleration Configuration** window. For more information, see Procedure for Configuring ICA Acceleration, on page 405.
- If you check the **MAPI Accelerator** check box, you can click the MAPI Settings link as a shortcut to the **MAPI Settings** window. For more information, see About MAPI Acceleration.

  When you check the **MAPI Accelerator** check box, **Encrypted MAPI Traffic Optimization** is enabled by default.

- If you check the **Encrypted MAPI Traffic Optimization** check box, you can click the **Mandatory Encryption Configuration** link as a shortcut to the **Encrypted Services Configuration** window. For more information, see Configuring Encrypted MAPI Acceleration.

  Note For Encrypted MAPI acceleration to be enabled, you must *first* enable MAPI acceleration.

- If you check the **SMB Accelerator** check box, you can click the SMB Settings link as a shortcut to the **SMB Acceleration Configuration** window. For more information, see Configuring SMB Acceleration.
- If you check the **SSL Accelerator** check box, you must configure additional settings to enable SSL acceleration. For more information, see Configuring SSL Acceleration, on page 407. For Cisco Version 6.2.1 and later, you can accelerate Microsoft Office 365 traffic. For more information, see Configuring Microsoft Office 365 for Cisco WAAS.
- If you check the **SSL Interposer (SSL Accelerator V2)** check box, you must configure additional settings to enable SMART-SSL acceleration. By default, the SSL Interposer is by default SMART SSL will be enabled on a fresh installation, that is, on new OVA deployments, ENCS platforms, 5.5.7 to 6.4.1 upgrades. It will be disabled when you upgrade the devices from Cisco WAAS Software Version 6.2.3 to 6.4.1. For more information, see Configuring SMART-SSL Acceleration.

  Both SSL accelerator and SMART-SSL can co-exist on a device.

Step 4 To enable the object cache, at the **Object Cache Settings** pane, check the **Object Cache** check box.

Cisco WAAS performs object caching to increase client application performance for SMB file access. Object caching also minimizes bandwidth and latency over the WAN, by avoiding the repeated transfer of data over the WAN.

Note Object Cache is not supported on Cisco vWAAS-200 and Cisco vWAAS-150 platforms.

- To enable an individual application accelerator object cache: Controls to enable and disable an individual object cache are displayed in that application accelerator's **Advanced Settings** screen.
- To ensure that the object cache and individual application accelerator object cache work successfully, consider these guidelines:
  - Each application accelerator object cache can be enabled or disabled independent of whether or not the global object cache is enabled or disabled.
  - Enabling the object cache does not automatically enable individual application accelerator object caches.
  - You can enable or disable an individual application accelerator object cache whether or not the associated application accelerator is enabled or disabled.
  - Verify that disk assignments have been made to object cache before you enable object cache.
  - The object cache has a limit of 15 GB. A request of a size larger than this limit will not cache the complete file. For example, for a file size of 25 GB, only 15 GB of this file would be cached.

Note To ensure that the object cache and SMB application accelerator work successfully, enable the object cache *before* you enable the SMB application accelerator.

Step 5 At the **Advanced Settings** pane, uncheck the **Blacklist Operation** check box if you want to disable it.

The **blacklist operation** feature allows a Cisco WAE to better handle situations in which TCP setup packets that have options are blocked or not returned to the Cisco WAE device.

This behavior can result from network devices (such as firewalls) that block TCP setup packets that have options, and from asymmetric routes. The Cisco WAE can keep track of origin servers (such as those behind firewalls) that cannot receive optioned TCP packets, and learns not to send out TCP packets with options to these blacklisted servers.

Cisco WAAS is able to accelerate traffic between Cisco branch WAEs and Cisco data center WAEs in situations where optioned TCP packets are dropped. We recommend that you leave the **blacklist operation** feature enabled.

Step 6 To change the default Blacklist Server Address Hold Time of 60 minutes, enter the new time in minutes in the **Blacklist Server Address Hold Time** field. The valid range is 1 minute to 10080 minutes (1 week).

When a server IP address is added to the blacklist, it remains there for the configured hold time. After that time, subsequent connection attempts will again include TCP options so that the WAE can redetermine if the server can receive them. It is useful to retry sending TCP options periodically because network packet loss may cause a server to be erroneously blacklisted.

You can shorten or lengthen the blacklist time by changing the **Blacklist Server Address Hold Time** field.

Step 7 Click **Submit**.

The changes are saved to the device or device group.

Configuring Optimization and Acceleration from the Cisco WAAS CLI

This section contains the following topics:

Global Configuration Commands Used to Configure Optimization and Acceleration

The following table shows the Cisco WAAS CLI global configuration commands used to configure optimization and acceleration.

Table 42: Cisco WAAS CLI Commands Used to Configure Optimization and Acceleration

Command Mode	Command	Optimization or Acceleration Configuration Task
Global Configuration	**tfo optimize**	Configure TFO optimization, DRE, and persistent compression.
	accelerator epm	Configure EPM acceleration.
	accelerator http	Configure HTTP acceleration.
	accelerator ica	Configure ICA acceleration.
	accelerator mapi	Configure MAPI acceleration.
	accelerator smb	Configure SMB acceleration.
	accelerator ssl	Configure SSL acceleration.
	object-cache enable	Configure global object cache.
	accelerator *ao-name* **object-cache enable**	Enable a specified application accelerator object cache.
	auto-discovery	Configure the Blacklist Operation feature.
EXEC	**show accelerator**	Display the status of the application accelerators.
	show statistics accelerator	Display statistics for the application accelerators.
	show statistics accelerator smb	Display statistics for the SMB print accelerator.

Optimization and Acceleration Configuration Guidelines

Consider the following guidelines for configuring optimization and acceleration:

- When object cache is enabled, you are prompted to confirm the repurposing of SMB resources if the disk has not already been partitioned for object cache.
- If this is the first time disk resources are being assigned to object cache, the **object-cache enable** command will prompt you to reboot the device, since the disk partitioning only takes effect on the next reboot. The configuration is then saved, and the object cache does not have to be re-enabled on the next reboot.
- To ensure success of the **object-cache enable** global configuration command, verify the following two conditions:
    - Disk assignments have been made to object cache *before* you run this command.
    - Run this command *before* you run the **accelerator smb** global configuration command.
- To ensure that each application accelerator object cache and the global object cache function successfully, note these guidelines:
    - Each application accelerator object cache can be enabled or disabled independent of whether or not the global object cache is enabled or disabled.

- Before you run the **no object-cache enable** global configuration command to disable the global object cache, you must disable *all* individual application accelerator object caches.
- The **object-cache enable** global configuration command does not automatically enable individual application accelerator object caches.
- You can enable or disable an individual application accelerator object cache whether or not the associated application accelerator is enabled or disabled.

Configuring Individual Features and Application Accelerators

This section contains the following topics:

Configuring DRE Settings

Before you begin

Data Redundancy Elimination (DRE) is one of the critical technologies used to identify redundant data patterns in application traffic, replacing them with signatures that Cisco WAAS devices transfer across the WAN to regenerate the original data. The result is optimal usage of WAN bandwidth and improved end-user response time.

To enable DRE settings: in the **Enabled Features** window, check the **Data Redundancy Elimination** check box.

Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **DRE Settings**.

The **DRE Settings** window appears.

Step 3 To generate an alarm and automatically DRE bypass application traffic, check the **Enable DRE auto bypass** check box.

Note If you do not enable DRE auto bypass, the **Device Status** alarm displays yellow and the traffic gets bypassed without forwarding to the Service Node (SN). We recommend that you do not disable DRE through the configuration. Instead, configure individual policies to bypass DRE functionality.

Step 4 To enable load report, check the **Enable DRE Load Monitor** check box.

- The disk latency maximum can be set from **1** to **1000**; the default value is **5**.
- The DRE load threshold can be set from **50** to **99**; the default value is **95**.

Step 5 Click **Submit**.

The changes are saved to the device or device group.

Step 6 To use the Cisco WAAS CLI to enable DRE settings:

- To enable DRE auto bypass from the CLI, run the **dre auto-bypass enable** global configuration command.
- To enable DRE load monitor from the CLI, run the **dre load-monitor report** global configuration command.

Configuring HTTP Acceleration

This section contains the following topics:

Procedure for Configuring HTTP Acceleration

Before you begin

The HTTP application accelerator accelerates HTTP traffic. To optimize HTTPS, you must enable both SSL and HTTP and also have protocol chaining enabled.

The default Web Optimization policy is defined to send traffic to the HTTP accelerator. The Web optimization policy uses the HTTP class map, which matches traffic on ports 80, 8080, 8000, 8001, and 3128. If you expect HTTP traffic on other ports, add the other ports to the HTTP class map.

Procedure

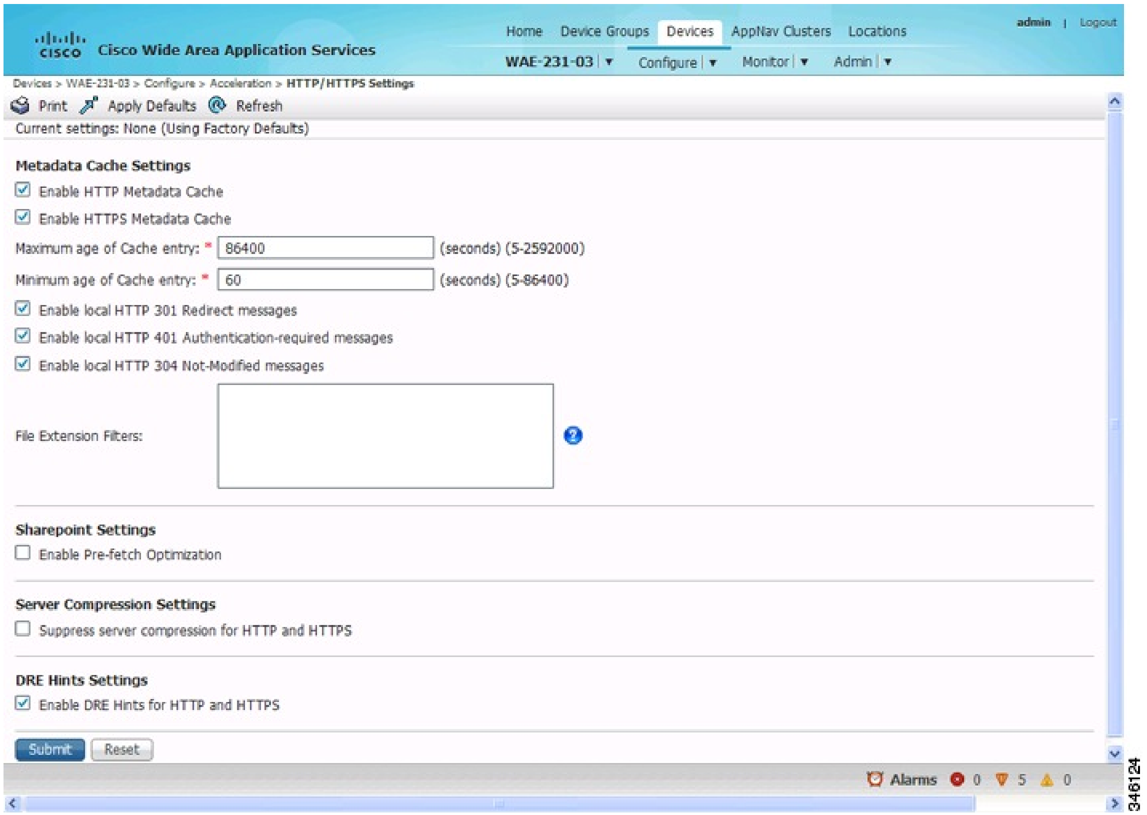
Step 1 To enable the HTTP accelerator: at the **Accelerator Optimization** pane of the **Enabled Features** window, check the **HTTP Accelerator** check box.

Step 2 From the Cisco WAAS Central Manager menu, choose **Devices >** *device-name* or **Device Groups >** *device-group-name*.

Step 3 Choose **Configure > Acceleration > HTTP/HTTPS Settings**.

The **HTTP/HTTPS Acceleration Settings** window appears.

Figure 51: HTTP/HTTPS Settings Window


Cisco Wide Area Application Services
Home Device Groups Devices AppNav Clusters Locations
admin | Logout
WAE-231-03 ▾ Configure ▾ Monitor ▾ Admin ▾
Devices > WAE-231-03 > Configure > Acceleration > HTTP/HTTPS Settings
Print Apply Defaults Refresh
Submit Reset
Alarms 0 5 0
346124

Current settings: None (Using Factory Defaults)

Metadata Cache Settings

☑ Enable HTTP Metadata Cache

☑ Enable HTTPS Metadata Cache

Maximum age of Cache entry: * 86400 (seconds) (5-2592000)

Minimum age of Cache entry: * 60 (seconds) (5-86400)

☑ Enable local HTTP 301 Redirect messages

☑ Enable local HTTP 401 Authentication-required messages

☑ Enable local HTTP 304 Not-Modified messages

File Extension Filters:

Sharepoint Settings

□ Enable Pre-fetch Optimization

Server Compression Settings

□ Suppress server compression for HTTP and HTTPS

DRE Hints Settings

☑ Enable DRE Hints for HTTP and HTTPS

Note For Cisco WAAS Express, the HTTP acceleration settings are the same, but the fields are laid out differently in the **HTTP/HTTPS Settings** window.

Step 4 Configure the metadata cache settings. At the **Metadata Cache Settings** pane:

a) To enable the Cisco WAE to cache each HTTP header (metadata) information, check the **Enable HTTP metadatacache caching** check box. The default setting is checked.

This check box *must* be checked to enable any of the other settings in the **Metadata Cache Settings** pane. If this box is not checked, no header caching is done.

For more information, see HTTP Metadata Caching.

b) To enable the Cisco WAE to cache HTTPS header (metadata) information (HTTP as payload in SSL traffic), check the **Enable HTTPS metadatacache caching** check box. The default setting is checked.

For more information, see HTTP Metadata Caching.

c) In the **Maximum age of a cache entry** field, enter the maximum number of seconds to retain HTTP header information in the cache. The default is **86,400 seconds (24 hours)**. Valid time periods range from 5–2,592,000 seconds (30 days).

d) In the **Minimum age of a cache entry** field, enter the minimum number of seconds for which to retain HTTP header information in the cache. The default is **60 seconds**. Valid time periods range from 5 to 86,400 seconds (24 hours).

e) To enable the Cisco WAE to cache and to locally serve HTTP 301 messages, check the **Enable local HTTP 301 redirect messages** check box. The default setting is checked.

f) To enable the Cisco WAE to cache and locally serve HTTP 401 messages, check the **Enable local HTTP 401 Authentication-required messages** check box. The default setting is checked.

g) To enable the Cisco WAE to cache HTTP 200 and HTTP 304 messages and locally serve HTTP 304 messages, check the **Enable local HTTP 304 Not-Modified messages** check box. The default setting is checked.

h) To configure specific file extensions to which metadata caching is to be applied, enter the file extensions in the **File extension filters** field at the far right of the window. Separate multiple extensions with a comma, for example, jpeg, gif, png, and do not include the dot at the beginning of the file extension.

By default, no file extension filters are defined and therefore, metadata caching applies to all file types.

Step 5 To allow the Cisco WAAS Edge WAE to prefetch data, at the **Sharepoint Settings** pane, check the **Enable Pre-fetch Optimization** check box. The default for this setting is unchecked.

- The prefetch optimization benefits the Web browser-based Microsoft Office applications when they access Microsoft Office Word and Microsoft Office Excel documents that are hosted on a Microsoft SharePoint Server 2010. To view Microsoft Word documents, you must have Microsoft Silverlight installed on your system.
- By checking the Enable Pre-fetch Optimization check box, you are directing the Cisco WAAS Edge WAE to prefetch the subsequent pages of the documents from the SharePoint server before the client actually requests them, and serve them from the cache when the request from the client arrives. You can now seamlessly scroll through the document without having to wait for the content to load.

Note SharePoint prefetch optimization works with view in browser mode only.

Step 6 Check the **Suppress server compression for HTTP and HTTPS** check box to configure the WAE to suppress server compression between the client and the server. The default setting is checked.

By checking this check box, you are telling the WAE to remove the **Accept-Encoding** value from HTTP and HTTPS request headers, preventing the web server from compressing HTTP and HTTPS data that it sends to the client. This allows the WAE to apply its own compression to the HTTP and HTTPS data, typically resulting in much better compression than the web server for most files. For some file types that rarely change, such as .css and .js files, this setting is ignored and web server compression is allowed.

Step 7 To configure the Cisco WAE to suppress server compression between the client and the server, at the **Server Compression Settings** pane, check the **Suppress server compression for HTTP and HTTPS** check box. The default setting is checked.

- By checking the **Suppress server compression for HTTP and HTTPS** check box, you are directing the Cisco WAE to remove the Accept-Encoding value from HTTP and HTTPS request headers, which prevents the web server from compressing HTTP and HTTPS data that it sends to the client. This allows the Cisco WAE to apply its own compression to the HTTP and HTTPS data, which typically results in more optimum compression than that of the web server, for most files.
- For some file types that rarely change, such as.css and.js files, this setting is ignored and web server compression is allowed.

Step 8 To send DRE hints to the DRE module for improved DRE performance, at the **DRE Hints Settings** pane, check the **Enable DRE Hints for HTTP and HTTPS** check box. The DRE hint feature is enabled by default.

Step 9 Click **Submit**.

The changes are saved to the device or device group.

What to do next

To configure HTTP acceleration from the CLI, run the **accelerator http** global configuration command.

To show the contents of the metadata cache, run the **show cache http-metadatacache** EXEC command.

To clear the metadata cache, run the **clear cache http-metadatacache** EXEC command.

To enable or disable specific HTTP accelerator features for specific clients or IP subnets, run the HTTP accelerator subnet feature. For more details, see Using an HTTP Accelerator Subnet, on page 383.

HTTP Metadata Caching

The metadata caching feature allows the HTTP accelerator in the branch WAE to cache particular server responses and respond locally to clients. The following server response messages are cached:

- **HTTP 200 OK** (Applies to **If-None-Match** and **If-Modified-Since** requests)
- **HTTP 301 redirect**
- **HTTP 304 not modified** (Applies to **If-None-Match** and **If-Modified-Since** requests)
- **HTTP 401 authentication required**

Metadata caching is not applied in the following cases:

- Requests and responses that are not compliant with RFC standards
- URLs containing over 255 characters
- 301 and 401 responses with cookie headers
- Use of HEAD method
- Pipelined transactions

Using an HTTP Accelerator Subnet

Before you begin

The HTTP accelerator subnet feature allows you to selectively enable or disable specific HTTP optimization features for specific IP subnets by using ACLs. This feature can be applied to the following HTTP optimizations: HTTP metadata caching, HTTPS metadata caching, DRE hints, and suppress server compression.

To define IP subnets, use the **ip access-list** global configuration command. Refer to this command in the *Cisco Wide Area Application Services Command Reference* for more information on configuring subnets. You can use both standard and extended ACLs.

Procedure

Step 1 Enable global configuration for all the HTTP accelerator features that you want to use.

Step 2 Create an IP access list to use for a subnet of traffic:

```
WAE(config)# ip access-list extended md_acl
WAE(config-ext-nacl)# permit ip 1.1.1.0 0.0.0.255 any
WAE(config-ext-nacl)# permit ip 2.2.2.0 0.0.0.255 3.3.3.0 0.0.0.255
WAE(config-ext-nacl)# exit
```

Step 3 Associate the ACL with a specific HTTP accelerator feature. For more information on associating an ACL with an HTTP accelerator feature, see the **accelerator http** global configuration command in the *Cisco Wide Area Application Services Command Reference*:

```
WAE(config)# accelerator http metadatacache access-list md_acl
```

In this example, the HTTP metadata cache feature applies to all the connections that match the conditions specified in the extended **access-list md_acl**.

What to do next

In the following example, the HTTP suppress-server-encoding feature applies to all the connections that match the conditions specified in the standard access-list 10:

```
WAE(config)# ip access-list standard 10
WAE(config-std-nacl)# permit 1.1.1.0 0.0.0.255
WAE(config-std-nacl)# exit
WAE(config)# accelerator http suppress-server-encoding accesslist 10
```

For the features (DRE hints and HTTPS metadata cache in this example) that do not have an ACL associated with them, global configuration is used and the features are applicable to all the connections.

Configuring MAPI Acceleration

This section contains the following topics:

About MAPI Acceleration

Consider the following MAPI acceleration features and guidelines:

- The MAPI application accelerator accelerates Microsoft Outlook Exchange traffic that uses the Messaging Application Programming Interface (MAPI) protocol.
  - For Cisco WAAS Version 5.3.x and later, Microsoft Outlook 2000 to 2013 clients are supported.
  - For Cisco WAAS Version 5.2.x and earlier, Microsoft Outlook 2000 to 2010 clients are supported.
- Clients can be configured with Outlook in cached or noncached mode; both modes are accelerated.
- Secure connections that use message authentication (signing) are not accelerated.
- Microsoft Outlook 2007 and 2010 have encryption enabled by default. You must disable encryption to benefit from the MAPI application accelerator.
- MAPI accelerator and the EPM accelerator:
  - The EPM application accelerator must be enabled for the MAPI application accelerator to operate. EPM is enabled by default. Additionally, the system must define an optimization policy of type

EPM, specify the MAPI UUID, and have an Accelerate setting of MAPI. This policy, MAPI for the Email-and-Messaging application, is defined by default.

- EPM traffic, such as MAPI, does not normally use a predefined port. If your Microsoft Outlook administrator has configured Microsoft Outlook in a nonstandard way to use a static port, you must create a new basic optimization policy that accelerates MAPI traffic with a class map that matches the static port that was configured for Microsoft Outlook.

- If the Cisco WAE becomes overloaded with connections, the MAPI application accelerator continues to accelerate MAPI connections by using internally reserved connection resources. If the reserved resources are also exceeded, new MAPI connections are passed through until connection resources become available.

- When you enable MAPI acceleration, Encrypted MAPI acceleration is enabled by default. For more information on Encrypted MAPI acceleration, see Configuring Encrypted MAPI Acceleration.

Configuring MAPI Acceleration Using the Cisco WAAS Central Manager

Procedure

Step 1 To enable the MAPI accelerator, choose **Configure** > **Acceleration** > **Enabled Features** window.

The **Enabled Features** window appears.

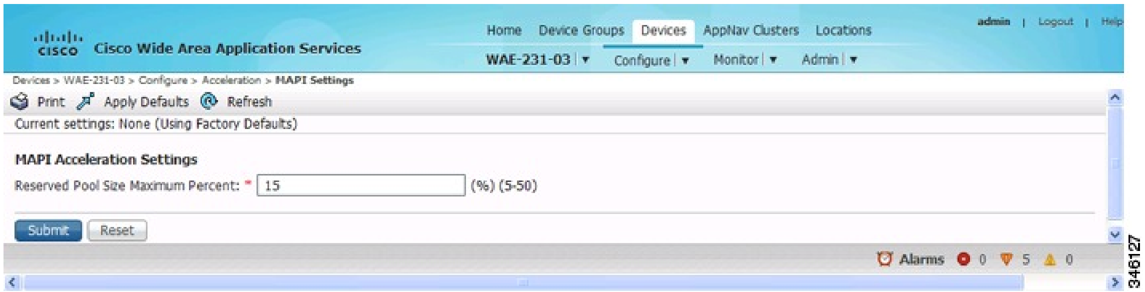
a) At the **Accelerator Optimization** pane, check the **MAPI Accelerator** check box.
b) Click **Submit**.

Step 2 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 3 Choose **Configure** > **Acceleration** > **MAPI Settings**.

The **MAPI Acceleration Settings** window appears.

Figure 52: MAPI Acceleration Settings Window



Current settings: None (Using Factory Defaults)

MAPI Acceleration Settings

Reserved Pool Size Maximum Percent: * 15 (%) (5-50)

Step 4 In the **Reserved Pool Size Maximum Percent** field, enter the maximum percent of connections in order to restrict the maximum number of connections reserved for MAPI optimization during TFO overload.

- The maximum percent of connections is specified as a percent of the TFO connection limit of the platform. Valid percent ranges from 5 to 50 percent. The default is 15 percent, which reserves approximately 0.5 connection for each client-server association group optimized by the MAPI accelerator.

- The client maintains at least one association group per server to which it connects, with an average of about three connections per association group. For deployments that see a greater average number of connections per association group, or where TFO overload is a frequent occurrence, a higher value for reserved pool size maximum percent is recommended.

- Reserved connections remain unused when the device is not under TFO overload. Reserved connections are released when the association group is terminated.

Step 5 Click **Submit**.

The changes are saved to the device or device group.

Configuring Encrypted MAPI Acceleration

This section contains the following topics:

About Encrypted MAPI Acceleration

The Encrypted MAPI acceleration feature provides WAN optimization for secure MAPI application protocols using Microsoft Kerberos security protocol and Microsoft Windows Active Directory identity for authentication of clients or servers or both in the domain.

Consider the following guidelines and terms for encrypted MAPI acceleration:

- You must enable MAPI acceleration first for Encrypted MAPI acceleration to be enabled. Encrypted MAPI acceleration is enabled by default.
- The following terms are used with Microsoft Windows Active Directory and Cisco Encrypted MAPI acceleration:
  - **Microsoft Active Directory**: A set of directory-based and identity-based services developed by Microsoft for Windows domain networks. The Microsoft Active Directory Domain Services (DS) domain controller stores information about domain users and devices
  - **User Identity**: An Active Directory user account. The Microsoft Active Directory employs the user identity to authenticate the user, and to grant appropriate access to domain resources.
  - **Machine Account Identity**: A computer (machine) account used to authenticate the user's computer access to Microsoft Active Directory Domain Services. Each Windows Active Directory computer has a unique machine (computer) account.

Workflow for Configuring Encrypted MAPI

To configure Encrypted MAPI traffic acceleration, complete the tasks listed in the following table. These tasks must be performed on both data center and branch WAEs unless specified as **Not Required** or **Optional**.

Table 43: Workflow for Configuring Encrypted MAPI

Step	Task	Additional Information and Instructions
1.	Configure DNS Settings.	To configure DNS settings, see Configuring the DNS Server in the chapter "Configuring Network Settings."

Step	Task	Additional Information and Instructions
2.	Configure NTP Settings.	To synchronize the time with Active Directory, see Configuring NTP Settings in the chapter "Configuring Other System Settings."
3.	Verify WAE devices are registered and online with the WAAS Central Manager.	To verify WAE devices are registered and online with the Cisco WAAS Central Manager, see Devices Window in the chapter "Monitoring Your Cisco WAAS System."
4.	Configure SSL Peering Service.	To configure SSL Peering Service, see Configuring SSL Peering Service, on page 424.
5.	Verify WAN Secure mode is enabled.	To verify WAN Secure mode is enabled, run the **show accelerator wansecure** EXEC command.
6.	(Optional) Configure windows domain settings and perform domain join. The domain join function automatically creates the machine account in Active Directory.	To configure Windows Domain Server Authentication settings, see Configuring Windows Domain Server Authentication Settings in the chapter "Configuring Administrative Login Authentication, Authorization, and Accounting." • Performing a domain join of the Cisco WAE is not required on Cisco branch WAE devices. • It is sufficient to create any one identity account, either machine or user. Domain-join is required only for machine account used as an identity account.
7.	Configure domain identities (for machine account and optional user accounts).	To configure a machine account identity, see Configuring a Machine Account Identity, on page 390. (Optional) To create a user account and configure a user account identity, see Creating and Configuring a User Account, on page 391. Note that configuring domain identities is not required on branch WAE devices.
8.	Enable Windows Domain Encrypted Service.	To enable the Windows Domain Encrypted Service, navigate to the **Configure** > **Security** > **Windows Domain** > **Encrypted Services** window and check the **Enable Encrypted Service** check box.
9.	Enable Encrypted MAPI Traffic Optimization.	To enable Encrypted MAPI Traffic, see Enabling and Disabling the Global Optimization Features, on page 373.

Configuring Encrypted MAPI Settings

Procedure

Step 1 Configure DNS settings.

The WAAS DNS server must be a part of the DNS system of Windows Active Directory domains to resolve DNS queries for traffic encryption.

For more information, see Configuring the DNS Server in the chapter "Configuring Network Settings."

Step 2 Configure NTP settings to synchronize the time with the Active Directory.

The Cisco WAAS device has to be in synchronization with the Active Directory for Encrypted MAPI acceleration. The Cisco WAAS NTP server must share time synchronization with the Active Directory Domain Controllers' domains for which traffic encryption is required.

Note Out-of-sync time will cause Encrypted MAPI acceleration to fail.

For more information, see Configuring NTP Settings in the chapter "Configuring Other System Settings."

Step 3 Verify if Cisco WAE devices are registered and are online with the Cisco WAAS Central Manager.

For more information, see Devices Window in the chapter "Monitoring Your Cisco WAAS Network."

Step 4 Configure the SSL Peering Service.

Note The SSL accelerator must be enabled and in running state.

For more information, see Configuring SSL Peering Service, on page 424.

Step 5 Verify that **WAN Secure mode** is enabled.

The default mode is **Auto**.

- To verify the state of WAN Secure mode, run the following EXEC command:

  show accelerator wansecure

- To change the state of WAN Secure mode, run the following global configuration command:

  accelerator mapi wansecure-mode {always | auto | none}

Step 6 (Optional on data center WAEs if only user accounts are used for domain identity configuration in Step 7.)

Configure Microsoft Windows domain settings and perform a **domain join**. (A **domain join** automatically creates the machine account in Active Directory.)

- It is sufficient to create any one identity account, either machine or user.
- **Domain join** is required only for machine account used as an identity account.

Note Performing a **domain join** of the WAE is not required on branch WAE devices.

For more information, see Configuring Windows Domain Server Authentication Settings in the chapter "Configuring Administrative Login Authentication, Authorization, and Accounting."

Note Kerberos and Microsoft Windows NT LAN Manager (Microsoft Windows NTLM) authentication are used for Encrypted MAPI acceleration. For Cisco WAAS Version 5.3.1 and later, encrypted NTLM traffic is supported for EMAPI, and the Cisco WAE device optimizes NTLM traffic for domains configured with NTLM authentication.

Step 7 Configure domain identities. This is not required for branch WAEs.

- As highlighted in Step 6, you must have at least one account, either user or machine, that is configured with a domain identity. Each device can support up to five domain identities, one machine account identity and four user account identities. This allows a Cisco WAAS device to accelerate up to five domain trees.
- You must configure a domain identity for each domain with an exchange server that has clients to be accelerated.

a) Configure the machine account identity.

A machine account for the core device is automatically created during the join process in the Windows Domain Server authentication procedure in Step 6. If you are using a machine account, a machine account identity must be configured for this account.

Each device supports only one machine account identity.

For more information, see Configuring a Machine Account Identity, on page 390.

b) Create and configure optional user accounts.

You can utilize up to four optional user accounts for additional security. Multiple user accounts provide greater security than having all of the core devices using a single user account. You must configure a user account identity for each user account, whether you are utilizing an existing user account or creating a new one.

For more information, see Creating and Configuring a User Account, on page 391.

Step 8 Enable **Windows Domain Encrypted Service**. (This is enabled by default.)

a) From the the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.
b) From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.

The **Encrypted Services** window appears.

c) Check the **Enable Encrypted Service** check box.
d) To save your changes, click **Submit**.

Step 9 Enable Encrypted MAPI Traffic Optimization.

a) Choose **Configure** > **Acceleration** > **Enabled Features**.

The **Enabled Features** window appears.

b) In the **Enabled Features** window, check the **Encrypted MAPI Traffic Optimization** check box.
c) In the **Enabled Features** window, check the **MAPI Accelerator** check box.

Note To enable Encypted MAPI, you must also check the MAPI Accelerator check box. (Encrypted MAPI traffic optimization is enabled by default.)

d) Click **Submit**.

For more information, see Enabling and Disabling the Global Optimization Features, on page 373.

Configuring a Machine Account Identity

Procedure

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

Step 2 From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.

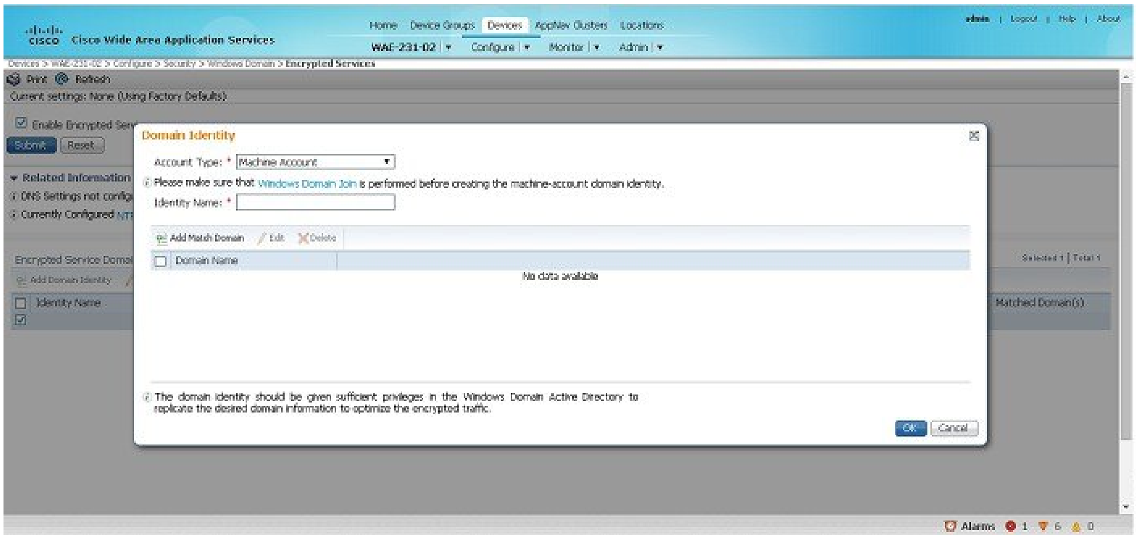
The **Encrypted Services** window appears.

Step 3 Click the **Add Domain Identity** button.

The **Domain Identity** dialog box appears.

Note Every Cisco WAAS device that has to be accelerated must have a domain identity.

Figure 53: Add Domain Identity—Machine Account



Current settings: None (Using Factory Defaults)

☑ Enable Encrypted Serv

DNS Settings not config

Currently Configured NT

Domain Identity

Account Type: * Machine Account ▾

Please make sure that Windows Domain Join is performed before creating the machine-account domain identity.

Identity Name: *

□	Domain Name
	No data available

The domain identity should be given sufficient privileges in the Windows Domain Active Directory to replicate the desired domain information to optimize the encrypted traffic.

a) In the **Domain Identit**y dialog box, from the **Account Type** drop-down list, choose **Machine Account**.

Note Windows domain join must be completed before creating the machine account domain identity. For more information, see Configuring Windows Domain Server Settings on a Cisco WAAS Device in the chapter "Configuring Administrative Login Authentication, Authorization, and Accounting."

b) Enter the identity name in the **Identity Name** field. Only alphanumeric characters are allowed. Space, ?, and | are not allowed. The length is not to exceed 32 characters.

Note The domain identity must have sufficient privileges in the Windows Domain Active Directory to replicate the desired domain information to optimize encrypted traffic. To configure privileges, see Configuring Microsoft Active Directory, on page 393.

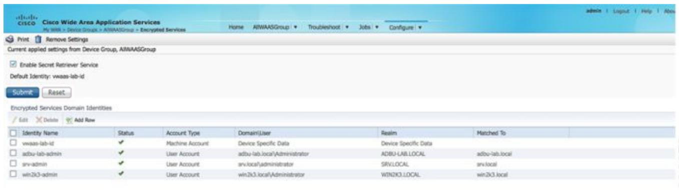
Step 4 Click the **Add Match Domain** button to add the child domains of the domain (with which the device is registered) for which the Domain Identity should optimize the encrypted traffic. You can add up to 32 child domains. If you do not want the Domain Identity to optimize the traffic for any of the child domains, you can delete the selected match domain items.

Note This is available only on devices running Cisco WAAS Version 5.4 and later.

Step 5 Click **OK**.

The domain identity appears in the **Encrypted Services Domain Identities** list.

Figure 54: Encrypted Services—Domain Identity



Current applied settings from Device Group, AllWAASGroup

☑ Enable Secret Retriever Service

Default Identity: vwaas-lab-id

Encrypted Services Domain Identities

□	Identity Name	Status	Account Type	Domain\User	Realm	Matched To
□	vwaas-lab-id	✓	Machine Account	Device Specific Data	Device Specific Data	
□	adbu-lab-admin	✓	User Account	adbu-lab.local\Administrator	ADBU-LAB.LOCAL	adbu-lab.local
□	srv-admin	✓	User Account	srv.local\administrator	SRV.LOCAL	srv.local
□	win2k3-admin	✓	User Account	win2k3.local\Administrator	WIN2K3.LOCAL	win2k3.local

333672

Step 6 To configure and verify Encrypted Services Domain Identities from the CLI, run the **windows-domain encrypted-service** global configuration command and the **show windows-domain encrypted-service** EXEC command.

Creating and Configuring a User Account

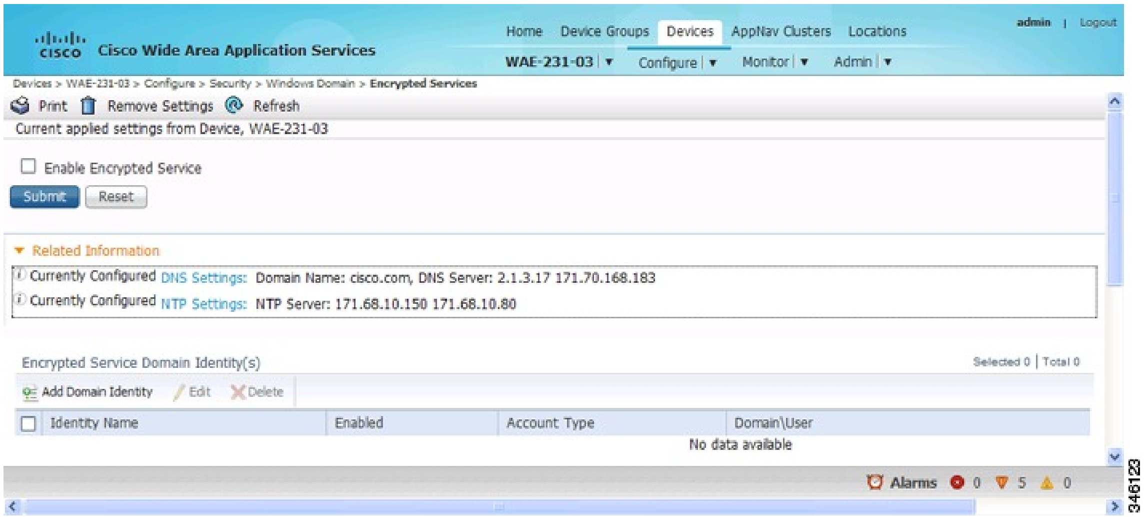
Procedure

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

Step 2 From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.

The **Encrypted Services** window appears.

Figure 55: Encrypted Services



Devices > WAE-231-03 > Configure > Security > Windows Domain > **Encrypted Services**

Current applied settings from Device, WAE-231-03

□ Enable Encrypted Service

Related Information

Currently Configured DNS Settings: Domain Name: cisco.com, DNS Server: 2.1.3.17 171.70.168.183

Currently Configured NTP Settings: NTP Server: 171.68.10.150 171.68.10.80

Encrypted Service Domain Identity(s) — Selected 0 | Total 0

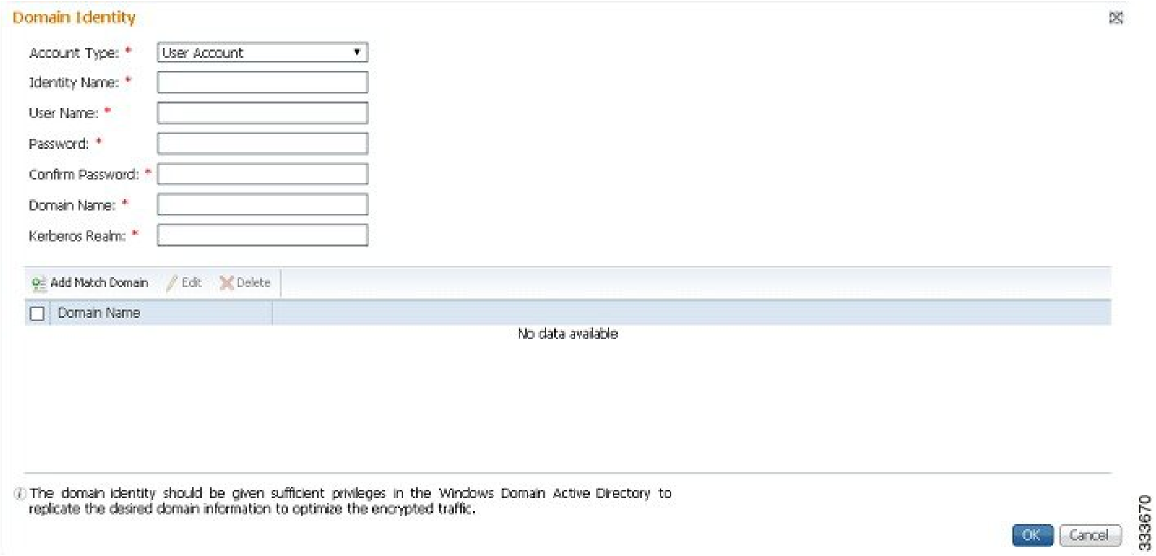
□	Identity Name	Enabled	Account Type	Domain\User

No data available

Step 3 To add a user account domain identity, in the **Encrypted Service Domain Identity(s)** table listing area, click **Add Domain Identity**.

The **Domain Identity** window appears.

Figure 56: Add Domain Identity—User Account



Domain Identity

Account Type: * User Account

Identity Name: *

User Name: *

Password: *

Confirm Password: *

Domain Name: *

Kerberos Realm: *

□	Domain Name

No data available

The domain identity should be given sufficient privileges in the Windows Domain Active Directory to replicate the desired domain information to optimize the encrypted traffic.

a) From the **Account Type** drop-down list, choose **User Account**.

b) In the **Identity Name** field, enter the identity name. Use only alphanumeric characters, up to a maximum of 32 characters.

c) Enter username and password.

d) Enter the domain name.

e) Enter the Kerberos realm.

f) To add the child domains of the domain (with which the device is registered) for which the Domain Identity should optimize the encrypted traffic, click the **Add Match Domain** button.

You can add up to 32 child domains. If you do not want the Domain Identity to optimize the traffic for any of the child domains, you can delete the selected match domain items.

Note The domain identity must have sufficient privileges in the Windows Domain Active Directory to replicate the desired domain information to optimize encrypted traffic. For more information, see Configuring Microsoft Active Directory, on page 393.

Step 4 Click **OK**.

The domain identity appears in the **Encrypted Services Domain Identities** list.

Note Secure store encryption is used for the user account domain identity password. If secure store cannot be opened, an alarm is raised indicating that the configuration updates could not be stored on the device. After secure store can be opened and the configuration updates are successfully stored on the device, the alarm is cleared.

Step 5 To configure and verify Encrypted Services Domain Identities from the CLI, run the **windows-domain encrypted-service** global configuration command and the **show windows-domain encrypted-service** EXEC command.

Configuring Microsoft Active Directory

Procedure

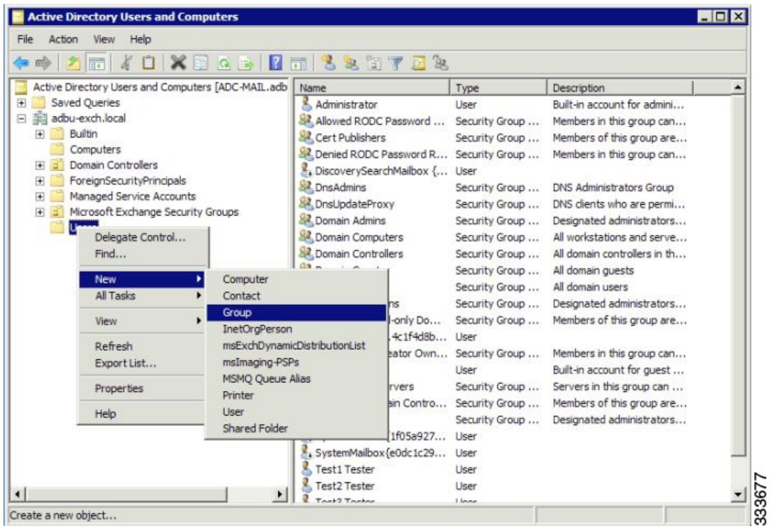
Step 1 To grant Cisco WAAS permission to accelerate Microsoft Exchange-encrypted email sessions: Using an account with Domain Administrator privileges, launch the Active Directory Users and Computers application.

Step 2 Create a new group.

Note This group is for accounts that Cisco WAAS will use to optimize Microsoft Exchange traffic. Regular users and computers should not be added to this group.

a) Right-click the **Unit** to contain the new group and choose **New** > **Group**.

Figure 57: Active Directory—Add Group



Name	Type	Description
Administrator	User	Built-in account for admini...
Allowed RODC Password ...	Security Group ...	Members in this group can...
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password R...	Security Group ...	Members in this group can...
DiscoverySearchMailbox {...	User	
DnsAdmins	Security Group ...	DNS Administrators Group
DnsUpdateProxy	Security Group ...	DNS clients who are permi...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
	Security Group ...	All domain guests
	Security Group ...	All domain users
ns	Security Group ...	Designated administrators...
-only Do...	Security Group ...	Members of this group are...
4c1f4d8b...	User	
eator Own...	Security Group ...	Members in this group can...
	User	Built-in account for guest ...
rvers	Security Group ...	Servers in this group can ...
in Contro...	Security Group ...	Members of this group are...
	Security Group ...	Designated administrators...
1f05a927...	User	
SystemMailbox{e0dc1c29...	User	
Test1 Tester	User	
Test2 Tester	User	

b) Enter a name in the **Group name** field and select the following attributes:

- Group scope: **Universal**
- Group type: **Security**

c) Click **OK**.

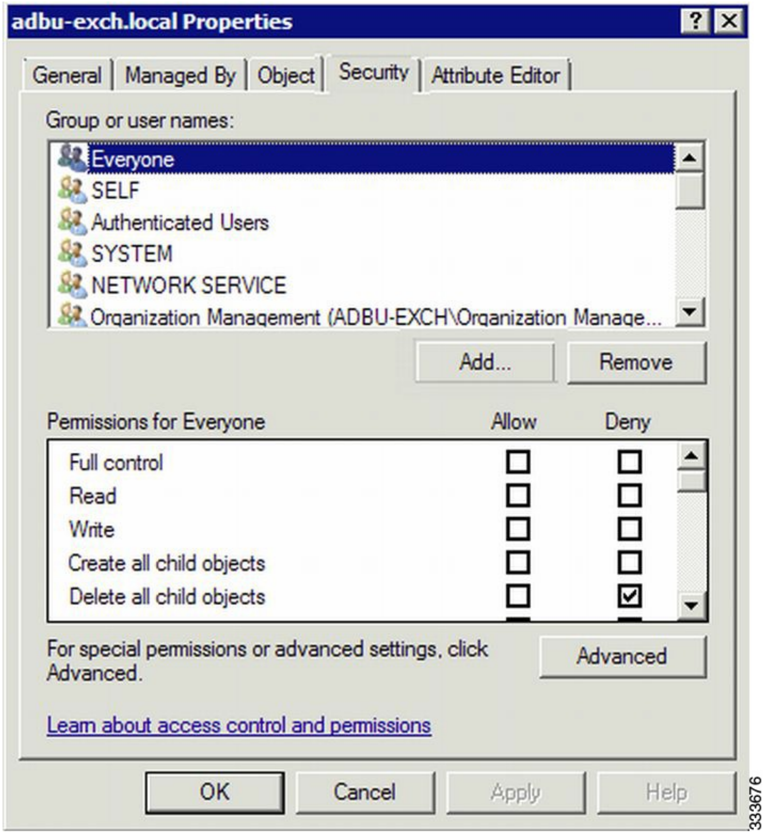
Step 3 Configure the permissions required by Cisco WAAS.

a) At the menu bar of the **Active Directory Users and Computers** window, choose **View** > **Advanced Features**.

b) Right-click the root of the domain and choose **Properties**.

c) Click the **Security** tab.

Figure 58: Active Directory—Security Tab



adbu-exch.local Properties

General | Managed By | Object | Security | Attribute Editor

Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- NETWORK SERVICE
- Organization Management (ADBU-EXCH\Organization Manage...

Permissions for Everyone	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	☑

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

d) In the **Group** or **User Names** section, click **Add**.

e) In the **Enter the object names to select** field, enter the name of the new group .

f) To add the new group to the list, click **OK**.

g) Check the check box adjacent to the new group in the **Group** or **User names** list and set the following permissions to **Allow**:

- Replicating Directory Changes
- Replicating Directory Changes All

h) Click **OK**.

Step 4 Add an account to the group.

User or workstation (computer) accounts must be added to the new group for WAAS Exchange Encrypted email optimization.

a) Right-click on the account you want to add and select the **Member Of** tab.
b) Click **Add**.
c) Choose the new group you created and click **OK**.

The configuration of **Active Directory** permissions is complete.

Managing Domain Identities and Encrypted MAPI State

This section contains the following topics:

Note To view the statistics for Encrypted MAPI connections, see MAPI Acceleration Charts in the chapter "Monitoring Your Cisco WAAS Network."

Editing an Existing Domain Identity

Before you begin

You can modify the attributes of an existing domain identity on a Cisco WAAS device, if needed.

Note If the password for a user account has been changed in the Active Directory, you must edit the user account domain identity on the Cisco WAAS device to match the new Active Directory password.

The following restrictions apply:

- For a machine account identity, only the state of the domain identity (enabled or disabled) can be modified from a Cisco WAAS device.
- For a user account identity, only the state of the domain identity (enabled or disabled) and the password can be modified from a Cisco WAAS device.

Procedure

Step 1 To change the password for a user account domain identity on a Cisco WAAS device when the password for the account in the **Active Directory** has changed: From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 2 From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.

The **Encrypted Services** window appears.

Step 3 Select the user account domain identity to modify and click the **Edit** icon.

The **Domain Identity** window appears.

Step 4 In the **Password** field, change the password. The password should be the same as the password for the account in **Active Directory**.

Step 5 Click **OK**.

Deleting an Existing Domain Identity

Procedure

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

Step 2 From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.

The **Encrypted Services** window appears.

Step 3 Select one or more domain identities to delete and click the **Delete** icon to remove the domain identity configured on the Cisco WAAS device.

If the domain identity is being used for optimizing encrypted traffic, a warning message appears.

Step 4 To accept the procedure, click **OK**, or to cancel the procedure, click **Cancel**.

Disabling Encrypted MAPI

Procedure

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

Step 2 Disable **Encrypted Service**.

a) From the menu, choose **Configure** > **Security** > **Windows Domain** > **Encrypted Services**.

The **Encrypted Services** window appears.

b) Uncheck the **Enable Encrypted Service** check box.

c) To save your changes, click **Submit**.

Step 3 Disable **Encrypted MAPI Traffic Optimization**.

a) From the menu, choose **Configure** > **Acceleration** > **Enabled Features**.

The **Enabled Features** window appears.

b) Uncheck the **Encrypted MAPI Traffic Optimization** check box.

c) To save your changes, click **Submit**.

To view the statistics for Encrypted MAPI connections, see MAPI Acceleration Charts in the chapter "Monitoring Your Cisco WAAS Network."

Cisco WAAS MAPI RPC over HTTP(S)

Remote Procedure Call over HTTP(S) (RPC over HTTP(S) allows Microsoft Outlook clients to access Exchange servers from outside the enterprise network using HTTP or HTTPS as a transport for RPC protocol. It allows a client on the Internet to connect securely to a Microsoft Exchange Server without having to log into a virtual private network (VPN) first.

An RPC-HTTP (RPC-H) module in Cisco WAAS, integrated into the existing Cisco WAAS MAPI optimizer will provide Cisco WAAS the ability to optimize MAPI over RPC-HTTP(S) traffic.

Cisco WAAS Version 6.2.x and later supports L7 optimization for RPC-HTTP(S) traffic.

Microsoft Outlook and Exchange Versions Supported for Cisco WAAS MAPI RPC over HTTP(S)

The following table shows the clients and servers supporting Cisco WAAS MAPI RPC over HTTP(S):

Table 44: Clients and Servers Supporting Cisco WAAS MAPI RPC over HTTP(S)

Clients Supported	Servers Supported
Microsoft Outlook 2016	Microsoft Exchange 2016
Microsoft Outlook 2013(for Windows 7 and Windows 8)	Microsoft Exchange 2013(for Windows Server 2012, 2012 R2, 2008 R2 [full installation])
Microsoft Outlook 2010(for Windows 7 and Windows 8)	Microsoft Exchange 2010(for Windows Server 2012, 2012 R2, 2008, and 2008 R2)
Microsoft Outlook 2007(for Windows Vista, Windows 7)	

Exchange 2013 and Exchange 2016 can be configured for MAPI over HTTP support. MAPI over HTTP traffic will not be optimized by MAPI accelerator. However, MAPI over HTTP traffic will get L4 optimization benefits from WAAS (THSDL).

Configuration Prerequisites for Optimizing MAPI RPC over HTTP(S)

Procedure

Step 1 Ensure that the SSL, HTTP and MAPI accelerators are enabled. If you have enabled SSL Interposer (SSL Accelerator V2) on both branch and data center devices, MAPI over RPC HTTPS will use Smart-SSL and not SSL Accelerator V1.

Step 2 Configure SSL acceleration. For more information, see Configuring SSL Acceleration, on page 407. If you enable SSL Interposer (SSL Accelerator V2) on both branch and data center devices, MAPI over RPC HTTPS will use Smart-SSL and not SSL Accelerator V1.

Step 3 When you configure SSL acceleration, be sure to enable protocol chaining, by checking the **Enable protocol chaining** check box in the **SSL Accelerated Services** window.

Note If protocol chaining is not enabled, the Cisco WAAS device will only optimize SSL traffic on the specified IP address and port.

Step 4 Configure a Microsoft Windows domain identity on the core device, for Encrypted MAPI connections.

Step 5 Verify that encryption is enabled in the MAPI accelerator. For more information, see Configuring Encrypted MAPI Settings, on page 388.

MAPI Acceleration Charts for Cisco WAAS MAPI RPC over HTTP(S)

The MAPI Acceleration report displays MAPI acceleration statistics. For Cisco WAAS Version 5.5.3 and later, the following MAPI acceleration charts are added or modified:

- **MAPI: Handled Traffic Pattern**: A new pie diagram that shows the three different types of traffic handled by the MAPI AO. For more information, see MAPI: Handled Traffic Pattern in the chapter "Monitoring Your Cisco WAAS Network."
- **MAPI: Connection Details**: An existing chart for MAPI session connection statistics, MAPI: Connection Details now includes a new classification for optimized TCP and RPC-HTTP(S) MAPI connections. For more information, see MAPI: Connection Details, on page 571 in in the chapter "Monitoring Your Cisco WAAS Network."

Cisco WAAS MAPI over HTTP

MAPI over HTTP provides the ability for Messaging API (MAPI) clients and servers to communicate across HTTP connection that no longer use RPC technology. This provides faster re-connects and improved reliability.

Cisco WAAS Version 6.4.3 and later provides optimization support for MAPI over HTTP traffic. This is enabled by default and uses SMART-SSL acceleration and protocol chaining to intercept and accelerate the MAPI over HTTP traffic. To ensure this optimization, you need to enable the SMART-SSL (SSL Accelerator v2) accelerator.

For more information on how to set up the exchange service, see, Using SSL Accelerated Services, on page 426.

The MAPI Acceleration report displays MAPI acceleration statistics. For more information, see MAPI: Handled Traffic Pattern and MAPI: Connection Details, on page 571 in the chapter "Monitoring Your WAAS Network."

Microsoft Outlook and Exchange Versions Supported for Cisco WAAS MAPI over HTTP

The following table shows the clients and servers supporting Cisco WAAS MAPI over HTTP:

Table 45: Clients and Servers Supporting Cisco WAAS MAPI over HTTP

Clients Supported	Servers Supported
Microsoft Outlook 2010 (Jan 2015 Public Update – For MAPIoHTTP)	Microsoft Exchange 2013 SP1(Win 2008 R2, Win 2012 R2)
Microsoft Outlook 2013 (SP1 – For MAPIoHTTP)	Microsoft Exchange 2016(Win 2012 R2, Win 2016)
Microsoft Outlook 2016	

Configuring SMB Acceleration

This section contains the following topics:

About SMB Acceleration

The Service Message Block (SMB) application accelerator handles optimizations of file server operations. These optimizations apply to SMBv1, SMBv2 and SMBv3. It can be configured to perform the following file server optimizations:

- **SMB Print Optimization**: A centralized print deployment reduces management overhead and increases cost savings. SMB Print Optimization optimizes print traffic by utilizing a centralized printer server, which resides in the data center. This removes the need for local print servers in the branches. The three most common uses for a centralized printer server are:
  - Print from branch client to branch printer.
  - Print from branch client to data center printer.
  - Print from data center client to branch printer.
- **Read Ahead Optimization**: The SMB accelerator performs a read-ahead optimization (SMBv1 only) on files that use the OpLock feature.
  - When a client sends a read request for a file, it is likely that the accelerator may issue more read requests for the same file.
  - To reduce the use of network bandwidth to perform these functions over the WAN on the file server, the SMB accelerator performs read-ahead optimization by proactively reading more file data than what has been initially requested by the client.
- **Directory Listing Optimization**: A significant portion of the traffic on the network is for retrieving directory listings. The SMB accelerator optimizes directory listings from the file server by prefetching.
  - For directory prefetching, a request from the client is expanded to prefetch up to 64 KB of directory listing content. The SMB accelerator buffers the prefetched directory listing data until the client has requested all the data.
  - If the directory listing size exceeds 64 KB, a subsequent request from the client is expanded by the SMB accelerator again to prefetch content up to 64 KB. This continues until all the entries of the directory are returned to the client.
- **Directory Browsing Optimization**: The SMB accelerator optimizes directory browsing by prefetching SMBv2 data from the file server and caching it in the RAM infrastructure of the WAE. When directory query requests are made by the client, the data is fetched from the cached data.
  - To accommodate multiple client requests, locking mechanisms are in place while accessing parent directory and child files.
  - Additionally, because the infrastructure has limited memory, new requests are cached only when memory is available.
- **Metadata Optimization**: The SMB accelerator optimizes fetching metadata from the file server through metadata prefetching. Additional metadata requests are tagged along with the client request and are sent to the file server to prefetch more information levels than what was requested by the client.

- **Named Pipe Optimization**: The SMB accelerator optimizes frequent requests from Microsoft Windows Explorer to the file server to retrieve share, server, and workstation information.
    - Each of these requests involves a sequence of operations that include opening and binding to the named pipe, making the RPC request, and closing the named pipe. Each operation incurs a round trip to the file server.
    - To reduce the use of network bandwidth to perform these functions over the WAN on the file server, the SMB accelerator optimizes the traffic on the network by caching named pipe sessions and positive RPC responses.
- **Write Optimization**: The SMB accelerator performs write optimization by speeding up the write responses to the client by acknowledging the Write requests to the client whenever possible and, at the same time, streaming the Write requests over the WAN to the server.
- **Not-Found Metadata caching**: Applications sometimes send requests for directories and files that do not exist on file servers.

  For example, Microsoft Windows Explorer accesses the Alternate Data Streams (ADS) of the file it finds. With negative Not-Found (NF) metadata caching, the full paths to those nonexistent directories and files are cached so that further requests for the same directories and files get local denies to save the round trips of sending these requests to the file servers.
- **DRE-LZ Hints**: The SMB accelerator provides DRE hints to improve system performance and resources utilization.
    - At the connection level, the SMB accelerator uses the BEST_COMP latency sensitivity level for all connections, because it gives the best compression.
    - At the message level, the SMB accelerator provides message-based DRE hints for each message to be transmitted over the WAN.
- **Microsoft Optimization**: The SMB accelerator optimizes file operations for Microsoft applications by identifying lock request sequences for file name patterns supported by Microsoft Office applications.
- **Invalid FID Optimization**: The SMB accelerator optimizes SMB2 and SMB3 clients by locally denying attempts to access files with invalid file handle values instead of sending such requests to the file servers.
- **Batch Close Optimization**: The SMB accelerator performs asynchronous file close optimizations on all SMB traffic.
- **Read Cache optimization**: The SMB accelerator optimizes read operations in SMB2 by caching read response data so that files can be served locally.
- **Write Optimization**: The SMB accelerator improves system performances by performing asynchronous write operations.
- **Signed Optimization**: The SMB accelerator provides L7 optimization of all SMB traffic.
- **SMB v3 Encrypted Optimization**: The SMB accelerator provides L7 optimization of encrypted SMB v3 traffic.

Configuring SMB Acceleration with the Cisco WAAS Central Manager

Procedure

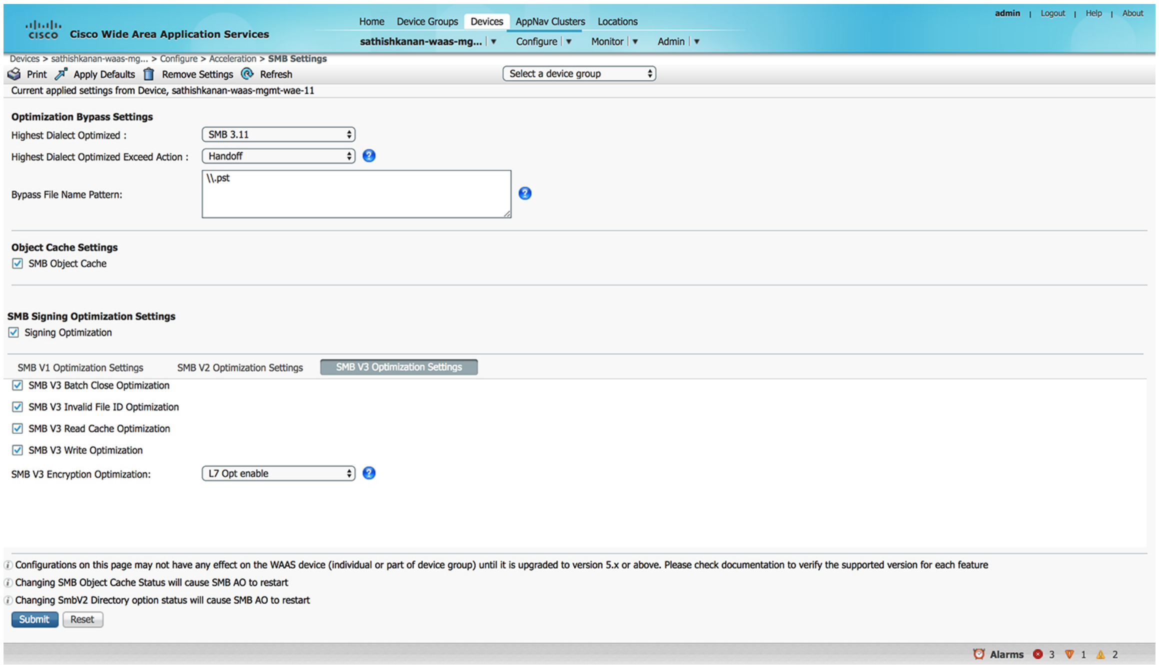
Step 1 To enable the SMB accelerator, check the **SMB Accelerator** check box in the **Enabled Features** window.

Step 2 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 3 Choose **Configure** > **Acceleration** > **SMB Settings**.

The **SMB Settings** window appears.

Figure 59: SMB Settings Window


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
admin | Logout | Help | About
sathishkanan-waas-mg... | ▾
Configure | ▾
Monitor | ▾
Admin | ▾
Devices > sathishkanan-waas-mg... > Configure > Acceleration > SMB Settings
Print
Apply Defaults
Remove Settings
Refresh
Select a device group
SMB V1 Optimization Settings
SMB V2 Optimization Settings
SMB V3 Optimization Settings
Submit
Reset
Alarms 3 1 2

Current applied settings from Device, sathishkanan-waas-mgmt-wae-11

Optimization Bypass Settings

Highest Dialect Optimized : SMB 3.11

Highest Dialect Optimized Exceed Action : Handoff

Bypass File Name Pattern: \\.pst

Object Cache Settings

☑ SMB Object Cache

SMB Signing Optimization Settings

☑ Signing Optimization

☑ SMB V3 Batch Close Optimization

☑ SMB V3 Invalid File ID Optimization

☑ SMB V3 Read Cache Optimization

☑ SMB V3 Write Optimization

SMB V3 Encryption Optimization: L7 Opt enable

Configurations on this page may not have any effect on the WAAS device (individual or part of device group) until it is upgraded to version 5.x or above. Please check documentation to verify the supported version for each feature

Changing SMB Object Cache Status will cause SMB AO to restart

Changing SmbV2 Directory option status will cause SMB AO to restart

Step 4 From the **Highest Dialect Optimized** drop-down list, choose the highest dialect to optimize. The available options are:

- NTLM 0.12 or NTLM 1.0
- SMB 2.0
- SMB 2.1
- SMB 3.0
- SMB 3.02
- SMB 3.1.1

Step 5 From the **Highest Dialect Optimized Exceed Action** drop-down list, choose the action for the dialects that are higher than the one chosen as the highest dialect to optimize:

Mute: The dialects higher than the one chosen as the highest dialect to optimize are removed from the negotiation list. This is the default selection.

Note The **Mute option** of SMB AO is deprecated in dialects 3.x and 2.0 of SMB; muting within these versions has been found to be unsuccessful in terms of optimization.

Handoff: If the negotiated dialect is higher than the chosen highest dialect to optimize, the connection is handed off to the generic accelerator.

Note For SMB 2.1 only, you must use the Cisco WAAS CLI to configure the Handoff parameter, running the **accelerator smb smb2-1 exceed-action handoff** global configuration command. If you use the Cisco WAAS Central Manager to select the Handoff parameter for SMB 2.1, the Highest Dialect Optimized Exceed Action will not take effect, and Handoff will not be displayed in commands like the **show running-configuration** command or the **show accelerator smb** command.

Step 6 In the **Bypass File Name Pattern** field, enter the patterns for the file names that you want the SMB accelerator to bypass optimization for. The files whose names match the specified expressions are not optimized.

Step 7 To enable disk caching for SMB traffic, check the **SMB Object Cache** check box.

Step 8 To enable optimization of signed SMB v2 and v3 traffic, check the **Signing Optimization** check box. This check box is checked by default.

An SMB connection request can originate from the Branch office to the Data Center or vice-versa. For every connection, the WAE near the requestor, takes the Edge WAE's role and WAE near the smb server takes the Core WAE's role.

The following prerequisites, at the Core and Edge WAE, are necessary to ensure that a signed connection is optimized:

- If an SMB connection is either a signed SMBv2 or an encrypted SMBv3, or has originated from an SMBv3 enabled client such as Windows 8 and above, then you must configure an identity as a pre-requisite to receive SMB optimization at Layer 7. Otherwise, you will only get Layer 4 (TDL) optimization benefits on these connections.
- It is sufficient to configure either a user identity or a machine identity; the administrator can decide based on ease of configuration. Both configurations are equal and serve the purpose of key retrieval. Domain-join is required only for machine identity.
    - On the Cisco Core WAE, configure a valid user-identity with administrator privileges to enable secret-retrieval to fetch and cache the longterm service key of the SMB server by running the following global configuration command.

      windows-domain encryption-service identity [*identity*] *user-account name* [*admin-username*] **domain** [*your.domain*] **realm** [*your.domain*] *password*

      To verify the identity configuration, run the following EXEC Command.

      show windows-domain encryption-service identity detail

      (Optional) To configure a machine identity, instead of using user identity, you can also follow the steps in the procedure Configuring a Machine Account Identity.
    - For Kerberos Authentication to work correctly, ensure time synchronization between Client, Server, Cisco Core WAE and the Domain Controller.
- To verify whether a connection is signed or not, look into the SMBv2 Negotiate packet. The Signing Required field should be set to True in either the Negotiate Request or the Negotiate Response exchange.

- To verify if a connection has originated from a SMB3 capable client, look into the SMBv2 Negotiate Request packet. Under the dialects list, you should see some or all of the following dialects: SMB3.0, SMB3.02, or SMB3.11.

  These configurations are similar to the EMAPI configuration. For more information, see Step 6 of the procedure Configuring Encrypted MAPI Settings.

- Verify that the **WAN Secure mode** is enabled. WAN Secure's secure connection enables the key to be transported to the Edge WAE.
  - The default recommended mode is **Auto**. To verify the state of **WAN Secure mode**, run the following EXEC command:

    show accelerator wansecure

  - To change the state of WAN Secure, run the following global configuration command:

    accelerator smb wansecure-mode {always | auto | none}

- Verify that the Cisco WAE devices are registered and are online with the Cisco WAAS Central Manager.

Step 9 Click the **SMBV1 Optimization Settings** tab to perform the following tasks:

- Check the **SMB v3 Batch Close Optimization** check box to enable asynchronous files close optimizations. This check box is checked by default.
- Check the **SMB v3 Invalid FID Optimization** check box to enable optimization of files with invalid file handle values. This check box is checked by default.
- Check the **SMB v3 Read Cache Optimization** check box to enable read response caching. This check box is checked by default.
- Check the **SMB v3 Write Optimization** check box to enable asynchronous write operations. This check box is checked by default.
- Select the type of optimization you want from the **SMB v3 Encryption Optimization** drop down box - L7 Optimization, L4 only optimization or disable SMB v3 encrypted optimization. L7 optimization is selected by default.

Step 10 Click the **SMBV2 Optimization Settings** tab to perform the following tasks:

- Check the **SMB v3 Batch Close Optimization** check box to enable asynchronous files close optimizations. This check box is checked by default.
- Check the **SMB v3 Invalid FID Optimization** check box to enable optimization of files with invalid file handle values. This check box is checked by default.
- Check the **SMB v3 Read Cache Optimization** check box to enable read response caching. This check box is checked by default.
- Check the **SMB v3 Write Optimization** check box to enable asynchronous write operations. This check box is checked by default.
- Select the type of optimization you want from the **SMB v3 Encryption Optimization** drop down box - L7 Optimization, L4 only optimization or disable SMB v3 encrypted optimization. L7 optimization is selected by default.

Step 11 Click the **SMBV3 Optimization Settings** tab to perform the following tasks:

- Check the **SMB v3 Batch Close Optimization** check box to enable asynchronous files close optimizations. This check box is checked by default.
- Check the **SMB v3 Invalid FID Optimization** check box to enable optimization of files with invalid file handle values. This check box is checked by default.
- Check the **SMB v3 Read Cache Optimization** check box to enable read response caching. This check box is checked by default.
- Check the **SMB v3 Write Optimization** check box to enable asynchronous write operations. This check box is checked by default.
- Select the type of optimization you want from the **SMB v3 Encryption Optimization** drop down box - L7 Optimization, L4 only optimization or disable SMB v3 encrypted optimization. L7 optimization is selected by default.

Step 12 To save the changes, click **Submit**.

To configure SMB acceleration from the CLI, run the **accelerator smb** global configuration command.

Configuring SMB Acceleration with the Cisco WAAS CLI

To configure SMB acceleration using the Cisco WAAS CLI, run the accelerator smb global configuration command.

Consider the following operating guidelines for running the **accelerator smb** global configuration command:

- The enterprise license is required to start the SMB accelerator.
- The **show running-config** EXEC mode command displays non-default settings only. Therefore, the command **no accelerator smb enable** does not display in the running configuration if the SMB accelerator is disabled, while the **accelerator smb enable** command does display if the SMB accelerator is enabled.
- Run the **accelerator smb signing unwrap enable** command to verify signature of the signed request packets at the Cisco Edge WAE. This checks whether the packet is modified/tampered while coming over the LAN. However, since the packet usually travels in the LAN from the Client to the Cisco Edge WAE, chances of man-in-middle attacks are less likely and you may choose to disable Edge side signature verification for request packets
- Run the **accelerator smb wansecure-mode always** command to enable WAN Secure mode for optimizing signed SMBv2 traffic. The default is always. The WAN Secure mode configuration for both the Cisco Edge WAE and Cisco Core WAE must match (be set at always) for the SMB accelerator to optimize signed SMBv2 connections. Even if one side has none set, then the signed connections would be handed over for generic optimization.
- Run the **accelerator smb wansecure-mode none** to disable the wansecure-mode.
- WAN Secure mode requires that the SSL application accelerator is enabled. Use the accelerator ssl enable global configuration command to enable the SSL accelerator
- For more information on the **accelerator smb** global configuration command, see the *Cisco Wide Area Application Services Command Reference*.

Configuring ICA Acceleration

This section contains the following topics:

Procedure for Configuring ICA Acceleration

Before you begin

The Independent Computing Architecture (ICA) application accelerator provides WAN optimization on a Cisco WAAS device for ICA traffic that is used to access a virtual desktop infrastructure (VDI). This is done through a process that is both automatic and transparent to the client and server.

ICA acceleration is enabled on a Cisco WAAS device by default.

To enable the ICA accelerator, check the **ICA Accelerator** check box in the **Enabled Features** window.

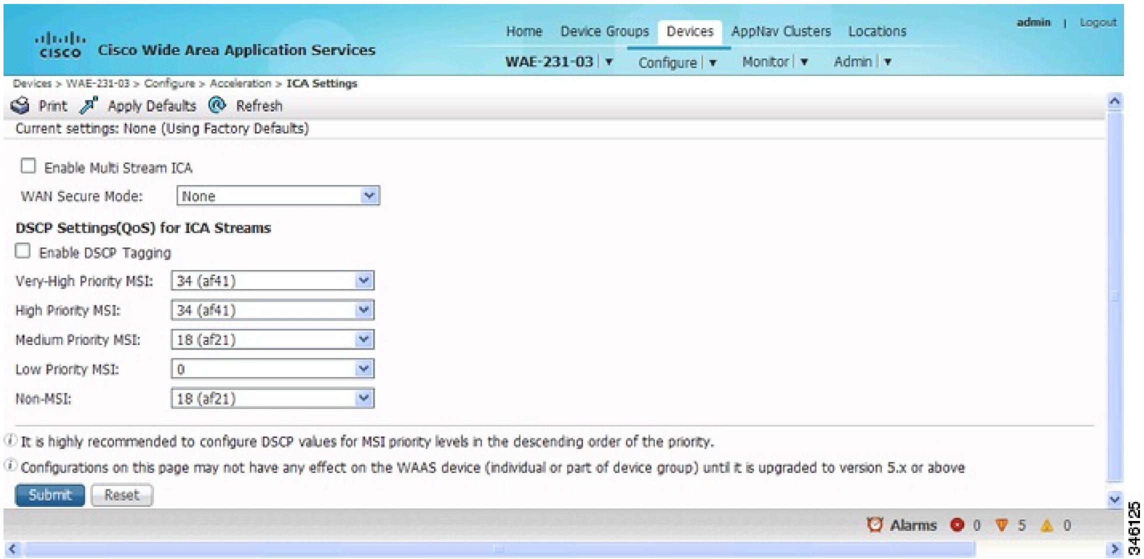
Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **ICA Settings**.

The **ICA Acceleration Configuration** window appears.

Figure 60: ICA Acceleration Configuration Window



Devices > WAE-231-03 > Configure > Acceleration > ICA Settings

Current settings: None (Using Factory Defaults)

☐ Enable Multi Stream ICA

WAN Secure Mode: None

DSCP Settings(QoS) for ICA Streams

☐ Enable DSCP Tagging

Very-High Priority MSI: 34 (af41)

High Priority MSI: 34 (af41)

Medium Priority MSI: 18 (af21)

Low Priority MSI: 0

Non-MSI: 18 (af21)

It is highly recommended to configure DSCP values for MSI priority levels in the descending order of the priority.

Configurations on this page may not have any effect on the WAAS device (individual or part of device group) until it is upgraded to version 5.x or above

Step 3 Check the **Enable Multi Stream ICA** check box to allow the client and server up to three additional TCP connections that optimize multistream ICA traffic.

Step 4 From the **WAN Secure Mode** drop-down list, choose the mode. The options are:

- **None**: Disables WAN Secure mode for ICA. This is the default.
- **Always**: Enables WAN Secure mode for ICA.

Note The state of WAN Secure mode in both Branch WAE and Data Center WAE must match for connections to get optimized with the ICA accelerator.

Step 5 To configure DSCP values for MSI priority levels: In the **DSCP Settings (QoS) under ICA Streams** section, check the **Enable DSCP Tagging** check box. These values override the defaults.

Consider the following ranges and guidelines:

- Configure DSCP values for MSI priority levels in the descending order of the priority.
- **Very High-Priority MSI**: Typically real-time traffic, such as audio. The default is **af41**.
- **High-Priority MSI**: Typically interactive traffic. The default is **af41**.
- **Medium-Priority MSI**: Typically bulk data. The default is **af21**.
- **Low-Priority MSI**: Typically background traffic, such as printing. The default is **0**, best effort.
- **Non-MSI**: (the default is **af21**)
- MSI priority configuration might not apply to devices earlier than Cisco WAAS Version 5.1.x.

Step 6 Click **Submit**.

The changes are saved to the device or device group.

To configure ICA acceleration from the CLI, run the **accelerator ica global** configuration command.

To verify the status of WAN Secure mode from the CLI, run the **show accelerator wansecure** EXEC command.

Configuring ICA over Socket Secure (SOCKS) Server

Before you begin

Consider the following about ICA over SOCKS:

- In a typical deployment where NetScaler is deployed as a SOCKS proxy, the connections from the client go to the SOCKS server instead of the XenApp server.
- Because the ICA optimizer accepts and intercepts only ICA and CGP packets, the packets with SOCKS headers are not recognized and the connection is handed off. The ICA traffic does not get optimized in such scenarios.
- The Cisco WAAS software supports optimizing ICA traffic redirected over SOCKS proxy servers for Cisco WAAS Version 6.3.1 and later.

Considering the following prerequisite configuration guidelines for ICA over SOCKS:

- Make the necessary changes on the NetScaler Gateway to enable the SOCKS proxy (Cache redirection server).
- Make the equivalent and required changes on the StoreFront server along with updates to the **default.ica** file.
- Consider the following NetScaler gateway limitations for ICA over SOCKS:

    - Non-default ports configured with Multi-Port Policy on XenApp for Multi-Stream ICA (MSI) are not supported.
    - SOCKS with ICA over SSL is not supported.
    - SOCKS Version 4 is not supported. ICA over SOCKS Version 5 is supported for the NetScaler gateway.
- For more information on the Netscaler gateway, see Citrix NetScaler documentation.

Procedure

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

Step 2 Next choose **Configure** > **Acceleration** > **Optimization Class-Map**.

Step 3 Edit the class-map named Citrix and add the required port number using the **Add Match Condition** option.

The port number added in the class-map should be the same as the one configured for the SOCKS proxy, on the NetScaler gateway.

Note If the SOCKS proxy port is running on ICA or CGP ports, 1494 or 2498, then you do not need to modify the existing configuration.

Step 4 Select the branch device and make the necessary changes for the port number.

Alternately, run the **class-map type match-any citrix** global configuration command to make these changes.

Configuring ICA over SSL

The Cisco WAAS software supports optimizing ICA over SSL. This allows the client and server to use the ICA protocol over an encrypted connection. To support optimizing ICA over SSL, you must perform the following steps:

- Configure ICA acceleration. See Configuring ICA Acceleration.
- Configure SSL acceleration. See Configuring SSL Acceleration, on page 407.

Note When you are configuring SSL acceleration, be sure to enable protocol chaining. If protocol chaining is not enabled, the Cisco WAAS device will only optimize SSL traffic on the specified IP Address and Port.

Configuring SSL Acceleration

This section contains the following topics:

About SSL Acceleration

The SSL (Secure Sockets Layer) application accelerator optimizes traffic on SSL encrypted connections. If SSL acceleration is not enabled, the Cisco WAAS software DRE optimizations are not very effective on SSL-encrypted traffic. The SSL application acceleration enables Cisco WAAS to decrypt and apply optimizations while maintaining the security of the connection.

Consider the following operating guidelines for SSL acceleration:

- On a Cisco WAAS Express device, only SSL cipher list, SSL certificate authorities, and SSL peering service configuration are supported.
- The SSL accelerator does not optimize protocols that do not start their SSL and Transport Layer Security (TLS) handshake from the very first byte. The only exception is HTTPS that goes through a proxy (where the HTTP accelerator detects the start of SSL and TLS). In this case, both HTTP and SSL accelerators optimize the connection.

  The SSL application accelerator supports SSL Version 3 (SSLv3) and Transport Layer Security Version 1 (TLSv1) protocols. If a TLSv1.1 or TLSV1.2 client request is received, negotiation will not occur. Manual bypass of TLSv1.1 or TLSv1.2 packets is required in order to make these client/server connections.

Workflow for Configuring SSL Acceleration

The following table provides an overview of the steps you must complete to set up and enable SSL acceleration.

Table 46: Workflow for Configuring SSL Acceleration

Step	Task	Additional Information and Instructions
1	Prepare for configuring SSL acceleration.	Identifies the information that you need to gather before configuring SSL acceleration on your Cisco WAAS devices. For more information, see Prerequisites for Configuring SSL Acceleration.
2	Enable secure store, the Enterprise License, and SSL acceleration.	Describes how to set up the Cisco WAAS Central Manager secure store, how to enable the Enterprise License, and how to enable SSL acceleration. Secure store mode is required for secure handling of the SSL encryption certificates and keys. For more information, see Prerequisites for Configuring SSL Acceleration.
3	Enable SSL application optimization.	Describes how to activate the SSL acceleration feature. For more information, see Enabling and Disabling the Global Optimization Features, on page 373.
4	Configure SSL acceleration settings.	(Optional) Describes how to configure the basic setup of SSL acceleration. For more information, see Configuring SSL Global Settings, on page 411.
5	Create and manage cipher lists.	(Optional) Describes how to select and set up the cryptographic algorithms used on your Cisco WAAS devices. For more information, see Working with Cipher Lists, on page 416.

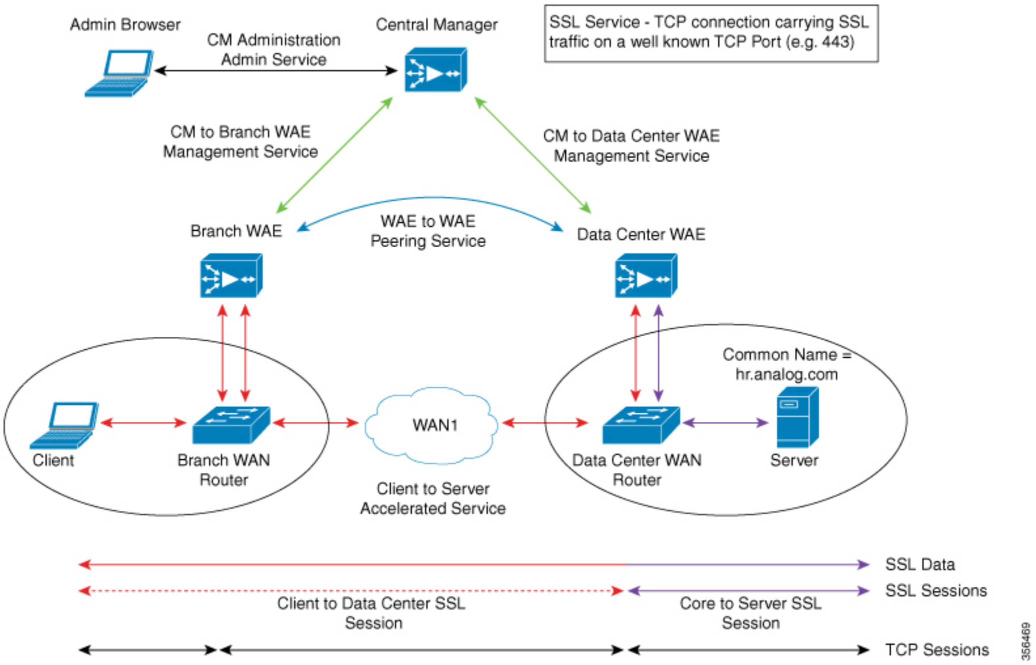
Step	Task	Additional Information and Instructions
6	Set up CA certificates.	(Optional) Describes how to select, import, and manage certificate authority (CA) certificates. For more information, see Working with CA Certificates, on page 418.
7	Configure SSL management services.	(Optional) Describes how to configure the SSL connections used between the Cisco WAAS Central Manager and Cisco WAE devices. For more information, see Configuring SSL Management Services, on page 422.
8	Configure SSL peering service.	(Optional) Describes how to configure the SSL connections used between peer Cisco WAE devices for carrying optimized SSL traffic. For more information, see the Configuring SSL Peering Service, on page 424.
9	Configure and enable SSL-accelerated services.	Describes how to add, configure, and enable services to be accelerated by the SSL application optimization feature. For more information, see Using SSL Accelerated Services, on page 426.

Prerequisites for Configuring SSL Acceleration

Considering the following prerequisites for configuring SSL acceleration:

- **Confirming your network information**
  - services that you want to be accelerated on the SSL traffic
  - server IP address and port information
  - Public Key Infrastructure (PKI) certificate and private key information, including the certificate common name and Certificate Authority (CA) signing information
  - cipher suites supported
  - SSL versions supported
  - The following figure shows how the Cisco WAAS software handles SSL application optimization.

Figure 61: SSL Acceleration Block



When you configure SSL acceleration, you must configure SSL-accelerated service on the Cisco server-side (Data Center) WAE devices. The Cisco client-side (Branch) WAE should have its Secure Store initialized and unlocked or opened, but does not need to have the SSL-accelerated service configured. However, for SSL acceleration services to work, the SSL accelerator must be enabled on both Cisco Data Center WAEs and Cisco Branch WAEs. The Cisco WAAS Central Manager provides SSL management services and maintains the encryption certificates and keys.

- **Enabling Secure Store Encryption on the Cisco WAAS Central Manager**

  Before you can use SSL acceleration on your Cisco WAAS system, you must enable Secure Store encryption on the Cisco WAAS Central Manager. For more information on this procedure, see Configuring Secure Store Encryption Settings in the chapter "Configuring Other System Settings."

- **Enabling Enterprise licenses on the Cisco WAAS Central Manager and Cisco WAEs**

  Before you can use SSL acceleration on your Cisco WAAS system, you must enable the Enterprise license. For more information on this procedure, see Managing Cisco WAAS Software Licenses in the chapter "Configuring Other System Settings."

- **Enabling SSL acceleration on Cisco WAAS Devices**

  Before you can use SSL acceleration on your Cisco WAAS system, you must enable SSL acceleration on Cisco WAAS devices. For more information, see Enabling and Disabling the Global Optimization Features.

Note If the SSL accelerator is already running, you must wait for two datafeed poll cycles to be completed when registering a new Cisco WAE with a Cisco WAAS Central Manager before making any configuration changes. Otherwise, the changes may not take effect.

Configuring SSL Global Settings

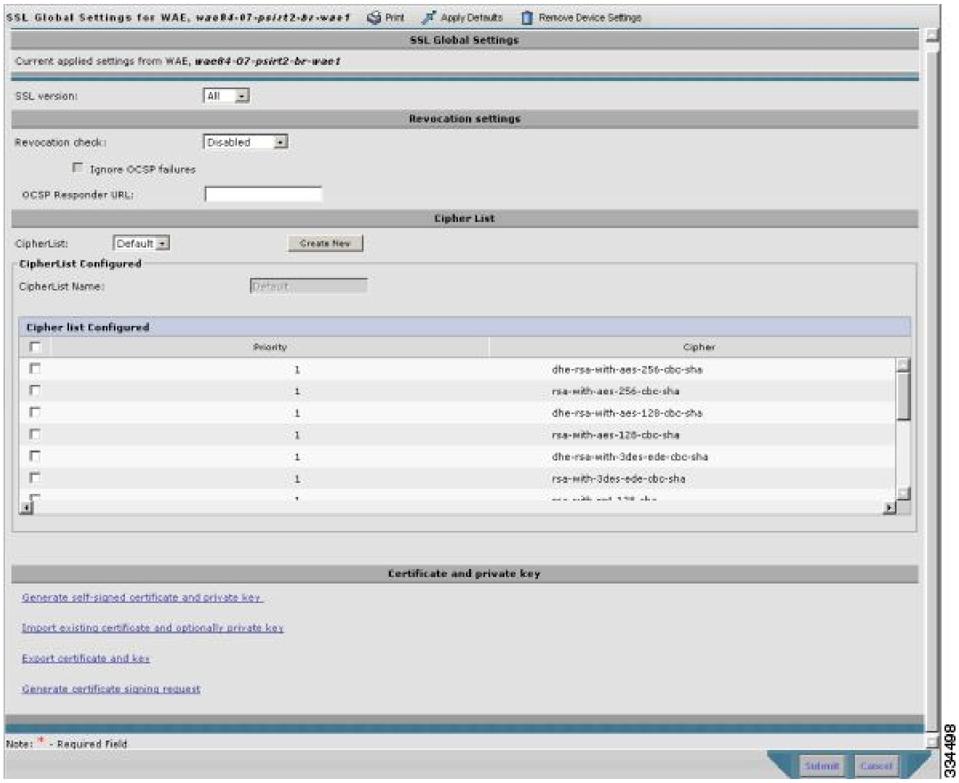
Procedure

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

Step 2 Choose **Configure** > **Security** > **SSL** > **Global Settings**.

The **SSL Global Settings** window appears.

Figure 62: SSL Global Settings Window



SSL Global Settings for WAE, wae84-07-psirt2-br-wae1

Current applied settings from WAE, *wae84-07-psirt2-br-wae1*

SSL version: All

Revocation check: Disabled

□ Ignore OCSP failures

OCSP Responder URL:

CipherList: Default

CipherList Name: Default

Cipher list Configured

□	Priority	Cipher
□	1	dhe-rsa-with-aes-256-cbc-sha
□	1	rsa-with-aes-256-cbc-sha
□	1	dhe-rsa-with-aes-128-cbc-sha
□	1	rsa-with-aes-128-cbc-sha
□	1	dhe-rsa-with-3des-ede-cbc-sha
□	1	rsa-with-3des-ede-cbc-sha

Note: * - Required Field

Print
Apply Defaults
Remove Device Settings
SSL Global Settings
Revocation settings
Cipher List
Create New
CipherList Configured
Certificate and private key
Generate self-signed certificate and private key
Import existing certificate and optionally private key
Export certificate and key
Generate certificate signing request
Submit
Cancel
334498

Step 3 To configure a device to use SSL settings from a particular device group: From the **Select a Device Group** drop-down list in the **SSL global settings** toolbar, choose a device group.

- A device can use its own SSL settings, or the SSL settings from a device group. However, you cannot configure a device to use SSL settings from multiple device group.

- If you have configured a device with specific SSL Accelerated Services and assigned it to a device group, these configurations are lost when you click the **Override Group Settings in the Device Group** > **Configure** > **Security** > **SSL** > **Global Settings** window.

Note If you have configured the device with specific SSL Accelerated Services and assigned it to a Device Group, those configurations are lost when you click on the Override Group Settings on the **Device Group** > **Configure** > **Security** > **SSL** > **Global Settings** window.

Step 4 From the **SSL version** drop-down list, choose the type of SSL protocol to use.

- For the SSL Version 3 protocol, choose **SSL3**.
- For the Transport Layer Security Version 1 protocol, choose **TLS1**.
- To accept both SSL3 and TLS1 SSL protocols, choose **All**.

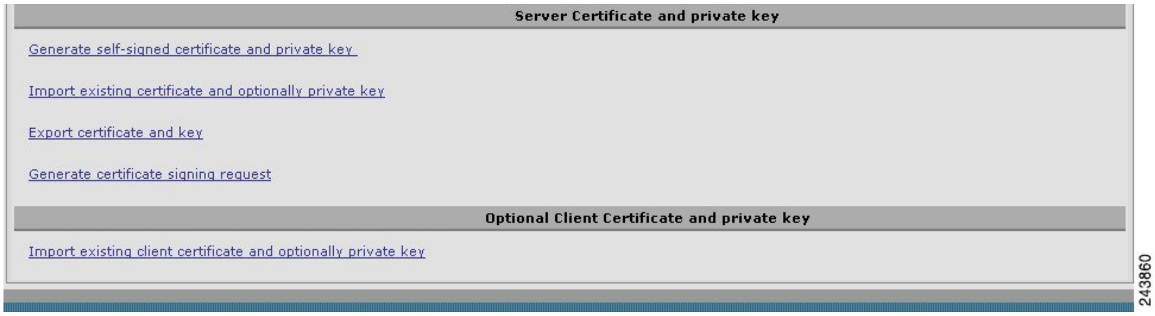
Step 5 (Optional) Set the Online Certificate Status Protocol (OCSP) parameters for certificate revocation:

- From the OCSP Revocation check drop-down list, choose the OCSP revocation method to check the revocation status of certificates:
  - To use the OCSP responder specified in the **OCSP Responder URL** field, choose **ocsp-url**
  - To use the OCSP responder URL specified in the Certificate Authority, choose **ocsp-cert-url**.
- If the **Ignore OCSP failures** check box is checked, the SSL accelerator will treat the OCSP revocation check as successful if it does not get a definite response from the OCSP responder.

Step 6 From the **Cipher List** drop-down list, choose a list of cipher suites to be used for SSL acceleration. For more information, see Working with Cipher Lists, on page 416.

Step 7 Choose a certificate/key pair method.

Figure 63: Configuring Service Certificate and Private Key Window



Server Certificate and private key
Generate self-signed certificate and private key
Import existing certificate and optionally private key
Export certificate and key
Generate certificate signing request
Optional Client Certificate and private key
Import existing client certificate and optionally private key
243860

- To direct Cisco WAAS devices to use a self-signed certificate and key pair for SSL, click **Generate Self-signed Certificate Key**.
- To upload or paste an existing certificate and key pair, click **Import Existing Certificate Key**.
- To export the current certificate and key pair, click **Export Certificate Key**.
- Click **Generate Certificate Signing Request** to renew or replace the existing certificate/key pair. The certificate signing request is used by the CA to generate a new certificate.

  The file that you import or export must be in either a **PKCS12** format or a **PEM** format.

- To use the client configured certificate, click **Import existing client certificate and optionally private key**.

For information about service certificate and private key configuration, see Generating, Importing, or Exporting a Service Certificate and Private Key, on page 413.

Step 8 Click **Submit**.

Generating, Importing, or Exporting a Service Certificate and Private Key

Procedure

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

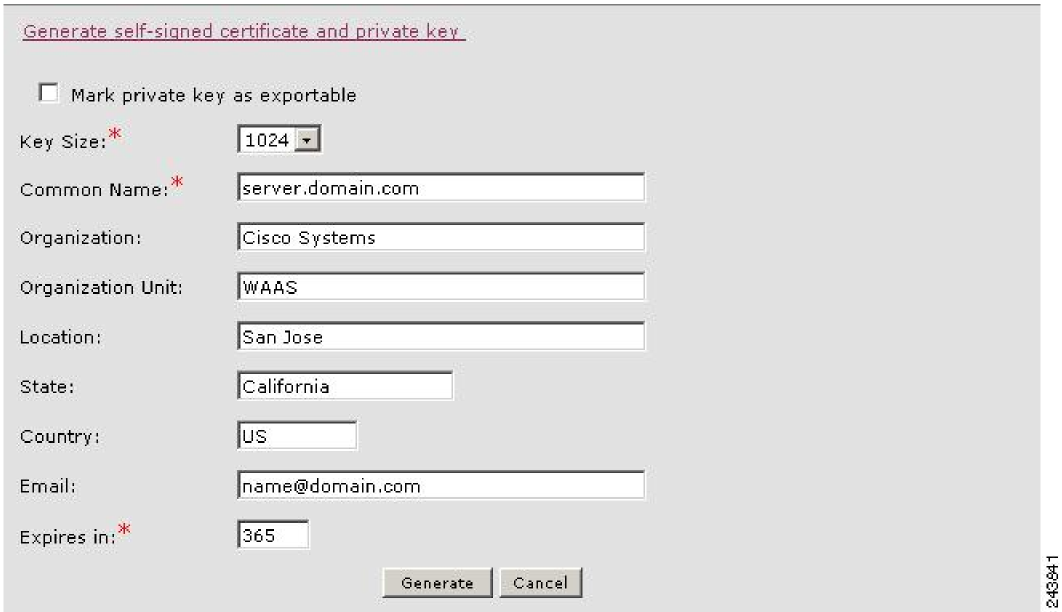
Step 2 Choose **Configure** > **Security** > **SSL** > **Global Settings**.

The **SSL Global Settings** window appears (Figure 62: SSL Global Settings Window).

Step 3 **To generate a self-signed certificate and private key**, at the **Certificate and private key** pane, click **Generate self-signed certificate and private key**.

The **Generate self-signed certificate and private key** window appears.

Figure 64: Generate Self-Signed Certificate and Private Key Window



Generate self-signed certificate and private key

☐ Mark private key as exportable

Key Size:* 1024

Common Name:* server.domain.com

Organization: Cisco Systems

Organization Unit: WAAS

Location: San Jose

State: California

Country: US

Email: name@domain.com

Expires in:* 365

a) To export this certificate/key in the Cisco WAAS Central Manager and device CLI later, check the **Mark private key as exportable** check box.

b) Fill in the certificate and private key fields.

c) Consider the following guidelines for the **Key Size** drop-down list:

Table 47: Key Size Field Guidelines

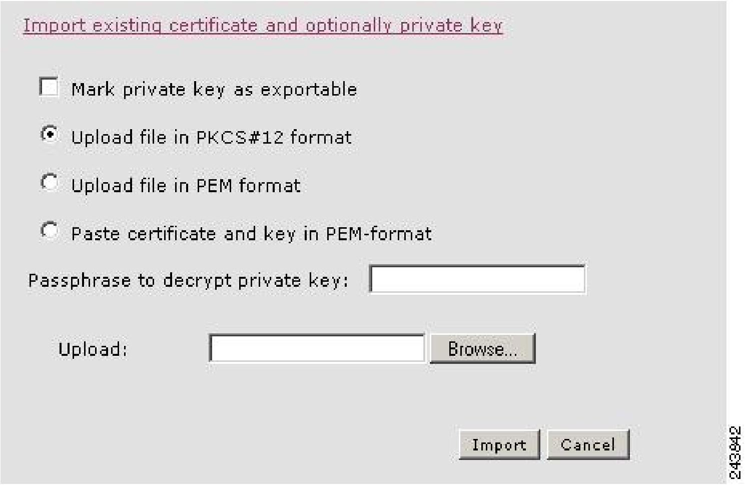
Cisco WAAS Version	Key Size Field Guideline
Cisco WAAS Version 6.1.x and earlier	• The **Key Size** drop-down list values are 512, 768, 1024, 1536, and 2048 • A self-signed certificate with an RSA modulus size of 512 is *not* compatible with Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later. • A self-signed certificate with an RSA modulus size of 512 is compatible with Internet Explorer 8 and later. • If you have previously configured the RSA modulus size as 512: to access the Cisco WAAS Central Manager Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later, you must regenerate the self-signed certificate with an RSA modulus size of 2048, and then upgrade to the specified version of Mozilla FireFox or Google Chrome.
Cisco WAAS Version 6.2.x and later	• The **Key Size** drop-down list values are 768, 1024, 1536, and 2048.

Step 4 **To import an existing certificate or certificate chain and, optionally, private key**:

The Cisco WAAS SSL feature only supports RSA signing/encryption algorithm and keys.

At the **Importing Existing Certificate or Certificate Chain** window:

Figure 65: Importing Existing Certificate or Certificate Chain Window



Import existing certificate and optionally private key

□ Mark private key as exportable

● Upload file in PKCS#12 format

○ Upload file in PEM format

○ Paste certificate and key in PEM-format

Passphrase to decrypt private key:

Upload:

a) Check the **Mark private key as exportable** check box to export this certificate/key in the WAAS Central Manager and device CLI later.

b) To import existing certificate or certificate chain and private key, perform one of the following tasks:

- **Upload the certificate and key in PKCS#12 format** (also as known Microsoft PFX format)
- **Upload the certificate and private key in PEM format**

- **Paste the certificate and private key PEM content**

Consider the following operating guidelines for importing an existing certificate or certificate chain and private key:

- If the certificate and private key are already configured, you can update only the certificate. In this case, the Cisco WAAS Central Manager constructs the certificate and private key pair using the imported certificate and current private key. This functionality can be used to update an existing self-signed certificate to one signed by the CA, or to update an expiring certificate.
- The Cisco WAAS Central Manager allows importing a certificate chain consisting of an end certificate that must be specified first, a chain of intermediate CA certificates that sign the end certificate or intermediate CA certificate, and end with a root CA.
- The Cisco WAAS Central Manager validates the chain and rejects it if the validity date of the CA certificate is expired, or the signing order of certificates in the chain is not consequent.

c) At the **Upload** field, use the **Browse** button to browse to the file and then select it.
d) In the **Passphrase to decrypt private key** field, enter a passphrase to decrypt the private key. If the private key is not encrypted, leave this field blank.

Step 5 **To export a configured certificate and private key**, in the **Export Certificate and Key** window:

a) In the **Encryption pass-phrase** field, enter the encryption pass-phrase.
b) Export current certificate and private key in either PKCS#12 or PEM formats. In the case of PEM format, the both certificate and private key are included in single PEM file.

The Cisco WAAS Central Manager will not allow the export of certificate and private key if the certificate and key were marked as nonexportable when they were generated or imported.

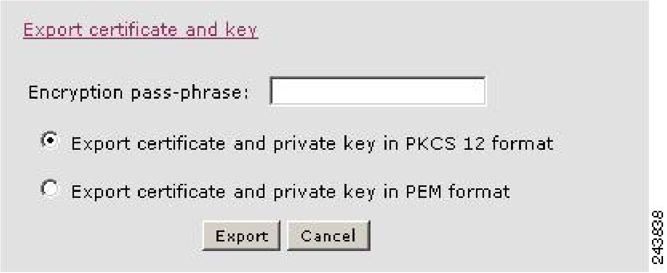
Step 6 **To generate a certificate-signing request from a current certificate and private key**, in the **Generate Certificate-Signing Request** window, follow these steps:

Step 7 To update the current certificate with one signed by the Certificate Authority, follow these steps:

a) At the **Certificate and private key** pane, click **Export certificate and key**.

The **Export certificate and key** window appears.

Figure 66: Export Certificate and Key Window



Export certificate and key

Encryption pass-phrase:

● Export certificate and private key in PKCS 12 format

○ Export certificate and private key in PEM format

b) In the **Encryption pass-phrase** field, enter the encryption passphrase.
c) Choose an export format for the certificate:

- **Export certificate and private key in PKCS 12 format**
- **Export certificate and private key in PEM format**

For PEM format, both the certificate and private key are included in a single PEM file

Note The Cisco WAAS Central Manager does not allow the export of certificate and private key if the certificate and key were marked as nonexportable when they were generated or imported.

Working with Cipher Lists

Before you begin

Cipher lists are sets of cipher suites that you can assign to your SSL acceleration configuration. A cipher suite is an SSL encryption method that includes the key exchange algorithm, the encryption algorithm, and the secure hash algorithm.

For dual-sided deployments that use SMART-SSL acceleration, only **rsa-with-aes-256-cbc-sha** is supported.

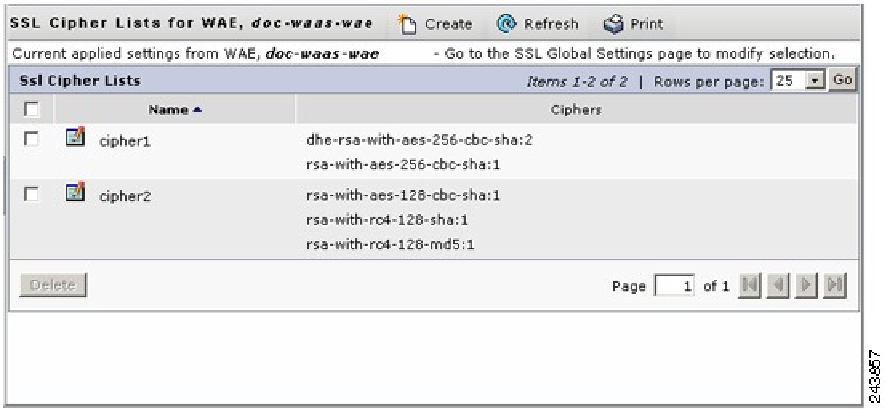
Procedure

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

Step 2 Choose **Configure > Security > SSL > Cipher Lists**.

The **SSL Cipher Lists** window appears.

Figure 67: SSL Cipher Lists Window



SSL Cipher Lists for WAE, *doc-waas-wae*

Current applied settings from WAE, *doc-waas-wae* - Go to the SSL Global Settings page to modify selection.

Ssl Cipher Lists *Items 1-2 of 2* | Rows per page: 25

□	Name ▲	Ciphers
□	cipher1	dhe-rsa-with-aes-256-cbc-sha:2 rsa-with-aes-256-cbc-sha:1
□	cipher2	rsa-with-aes-128-cbc-sha:1 rsa-with-rc4-128-sha:1 rsa-with-rc4-128-md5:1

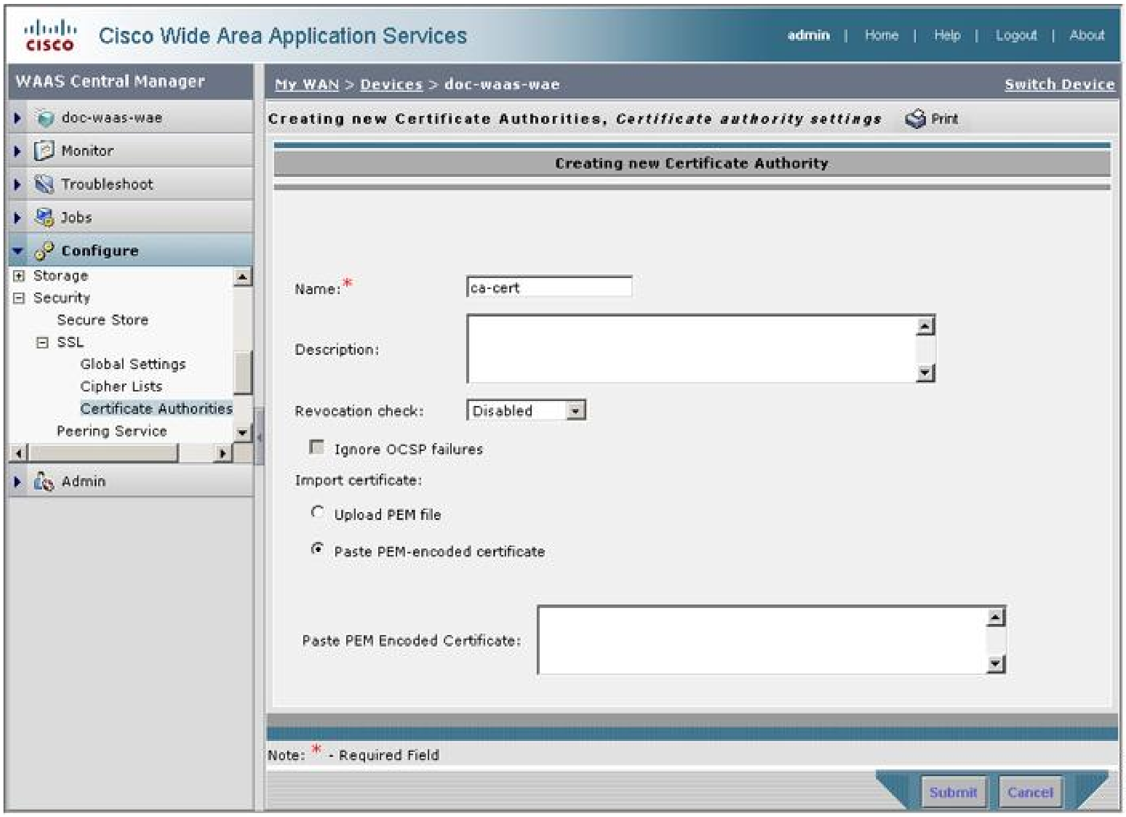
Page 1 of 1

For a Cisco WAAS Express device, the SSL Cipher Lists window shows the same name and cipher fields, but in a slightly different format.

Step 3 To add a new cipher list, click **Create**.

The **Creating New SSL Cipher List** window appears.

Figure 68: Creating New SSL Cipher List Window



Creating new Certificate Authorities, *Certificate authority settings*

Creating new Certificate Authority

Name:* ca-cert

Description:

Revocation check: Disabled

□ Ignore OCSP failures

Import certificate:

○ Upload PEM file

● Paste PEM-encoded certificate

Paste PEM Encoded Certificate:

Note: * - Required Field

To add a new cipher list for a Cisco WAAS Express device, click **Add Cipher List**.

Step 4 In the Cipher List Name field, type a name for your cipher list.

Step 5 To add cipher suites to your cipher list, click **Add Cipher**.

Note For a Cisco WAAS Express device, select the ciphers you wish to add, and proceed to Step 12.

Step 6 From the **Ciphers** drop-down list, choose the cipher suite that you want to add.

Note If you are establishing an SSL connection to a Microsoft IIS server, do not select a DHE-based cipher suite.

Step 7 From the **Priority** drop-down list, choose the priority for the selected cipher suite.

Note When SSL peering service is configured, the priority associated with a cipher list on a core device takes precedence over the priority associated with a cipher list on an edge device.

Step 8 To include the selected cipher suite on your cipher list, click **Add**. To leave the list as it is, click **Cancel**.

Step 9 To add more cipher suites to your list as desired, repeat Step 5 through Step 8 .

Step 10 (Optional) To change the priority of a cipher suite, check the cipher suite check box and then use the up or down arrow buttons located below the cipher list to prioritize.

Note The client-specified order for ciphers overrides the cipher list priority assigned here if the cipher list is applied to an accelerated service. The priorities assigned in this cipher list are only applicable if the cipher list is applied to SSL peering and management services.

Step 11 (Optional) To remove a cipher suite from the list, check the cipher suite's box and then click **Delete**.

Step 12 After you have completed configuring the cipher list, click **Submit**.

Note To save the cipher list configuration for a Cisco WAAS Express device, click **OK**. SSL configuration changes are not applied on the device until the security license has been enabled on the device.

Working with CA Certificates

Before you begin

Use the Cisco WAAS SSL acceleration feature to configure the Certificate Authority (CA) certificates used by your system. You can use one of the many CA certificates included with Cisco WAAS, or import your own CA certificate.

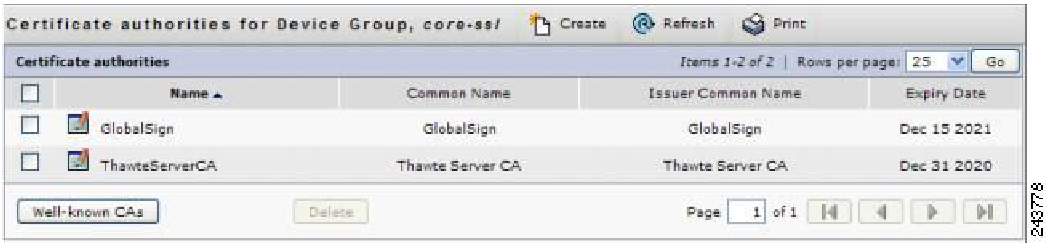
Procedure

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

Step 2 Choose **Configure** > **Security** > **SSL** > **Certificate Authorities**.

The **SSL CA Certificate List** window appears.

Figure 69: SSL CA Certificate List Window



Certificate authorities for Device Group, *core-ssl*

Certificate authorities *Items 1-2 of 2* | Rows per page: 25 Go

□	Name ▲	Common Name	Issuer Common Name	Expiry Date
□	GlobalSign	GlobalSign	GlobalSign	Dec 15 2021
□	ThawteServerCA	Thawte Server CA	Thawte Server CA	Dec 31 2020

For a Cisco WAAS Express device, the **SSL CA Certificate List** window shows the same **Name**, **Issued To**, **Issuer**, and **Expiry Date** fields, but in a slightly different format. There is also an **Aggregate Settings** field configurable as **Yes** or **No**. To finish the procedure for Cisco WAAS Express, proceed to Step 4 .

Step 3 To add one of the preloaded CA certificates that is included with Cisco WAAS:

a) Click **Well-known CAs**.

b) Choose the pre-existing CA certificate you want to add and click **Import**.

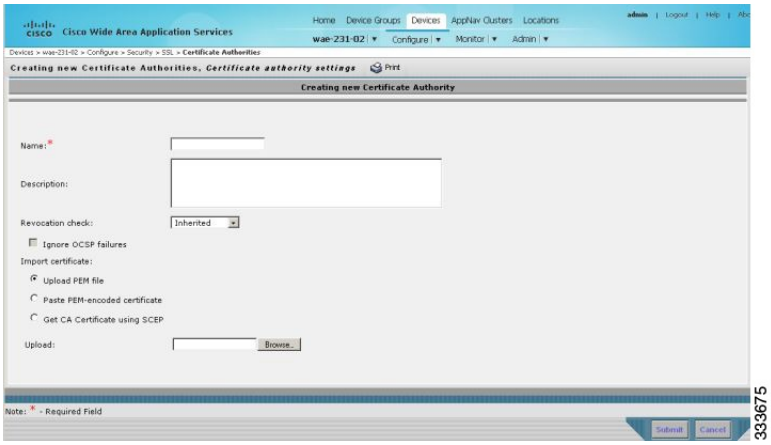
The selected CA certificate is added to the list on the **SSL CA Certificate List** display.

Step 4 To add your own CA certificate:

a) Click **Create**.

The **Creating New CA Certificate** window appears.

Figure 70: Creating New CA Certificate Window


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
admin | Logout | Help | Abc
wae-231-02
Configure
Monitor
Admin
Devices > wae-231-02 > Configure > Security > SSL > Certificate Authorities
Print
Browse..
Submit
Cancel
333675

Creating new Certificate Authorities, *Certificate authority settings*

Creating new Certificate Authority

Name:*

Description:

Revocation check: Inherited

□ Ignore OCSP failures

Import certificate:

● Upload PEM file

○ Paste PEM-encoded certificate

○ Get CA Certificate using SCEP

Upload:

Note: * - Required Field

For a Cisco WAAS Express device, click **Add CA** to add your own CA certificate. Enter the name and the URL, and then click **Get CA** Certificate. After this, proceed to Step 6.

b) In the **Certificate Name** field, type a name for the certificate.

c) (Optional) In the **Description** field, type a description of the CA certificate.

d) From the **Revocation** check drop-down list, choose **Disable** to disable OCSP revocation of certificates signed by this CA. Check the **Ignore OCSP failures** check box to mark revocation check successful if the OCSP revocation check failed.

e) To add the certificate information, choose one of the following:

- **Upload PEM File**

  If you are uploading a file, it must be in a PEM format. Browse to the file that you want to use and click **Upload**.

- **Paste PEM-encoded Certificate**

  If you are pasting the CA certificate information, paste the text of the PEM format certificate into the **Paste PEM-encoded certificate** field.

- **Get CA Certificate using SCEP**

  This option automatically configures the certificate authority using Simple Certificate Enrollment Protocol (SCEP). If you are using the automated certificate enrollment procedure, enter the CA URL and click **Get Certificate**. The contents of the certificate are displayed in text and PEM formats.

  To complete the automated certificate enrollment procedure, configure the SSL auto enrollment settings in Configuring SSL Auto Enrollment, on page 420.

f) Click **Submit** to save your changes.

Step 5 (Optional) To remove a CA from the list, select it and then click the **Delete** icon located in the toolbar.

Step 6 After you have completed configuring the CA certificate list, click **Submit**.

For a Cisco WAAS Express device, click **OK** to save the CA certificate configuration.

Configuring SSL Auto Enrollment

Before you begin

The Cisco WAAS SSL acceleration feature allows you to enroll certificates automatically for a device (or device group) using Simple Certificate Enrollment Protocol (SCEP). After the CA certificate is obtained, configure the SSL auto enrollment settings.

You must configure the CA authority before configuring auto enrollment settings.

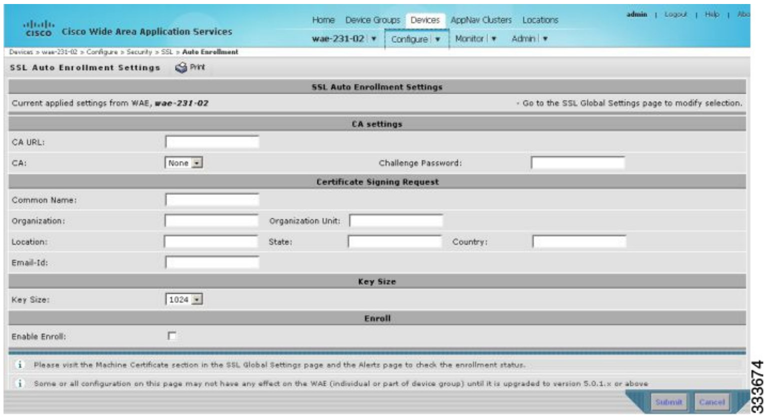
Procedure

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

Step 2 Choose **Configure** > **Security** > **SSL** > **Auto Enrollment**.

The **SSL Auto Enrollment Settings** window appears.

Figure 71: SSL Auto Enrollment Settings Window


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
admin | Logout | Help | Abo
wae-231-02 ▾
Configure ▾
Monitor ▾
Admin ▾
Devices > wae-231-02 > Configure > Security > SSL > Auto Enrollment
Print
Submit
Cancel
333674

SSL Auto Enrollment Settings

SSL Auto Enrollment Settings

Current applied settings from WAE, ***wae-231-02*** · Go to the SSL Global Settings page to modify selection.

CA settings					
CA URL:					
CA:	None ▾			Challenge Password:	
Certificate Signing Request					
Common Name:					
Organization:		Organization Unit:			
Location:		State:		Country:	
Email-Id:					
Key Size					
Key Size:	1024 ▾				
Enroll					
Enable Enroll:	□				

i Please visit the Machine Certificate section in the SSL Global Settings page and the Alerts page to check the enrollment status.

i 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 5.0.1.x or above

Step 3 Configure the following CA settings:

- CA URL
- CA: Select the appropriate CA from the drop-down list
- Challenge Password

CA, CA URL, and Challenge Password are mandatory for enabling SSL auto enrollment.

Step 4 Configure the following **Certificate Signing Request** settings:

- Common Name
- Organization and Organization Unit
- Location, State, and Country
- Email-Id

Step 5 From the **Key Size** drop-down list, choose the key size. Valid values are **512**, **768**, **1024**, **1536**, or **2048**.

Step 6 Check the **Enable Enroll** box.

Step 7 Click **Submit**.

After you have submitted the settings, you can check the enrollment status in the **Machine Certificate** section in the **SSL Global Settings** window and in the **Alerts** window.

Configuring SSL Admin Service

Before you begin

To enable trusted SSL communication between the Cisco WAAS Central Manager the web browser, export the SSL CA signed certificate. The default certificate for enabling SSL communication is the Cisco WAAS Central Manager self signed certificate. To use a different certificate, you must configure it.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > **CM** > **Configure** > **Security** > **SSL Admin Service**.

The default certificate is displayed.

Step 2 Select the PKI operation

a) To upload or paste an existing certificate and key pair, click **Import Existing Certificate Key**.

b) To export the current certificate and key pair, click **Export Certificate Key**.

The file that you import or export must be in either a PKCS12 format or a Privacy Enhanced Mail (PEM) format.

c) To configure the Cisco WAAS Central Manager and Cisco WAAS device to use a self-signed certificate and key pair for SSL, click **Generate Self-signed Certificate Key**.

Operating Considerations for **Key Size** field:

Cisco WAAS Version 6.1.x and earlier

- The **Key Size** drop-down list values are **512**, **768**, **1024**, **1536**, and **2048**.
- A self-signed certificate with an RSA modulus size of **512** is *not* compatible with Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later.
- A self-signed certificate with an RSA modulus size of **512** *is* compatible with Internet Explorer 8 and later.
- If you have previously configured the RSA modulus size as **512**: to access the Cisco WAAS Central Manager Mozilla FireFox Version 39 and later, or with Google Chrome Version 48 and later, you must regenerate the self-signed certificate with an RSA modulus size of **2048**, and then upgrade to the specified version of Mozilla FireFox or Google Chrome.

Cisco WAAS Version 6.2.x and later

- The **Key Size** drop-down list values are **768**, **1024**, **1536**, and **2048**.

- The key size **512** is *not* used with WAAS Version 6.2.x and later.

Step 3 Click Submit to register the certificate.

Step 4 To register the certificate, click **Submit**.

The Cisco WAAS Central Manager now uses the specified certificate for SSL communication.

Configuring SSL Management Services

Before you begin

SSL management services are the SSL configuration parameters that affect secure communications between the Cisco WAAS Central Manager and the Cisco WAE devices. The certificate and key pairs used are unique for each Cisco WAAS device. Therefore, SSL management services can only be configured for individual devices, not device groups.

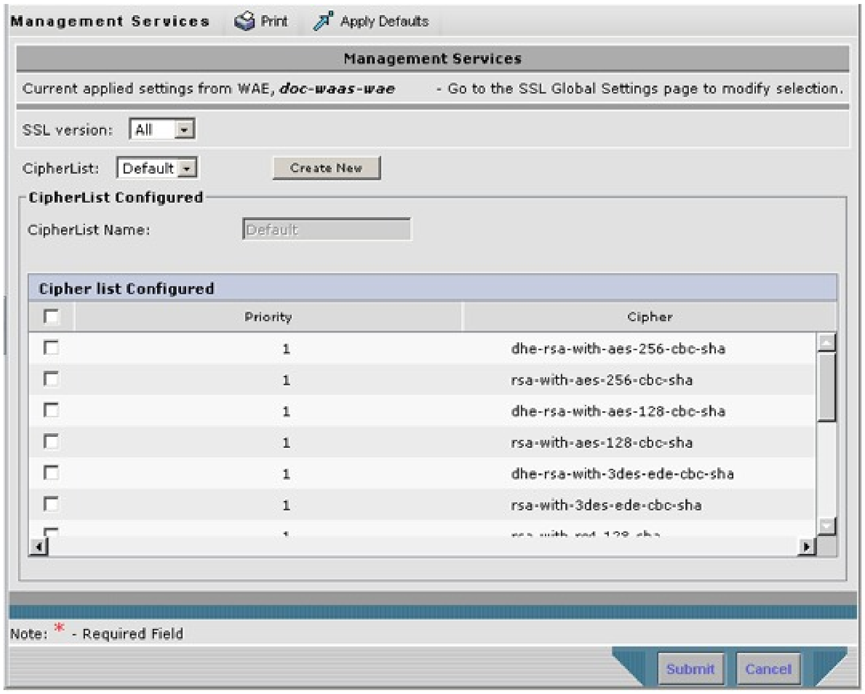
Procedure

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

Step 2 Choose **Configure** > **Security** > **Management Service**.

The **Management Services** window appears.

Figure 72: SSL Management Services Window



Management Services

Current applied settings from WAE, ***doc-waas-wae*** - Go to the SSL Global Settings page to modify selection.

SSL version: All

CipherList: Default

CipherList Configured

CipherList Name: Default

Cipher list Configured

□	Priority	Cipher
□	1	dhe-rsa-with-aes-256-cbc-sha
□	1	rsa-with-aes-256-cbc-sha
□	1	dhe-rsa-with-aes-128-cbc-sha
□	1	rsa-with-aes-128-cbc-sha
□	1	dhe-rsa-with-3des-ede-cbc-sha
□	1	rsa-with-3des-ede-cbc-sha
□	1	rsa-with-rc4-128-sha

Note: * - Required Field

Step 3 From the **SSL version** drop-down list, choose the type of SSL protocol to use:

- To use the SSL Version 3 protocol, choose **SSL3**.
- To use the Transport Layer Security Version 1 (TLS Version 1) protocol, choose **TLS1**.
- To use both SSL Version 3 and TLS Version 1 protocols, choose **All**.

Consider the following configuration guidelines for SSL connections:

- Management-service SSL version and cipher settings configured for the Cisco WAAS Central Manager are also applied to SSL connections between the Cisco WAAS Central Manager and the browser of the user.
- Primary and standby Cisco WAAS Central Managers must share a common management service version or cipher list. Changing the management service version and cipher list settings may result in a loss of connectivity between the primary Cisco WAAS Central Manager and the standby Cisco WAAS Central Manager and Cisco WAE devices.

The following cipher lists are supported in SSL Acceleration (Legacy SSL Acceleration).

- dhe-rsa-with-aes-256-cbc-sha
- rsa-with-aes-256-cbc-sha
- dhe-rsa-with-aes-128-cbc-sha
- rsa-with-aes-128-cbc-sha
- dhe-rsa-with-3des-ede-cbc-sha
- rsa-with-3des-ede-cbc-sha
- rsa-with-rc4-128-sha
- rsa-with-rc4-128-md5
- dhe-rsa-with-des-cbc-sha
- rsa-export1024-with-rc4-56-sha
- rsa-export1024-with-des-cbc-sha
- dhe-rsa-export-with-des40-cbc-sha
- rsa-export-with-des40-cbc-sha
- rsa-export-with-rc4-40-md5
- rsa-with-des-cbc-sha

Consider the following configuration guidelines for ciphers:

- All browsers support SSLv3 and TLSv1 protocols, but TLSv1 may not be enabled by default on certain browsers. Therefore, you must enable it in your browser.
- Configuring ciphers or protocols that are not supported in your browser will result in connection loss between the browser and the Cisco WAAS Central Manager. If this occurs, to restore the connection: configure the Cisco WAAS Central Manager management service SSL settings to the default in the Cisco WAAS CLI to restore the connection.

Some browsers, such as Internet Explorer, do not correctly handle a change of SSL version and cipher settings on the Cisco WAAS Central Manager, which can result in the browser showing an error page after you submit the changes. If this occurs, reload the page.

- To configure additional ciphers, see the supported ciphers in Preparing to Use SMART-SSL Acceleration.

Step 4 At the **Cipher List** pane, choose a list of cipher suites to be used for SSL acceleration. For more information, see Working with Cipher Lists, on page 416 for additional information.

Configuring SSL Peering Service

Before you begin

SSL peering service configuration parameters control the secure communications established by the SSL accelerator between WAE devices while optimizing SSL connections. The peering service certificate and private key is unique for each WAAS device and can only be configured for individual devices, not device groups.

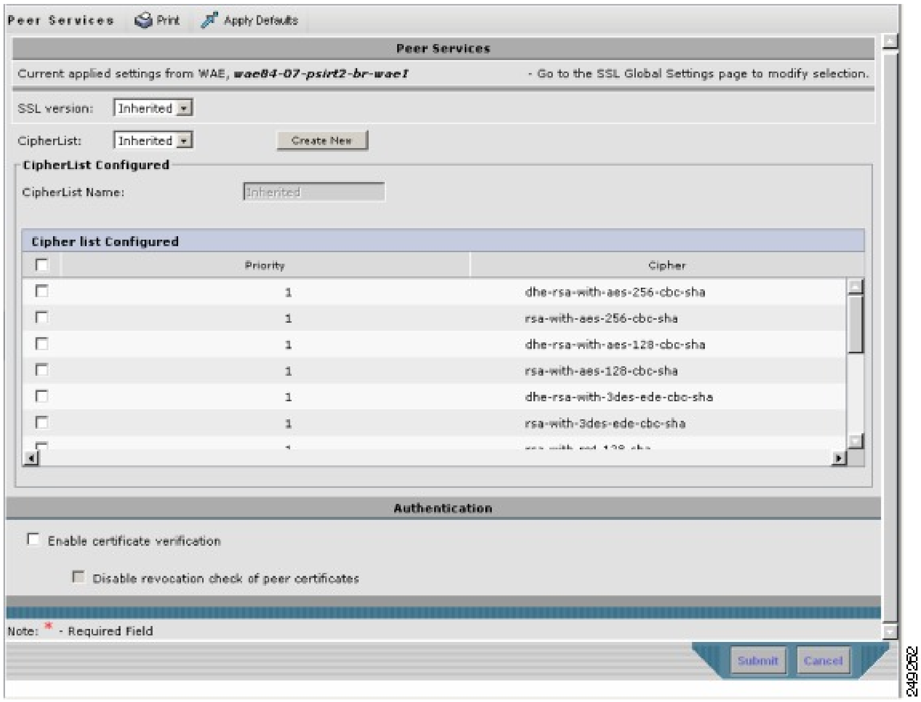
Procedure

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

Step 2 Choose **Configure** > **Security** > **Peering Service**.

The **Peering Service** window appears.

Figure 73: SSL Peering Service Window



Peer Services

Current applied settings from WAE, ***wae84-07-psirt2-br-wae1*** - Go to the SSL Global Settings page to modify selection.

SSL version: Inherited ▾

CipherList: Inherited ▾ Create New

CipherList Configured

CipherList Name: Inherited

Cipher list Configured

□	Priority	Cipher
□	1	dhe-rsa-with-aes-256-cbc-sha
□	1	rsa-with-aes-256-cbc-sha
□	1	dhe-rsa-with-aes-128-cbc-sha
□	1	rsa-with-aes-128-cbc-sha
□	1	dhe-rsa-with-3des-ede-cbc-sha
□	1	rsa-with-3des-ede-cbc-sha
□	1	rsa-with-rc4-128-sha

Authentication

□ Enable certificate verification

□ Disable revocation check of peer certificates

Note: * - Required Field

Consider the following guidelines for Cisco WAAS Express:

- For a Cisco WAAS Express device, the **Peering Service** window displays a subset of the fields in the standard **Peering Service** window in a slightly different format.
- The cipher list **Priority** setting and the **Disable revocation check of peer certificates** options are not applicable to Cisco WAAS Express.

Step 3 From the **SSL Version** drop-down list, choose the type of SSL protocol to use:

- For the SSL Version 3 protocol, choose **SSL3**.
- For the Transport Layer Security Version 1 protocol, choose **TLS1**.
- To accept both SSL3 and TLS1 SSL protocols, choose **All**

  .
- To use the protocol configured in **Global SSL Settings**, choose **Inherited**.

Consider the following SSL guidelines:

- For dual-sided deployments that use SMART-SSL acceleration, SSLv3, TLS1.0, TLS1.1, and TLS1.2 are supported.
- In a Cisco WAAS Express device, only SSL3 and TLS1 are supported for the SSL version.

Step 4 To enable verification of peer certificates, check the **Enable Certificate Verification** check box.

- If certificate verification is enabled, WAAS devices that use self-signed certificates will not be able to establish peering connections to each other and, thus, not be able to accelerate SSL traffic.
- For dual-sided deployments that use SMART-SSL acceleration, you can use your certificate or use the peer certificate.

Step 5 To disable OCSP certificate revocation checking, check the **Disable revocation check for this service check box**.

This option is not available for Cisco WAAS Express devices.

Step 6 At the **Cipher List** pane, choose a list of cipher suites to be used for SSL acceleration between the WAE device peers.

- To use the cipher list configured in SSL Global Settings, choose **Inherited**.
- For dual-sided deployments that use SMART-SSL acceleration, only **rsa-with-aes-256-cbc-sha** is supported.
- In a Cisco WAAS Express device, the list of cipher suites to be used for SSL acceleration is displayed in the **Cipher List** pane.
- For more information, see Working with Cipher Lists.

Step 7 Click **Submit**.

For a Cisco WAAS Express device, SSL configuration changes will not be applied on the device until the security license has been enabled on the device.

Using SSL Accelerated Services

Before you begin

After you have enabled and configured SSL acceleration on your WAAS system, you must define at least one service to be accelerated on the SSL path.

For Cisco WAAS Version 6.4.3 and later, the SMART- SSL feature has been enhanced to allow you more control of SSL traffic.

- Use the DSCP marking feature for optimized traffic, which allows better QoS management for the overall network.
- Configure more than one service with same port and “Any” Server IP address. However, the secondary flag should be marked to differentiate services with multiple Any/Port which have already been added by other service. Once configured, this is reflected in **Devices >** *device-name* or **Device Groups >** *device-group-name* **> Configure > Acceleration > SSL Accelerated Services**.

To modify the secondary flag the following conditions should be met.

- You should mark a service as Secondary to proceed with IP Any and same port.Once a service is marked as secondary no other IP Any is allowed, but you can add different IP with ports, server, name and domain name to the secondary service.
- You cannot mark a service as Secondary without "Any" server address configuration.
- You cannot remove the Secondary settings if the SSL accelerated service is enabled.
- The above features are visible on the Cisco WAAS Central Manager only when the devices are running Cisco WAAS Version 6.4.3 and later.

Procedure

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

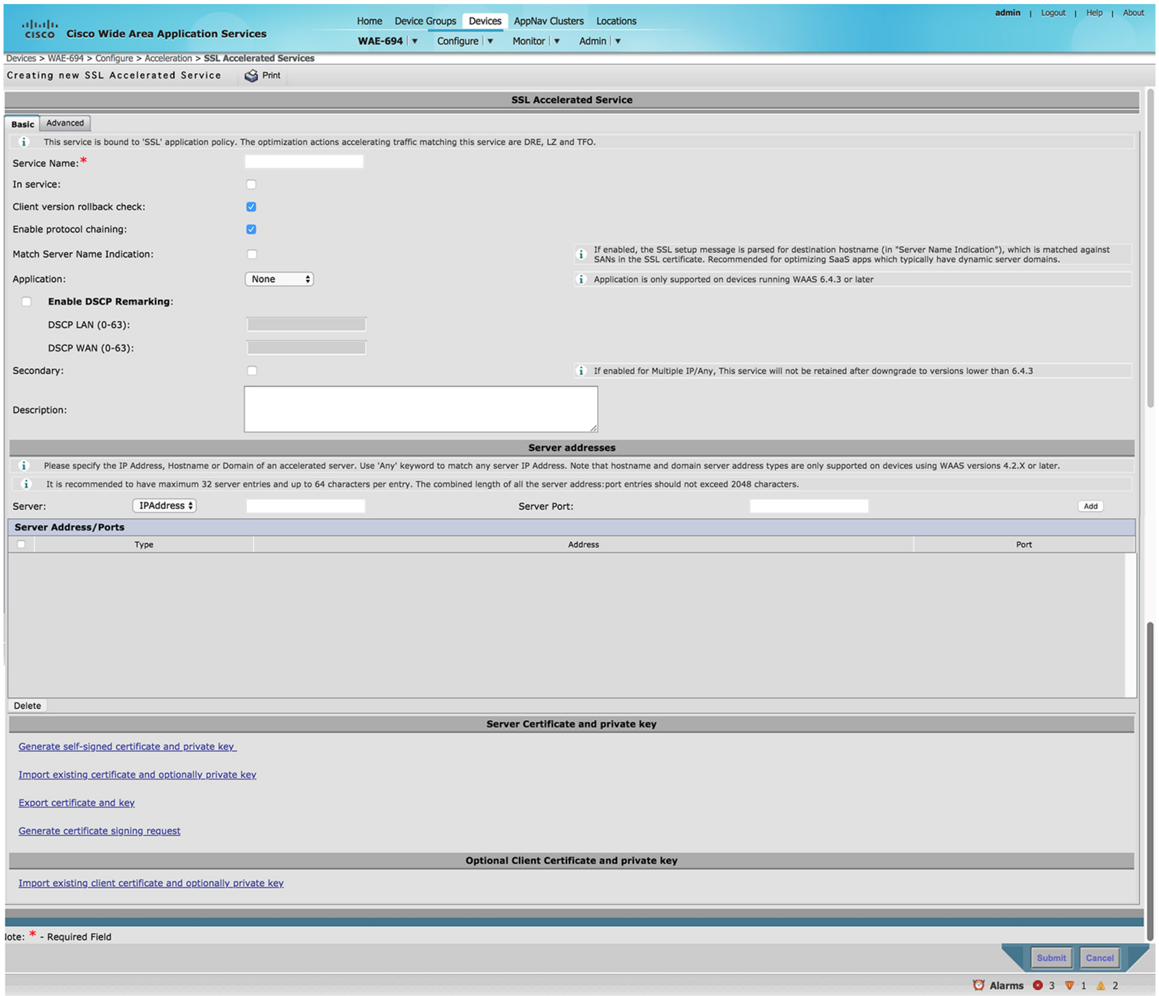
Step 2 Choose **Configure** > **Acceleration** > **SSL Accelerated Services**.

Step 3 To delete an accelerated service, select the service and click **Delete**.

Step 4 To define a new accelerated service, click **Create**. A maximum of 512 accelerated services are allowed.

The **Basic SSL Accelerated Services Configuration** window appears.

Figure 74: SSL-Accelerated Services (Basic tab) Window


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
WAE-694
Configure
Monitor
Admin
admin | Logout | Help | About
Devices > WAE-694 > Configure > Acceleration > SSL Accelerated Services
Print
Basic
Advanced
Add
Delete
Submit
Cancel
Alarms 3 1 2

Creating new SSL Accelerated Service

SSL Accelerated Service

This service is bound to 'SSL' application policy. The optimization actions accelerating traffic matching this service are DRE, LZ and TFO.

Service Name:*

In service: □

Client version rollback check: ☑

Enable protocol chaining: ☑

Match Server Name Indication: □

If enabled, the SSL setup message is parsed for destination hostname (in "Server Name Indication"), which is matched against SANs in the SSL certificate. Recommended for optimizing SaaS apps which typically have dynamic server domains.

Application: None

Application is only supported on devices running WAAS 6.4.3 or later

□ **Enable DSCP Remarking**:

DSCP LAN (0-63):

DSCP WAN (0-63):

Secondary: □

If enabled for Multiple IP/Any, This service will not be retained after downgrade to versions lower than 6.4.3

Description:

Server addresses

Please specify the IP Address, Hostname or Domain of an accelerated server. Use 'Any' keyword to match any server IP Address. Note that hostname and domain server address types are only supported on devices using WAAS versions 4.2.X or later.

It is recommended to have maximum 32 server entries and up to 64 characters per entry. The combined length of all the server address:port entries should not exceed 2048 characters.

Server: IPAddress   Server Port:

Server Address/Ports

□	Type	Address	Port

Server Certificate and private key

Generate self-signed certificate and private key

Import existing certificate and optionally private key

Export certificate and key

Generate certificate signing request

Optional Client Certificate and private key

Import existing client certificate and optionally private key

lote: * - Required Field

Step 5 At the **SSL Accelerated Service** pane:

a) In the **Service Name** field, enter a name for the service.

b) To enable this accelerated service, check the **In service** check box.

c) To enable client version rollback check, check the **Client version rollback** check check box.

Enabling the client version rollback check does not allow connections with an incorrect client version to be optimized.

d) To match subject alternative names, check the **Match Server Name Indication** check box.

For more information, see Configuring SSL Acceleration for SaaS Applications.

e) To enable protocol chaining, check the **Enable protocol chaining** check box.

Enabling protocol chaining allows other protocols to be optimized over SSL.

f) From the **Application** drop-down list, choose the SAAS application that needs to be optimized.

This field is visible only on the devices that are running Cisco WAAS Version 6.4.3 or later.

g) Check the **Enable DSCP Remarking** and enter values in the **DSCP LAN** and **DSCP WAN** fields. The available values are **0** to **63**.

- The **Enable DSCP Remarking** check box is unchecked (disabled) by default.
- For this configuration to be applicable to all devices that are part of a device group, all devices in the device group must be running Cisco WAAS Version 6.4.3 or later. If any of the devices has a version earlier than Cisco WAAS Version 6.4.3, the configurations will not apply to that device.

h) To configure the accelerated service to use multiple IP addresses, check the **Secondary** checkbox.

This is applicable only for Cisco WAAS devices running Cisco WAAS Version 6.4.3 or later.

- (Optional) In the **Description** field, enter a description.

Checking the **Secondary** check box ensures the following actions for this accelerated service:

- This accelerated service is distinguished from the primary accelerated service using multiple IP addresses.
- This accelerated service is not pushed down to other devices that are part of the device group that are running a Cisco WAAS version that is earlier than Cisco WAAS Version 6.4.3.
- This accelerated service is removed during a downgrade.

Step 6 At the **Server addresses** pane:

a) From the **Server** drop-down list, choose **IP Address**, **Hostname**, or **Domain as the SSL service endpoint** type.

b) In the associated **Server** field, enter one of the following:

- **Server IP address** (or **proxy IP address**) of the accelerated server, up to a maximum of 32 IP addresses.To specify any server IP address, use the keyword Any. Server IP address keyword Any is supported for Cisco WAAS Software Version 4.2.x and later.
- **Hostname** of the accelerated server, up to a maximum of 32 hostnames. Hostname server address type is supported for Cisco WAAS Version 4.2.x and later.
- **Domain** of the accelerated server, up to a maximum of 32 domains. Domain server address type is supported for Cisco WAAS Version 4.2.x and later.

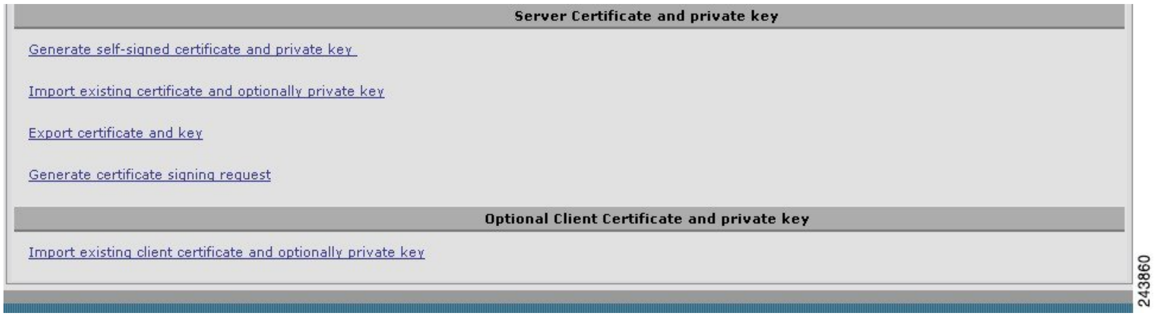
c) At the **Server Port** field, enter the port associated with the service to be accelerated.

Step 7 Click **Add** to add each address. If you specify a server hostname, the Cisco WAAS Central Manager resolves the hostname to the IP address and adds it to the **Server IP/Ports** table.

Step 8 To remove an IP address from the list, click **Delete**.

Step 9 Choose a certificate and key pair method.

Figure 75: Configuring Service Certificate and Private Key



Server Certificate and private key

Generate self-signed certificate and private key

Import existing certificate and optionally private key

Export certificate and key

Generate certificate signing request

Optional Client Certificate and private key

Import existing client certificate and optionally private key

- At the **Server Certificate and private key** pane:
  - To configure the Cisco WAAS devices to use a self-signed certificate and key pair for SSL, click **Generate self-signed certificate key**.
  - To upload or paste an existing certificate and key pair, click **Import Existing Certificate Key**.

    For SaaS applications, the certificate must have the Subject Alternative Name (SAN) information.
  - To export the current certificate and key pair, click **Export Certificate Key**.
  - To renew or replace the existing certificate and key pair, click **Generate Certificate Signing Request**. The certificate signing request is used by the CA to generate a new certificate.

    The file to be imported or exported must be in either PKCS12 format or PEM format.
  - To use the client configured certificate, click **Import existing client certificate and optionally private key**.

Step 10 (Optional) To change the service certificate or private key for an existing SSL-accelerated service, follow these guidelines:

a) At the **SSL Accelerated Service** pane, uncheck the In service check box.

b) To disable the service, click **Submit**, and then wait five minutes.

c) Check the **In service** check box.

d) To re-enable the service, click **Submit**.

e) Alternatively, in the Cisco WAE CLI:

- Run the **no inservice** SSL-accelerated service configuration command.
- Wait a few seconds.
- Run the **inservice** SSL-accelerated service configuration command.

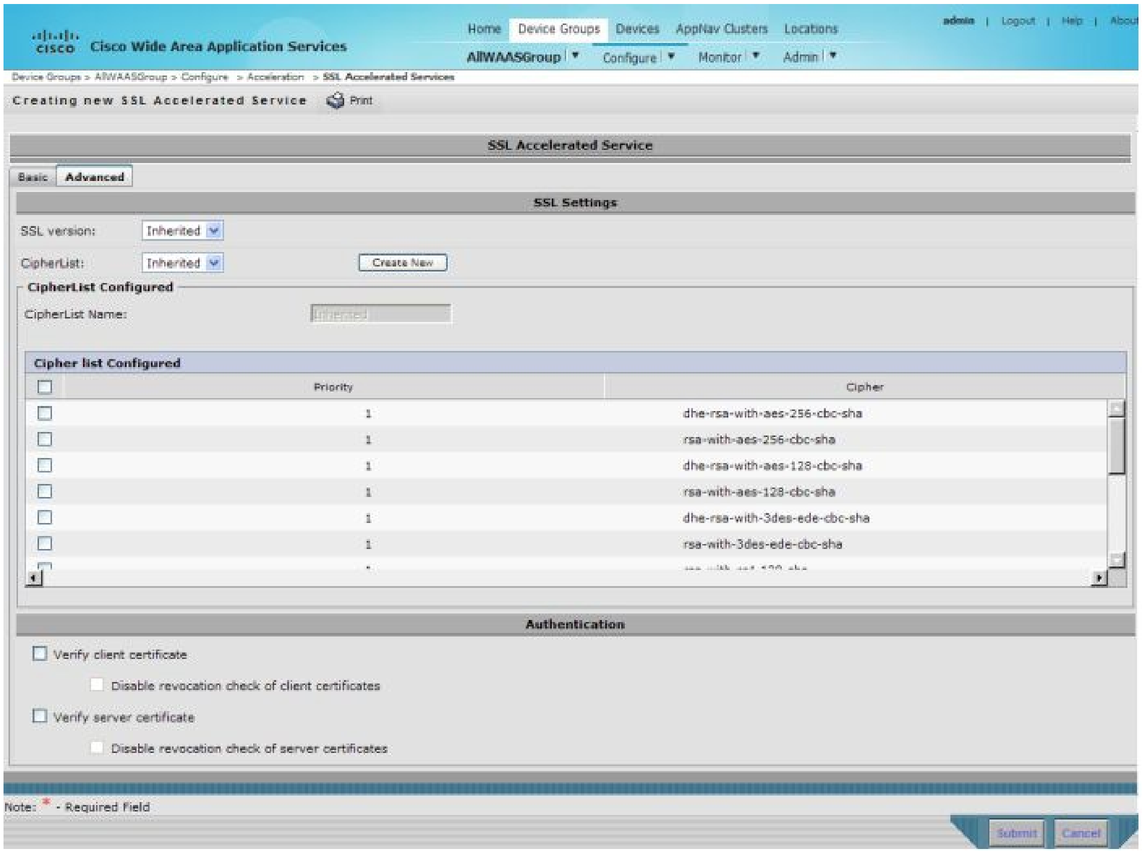
To change the service certificate or private key for multiple SSL-accelerated services, restart all the accelerated services by disabling and then re-enabling the SSL accelerator.

For service certificate and private key configuration steps, see Generating, Importing, or Exporting a Service Certificate and Private Key.

Step 11 To configure SSL parameters for the service, click the **Advanced Settings** tab.

The **SSL Accelerated Services Configuration** window, **Advanced** tab appears.

Figure 76: SSL Accelerated Services (Advanced tab) Window



SSL version: Inherited

CipherList: Inherited

CipherList Configured

CipherList Name: Inherited

Cipher list Configured

□	Priority	Cipher
□	1	dhe-rsa-with-aes-256-cbc-sha
□	1	rsa-with-aes-256-cbc-sha
□	1	dhe-rsa-with-aes-128-cbc-sha
□	1	rsa-with-aes-128-cbc-sha
□	1	dhe-rsa-with-3des-ede-cbc-sha
□	1	rsa-with-3des-ede-cbc-sha

□ Verify client certificate

□ Disable revocation check of client certificates

□ Verify server certificate

□ Disable revocation check of server certificates

Note: * - Required Field

a) (Optional) At the **SSL Settings** pane, from the **SSL version** drop-down list, choose the type of SSL protocol to use:

- To use the SSL protocol configured in **Global SSL Settings** window, choose **Inherited**. For more information on configuring global SSL settings, see Configuring SSL Global Settings.
- To use the SSL Version 3 protocol, choose **SSL3**.
- To use the Transport Layer Security Version 1 protocol (TLS Version 1), choose **TLS1**.
- To use both the SSL Version 3 and TLS 1 protocols, choose **All**.

b) (Optional) At the **SSL Settings** pane, from the **Cipher List** drop-down list, choose a list of cipher suites to be used for SSL acceleration between the Cisco WAE device peers, or choose Inherited to use the cipher list configured in SSL global settings. For more information, see Working with Cipher Lists.

c) (Optional) To set the OCSP parameters for certificate revocation, follow these steps:

- To enable the verification of client certificate check, check the **Verify client certificate** check box.
- To disable OCSP client certificate revocation checking, check the **Disable revocation check for this service** check box.
- To enable verification of server certificate check, check the **Verify server certificate** check box.

- To disable OCSP server certificate revocation checking, check the **Disable revocation check for this service** check box.

  If the server and client devices are using self-signed certificates and certificate verification is enabled, Cisco WAAS devices will not be able to accelerate SSL traffic.

d) After you have completed the configuration of the SSL accelerated service, click **Submit**.

Updating a Certificate or Private Key in an SSL Accelerated Service

Procedure

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

Step 2 Choose **Configure > Acceleration > SSL Accelerated Services**.

Step 3 In the **Name** column for the specified service, click **Edit SSL Accelerated Service**.

Step 4 Choose a certificate and key pair method to either regenerate a self-signed certificate and private key or to import an updated certificate and/or key.

a) Enter the required details.

b) Depending on the chosen method, click **Generate** or **Import**.

c) Click **Submit**.

- When you update a certificate for an SSL Accelerated Service and want it to be used by it, it is important to stop and start the configured SSL Accelerated Service.

  This step is required because the existing certificate and key are stored in memory on the accelerators. Updating the certificate/key via the steps described above is insufficient because it does not update the certificate/key in memory.

- To ensure the updated certificate for the SSL Accelerated Service is used, make sure to follow the steps below as well.

Step 5 In the **Name** column for the specified service, click **Edit SSL Accelerated Service** button.

Step 6 Remove the check mark for **In service**, and then click **Submit**.

Step 7 Click the **Edit SSL Accelerated Service** button in the **Name** column for the service in question for one last time.

Step 8 Enable the check mark for **In service**.

Step 9 Click **Submit**.

Configuring SSL Acceleration for SaaS Applications

Before you begin

SaaS applications are typically served from multiple SSL server farms, with multiple hosts spanning several data centers.

- For SSL services hosted in the enterprise data center, the IT administrator knows and controls the SSL server IP and can provide it to the Cisco data center WAAS. But for an SSL service that is hosted at a third-party SaaS provider in the cloud, the SSL server IP address is not controlled by the IT administrator because the cloud provider uses multiple Content Delivery Networks (CDNs) and data centers. Even for a single SaaS service, there might be multiple server IP addresses that can change dynamically. This leads to inadvertent errors due to namespace and certificate mismatch for SaaS applications.
- Cisco WAAS Version 6.4.3 and later support acceleration of two additional SaaS applications: ServiceNow and SalesForce over the SSL protocol. These are in addition to the existing applications: Microsoft Office 365 and YouTube.
- The configuration of SSL-accelerated services for SaaS applications solves the issue of namespace and certificate mismatch for SaaS applications, and ensures that these applications are optimized.

Procedure

Step 1 To create an SSL-accelerated service for a SaaS application, use Step 1 through Step 8 outlined in Using SSL Accelerated Services, on page 426.

Step 2 To match subject alternative names, check the **Match Server Name Indication** check box, or run the **match sni** command on the core Cisco WAAS device.

Consider the following guidelines to match subject alternative names:

- If enabled, the SSL accelerator parses the initial SSL connection setup message for the destination hostname (in the SSL protocol extension called Server Name Indication) and uses that to match it with the **Subject Alternate Names** list in the SSL certificate on the CIsco WAAS device.

  We recommend this setting for optimizing cloud-based SaaS applications to avoid namespace/certificate mismatch errors that are caused due to the changing nature of the SaaS server domains and IP addresses.
- Most current browsers provide Server Name Indication (SNI) support. Ensure that you use a browser that supports SNI.
- The **Match Server Name Indication** option is available on devices running Cisco WAAS Version 5.3.5 and later.

Step 3 To specify the server IP address of the accelerated server, use the keyword **Any**.

Step 4 Direct all SSL traffic for SaaS applications to **port 443**.

Consider the following guidelines for directing SSL traffic for SaaS applications to port 443.

- The above configuration overrides any wildcard configuration.
- If you have configured port 443 for traffic other than SaaS applications, review and reconfigure it appropriately.

Step 5 To upload or paste a certificate and key pair, click **Import Existing Certificate Key**.

- The certificate should be specifically used for the SaaS-accelerated service and should contain the Subject Alternate Names for the server domains that need to be optimized.
- To identify the server domains that need to be added for optimizing SaaS applications, follow the steps described in Determining Server Domains Used by SaaS Applications .

- To ensure that the connections are optimized, you *must* create a new certificate with the missing server domain names derived from the list at regular intervals.

Step 6 To complete the configuration of the SSL-accelerated service for the SaaS application, click **Submit**.

Determining Server Domains Used by SaaS Applications

Before you begin

This section describes how determine server domains used by SaaS applications, and (optionally) how to optimize these server domains.

To view the list of server domain names that do not match the existing SSL certificate, and therefore are not optimized:

1. Check the Match Server Name Indication check box.
2. Log in to the core Cisco WAAS device.
3. Run the **sh crypto ssl services accelerated-service service-name** command.
4. If you want to optimize any of these server domain names, select and add them to your certificate by performing the following steps below.

The server domain names list contains a maximum of 128 server names.

Procedure

Step 1 Identify the relevant servers to be added.

Step 2 Run the **sh crypto ssl services accelerated-service** *service-name* command to see additional details regarding the count and last seen information of the server name.

Step 3 To enable SNI debugs, to view additional information regarding IP address and hostnames, run the **debug accelerator ssl sni** command.

Step 4 To create a new Certificate Signing Request (CSR) with the relevant server domain names of the SaaS applications in the subject alternative names extension of the certificate, log in to the Microsoft Management Console (MMC), or OpenSSL, or other available customer tool.

- When you add the SAN to the certificate: use commas to separate domain names.
- A list of hostnames on a domain can be secured with a single certificate. For example, you can add **a.b.c.com** and **c.b.com** as ***.b.c.com**.
- For a new hostname on another domain, you must make a new entry. For example, you must add **b.c.com** as **b.c.com** or ***.c.com**.
- You can also secure hostnames on different base domains in the same certificate. For example, you can add **a.b.com** and **a.b.net**.
- Refer to the highlighted area in the example certificate below.

```
Certificate:
     Data:
          Version: 3 (0x2)
          Serial Number:
              ec:aa:9b:10:fa:9d:09:95
          Signature Algorithm: sha1WithRSAEncryption
          Issuer: C=US, ST=California, L=San Jose, O=Cisco
          Systems Inc, OU=WAAS,
          CN=Cisco_WAAS_CA/emailAddress=support@cisco.com
          Validity
              Not Before: Jul 31 06:49:56 2013 GMT
              Not After : Aug 30 06:49:56 2013 GMT
          Subject: C=US, ST=California, L=San Jose, O=Cisco
                  Systems Inc, OU=WAAS,
                  CN=Office365/emailAddress=support@cisco.com
          Subject Public Key Info:
              Public Key Algorithm: rsaEncryption
              Public-Key: (1024 bit)
              Modulus:
                  00:c6:85:0d:f9:df:4e:4f:c4:53:d5:3e:0f:c4:cb:
                  53:42:34:34:7d:92:7f:ea:c1:75:0b:21:3f:5f:a1:
                  be:34:f1:40:c3:32:52:a1:05:79:26:7b:a3:29:c5:
                  5e:9f:3f:92:6b:d1:b2:fd:bc:c9:2b:8b:e2:9f:1a:
                  91:83:9b:c8:7f:3f:d9:56:92:75:be:b6:ed:39:39:
                  2f:1a:2f:ba:39:1b:06:76:0a:17:b5:f0:ec:dd:4c:
                  fa:94:be:ea:7c:e0:4e:51:b4:d2:75:4d:8b:d9:6e:
                  de:34:10:c7:c5:e8:97:5f:f2:7f:97:1e:9a:e0:e2:
                  fc:b4:58:11:45:82:19:14:11
Exponent: 65537 (0x10001)
     X509v3 extensions:
         X509v3 Basic Constraints:
                CA:FALSE
         X509v3 Key Usage:
         Digital Signature, Non Repudiation, Key Encipherment
         X509v3 Subject Alternative Name:
            DNS:*.office365.com, DNS:outlook.com, DNS:*.aadcdn.microsoftonline-p.com,
DNS:*.aspnetcdn.com, DNS:*.client.hip.live.com, DNS:*.hip.live.com,
DNS:*.linkedinlabs.com, DNS:*.live.com, DNS:*.microsoft.com, DNS:*.microsoftonline-p.com,
DNS:*.microsoftonline-p.net, DNS:*.microsoftonline.com, DNS:*.microsoftonlineimages.com,
DNS:*.microsoftonlinesupport.net, DNS:*.msecnd.net, DNS:*.msocdn.com, DNS:*.office.net,
DNS:*.office365.com, DNS:*.officeapps.live.com, DNS:*.officecdn.microsoft.com,
DNS:*.onmicrosoft.com, DNS:*.outlook.com, DNS:*.res.outlook.com, DNS:*.sharepoint.com,
DNS:*.sharepointonline.com, DNS:*.telemetry.microsoft.com,
DNS:*.testexchangeconnectivity.com, DNS:*.vo.msecnd.net, DNS:*.webtrends.com

Signature Algorithm: sha1WithRSAEncryption
        46:db:34:7f:c0:8e:13:81:67:0b:3c:8d:15:3a:ee:1f:c7:cf:
        d1:6b:de:00:2a:35:9b:13:d6:bf:79:43:ce:31:c6:f9:de:f7:
        20:1f:0e:86:9e:d4:91:01:57:a2:7b:fe:91:00:de:cf:58:90:
        85:97:49:b3:11:4c:e9:05:d0:a1:a7:73:7e:50:64:8f:80:f4:
        ec:fa:a7:bb:7a:c2:df:5e:c5:e3:a8:52:c4:31:4e:8e:53:36:
        59:e9:0f:27:82:71:4e:3b:79:a4:c9:4f:18:7e:06:7a:0c:34:
        0a:cf:3c:3e:73:73:5a:52:7d:03:a0:75:50:5a:d4:a5:8b:a9:
        ea:96
```

Step 5 Submit the certificate to the Enterpise CA.

Step 6 Import the signed certificate from the Enterprise CA to the Trusted Root Certification Authorities store.

The Enterprise root CA must be present in the browser as trusted root CA.

Step 7 To disable the accelerated service, uncheck the In service checkbox and click **Submit**.

Step 8 Upload the new certificate and re-enable the service.

The server names vary as per the accelerated service that you have configured. Refer to the names below that need to be included in the certificate for the respective accelerated service.

Service Now

```
DNS:*.service-now.com, DNS:service-now.com, DNS:*.servicenow.com, DNS:servicenow.com,
DNS:*.cisco.com, DNS:cisco.com, DNS:*.cloudapps.cisco.com, DNS:cisco.sc.omtrdc.net,
DNS:tags.tiqcdn.com, DNS:ssl.gstatic.com, DNS:dpm.demdex.net, DNS:beacons.gcp.gvt2.com
```

SalesForce

```
DNS:ssl.gstatic.com, DNS:*.force.com, DNS:*.lightning.force.com, DNS:*.salesforce.com,
DNS:*.content.force.com, DNS:*.ap5.content.force.com, DNS:*.sfdcstatic.com,
DNS:*.demdex.net, DNS:salesforcecom.demdex.net, DNS:*.rlcdn.com, DNS:*.krxd.net,
DNS:*.partners.salesforce.com, DNS:*.everesttech.net
```

Configuring SMART-SSL Acceleration

This section contains the following topics:

About SMART-SSL Acceleration

SMART-SSL is an encryption service that enables Layer 7 application network services, such as FTP, HTTP, DNS, to optimize traffic on SSL and TLS encrypted applications. SMART-SSL enables content caching for SSL and TLS applications (HTTP object cache for HTTPS traffic) in both single-sided and dual-sided deployment.

With the evolution of cloud services, there is a critical need to provide application optimization. For Cisco WAAS Version 6.4.1 and later, SMART-SSL optimization is enabled using both single-sided and dual-sided mode.

- In a single-sided deployment, the interposing device does not require a peer device to process the SMART-SSL traffic flow. SMART-SSL traffic flows directly to the edge device without having to go through the core device.
- The dual-sided deployment uses the same configuration procedure as in SSL Accelerator V1. Therefore, the SSL accelerator service configuration is done at the core device in the data center.

  Dual-sided deployments for SMART-SSL (or SSL Accelerator V2), use TLS1.2 as the SSL version and **rsa-with-aes-256-cbc-sha** as the cipher suit.
- To configure SMART-SSL acceleration, you can use your own certificate or use the peering device's certificate. For more information, see Configuring SSL Peering Service.
- To ensure this optimization, you must to enable the SMART-SSL (SSL Accelerator v2) accelerator.

The table below provides an overview of the steps you must complete to set up and enable SMART-SSL acceleration.

Table 48: Checklist for Configuring SSL v2 Acceleration

Task	Additional Information and Instructions
1. Prepare to configure SMART-SSL acceleration.	Identifies the information that you need to gather before configuring SMART-SSL acceleration on your WAAS devices. For more information, see Preparing to Use SMART-SSL Acceleration, on page 436.

Task	Additional Information and Instructions
2. Set up to use existing Enterprise Root CA certificates.	(Optional) Describes how to create, import, and manage existing Enterprise Root certificate authority (CA) certificates. For more information, see Using an Existing Root CA Certificate, on page 438.
3. Enable SMART-SSL application optimization.	Describes how to activate the SMART-SSL acceleration feature. For more information, see Enabling and Disabling the Global Optimization Features, on page 373.
4. Set up accelerated service certificates.	Describes how to create, import, and use certificates for SMART-SSL acceleration. For more information, see Creating Single-Sided SMART-SSL Accelerated Service Certificate , on page 438.
5. Configure and enable SSL-accelerated services.	Describes how to add, configure, and enable services to be accelerated by the SMART-SSL application optimization feature. For more information, see Configuring and Managing SMART-SSL Accelerated Services on a Single-Sided Device Group, on page 439.

Preparing to Use SMART-SSL Acceleration

Before configuring SMART-SSL acceleration, consider these specifications:

- Services to be accelerated on the SMART-SSL traffic: You must create a certificate to optimize these services using their URLs or domain names, such as **www.google.com**, or ***.google.com**.
- Server IP address and port information: Optionally, if the URL or domain name cannot be used, you can specify a server IP address. If you have specified a URL, you can still specify a port.
- Public key infrastructure (PKI) certificate and private key information, including the certificate common name and CA-signing information.
- SSL versions supported: SSLv3, TLS1.0, TLS1.1, TLS1.2.

Note For SMART-SSL to work, the default SSL policy must be in place. If the policy is modified, for example, if the command **accelerate http policy** is applied for an SSL class map, the SSL accelerator starts optimizing, but the SMART-SSL accelerator does not optimize.

Supported ciphers: The following is a list of the 27 supported ciphers.

```
TLS_RSA_WITH_3DES_EDE_CBC_SHA, /* 0x000A */
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,/* 0x0016 */
TLS_RSA_WITH_AES_128_CBC_SHA,    /* 0x002F */
TLS_DHE_RSA_WITH_AES_128_CBC_SHA, /* 0x0033 */
TLS_RSA_WITH_AES_256_CBC_SHA, /* 0x002F */
TLS_DHE_RSA_WITH_AES_256_CBC_SHA, /* 0x0039 */
TLS_RSA_WITH_AES_128_CBC_SHA256, /* 0x003C */
TLS_RSA_WITH_AES_256_CBC_SHA256, /* 0x003D */
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA,/* 0x0041 */
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA, /* 0x0045 */
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, /* 0x0067 */
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, /* 0x006B */
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA, /* 0x0084 */
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA, /* 0x0088 */
TLS_RSA_WITH_SEED_CBC_SHA,   /* 0x0096 */
```

```
TLS_DHE_RSA_WITH_SEED_CBC_SHA, /* 0x009A */
TLS_RSA_WITH_AES_128_GCM_SHA256, /* 0x009C */
TLS_RSA_WITH_AES_256_GCM_SHA384, /* 0x009D */
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, /* 0x009E */
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, /* 0x009F */
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, /* 0xC012 */
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, /* 0xC013 */
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, /* 0xC014 */
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, /* 0xC027 */
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, /* 0xC028 */
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, /* 0xC02F
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 /* 0xC030 */
```

SSL compression is not supported.

Creating a Root CA Certificate

Before you begin

A root Certificate Authority (CA) certificate is a certificate issued by a trusted certificate authority and is in turn trusted by domain clients. A root CA certificate is used to sign all the certificates that will be used by the Cisco WAAS for SSL interposing during client and server SSL handshake for optimizing the applications or the URLs.

The root CA certificate must be able to accept Certificate Signing Requests (CSRs) that include subject alternative names and generate certificates that include subject alternative names.

- The subject alternative name is an extension to the X.509 protocol that allows various values to be associated with a security certificate (SSL certificate).
- Subject alternative names can include IP addresses, email addresses, universal resource identifiers (URIs), alternative common Domain Name System (DNS) names, alternatives to the distinguished name, and other information.You can install this on all machines that will be communicating with services using SSL certificates generated by this root certificate.
- If your organization already has a root CA for its internal use, you can use it instead of a new root CA. If not, use a Linux machine with openssl version of 1.0.1e or greater to create these certificates.

Procedure

Step 1 To create a new root CA certificate, use a Linux machine with an OpenSSL version of 1.0.1e or later.

Step 2 Create the root CA certificate key. This signs all issued certificates.

```
openssl genrsa -out rootCA.key.pem 2048
```

Step 3 Create the self-signed root CA certificate, with the key generated in Step 2.

```
openssl req -x509 -new -nodes -key rootCA.key -days 365 -out rootCA.crt
```

Step 4 Verify the root certificate.

Step 5 Import the certificate from the **Enterprise CA** to the **Trusted Root Certification Authorities** store in the client browser.

Step 6 Install the root CA certificate and intermediate CA certificate.

Using an Existing Root CA Certificate

If your organization already has a well-known root CA certificate, you can use it. You can also import a new CA certificate using the Cisco WAAS Central Manager GUI.

For more information, see Working with CA Certificates and Creating a Root CA Certificate.

Creating Single-Sided SMART-SSL Accelerated Service Certificate

Procedure

Step 1 To create a new encryption key pair, use OpenSSL as shown below:

```
openssl genrsa -out proxyserver.key 1024
```

Step 2 For the application to be optimized, create a Certificate Signing Request (CSR), key pair, and other needed attributes, such as **Common Name**, **Company** and **SubjAltName**.

For example, for YouTube, ensure that the **subjectAltNames** have all URLs that YouTube servers include in their certificate, which you want to optimize.

```
openssl req -new -key server.key -out server.csr
X509v3 extensions:
X509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
NGSSL Demo Certificate
X509v3 Subject Key Identifier:
65:C1:42:98:47:81:0E:04:7A:7D:83:A7:43:C9:A3:B8:1F:DB:BF:1E
X509v3 Authority Key Identifier:
keyid:8C:F6:0A:BC:E4:EB:2C:D9:6B:68:95:09:1B:B5:82:66:CE:ED:6B:77
X509v3 Subject Alternative Name:
DNS:*.google.com, DNS:*.android.com, DNS:*.appengine.google.com, DNS:*.cloud.google.com,
DNS:*.google-analytics.com, DNS:*.google.ca, DNS:*.google.cl, DNS:*.google.co.in,
DNS:*.google.co.jp, DNS:*.google.co.uk, DNS:*.google.com.ar, DNS:*.google.com.au,
DNS:*.google.com.br, DNS:*.google.com.co, DNS:*.google.com.mx, DNS:*.google.com.tr,
DNS:*.google.com.vn, DNS:*.google.de, DNS:*.google.es, DNS:*.google.fr, DNS:*.google.hu,
DNS:*.google.it, DNS:*.google.nl, DNS:*.google.pl, DNS:*.google.pt,
DNS:*.googleadapis.com, DNS:*.googleapis.cn, DNS:*.googlecommerce.com,
DNS:*.googlevideo.com, DNS:*.gstatic.cn, DNS:*.gstatic.com, DNS:*.gvt1.com,
DNS:*.gvt2.com, DNS:*.metric.gstatic.com, DNS:*.urchin.com, DNS:*.url.google.com,
DNS:*.youtube-nocookie.com, DNS:*.youtube.com, DNS:*.youtubeeducation.com,
DNS:*.ytimg.com, DNS:android.clients.google.com, DNS:android.com, DNS:g.co, DNS:goo.gl,
DNS:google-analytics.com, DNS:google.com, DNS:googlecommerce.com, DNS:urchin.com,
DNS:www.goo.gl, DNS:youtu.be, DNS:youtube.com, DNS:youtubeeducation.com
```

Alternately, to create a CSR from the CM GUI, follow the steps in Generating, Importing, or Exporting a Service Certificate and Private Key, on page 413.

Step 3 To create a new proxy server certificate, sign the above generated CSR with your existing Enterprise Root CA, or the one created above. This will generate a **.crt** or **.pem** certifcate file.

To ensure that the created accelerated service proxy certificate will be authenticated and accepted by the client browser, the CA certificate used to sign this accelerated service certificate must be present in the client browser root CA certificate store.

a) Refer to your browser’s Settings or Options menu for that browser’s Certificates and Import locations.
b) Import the certificate.
c) Clear the browser cache.

d) Reload the browser for the cloud application.

The browser will pick up the new certificate.

Step 4 Cisco WAAS allows importing certificates with **PKCS12** format. To generate the **PKCS12** format from the certificate file and your private key, run the **open ssl** command.

```
openssl pkcs12 -export -out server.p12 -inkey proxyserver.key -in proxyserver.crt
-certfile CACert.crt
```

Step 5 To import this certificate into the Cisco WAAS device group, run the **crypto import** EXEC command and thereafter be used in the accelerated server configuration as server-cert-key.

```
WAE# crypto import pkcs12 newcert.p12 pkcs12{disk| ftp | http | sftp | tftp}
```

Step 6 Follow these guidelines for importing the certificate:

- The CA certificate used to sign this Accelerated SSL Service (ASVC) certificate must exist in the browser root CA certificate store in order for the accelerated service proxy certificate creation to be authenticated and accepted by the browser.
- The Cisco WAAS Central Manager CA certificate repository does not include the **CN=GTE CyberTrust Global Root** certificate. You must manually import the **CN=GTE CyberTrust Global Root** certificate and then configure it from the Cisco WAAS Central Manager, or the device that will use it, to validate Microsoft Office 365 certificates.

Configuring and Managing SMART-SSL Accelerated Services on a Single-Sided Device Group

Before you begin

Consider the following prerequisites for using Cisco WAAS to optimize SMART-SSL traffic:

- Ensure that the Cisco WAAS Central Manager and Cisco WAEs are running Cisco WAAS Software Version 6.2.x or later.
- Ensure that the new device group supports single-sided acceleration. To create a device group, see Creating a Device Group in the chapter "Using Device Groups and Device Locations."
- Create an accelerated service certificate for WAN optimization.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose Device Groups > device-group-name.

Step 2 Select the device group to enable for SMART-SSL settings.

Note Add only branch devices to this group.These devices will optimize the SSL traffic as it passes through them.

Step 3 From the Cisco WAAS Central Manager menu, choose **Configure** > **Acceleration** > **Enabled Features**.

Step 4 To enable SMART SSL acceleration, at the **Accelerator Optimization** pane, check the **SSL Interposer (SSL Accelerator V2)** check box.

Step 5 To create an SSL accelerated service for the device group, choose **Acceleration > SSL Accelerated Services**.

Step 6 Click **Create**.

The **Creating New SSL Accelerated Service** window appears.

Step 7 At the **SSL Accelerated Service** pane, enter the name of your service, and check the **In service** box.

(Optional) Enter a short description for the SSL accelerated service.

Step 8 At the **Server Addresses** pane:

a) In the IP Address field, enter **Any**.
b) In the **Server Port** field, enter **443**.
c) Click **Add**.

Step 9 At the **Certificate and Private Key** pane:

a) Click **Import Existing Certificate and Optionally Private Key**.
b) Click **Upload File in PKCS#12 Format**.
c) In the **Password** field, enter the password to be used to export the certificate.
d) Use the **Browse** button to locate the certificate to be imported.
e) Click **Import** to import the certificate.

A confirmation screen appears, with the certificate information.

Step 10 To complete the configuration of the SSL-accelerated service to use single sided optimization, click **Submit**.

(Optional) Alternatively, to automate the entire process using a script, contact the Cisco Technical Assistance Center (TAC). For further information on contacting TAC, see the Cisco Support and Downloads page, Contacts/Support Cases section.

Step 11 To monitor the SMART-SSL accelerated service optimization statistics:

- To use the Cisco WAAS Central Manager, see the chapter "Monitoring Your Cisco WAAS Network."
- To use the Cisco WAAS CLI, run the **show statistics encryption-services** EXEC command.

What to do next

To configure and manage SMART-SSL accelerated services on a single-sided device group using the Cisco WAAS CLI, use these command guidelines:

Before You Begin

- Ensure that the Cisco WAAS Central Manager and Cisco WAEs are running Cisco WAAS Software Version 6.2.x or later.
- Ensure that the new device group supports single-sided acceleration. To create a device group, see Creating a Device Group in the chapter "Using Device Groups and Device Locations."
- Create an accelerated service certificate for Cisco WAN optimization.

To configure and manage SMART-SSL accelerated services on a single-sided device group using the Cisco WAAS CLI, use these command guidelines:

- To enable SMART-SSL acceleration from the Cisco WAAS CLI, run the **crypto encryption-service enable** global configuration command.
- The SSL accelerator and the SMART-SSL accelerator use the same configuration commands. However, for the SMART-SSL configuration, only a limited set of keywords are supported. The following table shows the Cisco WAAS CLI command keywords that are supported for SMART-SSL acceleration.

Table 49: Cisco WAAS CLI Command Keywords Supported for SMART-SSL Acceleration

Cisco WAAS CLI Command Mode	Keywords Supported for SMART-SSL Acceleration	Cisco WAAS CLI Command Mode	Keywords Not Supported for SMART-SSL Acceleration
(config-ssl-accelerated)	client-cert-key	(config-ssl-accelerated)	cipher-list
	client-cert-verify		client-version-rollback
	description		match
	inservice		protocol-chaining
	server-cert-key		version
	server-cert-verify		
	server-domain + port		
	configure IP + port		

Configuring Microsoft Office 365 for Cisco WAAS

This section contains the following topics:

About Microsoft Office 365 for Cisco WAAS

Microsoft Office365 supports business-critical applications such as Outlook, SharePoint, Excel and PowerPoint, and use of Microsoft Office 365 as SaaS has also increased. As enterprises move toward SaaS applications such as Microsoft Office 365, performance and user experience of these applications has also become more important.

Cisco WAAS support for Microsoft Office 365 traffic acceleration and optimization was introduced in Cisco WAAS Version 5.3.5 (for optimization between the on-premise data center and the customer branch, only). For Cisco WAAS Version 6.2.1 and later, traffic to Microsoft Office 365 is optimized until it reaches the cloud, by implementing a solution that includes:

- Enabling Cisco WAAS as SaaS over Microsoft Azure.
- Positioning Cisco WAAS as SaaS near to Microsoft Office 365 service by configuration.
- Routing and DNAT using CSR in Microsoft Azure.
- Using Cisco Intelligent WAN (Cisco IWAN) as transport.
- Detecting Microsoft Office 365 traffic using the Cisco SSL accelerator.

Checklist for Configuring Microsoft Office 365 for Cisco WAAS

The following list shows the steps needed to set up and enable Microsoft Office 365 for Cisco WAAS using the Cisco WAAS Central Manager.

1. **Prerequisites**: Before you create a Microsoft Office 365 accelerated service using the Cisco WAAS Central Manger, you must have completed the following:

   - Deployed Virtual Network in Azure
   - Deployed CSR 1000v for secure network extension and Destination Network Address Translation (DNAT)
   - Deployed Microsoft Azure on Cisco vWAAS
   - Configured Microsoft Azure route tables
   - Configured Microsoft Azure CSR
   - Registered the Microsoft Azure Cisco vWAAS device with the Cisco WAAS Central Manager

2. **Prepare to configure SSL acceleration**:

   Identify the information that you need to gather before configuring SSL acceleration on your Cisco WAAS devices.

   For more information, see Prerequisites for Configuring SSL Acceleration.

3. **Set up root CA certificates**:

   (Optional) Create, import, and manage certificate authority (CA) certificates.

   For more information, see Creating a Root CA Certificate.

4. **Enable SSL application optimization**:

   Enable the SSL acceleration feature.

   For more information, see Enabling and Disabling the Global Optimization Features and Configuring SSL Acceleration.

5. **Set up accelerated service certificates**:

   Create, import, and use certificates for Microsoft Office 365 acceleration.

   For more information, see Creating Microsoft Office 365 Accelerated Service Certificate.

6. **Configure and enable Microsoft 365 acceleration**:

   Add, configure, and enable Microsoft 365 acceleration using the Cisco WAAS Central Manager.

   For more information, see Configuring Microsoft Office 365 for Cisco WAAS.

Creating Microsoft Office 365 Accelerated Service Certificate

Procedure

Step 1 To create a new Certificate Signing Request (CSR) with the relevant server domain names of the Microsoft Office 365 application in the subject alternative names extension of the certificate, log in to the Microsoft Management Console (MMC), OpenSSL, or other available customer tool.

In the following example certificate, refer to the bolded text.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            ec:aa:9b:10:fa:9d:09:95
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, ST=California, L=San Jose, O=Cisco
        Systems Inc, OU=WAAS,
        CN=Cisco_WAAS_CA/emailAddress=support@cisco.com
        Validity
            Not Before: Jul 31 06:49:56 2013 GMT
            Not After : Aug 30 06:49:56 2013 GMT
        Subject: C=US, ST=California, L=San Jose, O=Cisco
                Systems Inc, OU=WAAS,
                CN=Office365/emailAddress=support@cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:c6:85:0d:f9:df:4e:4f:c4:53:d5:3e:0f:c4:cb:
                    53:42:34:34:7d:92:7f:ea:c1:75:0b:21:3f:5f:a1:
                    be:34:f1:40:c3:32:52:a1:05:79:26:7b:a3:29:c5:
                    5e:9f:3f:92:6b:d1:b2:fd:bc:c9:2b:8b:e2:9f:1a:
                    91:83:9b:c8:7f:3f:d9:56:92:75:be:b6:ed:39:39:
                    2f:1a:2f:ba:39:1b:06:76:0a:17:b5:f0:ec:dd:4c:
                    fa:94:be:ea:7c:e0:4e:51:b4:d2:75:4d:8b:d9:6e:
                    de:34:10:c7:c5:e8:97:5f:f2:7f:97:1e:9a:e0:e2:
                    fc:b4:58:11:45:82:19:14:11
Exponent: 65537 (0x10001)
     X509v3 extensions:
         X509v3 Basic Constraints:
                CA:FALSE
         X509v3 Key Usage:
          Digital Signature, Non Repudiation, Key Encipherment
         X509v3 Subject Alternative Name:
DNS.1 = *.virtualearth.net; DNS.2 = *.msocdn.com; DNS.3 = *.office365.com; DNS.4 =
*.outlook.com; DNS.5 = outlook.com; DNS.6 = *.microsoftonline.com; DNS.7 = *.res.outlook.com;
 DNS.8 = *.googleapis.com; DNS.9 = *.google-analytics.com; DNS.10 = *.google.com; DNS.11 =
 *.googleusercontent.com; DNS.12 = *.gstatic.com; DNS.13 = *.microsoftonline-p.com; DNS.14
 = *.aadcdn.microsoftonline-p.com; DNS.15 = *.aspnetcdn.com; DNS.16 = *.client.hip.live.com;
 DNS.17 = *.hip.live.com; DNS.18 = *.infra.lync.com; DNS.19 = *.linkedinlabs.com; DNS.20 =
 *.live.com; DNS.21 = *.lync.com; DNS.22 = *.microsoft.com; DNS.23 = *.microsoftonline-p.net;
 DNS.24 = *.microsoftonlineimages.com; DNS.25 = *.microsoftonlinesupport.net; DNS.26 =
*.msecnd.net; DNS.27 = *.msocdn.com; DNS.28 = *.office.net; DNS.29 = *.office365.com; DNS.30
 = *.officeapps.live.com; DNS.31 = *.officecdn.microsoft.com; DNS.32 = *.online.lync.com
DNS.33 = *.onmicrosoft.com; DNS.34 = *.sharepoint.com; DNS.35 = *.sharepointonline.com;DNS.36
 = *.telemetry.microsoft.com; DNS.37 = *.testexchangeconnectivity.com; DNS.38 =
*.vo.mscend.net; DNS.39 = *.webtrends.com; DNS.40 = *.office.com; DNS.41 =
*.portal.office.com;
```

```
Signature Algorithm: sha1WithRSAEncryption
        46:db:34:7f:c0:8e:13:81:67:0b:3c:8d:15:3a:ee:1f:c7:cf:
        d1:6b:de:00:2a:35:9b:13:d6:bf:79:43:ce:31:c6:f9:de:f7:
        20:1f:0e:86:9e:d4:91:01:57:a2:7b:fe:91:00:de:cf:58:90:
        85:97:49:b3:11:4c:e9:05:d0:a1:a7:73:7e:50:64:8f:80:f4:
        ec:fa:a7:bb:7a:c2:df:5e:c5:e3:a8:52:c4:31:4e:8e:53:36:
        59:e9:0f:27:82:71:4e:3b:79:a4:c9:4f:18:7e:06:7a:0c:34:
        0a:cf:3c:3e:73:73:5a:52:7d:03:a0:75:50:5a:d4:a5:8b:a9:
```

Step 2 Submit the certificate to the Enterprise CA.

Step 3 Import the signed certificate from the Enterprise CA to the Trusted Root Certification Authorities store.

Note The Enterprise root CA should be present in browser as trusted root CA.

Step 4 To ensure that the created accelerated service proxy certificate will be authenticated and accepted by the client browser, the CA certificate used to sign this accelerated service certificate must be present in the client browser root CA certificate store.

a) Refer to your browser's **Settings** or **Options** menu for that browser's **Certificates** and **Import** locations.
b) Import the certificate.
c) Clear the browser cache.
d) Reload the browser for the cloud application.

The browser will pick up the new certificate.

Procedure for Configuring Microsoft Office 365 for Cisco WAAS

Procedure

Step 1 Register your Azure vWAAS device with the Cisco WAAS Central Manager. If the Cisco WAAS Central Manager is in a different network add routes for reachability.

Step 2 Create a Microsoft Office 365 accelerated service for the device group:

a) Choose **Acceleration > SSL Accelerated Services**.
b) Click **Create**.

The **Creating New SSL Accelerated Service** window appears.

Step 3 At the **SSL Accelerated Service** pane:

a) In the **Service Name** field, enter the name of the service, **o365**.
b) To enable this service, check the **In Service** check box.
c) To match subject alternative names, check the **Match Server Name Indication** check box or run the match sni command on the core WAAS device.

Consider the following guidelines to match subject alternative names:

- If enabled, the SSL accelerator parses the initial SSL connection setup message for the destination hostname (in the SSL protocol extension called Server Name Indication) and uses that to match it with the Subject Alternate Names list in the SSL certificate on the WAAS device.

- We recommend this setting for optimizing cloud-based SaaS applications to avoid namespace/certificate mismatch errors that are caused due to the changing nature of the SaaS server domains and IP addresses.
- Most current browsers provide Server Name Indication (SNI) support. Ensure that you use a browser that supports SNI.
- The **Match Server Name Indication** option is available on devices running Cisco WAAS Version 5.3.5 and later.

d) (Optional) Provide a short description.

Step 4 At the Server addresses pane:

a) To specify the server IP address of the accelerated server, in the **Server Port** field, enter the keyword **Any**.
b) To direct traffic to port 443, in the **Server Port** field enter **443**.
c) Click **Add**.

Step 5 At the **Certificate and Private Key** pane:

a) Click **Import Existing Certificate and Optionally Private Key**.
b) Click **Upload File in PKCS#12 Format**.
c) In the **Password** field, enter the password to be used to export the certificate.
d) Use the **Browse** button to locate the certificate to be imported.
e) Click **Import** to import the certificate.

A confirmation screen appears, with the certificate information.

Step 6 To complete the configuration of the Microsoft Office 365, click **Submit**.

Step 7 To monitor accelerated service optimization statistics, see SSL Acceleration Charts in the chapter "Monitoring Your Cisco WAAS Network."

What to do next

To configure Microsoft Office 365 for Cisco WAAS using the Cisco WAAS CLI:

- To copy the Microsoft Office 365 certificate (**o365.pfx**) to the Cisco data center WAE and to import the certificate, run the following EXEC command:

  crypto import pkcs12 *Azure_o365.p12* **pkcs12 disk** *office365.pfx*

  Instead of importing multi-domain certificates from the device, you can use remote methods to import the certificate from servers, including the methods FTP and HTTP.

- To configure the application accelerated service in the Cisco WAE with the imported certificate, run the following SSL Accelerated Service Configuration Mode command:

  crypto ssl services accelerated-service *Azure_o365*

- To view statistics for Microsoft Office 365 acceleration, run the following EXEC command:

  show statistics connections optimized

Cisco Support for Microsoft Windows Update

This section contains the following topics:

About Cisco Support for Microsoft Windows Update

Cisco support for Microsoft Windows Update enables caching of objects used in Microsoft Windows Operating System (Microsoft Windows OS) and application updates. Cisco support for Microsoft Windows Update is enabled by default, and enabled only for specific sites.

The Microsoft Windows OS and application updates are managed by update clients such as Microsoft Update. Microsoft Update downloads the updates via HTTP, often in combination with Background Intelligent Transfer Service (BITS) to help facilitate the downloads. Clients use HTTP range request to fetch updates.

The objects that comprise the updates, such as **.cab** files, are typically cacheable, so that HTTP object cache is a significant benefit for this process.

For example, for Microsoft Windows 7 and Microsoft Windows 8 OS updates, via direct Internet or Windows Server Update Services (WSUS), Version 2012 and 2012 R2, more than 98% of the update files, such as **.cab**, **.exe**, and **.psf** files, are served from cache on subsequent updates. Cisco support for Microsoft Windows Update reduces the volume of WAN offload bytes and reduces response time for subsequent Windows updates.

Viewing Statistics for Cisco Support for Microsoft Windows Update

There are two ways to view data generated by Cisco support for Microsoft Windows Update:

- To use the Cisco WAAS Central manager to view data generated by Cisco support for Microsoft Windows Update, see Top Sites in the chapter "Monitoring Your Cisco WAAS Network." The Top Sites report provides information such as WAN response time and WAN offload bytes.
- For Cisco WAAS Version 6.1.1 and later, the cache engine access log file has two additional fields for Microsoft Windows Update statistics:
  - **rm-w** (range miss, wait): The main transaction, a cache miss, which waited for the sub-transaction to fetch the needed bytes.
  - **rm-f** (range miss, full): The sub-transaction, a cache write of the entire document.

Example 1:

Example 1 contains two log lines, the main transaction and sub-transaction, when a range is requested on an object that is not in cache:

```
ws8-rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
08/28/2015 12:22:29.663 (fl=27520) 300 13.164 0.000 446 - - 34912 172.25.30.4

191.234.4.50 2905 h - - rm-w 206 GET
http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/secu/2013/07/wind
ows8-rt-kb2863725- x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -

08/28/2015 12:24:31.448 (fl=27520) 300 134.949 0.000 355 344 3591542 568 172.25.30.4
191.234.4.50 2f25 m-s - - rm-f 200 GET
http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/secu/2013/07/wind
ows8-rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
```

Example 2:

Example 2 shows a cache hit when a range is requested on an object that is either completely in cache, or in the process of being downloaded. If it is in the process of being downloaded, then the main transaction has latched onto a sub-transaction like the one shown in Example 1.

```
08/28/2015 03:34:36.906 (fl=26032) 300 0.000 50.373 346 - - 13169 172.25.30.4
8.254.217.62 2905 h - - - 206 GET
http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/secu/2013/07/wind
ows8-\ rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
```

Cisco Support for Microsoft Windows Update and Akamai Cache Engine

Cisco support for Microsoft Windows Update enables Akamai Cache Engine to support Windows Update caching in two ways:

- Download and cache full objects even when ranges within objects that not in cache are requested.
- Future range requests on the objects can be served out of cache.

There is a limit, set by OTT metadata during the Akamai Connect registration process, from the start of the object (the number of bytes or the percent of file length) where the download functionality is triggered. A request of a size above the set limit does not initiate a full object download, and the request is forwarded to the origin as is.

Note Cisco Support for Microsoft Windows update is enabled by default, and enabled only for specific sites. The enabled sites are updated via OTT metadata. To disable Cisco Support for Microsoft Windows Update, you must disable OTT caching. To do this, uncheck the **Over the Top Cache** check box. However, unchecking the **Over the Top Cache** check box disables all OTT functionality, both global and custom OTT configurations.

For more information on the Akamai Connect registration process, see Activating and Managing the Akamai Connect License in the chapter "Configuring Cisco WAAS with Akamai Connect."

Creating a New Traffic Optimization Policy

This section contains the following topics:

Checklist for Creating an Optimization Policy

The following table provides a checklis for creating a new optimization policy.

Table 50: Checklist for Creating a New Optimization Policy

Task	Description
1. Prepare to create an optimization policy.	Complete prerequisite tasks before creating a new optimization policy on your Cisco WAAS devices. For more information, see the **Before You Begin** section of Creating an Optimization Policy, on page 449.

Task	Description
2. Create an application definition.	Identify general information about the application to be optimized, such as the application name and whether or not the Cisco WAAS Central Manager will collect statistics about this application. For more information, see Creating an Application Definition.
3. Create an optimization policy.	Determine the type of action your Cisco WAAS device or device group performs on specific application traffic. This step includes the following required tasks: • Create application class maps that enable a Cisco WAAS device to identify specific types of traffic. For example, you can create a condition that matches all traffic going to a specific IP address. • Specify the type of action your Cisco WAAS device or device group performs on the defined traffic. For example, you can specify that Cisco WAAS apply TFO and LZ compression to all traffic for a specific application. For more information, see Creating an Optimization Policy.

Creating an Application Definition

Before you begin

The first step in creating an optimization policy is to set up an application definition that identifies general information about the application, such as the application name and whether you want the Cisco WAAS Central Manager to collect statistics about the application. You can create up to 255 application definitions on your Cisco WAAS system.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **Acceleration** > **Applications**.

The **Applications** window appears, which displays a list of all the applications on your Cisco WAAS system, and the device or device group from which it gets the settings.

Step 2 From the **Applications** window, perform the following tasks:

- To modify a definition, select an application and click the **Edit** icon in the task bar.
- To delete a definition, click the **Delete** icon in the task bar.
- Determine if the Cisco WAAS system is collecting statistics on an application.

  If the statistics are being collected for the application, the **Enable Statistics** column displays **Yes**.
- Create a new application, as described in the steps that follow.

Step 3 Create a new application:

a) Click the **Add Application** icon in the taskbar.

   The **Applications** window appears.

b) In the **Name** field, enter a name for this application. Use only alphanumeric characters; the application name cannot contain spaces and special characters.

c) (Optional) In the **Comments** field, enter a comment.

   The entered comment appears in the **Applications** window.

d) To allow the Cisco WAAS Central Manager to collect data for this application, check the **Enable Statistics** check box. To disable data collection for this application, uncheck the **Enable Statistics** check box.

   - The Cisco WAAS Central Manager GUI can display statistics for up to 25 applications and 25 class maps. An error message is displayed if you try to enable more than 25 statistics for either applications or class maps.

     However, you can use the Cisco WAAS CLI to view statistics for all the applications that have policies on a specific Cisco WAAS device. For more information, refer to the *Cisco Wide Area Application Services Command Reference*.

   - Historical data for an application that has statistics collection enabled, and then disabled, and then re-enabled:

     The historical data is retained from when the statistics collection was first enabled, and when it was re-enabled, but a gap in data will exist for the period when statistics collection was disabled.

   - Historical data for a deleted and then re-created application for which statistics were collected:

     An application cannot be deleted if there is an optimization policy using it. However, if you delete an application for which statistics were collected, and then later recreate the application, the historical data for the application is lost. Only data collected since the re-creation of the application is displayed.

     The Cisco WAAS Central Manager does not start collecting data for this application until you finish creating the entire optimization policy.

e) Click **OK**.

   The application definition is saved and is displayed in the application list.

Creating an Optimization Policy

Before you begin

Before you create a new optimization policy, complete the following tasks:

- Review the list of optimization policies on your CIsco WAAS system and make sure that none of these policies already cover the type of traffic you want to define. To view a list of the predefined policies that come bundled with the Cisco WAAS system, see Appendix A, "Predefined Optimization Policy."

- Identify a match condition for the new application traffic. For example, if the application uses a specific destination or source port, you can use that port number to create a match condition. You can also use a source or destination IP address for a match condition.

- Identify the device or device group that requires the new optimization policy. We recommend that you create optimization policies on device groups so that the policy is consistent across multiple Cisco WAAS devices.
- After you create an application definition, create an optimization policy that determines the action a Cisco WAAS device takes on the specified traffic.

  Example:

  - You create an optimization policy that directs a Cisco WAAS device to apply TCP optimization and compression to all application traffic that travels over a specific port or to a specific IP address.

    You can create up to 512 optimization policies on your Cisco WAAS system.

  - The traffic-matching rules are present in the application class map. These rules, known as **match conditions**, use Layer 2 and Layer 4 information in the TCP header to identify traffic.

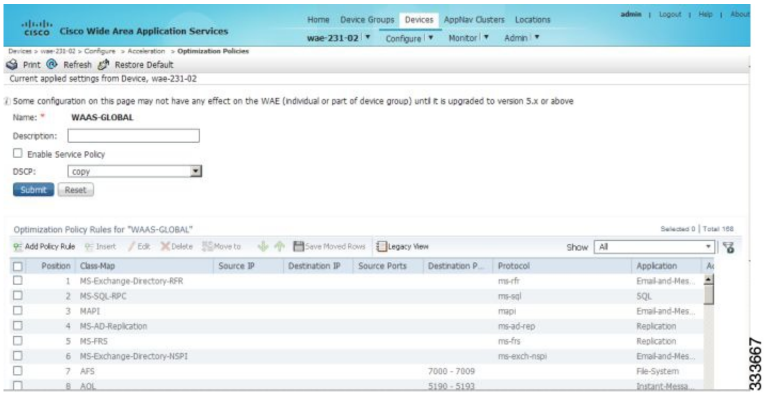
Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **Optimization Policies**.

The **Optimization Policies** window appears. This window displays information about all the optimization policies that reside on the selected device or device group, as well as the position of each policy.

Figure 77: Optimization Policies Window



Current applied settings from Device, wae-231-02

Some configuration on this page may not have any effect on the WAE (individual or part of device group) until it is upgraded to version 5.x or above

Name: * WAAS-GLOBAL

Description:

□ Enable Service Policy

DSCP: copy

Optimization Policy Rules for "WAAS-GLOBAL"

Selected 0 | Total 168

Show All

□	Position	Class-Map	Source IP	Destination IP	Source Ports	Destination P...	Protocol	Application	Ac
□	1	MS-Exchange-Directory-RFR					ms-rfr	Email-and-Mes...	
□	2	MS-SQL-RPC					ms-sql	SQL	
□	3	MAPI					mapi	Email-and-Mes...	
□	4	MS-AD-Replication					ms-ad-rep	Replication	
□	5	MS-FRS					ms-frs	Replication	
□	6	MS-Exchange-Directory-NSPI					ms-exch-nspi	Email-and-Mes...	
□	7	AFS				7000 - 7009		File-System	
□	8	AOL				5190 - 5193		Instant-Messa...	

Consider the following guidelines for configuring optimization policies:

- The position of each policy determines the order in which Cisco WAAS refers to that policy when determining how to handle application traffic.
- To change the position of a policy, see Modifying the Position of an Optimization Policy.
- The **Optimization Policies** window also displays the class map, source and destination IP addresses, source and destination ports, protocol, application, action, and accelerates assigned to each policy.
- If there are Cisco WAAS Version 4.x devices, click the **Legacy View** taskbar icon to view the policies as they appear in a Cisco WAAS Version 4.x device.

- All new devices, or devices that been configured with restore factory default settings, have their own polices and class maps. These devices that are not assigned to any device group within two data feeds continue to have their own policies, even after being registered with the Cisco WAAS Central Manager.
    - After these devices are assigned to device groups, the **Force Device Group Settings** icon appears in the **Optimization Policies** window in device group level. To correct this, use the **Force Group Settings** to ensure that all devices in the specified group have the same configuration.
    - For more information on **Force Group Settings**, see Procedure for Forcing Device Group Settings in the chapter "Using Device Groups and Device Locations."

At the **Optimization Policies** window, you can perform the following tasks:

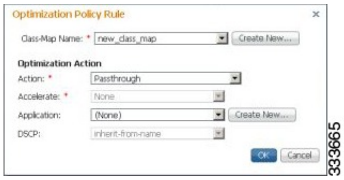
- Configure a description.
- Configure the **Enable Service Policy** setting.
- Configure the **DSCP** setting. This **DSCP setting** field configures DSCP settings at the device or device group level.

  The device uses this policy setting to determine what optimizations are performed only if the **Enable Service Policy** is set.
- To delete one or more optimization policies, select the policies to be deleted, and click the **Delete** icon.
- To modify a policy, check the policy and click the **Edit** icon.
- To restore predefined policies and class maps, see **Restoring Optimization Policies and Class Maps**.
- Create an optimization policy, as described in the following steps.

Step 3 To create a new optimization policy, click the **Add Policy Rule** icon in the taskbar.

The **Optimization Policy Rule** pop-up window appears.

Figure 78: Add Optimization Policy Rule Window



Optimization Policy Rule

Class-Map Name: * new_class_map

Optimization Action

Action: * Passthrough

Accelerate: * None

Application: (None)

DSCP: inherit-from-name

Step 4 From the **Class-Map Name** drop-down list, choose an existing class map for this policy, or click **Create New** to create a new class map for this policy. For more information, see Creating an Optimization Class Map.

Step 5 From the **Action** drop-down list, choose the action that your Cisco WAAS device should take on the defined traffic. The following table describes each action.

For a Cisco WAAS Express device, only a subset of actions are available: **Passthrough**, **TFO Only**, **TFO with LZ**, **TFO with DRE**, and **TFO with DRE and LZ**.

Table 51: Class Map Action Descriptions

Class Map Action	Description
Passthrough	Prevents the Cisco WAAS device from optimizing the application traffic defined in this policy by using TFO, DRE, or compression. Traffic that matches this policy can still be accelerated if an accelerator is chosen from the **Accelerate** drop-down list.
TFO Only	Applies a different TFO techniques to matching traffic. TFO techniques include BIC-TCP, window size maximization and scaling, and selective acknowledgment. For more information on the TFO feature, see Transport Flow Optimization in the chapter "Introduction to Cisco WAAS."
TFO with DRE (Adaptive Cache)	Applies both TFO and DRE with adaptive caching to matching traffic.
TFO with DRE (Unidirectional Cache)	Applies both TFO and DRE with unidirectional caching to matching traffic.
TFO with DRE (Bidirectional Cache)	Applies both TFO and DRE with bidirectional caching to matching traffic.
TFO with LZ Compression	Applies both TFO and the LZ compression algorithm to matching traffic. LZ compression functions similarly to DRE, but uses a different compression algorithm to compress smaller data streams and maintains a limited compression history.
TFO with DRE (Adaptive Cache) and LZ	Applies TFO, DRE with adaptive caching, and LZ compression to matching traffic.
TFO with DRE (Unidirectional Cache) and LZ	Applies TFO, DRE with unidirectional caching, and LZ compression to matching traffic.
TFO with DRE (Bidirectional Cache) and LZ	Applies TFO, DRE with bidirectional caching, and LZ compression to matching traffic.

Step 6 Consider the following guidelines for class map actions:

- For a Cisco WAAS Express device, the following subset of actions is available: **Passthrough**, **TFO Only**, **TFO with LZ**, **TFO with DRE**, and **TFO with DRE and LZ**.
- When ICA acceleration is enabled, all the connections are processed with the DRE mode as **Unidirectional**, and acceleration type is shown as **TIDL** (TCP optimization, ICA acceleration, DRE, and LZ).
- When configuring optimization policies on a device group:
    - If the device group contains devices running a Cisco WAAS version earlier than 4.4.1 and you are configuring an action that includes **Unidirectional** or **Adaptive** caching, the caching mode is converted to **Bidirectional**.

  - When devices running a Cisco WAAS version earlier than 4.4.1 join a device group that is configured with optimization policies that use **Unidirectional** or **Adaptive** caching, the caching mode is converted to **Bidirectional**.

In both of these cases, we recommend that you upgrade all the devices to the same software version or create different device groups for devices with incompatible versions.

Step 7 From the **Accelerate** drop-down list, choose one of the following additional acceleration actions that your Cisco WAAS device should take on the defined traffic:

- **None**: No additional acceleration is done.
- **MS PortMapper**: Accelerate using the Microsoft Endpoint Port Mapper (EPM).
- **SMB Adapter**: Accelerate using the SMB Accelerators.
- **HTTP Adapter**: Accelerate using the HTTP Accelerator.
- **MAPI Adapter**: Accelerate using the MAPI Accelerator.
- **ICA Adapter**: Accelerate using the ICA Accelerator.
- **For a Cisco WAAS Express device**, HTTP Express is available as an accelerator.

Step 8 Specify the application that you want to associate with this policy by performing either of the following:

- From the **Application** drop-down list, choose an existing application such as the one that you created, as described in Creating an Application Definition. This list displays all the predefined and new applications on your Cisco WAAS system.
- To create an application, click **New Application**.
  - Specify the application name.
  - Enable statistics collection.
  - To save the new application and return to the **Optimization Policy** window, click **OK**.

    The new application is automatically assigned to this device or device group.

Step 9 (Optional) From the **DSCP Marking** drop-down list, choose one of the following:

- To copy the DSCP value from the incoming packet and use it for the outgoing packet, choose copy.
- To use the DSCP value defined at the application or global level, choose inherit-from-name.
- Consider the following guidelines for using DSCP:
  - DSCP is the combination of IP Precedence and Type of Service (ToS) fields. DSCP is a field in an IP packet that enables different levels of service to be assigned to network traffic. Levels of service are assigned by marking each packet on the network with a DSCP code and associating a corresponding level of service. For more information, see RFC 2474.
  - DSCP marking does not apply to pass-through traffic.
  - In a Cisco WAAS Express device, the DSCP Marking drop-down list is not shown.

- For the DSCP marking value, you can choose to use the global default values (see Defining Default DSCP Marking Values) or select one of the other defined values. Or, you can use copy, as described above.

Step 10 Click **OK**.

The new policy appears in the **Optimization Policies** window.

Creating an Optimization Class Map

Before you begin

You can create an optimization class map for an optimization policy in two ways:

- In the device context, choose **Configure** > **Acceleration** > **Optimization Class-Map**, and then click the **Add Class-Map** taskbar icon.

  The **Optimization Class-Map** pane is displayed.

- While adding or editing a policy rule, as described in Creating an Optimization Policy, click **Create New** next to the **Class-Map Name** drop-down list.

  The **Optimization Class-Map** pane is displayed.

Procedure

Step 1 Enter a name for this application class map.

Consider the following guidelines:

- The name cannot contain spaces or special characters.
- You must create a unique class map name across all types. For example, you cannot use the same name for an optimization class map and an AppNav class map.
- For Cisco WAAS Express, the class map name cannot contain the following prefixes (case sensitive): class, optimize, passthrough, application, accelerate, tfo, dre, lz, or sequence-interval. Existing class map names containing any of these prefixes must be changed manually.

Step 2 (Optional) Enter a description.

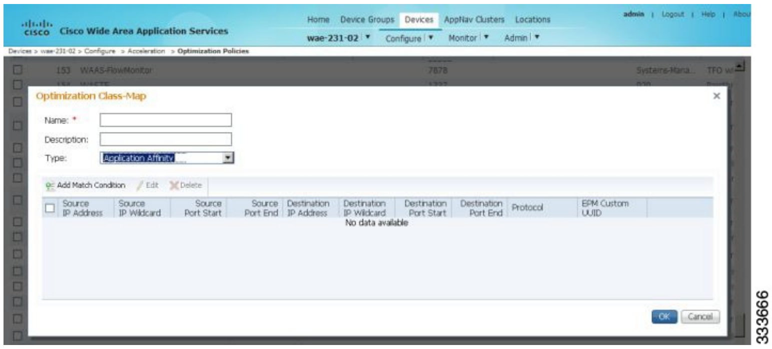
Step 3 From the **Type** drop-down list, choose the class map type.

- To match specific TCP traffic, choose **Application Affinity**.
- To match all TCP traffic choose **Any TCP Traffic**.

Step 4 After you have chosen the class map type, enter the match conditions. Click the **Add Match Condition** icon.

The **Adding a New Match Condition** Window appears.

Figure 79: Adding a New Match Condition Window



Name: *

Description:

Type: Application Affinity

☐	Source IP Address	Source IP Wildcard	Source Port Start	Source Port End	Destination IP Address	Destination IP Wildcard	Destination Port Start	Destination Port End	Protocol	EPM Custom UUID
					No data available					

Note For a Cisco WAAS Express device, Protocol and EPM Custom UUID settings are not applicable.

Step 5 To create a condition for a specific type of traffic, enter a value in a **Destination** or **Source** field.

For example, to match all the traffic going to IP address 10.10.10.2, enter that IP address in the **Destination IP Address** field.

Consider the following guidelines for creating conditions:

- To specify a range of IP addresses, enter a wildcard subnet mask in either the **Destination IP Wildcard** field or **Source IP Wildcard** field in dotted decimal notation, such as 0.0.0.255 for /24.
- To match traffic that uses dynamic port allocation, from the **Protocol** drop-down list, choose the corresponding application identifier.

  For example, to match Microsoft Exchange Server traffic that uses the MAPI protocol, choose **mapi**. To enter a custom EPM UUID, choose **epm-uuid** and enter the UUID in the **EPM Custom UUID** field.
- If you try to create a class map with an EMP UUID match condition that is already being used, that class map is removed and an error message is displayed stating that a class map already exists with the same EPM UUID match condition.

Step 6 Add additional match conditions, as needed. If any one of the conditions is matched, the class is considered as matched.

Step 7 To save the class map, click **OK**.

Managing Application Acceleration

This section contains the following topics:

Modifying the Accelerator Load Indicator and CPU Load-Monitoring Threshold

Before you begin

High CPU utilization can adversely affect current optimized connections. To avoid CPU overload, you can enable CPU load monitoring and set the load monitoring threshold:

- When the average CPU utilization on the device exceeds the set threshold for 2 minutes, the device stops accepting new connections and passes new connections, if any, through.
- When the average CPU utilization falls below the threshold for 2 minutes, the device resumes accepting optimized connections.
- When a CPU overload condition occurs, the polling interval is reduced to an interval of 2 seconds. Although the average CPU utilization may fall below the threshold during this time and the overload condition cleared, the CPU alarm may still be present. The CPU alarm is cleared *only when* the overload condition does not reappear in the next 2-minute-interval poll.

Procedure

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

Step 2 Choose **Configure > Acceleration > Accelerator Threshold**.

The **Accelerator Threshold** window appears.

Step 3 To enable CPU Load Monitoring, check the **Enable** check box. (The default is enabled.)

Step 4 In the **Accelerator Load Indicator Threshold** field, enter a percent value between **80** and **100**. The default is **95**.

Step 5 In the **CPU Load Higher Monitoring Threshold** field, enter a percent value between **1** and **100**. The default is **98**.

Step 6 In the **CPU Load Lower Monitoring Threshold** field, enter a percent value between **1** and **100**. The default is **90**.

Step 7 In the **Window Size** field enter a value between **1** and **16**. The default value is **4**.

Step 8 In the **Sampling Intervals Avg Time** field enter a value between **1** and **120**. The default is **10**.

Step 9 In the **Overloaded State Time** field, enter a value between **1** and **120**. The default value is **10**.

Step 10 Click **Submit**.

If the device group is running the Cisco WAAS Version 6.x, you can configure additional settings to monitor the CPU load for the device group.

Step 11 To enable CPU Load Monitoring, check the **Enable** check box. (The default is enabled.)

Step 12 To enable **softirq** monitoring , check the **Enable softirq Monitoring** checkbox.

Step 13 In the **Accelerator Load Indicator Threshold** field, enter a percent value between **80** and **100**. The default is **95**.

Step 14 In the **CPU Load Monitoring Threshold** field, enter a percent value between **80** and **100**. The default is **95**.

Step 15 In the **CPU Load Higher Monitoring Threshold** field, enter a percent value between **1** and **100**. The default is **98**.

Step 16 In the **CPU Load Lower Monitoring Threshold** field, enter a percent value between **1** and **100**. The default is **90**.

Step 17 In the **Window Size** field enter a value between **1** and **16**. The default value is **4**.

Step 18 In the **Sampling Intervals Avg Time** field enter a value between **1** and **120**. The default is **10**.

Step 19 In the **Overloaded State Time** field, enter a value between **1** and **120**. The default value is **10**.

Step 20 Click **Submit**.

Viewing a List of Applications

Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **Optimization Policies**.

The **Optimization Policies** window appears.

Step 3 Click the **Application** column header to sort the column by application name so that you can locate a specific application more easily.

Note If there are Cisco WAAS Version 4.x devices, click the **Legacy View** taskbar icon to view the policies as they appear in a Cisco WAAS Version 4.x device.

To edit an optimization policy, check the box next to the application and click the **Edit** taskbar icon.

If you determine that one or more policies are not needed, check the check box next to each of these applications and click the **Delete** taskbar icon.

If you determine that a new policy is needed, click the **Add Policy Rule** taskbar icon (see Creating an Optimization Policy).

Viewing a Policy Report

Procedure

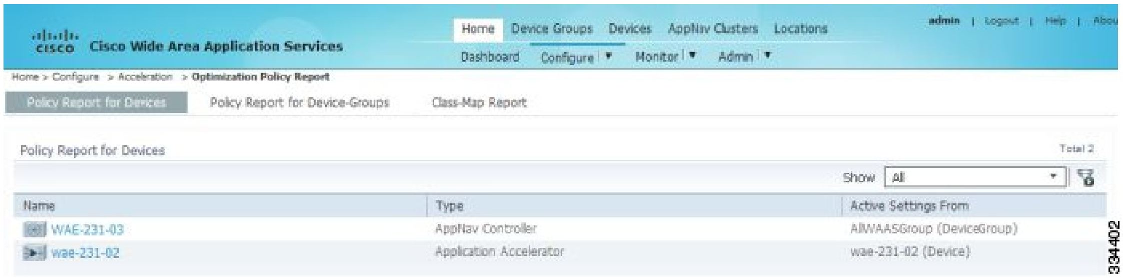
Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **Acceleration** > **Optimization Policy Report**.

The **Policy Report for Devices** tab appears.

Consider the following guidelines for viewing a policy report:

- The policy report lists each device (or device group) and the overall policy count on the device (or device group) referencing this application.
- The policy report includes both active policies (those in use by the device or device group), and backup policies (those not in use by the device when the device gets its configuration from a device group).
- When the device is deassigned from the device group, the backup policies are applied back to the device and become active again.
- An application cannot be deleted unless the **No. of Policies** field is **0**.

Figure 80: Optimization Policy Report


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
admin | Logout | Help | About
Dashboard
Configure
Monitor
Admin
Home > Configure > Acceleration > Optimization Policy Report
Policy Report for Devices
Policy Report for Device-Groups
Class-Map Report
Policy Report for Devices
Total 2
Show All
334402

Name	Type	Active Settings From
WAE-231-03	AppNav Controller	AllWAASGroup (DeviceGroup)
wae-231-02	Application Accelerator	wae-231-02 (Device)

Step 2 To view the number of devices per device group and the number of active policies in the device group, click the **Policy Report for Device-Groups** tab.

Step 3 To see the optimization policies that are defined on a particular device or group, click the corresponding device or device group. The policies are displayed in the **Optimization Policies** window.

For information about viewing a class map report, see Viewing a Class Map Report.

Viewing a Class Map Report

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **Acceleration** > **Optimization Policy Report**.

The **Policy Report for Devices** tab appears.

Step 2 To view a report of the devices and device groups on which the class map is configured, click the **Class-Map Report** tab.

Step 3 To see the devices or device groups on which the class maps reside, select the class map and click the **View** icon.

Restoring Optimization Policies and Class Maps

Before you begin

The Cisco WAAS system allows you to restore the predefined policies and class maps that shipped with the Cisco WAAS system. For a list of the predefined policies, see Appendix A, "Predefined Optimization Policy."

If you made changes to the predefined policies that have negatively impacted how a Cisco WAAS device handles application traffic, you can override your changes by restoring the predefined policy settings.

Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **Optimization Policies**.

The **Optimization Policies** window appears.

Step 3 To restore over 150 policies and class maps that shipped with the Cisco WAAS software, and to remove any new policies that were created on the system, click the **Restore Default** taskbar icon. If a predefined policy has been changed, these changes are lost and the original settings are restored.

Monitoring Applications and Class Maps

Before you begin

After you create an optimization policy, monitor the associated application to verify that your Cisco WAAS system is handling the application traffic as expected.

Before you monitor an application, you must have enabled statistics collection for that application, as described in the Creating an Application Definition.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Configure** > **Acceleration** > **Monitor Classmaps**.

Step 2 Select the class map on which to enable statistics and then click **Enable**.

Consider the following guidelines for monitoring applications and class maps:

- The Cisco WAAS Central Manager GUI can display statistics for up to 25 applications and 25 class maps.
    - To monitor a specific application, run the **TCP Summary report**. For more information, see the TCP Summary Report in the chapter "Monitoring Your Cisco WAAS Network."
    - If you try to display more than 25 statistics for either applications or class maps, an error message is displayed.
- To view statistics for all applications that have policies on a specific Cisco WAAS device, use the Cisco WAAS CLI. For more information, see the *Cisco Wide Area Application Services Command Reference*.

Step 3 To configure Cisco WAAS charts to display Class Map data:

a) Click the chart **Edit** icon.

b) Choose the **Classifier** series.

This configuration option applies to most Cisco WAAS charts.

Defining Default DSCP Marking Values

Before you begin

According to policies that you define in an application definition and an optimization policy, the WAAS software allows you to set a DSCP value on packets that it processes

- A DSCP value is a field in an IP packet that enables different levels of service to be assigned to the network traffic.
- The levels of service are assigned by marking each packet on the network with a DSCP code and associating a corresponding level of service.
- The DSCP marking determines how packets for a connection are processed externally to Cisco WAAS. DSCP is the combination of **IP Precedence** and **Type of Service (ToS)** fields.
- For more information, see RFC 2474.

These attributes can be defined at the following levels:

- **Global**: Define global defaults for the DSCP value for each device (or device group) in the Optimization Policies page for that device (or device group). This value applies to the traffic if a lower level value is not defined.
- **Policy**: Define the DSCP value in an optimization policy. This value applies only to traffic that matches the class maps defined in the policy and overrides the application or global DSCP value.

Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **Optimization Policies**.

The **Optimization Policies** window appears.

Step 3 Choose a value from the **DSCP** drop-down list. The default setting is copy, which copies the DSCP value from the incoming packet and uses it for the outgoing packet.

Step 4 To save the settings, click **OK**.

Modifying the Position of an Optimization Policy

Before you begin

Considering the following configuration guidelines for optimization policy positions:

- Each optimization policy has an assigned position that determines the order in which a Cisco WAAS device refers to the policy in an attempt to classify traffic.

For example, when a Cisco WAAS device intercepts traffic, it refers to the first policy in the list to try to match the traffic to an application. If the first policy does not provide a match, the Cisco WAAS device moves on to the next policy in the list.

- Consider the position of policies that pass through traffic as unoptimized, because placing these policies at the top of the list can cancel out optimization policies that appear farther down the list.

  For example, If you have two optimization policies that match traffic going to IP address 10.10.10.2, and one policy optimizes this traffic and a second policy in a higher position passes through this traffic, then all traffic going to 10.10.10.2 will go through the Cisco WAAS system unoptimized.

  For this reason, ensure that your policies do not have overlapping matching conditions, and monitor the applications you create to make sure that WAAS is handling the traffic as expected.

- For more information on monitoring applications, see the chapter Monitoring Your Cisco WAAS Network, on page 553

  .

Procedure

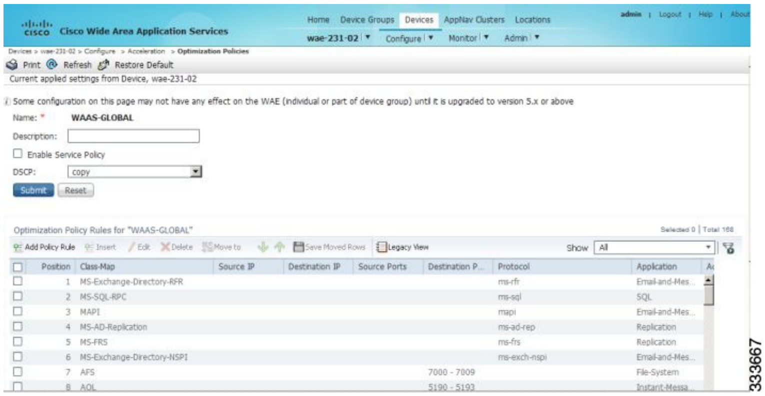
Step 1 From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 2 Choose **Configure** > **Acceleration** > **Optimization Policies**.

The **Optimization Policies** window appears.

Note For a Cisco WAAS Express device, all policies are grouped under the **waas_global** category.

Figure 81: Optimization Policies Window



Current applied settings from Device, wae-231-02

Some configuration on this page may not have any effect on the WAE (individual or part of device group) until it is upgraded to version 5.x or above

Name: * WAAS-GLOBAL

Description:

□ Enable Service Policy

DSCP: copy

Optimization Policy Rules for "WAAS-GLOBAL"

Selected 0 | Total 168

Show All

□	Position	Class-Map	Source IP	Destination IP	Source Ports	Destination P...	Protocol	Application	A(
□	1	MS-Exchange-Directory-RFR					ms-rfr	Email-and-Mes...	
□	2	MS-SQL-RPC					ms-sql	SQL	
□	3	MAPI					mapi	Email-and-Mes...	
□	4	MS-AD-Replication					ms-ad-rep	Replication	
□	5	MS-FRS					ms-frs	Replication	
□	6	MS-Exchange-Directory-NSPI					ms-exch-nspi	Email-and-Mes...	
□	7	AFS				7000 - 7009		File-System	
□	8	AOL				5190 - 5193		Instant-Messa...	

Step 3 To modify the position of the optimization policy, use one of the following methods, and then click the **Save Moved Rows** icon:

- Select the policy you want to move, and then use the up and down arrow icons in the taskbar to move that policy higher or lower in the list.
- Select the policy you want to move, and then, to specify the new position, click **Move To**.
- Select the policy, and then drag and drop it into the new position.

Step 4 To save the new policy position(s), click **Save Moved Rows**.

Step 5 (Optional) To create a new optimization policy at a particular position:

a) Select the policy *above* the location.

b) Click **Insert**.

Step 6 If a device goes through all the policies in the list without making a match, the Cisco WAAS device passes the traffic through unoptimized.

Note For a Cisco WAAS Express device, the class default policy must be last. This policy cannot be modified or deleted.

Step 7 To save changes, click the **Save Moved Rows**.

Step 8 If you determine that a policy is not needed, follow these steps to delete the policy:

a) Select the policy you want to delete.

b) Click the **Delete** icon in the taskbar.

A default policy that maps to a default class map matching any traffic cannot be deleted.

Step 9 If you determine that a new policy is needed, click the **Add Policy** taskbar icon to create the policy.

For more information, see Creating an Optimization Policy.

Modifying the Acceleration TCP Settings

Before you begin

In most cases, you do not need to modify the acceleration TCP settings, because your Cisco WAAS system automatically configures the acceleration TCP settings based on the hardware platform of the Cisco WAE device.

- Cisco WAAS automatically configures the settings only under the following circumstances:
  - When you first install the Cisco WAE device in your network.
  - When you run the **restore factory-default** CLI command on the Cisco WAAS device.

    For more information about this command, see the *Cisco Wide Area Application Services Command Reference*.
- The Cisco WAAS system automatically adjusts the maximum segment size (MSS) to match the advertised MSS of the client or server for each connection. The Cisco WAAS system uses the lower of 1432 or the MSS value advertised by the client or server.
- If your Cisco WAAS network has high BDP links, you may need to adjust the default buffer settings automatically configured for your WAE device. For more information, see Modifying the TCP Adaptive Buffering Settings.
- If you want to adjust the default TCP adaptive buffering settings for your Cisco WAE device, see Modifying the TCP Adaptive Buffering Settings.

Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **TCP Settings**.

The **Acceleration TCP Settings** window appears.

Step 3 Check the **Send TCP Keepalive** check box. (By default, this check box is checked.)

- Checking the **Send TCP Keepalive** check box allows this Cisco WAE device or group to disconnect the TCP connection from its peer device if no response is received from the TCP keepalive exchange.
  - In this case, the two peer WAE devices will exchange TCP keepalives on a TCP connection, and if no response is received for the keepalives for a specific period, the TCP connection will be torn down.
  - When the keepalive option is enabled, any short network disruption in the WAN will cause the TCP connection between peer WAE devices to be disconnected.
- If the **Send TCP Keepalive** check box is not checked, TCP keepalives will not be sent and connections will be maintained unless they are explicitly disconnected.
- To use the CLI to configure TCP keepalives:
  - To configure TCP keepalives, run the **tfo tcp keepalive** global configuration command.
  - To configure TCP acceleration settings, run the following global configuration commands:
    - **tfo tcp optimized-mss**
    - **tfo tcp optimized-receive-buffer**
    - **tfo tcp optimized-send-buffer**
    - **tfo tcp original-mss**
    - **tfo tcp original-receive-buffer**
    - **tfo tcp original-send-buffer**
  - To show the TCP buffer sizes, run the **show tfo tcp** EXEC command.

Step 4 Modify the TCP acceleration settings, as needed. See the following table for a description of these settings.

For information on how to calculate these settings for high BDP links, see Modifying the TCP Adaptive Buffering Settings.

Table 52: TCP Settings

TCP Setting	Description
Optimized Side	

TCP Setting	Description
Maximum Segment Size	Maximum packet size allowed between a Cisco WAAS device and other Cisco WAAS devices participating in the optimized connection. The default is 1432 bytes.
Send Buffer Size	Allowed TCP sending buffer size (in kilobytes) for TCP packets sent from a Cisco WAAS device to other Cisco WAAS devices participating in the optimized connection. The default is 32 KB.
Receive Buffer Size	Allowed TCP receiving buffer size (in kilobytes) for incoming TCP packets from other Cisco WAAS devices participating in the optimized connection. The default is 32 KB.
Original Side	
Maximum Segment Size	Maximum packet size allowed between the origin client or server and a Cisco WAAS device. The default is 1432 bytes.
Send Buffer Size	Allowed TCP sending buffers size (in kilobytes) for TCP packets sent from a Cisco WAAS device to the origin client or server. The default is 32 KB.
Receive Buffer Size	Allowed TCP receiving buffer size (in kilobytes) for incoming TCP packets from the origin client or server. The default is 32 KB.

Step 5 If you are deploying the WAE across a high Bandwidth-Delay-Product (BDP) link, you can set recommended values for the send and receive buffer sizes by clicking **Set High BDP** recommended values. For more information, see Modifying the TCP Adaptive Buffering Settings.

Step 6 Consider the following guideliens for segment sizes and configuring jumbo MTU settings:

- If the original and optimized maximum segment sizes are set to their default values and you configure a jumbo MTU setting, the segment sizes are changed to the jumbo MTU setting minus 68 bytes.
- If you have configured custom maximum segment sizes, their values are not changed if you configure a jumbo MTU.
- For more information, see Configuring a Jumbo MTU in the chapter "Configuring Network Settings."

Modifying the TCP Adaptive Buffering Settings

Before you begin

In most cases, you do not need to modify the acceleration TCP adaptive buffering settings because your Cisco WAAS system automatically configures the TCP adaptive buffering settings based on the network bandwidth and delay experienced by each connection. Adaptive buffering allows the Cisco WAAS software to dynamically vary the size of the send and receive buffers to increase performance and more efficiently use the available network bandwidth.

Procedure

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

Step 2 Choose **Configure** > **Acceleration** > **TCP Adaptive Buffering Settings**.
The TCP Adaptive Buffering Settings window appears.

Step 3 To enable TCP adaptive buffering, check the **Enable** check box. (By default, this is enabled.)

Step 4 In the Send Buffer Size and Receive Buffer Size fields, enter the maximum size, in kilobytes, of the send and receive buffers.

Step 5 Click **Submit**.

To configure the TCP adaptive buffer settings from the CLI, run the **tfo tcp adaptive-buffer-sizing** global configuration command:

```
WAE(config)# tfo tcp adaptive-buffer-sizing receive-buffer-max 8192
```

To disable TCP adaptive buffering from the CLI, run the no tfo tcp adaptive-buffer-sizing enable global configuration command.

To show the default and configured adaptive buffer sizes, run the **show tfo tcp** EXEC command.

What to do next

Calculating the TCP Buffers for High BDP Links:

Cisco WAAS software can be deployed in different network environments, involving multiple link characteristics such as bandwidth, latency, and packet loss. All Cisco WAAS devices are configured to accommodate networks with maximum **Bandwidth-Delay-Product (BDP)** of up to the values listed below:

- Cisco WAE-512: Default BDP is 32 KB
- Cisco WAE-612: Default BDP is 512 KB
- Cisco WAE-674: Default BDP is 2048 KB
- Cisco WAE-7326: Default BDP is 2048 KB
- Cisco WAE-7341: Default BDP is 2048 KB
- Cisco WAE-7371: Default BDP is 2048 KB
- All Cisco WAVE platforms: Default BDP is 2048 KB

Consider the following operating guidelines for BDP:

- If your Cisco WAAS network provides higher bandwidth, or if higher latencies are involved, use the following formula to calculate the actual link BDP:

  BDP [Kbytes] = (link BW [Kbytes/sec] * Round-trip latency [Sec])

- When multiple links **1..N** are the links for which the Cisco WAE is optimizing traffic, the maximum BDP should be calculated as follows:

  MaxBDP = Max (BDP(link 1),..,BDP(link N))

- If the calculated **MaxBDP** is greater than the **DefaultBDP** for your Cisco WAE model, modify the **Acceleration TCP** to accommodate that calculated BDP.
- After you calculate the size of the **MaxBDP**, enter a value that is equal to or greater than twice the **MaxBDP** in the **Send Buffer Size** and **Receive Buffer Size** fields for the optimized connection in the **Acceleration TCP Settings** window.

Note These manually configured buffer sizes are applicable only if TCP adaptive buffering is disabled. TCP adaptive buffering is normally enabled, and allows the Cisco WAAS system to dynamically vary the buffer sizes.

CHAPTER 13

Configuring WAAS with Akamai Connect

This chapter describes how to configure Cisco WAAS with Akamai Connect, which is an integrated solution that combines WAN optimization and intelligent object caching to accelerate HTTP/S applications, video, and content.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco Wide Area Application Services (Cisco WAAS) Central Managers and Cisco Wide Area Application Engines (WAEs) in your network. The term WAE refers to WAE and Cisco Wide Area Virtualization Engine (WAVE) appliances, and Cisco Virtual WAAS (vWAAS) instances.

This chapter contains the following sections:

Note Akamai Connect is the HTTP/S object cache component added to Cisco WAAS, integrated into the existing WAAS software stack and leveraged via the HTTP Application Optimizer. WAAS with Akamai Connect helps to reduce latency for HTTP/S traffic for business and web applications.Akamai Connected Cache is a component of Akamai Connect, which allows the Cache Engine to cache content that is delivered by an Edge server on the Akamai Intelligent Platform.

This chapter contains the following sections:

About Cisco WAAS with Akamai Connect

Akamai Connect is the HTTP/S object cache component added to Cisco WAAS, integrated into the existing WAAS software stack and leveraged via the HTTP Application Optimizer.

- Cisco WAAS with Akamai Connect helps to reduce latency for HTTP/S traffic for business and web applications, and can improve performance for many applications, including Point of Sale (POS), HD video, digital signage, and in-store order processing.
- Cisco WAAS with Akamai Connect provides significant and measurable WAN data offload, and is compatible with existing WAAS functions such as DRE (deduplication), LZ (compression), TFO (Transport Flow Optimization), and SSL acceleration (secure/encrypted) for first and second pass acceleration.

Akamai Connected Cache is a component of Akamai Connect, which allows the cache engine to cache content that is delivered by an edge server on the Akamai Intelligent Platform.

The following list highlights some of the benefits offered by Cisco WAAS with Akamai Connect:

- Intelligent transparent object caching.
- Seamless integration of Akamai Connect into Cisco WAAS software and configuration, using either the Cisco WAAS Central Manager or Cisco WAAS CLI.
- Integration with Akamai's Edge Grid Network, which provides low-latency Content Delivery Network transfers via Akamai Connected Cache.
- Significant and measurable WAN data offload.
- Cache prepositioning (warming) for websites that you specify.
- Hostname rules for cache control of specific websites or domains.
- First-pass and second-pass acceleration, with Akamai Connect working with Cisco WAAS middle-mile capabilities, including DRE, LZ, TFO, and SSL acceleration.
- Dual-sided or single-sided deployment.

Components of Cisco WAAS with Akamai Connect

The table provides overviews of Cisco WAAS with Akamai Connect components, links to further information, and links to Akamai Connect configuration procedures.

Table 53: Components of Cisco WAAS with Akamai Connect

Component	Description and Further Information
Deployment Options	You can deploy Cisco WAAS with Akamai Connect as a dual-sided or single-sided deployment. For more information, see Deployment Options for Cisco WAAS with Akamai Connect, on page 470.
Akamai Connect license	The Akamai Connect license for Cisco WAAS is an advanced license available for all supported Cisco with Akamai Connect devices. The Akamai Connect license for Cisco WAAS is aligned with the number of optimized connections in each supported Cisco WAAS device. For more information, see Activating and Managing the Akamai Connect License, on page 480.
Supported Cisco WAAS platforms	For Cisco WAAS Version 5.4.1 and later, Cisco with Akamai Connect supports WAAS and vWAAS devices up to 6,000 connections. For Cisco WAAS Versions later than Cisco WAAS Version 5.4.1, Cisco with Akamai Connect supports WAAS and vWAAS devices beyond 6,000 connections. For more information, see Supported Platforms for Cisco WAAS with Akamai Connect, on page 471.
Transparent cache and caching policies	The Transparent cache, Akamai's high-performance HTTP object cache, provides the ability to locally cache HTTP-based content for LAN-like performance, regardless of whether the web application was served from the private corporate cloud or the public Internet. This content includes on-demand and live HTTP video streams to deliver fast, high-quality, high-definition video experiences in the branch, all while offloading the enterprise network. There are four caching policies (modes): **Basic**, **Standard** (default), **Advanced**, and **Bypass**. For more information, see Setting Transparent Caching Policies, on page 489.
Akamai Connected Cache	Akamai's proprietary caching rules in connection with the edge servers of the Akamai Intelligent Platform lets you cache and deliver content inside the branch office that might otherwise be deemed noncacheable. This content could be an enterprise's own web content or any content that is delivered by the Akamai Intelligent Platform, which is up to thirty percent of all web traffic. For more information, see Enabling Akamai Connected Cache.
Over the Top (OTT) caching	Over-The-Top (OTT) caching is used for streamed content, particularly video content. OTT caching caches HTTP content served from dynamic URLs and content marked as noncacheable, such as YouTube videos. Akamai achieves this by using metadata logic to determine a unique cache key per video, which allows dynamic URLs to be cached. For more information, see Enabling Over the Top (OTT) Caching, on page 487.

Component	Description and Further Information
Cisco Cloud Web Security (CWS)	Cisco Cloud Web Security (CWS) provides content scanning of HTTP and HTTP/S traffic, and provides malware protection service to web traffic. CWS enforces content filtering by enabling force IMS for every cached object, for both single-sided and dual-sided deployment. For more information, see Enabling Cisco Cloud Web Security (Cisco CWS), on page 493.
Cisco WAAS connections to the Akamai network	There are three ways for Cisco WAAS devices to connect to the Akamai network: • No HTTP proxy • Use Cisco WAAS Central Manager as HTTP proxy • Use an external HTTP proxy For more information, see Configuring Cisco WAAS Connections to the Akamai Network, on page 494.
Cache prepositioning	Cache prepositioning, also known as cache warming, allows you to specify a policy to prefetch and cache content at a specified time. Cache prepositioning allows you to take advantage of idle time on the WAN to transfer large or frequently accessed files to selected Cisco WAAS devices, so that users can benefit from cache-level performance even during first-time access of these files. For more information, see Configuring Akamai Connect Cache Prepositioning, on page 501.
Cisco support for Microsoft Update	Cisco support for Microsoft Windows Update enables the Akamai cache engine to support Windows Update in two ways: to download and cache full objects even when ranges within objects that not in cache are requested, and future range requests on the objects can be served out of cache. For more information, see Cisco Support for Microsoft Windows Update, on page 508.

Deployment Options for Cisco WAAS with Akamai Connect

This section contains the following topics:

About Deployment Options for Cisco WAAS with Akamai Connect

You can deploy Cisco WAAS with Akamai Connect as a dual-sided or single-sided deployment:

- Dual-sided deployment of Cisco WAAS with Akamai Connect provides the following benefits for HTTP and HTTPS traffic:
    - Transparent caching of customer-owned, Intranet web resources.

- Caching in branch only.
- Includes prepositioning (for non-SSL content).

- Single-sided deployment of Cisco WAAS with Akamai Connect provides the following benefits for HTTP and HTTPS traffic:
  - Generic web resources that utilize proxy-specific HTTP cache-control headers.
  - Caching in branch only.
  - Includes prepositioning (for non-SSL content).

Note For Transparent caching in **Standard** mode, single-sided deployment of Cisco WAAS with Akamai Connect is enabled by default.

Operating Guidelines for Cisco WAAS with Akamai Connect

Consider the following operating guidelines for Cisco WAAS with Akamai Connect:

- There is no separate cache for HTTPS content. However, data is stored differently for the same site if both HTTP and HTTPS are accessing. (The way the sites are stored in the cache is based on the URL, and this will change between HTTP and HTTPS.)
- You cannot view the contents of the cache, and cannot pin content to make it remain in the cache, for example, for prepositioned content.
- The Akamai cache engine has no explicit integration with Cisco AppNav. The Cisco AppNav status is based on the Cisco HTTP application accelerator.

Supported Platforms for Cisco WAAS with Akamai Connect

The flow of allocated resources to the Akamai Cache Engine is controlled by the WAAS Central Manager, but the overall resource pool and the amount of resources that can be allocated to the Akamai Cache Engine is controlled by the hardware platform, and the number of supported connections and users that the router is designed to service.

This section contains the following topics:

Supported Platforms for Cisco WAAS with Akamai Connect up to 6,000 Connections

The flow of allocated resources to the Akamai cache engine is controlled by the Cisco WAAS Central Manager, but the overall resource pool and the amount of resources that can be allocated to the Akamai cache engine is controlled by the following:

- the hardware platform

- the number of supported connections and users that the router is designed to service

The following table shows supported platforms for Cisco WAAS with Akamai Connect up to 6,000 connections, for Cisco WAAS Version 5.4.1 and later. For information on supported platforms for Cisco WAAS with Akamai Connect beyond 6,000 connections, see Supported Platforms for Cisco WAAS with Akamai Connect beyond 6,000 Connections.

Table 54: Supported Platforms for Cisco WAAS with Akamai Caching up to 6,000 Connections

Appliance	SM	vWAAS	ISR-WAAS
N/A	N/A	vWAAS-150	ISR-G2 and ISR-G3
WAVE-294	SM-700	vWAAS-200	ISR-WAAS-750 • ISR-4451 • ISR-4431 • ISR-4351 • ISR-4331 • ISR-4321
WAVE-594	SM-900	vWAAS-750	ISR-WAAS-1300 • ISR-4451 • ISR-4431
WAVE-694	SM-710	vWAAS-1300	ISR-WAAS-2500 • ISR-4451
N/A	SM-910	vWAAS-2500	N/A
N/A	N/A	vWAAS-6000	N/A

Note If you are upgrading from a version earlier than Cisco vWAAS in Cisco WAAS Version 5.4.x, you will need a third disk and possibly more memory added. For more information, see the “Cisco vWAAS with Akamai Connect” chapter in the *Cisco Virtual Wide Area Application Services Configuration Guide*.

Supported Platforms for Cisco WAAS with Akamai Connect beyond 6,000 Connections

This section describes the supported Cisco platforms for Cisco WAAS with Akamai Connect beyond 6,000 Connections, and operating guidelines for these platforms.

The flow of allocated resources to the Akamai cache engine is controlled by the Cisco WAAS Central Manager, but the overall resource pool and the amount of resources that can be allocated to the Akamai cache engine is controlled by the hardware platform and the number of supported connections and users that the router is designed to service.

For Cisco WAAS Version 6.2.1 and later, the following list shows the Cisco WAAS with Akamai Connect supported platforms for scaling beyond 6,000 connections:

- Cisco WAVE-7541 or Cisco CSP 5228-W
- Cisco WAVE-7571 or Cisco CSP 5228-W
- Cisco WAVE-8541 or Cisco CSP 5436-W
- Cisco vWAAS-12000
- Cisco vWAAS-50000

For Cisco WAAS with Akamai Connect in Cisco WAAS Version 5.4.1 and earlier, see Supported Platforms for Cisco WAAS with Akamai Connect up to 6,000 Connections.

Consider the following operating guidelines for supported platforms for Cisco WAAS with Akamai Connect beyond 6,000 connections:

- Supported Cisco WAVE models with Akamai Connect beyond 6,000 Connections:
    - The table "Cisco WAAS with Akamai Connect Requirements for HTTP Object Cache" shows the supported Cisco WAVE models with Akamai Connect beyond 6,000 connections, and specifications for the total HTTP object cache connections and cache engine cache disk.

      Table 55: Cisco WAAS with Akamai Connect Requirements for HTTP Object Cache

Cisco WAVE Model	Total HTTP Object Cache Connections	Cache Engine Cache Disk
WAVE-7541	18 K	708 GB
WAVE-7571	45 K	839 GB
WAVE-8541	112 K	675 GB

    - The Akamai cache engine connection-handling capacity is determined by the upper limit of memory that is given to the Akamai cache engine at startup. The Akamai cache engine will allocate memory as needed up to the upper limit. In case of overload, the connection will be optimized by HTTP-AO, without a caching benefit.

      Note When a Cisco WAVE model used for Akamai Connect beyond 6,000 connections is assigned to a device group in the Cisco WAAS Central Manager *after* Akamai Connect is already enabled, you must manually reload the Cisco WAVE device. Akamai Connect will remain in shutdown state until the reload is performed.

- Supported Cisco vWAAS models with Akamai Connect beyond 6,000 connections:

- The table "Cisco vWAAS with Akamai Connect Requirements for Beyond 6,000 Connections" shows supported Cisco vWAAS models with Akamai Connect beyond 6,000 connections, and specifications for total HTTP object cache connections, cache engine cache disk, and additional resources that may be needed.

Table 56: Cisco vWAAS with Akamai Connect Requirements for Beyond 6,000 Connections

Cisco vWAAS Model	Total HTTP Object Cache Connections	Cache Engine Cache Disk	Additional Resource to be Added
vWAAS-12000	12 K	750 GB	6 GB RAM, 750 GB disk
vWAAS-50000	50 K	850 GB	850 GB disk

- For Cisco vWAAS-12000 and Cisco vWAAS-50000:
  - HTTP object cache will scale up to the platform TFO limit. To achieve this, you must augment the platform resources (CPU, RAM, and disk) during provisioning.
  - For Cisco vWAAS-12000 and Cisco vWAAS-50000, you must allocate Akamai cache engine cache disk resources. Cache disk requirements are shown in above table "Cisco vWAAS with Akamai Connect Requirements for Beyond 6,000 Connections."
  - For Cisco vWAAS-12000, you must allocate at least 6 GB of additional RAM.

- Consider the following overview of operating guidelines for Cisco vWAAS with Akamai Connect caching. For detailed information on configuring and using Cisco vWAAS with Akamai Connect caching, see the “Cisco vWAAS with Akamai Connect” chapter in the *Cisco Virtual Wide Area Application Services Configuration Guide*.
  - For Cisco vWAAS in Cisco WAAS Version 6.1.1 and later, Cisco vWAAS-150 on Cisco ISR-WAAS is supported for Akamai Connect.
  - For Cisco vWAAS in Cisco WAAS Version 6.2.1 and later, Cisco vWAAS-150 is also supported for RHEL KVM and Microsoft Hyper-V.
  - For vWAAS in Cisco WAAS versions earlier than 6.x, Akamai Connect beyond 6,000 connections is not supported for Cisco vWAAS on RHEL KVM or KVM on CentOS.

Configuring HTTP Object Cache

This section contains the following topics:

Configuring HTTP Object Cache in Cisco Devices with Akamai Connect

Before you begin

- HTTP object cache is used to enable the Akamai cache engine for a Cisco device, for Cisco WAAS Version 6.2.1 and later.

- Enabling HTTP object cache for Cisco WAVE-7541, Cisco WAVE-7571 or Cisco WAVE-8541 includes configuring the device profile feature, repartitioning the Cisco WAVE data disk, and if needed, upgrading your Cisco WAAS system to Cisco WAAS Version 6.2.1 or later.

Procedure

Step 1 If needed, upgrade the Cisco WAAS Central Manager and Cisco WAE devices to Cisco WAAS Version 6.2.1 or later.

- For complete upgrade instructions, including critical prerequisites before upgrading to Cisco WAAS Version 6.2.1 or later, see the Release Note for Cisco Wide Area Application Services for your Cisco WAAS version.
- To configure HTTP object cache on Cisco vWAAS-12000 or Cisco vWAAS-50000, and to avoid object and DRE caching being lost due to execution of the **disk delete-data-partitions** EXEC command, you must downgrade from WAAS Version 6.2.x to WAAS Version 5.x, and then upgrade to WAAS Version 6.2.x.

Step 2 To enable HTTP object cache on the Cisco WAVE device, run the **accelerator http object-cache enable** global configuration command.

A message is displayed to restart the system, with two prerequisite procedures:

a) Run the **disk delete-data-partitions** EXEC command.
b) Enable **Device Profile**.

You must provide approval for each of these procedures.

Step 3 Run the **disk delete-data-partitions** EXEC command.

To accommodate the larger-scale connections available for Cisco WAAS Version 6.2.1 and later with Akamai Connect, the single partition for the RAID5-based disk subsystem is split into multiple partitions.

Note The **disk delete-data-partitions** EXEC command deletes all data partitions on all logical drives, including CONTENT, PRINTSPOOL, and SYSFS partitions. These partitions include all DRE and SMB object cache files, SYSFS and print spool files. New partitions are created at system restart.

Step 4 Enable **Device Profile**: After the upgrade is complete, **Device Profile** is initially disabled.

Considering the following operating guidelines for **Device Profile**:

- For Cisco WAAS Version 6.2.1 and later, **Device Profile** enables the device mode as branch, which tunes the resource allocation for various Cisco WAAS services as a branch traffic scenario and branch services.
- For Cisco WAVE-7541 and Cisco WAVE-8541, the **Device Profile** is automatically set or unset when you enable or disable HTTP object cache.
- For Cisco WAVE-7571, the **Device Profile** feature requires you to reboot the system to change the Device Profile feature status.

You can enable Device Profile from the Cisco WAAS Central Manager or the Cisco WAAS CLI.

- To enable Device Profile from the Cisco WAAS Central Manager:

a. Choose **Device** > *device-name* > **Configure** > **Caching** > **Device Profile**.

   The **Device Profile** window is displayed.

b. To enable **Device Profile**, check the **Branch** check box.

   Note The **Device Profile** feature is enabled at the individual device level; it is not enabled for an entire device group.

c. Click **Submit**.

- To enable **Device Profile** from the Cisco WAAS CLI:
  - To configure the device to function as a branch device, and to configure resource pre-allocation resources for various WAAS services to be branch traffic scenario and branch services, run the **device mode application-accelerator profile branch** global configuration command.

Step 5 Restart the system.

When you restart the system using the Cisco WAAS Central Manager, the HTTP object cache is enabled on the device.

Step 6 Enable Akamai Connect.

For WAVE models 7541 and 8541, the **Device Profile** feature is automatically set/unset when you enable/disable HTTP OC. For WAVE-7571, the **Device Profile** setting requires you to reboot to change the **Device Profile** feature status.

Downgrading and Upgrading a Cisco vWAAS Device with Additional Akamai Cache Disk Removed and Reinstalled

Procedure

Step 1 For the Cisco vWAAS device in Cisco WAAS Version 6.2.x with Akamai Connect enabled:

a) From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, and then choose **Configure** > **Caching** > **Akamai Connect**.
b) To disable Akamai Connect, uncheck the **Enable Akamai Connect** check box.
c) Power down the Cisco vWAAS device.

Step 2 Remove the additional Akamai Cache disk.

Step 3 Power on the Cisco vWAAS device.

Step 4 Downgrade from Cisco WAAS Version 6.2.x to Cisco WAAS Version 5.x.

Step 5 Upgrade the Cisco WAAS Central Manager and Cisco WAE devices to Cisco WAAS Version 6.2.x.

Step 6 After the upgrade is complete, power off the device.

Step 7 Reinstall the additional Akamai Cache disk.

Step 8 Power on the Cisco vWAAS device.

Step 9 Enable Akamai Connect.

a) From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.
b) To enable Akamai Connect, check the **Enable Akamai Connect** check box.
c) Click **Submit**.

Step 10 Enable HTTP object cache from the Cisco WAAS Central Manager or from the Cisco WAAS CLI.

Consider the following guidelines for enabling HTTP object cache:

- A message is displayed regarding the required additional memory and disk resources. For resource guidelines, see the "Cisco WAAS with Akamai Connect Requirements for HTTP Object Cache" table.
- For information on enabling HTTP object cache for Cisco WAVE devices, see Configuring HTTP Object Cache.
- For information on enabling HTTP object cache for Cisco vWAAS devices, see Configuring HTTP Object Cache in Cisco Devices with Akamai Connect.

Step 11 Power down the Cisco vWAAS device and add the necessary resources to the Cisco vWAAS device.

Step 12 Power up the Cisco vWAAS VM.

HTTP object cache is enabled on the Cisco vWAAS device.

Downgrading and Upgrading a Cisco vWAAS Device with Additional Akamai Cache Disk Remaining In Place

Procedure

Step 1 Upgrade the Cisco WAAS Central Manager and Cisco WAE devices to Cisco WAAS Version 6.2.1 or later.

Step 2 Disable Akamai Connect.

a) From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, and then choose **Configure** > **Caching** > **Akamai Connect**.

   The **Akamai Connect** window appears, with the **Cache Settings** tab displayed.

b) To disable Akamai Connect, uncheck the **Enable Akamai Connect** check box.
c) Power down the Cisco vWAAS device.

Step 3 Downgrade from Cisco WAAS Version 6.2.x to Cisco WAAS Version 5.x.

Step 4 Upgrade the Cisco WAAS Central Manager and Cisco WAE devices to Cisco WAAS Version 6.2.x.

Step 5 Run the **disk delete-data-partitions** EXEC command and restart the system.

a) From the Cisco WAAS CLI, a message is displayed to run the **disk delete-data-partitions** EXEC command and restart the system.

   The Cisco WAAS Central Manager does not display this message.

b) After the upgrade, you must run the disk delete-data-partitions command to enable Akamai Connect.

Note The **disk delete-data-partitions** EXEC command deletes all data partitions on all logical drives, including CONTENT, PRINTSPOOL, and SYSFS partitions. These partitions include all DRE and SMB object cache files, SYSFS and print spool files. New partitions are created at system restart.

Step 6 Enable Akamai Connect.

a) From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.

The Akamai Connect window appears, with the **Cache Settings** tab displayed ().

b) To enable Akamai Connect, check the **Enable Akamai Connect** check box.

c) Click **Submit**.

Workflow for Enabling and Using Cisco WAAS with Akamai Connect

The following table shows the workflow for enabling and using Cisco WAAS with Akamai Connect.

Table 57: Workflow for Enabling and Using Cisco WAAS with Akamai Connect

Task	Description and Links to Associated Tasks
1. Receive and activate the Akamai Connect license.	• Activating and Managing the Akamai Connect License, on page 480 • About the Akamai Connect License, on page 480 • Prerequisites for Activating the Akamai License, on page 480 • Activating the Akamai Connect License File, on page 481
2. Enable Akamai Connect.	• Enabling Akamai Connect, on page 484 • Confirming Akamai Connect Configuration Prerequisites, on page 484 • Turning on the Akamai Cache Engine and Enabling Akamai Connect, on page 485
3. Enable Akamai Connected Cache.	• Enabling Akamai Connected Cache, on page 486 • About Akamai Connected Cache, on page 486 • Procedure for Enabling Akamai Connected Cache, on page 486

Task	Description and Links to Associated Tasks
4. Enable Over the Top (OTT) caching.	• Enabling Over the Top (OTT) Caching, on page 487 • About OTT Caching, on page 487 • Procedure for Enabling OTT Caching, on page 488
5. Set transparent caching policies.	• Setting Transparent Caching Policies, on page 489 • Transparent Caching and Caching Modes, on page 489 • Setting a Transparent Caching Policy for All Sites, on page 491 • Setting a Transparent Caching Policy for a Specific Site, on page 492
6. Enable Cisco Cloud Web Security (CWS).	• Enabling Cisco Cloud Web Security (Cisco CWS), on page 493 • About Cisco CWS, on page 493 • Procedure for Enabling Cisco CWS, on page 494
7. Configure Cisco WAAS connections to the Akamai network.	• Configuring Cisco WAAS Connections to the Akamai Network, on page 494 • About Cisco WAAS Connections to the Akamai Network, on page 494 • Configuring No HTTP Proxy, on page 495 • Configuring the Cisco WAAS Central Manager as HTTP Proxy, on page 496 • Configuring External HTTP Proxy, on page 497
8. Configure Server Address Validation.	• Configuring Server Address Validation, on page 498 • About Server Address Validation, on page 498 • Alarms Used with Server Address Validation, on page 499 • Configuring Server Address Validation, on page 498
9. Configure Akamai Connect cache prepositioning.	• Configuring Akamai Connect Cache Prepositioning, on page 501 • Configuring a Cache Prepositioning Task, on page 501 • Viewing Cache Prepositioning Task Status, on page 504 • Copying Cache Prepositioning Tasks, on page 505

Task	Description and Links to Associated Tasks
10. Configure Akamai Connect HTTP/S preposition proxy.	• Configuring HTTP/S Preposition Proxy for Akamai Connect, on page 506 • About HTTP/S Preposition Proxy for Akamai Connect, on page 506 • Configuring Global Proxy Host and Port for Preposition Tasks, on page 506 • Modifying Proxy Settings for an Individual Prepositioning Task, on page 507 • Removing Proxy Settings for an Individual Prepositioning Task, on page 507

Activating and Managing the Akamai Connect License

This section contains the following topics:

About the Akamai Connect License

The Akamai Connect license for Cisco WAAS is an advanced license available for all supported Cisco with Akamai Connect devices. The Akamai Connect license for Cisco WAAS is aligned with the number of optimized connections in each supported Cisco WAAS device.

Prerequisites for Activating the Akamai License

Before you upload a new Akamai license or before you enable Akamai Connect on Cisco WAAS and activate the Akamai Connect License file, consider these guidelines:

1. Before you upload a new Akamai license, collect or confirm the following Akamai License Customer ID information:

    - The new license activation file to be uploaded.
    - A customer ID snapshot from the Cisco WAAS Central Manager Akamai Diagnostics: Choose **Home** > **Monitor** > **Troubleshoot** > **Akamai Diagnostics** > **Akamai Connect License** > **Details**.
    - To capture the hostname and Akamai ID, copy the list of some devices, as either a snapshot or an Excel spreadsheet: Choose **Home** > **Monitor** > **Troubleshoot** > **Akamai Diagnostics** > **Akamai Connect License** > **Details** > **Test**.
    - Open a service request with this information so that Cisco TAC can assist you further. For further information on contacting TAC, see the Cisco Support and Downloads page, Contacts/Support Cases section.

2. Before you enable Akamai Connect on Cisco WAAS and activate the Akamai Connect License file, complete the following prerequisites:

- Confirm the readiness of your Cisco WAAS configuration, as described in the first bulleted text of this section.
- For information on the status of an active Akamai Connect license, see Akamai Connect Diagnostics Using the Cisco WAAS Central Manager in the chapter "Troubleshooting Your Cisco WAAS Network."

Activating the Akamai Connect License File

Procedure

Step 1 Enable Akamai Connect, as described in Workflow for Enabling and Using Cisco WAAS with Akamai Connect.

If this is the first time you are enabling Akamai Connect, you are prompted to provide the activation file for licensing.

Step 2 If you have not yet done so, purchase an Akamai Connect license from your Cisco account representative or reseller. The following actions are generated by this purchase:

- The account representative or reseller enters the order into the Cisco Commerce Workspace (CCW) system. The order *must* specify an email address for eDelivery of the Activation file.
- CCW contacts the Akamai Luna Portal to request a license or licenses for the number and type of Akamai licenses entered.
- Akamai generates and sends the license(s) to the CCW system in the form of a single activation file.
- The CCW system sends an email, with the activation file attached, to the email address specified in the order. The order of priority for selecting the email address in a CCW order is:
  - **Priority1**: eDelivery email address
  - **Priority2**: end customer email address
  - **Priority3**: shipping contact email address

  Note If you do not provide an email address in your order, you will not receive an activation file.

Step 3 To upload the **Akamai Connect License file**, choose **Home > Admin > Licenses > Akamai Connect**.

The **Upload Akamai Connect License** file window is displayed.

Step 4 Use to the **Browse** button to highlight and select the activation file, and click **Upload**.

- The authentication data in the activation file is transmitted to the Akamai Luna portal.
- After the device message is sent to the Akamai Luna portal, the Akamai Luna portal sends the Entitlement Code to the Cisco WAAS Central Manager and the Akamai Management Gateway (AMG). The Cisco WAAS Central Manager sends the Entitlement Code to Cisco WAAS, and the AMG rolls out the Entitlement Code to the edge servers on the Akamai Grid Network.

Each of these steps happens automatically, but each takes some time to complete.

- The Entitlement Code is maintained on the Akamai Luna portal, on the AMG, and on the Cisco WAAS device. Cisco WAAS connects to the AMG using a proxy/DNS server that can resolve the address **amg.terra.akamai.com**.

Step 5 The activation process begins.

The **Status of Devices with Akamai Connect Feature Configured** table listing displays the following types of status for one, some, or all devices. The Table 58: Status Indicator States for Device, Operational, and Connectivity Status table shows the states through which the indicators proceed: **Akamai Device Status**, **Operational Status**, and **Connectivity to Akamai**.

Table 58: Status Indicator States for Device, Operational, and Connectivity Status

Status Category	First Status	Second Status	Third Status	Fourth Status
Akamai Device Status	ActivationInProgress	ActivationInProgress	Active	Active
Operational Status	Disconnected	Connected	Connected	Connected
Connectivity to Akamai	Activating	Activating	Activated	Connected

Note The activation process for WAAS devices may take between 15-60 minutes to complete, and for this time period, the **Connectivity to Akamai** status displays as **Activating**. During this time, device(s) may not be able to communicate with the Akamai Network, because they are not recognized by the AMG until the activation process is complete, and the **Connectivity to Akamai** status displays as **Connected**.

Step 6 For the final steps in the registration process:

- Akamai Luna sends the Akamai Connected Cache credentials to the AMG and to the Akamai edge servers on the Akamai Grid network. The AMG forwards the Akamai Connected Cache credentials on to Cisco WAAS.
- With the Akamai Connected Cache credentials on both Cisco WAAS and the Akamai edge servers, the Akamai Connected Cache is enabled, and caching requests can be served by the Akamai edge servers. This authenticated connection can then service requests for Akamai Connected Cache and OTT caching from the Akamai Grid network Akamai edge servers.
- The registration of each Cisco WAE begins. The Cisco WAAS Central Manager provides information to the Akamai Luna Portal for each Cisco WAAS device that will be running Akamai Connect.

  Note The **Connected** Operational Status can take several minutes to complete. Rollout of the activation to the Akamai edge servers can take up to 45 minutes to complete. A device may take from a few minutes to up to two hours to show an **Active** Activation Status, depending on when the request was made, traffic conditions, and other variables.

Step 7 Each Cisco WAE that has been sent the entitlement code will try to make an SSL connection to the AMG using **amg.terra.akamai.com**. The Akamai Luna Portal will push out the Akamai Connected Cache credentials to the AMG and to the Akamai Grid Network (to the Akamai edge servers).

- The AMG will push the Akamai Connected Cache credentials out to each of the Cisco WAEs that are configured for Akamai Connected Cache. If OTT is enabled, the OTT metadata needed to help cache YouTube objects is also processed at this time.
- The Akamai Connected Cache credentials are sent by the Cisco WAE cache engine when going to the origin server. If the Cisco WAE cache engine has valid credentials according to the Akamai edge server, the Akamai edge server then provides objects to the Cisco WAE cache engine that are not normally cacheable to other devices.

Step 8 The Cisco WAE cache engine will request new credentials daily and will be good for two days. The connections are always established from the Cisco WAE or Cisco WAAS Central Manager over TCP 443 to the AMG.

- For security, firewalls are usually deployed by performing statefull inspection on traffic from within the company to the outside. They are also configured to block unknown traffic from the outside to the inside.

  Because connection should not initiate from AMG to any Cisco WAAS Central Manager or Cisco WAE at any time, there should not be an issue. If there is, then a hole will need to be made to allow the Cisco WAAS Central Manager or Cisco WAE to communicate with any device on port 443.
- The Devices listing on the All Devices window includes a column titled Akamai Connect, which shows the status of each device: **Active**, **Not Supported**, **Connected**, or **Disconnected**.

Step 9 As needed, configure HTTP proxy or external HTTP proxy, described in Configuring Cisco WAAS Connections to the Akamai Network.

Deregistering and Reregistering a Cisco WAAS Device

This section provides an overview of how to deregister and reregister a Cisco WAAS device. For more information, see Changing Device Mode in the chapter "Planning Your Cisco WAAS Network."

- To change the device mode of a Cisco WAAS device that is already registered with a Cisco WAAS Central Manager, you must perform the following tasks:
  1. Deregister the Cisco WAAS device from the Cisco WAAS Central Manager.
  2. Change the device mode of the Cisco WAAS device.
  3. Reload the Cisco WAAS device.
  4. Re-enable CMS services for the Cisco WAAS device.
- When you deregister a Cisco WAAS device from the Cisco WAAS Central Manager:
  - The Cisco WAAS Central Manager triggers the removal of the device record on the Akamai side, thereby invalidating the entitlement key used by the Cisco WAE cache engine to talk to AMG devices.
  - On the Cisco WAAS side, the Cisco WAE cache engine will continue to operate in **Transparent** caching mode.
- When you reregister a Cisco WAAS device with the Cisco WAAS Central Manager, one of two things happen:

- The Cisco WAAS Central Manager auto-assigns the Cisco WAAS device to device groups (that are so marked). If any of these device groups have Akamai Connect and HTTP cache settings, the Cisco WAAS Central Manager will trigger registration with Akamai.
- If no device group is configured with Akamai Connect and HTTP cache settings, the registration is done individually.
- After the Cisco WAAS device is registered, it will get a new entitlement key.

Replacing an Inactive or Expired Akamai Connect License

Procedure

Step 1 When a license is inactive or expired, a notification is displayed in one of these Cisco WAAS Central Manager windows:

- The following notification is displayed in the **Home** > **Admin** > **Akamai Connect** window: **Akamai Connect License is Inactive. Please remove current license and import valid license.**
- The following notification is displayed in the **Home** > **Monitor** > **Troubleshoot** > **Akamai Diagnostics** window: **Akamai Connect License is Inactive. Please remove existing license and import new one using Akamai License page.**

Step 2 Remove the inactive or expired license.

Step 3 To upload a new license file, choose **Home** > **Admin** > **Licenses** > **Akamai Connect**.

Step 4 The **Akamai Connect** window is displayed.

Step 5 Click **Choose File** and browse to the new license file, and then click **Upload**.

If you try to import an expired license, you will see the message: **Unable to communicate to Akamai server (Error: License is inactive or expired). See Central Manager log file for detailed error information.**

Step 6 To obtain a new license, contact your Cisco account representative or reseller.

Enabling Akamai Connect

This section contains the following topics:

Confirming Akamai Connect Configuration Prerequisites

Before you enable Akamai Connect, confirm that your Cisco WAAS configuration has the following Akamai Connect prerequisites:

- **Cisco WAAS Version**: The Cisco WAAS Central Manager and Cisco WAAS appliances are running at Cisco WAAS Version 5.4.1 or later.

- **NTP Service**: A verified Network Time Protocol (NTP) service that is within 30 seconds of the NTP standard server (NTP.org). For more information, see Configuring NTP Settings, on page 302 in the chapter "Configuring Other System Settings."
- **DNS Server**: A working public Domain Name System (DNS) server configured on the Cisco WAAS devices and the Cisco WAAS Central Manager. For more information, see Configuring the DNS Server in the chapter "Configuring Network Settings."
- **Akamai Luna system and Akamai Management Gateway**: The ability for the Cisco WAAS Central Manager to reach Akamai's Luna system via HTTPS on port 443. (The custom hostname is in your activation file.)

  The ability for Cisco WAAS devices to make a connection to the Akamai Management Gateway (AMG) to get the authentication key. The Cisco WAAS device configured for Akamai Connect needs the correct network connectivity to access the AMG every day to get correct credentials and updated metadata. Cisco WAAS will make an HTTPS connection on port 443 to the AMG to get this information.

  Note The Akamai Connected Cache feature will stop functioning if Cisco WAAS loses communication with the AMG for more than 48 hours.

  If the Cisco WAAS devices cannot go directly to the Internet, you can configure them to use the Cisco WAAS Central Manager as a proxy. For more information, see Configuring the Cisco WAAS Central Manager as HTTP Proxy, on page 496.

Turning on the Akamai Cache Engine and Enabling Akamai Connect

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.

The Akamai Connect window appears, with the **Cache Settings** tab displayed.

Note If you are configuring the Akamai Connect feature for a device group, the device group should have only devices that support Akamai Connect. For more information, see Supported Platforms for Cisco WAAS with Akamai Connect.

Step 2 To turn on the Akamai cache engine, check the **Enable Akamai Connect** check box.

The **End-User License Agreement - Akamai Connect** dialog box appears.

Step 3 Click **Accept**.

- When you create settings for the first time, either at the device or the group level, the **Akamai Connect Upload File** drop-down list is displayed. Choose the Akamai Connect license file and click **Submit**. For more information, see Activating and Managing the Akamai Connect License, on page 480.
- If you have not yet purchased an Akamai Connect license, see Activating and Managing the Akamai Connect License, on page 480.

Step 4 From the **Choose File** drop-down box, choose your Akamai Connect license file.

Step 5 Click **Submit** or proceed to Enabling Akamai Connected Cache.

Enabling Akamai Connected Cache

This section contains the following topics:

About Akamai Connected Cache

Akamai's proprietary caching rules in connection with the edge servers of the Akamai Intelligent Platform lets you cache and deliver content inside the branch office that might otherwise be deemed noncacheable. This content could be an enterprise's own web content, content that is served by the worldwide Akamai Content Delivery Network (Akamai CDN), or any content that is delivered by the Akamai Intelligent Platform, which is up to 30 percent of all web traffic.

Akamai Connected Cache contains the following features:

- Akamai Connected Cache is automatically enabled in Cisco WAAS when you enable Akamai Connect. You then specify the sites to be accelerated.
- Object caching is done on the client-side Cisco WAAS device only.
- Prepositioning can be leveraged to cache HTTP websites delivered via the Akamai Intelligent Platform.
- The Cisco WAAS/Akamai cache engine determines which sites can be "Akamaized" by Akamai Connected Cache from the HTTP headers in the first reply. The cache engine and the Akamai edge server then exchange credentials and agree that Akamai Connected Cache can occur. This is done again via HTTP headers in HTTP request and responses.
- During the enabling and registration of HTTP object cache, each Cisco WAE cache engine contacts the Akamai network to obtain credentials.

  After registration is complete, and Akamai Connected Cache is turned on, DNS requests are routed through the Akamai DNS system, and content is served up from an edge server to the Cisco WAAS router whenever it is possible.
- The Akamai edge server provides additional headers to allow the WAAS/Akamai cache engine to cache the objects for the objects it handles. The cache engine forwards this back to the corresponding client. The headers passed between the cache engine and the client are similar to what the client or enterprise proxy server would see if the Cisco WAE was not in the path.

Procedure for Enabling Akamai Connected Cache

Before you begin

For Akamai Connected Cache to function properly, you must have the following parameters configured:

- **Access to public DNS server**: For more information, see Configuring the DNS Server in the chapter "Configuring Network Settings."

- **NTP services**: For more information, see Configuring Date and Time Settings in the chapter "Configuring Other System Settings."

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure > Caching > Akamai Connect**.

The **Akamai Connect** window appears, with the **Cache Settings** tab displayed.

Step 2 At the **Edit Settings** pane, check the **Akamai Connected Cache** check box. The default is **Enabled**.

Consider the following configuration guidelines for Akamai Connected Cache:

- When Akamai Connected Cache is enabled, it is enabled for all suitable Akamaized content.
- You can apply Akamai Connected Cache to a specified device, or to all registered devices:
  - To apply Akamai Connected Cache to all registered Cisco WAAS devices, configure Akamai Connected Cache at the device group level.
  - To apply Akamai Connected Cache to a specific registered Cisco WAAS device, configure Akamai Connected Cache at the device level.
- After you enable Akamai Connected Cache, you can perform the following tasks:
  - Set a caching policy for all sites, as described in Setting a Transparent Caching Policy for All Sites, on page 491.
  - Set an individual caching policy for a specific site, as described Setting a Transparent Caching Policy for a Specific Site, on page 492.
  - Enable Over the Top (OTT) caching, as described in Enabling Over the Top (OTT) Caching, on page 487.
  - Configure cache prepositioning, as described in Configuring Akamai Connect Cache Prepositioning, on page 501.

Step 3 Click Submit or proceed to Enabling Over the Top (OTT) Caching, on page 487.

Enabling Over the Top (OTT) Caching

This section contains the following topics:

About OTT Caching

Over-The-Top (OTT) caching is used for streamed content, particularly video content. OTT caching caches HTTP content served from dynamic URLs and content marked as noncacheable, such as YouTube videos. Akamai achieves this by using metadata logic to determine a unique cache key per video, which allows dynamic URLs to be cached. The following figure shows an example of OTT caching.

Note OTT caching is disabled by default. You can enable OTT caching after you enable Akamai Connected Cache. For more information, see Enabling Akamai Connected Cache, on page 486.

Sites that support OTT caching include the following:

- Apple
- Google
- Lynda
- Microsoft Updates
- Office 365
- Pearson
- Salesforce
- Schoology
- Vimeo
- Youku
- YouTube

Because YouTube is delivered via HTTPS, you must follow the same process as you do for Software as a Service (SaaS) optimization. The domains that must be matched are ***.youtube.com**, ***.ytimg.com**, ***.googlevideo.com**, and ***.ggpht.com**. For more information, see Configuring SSL Acceleration for SaaS Applications in the chapter "Configuring Application Acceleration."

Procedure for Enabling OTT Caching

Before you begin

Confirm that Akamai Connected Cache is enabled. For more information, see Enabling Akamai Connected Cache.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.

The **Akamai Connect** window appears, with the **Cache Settings** tab displayed.

Step 2 At the **Edit Settings** pane, check the **Over the Top Cache** check box.

Note You must enable Akamai Connected Cache before you enable OTT caching. For more information, see Enabling Akamai Connected Cache.

Step 3 Click **Submit** or proceed to tasks for setting caching policies: Setting a Transparent Caching Policy for All Sites or Setting a Transparent Caching Policy for a Specific Site.

Setting Transparent Caching Policies

This section contains the following topics:

Transparent Caching and Caching Modes

This section contains the following topics:

About Transparent Caching and HTTP Object Cache

Transparent cache is Akamai's high-performance HTTP object cache, which provides the ability to locally cache HTTP-based content for LAN-like performance, whether the web application was served from the private corporate cloud or from the public Internet. This content includes on-demand and live HTTP video streams, to deliver fast, high-quality, high-definition video in the branch, while offloading the enterprise network. Akamai Connect supports the latest generation of streaming protocols including Apple HTTP Live Streaming (HLS), Adobe HTTP Dynamic Streaming (HDS), and Microsoft HTTP Smooth Streaming (HSS). Akamai's HTTP object cache also supports the caching of Apple software updates such as iOS and OS X, and Microsoft Windows Update, further offloading the enterprise network.

Transparent caching delivers content from an origin server to the client without any modification. Transparent caching sends a request from a client to a server along with the associated authentication. No changes are made by proxy servers to either the headers or the returned packets along the way, although there are some headers that mark proxy actions that can be altered without the meaning of the cache control headers being altered.

Note When accessing transparent caching via HTTPS, the default caching mode is Basic mode. This ensures that no sensitive content is accidentally cached (in Basic mode, only content that you explicitly mark is cached). If you want content cached in a different mode with HTTPS, create a host rule that matches the HTTPS server location. For more information on creating a host rule, see Setting a Transparent Caching Policy for All Sites and Setting a Transparent Caching Policy for a Specific Site.

Transparent caching modes are used to set caching policies. For more information, see Transparent Caching Modes, on page 489.

Transparent Caching Modes

There are four types of Transparent caching modes, or policies: Basic, Standard (default), Advanced, and Bypass.

- **Basic Transparent Caching Mode**

  Basic mode is the lowest level of caching, where it strictly complies with the client caching directives in the HTTP header, caching only objects marked explicitly as cacheable. Caching is only in the branch or local router, and content can be cached from the Internet regardless of the location of the original source.

- **Standard Transparent Caching Mode (default)**

  Standard (default) caching mode expands the breadth of caching objects by including objects marked as cacheable, objects that do not have caching directives, and with a last-modified date. For example, with Standard caching, the object will be cached for 10 percent of the current age of the response and then updated.

  Note A correctly configured website will work with Standard mode, but login pages, cookie setting pages, or dynamic content not properly marked as cacheable may break. We recommend that you test the website; this is particularly important for a newly-created website or one that does not have many users.

- **Advanced Transparent Caching mode**

  Advanced caching mode further extends the duration for which the objects without specific age limits are cached, thus allowing an aggressive amount of caching in appropriate situations, and to cache all object types for longer times, when there is no explicit expiration time. Advanced mode is best suited for media-rich Intranet sites.

  If cache-control or expire headers are not present and **Last Modified Time** appears, the cache engine performs a heuristic based on the **Last Modified Time** and stores objects for 20 percent of their apparent age, up to a maximum of one day.

  For certain media file types, listed in the table "Advanced Mode: Media Types That May be Cached for a Full Day," Advanced Mode will cache these for a full day if the media type is not specified as uncacheable or the media type has no obvious age in the request. For all other media types, the system caches the object for a minimum of one hour to a maximum of seven days - regardless of whether the **Last Modified Time** is present.

Table 59: Advanced Mode: Media Types That May be Cached for a Full Day

Media Types That May be Cached for a Full Day, if not specified as uncacheable or with no obvious age in request										
3g2	3gp	aac	aif	aiff	asf	asx	au	avi	bin	bmp
cab	carb	cct	cdf	class	css	dcr	doc	docx	dtd	dv
dvd	dvr	dvr-ms	exe	flv	gcf	gff	gif	grv	hdml	hqx
ico	ini	jpeg	jpg	js	mlv	m4a	midi	mov	mp3	mp4
mpeg	mpg	mpv	nv	pct	pdf	png	ppc	ppt	pptx	pws
qt	swa	swf	tif	txt	vbs	w32	wav	wbmp	wma	wml
wmlc	wmls	wmlsc	wmv	xsd	xsl	xls	xlsx	zip	—	—

Note A correctly configured website will work in Advanced mode, but Advanced mode may break the presentation of certain web pages if there are even minor caching misconfigurations. We recommend that you test the performance of this caching mode for your applications before you bring the cache engine into production. When testing, pay particular attention to dynamic URLs and to content that requires authentication to be presented to a client.

- **Bypass Transparent Caching Mode**

  Bypass mode turns off caching for a configured site or sites. When Bypass mode is set for a particular hostname, the caching for the site's hostname specified in a rule is suppressed.

  Bypass mode is useful when you want to turn off Akamai Connected Cache or OTT caching for a site or for a part of a site. For example, if you have servers of the type **images#.bar.com**, you can configure a bypass rule so that only **images2.bar.com** is excluded from caching. All other **images#.bar.com** servers will continue to be cached under the existing rules.

Order of Preference for Caching Types

Consider the following operating guidelines for order of preference for caching types:

- When there are multiple caching modes and policies in use, the Cache Engine applies an order of precedence in the execution of these. A rule that is higher in the order of precedence is executed first, and any other rules that are applied to that domain or digital property is ignored. The order of preference is:

  1. Transparent caching rules
  2. OTT/Akamai Connected Cache
  3. Default Transparent caching policy

  For example, if **test.com** is an Akamai Connected Cache property, but an Advanced mode cache rule is set for this site, then Advanced mode will take precedence and Akamai Connected Cache will be skipped.

- When cache prepositioning is turned on, it has the same priority as any other caching type.
- Akamai Connect determines cache type based on most exact hostname match followed by cache priorities. For example, **www.host.com** is more exact than ***.host.com**. In this scenario, if a lower-priority cache, such as Akamai Connected Cache (Order of Precedence #2), has a more exact match than a higher priority cache, such as transparent (Order of Precedence #1), the caching will occur with the more exact match and lower-priority cache.

Setting a Transparent Caching Policy for All Sites

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.

The **Akamai Connect window** appears, with the **Cache Settings** tab displayed.

Step 2 At the Advanced Cache Settings pane, from the Default Transparent Caching Policy drop-down list, choose one of the following caching policies as a default transparent caching policy for all sites:

- **Basic**: Caches only objects marked explicitly as cacheable.
- **Standard (default)**: Caches objects marked as cacheable, as well as objects that do not have caching directives or a last-modified date.
- **Advanced**: Further extends the duration for which the objects without specific age limits are cached, thus allowing an aggressive amount of caching in appropriate situations, and to cache all object types for longer times, when there is no explicit expiration time.
- **Bypass**: Turns off caching for a specific configured site or sites.

Considering the following about caching polices:

- Checking the Akamai Connected Cache check box () starts active caching with the default Standard caching policy. To use the Akamai cache engine with a Basic, Advanced, or Bypass caching policy, you must specify that caching policy with the Default Transparent Caching Policy drop-down list.
- To set a caching policy for a specific site, see Setting a Transparent Caching Policy for a Specific Site.
- For more information about caching policies, see Transparent Caching and Caching Modes, on page 489.

Step 3 Click **Submit** or proceed to Setting a Transparent Caching Policy for a Specific Site.

Setting a Transparent Caching Policy for a Specific Site

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.

The **Akamai Connect** window appears, with the **Cache Settings** tab displayed.

Step 2 At the **Advanced Cache Settings** pane, from the **Default Transparent Caching Policy** drop-down list, choose **Bypass**.

Choosing **Bypass** turns off caching, so that you can set a specific caching policy for the site.

Step 3 To add a site to contain a specific caching policy, at the **Site Specific Transparent Caching Policy** table listing, click **Add Hostname/IP**.

The **Site Caching Policy Task** dialog box appears.

Step 4 In the **Site Caching Policy Task** dialog box, in the **Hostname/IP** field, specify the hostname of the site to be configured.

Consider the following guidelines for creating a hostname:

- The hostname can be a specific server, or a domain name that contains a wildcard, such as ***.cisco.com**.

- You can configure up to 512 hostnames for each site-specific caching policy.
- From the **Transparent Caching Policy** drop-down list, select the cache policy for this site: **Basic**, **Standard**, **Advanced**, or **Bypass**.
- Consider the following guidelines for setting a site-specific cache policy:
    - The policy you set for a specific site takes precedence over the default caching policy set for all sites.
    - If you configure **Bypass** mode as the site-specific transparent caching policy, you must specify a complete server name or a complete domain name (a Fully Qualified Domain Name [FQDN]). If you use a wildcard to specify sites for **Bypass** mode, the sites will still be optimized via Akamai Cache.

Step 5 Click **OK**.

The new hostname/IP is added as a line item to the **Site Specific Transparent Caching Policy** table.

- To edit an existing site, highlight the site listing and click **Edit**.
- To delete an existing site, highlight the site listing and click **Delete**.

Step 6 Click **Submit** or proceed to Enabling Cisco Cloud Web Security (Cisco CWS).

Enabling Cisco Cloud Web Security (Cisco CWS)

This section contains the following topics:

About Cisco CWS

Cisco Cloud Web Security (CWS) provides content scanning of HTTP and HTTP/S traffic, and provides malware protection service to web traffic. CWS enforces content filtering by enabling force IMS for every cached object, for both single-sided and dual-sided deployment.

CWS servers scan web traffic content and either allow or block the traffic based on configured policies. Servers use credentials to identify and authenticate users and redirect the traffic for content scanning. Traffic is transparently proxied by Cisco routers to cloud-based CWS servers, where the web traffic is scanned and, if deemed acceptable, is provided to the origin server. All traffic coming back is through the CWS server.

Cisco CWS Operating Guidelines

Consider the following operating guidelines for Cisco CWS:

- Cisco CWS version interoperability:
    - For Cisco WAAS Version 6.2.1 and later, the CWS feature enforces content filtering by enabling force IMS for every cached object, for both single-sided and dual-sided deployment.
    - For Cisco WAAS Versions earlier than 6.2.1, content filtering is enforced on single-sided deployments.

- CWS can be used only when one Cisco WAAS device is present in the path.
- If preposition is enabled, the traffic flow may be redirected to a CWS server, follow these recommendations:
    - (Preferred choice): Configure a white list on the Cisco ISR or the Cisco CWS server to bypass the Cisco WAE IP address.
    - On the Cisco CWS server, configure a user or group that the Cisco WAE will fall into for authentication and allow it access to all sites on which the preposition is occurring.

Procedure for Enabling Cisco CWS

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.

The **Akamai Connect** window appears, with the Cache Settings tab displayed.

Step 2 At the **Advanced Cache Settings** pane, to enable Cisco CWS:

To enable CWS user policy enforcement for content access with Direct Internet Access (DIA), check the **Force IMS DIA** check box.

To apply CWS user policy enforcement for content access with all flows, check the **Force IMS Always** check box.

Step 3 Click **Submit**, or proceed to Configuring Cisco WAAS Connections to the Akamai Network, on page 494.

Configuring Cisco WAAS Connections to the Akamai Network

This section contains the following topics:

About Cisco WAAS Connections to the Akamai Network

This section provides an overview of the three ways for Cisco WAAS devices to connect to the Akamai network.

- Configure no HTTP proxy.
- Configure the Cisco WAAS Central Manager as HTTP proxy.
- Configure an external HTTP proxy.

When using Akamai Connect, the Cisco WAAS Central Manager and Cisco WAAS device(s) must be able to communicate with the Akamai Network: with the Akamai Luna API servers to provision entries for Cisco WAAS devices, and with the Akamai AMG devices for Akamai Connected Cache and OTT features.

However, some Cisco WAAS deployments may disallow outgoing connections to the Internet for the Cisco WAAS Central Manager or Cisco WAAS device(s). For these deployments, the Cisco WAAS device(s) may use an HTTP proxy to contact the Akamai Network.

Note HTTP proxy must support **HTTP CONNECT** for tunneling HTTPS connections.

The following table shows the available connection configurations.

Table 60: Connection Configurations for Cisco WAAS to Akamai Network

Connection Configuration	Configuration Connections	Cisco WAAS Central Manager to Luna API Servers	Cisco WAAS HTTP Cache Engine to Akamai AMG
No HTTP proxy use	Direct/ Direct	Direct	Direct
Cisco WAAS Central Manager as HTTP proxy	Direct/ Cisco WAAS Central Manager as proxy	Direct	Cisco WAAS Central Manager as HTTP proxy
External HTTP proxy	Direct/ External HTTP proxy	Direct	External HTTP proxy
External HTTP proxy	External HTTP proxy/ Direct	External HTTP proxy	Direct
External HTTP proxy	External HTTP proxy/ External HTTP proxy	External HTTP proxy	External HTTP proxy

The following considerations apply to all HTTP proxy deployments:

- You configure HTTP proxy from the Cisco WAAS Central Manager; there are no CLI commands for HTTP proxy. Configuring HTTP proxy settings does not require restart of the WAAS Central Manager.
- HTTP Proxy must support HTTP Connect method for tunneling HTTPS connections.
- Configuring the HTTP proxy setting does not require restart of the Cisco WAAS Central Manager.

Note Cisco WAAS v5.5.1 does not support HTTP proxy user authentication. We recommend that you restrict access to proxy using IP address ACLs.

Configuring No HTTP Proxy

Procedure

To configure a direct connection from the Cisco WAAS Central Manager and Cisco WAAS devices to the Akamai network: From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.

The Akamai Connect window appears, with the **Cache Settings** tab displayed.

a) At the **Advanced Cache Settings** pane, confirm that the **Use HTTP proxy for connections to Akamai network** check box is unchecked.

a) Click **Submit**.

Configuring the Cisco WAAS Central Manager as HTTP Proxy

This section contains the following topics:

Operating Guidelines for Cisco WAAS Central Manager as HTTP Proxy

Consider the following operating guidelines when using the Cisco WAAS Central Manager as an HTTP proxy to the Akamai network:

- When using Akamai Connected Cache, each Cisco WAAS cache engine device is communicating with the Akamai network. Some Cisco WAAS deployments may disallow WAE devices to establish outgoing connections to the Internet (i.e., private networks). In this case, the WAE device may use the Cisco WAAS Central Manager device(s) as proxy for all connections to the Akamai network.
- You may still have to allow a hole for the Cisco WAAS Central Manager to make communications on TCP port 443 outbound.
- There is no option for the Cisco WAAS Central Manager to use a proxy device to get to the Internet.
- All connections are made from the Cisco WAAS cache engine device or Cisco WAAS Central Manager out to the Akamai network; never from the Akamai network to the Cisco WAAS cache engine device or Cisco WAAS Central Manager.
- You configure this feature from the Cisco WAAS Central Manager only, not from the Cisco WAAS CLI.

Procedure for Configuring the Cisco WAAS Central Manager as HTTP Proxy

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure > Caching > Akamai Connect**.

The **Akamai Connect** window appears, with the **Cache Settings** tab displayed.

Step 2 At the **Advanced Cache Settings** pane, check the **Use HTTP proxy for connections to Akamai network** check box.

Step 3 From the **HTTP Proxy**: drop-down list, choose **Central Manager as HTTP Proxy**.

Step 4 Click **Submit**.

Configuring External HTTP Proxy

This section contains the following topics:

About External HTTP Proxy

When using Akamai Connect, some Cisco WAAS deployments may disallow outgoing connections to the Internet for the Cisco WAAS Central Manager or Cisco WAAS device(s). For these deployments, the Cisco WAAS device(s) may use an HTTP proxy to contact the Akamai Network.

Configuring External HTTP Proxy for a Device or Device Group

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure > Caching > Akamai Connect**.

The **Akamai Connect** window appears, with the **Cache Settings** tab displayed.

Step 2 Check the **Use HTTP proxy for connections to Akamai network** check box.

Step 3 At the **Advanced Cache Settings** pane, from the **HTTP Proxy**: drop-down list, choose **External HTTP Proxy**.

Step 4 Specify a **Proxy Host** and a **Proxy Port**:

Proxy Host field: Enter a hostname or IP address.

Proxy Port field: Enter a value between **1** to **65535**.

If the Cisco WAAS Central Manager is already using an external HTTP proxy, there is no option displayed to use the Cisco WAAS Central Manager as proxy; these fields will display the currently configured HTTP proxy.

Step 5 Click **Submit**.

Configuring External HTTP Proxy for All Devices

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure > Global > External HTTP Proxy**.

The following message is displayed:

Some deployments may disallow direct connections from Central Manager to Internet hosts. This would affect WAAS features such as Akamai Connect, where Central Manager needs to communicate with Akamai servers. For such deployments WAAS Central Manager may use an external HTTP proxy to contact Internet. HTTP proxy must support HTTP CONNECT method for tunneling HTTPS connections.

Step 2 Specify a **Proxy Host** and a **Proxy Port**:

Proxy Host field: Enter a hostname or IP address.

Proxy Port field: Enter a value between **1** to **65535**.

If the Cisco WAAS Central Manager is already using an external HTTP proxy, there is no option displayed to use the Cisco WAAS Central Manager as proxy; these fields will display the currently configured HTTP proxy.

Step 3 Click **Submit**.

Configuring Server Address Validation

This section contains the following topics:

About Server Address Validation

Server Address Validation prevents malicious content from infecting the Akamai Connect cache, by performing Domain Name Service (DNS) lookups on the name in the HTTP host header, comparing the lookup result with that connection's forward IP address, and, if there is a mismatch, the transaction is allowed to pass through the cache, but no content is allowed to be cached.

Server Address Validation is available for Cisco WAAS Version 6.4.1 and later.

Example:

1. The server IP address to which a DNS name resolves might be an IP address of a server that contains malicious content, rather than that of an expected and trusted server.
2. The resulting response would get cached, and the Akamai cache would then contain malicious content.
3. After the cache is "poisoned" with this malicious content, other clients accessing the same content would also get served with this malicious data.

To prevent such situations, Server Address Validation provides the following features:

- Performs DNS lookups on the name in the HTTP host header.

  A valid Domain Name System (DNS) configuration is required for Server Address Validation to work properly. For more information, see Configuring the DNS Server in the chapter "Configuring Network Settings."

- Compares the lookup result with that connection's forward IP address.
- If there is a mismatch, the transaction is allowed to pass through the cache, however, no content is allowed to be cached.

Note The Cisco Cloud Web Security (Cisco CWS) feature also performs traffic scanning and malware protection for the Akamai Connect cache. For more information on Cisco CWS, see Enabling Cisco Cloud Web Security (Cisco CWS).

Alarms Used with Server Address Validation

The following table shows the alarms used with Server Address Validation.

Table 61: Alarms Used with Akamai Connect Cache Server IP Address Validation

Alarm Name	Reason Alarm is Raised	User Action
DNS Lookup Failed	Too frequently, address checks have been unable to look up hostnames.	Verify that the DNS configured in Cisco WAAS is able to do host lookup.
Forward Proxy Detected Warning	Address checks are enabled, but a forward proxy that is re-looking up hostnames has been detected.	Do one of the following: • Disable address checks. • Disable the forward proxy from re-looking up hostnames. • Disable address checks for the forward proxies' IP addresses. • Add forward proxies' IP addresses to the whitelist.
Address Check Failures Warning	Server address validation has found that too many address mismatches, the IP address returned by DNS lookup does not contain the address used by the client, are occurring.	Use the **show hosts** EXEC command to list and verify the name servers and their corresponding IP addresses, and to list the hostnames, their corresponding IP addresses, and their corresponding aliases (if applicable).

Procedure for Configuring Server Address Validation

Before you begin

This section describes how to use the Cisco WAAS Central Manager to enable or disable Server Address Validation, and to add, edit, or delete bypass server addresses into or from a whitelist.

Before you configure Server Address Validation, consider these guidelines:

- A valid Domain Name System (DNS) configuration is required for Server Address Validation to work properly. For more information, see Configuring the DNS Server in the chapter "Configuring Network Settings."
- If Interposer-SSL is disabled, the following warning message is displayed:

  Interposer-SSL is in disabled state. Enable Interposer-SSL for HTTP Object Cache Server Validation feature to use SNI extension. Peformance for HTTPS connections, when this feature is enabled, might get affected in the absence of SNI.

  For more information, see Enabling and Disabling Global Optimization Features in the chapter "Configuring Application Acceleration."

- To configure Server Address Validation with the Cisco WAAS CLI, run the **accelerator http object-cache validate-address enable** and **accelerator http object-cache validate-address bypass** global configuration commands. For more information, see the *Cisco Wide Area Application Services Command Reference*.

Procedure

Step 1 To enable or disable Server Address Validation:

a) From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.

The **Akamai Connect** window appears, with the **Cache Settings** tab displayed.

b) At the **Server Address Validation** pane, check the **Enable server address validation** check box. The default is disabled.

Consider the following operating guidelines for enabling or disabling Server Address Validation:

- If Server Address Validation is enabled or disabled at the device group level, the option is enabled or disabled to all devices in the device group.
- If you have enabled or disabled Server Address Validation from the Cisco WAAS CLI, it will be reflected in the Cisco WAAS Central Manager within two data feed cycles.

Step 2 To create a server address whitelist:

a) At the **Bypass Server Address** table listing taskbar, click **Add Server IP Address**.

The **Bypass Server** dialog box appears.

b) In the **Bypass Server IP** field, specify the server IP address.
c) In the **Netmask** field, specify the netmask.
d) Click **OK**.

The new server IP address and netmask are added to the **Bypass Server Address** table listing.

- You can configure up to 50 server IP addresses per whitelist.
- To edit an existing bypass server address, highlight the bypass server address and click **Edit**.
- To delete an existing bypass server address, highlight the bypass server address and click **Delete**.

Note A server address whitelist that you have created is stored on the data server until you delete it. The server IP address whitelist is *not* automatically deleted if you disable Server Address Validation.

Upgrade and Downgrade Considerations for Server Address Validation

- Downgrading to a Cisco WAAS version earlier than WAAS Version 6.4.1: Server Address Validation is not available for Cisco WAAS versions earlier than 6.4.1.
- Upgrading from Cisco WAAS Version 6.4.1 to a later version: Server Address Validation is available for all Cisco WAAS versions 6.4.1 and later.

Configuring Akamai Connect Cache Prepositioning

This section contains the following topics:

About Akamai Connect Cache Prepositioning

Cache prepositioning, also known as cache warming, allows you to specify a policy to prefetch and cache content at a specified time. Cache prepositioning allows you to take advantage of idle time on the WAN to transfer large or frequently accessed files to selected Cisco WAAS devices, so that users can benefit from cache-level performance even during first-time access of these files.

Cache prepositioning fetches content based on:

- Predefined schedule
- URL and link depth level
- Excluded content types

Cache prepositioning runs at the same priority as other caching types, for example, Akamai Connected Cache or OTT.

For Cisco WAAS Version 6.2.1 and later with Akamai Connect, cache prepositioning for Akamai Connect also provides the following cache prepositioning features:

- Processing of manifest files for the video streaming protocols HLS (HTTP Live Streaming) and HDS (HTTP Dynamic Streaming).
- Prepositioning of JNLP (Java Network Launch Protocol) files, which contain URL reference for Java Web Start.

Operating Guidelines for Akamai Connect Cache Prepositioning

Consider the following operating guidelines for cache prepositioning for Akamai Connect:

- When a scheduled fetch operation begins or is complete, it is added to the Cache Preposition Status table.
- In order for HTTP/S content to be prepositioned, you must define an SSL accelerated service; otherwise, any HTTP requests encountered in the job will fail, although the preposition task will continue and any objects available via HTTP will be retrieved.

  For more information on how to define an SSL accelerated service, see Configuring SSL Acceleration, on page 407 in the chapter "Configuring Application Acceleration."

Configuring a Cache Prepositioning Task

Before you begin

The following table shows the dialog boxes, available from the **Cache Prepositioning** tab, used to configure a preposition task.

Table 62: Cache Prepositioning Dialog Boxes

Dialog Box	Description
Cache Prepositioning Task	Used to specify the preposition task name, base URLs for prepositioning, include and exclude types, download rate, recursion depth, and task duration.
Cache Prepositioning Task, Advanced Settings	Used to specify the recursion delay time and recursion domains.
Cache Prepositioning Schedule	Used to specify the schedule name for the preposition task, frequency of the task (such as daily or monthly), and start time.

Procedure

Step 1 From **Devices** or **Device Groups**, choose **Configure > Caching > Akamai Connect**.

The **Akamai Connect** window appears, with two tabs: **Cache Settings** and **Cache Prepositioning**.

Step 2 Choose the **Cache Prepositioning** tab.

At this tab, you can add, edit, or delete cache prepositioning tasks, as well as monitor cache preposition task status.

Step 3 (Optional) To enable DRE for preposition connections, check the Preposition with DRE check box. The default is disabled, to prevent negative impact to the DRE byte cache for data that will be stored at the object level.

Step 4 At the **Cache Prepositioning** table listing, click **Add Cache Preposition Task**.

The **Cache Prepositioning Task** dialog box appears.

Step 5 In the **Name** field, enter the name of the preposition task.

- Preposition task name is an alphanumeric identifier up to 47 characters. Special characters like ‘,/,\,{,},(,),?,",<,>,[,],&,*, are not allowed.
- You can configure up to 10 URLs per task.
- You can configure up to 10 schedules per task.
- You can configure up to 50 tasks per device or device group.

Step 6 In the **URLs** field, enter the base URLs for prepositioning.

- The maximum length for the URL is 900 characters. Characters that are not allowed in the URL are space, double quotes (“). ASCII characters are allowed in the range of ASCII 33 through ASCII 125.
- Use a space to separate multiple URLs.
- You can configure up to 10 URLs per task.

Step 7 In the **Exclude Types** field, enter the object types to exclude from caching, such as .jsp or .asp, each separated by a comma.

The list of object name patterns to be excluded has a total pattern field limit of 47 characters.

Step 8 In the **Download Rate** field, enter the maximum download rate, in KBps. Select any value between 0 to 10,000,000 KBps.

- The default is 20 KBps.
- A selection of 0 indicates unlimited, or no enforced rate limiting.

Step 9 To enable recursion for this cache preposition task, check the Recursive Task check box. To have recursion disabled for this cache preposition task, leave the Recursive Task check box unchecked. The default is unchecked.

Step 10 If you have checked the **Recursive Task** check box, from the **Recursion Depth** drop-down list, choose the depth of the link level at which content is retrieved: 1, 2, 3, 5, 8, 13, or 21. You can also enter a custom value from 1 to 1000. The default recursion depth value is 1.

The **Recursion Depth** drop-down list is active only if you check the **Recursive Task** check box.

Note A greater number of specified levels of links means a greater amount of data stored in the cache, sometimes exponentially more. If the amount of requested prefetched data becomes larger than the cache, the newly requested data will flush all previously stored data, and may slow down other operations that attempt to use the cache.

Step 11 To enable this cache preposition task, check the **Enable Task** check box. The task must specify at least one URL (specified in the URLs field) and one schedule, specified in the next step.

Step 12 At the **Cache Prepositioning Schedule** table listing, click Add Schedule.

The **Cache Prepositioning Schedule** dialog box appears.

a) In the **Schedule Name** field, enter the name of the schedule of this cache preposition task, up to 256 alphanumeric characters. The schedule name allows you to provide your own representation of a schedule. For example, you can name a schedule that occurs every Monday, Wednesday, and Friday at 10:30 a.m. as **Weekly MWF 10:30AM** or as **Every Week - Mon-Wed-Fri at 10:30AM**.

b) From the **Frequency** drop-down list, choose the specified time for prepositioning: yearly, daily, weekly, or monthly days.

For example, if you choose you choose monthly days, a calendar with check boxes opens for you to check one, some, or all the days in a month for this schedule.

c) From the **Start Time (HH:MM)** drop-down lists, choose the hour and minute at which this cache prepositioning task should start.

d) Click **OK**.

Step 13 At the **Advanced Settings** section of the **Cache Prepositioning Task** dialog box, you can specify recursion delay time and recursion hostnames.

In the **Recursion Delay Time** field, enter the delay time, in seconds, between requests during recursive download. This simulates user wait time. Recursive delay time is necessary because some servers use the lack of time between requests to detect and restrict web crawlers.

- Enter a value between 0 to 600 seconds. The default is 2 seconds.
- A value of zero provides the best performance when there are no web crawler restrictions.

Step 14 In the **Recursion Domains** field, enter the list of server domain suffixes for which recursive web crawling is permitted. If this list is empty, then web crawling is only permitted within the same domain as the specified URL.

You can configure up to ten servers:

- The server name is up to 255 alphanumeric characters.
- Server names are separated by comma or space.

Step 15 Click **OK**.

Step 16 In the **Cache Prepositioning Schedule** dialog box, click **OK**.

Step 17 In the **Cache Prepositioning Task** dialog box, click **OK**.

Step 18 Click **Submit**.

The new cache prepositioning task is added as a line item in the **Cache Prepositioning** table listing.

Viewing Cache Prepositioning Task Status

The **Cache Prepositioning** pane provides two tables to show the status of a cache preposition task.

- To view the status of a cache preposition task you have configured, highlight and select the task from the first table, the **Cache Prepositioning** table listing.
- The second table, the **Cache Prepositioning Status** table listing, displays information on the selected task.
    - For an individual device: The cache prepositioning status table shows the selected task status for the current device.
    - For a device group: The cache prepositioning status table shows the status of the selected cache preposition task, for all devices under that device group.

The following table displays information for the selected cache prepositioning task.

Table 63: Cache Prepositioning Task Status Details

Cache Prepositioning Task Status Table Column	Description
Device Name	The name of the selected device.
Start Time	The date, hour, and minute for the task schedule to start.
End Time	The date, hour, and minute for the task schedule to end.
Byte Count	The total number of bytes in cache during the most recent preposition task run.
Object Count	The total count of objects in cache during the most recent preposition task run.

Cache Prepositioning Task Status Table Column	Description
Refresh Bytes	The number of bytes refreshed in cache during the most recent preposition task run.
Refresh Count	The count of objects refreshed in cache during the most recent preposition task run.
Store Bytes	The number of unmodified bytes for objects found in cache during the most recent task run.
Store Count	The count of unmodified objects found in cache during the most recent task run.
Uncacheable Bytes	The number of bytes of uncacheable objects encountered during the most recent task run.
Uncacheable Count	The count of uncacheable objects encountered during the most recent task run.
Status	The status of the task, such as **Scheduled**, **Complete**, or **Error**.
Error	If the task status is **Error**, an error message describing the task status is displayed.

Copying Cache Prepositioning Tasks

Before you begin

You can copy cache prepositioning tasks that have a device or device group enabled with Akamai Connect. Use the following methods to copy cache prepositioning tasks:

- Device to device
- Device to device group
- Device group to device
- Device group to device group

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure > Caching > Akamai Connect**.

The **Akamai Connect** window appears, with two tabs: **Cache Settings** and **Cache Prepositioning**.

Step 2 Choose the **Cache Prepositioning** tab.

Step 3 At the **Cache Prepositioning** pane, click **Copy Tasks**.

Step 4 From the **From** drop-down list, choose a device or device group as the source.

Step 5 From the **To** drop-down list, choose a device or device group as the destination.

Note If you try to copy a task with the same name between device and device groups, the following error message is displayed: **One or more preposition tasks with the same name already exists in the destination device/DG**.

Step 6 At the **Existing Cache Prepositioning Tasks** table listing, select one, some or all of the cache preposition tasks to be copied.

Step 7 Click **OK**.

The selected cache prepositioning tasks are copied from the specified source to the specified destination.

Configuring HTTP/S Preposition Proxy for Akamai Connect

This section contains the following topics:

About HTTP/S Preposition Proxy for Akamai Connect

For Cisco WAAS Version 6.2.1 and later, you can preposition external content in the case of a deployment with proxy. Consider the following when configuring HTTP/S preposition proxy for Akamai Connect:

- IPv4 proxy is supported for HTTP/S prepositioning.
- The HTTP preposition proxy feature is a feature independent of the Cisco WAAS Central Manager and external HTTP proxy features described in the sections Configuring the Cisco WAAS Central Manager as HTTP Proxy and Configuring External HTTP Proxy.
- Specific IP address-based proxy configuration is supported for HTTP/S preposition proxy. File-based and auto-detected configurations are not supported for HTTP/S preposition proxy.

Configuring Global Proxy Host and Port for Preposition Tasks

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure** > **Caching** > **Akamai Connect**.

The **Akamai Connect** window appears, with two tabs: **Cache Settings** and **Cache Prepositioning**.

Step 2 Choose the **Cache Prepositioning** tab.

Step 3 In the **Proxy Host** field, enter the hostname or IP address for the proxy host.

Step 4 In the **Proxy Port** field, enter the port number. Valid port numbers are 0 to 65535.

Step 5 Click **Submit**.

Step 6 Create a preposition task, as described in Configuring a Cache Prepositioning Task, on page 501.

Step 7 In the **Cache Prepositioning Task** dialog box, check the **Enable Proxy** check box.

Step 8 Schedule the task, as described in Step 12 of Configuring a Cache Prepositioning Task.

Step 9 Click **Submit**.

Modifying Proxy Settings for an Individual Prepositioning Task

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure > Caching > Akamai Connect**.

The **Akamai Connect** window appears, with two tabs: **Cache Settings** and **Cache Prepositioning**.

Step 2 Choose the **Cache Prepositioning** tab.

Step 3 Select a cache prepositioning task that you have configured as proxy.

Step 4 Modify the particular setting or settings.

Step 5 Check the **Enable Task** check box.

Step 6 Check the **Enable Proxy** check box.

Step 7 In the **Cache Prepositioning Schedule** dialog box, select parameters to reschedule the task.

Step 8 Click **OK**.

Step 9 In the **Cache Prepositioning Task** dialog box, click **OK**.

Step 10 Click **Submit**.

Removing Proxy Settings for an Individual Prepositioning Task

Procedure

Step 1 From the Cisco WAAS Central Manager menu, from either the **Device Groups** or **Devices** tab, choose **Configure > Caching > Akamai Connect**.

The **Akamai Connect** window appears, with two tabs: **Cache Settings** and **Cache Prepositioning**.

Step 2 Choose the **Cache Prepositioning** tab.

Step 3 Select a cache prepositioning task that you have configured as proxy.

Step 4 Check the **Enable Task** check box.

Step 5 Uncheck the **Enable Proxy** check box.

Step 6 In the **Cache Prepositioning Schedule** dialog box, select parameters to reschedule the task.

Step 7 Click **OK**.

Step 8 In the **Cache Prepositioning Task** dialog box, click **OK**.

Step 9 Click **Submit**.

Cisco Support for Microsoft Windows Update

Cisco support for Microsoft Windows Update enables caching of objects used in Windows OS and application updates. Cisco support for Microsoft Windows Update is enabled by default, and enabled only for specific sites.

This section contains the following topics:

About Cisco Support for Microsoft Windows Update

The Microsoft operating system and application updates are managed by update clients such as Microsoft Update. Microsoft Update downloads the updates via HTTP, often in combination with BITS (Background Intelligent Transfer Service) to help facilitate the downloads. Clients use HTTP range request to fetch updates.

The objects that comprise the updates, such as .cab files, are typically cacheable, so that HTTP object cache is a significant benefit for this process.

For example, for Windows 7 and 8 OS updates, via direct Internet or WSUS (Windows Server Update Services), versions 2012 and 2012R2, more than 98% of the update files, such as .cab, .exe, and .psf files, are served from cache on subsequent updates. Cisco support for Microsoft Windows Update reduces the volume of WAN offload bytes and reduces response time for subsequent Windows updates.

Viewing Statistics for Cisco Support for Microsoft Windows Update

There are two ways to view data generated by Cisco support for Microsoft Windows Update:

- Akamai Connected Cache Charts in the chapter "Monitoring Your Cisco WAAS Network," provides information including WAN response time and WAN offload bytes.
- For Cisco WAAS Version 6.1.1 and later, the cache engine access log file has two new fields for Microsoft Windows Update statistics:
    - **rm-w** (range miss, wait): The main transaction, a cache miss, which waited for the sub-transaction to fetch the needed bytes

      .
    - **rm-f** (range miss, full): The sub-transaction, a cache write of the entire document.

  Example 1:

  Example 1 contains two log lines, the main transaction and sub-transaction, when a range is requested on an object that is not in cache:

  ```
  ws8-rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
  08/28/2015 12:22:29.663 (fl=27520) 300 13.164 0.000 446 - - 34912 172.25.30.4
  ```

  ```
  191.234.4.50 2905 h - - rm-w 206 GET
  http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/secu/2013/07/wind
  ows8-rt-kb2863725- x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
  ```

  ```
  08/28/2015 12:24:31.448 (fl=27520) 300 134.949 0.000 355 344 3591542 568 172.25.30.4
  191.234.4.50 2f25 m-s - - rm-f 200 GET
  http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/secu/2013/07/wind
  ows8-rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
  ```

  Example 2:

Example 2 shows a cache hit when a range is requested on an object that is either completely in cache, or in the process of being downloaded. If it is in the process of being downloaded, then the main transaction has latched onto a sub-transaction like the one shown in Example 1.

```
08/28/2015 03:34:36.906 (fl=26032) 300 0.000 50.373 346 - - 13169 172.25.30.4
8.254.217.62 2905 h - - - 206 GET
http://fg.v4.download.windowsupdate.com/d/msdownload/update/software/secu/2013/07/wind
ows8-\ rt-kb2863725-x64_dd8522e527483cd69bf61d98ee849a2406b97172.psf - -
```

Cisco Support for Microsoft Windows Update and Akamai Cache Engine

Cisco support for Microsoft Windows Update enables Akamai Cache Engine to support Windows Update caching in two ways:

- Download and cache full objects even when ranges within objects that not in cache are requested.
- Future range requests on the objects can be served out of cache.

There is a limit, set by OTT metadata during the Akamai Connect registration process, from the start of the object - the number of bytes or the percent of file length - where the download functionality is triggered. A request of a size above the set limit does not initiate a full object download, and the request is forwarded to the origin as is.

Note Cisco Support for Microsoft Windows update is enabled by default, and enabled only for specific sites. The enabled sites are updated via OTT metadata.

If you want to disable Cisco Support for Microsoft Windows Update, you must disable OTT caching. To do this, uncheck the Over the Top Cache check box. However, note that unchecking the Over the Top Cache check box disables all OTT functionality, both global and custom OTT configurations.

Cisco WAAS CLI Commands Used with Akamai Connect

This section contains the following topics:

Cisco WAAS Global Configuration Commands Used with Akamai Connect

The following table highlights the Cisco WAAS global configuration commands used with Akamai Connect.

Table 64: Cisco WAAS Global Configuration Commands Used with Akamai Connect

Command	Description
(config) accelerator http object-cache connected enable	Enables the Akamai Connected Cache to cache content that is delivered by an Edge server on the Akamai Intelligent Platform. Object caching is done on the client side Cisco WAAS device only. **Note** You must enable and register Akamai Connect from the Cisco WAAS Central Manager before you run the **accelerator http object-cache connected enable** global configuration command. Otherwise, running this command will invalidate the Akamai Connect End-User License Agreement.
(config) accelerator http object-cache cws-check enable	Enables Cisco Cloud Web Security feature.
(config) accelerator http object-cache enable	Turns on the Akamai cache engine for the Cisco WAAS device.
(config) accelerator http object-cache ott enable	Enables Over the Top (OTT) caching.
(config) accelerator http object-cache transparent enable	Enables the Akamai HTTP object cache (the Akamai cache engine) in **Basic** mode. **Note** When using the CLI to enable the HTTP object cache (the Akamai cache engine), the default caching mode is **Basic**. When using the Cisco WAAS Central Manager to enable HTTP object cache, the default caching mode is **Standard**.
(config) accelerator http object-cache transparent advanced	Enables the Akamai HTTP object cache (the Akamai cache engine) in **Advanced** mode.
(config) accelerator http object-cache transparent basic	Enables the Akamai HTTP object cache (the Akamai cache engine) in **Basic** mode.
(config) accelerator http object-cache transparent bypass	Enables the Akamai HTTP object cache (the Akamai cache engine) in **Bypass** mode.
(config) accelerator http object-cache transparent enable	Enables the Akamai HTTP object cache (the Akamai cache engine) in **Basic** mode.
(config) accelerator http object-cache transparent standard	Enables the Akamai HTTP object cache (the Akamai cache engine) in **Standard** mode.

Command	Description
(config) accelerator http object-cache validate-address bypass	Adds bypass server IP addresses to a whitelist for Server Address Validation.
(config) accelerator http object-cache validate-address bypass	Validates the IP server address configuration.
(config) device mode application-accelerator profile branch	For use with Cisco WAVE devices, to enable the device to function as a branch device, to configure resource pre-allocation resources for various Cisco WAAS services to be branch traffic scenario and branch services.
(config) http-object cache validate address enable	Validates the server IP address configuration.

Cisco WAAS Preposition Configuration Commands Used with Akamai Connect

The following table highlights the Cisco WAAS preposition configuration commands used with Akamai Connect.

Table 65: Cisco WAAS Preposition Configuration Commands Used with Akamai Connect

Command	Description
(config-preposition) accelerator http preposition dre enable	Enables Data Redundancy Elimination (DRE) for preposition connections.
(config-preposition) accelerator http preposition task task-name	Configure a preposition task for one or more sites.

Cisco WAAS EXEC Commands Used with Akamai Connect

The following table highlights the Cisco WAAS EXEC commands used with Akamai Connect.

Table 66: Cisco WAAS EXEC Commands Used with Akamai Connect

Command	Description
clear cache http-object-cache invalidate	Clears the HTTP object cache.
clear statistics accelerator http object-cache	Clears HTTP object cache statistics from a Cisco WAAS device.
debug accelerator http object-cache	Enables object cache debugging.
debug cms {router-config | stats}	Monitor and record CMS debugging for router configuration and statistics, from the Cisco WAAS Central Manager.

Command	Description
disk delete-data-partitions	Deletes all data partitions on all logical drives. Data partitions include the CONTENT, PRINTSPOOL, and GUEST partitions. These partitions include all DRE cache files and print spool files.
show accelerator http object-cache	Displays HTTP object cache configuration and status information for a Cisco WAAS device.
show hosts	Lists and verifies the name servers and their corresponding IP addresses, and lists the hostnames, their corresponding IP addresses, and their corresponding aliases (if applicable).
show statistics accelerator http preposition	Displays preposition task information for a Cisco WAAS device.
show statistics accelerator http object-cache	Displays object cache statistics for a Cisco WAAS device.

CHAPTER 14

Maintaining Your Cisco WAAS System

This chapter describes the tasks to perform to maintain your Cisco WAAS system.

Note Throughout this chapter, the term Cisco WAAS device is used to refer collectively to the Cisco WAAS Central Managers and Cisco Wide Area Application Engines (WAEs) in your network. The term WAE refers to WAE and WAVE appliances, and Cisco Virtual WAAS (vWAAS) instances.

This chapter contains the following sections:

Upgrading the Cisco WAAS Software

This section contains the following topics:

Operating Guidelines for Upgrading the Cisco WAAS Software

Consider the following guidelines when you upgrade your Cisco WAAS software:

- As shown in , upgrading is supported only from certain older releases to a particular release. If you have a Cisco WAAS device that is running a release from which upgrading to the desired release is not supported, first upgrade the device to an intermediate supported release and then to the final desired release.

When you perform a software upgrade using the Cisco WAAS Central Manager, there is only a limited system check to verify the support of the target Cisco WAAS version. To ensure that you have a successful Cisco WAAS upgrade, use Table 14-1 to verify that the target version is supported for your system.

For more information on Cisco WAAS software versions, see *Release Note for Cisco Wide Area Application Services*.

Table 67: Upgrade Paths to Cisco WAAS Version 6.4.3x

Current Cisco WAAS Version	Cisco WAAS Central Manager Upgrade Path	Cisco WAAS Upgrade Path
5.5.3 and later	Upgrade directly to 6.4.3x	Upgrade directly to 6.4.3x
4.3.x through 5.5.1	**1.** Upgrade to 5.5.3, 5.5.5x (5.5.5, 5.5.5a), or 5.5.7x **2.** Upgrade to 6.4.3x	**1.** Upgrade to 5.5.3, 5.5.5x, or 5.5.7x **2.** Upgrade to 6.4.3x
4.2.x	**1.** Upgrade to version 4.3.x through 5.4.x **2.** Upgrade to 5.5.3 or 5.5.5x (5.5.5, 5.5.5a), or 5.5.7x **3.** Upgrade to 6.4.3x	**1.** Upgrade to version 4.3.x through 5.4.x **2.** Upgrade to 5.5.3, 5.5.5x, or 5.5.7x **3.** Upgrade to 6.4.3x

- We recommend that all the devices in your Cisco WAAS network run the same version of the Cisco WAAS software. If some of your Cisco WAAS devices are running different software versions, the Cisco WAAS Central Manager should be the latest version. For details on Cisco WAAS version interoperability limitations, see the *Release Note for Cisco Wide Area Application Services*.
- If the Cisco WAAS Central Manager detects any registered Cisco WAE devices that are at a higher version level than the current one, it raises a minor alarm to alert you. Additionally, the Cisco WAE devices are shown in red on the device listing page.
- The Cisco WAAS Central Manager running Cisco WAAS Version 5.4.1 can manage Cisco WAE devices running Cisco WAAS Version 4.3.1 and later. However, some Cisco WAAS Central Manager windows with Cisco Version 5.4.1 features will not be applicable to Cisco WAAS devices that are running a version earlier than Cisco WAAS Version 5.4.1. If you modify this configuration, the configuration is saved, but it does not affect the earlier-version devices until these are upgraded to Cisco WAAS Version 5.4.1.
- If you are upgrading from a Cisco WAAS Version earlier than Cisco WAAS Version 6.1.1x to Cisco WAAS Version 6.x and use virtual blade, the upgrade procedure may get stuck in the Proceeding with Download phase. To remedy this scenario, follow these steps:

  1. To remove the Cisco WAAS device registration record and its configuration on the Cisco WAAS Central Manager, on the Cisco branch device, run the **cms degister** EXEC command.
  2. Wait ten minutes.
  3. To enable synchronization of the Cisco WAAS network configuration of the Cisco WAAS device with the local Cisco WAAS CLI configuration, on the Cisco WAAS branch device, run the **cms enable** EXEC command.

4. Using the Cisco WAAS Central Manager, install the specified Cisco WAAS 6.x version.

- Cisco WAAS Version 5.4.x is not supported running in a mixed-version Cisco WAAS network with any Cisco WAAS device that is running a Cisco WAAS version earlier than Cisco WAAS 4.3.1.

  Consider these upgrade guidelines:

  - If you have Cisco WAAS devices running versions earlier than Cisco WAAS Version 4.3.1, you must first upgrade these devices to Cisco WAAS Version 4.3.1, or a later version, before you install version Cisco WAAS Version 5.2 on the Cisco WAAS Central Manager.
  - Do not upgrade any Cisco WAAS device to a version later than the existing Cisco WAAS Central Manager version.
  - After all the Cisco WAAS devices are upgraded to Cisco WAAS Version 4.3.1 or later, you can begin the upgrade to Cisco WAAS Version 5.4.1 on the Cisco WAAS Central Manager.
  - Directly upgrading a device from Cisco WAAS Version 4.0, Version 4.1 or Version 4.2 to Cisco WAAS Version 5.4.1 is not supported.

Before Starting the Upgrade:

- Disable WCCP on all Cisco WAEs in an AppNav cluster. After upgrade is complete, confirm the following before you re-enable WCCP.
  - The Cisco WAEs are up and running.
  - The AppNav cluster is re-converged properly.
  - All disks are ready (not initializing).
  - There are no alarms on the device.
  - The **show accelerator** EXEC command shows all enabled Application Optimizers are healthy.

    After you have confirmed that each of these is complete, re-enable WCCP.

Checklist for Upgrading the Cisco WAAS Software

The Table 68: Checklist for Upgrading the Cisco WAAS Software table highlights the tasks needed to upgrade the Cisco WAAS software. In addition, consider these guidelines:

- To downgrade or roll back the Cisco WAAS software to a lower version, first downgrade or roll back the Cisco WAE devices' version, then the standby Central Manager (if applicable), and finally the primary Cisco WAAS Central Manager. For more information about downgrading, see the Release Note for Cisco Wide Area Application Services.
- You cannot downgrade an Cisco ENCS 5400-W device to a Cisco WAAS software version lower than 6.4.1, either from a device or a device group level. A warning message is displayed if you attempt to downgrade.

Table 68: Checklist for Upgrading the Cisco WAAS Software

Task	Additional Information and Instructions
1. Determine the current software version running on your Cisco WAAS network.	Check the software version that you are currently using so when you go to Cisco.com, you know if there is a newer version to download. For more information, see Determining the Current Software Version.
2. Obtain the new Cisco WAAS software version from **cisco.com**.	Visit **cisco.com** to download a newer software version and place this file on a local FTP or HTTP server. For more information, see Obtaining the Latest Cisco WAAS Software Version.
3. Register the new software version with the Cisco WAAS Central Manager.	Register the URL of the new software file so the Cisco WAAS Central Manager knows where to go to access the file. For more information, see Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI.
4. Upgrade all your Cisco WAAS Central Managers and Cisco WAAS devices.	Upgrade the Standby and Primary Cisco WAAS Central Managers. For more information, see Upgrading the Cisco WAAS Central Manager. After upgrading the Cisco WAAS Central Manager, upgrade all your Cisco WAAS devices that are members of a device group. For more information, see Upgrading Multiple Devices Using Device Groups.
5. Delete the software version file.	After completely upgrading your Cisco WAAS network, you can remove the software file if desired. For more information, see Deleting a Software File .

Determining the Current Software Version

To view the current software version running on a particular device, choose **Devices** > **All Devices**. The **All Devices** window displays the software version for each listed device.

You can also click **Devices** > *device-name* or the **Edit** icon next to the name of a device in the **Devices** window. The **Device Dashboard** window appears, listing the software version for that device.

Note The software version is not upgraded until a software upgrade is successfully completed. If a software upgrade is in progress, the version number displayed is the base version, not the upgraded version number.

Alternatively, in the device context, choose **Monitor** > **CLI Commands** > **Show Commands**. Choose the version and click **Submit**. A secondary window is displayed with the CLI output for the **show version** EXEC command.

Obtaining the Latest Cisco WAAS Software Version

Procedure

Step 1 Launch your web browser and access the Cisco Software Download page:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Choose **Application Networking Services** > **Wide Area Application Services** > **Cisco Wide Area Application Services (WAAS) Software** download area.

Step 3 Choose the Cisco WAAS software version that you want and download the appropriate software image.

Step 4 Register the location of the software file in the WAAS Central Manager GUI, as described in Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI, on page 517.

Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI

Before you begin

To upgrade your Cisco WAAS software, you must first specify the location of the Cisco WAAS software file in the Cisco WAAS Central Manager GUI and configure the software file settings.

There are two types of Cisco WAAS software files:

- **Universal**: Includes Cisco WAAS Central Manager, Application Accelerator, and AppNav Controller functionality. You can use this type of software file to upgrade a device operating in any mode.
- **Accelerator only**: Includes Application Accelerator and AppNav Controller functionality only. You can use this type of software file to upgrade only an Application Accelerator or AppNav Controller device. If you want to change an Application Accelerator or AppNav Controller to a Central Manager, you must install the Universal software file, reload the device, change the device mode to central-manager, and then reload the device again. Additionally, kdump analysis functionality is not included in the Accelerator only image.

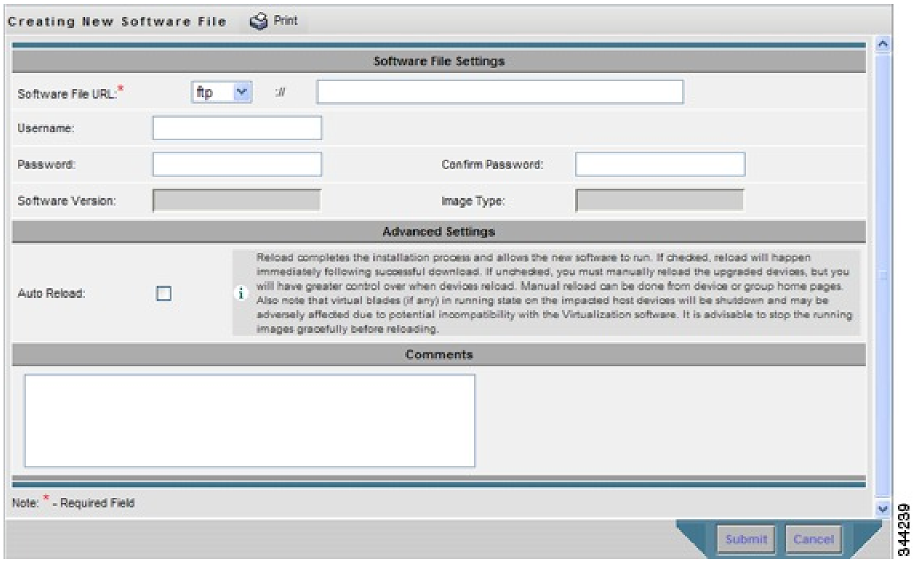
Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **Version Management** > **Software Update**.

Step 2 Click the **Create New Software File** icon in the taskbar.

The **Creating New Software File** window appears.

Figure 82: Creating New Software File Window



Software File URL:* ftp ://

Auto Reload: □

Reload completes the installation process and allows the new software to run. If checked, reload will happen immediately following successful download. If unchecked, you must manually reload the upgraded devices, but you will have greater control over when devices reload. Manual reload can be done from device or group home pages. Also note that virtual blades (if any) in running state on the impacted host devices will be shutdown and may be adversely affected due to potential incompatibility with the Virtualization software. It is advisable to stop the running images gracefully before reloading.

Note: * - Required Field

Step 3 In the **Software File URL** field, specify the location of the new WAAS software file as follows:

a) From the **Software File URL** drop-down list, choose a protocol (**HTTP** or **FTP**).

b) Enter the URL for the **.bin** software file that you downloaded from Cisco.com. For example, a valid URL might look like the following:

http://internal.mysite.com/waas/*WAAS-xxxx-K9***.bin**

http://2012:3:3:3::8/waas/*WAAS-xxxx-K9***.bin**

Here, **WAAS- xxxx -K9.bin** is the name of the software upgrade file. (The filename typically includes the version number.)

Be sure that the URL identifies the correct type of software image for the devices you want to upgrade, either **Universal** or **Accelerator** only.

If the Central Manager has been configured with an IPV6 address, it can be accessed using **https://[CM ipv6 address]:8443/**

Software update configuration with IPv6 address will be filtered in the **device /device group** level usage pages for unsupported device models and versions.

Step 4 (Optional) If your server requires user login authentication, enter your username in the **Username** field and enter your login password in the **Password** field. Enter the same password in the **Confirm Password** field.

The **Software Version** and **Image Type** fields cannot be edited. They are filled in automatically after you submit the settings and the image is validated.

Step 5 To automatically reload a device when you upgrade the software, at the **Advanced Settings** pane, check the **Auto Reload** check box. If you do not check this check box, you should manually reload a device after you upgrade the software on it to complete the upgrade process.

Step 6 (Optional) Enter comments in the **Comments** field.

Step 7 Click **Submit**.

The software image file is validated and the **Software Version** and **Image Type** fields are filled in with the appropriate information extracted from the image file.

Caution If your browser is configured to save the username and password for the Cisco WAAS Central Manager GUI, the browser will autopopulate the **Username** and **Password** fields in the **Creating New Software File** window. You must clear these fields before you click **Submit**.

The software file that you want to use is now registered with the Cisco WAAS Central Manager. When you perform the software upgrade or downgrade, the URL that you just registered becomes one of the choices available in the **Update Software** window.

Step 8 To reload a device from the CLI, run the **reload** EXEC command.

Note When you are viewing the list of registered software files, if the **Image Type** column displays **Unknown** for a software file, it indicates that the software file was added under a Cisco WAAS version earlier than Cisco WAAS Version 4.2.1. These **Unknown** software files must be resubmitted if you want to use them. Click the Edit icon next to the file to open the **Modifying Software File** window, and then, to resubmit the file, click **Submit**.

Upgrading the Cisco WAAS Central Manager

Before you begin

When upgrading software in your Cisco WAAS network, begin with Cisco WAAS Central Manager before upgrading Cisco WAAS WAE devices.

Primary and Standby Cisco WAAS Central Manager devices must be running the same version of Cisco WAAS software. If they are not, the Standby Cisco WAAS Central Manager detects this and will not process any configuration updates it receives from the Primary Cisco WAAS Central Manager. If the Primary Cisco WAAS Central Manager sees that the Standby Cisco WAAS Central Manager has a different version level, it shows the Standby Cisco WAAS Central Manager in red on the device listing page.

If you use the primary Cisco WAAS Central Manager to perform the software upgrade, you need to upgrade your standby Cisco WAAS Central Manager first, and then upgrade your primary Cisco WAAS Central Manager. We also recommend that you create a database backup for the primary Cisco WAAS Central Manager and copy the database backup file to a safe place before you upgrade the software.

Use this upgrade procedure for Cisco WAAS Central Manager devices. You can also use this upgrade procedure to upgrade Cisco WAAS devices one at a time (after the Cisco WAAS Central Manager).

Procedure

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

The **Device Dashboard** window appears.

Step 2 Verify that the device is not already running the version to which you plan to upgrade.

Step 3 Click **Update**.

The **Software Update** window appears.

Step 4 To choose the software file URL from the **Software Files** list, click the radio button next to the corresponding filename.

The list displays only software files with an image type of **Universal**, because you are upgrading a Cisco WAAS Central Manager device. If no such images are available, you must create a software file, as described in Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI.

Step 5 To confirm you decision, click **Submit** and then click **OK**.

The **Devices Listing** window is displayed again. You can monitor the progress of your upgrade from this window.

Software upgrade status messages are displayed in the **Software Version** column. These intermediate messages are also written to the system log on the Cisco WAAS devices. See theTable 69: Upgrade Status Messages, on page 520 table for a description of upgrade status messages.

Step 6 Clear your browser cache, close the browser, and restart the browser session to the WAAS Central Manager.

What to do next

The Cisco WAAS Central Manager may reboot at the conclusion of the upgrade procedure (if **Auto Reload** is in the **Creating New Software File** window), causing you to temporarily lose contact with the device and the Cisco WAAS Central Manager GUI.

Table 69: Upgrade Status Messages

Upgrade Status Message	Status
Pending	The request has not yet been sent from the Cisco WAAS Central Manager to the device, or receipt of the request is yet to be acknowledged by the device.
Downloading	The download method for the software file is being determined.
Proceeding with Download	The download method for the software file is determined to be a direct download. Proceeding with the request for direct download of the software file.
Download in Progress (Completed...)	The direct download of the software file is being processed. **Completed** indicates the number of megabytes processed.
Download Successful	The direct download of the software file is successful.
Download Failed	The direct download of the software file cannot be processed. Further troubleshooting is required; see the device system message log. If you are upgrading several devices at once, the download may fail if the server hosting the software file becomes overloaded with requests. Retry the upgrade by clicking the **Retry** link if it is displayed.
Proceeding with Flash Write	A request has been made to write the software file to the device flash memory.
Flash Write in Progress (Completed...)	The write of the device flash memory is being processed. **Completed** indicates the number of megabytes processed.

Upgrade Status Message	Status
Flash Write Successful	The flash write of the software file has been successful.
Reloading	A request to reload the device has been made in order to complete the software upgrade. The device may be offline for several minutes.
Reload Needed	A request to reload the device has not been made. The device must be reloaded manually to complete the software upgrade.
Cancelled	The software upgrade request was interrupted, or a previous software upgrade request was bypassed from the Cisco WAAS CLI.
Update Failed	The software upgrade could not be completed. Troubleshooting is required; see the device system message log. If you are upgrading several devices at once, the upgrade may fail if the server hosting the software file becomes overloaded with requests. Retry the upgrade by clicking the **Retry** link if it is displayed.

Upgrading Multiple Devices Using Device Groups

Before you begin

This procedure is for Cisco WAE devices only. Cisco WAAS Central Manager devices cannot be upgraded using device groups.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** > *device-group-name*.

Step 2 Choose **Admin** > **Versioning** > **Software Update**.

The **Software Update for Device Group** window appears.

Step 3 To choose the software file URL from the **Software File URL** list, click the radio button next to the filename. If no images are available, create a software file, as described in Specifying the Location of the Software File in the Cisco WAAS Central Manager GUI.

If you are updating many devices and you want to use a smaller size software file to save network bandwidth, specify a software file with an image type of Accelerator only, which is smaller than a Universal image. If you later want to change an **Accelerator-only** device to a **Cisco WAAS Central Manager**, you must install the **Universal software file**, reload the device, change the device mode to **central-manager**, and then reload the device again.

Step 4 Click **Submit**.

To view the progress of an upgrade, choose **Devices** > **All Devices** to display the **All Devices** window, and to view the software upgrade status message in the **Software Version** column. These intermediate messages are also written to the system log on Cisco WAAS devices. See the Table 69: Upgrade Status Messages, on page 520 table for a description of the upgrade status messages.

Upgrading Cisco WAAS Central Manager to New Hardware and Converting an Existing Cisco WAAS Central Manager to a Cisco WAE

Before you begin

Consider the following guidelines:

- To add a new piece of hardware as a primary Cisco WAAS Central Manager, and use the existing Cisco WAAS Central Manager as a Cisco WAE, it is important to first add it to the system and then configure it.
- To prevent the former Cisco WAAS Central Manager from later being used as a Cisco WAE, perform a database backup of the former Central Manager and restore it on the new device.

Procedure

Step 1 Add a hardware device as the new Cisco WAAS Central Manager and configure it as a Standby Cisco WAAS Central Manager. There may be multiple Standby Cisco WAAS Central Managers in the system. For more information, see Configuring the Cisco WAAS Central Manager Role.

Step 2 Enable the new hardware device to be the primary Cisco WAAS Central Manager after it is available online and has finished synchronizing with other systems. For more information, see Converting a Standby Cisco WAAS Central Manager to a Primary Cisco WAAS Central Manager.

Step 3 To remove the former Cisco WAAS Central Manager from the Cisco WAAS Central Manager database:

- Disable the CMS service.
- At the former Cisco WAAS Central Manager CLI interface, run the cms deregister EXEC command.
- If there is no connectivity between the devices anymore, run the **cms deregister force** EXEC command and manually delete the former Cisco WAAS Central Manager in the new Cisco WAAS Central Manager GUI.

```
wae# cms deregister force
Deregistering WAE device from Central Manager will result in loss of data on encrypted
file systems, imported certificate/private keys for SSL service and wafs preposition
credentials. If secure store is initialized and open, clear secure store and wait for
one datafeed poll rate to retain wafs preposition credentails.
Do you really want to continue (yes|no) [no]?yes Disabling management service.
management services stopped
Sending de-registration request to CM
Failed to contact CM(Unmarshaled: 9001). Please check connectivity with CM device and
status of management service on CM.
Device de-registration failed, removing device registration information.
Please delete the device record on the Central Manager.
Removing cms database tables.
Re-initializing SSL managed store and restarting SSL accelerator.Deregistration
complete. Save current cli configuration using 'copy running-config startup-config'
command because CMS service has been disabled.
#
```

Step 4 After the former Cisco WAAS Central Manager has been deregistered, perform the following tasks:

- Rename the former Cisco WAAS Central Manager.
- Change the IP address of the former Cisco WAAS Central Manager.

- To change the device mode, run the **device mode** global configuration command.
- To reload the device, run the **reload** EXEC command.

```
wae# configure
wae(config)# device mode application-accelerator
The new configuration will take effect after reload.
wae# reload
```

Step 5 After the device has been reloaded, perform the following tasks:

- Rename the new Primary Cisco WAAS Central Manager.
- Change the IP address to fully replace the former one. Otherwise, you will need to update the configuration of your devices to point to the new address of the Cisco WAAS Central Manager.
- Contact a Cisco TAC member for scripts.

```
wae(config)# hostname old primary central-manager name
wae(config-if)# ip address ipaddress netmask
```

Deleting a Software File

Before you begin

After you have successfully upgraded your Cisco WAAS devices, you can remove the software file from your Cisco WAAS system.

Note You may want to wait a few days before removing a software file in the event that you may have to downgrade your system for any reason.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **Version Management** > **Software Update**.

Step 2 Click the **Edit** icon next to the software file that you want to delete.

The **Modifying Software File** window appears.

Step 3 Click the **Trash** icon in the taskbar.

You are prompted to confirm your decision to delete the software file.

Step 4 Click **OK**.

The selected software file is removed from your Cisco WAAS network.

Backing Up and Restoring Your Cisco WAAS System

This section contains the following topics:

Backing Up and Restoring the Cisco WAAS Central Manager Database

Before you begin

Consider the following guidelines before you back up or restore the Cisco WAAS Central Manager database:

- If you have already performed a backup when the secure store was in **user-passphrase** mode and you restored it to a system where the secure store is in **auto-passphrase** mode, you must enter the user passphrase to proceed with the restore. After the restore, the system is in **user-passphrase** mode.

  If you already performed a backup when the secure store was in **auto-passphrase** mode and you restored it to a system where the secure store is in **user-passphrase** mode, you do not have to enter a password. After the restore, the system is in **auto-passphrase** mode.

- The Cisco WAAS Central Manager device stores Cisco WAAS network-wide device configuration information in its Centralized Management System (CMS) database. You can manually back up the CMS database contents for greater system reliability.

- The CMS database backup is in a proprietary format that contains an archive database dump, Cisco WAAS Central Manager registration information, and device information that the Cisco WAAS Central Manager uses to communicate with other Cisco WAAS devices. CMS database backup files are not interchangeable between primary and standby Cisco WAAS Central Manager devices. This means that you cannot use the backup file from a primary Cisco WAAS Central Manager to restore a standby Cisco WAAS Central Manager.

- To back up the CMS database for the Cisco WAAS Central Manager, run the **cms database backup** EXEC command. For database backups, specify the location, password, and user ID of the remote server that you want to store the backup file in. If you want to back up only the configuration information, run the **cms database backup config** EXEC command.

Procedure

Step 1 To back up the CMS database to a file, on the Cisco WAAS Central Manager GUI, run the **cms database backup** global configuration command, as shown in the following example:

```
CM# cms database backup
Creating database backup file backup/cms-db-11-05-2010-15-22_4.3.1.0.1.dump
Backup file backup/cms-db-11-05-2010-15-22_4.3.1.0.1 is ready.
Please use 'copy' commands to move the backup file to a remote host.
```

Note The backup file is automatically given a name in the format cms-db-*date-timestamp_version*.dump, for example, **cms-db-7-22-2010-17-36_4.3.1.0.1.dump**. Note that the timestamp is in a 24-hour format (HH:MM) that does not show seconds. It is stored in **/local1/backup**.

Step 2 Save the file to a remote server by using the **copy disk ftp** command. This command copies the file from a local disk to a remote FTP server.

Step 3 Restore the CMS database as follows:

a) Disable the CMS service:

```
CM# configure
CM(config)# no cms enable
CM(config)# exit
```

Note Stopping the CMS service disables the Cisco WAAS Central Manager GUI. All the users who are currently logged in to this GUI are automatically logged out after the CMS service is disabled.

b) To delete the existing CMS database, run the **cms database delete** EXEC command.

c) To initialize the CMS database, run the **cms database create** EXEC command.

d) Restore the CMS database contents from the backup file:

```
CM# cms database restore backup/cms-db-7-22-2008-17-36_4.1.3.0.1.dump
```

Note After the restore, any WAEs that were registered with the Cisco WAAS Central Manager during the time since the backup was created will be disconnected from the Cisco WAAS Central Manager because there is no information about them in the backup file. To bring these WAEs online, you must deregister and reregister them with the Cisco WAAS Central Manager. On each WAE that was disconnected, use the following commands:

```
WAE# cms deregister force
WAE# configure
WAE(config)# cms enable
```

e) To enable the CMS service on the Cisco WAAS Central Manager, run the **cms enable** global configuration command.

Step 4 (Optional) If you want to upgrade the Cisco WAAS Central Manager to a newer model, backing up the former Cisco WAAS Central Manager's database and restoring it on the new device prevents it from being used as a WAE later. For more information, see Upgrading Cisco WAAS Central Manager to New Hardware and Converting an Existing Cisco WAAS Central Manager to a Cisco WAE.

Backing Up and Restoring a Cisco WAE Device

You should back up the database of each Cisco WAAS device on a regular basis in case a system failure occurs.

Note The backup and restore methods described in this section apply only to a Cisco WAE device that is not configured as a Cisco WAAS Central Manager. For information on backing up the Cisco WAAS Central Manager device, see Backing Up and Restoring the Cisco WAAS Central Manager Database, on page 524.

To back up and restore a device's configuration, run the **copy running-config** EXEC command. This command saves the currently running configuration.

Additionally, you can restore a Cisco WAE to the default configuration that it was manufactured with at any time by removing the user data from the disk and Flash memory, and erasing all the existing files cached on the appliance. Basic configuration information, such as network settings, can be preserved. The appliance is accessible through Telnet and Secure Shell (SSH) after it reboots.

Note If software upgrades have been applied, the restoration process returns to the defaults of the currently installed version and not the factory defaults.

To restore a Cisco WAE to its factory defaults or the defaults of the current configuration from the CLI, run the **restore factory-default [preserve basic-config]** EXEC command.

For more information about the CLI commands, see the *Cisco Wide Area Application Services Command Reference Guide* .

Reinstalling the System Software

This section contains the following topics:

About Reinstalling the System Software

The Cisco WAAS software consists of three basic components:

- Disk-based software
- Flash-based software
- Hardware platform cookie (stored in flash memory)

All of these components must be correctly installed for Cisco WAAS software to work properly.

The software is contained in two types of software images provided by Cisco Systems:

- A **.bin** image that contains disk and flash memory components (the Universal version of the WAAS software)
- A **.sysimg** image that contains a flash memory component only

A software recovery CD-ROM ships with some WAE and WAVE hardware devices. Some WAVE devices use a USB flash drive for recovery.

Caution If you upgraded your software after you received your software recovery CD-ROM or image files, using the recovery software images may downgrade your system. Ensure that you are using the desired software recovery version.

An installation that contains only the Cisco WAAS flash memory-based software, without the corresponding disk-based software, boots and operates in a limited mode, allowing for further disk configuration before completing a full installation.

The **.sysimg** component is provided for recovery purposes and allows for repair of flash memory only without modifying the disk contents.

Note The system image that is used depends on your device. For all WAVE devices (64-bit platforms), use the 64-bit system image (with **x86_64** in its name). For all other devices, use the 32-bit system image named without this designator. A Network Processing Engine (NPE) image that has the disk encryption feature disabled for use in countries where disk encryption is not permitted, is provided.

If you have a Cisco WAVE appliance that requires a USB flash drive for software recovery, your USB flash drive must contain both of the needed software images in the form of an ISO archive file that you copy to the flash drive. (See Preparing the USB Flash Drive, on page 528).

These options are available from the software recovery installer menu:

- **Option 1, Configure Network**: If the **.bin** image you need to install is located on the network instead of the CD-ROM or USB flash drive (which may be the case when an older CD-ROM or USB image is used to install new software), then you must choose this option to configure the network before attempting to install the .bin image.

  This option is performed automatically if you install a .sysimg file from the network.

- **Option 2, Manufacture Flash**: This option verifies the flash memory and, if invalid, automatically reformats it to contain a Cisco standard layout. If reformatting is required, a new cookie is installed automatically.

  This option is performed automatically as part of a .bin or .sysimg installation.

- **Option 3, Install Flash Cookie**: This option generates a hardware-specific platform cookie and installs it in flash memory. Use this option only if there has been a change in the hardware components, such as replacing the motherboard, or if you moved a flash memory card between systems.

  This option is performed automatically during the flash manufacturing process, if needed, as part of a **.bin** or **.sysimg** installation.

- **Option 4, Install Flash Image from Network** and **Option 5, Install Flash Image from USB/CD-ROM**: These options allow installation of only the flash memory .sysimg and do not modify disk contents. They can be used when a new chassis has been provided and populated with a customer’s old disks that need to be preserved.

  These options automatically perform flash verification and hardware cookie installation, if required. When installing from the network, you are prompted to configure the network if you have not already done so.

- **Option 6, Install Flash Image from Disk**: This option is reserved for future expansion and is not available.

- **Option 7, Re-create RAID device**: This option applies only to WAVE-7541, WAVE-7571, and WAVE-8541 devices and re-creates the RAID array.

- **Option 8, Wipe Out Disks and Install .bin Image**: This option provides the preferred procedure for installing the Cisco WAAS software.

  Caution Option 8 erases the content from the all disk drives in your device.

  This option performs the following steps:

1. Checks that flash memory is formatted to Cisco specifications. If yes, the system continues to Step 2. If no, the system reformats the flash memory, which installs the Cisco file system, and generates and installs a platform-specific cookie for the hardware.
2. Erases data from all drives.
3. Re-manufactures the default Cisco file system layout on the disk.
4. Installs the flash memory component from the **.bin** image.
5. Installs the disk component from the **.bin** image.

Preparing the USB Flash Drive

Before you begin

If you have a Cisco WAVE appliance that requires a USB flash drive for software recovery, you must prepare the USB flash drive with the appropriate files before you can start the software recovery process. You will need the following:

- Windows PC (Windows XP or 7) or Mac computer
- USB flash drive that is 1 GB or larger in size
- The following software recovery files:
  - Cisco WAAS Rescue CD ISO image file, which is available on the Cisco WAAS Software Download page. The filename is similar to **waas-rescue-cdrom-x.x.x.x-k9.iso**, where the x's denote the software version number. Alternatively, the ISO image file is available on the Cisco WAAS release DVD, or you can make an ISO image file from a Cisco WAAS recovery CD.
  - The **syslinux.cfg** file, which is also available on the Cisco WAAS Software Download page and on the Cisco WAAS release DVD.
  - **Unetbootin** utility for Microsoft Windows or Apple Mac, which is available from the Unetbootin Sourceforge website.

Procedure

Step 1 Transfer the software recovery files on to the computer, noting the directory in which they are stored.

Step 2 Insert the USB flash drive into a USB port on the computer.

Step 3 Open **My Computer** (Microsoft Windows) or **Disk Utility** (Apple MAC).

Step 4 Format the USB flash drive:

- For Microsoft Windows, right-click the **Removable Disk** (drive letter will vary with system) and select **Format**.
  - In the formatting tool, from the **File System** drop-down list, select **FAT32**.
  - In the **Format Options** sections, check the **Quick Format** check box, and then click **Start**.
  - After formatting is complete, close the formatting tool.

- For Apple MAC, select the USB drive on the left side of window, and use the **Erase** tab to format for use with **MS-DOS (FAT)**.

Step 5 Launch the **Unetbootin** utility.

Step 6 Select the **Diskimage** option and click the corresponding browse button (...) to select the **waas-rescue-cdrom-***x.x.x.x***-k9.iso** image file.

Step 7 Ensure that USB Drive is selected in the **Type** drop-down list and that the correct drive letter is selected for **Drive**.

Step 8 To install the bootable imate in the USB flash drive, click **OK**. After the installation has completed, click **Exit**.

Step 9 Drag a copy of the **syslinux.cfg** file into the USB flash drive and click **Yes** to confirm the replacement. This file replaces the existing file on the USB flash drive with the one customized for your Cisco WAAS system.

Step 10 Remove the USB flash drive from the computer.

Step 11 To continue reinstalling the system software from the prepared USB flash drive, follow the instructions described in Reinstalling the System Software on a Cisco WAE or Reinstalling the System Software on a Cisco NME-WAE.

Reinstalling the System Software on a Cisco WAE

Procedure

Step 1 Connect a serial console to the Cisco WAE and use the console for the following steps.

Step 2 Insert the software recovery CD-ROM in the CD drive of the Cisco WAEor, if the WAE uses a USB flash drive for recovery, insert a bootable USB flash drive with the software recovery files into the USB port of the device (see Preparing the USB Flash Drive, on page 528). WAE-294, WAE-594, WAE-694, WAVE-7541, WAVE-7571, and WAVE-8541 devices do not have CD drives; they use a USB flash drive for software recovery.

Step 3 Reboot the Cisco WAE. During the boot process, the boot loader pauses for 30 seconds and you must choose the VGA console if you are using Cisco vWAAS. The prompt is displayed as follows:

```
Type "serial" for WAE/WAVE appliance.
Type "vga" for vWAAS.
boot:
```

At the prompt, enter the **vga** commandto continue the boot process for the VGA console on Cisco vWAAS. After 30 seconds with no input, the boot process continues with the standard serial console for Cisco WAAS appliances.

After the WAE boots, you will see the following:

```
Installer Main Menu:
1. Configure Network
2. Manufacture flash
3. Install flash cookie
4. Install flash image from network
5. Install flash image from usb/cdrom
6. Install flash image from disk
7. Recreate RAID device (WAE-7541/7571/8541 only)
8. Wipe out disks and install .bin image
9. Exit (reboot)
Choice [0]:
```

Note The option numbers in the installer main menu may vary, depending on the WAAS software release being installed.

Step 4 Choose **Option 2, Manufacture flash** to prepare the flash memory.

This step prepares a cookie for the device and also retrieves the network configuration that was being used by the Cisco WAAS software. This network configuration is stored in the flash memory and is used to configure the network when the Cisco WAAS software boots up after installation.

Step 5 Choose **Option 3, Install flash cookie** to install the flash cookie that you prepared in the previous step.

Step 6 Choose **Option 5, Install flash image from usb/cdrom** to install the flash image from a CD-ROM or USB flash drive.

Step 7 (Optional) If you are working with a WAVE-7541, WAVE-7571, or WAVE-8541 device, choose **Option 7** to recreate the RAID array.

Step 8 Choose **Option 8, Wipe out disks and install .bin image** to wipe the disks and install the binary image.

This step prepares the disks by erasing them. The Cisco WAAS software image is installed.

Step 9 If you are using a USB flash drive to install the software, remove it from the device.

Step 10 Choose **Option 9, Exit (reboot)** to reboot the WAE.

After the Cisco WAE reboots, it runs the newly installed Cisco WAAS software. The Cisco WAE has a minimal network configuration and is accessible via the terminal console for further configuration.

Reinstalling the System Software on a Cisco NME-WAE

Procedure

Step 1 Log in to the Cisco router in which the Cisco NME-WAE module is installed, and reload the Cisco NME-WAE module:

```
router-2851> enable
router-2851# service-module integrated-Service-Engine 1/0 reload
```

Step 2 Immediately open a session in the module:

```
router-2851# service-module integrated-Service-Engine 1/0 session
```

Step 3 While the module is loading, you will see the following option during boot phase 3. Enter ******* as instructed:

```
[BOOT-PHASE3]: enter `***' for rescue image: ***
```

Step 4 The **Rescue Image** dialog box is displayed. The following example shows how to interact with the **Rescue Image** dialog box (user input is denoted by entries in bold typeface):

```
This is the rescue image. The purpose of this software is to let
you install a new system image onto your system's boot flash
device. This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.
To download an image from network, this software will request
the following information from you:
- which network interface to use
- IP address and netmask for the selected interface
- default gateway IP address
- FTP server IP address
- username and password on FTP server
- path to system image on server
Please enter an interface from the following list:
0: GigabitEthernet 1/0
1: GigabitEthernet 2/0
enter choice: 0
Using interface GigabitEthernet 1/0
Please enter the local IP address to use for this interface:
[Enter IP Address]: 10.1.13.2
Please enter the netmask for this interface:
[Enter Netmask]: 255.255.255.240
Please enter the IP address for the default gateway:
[Enter Gateway IP Address]: 10.1.13.1
Please enter the IP address for the FTP server where you wish
to obtain the new system image:
[Enter Server IP Address]: 10.107.193.240
Please enter your username on the FTP server (or 'anonymous'):
[Enter Username on server (e.g. anonymous)]: username
Please enter the password for username 'username' on FTP server:
Please enter the directory containing the image file on the FTP server:
[Enter Directory on server (e.g. /)]: /
Please enter the file name of the system image file on the FTP server:
[Enter Filename on server]: WAAS-6.4.3.10-K9.sysimg
Here is the configuration you have entered:
Current config:
IP Address: 10.1.13.2
Netmask: 255.255.255.240
Gateway Address: 10.1.13.1
Server Address: 10.107.193.240
Username: username
Password: *********
Image directory: /
Image filename: WAAS-5.1.1.10-K9.sysimg
Attempting download...
Downloaded 15821824 byte image file
A new system image has been downloaded.
You should write it to flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no')]: yes
Ok, writing new image to flash
.................................................................................. done.
Finished writing image to flash.
Enter 'reboot' to reboot, or 'again' to download and install a new image:
[Enter reboot confirmation ('reboot' or 'again')]: reboot
Restarting system. After the module reboots, install the .bin image from an HTTP server:
NM-WAE-1# copy http install 10.77.156.3 /waas WAAS-6.4.3.10-k9.bin
 Reload the module:
NM-WAE-1# reload
```

Step 5 After the module reboots, it runs the newly installed Cisco WAAS software.

```
NM-WAE-1# copy http install 10.77.156.3 /waas WAAS-6.4.3.10-k9.bin
```

Step 6 Reload the module.

```
NM-WAE-1# reload
```

Ensuring that RAID Pairs Rebuild Successfully

RAID pairs will rebuild on the next reboot after you run the **restore factory-default** EXEC command, replace or add a hard disk drive, delete disk partitions, or reinstall Cisco WAAS from the booted recovery CD-ROM or USB flash drive.

Note You must ensure that all the RAID pairs have completed rebuilding *before* you reboot your Cisco WAE device. If you reboot while the device is still rebuilding, you risk corrupting the file system.

To view the status of the drives and check if the RAID pairs are in **Normal Operation** or in **Rebuilding** status, run the show disk details EXEC command. When you see that RAID is rebuilding, you must let it complete that rebuild process. This rebuild process can take several hours.

If you do not wait for the RAID pairs to complete the rebuild process before you reboot the device, you may see the following symptoms, indicating a problem:

- The device is offline in the Cisco WAAS Central Manager GUI.
- CMS cannot be loaded.
- Error message stating that the file system is read-only is displayed.
- The syslog contains errors such as:
  - **Aborting journal on device md2**
  - **Journal commit I/O error**
  - **Journal has aborted**
  - **ext3_readdir: bad entry in directory**
- Other unusual behaviors related to disk operations or the inability to perform them are visible.

If you encounter any of these symptoms, reboot the Cisco WAE and wait until the RAID rebuild finishes normally.

Recovering the System Software

Before you begin

Cisco WAAS devices have a resident rescue system image that is invoked if the image in flash memory is corrupted. A corrupted system image can result from a power failure that occurs while a system image is being written to flash memory. The rescue image can help you download a system image to the main memory of the device and write it to flash memory.

Note The system image used depends on your device. For all Cisco WAVE and Cisco WAE devices (64-bit platforms), use the 64-bit system image (with **x86_64** in its name). For all other devices, use the 32-bit system image named without this designator. An NPE image that has the disk encryption feature disabled for use in countries where disk encryption is not permitted is provided.

Procedure

Step 1 Download the system image file (***.sysimg**) to a host that is running an FTP server.

Step 2 Establish a console connection to the Cisco WAAS device and open a terminal session.

Step 3 To reboot the device, toggle the **power on/off switch**.

After a few seconds, the bootloader pauses and prompts you to enter **1** to boot Cisco WAAS, **r** to boot the rescue image, **x** to reboot, or **9** to escape to the loader prompt. You have 10 seconds to respond before the normal boot process continues.

Step 4 To boot the rescue image, enter **r**.

The **Rescue Image** dialog box is displayed and differs depending on whether your Cisco WAAS device was initially manufactured with Cisco WAAS Version 4.x or 5.x. **Step 5** describes the rescue image on a device that was initially manufactured with Cisco WAAS Version 5.x. **Step 6** describes the rescue image on a device that was initially manufactured with Cisco WAAS Version 4.x.

Step 5 If you see the following output (from a device that was initially manufactured with Cisco WAAS Version 5.x), log in and run the **copy install** EXEC command to install the Cisco WAAS system software image (**.bin** file), as shown in the following example (user input is denoted by entries in bold typeface):

```
The device is running WAAS rescue image. WAAS functionality is unavailable
in a rescue image. If the rescue image was loaded by accident, please reload
the device. If the rescue image was loaded intentionally to reinstall WAAS software
please use the following command:
copy [ftp|http|usb] install ...
SW up-to-date
...
Cisco Wide Area Virtualization Engine Console
Username: admin
Password:
System Initialization Finished.
WAVE# copy ftp install 172.16.10.10 / waas-universal-5.1.1.12-k9.bin
...
Installing system image to flash... Creating backup of database content before database
upgrade.
The new software will run after you reload.
WAVE# reload
Proceed with reload?[confirm]yes
Shutting down all services, will timeout in 15 minutes.
reload in progress ..Restarting system.
```

Step 6 If you see the following output (from a device that was initially manufactured with Cisco WAAS Version 4.x), log in and install the Cisco WAAS system image (**.sysimg** file), as shown in the following example (user input is denoted by entries in bold typeface):

```
This is the rescue image. The purpose of this software is to let
you download and install a new system image onto your system's
boot flash device. This software has been invoked either manually
(if you entered `***' to the bootloader prompt) or has been
invoked by the bootloader if it discovered that your system image
in flash had been corrupted.
To download an image, this software will request the following
information from you:
- which network interface to use
- IP address and netmask for the selected interface
- default gateway IP address
- server IP address
- which protocol to use to connect to server
- username/password (if applicable)
- path to system image on server
Please enter an interface from the following list:
0: GigabitEthernet 0/0
1: GigabitEthernet 0/1
enter choice: 0
Using interface GigabitEthernet 0/0
Please enter the local IP address to use for this interface:
[Enter IP Address]: 172.16.22.22
Please enter the netmask for this interface:
[Enter Netmask]: 255.255.255.224
Please enter the IP address for the default gateway:
[Enter Gateway IP Address]: 172.16.22.1
Please enter the IP address for the FTP server where you wish
to obtain the new system image:
[Enter Server IP Address]: 172.16.10.10
Please enter your username on the FTP server (or 'anonymous'):
[Enter Username on server (e.g. anonymous)]: anonymous
Please enter the password for username 'anonymous' on FTP server:
Please enter the directory containing the image file on the FTP server:
[Enter Directory on server (e.g. /)]: /
Please enter the file name of the system image file on the FTP server:
[Enter Filename on server (e.g. WAAS-x86_64-4.x.x-K9.sysimg)]:
waas-x86_64-5.1.1.12-k9.sysimg
Here is the configuration you have entered:
Current config:
IP Address: 172.16.22.22
Netmask: 255.255.255.224
Gateway Address: 172.16.22.1
Server Address: 172.16.10.10
Username: anonymous
Password:
Image directory: /
Image filename: waas-x86_64-5.1.1.12-k9.sysimg
Attempting download...
Downloaded 31899648 byte image file
A new system image has been downloaded.
You should write it to flash at this time.
Please enter 'yes' below to indicate that this is what you want to do:
[Enter confirmation ('yes' or 'no')]: yes
Ok, writing new image to flash
Finished writing image to flash.
Enter 'reboot' to reboot, or 'again' to download and install a new image:
[Enter reboot confirmation ('reboot' or 'again')]: reboot
Restarting system.
Booting system, please wait.........
```

Step 7 Log in to the device with the username **admin**. To verify that you are running the correct version, run the **show version** EXEC command:

```
Username: admin
Password:
Console# show version
Cisco Wide Area Application Services Software (WAAS)
Copyright (c) 1999-2020 by Cisco Systems, Inc.
Cisco Wide Area Application Services (universal-k9) Software Release 6.4.3 (build b49 Jan
14 2020)
Version: oe294-5.1.1.12
Compiled 12:23:45 Jan 14 2020 by dsmith
Device Id: 50:3d:e5:9c:8f:a5
System was restarted on Tue Jan 14 16:35:50 2020.
System restart reason: called via cli.
The system has been up for 8 hours, 10 minutes, 19 seconds.
```

Resetting a Lost Administrator Password

Before you begin

If an administrator password is forgotten, lost, or misconfigured, you will have to reset the password on the device.

Note You cannot restore a lost administrator password. You must reset the password, as described in this procedure.

Procedure

Step 1 Establish a console connection to the device and open a terminal session.

Step 2 Reboot the device.

While the device is rebooting, watch for the following prompt, and press **Enter** when you see it:

```
Cisco WAAS boot:hit RETURN to set boot flags:0009
```

Step 3 When prompted to enter bootflags, enter the value **0x8000**.

```
Available boot flags (enter the sum of the desired flags):
0x4000 - bypass nvram config
0x8000 - disable login security
[CE boot - enter bootflags]:0x8000
You have entered boot flags = 0x8000
Boot with these flags? [yes]:yes
[Display output omitted]
Setting the configuration flags to 0x8000 lets you into the system, bypassing all
security. Setting the configuration flags field to 0x4000 lets you bypass the NVRAM
configuration.
```

Step 4 When the device completes the boot sequence, you are prompted to enter the username to access the CLI. Enter the default administrator username (**admin**).

```
Cisco WAE Console
Username: admin
```

Step 5 When you see the CLI prompt, set the password for the user using the username passwd command in global configuration mode:

```
WAE# configure
WAE(config)# username admin passwd
```

This command invokes interactive password configuration. Follow the CLI prompts.

Step 6 Save the configuration change:

```
WAE(config)# exit
WAE# write memory
```

Step 7 (Optional) Reboot your device:

```
WAE# reload
```

Rebooting is optional. However, we recommend that you reboot to ensure that the boot flags are reset, and to ensure that subsequent console administrator logins do not bypass the password check.

Note In the Cisco WAAS software, the bootflags are reset to **0x0** on every reboot.

Recovering from Missing Disk-Based Software

Before you begin

This task describes how to recover from the following types of disk drive issues:

- Your Cisco WAAS device contains a single disk drive that needs to be replaced due to a disk failure.
- Your Cisco WAAS device contains two disk drives and you intentionally deleted the disk partitions on both drives (**disk00** and **disk01**).

  Systems with two or more disk drives are normally protected automatically by RAID-1 on critical system partitions. Therefore, the procedures in this section do not have to be followed when replacing a disk drive in a multidrive system.

Procedure

Step 1 Deactivate the device by completing the following steps:

a) From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.

b) Choose *device-name* > **Activation**.

   The **Device Activation** window appears.

c) Uncheck the Activate check box, and then click Submit.

   The device is deactivated.

Step 2 Power down the device and replace the failed hard drive.

Step 3 Power on the device.

Install the Cisco WAAS software. For more information on initial configuration, see the Cisco Wide Area Application Services Quick Configuration Guide .

Step 4 Use the CMS identity recovery procedure to recover the device CMS identity and associate this device with the existing device record on the Cisco WAAS Central Manager. For more information, see Recovering Cisco WAAS Device Registration Information.

Recovering Cisco WAAS Device Registration Information

Before you begin

Device registration information is stored both on the device itself and on the Cisco WAAS Central Manager. If a device loses its registration identity or needs to be replaced because of a hardware failure, the Cisco WAAS network administrator can issue a CLI command to recover the lost information, or in the case of adding a new device, assume the identity of the failed device.

Procedure

Step 1 To mark the failed device as **Inactive** and Replaceable by completing the following steps:

a) From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.
b) Choose *device-name* > **Activation**.
c) Uncheck the **Activate** check box. The window refreshes, displaying a check box for marking the device as replaceable.
d) Check the **Replaceable** check box, and click **Submit**.

Note This check box appears in the Cisco WAAS Central Manager GUI only when the device is inactive.

Step 2 If the failed device is configured as a nonoptimizing peer with another device, disable the peer settings on the other device.

A message is displayed if the failed device is a nonoptimizing peer, indicating that the device is a nonoptimizing peer. When a device is replaced, its device ID changes and therefore, the nonoptimizing peer configuration must be updated.

a) From the Cisco WAAS Central Manager menu, choose **Configure** > **Global** > **Peer Settings**.

   The **Peer Settings** window for all the devices appears.

b) Click the **Edit** icon next to the nonoptimizing device identified in the message, which will appear in red because its peer is unknown.

   The **Peer Settings** window for that device appears.

c) Click the **Remove Device Settings** icon in the taskbar.
d) Click **Submit**.

Step 3 Configure a system device recovery key as follows:

a) From the Cisco WAAS Central Manager menu, choose **Configure** > **Global** > **System Properties**.
b) Click the **Edit** icon next to the **System.device.recovery.key** property.

   The **Modifying Config Property** window appears.

c) Enter the password in the **Value** field, and click **Submit**.

   The default password is **default**.

Step 4 Configure the basic network settings for the new device.

Step 5 Open a Telnet session to the device CLI and enter the **cms recover identity** *keyword* EXEC command. Here, *keyword* is the device recovery key that you configured in the Cisco WAAS Central Manager GUI.

When the Cisco WAAS Central Manager receives the recovery request from the Cisco WAAS device, it searches its database for the device record that meets the following criteria:

- The record is inactive and replaceable.
- The record has the same hostname or primary IP address, as given in the recovery request.

If the recovery request matches the device record, then the Cisco WAAS Central Manager updates the existing record and sends the requesting device a registration response. The replaceable state is cleared so that no other device can assume the same identity. When the Cisco WAAS device receives its recovered registration information, it writes it to file, initializes its database tables, and starts.

Step 6 To enable the CMS service on the device, run the following commands:

```
WAE# config
WAE(config)# cms enable
WAE(config)# exit
```

Step 7 Activate the device:

a) From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name*.
b) Choose *Device Name* > **Activation**. The Cisco WAAS device status should be Online.
c) Check the **Activate** check box, and click **Submit**.

Step 8 (Optional) Reconfigure the device peer settings, if the device was configured as a nonoptimizing peer with another device. For more information, see the chapter "Configuring Traffic Interception."

Step 9 Save the device configuration settings by entering the **copy running-config startup-config** EXEC command.

Disk Maintenance for RAID Systems

This section contains the following topics:

About Disk Maintenance for RAID-1 Systems

Cisco WAAS supports hot-swap functionality for both failed disk replacement and scheduled disk maintenance. When a disk fails, Cisco WAAS automatically detects the disk failure, marks the disk as bad, and removes the disk from the RAID-1 volume. To schedule disk maintenance, you must manually shut down the disk.

You must wait for the disk to be completely shut down before you physically remove the disk from the Cisco WAE. When the RAID removal process is complete, Cisco WAAS generates a disk failure alarm and trap. In addition, a syslog error message is logged.

Note If the removal event (such as, a disk failure or software shutdown) occurs while the RAID array is in the rebuild process, the RAID removal process may take up to 1 minute to complete. The duration of this process depends on the size of the disk.

If the Cisco WAAS software removes a failed disk during the RAID rebuild process, a RAID rebuild failure alarm is generated. If you administratively shut down the disk during the RAID rebuild process, a RAID rebuild abort alarm is generated instead.

When you install a replacement disk, the Cisco WAAS software detects the replacement disk and performs compatibility checks on the disk, initializes the disk by creating partitions, and adds the disk to the software RAID to start the RAID rebuild process.

If the newly inserted disk has the same disk ID as a disk that was previously marked bad in the same physical slot, then the disk will not be mounted, and the post-replacement checks, initialization, and RAID rebuilding will not occur.

A newly installed disk must be of the same type and speed as the old disk and it must meet the following compatibility requirements:

- If the replacement disk is for **disk00**, **disk02**, or **disk04** of a RAID pair, the replacement disk must be the same size as the running disk in the array.
- If the replacement disk is for **disk01**, **disk03**, or **disk05** of a RAID pair, then the replacement disk must have the same or greater RAID capacity as the running disk in the array.

Compatibility checks, which are a part of the hot-swap process, check for capacity compatibility. Incompatibility generates an alarm and aborts the hot-swap process.

Performing Disk Maintenance for RAID-1 Systems

Procedure

Step 1 Manually shut down the disk.

a) Enter global configuration mode and then enter the **disk disk-name** *diskxx* **shutdown** global configuration command:

```
WAE# configure
WAE(config)# disk disk-name diskxx shutdown
```

b) Wait for the disk to be completely shut down before you physically remove the disk from the WAE. When the RAID removal process is complete, Cisco WAAS generates a disk failure alarm and trap. In addition, a syslog error message is logged.

Note We recommend that you disable the **disk error-handling reload** option if it is enabled because it is not necessary to power down the system to remove a disk.

Step 2 Insert a replacement disk into the slot in the WAE. The replacement disk must have a disk ID number that is different from the disk that it is replacing.

Step 3 To re-enable the disk, run the **no disk disk-name** *diskxx* **shutdown** global configuration command.

Removing and Replacing Disks in RAID-5 Systems

Procedure

Step 1 Enter the **disk disk-name** *diskxx* **replace** command in EXEC mode from the Cisco WAAS CLI on the Cisco WAE.

Step 2 Verify that the disk drive *diskxx* is in **Defunct** state by entering the **show disks details** command in EXEC mode. The RAID logical drive is in **Critical** state at this point.

Step 3 Move the handle on the drive to the open position (perpendicular to the drive).

Step 4 Pull the hot-swap drive assembly from the bay.

Step 5 Wait for one minute and then insert the new drive into the same slot by aligning the replacement drive assembly with guide rails in the bay and sliding the drive assembly into the bay until it stops. Make sure that the drive is properly seated in the bay.

Step 6 Close the drive handle.

Step 7 Check the hard disk drive status LED to verify that the hard disk drive is operating correctly. If the amber hard disk drive status LED for a drive is lit continuously, that drive is faulty and must be replaced. If the green hard disk drive activity LED is flashing, it means the drive is being accessed.

Note If a disk is shut down using the **disk disk-name** *diskxx* **replace** EXEC command and the same disk is removed and reinserted, it can be re-enabled by using the **disk disk-name** *diskxx* **enable force** EXEC command. This process is applicable even if the disk is not removed and needs to be re-enabled. This command is not applicable if a new disk is inserted.

Step 8 Wait for 1 minute. To verify that the replaced disk drive is in the **Rebuilding** state, run the **show disk details** command in EXEC mode.

Note The **ServeRAID** controller automatically starts the rebuild operation when it detects the removal and reinsertion of a drive that is a part of the logical RAID drive.

Step 9 Wait until the rebuild operation is complete. To check if the rebuild operation is complete, run the **show disk details** command in EXEC mode. The physical drive state will be **Online** and the RAID logical drive state will be **Okay** after the rebuild operation is completed.

Step 10 Reinstall the software on the device. For more information, see Upgrading the Cisco WAAS Central Manager, on page 519

Step 11 Add the license. For more information, see Managing Cisco WAAS Software Licenses, on page 291 in the chapter "Configuring Other System Settings."

Step 12 Register the Cisco WAE to the Cisco WAAS Central Manager.

A 300-GB SAS drive may take up to 5 hours to finish rebuilding.

Recreating the RAID-5 Array in RAID-5 Systems

Before you begin

If you have multiple disk failures and your RAID-5 logical status is **Offline**, you must recreate the RAID-5 array.

Procedure

Step 1 From the global configuration mode, run the **disk logical shutdown** command to disable the RAID-5 array.

Step 2 To save the running configuration to NV-RAM, run the **write** command in EXEC mode.

Step 3 To reload the system, run the **reload** command in EXEC mode.

Step 4 To check the system configuration after the system is reloaded, run the **show disks details** command in EXEC mode. At this point, the disks are not mounted and the logical RAID drive should be in the **Shutdown** state.

Step 5 To recreate the RAID-5 array, run the **disk recreate-raid** command in EXEC mode.

Step 6 To disable the logical disk shutdown configuration: After successful execution of the **disk recreate-raid** command, enter global configuration mode and run the **no disk logical shutdown** command.

Step 7 To save the configuration to NV-RAM, run the **write** command in EXEC mode.

Step 8 To reload the system, run the **reload** command in EXEC mode.

Step 9 To check the system configuration after the system is reloaded, run the **show disks details** command in EXEC mode.

At this point, the disks should be mounted and the logical RAID drive should not be in the **Shutdown** state.

Step 10 Wait until the rebuild operation is complete. To check if the rebuild operation is complete, run the **show disks details** command in EXEC mode. The physical drive state will be **Online** and the RAID logical drive state will be **Okay** after the rebuild operation is completed.

It takes several hours to finish rebuilding the RAID-5 array.

Step 11 After a multiple disk failure or RAID controller failure, and after the drives are replaced and the RAID disk is rebuilt, the logical disk may remain in the error state. To re-enable the disk, run the **no disk logical shutdown force** command, and then reload the WAE.

Configuring the Cisco WAAS Central Manager Role

This section contains the following topics:

Primary and Standby Cisco WAAS Central Managers

The Cisco WAAS software implements a Standby Cisco WAAS Central Manager. This process allows you to maintain a copy of the Cisco WAAS network configuration on a second Cisco WAAS Central Manager device. If the Primary Cisco WAAS Central Manager fails, the Standby can be used to replace the Primary.

For interoperability, when a Standby Cisco WAAS Central Manager is used, it must be at the same software version as the Primary Cisco WAAS Central Manager to maintain the full Cisco WAAS Central Manager configuration. Otherwise, the Standby Cisco WAAS Central Manager detects this status and does not process any configuration updates that it receives from the Primary Cisco WAAS Central Manager until the problem is corrected.

There is no specified number of Standby Central Managers for meeting redundancy purposes. Regular backup of CMS database content provides better reliability.

Note Primary and Standby Central Managers communicate on TCP ports 443 and 8443. If your network includes a firewall between primary and standby Central Managers, you must configure the firewall to allow traffic on TCP ports 443 and 8443 so that the Central Managers can communicate and stay synchronized.

Converting a Cisco WAE to a Standby Cisco WAAS Central Manager

Before you begin

There are two types of Cisco WAAS software files:

- **Universal**: Includes Central Manager, Application Accelerator, and AppNav Controller functionality.
- **Accelerator only**: Includes Application Accelerator and AppNav Controller functionality only. If you want to change an Application Accelerator or AppNav Controller to a Central Manager, you must use the Universal software file.

If the Cisco WAE is operating with an **Accelerator** only image, you cannot convert it to a Central Manager until after you update it with the Universal software file, reload the device, change the device mode to **central-manager**, and then reload the device again. For information on updating a Cisco WAE, see Upgrading the Cisco WAAS Software.

To check if the WAE is running an Accelerator only image, run the **show version** EXEC command. To display the image type, run the **show running-config** EXEC command.

Procedure

Step 1 To deregister the Cisco WAE from the Cisco WAAS Central Manager, run the **cms deregister force** EXEC command.

This command cleans up any previous association to any other Cisco WAAS Central Manager.

Step 2 To configure the device mode as **central-manager**, run the **device mode central-manager** global configuration command:

```
WAE# configure
WAE(config)# device mode central-manager
```

Step 3 You must reload the device to apply the changes. For more information, see see Rebooting a Device, on page 550.

Step 4 To configure the Cisco WAAS Central Manager role as Standby, run the **central-manager role standby** command.

Step 5 To configure the address of the Primary Cisco WAAS Central Manager, run the **central-manager address** *cm-primary-address* command:

Step 6 To enable the CMS service, run the **cms enable** command.

Converting a Primary Cisco WAAS Central Manager to a Standby Cisco WAAS Central Manager

Procedure

Step 1 To deregister the Cisco WAAS Central Manager, run the **cms deregister** EXEC command:

This command cleans up any previous association to any other Cisco WAAS Central Manager.

Step 2 To configure the Cisco WAAS Central Manager role as Standby, run the **central-manager role standby** global configuration command.

Step 3 To configure the address of the Primary Central Manager, run the **central-manager address** *cm-primary-address* global configuration command.

Step 4 To enable the CMS service, run the **cms enable** global configuration command.

Converting a Standby Cisco WAAS Central Manager to a Primary Cisco WAAS Central Manager

If your Primary Cisco WAAS Central Manager becomes inoperable, you can manually reconfigure one of your warm Standby Cisco WAAS Central Managers to be the Primary Cisco WAAS Central Manager. To configure the new rol, run the **central-manager role primary** global configuration command as follows:

```
WAE# configure
WAE(config)# central-manager role primary
```

This command changes the role from Standby to Primary and restarts the management service to recognize the change.

If a previous failed Primary Central Manager becomes available again, you can recover it to make it the Primary Cisco WAAS Central Manager again. For more information, see Cisco WAAS Central Manager Failover and Recovery, on page 545.

If you switch a warm Standby Cisco WAAS Central Manager to Primary while your Primary Cisco WAAS Central Manager is still online and active, both Cisco WAAS Central Managers detect each other, automatically shut themselves down, and disable management services. The Cisco WAAS Central Managers are switched to halted, which is automatically saved in flash memory.

To return halted Cisco WAAS Central Managers to an **online** status, decide which Cisco WAAS Central Manager should be the Primary and which should be the Standby. On the Primary, run the following CLI commands:

```
WAE# configure
WAE(config)# central-manager role primary
WAE(config)# cms enable
```

On the Standby, run the following CLI commands:

```
WAE# configure
WAE(config)# central-manager role standby
WAE(config)# central-manager address cm-primary-address
WAE(config)# cms enable
```

Switching Both the Cisco WAAS Central Manager Roles

Before you begin

Caution When you switch a Cisco WAAS Central Manager from Primary to Standby, the configuration on the Cisco WAAS Central Manager is erased. The Cisco WAAS Central Manager, after becoming a Standby, will begin replicating its configuration information from the current Primary Cisco WAAS Central Manager. If Standby and Primary units are not synchronized before switching roles, important configuration information can be lost.

Procedure

Step 1 Ensure that your Cisco WAAS Central Manager devices are running the same version of Cisco WAAS software.

Step 2 Synchronize the physical clocks on both devices so that both the Cisco WAAS Central Managers have the same Coordinated Universal Time (UTC) configured.

Step 3 To ensure that the Standby is synchronized with the Primary, check the status of the following items:

a) Check the online status of your devices.

The original Standby Cisco WAAS Central Manager and all currently active devices should be showing as **online** in the Cisco WAAS Central Manager GUI. This step ensures that all other devices know about both Cisco WAAS Central Managers.

b) Check the status of recent updates from the Primary WAAS Central Manager.

To check the time of the last update, run the **show cms info** EXEC command. To be current, the value of the **Time of last config-sync** field should be between **1** and **5 minutes** old. This time range verifies that the Standby Cisco WAAS Central Manager has fully replicated the Primary Cisco WAAS Central Manager configuration.

If the update time is not current, determine whether or not there is a connectivity problem or if the Primary Cisco WAAS Central Manager is down. Fix the problem, if necessary, and wait until the configuration has replicated, as indicated by the time of the last update.

Step 4 Switch roles in the following order:

a) Disable the original **Primary** Cisco WAAS Central Manager.

```
WAE2(config)# no cms enable
```

b) Switch the original **Standby** Cisco WAAS Central Manager to **primary mode**:

```
WAE2# configure
WAE2(config)# central-manager role primary

WAE1-CM3(config)# central-manager role standby
Switching CM to standby will cause all configuration settings made on this CM to be
lost.
Please confirm you want to continue (yes|no) [no]?yes
Restarting CMS services
```

c) Wait until the original **Standby** Cisco WAAS Central Manager is completely up and that you have verified that it is now working as the **Primary** Cisco WAAS Central Manager.

d) Switch the original **primary** Cisco WAAS Central Manager to **standby mode**:

```
WAE1# configure
WAE1(config)# central-manager role standby
WAE1(config)# cms enable
```

The CMS service is restarted automatically after you configure a role change.

Cisco WAAS Central Manager Failover and Recovery

Before you begin

If your Primary Cisco WAAS Central Manager becomes inoperable, you can reconfigure one of your Standby Central Managers to be the Primary Central Manager, and later, when the failed Cisco WAAS Central Manager becomes available, you can reconfigure it to be the Primary again.

Procedure

Step 1 Convert a Standby Cisco WAAS Central Manager to be the Primary Cisco WAAS Central Manager, as described in Converting a Standby Cisco WAAS Central Manager to a Primary Cisco WAAS Central Manager, on page 543.

Step 2 When the failed Cisco WAAS Central Manager becomes available again, configure it as a Standby Central Manager, as described in Converting a Primary Cisco WAAS Central Manager to a Standby Cisco WAAS Central Manager, on page 542, beginning with **Step 2**. Skip **Step 1** and do not use the **cms deregister** EXEC command.

Step 3 Switch both the Cisco WAAS Central Manager roles, as described in Switching Both the Cisco WAAS Central Manager Roles, on page 544.

Note In some scenarios, when a Standby Cisco WAAS Central Manager is registered newly with a Cisco WAAS Central Manager that is already managing more than 1000 Cisco WAEs, the devices may go off line. To avoid this, in case of large deployments, we recommend that you register the Standby Cisco WAAS Central Manager to the Primary Cisco WAAS Central ManagerCentral Manager at the beginning of the deployment, so that in case of an unexpected fail over the Standby takes up the Primary role.

Note When a backup operation is in progress on a Standby Cisco WAAS Central Manager that is supporting a Primary Cisco WAAS Central Manager managing more than 1000 Cisco WAEs: the Standby Cisco WAAS Central Manager goes off line if the backup operation takes more than 10 minutes. Additionally, you will not be able to login to the Primary Cisco WAAS Central Manager GUI when a backup operation is in progress.

Enabling Disk Encryption

Disk encryption addresses the need to securely protect sensitive information that flows through deployed Cisco WAAS systems and that is stored in Cisco WAAS persistent storage. The disk encryption feature includes two aspects: the actual data encryption on the Cisco WAE disk and the encryption key storage and management.

When you enable disk encryption, all the data in Cisco WAAS persistent storage will be encrypted. The encryption key for unlocking the encrypted data is stored in the Cisco WAAS Central Manager, and key management is handled by the Cisco WAAS Central Manager. When you reboot the Cisco WAE after configuring disk encryption, the Cisco WAE retrieves the key from the Cisco WAAS Central Manager automatically, allowing normal access to the data that is stored in Cisco WAAS persistent storage.

Note If a Cisco WAE is unable to reach the Cisco WAAS Central Manager during a reboot, it will do everything except mount the encrypted partitions. In this state, all traffic will be handled as pass-through. After communication with the Cisco WAAS Central Manager is restored (and the encryption key is obtained), the encrypted partitions are mounted. There is no loss of cache content.

Disk encryption requirements are as follows:

- You must have a Cisco WAAS Central Manager configured for use in your network.
- Your Cisco WAE devices must be registered with the Central Manager.
- Your Cisco WAE devices must be online (have an active connection) with the Cisco WAAS Central Manager. This requirement applies only if you are enabling disk encryption.
- You must reboot your Cisco WAE for the disk encryption configuration to take effect.

After you reboot your Cisco WAE, the encryption partitions are created using the new key, and any previously existing data is removed from the partition.

Any change to the disk encryption configuration, whether to enable or disable encryption, causes the disk to clear its cache. This feature protects sensitive customer data from being decrypted and accessed should the WAE ever be stolen.

If you enable disk encryption and then downgrade to a software version that does not support this feature, you will not be able to use the data partitions. In such cases, you must delete the disk partitions after you downgrade.

To enable and disable disk encryption from the Cisco WAAS Central Manager GUI, choose **Devices >** *device-name*, then choose **Configure > Storage > Disk Encryption**. To enable disk encryption, check the **Enable** check box and click **Submit**. This check box is unchecked by default. To disable disk encryption, uncheck the **Enable** check box and click **Submit**.

To enable and disable disk encryption from the Cisco WAE CLI, run the **disk encrypt** global configuration command.

Note If you are using an NPE image, note that the disk encryption feature is disabled in countries where disk encryption is not permitted.

When you enable or disable disk encryption, the file system is reinitialized during the first subsequent reboot. Reinitialization may take from ten minutes to several hours, depending on the size of the disk partitions. During this time, the Cisco WAE will be accessible, but it will not provide any service.

If you change the Cisco WAAS Central Manager IP address, or if you relocate the Cisco WAAS Central Manager, or replace one Cisco WAAS Central Manager with another Cisco WAAS Central Manager that has not copied over all of the information from the original Cisco WAAS Central Manager, and you reload the Cisco WAE when disk encryption is enabled, the Cisco WAE file system will not be able to complete the reinitialization process or obtain the encryption key from the Cisco WAAS Central Manager.

If the Cisco WAE fails to obtain the encryption key, disable disk encryption by running the **no disk encrypt enable** global configuration command from the CLI, and reload the Cisco WAE. Ensure connectivity to the Cisco WAAS Central Manager before you enable disk encryption and reload the Cisco WAE. This process will clear the disk cache.

Note When a Standby Cisco WAAS Central Manager has been in service for at least two times, the datafeed poll rate time interval (approximately 10 minutes), and has received management updates from the Primary Cisco WAAS Central Manager, the updates will include the latest version of the encryption key. Failover to the standby in this situation occurs transparently to the Cisco WAE. The datefeed poll rate defines the interval for the Cisco WAE to poll the Cisco WAAS Central Manager for configuration changes. This interval is **300 seconds** by default.

To view the encryption status details, run the **show disks details** EXEC command. While the file system is initializing, the **show disks details** command displays the message: **System initialization is not finished, please wait...**. You can also view the disk encryption status, whether it is enabled or disabled, in the Cisco WAAS Central Manager GUI's **Device Dashboard** window.

Configuring a Disk Error-Handling Method

Before you begin

Note Configuring and enabling disk error handling is no longer necessary for devices that support disk hot-swap. In Cisco WAAS Version 4.0.13 and later, the software automatically removes from service any disk with a critical error.

If the bad disk drive is a critical disk drive, and the automatic reload feature is enabled, then the Cisco WAAS software marks the disk drive bad and the Cisco WAAS device is automatically reloaded. After the Cisco WAAS device is reloaded, a syslog message and an SNMP trap are generated.

Note The automatic reload feature is automatically enabled, but is not configurable on devices running Cisco WAAS Version 4.1.3 and later.

Procedure

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

Step 2 Choose **Configure > Storage > Disk Error Handling**.

The **Disk Error Handling Current Settings** window appears.

Step 3 The **Disk Error Handling Current Settings** window has two check boxes:

- To enable the window for configuration, check the **Enable** check box.
- Check the **Enable Disk Error Handling Remap**. This forces the disks to attempt to remap disk errors automatically. This is checked (enabled) by default.

Step 4 To save the settings, click **Submit**.

Enabling Data Cache Management

Before you begin

The Cisco WAAS Central Manager allows you to configure existing Akamai Cache and Object Cache data partitions by increasing or decreasing the cache sizes whenever needed on the existing Cisco WAE system. Note the following scenarios with respect to Cisco WAAS devices, software version and new or subsequent Data Cache Management configuration.

Upgrading Cisco WAE-294, WAE-594, or WAE-694 with Cisco WAAS Software Version 6.1.1 and later:

- When you upgrade to Cisco WAAS Software Version 6.1.1 and later and configure the device(s) for data cache management for the first time and perform a reload.
- All the data-cache is lost on reload.

Upgrading Cisco vWAAS or Cisco ISR-WAAS for Cisco WAAS Software Version 6.x:

- When you upgrade to Cisco WAAS Software Version 6.1.1 and later, and configure the device/s for data cache management for the first time and perform a reload, both data and system partitions are re-created.
- Logs and Data Cache are cleaned up, but software version and Cisco WAAS Central Manager registration information is preserved.

Fresh deployment in all models:

- When you do a fresh deployment of Cisco WAAS Software Version 6.1.1 and later, and configure the device/s for data cache management for the first time and perform a reload, only Akamai and object-cache data is lost.

Second or subsequent configuration in all models:

- Configuring Data Cache Management for second or subsequent times cleans only the Akamai and Object cache partitions. All other partitions are retained.

Limitations for Data Cache Management

- If you want to configure data cache management from the Cisco WAAS Central Manager GUI, both the Cisco WAAS Central Manager and the devices registered with it need to be running Cisco WAAS Version 6.1.1 or later.
- The device needs to be in **Application Accelerator** mode to configure Akamai and Object Cache capability.
- The Cisco WAAS Central Manager supports mixed mode of devices in different versions. When you configure Data Cache Management at the **Device** level, the configurations apply only to the devices running Cisco WAAS Version 6.1.1 and later and not to those earlier than Cisco WAAS Version 6.1.1.
- Data Cache Management is not supported on the following hardware platforms: Cisco WAVE-7541, WAVE-7571 and WAVE-8541, Cisco vWAAS-12000 and vWAAS-50000.

Procedure

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

Step 2 Choose **Configure** > **Storage** > **Cache Size Management**.

The **Cache Size Management** window appears.

Step 3 Select from the available options.

- **Default**: Sets the available partition size for Akamai cache and Object cache according to predefined values.
- **Akamai-Object Cache-Equal**: Sets the available partition size to 50% each, for both Akamai cache and Object cache.
- **Akamai-weight1**: Sets the partition size to 60% for Akamai cache and 40% for Object cache.
- **Akamai-weight2**: Sets the partition size to 80% for Akamai cache and 20% for Object cache.
- **ObjectCache-weight1**: Sets the partition size to 60% for Object cache and 40% for Akamai cache.
- **ObjectCache-weight2**: Sets the partition size to80% for Object cache and 20% for Akamai cache.

Step 4 To save the settings, click **Submit**.

Consider the following:

- The data partition is effective only after the device is reloaded.
- To enable data cache management the CLI, run the **disk cache enable** global configuration command.
- To view the data cache details, choose choose **Devices** > *device-name* or **Device Groups** > *device-group-name* > **Monitor** > **CLI Commands** > **Show Commands** and select the **show disk cache-details** command. The cache details are displayed for devices that are running Cisco WAAS Version 6.1.1.

Note When you downgrade a device from Cisco WAAS Version 6.1.1 to any 5.x.x version, object-cache is no longer valid. As a result the associated CLIs are also not visible on the devices.

Activating All Inactive Cisco WAAS Devices

Procedure

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

The **All Devices** window appears.

Step 2 Click the **Activate All Inactive WAEs** icon in the taskbar.

The **Activate All Inactive WAEs** window appears.

Step 3 To choose existing location for all the inactivated Cisco WAAS devices, click the **Select an existing location for all inactive WAEs** radio button, and then choose a location from the corresponding drop-down list.

Alternatively, choose to create a new location for each inactive device by clicking the **Create a new location for each inactive WAE** radio button. Specify a parent location for all newly created locations by choosing a location from the Select a parent location for all newly created locations drop-down list.

Step 4 Click **Submit**.

The inactive Cisco WAEs are reactivated and placed in the specified location.

Rebooting a Device or Device Group

This sectontion contains the following topics:

Rebooting a Device

Before you begin

Using the Cisco WAAS Central Manager GUI, you can reboot a device or device group remotely. For how to reboot a device group, see Rebooting a Device Group, on page 551.

Note If you reboot a Cisco WAAS Central Manager that has Secure Store enabled with **user-provided passphrase** mode, you must reopen Secure Store after the reboot by running the **cms secure-store open** EXEC command.

Procedure

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

The device **Dashboard** window appears.

Step 2 In the **Device Info** pane, click the **Reload** icon.

You are prompted to confirm your decision.

Step 3 To confirm that you want to reboot the device, click **OK**.

Step 4 To reboot a device from the CLI, run the **reload** EXEC command.

Rebooting a Device Group

Before you begin

Using the Cisco WAAS Central Manager GUI, you can reboot a device or device group remotely. For how to reboot an individual device, see Rebooting a Device, on page 550.

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Device Groups** > *device-group-name*.

The **Modifying Device Group** window appears.

Step 2 In the taskbar, click the **Reboot All Devices in Device Group** icon.

You are prompted to confirm your decision.

Step 3 To confirm that you want to reboot the device group, click **OK**.

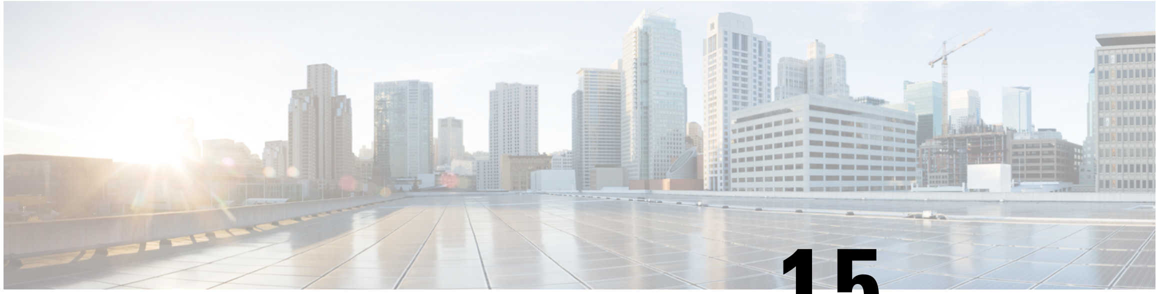
Performing a Controlled Shutdown

A controlled shutdown refers to the process of properly shutting down a Cisco WAAS device without turning off the power on the device (the fans continue to run and the power LED remains on). With a controlled shutdown, all of the application activities and the operating system are properly stopped on the appliance, but the power remains on. Controlled shutdowns can help you minimize the downtime when the appliance is being serviced.

⚠ **Caution** If a controlled shutdown is not performed, the Cisco WAAS file system can be corrupted. It also takes longer to reboot the appliance if it was not properly shut down.

You can perform a controlled shutdown from the CLI by running the **shutdown** EXEC command. For more details, see the *Cisco Wide Area Application Services Command Reference Guide* .

If you are running Cisco WAAS on a network module that is installed in a Cisco access router, perform a controlled shutdown from the router CLI by running the **service-module integrated-service-engine** *slot/unit* **shutdown** EXEC command. For more details, see *Configuring Cisco WAAS Network Modules for Cisco Access Routers*.



CHAPTER 15

Monitoring Your Cisco WAAS Network

This chapter describes the monitoring tools available in the Cisco WAAS Central Manager GUI that can help you monitor activity, configure flow monitoring, and customize reports.

For information on Cisco WAAS system logging and troubleshooting, see the chapter Troubleshooting Your Cisco WAAS Network, on page 619.

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

This chapter contains the following sections:

Viewing System Information from the System Dashboard Window

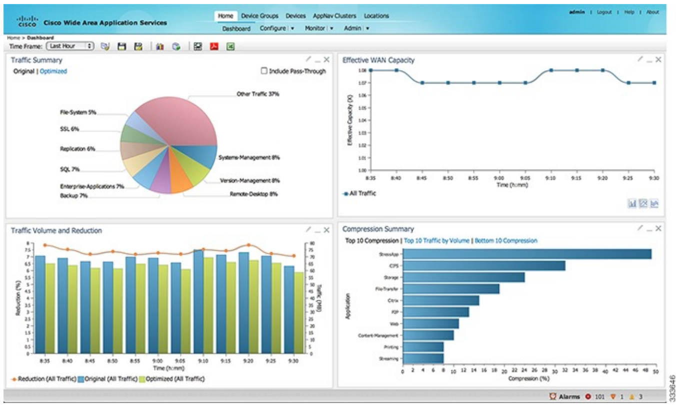
The Cisco WAAS Central Manager GUI allows you to view general and detailed information about your Cisco WAAS network from the System Dashboard window. This section describes the System Dashboard window and contains the following topic:

- Monitoring Graphs and Charts, on page 554

Note For information on viewing the alarm panel and on viewing device alarms, see Cisco WAAS Central Manager Alarm Panel in the chapter "Troubleshooting Your Cisco WAAS Network."

The following figure shows the **System Dashboard** window.

Figure 83: System Dashboard Window



The information displayed in the charts in the System Dashboard window is based on a snapshot of your WAAS network that represents the state of your WAE devices at the end of every two polling periods. You can configure the interval between polls in the Cisco WAAS Central Manager GUI (**Configure** > **Global** > **System Properties** > **System Properties** > **system.monitoring.collectrate**). The default polling rate is 300 seconds (5 minutes). Alarms are presented in real time and are independent of the polling rate.

Monitoring Graphs and Charts

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

- Traffic Summary, on page 568 chart: Displays the applications with the highest percentage of traffic in the WAAS network for the last hour.
- Effective WAN Capacity, on page 567 graph: Displays the effective increased bandwidth capacity of the WAN link as a result of WAAS optimization, as a multiple of the actual bandwidth.
- Traffic Volume and Reduction, on page 568 graph: Displays the original and optimized traffic volume and percentage of traffic reduction over the last hour.
- Compression Summary, on page 567 chart: Displays the ten applications with the highest percentage of traffic reduction for the Cisco WAAS network for the last hour. The percent calculation excludes pass-through traffic.

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

You can customize the graphical displays and tables that are displayed on the system dashboard. For more information, see Customizing a Dashboard or Report, on page 562. Individual charts are described in more detail in Cisco WAAS Chart Descriptions, on page 566.

Much of the device, statistical, and alarm information that is presented in the system dashboard and associated graphs and charts is also available programmatically through the monitoring API.

Note

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

Note

For information on how to troubleshoot device alarms, see in the chapter "Troubleshooting Your WAAS Network."

Viewing Device Information

This section describes how to use the Cisco WAAS Central Manager device windows:

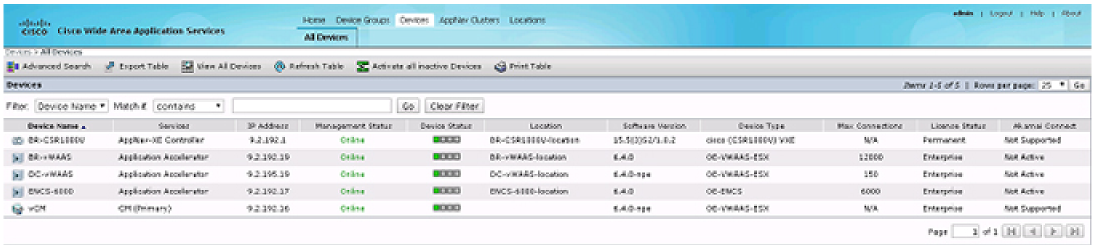
- The Devices Window, on page 555 displays a list of and basic information for all Cisco WAAS devices.
- The Device Dashboard Window, on page 558 displays detailed information about a specific device, such as the installed software version and whether the device is online or offline.
- The Device Status Dashboard Window, on page 559 displays traffic information for all Cisco WAAS devices.
- The Viewing and Unlocking Device Users, on page 561 window displays the list of users, in table format, with information including username, number of login failures, and time of last login failure.

Devices Window

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

The **Devices** window appears.

Figure 84: Devices Window


Cisco Wide Area Application Services
Home
Device Groups
Devices
AppNav Clusters
Locations
All Devices
admin | Logout | Help | About
Devices > All Devices
Advanced Search
Export Table
View All Devices
Refresh Table
Activate all inactive Devices
Print Table
Devices
Items 1-5 of 5 | Rows per page: 25 Go
Filter: Device Name Match if: contains Go Clear Filter
Page 1 of 1

Device Name	Services	IP Address	Management Status	Device Status	Location	Software Version	Device Type	Max Connections	License Status	Akamai Connect
BR-CSR1000V	AppNav-XE Controller	9.2.192.1	Online		BR-CSR1000V-location	15.5(3)S2/1.0.2	cisco (CSR1000V) VXE	N/A	Permanent	Not Supported
BR-vWAAS	Application Accelerator	9.2.192.19	Online		BR-vWAAS-location	6.4.0	OE-VWAAS-ESX	12000	Enterprise	Not Active
DC-vWAAS	Application Accelerator	9.2.195.19	Online		DC-vWAAS-location	6.4.0-npe	OE-VWAAS-ESX	150	Enterprise	Not Active
ENCS-5000	Application Accelerator	9.2.192.17	Online		ENCS-5000-location	6.4.0	OE-ENCS	6000	Enterprise	Not Active
vCM	CM (Primary)	9.2.192.16	Online			6.4.0-npe	OE-VWAAS-ESX	N/A	Enterprise	Not Supported

The **Devices** window displays the following information about each device:

- Services enabled on the device. For a description of these services, see the "Service Descriptions" table below.
- IP address of the device.

- Management Status (**Online**, **Offline**, **Pending**, or I**nactive**). For more information about the status, see Device Alarms in the chapter "Troubleshooting Your Cisco WAAS Network." A tool tip is displayed when you hover your cursor over the individual device **Management** status. It shows the timestamp for offline devices and the timestamp for the latest configuration for online devices.
- Device Status. The system status reporting mechanism uses four alarm lights to identify problems that have to be resolved. Each light represents a different alarm level as follows:
  - **Green**: No alarms (the system is in excellent health)
  - **Yellow**: Minor alarms
  - **Orange**: Major alarms
  - **Red**: Critical alarms

When you hover your mouse over the alarm light bar, a message provides further details about the number of alarms. Click the alarm light bar to troubleshoot the device. For more information, see the chapter Troubleshooting Your Cisco WAAS Network, on page 619.

- **Location associated with the device**: For more information about locations, see the chapter Using Device Groups and Device Locations, on page 53You can view reports that aggregate data from all the devices in a location. For more information, see Location-Level Reports, on page 589.
- **Software version installed and running on the device**: For Cisco WAAS Express and AppNav-XE devices, both the Cisco IOS and the Cisco WAAS Express or AppNav-XE software versions are shown.
- **Device Type**: If you see a type such as Cisco WAAS Express and AppNav-XE devices, the router platform is displayed. For Cisco vWAAS devices, **OE-VWAAS** is displayed, and for Cisco WAAS for Cisco Integrated Services Routers (ISR) devices, **ISR-WAAS** is displayed. For ENCS devices, **OE-ENCS** is displayed.
- **Max Connections**: The maximum number of connections that can be handled by the device.
- **License Status**: Displays the installed licenses. See the "License Status Descriptions" table below for a description of the possible values.
- **Akamai Connect**: Displays the Akamai Connect license status for the device whether the license is supported, active or disabled for the device.

WAE devices that are at a later software version level than the Cisco WAAS Central Manager are displayed in red. Also, if the Standby Cisco WAAS Central Manager has a different version level from the Primary Cisco WAAS Central Manager, the Standby Cisco WAAS Central Manager is displayed in red.

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

Table 70: Service Descriptions

Service	Description
CM (Primary)	The device has been enabled as the Primary Cisco WAAS Central Manager.
CM (Standby)	The device has been enabled as a Standby Cisco WAAS Central Manager.

Service	Description
Application Accelerator	The device has been enabled as an application accelerator.
AppNav Controller	The device has been enabled as an AppNav Controller.
AppNav-XE Controller	The device is a router using Cisco IOS XE with the AppNav-XE controller functionality enabled.
WAAS Express	The device is a router using Cisco IOS with the Cisco WAAS Express functionality enabled.

Table 71: License Status Descriptions

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

Note After the devices has been registered to the Cisco WAAS Central Manager, a Cisco WAAS Central Manager DB VACUUM (runs between 1 AM – 2 AM) process takes more time (Min:2 min, Avg:7 min, Max:25min) due to the augmented load on computing resources.

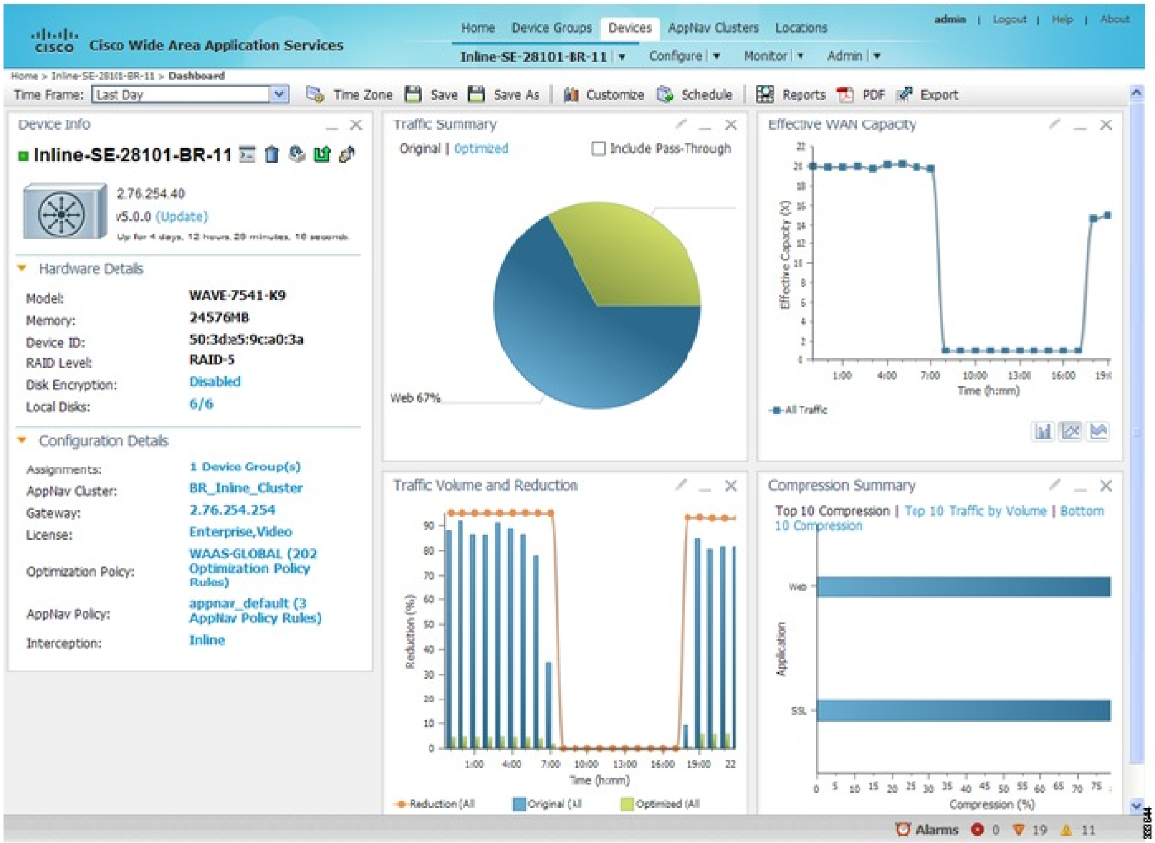
- A few of the WAEs may go temporarily offline. They are online automatically once the VACUUM process is complete.
- **Statistics Aggregation** threads may take more than 5 minutes and the same would be indicated in the logs. As a result statistics samples, might be missing at network level.
- **User**, including the administrator will not be able to use (login) the Cisco WAAS Central Manager as the complete DB will be locked.

Device Dashboard Window

The **Device Dashboard** window provides detailed information about a Cisco WAAS device, including device model (such as WAVE-7541-K9 or OE-VWAAS-KVM), IP address, interception method, and device-specific charts.

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

Figure 85: 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
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
Web
SSL
Application
Compression (%)
Alarms 0 19 11
328844

Time Frame: Last Day

Device Info

Inline-SE-28101-BR-11

2.76.254.40
v5.0.0 (Update)
Up for 4 days, 12 hours, 29 minutes, 10 seconds

Hardware Details

Model:	WAVE-7541-K9
Memory:	24576MB
Device ID:	50:3d:a5:9c:a0:3a
RAID Level:	RAID-5
Disk Encryption:	Disabled
Local Disks:	6/6

Configuration Details

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

The following tasks are available from the **Device Dashboard** window:

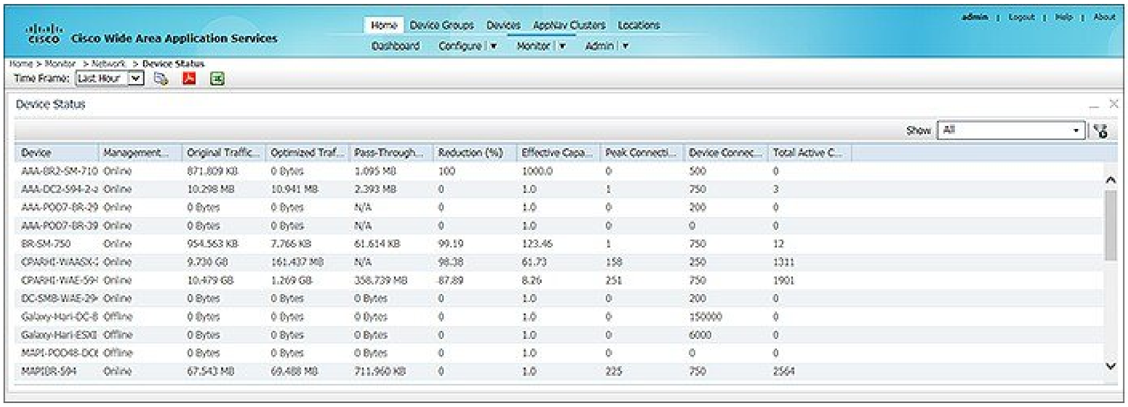
- View charts and graphs about the application traffic processed by the selected WAE device. (No charts or graphs are displayed if a Cisco WAAS Central Manager device is selected.)
- Customize the charts displayed in the window. For more information, see Customizing a Dashboard or Report, on page 562 and Cisco WAAS Chart Descriptions.
- View basic details, such as whether the device is online, the device's IP address and hostname, the software version running on the device, and the amount of memory installed in the device, the license status, and so forth.
- View the device groups to which the device belongs. For more information, see the chapter "Using Device Groups and Device Locations, on page 53". (Not available on AppNav-XE devices.)

- View the users that are defined on the device and unlock any locked-out users. For more information, see Viewing and Unlocking Device Users, on page 561. (Not available on WAAS Express and AppNav-XE devices.)
- To update the software on the device, click **Update**. For more information, see the chapter "Maintaining Your Cisco WAAS System." (Not available on WAAS Express and AppNav-XE devices.)
- To establish a Telnet session into the device and issue CLI commands, click the **Telnet** icon.
- To delete the device, click the **Delete Device** icon.
- To reapply the device configuration from the Cisco WAAS Central Manager to the device, click the **Full Update** icon. (Not available on Cisco WAAS Express and AppNav-XE devices.)
- To reboot the device, click the **Reload** icon. (Not available on Cisco WAAS Express and AppNav-XE devices.)
- To restore the default predefined policies on the device, click the **Restore Default Policies** icon. For more information, see Restoring Optimization Policies and Class Maps, on page 458 in the chapter "Configuring Application Acceleration." (Not available on Cisco AppNav-XE devices.)
- Assign and unassign the device to device groups. For more information, see the chapter "Using Device Groups and Locations." (Not available on Cisco AppNav-XE devices.)
- For a Cisco WAAS Express device, a **WAAS Enabled Interfaces** item shows the number of interfaces on which Cisco WAAS optimization is enabled. You can click the number to go to the **Network Interfaces** configuration window, which displays device interface details and allows you to enable or disable optimization on the available interfaces. For more details, see Enabling or Disabling Optimization on Cisco WAAS Express Interfaces in the chapter "Configuring Network Settings."
- For a Cisco WAAS Express device, you can view the DRE item to determine if the device supports data redundancy elimination (DRE) optimization, which is not supported on some Cisco WAAS Express device models. This item reads **Supported** or **Unsupported**.
- For a Cisco WAAS Express device, you can view the SSL item to determine if SSL acceleration is available. This item reads **Available** or **Unavailable**.
- For a Cisco vWAAS device, the **No. of CPUs**, **Max TCP Connections**, and **Interception Method** fields are shown. For more details, see the chapter "Configuring Traffic Interception, on page 127."
- On an AppNav Controller, an **AppNav Cluster** item shows any defined AppNav Clusters. You can click a cluster name to go to that cluster's home window. Also, an AppNav Policy item shows defined AppNav policies, if any. To go to the **Policy Configuration** window, click a policy name.

Device Status Dashboard Window

The **Device Status Dashboard** window lists all the Cisco WAAS devices that are registered with the WAAS Central Manager. To view this list, from the Cisco WAAS Central Manager choose **Home** > **Monitor** > **Network** > **Device Status**.

Figure 86: Device Status Dashboard Window



Time Frame: Last Hour

Show: All

Device	Management...	Original Traffic...	Optimized Traf...	Pass-Through...	Reduction (%)	Effective Capa...	Peak Connecti...	Device Connec...	Total Active C...
AAA-BR2-SM-710	Online	871.809 KB	0 Bytes	1.095 MB	100	1000.0	0	500	0
AAA-DC2-594-2-a	Online	10.298 MB	10.941 MB	2.393 MB	0	1.0	1	750	3
AAA-POD7-BR-29	Online	0 Bytes	0 Bytes	N/A	0	1.0	0	200	0
AAA-POD7-BR-39	Online	0 Bytes	0 Bytes	N/A	0	1.0	0	0	0
BR-SM-750	Online	954.563 KB	7.766 KB	61.614 KB	99.19	123.46	1	750	12
CPARHI-WAASX-:	Online	9.730 GB	161.437 MB	N/A	98.38	61.73	158	250	1311
CPARHI-WAE-59!	Online	10.479 GB	1.269 GB	358.739 MB	87.89	8.26	251	750	1901
DC-SMB-WAE-29	Online	0 Bytes	0 Bytes	0 Bytes	0	1.0	0	200	0
Galaxy-Hari-DC-8	Offline	0 Bytes	0 Bytes	0 Bytes	0	1.0	0	150000	0
Galaxy-Hari-ESXI	Offline	0 Bytes	0 Bytes	0 Bytes	0	1.0	0	6000	0
MAPI-POD48-DCI	Offline	0 Bytes	0 Bytes	0 Bytes	0	1.0	0	0	0
MAPIDR-594	Online	67.543 MB	69.488 MB	711.960 KB	0	1.0	225	750	2564

The following table displays information about each column in the **Device Status Dashboard** window:

Table 72: Device Status Dashboard Window Field and Columns

Device Status Field or Column	Device Status Column Description
Time Frame drop-down list	Choose one of the following time frame to display status for the device: • Last Hour • Last Day • Last Week • Last Month • Custom dates **Note** Data for **Management Status** and **Active Connections** is displayed only when you select **Last Hour**. For more information on time frames, see Customizing a Dashboard or Report, on page 562
Device	The name of the device.
Management Status	A status of Online, Offline, Pending, or Inactive. For more information on device management status and alarms related to device management status, see Device Alarms in the chapter "Troubleshooting Your Cisco WAAS Network."
Original Traffic	The amount of original traffic, in GB, passing through the device.
Optimized Traffic	The amount of optimized traffic, in GB, passing through the device.
Pass-Through Reduction (%)	The percentage of traffic reduction for the time period specified in the Time Frame drop-down list.

Device Status Field or Column	Device Status Column Description
Effective Capacity (X)	The effective bandwidth capacity of the device as a result of optimization.
Peak Connection	The peak optimized connections for the device.
Device Connection Limit	The maximum connection limit for the device.
Total Active Connections	The total number of current active connections for the device.

Device Status Report

You can choose to view the **Device Status** report as a **.pdf** or a **.csv** file by selecting the respective icons on the dashboard. The Time Zone option enables you to customize the time zone for the report, based on your preference. For more information on setting time zones, see Customizing a Dashboard or Report, on page 562.

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

Viewing and Unlocking Device Users

To view the users defined on a Cisco WAAS device, choose **Devices** > *device-name* and then, from the **Device Name** menu, choose Device Users. On a Cisco WAAS Central Manager device, choose **CM Users**.

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

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

Detecting and Resolving Configuration Conflicts

Before you begin

Configuration conflicts between the device group and devices are difficult to identify at the device group level. Whenever configuration conflicts occur, they show up in the **Force Device Group Detection** page. The Cisco WAAS Central Manager provides an easy way to identify, view and resolve these configuration conflicts.

Note **Force Device Group** detection is not applicable for Cisco routers.

Procedure

Step 1 To to see the impacted **Device Name**, **Device Group Name** and **Page Name**, from the Cisco WAAS Central Manager choose **Home** > **Admin** > **Force Device Group** > **View Pages**. This lists all the device groups that have conflicts with the devices and on which page.

Step 2 Click on the page link to navigate to the corresponding page to correct the configuration conflict.

Customizing a Dashboard or Report

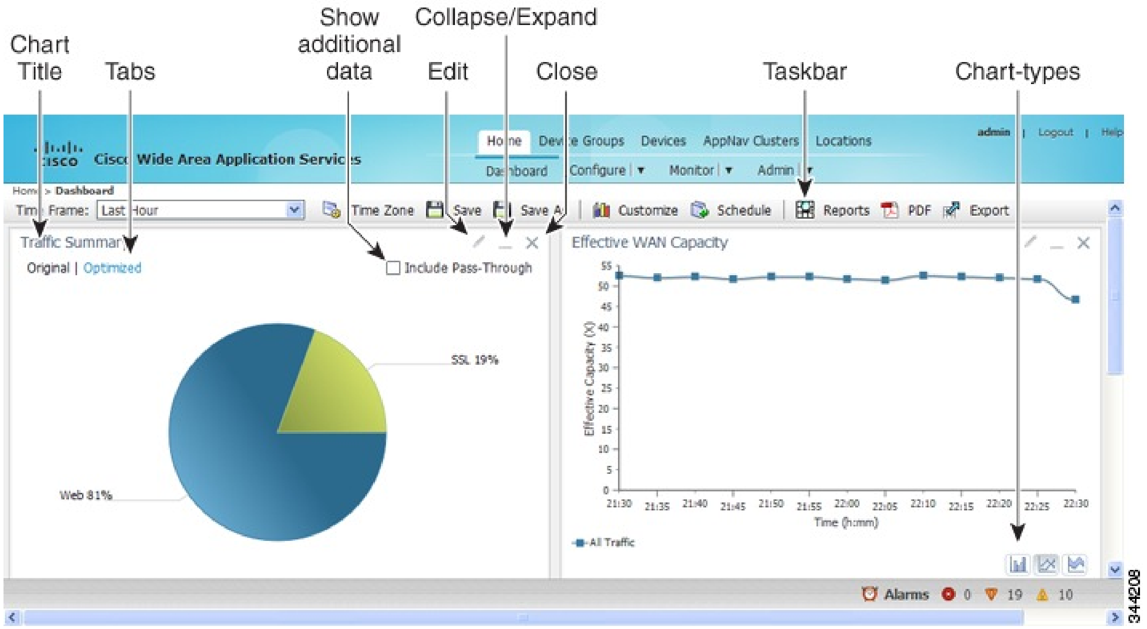
You can customize the system and device dashboards and reports, if any, in the same way. For more information about creating custom reports, see Managing Reports, on page 603.

This section contains the following topics:

The Cisco WAAS Central Manager Report Panel

The following figure shows a sample report.

Figure 87: Report Pane



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

- **Time Frame**: Allows you to choose one of the several common time frames from the drop-down list:
  - **Last Hour**: Displays data for the past hour, in five-minute intervals (default). You can change the interval using the **System.monitoring.collectRate** configuration setting described in Modifying Default System Properties in the chapter "Configuring Other System Settings."

    - **Last Day**: Displays data for the past day (in hourly intervals).
    - **Last Week**: Displays data for the past week (in daily intervals).
    - **Last Month**: Displays data for the past month (in daily intervals).
    - **Custom**: Enter starting and ending dates in the From and To fields. Click the calendar icon to choose dates from a pop-up calendar.

The time frame setting is stored individually for each report and Central Manager user. Additionally, the **System.monitoring.timeFrameSettings** system property controls the system default time frame setting. For more information, see Modifying Default System Properties in the chapter "Configuring Other System Settings."

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

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

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

- **Save**: Saves the dashboard or report with its current settings. The next time you view it, it is displayed with these settings.
- **Save As**: Saves the report with its current settings under a new name. A dialog box allows you to enter a report name and an optional description. You can enter only the following characters: numbers, letters, spaces, periods, hyphens, and underscores. The report will be available in the **Monitor** > **Reports** > **Reports Central** window.
- **Customize**: Allows you to add a chart or table to a dashboard or report. For information on adding a chart or table, see Adding a Chart or Table, on page 564.
- **Schedule**: Allows you to schedule reports to be generated once, or periodically, such as hourly, daily, weekly, or monthly. When a scheduled report is generated, you can have a PDF copy of the report e-mailed to you automatically.
    - In the **Date** field, enter the schedule date in the format **DD/MM/YYYY**, or click the calendar icon to display a calendar from which to choose the date.
    - From the **Hours** drop-down list, choose the hours. The time represents the local time at the WAAS Central Manager.
    - From the **Minutes** drop-down list, choose the minutes. The time represents the local time at the Cisco WAAS Central Manager.

    - From the **Frequency** drop-down list, choose **Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly** to set the report frequency.
    - In the **No. of Reports** field, enter the number of times that a reoccurring report is to be generated. After a report is generated a specified number of times, the report is no longer generated.
    - In the **Email Id(s)** field, enter the email addresses of the report recipients, separated by commas.
    - In the **Email Subject** field, enter the subject of the email message.

- **Reports**: Allows you to view the scheduled reports. For instructions about viewing scheduled reports, see Viewing or Deleting a Scheduled Report, on page 607.
- **PDF**: Generates a PDF format of a report, including the charts and table data. To include a custom logo in your PDF report, choose **Home Dashboard** > **Admin> Custom Logo**, and then click **Upload**. The custom logo is displayed in the PDF format of the report. Additionally, when you schedule a report, you can select **Custom Logo** for the logo to appear on the scheduled report. This option is available only when you have uploaded the custom logo.
- **Export**: Exports the chart and table statistical data to a CSV file. The statistical data shown in charts is rounded to whole units (KB, MB, or GB), while the exported data contains exact byte values.

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

- **Chart title**: Allows you to click and drag in order to move the chart to a different location in the report pane.
- **Edit icon**: Allows you to edit the chart settings, as described in Configuring Chart Settings, on page 565.
- **Collapse/Expand icon**: Allows you to collapse or expand the chart. When a chart is collapsed, this icon changes to Expand, which restores the chart to its normal size.
- **Close icon**: Closes the chart.
- **Tabs**: Allows you to have a choice of multiple tab views that you can access by clicking the desired tab name. Note that not all charts have this feature.
- **Check box to show additional data**: Allows you to check the check box labeled with an optional data statistic to include the data in the chart. Note that not all charts have this feature.

Chart-type icons at the bottom of individual charts allow you to choose the chart type as follows: **column chart**, **line chart**, **area chart**, **stacked line chart**, **stacked area chart**. Note that not all charts have this feature.

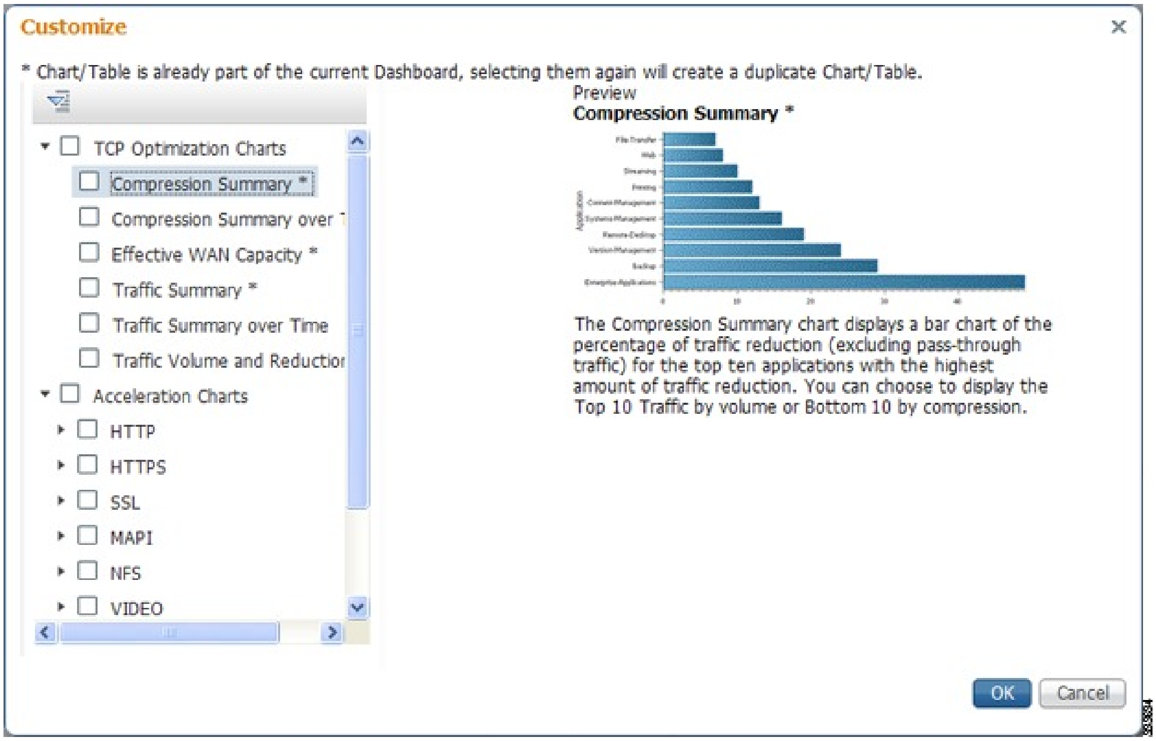
Adding a Chart or Table

Procedure

Step 1 From the dashboard or report chart panel, click the **Customize** icon in the taskbar.

The **Customize** window is displayed.

Figure 88: Customize Window



Customize

* Chart/Table is already part of the current Dashboard, selecting them again will create a duplicate Chart/Table.

- ▾ □ TCP Optimization Charts
  - □ Compression Summary *
  - □ Compression Summary over T
  - □ Effective WAN Capacity *
  - □ Traffic Summary *
  - □ Traffic Summary over Time
  - □ Traffic Volume and Reductior
- ▾ □ Acceleration Charts
  - ▸ □ HTTP
  - ▸ □ HTTPS
  - ▸ □ SSL
  - ▸ □ MAPI
  - ▸ □ NFS
  - ▸ □ VIDEO

Preview

Compression Summary *

The Compression Summary chart displays a bar chart of the percentage of traffic reduction (excluding pass-through traffic) for the top ten applications with the highest amount of traffic reduction. You can choose to display the Top 10 Traffic by volume or Bottom 10 by compression.

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

Step 3 Check the check box next to each chart or table that you want to be displayed as a report. Individual charts are described in more detail in Cisco WAAS Chart Descriptions, on page 566.

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

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

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

Step 5 Click **OK**.

Step 6 To delete a chart or table from a dashboard or report, click **Close** on the chart and save the report.

Configuring Chart Settings

Procedure

Step 1 Click the **Edit** icon in the upper right corner of a chart.

The **Settings** window is displayed.

Note Not all settings are available for all chart types.

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

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

Step 3 (Optional) From the **Access Mode** drop-down list, choose one of the following options:

- **Both**: Displays statistics for both single-sided and double-sided optimization.
- **With WAAS Peer**: Display statistics for double-sided optimization.
- **Without WAAS Peer**: Displays statistics for single-sided optimization.Use these options are to include or exclude single-sided optimization. The single-side statistics option is available only for the **Traffic Summary**, **Effective WAN Capacity**, **Traffic Volume and Reduction**, **Compression Summary**, **Traffic Summary over time**, **Compression Summary over time**, **Throughput Summary** and **Optimized Connections Over Time** charts.

Step 4 (Optional) From the **Select Series For** drop-down list, choose one of the following:

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

Step 5 (Optional) In the **Application** or **Classifier** list, check the check box next to the applications or classifiers whose statistics you want to include in the chart data. To include all the applications, check the **All Traffic** check box. You can filter the list items by using the **Quick Filter** above the list. These lists are available only for some chart types.

Step 6 (Optional) Some charts have other types of data series from which to choose. Check the check box next to each of the data series that you want to include in the chart data.

Step 7 Click OK.

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

Cisco WAAS Chart Descriptions

This section describes the charts that you can choose to include in a dashboard or report. For tables that provide information on system, device, traffic and acceleration, see Cisco WAAS Table Descriptions, on page 582,

The following chart categories are available:

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

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

TCP Optimization Charts

The following TCP optimization charts are available:

Compression Summary

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

Formula:

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

Compression Summary Over Time

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

Formula:

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

Effective WAN Capacity

The Effective WAN Capacity chart displays the effective increased bandwidth capacity of the WAN link as a result of WAAS optimization. You can choose which applications to include. The default is all traffic.

Formula:

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

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

Throughput Summary for TCP Optimization

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

Formula:

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

Note The WAN to LAN Throughput and the LAN to WAN Throughput charts for the Last Week and Last Month time periods do not display peak throughput data until after two days of data have accumulated. You may see 0 for peak throughput if it has been less than two days since a new WAAS software installation or upgrade.

Traffic Summary

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

Formula:

(App Traffic/ Total Traffic) * 100

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

Traffic Summary Over Time

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

Traffic Volume and Reduction

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

Formula:

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

Acceleration Charts

This section contains the following topics:

HTTP Acceleration Charts

This section contains the following topics:

HTTP: Connection Details

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

HTTP: Effective WAN Capacity

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

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

HTTP: Estimated Time Savings

The **HTTP Estimated Time Savings** chart displays a graph of the estimated percentage of the response time saved by the HTTP accelerator due to SharePoint prefetch optimization and metadata caching.

HTTP: Optimization Count

The **HTTP Optimization Count** chart displays a graph of the number of different kinds of optimizations performed by the HTTP accelerator. These optimizations are displayed in different colors. The optimizations included in this chart are metadata caching and SharePoint prefetch.

HTTP: Optimization Techniques

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

HTTP: Response Time Savings

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

HTTPS Acceleration Charts

This section describes the following charts:

HTTPS: Connection Details

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

HTTPS: Effective WAN Capacity

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

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

HTTPS: Estimated Time Savings

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

HTTPS: Optimization Count

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

HTTPS: Optimization Techniques

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

HTTPS: Response Time Savings

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

SSL Acceleration Charts

This section describes the Secure Sockets Layer (SSL) charts:

SSL: Acceleration Bypass Reason

The Secure Sockets Layer (SSL) Acceleration Bypass Reason pie chart displays the reasons because of which SSL traffic is not accelerated: version mismatch, unknown, nonmatching domain, server name indication mismatch, cipher mismatch, revocation failure, certificate verification failure, other failure, and non-SSL traffic.

SSL: Connection Details

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

SSL: Effective WAN Capacity

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

All the charts above display the cumulative statistical data of single sided and dual sided ssl counters.

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

MAPI Acceleration Charts

This section describes the Messaging Application Programming Interface (MAPI) charts:

MAPI: Acceleration Bypass Reason

The **Messaging Application Programming Interface (MAPI) Acceleration Bypass Reason** pie chart displays the reasons because of which encrypted MAPI traffic is not accelerated: acceleration disabled, secret retriever disabled, unsupported cipher, unsupported authentication mechanism, misconfigured domain identity, failure in secret retrieval, general security failure, insufficient system resources, and recovery mode connections.

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

MAPI: Average Response Time Saved

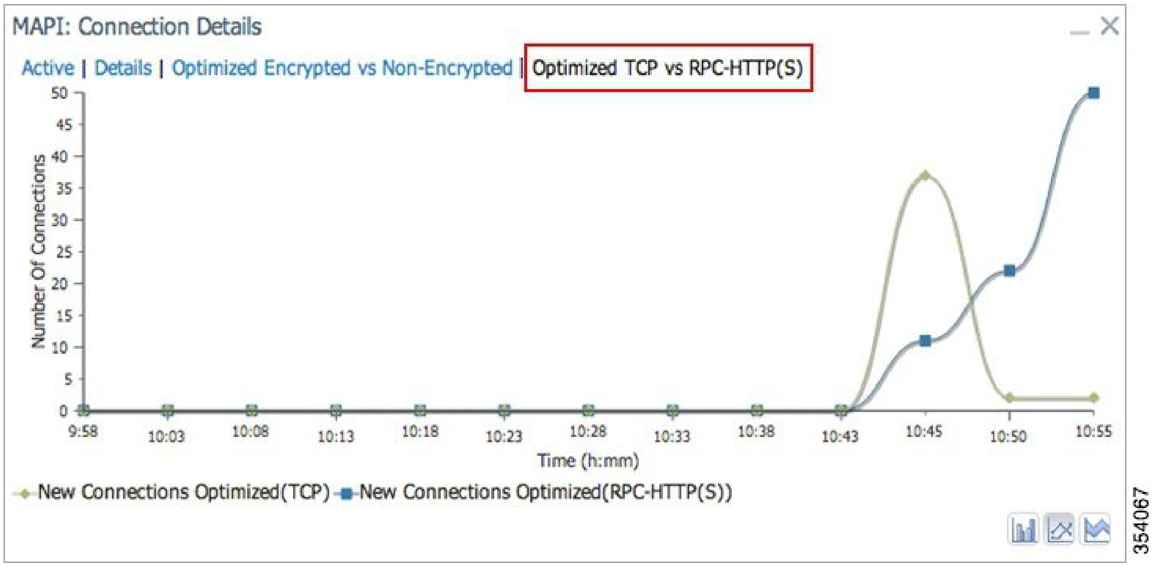
The **MAPI Average Response Time Saved** chart displays a graph of the estimated percentage of response time saved by the MAPI accelerator. The time units (microseconds, milliseconds, seconds, or minutes) at the left side depend upon the range.

MAPI: Connection Details

The MAPI Connection Details chart displays MAPI session connection statistics, showing the average number of active MAPI connections per device (at the device level, it shows the exact number for the last hour). In addition to information on newly handled MAPI connections, optimized connections, handed-off connections, dropped connections, and optimized vs. non-encrypted MAPI connections, WAAS Version 5.5.3 and later also provides information on optimized TCP vs. RPC-HTTP(S) MAPI connections, as shown in the following figure. Cisco WAAS Version 6.4.3 and later includes information on MAPI over HTTP connection in the following chart.

- To display the newly handled MAPI connections, optimized connections, handed-off connections, and dropped connections, click the **Details** tab.
- To display the new encrypted and unencrypted MAPI connections, click the **Optimized Encrypted vs Non-Encrypted** tab.
- To display the new optimized TCP and RPC-HTTP/S connections, click the **Optimized TCP vs RPC-HTTP(S)** tab.

Figure 89: Example of MAPI: Connection Details Chart


MAPI: Connection Details
Active | Details | Optimized Encrypted vs Non-Encrypted | Optimized TCP vs RPC-HTTP(S)
Number Of Connections
0
5
10
15
20
25
30
35
40
45
50
9:58
10:03
10:08
10:13
10:18
10:23
10:28
10:33
10:38
10:43
10:45
10:50
10:55
Time (h:mm)
New Connections Optimized(TCP)
New Connections Optimized(RPC-HTTP(S))
354067

MAPI: Effective WAN Capacity

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

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

MAPI: Request Optimization

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

MAPI: Response Time Optimization

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

MAPI: Average Accelerated Client Sessions

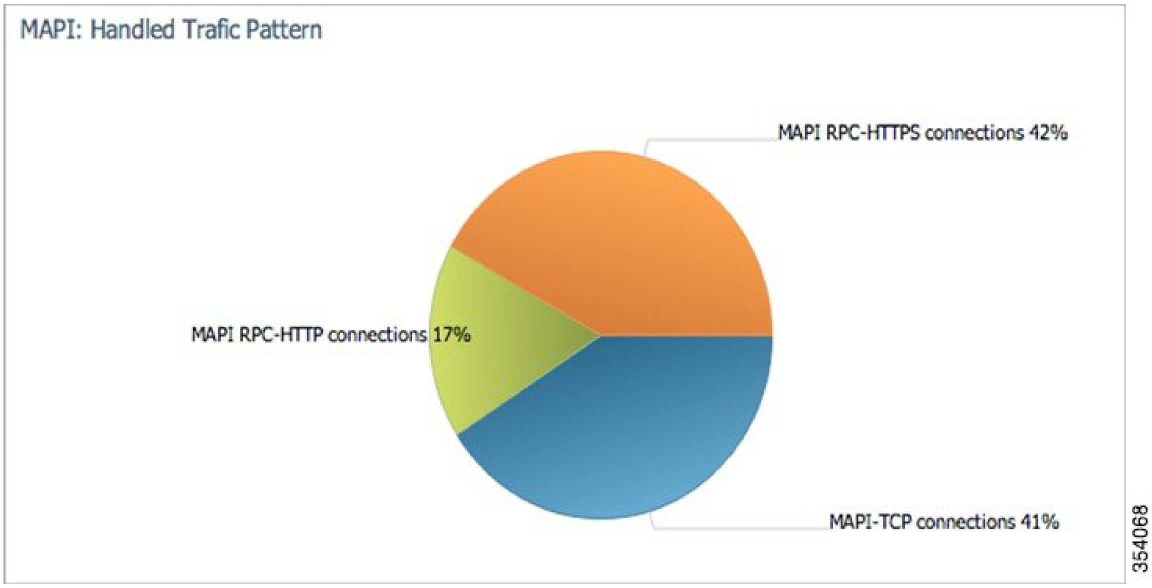
The **MAPI Average Accelerated Client Sessions** pie chart displays the average number of encrypted sessions that are accelerated from different versions (2000, 2003, 2007, and 2010) of the Microsoft Outlook client. Click the **Non-Encrypted** tab to display the unencrypted session counts.

MAPI: Handled Traffic Pattern

For Cisco WAAS Versions 5.5.3 and later, MAPI Acceleration reports include the MAPI: Handled Traffic Pattern pie chart. As shown in the following figure, this chart displays the percentage of three types of traffic:

- Total handled MAPI connections
- Total handled MAPI RPC-HTTP connections
- Total handled MAPI RPC-HTTPS connections

Figure 90: Example of MAPI: Handled Traffic Pattern Chart



SMB Acceleration Charts

This section describes the Server Message Block (SMB) charts:

SMB: Average Response Time Saved

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

SMB: Client Average Throughput

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

SMB: Connection Details

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

SMB: Effective WAN Capacity

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

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

SMB: Request Optimization

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

SMB: Response Time Savings

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

SMB: Versions Detected

The SMB Versions Detected pie chart displays the number of SMB messages detected for each SMB version:

- SMB v1.0 optimized, SMB v1.0 unoptimized, SMB v1.0 signed.
- SMB v2.0 optimized, SMB v2.0 unoptimized, SMBv 2.0 signed optimized and SMB v2.0 signed unoptimized.
- SMB v2.1 optimized, SMB v2.1 unoptimized, SMB v2.1 signed optimized, SMB v2.1 signed unoptimized.
- SMB v3.0 optimized, and SMB v3.0 unoptimized, SMB v3.0 signed, SMBv3.0 Encryption L4 optimized, SMBv3.0 Encryption L7 optimized, SMBv3.0 Encryption unoptimized.
- SMBv3.02 optimized, SMB v3.02 unoptimized and SMB v3.02 signed, SMBv3.02 Encryption L4 optimized, SMBv3.02 Encryption L7 optimized, SMBv3.02 Encryption unoptimized.

ICA Acceleration Charts

This section describes the Independent Computing Architecture (ICA) charts:

ICA: Client Versions

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

ICA: Connection Details

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

ICA: Effective WAN Capacity

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

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

ICA: Unaccelerated Reasons

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

Akamai Connected Cache Charts

The Cisco WAAS Central Manager provides the following types of monitoring reports for Akamai Connected Cache:

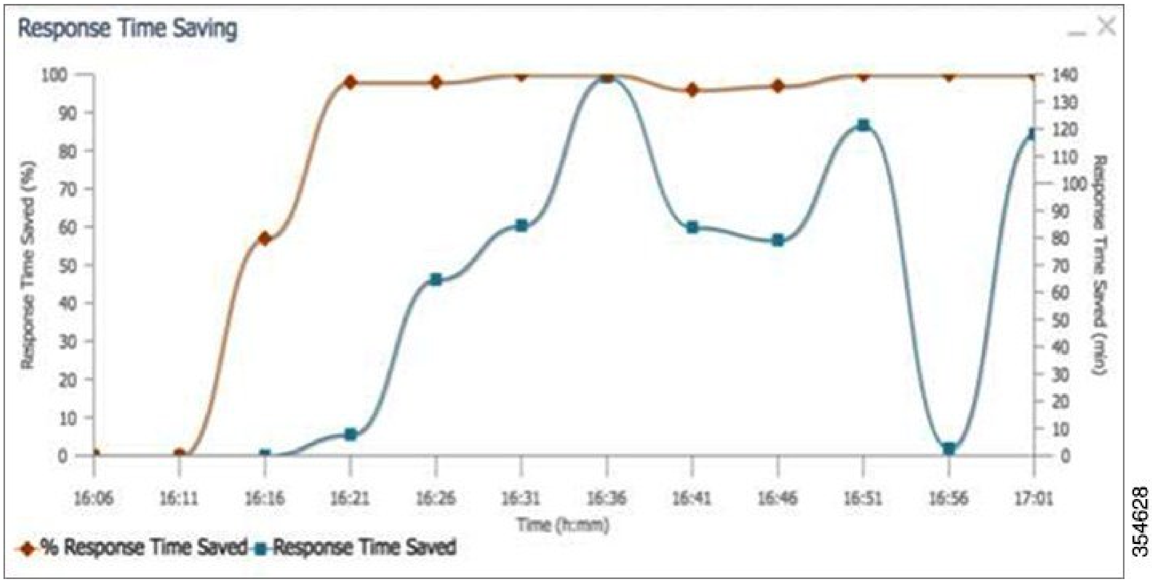
To access the following types of charts, choose **Monitor** > **Caching** > **Akamai Connect**.

Note Except for the **Top Sites** chart, you can view monitoring information at the device, network, location, or AppNav cluster levels.

Response Time Savings

As shown in the following figure, the **Response Time Savings** chart displays the aggregated amount of time saved due to Akamai Connect caching, showing the response time saved as a percentage, and total response time saved, for cache hit transactions, in minutes.

Figure 91: Example of Response Time Savings Chart



The Cisco WAAS Central Manager performs the following percentage calculations:

- Total response time saved
- Total adjusted download time
- Total response time without cache (total response time saved plus total adjusted download time)

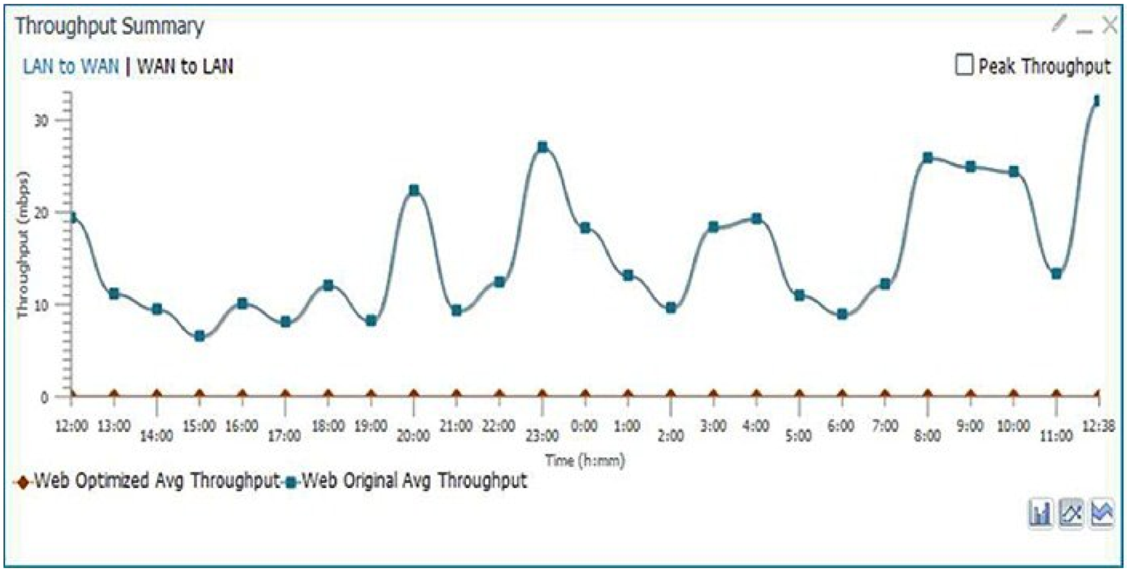
Note Output from the show statistics accelerator http CLI command also displays information on response time, including the **Total Time Saved** and **Percentage of Connection Time Saved** fields. For more information on Cisco WAAS CLI commands, see the *Cisco Wide Area Application Services Command Reference Guide*.

Throughput Summary for Akamai Connect

The Throughput Summary chart displays information on web-optimized and original throughput. Depending in the tab you click for this chart, LAN-to-WAN (outbound) or WAN-to-LAN (inbound), throughput is displayed. The WAN-to-LAN report is the default report.

If you hover your mouse over a bar, the total optimized or average throughput, in KBps, for a given time range is displayed.

Figure 92: Example of Throughput Summary Chart



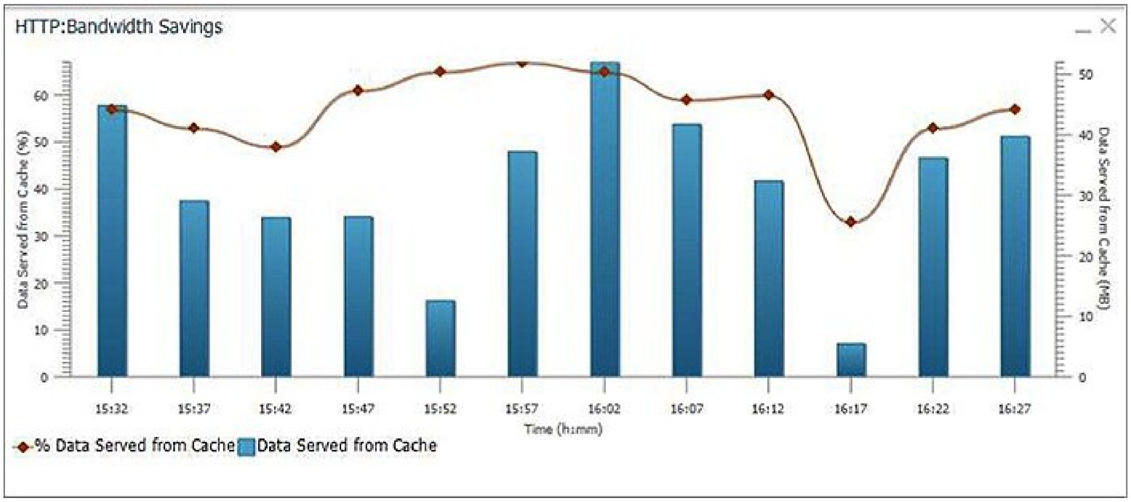
HTTP: Bandwidth Savings

The HTTP: Bandwidth Savings chart displays how much traffic, by percentage, is actually served by the Cache Engine (CE) that did not have to be fetched from the source.When this information is combined with overall incoming traffic into the router from the WAN, it indicates how effective the cache is in boosting the WAN performance in terms of request-response latency. The combination of the incoming (WAN) traffic flow to the router, plus the WAN data offload incoming traffic provides a truer measure of the traffic flow the router's clients (in aggregate) experience.

As shown in the following figure:

- The bar graph is the absolute byte count for data served out of cache for the specified interval
- The line graph represents the percentage of total bytes requested that were served out of cache for the specified interval.

Figure 93: Example of HTTP Bandwith Savings Chart

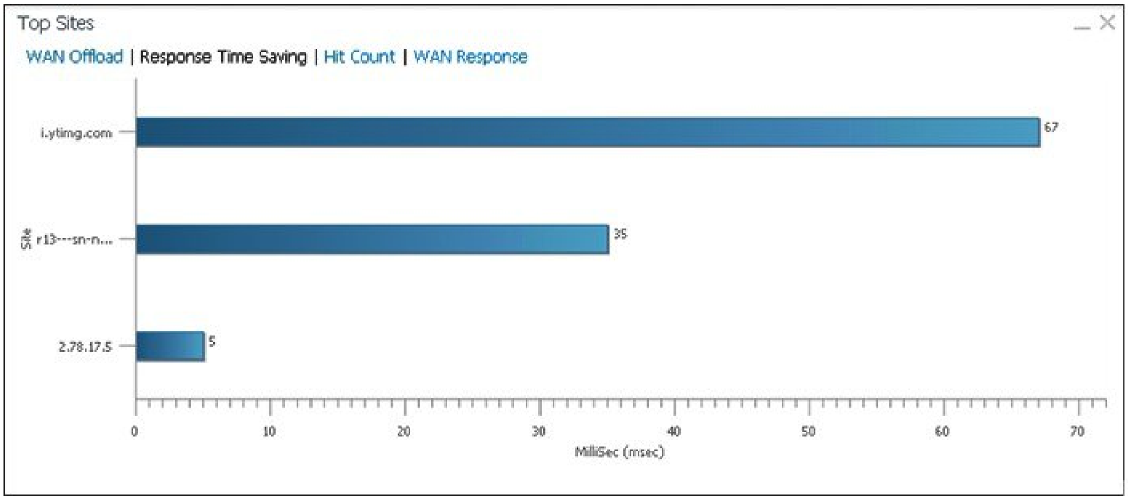


Top Sites

The Top Sites chart displays the top sites being served by the Cache Engine in terms of hostname and traffic, in bar chart format. The Top Sites chart displays the following types of information:

- **WAN Offload (Default report)**: The top URLs by number of bytes served out of the cache, and as a result did not come over the WAN.
- **Response Time Saving**: The response time saved due to Akamai Connect caching. The time unit, (milliseconds, seconds, or minutes) at the bottom of the chart depend on the time range specified for the chart.
- **Hit Count**: The top URLs by number of cache hits.
- **WAN Response**: The top URLs by number of bytes served over the WAN.

Figure 94: Top Sites Chart Showing Response Time Saving by Site



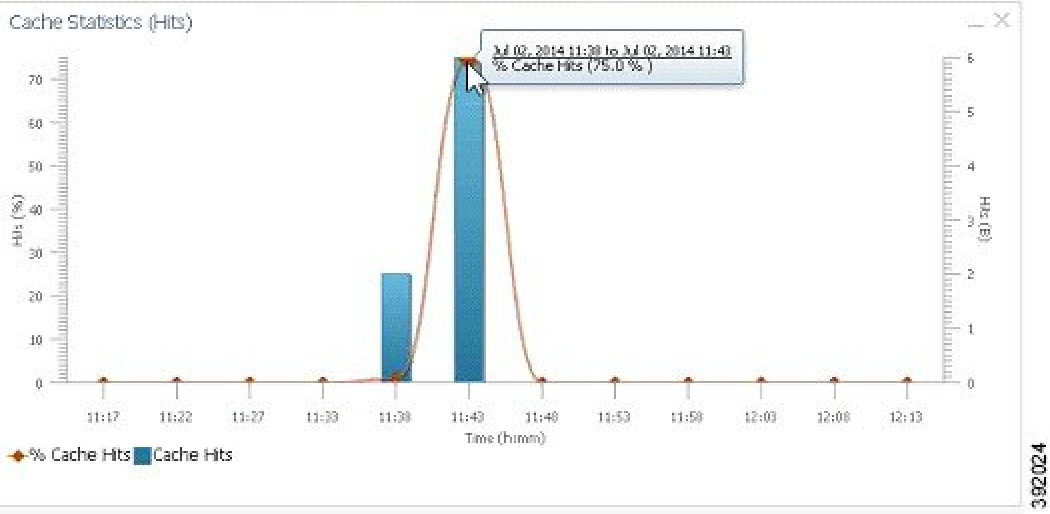
Note Information in the Top Sites chart corresponds to the output for the show statistics accelerator http object-cache EXEC command. Top ten sites information is shown as top hosts information, in the Object cache top hosts ordered by: hit count, output section for 0 to 10 hosts. For more information on CLI commands, see the Cisco Wide Area Application Services Command Reference Guide .

Cache Statistics (Hits)

The **Cache Statistics (Hits)** chart displays information on cache hits or on data served from the cache, in bar chart format. For each type of **Cache Statistics** chart, you can specify a time frame of Last Hour, Last Day, Last Week, Last Month, or set a Custom one.

- The Cache Statistics Hits chart shows the percentage and the number of cache hits (in millions) over a specified time frame.If you hover your mouse over a data point, the total percentage of cache hits for that data point is displayed.If you hover your mouse over a bar, the number of hits, in millions, is displayed.
- The Cache Statistics Data Served from Cache chart shows the percentage and the amount of data served from cache (in MB) over a specified time frame.If you hover your mouse over a data point, the total percentage of cache hits for that data point is displayed. If you hover your mouse over a bar, the total amount, in MB, of data served from the cache, is displayed.

Figure 95: Example of Cache Statistics Hits Chart Showing a Detailed View of a Data Point



Connection Trend Charts

This section contains the following topics:

Optimized Connections Over Time

The Optimized Connections Over Time chart displays the number of optimized connections over the selected time period. You can show the number of MAPI-reserved connections by checking the **MAPI Reserved Connections** check box. You can view the peak optimized connection values for all the data points in the chart by checking the **Peak Connections** check box. If you have opted to view the peak connections, the chart shows a combination of Optimized Connections as stacked legends and Peak Connections as overlaid lines for selected application/classifiers. In WAAS-XE devices, the **Optimized Connections Over Time** chart has only the **Peak Connections** option. You can customize the chart by choosing specific applications to be included. The default is all traffic.

The peak connection value is available for the following:

- **Last Hour**: The maximum value (optimized, pass-through connections counters) among the12 data samples available for the last hour.
- **Last Day**: The maximum value (optimized, pass-through connection counters) among the 12 data samples for each hour. For example, if the optimized connection counter values are 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110, and 120 for an hour, the peak optimized connection value would be 120.

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

Optimized vs Pass-Through Connections

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

You can view the peak pass-through connection values for all the data points in the chart by checking the Peak Connections check box.

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

Formula:

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

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

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

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

AppNav Charts

This section contains the following topics:

Total AppNav Traffic

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

AppNav Policies

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

From the **Show Details For** drop-down list, select a policy rule for viewing.

Top 10 AppNav Policies

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

From the Show Details For drop-down list, select a policy rule for viewing.

Top 10 Cisco WAAS Node Group Distribution

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

From the **Show Details** For drop-down list, select a Cisco WAAS Node Group whose individual Cisco WAAS node details you want to view.

Cisco WAAS Node Group Distribution

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

From the **Show Details** For drop-down list, select a Cisco WAAS Node Group whose individual Cisco WAAS node details you want to view.

Pass-Through Reasons

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

From the Show Details For drop-down list, select a reason whose details you want to view.

Top 10 Pass-Through Reasons

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

From the Show Details For drop-down list, select a reason whose details you want to view.

Platform Charts

This section describes these charts:

CPU Utilization

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

Disk Utilization

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

SMB Preposition Chart

The SMB Preposition chart represents the usage of SMB Pre-positioning feature.

This chart is applicable at the device level. It is a combination chart that collects statistics for every 5 minutes from statistics infrastructure and plots the graph to represent the below information based on the statistics collected.

- Data Served from cache (in bytes)
- Percentage of data served from cache.

Cisco WAAS Table Descriptions

This section describes tables that provide information on system, device, traffic and acceleration, For information on charts that you can choose to include in a dashboard or report, see Cisco WAAS Chart Descriptions, on page 566.

The following statistics details tables are available:

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

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

- **Original Inbound**: Traffic that is entering the Cisco WAAS device from the LAN (clients), and needs to be optimized before being sent out on the WAN to a peer Cisco WAAS device.
- **Original Outbound**: Traffic that is exiting the Cisco WAAS device to the LAN (clients) after being received on the WAN from a peer Cisco WAAS device.
- **Optimized Inbound**: Traffic that is entering the Cisco WAAS device from the WAN, and needs to be processed (deoptimized) before being sent out on the LAN to clients.
- **Optimized Outbound**: Traffic that is exiting the Cisco WAAS device to the WAN and a peer WAAS device after being optimized.
- **Pass-Through**: Traffic that is being passed through the Cisco WAAS device and is not optimized.

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

Traffic Summary Table

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

At the system and location levels, each row in the table displays the total traffic information for each device that is registered to the corresponding Central Manager or is in a particular location. At the device level, each row in the table displays the total traffic information for each application defined on the device. The data is described in the following table.

Table 73: Traffic Summary Table

Table Column	Description and Formulas Used to Calculate Value
Device	Displays the device name. (Appears only at the system and location levels.)
Application	Displays the application name. (Appears only at the device level.)
Original Traffic (Excludes Pass-Through)	Reports the amount of original traffic, excluding pass-through traffic. System: (Original Outbound + Original Inbound) / 2 Device / Device Group: Original Inbound + Original Outbound
Optimized Traffic (Excludes Pass-Through)	Reports the amount of optimized traffic, excluding pass-through traffic. System: (Optimized Inbound + Optimized Outbound)/2 Device/Device Group: Optimized Outbound + Optimized Inbound
Pass-Through Traffic	Reports the amount of pass-through traffic. (This value is not applicable for WAAS Express devices.) System: (Pass-through Client + Pass-through Server) / 2 Device/Device Group: Pass-through Client + Pass-through Server An asterisk (*) in the column heading indicates that a device whose data is included in this table is configured as a serial peer with another device and optimization is disabled between those two peer devices. The amount of pass-through traffic shown may be more than what is expected because the device passes through traffic coming from its peer. For more information, see About Clustering Inline Cisco WAEs in Chapter 5, "Configuring Traffic Interception."
Reduction (%)	Reports the percentage of bytes saved, considering only optimized traffic. (Original Excl Pass-through – (Optimized)) * 100 / (Original Excl Pass-through)
Effective Capacity	Reports the effective bandwidth capacity of the WAN link as a result of optimization, as a multiplier of its base capacity, considering only optimized traffic. 1 / (1 – % Reduction Excl Pass-through)

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

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

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

Network Application Traffic Details Table

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

HTTP Acceleration Statistics Table

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

Table 74: HTTP Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Device	Displays the device name. (Appears only at the system level.)
Start Time and End Time	Displays the start time and end time for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of HTTP connections handled for the time period.
Average Active Connections/Active Connections	Reports the average active number of connections currently being handled by the HTTP accelerator at the system level. At other levels, reports the number of active connections.
New Bypassed Connections	Reports the number of connections initially received by the HTTP accelerator and then pushed down to the generic accelerator.
Total Time Saved	Reports the amount of time saved due to HTTP optimization.
Total Round-Trip Time	Reports the total round-trip time for all connections plus the time for remotely served metadata cache misses.

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

HTTPS Acceleration Statistics Table

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

Table 75: HTTPS Acceleration Statistics Table

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

ICA Acceleration Statistics Table

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

Table 76: ICA Acceleration Statistics Table

Table Column	Description and Formulas Used to Calculate Value
Device	Displays the device name. (Appears only at the system level. WAAS Express devices are not included.)
Start Time and End Time	Displays the start time and end time for the time period. (Appears only at the device level.)

Table Column	Description and Formulas Used to Calculate Value
New Connections Handled	Reports the number of ICA connections handled for the time period.
Average Active Connections/Active Connections	Reports the average number of connections currently being handled by the ICA accelerator at the system level. At other levels, reports the number of active connections.
Dropped Connections	Reports the number of connections dropped by the ICA accelerator.
Bypassed Connections	Reports the number of connections initially received by the ICA accelerator and then pushed down to the generic accelerator.

MAPI Acceleration Statistics Table

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

Table 77: MAPI Acceleration Statistics Table

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

SMB Acceleration Statistics Table

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

Table 78: SMB Acceleration Statistics Table

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

SSL Acceleration Statistics Table

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

Table 79: SSL Acceleration Statistics Table

Table Column	Description
Device	Displays the device name. (Appears only at the system level.)
Start Time and End Time	Displays the start time and end time for the time period. (Appears only at the device level.)
New Connections Handled	Reports the number of SSL connections handled for the time period.
Average Active Connections/Active Connections	Reports the average number of connections currently being handled by the SSL accelerator at the system level. At other levels, reports the number of active connections.
New HTTPS Connections Handled	Reports the number of HTTPS connections handled by the SSL accelerator.
New ICA Connections Handled	Reports the number of ICA connections handled by the ICA accelerator.
Dropped Connections	Reports the number of connections dropped by the SSL accelerator.

Table Column	Description
Bypassed Connections	Reports the number of connections initially received by the SSL accelerator and then pushed down to the generic accelerator.

Using Predefined Reports to Monitor WAAS

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

You can customize these predefined reports by editing them with the **Manage Report** function available in the **Monitor** menu, as described in Viewing and Editing a Report, on page 605.

This section contains the following topics:

Predefined Reports Available by Cisco WAAS Level

The following table shows predefined reports available at the system, AppNav cluster, location, and device level.

Table 80: Predefined Reports Available at the System, AppNav Cluster, Location, and Device Level

Report Type	Available Reports
Optimization	• TCP Summary Report, on page 590
Acceleration (not all reports available for WAAS Express device level)	• HTTP Acceleration Report, on page 590 • HTTPS Acceleration Report, on page 590 • SSL Acceleration Report, on page 591 • MAPI Acceleration Report, on page 591 • SMB Acceleration Report, on page 591 • Summary Report, on page 592
Caching and Akamai Connected Cache	• Cache Statistics (Hits), on page 579 • Throughput Summary for Akamai Connect, on page 576 • HTTP: Bandwidth Savings, on page 577 • Top Sites, on page 578

The following table shows the predefined reports available at specified Cisco WAAS levels.

Table 81: Predefined Reports Available at Specified Levels

Cisco WAAS Level	Report Type	Available Reports
System level	• Network	• Summary Report, on page 592
System and Device levels	• Network/Peers	• Topology Report, on page 593
Device and Location levels	• Optimization	• Connection Trend Report, on page 593
Device level	• Optimization	• Connections Statistics Report, on page 593
	• Acceleration	• SMB Acceleration Report, on page 591
	• Platform (not available at WAAS Express or AppNav-XE device level)	• Resource Utilization Report, on page 595 • Disks Report, on page 595
AppNav Cluster level and Device level for AppNav Controller devices	• AppNav	• AppNav Report, on page 596

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

Location-Level Reports

Before you begin

Location-level reports aggregate data from all the Cisco WAEs present in a particular location. For more information about locations, see Working with Device Locations in the chapter "Using Device Groups and Device Locations."

Procedure

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

Step 2 From the Cisco WAAS Central Manager menu, choose **Monitor** and choose the report from the **Optimization** or **Acceleration** categories.

Step 3 Considering the following operating guidelines:

- When scheduling any report, you can also select one or more locations; the report will include data from all the devices within the selected locations. For more information, see Scheduling a Report, on page 605.
- The maximum number of devices supported in a location-level report is 25 by default. This number is configurable up to 250 by the **System.monitoring.maxDevicePerLocation** system property. For more information, see Modifying Default System Properties in the chapter "Configuring Other System Settings."

TCP Summary Report

The Transmission Control Protocol (TCP) Summary report displays a summary of all traffic. The following charts and tables are included:

HTTP Acceleration Report

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

The Cisco WAAS Central Manager provides monitoring information on the following types of caching: **Basic**, **Standard**, **Advanced**, **Bypass**, and **Connected Cache**. Except for the **Top Sites** chart, you can view monitoring information at the device, network, location, or AppNav cluster levels. The following charts are included:

- Akamai Connected Cache Charts, on page 575
    - Cache Statistics (Hits), on page 579
    - Throughput Summary for Akamai Connect, on page 576
    - HTTP: Bandwidth Savings, on page 577
    - Top Sites, on page 578

HTTPS Acceleration Report

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

- HTTPS: Estimated Time Savings, on page 570
- HTTPS: Effective WAN Capacity , on page 570
- HTTPS: Connection Details, on page 569
- HTTPS: Response Time Savings, on page 570
- HTTPS: Optimization Count, on page 570
- HTTPS: Optimization Techniques, on page 570
- HTTPS Acceleration Statistics Table, on page 585

SSL Acceleration Report

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

- SSL: Connection Details, on page 570
- SSL: Effective WAN Capacity, on page 571
- SSL: Acceleration Bypass Reason, on page 570
- SSL Acceleration Statistics Table, on page 587

MAPI Acceleration Report

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

- MAPI: Average Response Time Saved, on page 571
- MAPI: Effective WAN Capacity , on page 572
- MAPI: Connection Details, on page 571
- MAPI: Request Optimization, on page 572
- MAPI: Response Time Optimization, on page 572
- MAPI: Average Accelerated Client Sessions, on page 572
- MAPI: Acceleration Bypass Reason, on page 571
- MAPI Acceleration Statistics Table, on page 586

SMB Acceleration Report

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

- SMB: Average Response Time Saved, on page 573
- SMB: Effective WAN Capacity, on page 574
- SMB: Connection Details, on page 573
- SMB: Request Optimization, on page 574
- SMB: Response Time Savings, on page 574
- SMB: Client Average Throughput, on page 573
- SMB: Versions Detected, on page 574
- SMB Acceleration Statistics Table, on page 586

ICA Acceleration Report

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

- ICA: Effective WAN Capacity , on page 575
- ICA: Connection Details, on page 574
- ICA: Client Versions , on page 574
- ICA: Unaccelerated Reasons, on page 575
- ICA Acceleration Statistics Table, on page 585

Note The ICA charts in Cisco WAAS Version 5.0 and later are different from those used in Version 4.5. If you are viewing the data from a Cisco WAAS device running Cisco WAAS Version 4.5, the charts appear empty due to the different data that the device is collecting. The ICA data for Cisco WAAS devices running Cisco WAAS Version 4.5 is available in the system-level TCP Summary Report. For more information, see TCP Summary Report, on page 590.

Summary Report

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

- Traffic Summary, on page 568
- Effective WAN Capacity, on page 567
- Traffic Summary Over Time, on page 568
- Traffic Volume and Reduction, on page 568
- Compression Summary, on page 567
- Compression Summary Over Time, on page 567
- HTTP: Estimated Time Savings, on page 569
- HTTP: Effective WAN Capacity, on page 569
- MAPI: Effective WAN Capacity , on page 572
- SSL: Effective WAN Capacity, on page 571
- MAPI: Average Response Time Saved, on page 571

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

Topology Report

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

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

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

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

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

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

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

Connection Trend Report

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

- Optimized Connections Over Time, on page 579

  (included only at the device level)
- Optimized vs Pass-Through Connections, on page 580

Connections Statistics Report

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

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

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

The **Connection Statistics** table displays the following information about each connection:

- Source IP address and port.
- Destination IP address and port.
- Peer ID: Hostname of the peer device.
- Applied Policy/Bypass Reason: Displays icons representing the applied optimization policies, including TFO, DRE, LZ, and an application accelerator, respectively. (Hover your mouse over the icon to see its meaning.) If the connection is not optimized, the bypass reason is shown.
- Connection Start Time: Date and time at which the connection was started.
- Open Duration: Number of hours, minutes, and seconds that the connection has been open.
- Total number of original bytes.
- Total number of optimized bytes.
- Percentage of compression.
- Class map name: If no class map exists for the connection, this column contains a dash. To create a class map for this connection, click the radio button at the left of the row and then click the Create Class-Map taskbar icon to display the **Optimization Class-Map** pane. For more information, see the chapterConfiguring Application Acceleration, on page 371.

Note If the WAE is inheriting policies from a device group, the **Create Class-Map** button is dimmed, to prevent a user from unknowingly overriding device group policies. To create a class map, you must first override the device group policy page and then return to the Connection Statistics report.

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

From the **Connections Statistics** table, you can perform the following tasks:

- Apply filter settings to display particular connections based on specific criteria, by choosing Quick Filter from the Show drop-list in the taskbar.
- To refresh the table, click the **Refresh** taskbar icon.
- To export the table to a spreadsheet, click the **Export** taskbar icon.
- To view connection details, click the **Details** icon next to the connection entry.

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

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

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

Resource Utilization Report

The Resource Utilization report displays the following charts:

CPU Utilization

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

Disk Utilization

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

Disks Report

The **Disks Report** displays physical and logical disk information.

The report window displays the following information about each disk:

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

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

AppNav Report

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

The following charts and tables are included:

- Total AppNav Traffic, on page 580
- AppNav Policies, on page 581
- Top 10 AppNav Policies, on page 581
- Top 10 Cisco WAAS Node Group Distribution, on page 581
- Cisco WAAS Node Group Distribution, on page 581
- Pass-Through Reasons, on page 581
- Top 10 Pass-Through Reasons, on page 581

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

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

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

Exported Reports

Using the spreadsheet icon in the Central Manager taskbar, you can export chart values to a CSV file.

The following "Exported Report Column Headings" table provides descriptions of report column headings for exported reports. Because there are many report column headings, the table is divided into categories by types of traffic, in alphabetical order. For these heading descriptions, a time specification (for example, milliseconds) is not noted, as the time specification may change depending on the time period specified for the report (for example, hour or week).

Table 82: Exported Report Column Headings

Report Column Heading	Description
Akamai Connected Cache	

Report Column Heading	Description
ce_cachetype_hit_count ce_cachetype_hit_miss ce_cachetype_hit_response ce_cachetype_wan_response	For the Akamai Connect Cache Engine, exported reports show the following types of information: Hit Count—The top URLs by number of cache hits. Hit Miss—The number of object cache responses not cached. Hit Response—The number of object cache response bytes for cache-hit transactions. WAN Response—The top URLs by number of bytes served over the WAN. Depending on which cache types are enabled and what traffic is seen, the output may show statistics for any or all of the following cache types: • Connected Cache (example: ce_connect_hit_count) • Bypass (example: ce_bypass_hit_miss) • Standard, (example: ce_standard_hit_response) • Basic (example: ce_basic_wan_response) • Advanced (example: ce_advanced_hit_count) • OTT-youtube (example: ce_ott_hit_miss) • OTT-generic (example: ce_ott-generic_hit_response) • unknown (example: ce_unknown_wan_response)
total_aggregate_time_saved	Aggregated amount of time saved due to Akamai Connect caching.
Akamai Connected Cache Top Sites	
Hit Count	The top URLs by number of cache hits.
Response Time Savings	The response time saved due to Akamai Connect caching.
Site	The names of the top sites being served by the Akamai Cache Engine, in terms of hostname and traffic.
Timestamp	The date and time of the information recorded, for each row of the report.
WAN Offload	The top URLs by number of bytes served out of the cache, and as a result did not come over the WAN.
WAN Response	The top URLs by number of bytes served over the WAN.

Report Column Heading	Description
Application, Time, and Time Saved	
timestamp	The date and time of the information recorded, for each row of the report.
Application Name	Type of application for the reported data, such as enterprise, backup, replication, file system, email and messaging, file system, storage, web. file transfer, streaming, printing, or remote desktop.
time_saved	Total response time saved, for cache hit transactions. The time is incremented on the client side WAE by one RTT whenever an idle fast connection is reused instead of establishing a new WAN connection.
total_adjusted_download_time	The total adjusted download time.
total_aggregate_time_saved	Aggregated amount of time saved due to Akamai Connect caching.
Cache Control Header and Cache	
httpao_requests_cache_control_denies_cached_resp	Number of requests not to be cached, as specified by a Cache-Control header.
httpao_responses_cache_control_prevents_caching	Number of OK (200), Redirected (301), Not Modified (304), and Unauthorized (401) responses not to be cached, as specified by a Cache-Control header.
httpao_long_url	Number of responses not cached because the URL is longer than 255 characters. The URL length includes the length of the destination IP address.
httpao_total_time_cache_miss httpao_total_time_cache_miss_https	For HTTP/S, total time for HTTP AO cache misses.
Connections: Active, Dropped, Incomplete, Pending	
active connections	Number of WAN side connections currently established and either in use or free for fast connection use.
active_https_connections	Number of active HTTPS connections.
maximum_active_connections	Maximum value reached by the Current Active Connections counter. Maximum Active Connections is reset if the accelerator is restarted or if statistics are cleared.
dropped_connections	Number of connections dropped for any reason other than client/server socket errors or close (for example, out of resources).

Report Column Heading	Description
incomplete_connect	Number of SSL CONNECT requests with an incomplete message.
pending_connections	Number of connections pending to be accepted.
Connections: Handled, Optimized, Prepositioned	
handled_connections	Number of connections handled since the accelerator was started or its statistics were last reset; incremented when a connection is accepted or re-used; never decremented.
handled_https_connections	Number of HTTPS connections handled since the accelerator was started or its statistics were last reset; incremented when a connection is accepted or re-used; never decremented.
optimized_connections	Number of connections previously and currently optimized by the accelerator.
total_optimized_connections_https	For HTTPS, the total number of optimized connections.
Optimized Single Sided Connections	Number of optimized connections using single-sided mode.
preposition connections	Number of prepositioned connections.
Opt TCP Only Connections	Number of current active connections using TFO optimization only.
optimized TCP Plus Connections	Number of current active connections using DRE/LZ compression/optimization or handled by an accelerator.
Connections: Idle, Reused, Timeout	
idle	Number of Current Active Connections that are idle and available for reuse as a fast connection. Incremented when an in-use active connection becomes idle and is available for reuse as a fast connection; decremented an available idle active connection is reused or its idle timeout (5 secs) is reached.
reused	Number of times a client-side idle active WAN connection was able to be reused instead of establishing a new WAN connection.
reuse_failed	Number of times a client-side idle active WAN connection was attempted to be re-used but the reuse failed.

Report Column Heading	Description
max_reused	Maximum number of times a single connection was reused. This is the “best case” of number of reuses on a single connection.
reused_peer	Number of times a peer WAAS device connection was reused instead of establishing a new connection.
http_time_saved_fast_reuse	Time saved by fast connection reuse.
ao_syn_hndling_timeouts	Number of SYN (synchronize/start) timeouts because the AO accelerator was temporarily busy.
Connections: Handoffs, Pass Through, Piped Through	
handoff_failed	Number of connections attempted to be handed off but the handoff failed.
ssl_handoff	Number of connections handed off to the SSL accelerator as a result of SSL CONNECT requests received by the HTTP accelerator.
total_handoff	Total number of connections handed off.
PT Config Connections	Number of pass-through connections offloaded due to missing policy configurations.
PT Intermediate Connections	Number of pass-through connections due to an intermediate WAAS node.
PT Other Connections	Number of pass-through connections offloaded due to other reasons.
PT No Peer Connections	Number of pass-through connections offloaded due to the absence of a peer WAAS node.
pipe_through_connections	Number of connections bypassed by the SSL accelerator due to, for example, SSL cipher negotiated on the flow is not supported on the WAAS device, or the destination domain did not match domains to be accelerated.
pipe_through_uncompressed	The number of connections bypassed
DRE and LZ Compression	
httpao_dre_hints_flush httpao_dre_hints_flush_https	For HTTP/S, number of DRE hints by SMB accelerator to flush data.
httpao_dre_hints_skip_bytes httpao_dre_hints_skip_bytes_https	For HTTP/S, number of DRE hints by SMB accelerator to skip the header bytes.

Report Column Heading	Description
httpao_dre_hints_skip_lz httpao_dre_hints_skip_lz_https	Number of DRE hints by SMB accelerator to skip LZ compression.
httpao_accept_encoding_removed httpao_accept_encoding_removed_https	Number of HTTP/S requests with Accept-Encoding removed from the HTTP/S header (preventing the server from compressing HTTP/S data and allowing the WAE to apply its own compression).
Locally Served and Remotely Served	
httpao_locally_served_if_not_modified httpao_locally_served_if_not_modified_https	Number of locally served HTTP/S Not Modified (304) responses.
httpao_locally_served_redirect httpao_locally_served_redirect_https	Number of locally served HTTP Redirect (301) responses.
httpao_locally_served_unauthorized httpao_locally_served_unauthorized_https	Number of locally served HTTP/S Unauthorized (401) responses.
httpao_remotely_served_if_not_modified	Number of remotely served Not Modified (304) responses (cache misses).
httpao_remotely_served_redirect	Number of remotely served Redirect (301) responses (cache misses).
httpao_remotely_served_unauthorized	Number of remotely served Unauthorized (401) responses (cache misses).
Round Trip Time (RTT)	
setup_rtt	The initial RTT time, in milliseconds.
rtt	Round trip time saved for all WAN connections that have been established.
http_if_not_modified_cache_saved_rtt http_if_not_modified_cache_saved_rtt_https	For HTTP/S, round trip time saved by caching and locally serving Not Modified (304) responses, in milliseconds.
http_redirect_cache_saved_rtt http_redirect_cache_saved_rtt_https	For HTTP/S, round trip time saved by caching and locally serving Redirected (301) responses.
http_unauth_cache_saved_rtt http_unauth_cache_saved_rtt_https	For HTTP/S, round trip time saved by caching and locally serving Unauthorized (401) responses.
total_rtt_saved_all_caches_https	Total round trip time saved for all response types.
httpao_sharepoint_saved_rtt httpao_sharepoint_saved_rtt_https	For HTTP/S, total response time saved for HTTP AO in accessing SharePoint objects by enabling SharePoint optimization.

Report Column Heading	Description
Session	
httpao_move_session_to_v1_on_request	The number of HTTP AO transactions moved to the NTLM Version 1 Security Model on request, for this session.
httpao_move_session_to_v1_on_response	The number of HTTP AO transactions moved to the NTLM Version 1 Security Model on response, for this session.
httpao_pipelined session	Number of HTTP AO pipelined transactions during the session.
httpao_session_auth_required	Number of HTTP AO Unauthorized (401) responses for the session.
httpao_sharepoint_session_hit_count httpao_sharepoint_session_hit_count_https	Number of HTTP/S sessions using the SharePoint optimization feature to access objects from the SharePoint server.
Sharepoint	
httpao_sharepoint_saved_rtt httpao_sharepoint_saved_rtt_https	For HTTP/S, total response time saved for HTTP AO in accessing SharePoint objects by enabling SharePoint optimization.
httpao_total_time_sharepoint_miss httpao_total_time_sharepoint_miss_https	For HTTP/S, total time lost in accessing SharePoint data that is not already stored in cache.
httpao_sharepoint_session_hit_count httpao_sharepoint_session_hit_count_https	Number of HTTP/S sessions using the SharePoint optimization feature to access objects from the SharePoint server.
Throughput	
Original Throughput In(bits/sec)	Original input throughput, in bits per second.
Optimized Throughput Out(bits/sec)	Optimized output throughput, in bits per second.
Original Throughput Out(bits/sec)	Original output throughput, in bits per second.
Optimized Throughput In(bits/sec)	Optimized input throughput, in bits per second.
Original Peak Throughput In(bits/sec)	Original peak input throughput, in bits per second.
Optimized Peak Throughput Out(bits/sec)	Optimized peak output throughput, in bits per second.
Original Peak Throughput Out(bits/sec)	Original peak output throughput, in bits per second.
Optimized Peak Throughput In(bits/sec)	Optimized peak input throughput, in bits per second.
Transactions	

Report Column Heading	Description
httpao_handled_transaction	Number of HTTP AO handled transactions.

Managing Reports

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

This section contains the following topics:

Creating a Custom Report

This section contains the following topics:

Creating a New Custom Report

Before you begin

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

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

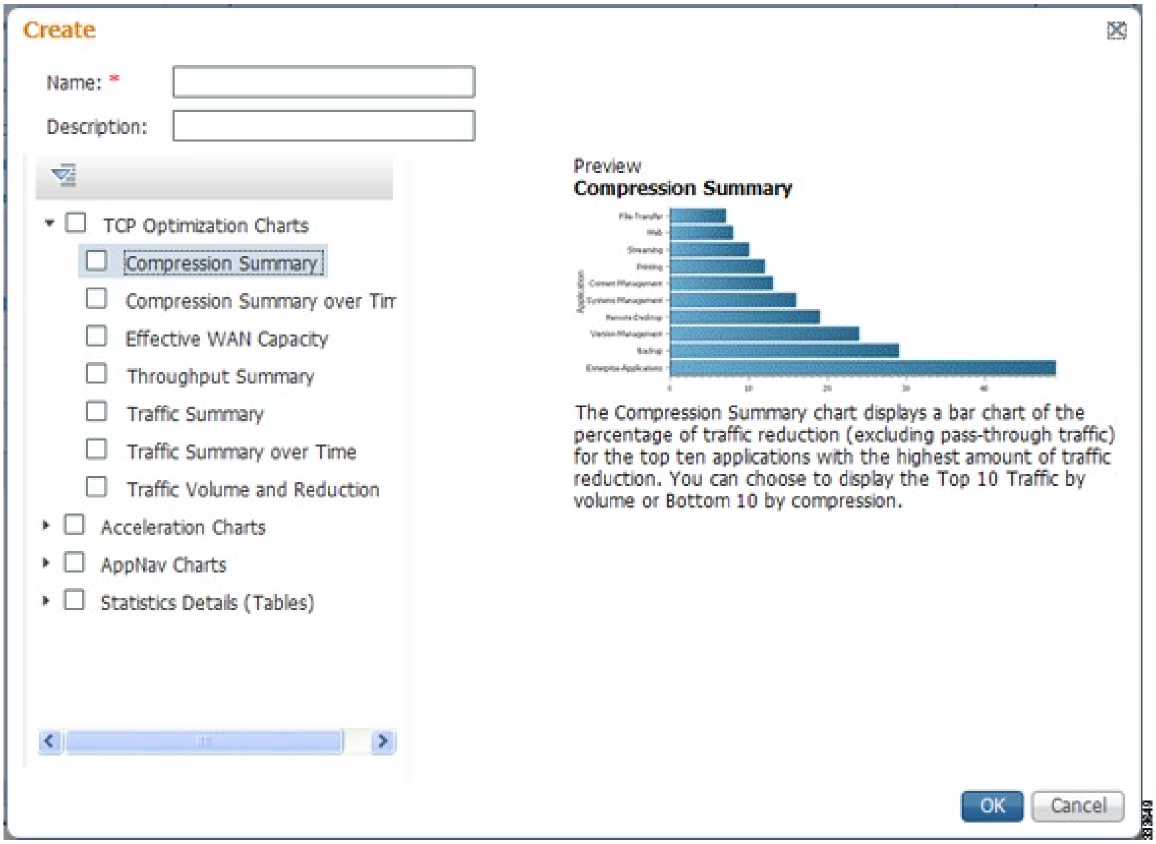
Procedure

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

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

The **Create Report** pane appears.

Figure 96: Create Report Pane



Create

Name: *

Description:

▾ □ TCP Optimization Charts

□ Compression Summary

□ Compression Summary over Tir

□ Effective WAN Capacity

□ Throughput Summary

□ Traffic Summary

□ Traffic Summary over Time

□ Traffic Volume and Reduction

▸ □ Acceleration Charts

▸ □ AppNav Charts

▸ □ Statistics Details (Tables)

Preview

Compression Summary

The Compression Summary chart displays a bar chart of the percentage of traffic reduction (excluding pass-through traffic) for the top ten applications with the highest amount of traffic reduction. You can choose to display the Top 10 Traffic by volume or Bottom 10 by compression.

Step 3 In the **Name** field, enter a name for the report. The maximum is 64 characters. Only numerals, letters, spaces, periods, hyphens, and underscores are allowed.

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

Step 5 In the list at the left side of the pane, check the check box next to each chart and table that you want to be displayed in the report. For more information, see Cisco WAAS Chart Descriptions, on page 566.

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

Step 6 Click **OK**.

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

a) To display the report, click the report name in the **Report Templates** table.

b) You can customize report settings, such as the time frame and the time zone, as described in Customizing a Dashboard or Report, on page 562.

c) To customize the chart settings, click the **Edit** icon in the upper left of a chart. For more information, see Configuring Chart Settings, on page 565.

d) Click **OK**.

Repeat the steps for each chart you want to customize.

Creating a New Custom Report from an Existing Report

Procedure

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

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

Step 3 Click the **Copy** taskbar icon.

The **Copy Report** window appears.

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

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

Step 6 Click **OK**.

The report is added to the **Reports** table.

Viewing and Editing a Report

Procedure

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

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

You can filter the list by choosing **Quick Filter** from the **Show** drop-down list and entering filter criteria.

Step 3 To change any of the charts or tables in the report, use the standard chart editing methods, as described in Customizing a Dashboard or Report, on page 562.

Step 4 Click **Save** to save the report, or click Save As to save the report under a different name.

What to do next

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

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

Scheduling a Report

Before you begin

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

Note You cannot delete a scheduled custom report after you have scheduled it and it is in pending status. You can delete a report only after it has been generated.

Procedure

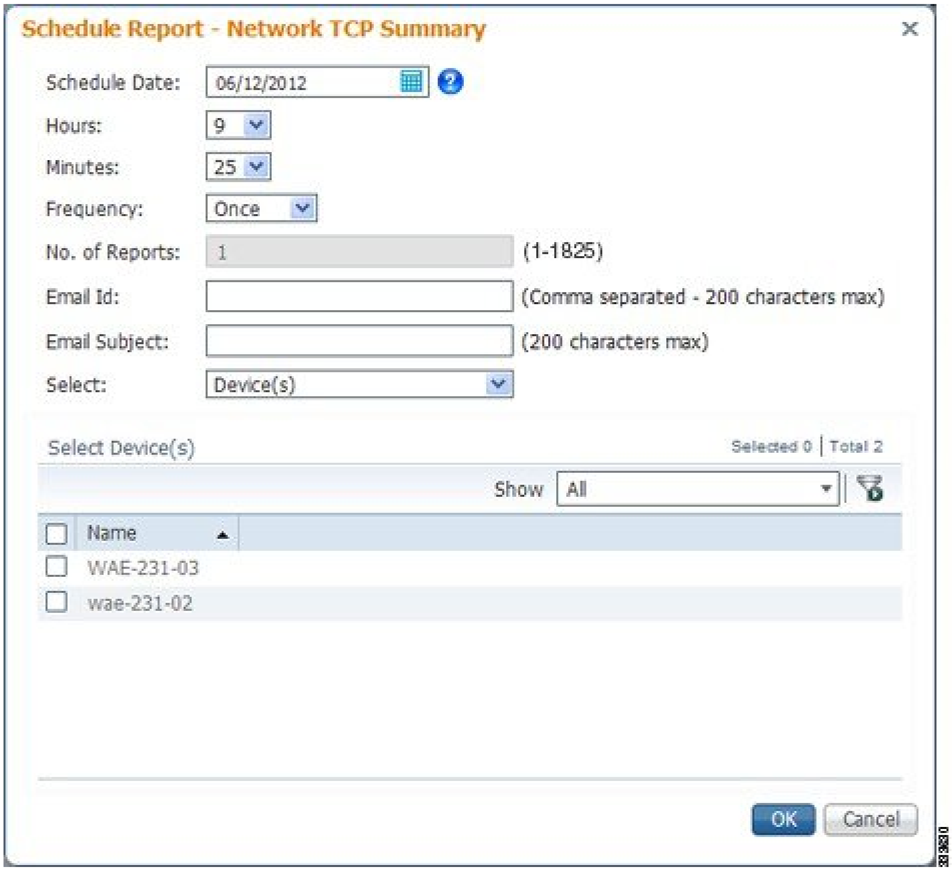
Step 1 From the Cisco WAAS Central Manager menu, choose **Monitor** > **Reports** > **Reports Central**.

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

Step 3 Click the **Schedule** icon in the taskbar.

The **Schedule Report** window appears.

Figure 97: Scheduling a Report



Schedule Report - Network TCP Summary

Schedule Date: 06/12/2012

Hours: 9

Minutes: 25

Frequency: Once

No. of Reports: 1 (1-1825)

Email Id: (Comma separated - 200 characters max)

Email Subject: (200 characters max)

Select: Device(s)

Select Device(s) Selected 0 | Total 2

Show All

□	Name ▲
□	WAE-231-03
□	wae-231-02

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

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

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

Step 7 In the **Frequency** drop-down list, choose the report frequency (**Once**, **Hourly**, **Daily**, **Weekly**, or **Monthly**). You can now schedule reports for multiple devices for Akamai Connect Reports. This is available only if you schedule a **Monthly** report.

- Select the **Aggregate** box to receive an aggregate report of all devices called **statistics.csv**. These files are stored in the **ftpconfig.properties** file in the FTP server that needs to be configured before.
- Deselect the **Aggregate** box to receive individual reports for all devices. This report is called **devicename_ddmmyyyy.csv**.

Step 8 In the **No. of Reports** field, enter the number of times a reoccurring report is to be generated. You can schedule it to be generated for up to 1825 times. After being generated the specified number of times, the report is no longer generated.

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

Step 10 In the **Email Id** field (enabled only when the **Email PDF** or **Email CSV** check box is checked), enter the email addresses of the report recipients, separated by commas.

Step 11 In the **Email Subject** field, enter the subject of the email message.

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

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

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

Step 14 Click **OK**.

Step 15 Configure the email server settings for e-mail notification when reports are generated. For more information, see Configuring the Email Notification Server in the chapter "Configuring Other System Settings."

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

Viewing or Deleting a Scheduled Report

Procedure

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

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

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

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

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

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

Consider the following operating guidelines:

- Cisco WAAS stores the 10 most recently completed or failed report instances for each custom report. This number is configurable by the **System.monitoring.maxReports** system property. For more information, see Modifying Default System Properties in the chapter "Configuring Other System Settings."
- Admin users can view reports scheduled by all users or the name of the report creator. Nonadmin users can view only reports scheduled by themselves.
- Any changes to predefined report settings are stored separately for individual users. That is, if one user changes a predefined scheduled report, only that user sees the changes, and other users (including admin users) continue to see the report with default settings.
- Reports scheduled by an external user are deleted if the maximum limit of days without a login passes and the user is deleted. For more information, see the **cdm.remoteuser.deletionDaysLimit** system configuration property in Modifying Default System Properties in the chapter "Configuring Other System Settings.

Note You cannot delete a scheduled custom report after you have scheduled it and it is in pending status. You can delete a report only after it has been generated.

Configuring Flow Monitoring

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

Configuring Flowing Monitoring with NetQoS

This section contains the following topics:

About Flow Monitoring with NetQoS

The NetQoS monitoring application can interoperate with the Cisco WAAS software to provide flow monitoring. To integrate this application with the Cisco WAAS software, configure the NetQoS FlowAgent module on the WAE devices. The NetQoS FlowAgent module on the WAE collects important metrics of packet flows, which are then sent across the network to the NetQoS SuperAgent. This monitoring agent analyzes the data and generates reports. For this feature to work, additional configuration is required on the NetQoS FlowAgent. (See the Example: Using NetQoS for Flow Monitoring, on page 610.)

The monitoring agent comprises two modules: the console (or host) and the collector. The WAE initiates two types of connections to these two monitoring agent modules: a temporary connection to the console and a persistent connection to the collector.

Configuration Considerations for Flow Monitoring with NetQoS

Consider the following when you configure flow monitoring with NetQoS:

- Configure the console IP address on the WAE by entering the **flow monitor tcpstat-v1 host** global configuration mode command in either the WAE CLI or through the Cisco WAAS Central Manager GUI. This temporary connection is referred to as the control connection.
- The control connection uses TCP port 7878. Its purpose is to obtain the IP address and port number of the collector to which the WAE is assigned.
- The WAE also pulls the configuration information regarding which servers are to be monitored over the control connection. After the WAE obtains the IP address and port number of the collector, the WAE opens a persistent connection to the collector. Collected summary data for the servers that are being monitored is sent over this persistent connection.
- You can place the console (or host) module and the collector module on a single device or on separate devices. These connections are independent of one another. Failure of one connection does not cause the failure of the other connection.
- You can view the state of these connections and various operation statistics display with the **show statistics flow monitor tcpstat-v1** EXEC mode command. Connection errors and data transfer errors trigger alarms on the WAE and in the Central Manager GUI. For information on flow monitoring alarms, see Troubleshooting Flow Monitoring Information, on page 616.
- To display debug information, use the **debug flow monitor tcpstat-v1** EXEC mode command.

Configuring Flow Monitoring with NetQoS Using the Cisco WAAS Central Manager

Procedure

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

a) When you create a device group, check the **Automatically assign all newly activated devices to this group** check box to enable this option.
b) Add your existing WAE devices to this new device group.

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

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

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

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

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

Step 6 To apply the settings to the devices in this device group, click **Submit**.

Configuring Flow Monitoring with NetQoS Using the CLI

Procedure

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

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

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

Step 2 Enable flow monitoring on the WAE appliance.

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

Step 3 To check the configuration, run the **show running-config** EXEC command.

Example: Using NetQoS for Flow Monitoring

Before you begin

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

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

Procedure

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

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

Step 2 From the **NetQoS SuperAgent** console, assign a WAE to a SuperAgent Aggregator (known as the collector in Cisco WAAS terminology) and configure the NetQoS networks, servers, and applications entities.

Configuring Flow Monitoring with NetFlow v9

This section contains the following topics:

About Flow Monitoring with NetFlow v9

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

Cisco WAAS Version 5.3.1 and later provide the following features for Netflow v9:

- Unlike NetFlow v5, which used a fixed format, NetFlow v9 utilizes a template format. All Cisco WAAS optimization engines can use this template format to export data to collectors such as Cisco Prime and Solarwinds.
- The template format allows new features to be quickly added to NetFlow v9.
- Templates are verified every few minutes for changes, and sent out hourly to provide collectors with field information for data records.
- NetFlow v9 uses Cisco WAAS transaction log information and adds an exporter code to allow data to be sent to external devices.
- NetFlow v9 can be used on all Cisco WAAS optimization engines; it is not used with Cisco WAAS AppNav.
- By default, all Cisco WAAS class maps are monitored. If you would like to have specific class maps to not be monitored, see Disabling NetFlow v9 Monitoring , on page 612.

Configuration Considerations for Flow Monitoring with NetFlow v9

To configure NetFlow v9 on your WAEs from the CLI, configure four monitoring areas:

- **Flow Record**: Contains the DNA-specific or WAAS-specific flow information or both that you want to send to the collector.
- **Flow Exporter**: Contains the destination details for the exported information, and the format for this information.
- **Flow Monitor**: Specifies which flow records are going to which flow exporter.
- **Class Map**: For Cisco WAAS v5.3.1 and later, monitors are enabled globally on all class map policies by default. If you do not want a particular device monitored, manually disable monitoring for that device.

Procedure for Configuring Flow Monitoring with NetFlow v9

Procedure

Step 1 Use the following command to create a flow record to configure which fields to collect as part of Netflow export:

```
WAE(config)# flow record Record name
WAE(config)# collect waas
```

Table 83: Collection Parameters

Collection Parameter	Description
application-name	Collects application name for the flow.
bytes	Collects byte counts for the flow.
class-name	Collects class name for the flow.
connection mode	Collects connection mode for the flow.
dre in	Collects DRE details for the flow.
lz in	Collects LZ details for the flow.
flow-direction	Collects direction for the flow.
packets	Collects packet counts for the flow.

Step 2 Use the following command to create the flow exporter, which includes the destination IP address and port for the Netflow:

```
WAE(config)# flow exporter ExporterName
WAE(config-flow_exporter)# destination 2.2.2.2
WAE(config-flow_exporter)# description DescriptiveName
WAE(config-flow_exporter)# export-protocol IPFIX
WAE(config-flow_exporter)# transport udp 12000
WAE(config-flow_exporter)# exit
```

Step 3 Use the following command to create the flow monitor and associate the flow record with the flow exporter:

```
WAE(config)# flow monitor MonitorName
WAE(config-flow_monitor)# description DescriptiveName
WAE(config-flow_monitor)# exporter ExporterName
WAE(config-flow_monitor)# record RecordName
WAE(config-flow_monitor)# enable
```

Disabling NetFlow v9 Monitoring

If flow monitoring is configured, it is enabled for all class-maps by default. Use the following command to disable monitoring for a particular class:

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

NetFlow v9 Exported Fields

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

Table 84: NetFlow v9 Exported Fields

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

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

NetFlow v9 Pass-Through Reasons

Pass-Through reasons are sent to the collector. The following table shows pass-through numbers and associated reasons.

Table 85: Pass-Through Number and Pass-Through Reason

Pass-Through Number	Pass-Through Reason
0	PE_CONN_UNKNOWN
1	PE_CONN_PT_APP_CONFIG
2	PE_CONN_PT_GLB_CONFIG
3	PE_CONN_PT_OVERLOAD
4	PE_CONN_PT_CPU_OVERLOAD
5	PE_CONN_PT_IN_PROGRESS
6	PE_CONN_PT_PE_INT_ERROR
7	PE_CONN_PT_DYN_BYPASS
8	PE_CONN_INT_CLIENT

Pass-Through Number	Pass-Through Reason
9	PE_CONN_INT_SERVER
10	PE_CONN_ACCEL_OPTIMIZED
11	PE_CONN_ACCEL_NON_OPTIMIZED
12	PE_CONN_APP_DYN_MITCH_OPTIMIZED
13	PE_CONN_APP_DYN_MITCH_NON_OPTIMIZED
14	PE_CONN_OPT_TCP_PLUS
15	PE_CONN_ORIG_TCP_PLUS
16	PE_CONN_OPT_PREPOSITION
17	PE_CONN_ORIG_PREPOSITION
18	PE_CONN_OPT_TCP_ONLY
19	PE_CONN_ORIGIN_TCP_ONLY
20	PE_CONN_PT_NO_PEER
21	PE_CONN_PT_RJCT_CAPABILITIES
22	PE_CONN_PT_RJCT_RESOURCES
23	PE_CONN_PT_NO_LICENSE
24	PE_CONN_PT_ASYMMETRIC
25	PE_CONN_PT_INTERMEDIATE
26	PE_CONN_PT_FB_INT_ERROR
27	PE_CONN_PT_AD_INT_ERROR
28	PE_CONN_PT_SQ_INT_ERROR
29	PE_CONN_PT_APP_OVERRIDE
30	PE_CONN_PT_SVR_BLACKLIST
31	PE_CONN_PT_AD_VER_MISMATCH
32	PE_CONN_PT_AD_AO_INCOMPAT
33	PE_CONN_PT_AD_AOIM_PROGRESS
34	PE_CONN_PT_DIRM_VER_MISMATCH
35	PE_CONN_PT_DIRM_INT_ERROR
36	PE_CONN_PT_PEER_OVERRIDE

Pass-Through Number	Pass-Through Reason
37	PE_CONN_PT_AD_OPT_PARSE_FAIL
38	PE_CONN_PT_AD_SERIAL_MODE_PEER
39	PE_CONN_PT_INTERCEPTION_ACL
40	PE_CONN_PT_WCCP_SHUTDOWN_ACTIVE
41	PE_CONN_PT_AD_IP_FRAG

Troubleshooting Flow Monitoring Information

This section has the following topics:

Alarms for Flow Monitoring

The following table shows the four different alarms that may be raised when errors occur with flow monitoring.

Table 86: Alarms for Flow Monitoring

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

Commands Used to Troubleshoot Flow Monitoring

The following table shows the commands used to troubleshoot flow monitoring.

Table 87: Commands Used to Troubleshoot Flow Monitoring

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

CHAPTER 16

Troubleshooting Your Cisco WAAS Network

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

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

This chapter contains the following sections:

Cisco WAAS Troubleshooting Guidelines

To troubleshoot your Cisco WAAS system, follow these guidelines:

1. Maintain a consistent and recommended software version across all your Cisco WAAS devices.

   If versions must differ, the Cisco WAAS Central Manager must be running the highest version. To determine the version in use, see Verifying the Cisco WAAS Image, on page 623.

2. See the Cisco WAAS Release Note for your Cisco WAAS software version.

See the Release Note for Cisco Wide Area Application Services for the latest features, operating considerations, caveats, and CLI command changes.

3. Before you introduce configuration changes on the Cisco WAAS Central Manager, use the CMS backup feature to save your configuration.

   If you run into problems with the new configuration, you can restore the previous configuration (see Backing Up and Restoring Your Cisco WAAS System in the chapter "Maintaining Your Cisco WAAS System." Troubleshoot any problems with new configuration changes immediately after making them.

4. Verify that your configuration is correct for your network application.

   Make any required changes to the running-config file, and then test the configuration. If it is satisfactory, save it to the startup-config file by running the **copy running-config startup-config** command.

5. Enable system message logging.

   See Configuring and Viewing Logs, on page 630.

6. Run the diagnostic tool to verify device functionality and connectivity.

   See Using Diagnostic Tests, on page 638.

7. Verify the physical connectivity between WAAS peers and to the application servers.

   See Verifying WAAS Physical Connectivity, on page 643.

8. Gather information that defines the specific symptoms.

   See Gathering Cisco WAAS Troubleshooting Information, on page 620.

9. After you have determined that your troubleshooting attempts have not resolved the problem, contact the Cisco Technical Assistance Center (TAC) or your technical support representative.

   See Contacting Cisco Technical Support, on page 644.

Gathering Cisco WAAS Troubleshooting Information

This section contains the following topics:

Rebooting the Cisco WAAS Device

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

Using the copy tech-support Command

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

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

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

Using show Commands

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

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

Using show Commands for WCCP Deployments

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

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

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

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

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

- **show tcam counts**
- **show mls stat**
- **show mls netflow table detail**
- **show mls netflow ip count**

- **show mls netflow ip sw-installed count**
- **show mls netflow ip sw-installed detail**
- **show fm interface** *interface_name*

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

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

Generating a System Report

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

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

Consider these guidelines when you generate a system report:

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

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

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

For example:

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

Capturing and Analyzing Packets

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

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

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

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

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

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

Verifying the Cisco WAAS Image

This section contains the following topics:

Verifying the Current Cisco WAAS Image

Before you begin

Run the **show version** command to display the version of the software image that is currently running in your WAAS device.

The command output includes:

- Copyright information
- Software Release number, for example: **Cisco Wide Area Application Services Software Release 6.4.3d**
- Device model and Cisco WAAS Version, for example:**oe-vwaas-6.4.3.17**
- Most recent compiled date and time
- Most recent restart date and time
- Device uptime, weeks, hours, minutes, and seconds

You can run the **show version** command from the CLI or from the Cisco WAAS Central Manager:

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

- wae# **show version**

Procedure

Step 1 To run the **show version** command from the Cisco WAAS Central Manager, choose **Navigate** > **Devices** > *DeviceName* > **Monitor** > **CLI Commands show commands**

Step 2 From the **show commands** dropdown list, choose **show version**.

Step 3 Click **Submit**.

Verifying a Pending Cisco WAAS Image

Before you begin

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

You can run the **show version** command from the CLI or from the Cisco WAAS Central Manager:

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

```
wae# show version pending
```

To run the **show version pending** command from the Cisco WAAS Central Manager, follow these steps:

Procedure

Step 1 To run the **show version pending** command from the Cisco WAAS Central Manager, choose **Devices** > *DeviceName* > **Monitor** > **CLI Commands** > **show commands**.

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

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

Step 4 Click **Submit**.

Cisco WAAS Central Manager Alarm Panel

This section has the following sections:

Viewing the Alarm Panel

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

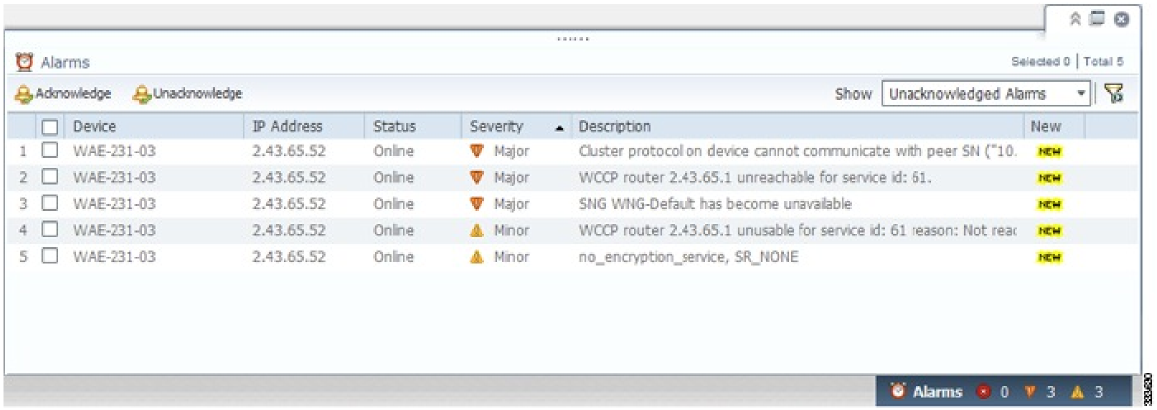
To view the alarms panel, click **Alarms** at the bottom right side of the Cisco WAAS Central Manager window.

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

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

The following figure shows the alarm panel.

Figure 98: Alarm Panel



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 reac	NEW
5	□	WAE-231-03	2.43.65.52	Online	Minor	no_encryption_service, SR_NONE	NEW

Acknowledging an Active Alarm

Procedure

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

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

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

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

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

Filtering and Sorting Alarms

Procedure

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

- **All**
- **Quick Filter**

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

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

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

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

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

Device Alarms

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

Table 88: Device Alarms for Reporting Problems

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

Alarm Email Notification

Before you begin

For Cisco WAAS Version 6.2.3d and later, the Cisco WAAS software supports an email notification mechanism, that is triggered whenever the Cisco WAAS Central Manager receives an alarm notification for a raised or cleared alarm.

Note In a mixed-version Cisco WAAS network, the email notification is triggered for all raised alarms for all Cisco WAAS devices. However, the email notification is triggered for cleared alarms only on devices running Cisco WAAS versions 6.2.3d or later.

Procedure

Step 1 To configure the email server settings: From the Cisco WAAS Central Manager menu choose **Devices** > **WCM** > **Configure** > **Monitoring** > **Email Notification**.

Step 2 To configure the email notification settings: From the Cisco WAAS Central Manager menu choose **Home** > **Admin** > **Alarm Email Notification** > **Configure**.

Step 3 Check the **Enable Alarm Email Notification** check box. It is disabled by default.

Step 4 Select the alarms based on the severity level for **Raised** and **Cleared** alarms. The **Minor Alarms** checkbox is disabled by default.

Step 5 To notify users, enter the valid email addresses in the **Address** fields. For multiple email addresses, use comma separators.

Step 6 Enter the subject in the **Subject** field.

Step 7 Click **Submit**.

Consider the following guidelines:

- After configuring, you are notified of all alarms for the devices that are registered with the Cisco WAAS Central Manager.
- The email subject consists of Device Information such as **Device name**, **IP Address** and **Alarm raised** and **Alarm cleared** count.
- The email summary consists of Alarm details in a tabular format.

An example of email content is shown in the following table.

Alarm ID	Sequence number	Module	Severity	Description	Time raised	Time cleared
700002	30	CMS	Major	WAE clock needs to be synchronized.	01-07-2017 09:10:36 PM GMT	N/A

The following details of the particular alarm can be seen in the mail notification.

- **Alarm ID**: ID of the Alarm
- **Sequence number**: Order of the alarm in the device. This is applicable only for alarms pertaining to the WAE devices and not applicable for Cisco WAAS Central Manager and Router alarms.
- **Module**: Component for the alarm, for example, CMS, disk, DRE, NHM, and others.
- **Severity**: Category of alarm: Critical, Major, or Minor.
- **Description**: Detailed description of the alarm, which includes the condition of the alarm.

- **Time Raised**: For **Raised Alarms**, the time when it was raised will be shown in the email content and the time when it was cleared will be shown as **N/A**.
- **Time Cleared**: For the **Cleared Alarms**, the time when it was cleared and the time when it was raised are both shown.
- You can configure the number of days you want the system to retain the records of the alarms. To do so, from the Cisco WAAS Central Manager menu, choose **Configure** > **Global** > **System Properties** and modify the **System.clearedAlarm.purging.interval**. The default value is **7 days**, but you can choose **up to 365 days**.

Troubleshooting Devices Using Alerts

Before you begin

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

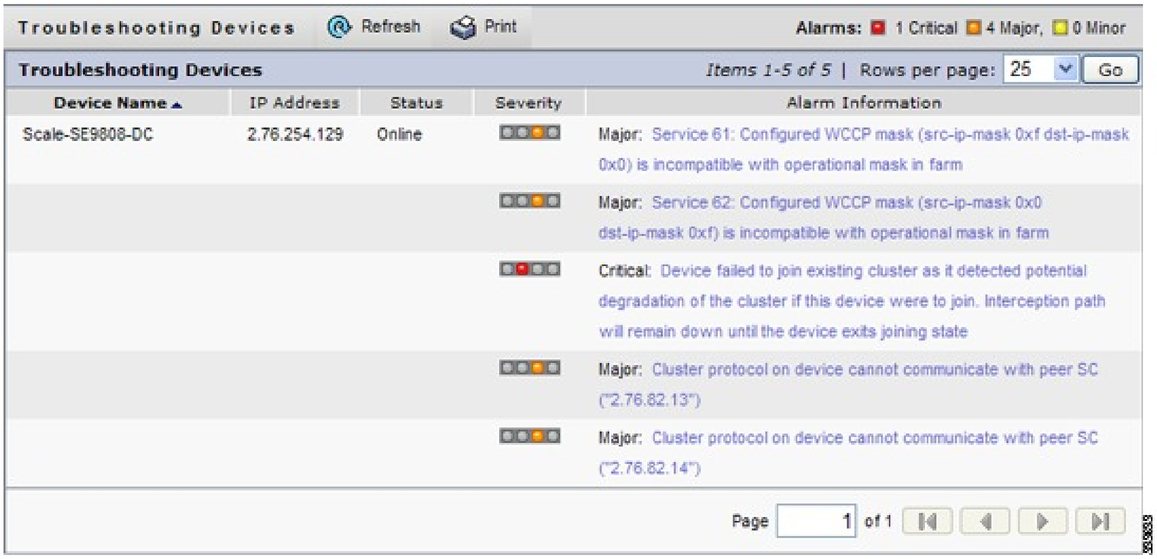
Procedure

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

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

The **Troubleshooting Devices** pane appears, either in the Cisco WAAS Central Manager window or as a separate dialog box.

Figure 99: Troubleshooting Devices Window



Troubleshooting Devices
Refresh
Print
Alarms: 🟥 1 Critical 🟧 4 Major, 🟨 0 Minor
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")

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

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

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

Table 89: Troubleshooting Tools for Device Alarms

Item	Navigation	Description
Update Software	Choose device, **Admin** > **Versioning** > **Software Update**	Displays the **Software Update** window for this device. Appears only if the device software version is lower than that of the Cisco WAAS Central Manager.
Edit/Monitor Device	Device dashboard	Displays the **Device Dashboard** for configuration.
Telnet to Device	Opens a Telnet window	Initiates a Telnet session using the device IP address.
View Device Log	Choose device, **Admin** > **History** > **Logs**	Displays system message logs filtered for this device.
Run **show** Commands	Choose device, **Monitor** > **CLI Commands** > **show Commands**	Displays the device **show** command tool. For more information, see Using the show and clear Commands from the Cisco WAAS Central Manager, on page 629.

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

Before you begin

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

Procedure

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

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

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

Step 4 Enter arguments for the command, if any.

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

A window displays the command output for that device.

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

Configuring and Viewing Logs

This section contains the following topics:

Configuring System Logging

This section contains the following topics:

Enabling System Logging

Before you begin

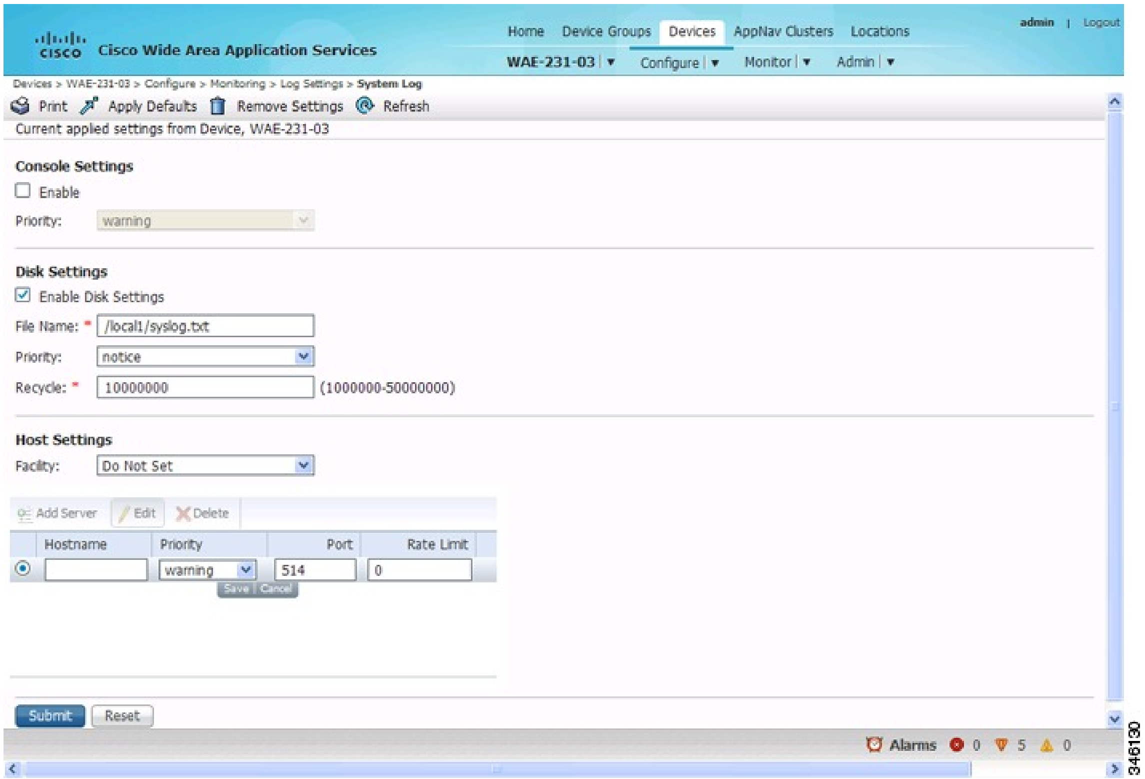
Use the Cisco WAAS system logging feature to set specific parameters for the system log file (syslog). This file contains authentication entries, privilege-level settings, and administrative details. The system log file is located in the system file system (sysfs) partition as /local1/syslog.txt.

Procedure

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

Step 2 Choose **Configure** > **Monitoring** > **Log Settings** > **System Log**. The **System Log Settings** window appears.

Figure 100: System Log Settings Window



Devices > WAE-231-03 > Configure > Monitoring > Log Settings > System Log

Current applied settings from Device, WAE-231-03

Console Settings

□ Enable

Priority: warning

Disk Settings

☑ Enable Disk Settings

File Name: * /local1/syslog.txt

Priority: notice

Recycle: * 10000000 (1000000-50000000)

Host Settings

Facility: Do Not Set

	Hostname	Priority	Port	Rate Limit
●		warning	514	0

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

a) In the **Console Settings** pane, check the **Enable** check box.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 6 Click **Submit**.

Step 7 To configure system logging from the CLI, run the **logging** global configuration command.

Priority Levels

The following table lists the different priority levels of detail that can be sent to the recipient of **syslog** messages for a corresponding event.

Table 90: System Logging Priority Levels and Descriptions

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

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

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

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

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

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

Multiple Hosts for System Logging

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

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

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

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

Configuring Transaction Logging

This section contains the following topics:

Enabling Transaction Logging

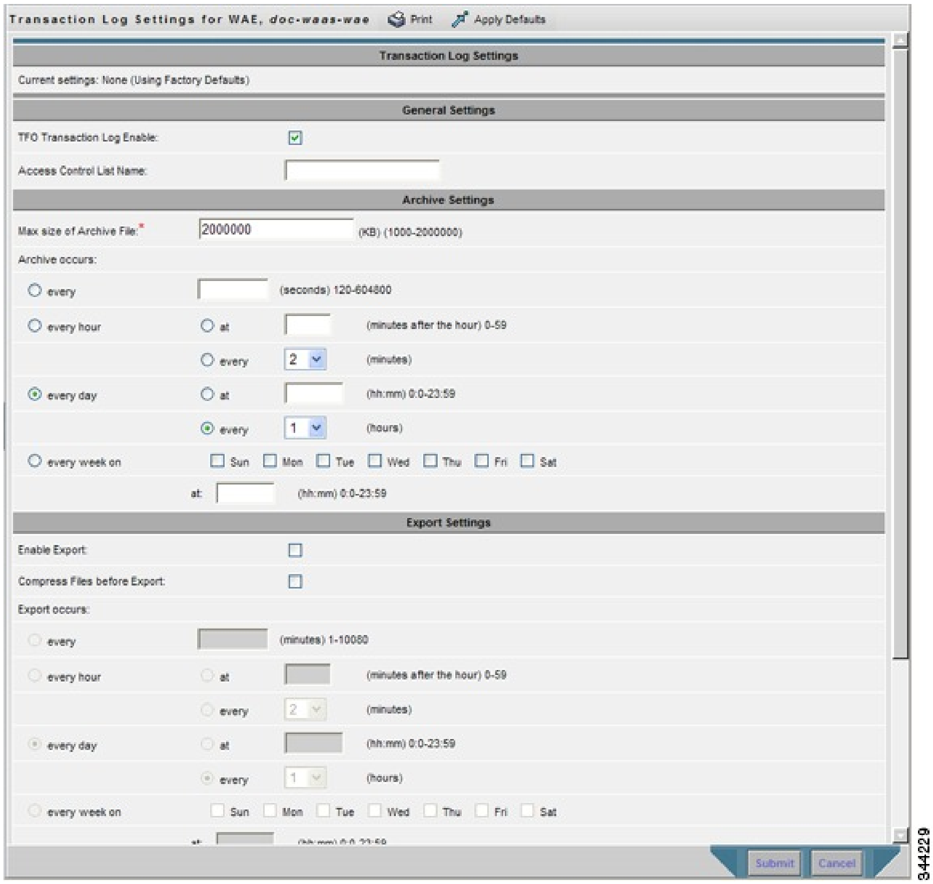
Procedure

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

Step 2 Choose **Configure** > **Monitoring** > **Log Settings** > **Transaction Log** for TFO transaction logging or **Configure** > **Monitoring** > **Log Settings** > **Video Acceleration Transaction Log** for video transaction logging.

The **Transaction Log Settings** window appears. (The **Video Transaction Log Settings** window looks the same, but does not include the **General Settings** area at the top.)

Figure 101: Transaction Log Settings Window



Transaction Log Settings for WAE, *doc-waas-wae*

Transaction Log Settings

Current settings: None (Using Factory Defaults)

General Settings

TFO Transaction Log Enable: ☑

Access Control List Name:

Archive Settings

Max size of Archive File:* 2000000 (KB) (1000-2000000)

Archive occurs:

○ every (seconds) 120-604800

○ every hour ○ at (minutes after the hour) 0-59

○ every 2 (minutes)

● every day ○ at (hh:mm) 0:0-23:59

● every 1 (hours)

○ every week on □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

at: (hh:mm) 0:0-23:59

Export Settings

Enable Export: □

Compress Files before Export: □

Export occurs:

○ every (minutes) 1-10080

○ every hour ○ at (minutes after the hour) 0-59

○ every 2 (minutes)

● every day ○ at (hh:mm) 0:0-23:59

● every 1 (hours)

○ every week on □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

at: (hh:mm) 0:0-23:59

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

The fields on the window become active.

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

To define an access list, run the **ip access-list** global configuration command.

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

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

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

The following table describes the fields in the **Export Settings** pane.

Table 91: Export Settings

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

Step 7 Click **Submit**.

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

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

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

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

Transaction Logs

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

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

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

- The archive filenames for TFO transactions use this format:

  tfo_IPADDRESS_YYYYMMDD_HHMMSS.txt

- The archive filenames for Windows media transactions use this format:

  wms_90_IPADDRESS_YYYYMMDD_HHMMSS.txt

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

Viewing the System Message Log

Before you begin

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

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Admin** > **Logs** > **System Messages**.

The **System Message Log** window appears.

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

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

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

a) Click the **Truncate** icon in the taskbar.

The **Truncate System Message Log** pane appears.

b) Choose one of the following options:

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

c) After you have finished specifying the truncation parameters, click **OK**.

Viewing the Audit Trail Log

Before you begin

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

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

Procedure

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

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

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

Viewing a Device Log

Before you begin

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

To view the events that have occurred on your entire Cisco WAAS network, see Viewing the System Message Log, on page 636.

Procedure

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

Step 2 Choose **Admin** > **Logs** > **Device Logs**.

The **Device Log** window appears.

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

CLI Commands for Verifying and Viewing Logs and System Image

- **Verify the WAAS image**: Run the **show version** command to display the version of the software image that is currently running in your Cisco WAAS device. This command also displays information including device model and WAE uptime.
- **Verify no pending software**: Run the **show version** pending command to verify that there is no pending software upgrade (waiting for a device reboot).
- **Verify WAAS error logging**: General system error WAAS logging to the disk file **/local1/syslog.txt** is enabled by default. Run the **show logging** command to verify that logging is enabled.
- **Enable console logging**: Run the **(config) logging console enable** command to enable logging to the console. You can set the following logging priority levels: **Alert** (Priority 1), **Critical** (Priority 2), **Error** (Priority 3), **Warning** (Priority 4), **Notice** (Priority 5), **Information** (Priority 6), and **Debug** (Priority 7).

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

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

Use the following commands to navigate and view these log files:

- **cd**
- **pwd**
- **dir**
- **type-tail filename line follow**
- **find-pattern**

Using Diagnostic Tests

This section contains the following topics:

Device Diagnostics Using the Cisco WAAS Central Manager

Procedure

Step 1 To use the Cisco WAAS troubleshooting and diagnostic reporting facility: From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 2 Choose **Monitor** > **Tools** > **Diagnostics Tests**.

The **Diagnostic Tool** window appears.

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

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

Note A Virtual Interface test is available for Cisco vWAAS devices.

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

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

Step 4 Click **Run**.

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

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

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

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

Device Diagnostics Using the Cisco WAAS CLI

To perform diagnostic and connectivity tests, run the **test** EXEC command.

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

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

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

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

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

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

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

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

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

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

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

Akamai Connect Diagnostics Using the Cisco WAAS Central Manager

Before you begin

For Cisco WAAS devices with Akamai Connect, the **Akamai Diagnostics** window provides status information for the Akamai Connect license and Akamai Connect service, and enables you to unregister or synchronize selected devices.

Procedure

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

The **Akamai Diagnostics** window appears.

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

Step 3 To display a dialog box of additional information, click the **Akamai Connect License Details** button:

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

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

a) To test the connection to the API server, click **Test**.
b) A **Device Registration Status** table listing is displayed, showing the total number of devices, and with columns displaying each **Cisco WAAS Device**, **Akamai ID**, **Akamai Device Status** (ActivationInProgress or Active), **Operational Status** (Disconnected, Connected, or Running), and **Connectivity to Akamai** (Disconnected, Activating, or Connected).).

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

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

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

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

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

Step 6 To unregister a device from this table listing:

a) Select the device(s).
b) Click the **Unregister** button in the table heading.

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

c) When you click **Unregister**, the following warning message is displayed: **De-registering device(s) would prevent Akamai Connected Cache and OTT features from working on devices that have these features enabled. Please confirm de-registration of selected device(s)**.
d) To de-register to the selected device(s), click **OK**. Or, to exit the procedure without de-registering the selected device(s), click **Cancel**.

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

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

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

Consider the following operating guidelines when using the **Synchronize** button:

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

Using the Kernel Debugger

Before you begin

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

Procedure

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

Step 2 Choose **Monitor** > **Tools** > **Kernel Debugger**.

The **Kernel Debugger** window appears.

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

Using WAAS TCP Traceroute

Before you begin

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

Procedure

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

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

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

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

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

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

Step 5 To view traceroute information from the Cisco WAAS CLI, run the **waas-tcptrace** EXEC command.

Another troubleshooting tool that you can use to trace connections on a WAAS appliance ANC is the **Connection Trace** tool. For details, see AppNav Connection Tracing in the chapter "Configuring Cisco AppNav."

Verifying WAAS Physical Connectivity

This section contains the following topics:

Verifying Physical Connectivity Between Peer WAAS Devices

Procedure

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

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

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

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

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

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

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

Verifying Physical Connectivity Between WAAS Data Center and Application Server Hosts

The procedure for verifying physical connectivity between the WAAS data center and application server hosts is the same procedure as described in Verifying Physical Connectivity Between Peer WAAS Devices, on page 643.

Troubleshooting Smart License Issues

There can be various issues with devices that are smart license enabled and not registered or authorized with Cisco Smart Software Manager (CSSM). Common issues include:

- invalid token
- communication issue with CSSM
- communication response error if CSSM is unavailable

For more information, and to troubleshoot any of the above scenarios, check the smart-license log files.

Contacting Cisco Technical Support

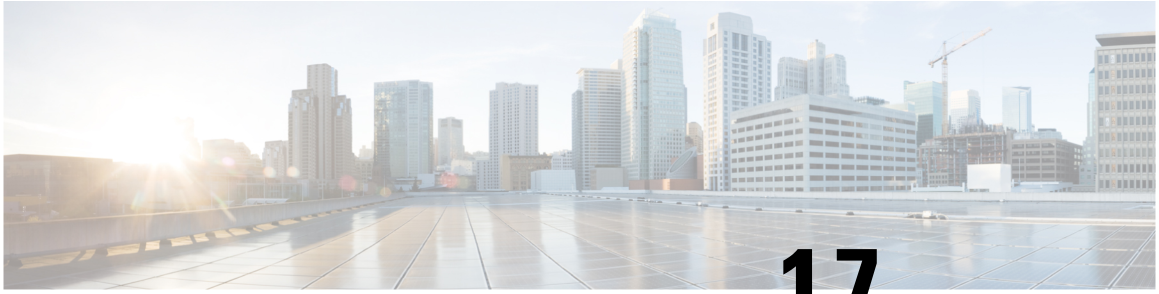
If you are unable to resolve a problem after using the troubleshooting suggestions in this chapter, contact the Cisco Technical Assistance Center (TAC) for assistance and further instructions. Before you call, have the following information ready to help your TAC engineer assist you as quickly as possible:

- Date that you received the Cisco WAAS hardware
- Chassis serial number
- Type of software and release number (if possible, run the **show version** EXEC command)
- Maintenance agreement or warranty information
- A good problem description including:
    - What is the problem and what are the user visible symptoms?
    - Where and when it occurs
    - Error messages, alerts, and alarms seen
    - Steps to duplicate the problem

- Brief explanation of the steps that you have already taken to isolate and resolve the problem
- The diagnostic test output (see Using Diagnostic Tests).
- A Cisco WAAS Central Manager database backup (run the **cms database backup** EXEC command)
- Information gathered in Gathering Cisco WAAS Troubleshooting Information
- Topology diagrams, including network, wiring, and logical diagrams
- Any other evidence of the problem such as packet captures, transaction logs, core files, WCCP **show** command output from routers, switches, and Cisco WAEs, and other log files.

You can contact support in these ways:

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



CHAPTER 17

Configuring SNMP Monitoring

This chapter describes how to configure Simple Network Management Protocol (SNMP) traps, recipients, community strings, group associations, user security model groups, and user access permissions.

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

This chapter contains the following sections:

Understanding SNMP

SNMP is an interoperable standards-based protocol that allows for external monitoring of Cisco WAAS devices through an SNMP agent.

An SNMP-managed network consists of the following primary components:

- **Managed device**: A network node that contains an SNMP agent and resides on a managed network. Managed devices include routers, access servers, switches, bridges, hubs, computer hosts, and printers. Each WAAS device running the WAAS software has an SNMP agent.
- **SNMP agent**: A software module that resides on a managed device. An agent has local knowledge of management information and translates that information into a form that is compatible with SNMP. The SNMP agent gathers data from the MIB, which is the repository for information about device parameters and network data. The agent can also send traps, or notification of certain events, to the management system.
- **Management station**: Also known as the SNMP host, the management station uses SNMP to send the agent an SNMP Get request to obtain information from the WAAS device. The managed devices then collect and store management information and use SNMP to make this information available to the management station.

Before you can access this SNMP information, you must have deployed an SNMP management application on a management station. This SNMP management station is referred to as the SNMP host because it uses SNMP to send the device agent an SNMP Get request to obtain information from the WAAS device.

This section contains the following topics:

SNMP Communication Process

The SNMP management station and the SNMP agent that resides on a Cisco WAAS device use SNMP to communicate as follows:

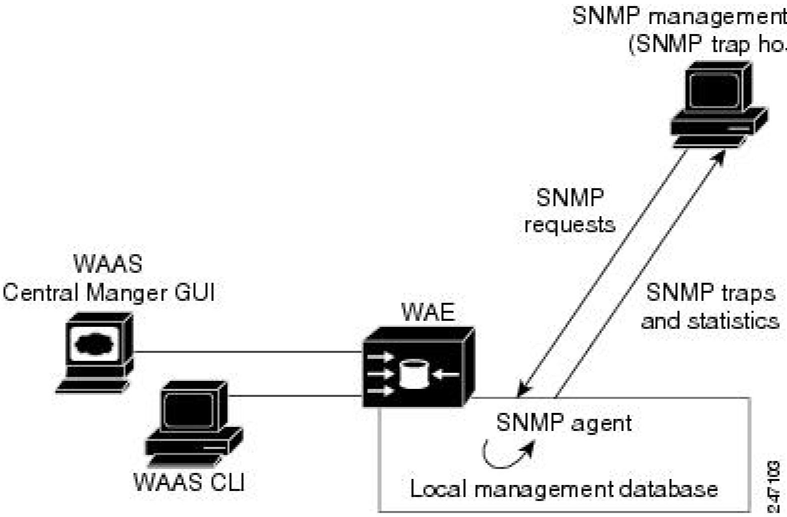
1. The SNMP management station (the SNMP host) uses SNMP to request information from the Cisco WAAS device.
2. After receiving these SNMP requests, the SNMP agent on the Cisco WAAS device accesses a table that contains information about the individual device. This table, or database, is called a MIB.

Note The SNMP agent on the Cisco WAAS device only initiates communication with the SNMP host under unusual conditions; it will initiate communication when it has a trap it needs to send to the host. For more information on this topic, see Enabling SNMP Traps, on page 683.

1. After locating the specified information in the MIB, the agent uses SNMP to send the information to the SNMP management station.

The following figure illustrates these SNMP operations for an individual Cisco WAAS device.

Figure 102: SNMP Components in a Cisco WAAS Network



Supported SNMP Versions

The Cisco WAAS software supports the following versions of SNMP:

- **Version 1 (SNMPv1)**: This is the initial implementation of SNMP. See RFC 1157 for a full description of its functionality.
- **Version 2 (SNMPv2c)**: This is the second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations.
- **Version 3 (SNMPv3)**: This is the most recent version of SNMP, defined in RFC 2271 through RFC 2275.

Each Cisco device running Cisco WAAS software contains the software necessary to communicate information about device configuration and activity using SNMP.

SNMP Security Models and Security Levels

SNMPv1 and SNMPv2c do not have any security (that is, authentication or privacy) features to keep SNMP packet traffic confidential. As a result, packets on the wire can be detected and SNMP community strings compromised.

To solve the security shortcomings of SNMPv1 and SNMPv2c, SNMPv3 provides secure access to WAAS devices by authenticating and encrypting packets over the network. The SNMP agent in the WAAS software supports SNMPv3 as well as SNMPv1 and SNMPv2c.

The following security features are provided in SNMPv3:

- **Message integrity**: Ensures that nothing has interfered with a packet during transmission.
- **Authentication**: Determines that the message is from a valid source.
- **Encryption**: Scrambles the contents of a packet to prevent it from being seen by an unauthorized source.

SNMPv3 provides security models as well as security levels. A security model is an authentication process that is set up for a user and the group in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security process is used when an SNMP packet is handled. Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

The following table describes the combinations of security models and security levels.

Table 92: SNMP Security Models and Security Levels

Model	Level	Authentication	Encryption	Process
v1	noAuthNoPriv	Community string	No	Uses a community string match for user authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for user authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for user authentication.
v3	AuthNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC)-MD5 or HMAC-SHA algorithms.
v3	AuthPriv	MD5 or SHA	Yes	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption (packet authentication) based on the cipher block chaining (CBC)-DES (DES-56) standard.

The SNMPv3 agent can be used in the following modes:

- **noAuthNoPriv** mode (that is, no security mechanisms turned on for packets)
- **AuthNoPriv** mode (for packets that do not have to be encrypted using the privacy algorithm [DES 56])
- **AuthPriv** mode (for packets that must be encrypted; privacy requires that authentication be performed on the packet)

Using SNMPv3, users can securely collect management information from their SNMP agents without worrying that the data has been tampered with. Also, confidential information, such as SNMP set packets that change a Content Engine’s configuration, can be encrypted to prevent their contents from being exposed on the wire. Also, the group-based administrative model allows different users to access the same SNMP agent with varying access privileges.

SNMPv3 with AES Encryption

This section containst the following topics:

About SNMPv3 with AES Encryption

This section describes DES and AES encryption for different Cisco WAAS versions.

- **SNMP in Cisco WAAS Version 6.4.3d and earlier**: Supports only Data Encryption Standard (DES) encryption.

- **SNMP in Cisco WAAS Version 6.4.3e and later**: Supports Advanced Encryption Standard (AES) encryption as well as DES encryption, which provides strong encryption capability for SNMPv3 messages. AES encryption uses the Cipher Feedback (CFB) mode with encryption key sizes of 128, 192, or 256 bits.

  The SNMPv3 User-based Security Model (USM) provides three modes of operation:

  - **noAuthNoPriv**: This mode is similar to the SNMPv1 and SNMPv2c model, in that a username is treated in a manner equivalent to the community string. This mode does not utilize strong authentication and does not encrypt SNMP traffic.
  - **authNoPriv**: This mode provides strong authentication via SHA or MD5, but does not encrypt SNMP traffic.
  - **authPriv**: This mode provides strong authentication via SHA or MD5, and encrypts SNMP messages using DES encryption algorithm.

  For Cisco WAAS Version 6.4.3e and later, Cisco provides support for AES as an additional option for message encryption under the SNMPv3 authPriv mode.

  Command modification for SNMPv3 with AES encryption:

  For Cisco WAAS Version 6.4.3e and later, the global configuration command **snmp-server user** *name group* contains the parameter **protocol AES {128 | 192 |256} | DES**. This parameter specifies the encryption method and key length. For more information, see the *Cisco Wide Area Application Services Command Reference*.

Operating Guidelines for SNMPv3 with AES Encryption

Consider the following operating guidelines for SNMPv3 with AES encryption:

- If one of the devices in a device group is running an earlier version than Cisco WAAS Version 6.4.3e, you must upgrade the device to Cisco WAAS Version 6.4.3e for the device group to create an AES encryption user for the group.
- If **Priv Password** is **Empty**, do not select Protocol Algorithm and AES Encryption.
- If **Priv Password** is entered, select **Priv Protocol** either (**DES** or **AES**).
- If Protocol is selected by AES, select **AES Encryption**.
- If **no-auth** is selected, do not select Protocol.
- If **Priv Password** is **Empty**, do not select AES Encryption.
- If the Cisco WAAS Central Manager is running Cisco WAAS Version 6.4.3e or later, and the device is part of a device group containing devices running 6.4.3e, then you can create the AES encryption user.

Upgrade and Downgrade Guidelines for SNMPv3 with AES Encryption

Consider the following upgrade and downgrade guidelines for SNMPv3 with AES encryption:

- Cisco WAAS 6.4.3d release and earlier Cisco WAAS versions support DES encryption only. The privacy protocol cannot be configured, and is not displayed in the **running-configuration** and **show** commands.

- If you downgrade from Cisco WAAS Version 6.4.3e to an earlier Cisco WAAS version, the downgrade will not proceed if there are SNMPv3 users configured in **authpriv mode** with **Priv Protocol AES**. A Warning message will be displayed in the CLI if AES encryption users are present in the running configuration. A pop-up message will also be displayed, if you attempt to downgrade from the WAAS Central Manager and if AES encryption users are present in the running configuration. You must remove the AES encryption users from configuration and downgrade again to complete the image installation.
- After upgrading to Cisco WAAS Version 6.4.3e or later, the existing SNMP users in **authpriv** mode, if present, will be added with **Priv Protocol DES**.

Cisco-Supported MIBs

This section contains the following topics:

About Cisco-Supported MIBs and CISCO-SMI

A Management Information Base (MIB) is a collection of managed objects, arranged in a hierarchical tree of MIB modules, groups, and objects:

- **MIB module**: Contains related MIB groups.

For example, CISCO-WAN-OPTIMIZATION-MIB contains many types of optimization groups, including cwoAoStats and cwoTfoStats.

- **MIB group**: Contains the prefix for a set of related MIB objects, such as cwoAoStats (AO statistics) and cwoTfoStats (TFO statistics).
- **MIB object**: Provides information about a specific aspect of the specified MIB group.

For example:

- The **cwoAoStatsIsConfigured** MIB object indicates if the AO is configured or not.
- The **cwoTfoStatsLoadStatus** displays the current TFO load status (such as "operating normally" or "overloaded").

The Structure of Management Information (SMI) defines the framework within which you can define or construct a MIB. The CISCO-SMI MIB group describes the structure of Cisco MIBs.

Types of MIB Output for SNMP Monitoring

This section contains the following topics:

MIB Output for Statistical Data

MIB output can provide information about a device, interface, or process at a specified moment in time. The following figure shows an example of MIB output of statistical data for the MIB object **cwoDreCacheStats**. This object displays DRE cache information, such as the current operational status, the portion of the disk space allocated for DRE cache, the age of the oldest data unit the data block, and the amount of data units replaced in the last hour.

Sample MIB Output for DRE Cache Information with cwoDreCacheStats

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsStatus.0 = STRING: Usable
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsTotal.0 = Counter64: 77822 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 96 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsDataUnitUsage.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsReplacedOneHrDataUnit.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsDataUnitAge.0 = STRING: 0s
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsSigblockUsage.0 = Counter64: 1695 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsReplacedOneHrSigblock.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsSigblockAge.0 = STRING: 14d17h
```

MIB Output for Trend Data

The greatest value provided by MIBs may be in enabling SNMP monitoring to use the external MIB tool to gather statistics — and then provide trend data from these statistics, in either text or graphical format. This enables you to more easily identify anomalies in your WAAS network, and therefore to more effectively plan or modify your network.

For example, in the output shown in the above Figure 17-2 , the MIB cwoDreCacheStatsUsed provides information on the percentage of DRE disk space currently being used:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 96 percent
```

If you want to monitor the trend of how DRE disk space is being used over a particular period of time, you could run the cwoDreCacheStatsUsed MIB for a specified time range. As shown below in Figure 17-3 , you could view data for a specified time range that displays the usage trend for the DRE cache disk space.

Sample MIB Output for Percentage of DRE Disk Space Being Used

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 85 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 91 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 96 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 98 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 93 percent
```

For more information on MIB usage with SNMP monitoring, and for more examples of MIB output, see Using MIBs to Monitor Cisco WAAS, on page 677.

Types of Cisco-Supported MIBs

This section describes the types of Cisco-supported MIBs, in alphabetical order by topic:

Akamai Connect (CISCO-WAN-OPTIMIZATION-MIB)

The following table shows the Akamai Connect MIB objects associated with the cwoAoHttpxStatsAKC MIB object, for a specified caching mode: Standard, Basic, Bypass, or Advanced. For each Akamai Connect caching mode, there are MIB objects that provide the following types of information:

- **Cache transactions**: The Akamai Connect cache statistics for the total number of cache-hit transactions that were served from cache in the specified caching mode.
- **Cache transactions percent**: The percentage of total number of cache-hit HTTP transactions in the specified caching mode.
- **Cache response time saved**: The total response time saved for cache-hit HTTP transactions in the specified Akamai Connect cache mode, in milliseconds.

- **Average cache response time saved**: The average response time saved per cache-hit HTTP transaction in the specified Akamai Connect cache mode, in milliseconds.
- **Response in bytes**: The total number of response bytes saved for cache-hit HTTP transactions in the specified Akamai Connect cache mode.
- **Response bytes percent**: The percentage of total number of response bytes saved for cache-hit HTTP transactions in the specified Akamai Connect cache mode.
- **Response time saved percent**: The percentage of total response time saved for cache-hit HTTP transactions in the specified Akamai Connect cache mode.

Table 93: Akamai Connect MIB Objects

MIB Object	Associated MIB Objects
cwoAoHttpxStatsAKCStdEntry	Provides information about the Akamai Connect cache in Standard mode (default), in which Akamai Connect caches objects marked as cacheable, as well as objects with no explicit cache marker and with a last-modified date. • cwoAoHttpxStatsAKCStdCacheTrans • cwoAoHttpxStatsAKCStdCacheTransPercent • cwoAoHttpxStatsAKCStdCacheRespTimeSaved • cwoAoHttpxStatsAKCStdAvgCacheRespTimeSaved • cwoAoHttpxStatsAKCStdRespBytes • cwoAoHttpxStatsAKCStdRespBytesPercent • cwoAoHttpxStatsAKCStdRespTimeSavedPercent
cwoAoHttpxStatsAKCBasicEntry	Provides information about the Akamai Connect cache in Basic mode, in which Akamai Connect caches only objects explicitly marked as cacheable. • cwoAoHttpxStatsAKCBasicCacheTrans • cwoAoHttpxStatsAKCBasicCacheTransPercent • cwoAoHttpxStatsAKCBasicRespBytes • cwoAoHttpxStatsAKCBasicRespBytesPercent • cwoAoHttpxStatsAKCBasicCacheRespTimeSaved • cwoAoHttpxStatsAKCBasicAvgCacheRespTimeSaved • cwoAoHttpxStatsAKCBasicRespTimeSavedPercent

MIB Object	Associated MIB Objects
cwoAoHttpxStatsAKCBypassEntry	Provides information about the Akamai Connect cache in Bypass mode, in which Akamai Connect caching is turned off for a configured site or sites. • cwoAoHttpxStatsAKCBypassCacheTrans • cwoAoHttpxStatsAKCBypassCacheTransPercent • cwoAoHttpxStatsAKCBypassCacheRespTimeSaved • cwoAoHttpxStatsAKCBypassAvgCacheRespTimeSaved • cwoAoHttpxStatsAKCBypassCacheRespTimeSavedPercent • cwoAoHttpxStatsAKCBypassRespBytes • cwoAoHttpxStatsAKCBypassRespBytesPercent
cwoAoHttpxStatsAKCAdvEntry	Provides information about the Akamai Connect cache in Advanced mode, in which Akamai Connect caches media types more aggressively, and caches all object types for longer times, when there is no explicit expiration time. • cwoAoHttpxStatsAKCAdvCacheTrans • cwoAoHttpxStatsAKCAdvRespBytes • cwoAoHttpxStatsAKCAdvCacheTransPercent • cwoAoHttpxStatsAKCAdvRespBytesPercent • cwoAoHttpxStatsAKCAdvCacheRespTimeSaved • cwoAoHttpxStatsAKCAdvAvgCacheRespTimeSaved • cwoAoHttpxStatsAKCAdvRespTimeSavedPercent
cwoAoHttpxStatsAKCTotalEntry	Provides summary information about the Akamai Connect cache, from all caching modes. • cwoAoHttpxStatsAKCTotalCacheTrans • cwoAoHttpxStatsAKCTotalRespBytes • cwoAoHttpxStatsAKCTotalCacheTransPercent • cwoAoHttpxStatsAKCTotalRespBytesPercent • cwoAoHttpxStatsAKCTotalCacheRespTimeSaved • cwoAoHttpxStatsAKCTotalAvgCacheRespTimeSaved • cwoAoHttpxStatsAKCTotalRespTimeSavedPercent

Alarms (CISCO-CONTENT-ENGINE-MIB)

The following table describes CISCO-CONTENT-ENGINE-MIB objects that are used to verify if there are critical, major, or minor alarms raised on the system.

Table 94: Alarms MIB Objects

MIB Object	Description
cceAlarmMinorCount	The number of alarms currently raised with a severity level of Minor.
cceAlarmMajorCount	The number of alarms currently raised with a severity level of Major.
cceAlarmCriticalCount	The number of alarms currently raised with a severity level of Critical.

AOs (CISCO-WAN-OPTIMIZATION-MIB)

The CISCO-WAN-OPTIMIZATION-MIB group displays information about the status and statistics associated with application optimizers.

The Application Optimizers (AOs), also known as Application Acclerators, statistics MIB group displays status information such as configuration or license information for AOs including HTTP, SSL, MAPI, SMB, and ICA.

This section contains the following tables for the **cwoAoStats** MIB objects:

- AO Name, Configuration, and License MIB Objects
- AO Operational Status, Startup Time, and Reset Time MIB Objects
- AO Summary Connection Information MIB Objects
- AO Current Connection Information MIB Objects
- AO Load Status and Bandwidth Information MIB Objects

Table 95: AO Name, Configuration, and License MIB Objects

MIB Object	Description
cwoAoStatsName	The name of the AO, such as HTTP, SSL, MAPI, SMB, and ICA.
cwoAoStatsIsConfigured	Indicates if the AO is configured or not. **Note** If the AO is not configured, then the cwoAoStatsOperationalState for this AO is Shutdown.
cwoAoStatsIsLicensed	Indicates if the license for the AO is valid or not. **Note** If the license for the AO is not valid, then the cwoAoStatsOperationalState for this AO is Shutdown.

Table 96: AO Operational Status, Startup Time, and Reset Time MIB Objects

cwoAoStatsOperationalState	The operational state of the AO: • shutdown (1) • initializing (2) • normalRunning (3) • normalDisabled (4) • licenseExpired (5) • cleaningup (6) • error (7) **Note** If the AO is not configured or if the license for this AO is not valid, the operational state is Shutdown.
cwoAoStatsStartUpTime	The date and time when the AO was started.
cwoAoStatsLastResetTime	The date and time of the last time the statistics of the AO were reset. When the specified AO's statistics are reset, then all statistics counters are also reset. **Note** When the specified AO is in the Shutdown state, the value of cwoAoStatsStartUpTime and cwoAoStatsLastResetTime is Null.

cwoAoStats MIB Objects for AO Summary Connection Information

Table 97: AO Summary Connection Information MIB Objects

MIB Object	Description
cwoAoStatsTotalHandledConn	Total number of connections handled by the AO since it was started or since its statistics were last reset.
cwoAoStatsTotalOptConn	Total number of connections optimized by the AO since it was started or since its statistics were last reset.
cwoAoStatsTotalHandedOffConn	Total number of connections handed off to generic optimization by the AO since it was started or since its statistics were last reset.
cwoAoStatsTotalDroppedConn	Total number of connections dropped by the AO since it was started or since its statistics were last reset.

Table 98: AO Current Connection Information MIB Objects

MIB Object	Description
cwoAoStatsActiveOptConn	The number of active connections that are getting optimized by the AO.
cwoAoStatsMaxActiveOptConn	The maximum number of active TCP connections the AO can optimize.

MIB Object	Description
cwoAoStatsPendingConn	The number of connections currently pending in the queue of connections to be optimized by the AO.

Table 99: AO Load Status and Bandwidth Information MIB Objects

MIB Object	Description
cwoAoStatsLoadStatus	The load status of the AO.
cwoAoStatsBwOpt	The percentage bandwidth optimization achieved due to optimization done by the AO.

Applications (CISCO-WAN-OPTIMIZATION-MIB)

The cwoAppStats MIB object displays information about application optimization and traffic.

Table 100: Applications Information MIB Objects

MIB Object	Description
cwoAppStatsAppName	The name of a particular application that is configured for optimization.
cwoAppStatsOriginalBytes	The total original traffic (uncompressed) in bytes of a particular application that has entered into the system.
cwoAppStatsOptimizedBytes	The total optimized traffic, in bytes, of a particular application.
cwoAppStatsPTBytes	The total pass-through traffic, in bytes, of a particular application.

AppNav (CISCO-APPNAV-MIB)

The CISCO-APPNAV-MIB group displays information about AppNavwhen the WAAS device is in AppNav Controller mode.

This section contains the following topics:

AppNav Controller MIB Objects

An AppNav Controller is a device that intercepts network traffic and, based on a flow policy, distributes that traffic to one more WAAS nodes for optimization. The following table displays AppNav Controller MIB objects.

Table 101: AppNav Controller Group MIB Objects

MIB Object	Descripton
cAppNavACIndex	An index of the cAppNavACTable. The unique integer value generated for each entry must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.

MIB Object	Descripton
cAppNavACIpAddrType	The address type of the cAppNavACIpAddr object. The cAppNavACEntries are only valid for address types of IPv4 and IPv6.
cAppNavACIpaddr	The IP address of the AppNav Controller.
cAppNavACServContextName	The name of the service context to which the specified AppNav Contoller belongs.
cAppNavACACGName	The name of the AppNav Controller Group to which the specified AppNav Controller belongs.
cAppNavACCurrentCMState	The current cluster membership state of the specified AppNav Controller. • **Green (1)**: Operational with no error conditions • **Yellow (2)**: Degraded (overloaded, joining cluster, or has other noncritical operational issues) • **Red (3)**:Critical (one or more processes is in a critical state) • **Gray (4)**: Disabled • **Black (5)**: Unknown status

AppNav Controller Group MIB Objects

An AppNav Controller Group is a group of AppNav Controllers that together provide the necessary intelligence for handling asymmetric flows and high availability. Table 17-11 displays AppNav Controller Group MIB objects.

Table 102: AppNav Controller Group MIB Objects

MIB Object	Description
cAppNavACGIndex	An index of the AppNavACGTable. The unique integer value generated for each entry must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.
cAppNavACGName	The name of the AppNav Controller Group.
cAppNavACGServContextName	The service context to which the specified AppNav Controller Group belongs.

AppNav Service Node MIB Objects

A WAAS node is also known as a service node. The following table displays AppNav service node MIB objects.

Table 103: AppNav Service Node MIB Objects

MIB Object	Description
cAppNavSNIndex	An index of the **cAppNavSNTable**. The unique integer value generated for each entry must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.
cAppNavSNIpAddrType	The address type of **cacSNIpAddr**. The **cacSNEntries** are valid for address types IPv4 and IPv6 only.
cAppNavSNIpAddr	The IP address of the specified service node.
cAppNavSNServContextName	The name of the service context to which the specified service node belongs.
cAppNavSNSNGName	The name of the service node group to which the specified service node belongs.
cAppNavSNCurrentCMState	The current cluster membership state of the specified service node. • **Green (1)**: Operational with no error conditions • **Yellow (2)**: Degraded (overloaded, joining cluster, or has other noncritical operational issues) • **Red (3)**: Critical (one or more processes is in a critical state) • **Gray (4)**: Disabled • **Black (5)**: Unknown status

AppNav Service Node Group MIB Objects

A WAAS node is also known as a service node. The following table displays AppNav service node MIB objects.

Table 104: AppNav Service Node MIB Objects

MIB Object	Description
cAppNavSNIndex	An index of the **cAppNavSNTable**. The unique integer value generated for each entry must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.
cAppNavSNIpAddrType	The address type of **cacSNIpAddr**. The cacSNEntries are valid for address types IPv4 and IPv6 only.
cAppNavSNIpAddr	The IP address of the specified service node.
cAppNavSNServContextName	The name of the service context to which the specified service node belongs.

MIB Object	Description
cAppNavSNSNGName	The name of the service node group to which the specified service node belongs.
cAppNavSNCurrentCMState	The current cluster membership state of the specified service node. • **Green (1)**: Operational with no error conditions • **Yellow (2)**: Degraded (overloaded, joining cluster, or has other noncritical operational issues) • **Red (3)**: Critical (one or more processes is in a critical state) • **Gray (4)**: Disabled • **Black (5)**: Unknown status

AppNav Service Node Group MIB Objects

A Service Node Group is also known as a WAAS Node Group. The following table displays AppNav Service Node Group MIB objects.

Table 105: AppNav Service Node Group Information MIB Objects

MIB Object	Description
cAppNavSNGIndex	An index of the **cAppNavSNGTable**. The unique integer value generated for each entry must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.
cAppNavSNGName	The name of the Service Node Group.
cAppNavSNGServContextName	The service context to which the specified Service Node Group belongs.

AppNav Service Context MIB Objects

A service context is used to tie the AppNav Controller group, service node group, and AppNav policy map together. The following table displays the AppNav Service Context MIB objects.

Table 106: AppNav Service Context Information MIB Objects

MIB Object	Description
cAppNavServContextIndex	An index of the **cAppNavServiceContextTable**. The unique integer value generated for each entry must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization.
cAppNavServContextName	The name of the service context.

MIB Object	Description
cAppNavServContextCurrOpState	The current operational state of the service context.
cAppNavServContextLastOpState	The last operational state of the service context.
cAppNavServContextIRState	The **Interception Readiness** (IR) state of the service context.
cAppNavServContextJoinState	The **Join** state of the service context.

Class Maps (CISCO-WAN-OPTIMIZATION-MIB)

AppNav class maps classify traffic according to one or more match conditions, such as peer device ID, or a mix of one peer device ID and the source IP, or destination IP, or destination port. The following table shows class map information MIB objects.

Table 107: Class Map Information MIB Objects

MIB Object	Description
cwoCmapStatsType	The class map type, such as HTTP, MAPI, NFS, or a custom class map.
cwoCmapStatsName	The name of the class map.
cwoCmapStatsDescr	The descriptive information of the class map configured on the WAN optimization system. If the description is not configured for a given class map, then this string will be a NULL string.
cwoCmapStatsTotalConns	The total number of connections processed by the class map.
cwoCmapStatsTotalBytes	The total number of bytes processed by the class map.
cwoCmapStatsTotalPTConns	The total connections made as pass-through, due to some reason by the class map.
cwoCmapStatsTotalPTBytes	The total number of bytes made pass-through by the class map.

Configuration (CISCO-CONFIG-MAN-MIB)

The CISCO-CONFIG-MAN-MIB group represents a model of configuration data that exists in various locations:

- **Running**: In use by the running system
- **Terminal**: Saved to whatever hardware is attached as the terminal
- **Local**: Saved locally in NVRAM or in flash memory
- **Remote**: Saved to a server on the network

Note The CISCO-CONFIG-MAN-MIB group includes only operations that are specifically related to configuration, although some of the system functions can be used for general file storage and transfer.

CPU and Memory (CISCO-PROCESS-MIB)

The CISCO-PROCESS-MIB group displays memory and CPU usage on the device and also describes active system processes.

CPU utilization presents a status of how busy the system is. The numbers are a ratio of the current idle time over the longest idle time. (This information should be used as an estimate only.)

Table 108: CPU and Memory Information MIB Objects

MIB Object	Description
cpmCPUTotal1minRev	The overall CPU percentage showing how busy the system was in the last 1 minute.
cpmCPUTotal5minRev	The overall CPU percentage showing how busy the system was in the last 5 minutes.

Devices (CISCO-CDP-MIB and CISCO-ENTITY-ASSET-MIB)

This section describes two MIB groups:

CISCO-CDP-MIB Group

The CISC-CDP-MIB group displays the ifIndex value of the local interface.

For example:

- For 802.3 repeaters on which the repeater ports do not have ifIndex values assigned, this value is a unique value for the port and is greater than any ifIndex value supported by the repeater.
- In this example, the specific port is indicated by the corresponding values of cdpInterfaceGroup and cdpInterfacePort, where these values correspond to the group number and the port number values of RFC 1516.

CISCO-ENTITY-ASSET-MIB Group

The CISCO-ENTITY-ASSET-MIB group provides information about items in the entPhysicalTable MIB object, including part number, serial number, hardware version, firmware ID and software ID. A full description of these is provided in RFC 2037.

Note the following about information listed in entPhysicalTable:

- Displayed information includes 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 entPhysicalTable. Entities that have none of this data available are not listed in this MIB.
- The entPhysicalTable is sparsely populated. Therefore, some variables may not exist for a particular entity at a particular time.

For example, a row that represents a powered-off module may have no values for software ID (ceAssetSoftwareID) and revision (ceAssetSoftwareRevision). Similarly, a power supply would probably never have firmware or software information listed in the table.

- The data may have other items encoded in it.

For example, a manufacturing date in the serial number, consider all data items to be a single unit. Do not decompose the items or parse them. Use only string equal and unequal operations on them.

DRE Cache (CISCO-WAN-OPTIMIZATION-MIB)

The following table displays optimization DRE cache statistics MIB objects, which provide information such as the portion of disk space allocated for DRE cache or the percentage of DRE disk space currently being used.

Table 109: DRE Cache Statistics MIB Objects

MIB Object	Description
cwoDreCacheStatsStatus	The status of the portion of the disk allocated for DRE cache: **Initializing**, **Usable**, or **Failed**.
cwoDreCacheStatsAge	The age of the oldest data present in the DRE cache. When new data is written to the DRE cache portion of the disk, it replaces the oldest data in the DRE cache.
cwoDreCacheStatsTotal	The portion of disk space allocated for DRE cache, in MB. For example, if the total cache disk space is 708 MB, and the portion allocated for DRE cache is 10%, then the value of cwoDreCacheStatsTotal, as shown below in the sample output, is 70800 MB.
cwoDreCacheStatsUsed	The percentage of DRE disk space currently being used. For example, if the disk space allocated for DRE is 70800 MB, and the value of **cwoDreCacheStatsUsed** is 85%, as shown below in the sample output, this indicates that 60,180 MB of the DRE cache disk space is being used, and 10,620 MB of the DRE cache disk space is free.
cwoDreCacheStatsDataUnitUsage	The DRE cache disk space currently being used, by data unit.
cwoDreCacheStatsReplacedOneHrDataUnit	The amount of data units replaced in the DRE cache in the last hour. Data is replaced on a First In/First Out (FIFO) order, and is stored in the DRE cache data block.
cwoDreCacheStatsDataUnitAge	The age of the oldest data unit in the data block. When new data is written to the data block when the data block is full, the oldest data unit is removed.
cwoDreCacheStatsSigblockUsage	The DRE disk space currently used by the signature block.
cwoDreCacheStatsReplacedOneHrSigblock	The amount of cache replaced within the last hour by the signature block.

MIB Object	Description
cwoDreCacheStatsSigblockAge	The time that the DRE Sigblock has been in the cache in days (d),hours (h), minutes (m), and seconds (s). For example, “1d1h” means 1 day, 1 hour.

DRE Performance (CISCO-WAN-OPTIMIZATION-MIB)

The following table displays DRE performance MIB objects, which provide information such as DRE compression ratio during decoding or the decoding average message size.

Table 110: DRE Performance Statistics MIB Objects

MIB Object	Description
cwoDrePerfStatsEncodeCompressionRatio	The DRE compression ratio during encoding.
cwoDrePerfStatsEncodeCompressionLatency	The Encoding average latency introduced to compress a message.
cwoDrePerfStatsEncodeAvgMsgSize	The Encoding average message size.
cwoDrePerfStatsDecodeCompressionRatio	The DRE compression ratio during decoding.
cwoDrePerfStatsDecodeCompressionLatency	The Decoding average latency introduced to compress a message.
cwoDrePerfStatsDecodeAvgMsgSize	The Decoding average message size.

HTTP (CISCO-WAN-OPTIMIZATION-MIB)

The following table shows the HTTP AO information MIB objects, which provide information such as the percentage estimated time saved due to optimizations done by HTTP AO since it was started or the total number of SharePoint Optimized HTTP sessions.

Table 111: HTTP AO Information MIB Objects

MIB Object	Description
cwoAoHttpxStatsTotalSavedTime	The total time saved due to optimizations done by HTTP AO since it was started.
cwoAoHttpxStatsTotalRTT	The total Round Trip Time (RTT) for all the connections going through HTTP AO since it was started.
cwoAoHttpxStatsTotalMDCMTime	The Meta Data Cache Misses (MDCM) for HTTP AO since it was started.
cwoAoHttpxStatsEstSavedTime	The percentage estimated time saved due to optimizations done by HTTP AO since it was started.

MIB Object	Description
cwoAoHttpxStatsTotalSPSessions	The total number of SharePoint Optimized HTTP sessions. This counter is incremented for every session on which SharePoint optimization can be performed. An HTTP session is tagged as a SharePoint Session based on the information present in the HTTP request.
cwoAoHttpxStatsTotalSPPFSessions	The total number of SharePoint Pre-fetch optimized HTTP sessions. • This counter is incremented for every session on which SharePoint pre-fetch optimization can be performed. • An HTTP session is tagged as a SharePoint pre-fetch Session based on the information present in the HTTP request. • A pre-fetch operation is one where the edge WAAS device fetches the next set of data (which it anticipates the client will request later) from the server based on the current HTTP Request information.
cwoAoHttpxStatsTotalSPPFObjects	The total number of pre-fetched objects served locally for SharePoint pre-fetch sessions. • The edge WAAS device maintains a local cache where the pre-fetched responses are saved. • This object is incremented whenever the SharePoint client request is served from the pre-fetch cache.
cwoAoHttpxStatsTotalSPRTTSaved	The total Round Trip Time (RTT) saved due to SharePoint pre-fetch optimizations since SharePoint pre-fetch optimization was started.
cwoAoHttpxStatsTotalSPPFMissTime	The total time for SharePoint pre-fetch Cache Misses since SharePoint pre-fetch optimization was started.

Note Discontinuities in the value of these HTTP counters can occur at re-initialization of the HTTP AO. The last discontinuity time is indicated by the value of **cwoAoStatsLastResetTime** for the HTTP AO.

Interfaces (IF-MIB)

The IF-MIB group 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.

Loopback interface interface information are not reported.

A transmission error or discard can point to Layer 1 or Layer 2 problems, such as a bad cable or a speed/duplex mismatch on a connected switch or router.

This section contains the following types of MIB objects for the IF-MIB group:

Interface Description MIB Object

The ifDescr MIB object displays information about the interface, including the name of the manufacturer, the product name, and the version of the hardware or software interface.

Interface Status MIB Objects

This section describes two interface status MIB objects:

- **ifAdminStatus**: Displays the desired (specified) status of the interface:
  - **up (1)**: The interface is up and ready to transmit and receive network traffic.
  - **down (2)**: The interface is down.
  - **testing (3)**: In the Testing state, no operational packets can be passed.

Note At system startup, all interfaces start with ifAdminStatus down. After either management action or configuration information, ifAdminStatus is changed to either up or testing, or remains down.

- **ifOperStatus**: Displays the current operational status of the interface:
  - **up (1)**: The interface is up and ready to transmit and receive network traffic.
  - **down (2)**: The interface is down.
  - **testing(3)**: In the Testing state, no operational packets can be passed.
  - **unknown(4)**: The status of the interface cannot be determined.
  - **dormant(5)**: The interface is waiting for an external action.
  - **notPresent(6)**: The interface has a missing component; usually a missing hardware component.
  - **lowerLayerDown(7)**: The interface is down due to a lower-layer interface.

Note If **ifAdminStatus** is down, then **ifOperStatus** should also be down. If **ifAdminStatus** is up, then **ifOperStatus** should also be up.

Interface Discards MIB Objects

Table 112: Interface Discards MIB Objects

MIB Object	Description
ifInDiscards	Displays the number of inbound packets selected to be discarded, even though no errors have been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding such a packet is to free up buffer space.
ifOutDiscards	The number of outbound packets selected to be discarded, even though no errors had been detected to prevent them from being transmitted. A possible reason for discarding such a packet is to free up buffer space. The **ifInDiscards** MIB object is usually a subset of the **locIfInputQueueDrops** MIB object.

Note Discontinuities in the value of **ifInDiscards** or of **ifOutDiscards** can occur at re-initialization of the management system and at other times, as indicated by the value **ifCounterDiscontinuityTime**.

Interface Errors MIB Objects

Table 113: Interface Errors MIB Objects

MIB Object	Description
ifInErrors	For packet-oriented interfaces, the number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol. For character-oriented or fixed-length interfaces, the number of inbound transmission units that contained errors preventing them from being deliverable to a higher-layer protocol.
ifOutErrors	For packet-oriented interfaces, the number of outbound packets that could not be transmitted because of errors. For character-oriented or fixed-length interfaces, the number of outbound transmission units that could not be transmitted because of errors.

Note Discontinuities in the value of **ifInErrors** or of **ifOutErrors** can occur at re-initialization of the management system and at other times, as indicated by the value **ifCounterDiscontinuityTime**.

IP Routing (IP-MIB, IP-FORWARD-MIB, MIB-II)

This section contains the following MIB groups:

IP-MIB Group

The IP-MIB group manages IP and ICMP implementations, excluding their management of IP routes.

IP-FORWARD-MIB Group

Displays Classless Inter-Domain Routing (CIDR) multi-path IP Routes.

MIB-II Group

The MIB-II group is the Internet Standard MIB, and is used with network management protocols in TCP/IP-based internets. The MIB-II is documented in RFC 1213, and is found in the RFC1213-MIB file in the v1 directory on the download site (other MIBs are in the v2 directory).

The following objects from this MIB are not supported:

- ifInUnknownProtos
- ifOutNUcastPkts
- ipRouteAge
- TcpConnEntry group
- egpInMsgs
- egpInErrors
- egpOutMsgs
- egpOutErrors
- EgpNeighEntry group
- egpAs
- atTable
- ipRouteTable

MAPI (CISCO-WAN-OPTIMIZATION-MIB)

The following table displays the Message Application Programming Interface (MAPI) AO MIB objects.

Note For these MIB objects, discontinuities in the value of the counter can occur at re-initialization of the MAPI AO. The last discontinuity time is indicated by the value of cwoAoStatsLastResetTime for the MAPI AO.

Table 114: MAPI AO MIB Objects

MIB Object	Description
cwoAoMapixStatsUnEncrALRT	The Average Local Response Time (ALRT) for unencrypted connections of MAPI AO since it was started.
cwoAoMapixStatsUnEncrARRT	The Average Remote Response Time (ARRT) for unencrypted connections of MAPI AO since it was started.
cwoAoMapixStatsTotalUnEncrLRs	The total requests served locally for unencrypted connections by MAPI AO since it was started.

MIB Object	Description
cwoAoMapixStatsTotalUnEncrRRs	The total Remote Requests(RR) served by remote servers for unencrypted connections of MAPI AO since it was started.
cwoAoMapixStatsUnEncrAvgRedTime	The average time reduced for unencrypted connections due to optimizations done by MAPI AO since it was started.
cwoAoMapixStatsEncrALRT	The Average Local Response Time (ALRT) for encrypted connections of MAPI AO since it was started.
cwoAoMapixStatsEncrARRT	The Average Remote Response Time (ARRT) for encrypted connections of MAPI AO since it was started.
cwoAoMapixStatsTotalEncrLRs	The total requests served locally for encrypted connections by MAPI AO since it was started.
cwoAoMapixStatsTotalEncrRRs	The total Remote Requests (RR) served by remote servers for encrypted connections by MAPI AO since it was started.
cwoAoMapixStatsEncrAvgRedTime	The average time reduced for encrypted connections due to optimizations done by MAPI AO since it was started.

Network Management (EVENT-MIB, HOST-RESOURCES-MIB)

This section contains the following MIB groups:

EVENT-MIB Group

The EVENT-MIB group defines the event triggers and actions for network management purposes. This MIB is described in RFC 2981.

HOST-RESOURCES-MIB Group

This MIB manages host systems. The term “host” implies any computer that communicates with other similar computers connected to the Internet.

The HOST-RESOURCES-MIB provides attributes that are common to all Internet hosts, for example, personal computers and systems that run variants of UNIX. It does not apply to devices whose primary function is communications services (terminal servers, routers, bridges, monitoring equipment).

The following objects from this MIB are not supported:

- HrPrinterEntry
- hrSWOSIndex
- hrSWInstalledGroup

Policy Maps (CISCO-WAN-OPTIMIZATION-MIB)

Policy maps associate policy actions with class maps. The following table shows the policy maps MIB objects, which display information such as the type of policy map or the total number of connections processed by the policy map since it has been active.

Table 115: Policy Maps MIB Objects

MIB Object	Description
cwoPmapStatsType	The type of policy map.
cwoPmapStatsName	The name of the policy map.
cwoPmapStatsDescr	The description of the policy map configured on the WAN optimization system. If a description is not configured for a particular policy map, this string will contain a NULL string.
cwoPmapStatsTotalConns	The total number of connections processed by the policy map since it has been active.
cwoPmapStatsTotalBytes	The total bytes processed by the policy map since it has been active.
cwoPmapStatsTotalPTConns	The total connections made as pass-through connections, due to some reason by the policy map, since it has been active.
cwoPmapStatsTotalPTBytes	The total bytes made as pass-through, due to some reason by the policy map, since it has been active.

SMB (CISCO-WAN-OPTIMIZATION-MIB)

The CISCO-WAN-OPTIMIZATION-MIB group displays information about the status and statistics associated with optimization and application accelerators.

Note For these MIB objects, discontinuities in the value of the counter can occur at re-initialization of the SMB AO. The last discontinuity time is indicated by the value of **cwoAoStatsLastResetTime** for the SMB AO.

This section describes the cwoAoSmbxStats MIB objects, and contains the following topics:

About SMB Statistics MIB Objects

The Server Message Block (SMB) application accelerator (AO) transparently accelerates traffic and supports prepositioning of files. It relies on automatic discovery. You can fine-tune this accelerator for specific traffic needs.

cwoAoSmbxStats MIB Objects for Cache Information

Table 116: SMB AO Cache MIB Objects

MIB Object	
cwoAoSmbxStatsBytesReadCache	The total number of bytes read from the SMB AO cache (Read-ahead and Metadata cache) since it was started.
cwoAoSmbxStatsBytesWriteCache	The total number of bytes written to SMB AO cache (Read-ahead and Metadata) since it was started.

MIB Object	
cwoAoSmbxStatsMDCacheHitCount	The SMB AO Metadata cache hit count since SMB AO was started.
cwoAoSmbxStatsMDCacheHitRate	The SMB AO Metadata cache hit rate since it was started.
cwoAoSmbxStatsMaxRACacheSize	The maximum disk space that can be allocated for Read Ahead data in the SMB AO cache.
cwoAoSmbxStatsMaxMDCacheSize	The maximum disk space that can be allocated for Metadata in the SMB AO cache
cwoAoSmbxStatsRAEvictedAge	The amount of time spent in the SMB AO Read Ahead cache by the resource that was last evicted since last update. **Note** If this amount is too short or too long, we recommend that you modify the size of the cache.
cwoAoSmbxStatsTotalFilesInRACache	The total number of files in the SMB AO Read Ahead cache.

cwoAoSmbxStats MIB Objects for Client and Server Information

Table 117: SMB AO Client and Server MIB Objects

MIB Object	Description
cwoAoSmbxStatsBytesReadServer	The total number of bytes read from file servers by SMB AO since it was started.
cwoAoSmbxStatsBytesWriteServer	The total number of bytes written to file servers by SMB AO since it was started.
cwoAoSmbxStatsBytesReadClient	The total number of bytes read by SMB AO clients since it was started.
cwoAoSmbxStatsBytesWriteClient	The total number of bytes written by SMB AO clients since it was started.

cwoAoSmbxStats MIB Objects for LAN and WAN Information

Table 118: SMB AO LAN and WAN MIB Objects

MIB Object	Description
cwoAoSmbxStatsRdL4SignWANBytes	The total number of Layer 4 (L4) optimized signed bytes read from WAN by SMB AO since the SMB AO was started. L4 optimization includes TFO, DRE and LZ optimizations.
cwoAoSmbxStatsWrL4SignWANBytes	The total number of Layer 4 (L4) optimized signed bytes written to WAN by SMB AO since SMB AO was started. L4 optimization includes TFO, DRE and LZ optimizations.
cwoAoSmbxStatsRdSignLANBytes	The total number of signed bytes read from LAN by SMB AO since the SMB AO was started.

MIB Object	Description
cwoAoSmbxStatsWrSignLANBytes	The total number of original signed bytes written to LAN by SMB AO since SMB AO was started. **Note** Discontinuities in the values of these counters can occur at re-initialization of the SMB AO. The last discontinuity time is indicated by the value of cwoAoStatsLastResetTime for the SMB AO.

cwoAoSmbxStats MIB Objects for RTT, Response Time, and File Information

Table 119: SMB RTT, Response Time, and File Information MIB Objects

MIB Object	Description
cwoAoSmbxStatsRTT	The total round trip time (RTT) for all SMB connections since it was started.
cwoAoSmbxStatsTotalRespTimeSaving	The total response time saved due to SMB AO optimizations since it was started.
cwoAoSmbxStatsOpenFiles	The number of files currently opened by the SMB AO.

cwoAoSmbxStats MIB Objects for SMB Requests Information

Table 120: SMB Requests MIB Objects

MIB Object	Description
cwoAoSmbxStatsProcessedReqs	The total number of requests processed by the SMB AO since it was started.
cwoAoSmbxStatsActiveReqs	The total number of active requests getting processed by the SMB AO.
cwoAoSmbxStatsTotalRemoteReqs	The total number of SMB requests sent to the remote file server since the SMB AO was started.
cwoAoSmbxStatsTotalLocalReqs	The total number of SMB requests served locally by the SMB AO since it was started.
cwoAoSmbxStatsRemoteAvgTime	The average duration of time taken by the SMB AO to process all remote requests since it was started.
cwoAoSmbxStatsLocalAvgTime	The average duration of time taken by the SMB AO to process all local requests since it was started.

SNMP (ENTITY, ISNMP, and SNMP MIB Groups)

This section describes the following SNMP MIB groups:

- ENTITY-MIB: Represents multiple logical entities supported by a single SNMP agent. This MIB is documented in RFC 2737. The following objects are supported:

    - entityPhysicalGroup
    - entityLogicalGroup
    - entConfigChange

- SNMP-FRAMEWORK-MIB: Facilitates remote configuration and administration of the SNMP entity. This MIB is documented in RFC 2571.
- SNMP-NOTIFICATION-MIB: Contains objects for the remote configuration of the parameters used by an SNMP entity for the generation of notifications. This MIB is documented in RFC 3413.
- SNMP-TARGET-MIB: Provides information about specifying targets of management operations for notification filtering and for proxy forwarding. This MIB is documented in RFC 3413.
- SNMP-USM-MIB: Provides information on the User-based Security Model.
- SNMP-VACM-MIB: Provides information on the View-based Access Control Model.
- SNMPv2-MIB: For this MIB group, WAAS supports the following MIB objects:
    - **coldStart**: Signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.
    - **linkUp**: The link up trap/notification.
    - **linkDown**: The link down trap/notification.
    - **authenticationFailure**: Signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.

This MIB is documented in RFC 1907.

TFO (CISCO-WAN-OPTIMIZATION-MIB)

The CISCO-WAN-OPTIMIZATION-MIB group displays information about the status and statistics associated with optimization and application accelerators.

This section describes the **cwoTfoStats** MIB objects, and contains the following topics:

About TFO Statistics MIB Objects

Cisco WAAS uses a variety Transport Flow Optimization (TFO) features to optimize TCP traffic intercepted by the Cisco WAAS devices. TFO protects communicating clients and servers from negative WAN conditions, such as bandwidth constraints, packet loss, congestion, and retransmission.

cwoTfoStats MIB Object for TFO Load Status

Table 121: TFO Load Status MIB Object

MIB Object	Description
cwoTfoStatsLoadStatus	Displays the current TFO load status: • **Unknown (1)**: TFO is in an unknown state, not active or disabled. • **Green (2)**: TFO is operating normally, within acceptable load limits. • **Yellow (3)**: TFO is overloaded, and new connections received may not be optimized. • **Red (4)**: TFO is not working properly, and both existing and new connections may not be optimized. **Note** If **cwoTfoStatsLoadStatus** shows **Unknown (1)**, **Yellow (3)** or **Red (4)**, then the TFO is either overloaded or has some other error condition, and no optimization can occur at any other level, such as DRE, LZ, or AO.
cwoTfoStatsTotalOptConn	The total number of connections optimized by the specified AO since it was started or since its statistics were last reset.
cwoTfoStatsTotalNormalClosedConn	The total number of optimized TCP connections that were closed normally since TFO was started, or since its statistics were last reset.
cwoTfoStatsResetConn	The total number of optimized TCP connections that have been reset since TFO was started or since its statistics were last reset.

cwoTfoStats MIB Objects for TFO Summary Connection Information

Table 122: TFO Summary Connection MIB Objects

MIB Object	Description
cwoTfoStatsLoadStatus	Displays the current TFO load status: • **Unknown (1)**: TFO is in an unknown state, not active or disabled. • **Green (2)**: TFO is operating normally, within acceptable load limits. • **Yellow (3)**: TFO is overloaded, and new connections received may not be optimized. • **Red (4)**: TFO is not working properly, and both existing and new connections may not be optimized. **Note** If **cwoTfoStatsLoadStatus** shows **Unknown (1)**, **Yellow (3)** or **Red (4)**, then the TFO is either overloaded or has some other error condition, and no optimization can occur at any other level, such as DRE, LZ, or AO.
cwoTfoStatsTotalOptConn	The total number of connections optimized by the specified AO since it was started or since its statistics were last reset.
cwoTfoStatsTotalNormalClosedConn	The total number of optimized TCP connections that were closed normally since TFO was started, or since its statistics were last reset.
cwoTfoStatsResetConn	The total number of optimized TCP connections that have been reset since TFO was started or since its statistics were last reset.

cwoTfoStats MIB Objects for TFO Current Connection Information

Table 123: TFO Current Connection MIB Objects

MIB Object	Description
cwoTfoStatsActiveOptConn	The number of active TCP connections that are getting optimized.
cwoTfoStatsMaxActiveConn	The maximum number of active TCP connections that the specified device can optimize.
cwoTfoStatsActivePTConn	The number of active pass-through TCP connections.
cwoTfoStatsActiveOptTCPPlusConn	The number of active TCP connections going through TCP plus other optimization.
cwoTfoStatsActiveOptTCPOnlyConn	The number of active TCP connections going through TCP optimization only.

MIB Object	Description
cwoTfoStatsActiveOptTCPPrepConn	The number of active TCP connections that were originated by an accelerator to acquire data in anticipation of its future use.
cwoTfoStatsStatsActiveADConn	The number of current active TCP connections in the auto-discovery state.
cwoTfoStatsReservedConn	The number of TCP connections that are reserved for the MAPI accelerator.
cwoTfoStatsPendingConn	The number of TCP connections that are pending in the queue of connections to be optimized.

Downloading MIB Files

You can download the MIB files for most of the MIBS that are supported by a device that is running the WAAS software from the following Cisco FTP site:

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

You can download the RFC1213-MIB file (for MIB-II) from the following Cisco FTP site:

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

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

Using MIBs to Monitor Cisco WAAS

This section contains usage examples and sample output for using MIB files to monitor WAAS:

Using MIBs to Display Alarm Status

This section provides usage examples and sample output for Cisco WAAS alarm information. For more information on these MIBs, see Alarms (CISCO-CONTENT-ENGINE-MIB), on page 656.

- To verify that there are no alarms on the system, use **cceAlarm**:

```
CISCO-CONTENT-ENGINE-MIB::cceAlarmMinorCount.0 = Gauge32: 0
CISCO-CONTENT-ENGINE-MIB::cceAlarmMajorCount.0 = Gauge32: 0
CISCO-CONTENT-ENGINE-MIB::cceAlarmCriticalCount.0 = Gauge32: 0
```

Using MIBs to Display AO Information and Status

This section provides usage examples and sample MIB output for WAAS AO information and status. For more information on these MIBs, see AOs (CISCO-WAN-OPTIMIZATION-MIB), on page 656.

- To verify the configuration status of WAAS AOs, use **cwoAoStatsIsConfigured**:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsIsConfigured."epm" = INTEGER: true(1)
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsIsConfigured."ica" = INTEGER: false(2)
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsIsConfigured."nfs" = INTEGER: true(1)
```

```
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsIsConfigured."smb" = INTEGER: true(1)
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsIsConfigured."ssl" = INTEGER: true(1)
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsIsConfigured."http" = INTEGER: true(1)
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsIsConfigured."mapi" = INTEGER: true(1)
```

- To verify the operational state of configured WAAS AOs, use **cwoAoStatsOperationState**:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsOperationalState."epm" = INTEGER: normalRunning(3)
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsOperationalState."ica" = INTEGER: shutdown(1)
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsOperationalState."nfs" = INTEGER: normalRunning(3)
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsOperationalState."smb" = INTEGER: normalRunning(3)
CISCO-WAN-OPTIMIZATION-MIB::cwoAoStatsOperationalState."ssl" = INTEGER: normalRunning(3)
```

Using MIBs to Display DRE Cache and Performance Information

This section provides usage examples and sample MIB output for DRE cache and performance information.

For overview information on these MIBs, see DRE Cache (CISCO-WAN-OPTIMIZATION-MIB), on page 664 andDRE Performance (CISCO-WAN-OPTIMIZATION-MIB), on page 665.

- To verify if DRE is operational and the DRE is in a usable state (the DRE states are **Initializing**, **Usable**, **Failed**), use **cwoDreCacheStatsStatus**:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsStatus.0 = STRING: Usable
```

- To display DRE cache age, use **cwoDreCacheStatsAge**:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsAge.0 = STRING: 5d17h
```

Note On both branch and datacenter devices, the cache age should provide an effective capacity-to-reduction ratio. It is important that you baseline this value and set triggers according to your specific use case.For a datacenter device, the cache age should be approximately 5 to 7 days. However, there are scenarios where your cache age could be much lower and Cisco WAAS is still providing a very good reduction ratio; for example, in replication or backup scenarios. For a branch device, the cache age in practice will likely be more than 5 to 7 days.

- To display DRE cache information, including the portion of the disk space allocated for DRE cache, the age of the oldest data unit the data block, and the amount of data units replaced in the last hour, use **cwoDreCacheStats** MIB objects:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsTotal.0 = Counter64: 77822 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsUsed.0 = Gauge32: 96 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsDataUnitUsage.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsReplacedOneHrDataUnit.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsDataUnitAge.0 = STRING: 0s
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsSigblockUsage.0 = Counter64: 1695 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsReplacedOneHrSigblock.0 = Counter64: 0 MB
CISCO-WAN-OPTIMIZATION-MIB::cwoDreCacheStatsSigblockAge.0 = STRING: 14d17h
```

- To display compression ratio values, use **cwoDrePerfStats** MIB objects. For datacenter devices, it is especially useful to view Encode compression ratio values, and for branch devices, it is especially useful to view Decode compression ratio values.

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsEncodeCompressionRatio.0 = Gauge32: 9 percent
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsDecodeCompressionRatio.0 = Gauge32: 51 percent
```

- To display compression latency values, use **cwoDrePerfStats** MIB objects. For datacenter devices, it is especially useful to view Encode compression latency values, and for branch devices, it is especially useful to view Decode compression latency values.

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsEncodeCompressionLatency.0 = Counter64: 0 ms
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsDecodeCompressionLatency.0 = Counter64: 0 ms
```

Note Set a baseline for the latency value. If the latency value begins to deviate higher than normal, it could indicate a potential disk problem or failing disk, or it could indicate that a new traffic pattern is driving higher than normal disk input/output.

- To display the average size of all the messages handled by DRE during encoding or decoding, use **cwoDrePerfStats** MIB objects:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsEncodeAvgMsgSize.0 = STRING: 1991 B
CISCO-WAN-OPTIMIZATION-MIB::cwoDrePerfStatsDecodeAvgMsgSize.0 = STRING: 1082 B
```

Using MIBs to Display Interface Information

This section provides usage examples and sample MIB output for interface information—description, status, and transmission errors and discards. For more information on these MIBs, see Interfaces (IF-MIB), on page 666.

- To check the up/down status of your interfaces, use **ifDescr**, **ifAdminStatus**, and **ifOperStatus**.

```
IF-MIB::ifDescr.1 = STRING: GigabitEthernet 0/0
IF-MIB::ifDescr.2 = STRING: GigabitEthernet 0/1
IF-MIB::ifAdminStatus.1 = INTEGER: up(1)
IF-MIB::ifAdminStatus.2 = INTEGER: up(1)
IF-MIB::ifOperStatus.1 = INTEGER: up(1)
IF-MIB::ifOperStatus.2 = INTEGER: down(2)
```

- To check if there are any transmission-related errors which could point to L1 and L2 problems (e.g. bad cable or speed/duplex mismatch on connected switch/router), use **ifInErrors** and **ifInDiscards**.

```
IF-MIB::ifInErrors.1 = Counter32: 0
IF-MIB::ifInErrors.2 = Counter32: 0
IF-MIB::ifOutErrors.1 = Counter32: 0
IF-MIB::ifOutErrors.2 = Counter32: 0
IF-MIB::ifInDiscards.1 = Counter32: 0
IF-MIB::ifInDiscards.2 = Counter32: 0
IF-MIB::ifOutDiscards.1 = Counter32: 0
IF-MIB::ifOutDiscards.2 = Counter32: 0
```

Using MIBs to Display TFO Information

This section provides usage examples and sample MIB output for TFO information and status. For more information on these MIBs, see TFO (CISCO-WAN-OPTIMIZATION-MIB), on page 674.

This section contains the following topics:

Performing Trend and Baseline Analysis with TFO MIBs

Before you begin

To be able to assess what normal load and benefits Cisco WAAS provides for your network, we recommend that you perform some trend and baseline analysis. Then, based on the results, you can create traps and alerts if the counters are above or below your defined thresholds, whichever is appropriate for the specific counter.

Procedure

Step 1 To verify key connection information, use the following MIB to verify the maximum number of connections the system can optimize.

```
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsMaxActiveConn.0 = Counter64: 750
```

Step 2 Use the following MIB object to verify the total number of active optimized connections:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsActiveOptConn.0 = Counter64: 21
```

Step 3 After verifying the maximum number of connections and the total active optimized connections, you can do one of the following:

- Set an alert in your monitoring tool.

Or

- Set an SNMP trap if the number gets close to the limit on a consistent basis.

For example, the WAAS poll interval is every 5 minutes. An alert is triggered if within a 1-hour or 4-hour period the total number of active optimized connections crosses 90% of the maximum number of connections the system can optimize 10 times.

For how to set an SNMP trap, see Enabling SNMP Traps, on page 683.

Displaying Connection Information Using cwoTfoStats

To display connection information, use **cwoTfoStats** MIB objects:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsTotalNormalClosedConn.0 = 0
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsPendingConn.0 = 0
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsReservedConn.0 = 0
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsResetConn.0 = 0
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsOptConn.0 = 0
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsMaxActiveConn.0 = 0
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsTotalOptConn.0 = 0
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsActivePTConn.0 = 0
```

Displaying TFO Auto-Discovery and Load Status Information Using cwoTfoStats

To display TFO auto-discovery and load status information, use **cwoTfoStats**:

```
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsActiveADConn.0 = 0
CISCO-WAN-OPTIMIZATION-MIB::cwoTfoStatsLoadStatus.0 = INTEGER: green(2)
```

Note If the TFO load status shows **Unknown(1)**, **Yellow(3)** or **Red(4)**, then the TFO is overloaded or has some other error condition, and no optimization can occur at any other level, such as DRE, LZ, or AO.

Enabling the SNMP Agent on a WAAS Device

By default, the SNMP agent on WAAS devices is disabled and an SNMP community string is not defined. The SNMP community string is used as a password for authentication when accessing the SNMP agent on a WAAS device. To be authenticated, the Community Name field of any SNMP message sent to the WAAS device must match the SNMP community string defined on the WAAS device.

The SNMP agent on a WAAS device is enabled when you define the SNMP community string on the device. The WAAS Central Manager GUI allows you to define the SNMP community string on a device or device group.

If the SNMPv3 protocol is going to be used for SNMP requests, the next step is to define an SNMP user account that can be used to access a WAAS device through SNMP. For more information on how to create an SNMPv3 user account on a WAAS device, see Creating an SNMP User, on page 693.

Checklist for Configuring SNMP

The following is a checklist for enabling SNMP monitoring on a Cisco WAAS device or device group.

Procedure

	Command or Action	Purpose
Step 1	Prepare for SNMP monitoring.	For more information, see Preparing for SNMP Monitoring, on page 682.
Step 2	Select the SNMP traps that you want to enable.	The Cisco WAAS Central Manager provides a wide-range of traps that you can enable on a Cisco WAAS device or device group. To define additional traps, see Defining SNMP Triggers to Generate User-Defined Traps, on page 686.
Step 3	Specify the SNMP host that receives the SNMP traps.	Specify the SNMP host to that the WAAS device or device group should send their traps to. You can specify multiple hosts so different WAAS devices send traps to different hosts.

	Command or Action	Purpose
		For more information, see Specifying the SNMP Host, on page 688.
Step 4	Specify the SNMP community string.	Specify the SNMP community string so external users can read or write to the MIB. For more information, see Specifying the SNMP Community String, on page 689.
Step 5	Set up SNMP views.	To restrict an SNMP group to a specific view, you must create a view that specifies the MIB subtree that you want the group to view. For more information, see Creating SNMP Views, on page 691.
Step 6	Create an SNMP group.	You must set up an SNMP group if are going to create any SNMP users or want to restrict a group to view a specific MIB subtree. For more information, see Creating an SNMP Group, on page 692.
Step 7	Create an SNMP user.	If the SNMPv3 protocol is going to be used for SNMP requests, you must create at least one SNMPv3 user account on the Cisco WAAS device in order for the WAAS device to be accessed through SNMP. For more information, see Creating an SNMP User, on page 693.
Step 8	Configure SNMP contact settings.	For more information, see Configuring SNMP Contact Settings, on page 695.

Preparing for SNMP Monitoring

Before you configure your Cisco WAAS network for SNMP monitoring, complete the following preparation tasks:

- Set up the SNMP host (management station) that the Cisco WAAS devices will use to send SNMP traps.
- Determine if all your Cisco WAAS devices will be sending traps to the same host, or to different hosts. Write down the IP address or hostname of each SNMP host.
- Obtain the community string used to access the SNMP agents.
- Determine if you want to create SNMP groups so you can restrict views by group.
- Determine what additional SNMP traps you need.
- Clock synchronization between the devices in a Cisco WAAS network is important. On each Cisco WAAS device, be sure to set up a Network Time Protocol (NTP) server to keep the clocks synchronized.

Enabling SNMP Traps

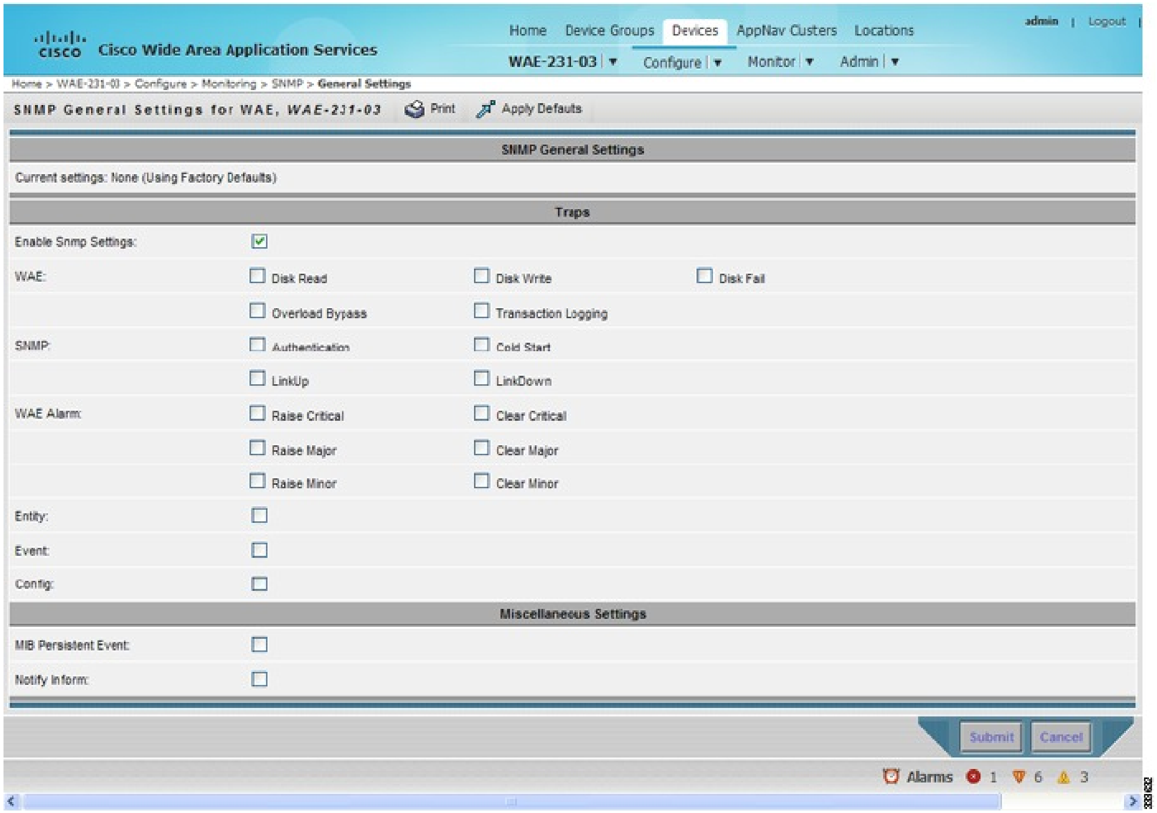
Procedure

Step 1 From the Cisco 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. The "SNMP General Settings" table desribes the fields in this window.

Figure 103: SNMP General Settings Window



SNMP General Settings for WAE, WAE-231-03

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:	□

Table 124: SNMP General Settings

GUI Parameter	Function
Traps	
Enable Snmp Settings	Enables SNMP traps.

GUI Parameter	Function
WAE	Enables SNMP WAE traps: • **Disk Read**: Enables disk read error trap. • **Disk Write**: Enables disk write error trap. • **Disk Fail**: Enables disk failure error trap. • **Overload Bypass**: Enables WCCP overload bypass error trap. • **Transaction Logging**: Enables transaction log write error trap.
SNMP	Enables SNMP-specific traps: • **Authentication**: Enables authentication trap. • **Cold Start**: Enables cold start trap. • **LinkUp**: Link up trap. • **LinkDown**: Link down trap.
WAE Alarm	Enables WAE alarm traps: • **Raise Critical**: Enables raise-critical alarm trap • **Clear Critical**: Enables clear-critical alarm trap • **Raise Major**: Enables raise-major alarm trap • **Clear Major**: Enables clear-major alarm trap • **Raise Minor**: Enables raise-minor alarm trap • **Clear Minor**: Enables clear-minor alarm trap
Entity	Enables SNMP entity traps.
Event	Enables the Event MIB.
Config	Enables CiscoConfigManEvent error traps.
Miscellaneous Settings	
MIB Persistent Event	Enables persistence for the SNMP Event MIB. (This check box is not shown when the selected device is a Central Manager.)

GUI Parameter	Function
Notify Inform	Enables the SNMP notify inform request. Inform requests are more reliable than traps but consume more resources in the router and in the network. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations. **Note** To send an SNMPv3 inform message, you must configure at least one SNMPv3 user with a remote SNMP ID option on the WAAS device. The SNMP ID is entered in octet string form. For example, if the IP address of a remote SNMP entity is 192.147.142.129, then the octet string would be 00:00:63:00:00:00:a1:c0:93:8e:81. (Colons will be removed in the show running-config command output.)

Step 3 Check the appropriate check boxes to enable SNMP traps.

Step 4 Click **Submit**.

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

What to do next

To enable SNMP traps from the CLI, run the **snmp-server enable traps** global configuration command.

To control access to the SNMP agent by an external SNMP server, run the **snmp-server access-list** global configuration command to apply an SNMP ACL.

Consider the following guidelines:

- If you are using an SNMP server ACL, you must permit the loopback interface.
- If you override the device group settings from the **SNMP General Settings** window, the Cisco WAAS Central Manager deletes the SNMP community, SNMP group, SNMP user, SNMP view, and SNMP host settings. You are asked to confirm this behavior.
- To define additional SNMP traps for other MIB objects of interest to your particular configuration, see Defining SNMP Triggers to Generate User-Defined Traps, on page 686.

Defining SNMP Triggers to Generate User-Defined Traps

Procedure

Step 1 From the Cisco 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 Entries** window appears. The columns in this window are the same as the parameters described in the "Creating New SNMP Trigger Settings" table

Step 3 In the taskbar, click the **Create New SNMP Trigger List Entry** icon.

The **Creating New SNMP Trigger** window appears. The "Creating New SNMP Trigger Settings" table describes the fields in this window.

Table 125: Creating New SNMP Trigger Settings

GUI Parameter	Function
Trigger Name	Custom-defined name for the notification trigger that you want to monitor.
MIB Name	MIB variable name of the object that you want to monitor.
Wild Card	(Optional) Check this check box if the MIB Name value is a wildcard. Note that this check box is disabled when editing the SNMP Trigger.
Frequency	Number of seconds (60–600) to wait between trigger samples.
Test	Test used to trigger the SNMP trap. Choose one of the following tests: • **absent**: A specified MIB object that was present at the last sampling is no longer present as of the current sampling. • **equal**: The value of the specified MIB object is equal to the specified threshold. • **greater-than**: The value of the specified MIB object is greater than the specified threshold value. • **less-than**: The value of the specified MIB object is less than the specified threshold value. • **on-change**: The value of the specified MIB object has changed since the last sampling. • **present**: A specified MIB object is present as of the current sampling that was not present at the previous sampling. • **threshold**: Configures a maximum and a minimum threshold for a MIB object.

GUI Parameter	Function
Sample Type	(Optional) Sample type, as follows: • **absolute**: The test is evaluated against a fixed integer value between zero and 2147483647. • **delta**: The test is evaluated against the change in the MIB object value between the current sampling and the previous sampling.
Threshold Value	Threshold value of the MIB object. This field is not used if absent, on-change, or present is chosen in the Test drop-down list.
MIB Var1MIB Var2MIB Var3	(Optional) Names of up to three alternate MIB variables to add to the notification. Validation of these names is not supported, so be sure to enter them correctly.
Comments	Description of the trap.

Step 4 In the appropriate fields, enter the MIB name, frequency, test, sample type, threshold value, and comments.

Note You can create valid triggers only on read-write and read-only MIB objects. If you create a trigger on a read-create MIB object, it is deleted from the Central Manager configuration after one one data feed poll cycle.

Step 5 Click **Submit**.

What to do next

Consider the following guidelines:

- The new SNMP trigger is listed in the **SNMP Trigger List** window.
- To edit an SNMP trigger, click the **Edit** icon next to the MIB name in the **SNMP Trigger List** Entries window.
- To delete an SNMP trigger, click the **Edit** icon next to the MIB name and then clicking the **Delete** taskbar icon.
- If you delete any of the default SNMP triggers, they will be restored after a reload.
- When you upgrade a WAE from an earlier version to the 6.0 version, all triggers are deleted.When you upgrade the Cisco WAAS Central Manager to Cisco WAAS Version 6.0, all the Device Group triggers will be copied to a WAE running a previous software version (if any) and all the Device Group triggers will be deleted. Also the Trigger Aggregate Settings will be set to false for all the WAES (running a version earlier than 6.0) that are being managed by the Cisco WAAS Central Manager (running Cisco WAAS Version 6.0 or later). This ensures that the DG triggers are no longer applied to any of the devices running a version earlier than Cisco WAAS Version 6.0.
- If you are using an SNMP server ACL, you must permit the loopback interface.
- When you downgrade a WAE from a Cisco WAAS Version 6.0 to an earlier release, all the IPv6 configurations will be removed. All the triggers and the monitor user configurations are deleted.
- To define SNMP traps from the CLI, run the **snmp trigger** global configuration command .

- To control access to the SNMP agent by an external SNMP server, run the **snmp-server access-list** global configuration command to apply an SNMP ACL.

Aggregating SNMP Triggers

An individual WAE device can have custom SNMP triggers defined and can belong to device groups that have other custom SNMP triggers defined.

In the SNMP Trigger List Entries window, the Aggregate Settings radio button controls how SNMP triggers are aggregated for an individual device, as follows:

- Choose **Yes** if you want to configure the device with all custom SNMP triggers that are defined for itself and for device groups to which it belongs.
- Choose **No** if you want to limit the device to just the custom SNMP triggers that are defined for itself.

When you change the setting, you get the following confirmation message: "This option will take effect immediately and will affect the device configuration. Do you wish to continue?" Click **OK** to continue.

Specifying the SNMP Host

Before you begin

Hosts are listed in the order in which they have been created. The maximum number of SNMP hosts that can be created is eight.

Procedure

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

Step 2 Choose **Configure** > **Monitoring** > **SNMP** > **Host**.

The **SNMP Hosts** window appears.

Step 3 In the taskbar, click the **Create New SNMP Host** icon.

The **Creating New SNMP Host** window appears. The following table describes the fields in this window.

Table 126: SNMP Host Settings

GUI Parameter	Function
Trap Host	Hostname or IP address of the SNMP trap host that is sent in SNMP trap messages from the WAE. This is a required field and now supports IPv6 addresses.
Community/User	Name of the SNMP community or user (64 characters maximum) that is sent in SNMP trap messages from the WAE. This is a required field.

GUI Parameter	Function
Authentication	Security model to use for sending notification to the recipient of an SNMP trap operation. Choose one of the following options from the drop-down list: • **No-auth**: Sends notification without any security mechanism. • **v2c**: Sends notification using Version 2c security. • **v3-auth**: Sends notification using SNMP Version 3 AuthNoPriv. • **v3-noauth**: Sends notification using SNMP Version 3 NoAuthNoPriv security. • **v3-priv**: Sends notification using SNMP Version 3 AuthPriv security.
Retry	Number of retries (1–10) allowed for the inform request. The default is 2 tries.
Timeout	Timeout for the inform request in seconds (1–1000). The default is 15 seconds.

Step 4 Enter the hostname or IP address of an SNMP trap host, SNMP community or user name, security model to send notification, and retry count and timeout for inform requests.

Step 5 Click **Submit**.

To specify the SNMP host from the CLI, run the **snmp-server host** global configuration command.

Specifying the SNMP Community String

Before you begin

An SNMP community string is the password used to access an SNMP agent that resides on Cisco WAAS devices. There are two types of community strings: group and read-write. Community strings enhance the security of your SNMP messages.

Community strings are listed in the order in which they have been created. The maximum number of SNMP communities that can be created is ten. By default, an SNMP agent is disabled, and a community string is not configured. When a community string is configured, it permits read-only access to all agents by default.

Procedure

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

Step 2 Choose **Configure** > **Monitoring** > **SNMP** > **Community**.

The **SNMP Community Strings** window appears.

Step 3 In the taskbar, click the **Create New SNMP Community** String icon.

The **Creating New SNMP Community String** window appears. The "SNMP Community Settings" table describes the fields in this window.

Table 127: SNMP Community Settings

GUI Parameter	Function
Community	Community string used as a password for authentication when you access the SNMP agent of the WAE. The **Community Name** field of any SNMP message sent to the WAE must match the community string defined here in order to be authenticated. Entering a community string enables the SNMP agent on the WAE. You can enter a maximum of 64 characters in this field. This is a required field.
Group name/rw	Group to which the community string belongs. The **Read/Write** option allows a read or write group to be associated with this community string. The **Read/Write** option permits access to only a portion of the MIB subtree. Choose one of the following three options from the drop-down list: • **None**: Choose this option if you do not want to specify a group name to be associated with the community string. The Group Name field remains disabled if you select this option. • **Group**: Choose this option if you want to specify a group name. • **Read/Write**: Choose this option if you want to allow read-write access to the group associated with a community string. The Group Name field remains disabled if you select this option. This is a required field.
Group Name	Name of the group to which the community string belongs. You can enter a maximum of 64 characters in this field. This field is available only if you have chosen the **Group** option in the previous field.

Step 4 In the appropriate fields, enter the community string, choose whether or not read-write access to the group is allowed, and enter the group name.

Step 5 Click **Submit**.

To configure a community string from the CLI, run the **snmp-server community** global configuration command.

Creating SNMP Views

Before you begin

To restrict a group of users to view a specific MIB tree, you must create an SNMP view using the Cisco WAAS Central Manager GUI. Once you create the view, you need to create an SNMP group and SNMP users that belong to this group as described in later sections.

Views are listed in the order in which they have been created. The maximum number of views that can be created is ten.

Procedure

Step 1 To create a Version 2 SNMP (SNMPv2) MIB view: From the Cisco WAAS Central Manager menu, choose **Devices** > *device-name* or **Device Groups** > *device-group-name*.

Step 2 Choose **Configure** > **Monitoring** > **SNMP** > **View**. The SNMP Views window appears.

Step 3 In the taskbar, click the **Create New View** icon.

The **Creating New SNMP View** window appears. The "SNMPv2 View Settings" table describes the fields in this window.

Table 128: SNMPv2 View Settings

GUI Parameter	Function
Name	String representing the name of this family of view subtrees (64 characters maximum). The family name must be a valid MIB name such as ENTITY-MIB. This is a required field.
Family	Object identifier (64 characters maximum) that identifies a subtree of the MIB. This is a required field.
View Type	View option that determines the inclusion or exclusion of the MIB family from the view. Choose one of the following two options from the drop-down list: • **Included**: The MIB family is included in the view. • **Excluded**: The MIB family is excluded from the view.

Step 4 In the appropriate fields, enter the view name, the family name, and the view type.

Step 5 Click **Submit**.

Step 6 Create an SNMP group that will be assigned to this view as described in the section that follows.

To create an SNMP view from the CLI, run the **snmp-server view** global configuration command.

Creating an SNMP Group

Before you begin

You must set up an SNMP group if you are going to create any SNMP users or want to restrict a group of users to view a specific MIB subtree.

Groups are listed in the order in which they have been created. The maximum number of SNMP groups that can be created is ten.

Procedure

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

Step 2 Choose **Configure** > **Monitoring** > **SNMP** > **Group**.

The **SNMP Group Strings for WAE** window appears.

Step 3 In the taskbar, click the **Create New SNMP Group String** icon.

The **Creating New SNMP Group String for WAE** window appears. The "SNMP Group Settings" table describes the fields in this window.

Table 129: SNMP Group Settings

GUI Parameter	Function
Name	Name of the SNMP group. You can enter a maximum of 64 characters. This is a required field.
Sec Model	Security model for the group. Choose one of the following options from the drop-down list: • **v1**: Version 1 security model (SNMP Version 1 [noAuthNoPriv]). • **v2c**: Version 2c security model (SNMP Version 2 [noAuthNoPriv]). • **v3-auth**: User security level SNMP Version 3 AuthNoPriv. • **v3-noauth**: User security level SNMP Version 3 noAuthNoPriv. • **v3-priv**: User security level SNMP Version 3 AuthPriv. **Note** A group defined with the SNMPv1 or SNMPv2c security model should not be associated with SNMP users; they should only be associated with the community strings.
Read View	Name of the view (a maximum of 64 characters) that enables you only to view the contents of the agent. By default, no view is defined. In order to provide read access to users of the group, a view must be specified. For information on creating SNMP views, see Creating SNMP Views, on page 691.

GUI Parameter	Function
Write View	Name of the view (a maximum of 64 characters) that enables you to enter data and configure the contents of the agent. By default, no view is defined. For information on creating SNMP views, see Creating SNMP Views, on page 691.
Notify View	Name of the view (a maximum of 64 characters) that enables you to specify a notify, inform, or trap. By default, no view is defined. For information on creating SNMP views, see Creating SNMP Views, on page 691.

Step 4 In the appropriate fields, enter the SNMP group configuration name, the security model, and the names of the read, write, and notify views.

Step 5 Click **Submit**.

Step 6 Create SNMP users that belong to this new group as described in the section that follows.

To create an SNMP group from the CLI, run the **snmp-server group** global configuration command.

Creating an SNMP User

Before you begin

Users are listed in the order in which they have been created. The maximum number of users that can be created is ten.

Procedure

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

Step 2 Choose **Configure** > **Monitoring** > **SNMP** > **User**. A list of SNMP users for the device or device group appears.

Step 3 In the taskbar, click the **Create New SNMP User** icon.

The **Creating New SNMP User** window appears. The "SNMP User Settings" table describes the fields in this window.

Table 130: SNMP User Settings

GUI Parameter	Function
Name	String representing the name of the user (32 characters maximum) who can access the device or device group. This is a required field.
Group	Name of the group (64 characters maximum) to which the user belongs. This is a required field.

GUI Parameter	Function
Remote SNMP ID	Globally unique identifier for a remote SNMP entity (10 to 64 characters). To send an SNMPv3 message to the WAE, at least one user with a remote SNMP ID must be configured on the WAE. The SNMP ID must be entered in octet string format. Only hexadecimal characters and the colon (:) are allowed in this field. If any colons appear in the entered string, they are removed when the page is submitted.
Authentication Algorithm	Authentication algorithm that ensures the integrity of SNMP packets during transmission. Choose one of the following three options from the drop-down list: • **No-auth**: Requires no security mechanism to be turned on for SNMP packets. • **MD5**: Provides authentication based on the hash-based Message Authentication Code Message Digest 5 (HMAC-MD5) algorithm. • **SHA**: Provides authentication based on the hash-based Message Authentication Code Secure Hash (HMAC-SHA) algorithm.
Authentication Password	Alphanumeric string (256 characters maximum) that configures the user authentication (HMAC-MD5 or HMAC-SHA) password. The number of characters is adjusted to fit the display area if it exceeds the limit for display. The following special characters are not supported: space, backwards single quote (\`), single quote ('), double quote ("), pipe (|), or question mark (?). This field is optional if the **no-auth** option is chosen for the authentication algorithm. Otherwise, this field must contain a value.
Confirmation Password	Authentication password for confirmation. The reentered password must be the same as the one entered in the previous field.
Private Password	Alphanumeric string (256 characters maximum) that configures the authentication (HMAC-MD5 or HMAC-SHA) parameters to enable the SNMP agent to receive packets from the SNMP host. The number of characters is adjusted to fit the display area if it exceeds the limit for display. The following special characters are not supported: space, backwards single quote (\`), double quote ("), pipe (|), or question mark (?). **Note** For SNMPv3 users using Cisco WAAS Software Version 6.x and later, the private password must be a minimum of 8 alphanumeric characters and a maximum of 256 characters.
Confirmation Password	Private password for confirmation. The reentered password must be the same as the one entered in the previous field.

Step 4 In the appropriate fields, enter the username, the group to which the user belongs, the engine identity of the remote entity to which the user belongs, the authentication algorithm used to protect SNMP traffic from tampering, the user authentication parameters, and the authentication parameters for the packet.

Step 5 Click **Submit**.

What to do next

To create an SNMP user from the CLI, run the **snmp-server user** global configuration command.

Additionally, if you want to set up a monitor user to monitor the configured triggers, you can select it from the **Monitor User Settings** drop-down box. Any SNMP V3 user can be configured as a Monitor User. All the SNMP users created with a group having V3 authentication other than v3-private are eligible to be a Monitor User. A monitor user cannot be deleted, while being in that role. Similarly the corresponding monitor user group also cannot be deleted when a monitor user is configured with that group.

To create a monitor user from the CLI, run the **snmp-server monitor user** global configuration command.

Configuring SNMP Asset Tag Settings

Procedure

Step 1 To configure SNMP asset tag settings, which create values in the CISCO-ENTITY-ASSET-MIB: From the Cisco WAAS Central Manager menu, choose **Devices >** *device-name* or **Device Groups >** *device-group-name*.

Step 2 Choose **Configure** > **Monitoring** > **SNMP** > **Asset Tag**.

The **SNMP Asset Tag Settings** window appears.

Step 3 In the **Asset Tag Name** field, enter a name for the asset tag.

Step 4 Click **Submit**.

To configure SNMP asset tag settings from the CLI, run the **asset tag** global configuration command.

Configuring SNMP Contact Settings

Procedure

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

Step 2 Choose **Configure** > **Monitoring** > **SNMP** > **Contact Information.**

The **SNMP Contact Settings** window appears.

Step 3 Enter a contact name and location in the provided fields.

Step 4 Click **Submit**.

To configure SNMP contact settings from the CLI, run the **snmp-server contact** global configuration command.

Configuring SNMP Trap Source Settings

Procedure

Step 1 From the Cisco WAAS Central Manager menu, choose **Devices >** *device-name*. This setting is not supported from device groups.

Step 2 Choose **Configure > Monitoring > SNMP > Trap Source**.

The **SNMP Trap Source Settings** window appears.

Step 3 From the **Trap Source** drop-down list, choose the interface to be used as the trap source. From the available physical, standby, and port-channel interfaces, only those with IP addresses are shown in the list. For Cisco vWAAS devices, virtual interfaces with assigned IP addresses are shown in the list.

Note An interface assigned as a trap source cannot be removed until it is unassigned as a trap source.

Step 4 Click **Submit**.

To configure SNMP trap source settings from the CLI, run the **snmp-server trap-source** global configuration command.

CHAPTER 18

Predefined Application Policies

Predefined Optimization Policy

The Cisco WAAS software includes over 200 predefined optimization policy rules that help your WAAS system classify and optimize some of the most common traffic on your network. The "Predefined Traffic Policy Rules" table lists the predefined applications and class maps that Cisco WAAS will either optimize or pass through based on the policy rules that are provided with the system.

Before you create an optimization policy, we recommend that you review the predefined policy rules and modify them as appropriate. Often, you can more easily modify an existing policy rule than create a new one.

When reviewing the "Predefined Traffic Policy Rules" table, note the following information:

- The subheadings represent the application names, and the associated class maps are listed under these subheadings. For example, Authentication is a type of application and Kerberos is a class map for that application.
- Applications and class maps with the word (*monitored*) next to them are monitored by the Cisco WAAS Central Manager, which can monitor statistics for up to 25 applications and 25 class maps at a time. To view statistics for one of the unmonitored applications, use one of the following methods:
  - Use the Cisco WAAS CLI, which can display statistics for all applications and class maps on a WAAS device. For more information, see the Cisco Wide Area Application Services Command Reference.
  - Modify the application or class map settings so the Cisco WAAS Central Manager GUI displays statistics for the desired application or class map. For more information, see the chapter Configuring Application Acceleration, on page 371.
- Cisco WAAS Express devices have similar default policy rules but provide application acceleration only for HTTP, SSL, and SMB traffic. Where a different application accelerator is listed in Table A-1 , it is not part of the WAAS Action for a Cisco WAAS Express device.

The Cisco WAAS software uses the following optimization technologies based on the type of traffic that it encounters:

- TFO (transport flow optimization): A collection of optimization technologies such as automatic windows scaling, increased buffering, and selective acknowledgment that optimize all TCP traffic over your network.
- DRE (data redundancy elimination): compression technology that reduces the size of transmitted data by removing redundant information before sending the shortened data stream over the WAN. DRE operates on significantly larger streams and maintains a much larger compression history than LZ compression. DRE can use bidirectional, unidirectional, or adaptive caching. Unless noted in Table A-1 , DRE caching is bidirectional.
- LZ (compression): Another compression technology that operates on smaller data streams and keeps limited compression history compared to DRE.
- Application accelerator: A collection of individual application accelerators for the following traffic types: EPM, HTTP, ICA, MAPI, NFS, SSL, and streaming video. (Some application accelerators are not available on Cisco WAAS Express devices.)

Table 131: Predefined Traffic Policy Rules

Application/Class Map	Cisco WAAS Action	Destination Ports
class-default (*monitored*)	LZ+TFO+DRE-adaptive	All ports not included in other class maps
Authentication		
apple-sasl	Passthrough	3659
auth	Passthrough	113
Kerberos	Passthrough	88, 888, 2053
kerberos-adm (*monitored*)	Passthrough	749
klogin	Passthrough	543
kpasswd	Passthrough	464
kshell	Passthrough	544
TACACS	Passthrough	49
tell	Passthrough	754
Backup*(monitored)*		
Amanda	TFO	10080
backup-express	TFO	6123
CommVault	TFO	8400–8403
connected	TFO	16384
IBM-TSM	LZ+TFO+DRE-unidirectional	1500-1502
Legato-NetWorker	TFO	7937, 7938, 7939

Application/Class Map	Cisco WAAS Action	Destination Ports
Legato-RepliStor	TFO	7144, 7145
Veritas-BackupExec (*monitored*)	TFO	1125, 3527, 6101, 6102, 6106
Veritas-NetBackup	TFO	13720, 13721, 13782, 13785
CAD		
PDMWorks	LZ+TFO+DRE	30000, 40000
Call-Management		
Cisco-CallManager	Passthrough	2443, 2748
cisco-q931-backhaul	Passthrough	2428
cisco-sccp	Passthrough	2000–2002
h323hostcall	Passthrough	1720
h323hostcallsc	Passthrough	1300
mgcp-callagent	Passthrough	2727
mgcp-gateway	Passthrough	2427
sip	Passthrough	5060
sip-tls	Passthrough	5061
VoIP-Control	Passthrough	1718, 1719, 11000–11999
Citrix		
Citrix (*monitored*)	TFO+ ICA accelerator	1494, 2598, or a dynamic port associated with the **citrix** protocol match
Conferencing		
cuseeme	Passthrough	7640, 7642, 7648, 7649
ezMeeting	Passthrough	10101–10103, 26260, 26261
MS-NetMeeting (*monitored*)	Passthrough	522, 1503, 1731
proshare	Passthrough	5713–5717
PSOM-MTLS	Passthrough	8057
VocalTec	Passthrough	1490, 6670, 25793, 22555
Console		
cmd	Passthrough	514

Application/Class Map	Cisco WAAS Action	Destination Ports
exec	Passthrough	512
login	Passthrough	513
sshell	Passthrough	614
Telnet	Passthrough	23, 107
Telnets	Passthrough	992
Content-Management *(monitored)*		
dmdocbroker	LZ+TFO+DRE	1489
Filenet	LZ+TFO+DRE	32768–32774
Directory-Services *(monitored)*		
LDAP	LZ+TFO+DRE-unidirectional	389, 8404
ldaps	Passthrough	636
msft-gc	LZ+TFO+DRE-unidirectional	3268
msft-gc-ssl	Passthrough	3269
Email-and-Messaging *(monitored)*		
ccmail	LZ+TFO+DRE	3264
groupwise	LZ+TFO+DRE	1677, 2800, 3800, 7100, 7101, 7180, 7181, 7205, 9850
imap	LZ+TFO+DRE	143
imap3	LZ+TFO+DRE	220
imaps	TFO	993
iso-tsap	LZ+TFO+DRE	102
lotusnote	LZ+TFO+DRE	1352
MAPI[1] (*monitored*)	LZ+TFO+DRE+ MAPI accelerator	UUID:a4f1db00-ca47-1067-b31f-00dd010662da
MDaemon	LZ+TFO+DRE	3000, 3001
MS-Exchange-Directory-NSPI1	Passthrough	UUID:f5cc5a18-4264-101a-8c59-08002b2f8426
MS-Exchange-Directory-RFR1	Passthrough	UUID:1544f5e0-613c-11d1-93df-00c04fd7bd09
NNTP (*monitored*)	LZ+TFO+DRE	119
nntps (*monitored*)	TFO	563

Application/Class Map	Cisco WAAS Action	Destination Ports
openmail	LZ+TFO+DRE	5755, 5757, 5766, 5767, 5768, 5729
pcmail-srv	LZ+TFO+DRE	158
pop3	LZ+TFO+DRE	110
pop3s	LZ+TFO+DRE	995
QMTP	TFO	209
smtp (*monitored*)	LZ+TFO+DRE	25
smtps	TFO	465
Enterprise-Applications *(monitored)*		
MS-GROOVE	TFO	2492
SAP (*monitored*)	LZ+TFO+DRE	3200–3204, 3206–3219, 3221–3224, 3226–325 3261–3263, 3265–3267, 3270–3282, 3284–330 3307–3351, 3353–3388, 3390–3399, 3600–365 3662–3699
Siebel	LZ+TFO+DRE	2320, 2321, 8448
File-System *(monitored)*		
afpovertcp	LZ+TFO+DRE	548
afs3	LZ+TFO+DRE	7000–7009
ncp	LZ+TFO+DRE	524
NFS	LZ+TFO+DRE+ NFS accelerator	2049
sunrpc	Passthrough	111
File-Transfer *(monitored)*		
BFTP	LZ+TFO+DRE	152
ftp (*monitored*)	Passthrough	21
ftp-data[2]	LZ+TFO+DRE	20 (source port)
ftps	TFO	990
ftps-data2	Passthrough	989 (source port)
sftp	LZ+TFO+DRE	115
TFTP	LZ+TFO+DRE	69
TFTPS	TFO	3713

Application/Class Map	Cisco WAAS Action	Destination Ports
Instant Messaging		
AOL	Passthrough	5190–5193
Apple-iChat	Passthrough	5297, 5298
ircs	Passthrough	994
ircu	Passthrough	531, 6660–6665, 6667–6669
msnp	Passthrough	1863, 6891–6900
sametime	Passthrough	1533
talk	Passthrough	517
xmpp-client	Passthrough	5222
xmpp-server	Passthrough	5269
Yahoo-Messenger	Passthrough	5000, 5001, 5050, 5100
Name Services		
DNS	Passthrough	53
isns	Passthrough	3205
nameserver	Passthrough	42
netbios	Passthrough	137
svrloc	Passthrough	427
WINS (*monitored*)	Passthrough	1512
Other		
Basic-TCP-services	Passthrough	1–19
BGP	Passthrough	179
corba-iiop-ssl	Passthrough	684
epmap (*monitored*)	TFO, EPM accelerator	135
msmq	LZ+TFO+DRE	1801, 2101, 2103, 2105
NTP	Passthrough	123

Application/Class Map	Cisco WAAS Action	Destination Ports
Other-Secure	Passthrough	261, 448, 695, 994, 2252, 2478, 2479, 2482, 2484, 2679, 2762, 2998, 3077, 3078, 3183, 319 3220, 3410, 3424, 3471, 3496, 3509, 3529, 353 3660, 3661, 3747, 3864, 3885, 3896, 3897, 399 4031, 5007, 7674, 9802, 12109
ssc-agent	LZ+TFO+DRE	2847, 2848, 2967, 2968, 38037, 38292
Unclassified	LZ+TFO+DRE	
P2P *(monitored)*		
BitTorrent	Passthrough	6881–6889, 6969
eDonkey	Passthrough	4661, 4662
Gnutella	Passthrough	5634, 6346–6349, 6355
Grouper	Passthrough	8038
HotLine	Passthrough	5500–5503
Kazaa	Passthrough	1214
Laplink-ShareDirect	Passthrough	2705
Napster	Passthrough	6666, 6677, 6688, 6700, 7777, 8875
Qnext	Passthrough	44, 5555
SoulSeek	Passthrough	2234, 5534
WASTE	Passthrough	1337
WinMX	Passthrough	6699
Printing *(monitored)*		
hp-pdl-datastr	LZ+TFO+DRE	9100
IPP	LZ+TFO+DRE	631
printer	LZ+TFO+DRE	515
print-srv	LZ+TFO+DRE	170
xprint-server	LZ+TFO+DRE	8100
Remote-Desktop *(monitored)*		
Altiris-CarbonCopy	Passthrough	1680
citrixadmin	LZ+TFO+DRE-unidirectional	2513

Application/Class Map	Cisco WAAS Action	Destination Ports
citrixima	LZ+TFO+DRE-unidirectional	2512
citriximaclient (*monitored*)	LZ+TFO+DRE	2598
ControlIT	TFO	799
Danware-NetOp	TFO	6502
ica (*monitored*)	LZ+TFO+DRE	1494
laplink	LZ+TFO+DRE-unidirectional	1547
Laplink-surfup-HTTPS	TFO	1184
ms-wbt-server (*monitored*)	TFO	3389
net-assistant	Passthrough	3283
netrjs-3	TFO	73
pcanywheredata	TFO	5631, 5632, 65301
radmin-port	TFO	4899
Remote-Anything (*monitored*)	TFO	3999, 4000
timbuktu	TFO	407
timbuktu-srv	TFO	1417–1420
Vmware-VMConsole	TFO	902
VNC (*monitored*)	TFO	5800–5809, 5900–5909
x11	TFO	6000–6063
Replication *(monitored)*		
Double-Take	LZ+TFO+DRE-unidirectional	1100, 1105
EMC-Celerra-Replicator	LZ+TFO+DRE-adaptive	8888
MS-AD-Replication1	LZ+TFO+DRE	UUID:e3514235-4b06-11d1-ab04-00c04fc2dcd2
ms-content-repl-srv	TFO	507, 560
MS-FRS1	LZ+TFO+DRE	UUID:f5cc59b4-4264-101a-8c59-08002b2f8426
netapp-snapmirror	LZ+TFO+DRE-adaptive	10565-10569
pcsync-http	LZ+TFO+DRE	8444
pcsync-https	TFO	8443
rrac	TFO	5678

Application/Class Map	Cisco WAAS Action	Destination Ports
Rsync (*monitored*)	LZ+TFO+DRE-unidirectional	873
SQL *(monitored)*		
gds_db	LZ+TFO+DRE	3050
IBM-DB2	LZ+TFO+DRE	523
intersys-cache	LZ+TFO+DRE	1972
ms-olap4	TFO	2383
ms-sql-m	LZ+TFO+DRE	1434
MS-SQL-RPC1	LZ+TFO+DRE	UUID:3f99b900-4d87-101b-99b7-aa0004007f0
ms-sql-s (*monitored*)	LZ+TFO+DRE	1433
MySQL	LZ+TFO+DRE	3306
Oracle	LZ+TFO+DRE	66
orasrv	LZ+TFO+DRE	1521, 1525
Pervasive-SQL	LZ+TFO+DRE	1583
PostgreSQL	LZ+TFO+DRE	5432
sqlexec	LZ+TFO+DRE	9088, 9089
sql-net	LZ+TFO+DRE	150
sqlserv	LZ+TFO+DRE	118
sqlsrv	LZ+TFO+DRE	156
ssql	LZ+TFO+DRE	3352
sybase-sqlany	LZ+TFO+DRE	1498, 2439, 2638, 3968
UniSQL	LZ+TFO+DRE	1978, 1979
SSH		
SSH (*monitored*)	TFO	22
SSL *(monitored)*		
HTTPS (*monitored*)	TFO	443
Storage *(monitored)*		
EMC-SRDFA-IP	LZ+TFO+DRE	1748
FCIP	LZ+TFO	3225

Application/Class Map	Cisco WAAS Action	Destination Ports
iFCP	LZ+TFO+DRE	3420
iscsi	LZ+TFO+DRE	3260
Streaming *(monitored)*		
Liquid-Audio	LZ+TFO+DRE-unidirectional	18888
ms-streaming (*monitored*)	LZ+TFO+DRE-unidirectional	1755
RTSP (*monitored*)	LZ+TFO+DRE-unidirectional	554, 8554
Systems-Management *(monitored)*		
BMC-Patrol	Passthrough	6161, 6162, 6767, 6768, 8160, 8161, 10128
eTrust-policy-Compliance	TFO	1267
flowmonitor	LZ+TFO	7878
HP-OpenView	Passthrough	7426–7431, 7501, 7510
LANDesk	LZ+TFO+DRE	9535, 9593–9595
NetIQ	Passthrough	2220, 2735, 10113–10116
Netopia-netOctopus	Passthrough	1917, 1921
netviewdm	Passthrough	729–731
novadigm	LZ+TFO+DRE	3460, 3461, 3464
novell-zen	LZ+TFO+DRE	1761–1763, 2037, 2544, 8039
objcall	LZ+TFO+DRE	94, 627, 1965, 1580, 1581
WBEM	Passthrough	5987–5990
Version-Management *(monitored)*		
Clearcase	LZ+TFO+DRE	371
cvspserver	LZ+TFO+DRE	2401
VPN		
L2TP	TFO	1701
OpenVPN	TFO	1194
PPTP	TFO	1723
Web *(monitored)*		
HTTP (*monitored*)	LZ+TFO+DRE+ HTTP accelerator	80, 3128, 8000, 8080, 8088

Application/Class Map	Cisco WAAS Action	Destination Ports
soap-http	LZ+TFO+DRE-adaptive	7627

[1] These classifiers use the EPM service in WAAS to accelerate traffic. EPM-based applications do not have predefined ports so the application's UUID must be used to identify the traffic.
[2] These classifiers identify the source port instead of the destination port.

CHAPTER 19

Transaction Log Format

Transaction Log Format

You can use the transaction logging feature to log individual TCP transactions for a Cisco WAAS device. For information on configuring transaction logging, see the Configuring Transaction Logging in the chapter "Troubleshooting Your Cisco WAAS Network."

TFO transaction logs are kept on the local disk in the local/local1/logs/working.log directory.

There are several kinds of transaction log messages, which have different templates:

Optimized Flow Start message

Time_Stamp :Conn_ID :Src_IP :Src_Port :Dst_IP :Dst_Port :OT :Log_type :Conn_type :Peer_ID :App_map_name :App_name :App_classifier_name :TFO_cfgd_policy :TFO_drvd_policy :TFO_peer_policy :TFO_neg_policy :TFO_applied_policy :TFO_reject_reason :AO_cfgd_policy :AO_drvd_policy :AO_neg_policy :AO_reject_reason :SSL_reject_reason :DSCP :Link_rtt

Optimized Flow End message

Time_Stamp :Conn_ID :Src_IP :Src_Port :Dst_IP :Dst_Port :OT :Log_type :Conn_type :AO_neg_policy :Original_bytes_read :Original_bytes_written :Optimized_bytes_read :Optimized_bytes_written

Pass Through Flow message

Time_Stamp :Src_IP :Src_Port :Dst_IP :Dst_Port :BP :Bypass_Reason :TFO_cfgd_policy :TFO_drvd_policy :TFO_peer_policy :TFO_reject_reason :AO_cfgd_policy :AO_drvd_policy :AO_reject_reason

Optimized Flow TFO End message

Time_Stamp :Conn_ID :Src_IP :Src_Port :Dst_IP :Dst_Port :SODRE :END :Original_bytes_read :Original_bytes_written :Optimized_bytes_read :Optimized_bytes_written :Conn_close_state

System Restart message

Time_Stamp :0 :0 :0 :0 :0 :RESTART

The following table describes the fields found in the transaction log messages.

Table 132: Transaction Log Field Descriptions

Field	Description
Time_Stamp	Time stamp indicating when the log message was generated.
Conn_ID	A unique identifier for the connection.
Src_IP, Src_Port	Source IP address and port number for the connection.
Dst_IP, Dst_Port	Destination IP address and port number for connection.
OT	Indicates an optimized connection.
BP	Indicates a pass-through connection.
SODRE	Indicates a log message generated by TFO.
Log_type	START or END indicates the start or end of the flow.
Conn_type	Type of connection: INTERNAL CLIENT–locally initiated connection from the WAE, EXTERNAL CLIENT–WAE acting as branch device for the connection,INTERNAL SERVER–locally terminated connection at the WAE, EXTERNAL SERVER–WAE acting as data center device for the connection.
Peer_ID	Device ID of the peer WAE.
App_map_name	Map name.
App_classifier_name	Classifier name.
App_name	Application name.
TFO_cfgd_policy	The TFO configured policy on the local device.
TFO_drvd_policy	The TFO derived policy on the local device based on the configured and dynamic conditions. This policy is used to negotiate with the peer WAE.
TFO_peer_policy	The TFO derived policy on the peer that is sent to the local device.
TFO_neg_policy	The TFO negotiated policy, which is the lowest common policy between the derived and peer policies.
TFO_applied_policy	The final policy applied to the connection. After the connection has been established, policy changes may be made to the connection based on the data on the connection, thus the applied policy can differ from the negotiated policy.
TFO_reject_reason	Indicates the reason for a rejected connection. “None” indicates the reject reason is not set.
AO_cfgd_policy	The application accelerator configured on the local device. This is derived from the accelerator configured in the corresponding policy.
AO_drvd_policy	The application accelerator derived policy on the local device.

Field	Description
AO_neg_policy	The application accelerator negotiated policy, which is the lowest common policy between the derived and peer policies.
AO_reject_reason	Indicates the reason an application accelerator rejected the connection. “None” indicates the reject reason is not set.
SSL_reject_reason	Indicates the reason the SSL accelerator rejected the connection. “None” indicates the reject reason is not set.
DSCP	Differentiated Services Code Point value set on the outgoing connection.
Link_rtt	Link round trip time in milliseconds.
Original_bytes_read	Bytes read on the original side of the connection.
Original_bytes_written	Bytes written on the original side of the connection.
Optimized_bytes_read	Bytes read on the optimized side of the connection.
Optimized_bytes_written	Bytes written on the optimized side of the connection.
RESTART	Indicates that the WAE was reloaded and the transaction log process was started.

Here are some examples of transaction log messages:

Fully Optimized on both sides (with SSL rejection)

```
Fri Jan 31 03:15:41 2020 :43 :2.57.223.130 :4808 :2.57.223.2 :443 :OT :START :EXTERNAL CLIENT
:00.14.5e.95.4c.85 :basic :SSL :HTTPS :F :(TFO) (TFO) (TFO) (TFO) (TFO) :<None> :(None) (None) (None)
:<None> :<Keepalive Timeout> :0 :0 Fri Jan 31 03:15:41 2020 :43 :2.57.223.130 :4808 :2.57.223.2 :443
:SODRE :END :0 :0 :0 :0 :0 Fri Jan 31 03:15:41 2020 :43 :2.57.223.130 :4808 :2.57.223.2 :443 :OT :END
:EXTERNAL CLIENT :(None) :284 :806 :806 :28
```

Fully Optimized on both sides

```
Mon Feb 3 14:31:21 2020 :16 :2.75.52.131 :4374 :2.75.52.3 :80 :OT :START :EXTERNAL CLIENT
:00.14.5e.83.8c.cf :basic :Web :HTTP :F :(DRE,LZ,TFO) (DRE,LZ,TFO) (DRE,LZ,TFO) (DRE,LZ,TFO)
(DRE,LZ,TFO) :<None> :(HTTP) (HTTP) (HTTP) :<None> :<None> :0 :0 Mon Feb 3 14:31:26 2020 :16
:2.75.52.131 :4374 :2.75.52.3 :80 :SODRE :END :370 :173 :299 :429 :0 Mon Feb 3 14:31:26 2020 :16
:2.75.52.131 :4374 :2.75.52.3 :80 :OT :END :EXTERNAL CLIENT :(HTTP) :0 :0 :299 :429
```

Optimized with only DRE enabled

```
Mon Feb 3 14:48:31 2020 :27 :2.75.52.131 :4389 :2.75.52.2 :80 :OT :START :EXTERNAL CLIENT
:00.14.5e.83.8c.cf :basic :Web :HTTP :F :(DRE,TFO) (DRE,TFO) (DRE,LZ,TFO) (DRE,TFO) (DRE,TFO)
:<None> :(HTTP) (HTTP) (HTTP) :<None> :<None> :0 :0 Mon Feb 3 14:48:36 2020 :27 :2.75.52.131 :4389
:2.75.52.2 :80 :SODRE :END :246 :468 :636 :405 :0 Mon Feb 3 14:48:36 2020 :27 :2.75.52.131 :4389
:2.75.52.2 :80 :OT :END :EXTERNAL CLIENT :(HTTP) :0 :0 :636 :405
```

Optimized with only LZ enabled

```
Mon Feb 3 14:39:12 2020 :20 :2.75.52.131 :4379 :2.75.52.3 :80 :OT :START :EXTERNAL CLIENT
:00.14.5e.83.8c.cf :basic :Web :HTTP :F :(LZ,TFO) (LZ,TFO) (DRE,LZ,TFO) (LZ,TFO) (LZ,TFO) :<None>
:(HTTP) (HTTP) (HTTP) :<None> :<None> :0 :0 Mon Feb 3 14:39:17 2020 :20 :2.75.52.131 :4379 :2.75.52.3
```

:80 :SODRE :END :370 :173 :219 :295 :0 Mon Feb 3 14:39:17 2020 :20 :2.75.52.131 :4379 :2.75.52.3 :80 :OT :END :EXTERNAL CLIENT :(HTTP) :0 :0 :219 :295

Optimized with both DRE and LZ disabled

Mon Feb 3 14:49:36 2020 :28 :2.75.52.131 :4390 :2.75.52.2 :80 :OT :START :EXTERNAL CLIENT :00.14.5e.83.8c.cf :basic :Web :HTTP :F :(TFO) (TFO) (DRE,LZ,TFO) (TFO) (TFO) :<None> :(HTTP) (HTTP) (HTTP) :<None> :<None> :0 :0 Mon Feb 3 14:49:41 2020 :28 :2.75.52.131 :4390 :2.75.52.2 :80 :OT :END :EXTERNAL CLIENT :(HTTP) :0 :0 :468 :246

Pass-Through Connection

Thu Jul 25 03:09:34 2019 :2.75.52.130 :40027 :2.75.52.2 :80 :BP :GLB_CFG :(DRE,LZ,TFO) (None) (None) :<Global Config> :(HTTP) (None) :<Global Config>

System Restart

Sun Oct 20 17:46:32 2019 :0 :0 : 0 :0 :0 :RESTART