



Introduction to Cisco WAAS

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



Note

Throughout this chapter, the term WAAS device is used to refer collectively to the WAAS Central Managers and WAEs in your network. The term WAE refers to WAE and WAVE appliances, SM-SRE modules running WAAS, and vWAAS instances.

This chapter contains the following sections:

- [About Cisco WAAS, page 1-1](#)
- [Key Services of Cisco WAAS, page 1-4](#)
- [Overview of the WAAS Interfaces, page 1-10](#)
- [Benefits of Cisco WAAS, page 1-20](#)

About Cisco WAAS

The WAAS system consists of a set of devices called wide area application engines (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.

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

You can deploy WAAS in the new AppNav model or in the traditional model without using AppNav Controllers.

You use the WAAS Central Manager GUI to centrally configure and monitor the WAEs and optimization policies in your network. You can also use the WAAS Central Manager GUI to create new optimization policy rules so that the WAAS system can optimize 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.
- Virtualize print and other local services to branch office users. Cisco WAAS allows you to configure a WAE with Windows in a virtual blade so that you do not need to deploy a dedicated system to provide local services such as Print Services, Active Directory Services, DNS, and DHCP services.
- 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 WAAS Express device, which is a Cisco router with WAAS Express functionality enabled, can interoperate with other WAAS devices. A WAAS Express device provides basic WAN optimization and some application optimization but no virtualization. For more information on WAAS Express, see [Configuring WAAS Express](#).

An AppNav-XE device, which is a Cisco router or virtual Cloud Services router with virtual AppNav functionality, can interoperate with other WAAS devices that are acting as WAAS nodes. An AppNav-XE device acts as an AppNav Controller that distributes traffic to other WAAS devices acting as WAAS nodes that optimize the traffic. An AppNav-XE device cannot interoperate with other AppNav Controller hardware appliances, however. For more information on AppNav-XE, see the AppNav-XE documentation. For more information on AppNav, see [Chapter 4, “Configuring AppNav.”](#)

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

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

This section contains the following topics:

- [Cisco WAAS Overcomes Common WAN Challenges, page 1-2](#)
- [Traffic Optimization Process, page 1-3](#)

Cisco WAAS Overcomes Common WAN Challenges

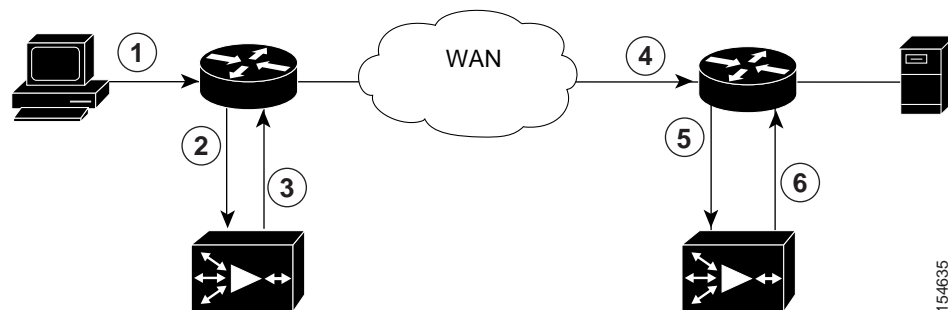
[Table 1-1](#) describes how Cisco WAAS uses a combination of TCP optimization techniques and application acceleration features to overcome the most common challenges associated with transporting traffic over a WAN.

Table 1-1 Cisco WAAS Solution

WAN Issue	WAAS Solution
High network latency	Intelligent protocol adapters reduce the number of roundtrip 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 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 WAAS overcomes the issues associated with high packet loss and protects communicating end points from the state of the WAN.

Traffic Optimization Process

Figure 1-1 shows the process that Cisco WAAS follows to optimize application traffic.

Figure 1-1 Traffic Optimization Process

The following steps describe how your 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 WAAS network uses WCCP or PBR to intercept the client request, or if deployed on an inline WAE, WAAS can intercept the request directly using inline mode. For more information on inline mode, see the [“Using Inline Mode Interception”](#) section on page 5-43.
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 that 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, then an optimized connection will not be 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 an AppNav deployment, see [Chapter 4, “Configuring AppNav.”](#)

- 6. 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 the traffic.
- The intercepted traffic matches an optimization or AppNav policy rule that specifies to pass the traffic 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.

Key Services of Cisco WAAS

Cisco WAAS contains the following services that help optimize traffic over your wide area network:

- [TFO Optimization, page 1-4](#)
- [Compression, page 1-6](#)
- [Application-Specific Acceleration, page 1-7](#)
- [File Services for Desktop Applications, page 1-8](#)
- [WAAS Print Services, page 1-9](#)
- [Virtualization, page 1-10](#)

**Note**

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

TFO Optimization

Cisco WAAS uses a variety of transport flow optimization (TFO) features to optimize TCP traffic intercepted by the 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:

- [Windows Scaling, page 1-5](#)
- [TCP Initial Window Size Maximization, page 1-5](#)
- [Increased Buffering, page 1-5](#)
- [Selective Acknowledgment, page 1-5](#)
- [BIC TCP, page 1-6](#)

Windows Scaling

Windows 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.

Windows 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 Windows scaling, refer to RFC 1323.

TCP Initial Window Size Maximization

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 more aggressively pull data from branch office clients and remote servers. This increased buffer helps the two WAEs participating in the connection keep the link between them full, increasing link utilization.

Selective Acknowledgment

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

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

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

For more information about SACK, see RFC 2018.

BIC 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

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

- Data Redundancy Elimination (DRE)
- 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, WAAS compression can 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, 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 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, WAAS uses a FIFO algorithm (first in, first out) to discard old data and make room for new.

LZ compression operates on smaller data streams and keeps 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

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 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 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.
- CIFS caching—Allows a WAAS device to reply to client requests using locally cached data instead of retrieving this data from remote file and application servers.
- Preposition—Allows a WAAS device to prefetch resource data and metadata in anticipation of a future client request. (Only the CIFS accelerator supports prepositioning.)

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

In a typical Common Internet File System (CIFS) application use case, the client sends a large number of synchronous requests that require the client to wait for a response before sending the next request. Compressing the data over the WAN is not sufficient for acceptable response time.

For example, when you open a 5 MB Word document, about 700 CIFS requests (550 read requests plus 150 other requests) are produced. If all these requests are sent over a 100 ms round-trip WAN, the response time is at least 70 seconds (700 x 0.1 seconds).

WAAS application acceleration minimizes the synchronous effect of the CIFS protocol, which reduces application response time. Each WAAS device uses optimization policies to match specific types of the traffic to an application and to determine whether that application traffic should be optimized and accelerated.

The following WAAS application accelerators are available:

- SMB—Accelerates CIFS traffic exchanged with a remote file server. Supports the SMB 1.0, 2.0, and 2.1 protocols for CIFS traffic and signed SMB traffic. For more information, see the [“File Services for Desktop Applications” section on page 1-8](#).
- CIFS—Accelerates CIFS traffic exchanged with a remote file server. Supports the SMB 1.0 protocol for CIFS traffic. For more information, see the [“File Services for Desktop Applications” section on page 1-8](#). The CIFS application accelerator is not available on ISR-WAAS devices.



Note The SMB and CIFS application accelerators both handle CIFS traffic but have slightly different features. You must choose one or the other to operate on WAAS peer devices because they cannot operate simultaneously on the same device and both peers must use the same accelerator.

- NFS—Accelerates Network File System (NFS) version 3 traffic exchanged with a remote file server. Secure NFS traffic is not accelerated.
- ICA—Accelerates Independent Computing Architecture (ICA) traffic that is used to access a virtual desktop infrastructure (VDI).
- HTTP—Accelerates HTTP and HTTPS traffic.

- **SSL**—Accelerates encrypted Secure Sockets Layer (SSL) and Transport Layer Security (TLS) traffic. The SSL accelerator provides traffic encryption and decryption within WAAS to enable end-to-end traffic optimization. The SSL accelerator also provides secure management of the encryption certificates and keys.
- **MAPI**—Accelerates Microsoft Outlook Exchange traffic that uses the Messaging Application Programming Interface (MAPI) protocol. Microsoft Outlook 2000–2010 clients are supported. Secure connections that use message authentication (signing) or encryption are accelerated. MAPI over HTTP is not accelerated.
- **Video**—Accelerates Windows Media live video broadcasts that use RTSP over TCP. The video accelerator automatically splits one source video stream from the WAN into multiple streams to serve multiple clients on the LAN. The video accelerator automatically causes a client requesting a UDP stream to do a protocol rollover to use TCP (if both the client and server allow TCP).
- **Windows Print**—Accelerates print traffic between clients and a Windows print server located in the data center. Signed Server Message Block (SMB) traffic is optimized by transport level optimizations (TFO, DRE, and LZ). The Windows print accelerator supports Windows 2000, Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 print servers. It supports clients running Windows 2000, Windows XP, Windows Vista, and Windows 7. The Windows Print accelerator operates only when the CIFS application accelerator is enabled.

**Note**

WAAS Express devices provide application acceleration for CIFS/SMB, HTTP, and SSL traffic.

To enable or disable application accelerators, see the [“Enabling and Disabling the Global Optimization Features” section on page 13-3](#).

You must enable the accelerator on both of the peer WAEs at either end of a WAN link for all application accelerators to operate.

File Services for Desktop Applications

The file services (SMB and CIFS accelerators) feature allows a WAE to more quickly fulfill a client’s requests instead of sending every request over the WAN to the file server. By fulfilling the 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 into data centers.

For more information, see [Chapter 12, “Configuring File Services.”](#)

**Note**

Legacy mode WAFS is no longer supported. Legacy WAFS users must migrate to the SMB or CIFS accelerators.

This section contains the following topics:

- [File Services Features, page 1-9](#)
- [Role of the Edge WAE, page 1-9](#)
- [Role of the Core WAE, page 1-9](#)

File Services Features

File Services include the following features:

- Data coherency and concurrency—Ensures data integrity across the WAAS system by managing the freshness of the data (coherency) and controlling the access to the data by multiple clients (concurrency).
- Automatic discovery—Allows you to use file services without having to register individual file servers in the WAAS Central Manager. With the automatic discovery feature, the WAAS device will automatically discover and connect to a new file server when a CIFS request is received.
- Prepositioning—Allows system administrators to proactively “push” frequently used files from the central file server into the cache of selected WAEs, which provides users with faster first-time file access, and makes more efficient use of available bandwidth. Prepositioning is supported only by the CIFS application accelerator.

Role of the Edge WAE

The Edge WAE is a client-side, file-caching device that serves client requests at remote sites and branch offices. The device is deployed at each branch office or remote campus, replacing file and print servers and giving local clients fast, near-LAN read and write access to a cached view of the centralized storage. By caching the data most likely to be used at these sites, Edge WAEs greatly reduce the number of requests and the volume of data that must be transferred over the WAN between the data center and the edge.

When requests for data that is not located in the cache are received, the Edge WAE encapsulates the original CIFS request using a TCP/IP-based protocol, compresses it, and sends it over the WAN to the Core WAE. Data returned from the data center is distributed by the Edge WAE to the end user who requested it.

Role of the Core WAE

The Core WAE is a server-side component that resides at the data center and connects directly to one or more file servers or network-attached storage (NAS). Core WAEs are placed between the file servers at the data center and the WAN connecting the data center to the enterprise’s remote sites and branch offices. Requests received from Edge WAEs over the WAN are translated by the Core WAE into its original file server protocol and forwarded to the appropriate file server. The data center Core WAEs can provide load balancing and failover support.

When the data is received from the file server, the Core WAE encapsulates and compresses it before sending it over the WAN back to the Edge WAE that requested it. Core WAEs can be arranged in logical clusters to provide scalability and automatic failover capabilities for high-availability environments.

WAAS Print Services

The WAAS software includes the following print services options:

- 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 CIFS application accelerator and Windows print acceleration be enabled. For more information, see the [“Enabling and Disabling the Global Optimization Features” section on page 13-3](#).

- Virtual blade based print server—Use this option when you want to deploy a local print server in the branch office but without installing separate print server hardware. You can install a Windows print server in a virtual blade on the branch WAE, which allows you to manage printing by using standard Windows print server functionality. For more information, see [Chapter 14, “Configuring Virtual Blades.”](#)



Note The legacy print services feature is no longer supported. Legacy print services users must migrate to another print services option.

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

Virtualization

The WAAS software allows you to configure a virtual blade, which allows you to add services running in their own operating environments to your WAAS system. For example, you could configure a virtual blade in a WAE device to run Windows services such as Print Services, Active Directory Services, DNS, and DHCP services.

A WAAS virtual blade provides an emulated hardware environment within your WAE device that acts as a generic computer. You can install an operating system and applications to work with your WAAS system and provide additional services for the users on your network. For more information, see [Chapter 14, “Configuring Virtual Blades.”](#)

Overview of the WAAS Interfaces

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

- [WAAS Central Manager GUI, page 1-10](#)
- [WAAS Central Manager Monitoring API, page 1-18](#)
- [WAE Device Manager GUI, page 1-18](#)
- [WAAS CLI, page 1-19](#)
- [WAAS CLI, page 1-19](#)

WAAS Central Manager GUI

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

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

- Configure system and network settings for an individual WAAS device, vWAAS device, WAAS Express device, device group, AppNav Controller, and AppNav Cluster.
- Create and edit optimization policies that determine the action that a WAAS device performs when it intercepts specific types of traffic.

- Create and edit AppNav policies that determine how AppNav Controllers distribute traffic to optimizing WAAS nodes.
- Configure file services and set up file preposition policies (preposition works only with the CIFS application accelerator).
- Create device groups that help you manage and configure multiple WAEs at the same time.
- View detailed reports about the optimized traffic in your WAAS network.

**Note**

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

This section contains the following topics:

- [Accessing the WAAS Central Manager GUI, page 1-11](#)
- [Components of the WAAS Central Manager GUI, page 1-12](#)
- [WAAS Central Manager Menus, page 1-15](#)
- [WAAS Central Manager Taskbar Icons, page 1-16](#)

Accessing the WAAS Central Manager GUI

To access the WAAS Central Manager GUI, 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 [Chapter 8, “Creating and Managing Administrator User Accounts and Groups.”](#)

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

**Note**

When using Internet Explorer to access the Central Manager GUI, you may see a “Choose a digital certificate” dialog. Click **Cancel** to proceed to the 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 Central Manager uses a self-signed certificate. Click on the link **Continue to this website (not recommended)**. You can permanently install the certificate to avoid this error in the future. To install the certificate in Internet Explorer 8, click the red **Certificate Error** button in the address bar and choose **View Certificates**. Click **Install Certificate**, then click **Next**. Select **Automatically select the certificate store based on the type of certificate** and click **Next**, click **Finish**, then click **Yes** on the security warning, click **OK** on the acknowledgement, and click **OK** on the Certificate dialog. The certificate installation procedure differs depending on the browser.

If you are using Internet Explorer to access the Central Manager GUI, we strongly recommend that you install the Google Chrome Frame plug-in to provide better performance. When you log into the 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 plugin, click the link to continue without installing Google Chrome Frame.

You can configure the WAAS Central Manager GUI 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 the [“Modifying the Default System Configuration Properties”](#) section on page 10-17.

**Note**

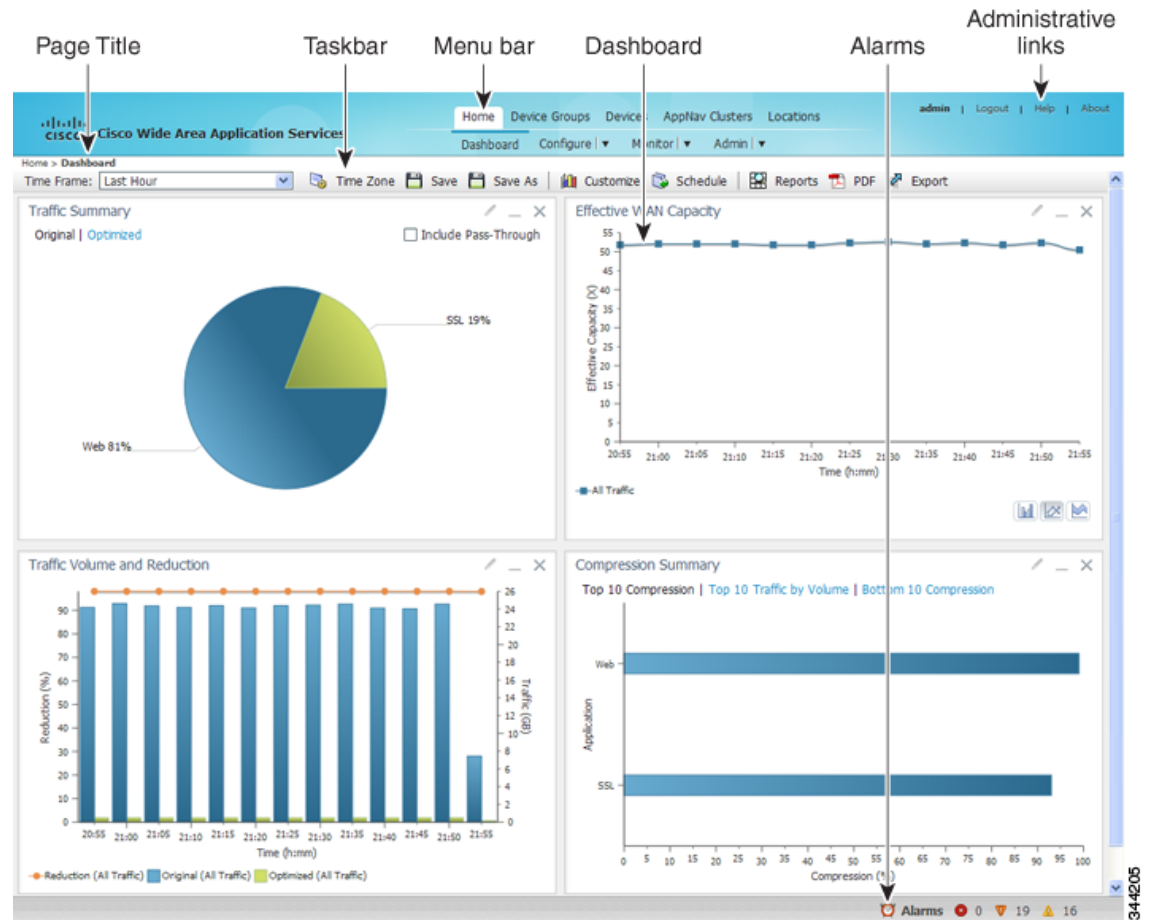
A user must log off the Central Manager to end a session. If a user closes the browser or connection without logging off, the session is not closed until after it times out (in 10 minutes by default, up to a possible maximum of 1440 minutes). If the number of concurrent sessions permitted also is exceeded for that user, there is no way for that user to regain access to the Central Manager GUI until after the timeout expires.

**Note**

After an upgrade, downgrade, or new installation, you must first clear the cache in your browser, close the browser, and restart the browser session to the WAAS Central Manager.

Components of the WAAS Central Manager GUI

[Figure 1-2](#) shows the main components of the WAAS Central Manager GUI.

Figure 1-2 Components of the WAAS Central Manager GUI

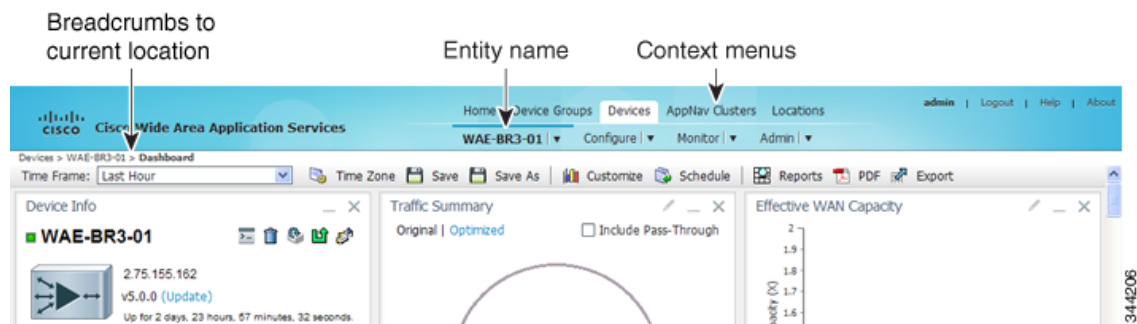
The WAAS Central Manager GUI includes the following main components:

- **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 are shown in [Figure 1-3](#).)
- **Menu bar**—The top level contains menus that allow you to choose the context. The lower level contains menus that group the WAAS Central Manager functions available within the chosen context. For more information, see the “[WAAS Central Manager Menus](#)” section on [page 1-15](#).
- **Taskbar**—Contains labeled icons that perform various functions depending on the content shown in the dashboard. For more information, see the “[WAAS Central Manager Taskbar Icons](#)” section on [page 1-16](#).
- **Dashboard**—Displays the main content, which changes depending on the function that is chosen in the menu.
- **Administrative links**—Includes these navigation links:
 - **Logout**—Logs out the current user from the WAAS Central Manager.
 - **Help**—Opens a separate window with the WAAS context sensitive help.
 - **About**—Displays the WAAS About screen that shows the Central Manager version number.
- **Alarms**—Opens the alarm panel, which displays alarms in your WAAS network.

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

- **Home**—Click 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 to enter the device group context. The page title and the first menu on the lower level displays the name of the chosen device group.
- **Devices**—Choose a device from this menu to enter the device context. The page title and the first menu on the lower level displays the name of the chosen device, as shown in [Figure 1-3](#).
- **AppNav Clusters**—Choose an AppNav Cluster from this menu to enter the AppNav Cluster context. The page title and the first menu on the lower level displays the name of the chosen AppNav Cluster.
- **Locations**—Choose a location from this menu to enter the location context. The page title and the first menu on the lower level displays the name of the chosen location.

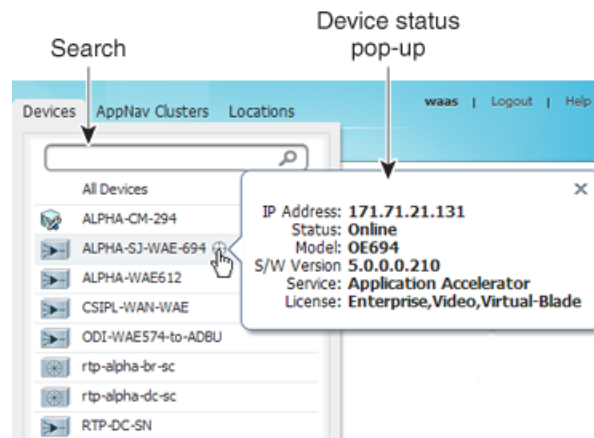
Figure 1-3 WAAS Central Manager Device Context



The 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 in the lower level of the menu bar shows the name of the chosen device group, device, AppNav Cluster, or location.
- **Context menus**—The top level of the menu bar contains menus that allow you to switch easily to any entity in any context. You can search for an item by entering part of its name in the search box at the top and clicking the magnifying glass icon or 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 full window that lists all entities of the selected type, has more advanced search functions, and has taskbar icons that perform functions appropriate to the entity group. You can also click the context menu name to go to the listing window.

In the Devices and AppNav Clusters menus, a small target icon appears when you hover over a device or cluster name. Place your cursor over the target icon to open a pop-up that shows the device or cluster status (see [Figure 1-4](#)).

Figure 1-4 **Devices Context Menu**

WAAS Central Manager Menus

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

- Top level—Contains menus that allow you to switch to any entity in any context.
- Lower level—Contains menus that group the WAAS Central Manager functions available within the chosen context. [Table 1-2](#) describes the menus 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 over the triangle to the right of the menu option name to open the submenu.



Note

The functions available for WAAS Express devices are a subset of those available for other WAAS devices; some functions are not available on WAAS Express devices.

Table 1-2 **Menu Descriptions**

Menu	Description
Dashboard or <i>Device, Device group, AppNav Cluster, or Location name</i>	In the global context, allows you to go to the dashboard for your WAAS network. In a context other than global, this menu is named with the 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 WAAS services and settings.
Monitor	Allows you to see network traffic and other charts and reports to monitor the health and performance of your WAAS network. Allows you to manage and schedule reports for your WAAS network. Contains troubleshooting tools.
Admin	Allows you to manage user accounts, passwords, secure store, licenses, and virtual blades, update the WAAS software, and view system logs and messages.

WAAS Central Manager Taskbar Icons

Table 1-3 describes the taskbar icons in the WAAS Central Manager GUI.

Table 1-3 Taskbar Icon Descriptions (continued)












Taskbar Icon	Function
Common icons	
 (Refresh)	Refreshes the current page of the WAAS Central Manager GUI.
 (Delete)	Deletes a WAAS element, such as a device, and device group.
 (Create or Add)	Creates a new WAAS element such as a report.
 (Edit)	Edits a WAAS element such as interface settings.
 (Advanced Search)	Filters the information in a table to make it easier to locate a specific item.
 (View All)	Displays all items in a table on a single page instead of displaying those items over multiple pages.
 (Print or Print Table)	Prints the information.
 (PDF)	Creates a PDF of the information.
 (Assign All)	Selects all valid items in a table. For example, if you are distributing print drivers to a WAAS print server, you can click this icon to select all drivers in the list that the print server should download.
 (Remove All)	Deselects all selected items in a table.
Devices and Device Group Icons	
 (Activate All Inactive Devices)	Activates all the inactive WAAS and WAAS Express devices in your WAAS network. For more information, see the “Activating All Inactive WAAS Devices” section on page 16-35.

Table 1-3 Taskbar Icon Descriptions (continued)









Taskbar Icon	Function
 (Force Update, Request FullUpdate)	<p>Reapplies the device configuration as seen in the WAAS Central Manager GUI to the device. Normally, changes made in the 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 can cause the configuration on the device to differ from what is seen in the WAAS Central Manager GUI. The Force Full Database Update icon applies the full configuration that the WAAS Central Manager has for the device to be updated to the device and the configuration reapplied.</p> <p>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.</p> <p>You can view device CLI errors in the System Message window described in the “Viewing the System Message Log” section on page 17-62.</p> <p>The Force Full Database Update icon appears on the Device Dashboard window, described in the “Device Dashboard Window” section on page 17-8. The Request FullUpdate icon appears on the Modifying Device Group window.</p> <p>These functions do not apply to WAAS Express devices.</p>
 (Reload)	<p>Reboots a WAE or device group depending on the location in the WAAS Central Manager GUI. For more information, see the “Rebooting a Device or Device Group” section on page 16-35. Reload is not available for WAAS Express devices.</p>
 (Force Group Settings)	<p>Forces the device group configuration across all devices in that group. For more information, see the “Forcing Device Group Settings on All Devices in the Group” section on page 3-7.</p>
 (Apply Defaults)	<p>Applies the default settings to the fields on the window.</p>
 (Export Table)	<p>Exports table information into a CSV file.</p>
 (Override Group Settings)	<p>Allows you to specify device-specific settings that override the group settings for the device. For more information, see the “Overriding the Device Group Settings on a Device” section on page 3-8.</p>
 (Deactivate Device)	<p>Deactivates a WAAS or WAAS Express device.</p>
 (Update Application Statistics)	<p>Updates the application statistics.</p>
 (Delete All)	<p>Deletes all WAAS elements of a particular type, such as IP ACL conditions.</p>
 (Display All Devices)	<p>Displays all WAE devices or device groups.</p>

Table 1-3 Taskbar Icon Descriptions (continued)

Taskbar Icon	Function
 (Configure Dashboard Display)	Allows you choose which charts to display in the Device Dashboard window.
 (Copy Settings)	Copies interception settings to other devices (not available for inline interception).
Acceleration Icons	
 (Restore Default Policies and Classifiers)	Restores the default predefined optimization policy rules on the device or device group. For more information, see the “Restoring Optimization Policies and Class Maps” section on page 13-61.
 (View Topology)	Displays the topology map that shows all the TFO connections among your WAE devices. For more information, see the “Topology Report” section on page 17-40.
 (Navigate to Application Configuration Page)	Displays the configuration page used to create applications. For more information, see the “Viewing a List of Applications” section on page 13-59.
System Message Log Icons	
 (Truncate Table)	Allows you to truncate the system message log based on size, date, or message content. For more information, see the “Viewing the System Message Log” section on page 17-62.

WAAS Central Manager Monitoring API

The 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 Central Manager monitoring API communicates with the WAAS Central Manager to retrieve status information and monitoring statistics.

The 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.

For more information on the monitoring API, see the [Cisco Wide Area Application Services API Reference](#).

WAE Device Manager GUI

The WAE Device Manager is a web-based management interface that allows you to configure, manage, and monitor an individual WAE device in your network. In some cases, the same device settings exist in both the WAE Device Manager and the WAAS Central Manager GUI. For this reason, we recommend that you always configure device settings from the WAAS Central Manager GUI when possible.

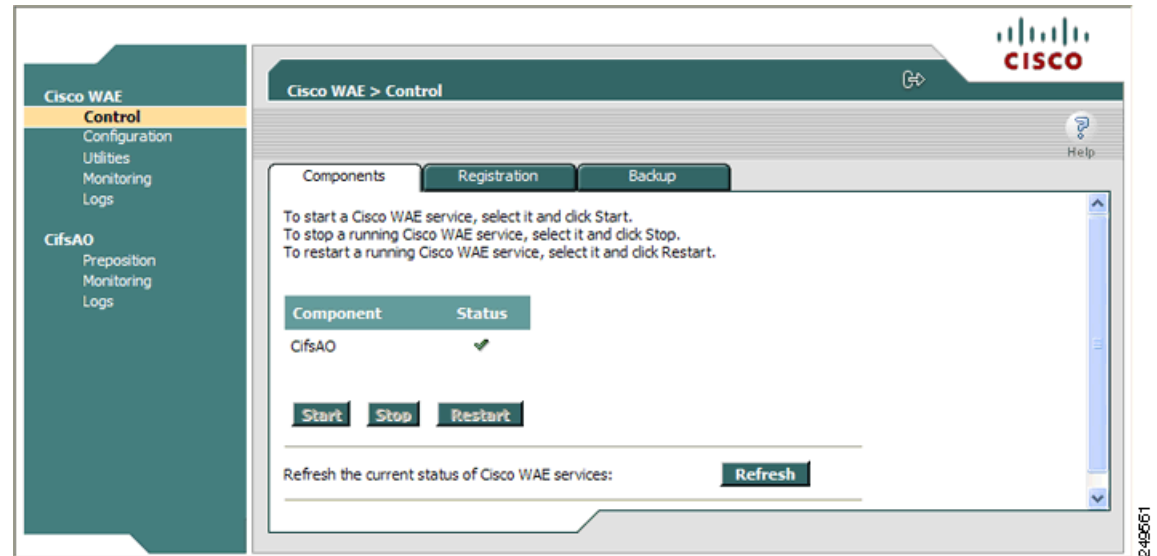
In some situations, you might need to use the WAE Device Manager GUI to perform certain tasks. For example, starting, stopping, and restarting the CIFS accelerator service can only be performed from the WAE Device Manager GUI and not from the WAAS Central Manager GUI.

For more information about the tasks you can perform from the WAE Manager, see [Chapter 11, “Using the WAE Device Manager GUI.”](#)

To access the WAE Device Manager for a specific device, go to the following URL:
<https://Device IP Address:8443/mgr>

Figure 1-5 shows an example of the WAE Device Manager window.

Figure 1-5 WAE Device Manager Window



WAAS CLI

The 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 WAAS CLI also allows you to configure certain features that are supported only through the CLI (for example, configuring the Lightweight Directory Access Protocol [LDAP] signing on a WAE). We strongly recommend that you use the WAAS Central Manager GUI instead of the WAAS CLI, whenever possible.



Note

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

The 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 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 CLI to configure a 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 describes the benefits of Cisco WAAS and includes the following topics:

- [Preservation of Source TCP/IP Information, page 1-20](#)
- [Autodiscovery of WAAS Devices, page 1-20](#)
- [Centralized Network Monitoring and Management, page 1-21](#)
- [Optimized Read and Write Caching, page 1-21](#)
- [WCCP Support, page 1-22](#)
- [PBR Support, page 1-22](#)
- [Inline Interception Support, page 1-23](#)
- [Failure Resiliency and Protection, page 1-23](#)
- [RAID Compatibility, page 1-23](#)
- [Streamlined Security, page 1-24](#)
- [SNMP Support, page 1-24](#)

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 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 WAAS devices is achieved using proprietary TCP options. These TCP options are only recognized and understood by WAAS devices and are ignored by non-WAAS devices.

Centralized Network Monitoring and Management

Cisco WAAS Web-based management tools (WAAS Central Manager and WAE Device Manager GUIs) enable IT administrators to centrally define, monitor, and manage policies for each 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 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/CIFS) 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 master 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. 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. CIFS 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. Once 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. 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 [Chapter 5, “Configuring Traffic Interception.”](#)

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 [Chapter 4, “Configuring AppNav.”](#)

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 the [“Using Inline Mode Interception”](#) section on page 5-43.

Failure Resiliency and Protection

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

If a WAE configured for CIFS 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 CIFS 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 CIFS 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 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.

- Logical Disk Handling with RAID-1—Logical disk handling with RAID-1 is implemented in 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**—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 [Chapter 16, “Maintaining Your WAAS System.”](#)

Streamlined Security

Cisco WAAS supports disk encryption, which addresses the need to securely protect sensitive information that flows through deployed 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 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 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 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, CIFS statistics, and cache statistics.

For more information about SNMP and supported MIBs, see [Chapter 18, “Configuring SNMP Monitoring.”](#)