



CHAPTER 1

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 appliances, WAE Network Modules (the NME-WAE family of devices), and SM-SRE modules running WAAS.

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 1-9](#)
- [Benefits of Cisco WAAS, page 1-17](#)

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 application policies to determine whether to optimize the traffic or allow it to pass through your network unoptimized.

You use the WAAS Central Manager GUI to centrally configure and monitor the WAEs and application policies in your network. You can also use the WAAS Central Manager GUI to create new application policies 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)

This section contains the following topics:

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

Cisco WAAS Overcomes Common WAN Challenges

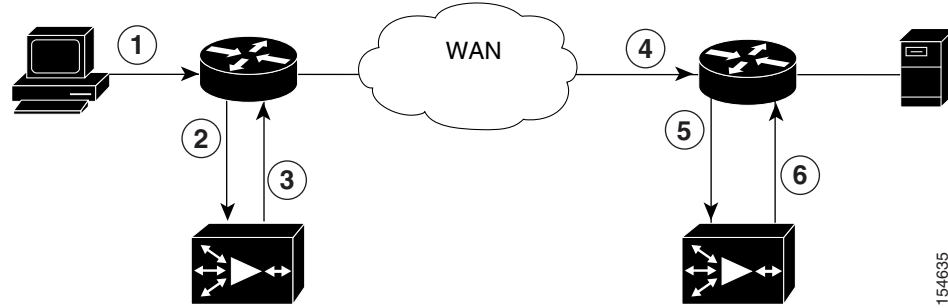
[Table 1-1](#) describes how Cisco WAAS uses a combination of TCP optimization techniques and application acceleration features to overcome the most common challenges associated with transporting traffic over a WAN.

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 a WAE with a Cisco WAE Inline Network Adapter, WAAS can intercept the request directly using inline mode. For more information on inline mode, see the [“Using Inline Mode to Transparently Intercept TCP Traffic”](#) section on page 4-42.
3. The branch WAE performs the following actions:
 - Examines the parameters in the traffic’s TCP headers and then refers to the application policies to determine if the intercepted traffic should be optimized. Information in the TCP header, such as the source and destination IP address, allows the branch WAE to match the traffic to an application policy. For a list of predefined policies, see [Appendix A, “Predefined Application Policies.”](#)
 - 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.
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 application policy 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 1-5](#)
- [Application-Specific Acceleration, page 1-6](#)
- [File Services for Desktop Applications, page 1-7](#)
- [WAAS Print Services, page 1-8](#)
- [Virtualization, page 1-8](#)

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 1-4](#)
- [TCP Initial Window Size Maximization, page 1-4](#)
- [Increased Buffering, page 1-5](#)
- [Selective Acknowledgment, page 1-5](#)
- [BIC TCP, page 1-5](#)

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.
- WAFS 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.

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 application policies to match specific types of traffic to an application and to determine whether that application traffic should be optimized and accelerated.

The following WAAS application accelerators are available:

- CIFS—Accelerates CIFS traffic exchanged with a remote file server. For more information, see the [“File Services for Desktop Applications” section on page 1-7](#).
- NFS—Accelerates Network File System (NFS) version 3 traffic exchanged with a remote file server. Secure NFS traffic is not accelerated.
- HTTP—Accelerates HTTP 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 2000–2007 clients are supported. Secure connections that use message authentication (signing) or encryption are not accelerated and 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. Server Message Block (SMB) signed traffic is not accelerated. The Windows print accelerator supports Windows 2000 and Windows Server 2003 print servers. It supports clients running Windows 2000, Windows XP, and Windows Vista.

To enable or disable application accelerators, see the [“Enabling and Disabling the Global Optimization Features” section on page 12-2](#).

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 (CIFS accelerator) feature allows a WAE to store remote file server data in its local cache so that the WAE can quickly fulfill a client’s data request instead of sending that request over the WAN to the file server. By fulfilling the client’s request 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 11, “Configuring Wide Area File Services.”](#)

WAAS version 4.1.1 and later supports two mutually exclusive file services modes: a transparent CIFS accelerator mode and a legacy mode. The transparent CIFS accelerator mode requires no core, edge, or connectivity configuration. You configure the legacy mode the same as in WAAS version 4.0.x. These two modes are mutually exclusive. We recommend using the transparent CIFS accelerator mode if you do not need to interoperate with WAAS 4.0.x devices.



Note

Legacy mode WAFS is deprecated in WAAS version 4.2.1. It still operates but is not supported and will be removed in a future version. Legacy WAFS users should migrate to the transparent CIFS accelerator.

File Services includes the following features:

- Prepositioning—Allows system administrators to proactively “push” frequently used files from the central file server into the cache of selected WAEs. This provides users with faster first-time file access, and makes more efficient use of available bandwidth.
- 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.

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 the CIFS accelerator and Windows print acceleration be enabled. For more information, see the [“Enabling and Disabling the Global Optimization Features” section on page 12-2](#).
- 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.”](#)
- Legacy WAAS print services—This legacy service also allows you to use the branch WAE as a local print server by using Samba and Common Unix Printing System (CUPS) software that is built into WAAS. For more information, see [Chapter 13, “Configuring and Managing WAAS Legacy Print Services.”](#)

**Note**

The legacy print services feature is deprecated in WAAS version 4.2.1. It still operates but is not supported and will be removed in a future version. Legacy print services users should migrate to the Windows print accelerator.

All three of 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 1-9](#)
- [WAE Device Manager GUI, page 1-15](#)
- [WAAS Print Services Administration GUI, page 1-16](#)
- [WAAS CLI, page 1-16](#)

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 or device group.
- Create and edit application policies that determine the action that a WAAS device performs when it intercepts specific types of traffic.
- Configure file services and set up file preposition policies.
- 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 file services, print services, or application acceleration 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 1-9](#)
- [Components of the WAAS Central Manager GUI, page 1-10](#)
- [WAAS Central Manager Navigation Pane, page 1-12](#)
- [WAAS Central Manager Taskbar Icons, page 1-12](#)

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 7, “Creating and Managing Administrator User Accounts and Groups.”](#)

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

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 9-17.

**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 after 120 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.

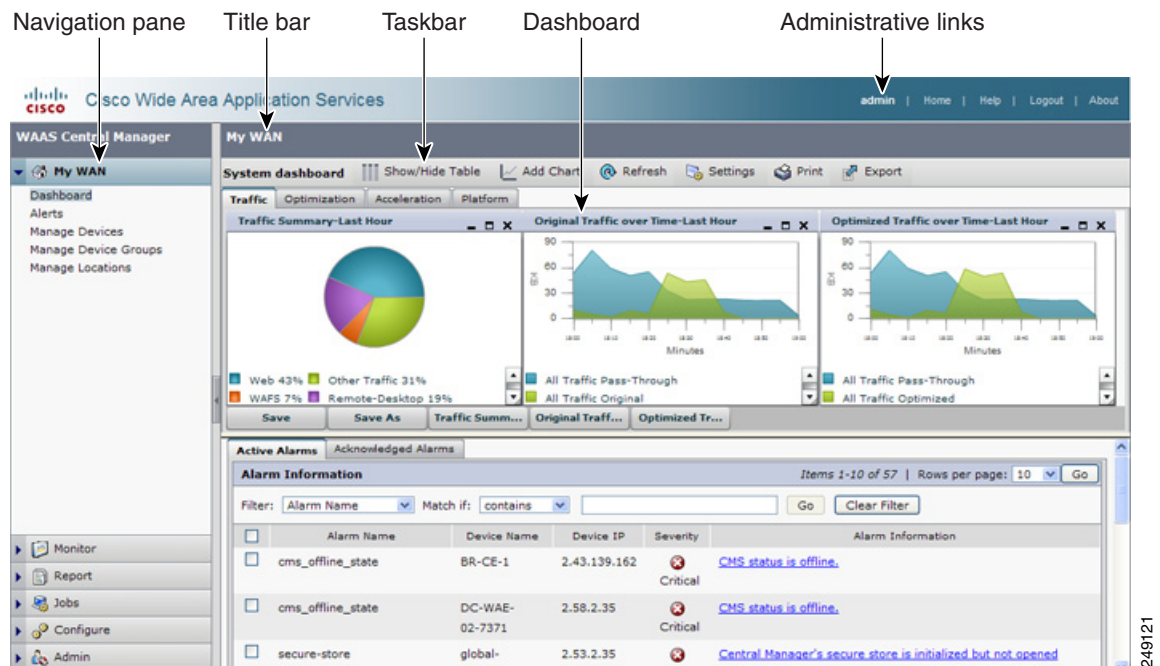
**Note**

After an upgrade, downgrade, or new installation, you must first clear the cache in Internet Explorer before restarting 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:

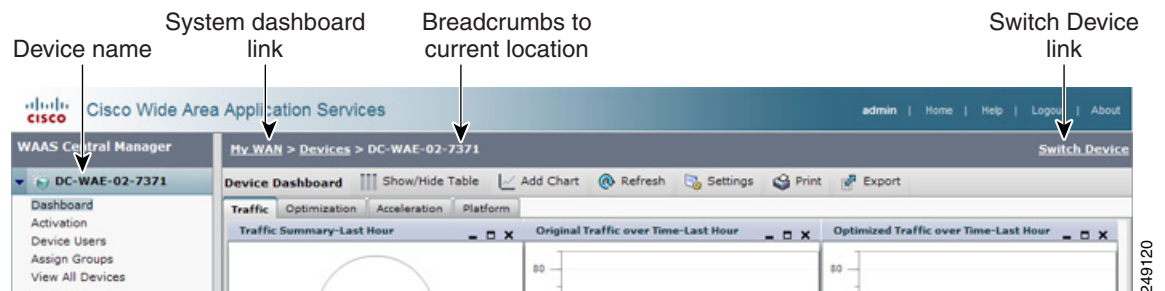
- Navigation pane—Contains drawers that group the WAAS Central Manager functions. For more information, see the [“WAAS Central Manager Navigation Pane”](#) section on page 1-12.
- Title bar—Displays the title of the page being viewed and breadcrumb links to ease navigation back to previous levels in the hierarchy. (Breadcrumb links are shown in [Figure 1-3](#).)

- Taskbar—Contains 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 1-12.
- Dashboard—Displays the main content, which changes depending on the function that is chosen in the navigation pane.
- Administrative links—Includes these navigation links:
 - Home—Displays the System Dashboard (shown in Figure 1-2).
 - Help—Opens a separate window with the WAAS context sensitive help.
 - Logout—Logs out the current user from the WAAS Central Manager.
 - About—Displays the WAAS About screen that shows the version number.

There are two main contexts in the WAAS Central Manager GUI:

- Global Context—You are in this context initially, when no particular device or device group is chosen. The top drawer in the navigation pane reads My WAN, as shown in Figure 1-2.
- Device Context—You are in this context after you have chosen a device or device group in the Manage Devices or Manage Device Groups pages. The top drawer in the navigation pane displays the name of the chosen device or device group, as shown in Figure 1-3.

Figure 1-3 WAAS Central Manager GUI Device Context



In the device context, the WAAS Central Manager GUI includes the following new items:

- Device name—The top drawer in the navigation pane shows the name of the chosen device or device group.
- System dashboard link—My WAN displays the system dashboard and returns to the global context.
- Breadcrumbs to current location—Displays the path to your current location in the GUI. You can click the Devices link to return to the Manage Devices page. If you are managing a device group, this link is named Device Groups and it returns you to the Manage Device Groups page.
- Switch Device link—Allows you to switch devices and stay on the same functional device context page in the GUI. Clicking this link opens the Switch Devices page, as shown in Figure 1-4. To switch to a different device, select the radio button next to the device and click the **Switch** button.

If you are managing a device group, the name of this link is Switch DeviceGroup, and it allows you to switch to a different device group, just like for devices.

Figure 1-4 Switch Devices Page



WAAS Central Manager Navigation Pane

The WAAS Central Manager GUI navigation pane contains drawers that serve to group WAAS Central Manager functions. Table 1-2 describes the drawers in the navigation pane.

Drawers may contain different functions when a particular device or device group is selected than when you are in the global context.

Table 1-2 Drawer Descriptions

Drawer	Description
My WAN or Device name	Allows you to go to the Dashboard and Alerts displays for your entire WAAS network and allows you to choose a specific device or device group for which to configure WAAS services and general settings. You can also view detailed device information and messages, and manage locations. When you have chosen a specific device or device group, this drawer is named with the device or group name and allows you to activate devices or assign groups or devices. Choose View All Devices to go back to the view of all devices.
Monitor	Allows you to see network traffic and other charts and reports to monitor the health and performance of your WAAS network. (This drawer appears only at the global level or when an individual device is chosen, not for a device group.)
Report	Allows you to manage and schedule reports for your WAAS network. (This drawer appears only at the global level when no device or device group is chosen.)
Troubleshoot	Allows you to use troubleshooting tools. (This drawer appears only when a device or device group is chosen, not at the global level.)
Jobs	Allows you to manage software update jobs.
Configure	Allows you to configure the main WAAS services (file, print, and application acceleration) and other settings.
Admin	Allows you to manage user accounts, passwords, licenses, and virtual blades, and view the system log.

WAAS Central Manager Taskbar Icons

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

Table 1-3 Taskbar Icon Descriptions












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, device group, print driver, or file service policy.
 (Create)	Creates a new WAAS element, such as a file service policy or an acceleration policy.
 (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.
 (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 WAEs)	Activates all the inactive WAEs in your WAAS network. For more information, see the “Activating All Inactive WAAS Devices” section on page 15-31 .
 (Force Update)	<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>You can view device CLI errors in the System Message window described in the “Viewing the System Message Log” section on page 16-61.</p> <p>The Force Full Database Update icon appears on the Device Dashboard window, described in the “Device Dashboard Window” section on page 16-9.</p>
 (Reload)	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 15-32 .

Table 1-3 Taskbar Icon Descriptions (continued)

















Taskbar Icon	Function
 (Force Group Settings)	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 3-8.
 (Apply Defaults)	Applies the default settings to the fields on the window.
 (Export Table)	Exports table information into a CSV file.
 (Switch Baseline Group)	Allows you to select another device group to associate with the baseline group. For more information, see the “Switching the Baseline Group for a Service” section on page 3-13.
 (Override Group Settings)	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 3-9.
 (Deactivate Device)	Deactivates a WAE.
 (Update Application Statistics)	Updates the application statistics.
 (Delete All)	Deletes all WAAS elements of a particular type, such as IP ACL conditions.
 (Display All Devices)	Displays all WAE devices or device groups in the navigation pane.
 (Configure Dashboard Display)	Allows you choose which charts to display in the Device Dashboard window.
Print Services Icons	
 (Retry Downloading Failed Drivers)	Attempts to download print drivers that previously failed to be distributed to the WAAS print server or device group. For more information, see Chapter 13, “Configuring and Managing WAAS Legacy Print Services.”
 (Print Services Administration GUI)	Opens the Print Services Administration GUI for the WAAS print server. For more information about the tasks you can perform from this GUI, see the “Using the Print Services Administration GUT” section on page 13-28.
Acceleration Icons	
 (Restore Default Policies and Classifiers)	Restores the default predefined application policies on the device or device group. For more information, see the “Restoring Application Policies and Classifiers” section on page 12-38.
 (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 16-44.
 (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 12-37.

Table 1-3 Taskbar Icon Descriptions (continued)

Taskbar Icon	Function
System Message Log Icons	
 (Truncate Table)	For more information, see the “Viewing the System Message Log” section on page 16-61.

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, the following tasks can only be performed from the WAE Device Manager GUI and not from the WAAS Central Manager GUI:

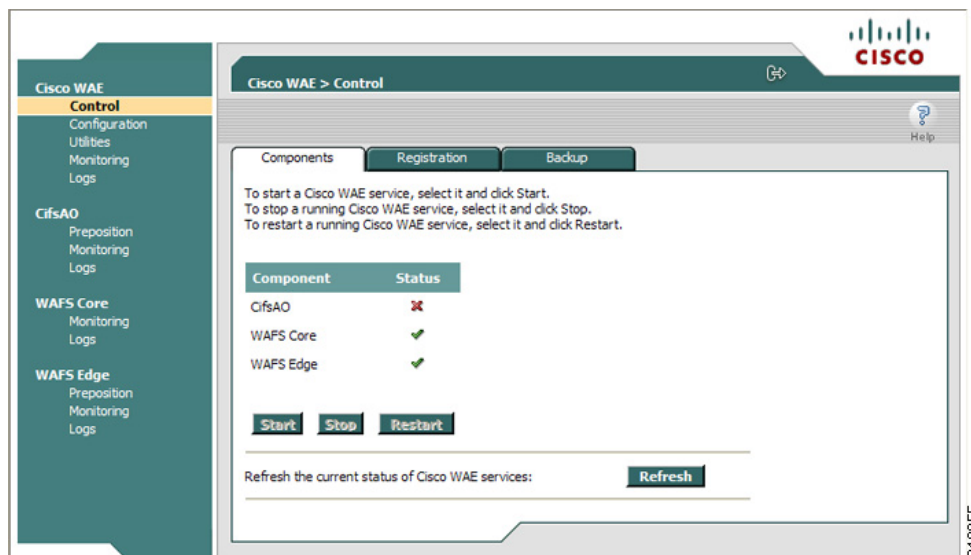
- Enabling print services on a WAE
- Shutting down device services

For more information about the tasks you can perform from the WAE Manager, see [Chapter 10, “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 Example of the WAE Device Manager Window

WAAS Print Services Administration GUI

The Print Services Administration GUI is a Web-based interface that allows you to configure an individual WAAS print server and view a list of active and completed print jobs.

You can perform the following common tasks from the Print Services Administration GUI:

- Add a printer to WAAS print server
- Modify the configuration of an existing printer
- Set up print clusters
- View print jobs

You can access the Print Services Administration GUI from the WAAS Central Manager GUI or from the WAE Manager GUI. For more information, see [Chapter 13, “Configuring and Managing WAAS Legacy Print Services.”](#)

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 1-17](#)
- [Autodiscovery of WAAS Devices, page 1-17](#)
- [Centralized Network Monitoring and Management, page 1-17](#)
- [Optimized Read and Write Caching, page 1-18](#)
- [WCCP Support, page 1-19](#)
- [PBR Support, page 1-20](#)
- [Inline Interception Support, page 1-20](#)
- [Failure Resiliency and Protection, page 1-20](#)
- [Namespace Support, page 1-21](#)
- [RAID Compatibility, page 1-21](#)
- [Streamlined Security, page 1-21](#)
- [SNMP Support, page 1-22](#)

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. If communication between WAEs is disrupted, the software automatically switches into Disconnected Mode, preventing operations that could jeopardize the coherency of files in the network.

Optimized Read and Write Caching

The wide area file services (WAFS) 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. WAFS 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.

In WAFS legacy mode, Cisco WAAS uses its own proprietary adaptation protocol layer over the WAN between the branch WAE and data center WAE, while retaining the standard CIFS protocol at the client and server ends. This proprietary network protocol provides reliable and efficient communication over WANs, especially under high-latency, low-bandwidth conditions.

The Cisco WAAS protocol offers the following benefits:

- Reliability—Maintains its own internal message queuing and ordering, enabling it to overcome transient disconnects, network jitters, and message loss. The Cisco WAAS transport layer handles temporary network failures by reestablishing the connection, then retransmitting requests that did not receive a response on the disconnected socket.
- Efficiency—Supports compound requests, grouping multiple, dependent requests and responses into a single message. The processing of individual calls within a compound message is serialized, enabling the output of one command to be used as input for the next.
- Link utilization optimization—Uses multiple concurrent TCP connections for each branch WAE-to-data center WAE link. Requests and responses may be delivered across any open connection. For example, multiple requests (and responses) for data delivery can be split across multiple connections to increase the effective use of the network in cases of high-latency or high-loss WAN connections, where TCP performance degrades.
- Command prioritization—Assigns high priority to requests from active clients, minimizing the WAN latency experienced by users. Batch tasks (such as preposition, for example) are assigned a lower priority and are performed in the background.
- Bandwidth conservation—Compresses all requests and responses. Before compression, the message is encoded, allowing efficient delivery of both textual and binary data. The protocol layer applies the compression automatically, regardless of the message content.
- Firewall-friendly—Is layered over TCP/IP and uses TCP port 4050. You should configure firewalls to open TCP port 4050 to traffic.

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 4, “Configuring Traffic Interception.”](#)

Inline Interception Support

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

The Cisco WAE Inline Network Adapter 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.

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

You can serially cluster WAE devices with the Cisco WAE Inline Network Adapter installed 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.

For more information about inline mode, see the [“Using Inline Mode to Transparently Intercept TCP Traffic”](#) section on page 4-42.

Failure Resiliency and Protection

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

If a WAE configured for WAAS 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.

When using legacy mode and communication is interrupted between the Edge WAE and the Core Cluster or between the Core Cluster and the file server, the Cisco WAAS network switches to working in a disconnected state until full communication is restored. If the interruption is brief, the network enters a transient disconnect state, enabling a select number of services and commands for a limited time (typically lasting about one minute), such as read commands for files that are already open.

If the network outage is prolonged, Cisco WAAS switches to a full disconnect state where no services are provided to clients. In this mode, the system denies access to any file (including cached files) until reconnection occurs. From a user viewpoint, the Edge WAE responds as if the network to which it is connected is disconnected.

This approach is required to maintain the security of the data. If a no-service state was not enforced, users connected locally to the file servers can continue working on files, which creates conflicts with other users who may have been working on those files remotely when the network interruption occurred. Cisco WAAS is designed to prevent scenarios that could compromise data coherency and concurrency.

**Note**

Disconnected operation functions only with CIFS legacy mode, not with the CIFS accelerator.

Namespace Support

For legacy CIFS users, there are several ways to access the file servers cached by the Edge WAEs and integrate them within the organizational namespace. One method is to use a prefix, suffix, or alias for a specific site, which creates a unique name for each file server. (Using an alias enables the old name to be retained after replacing the local file server with the new server in the data center.) Another method is to integrate the cached file servers within the DFS namespace as DFS links. When using DFS with legacy CIFS, the DFS site name must be configured manually for each Edge WAE (or edge device group). This information enables DFS to direct user requests correctly. Remote users are directed to file servers through the appropriate Edge WAE, while local users continue to access files directly, without making use of the Edge WAE cache.

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 15, “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.

Cisco WAAS exports parameters based on the following private, read-only MIBs:

- ACTONA-ACTASTOR-MIB.my
- CISCO-CONTENT-ENGINE-MIB

In addition, Cisco WAAS supports the full functionality of each of these standard MIBs, including the setting of traps. 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.

- MIB-2 General Network Statistics (RFC 1213 and 1157)—Contains essential parameters for the basic management of TCP/IP-based networks.
- Host Resources (RFC 1514)
- SNMPv3 MIBs (RFC 2571 through 2576)
- DISMAN-EVENT-MIB (RFC 2981)
- ENTITY-MIB (RFC 2037)

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 Support, see [Chapter 17, “Configuring SNMP Monitoring.”](#)