Planning Your Cisco WAAS Network

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

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

This chapter contains the following sections:

- Checklist for Planning Your Cisco WAAS Network, on page 1
- Site and Network Planning, on page 4
- Autoregistration and WAEs, on page 8
- Interoperability and Support, on page 10
- Cisco WAAS Devices and Device Modes, on page 16
- Calculating the Number of Cisco WAAS Devices Required, on page 19
- Supported Methods of Traffic Redirection, on page 20
- Access Lists on Routers and WAEs, on page 26
- Cisco WAAS Login Authentication and Authorization, on page 27
- Logically Grouping Your WAEs, on page 28
- Data Migration Process, on page 29

Checklist for Planning Your Cisco WAAS Network

This section contains the following topics:

Network Topologies

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

Cisco WAAS software supports the following three typical network topologies:

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

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

Planning Checklist

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

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

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

To plan your network, follow these guidelines:

1. Complete the sizing phase that includes the following tasks:
   - Determine which locations in your existing network require Cisco WAAS optimization, for example, branch offices and data centers.
   - Determine if you are going to use a traditional Cisco WAAS deployment model or the AppNav deployment model. For more information on AppNav, see the chapter Configuring Cisco AppNav.
   - Determine the number and models of the Cisco WAAS devices that are required for each location. Some key factors in this selection process is the WAN bandwidth, the number of users, and the expected use. Various hardware configurations are possible, for example, different hard disk models and RAM size. Consider running a cluster of WAEs where additional scalability and or failover is required. For more information, see Calculating the Number of Cisco WAAS Devices Required, on page 19
   - Verify that you have purchased sufficient licenses to cover your requirements.
2. Plan for management as follows:

- Complete site and network planning, for example, obtain the IP and routing information, including IP addresses and subnets, routers and default gateway IP addresses, and hostnames for devices. See the "Checklist of Cisco WAAS Network System Parameters" table in the *Cisco Wide Area Application Services Quick Configuration Guide*.
- Determine the login authentication and login authorization methods, for example, external RADIUS, TACACS+, Windows domain servers, and accounting policies that you want your Cisco WAAS Central Managers and WAEs to use. For more information, see the chapter .
- For security purposes, plan to change the predefined password for Configuring Administrative Login Authentication, Authorization, and Accountingthe predefined superuser account immediately after you have completed the initial configuration of a WAE. For more information, see Cisco WAAS Login Authentication and Authorization, on page 27.
- Determine if you need to create any additional administrative accounts for a Cisco WAAS device. For more information, see the chapter Creating and Managing Administrator User Accounts and Groups
- Determine if you should group your WAEs into logical groups. For more information, see Logically Grouping Your WAEs, on page 28.
- Determine which management access method to use. By default, Telnet is used, but SSH may be the preferred method in certain deployments. For more information, see Configuring Login Access Control Settings for Cisco WAAS Devices in the chapter "Configuring Administrative Login Authentication, Authorization, and Accounting."

3. Plan for application optimization as follows:
   - Determine and resolve router interoperability issues, for example, the supported hardware and software versions, router performance with interception enabled. For more information, see Site and Network Planning, on page 4
   - Determine the appropriate interception location when the data center or branch office is complex, for example, if your existing network uses a hierarchical topology.
   - Determine which Cisco WAAS services to deploy. For more information about the different Cisco WAAS services, see the chapter "Introduction to Cisco WAAS."
   - Determine which Cisco WAAS software licenses to install. Software licenses enable specific Cisco WAAS services. For more information about installing software licenses, see the Managing Cisco WAAS Software Licenses in the chapter "Configuring Other System Settings."
   - Determine which traffic interception methods to use in your Cisco WAAS network, for example, AppNav, inline mode, WCCP Version 2, or policy-based routing (PBR).
   - For more information on the advantages and disadvantages of using WCCP, see Supported Methods of Traffic Redirection, on page 20
   - For more information on WCCP traffic interception and redirection, see About Traffic Interception Methods in the chapter "Configuring Traffic Interception."

Note WCCP works only with IPv4 networks.

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

Note IP ACLs that are defined on a router take precedence over the ACLs that are defined on the WAE. For more information, see Access Lists on Routers and WAEs, on page 26.

- Determine whether you have to define IP ACLs or interception ACLs on the WAEs. For more information, see Access Lists on Routers and WAEs, on page 26

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

- If PBR is to be used, determine which PBR method to use to verify PBR next-hop availability for your WAEs. For more information, see Methods of Verifying PBR Next-Hop Availability in the chapter "Configuring Traffic Interception."
- Determine the major applications for your Cisco WAAS network. Verify whether the predefined application definition policies cover these applications and whether you should add policies if your applications are not covered by these predefined policies. For a list of the predefined application definition policies, see Appendix A, Predefined Optimization Policy.
- Consider day zero migration of file systems if file servers are to be centralized in the process. For more information, see Data Migration Process, on page 29

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

Site and Network Planning

This section contains the following topics:

About Site and Network Planning

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

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

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

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

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

The WAE attaches to the LAN as an appliance. A WAE relies on packet interception and redirection to enable application acceleration and WAN optimization. Consequently, traffic interception and redirection to a WAE must occur at each site where a WAE is deployed. Traffic interception and redirection occurs in both directions of the packet flow. Because Layer 3 and Layer 4 headers are preserved, you should ensure that you always connect a WAE to a tertiary interface (or a subinterface) on the router to avoid routing loops between the WAE and the WCCP or PBR-enabled router that is redirecting traffic to it. For more information on this topic, see Using Tertiary Interfaces or Subinterfaces to Connect WAEs to Routers, on page 25.

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

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

Microsoft Windows Network Integration

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

Data Center WAE Integration

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

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

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

Note User permissions are determined by the existing security infrastructure.

Branch WAE Integration

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

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

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

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

UNIX Network Integration

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

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

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

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

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

SMB-Related Ports in a Cisco WAAS Environment

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

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

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

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

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

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

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

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

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

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

Firewalls and Standby Cisco WAAS Central Managers

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

Performance Tuning for High WAN Bandwidth Branch Offices

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

Autoregistration and WAEs

This section contains the following topics:

About Autoregistration and WAEs

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

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

Autoregistration and DHCP

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Note Autoregistration is automatically disabled if a static IP address is configured or if you configure interface-level DHCP on the same interface that autoregistration uses. (See Selecting Static IP Addresses or Using Interface-Level DHCP, on page 10.)

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

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

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

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

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

Selecting Static IP Addresses or Using Interface-Level DHCP

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

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

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

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

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

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

Interoperability and Support

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

Unicode Support for Cisco WAAS GUI Interfaces

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

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

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

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

Note the following about Unicode support limitations:

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

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

Cisco WAAS and Cisco IOS Interoperability

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

Note The Cisco WAAS software does not support Mobile IP.

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

Cisco WAAS and the Cisco IOS QoS Classification Feature

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

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

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

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

Cisco WAAS and the Cisco IOS NBAR Feature

Unlike a traditional type of classification that is specified through a policy filter, as listed in Cisco WAAS and the Cisco IOS QoS Classification Feature, on page 11, Network-Based Application Recognition (NBAR) classification needs to consider payload. The classification keeps track of any interceptor that modifies the payload because this modification might cause NBAR to not be able to classify the packets. However, the Cisco WAAS software does support NBAR.

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

1. A packet, P1, which is a part of a TCP stream, S1, enters the router and is classified by NBAR on the LAN interface of the router as belonging to class C1. If the classification of P1 does not involve payload inspection, for example, only TCP/IP headers, no action is to be taken because the Cisco WAAS software preserves this information.
2. If P1 classification requires payload inspection, P1 should be marked using the TOS/DSCP bits in the packet (as opposed to using other internal marking mechanisms).
3. P1 is then intercepted through WCCP Version 2 (still on the LAN interface, WCCP is processed after NBAR) and is redirected to a WAE.
4. Cisco WAAS applies optimizations, if any, on the payload and copies the DCSP bits settings from the incoming TCP stream, S1, onto the outgoing stream, S2 (which is established between the local Cisco WAAS appliance and the remote Cisco WAAS appliance over the WAN). Because NBAR usually has to see some payload before performing the classification, it is unlikely that Cisco WAAS will have the proper bit settings at connection-establishment time. Consequently, the Cisco WAAS software uses polling to inspect the DSCP bits on the incoming TCP stream, and then copies it over to the stream from the Cisco WAAS device back to the router.
5. When S2 re-enters the router, NBAR will not classify S2 as belonging to C1 because the payload has been changed or compressed. However, the DSCP settings have already marked these packets as belonging to C1. Consequently, these packets will be treated appropriately as if they were classified through NBAR.

   As long as the flow is not identified, NBAR will continue to search for classification in the packets. Because compressed packets will not be classified, this situation can unnecessarily burden the CPU (performing packet inspection). Because of the potential degradation in performance and the slight possibility of correctness issues, we strongly recommend that you use a subinterface or a separate physical interface to connect the WAE to the router (as described in Using Tertiary Interfaces or Subinterfaces to Connect WAEs to Routers, on page 25). When you use a tertiary interface or subinterface to connect the WAE to the router, both the performance and correctness issues are addressed because each packet is processed only once.

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

Note This dynamic classification support requires support for marking DSCP/ToS settings, as specified in Cisco WAAS and the Cisco IOS QoS Classification Feature, on page 11, as well as the tracking of dynamic changes through polling.

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

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

Cisco WAAS and Cisco IOS Marking

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

Cisco WAAS and Cisco IOS Queuing

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

Cisco WAAS and Cisco IOS Congestion Avoidance

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

Cisco WAAS and Cisco IOS Traffic Policing and Rate Limiting

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

Cisco WAAS and Cisco IOS Signaling

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

Cisco WAAS and Cisco IOS Link-Efficiency Operations

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

Cisco WAAS and Cisco IOS Provisioning, Monitoring, and Management

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

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

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

Cisco WAAS and Management Instrumentation

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

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

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

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

Cisco WAAS and MPLS

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

Cisco WAAS Application Accelerators Interoperability with Third-Party Load Balancers

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

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

Table 1: Cisco WAAS AOs Interoperability with Load Balancers

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

Cisco WAAS Compatibility with Other Cisco Appliances and Software

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

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

Cisco WAAS Devices and Device Modes

This section contains the following topics:

About Cisco WAAS Devices and Device Modes

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

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

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

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

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

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

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

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

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

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

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

Changing Device Mode

Before you begin

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

Procedure

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

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

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

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

Step 3 Save the configuration and reload:

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

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

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

Step 5 Re-enable CMS services:

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

Step 6 Save the configuration:

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

What to do next

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

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

Calculating the Number of Cisco WAAS Devices Required

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

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

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

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

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

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

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

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

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

Supported Methods of Traffic Redirection

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

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

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

This section contains the following topics:

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

Advantages and Disadvantages of Using Inline Interception

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

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

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

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

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

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

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

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

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

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

Advantages and Disadvantages of Using WCCP

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

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

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

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

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

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

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

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

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

Advantages and Disadvantages of Using PBR

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

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

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

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

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

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

Configuring WCCP or PBR Routing for Cisco WAAS Traffic

This section contains the following topics:

About Configuring WCCP or PBR Routing for Cisco WAAS Traffic

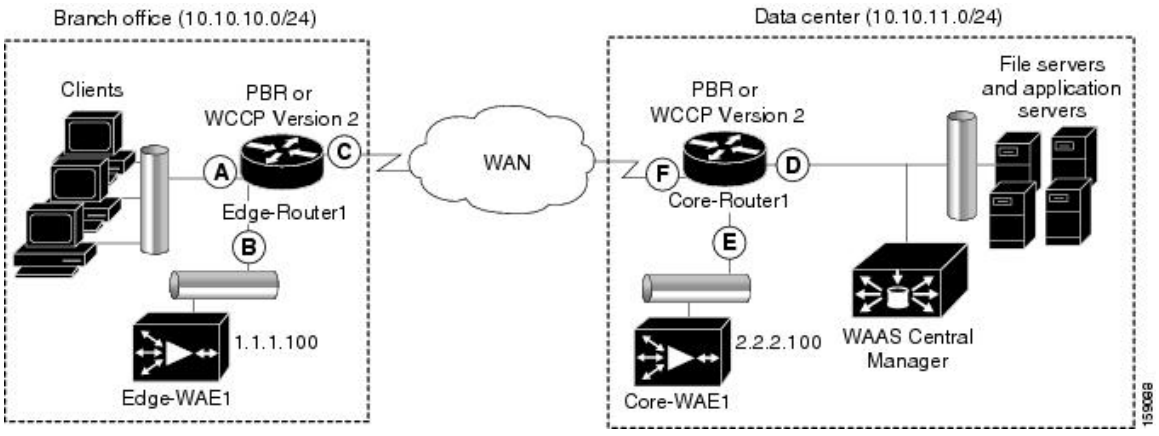
The primary function of Cisco WAAS is to accelerate WAN traffic. In general, Cisco WAAS accelerates TCP traffic, and uses a symmetric approach for application optimization. A WAE that has application-specific and network-specific intelligence is placed on each side of the WAN. These WAEs are deployed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

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

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

The following figure shows that the WAEs (Edge-WAE1 and Core-WAE1) must reside in an out-of-band network that is separate from the traffic's destination and source. For example, Edge-WAE1 is on a subnet that is separate from the clients (the traffic source), and Core-WAE1 is on a subnet that is separate from the file servers and application servers (the traffic destination). Additionally, you may have to use a tertiary interface (a separate physical interface) or a subinterface to attach a WAE to the router, which redirects traffic to it, in order to avoid an infinite routing loop between the WAE and the router. For more information about this, see Using Tertiary Interfaces or Subinterfaces to Connect WAEs to Routers, on page 25.

Figure 1: Using PBR or WCCP Version 2 for Transparent Redirection of All TCP Traffic to WAEs



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

Table 2: Router Interfaces for WCCP or PBR Traffic Redirection to WAEs

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

This traffic redirection does not use tunneling; the full original quadruple (source IP address, source port number, destination IP address, and destination port number) of the TCP traffic is preserved end to end. The original payload of the TCP traffic is not preserved end to end because the primary function of Cisco WAAS is to accelerate WAN traffic by reducing the data that is transferred across the WAN. This change in payload can potentially impact features on the router that is performing the WCCP or PBR redirection, and that needs to see the actual payload to perform its operation, for example, NBAR. For more information on this topic, see Cisco WAAS and Cisco IOS Interoperability, on page 11.

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

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

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

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

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

By default, IP Protocol 6 is specified for the TCP promiscuous mode service. Consequently, the routers that have been configured to the TCP promiscuous mode service will intercept all the TCP traffic destined for any TCP port to the local WAE. Because the TCP promiscuous mode service is configured on the WAE, the WAE will accept all of the TCP traffic that is transparently redirected to it by specified WCCP routers, for example, Edge-WAE1 will accept all TCP traffic that Edge-Router1 redirects to it. In the branch office, you can intercept packets at the edge LAN and WAN interfaces on the Edge routers and redirect the TCP traffic to the local WAE (the branch WAE). In the data center, you can intercept packets at the core LAN and WAN interfaces on the core routers and redirect the TCP traffic to the local WAE (the data center WAE). For more information, see Configuring WAEs as Promiscuous TCP Devices in a Cisco WAAS Network, on page 25.

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

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

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

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

Configuring WAEs as Promiscuous TCP Devices in a Cisco WAAS Network

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

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

Using Tertiary Interfaces or Subinterfaces to Connect WAEs to Routers

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

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

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

To avoid an infinite routing loop between the router and its local WAE, connect the WAE to the router through a tertiary interface (a separate physical interface) or a subinterface (a different virtual subinterface) from the router's LAN port. By using a tertiary interface or a subinterface to connect a WAE to the router that is performing the PBR or WCCP redirection, the WAE has its own separate processing path that has no Cisco IOS features enabled on it. In addition, this approach simplifies the process of integrating WAEs into an existing network. Because the WAEs are being connected to the routers through a tertiary interface or subinterface that has no Cisco IOS features enabled on it, the Cisco IOS features that are already enabled on your existing Cisco-enabled network elements, for example, Edge-Router1 or Core-Router1, will generally not be affected when you connect WAEs to these routers. For more information about Cisco WAAS and Cisco IOS interoperability, see Cisco WAAS and Cisco IOS Interoperability, on page 11.

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

Access Lists on Routers and WAEs

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

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

This section contains the following topics:

- IP ACLs on WAEs, on page 26
- Interception ACLs on WAEs, on page 27

IP ACLs on WAEs

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

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

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

Interception ACLs on WAEs

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

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

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

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

Cisco WAAS Login Authentication and Authorization

This section contains the following topics:

About Cisco WAAS Login Authentication and Authorization

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

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

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

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

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

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

Cisco WAAS Administrator Accounts

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

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

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

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

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

Logically Grouping Your WAEs

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

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

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

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

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

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

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

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

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

Data Migration Process

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

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

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

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

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

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

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

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