Cisco Wide Area Application Services Quick Configuration Guide

Software Version 4.0.19
March 27, 2009

This document describes how to perform a basic configuration of a Wide Area Application Services (WAAS) network that uses the Web Cache Communication Protocol (WCCP) and has three WAAS devices:

- WAAS Central Manager
- Core Wide Area Application Engine (WAE)
- Edge WAE

The example in this document also shows how to verify that the WAAS application acceleration feature is working properly after you have completed a basic configuration of your WAAS network.

Note If one of the WAE devices that you are configuring is an enhanced network module (NME-WAE) installed in a Cisco access router, you must configure its basic network settings using the access router CLI, not by using the WAAS CLI as described in this document. For details, see the document *Configuring Cisco WAAS Network Modules for Cisco Access Routers*.

Throughout this document, the term WAAS device is used to refer collectively to WAAS Central Managers and WAEs in your network. For detailed command syntax information for any of the CLI commands that are mentioned in this document, see the *Cisco Wide Area Application Services Command Reference*.

This document contains the following sections:

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Autoregistration of WAEs

Autoregistration automatically configures network settings and registers WAEs with WAAS Central Manager. On startup, devices running the WAAS software (with the exception of the WAAS Central Manager itself) automatically discover WAAS Central Manager and register with it. You do not have to do any manual configuration on the device. Once the WAE is registered, you must approve the device and configure it remotely by using the WAAS Central Manager GUI.

In the example configuration provided in this document, the autoregistration feature is intentionally disabled on the WAEs and you use the setup utility to perform the initial configuration of the device. After you complete the initial configuration of the WAE, you use the WAAS CLI to explicitly configure the WAE to register with a specific WAAS Central Manager.

For more information about the autoregistration feature, see the *Cisco Wide Area Application Services Configuration Guide*.

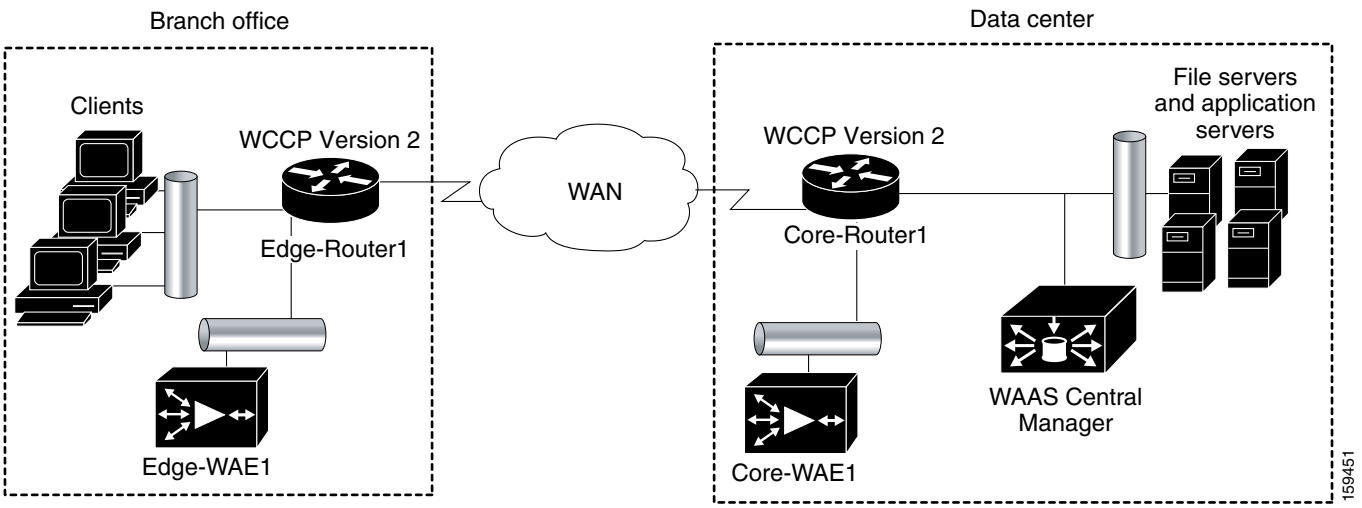
Network Configuration Overview

This section provides an overview of the basic configuration of a WAAS network. It contains the following topics:

Network Configuration Example

The example WAAS network configuration shown in Figure 1 contains one WAAS Central Manager device and two WAEs that will be centrally managed through the WAAS Central Manager device.

Figure 1 WAAS Network Configuration



Note If you are using inline mode with WAEs that have the Cisco WAE Inline Network Adapter installed, you must not enable WCCP. Instead, you position the WAEs directly in the traffic path between the router and the clients or file servers. The WAEs intercept traffic directly through the interfaces on the Cisco WAE Inline Network Adapters and redirection is not needed.

When you install any inlne WAE device, you must follow the cabling requirements described in the "Cabling" section of the "Installing the Cisco WAE Inline Network Adapter" document located on Cisco.com.

Note We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system's ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

WAAS Central Manager must run on a dedicated appliance. You should install WAAS Central Manager on a dedicated appliance that is located in your data center so that the WAAS Central Manager device is in the same physical location as your data center's web, file, and application servers.

Note You cannot install the WAAS Central Manager on a WAE network module (NME-WAE) device.

You should install the Edge WAE in the same branch office as the clients who will be requesting local services (for example, print services) from the Edge WAE.

Summary of the Configuration Process

The following steps summarize the tasks that are required to perform a basic configuration of a WAAS network:

1. Configure the basic network settings and define the primary interface and device mode for each of the WAEs by using the setup utility and the WAAS CLI, beginning with the WAAS Central Manager. Start with the "Configuring the WAAS Central Manager" section on page 5.

   The setup utility includes choosing and enabling an interception method: WCCP or inline. If you choose WCCP, the setup utility prompts you for a list of intercepting routers and enables TCP promiscuous mode on the WAEs.

2. If you are using WCCP interception, configure WCCP Version 2 on the routers as described in the "Configuring WCCP" section on page 11. This step is not required if you are using inline mode and a WAE with the Cisco WAE Inline Network Adapter installed.

3. Activate the WAEs and enable the predefined application definitions by using the WAAS Central Manager GUI. See the "Activating the WAEs and Enabling Application Acceleration Policies" section on page 17.

4. Verify that the WAAS application acceleration is working properly for HTTP. See the "Verifying Application Acceleration" section on page 19.

5. Change the password for the predefined superuser account. See the "Changing the Administrator Password" section on page 20.

For detailed command syntax information for any of the CLI commands that are mentioned in this document, see the *Cisco Wide Area Application Services Command Reference*.

Checklist for Configuring a WAAS Network

Table 1 specifies the different parameters and data needed to set up and configure the WAAS network. For your convenience, you can enter your values in the table and refer back to it when configuring the WAAS network.

Table 1 Checklist of WAAS Network System Parameters

Parameter	Data Center Values for WAAS Central Manager	Data Center Values for the Core WAE	Branch Office Values for the Edge WAE
Interface speed			
Duplex mode			
IP address			
Subnet mask			
Default gateway			
DNS server 1			
DNS server 2			
DNS domain			
WINS server			
WAAS device (hostname)			
Windows domain controller			
Windows file server(s)			
UNIX file server(s)			
Windows domain			
IP addresses of routers intercepting traffic with WCCP			

Configuring the WAAS Network

To perform a basic configuration of a WAAS network that will include one WAAS Central Manager and two WAEs, follow the procedures in the order that they are presented in the following sections:

- Configuring the WAAS Central Manager, page 5
- Configuring the Core WAE, page 7
- Configuring the Edge WAE, page 9
- Configuring WCCP, page 11
- Activating the WAEs and Enabling Application Acceleration Policies, page 17
- Verifying Application Acceleration, page 19

- Changing the Administrator Password, page 20

Configuring the WAAS Central Manager

To install and configure the WAAS Central Manager device, follow these steps:

Step 1 In the data center, unpack and connect the first WAAS device that you want to configure as the WAAS Central Manager device. You must set the port to which the WAE is connected to full duplex. For hardware installation instructions, refer to the hardware installation guide for the WAAS device.

Step 2 Power up the first WAAS device in the data center and open a console connection to configure the basic device network settings (see Table 1) for the WAE.

Note If you are connecting to the WAAS device using a PC as the console, the PC must have terminal emulation software installed. The terminal emulation software should be configured with the following parameters: 9600 baud, 8 data bits, no parity bits, and 1 stop bit.

You must use a console connection rather than a Telnet session for the initial configuration of these basic device network settings on the WAE. Once you have used a console connection to define the device network settings, you can use a Telnet session for subsequent CLI sessions. By default, the Telnet service is enabled on a WAAS device.

Step 3 When a WAAS device starts up, 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. When prompted, enter **y**.

The configuration prompt waits several seconds before proceeding with the WAE start up sequence.

Note If you do not enter **y** in time to enter basic configuration, you will need to log into the WAAS device through the terminal console and run the **setup** EXEC CLI command to manually invoke the setup utility.

Step 4 Enter the required information as prompted by the setup utility. For example, choose central-manager as the device mode that you want to configure on the WAAS device.

```
Please choose the device mode of the WAE
1.central-manager
2.application-accelerator
3.replication-accelerator
4.Skip device mode configuration
Enter your choice: 1

Please choose the primary interface:
1: GigabitEthernet 1/0
2: GigabitEthernet 2/0

Enter choice: 1
...
```

If you have Dynamic Host Control Protocol enabled in your network, enable DHCP on the WAAS device interface by answering yes (**y**) to the following question. If you do not have DHCP enabled in your network, answer no (**n**). No is the default.

```
Would you like to enable DHCP on this interface (y/n) [n]:y
```

...
Continue to answer the questions displayed in the setup utility.

When you see the prompt to configure a Network Time Protocol (NTP) server, we recommend that you answer yes (**y**), because clock synchronization between the WAEs in a WAAS network is important.

```
Would you like to configure NTP server (y/n) [n] :y

Please enter the IP address or domain name of the NTP server: 172.19.228.200
```

Also, configure the time zone of the device. Separate questions prompt you to enter the time zone name, the number of hours offset from UTC (rounded down to the nearest whole number), and the number of minutes of any partial hour of offset. For example, if your time zone offset is +5:30, then you would answer **5** for the hours offset and **30** for the minutes offset.

```
Would you like to configure the timezone (y/n) [y] :y

Please enter the name of the timezone : PDT

Please enter the hours offset from UTC <-23 to +23> : -8

Please enter the minutes offset from UTC : 0
```

Step 5 You see a summary of the information that you entered. Write down the IP address for future reference. You will need the IP address of the WAAS Central Manager device to launch the WAAS Central Manager GUI, which you will use later in the "Activating the WAEs and Enabling Application Acceleration Policies" section on page 17.

Accept the configuration when prompted. If you answer no (**n**), you can reenter and change any values (previous answers are used as the defaults).

```
Based on the input, the following CLIs will be configured:

        cms enable
        interface GigabitEthernet 1/0
         ip address 10.10.10.10 255.255.255.0
         autosense
         exit
        ip default-gateway 10.10.10.1
        ip name-server 172.19.228.233
        ip domain-name example.com
        hostname waas-cm
        ntp server 172.19.228.200
        clock timezone PDT -8 0

Do you accept these configs (y/n) [y]: y
```

Step 6 Apply the configuration when prompted. Once you apply the configuration, the device is visible on the network and it can be pinged.

```
Would you like to apply the configurations (y/n) [y]:y
```

Step 7 After specifying the basic network parameters for the designated WAAS Central Manager, save the configuration, and then reload the system so that the new configuration will take effect.

```
waas-cm# copy run start
waas-cm# reload
Proceed with reload?[confirm] y
Shutting down all services, will Reload requested by CLI@ttyS0.
Restarting system.
```

The system reboots and the WAAS Central Manager configuration that you just configured is loaded on the WAAS device named waas-cm, which has now been designated as a WAAS Central Manager.

Step 8 When prompted, enter the administrator username and password and press **Enter**.

```
Username: admin
Password:
System Initialization Finished.
```

Step 9 Specify that this device is to function as the primary WAAS Central Manager.

```
waas-cm# config
waas-cm(config)# central-manager role primary
```

Step 10 Create and initialize the management database and enable the management services on this WAAS Central Manager.

```
waas-cm(config)# cms enable
```

The following message appears:

```
Generating new RPC certificate/key pair
Restarting RPC services

Creating database backup file emerg-debug-db-01-25-2006-15-31.dump
Registering Wide Area Central Manager...
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 Wide Area Central Manager UI.
management services enabled
```

Step 11 Save the configuration on this WAAS Central Manager.

```
waas-cm(config)# exit
waas-cm# copy run start
```

The initial configuration of the WAAS Central Manager is completed. The next step is to initially configure and register the other two WAAS devices (the Core WAE and the Edge WAE) with this WAAS Central Manager. See the next two sections for details.

Configuring the Core WAE

To install and configure the WAAS Core WAE device, and register it with the WAAS Central Manager, follow these steps:

Step 1 In the data center, unpack and connect the second WAAS device that you want to configure as the Core WAE in the WAAS network. You must set the port to which the WAE is connected to full duplex. For hardware installation instructions, refer to the hardware installation guide for the WAE.

Note We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system's ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

Step 2 Power up the designated Core WAE and open a console connection.

Step 3 When a WAAS device starts up, you are prompted to run the first-time setup utility (enter basic configuration), which you use to set up the basic network parameters for the device. When prompted, enter **y**.

The configuration prompt waits several seconds before proceeding with the WAAS device start up sequence.

Note If you do not enter **y** in time to enter basic configuration, you will need to log in to the WAAS device through the terminal console and run the **setup** EXEC CLI command to manually invoke the setup utility. The username is admin and the password is default.

Step 4 Enter the required information as prompted by the setup utility (see Table 1). For example, choose application-accelerator as the device mode that you want to configure on the WAAS device.

```
Please choose the device mode of the WAE
1.central-manager
2.application-accelerator
3.replication-accelerator
4.Skip device mode configuration
Enter your choice: 2
...
```

Specify the IP address or hostname of the WAAS Central Manager that Core-WAE1 should register with. For example, specify the IP address of the WAAS Central Manager that you configured earlier in the "Configuring the WAAS Central Manager" section on page 5.

```
Please enter the IP address of the Central Manager: 10.10.10.10
```

Note If DNS is supported in your environment, we recommend that you specify the WAAS Central Manager's fully qualified hostname (for example, waas-cm.abc.com) instead of its IP address. By using the hostname, you can change the WAAS Central Manager's IP address in the future and you do not need to unregister and reregister all of the WAEs.You only need to change the WAAS Central Manager's IP address in the DNS table for the WAEs to remain registered with the same WAAS Central Manager.

Step 5 Continue to answer the questions displayed in the setup utility until your basic configuration is complete on the Core WAE. If you configured WCCP as the interception method, the setup utility displays a set of example router configurations for your convenience. These are the same configurations described in the "Configuring WCCP on the Core Router" section on page 12.

Step 6 When finished, you see a summary of the information that you entered. Accept the configuration when prompted, and then apply the configuration when prompted. Once you apply the changes, the device is visible on the network, and it can be pinged.

Step 7 Save the configuration on Core-WAE1.

```
Core-WAE1# copy run start
```

Step 8 Check the current running WAAS configuration on Core-WAE1.

```
Core-WAE1# show running-config
! WAAS version 4.0.0
!
device mode application-accelerator
!
!
hostname Core-WAE1
!
```

```
!
clock timezone America/New_York -5 0
!
!
ip domain-name abc.local
!
!
interface GigabitEthernet 1/0
 ip address 2.2.2.100 255.255.255.0
 no autosense
 bandwidth 100
 full-duplex
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
ip default-gateway 2.2.2.1
!
ip name-server 172.19.228.233
ip name-server 10.10.10.100
!
!
no wccp slow-start enable
!
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
!
!
authentication login local enable primary
authentication configuration local enable primary
!
!
central-manager address 10.10.10.10
cms enable
!
! End of WAAS configuration
```

The initial configuration of the Core WAE is completed. The next step is to initially configure and register the designated Edge WAE with the WAAS Central Manager device. See the next section for details.

Configuring the Edge WAE

To install and configure the WAAS Edge WAE device, and register it with the WAAS Central Manager, follow these steps:

Step 1 In the branch office, unpack and connect the third WAAS device that you want to configure as the Edge WAE in the WAAS network. You must set the port to which the WAE is connected to full duplex. For hardware installation instructions, refer to the hardware installation guide for the WAE.

Note We strongly recommend that you do not use half-duplex connections on the WAE or on routers, switches, or other devices. Use of half-duplex impedes the system's ability to improve performance and should not be used. Double-check each Cisco WAE interface as well as the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full-duplex is configured.

Step 2 Power up the designated Core WAE in the branch office and open a console connection.

Step 3 When a WAAS device starts up, you are prompted to run the first-time setup utility (enter basic configuration), which you use to set up the basic network parameters for the WAE. When prompted, enter **y**.

The configuration prompt waits several seconds before proceeding with the WAAS device start up sequence.

Note If you do not enter **y** in time to enter basic configuration, you will need to log in to the WAAS device through the terminal console and run the **setup** EXEC CLI command to manually invoke the setup utility. The username is admin and the password is *default*.

Step 4 Enter the required information as prompted by the setup utility (see Table 1). For example, choose Application accelerator as the device mode that you want to configure on the WAAS device.

```
Please choose the device mode of the WAE
1.central-manager
2.application-accelerator
3.replication-accelerator
4.Skip device mode configuration
Enter your choice: 2
...
```

Specify the IP address or hostname of the WAAS Central Manager that Edge-WAE1 should register with. For example, specify the IP address of the WAAS Central Manager that you configured earlier in the "Configuring the WAAS Central Manager" section on page 5.

```
Please enter the IP address of the central-manager: 10.10.10.10
```

Note If DNS is supported in your environment, we recommend that you specify the WAAS Central Manager's fully qualified hostname (for example, waas-cm.abc.com) instead of its IP address. By using the hostname, you can change the WAAS Central Manager's IP address in the future and you do not need to unregister and reregister all of the WAEs.You only need to change the WAAS Central Manager's IP address in the DNS table for the WAEs to remain registered with the same WAAS Central Manager.

Step 5 Continue to answer the questions displayed in the setup utility until your basic configuration is complete on the Edge WAE. If you configured WCCP as the interception method, the setup utility displays a set of example router configurations for your convenience. These are the same configurations described in the "Configuring WCCP on the Branch Router" section on page 14.

Step 6 When finished, you see a summary of the information that you entered. Accept the configuration when prompted, and then apply the configuration when prompted. Once you apply the changes, the device is visible on the network, and it can be pinged.

Step 7 Save the configuration on Edge-WAE1.

```
Edge-WAE1# copy run start
```

Step 8 Check the current running configuration for Edge-WAE1.

```
Edge-WAE1# show running-config

! WAAS version 4.0.19
!
device mode application-accelerator
!
!
hostname Edge-WAE1
!
!
ip domain-name abc.local
!
!
interface GigabitEthernet 1/0
 ip address 1.1.1.100 255.255.255.0
 no autosense
 bandwidth 100
 full-duplex
 exit
interface GigabitEthernet 2/0
 shutdown
 exit
!
ip default-gateway 1.1.1.1
!
ip name-server 10.10.10.100
!
!
no wccp slow-start enable
!
!
username admin password 1 bVmDmMMmZAPjY
username admin privilege 15
!
!
authentication login local enable primary
authentication configuration local enable primary
!
!
central-manager address 10.10.10.10
cms enable
!
! End of WAAS configuration
```

The initial configuration of the Edge WAE is completed. The next step is to configure WCCP. See the next section for details.

Configuring WCCP

Note Do not configure WCCP if you are using inline mode and a WAE with the Cisco WAE Inline Network Adapter installed, because WCCP will prevent inline mode from operating. With inline mode, traffic is directly intercepted and redirection is unnecessary.

WCCP provides the method to transparently redirect client requests to a WAE for processing. To configure basic WCCP, you must enable the WCCP service on at least one router in your network and on your WAE. It is not necessary to configure all of the available WCCP features or services to get your WAE up and running. In this configuration example, because there is a Core WAE and an Edge WAE in the WAAS network, you must configure WCCP Version 2 on four devices, as follows:

- Configuring WCCP on the Core Router, page 12
- Configuring WCCP on the Core WAE, page 13
- Configuring WCCP on the Branch Router, page 14
- Configuring WCCP on the Edge WAE, page 16

Note You must configure these devices to use WCCP Version 2 instead of WCCP Version 1 because WCCP Version 1 supports web traffic (port 80) only. For more information on WCCP configuration, see the *Cisco Wide Area Application Services Configuration Guide*.

Configuring WCCP on the Core Router

To complete a basic WCCP configuration on the router (Core-Router1) in the data center, follow these steps:

Step 1 Log on to Core-Router1 and enter global configuration mode.

```
Core-Router1 configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Core-Router1(config)#
```

Step 2 Enable WCCP Version 2 and WCCP services 61 and 62 (TCP promiscuous mode) on Core-Router1.

```
Core-Router1(config)# ip wccp version 2
Core-Router1(config)# ip wccp 61
Core-Router1(config)# ip wccp 62
```

Step 3 On Core-Router1, configure the LAN interface for redirection. This interface is where traffic will be intercepted from when leaving the data center network toward the WAN.

```
Core-Router1(config)# interface fa1/0.40
Core-Router1(config-subif)#
```

Step 4 Enable WCCP service 61 on the inbound direction of fa1/0.40.

```
Core-Router1(config-subif)# ip wccp 61 redirect in
Core-Router1(config-subif)# exit
```

Step 5 Configure the WAN interface for redirection. This interface is where traffic will be intercepted from when entering the data center network from the WAN.

```
Core-Router1(config)# interface serial0
```

Step 6 Enable WCCP service 62 on the inbound direction of serial0.

```
Core-Router1(config-if)# ip wccp 62 redirect in
Core-Router1(config-if)# exit
```

Step 7 To avoid redirection loops, configure the subinterface where Core-WAE1 will connect to Core-Router1. To avoid a routing loop, Core-WAE1 must not be attached to the same segment (subnet) as the interface on Core-Router1 that is performing the redirection. Make sure that you have a tertiary interface (a separate physical interface) or a subinterface (off the router's LAN port) from which Core-WAE1 connects. In the following example, a subinterface is being used:

```
Core-Router1(config)# interface fa1/0.41
```

Step 8 After you create the subinterface, enter the **ip wccp redirect exclude in** command to specify that Core-Router1 should not repeatedly redirect the same traffic to the local WAE, Core-WAE1.

```
Core-Router1(config-subif)# ip wccp redirect exclude in
```

Step 9 Exit subinterface configuration mode.

```
Core-Router1(config-subif)# exit
Core-Router1(config)
```

Step 10 Enable Cisco Express Forwarding (CEF) on Core-Router1.

```
Core-Router1(config)# ip cef
Core-Router1(config)# end
Core-Router1#
```

Note CEF is not required but it is recommend for improved performance. WCCP can use IP CEF if CEF is enabled on the router.

Step 11 Save the configuration changes that you just made by writing the running configuration to nonvolatile memory.

```
Core-Router1# write memory
Building configuration...
Core-Router1#
```

Step 12 Verify the new configuration for Core-Router1.

```
Core-Router1# show running-configuration
```

The configuration of WCCP on the core router is completed. The next step is to configure WCCP on the Core WAE. See the next section for details.

Configuring WCCP on the Core WAE

The setup utility previously prompted you to choose WCCP as the interception method, and if you did so, it prompted you for a list of intercepting routers. If you configured WCCP with the setup utility, you can skip this section and proceed to the "Configuring WCCP on the Branch Router" section on page 14.

If you did not configure WCCP by using the setup utility, follow these steps to complete a basic WCCP configuration on the data center's Core WAE (Core-WAE1), follow these steps:

Step 1 Log on to Core-WAE1 and enter global configuration mode.

```
Core-WAE1# configure terminal
Core-WAE1(config)#
```

Step 2 Enable WCCP Version 2 on Core-WAE1.

```
Core-WAE1(config)# wccp version 2
Core-WAE1(config)#
```

Step 3 Configure a WCCP router list for the TCP promiscuous mode service (WCCP services 61 and 62). The following example shows how to configure router list 1 for Core-Router1 that has an IP address of 2.2.2.1:

```
Core-WAE1(config)# wccp router-list 1 2.2.2.1
Core-WAE1(config)#
```

Note To create a router list on a WAE, use the **wccp router-list** global configuration command. Enter the IP address of every WCCP-enabled router that will support a particular WCCP service (for example, the TCP promiscuous mode service) for the WAE. If different routers will be used for different WCCP services, you must create more than one router list. Each router list command can contain up to six routers. Multiple router list commands may be used for the same list to specify up to 32 routers. A router list must be contain at least one IP address.

Step 4 On Core-WAE1, turn on the TCP promiscuous mode service and associate this WCCP service with the WCCP router list that you just created (router list number 1). The routers in the list are informed that Core-WAE1 is accepting TCP promiscuous mode service requests.

```
Core-WAE1(config)# wccp tcp-promiscuous router-list-num 1
WCCP configuration for TCP Promiscuous service 61 succeeded.
WCCP configuration for TCP Promiscuous service 62 succeeded.
Please remember to configure WCCP service 61 and 62 on the corresponding router.
```

Step 5 Exit global configuration mode.

```
Core-WAE1(config)# exit
Core-WAE1#
```

Step 6 Save the configuration changes that you just made by writing the running configuration to nonvolatile memory.

```
Core-WAE1# write memory
Core-WAE1#
```

Step 7 Verify the new configuration for Core-WAE1.

```
Core-WAE1# show running-configuration
```

The configuration of WCCP on the Core WAE is completed. The next step is to configure WCCP on the branch router. See the next section for details.

Configuring WCCP on the Branch Router

To complete a basic WCCP configuration on the router (Edge-Router1) in the branch office, follow these steps:

Step 1 Log on to Edge-Router1 and enter global configuration mode.

```
Edge-Router1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Edge-Router1(config)#
```

Step 2 Enable WCCP Version 2 and WCCP services 61 and 62 (TCP promiscuous mode) on Edge-Router1.

```
Edge-Router1(config)# ip wccp version 2
Edge-Router1(config)# ip wccp 61
Edge-Router1(config)# ip wccp 62
```

Step 3 On Edge-Router1, configure the LAN interface for redirection. This interface is where traffic will be intercepted from when leaving the branch office network toward the WAN.

```
Edge-Router1(config)# interface fa0/0.10
Edge-Router1(config-subif)#
```

Step 4 Enable WCCP service 61 on the inbound direction of fa0/0.10.

```
Edge-Router1(config-subif)# ip wccp 61 redirect in
Edge-Router1(config-subif)# exit
```

Step 5 Configure the WAN interface for redirection. This interface is where traffic will be intercepted from when entering the branch office network from the WAN.

```
Edge-Router1(config)# interface serial0
```

Step 6 Enable WCCP service 62 on the inbound direction of serial0.

```
Edge-Router1(config-if)# ip wccp 62 redirect in
Edge-Router1(config-if)# exit
```

Step 7 To avoid redirection loops, configure the subinterface where Edge-WAE1 will connect to Edge-Router1. To avoid a routing loop, Edge-WAE1 must not be attached to the same segment as Edge-Router1's interface that is performing the redirection. Make sure that you have a tertiary interface or a subinterface (off the router's LAN port) from which Edge-WAE1 connects. In the following example, a subinterface is being used:

```
Edge-Router1(config)# interface fa0/0.11
```

Step 8 After you create the subinterface, enter the **ip wccp redirect exclude in** command to specify that Edge-Router1 should not repeatedly redirect the same traffic to the local WAE, Edge-WAE1.

```
Core-Router1(config-subif)# ip wccp redirect exclude in
```

Step 9 Exit subinterface configuration mode.

```
Edge-Router1(config-subif)# exit
Edge-Router1(config)#
```

Step 10 Enable CEF on Edge-Router1.

```
Edge-Router1(config)# ip cef
Edge-Router1(config)# end
Edge-Router1#
```

Note CEF is not required but it is recommend for improved performance. WCCP can use IP CEF if CEF is enabled on the router.

Step 11 Save the configuration changes that you just made by writing the running configuration to nonvolatile memory.

```
Edge-Router1# write memory
Building configuration...
Edge-Router1#
```

Step 12 Verify the new configuration for Edge-Router1.

```
Edge-Router1# show running-configuration
```

The configuration of WCCP on the branch router is completed. The next step is to configure WCCP on the Edge WAE. See the next section for details.

Configuring WCCP on the Edge WAE

The setup utility previously prompted you to choose WCCP as the interception method, and if you did so, it prompted you for a list of intercepting routers. If you configured WCCP with the setup utility, you can skip this section and proceed to the "Activating the WAEs and Enabling Application Acceleration Policies" section on page 17.

If you did not configure WCCP by using the setup utility, follow these steps to complete a basic WCCP configuration on the Edge WAE (Edge-WAE1) in the branch office, follow these steps:

Step 1 Log on to Edge-WAE1 and enter global configuration mode.

```
Edge-WAE1# configure terminal
Edge-WAE1(config)#
```

Step 2 Enable WCCP Version 2 on Edge-WAE1.

```
Edge-WAE1(config)# wccp version 2
Edge-WAE1(config)#
```

Step 3 Configure a WCCP router list for the TCP promiscuous mode service (WCCP services 61 and 62). The following example shows router list 1 being created for Edge-Router1 that has an IP address of 1.1.1.1:

```
Edge-WAE1(config)# wccp router-list 1 1.1.1.1
Edge-WAE1(config)#
```

Step 4 On Edge-WAE1, turn on the TCP promiscuous mode service and associate this WCCP service with the WCCP router list that you just created (router list number 1). The routers in the list are informed that Edge-WAE1 is accepting TCP promiscuous mode service requests.

```
Edge-WAE1(config)# wccp tcp-promiscuous router-list-num 1
WCCP configuration for TCP Promiscuous service 61 succeeded.
WCCP configuration for TCP Promiscuous service 62 succeeded.
Please remember to configure WCCP service 61 and 62 on the corresponding router.
```

Step 5 Exit global configuration mode.

```
Edge-WAE1(config)# exit
Edge-WAE1#
```

Step 6 Save the configuration changes that you just made by writing the running configuration to nonvolatile memory.

```
Edge-WAE1# write memory
Edge-WAE1#
```

Step 7 Verify the new configuration for Edge-WAE1.

```
Edge-WAE1# show running-configuration
```

The configuration of WCCP on the Edge WAE is completed. The next step is to activate the WAEs and enable application acceleration policies. See the next section for details.

Activating the WAEs and Enabling Application Acceleration Policies

After the WAE designated as the WAAS Central Manager has been deployed, you can use the WAAS Central Manager GUI to complete the basic configuration of the WAAS network. You can also use the WAAS Central Manager GUI to centrally manage and monitor the geographically dispersed WAEs in the WAAS network.

To access the WAAS Central Manager GUI and complete the initial configuration of the WAAS network, follow these steps:

Step 1 Log in to the WAAS Central Manager GUI, as follows:

a. Enter the following URL in your web browser:

https://*IP_address_of_WAAS Central_Manager***:8443**

For example:

https://10.10.10.10:8443

or

https://*hostname_of_WAAS_Central_Manager***:8443**

For example:

https://waas-cm:8443

Note When you access the WAAS Central Manager GUI, make sure that you use HTTPS instead of HTTP to ensure that data is securely transmitted from the WAAS Central Manager to your web browser.

b. After the Security Alert window appears, click **Yes** to accept the security certificate.

c. After the Login window appears, enter the default username (admin) and the default password (default) for the predefined superuser account and click the **Login** button.

The System Home window of the WAAS Central Manager GUI appears in your browser and indicates the number of WAEs that are in the current configuration of this Central Manager.

Step 2 Activate the Core and Edge WAEs, as follows:

Note For security purposes, you need to approve all WAEs that are being added to the WAAS network. This security feature prevents unauthorized devices from joining the WAAS network.

a. In the WAAS Central Manager GUI, choose **Devices > Devices**.

The WAAS Central Manager window lists three WAAS devices:

– The WAAS Central Manager (waas-cm) in the data center that is the only WAAS device that is currently online. The WAAS Central Manager window indicates that this device is functioning as the primary WAAS Central Manager for this WAAS network.

- The Core WAE (Core-WAE1) in the data center that is recognized by the WAAS Central Manager but is currently inactive.
- The Edge WAE (Edge-WAE1) in the branch office that is recognized by the WAAS Central Manager but is currently inactive.

Note If the WAAS Central Manager window does not list the inactive WAEs, click the **View All Devices** icon in the taskbar. The WAAS Central Manager window is refreshed and should now list the inactive WAEs.

b. In the taskbar, click the **Activate all inactive WAEs** icon to activate the two inactive WAEs (Core-WAE1 and the Edge-WAE1).

The Activate all inactive WAE window appears. By default, the **Create a new location for each inactive WAE** option is selected and a default location for the inactive WAEs will be created and the inactive WAEs are assigned to that default location. You can create locations as part of the initial configuration, or use default locations to complete the initial configuration and then modify the default locations at a later time. In this configuration example, a default location is used to complete the initial configuration of the WAAS network. For information about how to create and modify locations, see "Working with Device Locations" in the *Cisco Wide Area Application Services Configuration Guide*.

c. Click **Submit**.

The current state of Core-WAE1 and Edge-WAE1 is now listed as pending instead of inactive.

Step 3 Enable the predefined application policies and classifications on all devices, as follows:

a. Choose **Devices > Device Groups**.

a. Click the **Edit** icon next to AllDevicesGroup. The Modifying Device Group, *AllDevicesGroup* window appears.

b. In the taskbar, click the **Restore default Application policy settings** icon.

c. When a dialog box appears prompting you to confirm that you want to restore the default application policy settings, click **OK**.

d. To save the changes, click **Submit**.

e. To view the application policy settings that are currently applied to all of the devices in the device group, choose **Acceleration > Policies > Definitions** in the Contents pane.

f. To view the application classifiers that are currently applied to your devices, choose **Services > Acceleration > Classifiers**. The classifier usage summary report appears. It lists each classifier that is defined, and the number of devices on which it is configured.

- To see a report of the devices and device groups on which the classifier is configured, click the **View** icon next to a classifier.
- To see the application policies that are defined on a device or device group, click the **Edit** icon next to the device.

The initial configuration of the WAAS network is completed. The next step is to verify that application acceleration is working correctly. See the next section for details.

The WAAS software comes with a set of predefined application policies that help your WAEs classify and optimize some of the most common application traffic. This set of default application policies are for applications that use well-known port numbers. For a list of the predefined application definition policies, see the *Cisco Wide Area Application Services Configuration Guide*.

You can use the WAAS Central Manager GUI to modify these predefined application policies, create new ones, and then centrally distribute these policies to one or more devices in the WAAS network. You can also modify the predefined set of application policies or create new ones through the WAAS CLI. However, we strongly recommend that you use the WAAS Central Manager GUI to perform this task in order to significantly reduce the complexity of this task and to increase the level of consistency. (For CLI command syntax information, see the *Cisco Wide Area Application Services Command Reference*.)

Verifying Application Acceleration

Verify that the WAAS application acceleration feature is working properly for one of the predefined applications. To verify that application acceleration is working properly for the HTTP application, follow these steps:

Step 1 Use Remote Desktop or a similar application to access a client desktop (Client A) at the branch office.

Step 2 From the Client A browser, enter the URL of a web page that resides on a server (Server A) that is located in the data center. The web page should contain links to large files (for example, Microsoft Word or Powerpoint files) that you can download from that page.

Note Make sure that you use HTTP instead of HTTPS to access the web page because you want to test whether application acceleration is working properly for HTTP.

The requested web page appears in Client A's browser.

Step 3 Click one of the links in the web page to download a file.

By clicking a link to download a file to Client A's desktop, this request involves an active transfer that will allow you to verify whether application acceleration is occurring between this client and server for an HTTP request that involves an active transfer.

Step 4 When you are prompted whether you want to open or save this file, click **Save** and specify the location on the client A desktop that you want to save this file (for example, save to a folder on the local disk drive). A dialog box appears indicating that the specified file is being downloaded and saved to the desktop.

Step 5 When the download is completed, the dialog box indicates the file has been downloaded to the specified location and shows the transfer rate of the download. When the dialog box prompts whether you want to open the downloaded file, click **Close** to close the dialog box.

Step 6 From the same web page, click the same download link to download the same file to Client A's desktop.

This second time the file is downloaded in less time and the transfer rate is faster. The significant decrease in the time it took to download the same file to the same desktop a second time indicates that the WAAS application acceleration feature is working properly for HTTP (for active transfer requests that are using HTTP between Client A and Server A).

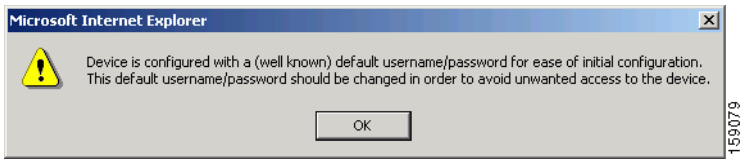
Note You can also verify whether a WAE is intercepting, optimizing, and compressing data by using such CLI commands as the **show statistics tfo savings** and **show statistics dre** EXEC commands. These commands are only supported in application-acceleration device mode; you must run these commands from a CLI session on the WAE. For more information about these CLI commands, see the *Cisco Wide Area Application Services Command Reference*.

Changing the Administrator Password

After you have initially configured your 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 WAAS device.

If the predefined password for this superuser account has not been changed on a WAAS Central Manager, the following dialog box is displayed each time that you log in to the WAAS Central Manager GUI using this superuser account. (See Figure 2.)

Figure 2 Message Indicating the Predefined Password for the Superuser Account Should Be Changed



If you have not changed the predefined password for this superuser account, the console will also display the following message each time that you use this superuser account to log in to the WAAS CLI on any WAAS device:

```
Device is configured with a (well known) default username/password
for ease of initial configuration. This default username/password
should be changed in order to avoid unwanted access to the device.

System Initialization Finished.
waas-cm#
```

To change the password for the superuser account across all WAE devices registered to the Central Manager, follow these steps:

Step 1 Log in to the WAAS Central Manager GUI with the admin account, if you are not already logged in.

Step 2 From the WAAS Central Manager GUI, choose **System > Password**.

The Changing Password for User Account window appears.

Step 3 In the New Password field, enter the new password. Passwords are case sensitive.

Step 4 In the Confirm New Password field, reenter the password for confirmation.

Step 5 Click **Submit**.

The message “Changes Submitted” appears at the bottom of the window confirming that your password has been changed. This password change is implemented on all registered WAEs.

Clock synchronization between the WAEs in a WAAS network is important. On each WAE, be sure to set up a Network Time Protocol (NTP) server to keep the clocks synchronized. The setup utility asks you to configure a NTP server, and you should configure one and your time zone when prompted. For information on setting up an NTP server, see the chapter, "Configuring Other System Settings" in the *Cisco Wide Area Application Services Configuration Guide*.

To set the clock manually, use the **clock** EXEC CLI command on each WAE. For details, see the *Cisco Wide Area Application Services Command Reference*.

After you initially configure your WAAS network for application acceleration, you can perform other WAAS administrative tasks. For details, see the *Cisco Wide Area Application Services Configuration Guide*.

Related Documentation

For additional information on the Cisco WAAS software, see the following documentation:

- *Release Note for Cisco Wide Area Application Services*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services Quick Configuration Guide* (this manual)
- *Cisco Wide Area Application Services Configuration Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Wide Area Application Engine 511 and 611 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 512 and 612 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7326 Hardware Installation Guide*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Cisco Network Modules Hardware Installation Guide*
- *Installing the Cisco WAE Inline Network Adapter*
- *Cisco Wide Area Application Services Online Help*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.