Welcome to **Cisco DocWiki**. We encourage registered Cisco.com users to contribute to this wiki to collaborate on Cisco product documentation. You do not need to log in to read the text. However, you must log in to edit the text. Select the "edit" tab to edit an article or select the "discussion" tab to submit questions or comments about documentation content.

See Terms of Use and About DocWiki for more information about Cisco DocWiki.

Click here to return to the Cisco WAAS documentation on www.cisco.com.

Contents

Cisco WAAS Quick Configuration Guide

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

- WAAS Central Manager
- Data Center Wide Area Application Engine (WAE)
- Branch WAE

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.

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:

- Network Configuration Overview
- Configuring the WAAS Network
- Related Documentation
- Obtaining Documentation and Submitting a Service Request

Network Configuration Overview

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

- Network Configuration Example
- Summary of the Configuration Process
- Checklist for Configuring a WAAS Network

Network Configuration Example

The example WAAS network configuration shown in Figure 1: WAAS Network Configuration contains one WAAS Central Manager device and two WAEs that will be centrally managed through the WAAS Central Manager device. The WAEs contain Cisco WAE Inline Network Adapter cards and are deployed inline between the WAN routers and the clients or servers.

Figure 1 WAAS Network Configuration
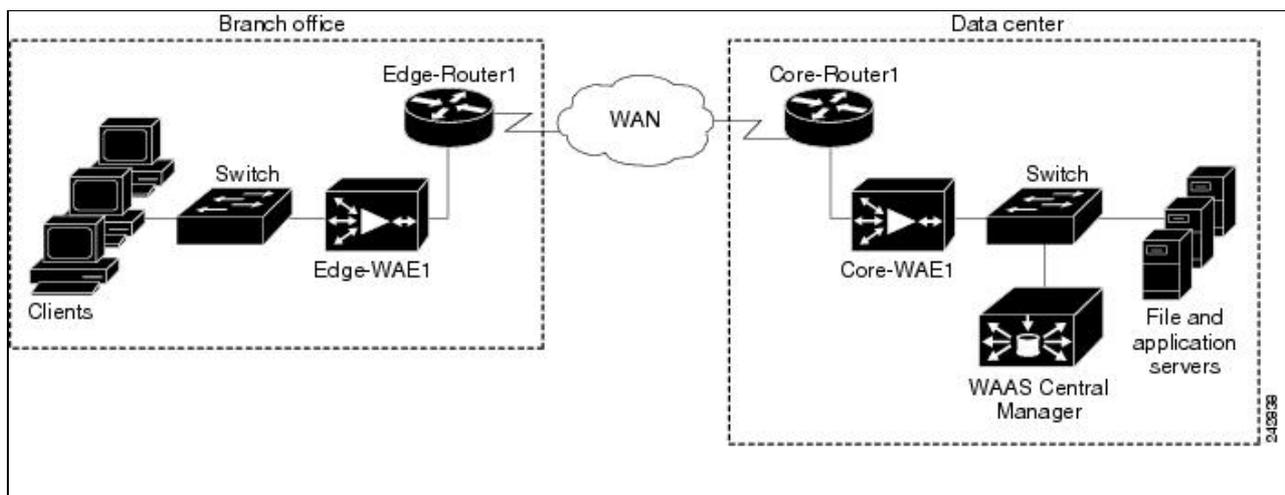
Note: Position the WAEs directly in the traffic path between the router and the clients or file servers. The

WAEs intercept traffic directly through the interfaces on the Cisco WAE Inline Network Adapters and redirection is not needed. When you install any inline 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. Check each Cisco WAE interface and the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full duplex is configured.

The WAAS Central Manager must run on a dedicated appliance. You should install the 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.

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. See the Configuring the WAAS Central Manager.

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

2. (Optional) If you are using WCCP interception, configure WCCP Version 2 on the routers as described in the Configuring WCCP. This step is not required if you are using inline mode and WAEs with the Cisco WAE Inline Network Adapter installed.

3. Access the WAAS Central Manager GUI to manage and monitor your WAAS network. See the Accessing the WAAS Central Manager GUI.

4. Verify that the WAAS application acceleration is working properly. See the Verifying Application Acceleration.

5. Change the password for the predefined superuser account. See the Changing the Administrator Password.

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.*

Figure 1 WAAS Network Configuration   3

Checklist for Configuring a WAAS Network

<u>Table 1: Checklist of WAAS Network System Parameters</u> 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	WAAS Central Manager Values	Data Center WAE Values	Branch Office WAE Values
Interface speed			
Duplex mode			
IP address			
Subnet mask			
Default gateway			
DNS server 1			
DNS server 2			
DNS domain			
WAAS device (hostname)			
Windows domain			
IP addresses of routers intercepting traffic with WCCP			
NTP server (optional)			
Time zone (optional)			

Configuring the WAAS Network

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

- <u>Configuring the WAAS Central Manager</u>
- <u>Configuring the WAEs for Inline Interception</u>
- <u>Configuring WCCP</u>
- <u>Accessing the WAAS Central Manager GUI</u>
- <u>Verifying Application Acceleration</u>
- <u>Changing the Administrator Password</u>

Configuring the WAAS Central Manager

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

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, see the hardware installation guide for the WAAS device.

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: Checklist of WAAS Network System Parameters) 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.

3. When a WAAS device starts up, you are prompted to run the first-time setup utility, which you use to set up the basic configuration for the device. When prompted, press **Enter** and then enter the administrator password, which is default.

> The configuration prompt waits several seconds before proceeding with the WAE setup sequence.

> If you want to quit the setup utility, you can press Esc at any time.

> **Note:** If you do not press **Enter** in time to enter the 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. When you log in, the username is admin and the password is default.

4. Enter **n** at the first prompt to change the default settings. You must change the defaults to configure a WAAS Central Manager.

5. 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.

```
Step 1:

Configure WAAS Settings

------------------------

Select device mode :

1.application-accelerator

2.central-manager

Enter your choice [1]: 2

This configuration takes effect after a reload.

Enable CMS automatically after reload (y/n) [y]: y

Step 2:

Configure network settings
```

Configuring the WAAS Central Manager   5

```
                          --------------------------

          Select interface to configure as management interface:

          NO INTERFACE NAME STATUS IP ADDRESS NETMASK

          1: GigabitEthernet 1/0 UP unassigned unassigned

          2: GigabitEthernet 2/0 DOWN unassigned unassigned

          Enter choice [1]: 1

          ...
```

Continue to answer the questions displayed in the setup utility. You can accept the default choice (shown in brackets) at a prompt by pressing **Enter**.

6. 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.

```
          Step 4: Enable DHCP on this interface (y/n) [n]:y

          ...
```

7. 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 enter the IP address of an NTP server, because clock synchronization between the WAEs in a WAAS network is important.

```
          Step 11: Configure NTP [none]:172.19.228.200
```

8. Configure the time zone of the device. Enter the time zone abbreviation, 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 -3:30, then you would set **-3** for the hours offset and **30** for the minutes offset.

```
          Step 12: Enter timezone [UTC 0 0] :EST −5 0
```

9. 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 Accessing the WAAS Central Manager GUI.

10. 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 configurations will be done:

          device mode central-manager

          no central-manager address
```

```
no wccp version 2

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

primary-interface GigabitEthernet 1/0

hostname waas-cm

clock timezone EST -5 0

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

11. 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
```

12. 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 running-config startup-config

waas-cm# reload

Proceed with reload?[confirm] y

Shutting down all services, will Reload requested by
CLI@ttyS0.

Restarting system.
```

The system reboots. 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.

13. When prompted, enter the administrator username (admin) and password (default) and press **Enter**.

```
Username: admin

Password:

System Initialization Finished.
```

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 data center WAE and the branch WAE) with this WAAS Central Manager. See the next section for details.

Configuring the WAEs for Inline Interception

This section describes configuring WAEs that have the Cisco WAE Inline Network Adapter installed. If you are using WAEs (or WAE network modules) that are using WCCP interception, see the section Configuring WCCP.

To install and configure the WAAS WAE devices, and register them with the WAAS Central Manager, follow these steps:

1. In the data center, unpack and connect the second WAAS device that you want to configure as the data center WAE in the WAAS network. You must set the port to which the WAE is connected to full duplex. For hardware installation instructions, see 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. Check each Cisco WAE interface and the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full duplex is configured.

2. Power up the designated data center WAE and open a console connection.

3. When a WAAS device starts up, you are prompted to run the first-time setup utility, which you use to set up the basic configuration for the device. When prompted, press **Enter** and then enter the administrator password, which is default.

> The configuration prompt waits several seconds before proceeding with the WAE setup sequence. If you want to quit the setup utility, you can press Esc at any time.
> **Note:** If you do not press **Enter** in time to enter the 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. When you log in, the username is admin and the password is default.

4. The first step of the setup utility displays a default configuration and allows you to continue with these default settings (enter **y**) or enter quick configuration mode to change them (enter **n**).

```
Step 1: The following defaults can be configured:

Device mode: Application-accelerator

Interception Method: Inline

Management Interface: InlineGroup 1/1

Autosense: yes

Timezone: UTC 0 0
```

```
        To keep above defaults and continue configuration, press 'y'.

        To change above defaults and continue configuration, press 'n'
        [y]:
```
If you use the default settings, the setup utility skips some of the following steps.

5. Enter the required information as prompted by the setup utility (see Table 1: Checklist of WAAS Network System Parameters). For example, choose **application-accelerator** as the device mode that you want to configure on the WAAS device. You can accept the default choice (shown in brackets) at a prompt by pressing **Enter**.

```
        Step 2:

        Configure WAAS Settings

        -----------------------

        Select device mode :

        1.application-accelerator

        2.central-manager

        Enter your choice [1]: 1
```

6. 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.

```
        Step 3: Enter Central Manager address : 10.10.10.10
```

7. Choose the interception method. The default method is normally the correct one to choose because it is automatically set to inline if a Cisco WAE Inline Network Adapter is installed or WCCP otherwise. Choose other if you want to use PBR interception or redirection from a Cisco Application Control Engine (ACE) or Catalyst 6500 series Content Switching Module (CSM).

```
        Step 4: Select interception method (inline|wccp|other)
        [inline]: inline
```
Note: When using inline interception, we recommend configuring a routable IP address on the Cisco WAE Inline Network Adapter interface. Though it is possible to configure no IP address on the Cisco WAE Inline Network Adapter interface, directed mode operation will not work without an IP address. For more information on using directed mode, see the section *Configuring Directed Mode* in the *Cisco Wide Area Application Services Configuration Guide*.

8. Choose the interface to configure as the management interface, for communicating with the WAAS Central Manager. With the Cisco WAE Inline Network Adapter, you can choose to share one of the inline interfaces for management traffic or you can use one of the built-in Gigabit Ethernet interfaces (out-of-band management).

```
        Step 5:

        Configure network settings
```

```
                        --------------------------

            Select interface to configure as management interface:

            NO INTERFACE NAME STATUS IP ADDRESS NETMASK

            1: InlineGroup 1/1 UP unassigned unassigned

            2: InlineGroup 1/0 UP unassigned unassigned

            3: GigabitEthernet 1/0 DOWN unassigned unassigned

            4: GigabitEthernet 2/0 DOWN unassigned unassigned

            Enter choice [1]: 1
```
Continue to answer the questions displayed in the setup utility.
When you are prompted for the IP address of the interface, the IP address that you enter is used for
the management interface that you chose in this step.

9. If you chose inline as the interception method, when you are prompted to enter the VLAN ID, enter a
VLAN ID between 1 and 4094, or if you are not using VLAN tagging, enter **none**.

```
            Step 9: Enter VLAN ID for InlineGroup IP(Range:1-4094 )
            [none]:
```
If the WAE with the Cisco WAE Inline Network Adapter is present in an 802.1Q VLAN trunk line
between a switch and a router, and you are configuring an inline interface with an IP address, you
must set the VLAN ID that is to be assigned to traffic that leaves the WAE. The VLAN ID should be
set to match the VLAN ID expected by the router.
Continue to answer the questions displayed in the setup utility.

10. If you chose inline as the interception method, when you are prompted to select an inline group to be
used for interception, choose the inline group.

```
            Step 16: Select interface for inline interception:

            1. InlineGroup 1/0

            2. InlineGroup 1/1

            Enter choice :
```

11. When you are prompted to choose a license, choose the licenses that you have purchased for use on your
WAE. Activating the appropriate licenses is required for various acceleration features to operate. All licenses
are not supported on all WAE models.

```
            Step 17:

            The product supports the following licenses:

            1. Transport

            2. Enterprise
```

```
                    3. Enterprise & Video

                    4. Enterprise & Virtual blade

                    5. Enterprise, Video & Virtual blade

                    Enter the license(s) you purchased [2]:
```

12. If you chose WCCP as the interception method, the setup utility displays a set of example router configurations for your convenience. These configurations are the same configurations that are described in the Configuring WCCP on the Routers. Press **Enter** to continue.

13. When finished, you see a summary of the information that you entered. Accept the configuration when prompted (enter **y**), and then apply the configuration when prompted (enter **y**). Once you apply the changes and the device finishes starting up, the device is visible on the network and it can be pinged.

> If you choose not to accept the configuration, you have the option to go through the setup questions again and reenter the values. Your previous values are used as the defaults.

14. Save the configuration on Core-WAE1.

```
          Core-WAE1# copy running-config startup-config
```

If you want to check the current running configuration on the WAE, you can use the **show running-config** EXEC command.

The initial configuration of the data center WAE is completed. The next step is to initially configure and register the designated branch WAE with the WAAS Central Manager device. Repeat the procedure in this section with the WAE in the branch office; the configuration is identical.

If you are using inline mode for the WAEs, you are finished with network configuration and you can proceed with the Accessing the WAAS Central Manager GUI.

If you are using WCCP interception, 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. Skip to the Accessing the WAAS Central Manager GUI.

If your network configuration is using WCCP instead of inline interception, WCCP provides the method to transparently redirect client requests to a WAE for processing. Figure 2: Example WCCP Network Configuration shows an example WAAS network configuration using WCCP.

Figure 2 Example WCCP Network Configuration
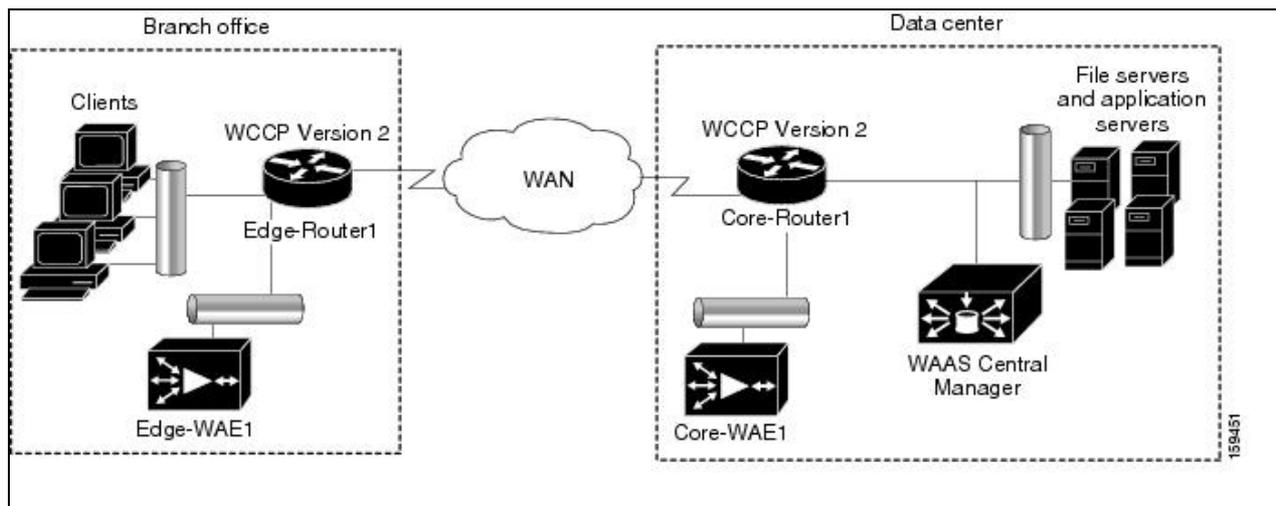
To configure basic WCCP, you must enable the WCCP service on at least one router in your network and on your WAEs. It is not necessary to configure all of the available WCCP features or services to get your WAEs up and running.

In this configuration example, because there is a data center WAE and a branch WAE in the WAAS network, you must configure WCCP Version 2 on four devices, as follows:

- Data Center WAE-To configure WCCP on the data center WAE, see the Configuring WCCP on the WAEs.
- Branch WAE-To configure WCCP on the branch WAE, see the Configuring WCCP on the WAEs.
- Data Center Router-To configure WCCP on the data center router, see the Configuring WCCP on the Routers.
- Branch Router-To configure WCCP on the branch router, see the Configuring WCCP on the Routers.

    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 WAEs

This section describes configuring WAEs that are using WCCP. If you are using WAEs that have the Cisco WAE Inline Network Adapter installed, see the section Configuring the WAEs for Inline Interception.

Note: If one of the WAE devices that you are configuring is a 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 section. For details, see the document *Configuring Cisco WAAS Network Modules for Cisco Access Routers*. After you configure the basic network settings, and open a session to the network module, you can use the procedures in this section to configure the other basic settings. The setup utility skips the questions on device mode (only application accelerator can be used) and basic network configuration, which is provided by the router configuration.

Figure 2 Example WCCP Network Configuration   12

To install and configure the WAAS WAE devices with WCCP, and register them with the WAAS Central Manager, follow these steps:

1. In the data center, unpack and connect the second WAAS device that you want to configure as the data center WAE in the WAAS network. You must set the port to which the WAE is connected to full duplex. For hardware installation instructions, see 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. Check each Cisco WAE interface and the port configuration on the adjacent device (router, switch, firewall, WAE) to verify that full duplex is configured.

2. Power up the designated data center WAE and open a console connection.

3. When a WAAS device starts up, you are prompted to run the first-time setup utility, which you use to set up the basic configuration for the device. When prompted, press **Enter** and then enter the administrator password, which is default.

> The configuration prompt waits several seconds before proceeding with the WAE setup sequence. If you want to quit the setup utility, you can press Esc at any time.
> **Note:** If you do not press **Enter** in time to enter the 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. When you log in, the username is admin and the password is default.

4. The first step of the setup utility displays a default configuration and allows you to continue with these default settings (enter **y**) or enter quick configuration mode to change them (enter **n**).

```
Step 1: The following defaults can be configured:

Device mode: Application-accelerator

Interception Method: WCCP

Management Interface: GigabitEthernet 1/0

Autosense: yes

DHCP: yes

Timezone: UTC 0 0

To keep above defaults and continue configuration, press 'y'.

To change above defaults and continue configuration, press 'n'
[y]:
```
If you use the default settings, the setup utility skips some of the following steps.

5. Enter the required information as prompted by the setup utility (see Table 1: Checklist of WAAS Network System Parameters). For example, choose **application-accelerator** as the device mode that you want to configure on the WAAS device. You can accept the default choice (shown in brackets) at a prompt by pressing **Enter**.

```
Step 2:

Configure WAAS Settings

-------------------------

Select device mode :

1.application-accelerator

2.central-manager

Enter your choice [1]: 1
```

6. 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 <u>Configuring the WAAS Central Manager</u>.

```
Step 3: Enter Central Manager address : 10.10.10.10
```

7. Choose the interception method. The default method is normally the correct one to choose because it is automatically set to WCCP if no Cisco WAE Inline Network Adapter is installed.

```
Step 4: Select interception method (inline|wccp|other) [wccp]:
wccp
```

8. Choose the interface to configure as the management interface, for communicating with the WAAS Central Manager. With the Cisco WAE Inline Network Adapter, you can choose to share one of the inline interfaces for management traffic or you can use one of the built-in Gigabit Ethernet interfaces (out-of-band management).

```
Step 5:

Configure network settings

---------------------------

Select interface to configure as management interface:

NO INTERFACE NAME STATUS IP ADDRESS NETMASK

1: GigabitEthernet 1/0 UP unassigned unassigned

2: GigabitEthernet 2/0 DOWN unassigned unassigned

Enter choice [1]: 1
```
Continue to answer the questions displayed in the setup utility.
When you are prompted for the IP address of the interface, the IP address that you enter is used for the management interface that you chose in this step.

9. When you are prompted to enter the WCCP router list, enter the IP addresses of 1-4 routers separated by spaces. The easiest configuration is to accept the default, which is the router you configured as the default gateway. To accept the default, press **Enter**.

```
Step 17: Enter the space separated list of routers(maximum 4)
for WCCPv2 [10.10.

10.1]:
```

10. When you are prompted to choose a license, choose the licenses that you have purchased for use on your WAE. Activating the appropriate licenses is required for various acceleration features to operate. All licenses are not supported on all WAE models.

```
Step 18:

The product supports the following licenses:

1. Transport

2. Enterprise

3. Enterprise & Video

4. Enterprise & Virtual blade

5. Enterprise, Video & Virtual blade

Enter the license(s) you purchased [2]:
```

11. The setup utility displays a set of example router configurations for your convenience. These configurations are the same configurations that are described in the Configuring WCCP on the Routers. Press **Enter** to continue.

12. When finished, you see a summary of the information that you entered. Accept the configuration when prompted (enter **y**), and then apply the configuration when prompted (enter **y**). Once you apply the changes, the device is visible on the network, and it can be pinged.

> If you choose not to accept the configuration, you have the option to go through the setup questions again and reenter the values. Your previous values are used as the defaults.

13. Save the configuration on Core-WAE1.

```
Core-WAE1# copy running-config startup-config
```

If you want to check the current running configuration on the WAE, you can use the **show running-config** EXEC command.

The initial configuration of the data center WAE is completed. The next step is to initially configure and register the designated branch WAE with the WAAS Central Manager device. Repeat the procedure in this section with the WAE in the branch office; the configuration is identical.

After you are finished configuring both WAEs with WCCP, proceed with the Configuring WCCP on the Routers.

Configuring WCCP on the Routers

To complete a basic WCCP configuration on the routers in the data center (Core-Router1) and in the branch office (Edge-Router1), follow these steps on each router:

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)#
```

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
```

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. This interface must be a Layer 3 interface (routed port or switch virtual interface [SVI]).

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

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

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
```

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. This interface must be a Layer 3 interface (routed port or switch virtual interface [SVI]).

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

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
```

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
```

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
```

9. Exit subinterface configuration mode.

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

Core-Router1(config)
```

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 recommended for improved performance. WCCP can use IP CEF if CEF is enabled on the router.

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#
```

12. Verify the new configuration for Core-Router1.

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

The configuration of WCCP on the data center router is completed. The next step is to configure WCCP on the branch router. Repeat the procedure in this section on the branch office router; the configuration is identical.

Accessing the WAAS Central Manager GUI

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:

1. 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.

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

3. 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 Dashboard window of the WAAS Central Manager GUI appears in your browser.

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 with DRE, TFO, and LZ optimizations. 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 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*.)

The WAAS software also comes with all application accelerators enabled. Enabled accelerators include the following: CIFS, EPM, HTTP, MAPI, NFS, and video. Enabled accelerators operate only if the proper license is installed. The Enterprise license is required for all accelerators and the video license is additionally required for the video accelerator.

Verifying Application Acceleration

Verify that WAAS optimization and application acceleration is working properly by following these steps:

1. Log into the WAAS Central Manager as described in the previous section.

2. In the left side navigation pane, choose **My WAN > Manage Devices**.

> The WAAS Central Manager displays the Devices list. You will see the WAAS Central Manager (CM in the Services column) and the two WAEs (Application Accelerator in the Services column).

3. Verify that each of the three WAAS devices show a CMS Status of Online and the Device Status has a green light, as shown in Figure 3: WAAS Central Manager Devices Window.

Figure 3 WAAS Central Manager Devices Window

4. Generate some traffic through the WAAS network for an application that WAAS optimizes.

5. In the WAAS Central Manager, choose **My WAN > Dashboard**.

6. Verify that your WAAS network is intercepting, optimizing, and compressing data by viewing the charts in the System Dashboard window. The Traffic Volume and Reduction chart (in the middle) should show an amount of optimized traffic that is lower than original traffic. The Top 10 Application chart (on the right side) should show a percentage of reduction for the type of application traffic that traversed the network.

For more information on monitoring WAAS performance, see the chapter, *Monitoring and Troubleshooting Your WAAS Network* in the *Cisco Wide Area Application Services Configuration Guide*.

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 4: Message Indicating the Predefined Password for the Superuser Account Should Be Changed.)

Figure 4 Message Indicating the Predefined Password for the Superuser Account Should Be Changed
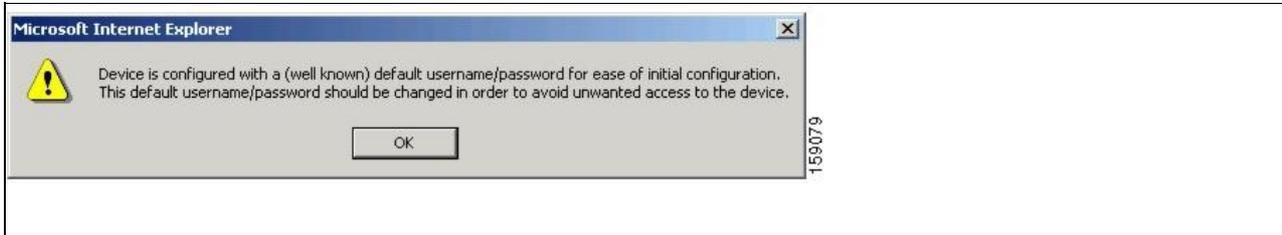
If you have not changed the predefined password for this superuser account, the console will also display the following message each time that you use this superuser account to log in to the WAAS CLI on any WAAS device:

```
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:

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

2. From the WAAS Central Manager GUI Contents pane, choose **Admin > Password**.

> The Changing Password for User Account window appears.

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

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

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 Configuration Guide
- Cisco Wide Area Application Services API Reference
- Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade
- 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
- WAAS Enhanced Network Modules
- Installing the Cisco WAE Inline Network Adapter
- Cisco Wide Area Application Services Online Help

Figure 4 Message Indicating the Predefined Password for the Superuser Account Should Be Changed