Cisco Wide Area Application Services Quick Configuration Guide

Software Version 5.0.1
July 2, 2012

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

Basic configuration settings are configured using the WAAS setup utility.

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

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

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

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. The WAEs contain Cisco Interface Modules or Cisco WAE Inline Network Adapter cards and are deployed inline between the WAN routers and the clients or servers. Alternately, you can use WCCP interception and position the WAEs off-path.

Figure 1　　　**WAAS Inline Network Configuration**
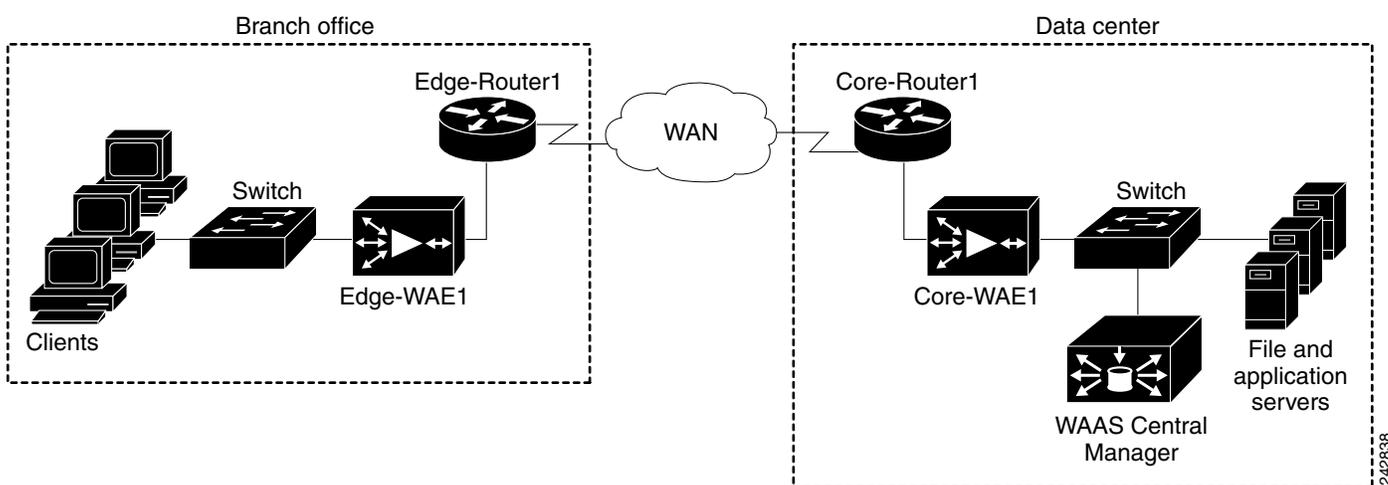
Note　Position the WAEs directly in the traffic path between the router and the clients or file servers. The WAEs intercept traffic directly through the inline interfaces and redirection is not needed.

When you install any inline device, you must follow the cabling requirements described in the hardware installation guide for your WAVE or WAE device.

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 configure the device mode as 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. You are given the choice to run diagnostics in the setup utility to verify the success of your configuration once all settings have been applied. See the "Configuring the WAAS Network" section on page 4.

   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" section on page 15. This step is not required if you are using inline mode and WAEs with the Cisco Interface Module or 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" section on page 25.

4. Verify that the WAAS application acceleration is working properly. See the "Verifying Application Acceleration" section on page 26.

5. Change the password for the predefined superuser account. See the "Changing the Administrator Password" section on page 27.

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

This section contains the following topics for configuring your WAAS network:

- Network System Parameters
- Setup Utility

Network System Parameters

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	WAAS Central Manager Values	Data Center WAE Values	Branch Office WAE Values
Interface speed			
Duplex mode			
IP address			
Subnet mask			

Table 1   Checklist of WAAS Network System Parameters (continued)

Parameter	WAAS Central Manager Values	Data Center WAE Values	Branch Office WAE Values
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)			

Setup Utility

The following restrictions, recommendations, and requirements apply to the WAAS setup utility:

- Designed for basic WAE configuration on new installations only (otherwise the running configuration of the existing system is not reflected in the tool).

- Requires a minimum 25 row x 80 column terminal window for proper display (terminal length, if configured, must be 24).

- For hyper terminal, the emulation should be set to vt100 so that all lines show up properly (input translation should be set to Shift-JIS on the File > Properties menu.

- Console logging should be disabled when executing the setup utility from the CLI to avoid system message flooding on the screen.

- After a **restore factory-default**, you are encouraged to run the setup utility (and are prompted with the option to do so).

Configuring the WAAS Network

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

- Configuring the WAAS Central Manager, page 5

- Configuring the WAEs for Inline Interception, page 10

- Configuring WCCP, page 15

- Accessing the WAAS Central Manager GUI, page 25

- Verifying Application Acceleration, page 26

- Changing the Administrator Password, page 27

✎
Note The setup utility is designed for basic WAE configuration only on new installations (not previously configured). If it is run on existing systems, the existing running configuration is not reflected in the tool and could be modified.

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, see the hardware installation guide for your WAVE or WAE 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, 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. For help, enter the **?** key.

✎
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.

Step 4 The default values for the basic configuration of the device are listed. Enter **n** at the first prompt to change the default settings or, to change a specific parameter, select the index number. You must change the defaults to configure a WAAS Central Manager.

```
ESC Quit ? Help ------------------ WAAS Default Configuration --------------------
Press 'y' to select above defaults, 'n' to configure all, <1-6> to change
specific default [y]: n
```

Step 5 Select the Device Mode as prompted. For example, choose **central-manager** as the device mode that you want to configure on the WAAS device.

```
ESC Quit ? Help ------------------ WAAS Default Configuration --------------------
1. Application Accelerator
2. Central Manager
3. AppNav Controller
Select device mode [1]: 2
```

> ![Note] **Note** The AppNav Controller device mode option is shown only on WAVE-294/594/694/7541/7571/8541 models and is not applicable for Central Manager configuration.

Step 6 Enter the Time Zone of the device. 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.

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
Enter Time Zone <Time Zone Hours (-23 to 23) Minutes (0-59)> [UTC 0 0]: EST -5 0
```

Step 7 Select the Management Interface of the device.

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
NO   INTERFACE NAME
 1: GigabitEthernet 1/0
 2: GigabitEthernet 2/0
Select Management Interface [1]: 1
```

You can accept the default choice (shown in brackets) at a prompt by pressing **Enter**.

Step 8 Configure Autosense for Management Interface.

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
Enable Autosense for Management Interface? (y/n) [y]:
```

> ![Note] **Note** Configuring Autosense is not required if the management interface is a TenGigabitEthernet interface.

Step 9 If you have Dynamic Host Control Protocol enabled in your network, enable DHCP on the WAAS device interface.

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
Enable DHCP for Management Interface? (y/n) [y]:
```

> ![Note] **Note** Enabling DHCP is not required if the management interface is a TenGigabitEthernet interface.

Step 10 Select the Management Interface Speed.

> ![Note] **Note** This option is available only if management interface **Autosense** is disabled. Management interface speed is not applicable if the interface is a TenGigabitEthernet interface.

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
1. 1000
2. 100
3. 10
Select Management Interface Speed [1]:
```

Step 11 Enter the Management Interface IP Address.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter Management Interface IP Address
<a.b.c.d or a.b.c.d/X (optional mask bits)> [Not configured]:
```

Step 12 Enter the Management Interface IP Mask.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter Management Interface IP Mask [Not configured]:
```

Step 13 Enter the Default Gateway IP Address.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter Default Gateway IP Address [Not configured]:
```

Step 14 Enter the Domain Name Server IP Address.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter Domain Name Server IP Address [Not configured]:
```

Step 15 Enter the Domain Names.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter Domain Name(s) [Not configured]:
```

Step 16 Enter the Host Name.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter Host Name [None]:
```

Step 17 For the 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.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter NTP Server IP Address [None]: 172.19.228.200
```

Step 18 Select the licenses that you purchased.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
The product supports the following licenses:
1. Enterprise
2. Enterprise & Video
Enter the license(s) you purchased [2]:
```

Step 19 Write down the IP address of the WAAS Central Manager for future reference. You will need it to launch the WAAS Central Manager GUI, which you will use later in the "Accessing the WAAS Central Manager GUI" section on page 25.

Press **F2** to see all of the configuration, enter **d** to toggle the defaults display, or enter a number to change a specific parameter. (See Figure 2.)

Figure 2   Central Manager Config

```
     Parameter                    Configured Value
 1. Device Mode                   Central Manager
 2. Time Zone                     UTC 0 0
 3. Management Interface          GigabitEthernet 1/0
 4.     Autosense                     Enabled
 5.     DHCP                          Disabled
 6.     IP Address                    2.75.38.34
 7.     IP Network Mask               255.255.255.224
 8. IP Default Gateway            2.75.38.33
 9. DNS IP Address                171.69.2.133
10. Domain Name(s)                cisco.com
11. Host Name                     dc-cm
12. NTP Server Address            None
13. License                       Enterprise


ESC Quit ? Help 1 CLI ──────────── WAAS Final Configuration ──────────
Press 'y' to select configuration, 'd' to toggle defaults display, <1-13> to
change specific parameter [y]: █
```

Step 20 Enter **y** when you are ready to accept the final configuration. The device is then visible on the network and it can be pinged.

```
ESC Quit ? Help ------------------ WAAS Final Configuration -------------------
Apply WAAS Configuration: Configuration will come into effect after a manual
reboot. At console prompt please issue CLI below to save configuration & then
reload ..
copy running-config startup-config
reload force
Please press ENTER to continue ...
```

Step 21 Save the configuration changes to the startup configuration file and reload the system to apply the final configuration.

```
WAE# copy run start
WAE# reload
Proceed with reload?[confirm] yes
```

The system reboots. The WAAS Central Manager configuration that you just configured is loaded on the WAAS device, which is now designated as a WAAS Central Manager.

Step 22 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 "Configuring the WAEs for Inline Interception" section on page 10 for details.
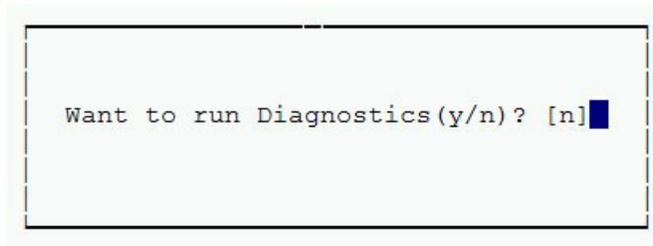
Running Diagnostics

Once your configuration has been applied, you are given the choice to run the diagnostic utility to verify connectivity. The option to run the diagnostic utility appears only if the setup utility was executed using the EXEC CLI command. (See Figure 3.)

Note If diagnostics fail because of transient configurations, such as before a DHCP server has completed learning, you can run diagnostics manually using the **test self-diagnostics all** EXEC CLI command.

Figure 3 *Configuration Diagnostics*

```
|                                                   |
|                                                   |
|    Want to run Diagnostics(y/n)? [n]█             |
|                                                   |
|                                                   |
|                                                   |
```

The diagnostic utility tests configuration properties including basic configuration, connectivity, interface link properties, and TFO configuration. (See Figure 4.)

Note Invalid IP addresses (Central Manager or WCCP router list) can lead to long delays when testing connectivity.

Figure 4 *Diagnostics*

```
Checking for presence of basic configs ...

        > Successful.

Checking connectivity ...

        > Device default gateway 2.75.38.33 is not reachable
        > Domain-name server(s) 171.69.2.133 is not reachable
        > Central Manager 2.2.2.2 is not reachable
        > NTP server(s) 2.43.65.25 171.69.2.133 are not reachable
        > Unable to check whether device hostname is resolvable because
          name servers are not configured/reachable

Checking for interface link properties ...

        > Interface GigabitEthernet 2/0 is not up

Checking for tfo configs ...

<-Press Any Key To Continue->█
```

Configuring the WAEs for Inline Interception

This section describes configuring WAEs that have the Cisco Interface Module or Cisco WAE Inline Network Adapter installed. If you are using WAEs (or WAE network modules) that are using WCCP interception, see the "Configuring WCCP" section on page 15.

To install and configure the WAAS WAE devices, and register them 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 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.

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

Step 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.

Step 4 The first step of the setup utility displays a default configuration and allows you to enter '**y**' to accept the default values, '**n**' to configure all, or enter a number to change a specific parameter.

```
Parameter                        Default Value
1. Device Mode                   Application Accelerator
2. Interception Method           Inline
3. Time Zone                     UTC 0 0
4. Management Interface          InlineGroup 1/1
5.      Autosense                Enabled
6.    DHCP                       Enabled

ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
Press 'y' to select above defaults, 'n' to configure all, <1-6> to change specific default
[y]:
```

If you use the default settings, the setup utility skips configuration of the parameters in the following steps.

Step 5 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. You can accept the default choice (shown in brackets) at a prompt by pressing **Enter**.

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
1. Application Accelerator
```

```
2. Central Manager
3. AppNav Controller
Select device mode [1]: 1
```

> ✎
> **Note** If you want to use AppNav Controller device mode, see the "Configuring an AppNav Controller" section on page 13.

Step 6 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, otherwise it is set to WCCP. The AppNav Controller interception method is for WAEs that are operating as WAAS nodes in an AppNav deployment; other AppNav-specific settings must be configured using the Central Manager. 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). PBR interception is not supported on an AppNav Controller.

```
1. Inline
2. WCCP
3. AppNav Controller
4. Other
Select Interception Method [1]: 1
```

> ✎
> **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*.

Step 7 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).

```
ESC Quit ? Help ------------------ WAAS Default Configuration --------------------
NO   INTERFACE NAME
1: InlineGroup 1/1
2: InlineGroup 1/0
3: GigabitEthernet 1/0
4: GigabitEthernet 2/0
Select Management Interface [1]: 1
```

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.

Step 8 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**.

```
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.

Step 9 If the management interface is a GigabitEthernet interface, then you are prompted to select an inline group to be used for interception, choose the inline group.

```
1. InlineGroup 1/0
2. InlineGroup 1/1
Select interface for inline interception:
```

Step 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.

```
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]:
```

Step 11 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" section on page 23. Press **Enter** to continue.

Step 12 When finished, the configuration is displayed. Enter **d** to toggle the defaults display, or enter a number to change a specific parameter. (See Figure 5.)

Figure 5 *WAE Config—Inline*

Enter **y** to select the configuration. 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.

Step 13 Once you apply the changes, the configuration is saved automatically and you are given the option to reload the system so that the new configuration will take effect. The option to reload the system appears only when the device mode is changed using the Setup wizard.

✎
Note If a Central Manager address has been configured, **cms enable** is automatically configured by the system (node manager) within 5 minutes after the reboot.

The system reboots and the device is then visible on the network and it can be pinged.

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" section on page 25.

If you are using WCCP interception, the next step is to configure WCCP. For details, see the "Configuring WCCP" section on page 15.

Configuring an AppNav Controller

This section describes how to configure a WAAS device as an AppNav Controller.

> **Note** AppNav Controller device mode is supported only on WAVE-294/594/694/7541/7571/8541 models. Advanced AppNav configuration is not supported using the setup utility and must be configured using the Central Manager. For more information on Cisco WAAS AppNav, see the "Configuring AppNav" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Step 1 When prompted by the setup utility for the device mode that you want to configure on the WAAS device, enter 3 to choose AppNav Controller.

```
ESC Quit ? Help ------------------ WAAS Default Configuration --------------------
1. Application Accelerator
2. Central Manager
3. AppNav Controller
Select device mode [1]: 3
```

Step 2 Reboot the device as prompted by entering **y** and then **y** again at the confirmation prompt.

```
Device Mode AppNav Controller selectedin SETUP; New configuration takes effect
after a reload. If applicable, AppNav Controller I/O Module is recognized after
the reboot. Re-run Setup CLI to perform AppNav Controller related configuration
post reboot.Initiate system reload? <y/n> [n] y
Are you sure? <y/n> [n]: y
```

The device restarts. Continue after the device finishes restarting.

Step 3 Rerun the setup utility.

```
WAE# setup
```

Step 4 The first step of the setup utility again displays a default configuration and allows you to enter 'y' to accept the default values, 'n' to configure all, or enter a number to change a specific parameter.

```
Parameter                          Default Value
1. Device Mode                     AppNav Controller
2. Interception Method             Inline
3. Time Zone                       UTC 0 0
4. Management Interface            GigabitEtherenet 0/0
5.      Autosense                  Enabled
```

```
6.    DHCP                    Enabled

ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
Press 'y' to select above defaults, 'n' to configure all, <1-6> to change specific default
[y]:
```

If you use the default settings, the setup utility skips configuration of the parameters in the following steps.

Step 5   Choose AppNav Controller as the device mode.

Step 6   Choose the interception method. The default method is normally the correct one to choose. Choose other if you want to use redirection from a Cisco Application Control Engine (ACE) or Catalyst 6500 series Content Switching Module (CSM).

```
1. Inline
2. WCCP
3. Other
Select Interception Method [1]: 1
```

Step 7   Choose the interface to configure as the management interface, for communicating with the WAAS Central Manager. With the Cisco AppNav Controller Interface Module, 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).

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
No.      Interface Name      IP Address    Network Mask

  1. GigabitEthernet 0/0           dhcp
  2. GigabitEthernet 0/1           dhcp
  3. GigabitEthernet 1/0      unassigned      unassigned
  4. GigabitEthernet 1/1      unassigned      unassigned
  5. GigabitEthernet 1/2      unassigned      unassigned
  6. GigabitEthernet 1/3      unassigned      unassigned
  7. GigabitEthernet 1/4      unassigned      unassigned
  8. GigabitEthernet 1/5      unassigned      unassigned
  9. GigabitEthernet 1/6      unassigned      unassigned
 10. GigabitEthernet 1/7      unassigned      unassigned
 11. GigabitEthernet 1/8      unassigned      unassigned
 12. GigabitEthernet 1/9      unassigned      unassigned
 13.GigabitEthernet 1/10      unassigned      unassigned
 14.GigabitEthernet 1/11      unassigned      unassigned
Select Management Interface [14]:
```

✎
Note   In AppNav Controller device mode, the last port of the AppNav Controller Interface Module is the default. When an AppNav Controller Interface Module port is chosen, DHCP and Autosense are supported only on 12xGE Copper or Fiber AppNav Controller Interface Modules.

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.

Continue to answer the questions displayed in the setup utility.

Step 8   When finished, the configuration is displayed. Enter **d** to toggle the defaults display, or enter a number to change a specific parameter.

Enter **y** to select the configuration. 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.

```
Service Context configuration, including interception settings, must be
```

```
performed using  central manager .......
Please press ENTER to continue ...
```

Note Advanced AppNav cluster configuration is not supported using the setup utility and must be configured using the Central Manager. For more information on Cisco WAAS AppNav, see the "Configuring AppNav" chapter in the *Cisco Wide Area Application Services Configuration Guide*.

Step 9 Finish the setup process and save the configuration by pressing **Enter**.

```
Testing Central-Manager reachability ... successful.
Configuring 'cms enable' ..

WAAS configuration applied successfully!!
Saved configuration to memory.

Press ENTER to continue ...
```

Step 10 Exit the setup utility by pressing **Enter**. You are prompted to run the diagnostics. Press **y** to run the diagnostics or **n** to exit the setup utility.

The device is visible on the network and it can be pinged.

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. On the WAE in the branch office, repeat the procedure in the "Configuring the WAEs for Inline Interception" section on page 10.

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" section on page 25.

If you are using WCCP interception, 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. With inline mode, traffic is directly intercepted and redirection is unnecessary. Skip to the "Accessing the WAAS Central Manager GUI" section on page 25.

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 6 shows an example WAAS network configuration using WCCP.

Figure 6 **Example WCCP Network Configuration**
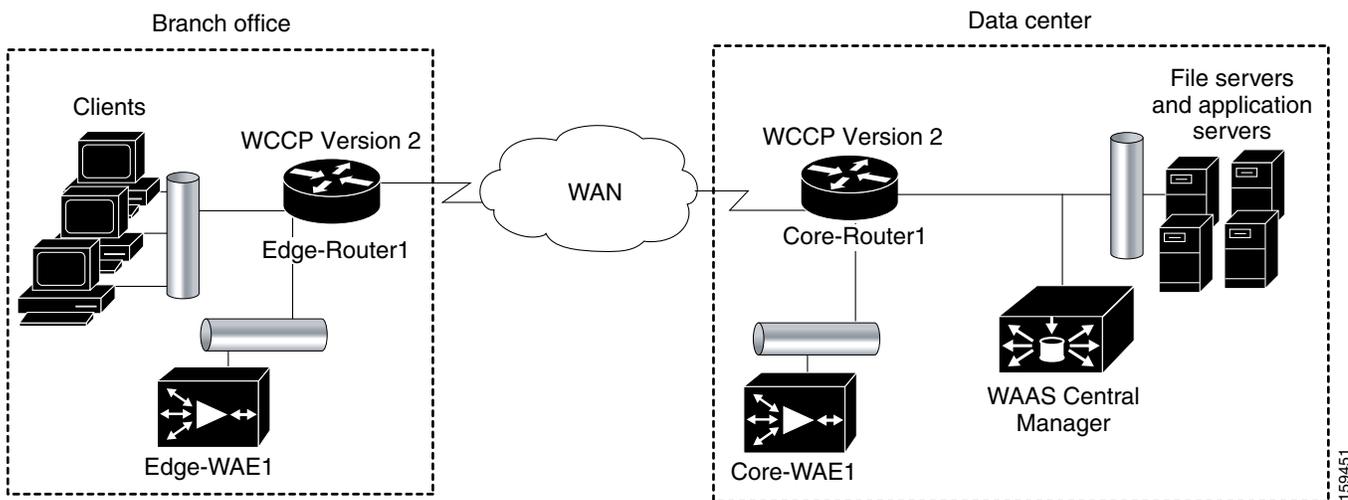
To configure basic WCCP, you must enable the WCCP service on at least one router in your network and on your WAEs. It is not necessary to configure all of the available WCCP features or services to get your WAEs up and running.

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" section on page 17.

- Branch WAE—To configure WCCP on the branch WAE, see the "Configuring WCCP on the WAEs" section on page 17.

- Data Center Router—To configure WCCP on the data center router, see the "Configuring WCCP on the Routers" section on page 23.

- Branch Router—To configure WCCP on the branch router, see the "Configuring WCCP on the Routers" section on page 23.

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*.

The following WCCP procedures are included in this section:

- Configuring WCCP on the WAEs

- Configuring WCCP on WAAS Network Modules

- Configuring WCCP on the Routers

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" section on page 10.

✎ **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*. For SM-SRE modules, see the document *Cisco SRE Service Module Configuration and Installation Guide*.

After you configure basic network settings, and open a session to the network module, you can use the procedures in this section to configure 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. For basic WCCP configuration, see the section "Configuring WCCP on WAAS Network Modules" section on page 20.

To install and configure the WAAS WAE devices with WCCP, and register them 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 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.

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

Step 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.

Step 4 The first step of the setup utility displays a default configuration and allows you to enter '**y**' to accept the default values, '**n**' to configure all, or enter a number to change a specific parameter.

```
Parameter                      Default Value
1. Device Mode                 Application Accelerator
2. Interception Method         WCCP
3. Time Zone                   UTC 0 0
4. Management Interface        Gigabit Ethernet 1/0
5.      Autosense              Enabled
```

```
6.    DHCP                      Enabled

ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
Press 'y' to select above defaults, 'n' to configure all, <1-6> to change specific default
[y]:
```

If you use the default settings, the setup utility skips the configuration of some of the parameters in the following steps.

Step 5 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. You can accept the default choice (shown in brackets) at a prompt by pressing **Enter**.

```
1. Application Accelerator
2. Central Manager
3. AppNav Controller
Select device mode [1]: 1
```

✎
Note   If you want to use AppNav Controller device mode, see the "Configuring an AppNav Controller" section on page 13.

Step 6 Choose the interception method. The default method is normally the correct one to choose.

```
1. WCCP
2. Other
Select Interception Method [1]: 1
```

Step 7 Enter the Time Zone of the device. 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.

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
Enter Time Zone <Time Zone Hours (-23 to 23) Minutes (0-59)> [UTC 0 0]: EST -5 0
```

Step 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).

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
NO   INTERFACE NAME
1: GigabitEthernet 1/0
2: GigabitEthernet 2/0
Select Management Interface [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.

Step 9 Configure Autosense for Management Interface. Autosense is disabled by default.

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
Enable Autosense for Management Interface? (y/n) [y]:
```

✎
Note   Autosense is not supported on the 4x10GE SFP+ fiber AppNav Controller Interface Module.

Step 10 If you have Dynamic Host Control Protocol enabled in your network, enable DHCP on the WAAS device interface.

```
ESC Quit ? Help ------------------ WAAS Default Configuration -------------------
Enable DHCP for Management Interface? (y/n) [y]:
```

✎

Note If an interface on the AppNav Controller Interface Module is selected as the management interface, DHCP is disabled and cannot be enabled.

Step 11 Enter the Central Manager IP Address.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter Central Manager IP Address (WARNING: An invalid entry will cause SETUP to take a
long time when applying WAAS configuration) [None]: 10.10.10.10
```

Step 12 Enter the Host Name.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter Host Name [None]:
```

Step 13 For the 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.

```
ESC Quit ? Help ------------------ WAAS Remaining Configuration -------------------
Enter NTP Server IP Address [None]: 172.19.228.200
```

Step 14 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**.

```
Enter the space separated list of routers (maximum 4) for WCCPv2 [10.10.10.1]:
```

Step 15 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.

```
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]:
```

Step 16 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" section on page 23. Press **Enter** to continue.

Step 17 When finished, the configuration is displayed. Enter **d** to toggle the defaults display, or enter a number to change a specific parameter. (See Figure 7.)

Figure 7 WAE Config—WCCP

```
        Parameter                 Configured Value
    2.  Interception Method        WCCP
    3.  Time Zone                  UTC 0 0
    4.  Management Interface       GigabitEthernet 0/0
    5.     Autosense                  Enabled
    6.     DHCP                       Disabled
    7.     IP Address                 10.0.0.2
    8.     IP Network Mask            255.255.255.0
    9.  IP Default Gateway         10.0.0.1
   10.  CM IP Address              None
   11.  DNS IP Address            2.2.2.2
   12.  Domain Name(s)             mydomain.com
   13.  Host Name                  M2-3
   14.  NTP Server Address         1.1.1.1
   15.  WCCP Router List           10.0.0.1
   16.  License                    Enterprise
ESC Quit ? Help ! CLI ——————— WAAS Final Configuration ———————
Press 'y' to select configuration, <F2> to see all configuration, 'd' to toggle
defaults display, <1-16> to change specific parameter [y]:
```

Enter **y** to select the configuration. 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.

Step 18 Once you apply the changes, the configuration is saved automatically and you are given the option to reload the system so that the new configuration will take effect.The option to reload the system appears only when the device mode is changed using the Setup wizard.

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

Note If a CM address has been configured, **cms enable** is automatically configured by the system (node manager) within 5 minutes after the reboot.

The system reboots and the device is then visible on the network and it can be pinged.

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" section on page 23.

Configuring WCCP on WAAS Network Modules

If one of the WAE devices that you are configuring is a network module (NME-WAE) installed in a Cisco access router, you can configure basic WCCP settings using the setup utility.

Note If an external interface is used as the primary interface, router WCCP configuration is not recommended. If configured, however, the default gateway must point to the router hosting the network module, and the interface must be either directly connected back to the router, or through a trusted network. Otherwise, there could be a security risk.

To configure basic WCCP settings on a network module, perform the following steps in the setup utility after initial configuration:

Step 1 Once you have entered **y** to select the final basic network module configuration, enter **y** to configure WCCP on the router.

(See Figure 8.)

Figure 8 **WAAS Network Module Config—Basic Config**

```
     Parameter                      Configured Value
 2. Time Zone                       UTC 0 0
 3. Management Interface            GigabitEthernet 1/0        (internal)
         Autosense                      Disabled
         DHCP                           Disabled
         Speed                          1000(full-duplex)
         IP Address                     2.75.38.138
         IP Network Mask                255.255.255.252
     IP Default Gateway             2.75.38.137
 4. CM IP Address                   2.75.38.34
 5. DNS IP Address                  171.69.2.133
 6. Dcmain Name(s)                  cisco.ccm
 7. Host Name                       nm
 8. NTP Server Address              171.69.2.133
 9. WCCP Router List                2.75.38.137
10. License                         Enterprise
ESC Quit ------------------------- WCCP Router Authentication --------------
Do you want to configure WCCP on the router? <y/n> [n] █
```

Step 2 Enter and confirm router login password.

If TACACS or RADIUS server authentication is configured on the router, that password takes precedence over the local password.

The router user ID should have the privilege level set to 15 for a successful configuration. The following message displays:

```
Please ensure that the router privilege level is set to 15. If the privilege level < 15,
router configurations will not be successful.
Do you want to proceed configuring WCCP on the router? <y/n> [n]
```

Enter **y** if the privilege level is set to 15. Else, enter **n** and set the privilege level to 15 and then proceed with the configuration.

Step 3 Choose a WCCP configuration (LAN redirection or WAN redirection). (See Figure 9.)

Figure 9   *WAAS Network Module Config—WCCP Config*

The following WCCP configuration is applied:

- LAN—ip wccp service 61 is configured as IN
- WAN—ip wccp service 62 is configured as IN
- NME-WAE interface of the router—ip wccp redirect exclude in is configured

In addition, a WAAS WCCP pilot redirect list of ACLs will are configured by default on the router. When you have completed the configuration, you can display the CLI using the **!** key to view the WAAS WCCP pilot redirect list of ACLs, and the rest of the configuration.

Step 4   Enter the **!** key to display the CLI.

```
conf t
    interface GigabitEthernet0/0.1720
        ip wccp 61 redirect in
    exit
    interface GigabitEthernet0/0.1726
        ip wccp 62 redirect in
    exit
    interface In2/0
        ip wccp redirect exclude in
    exit
    ip wccp version 2
    ip wccp 61 redirect-list waas-wccp-redirect-list
    ip wccp 62 redirect-list waas-wccp-redirect-list
    ip access-list extended waas-wccp-redirect-list
        remark WAAS WCCP Pilot Redirect list
        deny tcp any any eq telnet
        deny tcp any any eq 22
        deny tcp any any eq 161
        deny tcp any any eq 162
        deny tcp any any eq 123
        deny tcp any any eq bgp
        deny tcp any any eq tacacs
        deny tcp any any eq 2000
        deny tcp any any eq 5060
        deny tcp any any eq 1718
```

```
                          deny tcp any any eq 1719
                          deny tcp any any eq 1720
                          deny tcp any any eq 554
                          deny tcp any any eq 1755
                          deny tcp any eq telnet any
                          deny tcp any eq 22 any
                          deny tcp any eq 161 any
                          deny tcp any eq 162 any
                          deny tcp any eq 123 any
                          deny tcp any eq bgp any
                          deny tcp any eq tacacs any
                          deny tcp any eq 2000 any
                          deny tcp any eq 5060 any
                          deny tcp any eq 1718 any
                          deny tcp any eq 1719 any
                          deny tcp any eq 1720 any
                          deny tcp any eq 554 any
                          deny tcp any eq 1755 any

                          permit tcp any any
                   end
```

Step 5 Hit any key to continue and apply the configuration. Once you apply the changes, the configuration is saved automatically and you are given the option to reload the system so that the new configuration will take effect. The option to reload the system appears only when the device mode is changed using the Setup wizard.

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

> **Note** If a CM address has been configured and the device mode has changed from the current running device mode (**show device-mode running**), **cms enable** is automatically configured by the system (node manager) within 5 minutes after the reboot.

The system reboots and the device is then visible on the network and it can be pinged.

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:

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

Cisco Wide Area Application Services Quick Configuration Guide

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

```
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
```

✎
Note   If you plan to use the WCCP GRE return or generic GRE egress methods, you can place the WAE on the same VLAN or subnet as the clients and servers. When using these egress methods, it is important not to enable WCCP on the router until after these egress methods are configured on the WAEs, which can only be done after the setup utility has completed. For more information on configuring these egress methods, see the section "Configuring Egress Methods for WCCP Intercepted Connections" in the *Cisco Wide Area Application Services Configuration Guide*.

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 recommended 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 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:

Step 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.

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

Step 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 most application accelerators enabled. Enabled accelerators include the following: CIFS, EPM, HTTP, ICA, MAPI, NFS, SSL, 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:

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

Step 2   From the WAAS Central Manager menu, choose **Devices > All Devices**.

The WAAS Central Manager displays the Devices list, as shown in Figure 10. You will see the WAAS Central Manager (CM in the Services column) and the two WAEs (Application Accelerator in the Services column).

Step 3   Verify that each of the three WAAS devices show a Management Status of Online and the Device Status has a green light.

Figure 10   *WAAS Central Manager Devices Window*

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

Step 5   From the WAAS Central Manager menu, choose **Home**.

Step 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 should show an amount of optimized traffic that is lower than original traffic. The Compression Summary chart 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 *Cisco Wide Area Application Services Monitoring Guide* and the chapter, "Monitoring and Troubleshooting Your WAAS Network" in the *Cisco Wide Area Application Services Configuration Guide*. For troubleshooting information, see the *Cisco WAAS Troubleshooting Guide* on Cisco DocWiki.

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.

To change the password for the superuser account across all WAAS 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 menu, choose **Admin > Security > Password**.

The Changing Password for User Account window appears.

Step 3 In the New Password field, enter the new password. Passwords are case sensitive, must be 1 to 31 characters in length, and cannot contain the characters ' " | (apostrophe, double quote, or pipe) or any control characters.

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.

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

In addition to this document, the WAAS documentation set includes the following publications:

- *Release Note for Cisco Wide Area Application Services*
- *Cisco Wide Area Application Services Upgrade Guide*
- *Cisco Wide Area Application Services Quick Configuration Guide* (this manual)
- *Cisco Wide Area Application Services Configuration Guide*
- *Cisco Wide Area Application Services Command Reference*
- *Cisco Wide Area Application Services API Reference*
- *Cisco Wide Area Application Services Monitoring Guide*
- *Cisco Wide Area Application Services vWAAS Installation and Configuration Guide*
- *Cisco WAAS Installation and Configuration Guide for Windows on a Virtual Blade*
- *Configuring WAAS Express*
- *Cisco WAAS Troubleshooting Guide for Release 4.1.3 and Later*
- *Cisco WAAS on Service Modules for Cisco Access Routers*
- *Cisco SRE Service Module Configuration and Installation Guide*
- *Configuring Cisco WAAS Network Modules for Cisco Access Routers*
- *WAAS Enhanced Network Modules*
- *Cisco Wide Area Application Services Online Help*
- *Regulatory Compliance and Safety Information for the Cisco Wide Area Virtualization Engines*
- *Cisco Wide Area Virtualization Engine 294 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 594 and 694 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 7541, 7571, and 8541 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 274 and 474 Hardware Installation Guide*
- *Cisco Wide Area Virtualization Engine 574 Hardware Installation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Wide Area Application Engine 7341, 7371, and 674 Hardware Installation Guide*
- *Installing the Cisco WAE Inline Network Adapter*

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.