



Cisco Content Delivery Networking Products

- 1** Introduction to Cisco Content Delivery Networking Products
- 2** How to Use This Guide
- 3** Install the Chassis
- 4** Ground the Chassis
- 5** Connect the Cables
- 6** Perform an Initial Startup Configuration
- 7** Set Up and Enable the E-CDN Application
- 8** Enable Licensed Software
- 9** Obtaining Documentation
- 10** Obtaining Technical Assistance

1 Introduction to Cisco Content Delivery Networking Products

Cisco content delivery networking products include ACNS software and the content networking hardware devices that use ACNS software. Together these products are the components of a Content Delivery Network (CDN), which is a complete system that includes content routing, content switching, content distribution and management, and content services, as well as content delivery. A CDN is composed of Content Engines, Content Routers, and Content Distribution Managers that all run ACNS software.

ACNS Software Overview

ACNS is a software platform that unifies the Cisco Cache software and Cisco Enterprise Content Delivery Network (E-CDN) software into a single software platform. ACNS software allows you to access caching application features and E-CDN application features from a single software base. ACNS software is supported on Content Engines, Content Distribution Managers, and Content Routers. (See the “Hardware Overview” section on page 2.)

E-CDN Application Overview

The E-CDN application offers accelerated content delivery, hosting, and other content-based services. It addresses the need to distribute and receive high-bandwidth, media-rich content across the Internet or an intranet without performance losses or content delivery delays.

When the ACNS E-CDN application is enabled, Content Engines, Content Routers, Content Services Switches, and Content Distribution Managers can be deployed to create a complete Content Delivery Network system that includes content routing, content switching, content distribution and management, and content services, as well as content delivery.

Cache Application Overview

ACNS software provides content caching capabilities that accelerate content delivery and optimize bandwidth usage by caching frequently accessed content and fulfilling content requests locally rather than traversing the Internet or intranet to a distant server each time a request is made. The ACNS software Cache application can work in tandem with Cisco IOS routing software to handle web traffic, including user requests to view pages and graphics (objects) on World Wide Web servers—whether internal or external to your network.

Hardware Overview

The following table lists the content networking hardware models that are supported and not supported in ACNS software:

| Supported Hardware | Unsupported Hardware |
|--------------------------------------|----------------------|
| Content Engines | |
| CE-590, CE-590-DC | CE-505 |
| CE-560, CE-560-CDN, CE-560AV-CDN | CE-550 |
| CE-507, CE-507-CDN, CE-507AV-CDN | CE-570 |
| CE-7320, CE-7320-DC | CE-590-CDN |
| — | CE-7320-CDN |
| Content Routers | |
| CR-4430 | CR-4450 |
| — | CR-4430-B |
| Content Distribution Managers | |
| CDM-4630 | CDM-4670 |
| CDM-4650 | — |



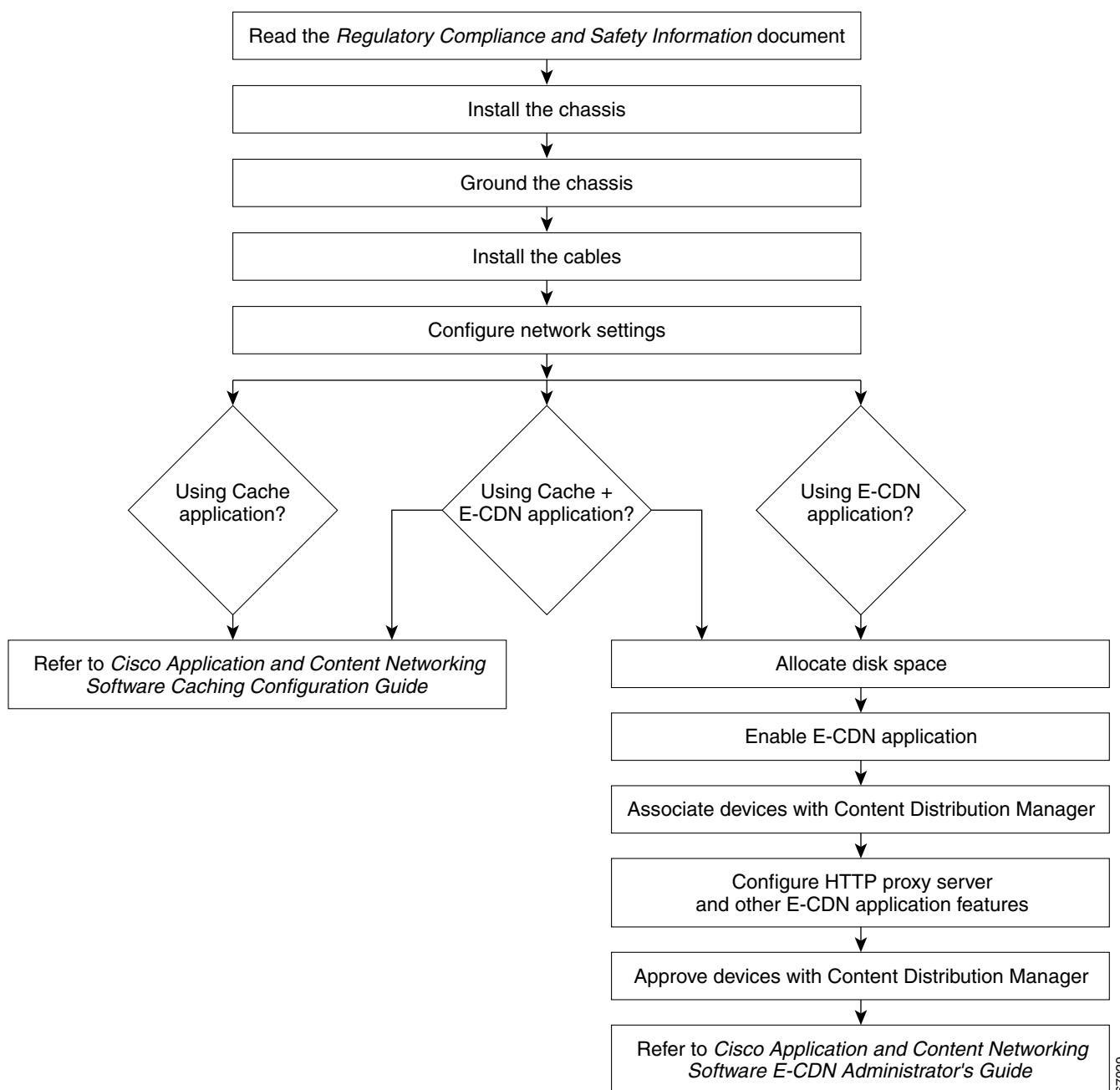
2 How to Use This Guide

This guide explains:

- How to install the device in a rack or on a tabletop
- How to ground the chassis
- How to connect network, console, and power cables
- How to initialize the ACNS software

After you have completed the initial configuration and setup, you are ready to configure Cache application features, E-CDN application features, or both.

Before using either the Cache application or the E-CDN application, complete the following tasks:



67929

3 Install the Chassis

Safety Information

Before you begin the installation, read the *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series* document and the *Site Preparation and Safety Guide* that shipped with your chassis.



Warning

Read the installation instructions before you connect the system to its power source.

Items Included with the Chassis

- Power cable
- Console cable
- Ethernet cable
- RJ-45-to-DB-9 adapters
- Rack-mount kit

Rack-Mount Kit for 1-Rack Unit Chassis

- Two rack-mount brackets
- Four 12-24 x 0.50-inch (12.7-mm) flat-head Phillips rack screws
- Four 18-8 x 0.37-inch (9.4-mm) flat-head Phillips bracket screws for 19-inch (48.26-cm) racks
- Four 8 x 0.375-inch (9.5-mm) round-head Phillips bracket screws for 23-inch (58.42-cm) racks
- One cable holder and screw (installation optional)
- Four self-adhesive feet (for optional tabletop installation)

Rack-Mount Kit for 7-Rack Unit Chassis

- One shelf
- Four shelf brackets
- Sixteen 12-24 x 0.75-inch (19.05-mm) panhead screws to attach the brackets to the posts (for 2-post rack installations only)
- Sixteen 10-32 x 0.38-inch (9.65-mm) panhead screws to attach the shelf to the brackets (also, to attach the brackets to the posts in 4-post rack installations)

Rack-Mounting the Chassis—1-Rack Unit Chassis

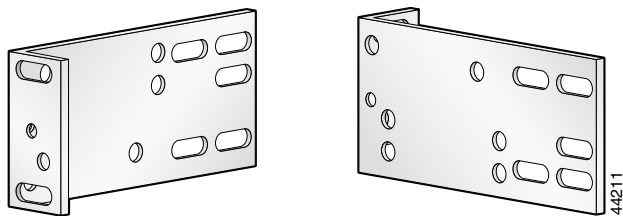
Single-rack unit (RU) chassis can be installed in 19-inch (48.26-cm) and 23-inch (58.42-cm) racks. The brackets for each rack are the same; however, they are mounted differently on the chassis. (See Figure 1.) Brackets for a 19-inch (48.26-cm) equipment rack require four rack screws in each bracket, and brackets for a 23-inch (58.42-cm) equipment rack require two screws in each bracket.

You can mount the chassis in the following ways:

- Front panel forward
- Rear panel forward
- Center-mounted in a 2-post rack with the front panel forward



Figure 1 *Rack-Mount Brackets*



Orientation for 19-inch rack Orientation for 23- or 24-inch rack

Attaching Brackets

Attach the mounting brackets to the chassis as shown, using the screws provided. (See Figure 1, Figure 2, Figure 3, Figure 4, and Figure 5.) Attach the second bracket to the opposite side of the chassis. Use a number 2 Phillips screwdriver to install the bracket screws.

Figure 2 *Bracket Installation—Front Panel Forward: 19-Inch (48.26-cm) Rack*

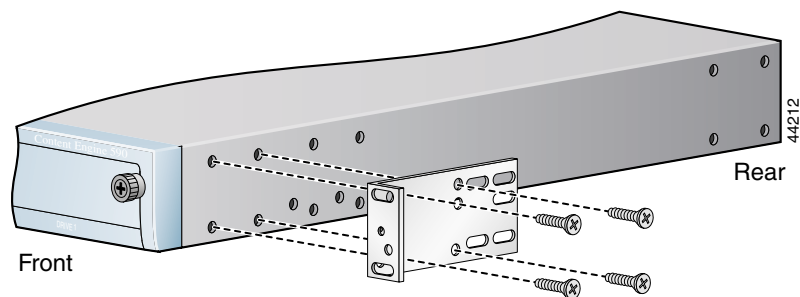


Figure 3 shows the bracket orientation for a front panel forward mount in a 23-inch (58.42-cm) equipment rack.

Figure 3 *Bracket Installation—Front Panel Forward: 23-Inch (58.42-cm) Rack*

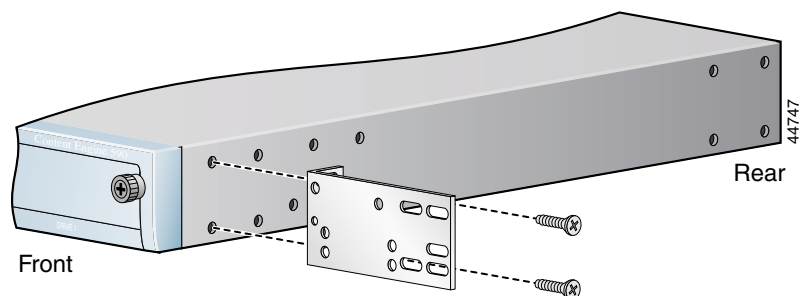
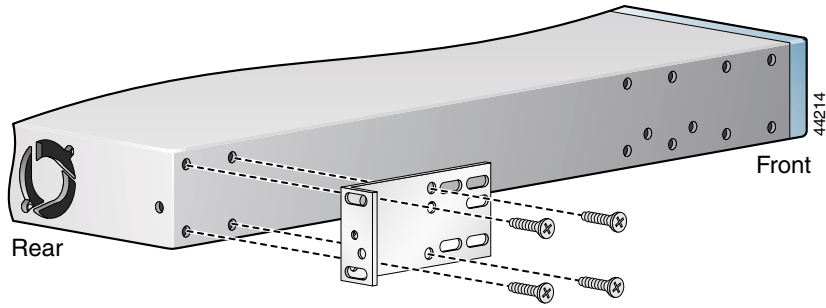


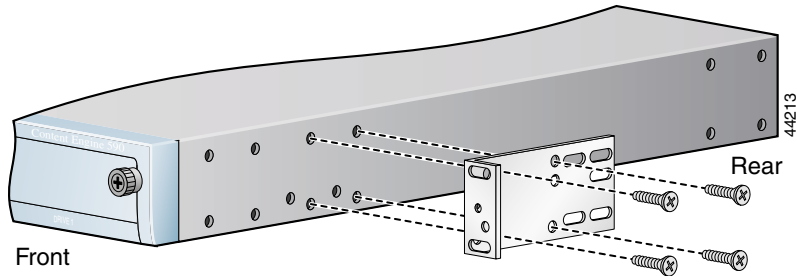
Figure 4 Bracket Installation—Rear Panel Forward: 19-Inch (48.26-cm) Rack



Note For a rear panel forward mount, the rear of the chassis is turned to face the front of the rack.

To center the chassis in a 2-post rack, use the bracket position shown in Figure 5.

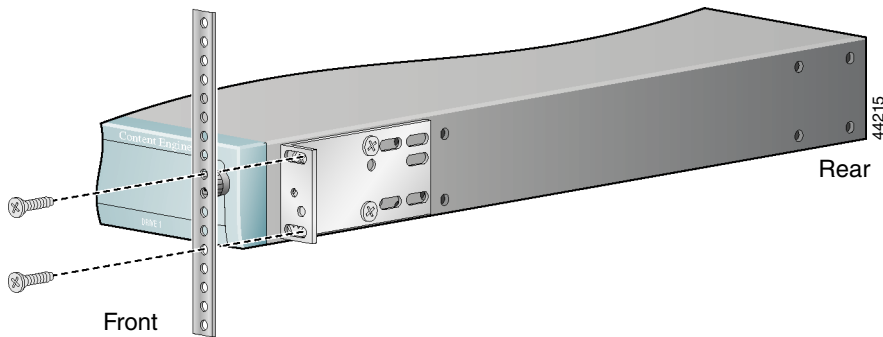
Figure 5 Bracket Installation—Center Mount with Front Panel Forward



Installing the Chassis in a Rack

After you secure the brackets to the chassis, rack-mount the chassis by securing the brackets to two posts or mounting strips in the rack. (See Figure 6.) Two people should install the chassis in the rack—one holds the chassis and the other secures it to the rack.

Figure 6 Installing the Chassis in a Rack



Note: The second bracket attaches to the other side of the chassis.



Rack-Mounting the Chassis—7-RU Chassis

The 7-RU chassis sits on a shelf that is attached to the equipment rack using brackets, the two flanges on the front of the shelf, or a combination of brackets and flanges. Secure the chassis to the shelf by attaching screws through the shelf into the chassis.

Installing the Shelf in a 2-Post Rack

Attach the shelf using four brackets, or else using only the flanges.



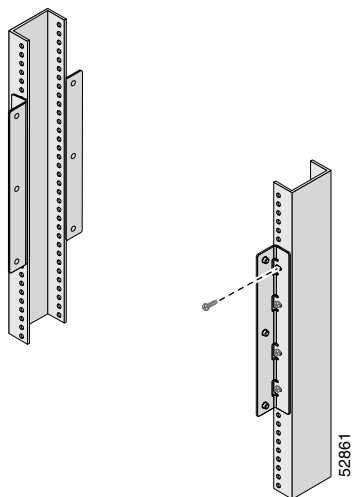
Warning The chassis should be mounted on a rack that is permanently affixed to the floor. Ensure that your equipment rack is bolted to the floor and secured.

Attaching the Shelf Using the Brackets

To attach the shelf using the brackets, first attach the brackets to the equipment rack posts, and then attach the shelf to the brackets. The brackets mount the shelf in the center of the rack. To attach the brackets to the rack posts, follow these steps:

-
- Step 1** Place the four-holed side of one bracket against the edge of one post with the three-holed flange perpendicular to and flush with the inside of the post. (See Figure 7.)
 - Step 2** Use four 12-24 x 0.75-inch (19.05-mm) screws to attach the bracket to the post.
 - Step 3** Repeat Step 1 and Step 2 to attach a bracket to the front and back edges of both posts. The brackets must be attached at the same height in the front and in the back and also at the same height on each post.
 - Step 4** Tighten the screws using a number 2 Phillips screwdriver.
-

Figure 7 Attaching the Brackets to the Rack Posts



Attaching the Shelf to the Brackets

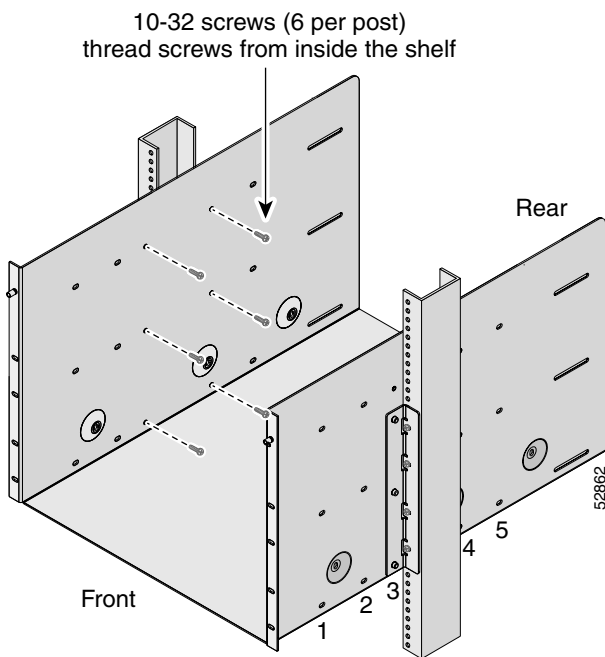
To attach the shelf to the brackets, follow these steps.



Caution At least two persons are required to perform this procedure. At least one person must hold the shelf in place while the other person attaches the shelf to the brackets.

-
- Step 1** Bring the shelf into the rack back-end first until it is centered in the rack. (See Figure 8.)
- Step 2** Align the shelf holes with the bracket holes. Use the third and fourth vertical line of holes from the front of the shelf. (See Figure 8.)
- Step 3** From inside the shelf, thread a 10-32 x 0.38-inch (9.65-mm) screw through the shelf and into the bracket standoff. Tighten the screw using a number 2 Phillips screwdriver.
- Step 4** Repeat Step 3 for all four brackets. Use three 10-32 x 0.38-inch (9.65-mm) screws for each bracket.
-

Figure 8 Attaching the Shelf to the Brackets



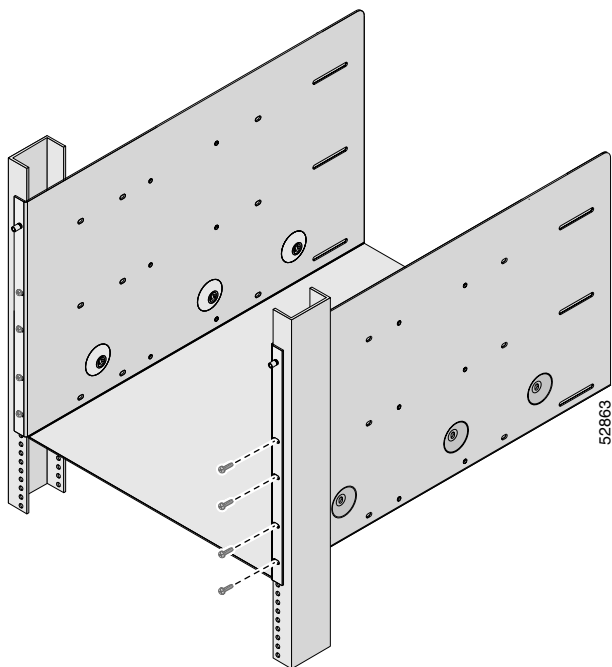
Attaching the Shelf Using the Flanges

To attach the shelf using the flanges on the front of the shelf, follow these steps. The flanges mount the shelf flush with the rack posts.

-
- Step 1** Bring the shelf into the rack back-end first until the front flanges on the shelf are flush against the front edges of the rack posts. (See Figure 9.)
- Step 2** Align the flange holes with the holes on the front edges of the rack posts.
- Step 3** Use four 12-24 x 0.75-inch (19.05-mm) screws in each flange to attach the shelf to the post.
- Step 4** Tighten the screws using a number 2 Phillips screwdriver.
-



Figure 9 Attaching the Shelf Using the Flanges



Installing the Shelf in a 4-Post Rack

To install the shelf in a 4-post rack, follow these steps.

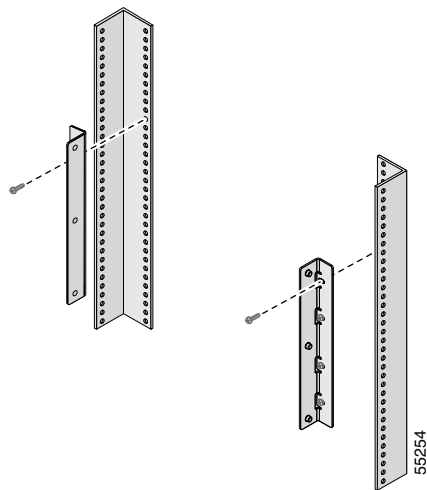


Warning

The chassis should be mounted on a rack that is permanently affixed to the floor. Ensure that your equipment rack is bolted to the floor and secured.

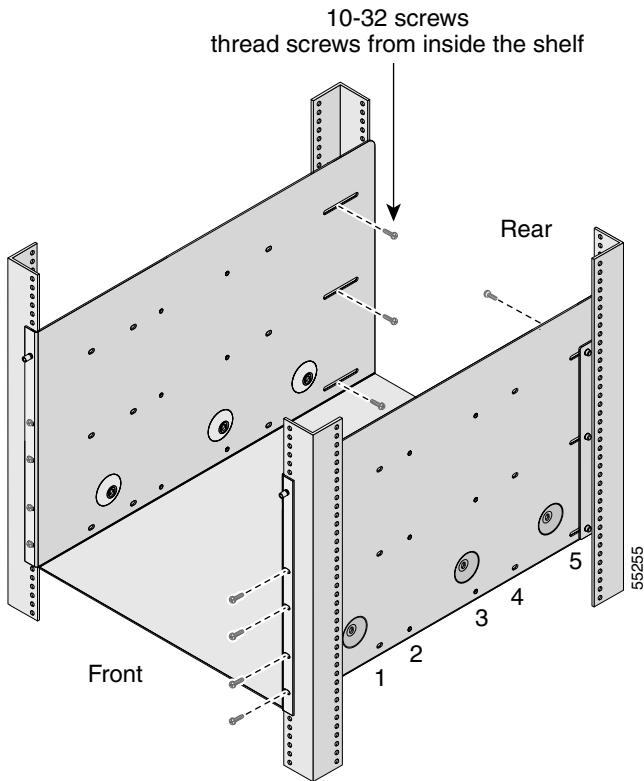
Step 1 Attach the brackets to the back mounting rails. (See Figure 10.)

Figure 10 Attaching Brackets to the Back Mounting Rails



Step 2 Attach the shelf to the front mounting rails using the flanges on the front of the shelf. (See Figure 11.)

Figure 11 Attaching the Shelf in a 4-Post Rack Using the Flanges



Step 3 Attach the shelf to the brackets on the back mounting rails. (See Figure 11.)

Mounting the Chassis in the Shelf



Caution At least two persons are required to lift the chassis.

To mount the chassis in the shelf, follow these steps:

Step 1 Lift the chassis onto the shelf and slide it into the rack back-end first. The front of the chassis should be flush with the front of the shelf.

Step 2 Secure the chassis to the shelf using the thumbscrews on the front of the chassis. The thumbscrews attach the chassis to the shelf through the flanges. (See Figure 12 and Figure 13.)



Figure 12 *Mounting the Chassis in a 2-Post Rack*

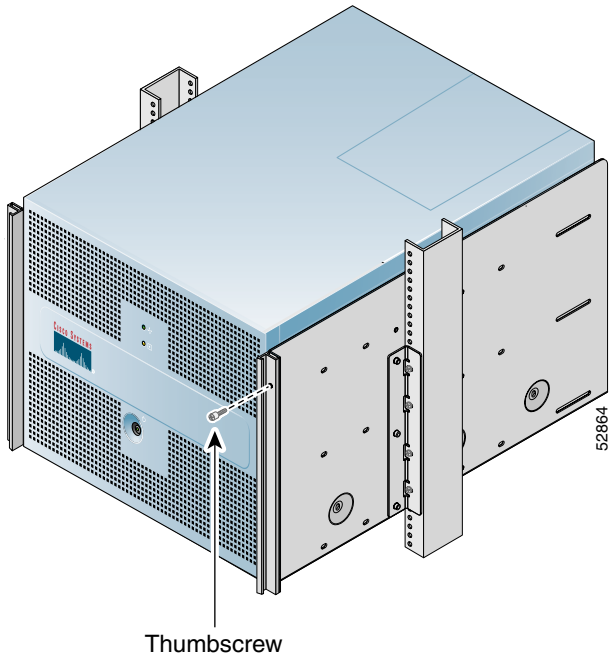
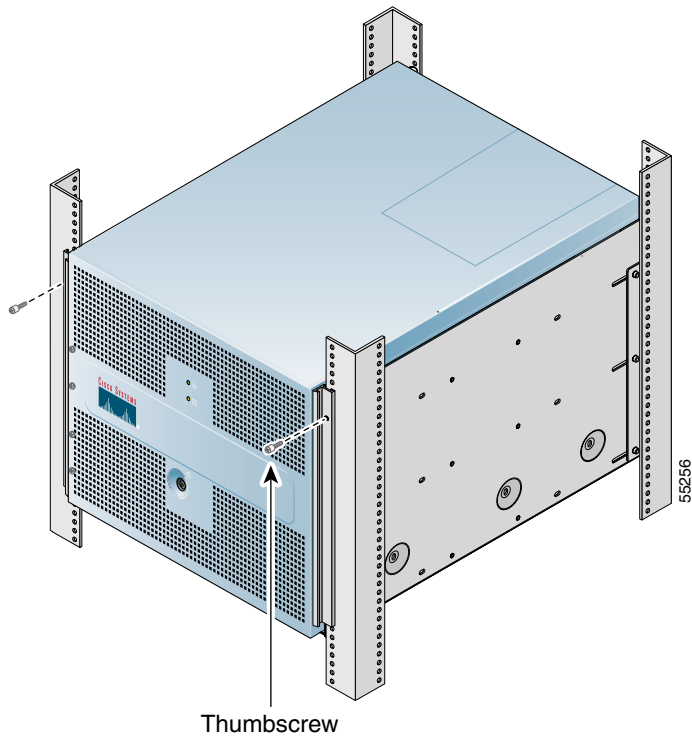


Figure 13 *Mounting the Chassis in a 4-Post Rack*



Installing the Chassis on a Tabletop

Ensure that the surface is clean and in a safe location and that you follow these guidelines:

- Install the chassis off the floor. (Dust that accumulates on the floor is drawn into the interior of the chassis by the cooling fans. Excessive dust inside the chassis can cause overtemperature conditions and component failures.)
- Provide approximately 19 inches (48.26 cm) of clearance at the front and rear of the chassis for accessing network cables or equipment.
- Ensure adequate ventilation (do not install the chassis in an enclosed cabinet where ventilation is inadequate).

Follow these steps to install the chassis on a workbench or tabletop:

-
- Step 1** Remove any debris and dust from the tabletop or workbench, as well as from the surrounding area. Also make sure that your path between the chassis and its new location is unobstructed.
- Step 2** Attach the rubber feet to the bottom of the chassis. The rubber feet have an adhesive backing. Peel the protective tape off the adhesive and stick the feet to the bottom of a clean chassis surface. Place one foot in each corner.
- Step 3** Place the chassis on the tabletop or workbench.
- Step 4** Ensure that no exhaust air from other equipment will be drawn into the chassis. Also, ensure that there is adequate clearance at the front and rear of the chassis.
-

4 Ground the Chassis

Before you connect power or turn on power to your system, we strongly recommend that you provide an adequate chassis ground (earth) connection for your chassis. Grounding receptacles are provided on each chassis.



Warning When installing the unit, the ground connection must always be made first and disconnected last.

The following parts and tools are required:

- Grounding lug
- Four 6 x 32 self-tapping screws
- 18-American Wire Gauge (AWG) grounding wire
- Flat-blade screwdriver
- Crimping tool large enough to accommodate the diameter of the wire receptacle on your grounding lug
- Wire stripper

To attach the grounding lug to the chassis grounding receptacles on your chassis, follow these steps:

-
- Step 1** Use the wire stripper to strip one end of the 18-AWG wire approximately 3/4 inch (19 mm).
- Step 2** Insert the ground wire into the wire receptacle on the grounding lug.
- Step 3** Use the crimping tool to carefully crimp the wire receptacle around the wire; this step is required to ensure a proper mechanical connection.
- Step 4** Insert the two screws through the holes in the grounding lug.
- Step 5** Locate the chassis grounding receptacles on your system chassis.
- Step 6** Use the flat-blade screwdriver to carefully tighten the screws until the grounding lug is held firmly to the chassis. Do not overtighten the screws.
- Step 7** Connect the opposite end of the grounding wire to the appropriate grounding point at your site.
-



5 Connect the Cables



Warning

Do not work on the system, or connect or disconnect cables during periods of lightning activity. To see translations of warnings that appear in this publication, refer to the *Regulatory Compliance and Safety Information* document that accompanied this device.



Warning

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables.

The connections described Table 1 provide network access, management access, and electrical power.

Table 1 Cable Connections

| Port or Connection | Connect To | Cable and Connector Type |
|---|---|---|
| Ethernet 0 (for 1-RU chassis use this network port only) | Hub or switch | Category 5 UTP cable with RJ-45-to-RJ-45 connectors (included) |
| 10BASE-T/100BASE-TX Ethernet/Fast Ethernet ports | Hub or switch | Category 5 UTP cables with RJ-45-to-RJ-45 connectors (included) |
| 1000BASE-SX Gigabit Ethernet ports | Hub or switch | Optical fiber cables with SC-type connectors |
| Console | PC or ASCII terminal communication port (usually labeled COM) | Rollover cable with RJ-45-to-RJ-45 connectors and 2 RJ-45-to-DB-9 adapters (included) |
| SCSI Channel B (for 7-RU chassis) SCSI LVD only (for 1-RU chassis) | Storage Array | SCSI cable (included with Storage Array only) |
| Power (AC) | 100–240 VAC, 50–60 Hz power outlet | Grounding power cord (included) |
| Power (DC) | See the “Connecting a DC Power Cord—1-RU Chassis” section on page 13 or the “Connecting a DC Power Cord—7-RU Chassis” section on page 14. | |

Connecting a DC Power Cord—1-RU Chassis

You need to supply your own DC power cord. In the United States use 14-American Wire Gauge (AWG) stranded or solid copper wire that is rated for a minimum temperature of 75°C (167°F); elsewhere consult local and national electrical code for proper wire sizing. Follow these steps to attach the wire to the DC connector terminals.



Caution

The DC power supply has a 130W output at 4.5A maximum current. Installation should be done in compliance with your national and local electrical code.



Warning

Before connecting or disconnecting ground or power wires to the chassis, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.

**Warning**

The customer 48 volt power system must provide reinforced insulation between the primary AC power and the 48 VDC output.

- Step 1** Loosen the terminal screws from the terminals marked plus (+) and minus (-) on the DC power receptacle.
- Step 2** Strip the ends of two DC power cable wires to expose approximately 1/4 inch (6.35 mm) of copper wire. Use only two strands of wire for the DC terminal. You do not need to wire the DC ground terminal. To ground the chassis, follow the grounding instructions in the “Ground the Chassis” section on page 12.
- Step 3** Depending on your site DC power source, connect two wires: one to the plus (+) terminal and one to the minus (-) terminal.
- If your source DC power is +48 volts, connect the +48 volt wire to the plus (+) terminal and the 0 (zero) volt wire to the minus (-) terminal.
 - If your source DC power is -48 volts, connect the -48 volt wire to the minus (-) terminal and the 0 (zero) volt wire to the plus (+) terminal.

**Note**

The higher-voltage wire is always connected to the plus (+) terminal. You can use a voltage meter to measure the voltage on each terminal. You must maintain a +48 voltage between the two terminals with the higher-voltage wire connected to the plus (+) terminal.

- Step 4** Tighten the terminal screws using a screwdriver.
- Step 5** Connect the other end of the DC power cord to your site power source.
- Step 6** To power up the device, press the power switch. This switch toggles between on and off. A power light on the front panel, when lit, indicates that the power is on.
-

The system should begin booting. Once the operating system boots, you are ready to configure the network settings. (See the “Perform an Initial Startup Configuration” section on page 16.)

**Note**

If you have wired the DC terminals incorrectly, the Content Engine will not boot. Incorrect wiring will not damage your system or cause you any harm. If your system fails to boot because you have wired the DC terminals incorrectly, simply switch the wires between the two terminals.

Connecting a DC Power Cord—7-RU Chassis

You need to supply your own DC power cord. In the United States use 14-AWG stranded or solid copper wire that is rated for a minimum temperature of 75°C (167°F); elsewhere consult local and national electrical code for proper wire sizing. Use the Cisco-supplied DC connector and follow these steps to attach the wire to the DC connector terminals.

**Caution**

The DC power supply cord requires 14-AWG wire that is rated for a minimum temperature of 75°C (167°F). The DC power supply has a 320W output at 14A maximum current. Installation should be done in compliance with your national and local electrical code.

**Warning**

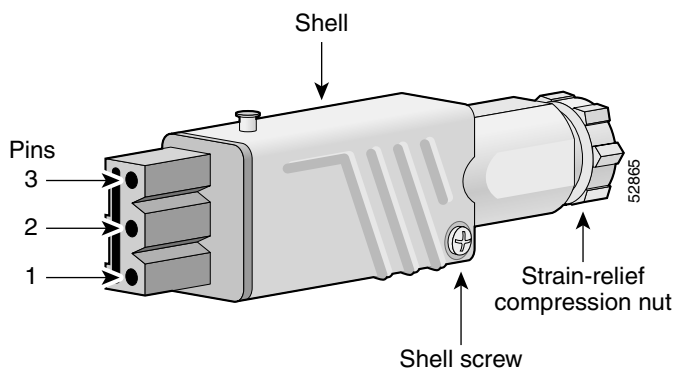
Before connecting or disconnecting ground or power wires to the chassis, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.



Warning The customer 48 volt power system must provide reinforced insulation between the primary AC power and the 48 VDC output.

Step 1 Loosen the strain-relief compression nut on the end of the DC connector shell. (See Figure 14.)

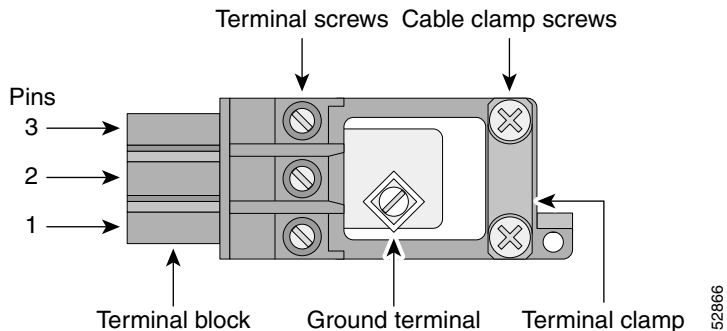
Figure 14 DC Connector with Shell



Step 2 Using a flat-blade screwdriver, loosen the shell screw and remove the shell from the terminal block.

Step 3 Loosen the two cable clamp screws. (See Figure 15.)

Figure 15 DC Connector with Shell Removed



Step 4 Loosen the terminal connector screws from terminal pin 1 and terminal pin 3.

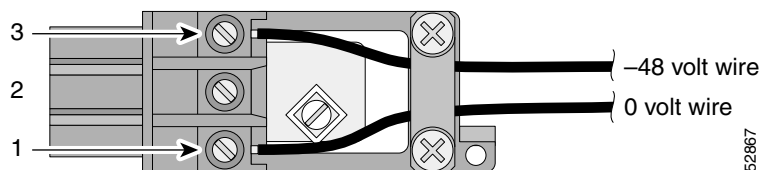
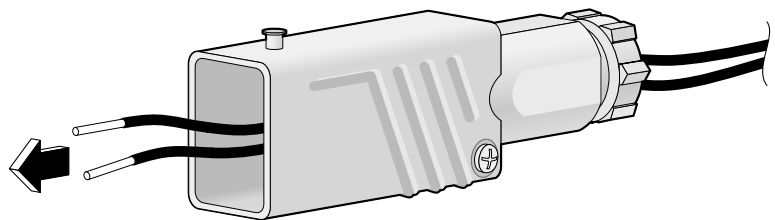
Step 5 Strip the ends of two DC power cable wires to expose approximately 1/4 inch (6.35 mm) of copper wire.

Step 6 Feed the two power cable wires through the shell and then through the cable clamp at the base of the terminal block.

Step 7 Connect the 0 (zero) volt wire to terminal pin 1 and tighten the terminal block connector screw.

Step 8 Connect the -48 volt wire to terminal pin 3 and tighten the terminal block connector screw. (See Figure 16.)

Figure 16 Wiring the DC Connector



Note Use only two strands of wire for the DC connector. Do not wire the DC connector ground terminal shown in Figure 15. To ground the chassis, follow the grounding instructions in the “Ground the Chassis” section on page 12.

- Step 9** Tighten the cable clamp screws.
- Step 10** Slide the shell over the DC terminal block and tighten the shell screw.
- Step 11** Tighten the strain-relief compression nut.
- Step 12** Plug the DC power cord into the DC power supply receptacle.
- Step 13** Connect the other end of the DC power cord to your site DC power source.
- Step 14** Repeat Step 1 through Step 11 for all power supplies in your system.
- Step 15** Power up the device.
The system should begin booting. Once the operating system boots, you are ready to perform an initial software configuration.

6 Perform an Initial Startup Configuration

After you physically install the hardware and power up your Content Engine, Content Router, or Content Distribution Manager, you must access the ACNS software and perform an initial startup configuration.

Initial Startup Overview

The initial configuration defines the network settings of your Content Engine, Content Router, or Content Distribution Manager so that your devices become active on your network.



Note If you have upgraded your software from a previous software release to ACNS software, your network configuration is preserved. You do not need to reconfigure your network settings.



Network Settings

If you have direct console access to the device, you can use the ACNS software initial startup dialog to configure your network settings and access the command-line interface (CLI). If you have a Windows-based PC on the same subnet as your content networking device, you can use the Installation Wizard that is part of the ACNS software E-CDN application to configure the network settings of your devices.

Application Information Summary

ACNS software can be used in the following ways:

- Cache application only
- E-CDN application only
- Both Cache and E-CDN applications running at the same time

To initialize ACNS software before using either application, you must complete the following tasks:

1. Configure network settings.
 - Using the CLI-based startup dialog—recommended when you are using only the Cache application
 - Using the PC-based Installation Wizard—recommended when you are using the E-CDN application alone or with the Cache application
2. (Optional) Set up and enable the E-CDN application.
 - a. Allocate disk space using the CLI.
 - b. Enable the E-CDN application using the CLI.
 - c. Associate the device with the IP address of the Content Distribution Manager using the Installation Wizard.
 - d. (Optional) Configure HTTP proxy server settings using the Installation Wizard.
 - e. Approve the newly associated Content Engine or Content Router using the Content Distribution Manager graphical user interface (GUI).



Note

In order to use the E-CDN application, you must enable it on all devices that are going to run the application. The E-CDN application can be enabled through the ACNS software CLI only. The Cache application is always enabled in the ACNS software.

The following table summarizes the initial configuration tasks and describes the recommended user interface.

| Application | Task | Recommended User Interface |
|------------------------------------|---|----------------------------------|
| Cache only | Configure network settings | CLI-based startup dialog |
| E-CDN only or both Cache and E-CDN | Configure network settings | Installation Wizard |
| | Allocate disk space | CLI (required) |
| | Enable the E-CDN application | CLI (required) |
| | Associate the device | Installation Wizard |
| | Configure HTTP proxy server settings (optional) | Installation Wizard (required) |
| | Approve device | Content Distribution Manager GUI |

Configuring Network Settings

In order to configure network settings, you must first gather the required network information for your device and then choose between two different methods of accessing the device:

1. Direct console access to the Content Engine, Content Router, or Content Distribution Manager
A console allows you to use the CLI-based startup dialog and to access the CLI.
2. Network access to the Content Engine, Content Router, or Content Distribution Manager
Network access from a Windows-based PC allows you to use the Installation Wizard and to access the CLI through a Telnet session. (Your PC workstation must be on the same subnet as your Content Distribution Manager, Content Engines, and Content Routers in order for the Installation Wizard to work properly.)

Gathering Required Network Information

Have the following information available. When you power up the Content Engine, Content Router, or Content Distribution Manager and open a console connection for the first time, you are prompted to provide this information:

- Host name
- Domain name
- Administrator password
- Interface identifier (initial physical network interface) (See “Identifying Interfaces”)
- IP address
- IP network mask
- Gateway IP address
- Domain Name System (DNS) name server IP address

Identifying Interfaces

When you configure network settings for the 1-rack unit and 7-rack unit chassis, use the following information to configure the network interfaces.

Interface Numbering—1-RU Chassis

The 1-RU chassis has two Ethernet/Fast Ethernet interfaces, which are identified as follows:

- Ethernet 0
- Ethernet 1

Interface Numbering—7-RU Chassis

The 7-RU chassis can have two Gigabit Ethernet interfaces (depending on the model) and four Ethernet/Fast Ethernet interfaces. These interfaces are identified by chassis slot number and port number in the form *slot/port*.



Note The 1000BASE-SX Gigabit Ethernet interfaces are not available in all hardware configurations of the 7-RU chassis.

The 1000BASE-SX ports are located in network interface card slot 1 and slot 2 (see Figure 17) and are numbered *slot/port* as follows:

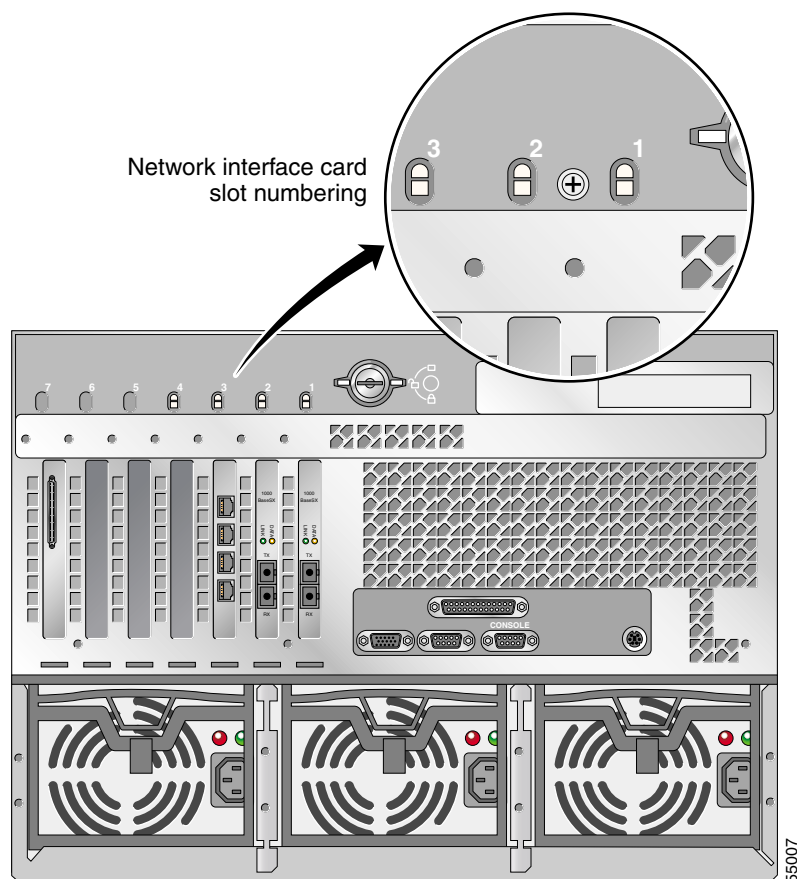
- GigabitEthernet 1/0
- GigabitEthernet 2/0



The 10BASE-T/100BASE-TX ports are located in network interface card slot 3 and are numbered *slot/port* from top to bottom as follows:

- Ethernet 3/0
- Ethernet 3/1
- Ethernet 3/2
- Ethernet 3/3

Figure 17 Network Interface Card Slot Numbering



Configuring Network Settings Using the CLI-Based Startup Dialog

To configure network settings, follow these steps:

Step 1 Power up the device and open a console connection.

After the operating system boots up, the following prompt appears:

```
ACNS boot:detected no saved system configuration
Do you want to enter basic configuration now?
hit RETURN to enter basic configuration:0028
```

At the appearance of this prompt, a 30-second countdown begins, during which you can respond to this prompt. If you do not respond, the system automatically continues booting.

Step 2 Enter **yes**, and then enter values for the following fields as you are prompted:

- Host name for the device
- Domain name for the device
- Admin password for the device

This is the case-sensitive password you want to use for the **admin** administrator user account. The password can include any printable character. You must enter a password for each Content Networking device.



Note After the device is connected to the Content Distribution Manager, the password specified in the Content Distribution Manager GUI will overwrite the one specified here.

- Interface identifier for the initial configuration
All other interfaces can be configured later with the CLI.
- IP address for the device, for example, 172.16.13.8
- IP network mask for the device, for example, 255.255.255.224
A netmask specifies which part of the IP address refers to the network; you can accept the default value by pressing **Enter**, or you can enter a different value.
- Gateway IP address for the device, for example, 172.16.13.7
This is the IP address of the router that allows the device to connect to the network.
- DNS name server IP address for the device

After you enter the initial configuration data, the following prompt appears:

```
Use this configuration? [yes]:
```

Step 3 If the initial configuration is acceptable, enter **yes** or press **Enter**.


The device performs hardware and software initialization tasks and then serves a login challenge that, when answered correctly, launches the CLI. At this point, the initial configuration is complete.

In the following sample startup dialog, administrator entries are shown in bold.

```
INIT:Entering runlevel:3
Nodemgr started!
ACNS boot:detected no saved system configuration
Do you want to enter basic configuration now?
hit RETURN to enter basic configuration:0028
host name:ce-590
domain name:cisco.com
admin password:*****
re-enter password:*****
Please enter an interface from the following list:
  0:FastEthernet 0/0
  1:FastEthernet 0/1
enter choice:0
local IP address:172.16.193.247
IP network mask:255.255.255.224
gateway IP address:172.16.193.225
DNS server:172.16.2.133
Use this configuration? [yes]:yes
```




Configuring Network Settings Using the Installation Wizard


 **Note** You must have a PC workstation running the Windows 95/98, Windows 2000, or Windows NT operating system on the same subnet as your Content Distribution Manager, Content Engines, and Content Routers in order for the Installation Wizard to work properly.

To configure network settings using the Installation Wizard that is part of the E-CDN application, follow these steps:

-
- Step 1** Insert the Installation Wizard CD-ROM into the CD-ROM drive on your workstation.
 - Step 2** Locate the *setup.exe* file and double-click it.
 - Step 3** After the Installation Wizard is automatically installed, go to C:/Program Files/Cisco Systems/CDN Wizard/cdnwiz.exe. Double-click the *cdnwiz.exe* file to launch the Installation Wizard. The Cisco Content Delivery Network Installation Wizard screen appears.
 - Step 4** Click **Next** to advance to the Select a Device screen, which lists all Enterprise CDN devices on the subnet by their device ID or by a user-friendly name previously assigned using the Installation Wizard.


 **Note** The Installation Wizard shows only the devices that are connected to the same local segment as the Windows PC that is running the Installation Wizard program.

- Step 5** Choose the first device that you want to configure and click **Next** to advance to the Name screen.

 **Tip** If you cannot determine by the MAC address which device to configure, choose a device and click **Details** to display the Device Details screen.

You can also sort devices by right-clicking in the area where the devices are listed and choosing one of the sort options from the shortcut menu that appears. You can sort devices by device name (Sort by Device), status, type, version, or IP address.

-
- Step 6** If you have not already done so, enter a user-friendly name in the field provided. This name supplements the alphanumeric device ID or MAC address and makes it easier to identify the device when you use the Installation Wizard or Content Distribution Manager GUI.
 - Step 7** Click **Next** to advance to the Obtain Network Settings Automatically (DHCP) screen.
 - Step 8** Indicate whether or not you are using a DHCP server:
 - If you are using DHCP, choose **Yes**.

 **Note** If you are configuring the Content Distribution Manager and want to use DHCP, you must have DHCP configured to statically assign an IP address to the Content Distribution Manager. That is, even with DHCP, the IP address of the Content Distribution Manager cannot be a different IP address assigned by DHCP between reboots.

- If you are not using DHCP and are configuring E-CDN devices manually, choose **No** and then click **Next**. The Network Settings screen appears.
 - Place your cursor in the IP address field and enter the network IP address, using the arrow key to move from block to block.
 - Press the **Tab** key to advance to the following fields and enter the subnet mask, as well as the gateway address used by the selected device.



Note If you do not know the exact IP address of any of these components, or if you are not sure whether your network is using static IP addresses, consult with your network administrator before proceeding.

- Step 9** Click **Next** to proceed to the DNS-Domain Name System screen and then perform one of the following actions:
- To configure a Domain Name Server, choose **Yes** and then click **Next** to advance to the DNS Servers screen and provide the IP addresses of DNS servers referenced by your E-CDN devices.
 - If you are not using DNS, choose **No**.

- Step 10** Click **Next** to advance to the Settings screen to review the configuration settings for your device.
- If the information is not accurate, click **Back** to step back through the Installation Wizard and change the configuration information.
 - Otherwise, click **Finish** to configure the device using the settings displayed and advance to the Configuring screen to confirm configuration of the device.



Note After you click **Finish** in the Installation Wizard, a status box appears. Ultimately, you see the device status as “online.” Before the device status shows as online, however, it may actually show as “failed.” This usually happens when the device needs to be rebooted for the changes to take effect. While it is rebooting, the Installation Wizard loses communication with it, and the device status shows as failed. However, if you wait for the device to finish booting, the status in the Installation Wizard should change to online.

- Step 11** From the Configuring screen, perform one of the following actions when the device comes online. (The machine status indicator turns green and reads “online” if the device is online.)
- Click **More** to return to the Select a Device screen and configure network settings for another device.



Tip If you want to copy the information for use in another application, document, or e-mail, click **Copy info** to copy the configuration settings to your Windows clipboard. You can then paste the information into another Windows application.

If the device fails to come online, click **Back** and review your configuration settings.



Note It is normal for the device status to be “offline” for a minute or so during an initial configuration. But if the device does not come online within a few minutes, you might need to run the Installation Wizard again.

- Click **Exit** to close the Installation Wizard.



Note Additional screens used to associate a Content Distribution Manager with E-CDN devices and configure proxy settings are available when you reopen the Installation Wizard after you have enabled the E-CDN application through the CLI.

Where to Go Next

Once you have completed the initial network configuration, you are ready to configure Cache application features or you can begin setting up the device for the E-CDN application.

To configure the Cache application, refer to the *Cisco Application and Content Networking Software Caching Configuration Guide* available on the Documentation CD-ROM and on Cisco.com.



You can access this document on the Documentation CD-ROM at **Cisco Product Documentation > Content Delivery Products > Cisco Application and Content Networking Software > Cisco Application and Content Networking Software, Release 4.1.**

On Cisco.com, go to <http://cisco.com/univercd/cc/td/doc/product/webscale/uce/uce41/index.htm>.

To set up the E-CDN application, proceed to the next section, which includes these tasks:

- Allocating disk space
- Enabling the E-CDN application
- Associating the device with the Content Distribution Manager
- Approving the device within the Content Distribution Manager GUI

7 Set Up and Enable the E-CDN Application

Before you can use the ACNS software E-CDN application, you need to complete the following tasks:

1. Allocate disk space on the Content Engine, Content Router, or Content Distribution Manager for the E-CDN application. You must use the device CLI to perform this task. If you do not have direct console access to the device CLI, you need to open a Telnet session to the device CLI.
2. Enable the E-CDN application on the Content Engine, Content Router, or Content Distribution Manager. You must use the device CLI to perform this task. If you do not have direct console access to the device CLI, you need to open a Telnet session to the device CLI.



Note If your system has been upgraded to ACNS software from a previous release of E-CDN software, then the E-CDN application in ACNS software is enabled by default. If you upgraded to ACNS software from Cache 2.x software or Cache 3.x software, then you must enable the E-CDN application before you can use it.

3. Associate the Content Engine or Content Router with the IP address of the Content Distribution Manager.



Note Although you can also associate the Content Engine or Content Router with the IP address of the Content Distribution Manager using the CLI, we recommend that you use the Installation Wizard to do this after enabling the E-CDN application on the CLI. Additional Content Distribution Manager and E-CDN proxy setting screens are accessible from the Installation Wizard once the E-CDN application has been enabled.

4. Approve the Content Engine or Content Router in the Content Distribution Manager GUI to bring the device online.



Note Only Content Engines or Content Routers that are newly associated with the Content Distribution Manager need to be approved in the Content Distribution Manager GUI.

Allocating Disk Space for the E-CDN Application

The E-CDN application uses the `ecdns` file system type for storage and must first be assigned some amount of disk space. If you do not have direct console access to the device CLI, then you need to open a Telnet session to the device CLI. To allocate disk space for the E-CDN application, follow these steps:

Step 1 Use the `show disks current` command to check the current disk configurations.



Note The `show disks details` command shows that there is 3 to 4 GB of disk space allocated to system use. This detail is not shown by using the `show disks current` command.

Step 2 To assign disk space to all file system types (sysfs, cfs, ecdnfs, and mediafs), use the **disk config** command. Amounts of disk space can be specified as percentages, megabytes, or gigabytes, or as “remaining” to assign all remaining disk space to a given file system.

Adjust the allocation percentages for the ecdnfs and other file system types as needed, for example:

```
ContentEngine# disk config sys 10% cfs 30% ecdnfs 40% mediafs 0%
```

For disk-space allocation guidelines, refer to the *Cisco ACNS System Maintenance and Troubleshooting Guide*.



Note Because of memory restrictions in the CE-507, the maximum disk storage allocation for cfs in the E-CDN application is 6 GB . For example, you might adjust the disk storage allocations as follows:

```
ce-507# disk config sysfs 2GB cfs 6GB mediafs 2GB ecdnfs remaining
```

Step 3 Check your disk-space allocation using the **show disks configured** command. This command shows what disk configuration is to take effect after you reboot your system.

Step 4 Reboot your system using the **reload** command for the new configuration to take effect.

You are now ready to enable the E-CDN application.

Enabling the E-CDN Application

Once you have allocated disk space for the ecdnfs, you can then enable the E-CDN application from the CLI. If you do not have direct console access to the device CLI, then you need to open a Telnet session to the device CLI. Complete the following steps to enable the E-CDN application:

Step 1 Enable the E-CDN application on the Content Engine, Content Router, or Content Distribution Manager from the CLI:

```
console(config)# ecdn enable
```

Step 2 To check the status of the E-CDN application, use the **show ecdn EXEC** command. Allow 2 minutes after enabling the E-CDN application and before checking the status for the settings to be applied.

```
ContentEngine# show ecdn  
ECDN content engine is loading, state is no-sonoma, Waiting for CDN configuration.  
For more information, point your browser to CDM 0.0.0.0
```

After the E-CDN application is enabled, see the “Associating Content Engines or Content Routers with the Content Distribution Manager” section on page 25 for information about using the Installation Wizard for further setup task options.

Disabling the E-CDN Application

To disable the E-CDN application, enter the following ACNS software command from the CLI:

```
console(config)# no ecdn enable
```

To verify the status of the E-CDN application, whether it is running or disabled, use the **show ecdn EXEC** command. Allow 5 minutes for the settings to be applied between disabling E-CDN and checking the status.

```
ContentEngine# show ecdn  
ECDN content engine is not running; server 'bootnet' is 0, 'checkup' is 0.  
If you'd like to turn on ECDN, use config command 'ecdn'.  
If you have, then the watchdog will restart in 10 mmin.
```




Associating Content Engines or Content Routers with the Content Distribution Manager

All Content Engines and Content Routers must be associated with a Content Distribution Manager in order for the Content Distribution Manager to be able to manage the Content Engine or Content Router. This is done by entering the IP address and, optionally, the port number of the Content Distribution Manager in the Content Engine or Content Router configuration.



Note Content Distribution Managers do not need to be associated with one another; therefore, this setup task applies only to the Content Engine and Content Router configuration.

You can associate the Content Engine or Content Router with the IP address of the Content Distribution Manager in two different ways:

1. Through network access to the Content Engine or Content Router from a Windows-based PC on the same subnet running the Installation Wizard (recommended).
2. Through direct console access to the Content Engine or Content Router command-line interface (CLI). If you do not have direct console access to the device CLI, then you need to open a Telnet session to the device CLI.

Associating Content Engines or Content Routers with the Content Distribution Manager Using the Installation Wizard

To use the Installation Wizard to associate the Content Engine or Content Router with the IP address of the Content Distribution Manager, follow these steps:

Step 1 Return to the Installation Wizard.

- If you are still on the Configuring screen, click **More** to return to the Select a Device screen, which lists all E-CDN devices on the subnet by their device ID or by a user-friendly name previously assigned using the Installation Wizard. If necessary, click **Refresh** for your newly configured device to appear in the Device List.
- If you previously exited from the Installation Wizard, reopen the wizard and navigate forward by clicking **Next** until you reach the Select a Device screen.



Note The Installation Wizard shows only the devices that are connected to the same local segment as the Windows PC that is running the Installation Wizard program.

Step 2 Choose the first device that you want to associate and click **Next** to advance to the Name screen.

Step 3 Click **Next** to accept the Name screen settings and advance to the Content Distribution Manager screen, or see the “Configuring Network Settings Using the Installation Wizard” section on page 21 for more information on providing a device name.

Step 4 Perform one of the following actions on the Content Distribution Manager screen:

- Choose **Name** to identify the Content Distribution Manager by its DNS name, and enter the DNS name in the field provided.
- Choose **IP address** to identify the Content Distribution Manager by its IP address, and enter the IP address in the field provided in valid “dotted quad” format, for example:

192.168.0.0

If the port number of the Content Distribution Manager is other than the default of 80, enter the new port number in the field provided.

**Note**

You have now entered the information necessary to associate your device with a Content Distribution Manager; however, in order for these settings to take effect, you must continue through the remainder of the Installation Wizard screens and click **Finish** at the end.

Configuring HTTP Proxy Server and Other E-CDN Application Settings

The following steps explain how to configure optional HTTP proxy server settings and other E-CDN application settings presented in the remainder of the Installation Wizard screens. If you have already configured these options, or choose not to configure them, continue to the end of the Installation Wizard by clicking **Next** at each screen, and then proceed to Step 7.

-
- Step 1** Click **Next** to advance to the Obtain Network Settings Automatically (DHCP) screen.
- Step 2** Click **Next** to accept the Obtain Network Settings Automatically (DHCP) screen settings and advance to the DNS-Domain Name System screen, or see the “Configuring Network Settings Using the Installation Wizard” section on page 21 for more information on configuring DHCP.
- Step 3** Click **Next** to accept the DNS-Domain Name System screen settings and advance to the Proxy Server screen, or see the “Configuring Network Settings Using the Installation Wizard” section on page 21 for more information on specifying DNS servers.
- Step 4** Indicate whether or not you are using a proxy server:
- If you are using a proxy server, choose **Yes** and then click **Next**. The Proxy Settings screen appears.
 - In the fields provided, enter the IP address of the proxy server and the number of the designated port through which traffic will pass (usually 80).
 - Click **Next** to advance to the Secure Proxy Server screen.
 - If you are not using a proxy server, choose **No** and then click **Next** to advance to the Secure Proxy Server screen.
- Step 5** Indicate whether or not you are using a secure proxy server:
- If you are using a secure proxy server, choose **Yes** and then click **Next**. The Secure Proxy Settings screen appears.
 - In the fields provided, enter the IP address, port number, and proxy server username and password.
 - Click **Next** to advance to the Proxy Exceptions List screen.
 - If you are not using a proxy server, choose **No** and then click **Next** to advance to the Proxy Exceptions List screen.
- Step 6** Perform one of the following actions on the Proxy Exceptions List screen:
- If you do not have addresses that you wish to treat as proxy exceptions, choose **No**, and then click **Next** to advance to the Settings screen to review the configuration settings for your selected device.
 - If you have addresses that you do not want to connect through your proxy or secure proxy server, choose **Yes** and then click **Next**. The Proxy Exceptions screen appears.
 - Enter the IP address of your first exception in the field provided, and then click **Add** to add it to the list of exceptions immediately below.
 - Repeat this step for each exception. If you make a mistake, choose the exception address in the list of exceptions, and then click **Remove** to remove the address from the list.
 - When you have finished adding exceptions, click **Next** to advance to the Settings screen to review the configuration settings for your Content Engine or Content Router.
- Step 7** Review the configuration settings for your device on the Settings screen.
- If the information is not accurate, click **Back** to step back through the Installation Wizard and change the configuration information.
 - Otherwise, click **Finish** to configure the device using the settings displayed and advance to the Configuring screen to confirm configuration of the device.

**Note**

After you click **Finish** in the Installation Wizard, a status box appears with configuration information. Ultimately, the device status is “online”; however, if it is a new Content Engine or Content Router, it must first be approved within the Content Distribution Manager GUI before the device status changes to online. Before the device status shows as online, however, it may actually show as “failed.” This usually happens when the device needs to be rebooted for the changes to take effect. While it is rebooting, the Installation Wizard loses communication with it, and the device status shows as failed. However, if you wait for the device to finish booting, the status in the Installation Wizard should change to online.

Step 8 From the Configuring screen, perform one of the following actions:

- Click **More** to return to the Select a Device screen and associate another of your CDN devices, or click **Exit** to close the Installation Wizard.

The following message appears in the status box:

```
Waiting for approval from CDM
```

The device will not come online until it has been approved within the Content Distribution Manager GUI.

- Click **Back** and review your configuration settings.

You are now ready to approve the device using the Content Distribution Manager GUI. See the “Approving Content Engines or Content Routers in the Content Distribution Manager GUI” section on page 28 for information on approving a new device.

Associating Content Engines or Content Routers with the Content Distribution Manager Using the CLI

You can associate Content Engines or Content Routers with the Content Distribution Manager IP address using the CLI. If you do not have direct console access to the device CLI, then you need to open a Telnet session to the device CLI.

**Note**

You must associate the Content Engine or Content Router with the IP address of the Content Distribution Manager using the CLI *before* enabling the E-CDN application on the Content Engine or Content Router.

To associate the Content Engine or Content Router with the IP address of the Content Distribution Manager using the CLI, follow these steps:

Step 1 From the Content Engine or Content Router CLI, enter the following command:

```
console(config)# ecdn cdm ip cdm-ip-address
```

You can optionally specify the port number, where a valid port number ranges from 1 to 65535, if the port number of the associated Content Distribution Manager has been configured to a number other than the default of 80:

```
console(config)# ecdn cdm ip cdm-ip-address port port-number
```

If the port number is not specified, the port number is set to a default value of 80.

Step 2 Enable the E-CDN application on the Content Engine, Content Router, or Content Distribution Manager from the CLI:

```
console(config)# ecdn enable
```

Step 3 To verify the IP address of the associated Content Distribution Manager on the Content Engine or Content Router, use the `show ecdn EXEC` command.

Allow 2 minutes for the settings to be applied after associating a device with the Content Distribution Manager and before checking the status.

```
ContentEngine# show ecdn
ECDN content engine is loading, state is no-studio, Waiting for approval from CDM.
ECDN is trying to connect to CDM
Please configure CDM ip and port and don't forget to approve it from CDM web UI
For more information, point your browser to CDM 172.31.76.76
```

You are now ready to approve the device using the Content Distribution Manager GUI.

Approving Content Engines or Content Routers in the Content Distribution Manager GUI

New Content Engines and Content Routers need to be approved by the Content Distribution Manager in order for the device to come online. To approve a Content Engine or Content Router using the Content Distribution Manager GUI, follow these steps:

Step 1 Open the Content Distribution Manager GUI from your web browser by entering the URL or IP address of the Content Distribution Manager. For example, from your browser, enter:

```
http://name_of_Content_Distribution_Manager
```

or

```
http://IP_address_of_Content_Distribution_Manager
```

If a screen appears requesting your username and password, the Content Distribution Manager was successfully activated and is up and running on your network.

Step 2 Enter the administrator username and password and then click **OK**. The Cisco Content Distribution Manager window appears.

Step 3 Click **Device Console**. The new device appears with a caution status indicator in the online column.

Step 4 Click **Edit** to edit the device settings. From the Identification screen, check the **Approve** check box.

Step 5 Click **Save Changes**.

Step 6 After the device has been approved from within the Content Distribution Manager GUI, verify the approval by performing one of the following actions:

- If you are running the Installation Wizard, return to the Installation Wizard and wait for the Content Distribution Manager approval to register.



Note It may take a few moments for the new device to integrate the new configuration settings and come back online. Monitor the status messages provided on the Configuring screen and verify that your Content Engine or Content Router device is able to come online properly.

The machine status indicator located beneath the **Copy info** button will turn green and read “online.”

- Once the device status is “online,” click **More** to return to the Select a Device screen and configure another of your CDN devices, or click **Exit** to close the Installation Wizard.
- If the device fails to come online, click **Back** and review your configuration settings.

**Note**

Ultimately, you see the device status as “online.” Before the device status shows as online, however, it may actually show as “failed.” This usually happens when the device needs to be rebooted for the changes to take effect. While it is rebooting, the Installation Wizard loses communication with it, and the device status shows as failed. However, if you wait for the device to finish booting, the status in the Installation Wizard should change to online.

- If you are using the device CLI, use the **show ecdn EXEC** command to verify that the E-CDN application is running. Allow 10 minutes for the settings to be applied after approving the device in the Content Distribution Manager GUI and before checking the status.

```
ContentEngine# show ecdn
ECDN content engine is running, state is online, Running normally.
For more information, point your browser to CDM 172.31.76.76
```

Where to Go Next

To use the E-CDN application, refer to the *Cisco Application and Content Networking Software E-CDN Administrator's Guide* available on the Documentation CD-ROM and on Cisco.com.

You can access this document on the Documentation CD-ROM at **Cisco Product Documentation > Content Delivery Products > Cisco Application and Content Networking Software > Cisco Application and Content Networking Software, Release 4.1**.

On Cisco.com, go to <http://cisco.com/univercd/cc/td/doc/product/webscale/uce/uce41/index.htm>.

8 Enable Licensed Software

The following licensed software programs require the purchase of a license from Cisco:

- Windows Media Technologies (WMT)—License covers use as both a proxy for the Cache application and as a WMT server for the E-CDN application
- RealNetworks proxy—License covers use for the Cache application
- RealSubscriber—License covers use for the E-CDN application
- Digital Fountain multicast client—License covers use for the E-CDN application

To enable these licensed software programs, you must perform the following tasks using the CLI:

- Accept the license agreement.
- Enter your Cisco license key or accept an evaluation license.
- Enable the software program.



Note You view the license agreement for each software program by using a **show** command. You must then accept the license agreement using the appropriate CLI configuration command before you can enable the program.

You can accept an evaluation license that allows you to use the licensed software for a limited period. The evaluation license can be invoked only once and does not require a license key. The evaluation license allows the licensed program to be enabled for 60 days. The evaluation license timer does not count down when the licensed program is disabled.

When the preset evaluation time has elapsed, the licensed program is automatically disabled. You can purchase a valid license key from Cisco Systems and enter the license key into the configuration at any time during the evaluation period for uninterrupted use of the program. To view the time remaining for an evaluation, you can use an appropriate **show** command.

The following sections explain how to enable the licensed software.

WMT License Commands

To enable WMT, follow these steps:

Step 1 Access the CLI and view the WMT license agreement by using the `show wmt license-agreement` command in EXEC mode.

```
ContentEngine# show wmt license-agreement
```

Step 2 After reading the license agreement, enter global configuration mode and accept the license agreement.

```
ContentEngine# configure
ContentEngine(config)# wmt accept-license-agreement
```

Step 3 Enter your Cisco license key.

```
ContentEngine(config)# wmt license-key licensekey
```

Step 4 Alternatively, accept an evaluation license by using the `wmt evaluation` command.

```
ContentEngine(config)# wmt evaluation
```

Step 5 Enable the WMT software program.

```
ContentEngine(config)# wmt enable
```

Now access the E-CDN Content Distribution Manager user interface, and choose **Devices > Bandwidth**. The Bandwidth screen appears. Adjust the WMT server bandwidth value as required. Otherwise, the default bandwidth is set to 100 kbps.

RealNetworks RealProxy License Commands

To enable the RealProxy, follow these steps:

Step 1 Access the CLI and view the RealProxy license agreement by using the `show rtsp license-agreement` command in EXEC mode.

```
ContentEngine# show rtsp license-agreement
```

Step 2 After reading the license agreement, enter global configuration mode and accept the license agreement.

```
ContentEngine# configure
ContentEngine(config)# rtsp proxy media-real accept-license-agreement
```

Step 3 Enter your Cisco license key.

```
ContentEngine(config)# rtsp proxy media-real license-key licensekey
```

Step 4 Alternatively, accept an evaluation license by using the `rtsp proxy media-real evaluation` command.

```
ContentEngine(config)# rtsp proxy media-real evaluation
```

Step 5 Set the IP address of the RealProxy.

This step is required only if your Content Engine is located behind a firewall and your RealPlayer client is on the opposite side of the firewall. You need to configure an IP address for the RealProxy that is visible to the RealPlayer clients that use it.

```
ContentEngine(config)# rtsp proxy media-real ipaddress
```

Step 6 Enable the RealProxy media cache.

```
ContentEngine(config)# rtsp proxy media-real enable
```



RealSubscriber License Commands

ACNS 4.1 software includes RealServer Version 8.0.1 as an optional component that is used as a streaming media engine. When RealServer software is configured for subscriber-only mode, it is referred to as RealSubscriber. RealServer is licensed by default to serve only 10 simultaneous streams.

To add additional licenses, you need to use the RealNetworks distributed licensing feature. This licensing feature allows you to configure a Content Engine RealServer so that it can obtain additional licenses from a RealServer that is acting as a publisher. You configure the Content Engine RealServer with the publisher's IP address (or host name) and administration port using the **real-subscriber publisher** command. You then enter the IP address and port information of every Content Engine in the publisher RealServer user interface.



Note The user hosts and maintains the RealNetworks publisher RealServer.

To configure RealSubscriber parameters, perform the following steps:

Step 1 Access the CLI and view the RealSubscriber license agreement by using the **show real-subscriber license-agreement** command in EXEC mode.

```
ContentEngine(config)# show real-subscriber license-agreement
```

Step 2 After reading the license agreement, enter global configuration mode and accept the license agreement.

```
ContentEngine# configure  
ContentEngine(config)# real-subscriber accept-license-agreement
```

Step 3 Enter your Cisco license key.

```
ContentEngine(config)# real-subscriber license-key licensekey
```

Step 4 Alternatively, use the **real-subscriber evaluation** command to accept a 60-day evaluation license.

```
ContentEngine(config)# real-subscriber evaluation
```

Step 5 Enable RealSubscriber.

```
ContentEngine(config)# real-subscriber enable
```

Now access the E-CDN Content Distribution Manager user interface and choose **Devices > Bandwidth**. The Bandwidth screen appears. Adjust the bandwidth value in the Real field as required. Otherwise, the default RealSubscriber bandwidth is set to 100 kbps.

If you want to run more than ten simultaneous media streams, you need to set up a publisher RealServer using the distributed licensing feature. See the next section, “Using the Distributed Licensing Feature.”

Using the Distributed Licensing Feature

The distributed licensing feature enables you to purchase a single license to be used by multiple RealServers on your network that share a pool of streams to be used for specific features. You need to use the distributed licensing feature if you want to use more than ten licenses.

The RealServers that share a license are called a license group. Clients are not denied service unless the entire pool of connections in the group is in use.

When you use this feature, you place the main license file on the main RealServer (called the publisher). You configure the publisher RealServer and then configure associated RealServers (called subscribers). The subscribers can be set up to look for a primary publisher RealServer, and if that RealServer is not available or has too few connections available for use, a secondary publisher RealServer can be called upon.

Within a given network or organization, you can have multiple groups, but you should not use this feature outside a network or across a firewall.

Each RealServer maintains its own configuration file, however, because the Content Engines run a fixed RealSubscriber license, and features cannot be configured independently.

Setting Up Distributed Licensing



Note You need to set up distributed licensing on the machine that is running the publisher RealServer. You are responsible for hosting and maintaining this machine.

Once you have configured both the publisher and the subscribers, you must remember to start the publisher before starting the subscribers. If you start the subscribers first, they will operate with minimum settings until the publisher comes online.



Note RealSubscriber allows you to configure up to two publisher RealServers.

Setting Up the Publisher RealServer

To set up the publisher, perform the following steps:

-
- Step 1** On the machine that is running the publisher RealServer, start RealSystem Administrator.
- Step 2** Look up the value of the admin port.
- In RealSystem Administrator, click **General Setup**. Click **Ports**.
 - Note the value for the admin port. You will use it in configuring the publisher RealServer.
- Step 3** In RealSystem Administrator, click **License Group**. Click **Configure**.
- Step 4** Add all license publishers for this group, including this publisher:
- In the License Publishers area, click **Add New**. A generic IP address appears in the Edit Publisher IP Address field.
 - In the Edit Publisher IP Address field, enter the IP address of the other license publisher.
 - Click **Edit**.
 - In the Admin Port field, enter the value of the other publisher's admin port.
- Step 5** Repeat Step 4 to add each additional publisher to the group.
- Step 6** Add the subscribers that will be sharing this RealServer license (repeat this step for each subscriber):
- In the License Subscriber area, click **Add New**. A generic description appears in the Edit Subscriber field.
 - Enter a descriptive name in the Edit Subscriber field to distinguish this subscriber from others.
 - Click **Edit**.
 - In the Subscriber Address field, enter the subscriber's IP address. This address must be the IP address of the Content Engine that is acting as a subscriber. To indicate a range of addresses, enter the subscriber's subnet mask (usually 255.255.255.255) in the Subscriber Netmask field.
- Step 7** Click **Apply**.
- Step 8** Repeat Step 1 through Step 7 for each publisher in the license group.
- Step 9** On the machine running the Content Engine, enter the **real-subscriber publisher** command to configure the publisher RealServer. Make sure that you use the same admin and port values you used when setting up the publisher RealServer (Step 4). For example,

```
ContentEngine(config)# real-subscriber publisher 192.168.123.78 20000 Leonidas myPasswd
```

where 192.168.123.78 is the IP address, 20000 is an admin port number, Leonidas is the username on the publisher RealServer, and myPasswd is the user password on the publisher RealServer.



Step 10 For all publisher settings to take effect, you need to disable RealSubscriber and then enable it again using the `real-subscriber no enable` and `real-subscriber enable` commands.

```
ContentEngine(config)# real-subscriber no enable  
ContentEngine(config)# real-subscriber enable
```



Note For more information about the RealNetworks distributed licensing feature, go to the following website: <http://www.service.real.com/help/library/guides/server8/htmlfiles/advanced.htm#61307>.

Accessing RealSubscriber Log Files

RealSubscriber status logs can be accessed from the following location:

/local/real-subscriber-logs

Digital Fountain Multicast Client License Commands

To enable the Digital Fountain multicast client, follow these steps:

Step 1 Access the CLI and view the Digital Fountain license agreement by using the `show multicast-client license-agreement` command in EXEC mode.

```
ContentEngine# show multicast-client license-agreement
```

Step 2 After reading the license agreement, enter global configuration mode and accept the license agreement.

```
ContentEngine# configure  
ContentEngine(config)# multicast-client accept-license-agreement
```

Step 3 Enter your Cisco license key.

```
ContentEngine(config)# multicast-client license-key licensekey
```

Step 4 Alternatively, accept an evaluation license by using the `multicast-client evaluation` command.

```
ContentEngine(config)# multicast-client evaluation
```

The evaluation license expires in 30 days.

Step 5 Enable the software program.

```
ContentEngine(config)# multicast-client enable
```

You are now ready to begin working with the E-CDN application software using the Content Distribution Manager GUI. Refer to the *Cisco Application and Content Networking Software E-CDN Administrator's Guide* for further information.

9 Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

<http://www.cisco.com>

Translated documentation is available at the following URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

10 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.



Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

<http://www.cisco.com/register/>

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.







Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11 Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
www-europe.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 317 7777
Fax: +65 317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the **Cisco Web site at www.cisco.com/go/offices**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia
Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2002 Cisco Systems, Inc. All rights reserved. AccessPath, AtmDirector, Browse with Me, CCIP, CCSI, CD-PAC, *CiscoLink*, the *Cisco Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, FrameShare, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, ScriptBuilder, ScriptShare, SMARTnet, TransPath, Voice LAN, Wavelength Router, and WebViewer, are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Discover All That's Possible are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert Logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, GigaStack, IOS, IP/TV, LightStream, MICA, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0110R)

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.
DOC-7813948=