



Configuring and Registering ACNS Network Devices

Initial device configuration requires the registering of local network values, such as IP address, netmask, DNS host, and gateway IP address, in order to bring the device online. These values can be set automatically through the default autoregistration feature, or they can be set manually through the local command-line-interface (CLI) on the device.

Once a device is registered, the administrator activates the device through the Content Distribution Manager GUI. This allows only approved devices to participate in the ACNS network and to communicate with other activated nodes.

This chapter tells you how to perform an initial configuration and how to activate the device in your ACNS network. It contains the following sections:

- [Getting Started, page 3-1](#)
- [Configuring the Device Mode, page 3-3](#)
- [Configuring the Content Distribution Manager, page 3-4](#)
- [Configuring the Device Network Settings, page 3-6](#)
- [Configuring Disk Space, page 3-9](#)
- [Registering a Device with the Content Distribution Manager, page 3-10](#)
- [Activating Devices in the Content Distribution Manager GUI, page 3-13](#)
- [Configuring Additional Network Interfaces, page 3-17](#)
- [Setting Device Clock and Time Zone Parameters, page 3-22](#)

Getting Started

This section provides a set of steps for quickly setting up and configuring your ACNS network.

1. Enable a Content Distribution Manager

- Change your Content Engine 565 or 7305 to a Content Distribution Manager by using the **device mode** command. (See the [“Configuring the Device Mode”](#) section on page 3-3.)
- Configure a primary Content Distribution Manager and enable management services using the CLI. Configure a backup Content Distribution Manager if you wish. (See the [“Configuring the Content Distribution Manager”](#) section on page 3-4.)

2. Enable a Content Router (Optional)

- Change your Content Engine 565 or 7305 to a Content Router by using the **device mode** command. (See the “[Configuring the Device Mode](#)” section on page 3-3.)
- Boot the Content Router and configure the network settings. (See the “[Configuring the Device Network Settings](#)” section on page 3-6.)
- Register the Content Router with the Content Distribution Manager, either manually using the CLI, or using the autoregistration feature. (See the “[Registering a Device with the Content Distribution Manager](#)” section on page 3-10.)
- Configure your DNS server for the Content Router. DNS entries for all fully qualified domain names (FQDNs) must be delegated to the Content Router. In the DNS server’s zone database file (db), you must enter a name server (NS) record that delegates the FQDN to the Content Router, and then restart your DNS server.

Make sure that your DNS administrator assigns you authoritative responsibility for some subdomain within your domain. (For more information on content routing, see [Chapter 4, “Setting Up Content Request Routing in the ACNS Network.”](#))

3. Enable Content Engines

Boot the Content Engine and configure the following network settings:

- Ethernet interface
- IP domain name
- Host name
- IP name server
- Default gateway
- Primary interface

See the “[Configuring the Device Network Settings](#)” section on page 3-6.

4. Configure Content Engine Disk Space

- Create disk space for caching (cfs), pre-positioning (cdnfs), streaming (mediafs), and system use (sysfs) using the **disk config** command. The sysfs should not be less than 3 GB.
- Save the configuration using the **write memory** command.
- Reload the device using the **reload** command.

See the “[Configuring Disk Space](#)” section on page 3-9.

See also [Appendix A, “Configuring Disk Space.”](#)

5. Enable ACNS Network Management Services

- Register Content Engines and Content Routers (optional) with the Content Distribution Manager using the **cdm ip** command.
- Enable management services using the **cms enable** command.

See the “[Registering a Device with the Content Distribution Manager](#)” section on page 3-10.

6. Configure Your Network for Content Distribution

- Build the location tree. Take into account WAN links, levels, mesh topologies, and route paths.
- Assign Content Engines to locations.
- Create a directory of content providers.

- Define websites for each content provider.
- Create channels.
- Assign Content Engines to each channel.
- Assign one root Content Engine to each channel.

See the [“Activating Devices in the Content Distribution Manager GUI”](#) section on page 3-13.

See also [Chapter 5, “Configuring the ACNS Network for Content Distribution.”](#)

7. Configure Your Network for Content Acquisition

- Assign channels to each website using a manifest file.
- Configure the acquisition bandwidth. The default bandwidths are very small and probably need to be increased.

See [Chapter 6, “Configuring the ACNS Network for Content Acquisition.”](#)

See also [Chapter 7, “Creating Manifest Files.”](#)

Configuring the Device Mode

This section explains how to change the device mode of a Content Engine before activating it in your ACNS network.



Note

Additional steps are required to change the device mode of a device that is already operating as part of your ACNS network. See the [“Repurposing an ACNS Network Device”](#) section on page 8-30.

Configuring the device mode is not a supported option on all hardware models. However, some hardware models can be configured to operate as any one of the three Content Networking device types.

The following hardware models support device mode configuration:

- CE-7305
- CE-565

To change the device mode of your eligible Content Engine, you must be prepared to configure the disk space allocations, as required by the different device modes, and to reboot the device for the new configuration to take effect.

Devices that can be reconfigured using the **device mode** global configuration command are shipped from the factory by default as Content Engines. When you change the device mode of a Content Engine to a Content Router or a Content Distribution Manager, you need to configure the system file system (sysfs). (See the [“Configuring Disk Space”](#) section on page 3-9.)

If, however, you are changing the device mode of a Content Router or a Content Distribution Manager back to a Content Engine, you must configure disk space allocations for caching (cfs), pre-positioning (cdnfs), streaming (mediafs), and system use (sysfs) that are used on the Content Engine. (See [Appendix A, “Configuring Disk Space.”](#)) For example:

```
DeviceName# disk config sysfs 10% cfs 20% mediafs 10% cdnfs 60%
```

To configure the device mode, follow these steps:

-
- Step 1** Boot the device and access the device CLI through the console or a Telnet session.
- Step 2** Enter the **show device-mode current** command to view the current device mode.
- ```
DeviceName# show device-mode current
Current device mode: content-engine
```
- Step 3** Configure the new device mode by using the **device mode** command in global configuration mode. For example:
- ```
DeviceName# configure
DeviceName(config)# device mode content-router
```
- Step 4** Save the configuration by issuing the **write memory** command or the **copy running-config startup-config** command.
- ```
DeviceName# write memory

DeviceName# copy running-config startup-config
```
- Step 5** Use the **restore factory-default preserve basic-config** command to reload the software and apply the device mode configuration. Your network settings are preserved.
- ```
DeviceName# restore factory-default preserve basic-config
```
- Step 6** Verify the new configuration. Check that the current and configured device modes are the same. For example:
- ```
DeviceName# show device-mode configured
Configured Device mode: content-router
DeviceName# show device-mode current
Current device mode: content router
```
- Step 7** Configure the disk space allocation based on the new device mode and needs of your network by using the **disk config** command.
- After the device reloads and you have verified the device mode configuration, you are ready to register the device with the Content Distribution Manager. (See the [“Registering a Device with the Content Distribution Manager”](#) section on page 3-10.)
- 

## Configuring the Content Distribution Manager

You must configure the Content Distribution Manager before you can register any Content Engines or Content Routers with the Content Distribution Manager.

In ACNS 5.x software, Content Distribution Managers can operate in two different roles: primary and standby. The primary role is the default. You can have only one primary Content Distribution Manager that is active in your network; however, you can have any number of Content Distribution Managers running in a standby role for failover and redundancy. We recommend that you configure the primary Content Distribution Manager first.

**Note**

Primary and standby Content Distribution Managers must be running the same version of ACNS software. If they are not, the standby Content Distribution Manager detects this and shuts down the Centralized Management System (CMS) until the problem is corrected. We recommend that you upgrade your standby Content Distribution Manager first and then upgrade your primary Content Distribution Manager.

To configure the primary Content Distribution Manager using the CLI, follow these steps:

- Step 1** Create and initialize the management database, and enable ACNS services by using the **cms enable** command.

```
CDM-4630(config)# cms enable
```

- Step 2** Verify that services have been enabled by using the **show cms processes** command. For example:

```
CDM-4630# show cms processes
Service cms_httpd running
Service cms_ui running
Service cms_cdm running
CDM-4630#
```

- Step 3** Verify the current running configuration by using the **show running-config** command.

```
CDM-4630# show running-config
```

A message similar to the following should appear:

```

...
cms enable
!
...

```

- Step 4** To save the configuration, use the **copy running-config startup-config** command.

```
CDM-4630# copy running-config startup-config
```

To configure a standby Content Distribution Manager role, follow these steps:

- Step 1** Configure the standby Content Distribution Manager role by using the **cdm role** command.

```
CDM-4630# cdm role standby
```

- Step 2** Configure the standby Content Distribution Manager with the IP address of the primary Content Distribution Manager by using the **cdm ip** *{ip-address | hostname}* command. For example:

```
CDM-4630# cdm ip 10.1.1.90
```

This command associates the device with the primary Content Distribution Manager so that it can be approved as a part of the network.

- Step 3** Create and initialize the management database, and enable ACNS services by using the **cms enable** command.

```
CDM-4630(config)# cms enable
```

**Step 4** Verify that services have been enabled by using the **show cms processes** command. For example:

```
CDM-4630# show cms processes
Service cms_httpd running
Service cms_ui running
Service cms_cdm running
```

**Step 5** Verify the current running configuration by using the **show running-config** command.

```
CDM-4630# show running-config
```

A message similar to the following should appear:

```

...
cms enable
!
...

```

**Step 6** To save the configuration, use the **copy running-config startup-config** command.

```
CDM-4630# copy running-config startup-config
```

## Configuring the Device Network Settings

After you physically install the hardware and power up your device, you can access the ACNS software and perform an initial startup configuration. The initial configuration defines the network settings of your devices so that they can become active on your network.



### Note

If you have upgraded your software from a previous ACNS software release to ACNS 5.x software, your network configuration is preserved. You do not need to reconfigure your network settings.

## About Selecting Static IP Addresses or Using DHCP

During the initial configuration, you have the option of configuring a static IP address for the device or choosing DHCP. This section describes these two options.

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

In the following sample startup dialog, the administrator has chosen to enable DHCP. Administrator entries are shown in bold. (See also the [“Configuring Interfaces for DHCP”](#) section on page 3-21.)

```
BOOT-100:sw-file systems mounted, applying pending upgrades...
SW up-to-date

ACNS boot:detected no saved system configuration
 Do you want to enter basic configuration now?
 hit RETURN to enter basic configuration:0019
admin password:
```

```

re-enter password:
Please enter an interface from the following list:
 0:GigabitEthernet 1/0
 1:GigabitEthernet 2/0
enter choice:0
Enable DHCP on this interface? (y/n) [n]:y

 [0] Go to the CLI command prompt without saving this config.
 [1] Return back to the setup without saving this config.
 [2] Save this configuration to flash and go to CLI prompt.

Choose one? [2]:2
Running pre-200 hooks...

```

## Configuring Network Settings Using the Startup Dialog

The startup dialog allows you to configure network settings using an interactive dialog instead of the CLI. If you wish, you can disable autoregistration by responding to the startup dialog prompt and configuring the first interface on your device (Ethernet 0/0 or GigabitEthernet 1/0) with either a static IP address or with interface-level DHCP. If you specify the configuration on the interface that uses autoregistration, autoregistration is automatically disabled.

You can also use the startup dialog to configure other interfaces if you have multiple interfaces on your device.

To use the startup dialog, follow these steps:

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

After the operating system boots, 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 and initiate the startup dialog. If you do not respond, the system continues booting and automatically registers with the Content Distribution Manager.

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

- Admin password for the device

This is the case-sensitive password you want to use for the 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 at the local device.

- 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 (if DHCP is not used)
- IP network mask for the device, for example, 255.255.255.224 (if DHCP is not used)

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 (if DHCP is not used)  
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
- Host name for the device
- Domain name for the device

**Step 3** Choose whether or not to save the configuration. After you choose to save the configuration, 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. The administrator has chosen not to enable DHCP.

```

BOOT-100:sw-file systems mounted, applying pending upgrades...
SW up-to-date

ACNS boot:detected no saved system configuration
 Do you want to enter basic configuration now?
 hit RETURN to enter basic configuration:0016
admin password:
re-enter password:
Please enter an interface from the following list:
 0:GigabitEthernet 1/0
 1:GigabitEthernet 2/0
enter choice:0
Enable DHCP on this interface? (y/n) [n]:n
local IP address:172.16.13.8
IP network mask:255.255.255.254
gateway IP address:172.16.13.7
DNS server:10.10.10.11
host name:CE7305
domain name:cisco.com

 [0] Go to the CLI command prompt without saving this config.
 [1] Return back to the setup without saving this config.
 [2] Save this configuration to flash and go to CLI prompt.

Choose one? [2]:2
Running pre-200 hooks...

```

**Step 4** To make sure that a primary interface has been configured, use the **show running-config** command. A primary interface should have been chosen automatically by the software during the initial startup; however, you can configure a primary interface manually by using the **primary-interface** command in global configuration mode.

## Configuring Network Settings Using the CLI

To configure network settings using the CLI, follow these steps:

**Step 1** Power up the device and log on through the console. At the login prompt, enter the username **admin** and the password **default**.

- You must log in to the CLI with an ACNS system account that has superuser privileges.
- You must use a console connection to complete this initial configuration. After this initial configuration is complete, you can use Telnet sessions to access the CLI for subsequent configuration tasks, such as disk configuration.

**Step 2** From the device CLI, enter global configuration mode.

```
CE-507# config
CE-507(config)#
```

**Step 3** In global configuration mode, configure the device network settings by using the following commands:

- Configure your Ethernet interface for DHCP.

```
CE-507(config)# interface {FastEthernet | GigabitEthernet} slot/port ip address dhcp
```

The remainder of your network settings are configured automatically. You have finished configuring your network settings.

- Alternatively, configure the static IP address of your Ethernet interface.

```
CE-507(config)# interface {FastEthernet | GigabitEthernet} slot/port ip address
ip-address netmask
```

**Step 4** Continue configuring the remaining network settings.

- Configure the IP domain name.

```
CE-507(config)# ip domain-name name1 name2 name3
```

- Configure the host name.

```
CE-507(config)# hostname name
```

- Configure the IP name server.

```
CE-507(config)# ip name-server ip-address
```

- Configure the IP default gateway.

```
CE-507(config)# ip default-gateway ip-address
```

- Configure the primary interface.

```
CE-507(config)# primary-interface {FastEthernet | GigabitEthernet} slot/port [dhcp]
```

## Configuring Disk Space

If you are configuring a device for the first time, you need to create disk space for system use (sysfs), caching (cfs), streaming (mediafs), and pre-positioning (cdnfs) on the Content Engine by using the **disk config** command in EXEC mode.

To configure disk space, follow these steps:

**Step 1** Exit configuration mode, if you have not already done so.

```
CE-507(config)# exit
CE-507#
```

**Step 2** Enter the **disk config EXEC** command. For example:

```
CE-507# disk config sysfs 10% cfs 20% mediafs 10% cdnfs 60%
```

**Step 3** Reload the Content Engine for the disk configuration to take effect.

```
CE-507# reload
```



**Tip**

For the new disk space configuration to take effect, you must first reboot the device; however, if you are going to change the device mode, you can wait to reboot until after you have configured the new device mode.

To update the disk configuration through the Content Distribution Manager GUI, follow the procedure in the [“Updating Storage Capacity on Your Content Engines”](#) section on page A-10.

For further disk space allocation guidelines, see [Appendix A, “Configuring Disk Space.”](#)

If you are attaching and configuring a Fibre Channel storage array, see the [“Using a Fibre Channel Storage Array”](#) section on page A-10. Do not attempt to assign the Fibre Channel storage to the Content Engine and configure the file systems with a single reload of the Content Engine. If you do, the Fibre Channel storage assignment is recognized, but the disk configuration is not applied. An error message appears at bootup, similar to the following:

```

ruby_disk:physical disk setup appears to have changed
ruby_disk:not applying 'disk config' changes. Please re-enter via CLI.

```

If you encounter this error message, reenter your disk configuration and use the **reload** command on the Content Engine for the disk configuration to be applied.

## Registering a Device with the Content Distribution Manager

Before a newly installed Content Engine or Content Router can be recognized by the Content Distribution Manager, it must be registered with the Content Distribution Manager. Registering a new device (also called a node) can be done automatically or manually through the CLI.



**Note**

To deregister a device, see the [“Deleting a Content Router”](#) section on page 8-20 or the [“Deleting a Content Engine”](#) section on page 8-11.

## Autoregistration

On bootup, devices running ACNS 5.x software (with the exception of the Content Distribution Manager itself) automatically discover the Content Distribution Manager and register with it. The administrator does not have to do any manual configuration locally on the device. When the device is registered, the administrator approves the device and configures it remotely using the Content Distribution Manager GUI. (See the [“Activating Devices in the Content Distribution Manager GUI”](#) section on page 3-13.)

Autoregistration uses a form of Dynamic Host Configuration Protocol (DHCP). You must have a DHCP server that is configured with the host name of the Content Distribution Manager and that is capable of handling vendor class option 43 for autoregistration to work.



### Note

The form of DHCP used for autoregistration is *not* the same as the interface-level DHCP that is configurable through the **ip address dhcp** interface configuration command. (See the [“About Selecting Static IP Addresses or Using DHCP”](#) section on page 3-6 for an explanation of interface-level DHCP.)

The vendor class option (option 43) information needs to be sent to the ACNS network device in the format for encapsulated vendor-specific options as provided in RFC 2132. The relevant section of RFC 2132, Section 8.4, is reproduced here as follows:

The encapsulated vendor-specific options field should be encoded as a sequence of code/length/value fields of syntax identical to that of the DHCP options field with the following exceptions:

1. There should not be a “magic cookie” field in the encapsulated vendor-specific extensions field.
2. Codes other than 0 or 255 may be redefined by the vendor within the encapsulated vendor-specific extensions field, but should conform to the tag-length-value syntax defined in section 2.
3. Code 255 (END), if present, signifies the end of the encapsulated vendor extensions, not the end of the vendor extensions field. If no code 255 is present, then the end of the enclosing vendor-specific information field is taken as the end of the encapsulated vendor-specific extensions field.

In accordance with the RFC standard, the DHCP server needs to send the Content Distribution Manager host name information in code/length/value format (code and length are single octets). The code for the Content Distribution Manager host name is 0x01. DHCP server management and configuration is not within the scope of the autoregistration feature.

The ACNS network device sends “CISCOCDN” as the vendor class identifier in option 60, to facilitate device groupings by customers.

Autoregistration DHCP also requires that the following options be present in the DHCP server’s offer to be considered valid:

- Subnet-mask (option 1)
- Routers (option 3)
- Domain-name (option 15)
- Domain-name-servers (option 6)
- Host-name (option 12)

In contrast, interface-level DHCP requires only subnet-mask (option 1) and routers (option 3) for an offer to be considered valid; domain-name (option 15), domain-name-servers (option 6), and host-name (option 12) are optional. All of the above options, with the exception of domain-name-servers (option 6), replace the existing configuration on the system. The domain-name-servers option is added to the existing list of name servers with the restriction of a maximum of eight name servers.

Autoregistration is enabled by default on the first interface of the device. The first interface depends on the Content Engine model as follows:

- For the CE-507, CE-507AV, CE-560, CE-560AV, CE-590, and CR-4430: FastEthernet 0/0
- For the CE-510, CE-565, CE-7305, CE-7325, and CE-7320: GigabitEthernet 1/0

If you do not have a DHCP server, the device is unable to complete autoregistration and eventually times out. You can disable autoregistration at any time after the device has booted and proceed with manual setup and registration. (See the [“About Selecting Static IP Addresses or Using DHCP”](#) section on page 3-6.)

To disable autoregistration, or to configure autoregistration on a different interface, use the **no auto-register enable** command in global configuration mode.



#### Note

Autoregistration is automatically disabled if a static IP address or interface-level DHCP is configured on the same interface as autoregistration.

The following example disables autoregistration on Fast Ethernet port 0/0:

```
CE(config)# no auto-register enable FastEthernet 0/0
```

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

```
CE# show status auto-register
```

## Manual Registration

If you do not have a DHCP server in your network, or if for some reason your DHCP server is configured incorrectly, you can set up and register a device manually.

To manually register your ACNS network devices, you must first disable autoregistration. This can be done using the startup dialog, or through the CLI after the device has booted.

To manually register a new device, follow these steps:

- Step 1** Set the IP address or host name of the Content Distribution Manager with which the device is to be associated by using the **cdm ip** command in global configuration mode.

```
CE-507# config
CE-507(config)# cdm ip {ip-address | hostname}
```

This command associates the device with the Content Distribution Manager so that the device can be approved as a part of the network.

After the device is configured with the Content Distribution Manager IP address, it presents a self-signed security certificate as well as other essential information, such as its IP address or host name, disk space allocation, and so forth, to the Content Distribution Manager.

- Step 2** To register the device, create and initialize the management database, and enable ACNS services, use the **cms enable** command in global configuration mode.

```
CE-507(config)# cms enable
```

The CMS database table stores the device node configuration, allowing the node to be centrally managed from the Content Distribution Manager.

**Step 3** Use the **show cms info** command to verify that your device has been registered.

```
CE-507# show cms info
```

A message similar to the following should appear:

```
Registration information :
CDM address = 10.1.1.90
Device Mode = ce
Model = CE507
Node Id = 84
ce507#
```

**Step 4** To verify that the CMS is running, use the **show cms processes** command.

```
CE-507# show cms processes
```

A message similar to the following should appear:

```
Service cms_ce running
ce507#
```

**Step 5** Verify the current running configuration by using the **show running-config** command.

```
CE-507# show running-config
```

A message similar to the following should appear:

```

...
cms enable
!
...

```

**Step 6** To save the configuration, use the **copy running-config startup-config** command.

```
CE-507# copy running-config startup-config
```

The next step is to authorize the device to become part of the ACNS network by approving the device in the Content Distribution Manager GUI, as described in the next section, “[Activating Devices in the Content Distribution Manager GUI](#).”

## Activating Devices in the Content Distribution Manager GUI

New Content Engines and Content Routers need to be approved by the network administrator. The network administrator approves each device by making it active in the Content Distribution Manager GUI. This security feature prevents unauthorized devices from joining the network.



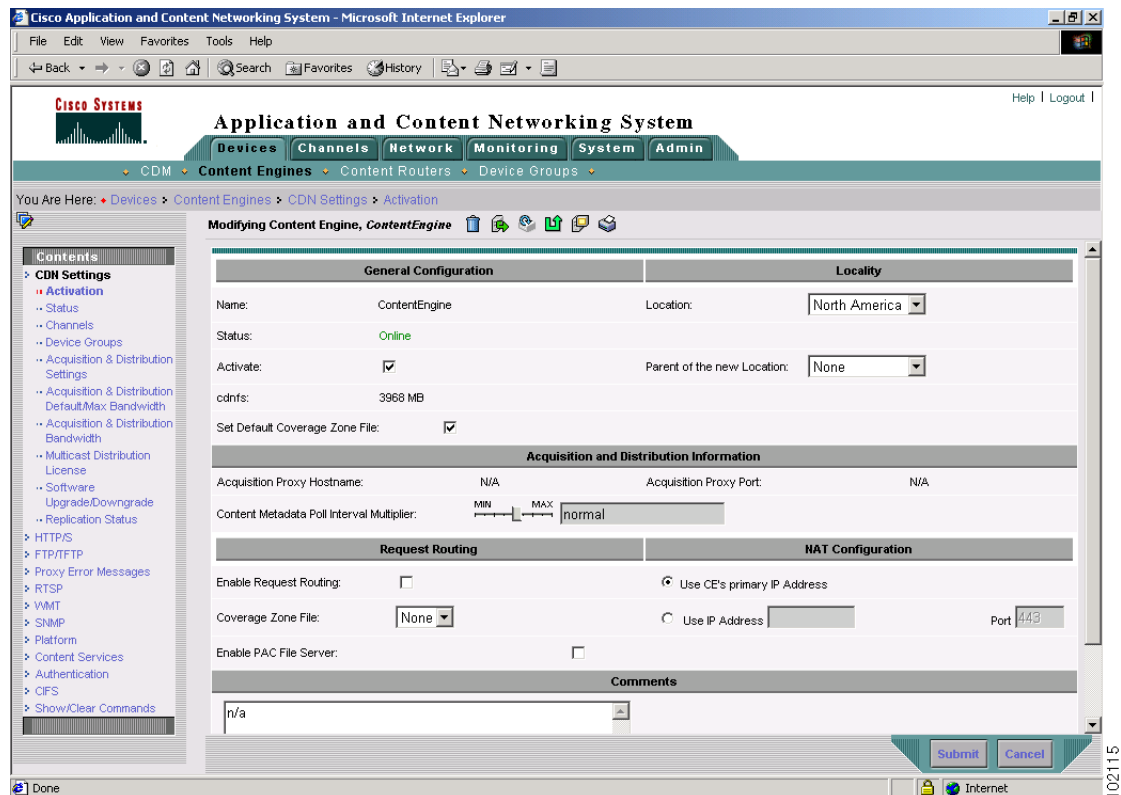
### Note

Before you can access the Content Distribution Manager GUI, you must use the CLI to register yourself as a user. Use the **username** global configuration command to configure your name and password for GUI access.

To activate 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:
- ```
https://name_of_Content_Distribution_Manager:8443
```
- or
- ```
https://IP_address_of_Content_Distribution_Manager:8443
```
- A window appears, requesting your username and password.
- Step 2** Enter the administrator username **admin** and the password **default** and then click **OK**. The Cisco Application and Content Networking System Home window appears.
- Step 3** Choose **Devices > Content Engines**. A list of all your registered Content Engines appears. For Content Routers, choose **Devices > Content Routers**.
- Step 4** Click the **Edit** icon next to the device name. The Modifying Content Engine (or Content Router) window appears. (See [Figure 3-1](#).)

Figure 3-1 Modifying Content Engine Window



**Step 5** Choose a location from the Location drop-down list. The list of locations that have been created using the Locations window are displayed in this drop-down list. If the location that has been chosen for the Content Engine contains a parent location, then the same location tree hierarchy is applied to the Content Engine.

This option allows you to choose an already created location. If you have not already created a location, see the [“Creating and Modifying Locations” section on page 5-1](#).

**Step 6** Alternatively, check the **Create a New Location** check box to create a default location for this Content Engine.



---

**Note** This field is visible only if the Content Engine is in Inactive status. When checked, a default location for an inactive Content Engine is created. This option automatically creates a new location named <CE-name>-location and assigns the Content Engine to that location.

---

**Step 7** Choose a parent location for the default location from the Parent of the new Location drop-down list. This option allows you to choose an already created location as the parent for the newly created default location.

**Step 8** To activate the Content Engine or Content Router, check the **Activate** check box in the Modifying Content Engine (or Content Router) window.

**Step 9** Click **Submit**.

When the device becomes active, the status changes from “Inactive” to “Online.”

Other Content Engine properties can be configured now or at a later time. To enable routing or to modify the default bandwidth settings, see the [“Modifying Content Engine Properties” section on page 8-6](#).

---

## Activating All Inactive Content Engines

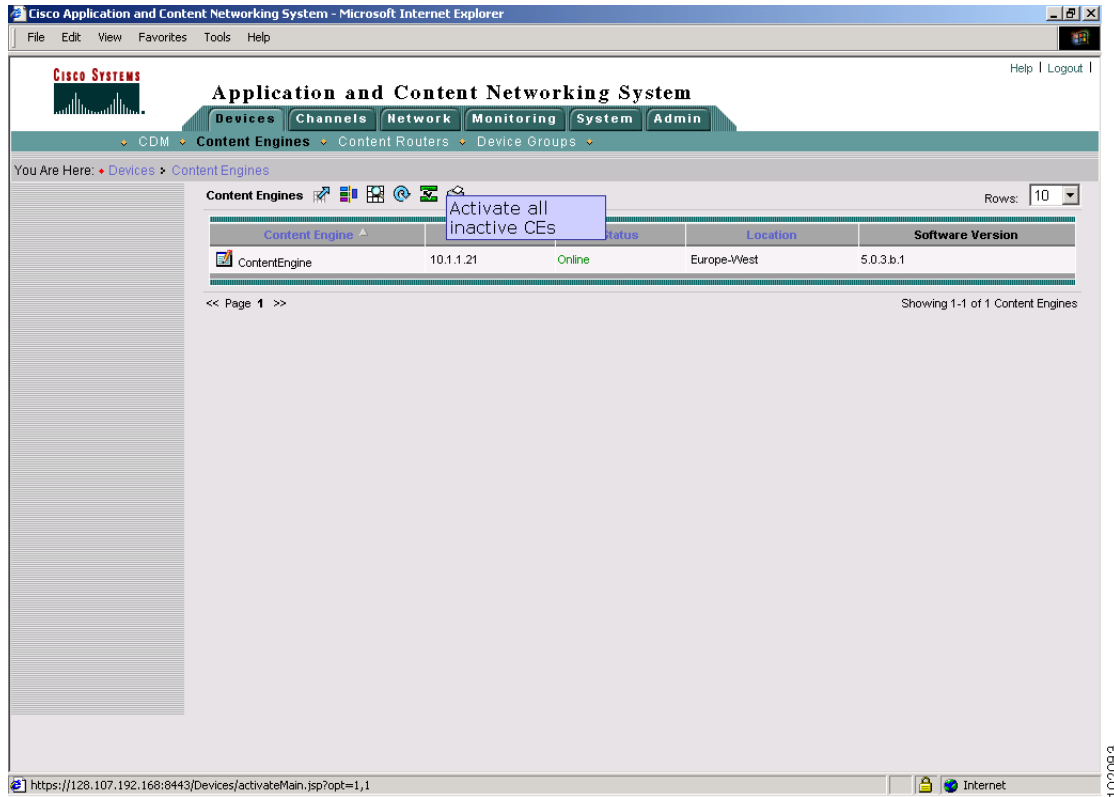
To activate all unactivated Content Engines as a group, follow these steps:

---

**Step 1** From the Content Distribution Manager GUI, choose **Devices > Content Engines**. The Content Engines window appears.

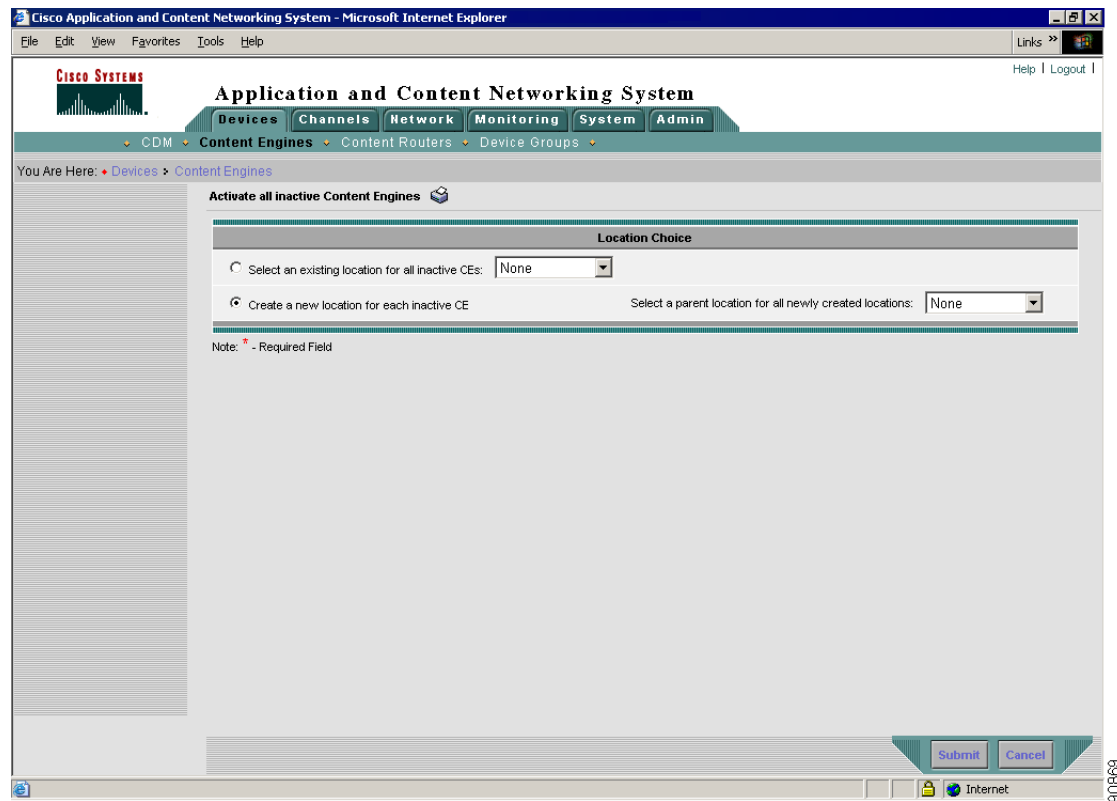
**Step 2** Click the **Activate all inactive CEs** icon. (See [Figure 3-2](#).) The Activate All Inactive Content Engines window appears.

Figure 3-2 Content Engines Window



- Step 3** In the Activate All Inactive Content Engines window, choose an existing location for all unactivated Content Engines by clicking the **Select an existing location for all inactive CEs** radio button. Then choose a location from the drop-down list.
- Step 4** Alternatively, choose to create a new location for each inactive Content Engine by clicking the **Create a new location for each inactive CE** radio button. Then specify a parent location for all newly created locations by choosing a location from the Select a parent location for all newly created locations drop-down list. (See [Figure 3-3](#).)

Figure 3-3 Activate All Inactive Content Engines Window



## Configuring Additional Network Interfaces

In the “Configuring Network Settings Using the Startup Dialog” section on page 3-7 and the “Configuring Network Settings Using the CLI” section on page 3-9, you chose an initial interface and either configured it for DHCP, or gave it a static IP address. This section describes how to configure additional interfaces using options for redundancy, load balancing, performance optimization, and so forth.

### Configuring Multiple Network Interfaces

You can configure multiple network interfaces as either active-active interfaces or as active-standby interfaces. You configure multiple interfaces as active-active by using the **interface** command and by assigning an IP address to each interface. When multiple interfaces are configured, they are active simultaneously. This configuration is used to achieve better performance.

For example:

```
ContentEngine# configure
ContentEngine(config)# interface FastEthernet 0/0
ContentEngine(config-if)# ip address 10.10.10.10 255.0.0.0
```

With an active-standby configuration, the interfaces are configured using the **standby** command, and they remain inactive unless an active interface fails. When an active network interface fails (because of cable trouble, Layer 2 switch failure, high error count, or other failure), and that interface is part of a standby group, a standby interface can become active and take the load off the failed interface. With active-standby interface configuration, only one interface is active at a given time. Active-standby is used mainly for fault tolerance purposes. The performance of the device is limited by the single active interface.

```
ContentEngine# configure
ContentEngine(config)# interface FastEthernet 0/1
ContentEngine(config-if)# standby ?
<1-4> Standby group number
ContentEngine(config-if)# standby 3 ?
 errors Set the maximum number of errors allowed on this interface
 ip Set the IP address of a standby group
 priority Set the priority of an interface for the standby group
ContentEngine(config-if)# standby 3 errors ?
<0-4294967295> Max. no. of errors allowed on this interface for the standby
 group
ContentEngine(config-if)# standby 3 ip ?
 A.B.C.D IP address of the standby group
ContentEngine(config-if)# standby 3 priority ?
<0-4294967295> Priority of this interface for the standby group
```

To configure standby interfaces, interfaces are logically assigned to standby groups. The following rules define the standby group relationships:

- A standby group comprises two or more interfaces.
- The maximum number of standby groups on a Content Engine is four.
- Each interface is assigned a unique IP address, and each standby group is assigned a unique standby IP address, shared by all members of the group.
- Configure the duplex and speed settings of the standby group member interfaces for better reliability.
- Each interface in a standby group is assigned a priority. The operational interface with the highest priority in a standby group is the active interface. Only the active interface uses the group IP address.
- If the active interface fails, the operational interface in its standby group that is assigned the next highest priority becomes active.
- If all the members of a standby group fail and then one recovers, the ACNS software brings up the standby group on the operational interface.
- The priority of an interface in a standby group can be changed at runtime. The interface that has the highest priority after this change becomes the new active interface (the default action is to preempt the currently active interface if an interface with higher priority exists).
- The maximum number of errors allowed on the active interface before the interface is shut down and the standby is brought up is configured with the **errors** option, which is disabled by default.

**Note**


---

Interface IP addresses and standby group IP addresses must be on different subnets to ensure reliable operation. You can use dummy IP addresses in the private address space to serve as interface primary IP addresses, and use the real Content Engine IP address to serve as the standby group IP address in a different subnet to satisfy this requirement.

---

**Note**


---

Make sure to configure the primary interface default gateway using the **ip default-gateway** global configuration command instead of the **ip route** global configuration command.

---

### Example

This example configures three interfaces to be part of the same standby group, with interface 3/0 as the active interface.

```

Console(config)# interface fastEthernet 3/0 standby 1 ip 172.16.10.10 255.255.254.0

Console(config)# interface fastEthernet 3/1 standby 1 ip 172.16.10.10 255.255.254.0

Console(config)# interface fastEthernet 3/2 standby 1 ip 172.16.10.10 255.255.254.0

Console(config)# interface fastEthernet 3/0 standby 1 priority 300

Console(config)# interface fastEthernet 3/1 standby 1 priority 200

Console(config)# interface fastEthernet 3/2 standby 1 priority 100

Console(config)# interface fastEthernet 3/0 standby 1 errors 10000

Console(config)# interface fastEthernet 3/1 standby 1 errors 10000

Console(config)# interface fastEthernet 3/2 standby 1 errors 10000

```

Use the **show standby** command to view your standby interface configuration.

```

Console# show standby
Standby Group:1
IP address: 172.16.10.10, netmask: 255.255.254.0
Maximum errors allowed on the active interface: 10000
 Member interfaces:
 FastEthernet 3/0 priority: 300
 FastEthernet 3/1 priority: 200
 FastEthernet 3/2 priority: 100
Active interface: FastEthernet 3/0

```

## Configuring Multiple IP Addresses on a Single Interface

You can configure more than one IP address on the same interface by using the **interface secondary** interface configuration command. You can configure up to four secondary IP addresses on a single interface. This configuration allows the device to be present in more than one subnet and can be used to optimize response time, because it allows the content to go directly from the Content Engine to the client that is requesting the information without being redirected through a router. The Content Engine becomes visible to the client because both are configured on the same subnet. For example:

```

ContentEngine# configure
ContentEngine(config)# interface FastEthernet 0/0
ContentEngine(config-if)# ip address 10.10.10.10 255.0.0.0 secondary

```

## Configuring the Fibre Channel Interface

ACNS 5.x software supports Fibre Channel interfaces. Fibre Channel is the chosen technology for interconnecting storage devices and servers in a storage area network (SAN). In a SAN, the storage need not be directly attached to the server, and data transfer happens over a high-throughput, high-availability network. Fibre Channel is capable of operating at speeds of 1 gigabit per second (Gbps) and 2 Gbps.

To detect the presence of Fibre Channel storage, the Fibre Channel array must be configured to assign storage space for the Content Engine, and the Content Engine must be reloaded before it can detect the storage assignment. To confirm whether the Content Engine has detected the storage assignment, use the **show disks** and the **show disks details** commands.

To configure the Fibre Channel interface on the Content Engine, use the **interface FibreChannel slot/port** command in interface configuration mode. For example:

```
DeviceName# configure
DeviceName(config)# interface FibreChannel 0/0
DeviceName(config-if)#?
 exit Exit from this submode
 mode Change the fibre channel interface operating mode
 no Negate a command or set its defaults
 speed Change the fibre channel interface speed
DeviceName(config-if)# mode ?
 autosense Use this mode to have the CE autosense
 direct-attached Use this mode when the CE is directly connected to storage array
 switched Use this mode when the CE is connected to a switch
DeviceName(config-if)# speed ?
 1 1Gbps
 2 2Gbps
 autosense autosense
```

For a complete description of the **interface FibreChannel** command syntax and usage, refer to the *Cisco ACNS Software Command Reference, Release 5.1* publication.

For information regarding which Fibre Channel storage arrays are supported by Cisco Systems, refer to the *Release Notes for Cisco ACNS Software, Release 5.1*.

## Configuring EtherChannel

EtherChannel for ACNS 5.x software supports the grouping of up to four same-speed network interfaces into one virtual interface. This grouping capability allows the setting or removing of a virtual interface that consists of two, three, or four Fast Ethernet interfaces or two Gigabit Ethernet interfaces. EtherChannel also provides interoperability with Cisco routers, switches, and other networking devices or hosts supporting EtherChannel; load balancing; and automatic failure detection and recovery based on each interface's current link status.

To create an EtherChannel, use the **interface PortChannel number** command in interface configuration mode. For example:

```
CE# configure
CE(config)# interface PortChannel 2
CE(config-if)# ip address 10.10.10.10 255.0.0.0
CE(config-if)# exit
```

To remove an EtherChannel, use the **no** form of the command:

```
CE(config)# interface PortChannel 2
CE(config-if)# no ip address 10.10.10.10 255.0.0.0
CE(config-if)# exit
CE(config)# no interface portchannel 2
```

To add or remove ports from an EtherChannel, use the commands in the following examples. These commands add a physical Fast Ethernet port to a previously created Fast EtherChannel. The channel number is the same as the channel number specified in the **interface PortChannel** command. You can use either the Fast Ethernet or the Gigabit Ethernet ports to form an EtherChannel; however, an EtherChannel cannot contain both Fast Ethernet and Gigabit Ethernet interfaces. Note that a physical interface can be added to an EtherChannel subject to the device configuration.

To add an interface to a channel group:

```
CE# configure
CE(config)# interface FastEthernet 1/1
CE(config-if)# channel-group 2
CE(config-if)# exit
```

To remove an interface from a channel group:

```
CE(config)# interface FastEthernet 1/1
CE(config-if)# no channel-group 2
CE(config-if)# exit
```

To configure for load balancing, use the **port-channel load-balance** global config command.

```
CE(config)# port-channel load-balance
```

The following **load-balance** options are available:

```
dst-ip Destination IP address
dst-mac Destination MAC address
round-robin Round robin each interface (default)
```

Round robin allows traffic to be distributed evenly between all interfaces in the channel group. The other balancing options give you flexibility in choosing interfaces when sending an Ethernet frame. The **load-balance** command is effective globally. If two channel groups are configured, they must use the same load-balancing option.

## Configuring Interfaces for DHCP



### Note

Autoregistration must be disabled before you can manually configure an interface for DHCP.

An interface can be enabled for DHCP by using the **ip address dhcp** [*client-id* | *hostname*] interface configuration command. The client identifier is an ASCII value.

```
ContentEngine# configure
ContentEngine(config)# interface FastEthernet 0/0
ContentEngine(config-if)#
ContentEngine(config-if)# ip address ?
 A.B.C.D IP address of the interface
 dhcp IP address negotiated via DHCP
ContentEngine(config-if)# ip address dhcp ?
 client-id Specify client-id to use
 hostname Specify value for hostname option
<cr>
```

The Content Engine sends its configured client identifier and host name to the DHCP server when requesting network information. DHCP servers can be configured to identify the client identifier information and the host name information that the Content Engine is sending, and then send back the specific network settings that are assigned to the Content Engine.

## Setting Device Clock and Time Zone Parameters

If you have an outside source on your network that provides time services (such as a Network Time Protocol [NTP] server), you do not need to set the system clock manually. When setting the clock, enter the local time. The Content Engine calculates Coordinated Universal Time (UTC) based on the time zone set by the **clock timezone** global configuration command.

Two clocks exist in the system: the software clock and the hardware clock. The software uses the software clock. The hardware clock is used only at bootup to initialize the software clock. The **clock set EXEC** command sets the software clock.