



Getting Started

This chapter provides an overview of how to configure, monitor, and troubleshoot standalone Content Engines that are running the ACNS 5.4.1 software and later releases. It also describes how to use the ACNS software Setup utility to configure the general settings (device network settings and disk configuration) and a set of commonly used caching services (listed in [Table 4-2](#)) on a standalone Content Engine.

This chapter contains the following sections:

- [Overview of Configuring, Monitoring, and Troubleshooting Standalone Content Engines](#), page 4-2
- [Configuring a Basic Configuration on Standalone Content Engines with the Setup Utility](#), page 4-10
- [Configuring Client Browsers and Media Players for Direct Proxy Routing](#), page 4-35
- [Configuring WCCP Routers for Transparent Redirection](#), page 4-47
- [Verifying the Basic Configuration](#), page 4-47
- [Modifying the Basic Configuration Through the Setup Utility](#), page 4-50
- [Logging in to Standalone Content Engines](#), page 4-50

The term *standalone Content Engines* is used throughout this guide to refer to Content Engines that ACNS administrators have intentionally not registered with the Content Distribution Manager so that they can configure, manage, and monitor these Content Engines as standalone devices. Multiple standalone Content Engines can be deployed (for example, you can deploy clusters of standalone Content Engines).

After you have done a basic configuration on a standalone Content Engine, you can perform other basic tasks such as the setting the system clock, managing login accounts, and managing and monitoring disks. For more information on this topic, see [Chapter 5, “Performing Other Basic Tasks for Standalone Content Engines.”](#)



Note

For complete syntax and usage information for the CLI commands used in this chapter, see the *Cisco ACNS Software Command Reference, Release 5.5* publication. For information about how to configure Content Engines that are registered with a Content Distribution Manager, see the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.5*.

Overview of Configuring, Monitoring, and Troubleshooting Standalone Content Engines

This section provides an overview of how to configure, monitor, and troubleshoot standalone Content Engines as caching and streaming engines, and contains the following sections:

- [Flowcharts of Configuring, Monitoring, and Troubleshooting Standalone Content Engines, page 4-2](#)
- [Checklist for Configuring, Monitoring, and Troubleshooting Standalone Content Engines, page 4-7](#)

Flowcharts of Configuring, Monitoring, and Troubleshooting Standalone Content Engines

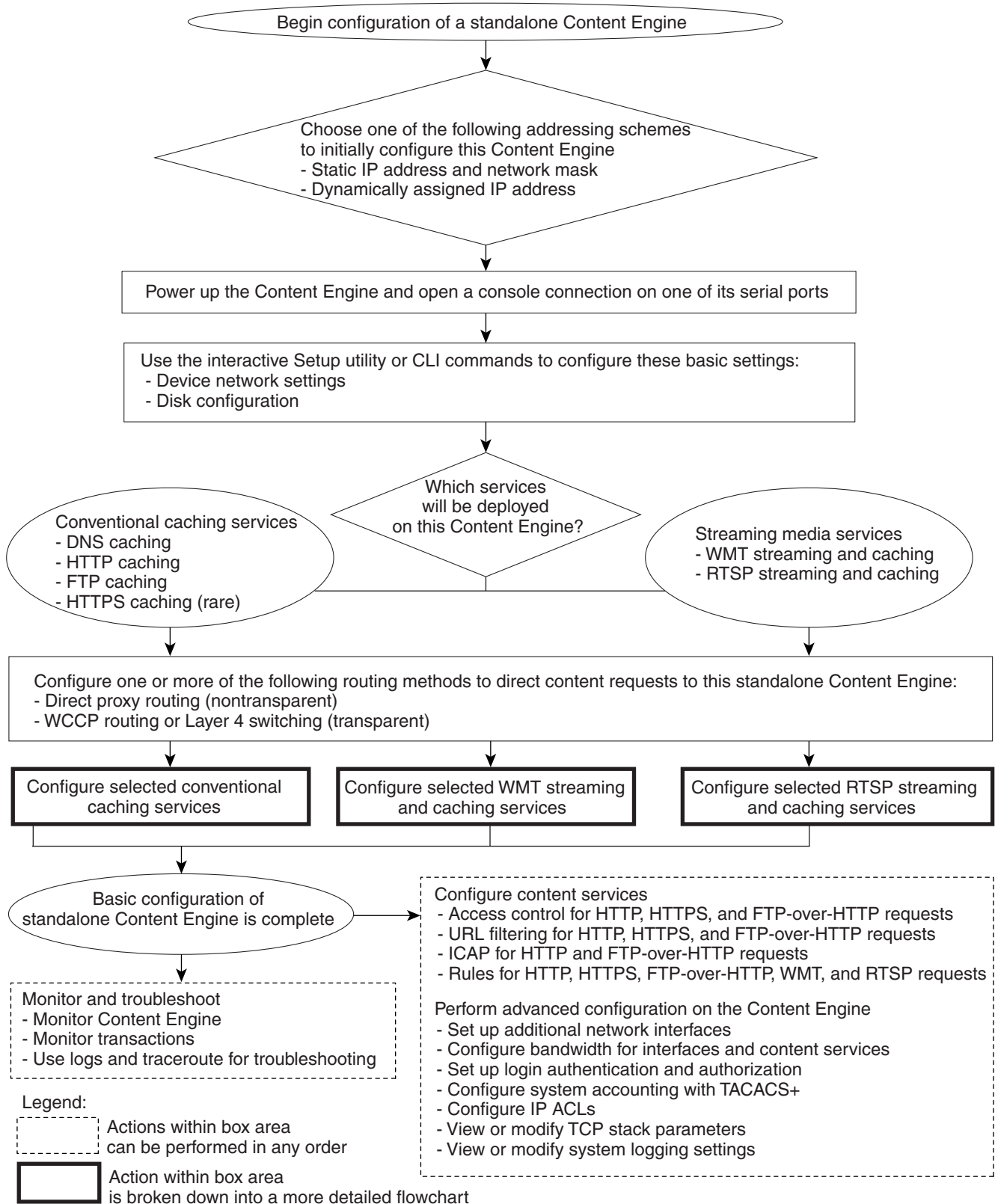
[Figure 4-1](#) shows a high-level view of a typical workflow for configuring, monitoring, and troubleshooting a standalone Content Engine. [Table 4-1](#) provides a checklist of tasks for completing the workflow that is shown in [Figure 4-1](#).



Note

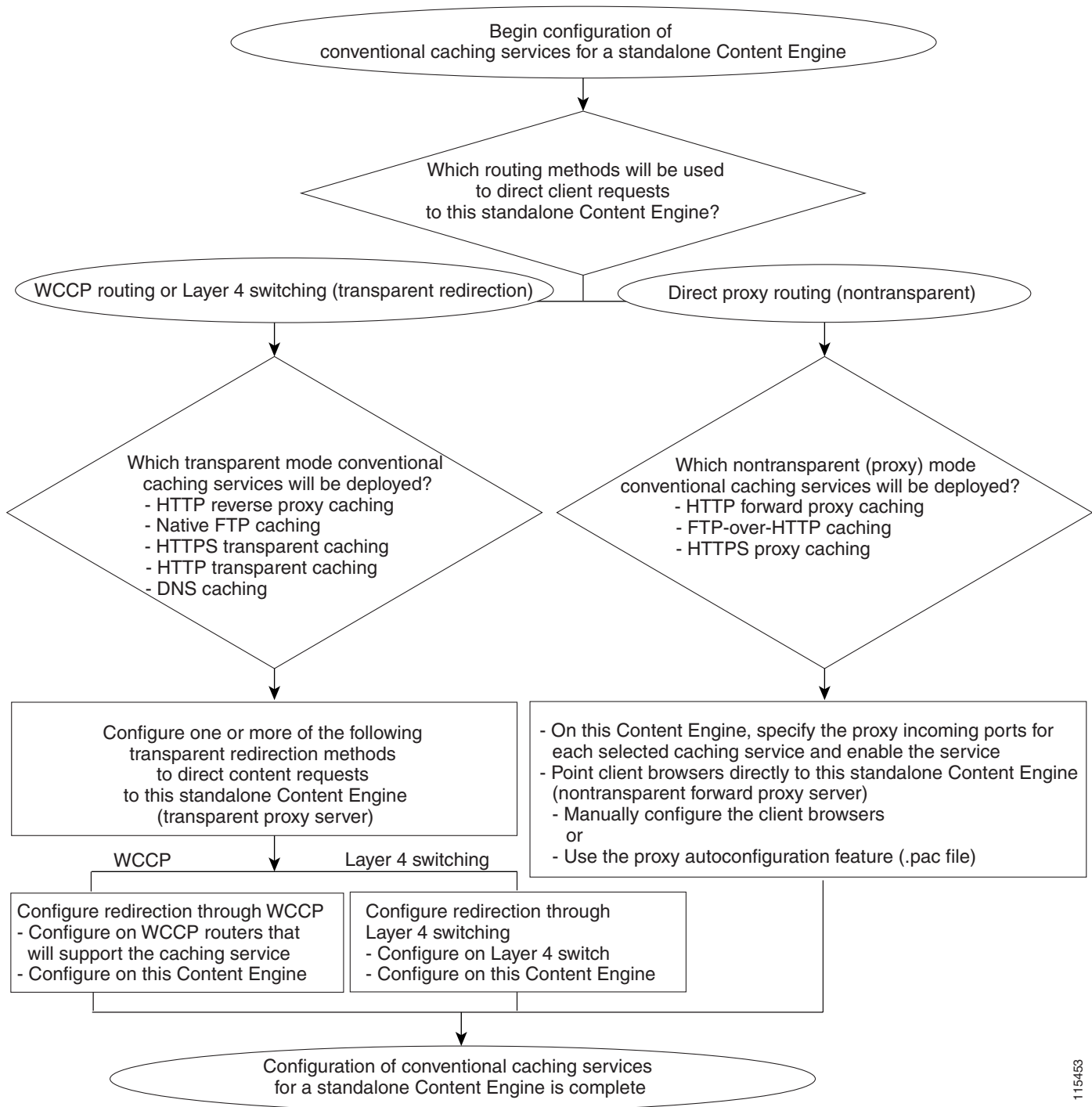
As the legend in [Figure 4-1](#) indicates, more detailed flowcharts are provided for configuring conventional caching services ([Figure 4-2](#)) and RealMedia streaming and caching services ([Figure 4-3](#)).

Figure 4-1 High-Level View of Configuring, Monitoring, and Troubleshooting Standalone Content Engines



115452

Figure 4-2 Detailed View of Configuring Conventional Caching Services for Standalone Content Engines

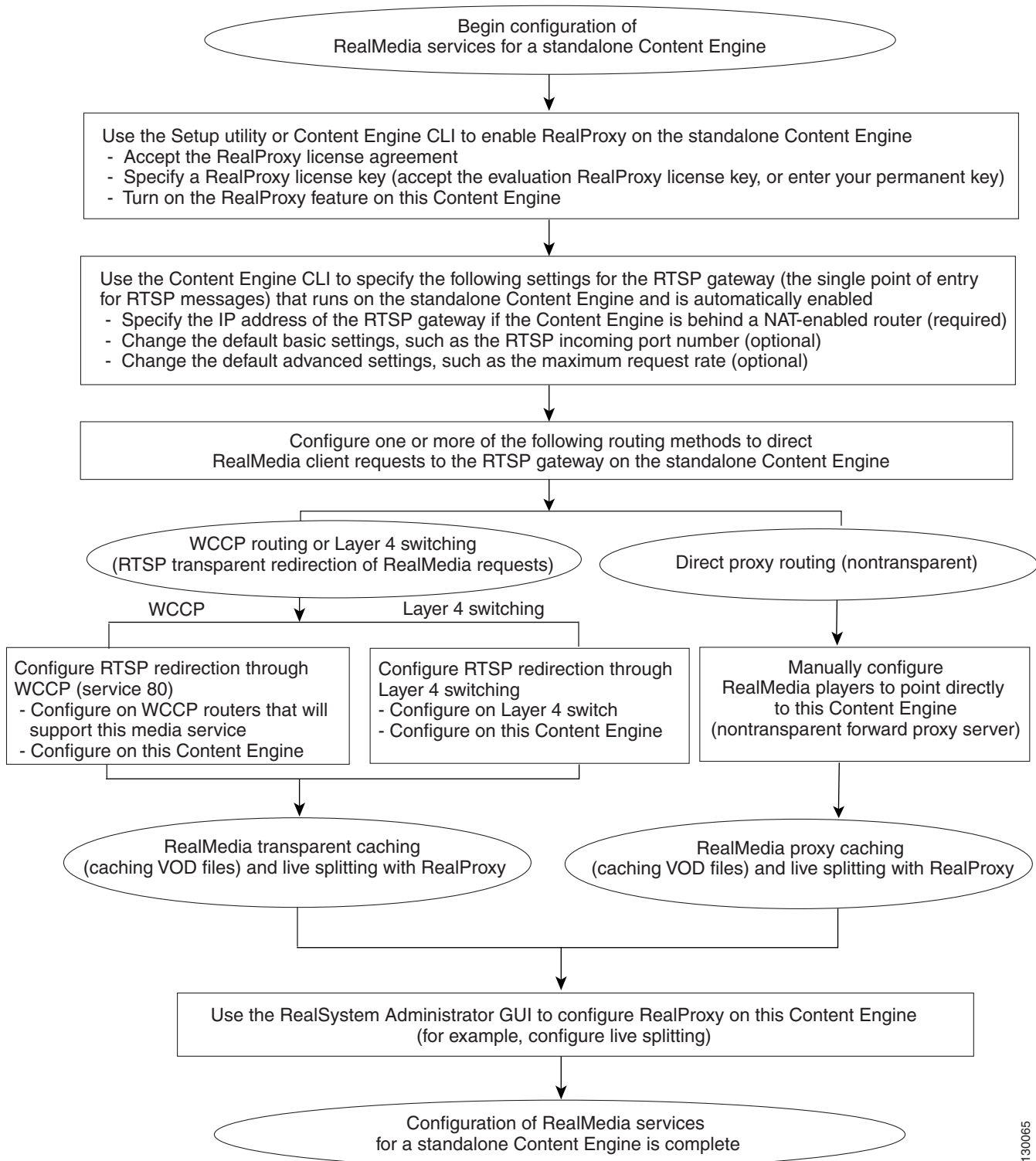


115463

This chapter describes how to use the Setup utility to configure the following three commonly used conventional caching services on standalone Content Engines: HTTP reverse proxy caching, HTTP transparent caching using WCCP Version 2, and HTTP forward proxy caching. For information about how to use the Content Engine CLI method (instead of the Setup utility) to configure these three services as well as other conventional caching services (for example, DNS caching and FTP caching), see [Chapter 7, “Configuring Conventional Caching Services for Standalone Content Engines.”](#)

This chapter describes how to use the Setup utility to configure the following two commonly used WMT MMS caching services on standalone Content Engines: WMT transparent caching and WMT proxy caching. For information about how to use the Content Engine CLI (instead of the Setup utility) to configure these caching services, other WMT RTSP services on a standalone Content Engine, see [Chapter 9, “Configuring WMT Streaming Media Services on Standalone Content Engines.”](#)

Figure 4-3 Detailed View of Configuring RealMedia Streaming and Caching Services for Standalone Content Engines



130065

This chapter describes how to use the Setup utility to configure the following two commonly used RealMedia caching services on standalone Content Engines: RealMedia transparent caching and RealMedia proxy caching. For information about how to use the Content Engine CLI (instead of the Setup utility) to configure these caching services or other RealMedia services (for example, RealProxy live splitting) on standalone Content Engines, see [Chapter 8, “Configuring RealMedia Services on Standalone Content Engines.”](#)

Checklist for Configuring, Monitoring, and Troubleshooting Standalone Content Engines

[Table 4-1](#) is a checklist of tasks for configuring, monitoring, and troubleshooting standalone Content Engines that are running the ACNS 5.4.1 software and later releases.

Table 4-1 Checklist for Configuring, Monitoring, and Troubleshooting Standalone Content Engines

Task	Additional Information and Instructions
<p>Start basic configuration</p> <ol style="list-style-type: none"> Decide which addressing scheme will be used to initially configure this standalone Content Engine. 	<p>The two supported addressing schemes are mutually exclusive:</p> <ul style="list-style-type: none"> Manually specify a static IP address and network mask Dynamically assign an IP address using the interface-level DHCP addressing scheme <p>See the “Deciding the Addressing Scheme for Standalone Content Engines” section on page 4-16.</p>
<ol style="list-style-type: none"> Decide which method will be used to configure this standalone Content Engine. <ul style="list-style-type: none"> Setup utility CLI command 	<p>This chapter describes how to use the Setup utility to expedite the basic configuration of standalone Content Engines. See the “Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine” section on page 4-21.</p> <p>A brief description of how to use the CLI method to configure general settings is provided in the “Using the CLI Command Method to Configure General Settings for Standalone Content Engines” section on page 4-18. For detailed information about the CLI commands used to configure general settings, see the <i>Cisco ACNS Software Command Reference, Release 5.5</i> publication.</p> <p>For information about how to use the CLI method to configure or modify one or more commonly used caching services and numerous other services (for example, DNS caching, FTP caching, WMT streaming, and RealMedia streaming services) running on standalone Content Engines, see the following chapters in this guide:</p> <ul style="list-style-type: none"> Chapter 7, “Configuring Conventional Caching Services for Standalone Content Engines” Chapter 8, “Configuring RealMedia Services on Standalone Content Engines” Chapter 9, “Configuring WMT Streaming Media Services on Standalone Content Engines”

Table 4-1 Checklist for Configuring, Monitoring, and Troubleshooting Standalone Content Engines (continued)

Task	Additional Information and Instructions
<p>3. Power up this Content Engine and open a console connection on one of its serial ports.</p>	<p>After you physically install the hardware and power up the Content Engine, you can access the ACNS software (Setup utility or CLI commands) to perform a basic configuration of this standalone (unregistered) Content Engine (instead of a Content Engine that will be registered with a Content Distribution Manager).</p>
<p>4. Use the Setup utility or CLI commands to configure the following general settings on this standalone Content Engine:</p> <ul style="list-style-type: none"> – Device network settings – Disk configuration 	<p>To use the Setup utility to configure the general settings, see the “Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine” section on page 4-21.</p> <p>To use the CLI command method to configure the general settings, see the “Using the CLI Command Method to Configure General Settings for Standalone Content Engines” section on page 4-18.</p>
<p>5. Choose which services will be deployed on this standalone Content Engine.</p> <ul style="list-style-type: none"> – Conventional caching services (DNS, HTTP, FTP, and HTTPS caching) – RealMedia streaming and caching services – WMT streaming and caching services 	<p>See the “Overview of Configuring Conventional Caching Services” section on page 7-2.</p> <p>See Chapter 8, “Configuring RealMedia Services on Standalone Content Engines.”</p> <p>See Chapter 9, “Configuring WMT Streaming Media Services on Standalone Content Engines.”</p>
<p>6. Configure one or more of the following routing methods to direct content requests to this standalone Content Engine:</p> <ul style="list-style-type: none"> – Direct proxy routing (nontransparent) – Transparent redirection (WCCP routing or Layer 4 switching) 	<p>For direct proxy routing, see the “Configuring Client Browsers and Media Players for Direct Proxy Routing” section on page 4-35.</p> <p>For WCCP routing, see the “Configuring WCCP Services on a Router” section on page 6-27.</p> <p>For Layer 4 switching, see the “Configuring Layer 4 Switching as a Redirection Method” section on page 6-50.</p>
<p>7. If direct proxy routing is to be used, is a *.pac file to be used?</p>	<ul style="list-style-type: none"> • If no, then manually configure each client browser to point directly to the standalone Content Engine as a direct proxy server, as described in the “Manually Pointing Client Browsers to a Standalone Content Engine” section on page 4-42. • If yes, then configure the standalone Content Engine and the client browsers to use a proxy autoconfiguration (PAC) file, as described in the “Using PAC Files to Point Client Browsers Directly to a Standalone Content Engine” section on page 4-37.
<p>8. Configure the chosen caching and streaming services on this standalone Content Engine.</p>	<p>The Setup utility allows you to configure a set of commonly used caching services (listed in Table 4-2) on a standalone Content Engine. We recommend that you use this utility to configure one or more of these caching services on your Content Engine. This allows you to get your Content Engine up and running a basic set of caching services. For more information, see the “Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine” section on page 4-21.</p>
<p>9. Verify the basic configuration.</p>	<p>Now that the basic configuration is completed, verify that these caching services are working properly. See the “Verifying the Basic Configuration” section on page 4-47.</p>

Table 4-1 Checklist for Configuring, Monitoring, and Troubleshooting Standalone Content Engines (continued)

Task	Additional Information and Instructions
10. You can now do any of the following tasks: <ul style="list-style-type: none"> – Configure content services. – Perform advanced configuration on this Content Engine. – Monitor and troubleshoot. 	See tasks 11 through 23 below in this table.
Configure content services (optional)	
11. Decide if end user access to the Internet is to be controlled (access control for HTTP, HTTPS, and FTP-over-HTTP requests).	<ul style="list-style-type: none"> • If no, then go to task 12. • If yes, then configure authentication and authorization, as described in Chapter 10, “Configuring Content Authentication and Authorization on Standalone Content Engines.”
12. Decide if URL filtering is to be used.	<ul style="list-style-type: none"> • If no, then go to task 13. • If yes, then configure URL filtering for HTTP, HTTPS, and FTP requests, as described in Chapter 11, “Configuring Content Preloading and URL Filtering on Standalone Content Engines.”
13. Determine whether there is an external ICAP server.	<ul style="list-style-type: none"> • If no, then go to task 14. • If yes, then configure the Internet Content Adaptation Protocol (ICAP) for HTTP and FTP-over-HTTP requests, as described in Chapter 12, “Configuring ICAP on Standalone Content Engines.”
14. Determine if there are any special requirements for processing content requests.	<ul style="list-style-type: none"> • If no, then go to task 15. • If yes, configure rules for HTTP, HTTPS, FTP-over-HTTP, WMT, and RTSP requests, as described in Chapter 13, “Configuring the Rules Template on Standalone Content Engines.”
Perform advanced configuration tasks (optional)	
15. Configure advanced transparent caching features (for example, traffic bypass, overload bypass, flow protection, and IP spoofing).	Chapter 15, “Configuring Advanced Transparent Caching Features on Standalone Content Engines”
16. Set up additional network interfaces on the standalone Content Engine.	Chapter 16, “Configuring Additional Network Interfaces and Bandwidth on Standalone Content Engines”
17. Configure bandwidth for interfaces and content services on this standalone Content Engine.	Chapter 16, “Configuring Additional Network Interfaces and Bandwidth on Standalone Content Engines”
18. Set up login authentication and authorization on this standalone Content Engine.	Chapter 17, “Configuring Administrative Login Authentication and Authorization on Standalone Content Engines”
19. Configure this standalone Content Engine for system accounting with TACACS+.	Chapter 18, “Configuring AAA Accounting on Standalone Content Engines”

Table 4-1 Checklist for Configuring, Monitoring, and Troubleshooting Standalone Content Engines (continued)

Task	Additional Information and Instructions
20. Configure IP access control lists (ACLs) on this standalone Content Engine.	Chapter 19, “Creating and Managing IP Access Control Lists for Standalone Content Engines”
21. View or modify TCP stack parameters for this standalone Content Engine.	Chapter 20, “Viewing and Modifying TCP Stack Parameters on Standalone Content Engines”
22. View or modify the system logging settings for this standalone Content Engine.	See the “ Monitoring the Performance of Specific URLs ” section on page 21-52 .
Monitor and troubleshoot	
23. Monitor this standalone Content Engine with SNMP, the ACNS software alarms, and the ACNS software logs.	Chapter 21, “Monitoring Standalone Content Engines and Transactions”
24. Use the traceroute and the other supported diagnostic tools for troubleshooting.	Chapter 22, “Troubleshooting”

Configuring a Basic Configuration on Standalone Content Engines with the Setup Utility

This section provides an overview of the Setup utility and describes how to use this tool to configure a basic configuration on a standalone Content Engine in either of the situations:

- Case 1—The Content Engine is being booted up for the first time (for example, the Content Engine was purchased with the ACNS 5.4 software), and you want to use the Setup utility to configure the basic configuration settings (the general settings [device network settings and disk configuration], and a set of commonly used caching services [listed in [Table 4-2](#)]).
- Case 2—The device is a standalone Content Engine with some basic configuration (for example, the Content Engine was upgraded to the ACNS 5.4 software, and already has device network settings, disk configuration, and HTTP proxy caching configured). You want to use the Setup utility to complete the basic configuration of this standalone Content Engine (for example, configure some of the other commonly used caching services that are not yet configured).

In Case 1, the Setup utility is automatically launched when you initially boot up a device. Completing the initial basic configuration in this situation involves these tasks:

- [Deciding the Addressing Scheme for Standalone Content Engines, page 4-16](#)
- [Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine, page 4-21](#)

In Case 2, you manually launch the Setup utility with the **setup** privileged EXEC command. For more information on this topic, see the “[Manually Launching the Setup Utility](#)” section on [page 4-19](#).

After completing this basic configuration, you must configure the client browsers and media players (see “[Configuring Client Browsers and Media Players for Direct Proxy Routing](#)”) for direct proxy routing, and configure the WCCP routers for transparent redirection (see “[Configuring WCCP Routers for Transparent Redirection](#)”). After verifying that this basic configuration is working properly, you can use

the CLI commands or Content Engine GUI to configure additional caching services (for example, DNS caching, FTP caching, and HTTPS caching), streaming services (WMT streaming and RTSP streaming), or content services. You can also perform advanced configuration or monitor this Content Engine.

**Note**

Throughout the rest of this chapter the term *WCCP Version 2-enabled router* denotes a router that is running WCCP Version 2.

Commonly Used Caching Services Configurable Through the Setup Utility

Table 4-2 lists the commonly used caching services that you can quickly configure on a standalone Content Engine through the Setup utility.

Table 4-2 Commonly Used Caching Services Configurable Through the Setup Utility

Caching Service	Description
HTTP forward proxy caching	The standalone Content Engine functions as a nontransparent forward proxy server for HTTP requests. After receiving an HTTP request directly from a client browser, the Content Engine retrieves and caches the requested content if it is not already stored in its local cache, and sends the requested content to the requester (client browser).
HTTP transparent caching	The standalone Content Engine functions as a transparent proxy server for HTTP requests. After receiving a redirected HTTP request, the Content Engine retrieves and caches the requested content if it is not already stored in its local cache, and sends the requested content to the requester (client browser). With the Setup utility, you can configure the Content Engine to accept redirected HTTP requests from a WCCP Version 2-enabled router. With the Content Engine CLI, you can configure the Content Engine to accept redirected HTTP requests from the WCCP Version 2-enabled router or a Layer 4 switch.
HTTP reverse proxy caching	The standalone Content Engine functions as a transparent proxy server for specific web servers (for example, web servers in a web server farm) as opposed to acting as a proxy for end users (web clients). After receiving a redirected reverse proxy request, the Content Engine retrieves and caches the requested content if it is not already stored in its local cache, and sends the requested content to the requester (client browser). With the Setup utility, you can configure the Content Engine to accept redirected reverse proxy requests from a WCCP Version 2-enabled router. With the Content Engine CLI, you can configure the Content Engine to accept redirected reverse proxy requests from a WCCP Version 2-enabled router or a Layer 4 switch.
WMT proxy caching	The standalone Content Engine functions as a nontransparent proxy server for end users who are using Windows Media Player to request WMT content. After receiving a WMT request directly from a client Windows Media Player, the Content Engine retrieves the requested content if it is not already stored in its local cache, stores a copy locally whenever possible, and sends the requested content to the requester (client Windows Media player).
WMT transparent caching	The standalone Content Engine functions as a transparent proxy server for end users who are using Windows Media player to request content. After receiving a transparently redirected WMT request, the Content Engine retrieves the requested content if it is not already stored in its local cache, stores a copy locally whenever possible, and sends the requested content to the requester (client Windows Media player). With the Setup utility, you can configure the Content Engine to accept redirected WMT requests from a WCCP Version 2-enabled router. With the Content Engine CLI, you can configure the Content Engine to accept redirected WMT requests from a WCCP Version 2-enabled router or a Layer 4 switch.

- When you are prompted for a particular configuration setting, the default value is displayed. Press **Enter** to select the default value. For example, press **Enter** to specify that you want to use the default WCCP router (default gateway that has the IP address of 10.0.1.1) when prompted as follows:

```
Please enter the IP addresses of WCCP routers [10.0.1.1]:
```

- After you specify whether you want to configure a particular setting, the corresponding menu option is marked as “Complete” or “Incomplete.” This helps you track which basic configuration settings you have configured and which ones still need to be configured on this standalone Content Engine.
- When you configure a particular setting by choosing a menu option in the Setup utility, the corresponding CLI command is configured. (See [Table 4-3](#).) After you use the Setup utility to specify a specific basic configuration setting, a list of configured CLI commands appears (see example). When you are asked if you want to save this configuration, press **Enter** to save the displayed configuration.

NOTE: Please remember to configure web-cache service on the router. Based on the input, the following CLIs will be configured:

```
wccp router-list 1 10.0.1.1
wccp version 2
wccp web-cache router-list 1
```

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

- To display a list of constructed CLI commands at any time during a Setup utility session, choose the **Print Configurations** option from the Setup utility menu.
- After you specify a configuration setting, the Setup utility reports any dependencies or incompatibility between the specified options. For example, if you have enabled any of the streaming caching services, then you are informed that you should allocate disk space for the media file system (mediafs) when you configure the disk.
- If any failure occurs when the Setup utility is applying the specified configuration settings (for example, the disk configurations and the corresponding CLI command), the Setup utility displays a message indicating which specific setting could not be applied. Error messages are also written to `/local1/errorlog/setup_(clildisk)_config_error`.
- A basic configuration (see example) is constructed based on the information that you specify through the Setup utility. The following is an example of a basic configuration for a standalone Content Engine that has all seven of the commonly used caching services configured:

```
Here is the current profile of this device
```

```
CDN device                : No
HTTP Proxy Caching        : Yes
HTTP Tranparent Caching   : Yes
HTTP Reverse Proxy Caching : Yes
WMT Proxy Caching         : Yes
WMT Transparent Caching   : Yes
Real Media Proxy Caching  : Yes
Real Media Transparent Caching: Yes
```

```
Do you want to change this (y/n) [n]:
```

```
Press the ESC key at any time to quit this session
```

This basic configuration is cached. A copy of the configurations generated through the Setup utility is stored on disk (`/local/local1/setup_gen_config.txt`).

- For information about how to launch the Setup utility, see the [“Launching the Setup Utility” section on page 4-19](#).

Setup Utility Menu Options and Corresponding CLI Commands

The menu structure of the Setup utility is hierarchical. For example, after you choose the General Settings option from the main menu, the General Settings submenu appears. As the following example shows, your current location in the menu structure is displayed after the menu options.

```

+-----+
|                                     |
|                               General Settings |
|-----+
|-> Network Configurations :Incomplete
|   Disk Configurations   :Incomplete
|   Print Configuration
|   Previous Menu (p)
|   Main Menu (m)
|   Exit (e)
+-----+

Main Menu
  ---> General Settings

```

Table 4-3 lists the Setup utility menu option and the corresponding Content Engine CLI command. For detailed descriptions of the CLI commands you can use to configure network settings and disk configuration, see the *Cisco ACNS Software Command Reference, Release 5.4* publication. Information about how to use the CLI method (instead of the Setup utility) to configure any of the commonly used caching services (listed in Table 4-2) and other features are provided in subsequent chapters of this guide.

Table 4-3 Setup Utility Menu Options and Corresponding CLI Commands for Standalone Content Engines

Setup Utility Menu Option	Content Engine CLI Command
General Settings	
Network Configuration	ip address {ip address netmask dhcp} ip default-gateway hostname ip name-servers ip domain-name
Disk Configuration	disk config sysfs {remaining disk-space} [cfs {remaining disk-space}] [mediafs {remaining disk-space}]
Caching-Related Configurations	
HTTP proxy caching	http proxy incoming
HTTP transparent caching	wccp router list wccp web-cache router-list wccp version 2
HTTP reverse proxy caching	wccp router list wccp reverse-proxy router-list wccp version 2

Table 4-3 Setup Utility Menu Options and Corresponding CLI Commands for Standalone Content Engines (continued)

Setup Utility Menu Option	Content Engine CLI Command
WMT proxy caching	wmt license-key wmt evaluate wmt accept-license-agreement wmt enable
WMT transparent caching	wccp router list wccp wmt router-list wccp version 2 wmt license-key wmt evaluate wmt accept-license-agreement wmt enable
RealMedia proxy caching	rtsp proxy media-real license-key rtsp proxy media-real evaluate rtsp proxy media-real accept-license-agreement rtsp proxy media-real enable
RealMedia transparent caching	wccp router list wccp rtsp router-list wccp version 2 rtsp proxy media-real license-key rtsp proxy media-real evaluate rtsp proxy media-real accept-license-agreement rtsp proxy media-real enable

Setup Utility Arrows and Keys

Table 4-4 describes the keys and arrows that you can use with the Setup utility.

Table 4-4 Keys and Arrows for the Setup Utility

Keys	Description
?	Displays information about why a particular menu item (for example, Network Configurations) is currently listed as “Incomplete.”
ESC	Quits the current dialog session and to return to the previous menu.

Table 4-4 Keys and Arrows for the Setup Utility (continued)

Keys	Description
e	<p>From a menu, use this hot key to exit the menu interface (to exit the current Setup utility session):</p> <pre> +-----+ General Settings +-----+ -> Network Configurations :Incomplete Disk Configurations :Incomplete Print Configuration Previous Menu (p) Main Menu (m) Exit (e) +-----+ </pre> <p>If any of the required options are incomplete, the following prompt appears:</p> <pre> Some of the configurations are still incomplete. Do you want to go back and complete them (y/n) [y]: </pre> <p>Press Enter to return to the main menu and complete the configuration of the required options, or enter n to quit the Setup utility session without completing the required options.</p>
m	Returns to main menu from a submenu.
p	Returns to the previous menu from a submenu.
Enter	Selects the highlighted menu option or to select the default option that is displayed.
Up arrow	Moves the cursor up one line.
Down arrow	Moves the cursor down one line.

Deciding the Addressing Scheme for Standalone Content Engines

Before beginning the initial configuration of a Content Engine as a standalone device, you should decide which addressing scheme will be used for this Content Engine. The two supported addressing schemes for standalone Content Engines that are running the ACNS 5.x software are mutually exclusive:

- Manually specify a static IP address and network mask.
- Dynamically assign an IP address using the interface-level DHCP addressing scheme.



Note

Autoregistration needs to be disabled on the Content Engine before you can configure a Content Engine interface with interface-level DHCP or a static IP address. For information about how to disable autoregistration through the Setup utility, see [Step 1](#) in the “Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine” section on page 4-21.

If you do not enable interface-level DHCP on the Content Engine, you must manually specify a static IP address and network mask for the Content Engine. If the Content Engine moves to another location in another part of the network, you must manually enter a new static IP address and network mask for this Content Engine.

If you want to enable DHCP and are using the Setup utility to configure a standalone Content Engine, answer **y** when prompted (as described in [Step 7](#) in the “Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine” section on page 4-21).

```
Do you want to enable DHCP on this interface? (y/n) [y]:y
```

If you are using the CLI method (instead of the Setup utility) to configure a standalone Content Engine, use the **ip address dhcp** interface configuration to enable interface-level DHCP on a standalone Content Engine.

About Device Network Settings for Standalone Content Engines

In order to deploy a device as a standalone Content Engine on your network, you must initially configure a set of network settings on the Content Engine. These settings are collectively referred to as *device network settings*. After the device network settings are defined for the standalone Content Engine, it can become active on your network.

The device network settings that you should have before you start the basic configuration include the following:

- Host name of the Content Engine (for example, if you assign the Content Engine the name CE7305, the prompt will appear as:
CE7305(config)#)
- Internet Protocol (IP) domain name (for example, cisco.com)
- Administrator password
- IP addresses for the Content Engine

If a static IP address is assigned to this Content Engine (for example, 10.0.1.2 as shown in [Figure 4-4](#)), then you must also assign it an IP address network mask (for example, 255.255.255.0).



Tip

You also have the option of using interface-level DHCP to dynamically assign an IP address to a Content Engine interface instead of manually assigning a static IP address and network mask.

- Default gateway (for example, the router with address 10.0.1.1 is the default gateway for the Content Engine shown in [Figure 4-4](#))
- DNS name server (for example, in [Figure 4-4](#), the Content Engine will use the DNS server with the address 172.16.0.2 for domain name resolution)

Figure 4-4 Configuring Device Network Settings on Standalone Content Engines

**Note**

Throughout the rest of this chapter, the term *general settings* is used to refer collectively to device network settings and disk configuration.

The ACNS 5.x software provides a Common Interface File System (CIFS) client and a Network File System (NFS) client for Content Engines to communicate with network attached storage (NAS) devices. For more information on this topic, see the [“Mounting to a Network Attached Storage Device”](#) section on page 5-13.

Using the CLI Command Method to Configure General Settings for Standalone Content Engines

To use the CLI command method (instead of the Setup utility) to configure the general settings on a standalone Content Engine, follow these steps:

- Step 1** Open a console connection on the Content Engine, and log in to the Content Engine CLI using an ACNS system account that has superuser privileges. For more information see the [“Using Telnet or a Console Session to Log in to a Standalone Content Engine”](#) section on page 4-50.
- Step 2** From privileged EXEC mode, enter global configuration mode to specify the general settings for this standalone Content Engine:

```
CE# config
```

Step 3 Configure the Ethernet interface on this Content Engine. You must do one of the following:

- To assign a static IP address and network mask (and not enable DHCP on this interface), enter the following command:

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

- To enable interface-level DHCP, enter the following command:

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

If you configure your Ethernet interface using interface-level DHCP, then the remainder of the device network settings for this standalone Content Engine are automatically configured and you are finished with the configuration of the device network settings. If you manually assigned a static IP address, use the **ip default-gateway**, **ip name-server**, **hostname**, **ip domain-name**, and **primary-interface** global configuration commands to specify the remaining device network settings. Use the **disk config sysfs** global configuration command to use the Content Engine CLI command method to configure disk space.

Launching the Setup Utility

The Setup utility can be launched in these ways:

- Manually at any time by entering the **setup** privileged EXEC command at the CLI prompt
- Automatically when you initially boot up a device



Note

A Content Engine that is running the ACNS software comes with a single predefined superuser user account (root administrator). This predefined account can be used to invoke the Setup utility. The username for this predefined superuser user account is `admin` and the default password is `default`. If these defaults have been changed by another ACNS system administrator, you must obtain the new username and password.

Manually Launching the Setup Utility

To launch the Setup utility manually on a standalone Content Engine that already has its device network settings defined, follow these steps:

Step 1 Using a login account that has the superuser privilege rights (privilege level of 15), log in to the Content Engine CLI through Telnet or Secure Shell (SSH) Version 1 or Version 2.



Note

For more information about logging in to the Content Engine CLI, see the [“Using Telnet or a Console Session to Log in to a Standalone Content Engine”](#) section on page 4-50. For more information about the different CLI modes, see the [“ACNS Software CLI Command Modes for Standalone Content Engines”](#) section on page B-8.

- Step 2** Launch the Setup utility manually to configure one or more of the commonly used caching services (listed in [Table 4-2](#)).

```
ContentEngine# setup
```

The current basic configuration for this standalone Content Engine appears.

The displayed basic configuration also indicates which of the commonly used caching services are already configured on this Content Engine. In this case, only the HTTP proxy caching service is currently configured on this Content Engine.

Here is the current profile of this device

```
CDN device                : No
HTTP Proxy Caching        : Yes
HTTP Transparent Caching  : No
HTTP Reverse Proxy Caching : No
WMT Proxy Caching         : No
WMT Transparent Caching   : No
Real Media Proxy Caching  : No
Real Media Transparent Caching: No
```



Note The displayed basic configuration indicates that this Content Engine is not a *CDN device*. This is because the standalone Content Engine is intentionally not registered with a Content Distribution Manager.

You can quickly modify the basic configuration of this standalone Content Engine by entering *y* when prompted as shown below.

```
Do you want to change this (y/n) [n]:y
```

For more information about how you can use the Setup utility to configure or modify the basic configuration of this Content Engine, see the [“Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine”](#) section on page 4-21.

Automatically Launching the Setup Utility

When you initially boot up a device, follow these steps to launch the Setup utility automatically:

- Step 1** Power up the Content Engine and open a console connection.

You must use a console connection rather than a Telnet session for initial configuration of these device network settings on the Content Engine. However, once you have used a console connection to define the device network settings, you can then use a Telnet session to perform subsequent configuration tasks on this Content Engine. For more information about using a console connection, see the [“Using Telnet or a Console Session to Log in to a Standalone Content Engine”](#) section on page 4-50.

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:0019
```

At the appearance of this prompt, a 30-second countdown begins, during which you can launch the Setup utility.

- Step 2** Press **Enter**.

Step 3 When prompted, enter the administrator password and press **Enter**.

```
admin password:
```

This is the case-sensitive password for the predefined superuser account. The password can include any printable character. By default, the username is *admin* and the password is *default*. The administrator password can be up to 20 characters long and is case sensitive. Each Content Engine in a farm must have a password. You must enter a password before pressing **Enter**.

Step 4 When prompted, reenter the administrator password and press **Enter**.

```
re-enter password:
```

The Setup utility is automatically launched, and you are prompted to specify the device mode for this particular device. When the Setup utility is launched on a Content Engine that supports device mode changes (for example, the CE-565), you are prompted to specify the device mode for that particular device.

Step 5 When prompted, press **Enter** or enter **CE** to specify the Content Engine device mode for this standalone Content Engine.

```
What is the mode of the device (CE/CR/CDM/PM) [CE]: CE
```

Step 6 When prompted, enter **no** to specify that this Content Engine is not going to be managed by a Content Distribution Manager.

```
Is this CE going to be managed by a CDM (Content Distribution Manager)  
(y/n) [y]: no
```

For more information about how to use the Setup utility after booting up a device for the first time, see the [“Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine”](#) section on page 4-21.

Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine

To use the Setup utility to configure a basic configuration on a standalone Content Engine, follow these steps:

Step 1 Launch the Setup utility.

- If this is the first time that the device is being booted up, follow these steps:
 - Power up the device, open a console connection, and automatically invoke the Setup utility. (For detailed instructions, see the [“Automatically Launching the Setup Utility”](#) section on page 4-20.)
 - When the Setup utility is launched on a Content Engine that supports device mode changes (for example, the CE-565), you are prompted to specify the device mode for that particular device. When prompted, press **Enter** or enter **CE** to specify the Content Engine device mode for this standalone Content Engine.

```
What is the mode of the device (CE/CR/CDM/PM) [CE]: CE
```

- When prompted, enter **n** to specify that this Content Engine is not going to be managed by a Content Distribution Manager.

```
Is this CE going to be managed by a CDM (Content Distribution Manager)
(y/n) [y]:n
```

By default, the autoregistration is enabled on a Content Engine. When autoregistration is enabled on a Content Engine, the Content Engine automatically searches for and registers with the Content Distribution Manager on the network. Because you want to deploy your Content Engine as a *standalone* device that is not registered with a Content Distribution Manager, you must specify **n** to disable autoregistration on this Content Engine.



Note If you are using the CLI method to configure a standalone Content Engine (instead of the Setup utility), you can manually disable autoregistration by specifying the **no auto-register enable** global configuration command.

- Proceed to [Step 2](#) below.
- If the standalone Content Engine is running the ACNS 5.4 software and already has some of its basic configuration settings configured, follow these steps:
 - Manually invoke the Setup utility, as described in the [“Manually Launching the Setup Utility” section on page 4-19](#).
 - Proceed to [Step 2](#) below.

Step 2 When prompted, press **Enter** or enter **y** to indicate that you want to configure one or more of the seven commonly used caching services on this standalone Content Engine.

```
Do you want to configure this CE for doing HTTP Proxy Caching (y/n) [y]:y
```

```
Do you want to configure this CE for doing HTTP Transparent Caching
using WCCP (y/n) [y]:y
```

```
Do you want to configure this CE for doing HTTP Reverse Proxy Caching
using WCCP (y/n) [y]:y
```

```
Do you want to configure this CE for doing WMT Proxy Caching (y/n) [y]:y
```

```
Do you want to configure this CE for doing WMT Transparent Caching
using WCCP (y/n) [y]:y
```

```
Do you want to configure this CE for doing Real Media Proxy Caching (y/n) [y]:y
```

```
Do you want to configure this CE for doing Real Media Transparent Caching
using WCCP (y/n) [y]:y
```


Step 5 Press **Enter** to choose the highlighted Network Configurations menu option.

The following warning appears.

```
WARNING: Changing any of the network settings from a
telnet session may render the device inaccessible on
the network. Therefore it is suggested that you have
access to the console before modifying the network settings.
```

Step 6 After the warning appears, you are prompted to choose an interface identifier for the initial configuration of this Content Engine. Enter an interface identifier (for example, enter **1** to specify the Gigabit Ethernet 1/0 interface).

```
Please choose an interface to configure from the following list:
1: GigabitEthernet 1/0
2: GigabitEthernet 2/0
```

```
Enter choice:1
Press the ESC key at any time to quit this session
```



Note You can configure additional interfaces for this Content Engine through CLI commands at a later time, as described in the [“Configuring Additional Network Interfaces”](#) section on page 16-2.

Step 7 After specifying an interface identifier, you are asked if you want to enable interface-level DHCP on this particular interface.

- To not enable DHCP on this interface, go to [Step 8](#).
- To enable DHCP on this interface, when prompted, enter **y**:

```
Do you want to enable DHCP on this interface? (y/n) [y]:y
```

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

```
interface GigabitEthernet 1/0
 ip address dhcp
 exit
```

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

When you enter it again to accept the configuration, the remainder of your device network settings are automatically configured for this Content Engine. The main menu of the Setup utility appears and indicates that the configuration of the device network settings (Network Configuration) for this Content Engine is now “Complete.” Go to [Step 9](#).

Step 8 Alternatively, to continue the configuration process using the static IP address method (and not enable interface-level DHCP on this Content Engine), follow these steps:

a. When prompted, enter **n**:

```
Do you want to enable DHCP on this interface? (y/n) [y]:n
```

b. When prompted for a local IP address, specify a static IP address (for example, 10.0.1.2).

```
Please enter the IP address of this interface:10.0.1.2
```

c. When prompted, specify the network mask (for example, 255.255.255.0)

```
Please enter the netmask of this interface:255.255.255.0
```

d. When prompted, specify the IP address of the gateway (for example, 10.0.1.1).

```
Please enter the default gateway:10.0.1.1
```

- e. When prompted, specify the IP address of the DNS server (for example, 172.16.0.2).

Please enter the domain name server IP: **172.16.0.2**

- f. When prompted, specify the IP domain name of this Content Engine (for example, cisco.com).

Please enter the domain name: **cisco.com**

- g. When prompted, specify the host name of this Content Engine (for example, CE7305).

Please enter the hostname: **CE7305**

A message appears, indicating which CLI commands will be configured based on your input.

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

```
interface GigabitEthernet 1/0
ip address 10.0.1.2 255.255.255.0
exit
ip default-gateway 10.0.1.1
ip name-server 172.16.0.2
ip domain-name cisco.com
hostname CE7305
```

- h. When prompted, enter **y** to save these network configurations on this standalone Content Engine.

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

The main menu appears, indicating that the configuration of the device network settings (network configuration) for this standalone Content Engine is now complete.



Note You are now finished with the configuration of the device network settings for this Content Engine, which is now standalone. The next step is to configure the disk space on this standalone Content Engine. Go to [Step 9](#).

Step 9 Configure the disk configuration for this standalone Content Engine, as follows:

- a. From the main menu, choose the General Settings option. In the displayed General Settings submenu, choose the Disk Configurations option. The current storage allocation for this standalone Content Engine appears as shown in the following example:

```
Here is the current storage allocation scheme:
SYSFS                29.9GB
CFS                  0.0GB
MEDIASF              0.0GB      0.0% (from-unused)
CDNFS                1.0GB
```

Do you want to change this (y/n) [n]:

Disk space in ACNS software is allocated on a per-file system basis, rather than on a per-disk basis. You can configure your overall disk storage allocations according to the kinds of client protocols you expect to use and the amount of storage that you need to provide for each of the functions, as described in this table.

Disk Storage Type	Function
sysfs (system file system)	Stores log files, including transaction logs, syslogs, and internal debugging logs. Also can store image files and configuration files.
cfs (cache file system)	Caches HTTP and FTP objects.
mediafs (media file system)	Caches content that is fetched through the two streaming protocols (RTSP and WMT). By default 30 percent of the mediafs space is reserved for RTSP streaming content, and 70 percent is reserved for WMT streaming content.

- b. When prompted, enter **y** to change the current storage allocations on this Content Engine.

```
Do you want to change this (y/n) [n]:y
```

The following questions will prompt you how the available storage is to be allocated to different file systems. You can either enter an absolute amount of storage in GB or MB, or a percentage of the available storage. In the former case, the desired amount should be entered followed by either 'GB' or 'MB', and in the latter case, the number should be followed by '%'

- c. When prompted, enter the amount of storage to be allocated to the system file system (sysfs). For example, enter **2GB**.

```
Please enter the amount of storage to be allocated
to SYSFS (This file system is used for storing user
and logging files; at least 1GB required):2GB
```

- d. When prompted, enter the amount of storage to be allocated to the cache file system (cfs). For example, enter **20MB**.

```
Please enter the amount of storage to be allocated
to CFS (This file system is used for storing HTTP
objects):20MB
```

- e. When prompted, enter **0GB** or **0%** to specify that no amount of storage is to be allocated to the ACNS network file system (cdnfs).

```
Please enter the amount of storage
to CDNFS (This file system is used for
prepositioned content):0GB
```



Note You do not want to allocate any storage to the cdnfs because this file system is used to store pre-positioned content on a registered Content Engine. You cannot pre-position content on a standalone Content Engine. However, you can preload content on a standalone Content Engine at a later time, as described in the [“Configuring Content Preloading for Standalone Content Engines”](#) section on page 11-2.

- f. When prompted, enter the amount of storage to be allocated to the media file system (mediafs). If you plan to enable WMT caching or RTSP caching on this standalone Content Engine, then you must allocate storage for the mediafs. For example, enter **10MB**.

```
Please enter the amount of storage to be allocated
to MEDIAFS (This file system is used for storing WMT
and Real media content):10MB
```

The new disk configuration for this standalone Content Engine appears, as shown in the following example:

Here is the new disk configuration:

```

SYSFS          2GB
CFS            20MB
CDNFS         0GB
MEDIASF       10MB

```

- g. When prompted, enter **y** to accept the new disk configuration.

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

The General Settings submenu appears and the Disk Configurations option is now reported as “Complete.” The general settings (network configuration settings and the disk configurations) are now configured on this standalone Content Engine.

```

+-----+
|                                     |
|                               General Settings                               |
|-----+
|-> Network Configurations :Complete
|   Disk Configurations   :Complete
|   Print Configuration
|   Previous Menu (p)
|   Main Menu (m)
|   Exit (e)
+-----+

```

```

Main Menu
---> General Settings

```

Configure IP address, default gateway, name servers, domain name, etc

Step 10 Configure one or more of the commonly used caching services (see [Table 4-2](#) for list) on this standalone Content Engine, as follows:

- a. Use one of the following methods to display the Caching Related Configurations submenu:
 - From the General Settings submenu, choose the **Main Menu** option to return to the main menu. The Caching Related Configurations menu option is currently reported as “Incomplete” because you have not configured any caching services on this Content Engine yet.

Step 12 Configure HTTP proxy caching as follows:

- a. From the HTTP Caching submenu, choose the **HTTP Proxy Caching** option.
- b. When prompted, specify the incoming proxy ports for proxy-style HTTP requests from client browsers. These are the port numbers on which this standalone Content Engine will accept incoming proxy-style HTTP requests. These are also the ports that the Content Engine will use to serve the requested content to the requester (the client browser). For HTTP proxy caching, this standalone Content Engine is functioning as a nontransparent forward proxy server that receives HTTP requests directly from the client browsers.

The incoming proxy port numbers can be from 1 to 65535. You can specify up to eight incoming proxy ports, each separated by a space. The incoming proxy ports can be the same ports that are used by transparent mode services (for example, HTTP transparent caching) on this standalone Content Engine.

```
Please enter all the HTTP Proxy incoming ports
(up to 8, separated by spaces) [80 8080]:80 8080 8081
```

A list of the configured CLI commands appears and you are asked if you want save this configuration. Enter **y** to accept this configuration.

```
Based on the input, the following CLIs will be configured:
http proxy incoming 80 8080 8081
```

- c. When prompted, enter **y** to accept this configuration.

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

The specified settings are saved and the HTTP Caching submenu reappears. The HTTP Proxy Caching option is now listed as “Complete.” Remember that you still must configure the client browsers to point directly to this Content Engine as their HTTP proxy server, as described in the [“Pointing Client Browsers Directly to a Standalone Content Engine”](#) section on page 4-36.

Step 13 Configure HTTP transparent caching using WCCP as follows:

- a. From the HTTP Caching submenu, choose the **HTTP Transparent Caching** option.
- b. When prompted, specify the IP addresses of the WCCP Version 2-enabled routers that will transparently redirect HTTP requests to this standalone Content Engine on port 80 only, or press **Enter** to use the default gateway. In this case, the default gateway (the WCCP Version 2-enabled router that was specified as this Content Engine’s default gateway) has an IP address of 10.0.1.1.

```
Please enter the IP addresses of WCCP routers [10.0.1.1]:
```

- c. Enter **y** to enable HTTP transparent caching on this Content Engine.

```
Do you want to enable HTTP transparent caching (y/n) [y]:y
```

A list of the configured CLI commands appears, along with a reminder that you must configure the web-cache service (WCCP service 0) on the WCCP Version 2-enabled router.

NOTE: Please remember to configure web-cache service on the router.
Based on the input, the following CLIs will be configured:

```
wccp router-list 1 10.0.1.1
wccp version 2
wccp web-cache router-list 1
```

- d. Enter **y** to accept this configuration.

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

The specified settings are saved and the HTTP Caching submenu reappears. The HTTP Transparent Caching option is now listed as “Complete.” Remember that you still must configure the web-cache service (WCCP service 0) on the WCCP Version 2-enabled routers, as described in the [“Configuring WCCP Services on a Router”](#) section on page 6-27.

Step 14 Configure HTTP reverse proxy caching using WCCP as follows:

- a. From the HTTP Caching submenu, choose the **HTTP Reverse Proxy Caching** option.
- b. When prompted, specify the IP addresses of the WCCP Version 2-enabled routers that will redirect reverse proxy packets to this Content Engine, or press **Enter** to use the default gateway (for example, the WCCP Version 2-enabled router with the IP address of 10.0.1.1).

```
Please enter the IP addresses of WCCP routers [10.0.1.1]:
```

- c. Enter **y** to enable HTTP reverse proxy caching on this Content Engine.

```
Do you want to enable HTTP reverse proxy caching (y/n) [y]:y
```

A list of the configured CLI commands appears, along with a reminder that you must still configure WCCP service 99 (reverse proxy caching) on the WCCP Version 2-enabled router.

NOTE: Please remember to configure service 99 on the router. Based on the input, the following CLIs will be configured:

```
wccp router-list 1 10.0.1.1
wccp version 2
wccp reverse-proxy router-list 1
```

- d. Enter **y** to accept this configuration.

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

The specified settings are saved and the HTTP Caching submenu reappears. The HTTP Reverse Proxy Caching option is now listed as “Complete.” Remember to configure the reverse proxy caching service (WCCP service 99) on the WCCP Version 2-enabled router, as described in the [“Configuring the Reverse-Proxy Service \(Service 99\) on a Router”](#) section on page 6-33.

Step 15 Configure WMT caching as follows:

- a. Use one of the following methods to display the WMT Caching submenu.
- From the HTTP Caching submenu, choose the **Previous Menu** option and then choose the **WMT Caching** option from the Caching Related Configurations submenu.
 - From the Caching Related Configurations submenu, choose the **WMT Caching** option.

- From the main menu, choose the **Caching Related Configurations** option and then choose the **WMT Caching** option from the Caching Related Configurations submenu.

In the following example, both WMT caching services (WMT proxy caching and WMT transparent caching) are to be configured on this standalone Content Engine:

```

+-----+
|                                     |
|                               WMT Caching |
|-----+-----+
| -> WMT Proxy Caching           :Incomplete |
|     WMT Transparent Caching   :Incomplete |
|     Print Configuration        |
|     Previous Menu (p)         |
|     Main Menu (m)             |
|     Exit (e)                  |
+-----+-----+

```

```

Main Menu
----> Caching Related Configurations
      ---> WMT Caching

```

Configure this CE for doing WMT Proxy caching

- To configure WMT proxy caching, complete [Step 16](#).
- To configure WMT transparent caching using WCCP Version 2, complete [Step 17](#).

Step 16 Configure WMT proxy caching, as follows:

- From the WMT caching submenu, choose the **WMT Proxy Caching** option.
- If there is a WMT license already installed on this Content Engine, enter **n** when the following prompt appears:

```

WMT license key is already installed. Do you want to install
a different license key (y/n) [n]:n

```

Otherwise, specify whether or not you have a license key for WMT when prompted. If you have your Cisco license key for the WMT product, then enter **y**. Otherwise, enter **n** to use the evaluation license for the WMT feature on this standalone Content Engine (as shown in this example).

```

Do you have the license key for WMT (y/n) [y]:n
Do you want to evaluate WMT (y/n) [y]:y

```



Note When you use the Setup utility to configure WMT proxy caching, the Content Engine automatically is configured to use the default port (port 1755) to listen for incoming WMT requests.

A list of the configured CLI commands appears, and you are asked if you want save this configuration. If you used the evaluation license to enable WMT on this Content Engine, the **wmt evaluate** command is included in the list of constructed CLI commands. If you used your Cisco WMT license, then the **wmt license-key** command is listed instead of the **wmt evaluate** command.

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

```

wmt evaluate
wmt accept-license-agreement
wmt enable

```

- c. When prompted, enter **y** to accept this configuration.

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

The specified settings are saved and the WMT Caching submenu reappears. The WMT Proxy Caching option is now listed as “Complete.” Remember that you still must configure Windows Media Player on the end user desktops to point directly to this Content Engine as their proxy server.



Tip

You can also use the Content Engine CLI to configure WMT streaming on this Content Engine at a later time, as described in [Chapter 9, “Configuring WMT Streaming Media Services on Standalone Content Engines.”](#)

Step 17 Configure WMT transparent caching as follows:

- a. From the WMT caching menu, choose the **WMT Transparent Caching** option.
- b. When prompted, specify the IP addresses of the WCCP Version 2-enabled routers that will redirect WMT requests to this Content Engine. Press **Enter** to use the default gateway, or enter the IP addresses of other WCCP Version 2-enabled routers that you want to redirect WMT requests to this Content Engine. In this case, the default gateway (the WCCP Version 2-enabled router that was specified as this Content Engine’s default gateway) has an IP address of 10.0.1.1.

```
Please enter the IP addresses of WCCP routers [10.0.1.1]:
```

- c. If there is a WMT license already installed on this Content Engine, enter **n** when the following prompt appears:

```
WMT license key is already installed. Do you want to install
a different license key (y/n) [n]:n
```

Otherwise, specify whether or not you have a license key for WMT when prompted. If you have your Cisco license key for the WMT product, then enter **y**. Otherwise, enter **n** to use the evaluation license for the WMT feature on this standalone Content Engine (as shown in this example).

```
Do you have the license key for WMT (y/n) [y]:n
Do you want to evaluate WMT (y/n) [y]:y
```

- d. When prompted, enter **y** to enable WMT transparent caching on this Content Engine.

```
Do you want to enable WMT transparent caching (y/n) [y]:y
```

A list of the configured CLI commands appears. If you used the evaluation license to enable WMT on this Content Engine, the **wmt evaluate** command is included in the list of configured CLI commands. If you used your Cisco WMT license, then the **wmt license-key** command is listed instead of the **wmt evaluate** command.

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

```
wmt evaluate
wmt accept-license-agreement
wmt enable
wccp router-list 1 10.0.1.1
wccp version 2
wccp wmt router-list 1
```

- e. When prompted, enter **y** to accept this configuration.

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

The specified settings are saved and the WMT Caching submenu appears. The WMT Transparent Caching option is now listed as “Complete.”

Step 18 Configure RealMedia caching, as follows:

- a. Use one of the following methods to display the RealMedia Caching submenu.
 - From the WMT Caching submenu, choose the **Previous Menu** option and then choose the WMT Caching option from the Caching Related Configurations submenu (shown below).
 - From the Caching Related Configurations submenu, choose the **Real Media Caching** option.
 - From the main menu, choose the **Caching Related Configurations** option and then choose the **Real Media Caching** option from the Caching Related Configurations submenu.

In the following example, both RealMedia caching services (RealMedia proxy caching and Real Media transparent caching using WCCP Version 2) are to be configured on this standalone Content Engine:

```

+-----+
|                                     |
|                               Real Media Caching                               |
|-----+-----+
| -> Caching           :Incomplete                                         |
|   Real Transparent Caching :Incomplete                                   |
|   Print Configuration                                                |
|   Previous Menu (p)                                                  |
|   Main Menu (m)                                                      |
|   Exit (e)                                                            |
+-----+-----+

Main Menu
  ---> Caching Related Configurations
        ---> Real Media Caching
Configure this CE for doing Real Proxy caching
Press '?' to see why this item is incomplete

```

- b. To configure RealMedia proxy caching, complete [Step 19](#).
- c. To configure RealMedia transparent caching using WCCP Version 2, complete [Step 20](#).

Step 19 Configure RealMedia proxy caching, as follows:

- a. From the RealMedia Caching submenu, choose the **Real Proxy Caching** option.
- b. If there a RealProxy license already installed on this Content Engine, enter **n** when the following prompt appears:

```
Real Proxy license key is already installed. Do you
want to install a different license key (y/n) [n]:n
```

Otherwise, specify whether or not you have a RealProxy license key. If you have your Cisco RealProxy license key, then enter **y**. Otherwise, enter **n** to use the RealProxy evaluation license for this standalone Content Engine (as shown in this example).

```
Do you have the license key for Real Proxy (y/n) [y]:n
Do you want to evaluate Real Proxy (y/n) [y]:y
```

A list of the configured CLI commands appears, and you are asked if you want save this configuration. If you used the evaluation license to enable the RTSP proxy for RealMedia requests, the **rtsp proxy media-real evaluate** command is included in the list of configured CLI commands.

```
Based on the input, the following CLIs will be configured:
rtsp proxy media-real accept-license-agreement
  rtsp proxy media-real enable
  rtsp proxy media-real evaluate
```

- c. When prompted, enter **y** to accept this configuration.

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



Note When you use the Setup utility to configure RealMedia proxy caching, the Content Engine automatically is configured to use the standard RTSP port (default port 554) to listen for incoming RealMedia requests. The RTSP gateway is the single point of entry for RTSP messages on the standalone Content Engine. The RTSP gateway runs on the Content Engine and is automatically enabled. By default, the RTSP gateway listens on port 554 for incoming RTSP requests. If you want to configure the RTSP gateway to listen for incoming RTSP requests on a port other than the default port (port 554), you must change the incoming RTSP port. You must use the Content Engine CLI (the **rtsp port incoming** *rtsp-gateway-incoming-port-number* global configuration command) to change the RTSP incoming port on a standalone Content Engine. For more information, see the [“Configuring Basic Settings for the RTSP Gateway”](#) section on page 8-16.

The specified settings are saved and the RealMedia Caching submenu reappears. The RealProxy Caching option is now listed as “Complete.” Remember that you still must configure the RealMedia players on the client desktops to point directly to this Content Engine as their proxy server, as described in the [“Pointing RealMedia Players Directly to a Standalone Content Engine”](#) section on page 4-46.



Tip You can also configure RealMedia streaming (VOD files and live splitting) on this Content Engine at a later time, as described in [Chapter 8, “Configuring RealMedia Services on Standalone Content Engines.”](#)

Step 20 Configure RealMedia transparent caching using WCCP as follows:

- From the RealMedia Caching submenu, choose the **Real Transparent Caching** option.
- When prompted, specify the IP addresses of the WCCP Version 2-enabled routers that will redirect RealMedia requests to this Content Engine. Press **Enter** to use the default gateway, or enter the IP addresses of other WCCP Version 2-enabled routers that you want to redirect RealMedia requests to this Content Engine. In this case, the default gateway has an IP address of 10.0.1.1 (the WCCP Version 2-enabled router that was specified as this Content Engine’s default gateway).

```
Please enter the IP addresses of WCCP routers [10.0.1.1]:
```

- If there is a RealProxy license already installed on this Content Engine, enter **n** when the following prompt appears:

```
Real Proxy license key is already installed. Do you  
want to install a different license key (y/n) [n]:n
```

Otherwise, specify whether or not you have a RealProxy license key. If you have your Cisco RealProxy license key, then enter **y**. Otherwise, enter **n** to use the RealProxy evaluation license for this standalone Content Engine (as shown here in this example).

```
Do you have the license key for Real Proxy (y/n) [y]:n  
Do you want to evaluate Real Proxy (y/n) [y]:y
```

- d. Enter **y** to enable RealMedia transparent caching on this Content Engine.

Do you want to enable Real Media transparent caching (y/n) [y]:**y**

A list of the configured CLI commands appears along with a reminder that you still must configure the rtsp service (service 80) on the WCCP Version 2-enabled router. If you used the evaluation license to enable the RTSP proxy for RealMedia requests, the **rtsp proxy media-real evaluate** command is included in the list of configured CLI commands.

NOTE: Please remember to configure service 80 on the router.

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

```
rtsp proxy media-real accept-license-agreement
rtsp proxy media-real enable
wccp router-list 1 10.0.1.1
wccp version 2
wccp rtsp router-list 1
```

- e. When prompted, enter **y** to accept this configuration.

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

The specified settings are saved and the RealMedia Caching submenu reappears. The Real Transparent Caching option is now listed as “Complete.” Remember that you still must configure the rtsp service (service 80) on the WCCP Version 2-enabled router, as described in the [“Configuring the RTSP Service \(Service 80\) on a Router”](#) section on page 6-30.



Note

If the Content Engine is behind a network address translation (NAT)-enabled router, you must also specify the IP address of the RTSP gateway. After you have used the Setup utility to complete the basic configuration of a Content Engine, you can exit the Setup utility and then use the Content Engine CLI to specify the IP address of the RTSP gateway. To specify the IP address of the RTSP gateway, use the **rtsp ip-address** *rtsp-gateway-ip-address* global configuration command, as described in the [“Configuring Basic Settings for the RTSP Gateway”](#) section on page 8-16.

Configuring Client Browsers and Media Players for Direct Proxy Routing

Remember that after you configure the standalone Content Engine for nontransparent (proxy) caching, you must configure the client browsers and media players to route their content requests directly to this Content Engine (direct proxy routing). For information about how to point client browsers or media players to a standalone Content Engine that is functioning as a nontransparent proxy server for these clients, see [Table 4-5](#).

Table 4-5 *Configuring Client Browsers and Media Players to Support Direct Proxy Routing of Content Requests*

Nontransparent Caching	Additional Information and Instructions
HTTP proxy caching	See the “Pointing Client Browsers Directly to a Standalone Content Engine” section on page 4-36.
HTTPS proxy caching	See the “Pointing Client Browsers Directly to a Standalone Content Engine” section on page 4-36.
WMT proxy caching	See the “Pointing Windows Media 9 Players Directly to a Standalone Content Engine for WMT RTSP Requests” section on page 4-43.
RealMedia proxy caching	See the “Pointing RealMedia Players Directly to a Standalone Content Engine” section on page 4-46.

Pointing Client Browsers Directly to a Standalone Content Engine

If nontransparent caching is to be used to direct content requests to a standalone Content Engine that is functioning as a nontransparent proxy server, you must configure the client browsers to point directly to this Content Engine. To point a client browser to a Content Engine you can use proxy autoconfiguration (PAC) files, or you can manually configure the browser to point to a specific standalone Content Engine.

For more information on these two different methods, see the following sections:

- [Using PAC Files to Point Client Browsers Directly to a Standalone Content Engine, page 4-37](#)
- [Manually Pointing Client Browsers to a Standalone Content Engine, page 4-42](#)

Using PAC Files to Point Client Browsers Directly to a Standalone Content Engine

The ACNS 5.x software provides support for PAC files to point client browsers directly to a standalone Content Engine (nontransparent forward proxy server for these client browsers). A PAC file is a configuration file that is written in JavaScript and stored on an FTP server in your intranet. To use PAC files to point client browsers directly to a standalone Content Engine, follow these steps:

-
- Step 1** Create the PAC file on an FTP server.
- Step 2** Download the PAC file from the FTP server to the Content Engine that will act as the proxy server for the client browsers.

Each time you download a new PAC file to a standalone Content Engine, follow these steps:

- a. Disable proxy autoconfiguration on the Content Engine (**no proxy-auto-config enable** command).
- b. Download the new PAC file to the Content Engine.



Note You must configure disks /local1 or /local2 as a sysfs volume on the Content Engine before downloading the autoconfiguration file to either of these two disk locations.

- c. Enter the **proxy-auto-config enable** command to reenable the automatic proxy configuration feature on the Content Engine.

Manually configure the browser for automatic proxy configuration by explicitly specifying the Content Engine's IP address, incoming port number, file directory, and the name of the PAC file in the browser.



Note Microsoft Internet Explorer and Netscape browsers support the use of PAC files.

- Step 3** If a browser is configured for automatic proxy configuration, then when the browser starts up, it will obtain the necessary proxy information (for example, the proxy server's IP address and port configuration information) from the PAC file (.pac file).

The following is an example of how to use a PAC file to point client browsers to the Content Engine:

- Step 1** Create a PAC file on an FTP server.

The following is an example of a very simple PAC file named proxyfile.pac. In this case, there is only one proxy (one standalone Content Engine) and traffic that is not destined for "cisco.com" is sent to the proxy server (Content Engine) for all Internet requests.

```
Example #1: Use proxy for everything except local hosts
This would work in Netscape's environment. All hosts which aren't fully
qualified, or the ones that are in local domain, will be connected to
directly. Everything else will go through w3proxy:8080. If the proxy goes
down, connections become automatically direct.
```

```
function FindProxyForURL(url, host)
{
    if (isPlainHostName(host) ||
        dnsDomainIs(host, ".cisco.com"))
        return "DIRECT";
    else
        return "PROXY ce1.cisco.com:8080; DIRECT";
```

}Note: This is the simplest and most efficient autoconfig file for cases where there's only one proxy.

- Step 2** Download the PAC file from the specified FTP server to the Content Engine. By default, the PAC file is downloaded to the present working directory of the Content Engine.

This example shows how to download a PAC file named the proxyfile.pac from an FTP server that has an IP address of 172.16.10.10 to the Content Engine. The Content Engine is functioning as a PAC file server because the client browsers will be pointed to this PAC file when the browsers are started up.

```
ContentEngine# proxy-auto-config download 172.16.10.10 remotedirname proxyfile.pac
```

- Step 3** Enable the browser autoconfiguration feature on this standalone Content Engine.

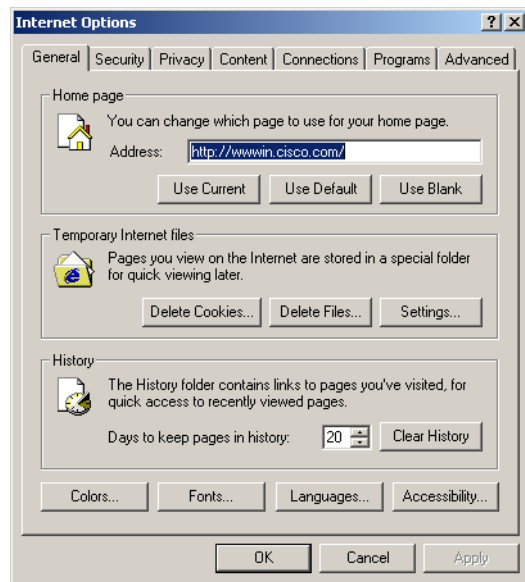
```
ContentEngine(config)# proxy-auto-config enable
```

- Step 4** Manually configure each client browser for automatic proxy configuration. If a browser is configured for automatic proxy configuration, the browser will obtain the necessary information from the specified .pac file on the Content Engine each time the browser starts up. You must explicitly specify the Content Engine's IP address, incoming port number, file directory, and name of the .pac file in the browser.

The following steps show how to perform this task from Internet Explorer Version 6.0:

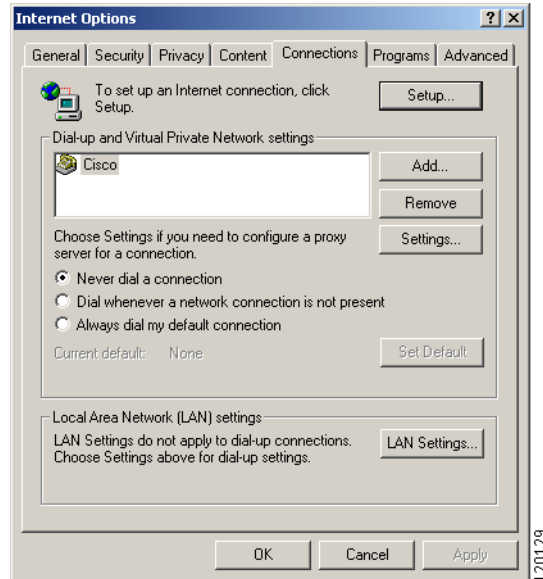
- a. From the Internet Explorer GUI, choose **Tools > Internet Options**. The Internet Options window appears. (See [Figure 4-5](#).)

Figure 4-5 Internet Options Window



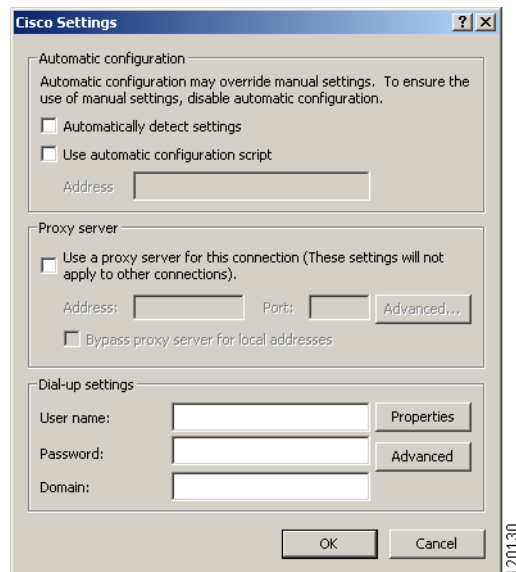
- b. At the top of the Internet Options window, click the **Connections** tab to bring this tab to the front. (See [Figure 4-6](#).)

Figure 4-6 Connections Tab Window



- c. On the Connections tab, click the **Settings** button. The Settings window appears. (See Figure 4-7.)

Figure 4-7 Settings Window



- d. Check the **Use automatic configuration script** check box.
- e. In the Address field, enter the URL of the .pac file that this browser should use to determine which proxy server (the Content Engine) it should direct its content requests to.

http://ContentEngine-IPaddress:portnumber/pac filename

In the following example, the URL of the .pac file specifies that the .pac file is named proxyfile.pac, and is stored on a Content Engine (nontransparent forward proxy server) that has an IP address of 172.16.10.10 and 8080 as an incoming port of 8080.

```
http://172.16.10.10:8080/proxyfile.pac
```



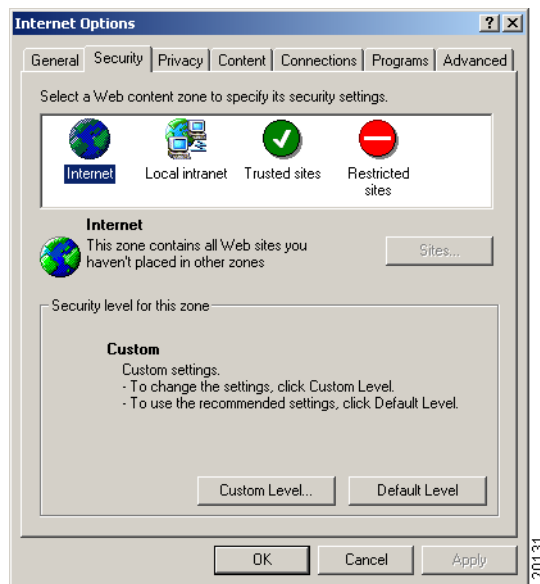
Note When specifying the port number in the URL of the .pac file, use the same port number that was specified as the proxy's incoming port number (through the **http proxy incoming portnumber** global configuration command, or the Setup utility as described in [Step 12 of "Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine"](#)). For instance, if port 8080 is specified with the **http proxy incoming 8080** command, then use 8080 as your port number in the URL of the .pac file.

- f. Click **OK** to save the settings and close the Settings window.

Step 5 If NTLM is used in this environment to control user Internet access, you must change the default setting for user authentication in the client browser to prevent the user from being prompted by a popup window to log in every time the user attempts to access a new website. The following steps show how to change this default setting in Internet Explorer Version 6.0:

- a. In the Internet Options window ([Figure 4-5](#)), click the **Security** tab. The Security tab appears with the Internet selected as the web content zone. (See [Figure 4-8](#)).

Figure 4-8 Security Tab



- b. Click the **Custom Level** button. The Security Settings window appears.
- c. In the Security Settings window, scroll down to the User Authentication section of the window. (See [Figure 4-9](#).)

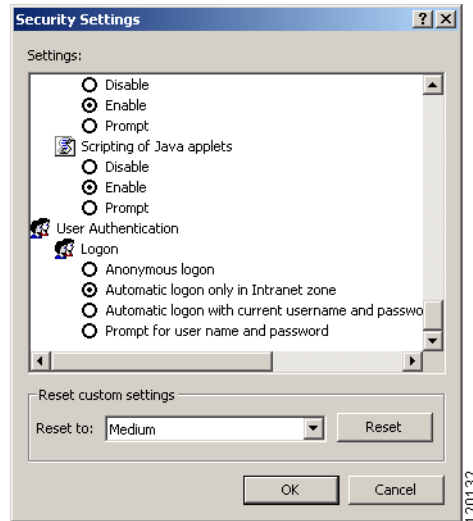
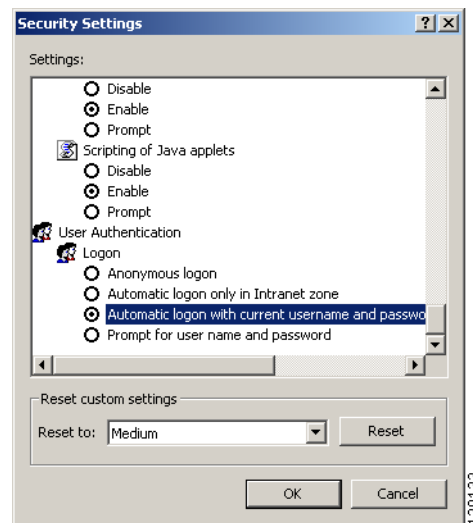
Figure 4-9 Security Settings Window

Figure 4-9 shows that the default user authentication setting is for automatic logon for an intranet zone only.

- d. Change the default user authentication setting by clicking the **Automatic logon with current username and password** radio button. (See Figure 4-10).

Figure 4-10 Changing the Default User Authentication Setting

- e. Click **OK** to close the Security Settings window.

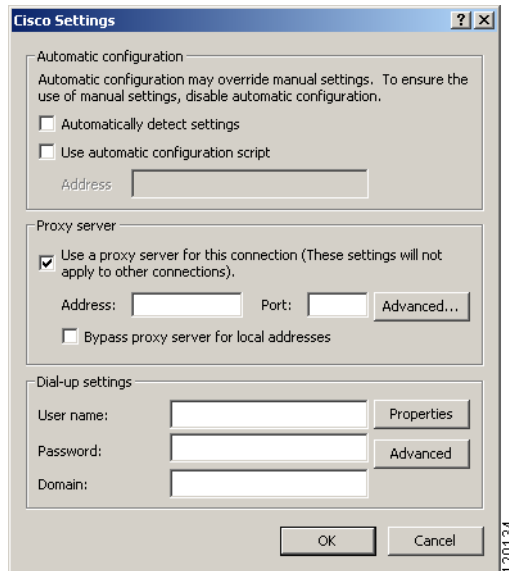
Manually Pointing Client Browsers to a Standalone Content Engine

To manually point a client browser to a standalone Content Engine instead of using proxy autoconfiguration (PAC) files, you must explicitly specify the IP address and port number of the Content Engine (nontransparent proxy server for this client browser) in the browser.

The following example describes how to perform this task from Internet Explorer, Version 6.0:

-
- Step 1** From the Internet Explorer GUI, choose **Tools > Internet Options**. The Internet Options window appears. (See [Figure 4-5](#).)
 - Step 2** At the top of the Internet Options window, click the Connections tab to bring it to the front. (See [Figure 4-6](#).)
 - Step 3** On the Connections tab, click the **Settings** button. The Settings window appears. (See [Figure 4-7](#).)
 - Step 4** In the Settings window, check the **Use a proxy server for this connection** check box to manually point the browser directly to a Content Engine. (See [Figure 4-11](#).)

Figure 4-11 Manually Pointing a Browser Directly to a Content Engine



- Step 5** In the Address field, enter the IP address of the Content Engine that you want this browser to point to. Specify the IP address of the Content Engine that this client browser will directly send its content requests. For example, to specify the Content Engine that has an IP address of 172.16.10.10 as the direct proxy server, enter **172.16.10.10** into the Address field.

- Step 6** In the Port field, enter the port number of the standalone Content Engine that will be the proxy server for this browser.



Note Use one of the port numbers that you specified as an incoming proxy port when you configured HTTP proxy caching on the standalone Content Engine (through the Setup utility as described in [Step 12](#) of “Using the Setup Utility to Configure a Basic Configuration on a Standalone Content Engine,” or by entering the **http proxy incoming portnumber** global configuration command). For instance, if port 8080 is specified as the incoming proxy port (**http proxy incoming 8080** command), then enter 8080 as your port number in the Port field.

- Step 7** Click **OK**.
- Step 8** If NTLM is used in this environment to control user Internet access, you must change the default setting for user authentication in the client browser to prevent the user from being prompted by a popup window to log in every time the user attempts to access a new website.

For an example of how to change this default setting in Internet Explorer Version 6.0, see [Step 5](#) on [page 4-40](#).

Pointing Windows Media 9 Players Directly to a Standalone Content Engine for WMT RTSP Requests

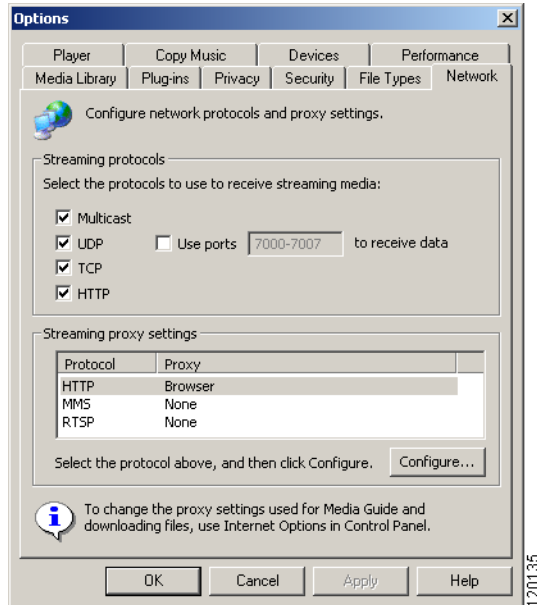
If direct proxy routing is being used instead of WMT transparent redirection to direct Windows Media 9 players requests to send their WMT RTSP requests directly to a standalone Content Engine, you must configure Windows Media 9 players on client desktops to point directly to the Content Engine (a nontransparent WMT proxy server for these web clients).

The Content Engine must be running the ACNS 5.3.1 software and later releases to support direct proxy routing of WMT RTSP requests from Windows Media 9 players.

To explicitly configure Windows Media 9 players on client desktops to point directly to a specific standalone Content Engine, follow these steps:

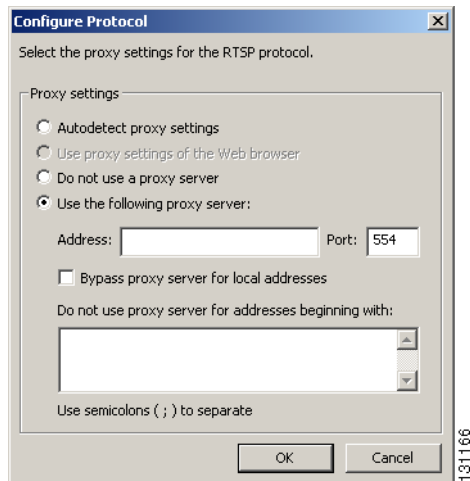
-
- Step 1** Open Windows Media player on the client desktops.
- Step 2** In the Windows Media player menu bar, choose **Tools > Options**. The Options window appears.
- Step 3** In the Options window, click the Network tab. (See [Figure 4-12](#).)

Figure 4-12 Network Options Tab



- Step 4** On the Network tab under Streaming protocols, click the **Multicast**, **UDP**, **TCP** and **HTTP** check boxes if they are not already selected.
- Step 5** On the Network tab, under Streaming proxy settings, choose **RTSP** and click **Configure**. The Configure Protocol window appears. (See Figure 4-13.)

Figure 4-13 Configuring RTSP as a Streaming Protocol



- Step 6** Click the **Use the following proxy server** radio button.
- Step 7** In the Address field, enter the IP address of the Content Engine (the nontransparent WMT proxy server for RTSP requests from this Windows Media 9 player).

- Step 8** In the Port field, enter the port number on which the Content Engine will accept incoming WMT RTSP requests from this Windows Media 9 player. Port 554 is the default port for RTSP incoming requests.
- By default, the Content Engine listens on port 554 for incoming RTSP requests. If you have changed this default port setting on the Content Engine (that is, you have used the **rtsp port incoming port-number** global configuration command to configure the Content Engine to listen for incoming RTSP requests on a port other than port 554), make sure that you enter that port number into the Port field of the Configure Protocol window.
- Step 9** Click **OK** to close the Configuration Protocol window.
- Step 10** Click **Apply** to apply the settings to the Windows Media 9 player.
- Step 11** Click **OK** to close the Options window in the Windows Media 9 player.
-

Pointing Windows Media Players Directly to a Standalone Content Engine for WMT MMS Requests



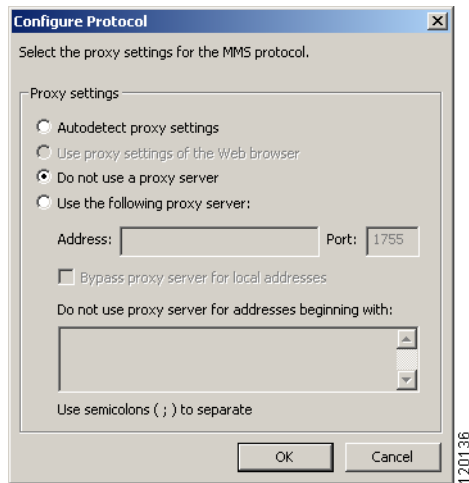
Note

In ACNS 5.5 software release, MMS requests are transparently redirected to the HTTP or RTSP protocol, and the request is served over RTSP or HTTP in the same order.

If direct proxy routing is being used to direct WMT MMS requests from Windows Media players directly to a standalone Content Engine, you must configure Windows Media player on client desktops to point directly to the Content Engine (a nontransparent WMT proxy server for these web clients).

To explicitly configure Windows Media players on client desktops to send their WMT MMS requests directly to a specific standalone Content Engine, follow these steps:

- Step 1** Open Windows Media player on the client desktops.
- Step 2** In the Windows Media player menu bar, choose **Tools > Options**. The Options window appears.
- Step 3** In the Options window, click the Network tab. (See [Figure 4-12](#).)
- Step 4** On the Network tab under Streaming protocols, click the **Multicast**, **UDP**, **TCP** and **HTTP** check boxes if they are not already selected.
- Step 5** On the Network tab, under Streaming proxy settings, choose **MMS**, and click **Configure**. The Configure Protocol window appears. (See [Figure 4-14](#).)

Figure 4-14 Configure Protocol Window

- Step 6** Click the **Use the following proxy server** radio button.
- Step 7** In the Address field, enter the IP address of the Content Engine (the nontransparent WMT proxy server for this Windows Media player).
- Step 8** In the Port field, enter the port number on which the Content Engine will accept incoming WMT MMS requests from this Windows Media player.
- By default, the Content Engine listens on port 1755 for incoming MMS requests from WMT clients. When you use the Setup utility to configure WMT proxy caching, the Content Engine automatically is configured to use the default port (port 1755) to accept incoming MMS requests. If you have changed this default port setting on the Content Engine (that is, you have used the **wmt incoming port-number** global configuration command to configure the Content Engine to listen for incoming MMS requests on a port other than port 1755), make sure that you enter that port number into the Port field of the Configure Protocol window.
- Step 9** Click **OK** to close the Configuration Protocol window.
- Step 10** Click **Apply** to apply the settings to the Windows Media player.
- Step 11** Click **OK** to close the Options window in the Windows Media player.

Pointing RealMedia Players Directly to a Standalone Content Engine

If direct proxy routing is being used instead of RTSP transparent redirection to direct RTSP requests from RealMedia players directly to a standalone Content Engine, you must configure the RealMedia players (RealPlayer or RealOne player) on client desktops to point directly to this Content Engine (a nontransparent RealProxy server for these web clients).

To explicitly configure the RealMedia player (RealPlayer Version 8.02 or 9.0) on the client desktops to point directly to a specific standalone Content Engine as their RTSP proxy server, follow these steps:

- Step 1** Open RealPlayer on the client desktop.
- Step 2** From the RealPlayer menu, choose **View > Preferences**.
- Step 3** Click the **Proxy** option under Category settings.

- Step 4** Click **Change Settings** under Streaming Settings.
- Step 5** Click the **Use proxies** radio button.
- Step 6** In the RTSP Proxy address field, enter the IP address of the standalone Content Engine that you have configured for RealMedia proxy caching.
- Step 7** In the Port field, enter the port number on which the Content Engine will accept RTSP incoming requests.
- By default, the Content Engine listens on port 554 for incoming RTSP requests. If you have changed this default port setting on the Content Engine (that is, you have used the **rtsp port incoming port-number** global configuration command to configure the Content Engine to listen for incoming RTSP requests on a port other than port 554), make sure that you enter that port number into the Port field of the Configure Protocol window.
- Step 8** Click **OK**.

Configuring WCCP Routers for Transparent Redirection

Remember that after you configure a standalone Content Engine for transparent proxy caching, you must configure the WCCP Version 2-enabled routers to intercept and redirect content requests transparently to this Content Engine. For information about how to configure the necessary WCCP service on a WCCP Version 2-enabled router, see [Table 4-6](#).

Table 4-6 *Configuring WCCP Routers to Support Transparent Proxy Routing of Content Requests*

Transparent Caching Using WCCP	Additional Information and Instructions
HTTP transparent caching	Configuring the Standard Web-Cache Service (Service 0) on a Router Configuring the Custom-Web-Cache Service (Service 98) on a Router
HTTP reverse proxy caching	Configuring the Reverse-Proxy Service (Service 99) on a Router
WMT transparent caching with WMT RTSP transparent redirection	Configuring the RTSP Service (Service 80) on a Router Configuring the WMT-RTSPU Service (Service 83) on a Router
RealMedia transparent caching	Configuring the RTSP Service (Service 80) on a Router

Verifying the Basic Configuration

This section provides an example of how to verify the basic configuration on a standalone Content Engine. This is an example of how to verify the configuration of the web-cache service (HTTP transparent caching through WCCP) on a standalone Content Engine. In this example, the following assumption applies:

- There is a single standalone Content Engine (Content Engine A) that has WCCP Version 2 enabled on it.
- There is a single WCCP Version 2-enabled router (Router A) that has been configured to redirect HTTP requests to Content Engine A (transparent proxy server).
- The HTTP transparent caching service has been enabled on Content Engine A, and Content Engine A is configured to accept redirected HTTP requests from Router A.

- The Client A and Client B browsers are not configured to point directly to Content Engine A.
- Client A and Client B are on the same subnet.

To verify that the web-cache service (HTTP transparent caching through WCCP) is working properly, follow these steps:

Step 1 From Client A, use the client browser to open various web pages on the Internet or your intranet. Request the pages more than once. The web servers you connect to must be on a different subnet than Client A, so that the HTTP requests that the Client A browser issues are routed to Router A.

Step 2 Use a login account that has administrator privileges (privilege level of 15) to log in to the Content Engine CLI on Content Engine A.

For more information about how to log in to a standalone Content Engine through the Content Engine CLI, see the [“Using Telnet or a Console Session to Log in to a Standalone Content Engine”](#) section on page 4-50.

Step 3 From Content Engine A, display the HTTP caching saving statistics for this Content Engine.

```
ContentEngineA# show statistics http savings
```

	Statistics - Savings	
	Requests	Bytes
Total:	525980242	79047534484
Hits:	1966223	19865155481
Miss:	524014019	59182379003
Savings:	0.4 %	25.1 %



Tip You can also display these statistics by choosing **Reporting > Savings** from the Content Engine GUI. For information about how to log in to the Content Engine GUI, see the [“Logging in to the Content Engine GUI”](#) section on page 4-55.

Step 4 From Content Engine A, display the number of HTTP requests that this Content Engine has received.

```
ContentEngineA# show statistics http requests
```

Step 5 From Client B, use the browser to request the same web pages that you just requested from Client A.

This step allows you to check whether Content Engine A is storing a copy of the requested web pages in its local cache instead of retrieving the web pages again from the origin web servers.

- The number of cache hits displayed in the output of the **show statistics http savings** command should increase as you use the Client B browser to request the same web pages that you just requested from Client A.
- The number of HTTP requests displayed in the output of the **show statistics http requests** command should increase as you use the Client B browser to request the same web pages that you just requested from Client A.

Step 6 On Router A, open a console or Telnet session.

Step 7 On Router A, display statistics and status information for Router A.

```
RouterA# show ip wccp
```

The statistics should show a number greater than 0 for packets redirected. Also, check for hash assignments, which indicate at the very least that Content Engine A is registered and communicating with Router A.

Step 8 Check to see if Router A shows that packets are being redirected to Content Engine A.

- If Router A shows that there are packets being redirected to Content Engine A, the service (transparent redirection of HTTP requests) is operating properly on Content Engine A and Router A.
- If Router A shows that no packets are being redirected to Content Engine A, the web cache service is not operating properly. In this case, you should troubleshoot the problems with your configuration of the web cache service. The following are some examples of how to do this.

- From Content Engine A, display the list of WCCP services that are currently configured on Content Engine A. See if the standard web-cache service (Web Cache) is listed. Partial sample output is shown here in this display example:

```
ContentEngineA# show wccp services
Services configured on this Content Engine
  Web Cache
  RTSP
  FTP
ContentEngine#
```

- From Content Engine A, display a list of WCCP-enabled routers that recognize Content Engine A. Partial sample output is shown here in this display example:

```
ContentEngineA# show wccp routers
Routers Seeing this Content Engine
  Router Id      Sent To
  10.0.0.0       10.1.1.1
Routers not Seeing this Cache Engine
  10.1.1.1
Routers Notified of but not Configured
  -NONE-
```

Check the command output to determine if Router A is on the list of WCCP-enabled routers that recognize Content Engine A.

- From Content Engine A, display WCCP generic routing encapsulation (GRE) packet-related information for Content Engine A.

```
ContentEngineA# show wccp gre
```

Check the command output to view the number of redirected packets that Content Engine A has rejected and accepted. See if the number of accepted packets is increasing as you continue to request web pages that are on web servers located on different subnets than the requesting client (Client A and Client B).



Note

For information about how to use the ACNS software logs, see [Chapter 21, “Monitoring Standalone Content Engines and Transactions.”](#)

Modifying the Basic Configuration Through the Setup Utility

If you have previously run the Setup utility on a Content Engine, then when you subsequently launch the Setup utility manually (using **setup** privileged EXEC command), the current basic configuration for the standalone Content Engine appears. You can quickly change the current basic configuration through the Setup utility by entering **y** when prompted, as shown here in this display example:

```
Here is the current profile of this device
CDN device
No
HTTP Proxy Caching           : Yes
HTTP Tranparent Caching      : Yes
HTTP Reverse Proxy Caching   : Yes
WMT Proxy Caching            : Yes
WMT Transparent Caching      : Yes
Real Media Proxy Caching     : Yes
Real Media Transparent Caching: Yes
Do you want to change this (y/n) [n]:y
```

Logging in to Standalone Content Engines

This section provides an overview of how to use any of the following methods to log in to a standalone Content Engine:

- [Using Telnet or a Console Session to Log in to a Standalone Content Engine, page 4-50](#)
- [Using Secure Shell Version 1 or Version 2 to Log in to a Standalone Content Engine, page 4-52](#)
- [Using the Content Engine GUI to Log in to a Standalone Content Engine, page 4-53](#)

The ACNS software comes with a single predefined login account (root administrator) that can be used to access the Content Engine initially, and then to add other users to the system. This login account has superuser privilege rights (privilege level of 15). The username for this predefined login account is **admin** and the default password is **default**. If these defaults have been changed by another ACNS system administrator, you must obtain the new username and password.

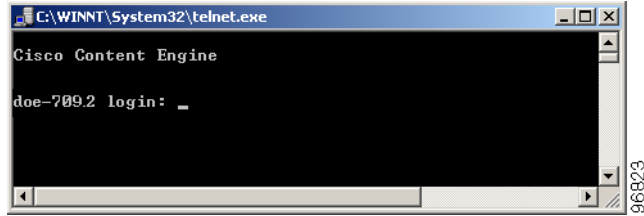
Using Telnet or a Console Session to Log in to a Standalone Content Engine

To log in to a standalone Content Engine using Telnet or a console session, follow these steps:

Step 1 Log in to the Content Engine using Telnet or a console connected to the Content Engine serial port. For example, after starting a Telnet session, use the **open** command to specify the Content Engine that you want to log in to:

```
Microsoft Telnet> open IP_address_of_Content_Engine
```

Step 2 When prompted for a login, enter a username and password. (See [Figure 4-15](#).)

Figure 4-15 Example of the Telnet Session Login Window

Step 3 After you have successfully logged in, the Content Engine CLI displays one of the following prompts depending on the privilege level of the login account:

- Privileged EXEC mode (privilege level of 15):

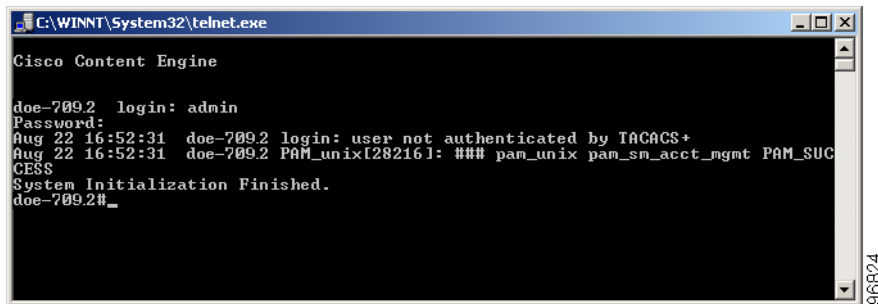
```
ContentEngine#
```

- User EXEC mode (privilege level of 0):

```
ContentEngine>
```

where ContentEngine is the host name of the Content Engine.

Figure 4-16 shows an example of the system prompt for privileged EXEC mode.

Figure 4-16 CLI System Prompt for Privileged EXEC Mode**Tip**

A Telnet session with the Content Engine can remain open and inactive for the interval of time specified by the **exec-timeout** global configuration command. The default timeout is 15 minutes; valid values are 0–44640 minutes. When the **exec-timeout** interval elapses, the Content Engine automatically closes the Telnet session.

Step 4 Use the Content Engine CLI commands to launch the Setup utility (enter the **setup** privileged EXEC command) or to use CLI commands to configure or monitor this standalone Content Engine.

See the “[ACNS Software CLI Command Modes for Standalone Content Engines](#)” section on page B-8 for a description of the different command modes you can work in when using the ACNS software CLI to configure or monitor a standalone Content Engine. See the “[ACNS Software CLI Online Help and Keyboard Shortcuts](#)” section on page B-10 for information about using online help and keyboard shortcuts.



Note The ACNS software device mode determines whether the device is functioning as a Content Engine, Content Distribution Manager, Content Router, or IP/TV Program Manager. The commands available from a specific CLI mode are determined by the ACNS software device mode in effect. The default device operation mode is Content Engine.

Step 5 Enter the **logout** or **exit** EXEC commands to end the CLI session at any time.

A Telnet session with the Content Engine can remain open and inactive for the interval of time specified by the **exec-timeout** global configuration command. The default timeout is 15 minutes; valid values are 0–44, or 640 minutes. When the **exec-timeout** interval elapses, the Content Engine automatically closes the Telnet session.

Using Secure Shell Version 1 or Version 2 to Log in to a Standalone Content Engine

Secure Shell (SSH) enables login access to the Content Engine through a secure and encrypted channel. SSH consists of a server and a client program. Like Telnet, you can use the client program to remotely log on to a machine that is running the SSH server, but unlike Telnet, messages transported between the client and the server are encrypted. The functionality of SSH includes user authentication, message encryption, and message authentication.

Before you enable the **sshd** command, use the **ssh-key-generate** global configuration command to generate a private and a public host key, which the client programs use to verify the server's identity.

When a user runs an SSH client and logs in to the Content Engine, the public key for the SSH daemon running on the Content Engine is recorded in the client machine `known_hosts` file in the user's home directory. If the Content Engine administrator subsequently regenerates the host key by issuing the **ssh-key-generate** command, the user must delete the old public key entry associated with the Content Engine in the `known_hosts` file before running the SSH client program to log in to the Content Engine. When the user runs the SSH client program after deleting the old entry, the `known_hosts` file is updated with the new SSH public key for the Content Engine.



Note The Telnet daemon can still be used with the Content Engine. SSH does not replace Telnet.

This example shows how to generate an SSH public key and then enables the SSH service:

```
Console(config)# ssh-key-generate
Ssh host key generated successfully
Saving the host key to box...
Host key saved successfully
```

```
Console(config)# sshd enable
Starting ssh daemon ..
Ssh daemon started successfully
```

Secure File Transfer Protocol Access for Nonadministrative Users

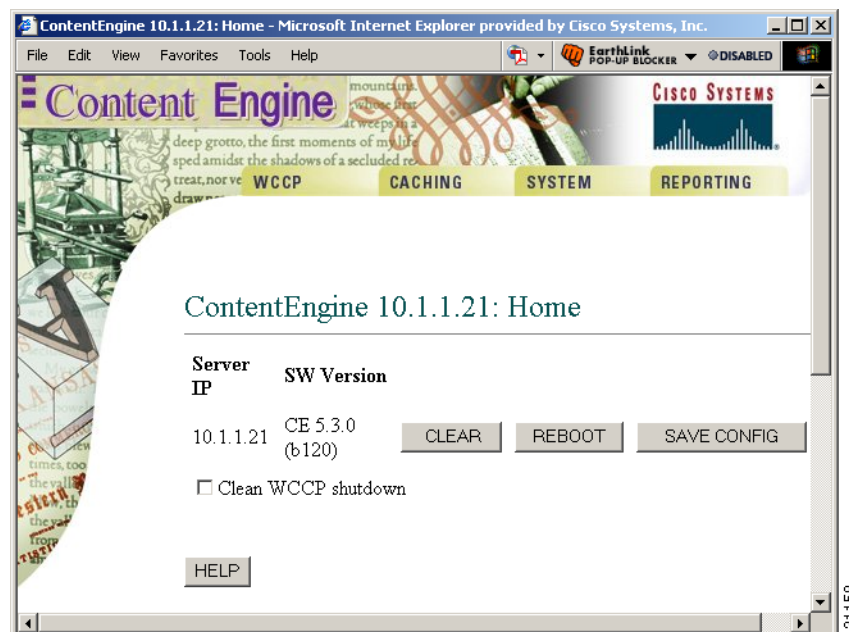
In the ACNS 5.3.5 software release, the Secure File Transfer Protocol (SFTP) server on the Content Engine was enhanced to allow nonadministrative users (that is, a user with a nonzero UID) to use SFTP to access the Content Engine. In the ACNS 5.3.5 software release, the **sshd allow-non-admin-users** and **no sshd allow-non-admin-users** CLI global configuration commands were added to enable and disable this new feature. By default, this feature is disabled on the Content Engine, and nonadministrative users cannot use SFTP to access the Content Engine. To enable this feature, enter the **sshd allow-non-admin-users** command on the Content Engine. After enabling this feature, you can disable it again by entering the **no sshd allow-non-admin-users** command on the Content Engine.

If this feature is enabled, the output of the **show running-config EXEC** command shows that this feature is enabled on the Content Engine.

Using the Content Engine GUI to Log in to a Standalone Content Engine

The Content Engine GUI (Figure 4-17) is the web portal for configuring a standalone Content Engine as a caching and streaming engine.

Figure 4-17 Content Engine GUI



Note

The Content Engine GUI provides access to all of the administrative and operator functions that are accessible to the specific user logged in to the GUI.

After the ACNS software is installed on the Content Engine, use a standard web browser to log in and access the Content Engine GUI.

Before logging in to the Content Engine GUI, check that you have the following information:

- Name or IP address of the Content Engine that you want to log in to.
- Login account (username and password) that you want to log in to the Content Engine for configuration, monitoring, or troubleshooting purposes. If you do not have a login account, your ACNS system administrator must create one for you.
- Type of access enabled on the Content Engine GUI (secure or nonsecure).



Note For more information about enabling secure or nonsecure access to the Content Engine GUI, see the [“Enabling or Disabling Access to the Content Engine GUI”](#) section on page 4-54.

Enabling or Disabling Access to the Content Engine GUI

You can configure secure or nonsecure access to the Content Engine GUI. Secure access is the default. Either secure or nonsecure access to the Content Engine GUI is possible but not both. For example, if the secured Content Engine GUI is enabled (for example, https:// access on port 8003), then nonsecure access to the Content Engine GUI (for example, http:// access on port 8001) is not allowed.

- To enable or specify the port number of the Content Engine GUI server, use the **gui-server** global configuration command.

```
ContentEngine(config)# gui-server {enable | port port |
secure {enable | port port}}
```

- To enable secure access to the Content Engine GUI, use the **gui-server secure enable port** global configuration command.

```
ContentEngine(config)# gui-server secure enable port 8003
```

The port number can be between 1 and 65535. The default port for secure access to the GUI is 8003. In this example, secure access to the Content Engine GUI is enabled on the default port number 8003.

- To enable nonsecure access to the Content Engine GUI, use the **gui-server enable port** global configuration command.

```
ContentEngine(config)# gui-server enable port 8001
```

The port number can be between 1 and 65535. The default port for nonsecure access to the GUI is 8001. In this example, nonsecure access to the Content Engine GUI is enabled on the default port number 8001.



Note When secure or nonsecure access to the Content Engine GUI is enabled, you can access the GUI as described in the [“Logging in to the Content Engine GUI”](#) section on page 4-55.

To disable the Content Engine GUI, use the **no gui-server** global configuration command:

```
no gui-server {enable | port | secure {enable | port port}}
```

For example, if secure access to the Content Engine GUI is enabled on port 8003, enter the following command to disable it:

```
ContentEngine(config)# no gui-server secure enable port 8003
```

In the following example, nonsecure access to the Content Engine on port 8001 is being disabled:

```
ContentEngine(config)# no gui-server enable port 8001
```

Logging in to the Content Engine GUI

To log in to the Content Engine GUI, follow these steps:

- Step 1** Start a web browser on a device that has access to the network on which the Content Engine resides.



Tip If you are using Microsoft Internet Explorer (IE), verify that Java, JavaScript, and Cascading Style Sheets are enabled on IE. If you are using Netscape, use Version 4.0 or later.

- Step 2** In the web browser, enter the URL or IP address of the Content Engine. Append the port number. The URL (location) of the Content Engine is determined during the installation of the ACNS software. If your network supports DNS and the IP address of the Content Engine has been added to your DNS table, you can access the Content Engine GUI by using the DNS name of the Content Engine.

The port number of the Content Engine GUI is determined when the ACNS software is installed on the Content Engine. The default port number for nonsecure access is 8001. The default port number for secure access is 8003. Secure access to the Content Engine GUI is enabled on the default port number 8003. HTTP is used for nonsecure access and HTTPS is used for secure access.

The following example shows the URL for accessing the Content Engine GUI in nonsecure mode if nonsecure mode is enabled on the default port (port 8001):

```
http://ContentEngine-name:8001
```

Alternatively, enter the IP address:

```
http://ContentEngine-IP-address:8001
```

The following example shows the URL for accessing the Content Engine GUI in secure mode if secure mode is enabled on the default port (port 8003):

```
https://ContentEngine-name:8003
```

Alternatively, enter the IP address:

```
https://ContentEngine-IP-address:8003
```

- Step 3** If you specified secure access, then the Security Alert window appears. Click **Yes** to accept the security certificate. The Enter Network Password window appears.

- Step 4** Enter your username in the Username field. Enter your password in the Password field and click **OK**.

```
Username: admin  
Password: password
```

- Step 5** After the system verifies the specified login information, the main window for the Content Engine GUI appears in your browser. If you are the default administrator, you should create login accounts for your ACNS system administrators or other ACNS administrative who need to access the Content Engine for configuration, monitoring, or troubleshooting purposes.

When you access the Content Engine GUI, it appears with a window (page) that is referred to as the Content Engine main window. (See [Figure 4-17](#).) The Content Engine GUI has a set of tabs and buttons. For a descriptive list of menu options, see [Appendix A, “Content Engine GUI Menu Options.”](#)



The lock icon in the lower-right corner of the browser window indicates that the Content Engine GUI has been accessed in secure mode instead of nonsecure mode. For information about enabling secure or nonsecure access to the Content Engine GUI, see the “[Enabling or Disabling Access to the Content Engine GUI](#)” section on page 4-54.

Table 4-7 describes the main buttons of the Content Engine GUI and their associated function.

Table 4-7 Content Engine GUI Buttons

Button	Description
Clear	Removes all cacheable objects from the Content Engine memory and hard disks.
Reboot	Reboots the Content Engine.
Save Config	Saves the running system configuration to the startup system configuration.
Update	Applies the changes specified in the current Content Engine GUI window to the running system configuration.
Help	Displays context-sensitive help for the particular Content Engine GUI window. Click the Back button in the Help window to return to the Content Engine GUI window from which you launched the context-sensitive help.

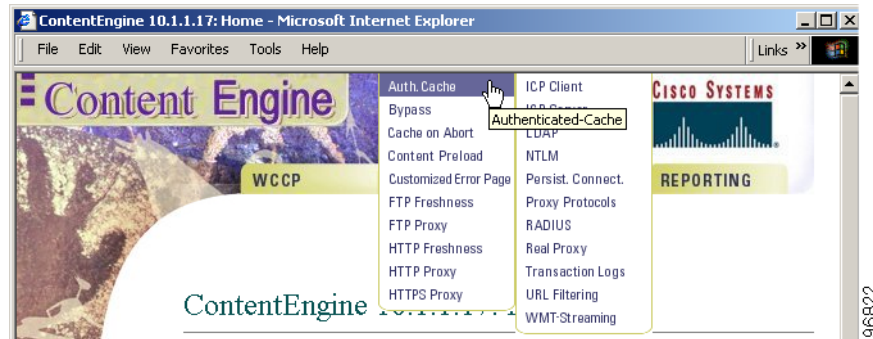
Step 6 To return to the main window, click the words **Content Engine** in the upper-left corner of any Content Engine window (see [Figure 4-18](#)).

Figure 4-18 Content Engine GUI Navigation Bar



Step 7 To navigate to another window in the Content Engine GUI, click one of the tabs to display its subtabs. Click a subtab to choose it (see [Figure 4-19](#)).

Figure 4-19 Content Engine GUI Tabs and Subtabs



Logging out of the Content Engine GUI

To log out of the Content Engine GUI, follow these steps:

-
- Step 1** Click the **Update** button to save any changes that you made in the current Content Engine window, or click **Cancel** to cancel these changes.
 - Step 2** Return to the Content Engine main window (Figure 4-17) by clicking the words Content Engine in the upper-left corner of the current Content Engine window.
 - Step 3** To save any changes made during this current session before logging out, click the **Save Config** button in the Content Engine main window.
 - Step 4** Choose **File > Close**, or click the browser **Close** button.
-

