



Reference Material for Standalone Content Engine Deployments

This appendix contains important reference material that is pertinent to configuring and monitoring standalone Content Engines.

This appendix includes the following sections:

- [Supported Network Protocols, page B-2](#)
- [Supported Streaming Media Protocols, page B-3](#)
- [Supported WCCP Services, page B-4](#)
- [Matrix of Supported Caching, Filtering, and Authentication Mechanisms, page B-7](#)
- [Supported Access Control and Filtering Services for Content Requests, page B-8](#)
- [ACNS Software CLI Command Modes for Standalone Content Engines, page B-9](#)
- [ACNS Software CLI Online Help and Keyboard Shortcuts, page B-11](#)
- [Unusable Multicast Address Assignments, page B-12](#)



Note

The term “standalone Content Engines” is used throughout this guide to refer to Content Engines that ACNS administrators have intentionally not registered with a Content Distribution Manager (if there is one in the network) so that they can configure, manage, and monitor these Content Engines as standalone devices. This is the focus of this guide. For information about configuring, managing, or monitoring Content Engines that are registered with a Content Distribution Manager, refer to the *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.2*.

Supported Network Protocols

Table B-1 lists the network protocols that standalone Content Engines, which are running the ACNS software, Release 5.1 or later, can use to serve content to the web client. Support for HTTP, FTP, TFTP, HTTPS and the IETF standard RTP/RTSP protocols is included as part of the ACNS software product. Whereas, support for the following two product features each need a separate license:

- The WMT product feature that uses Microsoft’s proprietary protocol (the Microsoft Media Server [MMS] protocol) requires a WMT license.
- The RealNetworks’ RealProxy feature that uses RealNetworks’ RTSP protocol, which includes proprietary extensions to the standard IETF standard RTSP protocol, requires a RealProxy license.

To enable the licensed WMT product feature on a Content Engine, you must have a WMT license key, which is supplied on a certificate shipped with the Content Engine. If you are downloading the ACNS 5.x software, you can purchase a WMT license through the Cisco.com website. For more information, see the [“Enabling WMT on Standalone Content Engines” section on page 7-17](#).

To enable the licensed RealProxy product feature on a Content Engine, you must have a RealProxy license key, which is supplied on a certificate shipped with the Content Engine. If you are downloading the ACNS 5.x software, you can purchase a RealProxy license through the Cisco.com website. For more information, see the [“Configuring RealProxy Streaming and Caching Services for Standalone Content Engines” section on page 8-8](#).

Table B-1 Supported Network Protocols

Network Protocol	More Information
HTTP	The main protocol used on the web for communication between web browsers and web servers. There are two commonly implemented HTTP versions today: HTTP 1.0 and HTTP 1.1. ACNS 5.x software supports both HTTP 1.0 and HTTP 1.1. See the “Configuring HTTP Caching for Standalone Content Engines” section on page 6-6 .
FTP	The prevalent file transfer protocol before HTTP became the main protocol. FTP is typically used in applications such as software distribution applications. For more background information, see the “Overview of FTP Caching with Standalone Content Engines” section on page 6-35 . For information about configuring FTP caching on a standalone Content Engine, see the “Configuring FTP Caching for Standalone Content Engines” section on page 6-35 .
TFTP	A simple file transfer protocol that is similar to FTP but has fewer features and is therefore is less complicated. It is still being used by devices that need to download boot images or configurations using a simple protocol (for example, it is used by routers and IP phones). For more background information, see the “Configuring the TFTP Server and Gateway for Standalone Content Engines” section on page 6-43 .

Table B-1 Supported Network Protocols

Network Protocol	More Information
HTTPS	<p>The HTTPS protocol is essentially the HTTP protocol running over a Secure Socket Layer (SSL) transport. SSL is a protocol that provides a secure channel between two machines (for example, a client and a server). SSL uses public-key cryptography to ensure the security and privacy of the conversation between the client browser and the server. HTTPS uses a unique URL that begins with an https:// (for example, https://abc.com). The default port number for HTTPS is port 443 instead of port 80, which is the default port for HTTP.</p> <p>In ACNS 5.1 software, HTTPS requests could only be SSL-terminated on the Content Engine in WCCP mode (client browsers' HTTPS requests are transparently redirected to the Content Engine through WCCP Version 2). In ACNS 5.1 software, in WCCP mode only HTTPS requests to specific sites (HTTPS origin servers that the Content Engine was specifically configured to support) were SSL terminated. In ACNS 5.1 software, the Content Engine would bypass HTTPS requests that were directed to HTTPS servers that it had not been explicitly configured to support.</p> <p>In ACNS 5.2 software, HTTPS requests are now SSL-terminated on the Content Engine in manual proxy mode (direct proxy routing in which client browsers send their HTTPS requests directly to the Content Engine). See the “Pointing Client Browsers Directly to a Standalone Content Engine” section on page 3-36.</p>
MMS	<p>A proprietary protocol designed by Microsoft for streaming media content. This application-level protocol is used by WMT to send active streaming format (ASF) files across the Internet. MMS runs over UDP, TCP, or HTTP. It can also utilize IP multicast to broadcast media contents. See the “Supported Streaming Media Protocols” section on page B-3.</p>
RTSP	<p>A standard Internet streaming control protocol (RFC 2326). This widely used application-level protocol controls the delivery of data with real-time properties, such as video and audio. Apple QuickTime, RealNetworks, and the Cisco Streaming Engine use RTSP as a streaming control protocol. See the “Supported Streaming Media Protocols” section on page B-3 and the “Overview of RTSP Streaming and Caching for Standalone Content Engines” section on page 8-2.</p>

Supported Streaming Media Protocols

Table B-2 lists the streaming media protocols, control channels, the corresponding data format, and transport types that can be used to deliver streaming media files with standalone Content Engines.

Table B-2 Streaming Media Protocols

Streaming Media Protocol	Control Channel	Data Format	Transport Protocol
Windows Media format	TCP	MMS ¹	UDP, ² TCP, HTTP, IP multicast
RealNetworks media format	TCP	RTSP, PNA ³	UDP, TCP, HTTP, IP multicast

1. MMS = Microsoft Media Server protocol
2. User Datagram protocol
3. PNA = Progressive Networks Audio

The MMS protocol automatically looks for the optimal transport to deliver the streaming media in the following order:

- User Datagram Protocol (UDP)
- Transmission Control Protocol (TCP)
- HTTP

MMSU is the Microsoft Media Server protocol with transport over UDP. UDP is a connectionless, transport-layer protocol that is ideal for real-time media because it does not guarantee delivery. Although this sounds like a drawback rather than an advantage, it is a characteristic particularly suited for streaming media. Unlike data such as files or e-mail, which must be delivered in their entirety no matter how long the transmission time, the value of streaming media data is constrained by time. If a frame of video is lost, it is worthless because it will not arrive within the correct time frame.

MMST is the Microsoft Media Server protocol with transport over TCP.

Supported WCCP Services

The type of WCCP services supported by a standalone Content Engine and a WCCP-enabled router varies based on whether WCCP Version 1 or Version 2 is used, as indicated in [Table B-3](#). All of the services except for the standard web-cache service (service 0) requires that WCCP Version 2 (as opposed to WCCP Version 1) is running on the router and the standalone Content Engine for a particular WCCP service to be supported. These services are called “predefined” WCCP services.

Some of the WCCP services that the routers can supply have a well known set of criteria and have a predefined service identifier. For instance, the standard web-cache service (service 0) is a currently supported web-caching service that has a predefined service identifier and well know set of criteria (for example, redirects HTTP requests to port 80). See [Table B-3](#) for a list of WCCP services that have a predefined service identifier (service number).

Other services, that are not well known, may be defined by the configuration of a set of criteria and assigned a service identifier to it. This configuration can be performed by the Content Engines (web caches) that form a particular WCCP service group so that they can define what the criteria is as new WCCP services are developed, but is gated by the routers that need to enable the acceptance of the particular service identifier that the Content Engines are defining the criteria for. WCCP services 90 to 97 are provided to allow you to configure such user-defined services, define the criteria for the new service, and then assign it a service number (identifier).



Note

In ACNS software releases earlier than Release 5.2, a maximum of eight active WCCP services were supported by a WCCP Version 2-enabled router and a Content Engine. In ACNS 5.2 software, up to 25 active WCCP Version 2 services are now supported. In ACNS 5.2 software, there are currently 17 WCCP Version 2 services that can be configured.

Table B-3 Supported WCCP Services with Standalone Content Engines

Service Number	Service Name	Type of Service	Service Description
0	web-cache	Predefined	<p>Web caching service that permits WCCP Version 1 or Version 2-enabled router to redirect HTTP traffic to a single port on the Content Engine. The Content Engine is functioning as a transparent forward proxy server. Only a single WCCP-enabled router is supported with WCCP Version 1; whereas, multiple WCCP-enabled routers (router list) are supported with WCCP Version 2.</p> <p>The Content Engine listens for redirected HTTP requests on the standard HTTP port (default port 80). To enable the Content Engine to listen for WCCP intercepted HTTP traffic on ports other than the default port, configure the custom-web-cache service or a user-defined WCCP service (services 90 to 97). See the “Configuring the Standard Web Cache Service (Service 0) on a Router” section on page 5-24.</p>
53	dns	Predefined	<p>DNS caching service that permits WCCP Version 2-enabled routers to redirect client requests transparently to a Content Engine for the Content Engine to resolve the DNS name. After the Content Engine resolves the DNS name, it stores the resolved DNS name locally so that it can use these resolved names for future DNS requests. See the “Configuring the DNS Caching Service (Service 53) on a Router” section on page 5-25.</p>
60	ftp	Predefined	<p>Caching service that permits WCCP Version 2-enabled routers to redirect native FTP requests transparently to a a single port on the Content Engine. The Content Engine retrieves the requested FTP content, stores a copy locally (native FTP caching), and serves the requested content to the requestor. See the “Configuring Native FTP Caching (Service 60) on a Router” section on page 5-26.</p>
70	https-cache	Predefined	<p>Caching service that permits WCCP Version 2-enabled routers to intercept port 443 TCP traffic and redirect this HTTPS traffic to the Content Engine (transparent forward proxy server that is configured for HTTPS transparent caching). The Content Engine retrieves the requested content, stores a copy locally (HTTPS transparent caching), and serves the requested content to the client.</p> <p>In ACNS 5.2 software, another interception mode (the accept-all mode) was added for the WCCP https-cache service. This mode was added to support the filtering of HTTPS traffic. This mode works the same way as the traditional WCCP services (for example, the web-cache service that intercepts all web traffic by default).</p> <p>By default, the Content Engine accepts all HTTPS traffic.</p> <pre>ContentEngine(config)# wccp https-cache ? accept-all Accept all https traffic by default mask Specify mask used for CE assignment router-list-num Router list number</pre> <p>If the wccp https-cache accept-all global configuration command is used, the HTTPS cache (the Content Engine that has the https-cache service configured and enabled) operates in “accept-all” mode (all HTTPS traffic is intercepted by the Content Engine), otherwise the Content Engine (the HTTPS cache) works in “accept-only” mode, as in ACNS 5.1.x software.</p> <p>The Content Engine listens for redirected HTTPS requests on the standard HTTPS port (default port 443). To intercept HTTPS traffic on ports other than the default port, configure a user-defined WCCP service (services 90 to 97). See the “Configuring the HTTPS Cache Service (Service 70) on a Router” section on page 5-26.</p>

Table B-3 Supported WCCP Services with Standalone Content Engines (continued)

Service Number	Service Name	Type of Service	Service Description
80	rtsp	Predefined	<p>Media caching service that permits WCCP Version 2-enabled routers to redirect RTSP client requests transparently to a single port on a Content Engine (RealMedia transparent caching).</p> <p>The Content Engine listens for redirected RTSP requests on the standard RTSP port (default port 554). To intercept RTSP traffic on ports other than the default port, configure a user-defined WCCP service (services 90 to 97). See the “Configuring the RTSP Service (Service 80) on a Router” section on page 5-27.</p>
81	mmst	Predefined	<p>Media caching service that permits WCCP Version 2-enabled routers to use MMST redirection to redirect WMT client requests transparently to a single port (port 1755) on a Content Engine (a transparent proxy server that is configured for WMT transparent caching).</p> <p>Note MMST is the Microsoft Media Server protocol with transport over TCP. See the “Configuring the MMST Service (Service 81) on a Router” section on page 5-28.</p>
82	mmsu	Predefined	<p>Media caching service that permits WCCP Version 2-enabled routers to use MMSU redirection to redirect WMT client requests transparently to a single port (port 1755) on a Content Engine (a transparent proxy server that is configured for WMT transparent caching).</p> <p>Note MMSU is the Microsoft Media Server protocol with transport over UDP. See the “Configuring the MMSU Service (Service 82) on a Router” section on page 5-28.</p>
90–97	User-configurable	User-defined	<p>Eight user-defined (dynamic) WCCP services that each support multiple ports (up to eight ports per WCCP service). In order to configure these services (services 90 to 97), you must create one port list for each user-defined service that will be used (for example, create port list number 1 for service 90). The port list contains the port numbers that the WCCP Version 2-enabled router will support WCCP redirection on for that particular WCCP service. When configuring these user-defined services, you must specify whether the traffic is to be redirected to the HTTP caching application, HTTPS caching application, or the streaming application on the Content Engine.</p> <p>To configure the Content Engine to cache web traffic using multiple ports, configure a user-defined WCCP service (services 90 to 97) Use these user-defined WCCP services to support WCCP redirection of HTTP, MMS, HTTPS, and RTSP requests on multiple ports (up to eight ports per service) for standard WCCP services (for example, the https-cache, rtsp, mmst, and reverse-proxy services) that ordinarily only support a single port. See the “Configuring User-Defined WCCP Services (Services 90-97) on a Router” section on page 5-29.</p>

Table B-3 Supported WCCP Services with Standalone Content Engines (continued)

Service Number	Service Name	Type of Service	Service Description
98	custom-web-cache	Predefined	Caching service that permits WCCP Version 2-enabled routers to redirect HTTP traffic to a Content Engine on multiple ports other than port 80. The Content Engine is functioning as a transparent forward proxy server. This service allows you to support WCCP redirection of HTTP requests on multiple ports (up to eight ports) without having to configure a user-defined WCCP service (services 90 to 97). See the “Configuring the Custom Web Cache Service (Service 98) on a Router” section on page 5-30.
99	reverse-proxy	Predefined	Caching service that permits WCCP Version 2-enabled routers to redirect HTTP reverse proxy traffic to a Content Engine (a transparent reverse proxy server) on a single port (port 80). To intercept reverse proxy traffic on ports other than the default port (port 80), configure a user-defined WCCP service (services 90 to 97). See the “Configuring the Reverse Proxy Service (Service 99) on a Router” section on page 5-30.

Matrix of Supported Caching, Filtering, and Authentication Mechanisms

Table B-4 lists the caching, filtering, and authentication mechanisms supported by standalone Content Engines that are running ACNS software, Release 5.2 or later. An asterisk (*) indicates a feature is supported for that particular protocol.

Table B-4 Caching, Filtering, and Authentication Mechanisms – Support Matrix with Respect to Different Protocols

Protocol	Filtering				Proxy Authentication			
	Caching	N2H2	Websense	SmartFilter	RADIUS	LDAP	NTLM	TACACS+
HTTP	*	*	*	*	*	*	*	*
FTP-over-HTTP	*	*	*	*	*	*	*	*
HTTPS-over-HTTP	*	*	*	*	*	*	*	*
RTSPG	*							
MMSU	*							
MMST	*							
MMS-over-HTTP	*				*	*		
HTTP-WCCP	*		*	*	*	*	*	*
FTP-WCCP (native FTP)	*							
HTTPS-WCCP	*		*	*				
RTSPG-WCCP	*							
MMSU-WCCP	*							

Table B-4 Caching, Filtering, and Authentication Mechanisms – Support Matrix with Respect to Different Protocols

Protocol	Filtering				Proxy Authentication			
	Caching	N2H2	Websense	SmartFilter	RADIUS	LDAP	NTML	TACACS+
MMST-WCCP	*							
MMS-over-HTTP-WCCP	*				*	*		

Supported Access Control and Filtering Services for Content Requests

Table B-5 lists the access control and filtering content services that are supported with standalone Content Engines that are running ACNS software, Release 5.2 or later. An asterisk (“*”) indicates a feature is supported for that particular protocol.

Table B-5 Supported Access Control and Filtering Services for Standalone Content Engines

Protocol	Access Control	URL Filtering	ICAP	Rules
Caching				
HTTP	*	*	*	*
HTTPS	*	*		*
FTP-over-HTTP	*	*	*	*
Native FTP (FTP-WCCP)				
Streaming				
MMSU		* Local list URL filtering only		*
MMST		* Local list URL filtering only		*
MMS		* Local list URL filtering only		*
RTSP		* Local list URL filtering only		*

For more information, see the following chapters in this guide:

- Chapter 9, “Configuring Content Authentication and Authorization on Standalone Content Engines”
- Chapter 10, “Configuring URL Filtering on Standalone Content Engines”
- Chapter 11, “Configuring ICAP on Standalone Content Engines”
- Chapter 12, “Configuring the Rules Template on Standalone Content Engines”

ACNS Software CLI Command Modes for Standalone Content Engines

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.

Table B-6 summarizes the purpose of the different CLI command modes that are available from the Content Engine CLI that is configured as a standalone Content Engine that is running ACNS 5.x software. The table also describes how to access the different command modes.



Note

Examples of subglobal configuration modes are the following: interface configuration mode, HTTPS server configuration mode, standard IP ACL configuration mode, and extended IP ACL configuration mode. For more detailed information about these modes, refer to the *Cisco ACNS Software Command Reference, Release 5.2* publication.

Table B-6 ACNS Software CLI Command Modes for Standalone Content Engines

CLI Command Mode	Purpose	Access	Prompt	Exit
User EXEC	Used to monitor the operation of the unit (the standalone Content Engine) and issue some system commands such as telnet , traceroute , and ping .	If you log in using an account that does not have superuser privileges, the following CLI prompt is displayed: ContentEngine> To access user EXEC mode from privileged EXEC mode, enter: ContentEngine# disable where <i>ContentEngine</i> is the host name of the standalone Content Engine.	ContentEngine>	Use the exit or end command: ContentEngine> exit

Table B-6 ACNS Software CLI Command Modes for Standalone Content Engines (continued)

CLI Command Mode	Purpose	Access	Prompt	Exit
Privileged EXEC	Used to set up, monitor, and debug the standalone Content Engine, including all commands in user EXEC mode.	From user EXEC mode, enter: ContentEngine> enable Can also access privileged EXEC mode by logging into the CLI with an account with superuser privileges. ¹	ContentEngine#	Use the disable command to return to user EXEC mode. ContentEngine# disable
Global configuration	Used to set, view, and test the configuration of ACNS software features for the entire unit.	From privileged EXEC mode, enter: ContentEngine# configure	ContentEngine(config)#	Use the exit or end command to return to privileged EXEC mode. Alternatively, press Ctrl-Z simultaneously.
Interface configuration	Used to configure a particular interface on a standalone Content Engine.	From global configuration mode, use the interface global configuration command. For example, enter: ContentEngine(config)# interface FastEthernet 0/1 ContentEngine (config-if)#	ContentEngine(config-if)#	Use the exit command to return to the previous configuration mode. Use the end command to exit directly to privileged EXEC mode.
HTTPS server configuration	Used to configure the HTTPS server on a standalone Content Engine.	From global configuration mode, enter: ContentEngine(config)# https server <i>HTTPS_server_name</i>	ContentEngine(config-https)#	Use the exit command to return to the previous configuration mode. Use the end command to exit directly to privileged EXEC mode.
Standard IP ACL configuration	Used to configure standard IP access control lists (ACLs) on a standalone Content Engine.	From global configuration mode, enter: ContentEngine(config)# ip access-list standard <i>acl-name acl-num</i>	ContentEngine(config-std-nacl)#	Use the exit command to return to the previous configuration mode. Use the end command to exit directly to privileged EXEC mode.
Extended IP ACL configuration	Used to configure extended IP ACLs on a standalone Content Engine.	From global configuration mode, enter: ContentEngine(config)# ip access-list extended <i>acl-name acl-num</i>	ContentEngine(config-ext-nacl)#	Use the exit command to return to the previous configuration mode. Use the end command to exit directly to privileged EXEC mode.

1. The predefined admin account has superuser privileges. By default, the username is *admin* and the password is *default* for this predefined admin superuser account. Global configuration commands are device-level commands, whereas subglobal configuration commands are not device-level. Examples of subglobal configuration modes are the following: interface configuration mode, HTTPS server configuration mode, standard IP ACL configuration mode, and extended IP ACL configuration mode.

The ACNS software CLI EXEC mode is used for setting, viewing, and testing system operations. It is divided into two access levels, user and privileged. To access privileged-level EXEC mode, enter the **enable** EXEC command at the user access level prompt and specify a privileged EXEC password (superuser or admin-equivalent password) when prompted for a password.

In TACACS+ there is an “enable password” feature that allows an administrator to define a different enable password for each user. If an ACNS user logs in to the Content Engine with a normal user account (privilege level of 0) instead of an admin or admin-equivalent user account (privilege level of 15), the user must enter the admin password in order to access privileged-level EXEC mode.

```
ContentEngine> enable
Password:
```

This caveat applies even if these ACNS users are using TACACS+ for login authentication.

ACNS Software CLI Online Help and Keyboard Shortcuts

To view the CLI online help, enter a **?** as follows:

- After the prompt to view a list of the commands available in the current mode

```
ContentEngine(config-std-nacl)# ?

delete Delete a condition
deny Specify packets to reject
exit Exit from this submode
insert Insert a condition
list List conditions
Move Move a condition
no Negate a command or set its defaults
permit Specify packets to accept
ContentEngine(config-std-nacl)#
```

- After a typed command to view the available parameters

```
ContentEngine(config)# ip access-list extended ?
<100-199> Extended IP access-list number
WORD Access-list name (max 30 characters)
```

- After a partially typed keyword to view the possible completions

To view a description of the online help for the ACNS software CLI, enter the **help** command.

As a shortcut, you can abbreviate commands to the fewest letters that make them unique. For example, the letters **sho** can be entered for the **show** command.

Certain EXEC commands display multiple screens with the following prompt at the bottom of the screen:

```
--More--
```

Press the **Spacebar** to continue the output, or press **Return** to display the next line. Press any other key to return to the prompt. Also, at the **--More--** prompt, you can enter a **?** to display the help message.

Table B-7 summarizes the keyboard shortcuts.

Table B-7 Command-Line Processing Keystroke Combinations

Keystroke Combinations	Function
Ctrl-A	Jumps to the first character of the command line.
Ctrl-B or the Left Arrow key	Moves the cursor back one character.
Ctrl-C	Escapes and terminates prompts and tasks.
Ctrl-D	Deletes the character at the cursor.
Ctrl-E	Jumps to the end of the current command line.
Ctrl-F or the Right Arrow key ¹	Moves the cursor forward one character.
Ctrl-K	Deletes from the cursor to the end of the command line.
Ctrl-L	Repeats the current command line on a new line.
Ctrl-N or the Down Arrow key ¹	Enters the next command line in the history buffer.
Ctrl-P or the Up Arrow key ¹	Enters the previous command line in the history buffer.
Ctrl-T	Transposes the character at the cursor with the character to the left of the cursor.
Ctrl-U; Ctrl-X	Deletes from the cursor to the beginning of the command line.
Ctrl-W	Deletes the last word typed.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or Backspace key	Erases a mistake when entering a command; reenter the command after using this key.

1. The arrow keys function only on ANSI-compatible terminals such as VT100s.

Unusable Multicast Address Assignments

The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. The IANA has assigned the IPv4 Class D address space to be used for IP multicast. Therefore, all IP multicast group addresses fall in the range from 224.0.0.0 through 239.255.255.255. However, some combinations of source and group address should not be routed for multicasting purposes. Table B-8 lists the unusable multicast address ranges and the reasons they should not be used.

Some of these addresses have been reserved for use by multicast applications through the IANA. For example, IP address 224.0.1.1 has been reserved for the Network Time Protocol (NTP).

IP addresses reserved for IP multicast are defined in RFC 1112, *Host Extensions for IP Multicasting*. More information about reserved IP multicast addresses can be found at the following location: <http://www.iana.org/assignments/multicast-addresses>.



Note

You can find all RFCs and Internet Engineering Task Force (IETF) drafts on the IETF website (<http://www.ietf.org>). The Class D address range is used only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.

Table B-8 Unusable Multicast Address Assignments

Address Range	Reason
224.0.1.2/32	Known insecure service address. See the “Insecure Services” section on page 2-14.
224.0.1.3/32	Reserved for the discovery of resources within the administrative domain. See the “Limited Scope Addresses” section on page 2-14.
224.0.1.22/32	Known insecure service address.
224.0.1.35/32	Reserved for the discovery of resources within the administrative domain.
224.0.1.39/32	Reserved for the discovery of resources within the administrative domain.
224.0.1.40/32	Reserved for the discovery of resources within the administrative domain.
224.0.2.2./32	Known insecure service address.
224.77.0.0/16	Used to copy files between servers and clients in a local network. See the “Copying Files Between Servers and Clients” section on page 2-14.
224.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches. See the “Layer 2 Multicast Addresses” section on page 2-15.
225.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
225.1.2.3/32	Used to copy files between servers and clients in a local network.
225.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
226.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
226.77.0.0/16	Used to copy files between servers and clients in a local network.
226.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
227.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
227.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
228.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
228.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
229.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
229.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
230.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
230.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
231.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.

Table B-8 Unusable Multicast Address Assignments (continued)

Address Range	Reason
231.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
232.0.0.0/24	Source-specific multicast address. See the “Source-Specific Multicast Addresses” section on page 2-14.
232.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
233.0.0.0/8	GLOP address. See the “GLOP Addresses” section on page 2-15.
233.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
233.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
234.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
234.42.42.42/32	Used to copy files between servers and clients in a local network.
234.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
234.142.142.42/31	Used to copy files between servers and clients in a local network.
234.142.142.44/30	Used to duplicate files between clients and servers in a local network.
234.142.142.48/28	Used to copy files between servers and clients in a local network.
234.142.142.64/26	Used to copy files between servers and clients in a local network.
234.142.142.128/29	Used to copy files between servers and clients in a local network.
234.142.142.136/30	Used to copy files between servers and clients in a local network.
234.142.142.140/31	Used to copy files between servers and clients in a local network.
234.142.142.142/32	Used to copy files between servers and clients in a local network.
235.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
235.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
236.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
236.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
236.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
236.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.

Table B-8 *Unusable Multicast Address Assignments (continued)*

Address Range	Reason
237.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
237.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
238.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
238.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
239.0.0.0/8	Administratively scoped address that should not be passed between administrative domains. See the “Limited Scope Addresses” section on page 2-14.
239.0.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.
239.128.0.0/24	Local address that maps to an Ethernet multicast address range and may overwhelm the mapping table of LAN switches.

■ Unusable Multicast Address Assignments