



# Release Notes for Cisco ACNS Software, Release 5.0

---

February 17, 2004



**Note**

---

The most current Cisco documentation for released products is available at Cisco.com at <http://www.cisco.com>. The online documents may contain updates and modifications made after the hardcopy documents were printed.

---

## Documentation Survey

Is Cisco documentation helpful? Click [here](#) to give us your feedback.

## Contents

These release notes contain information about ACNS 5.0 software. These release notes describe the following topics:

- [Introduction, page 2](#)
- [Installation Notes, page 3](#)
- [New and Changed Information, page 4](#)
- [Hardware Supported, page 7](#)
- [Software Supported, page 8](#)
- [New and Changed CLI Commands, page 8](#)
- [Important Notes, page 10](#)
- [Limitations and Restrictions, page 12](#)
- [Caveats, page 14](#)
- [Documentation Updates, page 25](#)



---

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

- [Related Documentation, page 30](#)
- [Obtaining Documentation, page 31](#)
- [Obtaining Technical Assistance, page 32](#)
- [Obtaining Additional Publications and Information, page 34](#)

## Introduction

ACNS 5.0 software unifies the Content Networking components into a common Content Distribution Manager, Content Engine, and Content Router that can serve multiple market deployments.

In ACNS 5.0, Content Engines can be deployed as “standalone” proxy caches, or as part of a CDN solution using a Content Distribution Manager for central management and an optional Content Router for HTTP and Real-Time Streaming Protocol (RTSP) redirection. When Content Engines are deployed as standalone caches, configuration is implemented using the Content Engine command-line language interface (CLI) or the Content Engine graphical user interface (GUI).

When Content Engines are deployed as part of a Content Delivery Network (CDN) solution, then a Content Distribution Manager is required to configure the services and topology necessary to enable content distribution from origin servers to authorized Content Engines. The ACNS 5.0 software content distribution system increases scalability of Content Engines which support unicast and multicast networks, tunnel between multicast network islands, distribute to Content Engines located behind firewalls, and support network bandwidth controls for distribution.

Client (browser, player) requests for content are intercepted and redirected to a Content Engine best-positioned to serve that client based on proximity. Enterprise edge routers can be configured to intercept user requests through Web-Cache Communication Protocol (WCCP) and redirect them to a Content Engine. Browsers and players can be set to proxy all requests through a Content Engine, or a Content Router can be used to intercept Domain Name System (DNS) requests and perform an HTTP or RTSP redirection to a Content Engine.

By significantly increasing scalability, ACNS 5.0 software can now address CDN deployments of up to 2000 Content Engines and up to 1,000,000 pre-positioned items in Content Engines with sufficient memory and disk space.

## Content Acquisition

In ACNS 5.0 software, all content is pulled from a web server or an FTP server (the origin server) and sent directly to the Content Engines. Certain Content Engines are designated as “root” Content Engines. Root Content Engines are responsible for acquiring content from the origin servers and then distributing the content to other Content Engines subscribed to the same channel of content. This means that you do not need to store content on the Content Distribution Manager. Content now resides on the origin server that is accessible to the root Content Engines. The protocols supported in Cisco ACNS 5.0 Software for acquiring content are HTTP, Hypertext Transfer Protocol Secure (HTTPS) or FTP.

A manifest file is used to identify which files should be acquired from the origin server and then pre-positioned on the Content Engines. This manifest file is in Extensible Markup Language (XML) format and should be placed on a web server or FTP server that the Content Engines can access. The Content Distribution Manager facilitates management and configuration and determines which root Content Engines obtain which manifest file based on the channels of content for which they are responsible.

Many CDN installations will need to add a root Content Engine in order to take advantage of the new content distribution system. The root Content Engine should be placed in a location close to the origin servers and with good connectivity close to the origin servers.

## Edge Intercept Methods

ACNS 5.0 software allows you to use either of the following edge-intercept methods to redirect clients to the best Content Engine regardless of whether the content is requested or pre-positioned:

- WCCP supported on routers and switches running Cisco IOS software
- Browser proxy auto configuration

Your router must support WCCP in order for you to use WCCP as an edge-intercept method. With edge-intercept methods, you do not need a Content Router in ACNS 5.0 software. The Content Distribution Manager no longer redirects requests, so if you do not use WCCP or proxy auto configuration, you must use a Content Router.

## Using a URL to Request Content

In ACNS 5.0 software, when you use an edge-intercept method to request content the URLs that are used are the original URLs from the web server. However, when you use content routing the URL for pre-positioned content on the web server has change. In ACNS 4.2 software, the URL pointed to the Content Distribution Manager that redirected requests to the appropriate Content Engine. In ACNS 5.0 software, all requests are sent to a Content Router that then issues the redirected requests to a Content Engine. Requests are directed to a Content Router using the Domain Name System (DNS). The Content Router becomes authoritative for a domain which is hosted by the CDN. This means that all URLs referring to content served by the CDN must include the domain hosted by the content routers.

## XML APIs for Content Distribution Manager and CDN Management

The following central management APIs are provided through the Content Distribution Manager:

- Replication Status API
- Provisioning APIs
- Listing API
- Streaming Statistics API

## Installation Notes

Instructions for installing the hardware and initial installation and configuration of new devices are located in the *Cisco Content Delivery Networking Products Getting Started Guide*.

See the *Cisco ACNS Migration Guide, Release 5.0* for instruction on migrating your system from ACNS 4.2 software to ACNS 5.0 software. The migration guide explains how to migrate your Cisco ACNS 4.2 CDN to a Cisco ANCS 5.0 CDN in two migration deployment scenarios as well as how to configure the Content Distribution Manager, the Content Engine, and the Content Router needed to control content delivery using the Content Distribution Manager graphical user interface (GUI).

**Caution**

Users who use the CDN features need to migrate their content from ACNS 4.2 software to ACNS 5.0 software. See the *Cisco ACNS Migration Guide, Release 5.0* for instructions on migrating content. Users must follow instructions in the Migration Guide or the CDN will be non-functional.

**Note**

Users who only use caching functions do not have to make many changes to their system in order to upgrade. .

## New and Changed Information

ACNS 5.0 software features can be organized into several subsystems, all of which contain new features. Subsystems include the following:

- Management
- Request routing
- Acquisition and distribution
- Content delivery
- Software platform
- Security

## Management

The ACNS 5.0 software Configuration Management System (CMS) is responsible for the local and remote configuration and monitoring of the ACNS 5.0 software CDN services.

The role of the CMS is to enable you to configure, reconfigure, and monitor CDN services both locally (on the managed nodes) and centrally using the Content Distribution Manager.

This management is directly available through HTML GUI, XML-based system API, and CLI on each of the nodes. Clients are able to configure all aspects of the node including proxy cache, pre-positioned content cache, and playback media servers using the system API's. CMS features include the following:

- Management through the GUI and CLI
- Embedded database in the Content Distribution Manager
- Crawler tool extended to meet any new manifest file rules
- Low bit rate system messaging
- Multicast and unicast system messaging
- Multi-Cast island hopping messaging
- Creating and configuring device groups using the Content Distribution Manager
- Secure Content Distribution Manager login
- Content Distribution Manager GUI timeouts
- Configuring distribution topology using the GUI
- Authentication, authorization, accounting (AAA) support

- Redundant Content Distribution Manager
- Basic access and usage log configuration
- Audit and system logs
- SNMP (Traps and MIBS) monitoring with CiscoWorks integration
- Secure inter-box communication, authentication, messaging, logging
- Application Licensing using license keys
- Software Upgrades and downgrades using the Content Distribution Manager and CLI
- Ability to enable and disable applications
- Third-party licensing
- Playlist management
- Virtual CDN using device groups

## Request Routing

Application level request routing in ACNS 5.0 software can be implemented through the Local Request Intercept or Centralized Request Intercept. In Local Request Intercept, Content Engines are deployed at the edges of enterprise network. In Centralized Request Intercept, Content Routers are deployed and DNS entries are required for hosted domains (channels). Request routing does not take content placement into account in either Local Intercept or Centralized Request Routing.

Local intercept, when available and enabled, provides the best CDN service proximity and does not impose any global scalability restrictions. It does not require deployment of a Content Router. In this mode the decision on whether and how to serve a request is done locally. Content is always served by local Content Engines. In some cases the Content Engine that intercepted request will not have the content. It can fetch content on demand, or if it was pre-positioned content return an Alternative Media, depending on the policy for this content category.

ACNS 5.0 software request routing consists of combining DNS intercept with HTTP redirection. Request routing features include the following:

- WCCP Intercept for HTTP, RTSP, MMS
- Centralized request routing through DNS/HTTP redirect in with coverage zones. Content Routing Service can be enabled in a dedicated Content Router as well on a Content Engine, with different performance expectations.
- Intercepted request can be manipulated through a rules-based approach
- DNS/HTTP content routing
- DNS Cache

## Content Acquisition and Distribution

ACNS 5.0 software is a new module and allows content to be fetched from an origin server through HTTP, HTTPS, or FTP. The fetching of content will be directed by a *manifest file* that lists the content items to be acquired, as well as a number of attributes about that content. Each manifest file assigns content to one or more channels.

- Virtual import
- Real live pull splitting through RealServer

- WMT live pull splitting through WMT Server
- HTTP and HTTPS Acquisition and distribution
- FTP acquisition
- Manifest File driven acquisition
- Crawler-based acquisition
- Settable content attributes, real-time Time-To-Live override, rules based content policy
- Real-time acquisition and distribution status
- Low bit rate distribution and messaging
- Reliable multicast content replication
- Pull replication for cache miss
- Pull replication for new CE that does not have pre-positioned content
- Push multicast replication for pre-positioning video on demand
- Configurable bandwidth control for QoS
- Content distribution fault tolerance
- Content pre-positioning based on Content Engine group and assignment to a channel
- Ability to identify amount of disk space (quotas) per file system and use for pre-positioning on a per device basis

## Content Delivery

Content delivery, or request processing and streaming, contains the HTTP proxy, and Windows Media Technologies (WMT) server, RealServer, and the Quick Time Streaming Server (QTSS). Content Delivery features include:

- Support for IETF standard based RTP/RTSP streaming
- Extends HTTP caching rules template to Real and WMT services as allowed by protocols
- Support for WMT proxy, live, and video on demand
- WMT request authentication and authorization pass through for pre-position only, rules based request processing, QoS, URL filtering, unified name space, bandwidth control, and configuration of most WMT streaming features
- Support for RealNetworks proxy, live, and video on demand
- RealNetworks rules based request processing, QOS, URL filtering, unified namespace, bandwidth control, configuration of most WMT streaming features
- QTSS integration and QTSS video on demand
- Content Engine bandwidth control across WMT and RealNetworks servers
- Access pre-positioned content through HTTP, WMT, and Real servers
- TACACS+, RADIUS, content request authentication for HTTP content
- Extend URL filtering to RealNetworks and WMT servers

## Software Platform

ACNS 5.0 software platform features include the following:

- TV-out Playlist with support for central playlist management, central playback controls, distributed playlist, multiple playlists, and flexible playlists
- Diskless operation
- Common disk access, namespace for pre-positioned and cached content is unified
- Fibre channel on Thunder and/or Lightning
- EtherChannel support
- WCCP support for EARL6
- HTTP caching performance enhancements
- Disk fault monitoring
- Multiple-NIC (Active-Active, and Active-Standby) support
- IP spoofing support

## Security

ACNS 5.0 software high-level security features include the following:

- A CDN management system that offers role-based security and support of AAA system for very large-scale CDN deployments from a single Web GUI interface
- Secure file replication from origin server to Content Engines and configurable through the Content Distribution Manager
- Secure file replication to FTP servers through either SCP or FTP of encrypted Files
- Content Distribution Manager GUI access through HTTPS session
- Secure telnet session to CDN devices
- License key that defines the Content Engine or Content Distribution Manager capability.
- License key that defines which application services are supported such as WMT, RealNetworks, or QTSS.
- Content Engine content delivery for HTTP authentication against TACACS+ and RADIUS management system.

## Hardware Supported

ACNS 5.0 software supports the following existing and new platforms:

- CDM-4630
- CDM-4650
- CE-7320
- CR-4430
- CE-590
- CE-590-DC

- CE-560
- CE-560AV
- CE-507
- CE-507AV
- CE-510-K9
- CE-565-K9
- CE-7325-K9
- CE-7325-DC-K9
- CE-7305-K9
- CE-7305-DC-K9

The 1000BASE-TX twisted-pair cabling Gigabit Ethernet port is supported.



**Note**

ACNS5.0 software does *not* support the Content Engine Network Module for the 2600, 3600, and 3700 Series branch routers.



**Note**

ACNS 5.0 software does *not* support the 1000BASE-SX or 1000BASE-FX Gigabit Ethernet ports. Fiber-optic cabling is not supported.

## Software Supported

The following features are incorporated in ACNS 5.0 software and can be optionally turned on through a license key:

- RealProxy
- RealSubscriber
- Windows Media proxy and server

ACNS 5.0 software supports SmartFilter, Version 3.1.2 software for URL filtering. After upgrading to ACNS 5.0 software, you need to use SmartFilter, Version 3.1.2.

## New and Changed CLI Commands

The following CLI commands are new or have changed syntax options in ACNS 5.0 software. See the *Cisco ACNS Software Command Reference, Release 5.0* for detailed information about all ACNS 5.0 software CLI commands.

New or Changed CLI Command	Description
<b>access-lists</b>	Configures access control list entries.
<b>acquirer</b>	Starts or stops content acquisition on a specified acquirer channel.

<b>New or Changed CLI Command</b>	<b>Description</b>
<b>acquisition-distribution</b>	Starts or stops the content acquisition and distribution process.
<b>asset tag</b>	Sets the tag name for the asset tag string
<b>bandwidth allow</b>	Sets an allowable bandwidth usage limit and its duration for Cisco Streaming Engine, RealProxy, RealServer, and WMT streaming media.
<b>cdm</b>	Configures the Content Distribution Manager IP address and primary or standby role settings.
<b>cdnfs</b>	Manages the CDN file system (cdnfs).
<b>channel</b>	Assigns, creates, deletes, adds, modifies, or otherwise configures a channel.
<b>cms</b>	Configures the configuration management subsystem (CMS) embedded database parameters. Schedules maintenance and enables the configuration management subsystem (CMS) on a given node.
<b>clear</b>	Clears the HTTP object cache, the hardware interface, statistics, archive working transaction logs, and other settings.
<b>copy</b>	Copies configuration or image data from a source to a destination.
<b>debug</b>	Monitors and records cache software functions.
<b>device</b>	Configures the mode of operation on a device to be that of a Content Distribution Manager, Content Engine, or Content Router.
<b>interface</b>	Configures a Fast Ethernet, Fibre Channel, Gigabit Ethernet, or Port Channel interface. To disable selected options, restore default values, or enable a shut down interface, use the no form of this command.
<b>multicast</b>	Configures multicast client options.
<b>ntp</b>	Configures the Network Time Protocol (NTP) and to allow the system clock to be synchronized by a time server.
<b>primary-interface</b>	Configures the primary interface for the CDN.
<b>restore</b>	Restores the device to its manufactured default status, removing user data from disk and in Flash memory.
<b>rtsp</b>	Configures Real-Time Streaming Protocol (RTSP) related parameters.
<b>show acquirer</b>	Displays the acquirer information and progress for a specified channel number or name.
<b>show cdn-statistics</b>	Displays CDN Content Engine and device group statistical data.
<b>show cms</b>	Displays the content management subsystem (CMS) protocol embedded database content and maintenance status, and other information.
<b>show content-routing</b>	Displays the Content Router simplified hybrid routing table.

New or Changed CLI Command	Description
<b>show distribution</b>	Displays the distribution information for a specified channel.
<b>show multicast</b>	Displays a multicast client configuration and license.
<b>show rtsp</b>	Displays the Real-Time Streaming Protocol (RTSP) configurations. If the license-agreement option is included in the command string, the full text of the RealProxy license agreement is displayed.
<b>show statistics acquirer</b>	Displays Content Engine acquirer channel statistics.
<b>show statistics content-routing</b>	Displays simplified hybrid content routing statistics.
<b>show statistics distribution</b>	Displays the statistics of the content distribution components.
<b>show statistics http</b>	Displays Content Engine HTTP statistics.
<b>show statistics replication</b>	Displays channel replication status and related statistical data on the Content Distribution Manager or Content Engine.
<b>show statistics tvout</b>	Displays Content EngineTV output statistics.
<b>show statistics wmt rule</b>	Displays Content Engine WMT (Windows Media Technologies) statistics.
<b>show tvout</b>	Displays TV output information.
<b>snmp-server</b>	Configures snmp parameters.
<b>tvout</b>	Enables and configures TV output service.
<b>wmt</b>	Configures Windows Media Technologies (WMT).
<b>write</b>	Saves startup configurations.

## Important Notes

This section emphasizes important information regarding ACNS 5.0 software.

### Insufficient Bandwidth Errors Occur When Using the WMT Evaluation License

Open Caveat CSCdz89924

Symptom: All users see the following error message on the Windows Media Play when playing any WMT stream:

"There is insufficient bandwidth available to fulfill the request."

Condition: This condition occurs when "wmt evaluate" is first configured and the Content Engine has never been reloaded with the running configuration copied to the startup configuration.

Workaround: There are 3 possible workarounds.

1. The simplest workaround is to reload the Content Engine if this is feasible. Save the running configuration to the startup configuration and the reload the Content Engine using the following CLI Exec commands.

```
ContentEngine# copy running-config startup-config
ContentEngine# reload
```

2. If a reload of the Content Engine is not feasible, another workaround is to explicitly set the WMT bandwidth limit in the running configuration using the **bandwidth** configuration command.

To determine the maximum bandwidth allowed during evaluation for your hardware platform, run the **show wmt** Exec command:

```
ContentEngine# show wmt
```

In the command output, look at the following line and note the value of “N”:

```
WMT max bandwidth limit enforced during evaluation: "N" Kbits/sec
```

To explicitly configure the maximum bandwidth allowed for all time slots, run the following config command. The following example uses 168000 as the value for “N”:

```
ContentEngine(config)# bandwidth all 168000 wmt start-time Sunday 00:00 end-time Saturday 23:59
```

To confirm the bandwidth has been set, run the **show bandwidth** Exec command to verify the output.

```
ContentEngine# show bandwidth
```

```
-----
MODULE           Bandwidth   Start Time   End Time
                Kbps
-----
wmt              168000     Sunday      00:00      Saturday   23:59
```



**Note**

It is not required to save this bandwidth configuration to the startup configuration for proper behavior after the next Content Engine reload as long as the **wmt evaluate** has been copied to the startup configuration before the next reload. If the bandwidth command is already being used for some time slots, then the workaround is to configure only the unused time slots with the maximum allowed bandwidth.

3. Another workaround is to purchase a permanent license key for WMT from Cisco if you are ready to purchase the feature.

## Media File System Issues When Downgrading to ACNS 5.0 Software

If you have configured the media file system (mediafs) with ACNS 5.1 software or later, and then downgrade to ACNS 5.0 software, the mediafs disk space assignment is lost and it reverts to ACNS network file system (cdnfs) disk space. (The mediafs is used for on-demand content that is fetched through the two streaming protocols [RTSP and WMT]. The cdnfs is used for pre-positioned content in the ACNS network.)

This situation occurs because of a design change that was implemented in ACNS 5.1 software. Because ACNS 5.0 software is not compatible with this change, the disk space becomes assigned to cdnfs instead of mediafs. To work around this problem, follow these steps:

1. After you downgrade to ACNS 5.0 software, use the CLI (**disk config EXEC** command) or the GUI to assign the mediafs disk space.

Use the Content Distribution Manager GUI for Content Engines that are registered with a Content Distribution Manager. Use the Content Engine GUI for standalone Content Engines (that is, Content Engines that are not registered with a Content Distribution Manager and are being managed through the Content Engine GUI or CLI).

2. Reboot the Content Engine for the disk configuration changes to take effect.

## Websense Issues When Downgrading to ACNS 5.0 Software or ACNS 5.1 Software

If the local (internal) Websense server is enabled on the Content Engine and you downgrade from the ACNS 5.2.x software to ACNS 5.0 software or ACNS 5.1 software, the WebsenseEnterprise directory is removed from the Content Engine and the local Websense server stops working. Note that the ACNS 5.2.x software does not generate an error message indicating that the WebsenseEnterprise directory has been removed.

To avoid this problem when downgrading from ACNS 5.2.x software to ACNS software 5.1 or ACNS 5.0 software, follow these steps:

1. Disable the local (internal) Websense server on the Content Engine.
2. Deactivate the Websense services on the Content Engine.
3. Install the ACNS 5.1 software or ACNS 5.0 software downgrade image on the Content Engine.

## Limitations and Restrictions

This section contains a list of limitations and restrictions regarding ACNS 5.0 software.

### CLI Commands

- The ACNS 5.0 software manages certain CLI commands that are particularly important for CDN functionality, and which are likely to be managed using device groups. If you configure any of these from the Content Engine, either through the Content Engine GUI or CLI, then the settings are not stored as part of the Content Distribution Manager's CDN-wide configuration data, and are likely to be overwritten by the Content Distribution Manager. These commands include the following:
  - **cdp**
  - **ldap**
  - **logging**
  - **ntp**
  - **radius-server**
  - **tacacs**
  - **bandwidth**
  - **bypass**
  - **dns-cache**
  - **ftp**
  - **http**
  - **https**
  - **icp**
  - **multicast**

- **ntlm**
- **proxy-auto-config**
- **proxy-protocols**
- **rtsp**
  - excluding:
    - rtsp server real-subscriber accept-license-agreement**
    - rtsp proxy media-real accept-license-agreement**
    - rtsp-proxy**
- **rule**
- **transaction-logs**
- **url-filter**
- **multicast accept-license-agreement**
- **wmt**
  - excluding:
    - wmt proxy**
    - wmt accept-license-agreement**
    - wmt live-url-stripping**
    - authentication**
    - error-handling**
    - dns enable**

## Windows Media Player

- If proxy mode is used for content routing, then Windows Media Player (WMP) version 6.4 cannot be used as it does not have the option to set mms proxy.
- When the WMP issues an http request, it actually issues two http requests. The first request is to obtain the header from server, but it only reads some of the data received and terminates connection with the server without obtaining all the response data from the server. This causes the server to report a client (Content Engine) error. Then the WMP sends another request for the real media data.

## Boomerang Commands

Boomerang commands are not supported in ACNS 5.0 software.

## Netscape Browser

Only Netscape browser version 7.0 and later is supported by the Content Distribution Manager GUI. Netscape browser versions prior to version 7.0 are not supported.

When you use the Content Distribution Manager GUI online help from Netscape browser version 7.0, the Contents and Index pane on the left side of the help window cannot be displayed unless you install the following Java plugin: mime type: application/x-java-applet;version=1.1.1

You can find this plugin at the following location:

[http://wp.netscape.com/plugins/search\\_pi.html?cp=plp](http://wp.netscape.com/plugins/search_pi.html?cp=plp)

## Websense

Only Websense version 4.4 is compatible with ACNS 5.0 software. Prior versions of Websense do not work with ACNS 5.0 software.

## FTP

If you use FTP to acquire content using a CDN URL, and the content-type is not specified in the manifest file, then the CDN URL must have the correct extension. Otherwise the wrong content-type is generated and you will not be able to play the content.

## Caveats

This section lists and describes caveats that are open in ACNS 5.0 software.

Caveats describe unexpected behavior in ACNS 5.0 software. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

## Open Caveats - Release 5.0

- CSCdy64673

Symptom: Improper reverse DNS lookup configuration does not allow the Content Engine to obtain the DNS name of the origin server, which might cause additional traffic from the Content Engine.

Condition: This occurs when you are using WCCP interception and a Windows Media Player 6.4 for playback of pre-positioned content.

When the above conditions occur, the initial request sent by the Windows Media Player 6.4 to the Content Engine that intercepted the WCCP request has the IP address of the target server. The Content Engine matches the request with the pre-positioned content only if it can deduce the DNS name from the IP address (by doing reverse DNS lookup). Thus, if the DNS configuration is not correct, the Content Engine is not able to get the DNS name of the origin server.

Workaround: You need to make sure that all IP addresses are reverse-mapped to the DNS name of the origin server.

- CSCdy82311

Symptom: Content cannot be acquired using strong authentication from secure origin servers that use certificates from nonstandard certificate authorities (CAs). If strong authentication was chosen for content acquisitions from such a site, the acquirer error statistics will contain a 401 (Unauthorized) error code, and the acquirer error log will contain the following error message:

```
Strong Cert Authentication rejects certificate due to error: ssl error code
```

Condition: This problem occurs if the origin server uses a certificate that is not known as a standard certificate to the ACNS acquirer. For content acquisition from secure sites over HTTPS using strong authentication, only sites with certificates from standard certificate authorities are supported.




---

**Note** With strong authentication, if there are any errors during certificate verification by the ACNS acquirer, then content from that site will not be acquired. With weak authentication, certain errors (for example, errors such as certificate has expired, certificate is not yet valid, and subject issuer mismatch) are allowed during certificate verification.

---

Workaround: Use one of these workarounds:

- Use weak authentication.

On the secure server, use a certificate that was generated by one of the standard certificate authorities. ACNS network administrators should refer to the following information to determine which CA certificate they should install on their origin servers. Note that the certificate list differs based on the version of the ACNS software. For the ACNS 5.0 software release, refer to the following certificate list:

```
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary
Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After  : Jan  7 23:59:59 2020 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 1 Public Primary
Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary
Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After  : Jan  7 23:59:59 2004 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 2 Public Primary
Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary
Certification Authority
    Validity
        Not Before: Jan 29 00:00:00 1996 GMT
        Not After  : Jan  7 23:59:59 2004 GMT
    Subject: C=US, O=VeriSign, Inc., OU=Class 3 Public Primary
Certification Authority
-----END CERTIFICATE-----
```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=RSA Data Security, Inc., OU=Secure Server
Certification Authority
    Validity
        Not Before: Nov  9 00:00:00 1994 GMT
        Not After  : Jan  7 23:59:59 2010 GMT
    Subject: C=US, O=RSA Data Security, Inc., OU=Secure Server
Certification Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=VeriSign, Inc, OU=www.verisign.com/repository/TestCPS Incorp. By
Ref. Liab.LTD., OU=For VeriSign authorized testing only. No assurances (C)VS1997
    Validity
        Not Before: Mar  4 00:00:00 1997 GMT
        Not After  : Mar  4 23:59:59 2025 GMT
    Subject: O=VeriSign, Inc, OU=www.verisign.com/repository/TestCPS Incorp.
By Ref. Liab. LTD., OU=For VeriSign authorized testing only. No assurances
(C)VS1997
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
    Validity
        Not Before: Dec  2 21:38:51 1999 GMT
        Not After  : Jul 10 21:38:51 2005 GMT
    Subject: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test CA (1024 bit)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
    Validity
        Not Before: Jun 15 02:14:29 1997 GMT
        Not After  : Jul 15 02:14:29 1997 GMT
    Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
    Validity
        Not Before: Jun 14 22:54:45 1997 GMT
        Not After  : Jul 14 22:54:45 1997 GMT
    Subject: C=AU, ST=Some-State, O=Internet Widgits Pty Ltd, CN=PCA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=GB, O=UCL, OU=ICE-TEL Project, CN=TrustFactory
    Validity
        Not Before: Apr 22 14:39:14 1997 GMT
        Not After  : Apr 22 14:39:14 1998 GMT
    Subject: C=GB, O=UCL, OU=ICE-TEL Project, CN=TrustFactory
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=European ICE-TEL project, OU=V3-Certification Authority
    Validity
        Not Before: Apr  2 17:35:53 1997 GMT
        Not After  : Apr  2 17:35:53 1998 GMT
    Subject: O=European ICE-TEL project, OU=V3-Certification Authority,
L=Darmstadt
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: O=European ICE-TEL project, OU=V3-Certification Authority
    Validity
        Not Before: Apr  2 17:33:36 1997 GMT
        Not After  : Apr  2 17:33:36 1998 GMT
    Subject: O=European ICE-TEL project, OU=V3-Certification Authority
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: O=European ICE-TEL project, OU=V3-Certification Authority,
L=Darmstadt
    Validity
        Not Before: Apr  2 17:35:59 1997 GMT
        Not After  : Apr  2 17:35:59 1998 GMT
    Subject: O=European ICE-TEL project, OU=V3-Certification Authority,
L=Darmstadt, CN=U
SER
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=Ca, L=Nepean, OU=No Liability Accepted, O=For Demo Purposes
Only, CN=Entrust Demo Web CA
    Validity
        Not Before: Apr 26 13:35:01 1996 GMT
        Not After  : Apr 26 13:35:01 2006 GMT
    Subject: C=Ca, L=Nepean, OU=No Liability Accepted, O=For Demo Purposes
Only, CN=Entrust Demo Web CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
    Validity
        Not Before: Dec  2 21:35:48 1999 GMT
        Not After  : Jul 11 21:35:48 2005 GMT
    Subject: C=AU, ST=Queensland, O=CryptSoft Pty Ltd, CN=Test PCA (1024 bit)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=US, O=RSA Data Security, Inc., OU=Commercial Certification
Authority
    Validity
        Not Before: Nov  4 18:58:34 1994 GMT
        Not After  : Nov  3 18:58:34 1999 GMT
    Subject: C=US, O=RSA Data Security, Inc., OU=Commercial Certification
Authority
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification
Services Division, CN=Thawte Server CA/Email=server-certs@thawte.com
    Validity
        Not Before: Aug  1 00:00:00 1996 GMT
        Not After  : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division, CN=Thawte Server
CA/Email=server-certs@thawte.com
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification
Services Division, CN=Thawte Premium Server CA/Email=premium-server@thawte.com
    Validity
        Not Before: Aug  1 00:00:00 1996 GMT
        Not After  : Dec 31 23:59:59 2020 GMT
    Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division, CN=Thawte Premium Server
CA/Email=premium-server@thawte.com
-----END CERTIFICATE-----

```

```

-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=development, CN=CryptSoft Dev CA
    Validity
        Not Before: Mar 22 13:34:04 1997 GMT
        Not After  : Mar 22 13:34:04 1998 GMT
    Subject: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=development, CN=CryptSoft Dev CA
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
    Issuer: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=WORTHLESS CERTIFICAT
ION AUTHORITIES, CN=ZERO VALUE CA - DEMONSTRATION PURPOSES ONLY
    Validity
        Not Before: Apr  3 13:22:54 1997 GMT
        Not After  : Apr  3 13:22:54 1998 GMT
    Subject: C=AU, ST=Queensland, L=Brisbane, O=CryptSoft Pty Ltd,
OU=WORTHLESS CERTIFICA
TION AUTHORITIES, CN=ZERO VALUE CA - DEMONSTRATION PURPOSES ONLY
-----END CERTIFICATE-----

```

- CSCdz27870

**Symptom:** The following systems that contain a FC2-133 card print repeated error messages to the boot log when they are booted: CE-510, CE-565, CE-7305, and CE-7325.

**Condition:** When WWN level zoning or port level zoning is configured on a Fibre Channel switch, the above Content Engine systems print repeated error messages to the boot log when systems are booted.

**Workaround:** Insert the FC2-133 card on the Content Engine. Wait until the Fibre Channel switch polls and recognizes the new device. Add the new Content Engine to the zones from the switch graphical user interface and reboot the Content Engine. Or, disable zoning temporarily, reboot the Content Engine and then add the zoning.

The workaround is a required procedure for zoning enabled situations. If zoning is not enabled, then this symptom does not occur. Simply power down the system, insert the FC2-133 card and reboot the Content Engine.

- CSCdz30808

**Symptom:** A “404 Object Not Found” response appears in the client browser.

**Condition:** This response occurs during the following conditions:

- Request translation is done with the origin server IP
- WCCP setup is configured
- The Content Engine to which the request is being redirected does not have the pre-positioned content (The Content Engine is not subscribed to the channel.)

**Workaround:** Make sure that the request is redirected to the Content Engine that contains the pre-positioned content.

- CSCdy34699

**Symptom:** Media does not play successfully. Windows Media Player experiences client errors and forced reloads.

**Condition:** This occurs when you are configuring manual proxy to play pre-positioned content using HTTP.

**Workaround:** Configure the browser proxy settings even if you are using Windows Media Player to play the media directly.

- CSCdz35191

Symptom: For prepositioned windows media content, if the content is defined to be HTTP play from the manifest file and the NTLM authentication is enabled from the Content Distribution Manager. The Content Engine fails to handle the authentication with the original server properly. You are repeatedly prompted for an username and password although you have already entered the proper username and password.

Condition: This is a limitation and will be resolved in a future release.

Workaround: Choose one of the following options to avoid this problem.

- Use MMS play rather than HTTP play in the manifest file definition.
- Use HTTP play, but disable authentication.
- Use HTTP play with Basic authentication.

- CSCdz41188

Symptom:Cache process automatically reboots after running for three months

Condition:Cache process automatically reboots when it runs for a relatively long time under production traffic.

Workaround:The cache process is automatically restarted by a node manager.

- CSCdz43701

Symptom: When you change a playlist's schedule while that playlist is currently active for tv-out playback, then all tv-out playback may stop. This generally occurs when that playlist's schedule is still applicable to the current time.

Condition: This occurs on CE -510 or CE-565 platforms which have optional AV decoder cards installed and are running ACNS 5.0 software.

Workaround: Change playlist schedules while they are not currently active for tv-out playback. Optionally, an active playlist's schedule can be first changed to unscheduled, and then changed to the desired play time. However, note that this may cause some interruption in the tv-out playback.

If the problem has already occurred, then you need to disable and then re-enable tv-out service on the Content Engine. To do this, enter the following CLI commands:

```
(config)# no tvout enable
```

```
(config)# tvout enable
```

- CSCdz48578

Condition: The problems occurs when in an HTTP to the CE HTTP proxy in the following scenario: Client issued an IMS request to the Content Engine with a Pragma: no-cache header. The object is in the cache and the Content Engine determines it needs to revalidate the object because of the Pragma: no-cache. The Content Engine sends an IMS to the server and receives a 304 response. The Content Engine sends a 304 to the client.

Symptom: Under this condition, when using the Squid transaction log format, the Content Engine logs the transaction in the HTTP transaction log as a TCP\_CLIENT\_REFRESH\_MISS/304. This is not considered a problem because this is the correct transaction log code based on the Squid documentation.

However, if a third party transaction log reporting tool is considering a TCP\_CLIENT\_REFRESH\_MISS transaction a Content Engine cache miss, then the cache hit rate it reports will not be accurate.

Workaround: Since this is not a problem on the Content Engine, there is no workaround required. Note that third party transaction log reporting tools should consider a TCP\_CLIENT\_REFRESH\_MISS as a Content Engine cache miss if they are not doing so already.

- CSCdz62824

Symptom: WMT content is not served.

Condition: When using direct manual proxy or WCCP transparent proxy to serve pre-positioned WMT content from a Content Engine (assuming no authentication is required), the origin server does not need to be up and running. However, when using Layer 4 transparent proxy to serve content from a Content Engine, the origin server has to be up and running, or the content cannot be served.

Workaround: Make sure the origin server is up and running.

- CSCdz67216

Condition: You use the cli to assign a device group to a channel, and multiple CEs have insufficient space for the channel quota.

Symptom: CLI will not allow you to assign the group, but will report only the first ce with insufficient space. You may have to try a few times.

Workaround: Either verify which ce's have space before you call the cli, or make sure device groups contain similar ce's and are assigned consistently to device groups.

- CSCdz67759

Condition: More than one Content Engine is frequently sending Content Distribution Manager system messages.

Symptom: The system message log page can take up to one minute to appear.

Workaround: Currently there is no known workaround.

- CSCdz68730

Symptom: Processes may restart automatically.

Condition: Processes restart while system is acquiring a large amount of content.

Workaround: Currently there is no known workaround.

- CSCdz69318

Condition: A client browser requests pre-positioned content from CDNFS.

Symptom: The last modified date value returned in the response does not match that of the pre-positioned content "Last-Modified" attribute. This will cause a "200 OK" to be returned to the client instead of a "304 Not Modified" if the client browser issues an "If-Modified-Since" conditional GET request and the pre-positioned content is in the CFS cache, but needs revalidation because it is old.

Workaround: Currently there is no known workaround.

- CSCdz70986

Symptom: Content Distribution Manager is responding slowly.

Condition: Multiple nodes on the network are communicating with the Content Distribution Manager by sending system messages as well as requesting full updates. A .cms on a node shuts down 10 consecutive StoreExceptions are detected, and therefore stops the flood of traffic from a troubled nodes to the Content Distribution Manager.

Workaround: Content Distribution Manager administrator needs to observe the activities in the system log GUI screen and correct events when necessary.

- CSCdz71976
 

Symptom: The following error message appears in the Content Distribution Manager log:  
“Unexpected critical error on the node %CE-SCHED-2-189000: One worker thread is gone! Error code 3. We are quitting.”

Condition: After running the **copy ftp install** command on the Content Engine, reloading the Content Engine, and starting WMT and RealNetworks streaming on the Content Engine.

Workaround: Currently there is no known workaround.
- CSCdz74319
 

Condition: A DNS failure occurs.

Symptom: You will see a DNS failure while attempting to access a web site.

Workaround: Use the browser Reload function.
- CSCdz75101
 

Condition: The Content Distribution Manager accepts invalid IP address's that you enter in the NTLM server.

Symptom: Error alert on system logs page indicates the failure to configure an IP address.

Workaround: Make sure you are enter a valid IP address.
- CSCdz75188
 

Symptom: If you use the Content Router for routing WMT content and the content is not yet replicated to a Content Engine, and the playback request on the cr-fqdn is redirected to a Content Engine, then the Content Router returns an error instead of proxying the request from the origin server.

Condition: This occurs in ACNS 5.0 software when the following circumstances have occurred:

  - Administrator publishes an incorrect URL.
  - Administrator publishes a URL without first prepositioning the content.

Workaround: Publish the CR-fqdn URL only after content has been fully replicated on the Content Engine.
- CSCdz76658
 

Symptom: After removing the primary IP address, the **show running-config** command output shows that the interface is in shutdown status. However, you may be able to ping external hosts.

Condition: A FastEthernet/GigabitEthernet interface originally has the primary IP address and a secondary IP address configured, and the primary IP address has been removed.

Workaround: Shut down the interface again using the **shutdown** command in the interface configuration submode.
- CSCdz77130
 

Condition: When handling a large amount of I/O activity, the disk controller will, in rare situations, stop generating interrupts, which halts all disk activity.

Symptom: Anything that accesses the disk will freeze. Syslog cannot write to disk, so anything that writes to syslog will also freeze. The user will probably not be able to login, as Telnet cannot demand-page in its executable.

Workaround: Currently there is no known workaround.

- CSCdz77555
 

Symptoms: Windows Media Player 6.4 only supports two levels of asx redirect. As a result, in a NATed network, the Content Router can only redirect the user request to only one Content Engine when the Content Engines are behind the NAT (rather than redirect the request further to the Content Engine closest to the client.)

Condition: The problem is more of a concern if many Content Engines are behind the NAT because our WMT redirection scheme ended at the first Content Engine behind the NAT.

Work around: Currently there is no known workaround.
- CSCdz80600
 

Symptom: When you downgrade ACNS 5.0 software to ACNS 4.2 software, the **show rtsp** command does not appear in ACNS 4.2 software.

Condition: The RTSP redirectory and REAL PROXY are tied together in ACNS 4.2 software. If Real Proxy is not enabled, then the **show rtsp** command does not show incoming port information for the rtsp redirector. Either both (Real Proxy & rtsp redirector) are running or both are not running.

Workaround: Currently there is no known workaround.
- CSCdz80758
 

Condition: A wrong version was entered into the upgrading meta file.

Symptom: The error message “upgrade Failed” appears in the Content Distribution Manager GUI Devices > Content Engine Status field although the Content Engine was upgraded successfully.

Workaround: Change the version of meta file to a correct version.
- CSCdz88110
 

Symptom: The Content Router does not recognize any Content Engines. No Content Engines show when you use the **show content-routing routes** command.

Condition: When the Content Router's IP address is changed and the Content Engines are not aware of this change. Thus, the Content Engines are sending keep-alives to the wrong address, and the Content Router does not know that any of them are alive.

Workaround: On the Content Router, use the **no cms enable** configuration command followed by the **cms enable** configuration command.
- CSCdz89825
 

Symptom: The BIOS configuration utility and BIOS boot menu cannot be accessed from the console because the F1 and F12 keys do not work properly.

Condition: The BIOS configuration utility and BIOS boot menu cannot be accessed using the F1 and F12 keys from a serial console. However, the F1 and F12 keys work when used from an attached keyboard.

Workaround: Use ESC-1 instead of F1 and ESC-@ instead of F12 on the CE-510 and CE-565 platforms. Note that the F1 and F12 keys work on the CE-7305 and CE-7325 platforms that have a serial console and a directly attached keyboard.
- CSCdz89924
 

Symptom: All users see the following error message on the Windows Media Play when playing any WMT stream:

“There is insufficient bandwidth available to fulfill the request.”

Condition: This condition occurs when “wmt evaluate” is first configured and the Content Engine has never been reloaded with the running configuration copied to the startup configuration.

Workaround: There are 3 possible workarounds.

1. The simplest workaround is to reload the Content Engine if this is feasible. Save the running configuration to the startup configuration and the reload the Content Engine using the following CLI Exec commands.

```
ContentEngine# copy running-config startup-config
ContentEngine# reload
```

2. If a reload of the Content Engine is not feasible, another workaround is to explicitly set the WMT bandwidth limit in the running configuration using the **bandwidth** configuration command.

To determine the maximum bandwidth allowed during evaluation for your hardware platform, run the **show wmt** Exec command:

```
ContentEngine# show wmt
```

In the command output, look at the following line and note the value of “N”:

```
WMT max bandwidth limit enforced during evaluation: "N" Kbits/sec
```

To explicitly configure the maximum bandwidth allowed for all time slots, run the following config command. The following example uses 168000 as the value for “N”:

```
ContentEngine(config)# bandwidth all 168000 wmt start-time Sunday 00:00 end-time
Saturday 23:59
```

To confirm the bandwidth has been set, run the **show bandwidth** Exec command to verify the output.

```
ContentEngine# show bandwidth
```

```
-----
MODULE           Bandwidth   Start Time           End Time
                  Kbps
-----
wmt              168000      Sunday 00:00        Saturday 23:59
```



**Note** It is not required to save this bandwidth configuration to the startup configuration for proper behavior after the next Content Engine reload as long as the **wmt evaluate** has been copied to the startup configuration before the next reload. If the bandwidth command is already being used for some time slots, then the workaround is to configure only the unused time slots with the maximum allowed bandwidth.

3. Another workaround is to purchase a permanent license key for WMT from Cisco if you are ready to purchase the feature.

- CSCea45436

Symptom: SSH to the device does not function after you upgrade from ACNS 4.2 software to ACNS 5.0 software.

Condition: This only occurs as a result of an upgrade, which installs a new version of SSH requiring an additional key to be generated.

Workaround: Enable Telnet or have console access to the device before upgrading it, so you can connect in after the upgrade to re-generate the SSH keys.

- CSCin13785

Symptom: When overlapping playlist schedules of different playlists where a subsequent playlist preempts playback another playlist, that playlist may not resume playback after the completed playback of the subsequent playlist.

Condition: This occurs on any AV model Content Engine running ACNS 4.2 or 5.0 software. Playlists are configured to Play Once and Stop and have overlapping schedules.

Workaround: Currently there is no known workaround.
- CSCin25967

Symptom: Querying `cdpInterfaceEnable` MIB variable returns nothing

Condition: This occurs on a CE-7320 that is running ACNS 5.0.x software.

Workaround: You can retrieve the same information by running the **show cdp interface** CLI command.
- CSCin28274

Symptom: If a user has configured one invalid and one valid FTP server for transporting logs, under certain conditions when you run the **show stat translog** command, the valid server appears twice. For example, a duplicate entry for the valid FTP server appears twice.

Condition: This symptom occurs on systems running ACNS 5.0 software.

Workaround: Run the **clear stat trans** command to clear duplicate entries.
- CSCin30153

Symptom: Client does not receive the object that is being served.

Condition: When the Websense server not reachable and the Websense timeout value is large (close to or above 60 seconds).

Workaround: Configure the Websense server timeout value to 60 seconds or smaller.
- CSCin30451

Symptom: When overlapping playlist schedules of different playlists where a subsequent playlist preempts playback another playlist, that playlist may not resume playback after the completed playback of the subsequent playlist.

Condition: This occurs on any AV model Content Engine running ACNS 4.2 or 5.0 software. Playlists are configured to Play Once and Stop and have overlapping schedules.

Workaround: Currently there is no known workaround.
- CSCin30480

Symptom: If you use the Content Router for routing WMT content and the content is not yet replicated to a Content Engine, and the playback request on the `cr-fqdn` is redirected to a Content Engine, then the Content Router returns an error instead of proxying the request from the origin server.

Condition: This occurs in ACNS 5.0 software when the following circumstances have occurred:

  - Administrator publishes an incorrect URL.
  - Administrator publishes a URL without first prepositioning the content.

Workaround: Publish the `CR-fqdn` URL only after content has been fully replicated on the Content Engine.

## Documentation Updates

The ACNS Software, Release 5.0 documentation requires the following updated information.

### Changes to the *Cisco ACNS Software Deployment and Configuration Guide*

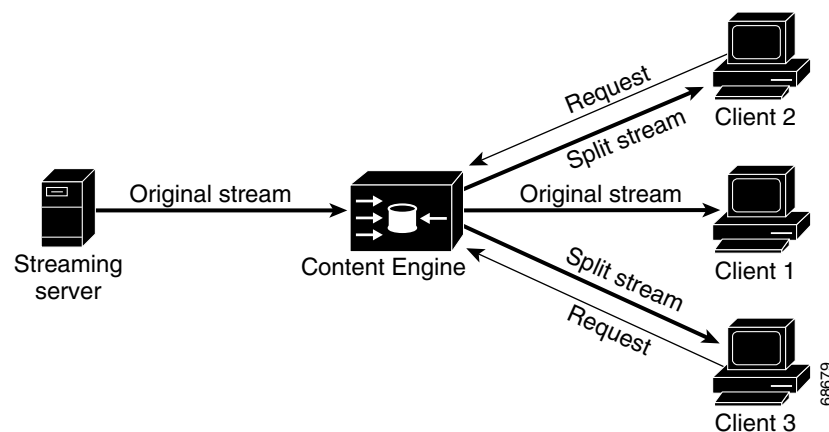
The “Configuring WMT Multicasting” section in the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.0* has been changed to “Configuring WMT Live Splitting for Unicast and Multicast Transmissions” and contains the following changed information:

#### Configuring WMT Live Splitting for Unicast and Multicast Transmissions

Splitting is a method of sending live data transmissions across the internet to a proxy edge device. The live stream is then fanned out to multiple downstream clients using unicast or multicast. (See [Figure 9-25](#).)

The WMT-enabled Content Engine acts as a proxy for the streaming server or broadcast server and replicates the stream to local users. Splitting the stream at the Content Engine proxy is better than splitting it at the server, because the proxy is closer to the clients, thereby potentially saving considerable network bandwidth between the client and the server.

**Figure 9-25** Live Splitting



When a client requests a publishing point on a server (without specifying an ASF file), then the Content Engine dynamically creates an alias file that references the remote server. All further requests to that station are served by splitting the stream. Note that when the first client (Client 1) that requested the original stream disconnects from the network, the proxy continues to serve the other clients (Client 2 and Client 3), until all clients disconnect from the network.



#### Note

Live splitting is supported for different data packet transport protocols (HTTP, MMS TCP [MMST], MMS UDP [MMSU], and IP multicast).

## Live Stream Splitting Scenarios

Based on the capabilities and limitations of the network, a Content Engine can receive and deliver WMT streaming content through IP multicast or unicast transmissions in the following four combinations:

- Unicast-In Multicast-Out
- Multicast-In Multicast-Out
- Multicast-In Unicast-Out
- Unicast-In Unicast-Out

The two WMT multicast-out features combined enable you to receive and deliver WMT streaming media content through IP multicasting, and to do conversions from multicast to unicast (and vice versa).



### Note

You must accept a WMT license and enable WMT on the Content Engine and Device Groups before you can use enable WMT multicasting in your ACNS 5.x network.

Each station needs a multicast IP address. You must enter a valid Class D IP address multicast address in the range 224.0.0.0 to 239.255.255.255, except for the reserved IP ranges based on RFC 1700 and related documents as follows:

- 224.0.0.0 to 224.0.6.255
- 224.0.13.0 to 224.0.13.255
- 224.1.0.0 to 224.2.255.255
- 232.0.0.0 to 232.255.255.255



### Note

You must choose a multicast IP address that does not conflict internally within the same multicast-enabled network configuration. This multicast IP address is not related to the IP address of the Content Engine.

The allowed multicast port range defined ranges from 1 through 65535. However, the multicast-enabled network may impose certain restrictions on your choice of port. Normally, port numbers below 1024 should be avoided, but the Content Engine does not enforce any restrictions.



### Note

If a live stream is interrupted at the server side, you must stop the multicast station and then restart the same station to resume live multicasting.

## Omissions

The following information was omitted from the *Cisco ACNS Software Deployment and Configuration Guide, Release 5.0*.

## Configuring Unicast-In Unicast-Out

In this scenario, unicast-in unicast-out provides a point-to-point connection between the client and the Content Engine. The Content Engine in turn makes a single connection to the media server. Multiple requests for the same stream can be split by the Content Engine so that each client receives a distinct data stream directly from the Content Engine, while the Content Engine maintains its single stream connection to the media server. The client can request a stream that contains either stored or live content.

The advantage of unicasting when streaming media over a network is that only a single stream needs to be pulled over the network between the origin server and Content Engine, but that stream can be delivered to multiple clients in a non-multicast environment. A server running Windows Media Services can provide a unicast video stream to multiple clients through a single stream delivered to the Content Engine. Those clients can take advantage of the VCR-like controls in the Windows Media Player to pause the stream or to skip backward or forward (in the case of stored content [video-on-demand]).

There are two ways to configure unicast-in unicast-out:

- By live splitting without any configuration. In this case, the Content Engine acts as a proxy. When clients request the same unicast URL, the Content Engine proxy automatically splits the stream from the source to the clients.
- By configuring the Content Engine with a broadcast alias. In this case, a client makes the request to the Content Engine as if it were the Windows Media Server and the Content Engine checks to see whether the incoming stream is present. If it is, then the Content Engine joins the stream and splits it to the new client. If the request is the first client request for this stream, the Content Engine sends the request out to server and then serves it to the new client.

To enable WMT services for unicast-in unicast-out, follow these steps:

- 
- Step 1** From the Content Distribution Manager GUI, choose **Devices > Content Engines**.
- Step 2** Click the **Edit** icon next to the Content Engine that you want to configure. The Contents pane appears on the left.
- Step 3** From the Contents pane, choose **WMT > WMT Broadcast Alias**. (See [Figure 9-28](#)).
- Step 4** Click the **Create New WMT Broadcast Alias** icon.
- Step 5** In the Broadcast Alias field, enter an alias name for the source URL.
- Step 6** In the Source URL field, enter the source URL of the content to be used for the broadcast. For example:  
`mms://wms.company.com/cotv`  
 where `wms.company.com` is the name of the Windows Media Server, and `cotv` is the name used when the broadcast alias is created. The MMS protocol is used to retrieve the stream.
- Step 7** Click **Submit** to save the settings.
- Step 8** Open your Windows Media Player and choose **File > Open URL**. Enter the following URL:  
`mms://CEIPaddress/broadcast1`  
 where `CEIPaddress` is the IP address or domain name of the Content Engine, and `broadcast1` is the alias name used in [Step 5](#).
- Step 9** Click **OK**. The Windows Media Player should receive the MMS media source specified in [Step 6](#).
-

## SmartFilter and the No-Auth Rule Interaction

The **no-auth** rule permits specific login and content requests to bypass authentication and authorization features such as LDAP, RADIUS, SSH, or TACACS+. For example, any requests from the source IP address (src-ip) of 172.16.53.88 are not authenticated.

```
ContentEngine(config)# rule enable
ContentEngine(config)# rule action no-auth pattern-list 1 protocol all
ContentEngine(config)# rule pattern-list 1 src-ip 172.16.53.88 255.255.255.255
```

If ACNS software is configured for authentication and SmartFilter URL filtering, requests that are allowed to bypass authentication will also bypass the URL filter.

## Changes to the *Cisco ACNS Software Caching Configuration Guide*

The “Configuring WMT Multicasting” section in Chapter 9 of the *Cisco ACNS Software Caching Configuration Guide, Release 5.0* has been changed to “Configuring WMT Live Splitting for Unicast and Multicast Transmissions.”

The following section replaces the section titled “Configuring WMT Multicasting” in Chapter 9.

# Configuring WMT Live Splitting for Unicast and Multicast Transmissions

Based on the capabilities and limitations of the network, a Content Engine can receive and deliver WMT streaming content through IP multicast in the following four combinations:

- Configuring Unicast-In Multicast-Out
- Configuring Multicast-In Multicast-Out
- Configuring Multicast-In Unicast-Out
- Configuring Unicast-In Unicast-Out

The unicast-in multicast-out multicast delivery feature enables you to distribute streaming media efficiently by allowing different devices on the IP multicast to receive a single stream of media content from the Content Engine simultaneously. This can save significant network bandwidth consumption, because a single stream is sent to many devices, rather than sending a single stream to a single device every time that this stream is requested. This multicast delivery feature is enabled by setting up a multicast address on the Content Engine to which different devices, configured to receive content from the same channel, can subscribe. The delivering device sends content to the multicast address set up at the Content Engine, from which it becomes available to all subscribed receiving devices.

The multicast-in multicast-out multicast receive feature enables you to receive multicast WMT streams delivered through IP multicasting, then relay them to end users through another delivery channel (unicast or multicast). The two WMT multicast-out features combined enable you to receive and deliver WMT streaming media content through IP multicasting, and to do conversions from multicast to unicast (and vice versa).

The multicast-in unicast-out scenario enables you to create a broadcasting publishing point to deliver an incoming stream live to requesting clients using multicast as the source of the streaming media.

The unicast-in unicast-out scenario provides a point-to-point connection between the client and the Content Engine. The Content Engine in turn makes a single connection to the media server. Multiple requests for the same stream can be split by the Content Engine so that each client receives a distinct data stream directly from the Content Engine, while the Content Engine maintains its single stream connection to the media server. The client can request a stream that contains either stored or live content.

## Omissions from the *Cisco ACNS Software Caching Configuration Guide*

The following information was omitted from the *Cisco ACNS Software Caching Configuration Guide*. It should reside in Chapter 9 immediately following the “Configuring Multicast-In Unicast-Out” section.

### Configuring Unicast-In Unicast-Out

In this scenario, unicast-in unicast-out provides a point-to-point connection between the client and the Content Engine. The Content Engine in turn makes a single connection to the media server. Multiple requests for the same stream can be split by the Content Engine so that each client receives a distinct data stream directly from the Content Engine, while the Content Engine maintains its single stream connection to the media server. The client can request a stream that contains either stored or live content.

The advantage of unicasting when streaming media over a network is that only a single stream needs to be pulled over the network between the origin server and Content Engine, but that stream can be delivered to multiple clients in a non-multicast environment. A server running Windows Media Services can provide a unicast video stream to multiple clients through a single stream delivered to the Content Engine. Those clients can take advantage of the VCR-like controls in the Windows Media Player to pause the stream or to skip backward or forward (in the case of stored content [video-on-demand]).

There are two ways to configure unicast-in unicast-out:

- By live splitting without any configuration. In this case, the Content Engine acts as a proxy. When clients request the same unicast URL, the Content Engine proxy automatically splits the stream from the source to the clients.
- By configuring the Content Engine with a broadcast alias. In this case, a client makes the request to the Content Engine as if it were the Windows Media Server and the Content Engine checks to see whether the incoming stream is present. If it is, then the Content Engine joins the stream and splits it to the new client. If the request is the first client request for this stream, the Content Engine sends the request out to server and then serves it to the new client.

To enable WMT services for unicast-in unicast-out, follow these steps:

- 
- Step 1** Enable the Content Engine graphical user interface (GUI) with the **gui-server enable** global configuration command. Then configure the graphical user interface server port with the **gui-server port** command:
- ```
ContentEngine(config)# gui-server enable
ContentEngine(config)# gui-server port 8002
```
- In this example, the Content Engine graphical user is enabled on the default port number 8002.
- Step 2** From the Content Engine GUI, choose **Caching>WMT-Streaming**. The WMT Streaming window appears.
- Step 3** Click **WMT Config**. The WMT Configurations window appears.
- Step 4** Choose the Broadcast Unicast Publishing link. The WMT Broadcast Unicast Publishing window appears.

- Step 5** In the Alias field, enter a broadcast alias for the broadcast live configuration.
- Step 6** In the Source field, enter the broadcast source for the broadcast live configuration. Configure in the following format. For example:
- ```
<protocol>://<server-name>:<port-num>/<path>/<file-name>
```
- where:
- <protocol> is either mms or http
  - <path> is the full pathname
  - <port-num> is the port number. 1755 is the default.
  - <file-name> is a media file name if the file is in the content root directory
- For example:
- ```
mms://w2k-mediaserver.cisco.com/welcome.asf
http://w2-mediaserver.cisco.com/live/liveprogram1
```
- Step 7** Click **Update** to save the settings.
- 

## Related Documentation

Your product shipped with a minimal set of printed documentation, as well as a Documentation CD. The printed documentation provides enough information for you to install and initially configure your product. The CD contains additional product documentation (user guides, configuration manuals, and so forth), which you can access and print out.

### Product Documentation Set

In addition to these release notes, the product documentation set includes:

- *Documentation Guide*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*
- *Cisco Content Delivery Networking Products Getting Started Guide*

Refer to the *Documentation Guide* for a complete documentation roadmap and URL documentation links for this product.

### Hardware Documentation

- *Cisco Content Engine 7305 and 7325 Hardware Installation Guide*
- *Installing the Cisco Content Engine 7305 and 7325*
- *Installing Field-Replaceable Units in the Cisco Content Engine 7305 and 7325*
- *Cisco Content Engine 7320 Product Description Note*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *Installing the Cisco Content Engine 510 and 565*
- *Installing Field-Replaceable Units in the Cisco Content Engine 510 and 565*
- *Cisco Storage Array Installation and Configuration Guide*
- *Release Notes for Cisco Content Delivery Manager 4630*
- *Cisco Content Distribution Manager 4650 Product Description Note*

- *Cisco Content Distribution Manger 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*
- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Release Notes for the Cisco Content Engine 500 Series*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*

#### Software Documentation

- *Cisco ACNS Software Deployment and Configuration Guide, Release 5.0*
- *Cisco ACNS Software Caching Configuration Guide, Release 5.0*
- *Cisco ACNS Software Command Reference, Release 5.0*
- *Cisco ACNS Software Maintenance and Troubleshooting Guide*
- *Cisco ACNS Software Migration Guide, Release 5.0*
- *Cisco ACNS Software API Guide, Release 5.0*
- *SmartFilter for Cisco Content Engine User's Guide, Release 3.1*

#### Online Help

Content Distribution Manager GUI online help system

## Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

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

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Documentation CD-ROM

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

Registered Cisco.com users can order the Documentation CD-ROM (product number DOC-CONDOCCD=) through the online Subscription Store:

<http://www.cisco.com/go/subscription>

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

## Obtaining Technical Assistance

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

## Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

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

## Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC website, go to this URL:

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

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

<http://tools.cisco.com/RPF/register/register.do>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/en/US/support/index.html>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

## Cisco TAC Escalation Center

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

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

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

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

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:  
[http://www.cisco.com/en/US/products/products\\_catalog\\_links\\_launch.html](http://www.cisco.com/en/US/products/products_catalog_links_launch.html)
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:  
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco monthly periodical that provides industry professionals with the latest information about the field of networking. You can access *Packet* magazine at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac114/about\\_cisco\\_packet\\_magazine.html](http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_packet_magazine.html)
- *iQ Magazine* is the Cisco monthly periodical that provides business leaders and decision makers with the latest information about the networking industry. You can access *iQ Magazine* at this URL:  
[http://business.cisco.com/prod/tree.taf%3fasset\\_id=44699&public\\_view=true&kbns=1.html](http://business.cisco.com/prod/tree.taf%3fasset_id=44699&public_view=true&kbns=1.html)
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in the design, development, and operation of public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:  
[http://www.cisco.com/en/US/about/ac123/ac147/about\\_cisco\\_the\\_internet\\_protocol\\_journal.html](http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html)
- Training—Cisco offers world-class networking training, with current offerings in network training listed at this URL:  
[http://www.cisco.com/en/US/learning/le31/learning\\_recommended\\_training\\_list.html](http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html)

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratum, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0301R)

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

