



Release Notes for Cisco ACNS Software, Release 5.2.7

August 4, 2005

ACNS Build 5.2.7-b7



Note

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

Contents

These release notes contain information about the Cisco Application and Content Networking System (ACNS) 5.2.7 software. These release notes describe the following topics:

- [Introduction, page 2](#)
- [New and Changed Information, page 3](#)
- [Caveats, page 7](#)
- [Documentation Updates, page 33](#)
- [Related Documentation, page 41](#)
- [Obtaining Documentation, page 42](#)
- [Documentation Feedback, page 43](#)
- [Cisco Product Security Overview, page 43](#)
- [Obtaining Technical Assistance, page 44](#)
- [Obtaining Additional Publications and Information, page 46](#)



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

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Introduction

The ACNS software combines the technologies of demand-pull caching and pre-positioning for accelerated delivery of web applications, objects, files, and streaming media. The ACNS software runs on Cisco Content Engines, Content Distribution Manager, and Content Router hardware platforms.

These release notes are intended for administrators who will be configuring, monitoring, and managing devices that are running the ACNS 5.2.7 software. These release notes describe the new product features, the supported hardware, and the open and resolved caveats regarding the ACNS 5.2.7 software release

Hardware Supported

The ACNS 5.2.7 software supports the following hardware platforms. All of the listed platforms also support the ACNS 5.1.x software except for the CE-511 and CE-566. The CE-511 and CE-566, which are both new platforms that are supported in the ACNS 5.2.x software, do not support the ACNS 5.1.x software.

- NM-CE-BP-SCSI
- NM-CE-BP-80G
- NM-CE-BP-40G
- NM-CE-BP
- CDM-4630
- CDM-4650
- CE-507
- CE-507AV
- CE-510-K9
- CE-510A-80GB-K9
- CE-510A-160GB-K9
- CE-511
- CE-566-K9
- CE-565-K9
- CE-565A-72GB-K9
- CE-565A-144GB-K9
- CE-590
- CE-590-DC
- CE-7320
- CE-7305-K9
- CE-7305A-K9
- CE-7325-K9
- CE-560
- CE-560AV
- CE-7325A-K9
- CR-4430

New and Changed Information

This section describes new and changed features in the ACNS 5.2.7 software release. It also lists the supported hardware.

Configuring TCP Memory Limits through the CLI

In the ACNS 5.1.15 software release, the ability to change the TCP memory limit on a Content Engine through the CLI was added. To support this new feature, the **tcp memory-limit** global configuration command was added.

By default, appropriate default values for the TCP memory limit are assigned for the different supported platforms and they should not be changed under normal circumstances.

To display the currently configured values for the TCP memory limit, enter the **show tcp EXEC** command.

Important Notes

This section emphasizes important information regarding the ACNS 5.2.x software:

- [Media File System Issues When Downgrading to the ACNS 5.0 Software, page 3](#)
- [Websense Issues When Downgrading to the ACNS 5.0 Software or the ACNS 5.1 Software, page 4](#)
- [Changes to WCCP Support, page 4](#)
- [Multicast File Transfer Enhancements, page 6](#)

Media File System Issues When Downgrading to the ACNS 5.0 Software

If you have configured the media file system (mediafs) with the ACNS 5.1 software and later releases, and then downgrade to the ACNS 5.0 software, the mediafs disk space assignment is lost and it reverts to the 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 the ACNS 5.1 software. Because the 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 the 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 the ACNS 5.0 Software or the 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 either the ACNS 5.0 software or the 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 the ACNS 5.2.x software to either the ACNS 5.1 software or the 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 the ACNS 5.0 software downgrade image on the Content Engine.

Changes to WCCP Support

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

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

Table 1 Supported WCCP Services with the ACNS 5.2 Software

Service Number	Service Name	Type of Service	Service Description
0	web-cache	Predefined	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. Multiple WCCP-enabled routers (those on the router list) are supported with WCCP Version 2. 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).
53	dns	Predefined	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 the resolved names for future DNS requests.
60	ftp	Predefined	Caching service that permits WCCP Version 2-enabled routers to redirect native FTP requests transparently to a single port on the Content Engine. The Content Engine retrieves the requested FTP content, stores a copy locally, and serves the requested content to the requester.

Table 1 Supported WCCP Services with the ACNS 5.2 Software (Continued)

Service Number	Service Name	Type of Service	Service Description
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 (acting as a 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 the 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 the 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).</p>
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 (port 554), configure a user-defined WCCP service (services 90 to 97).</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.</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.</p>

Table 1 Supported WCCP Services with the ACNS 5.2 Software (Continued)

Service Number	Service Name	Type of Service	Service Description
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 on which the WCCP Version 2-enabled router will support WCCP redirection 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.</p>
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).
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).

Multicast File Transfer Enhancements

The ACNS 5.2 software supports new multicast file transfer features that enhance the reliability and performance of multicast file distribution in the ACNS 5.2 network. In earlier ACNS software releases (the ACNS 5.0 software and ACNS 5.1 software), the file transfer session depended on a window of time to resend the missing packets. The sender had to transmit the packets within this window of time for each retransmission request (NACK) from receiver Content Engines. If a multicast receiver joined the session too late and missed blocks of data that were outside the transmission window, the sender would not resend the missing blocks. The receiver could not receive the entire file, and the transmission failed. The receiver had to wait until a subsequent carousel pass to recover the missed files. The receiver could only receive the entire file or nothing. A slow receiver often failed to receive a large file if the receiving rate lagged behind the sending rate.

The multicast file transfer enhancements in the ACNS 5.2 software resolve these issues by eliminating the window of time for file transmissions. This feature is called checkpoint. Checkpoint allows the sender to divide the transferring file into blocks and to retransmit any and all blocks until the transfer session ends. At any time during the transfer session, a receiver can request retransmission of any block that it has missed. Also, receiver Content Engines can receive the blocks of a transfer in any order. Data transmission can occur over a longer period, and receivers can recover missed data blocks to successfully complete the transfer in most situations. Thus, file transfers are much more resistant to loss of data.

This feature also solves the problem of a multicast receiver joining a transfer session late. (In an extreme example, even if a receiver joins so late that the sender has multicast nearly all of a very large file, the receiver can still receive the data. Also, the receiver can request retransmission for all the blocks that it has missed.) Even if a receiver goes offline and restarts during a transfer, it can recover missing data without requesting retransmission of the blocks that it has already received.



Note

Because of these enhancements, receivers using the ACNS 5.2 software *cannot* interact with senders using the ACNS 5.0 or 5.1 software. The ACNS 5.2 multicast receiver will ignore files sent from an ACNS 5.0 or 5.1 multicast sender. However, an ACNS 5.2 multicast sender can interoperate with the ACNS 5.0 or 5.1 multicast receivers because the software detects the lower software version and disables the checkpoint feature. Therefore, we recommend that you upgrade your multicast sender to the ACNS 5.2 software first and then upgrade your receivers to the ACNS 5.2 software.

Caveats

This section lists and describes the open and resolved caveats in the ACNS 5.2.7 software. Caveats describe unexpected behavior in the ACNS 5.2.7 software. Severity 1 caveats are the most serious; Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

Open Caveats—ACNS 5.2.7 Software

This section lists caveats that have not been resolved in the ACNS 5.2.7 software. The open caveats are grouped into two categories:

- [Open ACNS-IP/TV 5.2.7 Software Integration Caveats, page 7](#)
- [Other Open ACNS 5.2.7 Software Caveats, page 8](#)

Open ACNS-IP/TV 5.2.7 Software Integration Caveats

This section lists and describes the caveats that are open in the ACNS 5.2.7 software and are related to ACNS-IP/TV software integration:

- CSCec52492

Symptom: Requests for on-demand programs from clients in an ACNS network are sent to IP/TV Program Manager. IP/TV Program Manager treats these requests as standalone IP/TV on-demand program requests and directs them to the IP/TV Broadcast Server that can serve the request. This situation causes bandwidth issues and affects the functioning of IP/TV Server.

Condition: This problem occurs when IP/TV has been integrated in an ACNS network. It occurs when requests for on-demand programs that are exported to the ACNS network reach IP/TV Program Manager instead of being routed to the Content Engine that has the programs. This problem is related to a routing failure or a routing error.

Workaround: Configure routing correctly in ACNS networks so that on-demand requests are directed to the nearest Content Engine that is capable of serving the program. Alternatively, you can change the proximity settings in IP/TV Program Manager so that it does not redirect the on-demand program requests to IP/TV Broadcast Servers. However, the second approach can also affect the serving of standalone on-demand programs.

Other Open ACNS 5.2.7 Software Caveats

This section lists and describes the caveats that are open in the ACNS 5.2.7 software and are not related to ACNS-IP/TV software integration:

- 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 contains 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 software 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 any errors occur during certificate verification by the ACNS acquirer, then content from that site will not be acquired. With weak authentication, certain errors (for example, a certificate has expired, certificate is not yet valid, and a subject issuer mismatch has occurred) 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 to install on their origin servers. Note that the certificate list differs based on the version of the ACNS software. For the ACNS 5.1.x software and later releases, refer to the certificate list in the *Cisco ACNS Software Upgrade and Maintenance Guide, Release 5.x*.
- CSCea51815

Symptom: When a Content Engine model CE-565 is attached to a Storage Array SA-7 device, if too large a cache file system (cfs) partition is configured, and a combined streaming and caching workload is used, then a lower HTTP performance is observed.

Condition: This problem occurs when the CE-565 has Windows Media Technologies (WMT) enabled, a combined streaming and caching workload is used, and the Content Engine is attached to an SA-7 device.



Note The Storage Array device is used for the cache file system (cfs).

Workaround: Allocate less space to the cfs if a Storage Array is attached to the Content Engine.

- CSCec52221

Symptom: Windows Media Technologies (WMT) is enabled with no media file system (mediafs) after you downgrade from the ACNS 5.1b300 software to the ACNS 5.0.7b8 software.

Condition: This problem occurs if you upgrade from the ACNS 5.0.7b8 to the ACNS 5.1bx software, configure the disk, and then downgrade to the ACNS 5.0.7b4 software.

Workaround: Reconfigure the disk with a mediafs partition and reload the software.
- CSCec52319

Symptom: Using FTP inside the .meta file to have the Content Engine obtain the .bin file for a Content Distribution Manager GUI-initiated upgrade is unsuccessful if the user's home directory differs from the FTP root.

Condition: Either you receive an error in the Content Distribution Manager GUI when you are creating the definition for the upgrade (when the .bin file does not exist in the user's home directory), or the Content Engine displays an error message on the upgrade (when the .bin file does not exist in the FTP root directory).

Workaround: Copy the .bin file to both the FTP root and the user's home directory, or use a user whose home directory is the FTP root.
- CSCed34718

Symptom: If you edit a file-based scheduled program and the Quality of Service (QoS) feature is configured, the revised program retains the QoS configuration even if you disable the QoS feature.

Condition: This problem occurs only with file-based scheduled programs; it does not occur with live programs.

Workaround: The only known workaround is re-creation. To remove the QoS configuration, delete the program and then re-create the program without configuring the QoS feature.
- CSCed68360

Symptom: A constant stream of bandwidth error messages (one about every 2 seconds) is reported in the syslog. As the following sample messages indicate, these messages are not very useful.

```
Feb 11 13:24:26 webcache01 bandwd: %CE-BANDWD-3-115002: BANDWD: Trying again in two seconds
Feb 11 13:24:28 webcache01 bandwd: %CE-BANDWD-3-115003: BANDWD: verification registration failed, err=30
```

Condition: None.

Workaround: There is no known workaround.
- CSCed68727

Symptom: The Content Distribution Manager only checks if coverage zone files refer to invalid Content Engines after there is a fresh import. When there is a configuration change that can cause already imported coverage zone files to refer to invalid Content Engines, the Content Distribution Manager does not check or display the correct error message until the next fresh import.

Condition: This problem occurs if there is a coverage zone configuration change that causes already-imported coverage zone files to refer to invalid Content Engines.

Workaround: There is no known workaround.

- CSCed77655

Symptom: The Content Engine stops spoofing the client IP address and uses its own IP address to fetch content from the origin server.

Condition: The **http l4-switch spoof-client-ip enable** global configuration command turns on IP spoofing on a Content Engine that is functioning as a caching engine. When a **rule action use-server** global configuration command is used, the Content Engine stops spoofing the client IP address and instead uses its own IP address to fetch the content.

Workaround: There is no known workaround.
- CSCed84227

Symptom: The network management system (NMS) host does not know where SNMP traps are coming from.

Condition: This problem occurs if there are two interfaces and you configure interface redundancy using both interfaces. You must use a dummy address for the physical addresses. You then configure a real address that floats between the two interfaces. If you then configure SNMP traps, the traps are being sourced from the dummy address and not the routable address. Therefore, the NMS host does not know where the trap is coming from.

Workaround: There is no known workaround.
- CSCee17283

Symptom: The cdnfs files are turned into directories (which are visible if you enter the **cdnfs browse EXEC** command on the Content Engine).

Conditions: This problem is rare and occurs only when the file system corruption has caused a directory entry to be a subdirectory when it should have been a file. This problem occurs only if multiple cdnfs entries are being updated and the Content Engine crashes (for example, the Content Engine crashes because of a power failure).

Workaround: Enter the **cdnfs cleanup start EXEC** command on the Content Engine.
- CSCee25042

Symptom: Even though you entered the **url-filter wmt bad-sites-deny** global configuration command on the Content Engine, the Content Engine is not filtering requests for content that is pre-positioned in its wmt_vod directory.

Condition: This problem occurs in the following situation:

 - a. You pre-position a file (for example, file.asf) on the Content Engine in its wmt_vod directory.
 - b. After pre-positioning the file, you configure the bad site list for URL filtering using `mmst://Content Engine IP address/wmt_vod/file.asf`.
 - c. A user makes a content request for this URL (that is, `mmst://Content Engine IP address/wmt_vod/file.asf`).

Workaround: Configure the bad site list using `mmst://127.0.0.1/wmt_vod/file.asf` instead of `mmst://Content Engine IP address/wmt_vod/file.asf`.

- CSCee38190

Symptom: A WMT live stream in a managed live event environment is accessible for a period longer than the scheduled duration.

Condition: This problem occurs only with WMT live programs that have unicast access enabled. In this situation, streams can be accessible for up to 24 hours after the last playtime of the event if “Auto Delete” is set to true or can be accessible indefinitely if “Auto Delete” is set to false.

Workaround: Control the live stream source through the schedule for the event. Typically, this process involves starting and stopping the WMT encoder.

- CSCee40593

Symptom: Syslog messages contain the following text:

```
uns-server: %CE-CDNFS-0-480000: uns_read_meta: WOW! url mismatch:
wanted 'URL>', saw '^C'
```

Condition: This problem occurs because of file system corruption; the cdnfs metadata files have the wrong content (the content is internally consistent but is in the incorrect file). This problem occurs infrequently. For example, it can occur if the cdnfs content is being updated and a crash occurred because of a kernel panic (which occurs infrequently).

Workaround: Although there is no known workaround to stop the syslog messages shown above, lookups for the target URL (listed in the syslog message) may succeed if the ACNS software has created a new cdnfs entry for the target URL.

You can enter the **cdnfs lookup url EXEC** command to see if the URL is found. If the URL is not found, a way to force it to be replicated is to modify the file on the origin server (for example, by entering the **touch** command on a UNIX-based origin server).

Alternatively, you can enter the **acquisition-distribution database-cleanup start** command on the affected Content Engine to query the cdnfs for all the objects that are supposed to be on the Content Engine. Missing objects should be detected and replicated.

- CSCee49106

Symptom: The content replication status can show an incorrect manifest item count.

Condition: This problem can occur if too many channels share the same content (for example, if over 100 channels share the same 30 files in each channel). Even though all 100 channels should show the 30 files that were acquired and distributed, it takes an extended period (days) before the correct manifest item count is displayed.

Workaround: Reduce the number of channels that share the same contents.

- CSCee56998

Symptom: The CPU usage on the Content Engine hits a peak of 100 percent.

Condition: This problem can occur if the internal (local) Websense server is enabled on the NM-CE-BP models.

Workaround: There is no known workaround.

- CSCee67227

Symptom: If you specify “foo” as a folder URL in the manifest file, and there is a single item redirection from foo to foo/ by the web server, the ACNS acquirer fails to process such redirections and generates a 716 error message. If you are using the quick crawl tool in the Channel Content window, some of the files also report 716 error messages.

Condition: This problem occurs if you are using the quick crawl tool and there is a single item redirect from foo to foo/. However, if foo is a link from a crawl job, single item redirections from foo to foo/ are allowed.

Workaround: Specify foo/ in the manifest file, or specify a crawl job instead of using the quick crawl tool.
- CSCee67330

Symptom: Microsoft NT LAN Manager (NTLM) authentication fails and the pop-up window is displayed again.

Condition: This problem occurs if NTLM authentication is being used and the specified domain name is longer than 50 characters.

Workaround: For NTLM authentication, use a domain controller (DC) that has a domain name shorter than 35 characters.
- CSCee68339

Symptom: Proxy requests to the Content Engine proceed to allow mode (if allow mode is enabled) or are blocked (if allow mode is disabled) when the Websense URL filtering mechanism is configured to use the local Websense server.

Because the connections from the Content Engine to the Websense server time out, all requests go to allow mode until all 40 connections are exhausted. (This situation makes it appear as if the Websense server is not responding.) After all 40 connections are attempted, the Content Engine successfully connects to the Websense server and works properly thereafter.

Condition: This problem can occur under the following conditions:

 - The Content Engine is configured to use the local (internal) Websense server for URL filtering.
 - The local Websense server is running on the Content Engine.
 - There are long periods of inactivity.
 - The cache process has difficulty connecting to the local Websense server.

Workaround: Reconfigure Websense URL filtering on the Content Engine so that the Content Engine will attempt to establish new connections to the Websense server.
- CSCee71157

Symptom: Channel routing causes loops for several Content Engines.

Condition: This problem can occur if there are Content Engines that are running the ACNS 5.1.x software or earlier, and these Content Engines are registered with a Content Distribution Manager that is running the ACNS 5.2.x software.

Workaround: Upgrade the Content Engines to the ACNS 5.2.x software. Currently, a Content Distribution Manager that is running the ACNS 5.2.x software does not propagate some configuration changes to Content Engines that are running ACNS software earlier than the ACNS 5.2.x software. Therefore, Content Engines that are running the ACNS 5.1.x software or earlier, may not recognize that the root Content Engine was changed from one Content Engine to another. Consequently, routing loops can develop within the system.

- CSCee78190

Symptom: When a root Content Engine is downgraded from the ACNS 5.2.x software to the ACNS 5.1 software, some channels are disabled and some content fails to be acquired.

Condition: This problem occurs when the manifest file URL is a Server Message Block (SMB) URL with a uniform naming convention (UNC) path format (for example, \\host\share\file), or when an item or crawl task specified in either the **src** or **start-url** attribute has a UNC path format.

Because the ACNS 5.1 software does not support SMB file acquisition, the root Content Engine running the ACNS 5.1 software is not able to fetch the manifest file or acquire content from the SMB shares.

Workaround: Either before or after you downgrade the root Content Engine from the ACNS 5.2.x software to the ACNS 5.1 software, remove the SMB URL from the Manifest URL field in the Channel configuration window of the Content Distribution Manager GUI and use a URL with supported protocols (HTTP, FTP, or HTTPS).



Note From an ACNS 5.1 Content Distribution Manager GUI, choose **Channels > Channels > Edit Channel**.

From an ACNS 5.2.x Content Distribution Manager GUI, choose **Content > Channels > Edit Channel > Channel Content**.

Edit the manifest file by removing content items and crawl tasks that have UNC formatted paths.

Use the **acquirer start-channel EXEC** command to initiate channel acquisition and verify that the workaround is successful.

- CSCee81376

Symptom: The CMS service on the Content Distribution Manager cannot start and fails to create the CMS database backup file.

Condition: This problem can occur if the ACNS network configuration is very large (for example, with 2000 configured Content Engines) and the sysfs partition is 2 GB or less.

Workaround: Create a sysfs partition that is greater than 2 GB.

- CSCee90245

Symptom: Microsoft NT LAN Manager (NTLM) authentication occurs even though you disabled it on the Content Engine.

Condition: This problem occurs very rarely. In very rare situations, even though you entered the **no ntlm server enable** global configuration command to disable NTLM proxy authentication on the Content Engine, NTLM proxy authentication is still not turned off. In such cases, NTLM authentication can still occur, although the output of the **show running EXEC** command shows that the NTLM server is not enabled on the Content Engine.

Workaround: Enter the **no ntlm server enable** global configuration command again on the Content Engine.

- CSCee92250

Symptom: ICAP-related transaction logs appear only for response modification (RESPMOD) transactions and not for request modification (REQMOD) transactions.

Condition: This problem occurs on all Content Engines that are running the ACNS 5.0 software and later releases, which have the ICAP service and ICAP transaction logging enabled.

Workaround: There is no known workaround.

- CSCee92698

Symptom: The ICAP service is enabled on the Content Engine, but the Content Engine is unable to retrieve the content.

Condition: This problem can occur if the Content Engine is running the ACNS 5.x software, and you configure two or more ICAP services to subscribe to the same vectoring point (the response modification [RESPMOD] vectoring point).

Workaround: There is no known workaround.
- CSCee92917

Symptom: A cleanup of the sysfs partition removes all pre-positioned RealMedia contents from the /local1/real_vod/ directory on the Content Engine.

Condition: This problem occurs if the sysfs partition is saturated because of the population of content in the real_vod directory.

Workaround: There is no known workaround.
- CSCef11091

Symptom: The WCCP cache farm (that is, a cluster of Content Engines that are running WCCP) is formed using the assignment method even though you specified the **mask-assignment assign-method- strict** option when configuring the WCCP service.

Condition: This problem occurs if the WCCP cache farm is associated with Cisco routers instead of switches.

Workaround: There is no known workaround. Mask assignment was only designed for Catalyst 6500 series switches and is not supported by Cisco routers.
- CSCef16345

Symptom: The stream scheduler in the edge Content Engine retrieves stale Session Description Protocol (SDP) information from its forwarder and stores it in its local1/cse_live/ucast folder if the encoding is modified through IP/TV Program Manager. All further RTSP requests are served with this stale SDP content.

Condition: This problem occurs if the stream scheduler retrieves stale SDP information from its forwarder because the program has been edited and the encoding changed for a program. This situation occurs if the Content Distribution Manager notification at the edge Content Engine triggers the stream scheduler before the same occurs at the root Content Engine. Consequently, the edge Content Engine obtains the SDP content from its forwarder, which is valid content at that moment.

Workaround: Reload the Content Engine.
- CSCef27174

Symptom: After you reload a parent Content Engine in a live split-tree type environment, its children Content Engines lose their RTSP connections to this parent and do not attempt to reestablish these RTSP connections after the parent comes back up.

Condition: This problem occurs only if the Cisco Streaming Engine is restarted on the parent Content Engine (for example, the Content Engine is reloaded, or you enter a **clear statistics EXEC** command on the Cisco Streaming Engine).

Workaround: Initiate the live split again by using the Content Distribution Manager GUI to change one of the program's attributes (for example, its description). The change in the program's attribute is sent to the individual Content Engines, and the program is triggered again.

- CSCef37606

The Content Engine becomes unresponsive, and it takes a long time for commands to be executed.

Condition: This problem occurs when the load that is running on the Content Engine is almost as high as the maximum permissible load for a Content Engine, and you then enable ICAP (especially with request modification [REQMOD] transactions). This situation causes the Content Engine to go into an overload state and not recover easily.

Workaround: The load on the Content Engine with ICAP enabled (for the response modification [RESPMOD] transactions) should be kept to 50 percent of the load that it can handle without ICAP.
- CSCef37947

Symptom: A URL in the Synchronized Multimedia Integration Language (SMIL) file that has the “repeatCount” value set, may not be requested as many times as specified by the “repeatCount” setting.

Condition: This problem occurs only when RealPlayer Version 10 is used. The player exhibits the same behavior whether or not there is a Content Engine between the client and the origin server.

Workaround: Use RealOne player instead of RealPlayer Version 10, or request the SMIL file again. The URL will be played at least once in the player.
- CSCef44709

Symptom: An HTTP 1.0 request that is received by the Content Engine from a client web browser is sent as an HTTP 1.1 request by the Content Engine to the origin server.

Condition: This problem occurs only when the ICAP service is enabled on the Content Engine.

Workaround: There is no known workaround.
- CSCef57641

Symptom: The cache process on the Content Engine restarts.

Condition: This problem occurs if a large volume of HTTPS and FTP traffic is being directed to the Content Engine, which is operating in transparent mode.

Workaround: There is no known workaround.
- CSCef60282

Symptom: Even though you entered a **write memory** command, after an immediate reload, a prompt appears that the configuration has been changed.

Conditions: This problem occurs if the following conditions are met:

 - You have enabled Websense on the Content Engine.
 - The IP address of the Content Engine is removed or changed.
 - You enter a **write memory** command on the Content Engine.
 - You reload the Content Engine.

Workaround: Note that ACNS functionality is not affected if this problem occurs. However, if a prompt appears stating that the configuration has been changed, enter **yes** to save the configuration.
- CSCef61845

Symptom: Unicast access to a live program does not work.

Condition: This problem occurs only when you use special characters (“?” and “#”) in the unicast reference URL.

Workaround: To publish a live event, use URLs that do not contain special characters.

- CSCef62968

Symptom: The Content Engine reboots suddenly when you are performing database maintenance.

Condition: The problem can occur because of a platform issue in the power supply of the device.

Workaround: Properly trim the power supply of the Content Engine.
- CSCef65567

Symptom: You are not able to download the control list or apply a policy (for example, the policies that control when the SmartFilter subscription or control list expire) to the SmartFilter 3.x plug-in.

Condition: This problem occurs if you use the SmartFilter 4.0 Administrator Console to define the SmartFilter 3.x plug-ins as part of a plug-in group.

Workaround: Use the SmartFilter 4.0 Administrator Console to define the SmartFilter 3.x plug-ins as individual plug-ins.
- CSCef67938

Symptom: When using the quick start tool in the Content Distribution Manager GUI, if you repeatedly click the **Add-Router to List** button before the window completely loads in your browser, the following message appears in your browser:

```
The system had trouble processing your last request.
```

This situation can occur under the following circumstances:

 - You click the **BACK** or **REFRESH** browser buttons.
 - Multiple browser windows from the same client machine are accessing the Content Distribution Manager GUI.
 - Another user deletes the item that you are working with in the Content Distribution Manager GUI.

Condition: This problem occurs only when there is a slow connection between the Content Distribution Manager and your browser and you perform any of the unsupported actions described above.

Workaround: Return to the Content Distribution Manager GUI and wait until the window is completely loaded in your browser before you click the **Add-Router to List** button.
- CSCef70012

Symptom: The crond process generates a core file on devices that are running the ACNS 5.2.x software.

Condition: This problem can occur occasionally in random situations. This problem is known to occur when a device boots after you have upgraded the image on the device.

Workaround: A workaround is not necessary because the crond is restarted automatically by the system, and functionality is not affected.

- CSCef96069

Symptom: The output of the **show tech-support EXEC** command displays the following warning message in the “system log info” section (the kernel log):

```
Warning - running *really* short on DMA buffers
```

Conditions: This problem can occur under situations such as the following:

- You have performed a software upgrade, and you reboot the ACNS software.
- Other conditions, which involve substantial disk I/O shortly after startup, have occurred.

Note that the above message does not indicate that the ACNS software is not functioning properly. Typically, the system recovers and no actual problems occur.

Workaround: There is no known workaround.

- CSCeg18280

Symptom: The value that is shown in the host-resource-MIB for CPU usage is incorrect (it is too high).

Condition: This problem can occur if the Content Engine is running the ACNS 5.1.x software release or an earlier release.

Workaround: There is no known workaround.

- CSCeg27152

Symptom: The clients of HTTP or streaming services may see broken pages or broken connections.

Condition: This problem can occur because the Content Engine enters or exits a WCCP cache farm, which can result in inconsistent views of bucket ownership on the Content Engines in the cache farm.

Workaround: Disable WCCP on the router, and then wait two minutes before you reenable WCCP on the router.

- CSCeg47793

Symptom: If you modify the contents of a Content Engine GUI page and reload the page without first clicking the Update button, the new (unsaved) values are displayed on the page instead of the old (saved) values.

Condition: This problem occurs only if you are using the latest versions of the Netscape browser (Version 7.0 or later) to access the Content Engine GUI.

Workaround: Go to another Content Engine GUI page, and then return to the same Content Engine GUI page instead of reloading the page. The redisplayed Content Engine GUI page will display the old (saved) values instead of the new (unsaved) values.

- CSCeg49287

Symptom: When WCCP transparent redirection is being used to redirect RTSP client requests transparently to WCCP routers, the client receives an error stating that it is unable to locate the server when it attempts to retrieve the RTSP URL. This problem can occur because the URL presented to the client is a modified “bad” URL. This modified URL is the original URL with the Content Engine’s RTSP gateway IP address prepended before the domain name. For example, if the original RTSP URL is “rtsp://website.com.domain:554/url-path-info,” then the following modified “bad” URL is returned to the client:

```
rtsp://ciscoRTSPG.ipaddress-of-rtsp-gateway.website.com.domain:554/url-path-info
```

The reason that the client is unable to resolve the DNS is because the Content Engine is using the modified URL.

Condition: The problem can occur when the WCCP router list (**wccp router-list** *x.x.x.x* CLI command) on the Content Engine is configured with a router IP address that the router does not use in its WCCP “I See You” messages.

Workaround: Configure the WCCP router list to use the IP address that the WCCP router is using on its “I See You” messages.

- CSCeg50167

Symptom: The Content Engine is not appending an “X-Forwarded-for:” header to the HTTP request.

Condition: This problem can occur if the **http append x-forwarded-for-header** global configuration command has been entered on the Content Engine and the HTTP request already has an “X-Forwarded-for:” header.

Workaround: There is no known workaround.

- CSCeg55742

Symptom: Multiple connections are seen between the root Content Engine and the Windows Media server/encoder.

Condition: This problem can occur if the root Content Engine is under a heavy load and multiple Content Engine children or clients connect to the root Content Engine to access a unicast stream. Because of timing issues, the root Content Engine can create multiple connections to the encoder/server. This problem does not adversely impact the clients that are watching the stream; however, one side effect is that more bandwidth will be used between the root Content Engine and the encoder/server.

Workaround: There is no known workaround.

- CSCeg57195

Symptom: After changing the DNS configuration, WMT fails and the WMT error logs show that there is a problem with resolving URLs.

Condition: This problem occurs because WMT is not recognizing that a DNS change has occurred and is trying to use the old DNS configuration that may point to a server that is down or is inaccessible.

Workaround: After you change the DNS configuration, reload the Content Engine to ensure that all of the processes will obtain the current DNS configuration when they start up.

- CSCeg60760
Symptom: CPU usage on the Content Engine reaches 99 percent.
Condition: This high CPU usage can occur if the Content Engine is serving numerous live streaming requests and it is running the ACNS 5.1.11 software and later releases.
Workaround: If you are not expecting a very high load on the Content Engine, you can turn off kernel optimization by entering the **no wmt accelerate live-split** global configuration command.
- CSCeg69790
Symptom: After you configure a live event through the ACNS 5.2 Content Distribution Manager GUI, the URL link generated by the Content Distribution Manager cannot be played.
Condition: This problem occurs only if the media filename or program name includes a blank space.
Workaround: Do not use a blank space in either the media filename or the program name when using the Content Distribution Manager to configure a live event. For example, use “-” or “_” instead of a blank space.
- CSCeg74062
Symptom: Internet Explorer does not display the RealServer License Monitor window correctly. (This window is displayed by logging in to the RealServer administrative interface and then selecting **Logging & Monitoring** and **License Monitor**.)
Condition: This problem occurs only with Internet Explorer.
Workaround: Use the Firefox or Netscape browsers, which display the License Monitor window correctly.
- CSCeg74070
Symptom: Both Internet Explorer and Firefox browsers do not correctly display changed settings for the broadcast transmitter and receivers.
Condition: This problem occurs if the Content Engine is running the ACNS 5.2 software and using RealServer as a back-end RTSP server.
Workaround: There is no known workaround.
- CSCeh20894
Symptom: The Content Engine cannot play a media file without any problems from a Windows Media Series 9.1 server.
Condition: When the WMT media player plays a media file from a Windows Media Series 9.1 server through the Content Engine, one of the following problems can occur:
 - The player will not play the media file from the Windows Media Series 9.1 server and keeps buffering.
 - The Content Engine plays the media file partially and then enters into buffer mode repeatedly while it is playing the file.Workaround: There is no known workaround.

- CSCeh62735
Symptom: An attempt to download a SmartFilter control list fails.
Condition: This problem occurs if the Content Engine is running the ACNS 5.2.3 software and later releases, and SmartFilter Version 4.0 is being used for URL filtering. If the automatic update of control list does not complete successfully, the download of the SmartFilter control list will fail because the sfdownload.stat file is not modified and the sfcontrol.tmp file exists on the Content Engine.
Workaround: Delete the sfcontrol.tmp file on the Content Engine so that the download of the control SmartFilter control list can work.
- CSCeh73477
Symptom: The acquirer experiences a problem with a samba crawl. The acquirer is recrawling the same crawl job.
Condition: This problem can occur if both of the following conditions exist:
 1. A channel contains a samba crawl from a Network Appliance file server, which contains such media files as .wmv files.
 2. The time to live (TTL) is set to recrawl the file at a fixed interval that is specified by the TTL attribute.Workaround: There is no known workaround.
- CSCeh93212
Symptom: The Websense Manager cannot connect to the local (internal) Websense server that is running on the Content Engine, and clients receive the following error: “Failed to connect, the server is not yet fully started. Please try again in a little while.”
Condition: This problem can occur if a standby IP address is used on both the primary and secondary interfaces, which prevents the Websense Manager from connecting to the Content Engine.
Workaround: Disable the standby IP group and use a single IP address on the interface.
- CSCei05034
Symptom: NTLM failover does not work correctly.
Condition: The client requests takes about two minutes to time out from the authentication failure and the Content Engine does not detect the domain controller (DC) failure. This problem can occur if the following circumstances exist:
 - a. NTLM request authentication is enabled on the Content Engine.
 - b. The domain controller service stops responding but the domain controller hardware is still up.Workaround: Bring up the domain controller service again, or restart the domain controller hardware to force the Content Engine to fail over.

- CSCei05765

Symptom: When you are using the Content Distribution Manager GUI to view any of the statistics graphs (for example, Bytes Served, Bandwidth Efficiency Gain, Streaming Sessions, and CPU Utilization), the time axis is not accurate. The reading is off by the UTC time of the local Content Engine or the Content Distribution Manager.

Condition: This problem can occur if the Content Distribution Manager is configured to use a nonstandard time zone.

Workaround: Configure the Content Distribution Manager with a time zone that is recognized by the Java platform. The following time zone format is recognized:

Etc/GMT-X

Etc/GMT+X

where “X” is the appropriate hour offset from GMT for the Content Distribution Manager time zone. You can perform this configuration through the Content Distribution Manager CLI or through the Content Distribution Manager GUI by specifying a custom time zone.
- CSCei06964

Symptom: The Windows Media player is not able to play the URL.

Condition: This problem can occur if the Content Engine is in between the Windows Media player and an ISA proxy, and NTLM authentication is enabled on the ISA proxy.

Workaround: There is no known workaround.
- CSCei13929

Symptom: Websense configurations are lost (for example, the downloaded database and license information).

Condition: This problem occurs only if you use the Content Distribution Manager GUI to perform the Websense configuration.

Workaround: Perform the Websense configuration through the CLI instead of through the Content Distribution Manager GUI.
- CSCei17023

Symptom: LDAP may take over 60 seconds to send the prompt to a client.

Condition: This problem can occur if you have entered the **http avoid-multiple-auth-prompts** and the **rule enable** global configuration commands. After the first request, if the user clicks Cancel instead of specifying the requested credentials, the prompt to client is delayed for more than 60 seconds.

Workaround: Disable the **http avoid-multiple-auth-prompts** command by entering the **no http avoid-multiple-auth-prompts** command.
- CSCei18400

Symptom: There is a problem with playing high definition/high bit rate video on-demand streams.

Condition: This problem can occur if there are more than 14 unique 2-Mbps streams with two clients per stream (28 connections).

Workaround: There is no known workaround.

- CSCei20296
Symptom: Replication of content stalls.
Condition: This problem can occur if a channel is configured with a root Content Engine and some receiver Content Engines. After content acquisition is completed, the distribution starts but stalls at a point where the Content Engines repeatedly download the same files from the forwarder Content Engines.
Workaround: Delete and recreate the database on the root Content Engine.
- CSCei23360
Symptom: A large-size post request fails if the ICAP service is enabled for the reqmod-precache vector point.
Condition: This problem can occur only if the ICAP server is on a fast network to the Content Engine and the origin server is on a very slow network. The problem occurs only with certain ICAP servers.
Workaround: There is no known workaround.
- CSCei24143
Symptom: The Windows Media player displays the following error message when a WMV file is requested: “Windows Media Player cannot connect to the server. The server name may be incorrect or the server is busy. Try again later.” The directory core_dir on the Content Engine has a mms_server process core dump. The Windows Media player might play the file if the cache is bypassed but the play duration might be wrong.
Condition: This problem can occur if the following circumstances exist: the Windows Media services is enabled on the Content Engine and the WMV file has incorrect ASF header information. For example, files are encoded with “Flip4Mac WMV Export Component for QuickTime (Mac) Ver.1.0.3.”
Workaround: There is no known workaround.
- CSCei28716
Symptom: The system crashes and there is a kernel core dump.
Condition: This problem occurs only rarely.
Workaround: If this problem occurs, the ACNS device will automatically reboot at which time the system will work normally after the reboot.
- CSCei31433
Symptom: The Cisco Streaming Engine crashes on the Content Engine.
Condition: This problem can occur if the Content Engine is booted and it has been configured to use the Cisco Streaming Engine in its bootup configuration (that is, the **rtsp server cisco-streaming-engine enable** command has been specified on the Content Engine).
Workaround: There is no known workaround.
- CSCei38074
Symptom: Even though you have activated the Websense Network Agent on the Content Engine, usernames are not being used for the user-based policy filtering.
Condition: This problem occurs because the Websense Network Agent, which is a Websense service, is not using usernames for the user-based policy filtering.
Workaround: There is no known workaround.

- CSCei62672

Symptom: When you click links from the table of contents or the index of the ACNS Content Distribution Manager online help, the links open in the same pane, that is, the left pane, which contains the table of contents and the index, instead of opening in the right pane, which contains the help topics.

Condition: This problem occurs after you install Microsoft security update MS05-026. This security patch disables cross-frame navigation features that are based on HTML Help ActiveX control (HHCTRL).

Workaround: To reenble cross-frame navigation features that are based on HHCTRL, modify your Windows registry as explained in Microsoft Knowledge Base article 896905, which is available at this URL:

<http://support.microsoft.com/kb/896905/>

- CSCin54434

Symptom: Websense Manager cannot connect to the local Websense server (the Websense server runs as a separate process on the Content Engine instead of running on a separate system).

Condition: This problem occurs if an external IP address is used from Websense Manager to connect to the local Websense server (Version 5.0.1) that is running on the Content Engine.

Workaround: There is no known workaround.

- CSCin58464

Symptom: The Websense policy server and user server generate core files.

Condition: This problem occurs when the Websense server is running on the ACNS 5.1.x software with a version of the Websense Manager that is earlier than Version 5.0.1 build 20030722. This problem does not exist when the Websense server is running on the ACNS 5.0.3 software.

Workaround: Download Websense Manager Version 5.0.1 build 20030722.

- CSCin59462

Symptom: An FTP client application stops receiving data for a data transfer operation such as a directory listing (ls) or file transfer (GET). The same symptom can occur for FTP-over-HTTP data transfers from the FTP server to the Content Engine.

Condition: For FTP client applications, the Content Engine must be using the FTP proxy through WCCP redirection, configured for following the FTP client's mode for establishing a data connection. The FTP client application must have also been set to use active mode to the FTP server.

```
ContentEngine(config)# wccp ftp router-list-num number
ContentEngine(config)# wccp version 2
ContentEngine(config)# ftp proxy active-mode enable
```

For FTP-over-HTTP data transfers, the Content Engine must be configured for an FTP incoming proxy and configured to use active mode to the FTP server. The client browser must be configured to use the Content Engine FTP proxy for FTP URLs.

```
ContentEngine(config)# ftp proxy incoming port
ContentEngine(config)# ftp proxy active-mode enable
```

The symptoms can occur with the configurations described above and when the FTP server starts sending data packets that are received out of order by the Content Engine before the Content Engine sends the TCP connection establishment SYN-ACK packet to the FTP server.

Workaround: Remove the Content Engine active mode configuration by entering the following global configuration command:

```
ContentEngine(config)# no ftp proxy active-mode enable
```

When this symptom occurs on an FTP client application, press **Ctrl-C** simultaneously to stop the partial data transfer operation.

When this symptom occurs on a browser configured for FTP-over-HTTP, click the **STOP** button to stop the partial data transfer operation.

- CSCin59781

Symptom: The cache process crashes while passing traffic for both predefined and user-defined HTTPS services.

Condition: This problem can occur when heavy HTTPS traffic is passing through the Content Engine. Using predefined and user-defined WCCP services and having the debug function enabled when HTTPS traffic is heavy may contribute to this problem.

Workaround: There is no known workaround. However, the cache process will restart and work normally after such a crash.

- CSCin60029

Symptom: When a rule with the **redirect** action is configured with a URL of 0 and with a matching pattern (no replacing pattern), the cache process crashes if the request matches the pattern.

Condition: This problem occurs when you configure a numeric value of 0 for the redirected URL (for example, if *www.yahoo.com* is redirected to 0). If you want the Content Engine to redirect URL *x* to URL *y*, then you can configure the **rule redirect** action. While doing so, you must configure URL *x* and URL *y*.

Workaround: There is no known workaround.

- CSCin65344

Symptom: When MPEG-2 is specified as the preferred format in a channel, the programs cannot be created in that channel.

Condition: This problem occurs only if MPEG-2 is the preferred format.

Workaround: When MPEG-2 is chosen as the preferred format for a channel-based program, the default bandwidth is set to 1150 (the default for non-MPEG-2 programs). The default bandwidth for MPEG-2-based programs should be 2000 for MPEG-2 half duplex, and 3000 for MPEG-2 full duplex. Manually set the bandwidth while creating the program as follows:

- If the preferred format is MPEG-2 half duplex, set the bandwidth to 2000.
- If the preferred format is MPEG-2 full duplex, set the bandwidth to 3000.

- CSCin67818

Symptom: The manifest validator fails to fetch the XML file if the source is authenticated.

Condition: This problem occurs only if the file is located at an authenticated location.

Workaround: Put a copy of the manifest file in a nonauthenticated location to use the manifest validator.

Resolved Caveats—ACNS 5.2.7 Software

This section lists the caveats that have been resolved in the ACNS 5.2.7 software release. The resolved caveats are grouped into the following categories:

- [Acquisition and Distribution Resolved Caveats, page 25](#)
- [DNS Resolved Caveats, page 26](#)
- [ICAP Resolved Caveats, page 26](#)
- [Management Resolved Caveats, page 26](#)
- [Media and Streaming Resolved Caveats, page 28](#)
- [Proxy and Caching Resolved Caveats, page 29](#)
- [Rules Resolved Caveats, page 31](#)
- [Other Resolved Caveats, page 32](#)

Acquisition and Distribution Resolved Caveats

- CSCeh06795

A live channel may fail to be played from the clients. The replication fails as indicated by the output from the **show programs EXEC** command. This problem can occur in the following condition:

 - a. You are running the ACNS 5.2.1b7 software and later releases.
 - b. You configure a live channel and then schedule it through the Content Distribution Manager GUI.
 - c. You use uppercase letters when specifying the program name.

Because uppercase letters are sometimes rejected, you need to avoid using uppercase when specifying the program name in the Content Distribution Manager GUI. This problem was fixed in the ACNS 5.2.7 software release.
- CSCeh09178

If you enter the **show distribution remote sender-IP address unicast-sender EXEC** command, unicast distribution is triggered. (Entering this EXEC command should not trigger unicast distribution from the sender Content Engine.)
- CSCeh10340

The ACNS 5.x software provides a Common Interface File System (CIFS) client and a Network File System (NFS) client for Content Engines to communicate with network attached storage (NAS) devices. CIFS website-based access control is not working properly. This problem was fixed in the ACNS 5.2.7 software release.
- CSCeh40754

The root Content Engine is not able to acquire content. The Content Distribution Manager GUI replication status window indicates that the Content Distribution Manager has no content, and the receiver Content Engines indicate “No Status Reported.” This problem can occur if the root Content Engine has recently experienced a failure that took it down, or it required a hard reboot that caused a database corruption on the root Content Engine, which in turn prevented the acquirer from acquiring the content.

- CSCeh44689
The acquirer fails to load or start if the origin server requires NTLM authentication and the NTLM credentials are not provided to the acquirer.

DNS Resolved Caveats

- CSCed94383
In a forward proxy setup, the output of the **show statistics dns** EXEC command shows two DNS lookups for each HTTP request.
- CSCeh41983
The DNS process can stop responding after a corrupted DNS response is received.

ICAP Resolved Caveats

- CSCeh15889
When the Content Engine is operating in proxy mode and the ICAP service is enabled on it, RealPlayer cannot properly handle RTSP-over-HTTP requests.
- CSCeh96632
The connection to the ICAP server is not terminated for up to 1.5 minutes after the server is unreachable. This problem occurs regardless of the keepalive timer setting.

Management Resolved Caveats

- CSCeg48024
Duplicate key error messages are reported for certain operations that you perform through the Content Distribution Manager GUI as follows:

```
Dec 6 22:39:04 ODI-MGMT-CE-510 java: %CE-CMS-4-700001: ce(Dispatcher-1): Duplicate key: System.ftpcache.proxyEnable
Dec 6 22:39:04 ODI-MGMT-CE-510 java: %CE-CMS-4-700001: ce(Dispatcher-1): Duplicate key: System.https.tcpRWTimeOutEnable
Dec 6 22:39:04 ODI-MGMT-CE-510 java: %CE-CMS-4-700001: ce(Dispatcher-1): Duplicate key: System.ftpcache.proxyEnable
```
- CSCeg89767
In the WCCP Bypass List window of the Content Distribution Manager GUI, duplicate bypass list entries are shown if you have specified “any” as the client or server address for a device group.
- CSCeh48631
The LocationApiServlet fails with a constraint exception when the name is not set.
- CSCeh55264
The DeviceGroup TimeZone Settings with SummerTime set are overridden by each of the devices in the device group. This problem can occur if the CMS agent that is running on the Content Engine fails to properly parse the time zone configuration on the device and reports the time zone as having been changed from that of the Content Distribution Manager configuration. This situation causes the values to be overridden. This problem occurs only for the default time zone of UTC.

- CSCeh57366

If you are running the ACNS 5.0 or 5.1 software on the Content Distribution Manager and one or more of the registered Content Engines are running the ACNS 5.2.x software or the ACNS 5.3.1 software, the NTLM server may appear out of order when you check the running configuration on the Content Engine. This problem can occur if you have specified both the primary and secondary domain servers for one of these Content Engines (or for a group that contains one of these Content Engines) through the NTLM Server Settings window of the Content Distribution Manager GUI.
- CSCeh58488

Clients receive a “Page cannot be displayed” error message when they access a site that requires NTLM authentication. This problem can occur with chunked-encoded responses and responses with no content length header.
- CSCeh60484

If you perform a software download from the Content Distribution Manager GUI and the download file is larger than 1 MByte, the GUI displays an incorrect status message about the software download (Download failed) while performing the software update.
- CSCeh84287

In rare circumstances, the Content Distribution Manager GUI can become suddenly inaccessible. This problem occurs only rarely and if the Content Distribution Manager is running the ACNS 5.2.5 software release. This problem was fixed in the ACNS 5.2.7 software release.
- CSCei26545

Content routing statistics show zeros in the Content Distribution Manager GUI (in the CDM GUI Monitoring/Statistics window) and is not updated after you use the Content Distribution Manager GUI to request statistics from the Content Router. This problem can occur if there is a Content Router that has request routing enabled on it, and it is registered with the Content Distribution Manager. Even though the Content Distribution Manager GUI displays incorrect data, the output of the **show statistics content-routing** EXEC command displays the correct data. In the ACNS 5.2.7 software release, this Content Distribution Manager GUI problem was fixed.
- CSCei26550

Every two minutes, an ACNS device that is registered with a Content Distribution Manager, sends an RPC request to the Content Distribution Manager. When debugging is enabled on primary Content Distribution Manager, it shows that the alarm is an “empty” alarm update:

```
06/14/2005 05:39:20.849(Local) [D] cdm(RpcWorker-1): Processing partial alarm update
from
device ... events size 0
```

This RPC call results in extra bandwidth and CPU consumption on the primary Content Distribution Manager.
- CSCei44218

A standby Content Distribution Manager goes offline during the period that the statistical records are being consolidated daily. This problem occurs only if the Content Distribution Manager is managing a large number of Content Engines (for example, 1,400 Content Engines).

Media and Streaming Resolved Caveats

- CSCeg35981
RTSP requests are failing when the RTSP gateway, which is running on the Content Engine, is used. This problem occurs when a request is using nonstandard RTSP ports, which are not allowed through the firewall (the RTSP gateway is not properly handling the switch from RTSP to RTSP-over-HTTP).
- CSCeh00301
Windows Media Technologies (WMT) fails to route around the primary source stream Content Engine after a failover occurs. This problem occurs only when the primary Content Engine fails prior to any connection to it. Connectivity is restored only after the primary Content Engine is recovered.
- CSCeh15889
When the Content Engine is operating in proxy mode and the ICAP service is enabled on the Content Engine, RealPlayer cannot properly handle an RTSP-over-HTTP request.
- CSCeh41537
The media player enters into a buffering state for managed live programs that are created with a broadcast publishing point as the source. This problem occurs with files that contain a large number of script events, which are used as the source for creating the publishing point in a Windows Media server.
- CSCeh43420
A cache crash and core dump can occur on a Content Engine during a chunk-encoded object data transfer. However, when this problem occurs, the cache process is automatically restarted.
- CSCeh72679
Even though all of the NTLM credentials are provided, the proxy still fails authentication because the acquirer always uses unicode for the credentials.
- CSCeh94630
The RealProxy administrator GUI shows garbled content. This problem can occur if you change the RealProxy configuration through the administrator GUI. A new window opens and displays garbled content.
- CSCei10904
The output of the **show statistics wmt streamstat EXEC** command shows that the fast-cache acceleration bandwidth is being allocated for live HTTP requests. This problem can occur if the fast cache feature is enabled on the Content Engine for WMT requests and the Content Engine is running the ACNS 5.2.5 software or earlier releases. This problem was fixed in the ACNS 5.2.7 software release.

Proxy and Caching Resolved Caveats

- CSCef90286

The Content Engine returns HTTP 1.1 content instead of HTTP 1.0 content to HTTP 1.0 client browsers. This problem occurs because the Content Engine is not distinguishing between HTTP 1.1 and HTTP 1.0 client requests. Consequently, the Content Engine sends HTTP 1.1 content in response to HTTP 1.0 requests. This problem was fixed in the ACNS 5.2.7 software release.
- CSCeg36621

File transfers of large files fail and connection reset error messages are generated. This problem occurs with HTTP, native FTP, and FTP-over-HTTP proxies (Content Engines) that are running the ACNS 5.2.x and 5.1.x software. This problem was fixed in the ACNS 5.2.7 software release.
- CSCeg53927

On a CE-511 model, the Real System Administrator home page is not accessible from the Content Engine GUI. When you attempt to access it from the GUI of a CE-511 model, a page not found error is displayed.
- CSCeg63788

The internal Websense server on the Content Engine is not responding to a block page message. This problem can occur if certain clients do not behave properly and fail to send the requested data back to the Websense block page server. The block page server is not timing out these requests, reaches a limit, and then stops responding.
- CSCeg82504

Every two seconds, syslog messages such as the following, are being continuously generated:

```
Jan 16 01:37:02 CE7325-CE1 bandwd: %CE-BANDWD-3-115003: BANDWD:
verification registration failed, err=30
Jan 16 01:37:02 CE7325-CE1 bandwd: %CE-BANDWD-3-115002: BANDWD:
Trying again in two seconds
```
- CSCeg83927

When the Content Engine is handling chunked HTTP responses, the HTTP GET responses may fail and the connection is terminated. No user intervention is required because the cache process is automatically restarted.
- CSCeh00314

In the case of WMT live and content routing, the HTTP failover URL does not work. In the case of a WMT live using content routing, after the initial communication between the client and the Content Router, the client is redirected to the Content Engine. When the Content Engine receives this request, it sends the client an .asx file that contains two URLs (an MMS URL and an HTTP URL). In the case of WMT live, this HTTP URL is not valid. If the client fails over to this HTTP URL if the MMS URL fails, the stream will not be served by the Content Engine. This problem occurs on systems that are running the ACNS 5.1.x, 5.2.x, and 5.3.1 software. This problem was fixed in the ACNS 5.2.7 and ACNS 5.3.3 software releases.
- CSCeh02627

If a POST request includes an Expect: 100 Continue response, the Content Engine can experience problems in processing these POST requests properly.
- CSCeh12282

A client might stop responding when it is waiting to receive a close to the connection from a Content Engine that has received a 304 response from the origin server.

- CSCeh15968

The client receives an unexpected 400 bad request HTTP response from the origin server when the request is going through a Content Engine. This problem can occur if the client sends an unnecessary carriage return/line feed (\r\n) in between the end of one request and the beginning of another request. These extra characters have been seen using the following version of the browser: Internet Explorer Version: 6.0.2800.1106.xpsp2.040919-1003, Cipher Strength: 128-bit, Update Versions: SP1; Q832894; Q837009; Q831167; Q823353; and Q871260.

- CSCeh17930

Not all of the syslog.txt messages have a message code associated with them. This problem causes the syslog error log to fill up because the syslog machines, which expect a message code, are writing error messages to the syslog error log.

- CSCeh21067

Windows Media player files are not being downloaded properly. This problem can occur if you have entered the **wmt disallowed-client-protocols http** global configuration command on the Content Engine and the Content Engine is rebooted.

- CSCeh30618

The **ip domain name** *domain name* global configuration command does not allow the domain name to start with a number. The command requires that the domain names begin with a letter and then only contain numbers and letters as shown in the following example:

```
ContentEngine(config)# ip domain name 123abc.mydomain.com
Illegal domainname 123abc.mydomain.com.
Valid domainname can contain only alphanumerics, hyphen and dot.
```

In the ACNS 5.2.7 software release, the **ip domain name** *domain name* global configuration command was modified to allow domain names that begin with a number.

- CSCeh48360

The rewrite action fails for WMT requests if the no-proxy action is also configured for a matching pattern. This problem causes the no-proxy action to be executed first instead of the rewrite action being executed first. An example is shown as follows:

```
ContentEngine# show rule all
Rules Template Configuration
-----
Rule Processing Enabled
Actions :
rule action rewrite pattern-list 5
rule action no-proxy pattern-list 7
Pattern-Lists :
rule pattern-list 5 group-type or
rule pattern-list 5 url-regex (mms.*://www.wm-server-1.com).* \1/pinball.wmv rule
pattern-list 7 group-type or rule pattern-list 7 dst-ip 10.77.157.169 255.0.0.0
```

In this case, 10.77.157.169 is the IP address of the www.wm-server-1.com.

If a request is given for mmst://www.wm-server-1.com/100kbs.wmv, it must be rewritten to the URL mmst://www.wm-server-1.com/pinball.wmv. However, because the no-proxy action is executed first, such a rewrite does not occur.

- CSCeh55335

If the **http cache-vary-user-agent enable** global configuration command has been specified on the Content Engine, a cache crash can occur on the Content Engine.

- CSCeh69442
The Content Engine does not cache the content and is not receiving any requests even though the router is redirecting traffic to the Content Engine. This problem can occur if the request header line in the packet is greater than 8 KBytes, which causes the Content Engine to reset the connection and to have an entry created in the bypass list.
- CSCeh73714
The cache process stops and the output of the **show tech-support EXEC** command shows a back trace.
- CSCeh90745
WCCP goes into bypass mode and bypasses a large number of connections. This problem can occur in the following circumstance: the Content Engine is receiving a large number of connections over WCCP, and a substantial number of these connections are proxy-style requests. If the **http proxy incoming 80** global configuration command has not been entered on the Content Engine, these connections result in a “wrong destination address in proxy mode” errors. If too many of these errors occur, the Content Engine goes into overload bypass mode because it assumes that there is an overload situation.
- CSCei04882
Certain requests (for example, when you click on links from the results of a Goggle search) to the Content Engine time out without any response from the Content Engine. This problem can occur if all of the following conditions exist:
 - a. The server response is noncacheable.
 - b. The server transfer encoding is chunked.
 - c. The Content Engine is configured to keep a persistent connection with the server.
 This problem was fixed in the ACNS 5.2.7 software release.

Rules Resolved Caveats

- CSCee56298
Blank spaces are not allowed in a rule group name even though a blank space is allowed in an access list group name (for example, the **access-lists 300 permit groupname "CNBU1.LOCAL\Domain Users"** global configuration command accepts the “Domain Users” as a group name even though it contains a blank space). In the ACNS 5.2.7 software release, support for a blank space in a rule groupname string was added.
- CSCef27163
The command output of the **show rule pattern *pattern-list number* all EXEC** command does not display the configured group-type pattern for the specified pattern list.
- CSCeg85614
The use proxy rules configuration does not work if the use proxy failover rules configuration is also configured with the same pattern list number. For example, if a configuration such as the following exists and pattern list 1 is used, then the **use-proxy failover** action (shown in “a” of this example) takes precedence over the **use-proxy** action (shown in “b” of this example) and the second CLI is never executed (it becomes a dummy rule):
 - a.

```
ContentEngine(config)# rule action use-proxy 1.2.3.4 8080
failover pattern-list 1
```
 - b.

```
ContentEngine(config)# rule action use-proxy 128.107.193.242 8080
pattern-list 1
```

- CSCeg88824
The Content Engine enters into kernel debugging (kdb) mode.
- CSCeh34039
The **no proxy** rule action does not work for transparently redirected proxy style requests. This problem occurs if there is a pattern configured for a domain name, such as abccorp.com, and a request is given to a source that is not a FQDN (for example, http://www). This problem was fixed in the ACNS 5.2.7 software release.

Other Resolved Caveats

- CSCeb85057
The Content Engine displays this error message during normal operation:

```
KERNEL: assertion (atomic_read(&sk->wmem_alloc) == 0) failed
```
- CSCeg68274
SNMP management is not able to learn the standby interface in order to test the standby interface for accessibility. This problem can occur if the Content Engine is configured with a standby interface and the SNMP management station uses an MIB query for ipAdEntAddr. The SNMP management system learns the addresses of the individual interfaces but not the address of the standby group.
- CSCeh16755
For HTTP POSTs through a forward proxy, uploads of large files can be slower through the Content Engine and the Content Engine advertises a TCP receive window size that is much smaller than expected. This problem is caused because the TCP receive window decreases to 2 KBytes on a POST through a forward proxy for certain applications and operating systems.
- CSCeh28890
When you perform a software upgrade or downgrade between the ACNS 5.3 software release and the ACNS 5.0 software release, the TCP Explicit Congestion Notification (ECN) configuration is not retained. This problem can occur if you enter the **tcp ecn enable** global configuration command when the device is running the ACNS 5.0 software release and then upgrade the device to a later software release. This problem was fixed in the ACNS 5.2.7 software release.
- CSCeh19530
In rare circumstances, the CE-511 and CE-566 models can lock up. The syslog does not indicate any kernel crash or other problems that might explain the cause of such lockups. In this situation, these Content Engines disconnect from the network and do not respond to the console. However, the Content Engine does come back up after a power cycle. This problem was fixed in the ACNS 5.2.7 software release. (This problem was also fixed in the ACNS 5.3.3 software release.)
- CSCeh34279
The Content Engine does not export the transaction logs when the transaction log export feature is enabled. This problem occurs only if there are Cisco Streaming Engine logs files in the /local1/logs/cisco-streaming-engine directory.
- CSCeh48047
The Content Engine stops responding or enters kernel debug mode when there is high memory usage for TCP.

- CSCeh48187

In rare circumstances, the Content Engine may not let anyone log in. This problem occurs only if all of the following conditions exist:

- The system file system (sysfs) is not mounted on the Content Engine.
- TACACS or RADIUS is enabled on the Content Engine and is the primary authentication mechanism.
- Authentication failover is configured on the Content Engine.
- The network is up and the TACACS or RADIUS server is reachable.

This problem was fixed in the ACNS 5.2.7 software release.

- CSCeh69177

A “Critical: Disk failure error occurred on *disk drive in Storage Array number*” alarm is displayed on the Content Distribution Manager even though the disk has not really failed. Even though the syslog.txt shows that the disk is reset and has returned to normal operation shortly after the alarm is raised, the alarm is not reset.

If you enter a **show disks details EXEC** command, the command output shows the state of the drive as normal. If the drive is bad, the command output of the **show disks details** command would show that there is a problem with the disk. This problem occurs only on storage arrays that are attached to a Content Engine CE-7325 model that is running the ACNS 5.2.3 software. This problem was fixed in the ACNS 5.2.7 software release.

- CSCeh82112

The DNS service can crash or stop responding when it receives a certain type of maliciously coded DNS request from a client.

- CSCei33461

Certain network modules, which are running the ACNS software, do not respond to MIB queries. This problem was fixed in the ACNS 5.2.7 software release.

- CSCei39177

The SNMP agent on a Content Engine could stop responding to MIB queries and the only workaround this problem was to restart the snmpcd process. This problem was fixed in the ACNS 5.2.7 software release.

Documentation Updates

This section describes the following documentation updates:

- [CLI-Related Changes in the ACNS 5.2.7 Software Release, page 34](#)
- [ACNS 5.2.x TV-Out Changes, page 34](#)
- [Bypassing URL Filtering for Certain HTTP and HTTPS Requests, page 36](#)
- [Configuring URL-Based Monitoring, page 38](#)
- [Downgrading ACNS 5.x Software, page 40](#)

CLI-Related Changes in the ACNS 5.2.7 Software Release

These documentation updates apply to the following two ACNS 5.2 software guides:

- *Cisco ACNS Software Configuration Guide for Locally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Command Reference, Release 5.2*

In the ACNS 5.2.7 software release, the ability to use the CLI to configure TCP memory limits was added. For more information, refer to the [“Configuring TCP Memory Limits through the CLI” section on page 3](#).

ACNS 5.2.x TV-Out Changes

This documentation update applies to the following two ACNS 5.2 software guides:

- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Command Reference, Release 5.2*

Changes Related to the TV-Output Feature

In the ACNS 5.2.1 software and later releases, the output of the **show hardware EXEC** command notifies you if the Content Engine has TV-out hardware that is not supported by the ACNS software release that is running on the Content Engine.

In the ACNS 5.2.1 software and later releases, the output of the **show tvout EXEC** command also notifies you if the Content Engine has TV-out hardware that is not supported by the ACNS software that is currently running on the Content Engine.

In the ACNS 5.2.3 software and later releases, the output of the **show hardware EXEC** command displays the version of the TV-out hardware that is contained in the Content Engine.

The TV-output service supports the local playback of the pre-positioned MPEG content through a hardware decoder. The hardware decoder converts the digital information into an analog TV signal. The TV-output service is only functional if the Content Engine is equipped with a supported MPEG hardware decoder. The **tvout enable** global configuration command is used to enable the TV-output service on a Content Engine that is registered with a Content Distribution Manager.



Note

The pre-positioned content is only supported on registered Content Engines; it is not supported on standalone Content Engines (that is, Content Engines that are not registered with a Content Distribution Manager and are being managed and monitored with the Content Engine GUI or CLI). Consequently, the TV-out service, which involves the pre-positioned content, is not supported on standalone Content Engines.

The changes that are related to the TV-output service are as follows:

- In the ACNS 5.2.x software, the ACNS TV-out functionality now works for the CE-510 and CE-565 models equipped with newer Vela II Revision D and Revision E MPEG hardware decoder cards. (In the ACNS 5.2.1 software, this functionality did not work for these cards.)
- New driver software was incorporated into the ACNS 5.2.3 software. This new driver software supports both the existing Vela II Revision A cards as well as the newer Vela II Revision D and Revision E cards.

- In the ACNS 5.2.3 software and later releases, the output of the **show hardware** EXEC command displays the version of the TV-out hardware that is contained in the Content Engine. In the following excerpt of the sample output from the **show hardware** command, this particular information is highlighted in bold. The “rev 3” in the command output indicates that the TV-out hardware uses the newer Revision 3 MPEG decoder PCI part. The Vela II Revision D and Revision E cards use the Revision 3 part.

```
ContentEngine# show hardware
.
.
.
Total 1 CPU.
1024 Mbytes of Physical memory.
1 CD ROM drive (CD-224E)
1 AV card (Vela II)
2 GigabitEthernet interfaces
1 Console interface
2 USB interfaces [Not supported in this version of software]

The following PCI cards were found:
PCI-Slot-1 MPEG-Decoder-AV [1105:8476 (Sigma Designs, Inc.) (rev 3)]
PCI-Slot-2 SCSI
Manufactured As: Pre-FCS 565 [867383Z]
.
.
.
```



Note To support the TV-output service with a Revision D or Revision E card, the Content Engine must be running the newer driver software, which is included in the ACNS 5.2.3 software and later releases, instead of an earlier version of the driver.

- In the ACNS 5.0.17 software, the ACNS 5.1.11 software, or the ACNS 5.2.1 software and later releases, the output of the **show hardware** EXEC command notifies you if the Content Engine is running a version of the ACNS software that does not support the TV-out hardware contained in the Content Engine. In the following example, you are notified that the Content Engine has a Vela II audio-video (AV) card that is not supported by the ACNS software release that is running on the Content Engine. In the following excerpt of the sample output from the **show hardware** command, this particular information is highlighted in bold.

```
ContentEngine# show hardware
.
.
CPU 0 is GenuineIntel Intel(R) Celeron(R) CPU 1.70GHz (rev 1) running at 1699MHz
.
.
Total 1 CPU.
1024 Mbytes of Physical memory.
1 CD ROM drive (CD-224E)
1 AV card (Vela II) [***Revision not supported in this version of software***]
2 GigabitEthernet interfaces
1 Console interface
2 USB interfaces [Not supported in this version of software]

The following PCI cards were found:
.
.
.
```

- In the ACNS 5.0.17 software, the ACNS 5.1.11 software, or the ACNS 5.2.1 software and later releases, the output of the **show tvout** EXEC command also notifies you if the Content Engine is running an ACNS software release that does not support the TV-output hardware contained in the Content Engine. In the following excerpt of the sample output from the **show tvout** command, this particular information is highlighted in bold.

```
ContentEngine# show tvout
.
.
.
TV-out model: ce565-002 (sigma)
  ***Hardware revision level not supported in this version of software***

TV-out service is not enabled
TV-out signal: ntsc

TV-out service is not running
.
.
```

Bypassing URL Filtering for Certain HTTP and HTTPS Requests

This documentation update applies to the following three ACNS 5.2 software guides:

- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Configuration Guide for Locally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Command Reference, Release 5.2*

Configuring Content Engines to Bypass URL Filtering for Specific HTTP and HTTPS Requests

In the ACNS 5.2.3 software, the ability to configure a Content Engine to bypass URL filtering for certain HTTP and HTTPS requests was added. This feature is supported for local list URL filtering (good and bad site lists), as well as Websense, SmartFilter, or N2H2 URL filtering.

For example, if you enable local URL filtering on the Content Engine and enable the bad sites deny feature (for example, the badfile.txt file contains the URLs that should be blocked), if the **rule no-url-filtering** action is a hit (a match), the Content Engine bypasses the URL filtering for that particular request; otherwise, it proceeds with URL filtering and blocks the URL request.

To support this new feature, the following CLI changes were made:

- The **rule** global configuration command supports a new action called the **no-url-filtering** action.

The **no-url-filtering** action supports the following rule patterns: src-ip, dst-ip, dst-port, domain, group-name, groupname-regex, header-field, url-regex, and username.



Note Patterns can be ANDed or ORed by using the group-type pattern (for example, **rule pattern-list 1 group-type and**). The default is OR.

- The output of the **show run**, **show statistics rule all**, and **clear statistics rule all** EXEC commands now includes information about the new **no-url-filtering** action.
- The **show statistics rule http action no-url-filtering** EXEC command was added to enable you to display statistics for the **no-url-filtering** action.

The following example shows how you can use this new bypass URL filtering feature with Websense URL filtering. First, the **rule action no-url-filtering** command is specified and then associated with a specific pattern list (pattern list 100). Next, the **domain** pattern type is added to pattern list 100 in order to configure the Content Engine to match requests that have “foo.com” as the domain. In this scenario, Websense URL filtering has already been configured and enabled on the Content Engine.

```
ContentEngine (config)# rule action no-url-filtering pattern-list 100
ContentEngine (config)# rule pattern-list 100 domain .*foo.com
ContentEngine (config)# rule enable
```

When the Content Engine receives an HTTP or HTTPS request that has “foo.com” as the domain, the **rule action no-url-filtering** rule is matched. Consequently, the Content Engine bypasses URL filtering for that particular request as shown in the partial output of the **debug http proxy** command as follows:

```
Oct 28 12:25:12 Content Engine 3: Rule action no-url-filtering match -
Bypassing urlfiltering
```

If the **rule action no-url-filtering** rule is matched and SmartFilter URL filtering is being used instead of Websense URL filtering, the output of the **debug http proxy** command would be as follows:

```
Oct 28 12:25:12 Content Engine 3: Rule action no-url-filtering match -
Bypassing SmartFilter processing
```

When the Content Engine receives an HTTP or HTTPS request for websites other than “foo.com” (for requests that have “www.abc.com” as the domain), the **rule action no-url-filtering** rule is not matched. Consequently, the Content Engine proceeds with Websense URL filtering for that particular request as shown in the partial output of the **debug http proxy** command as follows:

```
Oct 28 12:28:06 Content Engine 3: Rule action no-url-filtering not hit -
Proceed with urlfiltering
```

If the **rule action no-url-filtering** rule is not matched and SmartFilter URL filtering is being used instead of Websense URL filtering, the output of the **debug http proxy** command would be as follows:

```
Oct 28 12:25:12 Content Engine 3: Rule action no-url-filtering not hit-
Proceed with SmartFilter processing
```

Execution Order of Rule Actions

In the ACNS 5.2.3 software and later releases, the order in which the rule actions are executed is as follows:

1. Redirect-url-for-cdn (this action is only applicable for Content Engines that are registered with a Content Distribution Manager and is not applicable for standalone Content Engines)
2. No-auth (before authentication using RADIUS, LDAP, or NTLM)
3. Reset
4. Block
5. Redirect (before cache lookup)
6. Rewrite (before cache lookup)
7. No-url-filtering
8. Refresh (after cache lookup, in the case of a cache hit)
9. Freshness-factor (after cache lookup, in the case of a cache hit)
10. Use-server
11. No-proxy

12. Use-proxy-failover
13. Use-proxy
14. Use-dns-server
15. ToS/DSCP server (ToS bits on the connection to the server)
16. ToS/DSCP client (ToS bits on the connection that the server uses to send a response to the client)
17. DSCP client cache-miss
18. DSCP client cache-hit
19. Insert-no-cache
20. No-cache
21. Cache (when the response is received from the server)
22. Selective-cache (when the response is received from the server)
23. Append-username-header
24. Use-icap-service
25. Use-xforward-clt-ip
26. No-persistent-connection
27. Cache-cookie
28. No-selective-cache
29. Allow

Configuring URL-Based Monitoring

This documentation update applies to the following three ACNS 5.2 software guides:

- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Configuration Guide for Locally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Command Reference, Release 5.2*

CLI Enhancements for URL-Based Monitoring

In the ACNS 5.2.3 software, the ability to configure a Content Engine to monitor the performance of specific URLs was added. In order to support this new feature, the following CLI changes were made:

- The **http monitor url** *url* global configuration command. This command enables you to specify up to 10 URLs that you want the Content Engine to monitor. The Content Engine maintains statistics about the various response characteristics for each of the monitored URLs. (You can use the new **show statistics http monitor** command to view these statistics, as described later in this section.)

```
ContentEngine(config)# http monitor url ?
WORD URL for monitoring
```

The **http monitor url** *url* command has two command options, the **acceptable-delay** and **interval** options. As the following sample output indicates, the **acceptable-delay** option is used to specify the acceptable delay in seconds (the maximum number of seconds that the specified monitored URL should be retrieved within). The default acceptable delay is 60 seconds.

```
Content Engine(config)# http monitor url http://www.abc.com/ ?
  acceptable-delay Threshold time in seconds before which the URL
  should be retrieved. (default is 60 seconds)
  interval          Interval in seconds for monitoring the URL.
  (default is 60 seconds)
<cr>
```

As the following sample command output indicates, the **acceptable-delay** option is used to specify the acceptable delay, which is the maximum number of seconds that the specified URL should be retrieved within.

```
Content Engine(config)# http monitor url http://www.abc.com/ acceptable-delay ?
<1-3600> Acceptable delay in seconds
```



Note If you use the **http monitor url** *url* command to configure the same URL with a different interval or acceptable-delay setting, the most recently configured setting takes precedence and overrides any previously configured settings for that particular URL.

As the following sample command output indicates, the **interval** option specifies the monitoring interval (that is, how frequently the Content Engine should monitor requests for a specific URL). The monitoring interval is specified in seconds. The default monitoring interval is 60 seconds.

```
ContentEngine(config)# http monitor url http://www.abc.com/
acceptable-delay 100 interval ?
<1-3600> Monitor interval in seconds
```

In the following example, the Content Engine is configured to monitor the URL named “http://www.abc.com/” using the default values (an interval of 60 seconds and an acceptable delay of 60 seconds).

```
ContentEngine(config)# http monitor url http://www.abccorp.com/
```

In the following example, the Content Engine is configured to monitor the URL named “http://www.abc.com/.” The Content Engine is configured to wait up to 100 seconds for the URL to be retrieved and to monitor requests for this URL every 100 seconds.

```
ContentEngine(config)# http monitor url http://www.abc.com/
acceptable-delay 100 interval 100
```

If it takes more than 100 seconds for the URL to be retrieved, the specified acceptable delay is exceeded. The Content Engine tracks the response time (minimum and maximum delay time) as well as the number of times that the acceptable delay is exceeded for a particular URL. These statistics are shown in the output from the new **show statistics http monitor** EXEC command. (An example of the output from the **show statistics http monitor** EXEC command is provided below.)

- The **show statistics http monitor** EXEC command was added to enable you to display statistics for the monitored URLs. As the following example shows, the following statistics are reported for each of the monitored URLs:

```
ContentEngine# show statistics http monitor
HTTP Monitor URL statistics
-----

Monitor URL                = http://www.abc.com/
Total requests              = 118
Failed requests             = 30
Requests above acceptable delay = 37
Minimum response time      = 8.183 seconds
Maximum response time      = 210.021 seconds

Monitor URL                = http://www.abccorp.com/
Total requests              = 275
Failed requests             = 44
Requests above acceptable delay = 26
Minimum response time      = 0.071 seconds
Maximum response time      = 164.061 seconds
```

“Failed requests” are requests that did not succeed (for example, the request failed to resolve the domain name of that URL).

“Requests above acceptable delay” are the requests that took longer than the specified acceptable delay (the maximum number of seconds specified by the acceptable-delay setting).

Downgrading ACNS 5.x Software

This documentation update applies to the following three ACNS 5.2 software guides:

- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Configuration Guide for Locally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Command Reference, Release 5.2*

If you have configured the mediafs with the ACNS 5.1 software and later releases, and then downgrade to the ACNS 5.0 software, the mediafs disk space assignment is lost and it reverts to cdfs disk space. For more information, see the [“Media File System Issues When Downgrading to the ACNS 5.0 Software” section on page 3](#).

If the local (internal) Websense server is enabled on the Content Engine and you downgrade from the ACNS 5.2.x software to either the ACNS 5.0 software or the ACNS 5.1 software, the WebsenseEnterprise directory is removed from the Content Engine and the local Websense server stops working. For more information, see the [“Websense Issues When Downgrading to the ACNS 5.0 Software or the ACNS 5.1 Software” section on page 4](#).

Related Documentation

Your product shipped with a minimal set of printed documentation. The printed documentation provides enough information for you to install and initially configure your product.

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*

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*
- *Cisco Content Engine 511 and 566 Hardware Installation Guide*
- *Cisco Content Engine 510 and 565 Hardware Installation Guide*
- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Cisco Content Distribution Manager 4630 Hardware Installation Guide*
- *Cisco Content Router 4430 Hardware Installation Guide*
- *Cisco Content Networking Hardware Installation Guide for the Seven-Rack Unit Chassis*

Software Documentation

- *Documentation Guide and License and Warranty for Cisco ACNS Software, Release 5.2*
- *Cisco ACNS Software Configuration Guide for Centrally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Configuration Guide for Locally Managed Deployments, Release 5.2*
- *Cisco ACNS Software Command Reference, Release 5.2*
- *Cisco ACNS Software API Guide, Release 5.2*
- *Cisco IP/TV Release 5.2 Addendum*
- *Cisco ACNS Software Program Manager for IP/TV User Guide, Release 5.1*
- *Release Notes for Cisco IP/TV, Release 5.2*

Online Help

- Content Distribution Manager GUI online help system for centrally managed ACNS networks
- Content Engine GUI online help system for locally deployed Content Engines

**Note**

The term “locally deployed Content Engine” refers to a Content Engine that was initially configured with the autoregistration feature turned off so that the Content Engine would not automatically register with the Content Distribution Manager. Because the Content Engine did not register with the Content Distribution Manager, it can be individually managed through the Content Engine CLI or GUI as a locally deployed device. The Content Engine GUI allows you to remotely configure, manage, and monitor locally deployed Content Engines through your browser.

The Content Distribution Manager GUI and the Content Engine GUI both have context-sensitive online help that can be accessed by clicking the **HELP** button.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

- Instructions for ordering documentation using the Ordering tool are at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) 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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

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

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0502R)

