



Release Notes for Cisco ACNS Software, Release 5.2

August 4, 2005

ACNS Build 5.2.1-b7



Note

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

Contents

These release notes contain information about the Cisco Application and Content Networking System (ACNS) software, Release 5.2. These release notes describe the following topics:

- [Introduction, page 2](#)
- [New and Changed Information, page 2](#)
- [Important Notes, page 11](#)
- [Caveats, page 15](#)
- [Documentation Updates, page 38](#)
- [Related Documentation, page 39](#)
- [Obtaining Documentation, page 40](#)
- [Documentation Feedback, page 41](#)
- [Cisco Product Security Overview, page 41](#)
- [Obtaining Technical Assistance, page 42](#)
- [Obtaining Additional Publications and Information, page 44](#)



Corporate Headquarters:

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

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

Introduction

ACNS software combines the technologies of demand-pull caching and pre-positioning for accelerated delivery of web applications, objects, files, and streaming media; 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 ACNS 5.2 software. These release notes describe the new product features, the supported hardware, and the open and resolved caveats regarding ACNS software, Release 5.2.

New and Changed Information

This section describes new and changed features in the ACNS 5.2 release. It also lists the supported hardware.

New Features

[Table 1](#) lists the new features in ACNS software, Release 5.2.

Table 1 **New Features in ACNS 5.2 Software**

Feature Type	Features
Feature-rich server and proxy HTTP server and proxy	<ul style="list-style-type: none"> • Demand-pull caching features: <ul style="list-style-type: none"> – Forward and reverse proxy caching – Transparent (Web Cache Communication Protocol [WCCP] Version 2), nontransparent (browser proxy configuration), and Layer 4 redirection – HTTP 1.0 and 1.1 web caching, FTP-over-HTTP proxy, HTTPS tunneling, and Internet Cache Protocol (ICP) – Caches files served with HTTP 1.1 chunked encoding – Rules Template for cache policies and rules – Type of Service (ToS) and differentiated services code point (DSCP) set by a cache hit or cache miss, URL, file type, or domain to classify traffic using the Rules Template – IP spoofing that presents clients IP addresses for easy tracking of users – Split DNS that allows you to configure a Content Engine with multiple DNS servers based on domain name – DNS caching that enables the Content Engine to cache DNS entries to avoid multiple WAN accesses for DNS server resolution (for proxy and WCCP mode) • Content pre-positioning features: <ul style="list-style-type: none"> – Web content preloading through the CLI or the local Content Engine GUI – For a small number of Content Engines, preload HTTP, FTP, and Microsoft Media Server (MMS) files through preload URL list files – Intelligent content pre-positioning through content acquisition and distribution – For a large number of Content Engines, HTTP delivery of static files for any file format that is managed by the Content Distribution Manager • Bandwidth controls, day-of-week and time-of-day scheduling, replication status, and authentication support

Table 1 *New Features in ACNS 5.2 Software (Continued)*

Feature Type	Features
HTTPS server and proxy	<ul style="list-style-type: none"> • Terminates and stores content served through HTTPS (Secure Socket Layer [SSL]) at branch offices <ul style="list-style-type: none"> – SSL termination of SSL 2.0, 3.0, TLS 1.0 – Cost-effective software-based termination of HTTPS for up to 200 users – Transparent (WCCP) or proxy configuration support – Demand-pull caching and pre-positioning support – Backend SSL support to origin servers – Secured import and storage of keys and certificates with certificate management GUI – Support of all major certificate authorities for origin server certificates (for example, Verisign and Entrust) for reverse proxy SSL as well as enterprise self-issued certificates for forward proxy SSL – Maximum of 255 key pairs (keys and certificates) supported – Bulk encryption supported: RC4, DES, DES3 – Hash algorithm supported: MD5, SHA1
Native FTP proxy	<ul style="list-style-type: none"> • Native FTP (port 20, 21), active and passive modes • Demand-pull caching supported <ul style="list-style-type: none"> – Transparent (WCCP) redirection support with basic authentication – Transactions logged to HTTP logs
Native TFTP server and gateway	<ul style="list-style-type: none"> • Serving of software images and configuration files to routers, switches, IP phones, and set top boxes (STBs) • Demand-pull caching and pre-positioning supported • Non-transparent (proxy) redirection supported • Content expiration, logs, and backend HTTP authentication supported
Windows file system server	<p>Access files from a Windows file share with Common Internet File System (CIFS) file path support</p> <ul style="list-style-type: none"> • Pre-positioning supported, including the ability to acquire files from a Windows file share for distribution to the edge • Access control, NTLM user authentication, and access logs supported
NFS/CIFS	<ul style="list-style-type: none"> • Content Engine acts as a Network File System (NFS)/CIFS client and mounts file systems from a network-attached storage (NAS) device as external storage • Pre-positioned content, and Windows Media Technologies (WMT) and RealProxy content supported

Table 1 ***New Features in ACNS 5.2 Software (Continued)***

Feature Type	Features
Comprehensive streaming media support	<ul style="list-style-type: none"> • Concurrent streaming of RealNetworks, WMT, Cisco Streaming Engine (compatible with Apple Computers QuickTime and MPEG-4), and HTTP <ul style="list-style-type: none"> – Live splitting (auto setup with tree structure and live event scheduling GUI), IP multicast, and video on demand (VOD) can all be delivered in both proxy and server mode for RealNetworks, WMT, and the Cisco Streaming Engine – Rule-based filtering for MMS and the Real-Time Streaming Protocol (RTSP) – Streaming bandwidth throttles, including restrictions based on the time of day for all streaming protocols • Cisco Streaming Engine: (no additional license fee) <ul style="list-style-type: none"> – VOD server for standards-based hinted MPEG-4, MPEG-2, MPEG-1, and QuickTime video over RTP/RTSP to Apple Computer QuickTime-compatible players – Live-stream pull splitting (unicast in) and push splitting (multicast or unicast in) with multicast and unicast out of the Content Engine to the connected clients – Interoperates with IP/TV 5.2 Broadcast Server, IP/TV Program Manager, and IP/TV Viewer – Standards-based (ISO/IEC) MPEG encoder interoperability: Compatible with ISO/International Electrotechnical Commission (IEC) MPEG-4 Advanced Simple AV Profile (ISMA v1.0) and ISO/IEC MPEG-4 Advanced 2D level 1 as well as MPEG-1 and MPEG-2 profiles • RealNetworks Helix Universal Gateway (additional license fee) <ul style="list-style-type: none"> – RealNetworks RTP/RTSP delivery over TCP or User Datagram Protocol (UDP) – Live-stream pull splitting (unicast in) and push splitting (multicast or unicast in) with multicast and unicast out of the Content Engine to the connected clients – Encoder failover – Content pre-positioning for VOD streaming of RealNetworks format of RTP/RTSP content – Support for MMS, QuickTime, and RTSP through manual configuration • Microsoft Windows Media server and proxy (additional license fee) <ul style="list-style-type: none"> – Windows Media MMS delivery over TCP, UDP, or HTTP – Content pre-positioning for VOD streaming – Variable-bit-rate support – Content Engine as a live stream source (publishing point) – Support for live-stream pull splitting, including multicast or unicast into the Content Engine and multicast or unicast out of the Content Engine to connected clients – Certified by Microsoft – Windows Media Version 9 encoder interoperability for MMS, including Windows Media Codec Version 7, 8, and 9 – WMT upstream proxy bandwidth controls – Fast start support through MMS-over-HTTP • HTTP paced delivery of MPEG, Advanced Streaming Format (ASF), RealNetworks and QuickTime movie format files

Table 1 *New Features in ACNS 5.2 Software (Continued)*

Feature Type	Features
MPEG video display for retail kiosks	<ul style="list-style-type: none"> • Predefined playlists with multiple video clips and time-of-day setting, centrally managed by the Content Distribution Manager, multiple playlists per Content Engine • One video stream per audio video (AV)-decoder card option or Content Engine: integrated MPEG-1 and -2 decoders, National Television Standards Committee (NTSC) and Phase Alternating Line (PAL) TV output • Set top box (STB) interoperability: <ul style="list-style-type: none"> – Playlists exported to STBs through the program application programming interface (API) – Content Engine acts as the TFTP server for set top box software image and configuration files
Powerful streaming automation	<ul style="list-style-type: none"> • Program import, export, scheduling API: <ul style="list-style-type: none"> – XML-based API for creating, managing, and scheduling programs – Live and scheduled rebroadcast, multicast, and stream splitting programs support – Cisco Streaming Engine and WMT support – Playlists exported to set top boxes • Manifest API <ul style="list-style-type: none"> – XML-based API to manage pre-positioning of video files for VOD serving by the Content Engines, including bandwidth, content expiration and user authentication policies for acquisition, distribution and stream serving – Cisco Streaming Engine, WMT, and RealNetworks protocol and file formats support • Live streaming redundancy <ul style="list-style-type: none"> – Redundant encoders specified in the program API or live event scheduling GUI – Root Content Engine failover: contact origin server – Intermediate Content Engine failover: go to parent Content Engine or fail over to other Content Engines in the same location – Client Content Engine failover: roll over to unicast from multicast, includes next-click failover
Turnkey IP/TV software, Release 5.2 integration	<ul style="list-style-type: none"> • ACNS software and Content Engine replace IP/TV Archive Server • Interoperates with IP/TV Release 5.2 Broadcast Server and extends its reach to multicast islands with Cisco Streaming Engine stream splitting and streaming automation • IP/TV software, Release 5.2 Program Manager: <ul style="list-style-type: none"> – Inserts content into an ACNS network using the manifest file and the program API – IP/TV Program Manager as a personality of the Content Engine – Publishes URLs to QuickTime players and IP/TV Release 5.2 Viewers

Table 1 ***New Features in ACNS 5.2 Software (Continued)***

Feature Type	Features
Superior management	<p>Scalable content acquisition and distribution</p> <ul style="list-style-type: none"> • Content acquisition from origin servers by root Content Engines for HTTP, HTTPS, FTP, MMS, and CIFS (Windows file sharing) • Easy to use GUI that builds an acquisition list of origin server files or web pages to crawl • Channel-based control with bandwidth-shaping, priority, scheduling, content expiration, and authentication policies • Secured content distribution with HTTPS • Hierarchical tree distribution for scalability and optimal performance • Multicast replication option available (additional license fee) with intelligent on-demand carousels for retransmissions and hot standby multicast sender failover <p>Multiple, flexible client request redirections:</p> <ul style="list-style-type: none"> • Transparent edge intercept with advanced WCCP Version 2 that includes the following: <ul style="list-style-type: none"> – Scalable clustering (WCCP flow protection and WCCP slow start) – Fault tolerance (WCCP multihome router support and client bypass) – TCP tuning knobs – WCCP standby mode for easy maintenance • Nontransparent edge intercept with browser proxy configuration, including support for proxy autoconfiguration (PAC) file delivery by Content Engines • Content routing with DNS intercept and HTTP redirect with the Content Router that uses the coverage zone file to specify the client source-IP addresses and which Content Engines serve that zone • Dynamic proxy autoconfiguration uses coverage zone information to automatically generate custom PAC files at Content Engines designated as PAC file servers to redirect client browsers to local Content Engines • CLI similar to that of Cisco IOS software for individual Content-Engine and Content Distribution Manager-configuration management • Interactive setup utility that is available through the CLI • Online Quick Start wizards that are available through the Content Distribution Manager GUI • Integrated graphical alert system for proactive warning of problems with devices or content replication • Remote device management <ul style="list-style-type: none"> – Role-based administration – Device group configuration – Autoregistration of devices from the Content Distribution Manager GUI

Table 1 *New Features in ACNS 5.2 Software (Continued)*

Feature Type	Features
	<ul style="list-style-type: none"> • Extended SNMP Version 2 and Version 3 MIBs • Local Content Engine GUI, SSH Version 1 and 2, HTTPS, and Telnet access • CiscoWorks2000 Resource Management Essentials (RME) Version 3.4 support for Content Engines and Content Distribution Manager: CLI editor, inventory, network configuration, syslog analyzer, and device availability • CiscoWorks2000 CiscoView support of Content Engines: a graphical SNMP-based device management tool that provides real-time views of the operational status of Content Engines • Comprehensive industry-standard logging <ul style="list-style-type: none"> – Transaction logging and log pushing through FTP, interoperate with reporting partners for customizable performance and activity reports – HTTP cache transaction logs: Squid logs, W3C-compliant Apache common logs – WMT proxy and server logs: standard WMS Version 9 format – RealServer and proxy logs: standard RealNetworks format – Configurable log formats: referrer headers and user agent headers
Secure content access management	<ul style="list-style-type: none"> • Administrator authentication <ul style="list-style-type: none"> – RADIUS and TACACS+ client authentication against an Lightweight Directory Access Protocol (LDAP) or Active Directory database – TACACS+ supports authentication and accounting • User authentication <ul style="list-style-type: none"> – RADIUS and TACACS+ client authentication against an LDAP or Active Directory database – Full NT LAN Manager (NTLM) authentication for the following: NTLM object caching, NTLM pass-through, and user authentication for WMT streaming • Basic, NTLM, and LDAP authentication against an Active Directory database. Basic and NTLM authentication against Windows NT domain controller (DC). Both user and group authentication are supported. • Load balancing of NTLM domain controllers for scalability and redundancy • NTLM authentication supported for demand-pull caching and pre-positioning • LDAP enhancements <ul style="list-style-type: none"> – LDAP password expiration – iPlanet single sign-on – LDAP attribute for accept use policy

Table 1 ***New Features in ACNS 5.2 Software (Continued)***

Feature Type	Features
	<ul style="list-style-type: none"> • Web filtering (URL and file type) <ul style="list-style-type: none"> – Websense Enterprise Version 5.2 server and client content-filtering support on Content Engine (additional per 100-user license fee)—Embedded in the Content Engine and does not require a separate (external) Websense server. Websense Version 5.2 includes dynamic protocol management for instant messaging, peer-to-peer and malicious applications, bandwidth optimizer, real-time analyzer, file type management and central policy distribution, and a network agent that runs on the Content Engine. – Secure Computing SmartFilter Version 4.0 server and client content-filtering support (additional per-user license fee)—On-box (internal) Content Engine solution that does not require separate SmartFilter server. Administrator Console Version 4.0 is enhanced for central device policies, LDAP group-authentication support and extensive customizable reporting tools. – N2H2 Internet Filtering Protocol Version 1.0 client content-filtering support on Content Engine—Requires a separate (external) N2H2 server.
ICAP Version 1.0	<ul style="list-style-type: none"> • Scales antivirus servers and caches clean content • Request modification (REQMOD) and response modification (RESPMOD) supported • Load balancing and failover of ICAP servers • Demand-pull caching and pre-positioning supported • Tested with Trend Micro and Symantec antivirus products • Access control lists (ACLs) to control access to Content Engine interfaces <ul style="list-style-type: none"> – Permit or deny Telnet, SSH, SNMP, TFTP, WCCP, and Content Distribution Manager traffic per interface – Standard and extended IP access lists for inbound and outbound traffic
Alarm reporting	<p>ACNS applications can now raise and clear alarms to report failures detected within the ACNS software or hardware.</p> <ul style="list-style-type: none"> • Alarms are classified by severity (critical, major or minor) depending on their impact • Notification mechanisms include the following: <ul style="list-style-type: none"> – ACNS devices can be configured to send SNMP traps to your SNMP manager when alarms are raised or cleared. This informs you about problems as they occur, and enables you to respond more quickly. – If you are using a Content Distribution Manager to manage your ACNS system, the new system status bar notifies you when there are alarms on the managed ACNS devices, regardless of whether SNMP traps are configured. The status bar, which is always visible when you are logged into the Content Distribution Manager GUI, automatically refreshes every two minutes to reflect changes in the alarm status for all the managed ACNS devices. – Each ACNS device supports a set of CLI commands that enables you to obtain alarm status and details on demand.

Table 2 lists the caching, filtering, and authentication mechanisms supported by standalone Content Engines (Content Engines that are not registered with a Content Distribution Manager) or registered Content Engines that are running ACNS software, Release 5.2 or later.

An asterisk (*) indicates that a feature is supported for that particular protocol for standalone Content Engines as well as registered Content Engines. WCCP means transparent support. Content Engines also support local list filtering with all of the listed protocols except for FTP-WCCP (native FTP).

Table 2 Caching, Filtering, and Authentication Mechanisms – Support Matrix with Respect to Different Protocols

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

Hardware Supported

ACNS software, Release 5.2 supports the following hardware platforms. All of the listed platforms also support ACNS software, Release 5.1.x 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 software, Release 5.2, do not support 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

Important Notes

This section emphasizes important information regarding ACNS 5.2 software.

Media File System Issues When Downgrading to ACNS 5.0 Software

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

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

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

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

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

WebSense Issues When Downgrading to ACNS 5.0 Software or ACNS 5.1 Software

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

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

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

Changes to WCCP Support

In ACNS software releases earlier than Release 5.2, a maximum of eight active WCCP services were supported by a WCCP Version 2-enabled router and a Content Engine. In ACNS 5.2 software, up to 25 active WCCP Version 2 services can be supported. In 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 3](#). All of the services except for the standard web-cache service (service 0) requires that WCCP Version 2 (instead of WCCP Version 1) be running on the router and the standalone Content Engine for a particular WCCP service to be supported. These services are called “predefined” WCCP services.

Table 3 Supported WCCP Services with ACNS Software, Release 5.2

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

Table 3 Supported WCCP Services with ACNS Software, Release 5.2 (Continued)

Service Number	Service Name	Type of Service	Service Description
80	rtsp	Predefined	<p>Media caching service that permits WCCP Version 2-enabled routers to redirect RTSP client requests transparently to a single port on a Content Engine (RealMedia transparent caching).</p> <p>The Content Engine listens for redirected RTSP requests on the standard RTSP port (default port 554). To intercept RTSP traffic on ports other than the default port (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 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 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>
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	<p>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).</p>
99	reverse-proxy	Predefined	<p>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).</p>

Multicast File Transfer Enhancements

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 (Release 5.0 and Release 5.1), 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 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 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 it has already received.



Note

Because of these enhancements, receivers using ACNS 5.2 software *cannot* interact with senders using 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 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 ACNS 5.2 software first and then upgrade your receivers to ACNS 5.2 software.

Caveats

This section lists and describes the open and resolved caveats in ACNS software, Release 5.2. Caveats describe unexpected behavior in ACNS 5.2 software. Severity 1 caveats are the most serious; Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

Open Caveats - ACNS Software, Release 5.2

This section lists caveats that have not been resolved in ACNS software, Release 5.2. The open caveats are grouped into two categories:

- [Open ACNS-IP/TV Software Integration Caveats, Release 5.2](#)
- [Other Open ACNS Software, Release 5.2 Caveats](#)

Open ACNS-IP/TV Software Integration Caveats, Release 5.2

This section lists and describes the caveats that are open in ACNS software, Release 5.2, 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 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 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 Software, Release 5.2 Caveats

This section lists and describes the caveats that are open in ACNS software, Release 5.2 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 ACNS 5.1b300 software to ACNS 5.0.7b8 software.

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

Conditions: 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 is visible if you enter the **cdnfs browse EXEC** command on the Content Engine).

Conditions: This problem is rare and only occurs when the file system corruption has caused a directory entry that should be a file to actually be a subdirectory. This only occurs 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 only occurs 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 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>', swaw '^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.

A way to test this is to use the `cdnfs lookup url EXEC` command and 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 using 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; this queries 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%.

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: 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 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 ACNS software, Release 5.1.x or earlier, and these Content Engines are registered with a Content Distribution Manager that is running ACNS software, Release 5.2.

Workaround: Upgrade the Content Engines to ACNS software, Release 5.2. Currently, a Content Distribution Manager that is running ACNS software, Release 5.2 does not propagate some configuration changes to Content Engines that are running ACNS software releases earlier than Release 5.2. Therefore, Content Engines that are running ACNS software, Release 5.1.x 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 ACNS 5.2 software to 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 ACNS 5.1 software does not support SMB file acquisition, the root Content Engine running 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 ACNS 5.2 to 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 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: 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 which are running ACNS software, Release 5.0 or later, 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 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 6000 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 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 only occurs 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 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 only occurs when the ICAP service is enabled on the Content Engine.

Workaround: There is no known workaround.
- CSCef44726

Symptom: Chunked responses sent by the origin server are received by the client without chunking and without the content length information. Even though this can cause certain browsers not to work properly, the major browsers seem to work properly in this situation.

Condition: This problem occurs only when ICAP 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.

Condition: 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 configuration.

- CSCef61845
Symptom: Unicast access to a live program does not work.
Condition: This problem only occurs 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.
- CSCef65579
Symptom: When HTTP authentication is enabled on the Content Engine, the syslog.txt file fills up with error messages that report that the servers are dead.
Condition: This problem can occur if an LDAP or TACACS+ server is authenticating HTTP requests.
Workaround: There is no known workaround.
- 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 can occur in any of the following situations:
 - 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 only occurs when 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 ACNS software, Release 5.2.
Conditions: 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.

- 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 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 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 issuing 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 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, 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 Software, Release 5.2

This section lists caveats that have been resolved in ACNS software, Release 5.2. The resolved caveats are grouped into the following categories:

- [ACNS-IP/TV Software Integration Resolved Caveats, page 27](#)
- [Acquisition and Distribution Resolved Caveats, page 29](#)
- [Proxy and Caching Resolved Caveats, page 30](#)
- [Management Resolved Caveats, page 32](#)
- [Request Processing Resolved Caveats, page 34](#)
- [DNS Resolved Caveats, page 34](#)
- [ICAP Resolved Caveats, page 34](#)
- [Media and Streaming Resolved Caveats, page 35](#)
- [Rules Resolved Caveats, page 37](#)

ACNS-IP/TV Software Integration Resolved Caveats

- CSCec65255

The audio stream sounds discontinuous when you listen to a rebroadcast or video on demand (VOD) of a recorded MP4 file. The problem occurs with IP/TV-generated MP4 files that are streamed from a Cisco Streaming Engine. The problem only occurs with MP4 files that contain an MP3 audio track sampled at 8000 Hz. Streaming the file directly from IP/TV Server does not result in this problem.
- CSCec74830

Some versions of IP/TV software supported Japanese characters encoded in Windows native Shift JIS encoding. For IP/TV software, Release 5.1, Shift JIS Japanese data is applied to the following data items:

 - For on-demand programs, Category name - Program name - Description - Administrator name - Producer name - Scheduled Program - Channel name - Program name - Description - Administrator name - Producer name Japanese characters are corrupted in all on-demand program data items.
 - For scheduled program data items, only certain characters (for example, the small circle and code point 0x818B) are corrupted. Microsoft Internet Explorer and Netscape Navigator support UTF-8 encoding, in which Japanese characters are available.

With UTF-8, all Japanese data are corrupted for both on-demand and scheduled programs even though they are corrupted in different ways. This problem can occur with multibyte Japanese text for on-demand program information (for example, the category name and the program name). Also for scheduled programs, certain Shift JIS Japanese characters are corrupted (for example, the channel name and program name), even though the other characters are saved and restored correctly.
- CSCee13486

IP/TV Program Manager should restrict the recording of a live split-only program.

- CSCee35120

When you upgrade IP/TV software, Release 3.5 to Release 5.1, the functionality of the IP/TV Archive Server is replaced by Content Engines in the ACNS network. The Content Engines requires that the content be present on an IP/TV Broadcast Server. However, IP/TV Broadcast Servers often have limited disk space. This problem is only applicable if you plan to upgrade from IP/TV Release 3.5 to Release 5.1 software, which requires that you use IP/TV Broadcast Servers that have limited disk space.
- CSCee77479

Integration of IP/TV and an ACNS network requires communication between IP/TV Program Manager and the ACNS Content Distribution Manager. You must enter the Content Distribution Manager username and password in the IP/TV Program Manager Preferences window. If the Content Distribution Manager password contains a dollar sign (“\$”), the IP/TV Program Manager does not obtain the Content Distribution Manager data (for example, the channel [live or VOD] information).
- CSCef38189

An ACNS network import operation fails if IP/TV program names contain Japanese characters. Scheduled programs with Japanese names cannot be associated with ACNS channels. Creation of a Japanese scheduled program with ACNS channel information is successful. However, immediately after creation of the program, the import status of the program in the Scheduled Program window changes to “Failed.” Clicking the **Import Status** link shows the following error information:

```
Associated programs at ACNS CDM is not created.
```
- CSCef38218

The IP/TV Content Manager to IP/TV Program Manager Migration utility fails with program names that contain Japanese characters. Migration of such programs from IP/TV Content manager Release 3.5 to IP/TV Program Manager Release 5.2 fails, and IP/TV Program Manager’s scheduled program and on-demand windows report error messages. This problem occurs when the scheduled or on-demand program contains Japanese characters.
- CSCef61043

IP/TV scheduled programs that contain a Japanese name, administrator name, or description corrupt specific characters. In the IP/TV scheduled programs information GUI, certain characters in the Japanese program name, administrator name, and description are displayed as dots.

If Japanese program, administrator names, or description of the IP/TV scheduled program contain a double byte character set with a second byte of 0x5E or 0x7C, the double byte character set is displayed as a dot. Single byte character set ASCII characters of 0x5E, 0x7C (^, l) also are corrupted (displayed as “?”) when used for these data items.
- CSCin63849

A file transfer scheduled from IP/TV Program Manager fails. This problem can occur if you initially entered the wrong password in IP/TV Program Manager for an IP/TV Server (using the File Transfer Information section of the Server Information window) and then later corrected the password.
- CSCin63942

IP/TV Program Manager generates a “database inconsistent” error. This problem occurs if the “#” character is entered as part of the username.
- CSCin70882

For ACNS-based IP/TV scheduled programs that use live-split-only content delivery mode, the IP/TV Program Manager allocates multicast addresses to individual streams that are never used along the content delivery path. The problem occurs with live-split-only programs.

- CSCin71201
While a live program is defined in an ACNS environment, the “Capture Live MPEG Data for Recording to File; Do Not Multicast” option should be removed.
- CSCin71634
After you edit a defined recording on IP/TV Program Manager, the server is not updated. This problem only occurs when you edit the recording and then change the destination server.

Acquisition and Distribution Resolved Caveats

- CSCec52246
If you click the **Fetch Manifest** button twice in the Channel window of the Content Distribution Manager GUI and some of the HTML links on the web server were removed, these removed links are not deleted in ACNS. This problem occurs if you click the button a second time before the recrawl operation is finished, because this causes the acquirer to abort the crawl job and start another recrawl. If some links are removed from the HTML files on the web server, these links should be removed in ACNS software. However, if the first recrawl operation is aborted, the second recrawl does not delete these removed links.
- CSCed76727
The Content Engine acquirer is always in full reload mode if the last item in the manifest file is an expired item. This problem occurs with ACNS software, Release 5.0.x and 5.1.x.
- CSCee55993
If a filename has a question mark (“?”), ACNS software fails to pre-position such files.
- CSCee60082
The Content Router only uses the default coverage zone, and ignores (or does not retrieve) the coverage zone file that the Content Router was configured to use. This problem occurs if the primary Content Distribution Manager has been taken down, and the secondary Content Distribution Manager was configured as the new primary Content Distribution Manager. But the Content Routers were not configured to point to the IP address of the new primary Content Distribution Manager. Even though ACNS devices should normally failover to use the secondary address, that does not occur for the Content Router that is fetching the coverage zone file.
- CSCee64255
Even though you increase the channel disk quota, the acquisition of some content fails. An “exceed disk quota” error message is reported. This problem occurs if you increase the disk quota during the crawling, and ACNS software, Release 5.1.x is being used.
- CSCee68315
Some content in the ACNS network is deleted when the fully qualified domain name (FQDN) is swapped between two websites that are configured for two different channels. This problem occurs when the contents in both of the the channels have the same relative ACNS network URL. If the FQDN is changed, some contents are deleted.
- CSCee69664
If half of the content in a channel is deleted, some content (for example, database records and UNS objects) may be removed if the deletion is interrupted midway by stop-ad and when it comes back, the channel is subscribed again.

- CSCee70790
There is a slight difference in the output of the **show statistics replication** and **show statistics acquirer EXEC** commands in ACNS 5.1.x software with regard to the replication status disk quota. The output of the **show statistics replication** command displays the correct information.
- CSCef11301
The **show statistics distribution mcast-data-send detail EXEC** command shows that the multicast sender is not making any progress even though several files are ready to be sent. This problem occurs if multicast is enabled on a multicast sender and the Content Engine clock has been changed.
- CSCef43905
When you use the **acquirer stop-channel** command to suspend the content acquisition for a channel at the root Content Engine, some contents may be inadvertently removed. This problem can occur if you enter this command at the end of a crawl job after it completes a successful recrawl. This problem only occurs with ACNS software, Release 5.1.x.
- CSCin59084
If there is a WCCP transparent proxy between the ACNS network root Content Engine and the content origin server, and the proxy requires NTLM authentication, then the ACNS network acquirer may fail to acquire content in the following scenario:
 1. You specify the WCCP transparent proxy authentication information by using the **acquirer proxy authentication transparent** global configuration command. Content acquisition works correctly.
 2. You remove the proxy authentication through the **no acquirer proxy authentication transparent** command. Content acquisition stops working, which is the expected behavior.
 3. You restore proxy authentication using the **basic-auth-disable** option of the **acquirer proxy authentication** command. Content acquisition should work, but it does not. Content acquisition results in a 401 error message.

This problem can occur with ACNS 5.1.x software.
- CSCin66906
The primary multicast sender continues to send heartbeat messages to the backup multicast sender Content Engine even though you entered the **no multicast enable** command on the primary sender Content Engine.

Proxy and Caching Resolved Caveats

- CSCed06490
When the ACNS system receives a request that has a long URL (one that is over 2 KB), it does not log the domain and IP address. Users may be interested in knowing the source domain and IP address, for tracking purposes. If there was a denial of service attack on the system, logging of such URLs in the system log could be quite useful in tracing the source of the attack.
- CSCed60193
If you reload a CE-7325, cfs content is lost on the Content Engine.
- CSCed66871
If you configure the Content Engine to use port 485 as the HTTP proxy outgoing port, the Content Engine cannot use this port as its outgoing HTTP proxy port unless you also enter the **http destination-port allow 485** global configuration command on the Content Engine.

- CSCed75666
The output of the **show statistics cfs EXEC** command regarding the disk labels can show misleading information about where the cfs volumes are located.
- CSCef20911
The Content Engine can generate a core file if it is handling a high load of traffic or if CPU utilization is high. The core file is in the core_dir directory, and cache restart messages appear in the system log. However, the cache process automatically restarts on the Content Engine.
- CSCef29584
The Content Engine can stop accepting connections (if it is operating in proxy mode), or go in and out of overload bypass mode (if it is operating in WCCP mode). If this problem occurs, syslog messages such as the following are reported:

```
Thread 1 really low memory
```


or

```
Thread 2 really low memory
```
- CSCef34798
Certain TN3270 applications (that is, “green screen” applications) time out and hang. This problem can occur if the TN3720 application is going through a Content Engine.
- CSCef42854
The CPU statistics on the Content Engine show negative numbers and the peak usage is a very high and unrealistic number (for example, the peak usage is greater than 100 percent). This problem can occur if the Content Engine has been running for more than 41 weeks and there is a heavy load on it.
- CSCef71971
MMS-over-HTTP requests with proxy authentication can fail if there is a proxy chain, and proxy authentication (with LDAP) is enabled on the proxies (the Content Engines in the proxy chain).
- CSCef89549
If URL filtering using N2H2 is enabled on the Content Engine, such URL filtering does not work, and the cache process repeatedly restarts on the Content Engine.
- CSCef96045
The cache process on the Content Engine can crash if the Content Engine receives a request for chunked encoded objects and both of the following conditions exist:
 - The Content Engine is running a third-party application for URL filtering (for example, SmartFilter software, Websense software, or N2H2).
 - The Content Engine is configured to cache chunked encoded objects. (This is the default configuration on the Content Engine, but such caching can also be explicitly enabled by issuing the **http cache-chunked-encoded enable** global configuration command).

This problem has been addressed, so if you enable URL filtering using third-party software (for example, SmartFilter software), the caching of chunked encoded objects is now automatically disabled on the Content Engine. You no longer need to explicitly disable such caching by issuing the **no http cache-chunked-encoded enable** command.

- CSCin63189
The cache process fails with numerous error log message that indicate that “dmbuf” low. This problem occurs if either of the following situations exists: (1) there is a heavy traffic load on the cache process, or (2) the cache process is leaking dmbuf buffer memory. However, the cache process recovers automatically within a few seconds.
- CSCin71822
The Content Engine can generate a core file during a preload operation. This problem can occur if the preload URL list file contains a URL that is longer than 400 characters.

Management Resolved Caveats

- CSCec55708
There is no remote notification to the end user if a physical disk drive within a RAID5 logical disk drive goes bad. Even though there is an audible alarm and the amber status light is turned on, the logical unit error is not reported from the RAID controller to the ACNS software error logs. This problem occurs only on the CDM-4650 model, and users can still periodically check drive status by entering the **show disk raid EXEC** command.
- CSCed00466
The following error is reported when the ceApiServlet is called:

```
type Exception report
message
description The server encountered an internal error () that prevented it from
fulfilling this request.
exception
java.lang.NullPointerException
```


This problem occurs if the Content Engine does not have an explicit management IP address configured.
- CSCed46150
The API program is created with multicast settings, with no multicast address ports specified within the program file. The program address pool is configured, including the pool TTL. This problem occurs if the program multicast TTL is set to 255 instead of to the address pool TTL value.
- CSCed60538
The **wmt mms allow extension** global configuration command was replaced by the **wmt http allow extension** global configuration command to clarify that MMS-over-HTTP and not MMS is the protocol that is being referenced.
- CSCee07256
The quota value of the export channel is not modified if the channel is not assigned to a media program.
- CSCee08893
The TV-out start time is incremented in the Content Distribution Manager GUI when the page reloads. This problem can occur if the time zone on the Content Distribution Manager is not GMT, and a playtime is scheduled to begin during daylight saving time (while the current time is standard or the other way around).

- CSCee12183
If you use the CLI to change the time zone setting on the Content Distribution Manager, the change is not reflected in the Content Distribution Manager GUI until you restart the Content Distribution Manager GUI.
- CSCee31107
If there is a parsing failure in a manifest file, the Content Distribution Manager GUI shows partial URLs (that is, the origin server without the filename) as filenames in the detailed replication status.
- CSCee57732
For a particular Content Engine, the Content Distribution Manager database contains device information about more than one device.
- CSCee72703
The Websense configuration on the Content Engine is not saved when you make a change to the disk configuration.
- CSCee80817
The **show http methods unsupported** EXEC command does not show all of the unsupported request methods.
- CSCee93023
A Cisco Content Engine that is running ACNS software, Release 5.1 or earlier, returns an incorrect object identifier (OID) in response to an SNMP query about entPhysicalVendorType.
- CSCef01624
The Content Engine may lose its IP address if you enter the **no ip address** command, even if the IP address was obtained through DHCP. This problem can occur if you enter this command to unconfigure the IP address that was obtained and configured through DHCP.
- CSCef08399
The Java monitor in the Content Engine GUI does not show statistics for all of the Content Engines that are using the same WCCP-enabled router. The Content Engine GUI only shows statistics for the Content Engine from which you accessed the Content Engine GUI.
- CSCef09244
The Content Engine may not set the Don't Fragment (DF) bit in the IP header even though by default the path MTU discovery should be enabled. This problem can occur if the Content Engine is reloaded and the **ip path-mtu-discovery enable** global configuration command is not used.
- CSCef31454
Writing memory fails with ACNS software, Release 5.1, and the syslog.txt file contains such messages as the following:

```
: writemem.sh: %CE-CLI-2-170057: running-config is not text (<Description>) exec_copy:
%CE-CLI-3-170055: Copy running-config to startup-config failed!. status(1.15).
```
- CSCef72422
The Content Distribution Manager GUI is slow, and thousands of syslog messages appear in the Content Distribution Manager GUI. This problem can occur if a Content Engine is sending an enormous number of syslog messages to the Content Distribution Manager, which forces the Content Distribution Manager to handle and log all of these messages.

- CSCin63504
When you are using the Content Engine GUI to configure SNMP Version 3 community configurations, the Content Engine generates a core file.

Request Processing Resolved Caveats

- CSCec85751
The disk health checking method is very CPU intensive and input-output (I/O)-intensive, which causes a CPU spike from time to time. ACNS software releases later than Release 5.1.3 and earlier than Release 5.2 removed the disk health checking procedure. The method of checking disk health before sending keepalives from the Content Engine to a Content Router or a routing Content Engine needs to be improved.

DNS Resolved Caveats

- CSCed44027
A **dns enable** command does not turn on the DNS service on a routing Content Engine.
- CSCed44073
The local DNS server on the Content Engine is started after a reload, even though you have not enabled the DNS server on the Content Engine.
- CSCee90805
If the logging file system fills up, the cache process on the Content Engine can hang.
- CSCin65511
The DNS server restarts too often when the **dns listen all** command is used. This problem occurs when the Content Engine is configured with a Port Channel as its primary interface.

ICAP Resolved Caveats

- CSCee19716
The cache process restarts when the ICAP feature is enabled. This problem occurs if ICAP functionality is unstable.
- CSCef12939
The ICAP service restarts on the Content Engine. This problem can occur if there is a heavy load and an ICAP server error occurs.
- CSCef20648
The browser displays an error message and is unable to complete the response modification (RESPMOD) process. This problem occurs only if there are two RESPMOD services configured even though only one of these services is enabled and the Rules Template is being used to identify ICAP traffic.
- CSCef30670
The ICAP process crashes on the Content Engine. This problem can occur if the ICAP process that is running on the Content Engine receives some bad data from the external ICAP server. However, the ICAP process automatically restarts on its own.

Media and Streaming Resolved Caveats

- CSCec59518
The console displays an error message from the RealServer Manager even though there is no error.
- CSCec71296
A QuickTime client that is running an EnvivioTV plug-in may take approximately 30 seconds before it renders Envivio content that has the advanced 2D encoding. This problem occurs for all Envivio 2D content.
- CSCed33580
The WMT proxy incorrectly handles a broadcast alias as a video-on-demand (VOD) file. For example, each WMT client gets its own session of the stream file, and Content Engine 2 (CE2) actually caches the file. The correct behavior should be that client 2 should just join the existing client 1 session, resulting in only one stream from Content Engine 1 (CE1) to CE2.
- CSCed40260
There is a RealServer and proxy security vulnerability. This problem can occur if RealServer and the proxy contain potential denial-of-service attacks.
- CSCed62275
There is a slow response (for example, a delay of 15 to 20 seconds) from the Content Distribution Manager. This problem can occur when you move on-demand programs from one category to another or when you have created about 18 to 22 on-demand programs.
- CSCed93296
In very rare cases, the Content Engine mediafs partition reaches 100 percent of capacity, which causes the WMT streaming server to crash. This problem can occur if you power off the Content Engine multiple times. The cleaner code can fail to write the cache object list to disk, thus causing the cached files never to be cleaned up.
- CSCee92902
Clients may continue to access a program after its scheduled end time. This problem can occur if a program is deleted, either explicitly through the Content Distribution Manager GUI or API, or automatically through a Content Distribution Manager autodeletion operation.
- CSCef09106
The video quality of RTSP content degrades when 500 to 700 RTSP requests are made to the Content Engine.
- CSCef30762
After the system reboots, it may indicate that it has an empty configuration. The system prompt may be “(none)#”. This problem can occur if disk00 is experiencing problems, and the part of the disk used to store some system configuration files goes bad.
- CSCef66974
After the time on the Content Engine has been changed, WCCP communication for the Real-Time Streaming Protocol (RTSP) WCCP service does not work. This problem occurs if you set the time on the Content Engine to a time that is earlier than the current time.
- CSCin61421
The Cisco Content Streaming Engine stops serving video-on-demand (VOD) files when the throughput is around 20 Mbps.

- CSCin63217
The WMT service stops when you configure port 1799 as the WMT incoming port.
- CSCin63878
When a WMP player plays an alias that is configured on the Content Engine and has a multicast station as the source, if you click the **Pause** button and then the **Play** button, the WMP player displays only the buffered content and no longer displays the video stream. This problem occurs only if the requested stream is an alias and the alias source is a multicast station using MMST or MMSU; this problem does not occur if HTTP is the protocol.
- CSCin64026
Repeat schedules are ignored when a transfer of a media file is scheduled to occur within 5 minutes of your creating the transfer job. This problem occurs when you select FTP to transfer a media file immediately (transfer scheduled to begin within five minutes after you create the transfer job) and when repeat schedules are configured for that transfer, the repeat schedules are ignored. They are not seen in the Review or Edit windows, and the transfer does not occur.
- CSCin65854
If Quality of Service (QoS) for MP2T audio-only programs is set, QoS parameters are not included in the Session Description Protocol (SDP) information for the program. Consequently, the MP2T stream is streamed without the intended QoS characteristics. This problem occurs with MP2T audio-only programs and when the audio QoS option is specified.
- CSCin70918
A three-stream .asf file (audio, video, and URL) is not played in the plug-in when the file is streamed from WMT. This problem occurs only if the .asf file is launched through the plug-in option.
- CSCin71282
When the Content Engine is acting as a WMT proxy server and WMT caching is enabled, all requests for Windows Media streaming media are served from the Content Engine cache instead of from the origin server once the object is fully cached on the Content Engine. However, if users click the **Fast Forward** or **Rewind** buttons in their WMT players while the file is playing, the streaming media is not served from the Content Engine cache, and the request is sent to the origin server even though the Content Engine has already cached the file.
- CSCin71738
If users request playback of a pre-positioned video-on-demand (VOD) .MOV file, the audio and video can become unsynchronized.

Rules Resolved Caveats

- CSCee01453

You experience problems when trying to add rules that have the pipe character (|). You cannot add rules that contain the pipe character (|).

- CSCef96948

The Content Engine does not accept a rule pattern list that contains a source or destination IP address that has all zeros in the host portion of the address indicating it is a network address for its associated address class.

For example, the following rule pattern list would not be accepted because it contains zero (0) in the host portion of the source IP address indicating that it is a network address for this class C address whose host portion is the least significant dotted-decimal octet.

```
rule pattern-list 1 src-ip 192.168.76.0 255.255.255.0
```

- CSCin59100

In ACNS 4.2 software, rules are configured only for HTTP and not for streaming protocols. If a Content Engine that is configured with rules and is running ACNS 4.2 software is upgraded to ACNS 5.1.x software, then these rules are configured with the protocol type “all.” This problem occurs when the software is upgraded to ACNS software Release 5.1.x from ACNS software Release 4.2.

- CSCin59581

In ACNS 5.0 software, only “AND” is allowed between group of patterns with the same pattern list number. When you downgrade from ACNS 5.1 software to ACNS 5.0 software, the ORing of patterns configuration is not supported and is converted to ANDing of patterns. For example:

- Rule configuration in ACNS 5.1 software:

```
rule action block pattern-list 3 protocol http
rule pattern-list 3 url-regex sen
rule pattern-list 3 domain cisco
```

In ACNS 5.1 software, the default behavior is ORing of patterns.

- Rule configuration in ACNS 5.0 software:

```
rule action block pattern-list 3 protocol http
rule pattern-list 3 url-regex sen
rule pattern-list 3 domain cisco
```

In ACNS 5.0 software, the only behavior is ANDing of patterns.

This problem occurs when the configuration on the Content Engine has many pattern lists that are configured (ORed together) in ACNS 5.1 software and the Content Engine is downgraded to ACNS 5.0 software. Then only the first pattern list configuration is used.

- CSCin59582

After a ContentEngine is downgraded from ACNS 5.1 software to ACNS 4.2 software, some patterns in the pattern list are lost. For example:

- Rule configuration in ACNS 5.1 software:

```
rule action block pattern-list 3 protocol http
rule pattern-list 3 url-regex sen
rule pattern-list 3 domain cisco
```

- Rule configuration in ACNS 4.2 software:

```
rule block url-regex sen
```

This problem occurs when the configuration on the ContentEngine has many pattern lists that are configured (ORed together) in ACNS 5.1 software, and the Content Engine is downgraded to ACNS 4.2 software. Then only the first pattern list configuration is used. All other pattern lists are lost.

- CSCin72282

The output of the **show rule pattern-list number ? EXEC** command does not display the **url-regsub** and the **header-field-sub** options.

- CSCin72295

You are unable to configure the **header-field-sub request-line** pattern type with the rule rewrite action. This problem can occur if you configure a pattern list that has a **header-field-sub request-line** pattern type.

Documentation Updates

This section describes documentation updates.

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 ACNS 5.1 software or later, and then downgrade to ACNS 5.0 software, the mediafs disk space assignment is lost and it reverts to cdnfs disk space. For more information, see the [“Media File System Issues When Downgrading to ACNS 5.0 Software”](#) section on page 11.

If the local (internal) Websense server is enabled on the Content Engine and you downgrade from the ACNS 5.2.x software to ACNS 5.0 or 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 ACNS 5.0 Software or ACNS 5.1 Software”](#) section on page 12.

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*
- *Release Notes for Cisco ACNS Software, Release 5.2* (the release notes you are reading now)

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/univercd/home/home.htm>

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco 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

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

- 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 send comments about technical 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
- Nonemergencies—psirt@cisco.com

**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 that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support 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, 365 days a year, at this URL:

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

Access to all tools on the Cisco Technical Support 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 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 TAC 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 TAC 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, 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>

- *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>

- 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, 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, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO 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. (0501R)

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

 Printed in the USA on recycled paper containing 10% postconsumer waste.

