



# Release Notes for Cisco ACNS Software, Release 4.2

---

July 26, 2002



**Note**

---

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

---

## Documentation Survey

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

## Contents

These release notes contain information about ACNS software, Release 4.2. These release notes describe the following topics:

- [Introduction, page 2](#)
- [Installation Notes, page 2](#)
- [New and Changed Information, page 2](#)
- [Important Notes, page 9](#)
- [Caveats, page 10](#)
- [Documentation Updates, page 14](#)
- [Related Documentation, page 16](#)
- [Obtaining Documentation, page 16](#)
- [Obtaining Technical Assistance, page 17](#)



---

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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

# Introduction

These release notes describe new features, limitations, caveats, and other important information regarding ACNS software, Release 4.2.

## Installation Notes

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

Instructions for upgrading and downgrading devices to and from ACNS software, Release 4.2 are located in Chapter 3 of the *Cisco ACNS Software Maintenance and Troubleshooting Guide*. See the “[Related Documentation](#)” section of these release notes for a description of the entire ACNS software, Release 4.2 documentation set.

## New and Changed Information

This section describes existing features that have changed and new features in ACNS software, Release 4.2. These features include the following:

- [Configuring RealServer in ACNS Software, Release 4.2](#)
- [Recovering Missing Disk-Based Software](#)
- [CiscoWorks2000 Resource Manager Essentials 3.4.1](#)
- [Manually Organized Distributed Architecture Technology](#)
- [Playlists for TV-Out Playback](#)
- [RealSystem Administrator Graphical User Interface Features](#)
- [Resetting the Default Administrator Password for the E-CDN Application](#)
- [Content Preloading](#)
- [Caching Entire Objects Under Range Requests](#)
- [User Authentication and Authorization Using RADIUS](#)
- [HTTP Request Authentication Using TACACS+](#)
- [Using Access Control Lists](#)
- [Transaction Logging and NTLM Authentication](#)
- [Traceroute Support](#)
- [TCP Dump Support](#)
- [IP Spoofing](#)
- [New Rules Template Operations](#)
- [New and Changed ACNS Software Command-Line Interface Commands](#)

## Configuring RealServer in ACNS Software, Release 4.2

In ACNS software, Release 4.1, you configured the Content Engine RealServer with the publisher's IP address (or host name) and admin port using the **real-subscriber publisher** command. You then entered the IP address and port information of every Content Engine in the publisher RealServer user interface.

In ACNS software, Release 4.2, you configure the Content Engine RealServer through the RealServer administrator GUI. To access the RealServer GUI, you must first enable the E-CDN application.

## Recovering Missing Disk-Based Software

In earlier versions of ACNS software, a feature called the software recovery shell was used to recover from missing disk-based software. A new procedure that uses the CLI has been implemented in ACNS software, Release 4.2. At startup, if a problem is detected with disk00, a console message urges users to check disk00, replace the disk if necessary, and run the **disk recover** command. The **disk recover** command is a new command in ACNS software, Release 4.2.

If the system disk (disk00) fails or is missing, ACNS software, Release 4.2 continues to boot up and run; however, it runs in a degraded mode in which HTTP proxy and related HTTP features still work, but most other features fail. The following features continue to work even if disk00 is missing:

- CLI
- Most CLI commands with the exception of the **disk config** command, which is disabled
- HTTP proxy and proxy-related features, including external authentication

For further information on how to recover from missing disk-based software in the ACNS software, Release 4.2, refer to the *Cisco ACNS Software Maintenance and Troubleshooting Guide* (OL-1888-02), which is available on Cisco.com at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/acns41/sysmnt/index.htm>

## CiscoWorks2000 Resource Manager Essentials 3.4.1

The CiscoWorks2000 Resource Manager Essentials (RME), also called Essentials 3.4.1, IDS patch provides support for the following Cisco Content Engines: CE-507, CE-507AV, CE560, CE560AV, CE-590, and CE-7320. To obtain the patch, go to the EMBU Patch Repository at the following location: <http://embu-web.cisco.com/Patches/patch-publisher/patch-request.cfm>.

In the Search by BugID field enter **CSCin10877**. A Readme document (in PDF format) is also available at this location.



### Note

Support for distribution of software onto Content Engines that are running ACNS software in E-CDN mode is *not* available. Such devices, if selected, are skipped during the software distribution.

## Manually Organized Distributed Architecture Technology

Manually Organized Distributed Architecture (MODA) is a proprietary technology that allows the network administrator to control network hierarchy manually. This feature is geared towards those users who do not want to use SODA technology and require something more sophisticated than simply disabling the existing Tree Building Protocol (TBP) feature. You can configure devices to use MODA by accessing the System window on the Content Distribution Manager graphical user interface.

## Playlists for TV-Out Playback

Content Engines that are equipped with an integrated Moving Picture Experts Group (MPEG) decoder are also known as TV-out enabled devices. These devices play media files using National Television Standards Committee (NTSC) or Phase Alternation Line (PAL) video signals. The Content Engine can thus play video directly to a TV monitor in applications such as kiosks, cable TV systems, and video walls. Playback, which is the act of streaming a file or set of files, can be scheduled or controlled manually. You can manually control playlists using VCR-like controls from any web browser.

A playlist is a list of media files and their associated attributes that defines when and how the files are played back. You can create local and system playlists. Local playlists are created, managed, and played from a single TV-out enabled device. System playlists are created and managed by the Content Distribution Manager and then played across one or more TV-out devices.

## RealSystem Administrator Graphical User Interface Features

ACNS software, Release 4.2 allows you to use several configuration features on the RealSystem Administrator graphical user interface.

## Resetting the Default Administrator Password for the E-CDN Application

If the E-CDN application is enabled and the administrator password is forgotten, lost, or misconfigured, you can reset the password, using a new procedure, on the Content Distribution Manager. Password changes propagate out to any Content Router or Content Engine devices that are managed by the Content Distribution Manager.

For more information about this procedure, see Chapter 2 in the *Cisco ACNS Software E-CDN Administrator's Guide, Release 4.2*, or Chapter 4 in the *Cisco ACNS Software Maintenance and Troubleshooting Guide*.

## Content Preloading

In ACNS software, Release 4.2, if content preloading is not completed before the scheduled end time, you can resume the preloading process to capture content using the **pre-load resume** global configuration command. You can also configure maximum bandwidth for the preloading process using the **pre-load max-bandwidth** global configuration command. ACNS software, Release 4.2 also includes Type of Service (ToS) or differentiated services code point (DSCP) support for HTTP, FTP and Microsoft Media Server (MMS) preload traffic.

## Caching Entire Objects Under Range Requests

The command **http smart-range** enables the Content Engine to cache an entire HTTP response even if the client issues a Range request and the object is not in cache. The **http smart-range enable** global configuration command activates this caching feature. Use the **no** version of this command, **no http smart-range enable**, to disable it.

## User Authentication and Authorization Using RADIUS

Authentication, also referred to as “login,” is the act of verifying usernames and passwords. Authorization, or “configuration,” refers to the setting of privileges for authenticated users in a network. Generally, authentication precedes authorization in a network. ACNS software, Release 4.2 allows you to use a RADIUS server to further authenticate and authorize users in your network, in addition to using the local and TACACS+ databases. The **authentication login radius** and **authentication configuration radius** commands use a remote RADIUS server to determine the level of user access, whereas previous releases of ACNS software only allowed the use of a RADIUS server to check against HTTP request authentication.

## HTTP Request Authentication Using TACACS+

The ACNS software, Release 4.2 Cache application offers additional supports for TACACS+ server HTTP request authentication. HTTP request authentication authenticates a user’s domain, username, and password with a preconfigured primary domain controller (PDC) before allowing requests from the user to be served by the Content Engine.

## Using Access Control Lists

In ACNS software, Release 4.2 you can also configure group authorization using access control lists (ACLs) after a user has been authenticated against an NTLM or LDAP server. The use of these lists configures a group privilege when the group accesses content provided by the Content Engine. In other words, using ACLs allows or prevents users from certain groups from viewing specific content. This authorization feature offers more granular access control by specifying that access is allowed only to certain groups.

## Transaction Logging and NTLM Authentication

If your device is configured for NT LAN Manager (NTLM) authentication, the **transaction-logs log-windows-domain** command records the Windows domain name and username in the “authenticated username” field of the transaction log. This feature is available for transaction logs in Apache-style as well as Extended-Squid format.

## Traceroute Support

Traceroute is a widely available utility on most operating systems today. Much like ping, it is a valuable tool for determining connectivity in a network. Ping allows the user to find out if there is a connection between two end systems. Traceroute does this as well, but it additionally lists the intermediate routers between the

two systems. Users can therefore see the routes that packets can take from the Content Engine to another system. Use the **traceroute** EXEC command to find the route to a remote host, when either the host name or IP address is known.

## TCP Dump Support

Use the **tcpdump** EXEC command to view packet trace information on the Content Engine. This information can be saved to your hard drive and later be used by technical support for packet analysis.

## IP Spoofing

In transparent caching, when the Content Engine contacts the origin web server, it uses the Content Engine's own IP address instead of the client's IP address on behalf of which the Content Engine is making the request. With IP spoofing, the transparent redirection process can enable the Content Engine to send out the client's IP address for authentication purposes on origin web servers. You can enable IP spoofing with the **wccp spoof-client-ip enable** global configuration command. You can disable this feature with the **no wccp spoof-client-ip enable** command.



### Note

Do not enable IP spoofing on the Content Engine without configuring proper traffic redirection capabilities on the WCCP routers involved. See the *Cisco ACNS Software Caching Configuration Guide, Release 4.2* for more information on how to configure IP spoofing.

## New Rules Template Operations

A new rule has been added to the Content Engine to tell the Content Engine to use different DNS name servers based on the URL provided. Another new rule helps the user specify that certain content can be cached even though the response from the server prohibits the caching operation.

The Rules Template feature support the following new types of actions:

- **Cache**—Overrides HTTP response headers to cache objects.
- **Insert-no-cache**—Inserts a no-cache header to the response.
- **Use-dns-server**—Uses the DNS server specified to resolve specific domain name.

## New and Changed ACNS Software Command-Line Interface Commands

The following tables list and describe new and changed command-line interface commands for ACNS software, Release 4.2. For more information on the WMT commands, see the latest version of the *Cisco ACNS Software Command Reference, Release 4.2*.

Table 1 New ACNS Software Privileged EXEC Commands

Privileged EXEC Command	Syntax	Description
<b>clear</b>	<b>clear statistics access-lists 300</b>	Clears access control list statistics.
<b>copy</b>	<b>copy http install</b> {hostname   ip-address} remotefiledir remotefilename	Copies HTTP configuration or image files to and from Flash memory, disk, or remote hosts.
<b>disk</b>	<b>disk recover</b>	Recovers the system disk (disk00).
<b>find-pattern</b>	<b>find-pattern</b> { <b>binary</b> reg-expression filename   <b>case</b> { <b>binary</b> reg-expression filename   <b>count</b> reg-expression filename   <b>lineno</b> reg-expression filename   <b>match</b> reg-expression filename   <b>nomatch</b> reg-expression filename   <b>recursive</b> reg-expression filename}   <b>count</b> reg-expression filename   <b>lineno</b> reg-expression filename   <b>match</b> reg-expression filename   <b>nomatch</b> reg-expression filename   <b>recursive</b> reg-expression filename }	Searches for a particular pattern in a file.
<b>tcpdump</b>	<b>tcpdump</b> [LINE]	Dumps network traffic.
<b>traceroute</b>	<b>traceroute</b> {hostname   ip-address}	Traces the route to a remote host.

Table 2 New ACNS Software Global Configuration Commands

Global Configuration Command	Syntax	Description
<b>access-lists</b>	<b>access-lists</b> { <b>300</b> { <b>deny</b> groupname {any [position number]   groupname [position number]}}   { <b>permit</b> groupname {any [position number]   groupname [position number]}}   <b>enable</b> }	Configures access control list entries.
<b>http</b>	<b>http smart-range</b> { <b>enable</b>   <b>max-start</b> offset <b>max-interval</b> interval}	Manages config options for Range requests when cache misses occur.
<b>pre-load</b>	<b>pre-load dscp</b> { <b>set-dscp</b> dscpvalue   <b>set-tos</b> tosvalue}  <b>pre-load max-bandwidth</b> bandwidth <b>pre-load resume</b>	Sets the preload DSCP feature.  Configures the maximum bandwidth. Continues preload from a previous operation.
<b>proxy-protocols</b>	<b>proxy-protocols transparent reset</b>	Resets the incoming transparent mode behavior for proxy requests.

Table 2 New ACNS Software Global Configuration Commands (continued)

Global Configuration Command	Syntax	Description
<b>rule</b>	<p><b>rule cache ttl</b> { <b>days</b> <i>days</i> [<b>domain</b> <i>LINE</i>] [<b>dst-ip</b> <i>d_ipaddress d_subnet</i>] [<b>mime-type</b> <i>LINE</i>] [<b>url-regex</b> <i>LINE</i>]   <b>hours</b> <i>hours</i> [<b>domain</b> <i>LINE</i>] [<b>dst-ip</b> <i>d_ipaddress d_subnet</i>] [<b>mime-type</b> <i>LINE</i>] [<b>url-regex</b> <i>LINE</i>]   <b>minutes</b> <i>minutes</i> [<b>domain</b> <i>LINE</i>] [<b>dst-ip</b> <i>d_ipaddress d_subnet</i>] [<b>mime-type</b> <i>LINE</i>] [<b>url-regex</b> <i>LINE</i>]   <b>seconds</b> <i>seconds</i> [<b>domain</b> <i>LINE</i>] [<b>dst-ip</b> <i>d_ipaddress d_subnet</i>] [<b>mime-type</b> <i>LINE</i>] [<b>url-regex</b> <i>LINE</i>]</p> <p><b>rule insert-no-cache</b> [<b>domain</b> <i>LINE</i>] [<b>dst-ip</b> <i>d_ipaddress d_subnet</i>] [<b>url-regex</b> <i>LINE</i>]</p> <p><b>rule use-dns-server</b> { <i>hostname</i>   <i>ip-address</i> } { <b>domain</b> <i>LINE</i>   <b>dst-ip</b> <i>d_ipaddress d_subnet</i> }</p>	<p>Caches this object while overriding HTTP response headers.</p> <p>Inserts a no-cache header in the response.</p> <p>Uses the specific DNS server configured.</p>
<b>transaction-logs</b>	<b>transaction-logs log-windows-domain</b>	Logs Windows domain with authenticated username, if available.
<b>wccp custom-web-cache</b>	<p><b>wccp custom-web-cache</b> { <b>mask</b> { [<b>dst-ip-mask</b> <i>hex_num</i>] [<b>dst-port-mask</b> <i>hex_num</i>] [<b>src-ip-mask</b> <i>hex_num</i>] [<b>src-port-mask</b> <i>hex_num</i>] }</p> <p><b>wccp custom-web-cache router-list-num</b> <i>num</i> [<b>mask-assign</b>]</p>	<p>Specifies Web Cache Communication Protocol (WCCP) custom web cache mask to be used for Content Engine assignment.</p> <p>Uses the mask method for Content Engine assignment.</p>
<b>wccp media-cache</b>	<p><b>wccp media-cache</b> { <b>mask</b> { [<b>dst-ip-mask</b> <i>hex_num</i>] [<b>dst-port-mask</b> <i>hex_num</i>] [<b>src-ip-mask</b> <i>hex_num</i>] [<b>src-port-mask</b> <i>hex_num</i>] }</p> <p><b>wccp media-cache router-list-num</b> <i>num</i> [<b>mask-assign</b>]</p>	<p>Specifies that WCCP Version 2 media cache mask be used for Content Engine assignment.</p> <p>Uses the mask method for Content Engine assignment.</p>
<b>wccp reverse-proxy</b>	<p><b>wccp reverse-proxy</b> { <b>mask</b> { [<b>dst-ip-mask</b> <i>hex_num</i>] [<b>dst-port-mask</b> <i>hex_num</i>] [<b>src-ip-mask</b> <i>hex_num</i>] [<b>src-port-mask</b> <i>hex_num</i>] }</p> <p><b>wccp reverse-proxy router-list-num</b> <i>num</i> [<b>mask-assign</b>]</p>	<p>Specifies that WCCP Version 2 reverse proxy mask be used for Content Engine assignment.</p> <p>Uses the mask method for Content Engine assignment.</p>
<b>wccp service-number</b>	<p><b>wccp service-number</b> <i>servnumber</i> { <b>mask</b> { [<b>dst-ip-mask</b> <i>hex_num</i>] [<b>dst-port-mask</b> <i>hex_num</i>] [<b>src-ip-mask</b> <i>hex_num</i>] [<b>src-port-mask</b> <i>hex_num</i>] }</p> <p><b>wccp service-number</b> <i>servnumber</i> <b>router-list-num</b> <i>num</i> <b>port-list-num</b> <i>port</i> <b>application</b> { <b>cache</b>   <b>streaming</b> } [<b>mask-assign</b>]</p>	<p>Specifies that WCCP Version 2 service number mask be used for Content Engine assignment.</p> <p>Uses the mask method for Content Engine assignment.</p>

Table 2 New ACNS Software Global Configuration Commands (continued)

Global Configuration Command	Syntax	Description
wccp spoof-client-ip	wccp spoof-client-ip enable	Enables client IP spoofing while connecting to the origin server.
wccp web-cache	wccp web-cache {mask {[dst-ip-mask hex_num] [dst-port-mask hex_num] [src-ip-mask hex_num] [src-port-mask hex_num]}} wccp web-cache router-list-num num [mask-assign]	Specifies that standard web caching mask be used for Content Engine assignment.  Uses the mask method for Content Engine assignment.
wccp wmt	wccp wmt {mask {[dst-ip-mask hex_num] [dst-port-mask hex_num] [src-ip-mask hex_num] [src-port-mask hex_num]}} wccp wmt router-list-num num [mask-assign]	Specifies that WCCP Windows Media Technologies (WMT) mask be used for Content Engine assignment.  Uses the mask method for Content Engine assignment.

Table 3 New ACNS Software show Commands

EXEC show Command	Syntax	Description
show access-lists	show access-lists 300	Displays access control list configuration.
show rule	show rule {action {action-type {all   pattern pattern-type}   all}}	Displays the Rules Template configuration information for new rules (see <b>rule</b> in Table 2).
show statistics access-lists	show statistics access-lists 300	Displays access control list statistics.
show statistics rule	show statistics rule {action {action-type {all   pattern pattern-type}   all}}	Displays rule statistics for new rules (see <b>rule</b> in Table 2).
show wccp	show wccp masks {custom-web-cache   media-cache   reverse-proxy   web-cache}	Displays WCCP caching service mask assignments.

## Important Notes

### Performance Characteristics of ACNS Software, Release 4.2

To view performance characteristics of ACNS software, Release 4.2, see the document titled *ACNS 4.2 Performance Bulletin* at the following URL:

<http://www.warp/public/cc/pd/cxsr/ces/prodlit/>

## WCCP Masking Feature

Note that the WCCP masking feature in each WCCP-related CLI is documented in the *Cisco ACNS Software Command Reference, Release 4.2*. guide. However, this feature is not supported in ACNS software, Release 4.2.

## RealServer Default Licenses

In ACNS software, Release 4.2, RealServer is no longer licensed, by default, to serve up to 10 simultaneous streams. To add licenses, you need to use the RealNetworks distributed license feature. Refer to the *Cisco Content Delivery Networking Products Getting Started Guide, Release 4.2* for more information.

## Caveats

This section lists and describes caveats that were resolved in ACNS software, Release 4.2, and caveats that are still open in this release.

Caveats describe unexpected behavior in ACNS software, Release 4.2. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

## Resolved Caveats - Release 4.2

- CSCdu36845  
The TV-out GUI allows a non-BMP file type to be used as an overlay image. For example, if an .mpeg file larger than 64 KB is used as the overlay image, the system goes into a loop.
- CSCdu79580  
If you repeatedly click NEXT (10–15 times) from the GUI or the API while the playlist is in PLAY mode, the video server may pause indefinitely. The video monitor flickers for awhile as it attempts to play the next file and then it pauses indefinitely.
- CSCdw33364  
Occasionally, the user cannot access the RealServer and receives the following error message:  
`Server has reached its capacity`
- CSCdw71468  
When the user programmatically imports content into a channel on the Content Distribution Manager, if the status return field is HTML or MX (E-CDN application proprietary format), then the status is not returned.
- CSCdw76156  
Removing a Storage Array 6 that had the only sysfs partition results in a system with two disks allocated only to cfs and ecdnfs.
- CSCdw91108  
Symptom: The Content Engine does not accept requests on secondary addresses.
- CSCdx00361

When multiple plug-ins (for example, Content Optimization and SmartFilter) are enabled at the same time, the caching process automatically reboots.

- CSCdx03843

All traffic to the Content Engine is bypassed after the following CLI command is issued:

```
show wccp flows web-cache detail
```

- CSCdx04156

The Pluggable Authentication Module (PAM) creates unnecessary system log entries during user login.

- CSCdx13400

If the media player tries to play a clip through the HTTP protocol (the user chooses to only use the HTTP protocol as the transport), it will not work.

- CSCdx20175

When you try to use the **cfs clear** command, the following error results:

```
umhscache#cfs clear disk00/03 force
unable to create lock file
```

- CSCdx23688

When logging in as a TACACS user, the user does not appear in the user list.

- CSCdx37517

The rtsp\_proxy did a core dump when it tried to connect to the WCCP process. The WCCP module in the rtsp\_proxy was not able to free all the resources cleanly.

- CSCin06968

When the proxy automatic configuration (.pac file) feature is used, a request for the proxy.pac file should not be forwarded to an upstream proxy device, even if an upstream proxy is configured.

- CSCin07452

The rule cache feature does not work when the pattern type is mime-type.

## Open Caveats - ACNS Software Release 4.2

- CSCdv29357

**Symptom:** During the playback of some MPEG-2 files using TV-out, the video decode freezes at some position in the file while the audio decode continues. Repeated playback shows that the video freeze occurs at the same position. In some extreme cases, the problem occurs on the first frame of video, causing playback to fail entirely.

**Condition:** This symptom occurs on systems running any Enterprise-CDN or ACNS software version. The hardware is the CE-507AV-CDN or CE-560AV-CDN, manufactured with the Vela CineView 2083 MPEG decoder card.

**Workaround:** The problem occurs with MPEG-2 files encoded at a variable bit rate (VBR). The hardware decoder interprets some sequences as an error, and stops the decode. We recommend that MPEG-2 files encoded for TV-out use constant bit rate (CBR) to avoid this problem. Files exhibiting this behavior should be re-encoded.

In the extreme case noted above, the TV-STATUS record may need to be removed to recover playback operation. This is only if the VBR file cannot be removed from the playlist through the TV Controller GUI. Go to the following URL:

http://<CE IP>/cgi/box

where <CE IP> is the Content Engine IP address.

1. Choose **ShowLib** and enter **TV-STATUS** in the Table regex field.
2. Click **Show**, choose **Record**, and click **Delete checked records**.

- CSCdv66971

Symptom: Under the circumstances described, the downgrade process from ACNS 4.x software to ECDN 3.x software fails to be completed.

Condition: This failure occurs when the Content Engine, Content Router, or Content Distribution Manager console port is physically connected to a console server and there is no active Telnet session running between the two devices. Without an open Telnet session, the console output that is generated during the downgrade fills the console buffer. Once the console buffer is filled, any application that generates console output is blocked. This effectively blocks the downgrade from continuing.

Workaround: There are three possible ways to work around this problem.

- Initiate a Telnet session on the console server during the upgrade or downgrade process so that the console output from the Content Engine, Content Router, or Content Distribution Manager can be displayed in the Telnet session. An open Telnet session keeps the console buffer cleared.
- Remove the console cable from the device.
- Connect the serial cable to a PC running communications software.

When a downgrade has already been initiated and the device has paused indefinitely, configure the serial connection as above, and reboot the device. In most cases the downgrade will run to completion.

- CSCdw68467

Symptom: When the **copy startup-config running-config** command is used, the shell prompt is not returned.

Condition: If the **copy startup-config running-config** command is used when the CLI\_INTERACTIVE flag is set, it triggers the execution of /diamond/bin/config (generated from bfc/systems/cli/exec/src).

This **/diamond/bin/ config** command executes the content in the startup configuration line by line. Certain **config** commands prompt the user and wait for the user's response, causing the **copy** command to pause indefinitely (stdout and stderr have been redirected) because there is no user response to the prompt.

This condition does not occur when the system boots up, because the CLI\_INTERACTIVE flag is not set during bootup.

Those configuration commands that need user interaction call the function GetCLIMode(), which determines whether or not to enter interactive mode.

Workaround: If the **copy startup-config running-config** command pauses indefinitely, press **Enter** as needed, until the command has finished executing.

- CSCdw82157

Symptom: The **disk configure** command does not use the remaining (unused) space on disk00 for mediafs storage.

Condition: After upgrading from ACNS software, Release 4.0 to ACNS 4.1 software, Release 4.1 beta (4.1.0b14), disk00 has 12GB of “free” space. This space cannot be used for mediafs storage, because ACNS software does not support the **disk partition** command to manually create a disk00/03 partition. The **disk configure** command does not touch disk00 at all, so the result is lost disk space. This means that not all purchased disk space is usable.

Workaround: There is no workaround.

- CSCdw84848

Symptom: The contents of a file whose name exceeds 215 characters in length cannot be imported.

Condition: This occurs on a Content Distribution Manager 4630 or 4650 running ACNS software, Release 4.2.

Workaround: There is no known workaround. Internal software appends about 40 characters to a filename to keep track of content metadata such as channel-info. The Linux's ext2 file system supports FILENAME\_MAX constant as 255. Thus, a filename that is greater than 215 characters is not supported.

- CSCdx04092

Symptom: Using an embedded Windows Media Player object in an HTML page to point to an ASX file that contains the WMT Play URL from the CDM Previewer page for an imported ASF file does not work. You receive an error message saying that the filename is invalid.

Condition: This symptom only occurs when you are using the embedded Windows Media Player object in an HTML page. This symptom does not occur if you are using the full Windows Media Player.

Workaround: Use the Windows Media Player (not the embedded object). Or, if you must use the embedded player, have it point directly to the WMT Play URL instead of an ASX file.

- CSCdx04177

Symptom: You cannot use .sami (Synchronized Accessible Media Interchange) files with WMT playing from the Content Distribution Manager or Content Engine.

Workaround: There is no known workaround.

- CSCdx18600

Symptom: The output from the **show clock** CLI command may not display the correct time zone name.

Conditions: This symptom occurs when the **show clock** CLI command is used on systems running ACNS software.

Workaround: There is no known workaround.

- CSCdx28999

Symptom: “Permission denied” messages are received when you import a folder using FTP drag and drop with Netscape 4.7. Subsequent attempts to import files using FTP drag and drop fail, and “unable to find the file or directory” messages are displayed.

Condition: This symptom occurs with ACNS software, Release 4.2.

Workaround: Use a different browser (Internet Explorer) if you need to import folders using FTP drag and drop. If you need to use Netscape 4.7, exiting and restarting the browser eliminates the subsequent “unable to find the file or directory” errors.

- CSCdx93083

Symptom: RADIUS authentication fails when the primary RADIUS server is not responding or is slow to respond even though the secondary RADIUS server is available.

Condition: If the primary RADIUS server is down or responding slowly and the rate of authentication requests sent to the Content Engine is high, then the client may see the authentication request timeout before receiving a response from the available secondary RADIUS server. One indication of this condition is a steadily increasing “Bad AC Entry” statistic in the output from the **show statistics http-authcache** command.

Workaround: Reconfigure the “radius-server host” parameter to remove the primary RADIUS server until the RADIUS server problem can be corrected.

- CSCdy16548

Symptom: When you use ACNS software, Release 4.2 to verify an NTLM-supplied password on a Windows server, the authentication fails if the password length is longer than 14 characters.

Condition: Password authentication fails on a Windows 2000 or Windows XP system.

Workaround: Do not use an NTLM user password that is longer than 14 characters. The maximum supported password length is 14 characters.

- CSCin06235

Symptom: The SNMP client cannot authenticate itself using Secure Hash Algorithm (SHA)-based authentication.

Condition: Unknown.

Workaround: SNMPv3 supports a user-based authentication mechanism. Two authentication mechanisms, MD5 (Message Digest-5) and SHA (Secure Hash Algorithm), are supported by the SNMPv3 protocol. Since a MD5 authentication works, the user should choose MD5 as an authentication option while configuring the **snmp-server user** command.

- CSCin10011

Symptom: If a user is in more than one group (with the same user ID) and if one of the groups has been configured in an access list, then the user will always be denied access even if the group is allowed.

Workaround: You need to set the access list to “permit any.”

## Documentation Updates

The following two commands were omitted from the *Cisco ACNS Software Command Reference, Release 4.2*.

- **ecdn reset-cdm-gui password** EXEC command
- **wmt proxy outgoing http host** global configuration command

## ecdn reset-cdm-gui password Command

Use the **ecdn reset-cdm-gui-password** EXEC command option to reset the administrator’s CDM GUI password on the Enterprise CDN (E-CDN) application. The new password takes effect after the device is reloaded.

The following two examples demonstrate how this command is used to reset the administrator’s CDM GUI password to its default value. The first example aborts the command after you answer **no** to the confirmation question three times.

```
ecdn-cdm# ecdn reset-cdm-gui-password
```

This command will reset CDM GUI password for user admin to the default value.

```
The default password is the word 'default'.
Are you sure you want to go ahead?[yes/no]
Please enter yes or no:
Please enter yes or no:
Please enter yes or no: no
Command aborted.
```

The second example resets the password to its default value after you answer **yes** to the confirmation question.

```
ecdn-cdm# ecdn reset-cdm-gui-password
This command will reset CDM GUI password for user admin to the default value.
The default password is the word 'default'.
Are you sure you want to go ahead?[yes/no] yes
```

## wmt proxy outgoing http host Command

You can designate an outgoing HTTP proxy server for streaming media in MMS format. Use the **wmt proxy outgoing http host** command to configure the outgoing proxy for this format. This command allows the forwarding of MMS data over HTTP to a standard 8080 proxy port.



### Note

MMS protocol can run on top of three different data protocols: MMS over TCP, MMS over UDP, and MSS over HTTP. ACNS software, Release 4.2 only supports MMS over HTTP at this time.

In this example, the host 10.1.1.1 on port 8088 is designated the primary outgoing proxy server, and host 10.1.1.2 is a backup proxy server.

```
ContentEngine(config)# http proxy outgoing host 10.1.1.1 8088 primary
ContentEngine(config)# http proxy outgoing host 10.1.1.2 220
```

In this example, the Content Engine is configured to redirect requests directly to the origin server if all of the proxy servers fail.

```
ContentEngine(config)# http proxy outgoing origin-server
```

In this example, the Content Engine is configured to monitor the proxy servers every 120 seconds.

```
ContentEngine(config)# http proxy outgoing monitor 120
```

For more information on the WMT commands, see the latest version of the *Cisco ACNS Software Command Reference, Release 4.2*.

## SmartFilter and the No-Auth Rule Interaction

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

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

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

## Related Documentation

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

### Product Documentation Set

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

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

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

### Hardware Documentation

- *Cisco Content Engine 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

- *Cisco ACNS Software Caching Configuration Guide, Release 4.2*
- *Cisco ACNS Software Command Reference, Release 4.2*
- *Cisco ACNS Software E-CDN Administrator's Guide, Release 4.2*
- *Cisco ACNS Software Maintenance and Troubleshooting Guide*
- *SmartFilter for Cisco Content Engine User's Guide, Release 3.0.2*

## Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at this URL:

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

## Documentation CD-ROM

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

## Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

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

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

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

We appreciate your comments.

## Obtaining Technical Assistance

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

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

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

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

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

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

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

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

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

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

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

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

---

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

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

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0206R)

