Release Notes for Cisco Application and Content Networking Software, Release 4.1

February 20, 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 4.1. These release notes describe the following topics:

- Introduction, page 2
- Installation Notes, page 2
- New and Changed Information, page 3
- Limitations, page 10
- Important Notes, page 10
- Caveats, page 10
- Documentation Updates, page 18
- Related Documentation, page 23
- Obtaining Documentation, page 24
- Obtaining Technical Assistance, page 25

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

Introduction

These release notes describe new features, limitations, caveats, and other important information regarding ACNS software, Release 4.1.

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 4.1 software 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 4.1 software documentation set.

Third Party Software

This section provides information about third-party software supported in the ACNS 4.1 software release.

SmartFilter 3.0.2 for Cisco Content Engine

SmartFilter™ 3.0.2 for Cisco Content Engine is a URL filtering server that is preinstalled and fully integrated in the Content Engine in ACNS software, Release 4.1. To enable SmartFilter from the Content Engine GUI, select the SmartFilter enable option to download and install a remote SmartFilter GUI (either Solaris, Linux, or Windows) from the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/uce41

Download the appropriate file:

- sf30_admin_lin7.tar.gz (for SmartFilter administration GUI for Linux)
- sf30_admin_sol7.tar.gz (for SmartFilter administration GUI for Solaris)
- sf30_admin_win32.exe (for SmartFilter administration GUI for Windows)

To evaluate SmartFilter, you need an activation key, login ID, and password. You can obtain this information from the following URL:

http://www.smartfilter.com/cisco

Licenses

The following licensed software programs require the purchase of a license from Cisco:

- Windows Media Technologies (WMT)—The license covers use both as a proxy for the Cache application and as a WMT server for the E-CDN application
- RealNetworks proxy—The license covers use for the Cache application
- RealSubscriber—The license covers use for the E-CDN application
- Digital Fountain multicast client—The license covers use for the E-CDN application

Refer to the *Cisco Content Delivery Networking Products Getting Started Guide* for additional license key information.

New and Changed Information

The following features are now supported in the ACNS software, Release 4.1:

- Command-Line Interface License Support for RealSubscriber and Digital Fountain Clients, page 3
- Evaluation License Support for RealProxy, WMT, RealSubscriber, and Digital Fountain Clients, page 3
- RealServer Version 8.0.1, page 3
- Device Groups in the E-CDN GUI, page 4
- Setting the Playback Bandwidth Allocation, page 4
- Transparent Caching with the Cisco CSS 11000 Series Switch, page 4
- URL Filtering with the N2H2 Server, page 4
- Apache-Style Transaction Logging, page 4
- Support for SNMPv3, page 5
- CiscoWorks2000, page 5
- Cisco Discovery Protocol, page 5
- Caching of HTTP If-Range Requests, page 5
- Configuring the Content Engine as a Content Routing Agent, page 6
- Configuring Microsoft Windows Media Player 7.01, page 6

Command-Line Interface License Support for RealSubscriber and Digital Fountain Clients

You can now enable licensed programs for Real Proxy, RealSubscriber, WMT, and Digital Fountain clients through the command-line interface (CLI).

Evaluation License Support for RealProxy, WMT, RealSubscriber, and Digital Fountain Clients

An evaluation license is available that allows you to use the licensed software for a limited period. The evaluation license can be invoked only once and does not require a license key. The evaluation period countdown begins once you enable the license evaluation program.

RealServer Version 8.0.1

RealServer Version 8.0.1 is supported as an optional component that is used as a streaming media engine. When RealServer software is configured for subscriber-only mode, it is referred to as RealSubscriber.

Device Groups in the E-CDN GUI

The device groups feature lets E-CDN system administrators group individual devices by category in order to efficiently apply bandwidth settings across many devices at one time.

Setting the Playback Bandwidth Allocation

Content Engines and the Content Distribution Manager use a specific playback bandwidth when streaming media to user desktops. You can now set the playback bandwidth on the E-CDN GUI between three servers: WMT server, HTTP server, and RealServer.

Transparent Caching with the Cisco CSS 11000 Series Switch

When you configure transparent caching on the CSS 11000 switch, the switch intercepts and redirects outbound client requests for Internet data to the cache servers on your network. The cache either returns the requested content if it has a local copy or sends a new request to the origin server for the information. If all cache servers are unavailable in a transparent cache configuration, the CSS 11000 switch allows all client requests to progress to the origin servers.

URL Filtering with SmartFilter 3.0.2 Cisco Content Engine Software

Cisco Systems, Inc. integrates Secure Computing Corporation's SmartFilter 3.0.2 for Cisco Content Engine software into the Cisco Content Engine. SmartFilter software is a network filtering software solution that allows businesses to configure and manage website access across their entire organization. SmartFilter software facilitates consistent and effective implementation of Internet security policies and user guidelines.

SmartFilter software provides Employee Internet Management (EIM) functionality with proxy servers, firewalls, and caching appliances. The integrated Content Engine and SmartFilter product preserves all functionality available in a regular Content Engine. The SmartFilter filtering capability is available as an add-on service on the Content Engine, and the service may be enabled or disabled as desired through the Content Engine CLI or Graphical User Interface (GUI).

URL Filtering with the N2H2 Server

The Content Engine can perform URL filtering using an N2H2 server. The Content Engine and the N2H2 server use the Internet Filtering Protocol (IFP) Version 1 to communicate with each other. When the Content Engine receives a URL request, it sends an IFP request to the N2H2 server with the requested URL. The N2H2 server does some necessary lookups for the URL and sends back an IFP response. Based on the N2H2 server's IFP response, the Content Engine either blocks the HTTP request by redirecting the browser to a block page or proceeds with normal HTTP processing.

Apache-Style Transaction Logging

This format is the Common Log File (CLF) format defined by the World Wide Web Consortium (W3C) working group. This format is compatible with many industry-standard log tools. For more information, see the W3C Common Log Format website at http://www.w3.org/Daemon/User/Config/Logging.html.

Support for SNMPv3

ACNS 4.1 software supports the following versions of Simple Network Management Protocol (SNMP):

- Version 1 (SNMPv1)—This is the initial implementation of SNMP. Refer to RFC 1157 for a full description of its functionality.
- Version 2 (SNMPv2c)—This is the second release of SNMP, described in RFC 1902. It provides additions to data types, counter size, and protocol operations.
- Version 3 (SNMPv3)—This is the most recent version of SNMP defined in RFC 2271 through RFC 2275.

SNMPv1 and SNMPv2C do not have any security (that is, authentication or privacy) mechanisms to keep SNMP packet traffic on the wire confidential. As a result, packets on the wire can be detected and SNMP community strings compromised.

To solve the security shortcomings of SNMPv1 and SNMPv2c, SNMPv3 provides secure access to Content Engines by authenticating and encrypting packets over the network. In ACNS 4.1 software, SNMPv3 features are added to the SNMP agent in addition to SNMPv1 and SNMPv2c.

Use the following link to access all MIBs supported in the ACNS 4.1 software:

ftp://ftp.cisco.com/pub/mibs/v2/.

CiscoWorks2000

CiscoWorks2000 (CW2K) is a Cisco product that provides a suite of management applications used to manage most Cisco devices. The Content Engine can interoperate with CiscoWorks2000 without any modification in the following ways:

- CW2K can list the Content Engine under “Generic SNMP” devices.
- The CW2K inventory module lists the Content Engine with the device name, system name, description (including the software version), uptime, and network interface information.
- The CW2K syslog module can understand Content Engine syslogs.
- The CW2K availability module can track the Content Engine.

Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a device discovery protocol that runs on all Cisco-manufactured devices. With CDP, each device within a network sends periodic messages to all devices within the network. These devices listen to periodic messages sent by others in order to learn about neighboring devices and determine the status of their interfaces.

With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. Applications are then able to send SNMP queries within the network.

Caching of HTTP If-Range Requests

If a client has a partial copy of an entity in its cache and wishes to have an up-to-date copy of the entire entity in its cache, it could use the Range request header with a conditional GET request (using either or both If-Unmodified-Since and If-Match.) However, if the GET request fails because the entity has been modified, the client would then have to make a second request to obtain the entire current entity.

The If-Range header allows a client to short-circuit the second request. Informally, the meaning of this header is “If the entity is unchanged, send me the part(s) that I am missing; otherwise, send me the entire new entity.”

Configuring the Content Engine as a Content Routing Agent

ACNS 4.1 software adds support that allows you to configure a Content Engine as a content routing agent. A content routing agent is used in conjunction with the Cisco Content Router 4430 (CR-4430) running the Content Routing software, Release 1.1. The Content Router redirects a user request to the “closest” (best) replicated-content site, based on network delay and other parameters, using a technology called boomerang.

Boomerang agents support multiple domains, where each agent domain may be associated with a different boomerang server. Other than memory limits, there are no limits to the number of domains supported on the agent

Configuring Microsoft Windows Media Player 7.01

Microsoft Windows Media Technologies (WMT) is a set of streaming solutions for creating, distributing, and playing back digital media files on the Internet. WMT includes the end user application (Windows Media Player) Version 7.01, and the server and distribution application (Windows Media Server). To disseminate live and pre-positioned Windows Media content on a Content Delivery Network (CDN), you need WMT caching proxy and server capabilities on the Content Engine.

WMT Conventional Proxy Support

The Content Engine acting as a WMT caching proxy supports a basic proxy feature—it accepts incoming WMT streaming requests from clients and acts on behalf of the clients communicating with the origin server. The WMT caching proxy accepts and serves the streaming requests over Microsoft Media Server (MMS) protocol as well as the HTTP protocol. MMS is the protocol that WMT uses for communication between players and servers.

WMT Transparent Proxy Support

The WMT caching proxy also accepts transparently intercepted requests (through WCCP or Layer 4 redirect) as well as manual proxy requests (clients configured to use an upstream proxy).

Live Splitting

The Content Engine splits requests for live streams. That is, a single stream from the origin streaming server is split to serve each client that requested the stream. In the case of the WMT caching proxy, when the client requests a publishing point on a server (without specifying an ASF file), then the WMT caching proxy dynamically creates an alias file that references the remote server. All further requests to that station are served by splitting the stream.

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

Proxy Authentication

The WMT proxy supports both basic and NTLM authentication by the origin server. When a client requests content that needs user authentication, the proxy acts as an agent, conveying the authentication information to and from the client and server to authenticate the client. Once the client is authenticated, the content is streamed as usual. The authentication is performed for both cached content as well as noncached video on demand content.

Cache Features in ACNS Software, Release 4.1

The following table lists the principal features of the ACNS software Cache application, with the associated command-line interface (CLI) commands.

ACNS Software, Release 4.1 Feature (Cache)	Related CLI Commands
Transparent caching	
Transparency through WCCP	**wccp version 2** **wccp router-list**
Authentication bypass	**bypass auth-traffic** **bypass timer**
Dynamic bypass	**bypass auth-traffic** **bypass timer**
Overload bypass	**bypass load**
Static bypass	**bypass static**
Multiport transparent redirection	**proxy-protocols** **wccp port-list** **wccp service-number**
WCCP flow protection	**wccp slow-start** **wccp flow-redirect**
Accelerated WCCP Layer 2 support	**wccp custom-web-cache** **wccp media-cache** **wccp reverse-proxy** **wccp service-number** **wccp web-cache**
Transparent caching with the Cisco CSS11000 series switch	**http l4-switch enable**
Proxy-style caching (nontransparent operation)	
HTTP proxy caching	**http proxy incoming**
FTP proxy caching	**ftp proxy incoming**
SSL tunneling	**https proxy incoming**
Cache parameter settings	
Caching of authenticated content	**http cache-authenticated**

ACNS Software, Release 4.1 Feature (Cache)	Related CLI Commands
Cache freshness	**http min-ttl** **http max-ttl** **http age-multiplier** **http reval-each-request**
Caching of binary content with cookies	**http cache-cookies**
Object size capping	**http object**
Selective abort of object downloading on client-abort (also called “quick_abort”)	**http cache-on-abort**
HTTP Range request caching	**http cache-on-abort**
Cache hierarchy	
Parent proxy failover	**http proxy outgoing**
Outgoing proxy	**http proxy outgoing** **proxy-protocols**
ICP	**icp client** **icp server**
Employee Internet management	
URL filtering	**url-filter** **url-filter bad-list-deny**
N2H2 filtering	**url-filter N2H2 server** **url-filter N2H2 allowmode**
Websense enterprise server filtering	**url-filter websense enable** **url-filter websense server**
SmartFilter filtering	**url-filter smartfilter**
Logging	
Squid-style transaction logging	**transaction-logs format squid**
Extended Squid transaction logging	**transaction-logs format extended-squid**
Apache-style transaction logging	**transaction-logs format apache**
Sanitized transaction logs	**transaction-logs sanitize**
Exporting log files	**transaction-logs export enable** **transaction-logs export ftp-server**
User authentication	
User authentication configuration	**authentication login** **authentication configuration**
TACACS+ authentication	**authentication** **tacacs**

ACNS Software, Release 4.1 Feature (Cache)	Related CLI Commands
Microsoft NT LAN Manager (NTLM) authentication	**http cache-authenticated** **ntlm server** **http authenticate-strip-ntlm**
RADIUS authentication	**http authentication cache** **http authentication header** **radius-server**
LDAP authentication	**http authentication cache** **http authentication header** **ldap server**
Network management	
SNMP agent support	**snmp-server community**
SNMP traps	**snmp-server enable traps** **snmp-server host**
CiscoWorks2000 syslog format	**logging cw2k**
Cisco Discovery Protocol	**interface FastEthernet 0/0 cdp enable**
TCP stack parameters	
User-configurable TCP parameters	**tcp**
TCP-over-satellite extensions	**tcp client-satellite** **tcp server-satellite**
Streaming media splitting and caching	
Microsoft Windows Media Technologies (WMT) 7.01	**disk config sysfs** *partitionsize* **disk config mediafs** *partitionsize* **wmt enable**
RealProxy 8.01 support	**disk config sysfs** *partitionsize* **disk config mediafs** *partitionsize* **rtsp proxymedia-real enable**
Miscellaneous features	
Rules Template	**rule enable**
Boomerang agent	**boomerang dns enable**
Browser autoconfiguration	**proxy-auto-config**
Healing mode	**http cluster** **http cluster misses** **http cluster max-delay** **http cluster http-port**
Content preloading	**pre-load enable** **pre-load url-list-file**

Limitations

On a CE-507, the number of streams that RealProxy can serve is limited. This occurs when WMT or RealSubscriber is also enabled on the same system, even though they are not serving any streams.

Important Notes

Performance Characteristics of ACNS 4.1

To view performance characteristics of ACNS 4.1 software, see the document titled *ACNS 4.1 Performance Bulletin* at the following URL location:

http://www/warp/public/cc/pd/cxsr/ces/prodlit/

SmartFilter Software

Launching the SmartFilter Administration Console

When you launch the SmartFilter Administration Console, a series of error messages appears before the Configure Remote Servers window opens. These messages state that the program cannot find paths to the required files. Press **OK** for each message until the Configure Remote Servers window opens.

When the Configure Remote Servers window opens with its login prompts, enter the remote server name, IP address, and port number. The error messages should cease once the remote server configuration parameters have been entered.

Content Engine Disk Configuration

SmartFilter files, including the Control List, in the local1/smartfilter directory will return to their default sizes when the Content Engine disk configuration is changed. After disk reconfiguration, either download a new Control List from the FTP site, or if a backup configuration has been created, restore the Control List from the backup Control List XML file.

Content Engine local1 Directory Full

If the local1 directory becomes full, new configurations cannot be applied, nor can a new Control List be downloaded. However, old configuration files, including the Control List, are preserved. After the local1 directory becomes full, it is also possible that the caching process will become unresponsive.

Caveats

This section lists and describes caveats that were resolved in ACNS software, Release 4.1, and caveats that are still open in this release.

Caveats describe unexpected behavior in ACNS software, Release 4.1. Severity 1 caveats are the most serious; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

Open Caveats - ACNS Software Release 4.1

- CSCdu79580

  Symptom: 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.

  Condition: This symptom occurs on systems running the E-CDN application, Release 3.0 and 4.0.

  Workaround: The E-CDN application must stopped and restarted to clear the error condition. Follow these steps:

  1. Wait for an automatic restart; this may take up to 60 minutes (all versions).

  2. Disable and then enable the E-CDN application (for the E-CDN Release application, Release 4.0 and later).

  3. Reboot the system (all versions).

  4. Use Telnet to access the system and use the **vbox stop** and the **vbox start** commands (Version 3.0).

  This pause *only* occurs when you click the NEXT button several times a second because the problem is the frequency of clicking and not the actual click count. You can avoid the pause by clicking NEXT at a slower pace, and pausing for a second or two between clicks.

- CSCdv72664

  Symptom: Under very rare circumstances, a Content Engine (CE-5xx) may display messages as shown below when saving the running-config to the startup-config, when performing an upgrade or downgrade, or when the Content Engine is booting up:

  ```
  PRIMARY AND BACKUP CONFIGFILES ARE CORRUPT!
  YOUR SYSTEM NEEDS A NEW FLASH DEVICE
  CONTACT CISCO TECHNICAL ASSISTANCE CENTER IMMEDIATELY
  DO NOT POWER DOWN YOUR SYSTEM
  ```

  Condition: This most likely occurs because you have a defective Flash device.

  Workaround: There is no known workaround. Contact the Cisco Technical Assistance Center (TAC) to have the system returned for further analysis.

- CSCdw25217

  Symptom: NTLM authentication fails if either of the following occurs:

  – There is no reverse DNS lookup for primary domain controller (PDC) (NTLM domain controller)

  or

  – The NetBIOS name of the primary domain controller is different from its DNS name.

  Condition: This occurs in ACNS software, Release 4.1.

  Workaround: Users can enter a hidden CLI **config** command to set the NetBIOS name for the primary domain controller. In global configuration mode, enter:

  ntlm server pdc-netbios-name xxxxx

- CSCdw51456

  Symptom: Although the **copy disk ftp** command functions normally, it does not display any output data.

  Condition: This occurs in ACNS software, Release 4.x.

  Workaround: Enter the username and password properly even though the user prompt is not shown.

- CSCdw53913

  Symptom: An error message, such as the following, may appear in the syslog.txt file:

  ```
  Jan 20 18:30:34 bfc9000 Diamond: KERNEL: assertion (req->sk == NULL) failed at
  tcp_ipv4.c(780):tcp_v4_search_req
  ```

  Condition: This happens only on a CE-7320 and when WCCP is enabled. It does not appear to have any adverse effect on system functionality. WCCP continues to work as expected.

  Workaround: There is no known workaround.

- CSCdw62458

  Symptom: HTTPS performance over the Content Engine is much slower than without the Content Engine.

  Condition: Occasionally, this is due to a duplex mismatch between the Content Engine and the switch. Sometimes it is due to slowness in the HTTP implementation inside the Content Engine.

  Workaround: For the first condition, check the duplex setting on both the Content Engine and the switch. For the second condition, upgrade to the latest Content Engine software.

- CSCdw64167

  Symptom: The CPU usage data shown with the **show statistics http usage** command is different from the data shown with the **show processes cpu** command.

  Condition: This occurs in ACNS software, Release 4.x.

  Workaround: There is no workaround. The CPU usage data shown when you use the **show processes cpu** command is the CPU average usage since the last time the system was rebooted. The CPU usage data shown when you use the **show statistics http usage** command is the current CPU usage and peak CPU usage in history.

- CSCdw66215

  Symptom: The cache process fails and then restarts.

  Condition: This happens under high load conditions when the SmartFilter feature is enabled. It occurs on CE-7320 hardware only.

  Workaround: Currently the only workaround is to disable the SmartFilter feature.

- CSCdw68848

  Symptom: When you try to downgrade from ACNS software Release 4.1 to E-CDN Release 3.x software on a system where the **disk config** command has been used to assign non-ecdnfs storage, the downgrade sometimes fails.

  Condition: Downgrade code requires that an ecdnfs file system be present on disk00. This is not always the case after the **disk config** command has been run.

  Workaround: Before installing the downgrade image, ensure that the device in question has an ecdnfs file system on disk00. This can be done by inspecting the output of show disk details. If there is no ecndfs file system on disk00, you can create it by entering the **disk config** command as follows:

  disk config sysfs 1GB ECDNFS remaining

Following a reboot, every drive in the system will have an ecdnfs file system on it, and the downgrade will succeed.

- CSCdw71468

  Symptom: When you do a programmatic import 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.

  Condition: This occurs in ACNS software, Release 4.1.

  Workaround: There is no known workaround.

- CSCdw71953

  Symptom: The HTTP proxy stops accepting new requests.

  Condition: The sysfs (/local/local1) partition is full.

  Workaround: Delete some unused files on the sysfs to free some disk space, and then reboot the system.

- CSCdw73052

  Symptom: The Cache application unexpectedly reloads on a CE-7320 when initializing service.

  Condition: The problem happens very rarely. It occurs on the CE-7320 during HTTP cache service initialization because of an internal system error.

  Workaround: There is no workaround. The Content Engine's internal system monitoring facility detects the crash and restarts the Cache application automatically so that normal HTTP service will resume.

- CSCdw75147

  Symptom: TACACS authentication does not work when authenticating for Secure Shell (SSH) sessions.

  Condition: This occurs when you attempt to log on to SSH on a Content Engine that has TACACS authentication enabled.

  Workaround: The user must use the local username and password authentication on the Content Engine if you want to use SSH sessions.

- CSCdw75439

  Symptom: The Storage Array 6 (SA-6) is not recognized by the Content Engine.

  Condition: The LED on the defective drive flickers once per second. The SA-6 is not recognized and does not appear in the **df** command display.

  Workaround: Remove the corrupted drive to allow the remaining drives to come on line and be recognized by the Content Engine.

- CSCdw76569

  Symptom: The Cache application unexpectedly reloads on a CE-7320 platform when this platform is overstressed.

  Condition: The problem happens on an overstressed CE-7320 platform that is serving HTTP traffic at 1600 transactions per second with some rules turned on and minimal WMT streaming traffic going through. The Cache Engine's HTTP cache becomes overloaded and runs out of memory buffer, with the result that the system unexpectedly reloads.

  Workaround: There is no known workaround. The Content Engine's internal system monitoring facility detects the unexpected reload of the cache process and restarts the cache process automatically so that the Content Engine resumes normal functioning.

- CSCdw77632

  Symptom: The system slows when using rules that do regular expression (regex) matching.

  Condition: This situation occurs when rules that do regex matching are configured.

  Workaround: There is no workaround. However, removing some noncritical rules and rewriting certain rules may improve performance.

- CSCdw77773

  Symptom: The HTTP proxy unexpectedly reloads.

  Condition: This happens very rarely. A rare combination of URL characters may cause this problem.

  Workaround: There is no workaround.

- CSCdw77966

  Symptom: The **cache clear** command sometimes does not finish. Instead, a message appears that includes the text "verifier error." Cache service is not interrupted. However, cfs volumes may have been cleared, while other volumes may not have been cleared. The **show statistics cfs** command shows which volumes were cleared (low count of bytes in use) and which were not cleared (high or unchanged count of bytes in use).

  Condition: This situation occurs when the CE-7320 is running ACNS 4.1.x software (and possibly other versions) and actively passing traffic. The may or may not happen on other Content Engine platforms.

  Workaround: Run the **cache clear** command when the Content Engine is not accepting any new traffic and all requests have been serviced. You can also try using the **cache clear force** command.

- CSCin03870

  Symptom: The web server unexpectedly reloads when transitioning from an SNMP page to a SNMPv3 GUI page.

  Condition: This occurs when the SNMP community string is longer than 27 characters. This string is set in the SNMP GUI page or through the CLI.

  Workaround: Change the community string to be less than 27 characters, for example,

  ```
  snmp-server host [host_ip_address] [community_string]
  ```

- CSCdv24940

  Symptom:A configuration command such as **hostname** or **ip address** may return the following error message:

  ```
  touch:/sonoma/state/setup-flags/manual-netrcm-config:No such file or directory
  ```

  Condition:The error condition does not affect the configuration and can be ignored. These messages occur when an ECDNFS partition is not configured. This error condition has been observed in ACNS 4.1 software.

  Workaround:If preserving data on the disk drives is not a concern, repartition the disk drives and create a nonzero-size ECDNFS partition with the **disk config** EXEC command.

Resolved Caveats - Resolved in ACNS Software, Release 4.1

- CSCsp01083

  If you try to import media files in a Netscape browser by clicking the computer name in the Using PC Folders for Importing section of the Media Importer page, you see a Login Incorrect error message.

A Content Distribution Manager is connected to two Content Engines, A and B. The Content Distribution Manager and Content Engine A are on one subnet, and Content Engine B is on another subnet. If the Content Distribution Manager and Content Engine A are rebooted, a file imported on a multicast channel is replicated only to Content Engine A.

- CSCdt77959

  If the user sets the timeout value through the Multicast Server page on the Content Distribution Manager GUI and if the Digital Fountain server is overloaded, then the files that the Digital Fountain server has not started serving may never be served.

- CSCdt84468

  A change in the multicast timeout on the Content Distribution Manager is ignored if the change is made after the Digital Fountain client on the Content Engine has already begun downloading the content.

- CSCdu26321

  Inconsistent behavior occurs between the Internet Explorer 5.0 and Netscape Navigator 4.7.7 browsers. A Digital Fountain server that appears as online when you use Internet Explorer 5.0 appears as offline when you use Netscape Navigator 4.7.7.

- CSCdu48145

  FIN packets, which are harmless to the operation of Content Engine as well as to the network in general, are present on the customer network.

- CSCdu58231

  Deleting a channel with a large number of items causes the Content Distribution Manager GUI to freeze.

- CSCdu58252

  Deleting a channel with a large number of items takes a very long time.

- CSCdu89034

  If connection to the Content Distribution Manager is lost, then all the devices attached to the Content Distribution Manager send frequent TCP SYN messages to the Content Distribution Manager. If more devices are attached to this Content Distribution Manager, this may cause a SYN storm. This symptom also occurs with a Content Engine that has lost its network connection, and has many children attached to its hierarchy.

- CSCdv02664

  RADIUS authentication fails if a username or password length is greater than the maximum length of 20 characters for a RADIUS username and 16 characters for a password.

- CSCdv15269

  Removing a channel from the Content Distribution Manager GUI while the Content Engine is off line leaves the contents on the Content Engine. The contents stay on the Content Engine even after it comes on line again.

- CSCdv20665

  The Content Distribution Manager GUI is very slow or unusable.

- CSCdv20680

  When you perform Content Distribution Manager GUI operations, requests for content from clients are processed slowly.

- CSCdv20748

  The Content Distribution Manager restarts itself internally during very heavy operations.

- CSCdv20754

  After the Content Router 4430 IP address is changed, the Device Console shows it as green (online), but with the old IP address. Even though the System page shows the new IP address, Content Engines try to contact the Content Router using the old IP address.

- CSCdv20780

  While the Content Distribution Manager is attempting to import files, not all files are imported.

- CSCdv25987

  The search facility on the Content Distribution Manager is unpredictable and is difficult to use. When a search for devices is done on the Content Distribution Manager using a substring, it can return duplicate results for the Content Engine and miss Content Engines that are meant to be listed.

- CSCdv38067

  In a network where Content Engines are behind a firewall (in a private address space), the Content Distribution Manager is able to route a request behind the firewall, but a Content Router is not. When there is no firewall, no problem occurs.

- CSCdv41455

  The Content Distribution Manager reboots if the user exits the Backup/Restore Utility through the close box without starting the restore procedure.

- CSCdv44014

  When a playlist is defined but no audio/video card is present or it is no longer detected by the MPEG decode driver, the video server attempts playback. This causes an event record to be written and an exception.

- CSCdv46802

  After the HTTP port is changed and the Content Distribution Manager is rebooted, the HTTP server listens on the new port, but all Content Engines go off line. This symptom occurs with regard to changing the Alternate IP Port setting as well.

- CSCdv60905

  If a user disables the E-CDN application, uses the CLI to change network settings, and then enables the E-CDN application within 40 seconds, the following symptoms may occur:

  1. The changes are lost and are replaced with old network settings stored in the library of the E-CDN application.

  2. The E-CDN application pauses indefinitely in an “IP missing” state.

- CSCdv61722

  The upgrade/downgrade manager may be blocked from servicing FTP requests if the E-CDN application is enabled.

- CSCdv28262

  Even with automatic hierarchy disabled, there will still be router requests sent by every Content Engine every 30 seconds for every channel on each of those Content Engines.

- CSCdv43167

  Certain commands generate a spurious diagnostic error in configuration mode, including host name and IP default gateway, but there is no impact on the command itself:

  ```
  touch: /sonoma/state/setup-flags/manual-netrcm-config: no such file or directory in the session output
  ```

- CSCdv54977

  The cache process may restart on a Content Engine 7320.

- CSCdv66971

  In certain circumstances, downgrading from ACNS 4.0.3 software to E-CDN 3.x software can hang the system. This occurs only if the Content Engine, Content Router, or Content Distribution Manager console port is connected to a console server, a Cisco 2500 Series server, for instance, *and* if there is no active session on the serial port of the console server to which the device is connected.

- CSCdv70012

  The cache process may fail if healing mode is enabled.

- CSCdv71152

  Deleting several messages using Microsoft Hotmail or Microsoft Outlook Express Version 6 fails.

- CSCdv72187

  If no name server has been configured, the cache process exits while serving a request that requires name resolution.

- CSCdv72270

  The Windows Media Technologies (WMT) service stops working if it is under extremely high load for a long period. In this case, WMT traffic will be refused by the Content Engine.

- CSCdv72605

  The cache process may fail if healing mode is enabled.

- CSCdv73439

  Rebooting with a communications server connected to the console brings a Content Engine into rescue mode.

- CSCdv73808

  The static bypass list does not support more than 32 entries.

- CSCdv75250

  If an HTTPS request is directed to the Content Engine on port 443 with the URL filtering feature enabled, it may cause the cache process to crash.

- CSCdv76775

  When you downgrade from ACNS 4.0 software to Cache 3.x software, Cache 3.x software detects a problem with the software file system (swfs) and decides to reformat it.

- CSCdv77157

  When you use the **disk add** CLI command to incorporate newly added disks with the E-CDN file system (ecdnfs) allocated on them, the E-CDN application does not make use of the additional storage partitions. E-CDN-fill happens continuously, sometimes causing the E-CDN application not to start.

- CSCdv80480

  The ACNS 4.x to Cache 2.x software downgrade fails, rebooting the system continuously.

- CSCdv80694

  The HTTP proxy service crashes.

- CSCdv81077

  The backup and restore functionality on a Content Distribution Manager 4650 with ACNS 4.0.3 software and with total channel size of more than 40 GB does not go through successfully.

- CSCdw05501

  The cache process crashes when end-to-end NTLM authentication is triggered and the connection between the Content Engine and the browser is lost before the connection between the Content Engine and the web server is closed.

- CSCdw16537

  The **icp server remote-client** CLI command is now limited to eight entries.

- CSCdw16542

  Because of a limitation on the total cache file system (cfs) storage space supported, the **cfs mount** CLI command is now limited to seven entries.

- CSCdw19568

  Clicking the Update button in the Cache software GUI after modifications have been made saves changes only to the running configuration, but does not write changes to the startup configuration in NVRAM. Upon reboot, all GUI changes are lost.

- CSCdw27994

  The cache process stops servicing requests that need a DNS lookup.

Documentation Updates

The following information updates several sections in the ACNS software, Release 4.1 documentation set.

Errors

The following information updates the "RealSubscriber License Commands" and the "Using the Distributed Licensing Feature" sections of the *Cisco Content Delivery Networking Products Getting Started Guide*. This information also updates the "Splitting Live RealServer Broadcasts" section of Chapter 3 of the *Cisco Application and Content Networking Software E-CDN Administrator's Guide*.

The statement that "RealServer is licensed by default to serve 10 simultaneous streams" is *not* a true statement. All streams have to be purchased.

Omissions

Splitting Live WMT Broadcasts

The following information updates the "Splitting Live WMT Broadcasts" section of Chapter 3 of the *Cisco Application and Content Networking Software E-CDN Administrator's Guide, Release 4.1*.

Note that the name for the broadcast station must end in an .asf suffix.

RADIUS Authentication Redirection

The following information updates the "RADIUS HTTP Request Preloading" section of Chapter 10 of the *Cisco Application and Content Networking Software Caching Configuration Guide, Release 4.1*.

The **redirect** option of the **radius-server** command redirects an authentication response to a different authentication server if an authentication request using the RADIUS server fails.

Note The **rule** command is relevant to RADIUS authentication only if the **redirect** option as been configured.

WMT Multicasting

The following information updates the "Configuring Microsoft Windows Media Player 7.01" section of Chapter 13 of the *Cisco Application and Content Networking Software Caching Configuration Guide, Release 4.1*

Based on the capabilities and the limitations of the network, a Content Engine can receive and deliver WMT streaming content through IP multicast. This multicast feature enables you to distribute streaming media efficiently by allowing different devices on the IP multicast to receive a single stream of media content simultaneously. This can save significant network bandwidth consumption because a single stream is sent to many devices, rather than sending a single stream to just a single device every time this stream is requested.

Enable the multicast feature by setting up a multicast address in the Content Engine to which different devices, configured to receive content from the same channel, can subscribe. The delivering device sends content to this multicast address, from which it becomes available to all subscribed receiving devices.

Use the **wmt multicast** {**schedule-start** *name minute hour day month* | **station-configuration** *name dest_addr dest_port media_source* [**play-forever**]} command to enable WMT multicasting on the Content Engine. The **schedule-start** *name minute hour day month* option creates a scheduling option to allow the Content Engine to start a multicast at a specified time. This option only works if you have configured a multicast station first.

Note You must enable WMT on the Content Engine before you can use the **wmt multicast** command. See the "Enabling WMT on the Content Engine" section on page 13-6 for more information on this feature.

The **station-configuration** *name dest_addr dest_port media_source* option specifies a multicast station name, an IP address, port number and media source for the multicast station created. One station needs a multicast IP address. You must enter a valid class D IP address multicast address in the range 224.0.0.0 to 239.255.255.255, except for the reserved IP ranges based on RFC 1700 and related documents as follows:

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

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

The allowed multicast port range defined by the *dest_port* option is 1 through 65535. However, the multicast-enabled network may impose certain restrictions on your choice of port. Normally port numbers below 1024 should be avoided, but the Content Engine does not enforce any restrictions. The *media_source* option determines the source of the multicast. The source can be any valid WMT URL. In other words, if you can play the URL on your Windows Media player, then you can make this URL the source of your multicast.

The Content Engine can support the following multicast scenarios:

- Multicast in and unicast out
- Multicast in and multicast out
- Unicast in and multicast out

Unicast in and Multicast out

The unicast input can be from a video- on-demand (VOD) publishing point, a live unicast publishing point, an encoder, or a streaming media source from a local disk. The asf header obtained from the unicast input and a configured multicast-out IP address are used to create the multicast description .nsc file. The clients use this easily accessible file to subscribe and request the multicast.

Enabling WMT Multicasting in the Unicast in and Multicast out Scenario

To enable WMT multicasting in this scenario with CLI commands, follow these steps:

Step 1 Enable WMT multicasting and configure a multicast station on the Content Engine in global configuration mode with the **wmt multicast station-configuration** command:

```
ContentEngine(config)# wmt multicast station-configuration test1 233.33.33.33 6666
mms://sourceIPaddress/source.asf play-forever
ContentEngine(config)#
```

In this example a station named *test1* that acts as the multicast source file is configured. Its class DIP address is 233.33.33.33 and the multicast port is 3333. The **play-forever** option is used. This option automatically restarts the stream from the beginning once the end of the multicast has been reached.

Note This source file can be located on any WMT server, including a Windows server, or the Content Engine, assuming that the source device and the requesting clients are on the same subnet. In the case of the Content Engine, pre-positioned media files should be stored in the /local1/wmt_vod directory. In this scenario, the media source is represented by mms://CEIPaddress/wmt_vod/sourcefile.nsc.

Step 2 Start the multicast from the source file. Use the **wmt** command in EXEC mode.

```
ContentEngine# wmt multicast-station start test1
ContentEngine#
```

Step 3 Open your WMT player and choose **File** > **Open URL**. Enter the following:

```
http://CEIPaddress/test1.nsc
```

Step 4 Click **OK**. The WMT player should connect to the MMS media source specified in Step 1.

Multicast in and Multicast out

In this multicasting scenario, another description file *.nsc is created that is accessible through multicast out to clients. The clients use this file to subscribe and to request the multicast. Use the steps described in the "Enabling WMT Multicasting in the Unicast in and Multicast out Scenario" section on page 20 to add another multicasting station and play the multicast request through the requesting WMT player.

Note The initial delivery of the requested file is through unicast out. However, once a single client has access to this file, other clients can join the multicast group and receive the same content.

Multicast-in and Unicast-out

In this scenario a unicast-out publishing point is created to deliver the incoming stream live to requesting clients.

Enabling WMT Multicasting in the Multicast in and Unicast out Scenario

To enable WMT multicasting in this scenario with CLI commands, follow these steps:

Step 1 Enable WMT multicasting and configure a broadcasting station on the Content Engine in global configuration mode with the **wmt broadcast** command:

```
ContentEngine(config)# wmt broadcast alias-name unicast-station source
http://172.16.30.31/station.nsc
ContentEngine(config)#
```

In this step a unicast station with an alias name *unicast-station* is configured with a multicast source station.nsc file.

Step 2 Open your WMT player and choose **File** > **Open URL**. Enter the following URL:

```
mms://CEIPaddress/unicast-station
```

Click **OK**. The WMT player should connect to the MMS media source specified in Step 1.

Rules Template Processing Considerations

The following information updates the "Actions and Patterns" section of Chapter 15 of the *Cisco Application and Content Networking Software Caching Configuration Guide, Release 4.1*.

There is a predefined order of execution among rule actions and rule patterns. In other words, a group of rules with the same action will always be executed either before or after another group of rules with a different action. See the "Rule Action Execution Order" section on page 22 for the order of rule action execution. This order is not affected by the order in which the rules are entered using CLI commands.

Among rules of the same action, there is also predefined execution order among the rule patterns. This means that within a group of rules of the same action, one group of rules with the same pattern will always be executed either before or after another group of rules with a different pattern. See the "Rule Pattern Execution Order" section on page 22 for the order of rule pattern execution. This order is not affected by the order in which the rules are entered using CLI commands.

Rule Action Execution Order

The order of rule action execution is as follows:

1. **No-Auth**—Before authentication using RADIUS/LDAP/NTLM
2. **Reset**—Before cache lookup
3. **Block**—Before cache lookup
4. **Redirect**—Before cache lookup
5. **Rewrite**—Before cache lookup
6. **Refresh**—On cache hit
7. **Freshness-factor**—On cache hit
8. **Use-server**—On cache miss
9. **No-proxy**—On cache miss
10. **Use-proxy-failover**—On cache miss
11. **Use-proxy**—On cache miss
12. **TOS/DSCP server**—On cache miss
13. **TOS/DSCP client**—On cache miss
14. **No-cache**—On cache miss
15. **Selective-cache**—On cache miss

Note The commands **rule no-proxy**, **rule use-proxy-failover**, and **rule use-proxy** take precedence over **https proxy outgoing**, **http proxy outgoing**, and **ftp proxy outgoing** commands.

During a request using the Rules Template CLI commands, rule actions 1 through 4 use the original URL request for pattern matches. After a URL rewrite (rule action 5), rule actions 6 through 15 use the transformed URL for rule executions.

The commands **rule reset**, **rule block**, **rule rewrite**, and **rule redirect** support the following additional patterns for Rule Templates requesters:

- **Request-line**—Matches first line
- **Referer**—Matches referer header
- **User-agent**—Matches User-agent header

Rule Pattern Execution Order

The order of rule pattern execution is as follows:

1. **Dst-port**—Destination port check
2. **Src-ip**—Source IP address check
3. **URL-regex**—URL regex check
4. **Domain**—Domain rule check

5. **Dst-ip**—Destination IP address check
6. **MIME-type**—MIME-type regex check

Note Because the MIME type exists only in the response, only the actions **freshness-factor**, **refresh**, **no-cache**, and **selective-cache** apply to a rule of MIME type.

A search for a rule match with the remaining pattern will not be performed if a match has already been found. For instance, if a match for the **rule block** action is found with a **url-regex** request, then the remaining patterns **domain**, **dst-ip**, or **mime-type** are not searched.

Rules are ORed together. Multiple rules may all match a request; then all actions are taken, with precedence among conflicting actions. Each rule contains one pattern; patterns cannot be ANDed together. In future releases, ANDed patterns may be supported.

It is possible to circumvent some rules. For example, to circumvent a rule with the **domain** pattern, enter the web server IP address instead of the domain name in the browser. A rule may have unintended effects. For instance, a rule with the **domain** pattern specified as “ibm” that is intended to match “www.ibm.com” can also match domain names like www.ribman.com.

A **src-ip** rule may not apply as intended to requests that are received from another proxy because the original client IP address is in an X-forwarded-for header.

If a rule pattern match occurs, then the rest of the patterns are not searched. If the server has already marked an object as noncacheable, **no-cache** rules are not checked at all, since the server already recognizes that this object is not cached. Any **no-cache** rule checks are performed only for cacheable requests.

Order of Execution Among Rules of Same Action and Same Pattern

Among rules of the same action and the same pattern, the order of execution of rules is in the reverse order from which the rules are entered. For instance, if **use-proxy** commands are entered in the following order:

use-proxy 1.2.3.4 abc.abc.com

use-proxy 2.3.4.5 *.abc.com

then a request to abc.abc.com is sent to proxy 2.3.4.5 because the **use-proxy 2.3.4.5 *.abc.com** command is entered last and evaluated first. However, if the same commands are entered in the reverse order as follows:

use-proxy 2.3.4.5 *.abc.com

use-proxy 1.2.3.4 abc.abc.com

then a request to abc.abc.com is sent to proxy 1.2.3.4, because the **use-proxy 1.2.3.4 abc.abc.com** command is entered last and evaluated first.

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

Obtaining Documentation

The following 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 the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

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

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  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 corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write 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 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 to

- 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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

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

Inquiries to Cisco TAC 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.

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

Cisco TAC Web Site

The Cisco TAC Web Site allows you 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 the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services 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 the following URL to register:

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

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

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; 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 will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following 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). In addition, 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.