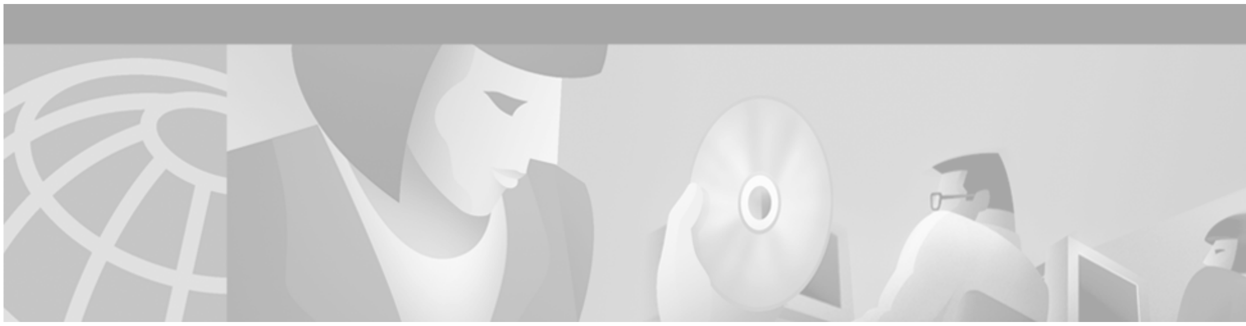


Release Notes for Cisco Cache Software, Release 2.3.1

May 1, 2001

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

Contents

These release notes describe the following topics:

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

Introduction

These release notes describe command enhancements and the open and resolved caveats included in the Cisco Cache software, Release 2.3.1 for the Cisco Content Engines and Cisco Cache Engines. Software Release 2.3.1 is an extension of Release 2.3.0. To simplify terminology, both the Cache Engine and the Content Engine are referred to as the "CE." Refer to the *Cisco Cache Software Configuration Guide, Software Versions 2.2.x, 2.3.x* for the following information:

- Instructions for configuring and maintaining the Cisco Cache software
- Descriptions of Web Cache Communication Protocol (WCCP) Version 1 and Version 2

Note WCCP is also known as the Web Cache Control Protocol and the Web Cache Coordination Protocol.

Refer to the *Cisco Cache Software Command Reference, Release 2.3.0* for global configuration, EXEC, **show**, and interface command descriptions. Refer to the *Cisco Content Engine 500 Series Hardware Installation Guide* for information on the Cisco Content Engines. See the "Related Documentation" section on page 10 for information about the web sites from which to obtain related documentation.

Determining the Operating Software Version

Note We recommend that you install the most recent software release available for your model of the CE.

To determine the version of the software currently running on the Cisco CE, log on to the CE and enter the **show version** EXEC command.

Downloading Cache Software

CE Cache software can be downloaded from the Cisco Systems Software Center at the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/cache-engine20

Upgrading to a New Software Release

Two types of CE Cache software files are available on Cisco.com to download: files with the .pax suffix and files with the .bin suffix. The .pax file contains the full-image software with the graphical user interface (GUI) and is the file routinely installed. The .bin file software is for recovery situations that require booting from the network, or restoring Flash memory. Refer to the section "Recovering the System Software" in the *Cisco Cache Software Configuration Guide, Software Versions 2.2.x, 2.3.x* for instructions on loading your system image with the .bin file.

Step 1 Use an FTP client to transfer the .pax file to the */local* directory of your CE.

Step 2 Log on to the CE, and at the privileged level EXEC command prompt enter:

```
install filename.pax
```

where *filename* is the name of the .pax file.

Step 3 Follow the command-line interface instructions as prompted. At the following prompt, enter **y**:

```
Copy new image to flash memory?[yes]:
```

Step 4 After the CE has rebooted, use the **show version command** to display the current software version.

New and Changed Information

Release 2.3.1, like Release 2.3.0, operates on all models of the Cisco 500 series Cache Engines, as well as the Cisco Content Engine 507, 560, and 590.

The following topics are described in this section:

- NTLM Authenticated Traffic Bypass, page 4
- New radius-server Command Options, page 4
- New SNMP Object Identifiers, page 4
- Enhanced WCCP Services Page, page 7

NTLM Authenticated Traffic Bypass

The **bypass auth-traffic** command now supports the bypassing of Windows NT LAN Manager (NTLM) authenticated traffic. You can now configure the Cache Engine software to bypass all the authenticated traffic using the new command option **all** or bypass only NTLM authenticated traffic using the new command option **ntlm-only**.

The following are the enhancements to the **bypass auth-traffic** command:

bypass auth-traffic all

bypass auth-traffic ntlm-only

For backward compatibility, the **bypass auth-traffic enable** command is still supported.

The **show bypass list** command also now provides information about bypassed NTLM authentication traffic. For example:

```
console# show bypass list

         Client               Server       Entry type
         ------               ------       ----------
     10.1.200.2:0         172.16.7.52:0 ntlm-auth-traffic
```

New radius-server Command Options

Two new **radius-server** command options have been added to Release 2.3.1 to ensure that the CE does not issue unnecessary user prompts during a session. These were added to resolve caveat CSCds63770. The following are the new **radius-server** command options:

radius-server multiple-user-prompt-timeout *value*

radius-server multiple-user-prompt-fix enable

The **multiple-user-prompt-timeout** command option denotes the amount of time after which the next prompt, the 401 (unauthorized) response, will be sent to the user. The default value is 25 seconds. The **multiple-user-prompt-fix enable** command option is used to enable the fix to caveat CSCds63770 and is enabled by default.

See the "Resolved Caveats—Software Release 2.3.1" section for information about caveat CSCds63770.

New SNMP Object Identifiers

New Simple Network Management Protocol (SNMP) MIB objects have been added to the Cisco Cache software, Release 2.3.1. Most of these objects are used to obtain more information about the cache file system (cfs) disk volumes and the DOS file system (dosfs) disk volumes. One new MIB object is used to determine the duplex value of the Ethernet port. See Table 1 for information about the new 2.3.1 SNMP MIB objects.

New SNMP traps have also been added to the Cisco Cache software, Release 2.3.1. See Table 2 for information about the new 2.3.1 SNMP traps.

Table 1 provides the name of each new SNMP MIB object and its description.

Table 1 New 2.3.1 SNMP MIB Objects

Variable Name	Description
cceUsageDiskVolumeName	Name of the cfs disk volume.
cceUsageDiskVolumeEverMounted	Indicates whether the cfs disk volume was ever mounted.
cceUsageDiskVolumeCurrentlyMounted	Indicates whether the cfs disk volume is currently mounted.
cceUsageDiskVolumeUnmountReason	Indicates the reason why the cfs disk volume is currently unmounted. The possible reasons for the unmounted state are: • normal(1)—user-initiated unmount **using cfs unmount** command • error(2)—cfs unmounted disk volume because of errors If the given cfs disk volume is unmounted because of an error, then a trap (**cacheTrapDiskVolUnmounted)** is generated to notify the managing station. See Table 2.
cceUsageDiskVolumeCurrent	Specifies the percentage of the cfs disk volume currently being used.
cceUsageDiskVolumePeak	Specifies the percentage of the cfs disk volume that was used during its peak usage.
cceIfFullDuplex	Specifies the duplex value of the Ethernet port. The possible duplex values are: • true(1)—full duplex • false(2)—half duplex
cceLoggingWriteFailReason	Indicates the reason the last translog write operation failed. If the last operation was successful, this object displays as “NotApplicable.”
cceUsageDosfsVolumeName	Specifies the dosfs volume name.

Table 1 New 2.3.1 SNMP MIB Objects

Variable Name	Description
cceUsageDosfsVolumeState	Specifies the state of a given dosfs volume. The following are the possible state values and associated descriptions: • 0—DOSFS volume not accessed since ready change. The dosfs volume enters into this state whenever a driver senses that a device has come online or gone offline. • 1—DOSFS volume reset but not mounted. • 2—DOSFS volume mounted. • 3—DOSFS volume reset failed. • 4—DOSFS volume mount failed. • 5—DOSFS volume is being unmounted. • 6—DOSFS volume has been unmounted. • 7—Unmounts on DOSFS volume disabled.
cceUsageDosfsVolumeFreeSpace	Specifies the amount of free space available on a given dosfs volume.
cceUsageDosfsVolumeTotalSpace	Specifies the total space available on a given dosfs volume.

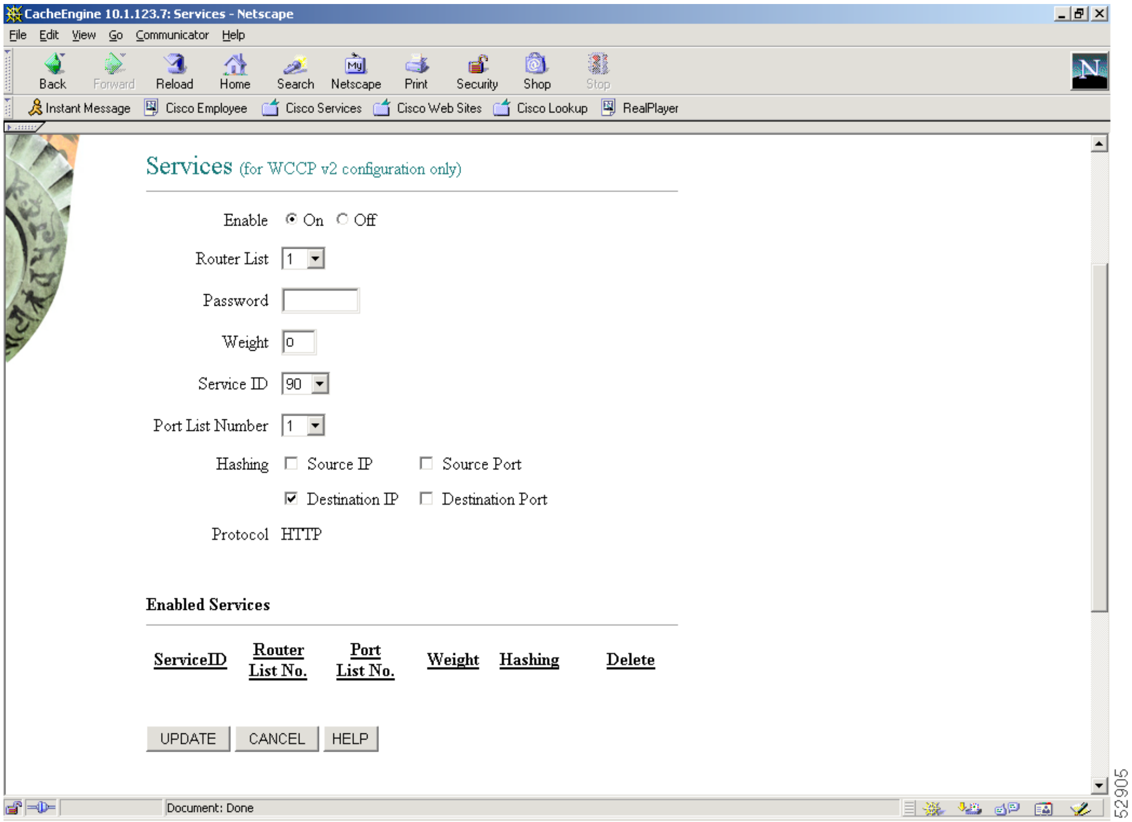
Table 2 New 2.3.1 SNMP Traps

Trap Name	Description
cacheTrapDiskVolUnmounted	Indicates the cfs disk volume has been unmounted because of an error.
cacheTrapDosfsVolFull	Indicates the dosfs volume is full.

Enhanced WCCP Services Page

The graphical user interface WCCP Services page shown in Figure 1 has been enhanced to display the list of enabled services. The WCCP Services page now also provides an option to selectively delete the individual services. Refer to the WCCP Services page online help for more information.

Figure 1 Management GUI—WCCP Services Page


CacheEngine 10.1.123.7: Services - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Instant Message Cisco Employee Cisco Services Cisco Web Sites Cisco Lookup RealPlayer
UPDATE
CANCEL
HELP
Document: Done
52905

Services (for WCCP v2 configuration only)

Enable ● On ○ Off

Router List 1

Password

Weight 0

Service ID 90

Port List Number 1

Hashing □ Source IP □ Source Port

☑ Destination IP □ Destination Port

Protocol HTTP

Enabled Services

ServiceID	Router List No.	Port List No.	Weight	Hashing	Delete

Caveats

The following sections describe the open and resolved caveats for Release 2.3.1. Caveats describe unexpected behavior in the Cisco Cache software.

Open Caveats—Software Release 2.3.1

The following section lists and describes the open caveats for Release 2.3.1:

CSCdt18114

When the CE is made to boot up from a TFTP server, it fails because of a transfer timeout. This failure is due to the extra time taken by the switch connected to the CE to run the spanning tree algorithm.

Workaround: Enable the PortFast-start feature within the switch using the **set spantree portfast** command. This command allows a port that is connected to a single device to start faster. This feature can be used only if one device is connected to the port. This example shows how to enable the spanning tree PortFast-start feature on port 2 on module 1:

```
Console> (enable) set spantree portfast 1/2 enable
```

As another workaround, use the Tool Command Language (TCL) shell command **reboot tftp host filename username**.

Resolved Caveats—Software Release 2.3.1

The following section lists and describes the caveats from previous releases that are resolved in Release 2.3.1:

- CSCds47110

  If an Expiry HTTP response header does not conform to one of the three CE-supported date field formats, the CE ignores the expiration date within this header. In the absence of a valid expiration date, the CE relies on the minimum Time To Live configuration setting to determine when a given object reaches its expiration date.

- CSCds64770

  The CE using a Lightweight Directory Access Protocol (LDAP) server for LDAP authentication allows a user to be authenticated using a valid username and a null password, although a valid password for the user is configured within the LDAP server.

- CSCds43514

  During a WCCP clean shutdown, the CE does *not* wait until all or most of the connections have been serviced before proceeding with a reboot, as it is designed to do. Instead the CE only waits for the configured **max-wait** interval to elapse and then reboots thereby not allowing adequate time for the remaining open connections to close.

  With Release 2.3.1, the CE first waits until all or most of the connections have been serviced and then waits until the configured **max-wait** interval elapses before it reboots.

- CSCds53244

  The Remote Authentication Dial-In User Service (RADIUS) server deletes the connections of the most recently logged-in users when it has approximately 1000 active users logged in. These users are then prompted to reenter their user name and password for authentication with the RADIUS server.

- CSCds61518

  When Hypertext Transfer Protocol (HTTP) revalidation is turned on for text objects, the CE also revalidates the associated binary objects during its revalidation of the text objects. The CE performs simultaneous revalidation of both types of objects regardless of whether revalidation is turned on for the binary objects or whether the binary objects have expired. The problem is that the CE does not distinguish between a text and a binary object during the revalidation process. The CE applies the text object's **age-multiplier** value to the binary object when calculating the expiration date of each object.

- CSCds63770

  The CE unnecessarily sends multiple popup windows to the browser for user authentication when the following conditions are met:

  - The CE is configured to be the HTTP proxy.
  - The CE is configured for RADIUS authentication.
  - The **radius-server** exclude list configuration is enabled.
  - Your browser deploys local caching.
  - The requested cached web site contains objects that belong to different domains.

  When a page is retrieved from a local disk cache and the page contains objects belonging to different domains or servers, the browser opens multiple simultaneous connections to fetch the objects from their origin servers. The CE in turn sends a request to the browser for user authentication for each opened connection.

  For a given session, the CE now sends only one prompt for user authentication when the above listed conditions are met. See the "New radius-server Command Options" section on page 4 for the new **radius-server** command options implemented in Release 2.3.1 to resolve this caveat.

- CSCdt02110

  CPU utilization has been added as one of the CE unit's **load bypass** parameters. This means that if the CE CPU reaches 98 to 100 percent utilization and remains at this capacity for 5 minutes, the CE can bypass the traffic to offload it.

- CSCdt02952

  WCCP hot spot bucket shedding is too slow because the CE is using an incorrect parameter for its bypass function. The incorrect parameter causes 256 messages to be logged in the debug WCCP log each time the overloaded CE tries to shed a bucket. The result is that the buckets are not shed quickly enough during an overload condition, causing the CE to select to shed the same hot bucket multiple times before the next-hottest bucket is selected for shedding.

- CSCdt07163

  The CE CPU utilization goes to 100 percent when the transaction log export fails. The translog export fails when the CE attempts to use the File Transfer Protocol (FTP) to send a file to a file system that is full.

- CSCdt08172

  In certain cases during a refresh of cached contents, the browser reports a Java Script error, or some objects on the page do not load properly. The problem can occur when the following conditions are met:

  - Persistent connection is enabled on the CE.
  - The object is not available in the cache.
  - The Content-Length of the object is larger than 4096 bytes.
  - The client issues an If-Modified-Since (IMS) request.

  Release 2.3.1 addresses the timeout issues on both the client and the server that caused this problem.

- CSCdt12371

  When you use the Internet Explorer (IE) browser and the CE is configured for persistent connections, IE times out when accessing a URL. The problem will be seen if the origin server sends extra carriage return line feed (CRLF) characters of "\r\n" that is not accounted for in the Content-length of the response message. The CE now ignores those CRLF characters and continues parsing the rest of response. In the CE unit's response to the client, the CE sends the CRLF characters.

- CSCdt13005

  The CE sends extra junk bytes to the client. The problem occurs because the Websense Server sends a block message length to the CE, which the server uses in network byte order. The CE in its response to the WebSense server sends the extra junk bytes to the client.

Related Documentation

Use this document in conjunction with the following Cisco Cache Software and Cisco Content Engine documentation:

- *Cisco Content Engine 500 Series Hardware Installation Guide*
- *Cisco Cache Software Configuration Guide, Software Versions 2.2.x, 2.3.x*
- *Cisco Cache Software Command Reference, Release 2.3.0*
- *Release Notes for the Cisco Content Engine 500 Series*
- *Release Notes for the Cisco Cache Engine*
- *Regulatory Compliance and Safety Information for the Cisco Content Networking Product Series*

You can find this document and the above listed documents at the following sites:

- http://www.cisco.com/univercd/cc/td/doc/product/webscale/index.htm

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships 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 as 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, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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:

Attn Document Resource Connection
Cisco Systems, Inc.
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. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.