CISCO SYSTEMS

Text Part Number: 78-6227-02

Release Notes for Cisco Cache Engine, Version 2.0.3

December 1999

These release notes are for use with the *Cisco Cache Engine User Guide, Version 2.0.0* publication and contain information that was not available for inclusion in that manual. These release notes discuss the following topics:

- New and Changed Features, page 2
- Installation Changes, page 10
- Hardware Caveats, page 11
- Resolved Caveats, page 11
- Unresolved Caveats, page 12
- Related Documentation, page 13
- Cisco Connection Online, page 14
- CD-ROM Documentation, page 15

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

New and Changed Features

Port Range Values Expanded

The port range values for the CLI commands have been increased from Version 2.01. The new port range values are 1 to 65,535 inclusive.

Command-Line-Interface Changes and Additions

The following commands have port range values between 1 and 65,535:

- **http** global configuration command
- **icp** global configuration command
- **radius** global configuration command
- **wccp custom-web-cache** global configuration command

For a complete description of the these commands, refer to the "Command Reference" appendix in the *Cisco Cache Engine User Guide, Version 2.0.0* publication. This appendix is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/webcache/ce20/ver20/wc202cli.htm

URL Validation

The **http** global configuration command has been updated to include the **object url-validation** option. This command has a dependency with the **ip name-server** CLI command.

When the **ip name-server** is not configured (for example, during transparent proxy), **http object url-validation** should be dynamically turned off.

When **ip name-server** is configured, **http object url-validation** should be turned on automatically if and only if it was configured to be on.

Command-Line-Interface Changes and Additions

- The **url-validation** option has been added to the **http** global configuration:

  http object url-validation enable

- The show http command has been updated to include the **object** option:

  show http object

For a complete description of the updated **http** and **show http** commands, refer to the "Command Reference" appendix in the *Cisco Cache Engine User Guide, Version 2.0.0* publication. This appendix is available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/webcache/ce20/ver20/wc202cli.htm

Caution URL Validation is on by default. Cisco Systems strongly recommends that you keep URL Validation enabled, because disabling URL validation might make the Cache Engine vulnerable to corruption from the HTTP objects in the cache.

No-Proxy for Specified Domains

With this feature users can specify a list of IP addresses or domain names in the form mydomain.com, for which the Cache Engine will not use an upstream proxy and will contact the end server directly. This feature is supported in transparent and proxy mode.

The maximum number of no-proxy domains is 64. The Cache Engine will not use an upstream proxy for any domain that ends with a listed domain name. For example, if you specify cisco.com, the configured outgoing proxy server will be bypassed each time the cache engine tries to retrieve a web page from videos.cisco.com, or personals.cisco.com.

For IP addresses, enter the full IP address or use the asterisk “*” as a wild card for IP address fields. For example, when you enter 161.102.*.*, the Cache Engine will bypass the configured outbound proxy server and try to connect with web servers with IP addresses in the range 161.102.0.0 to 161.102.255.255.

Note In Version 2.0.3, the Cache Engine can only filter out one level of local domain, such as cisco.com, it cannot filter out proxy for sublocal domains, such as web1.cisco.com or web2.cisco.com.

Cache Engine Management Interface GUI Additions

On the Cache Engine Management Interface GUI, on the **Caching** menu, under the **HTTP Proxy** option, a **Do not use Outgoing HTTP Proxy for the following local domains** checkbox has been added. Click this box to bypass the outgoing proxy server for the domains entered in the adjacent list box. Each user-specified no-proxy IP address or domain name in the list box should be delimited by a carriage-return.

Command-Line-Interface Changes and Additions

The exclude list option has been added to the **http proxy outgoing** global configuration command. Use this command to specify domains for which the Cache Engine will not use an upstream proxy.

http proxy outgoing {exclude {enable | list {*domain-name* **|** *ip-address* **}} | host {***hostname* **|** *ip-address***}}**

Only one domain can be specified per command line. To specify multiple domains for proxy exclusion, execute the command for each domain. In the following example, cisco.com and the address 10.9.8.7 are proxy-excluded.

```
console(config)#http proxy outgoing exclude list cisco.com
console(config)#http proxy outgoing exclude list 10.9.8.7
```

For a complete description on the updated **http** command, refer to the section "Related Documentation" for CCO location for the updated Appendix A, "Command Reference" in the *Cisco Cache Engine User Guide, Version 2.0.0* publication.

Custom Web Cache

Custom web caching allows a user-configurable port of interception to efficiently perform transparent caching at branch offices where enterprises run HTTP traffic on ports other than port 80. In Version 2.0.3, custom web caching provides support for transparent interception of HTTP traffic on any configurable port (1 to 65,535). In Version 2.0.1, the transparent mode web caching is hard-coded to HTTP standard port number 80.

Figure 1 shows a network topology using transparent web caching.

Figure 1 Network Topology Using Transparent Web Caching

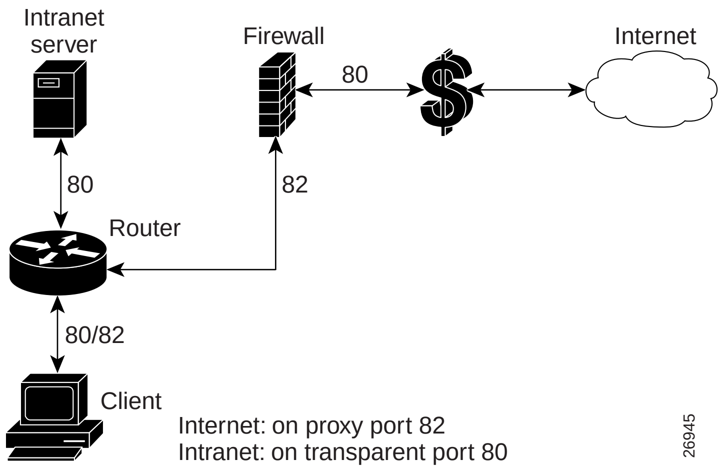
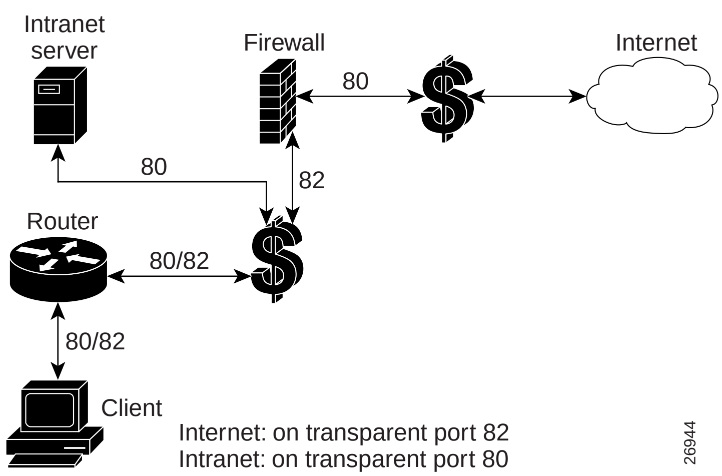


Figure 2 shows a network topology using the custom transparent cache server.

Figure 2 Network Topology Using Custom Transparent Cache Server



Cache Engine Management Interface GUI Additions

On the Cache Engine Management Interface GUI, the **Custom Web Cache** option has been added under the **WCCP** menu. Using this GUI option you can configure the Cache Engine to cache custom web traffic (custom configured outgoing port HTTP requests). This service requires you to use WCCP Version 2. Click **HELP** for information on configuring custom HTTP caching services.

Command-Line-Interface Changes and Additions

The global configuration command **wccp custom-web-cache** and **no wccp custom-web-cache** has been added. Using this command you can configure the Cache Engine to cache custom web traffic (custom configured outgoing port HTTP requests). To use this command, you must be using WCCP Version 2.

wccp custom-web-cache router-list-num *list-number* **port** *port-number* [**hash-destination-ip** | **hash-destination-port** | **hash-source-ip** | **password** *word* | *weight*]

Refer to the section “Related Documentation” for CCO location for the updated Appendix A, “Command Reference” in the *Cisco Cache Engine User Guide, Version 2.0.0* publication.

Transparent Error Reporting

In Version 2.0.1, error conditions are not handled transparently by the Cache Engine. When an error occurs, either during the processing of the request from the client or during the processing of the response from the server, the Cache Engine sends back an HTML page to the client which contains the error description. The end users see this Cache Engine generated page instead of the familiar browser pop-up error window or alert box compromising the claim of transparency.

With the transparent error reporting feature, the end users can continue to see browser-generated messages for errors that the Cache Engine encounters while processing the request or response.

In Version 2.0.3, transparent error reporting is implemented as follows:

- Cache Engine Running WCCP Version 2

  To make the error messages transparent to the user, the client/server pair is added to the bypass list and an HTTP redirect message is sent to the client requesting the client to redirect the request to the same URL as before. The client, on receiving the redirect message, sends back the request once again. This time the request gets bypassed by the cache because the client/server pair is on the bypass list. The request now goes to the server directly. Since the connection was not accepted by the cache, any time-out error or failure to connect to the server or mangled response from the server will be handled by the browser. Thus the error messages will be transparent. Currently all entries on the bypass list will be kept for a configurable period of time (for example, five minutes).

  When there is an internal failure in the cache while processing a request, a reset is sent back to the client and closes the connection. This is because memory is needed to add the client/server pair to the bypass list. When a browser receives a connection reset, it pops up a “Connection Reset By Peer” alert box.

- Cache Engine Running WCCP Version 1

  For all error conditions, the Cache Engine sends back a reset and closes the connection. It does not send back any error pages. All errors seen by the clients are in the familiar browser error format.

- Cache Engine Acting as an Incoming Proxy Server

  In this case, the Cache Engine sends back error pages as in Version 2.0.1. When clients are using the Cache Engine as an incoming proxy server, they will continue to see the HTML error pages generated by the clients.

Command-Line-Interface Changes and Additions

The global configuration command **error-handling** and **no error-handling** has been added. Using this command you can customize how the Cache Engine should handle errors. To use the **transparent** option, you must be using WCCP Version 2.

error-handling {**reset-connection** | **send-cache-error** | **transparent**}

Refer to the section "Related Documentation" for CCO location for the updated Appendix A, "Command Reference" in the *Cisco Cache Engine User Guide, Version 2.0.0* publication.

Flow Protection

In Version 2.0.1, WCCP currently redirects all packets for certain traffic to be intercepted (for example, HTTP) to the Cache Engines as they come online. The drawback is that existing TCP connections to the web server are broken. The same thing happens when WCCP goes down and then the TCP connections established by the Clients to the Cache Engine are broken. This problem is worse when there is a cluster of Cache Engines. As new Cache Engines are added and existing ones removed, the TCP connections end up being redirected to the wrong Cache Engine and the clients get a TCP RESET, which breaks the connection. In Version 2.0.2, the flow protection feature is designed to keep the TCP flow intact as well as not overwhelm the Cache Engines when they come up or are reassigned new traffic. This feature also has a slow start mechanism whereby the Cache Engines try to take load appropriate for their capacity.

Command-Line-Interface Changes and Additions

The global configuration command **wccp flow-redirect** and **no wccp flow-redirect** has been added. Using this command you can enable flow redirection. To use this command, you must be using WCCP Version 2.

wccp flow-redirect enable

Refer to the section "Related Documentation" for CCO location for the updated Appendix A, "Command Reference" in the *Cisco Cache Engine User Guide, Version 2.0.0* publication.

Bypass

The bypass feature has been enhanced as described in the following two subsections. There are two kinds of bypass (load based and authentication based).

In V2.0.1, the method of doing Load Bypass was to bypass all new connections for a short period of time (two to four seconds) and then start accepting the connections again. The new method in V2.0.3, is to bypass only a bucket at a time but for longer periods of time (ten minutes by default). If the load is still high, more buckets are bypassed until the load becomes such that the Cache Engine can handle it. Once the Cache Engine has bypassed enough buckets to be able to handle the load, it will start accepting bypassed buckets, one at a time and based on the bucket return configuration, until all buckets are serviced again.

Cache Engine Management Interface GUI Changes and Additions

The Cache Engine Management Interface GUI, **WCCP** menu, **BYPASS** Proxy option, has been moved to the **Caching** menu, under the **Bypass** option. You can now do the following:

- Enable Load Bypass. If a Cache becomes overwhelmed with traffic, it can use the Load Bypass feature to reroute overload traffic back out to the Internet.
- Set the time interval between bypassing buckets in seconds. Once the Cache Engine becomes overwhelmed with traffic, it will bypass one bucket at a time until it is no longer over-loaded. The amount of time between the bypassing of one bucket and the next is the time interval between bypassing buckets. The default is four seconds. The range is 4 to 600 seconds.

Note A bucket is defined as a certain subsection of the allotted hash assigned to each Cache Engine in a caching cluster. If only one cache exists in the environment, then it will have 256 buckets assigned to it.

- Set the time that a bucket is bypassed in minutes. Once a bucket (or numerous buckets) has been bypassed, and the Cache Engine is in bypass mode, it will not attempt to pick up the bypassed load for this set number of minutes. The default value is ten minutes. The range is 1 to 1440 minutes.
- Set the time interval between buckets coming back in seconds. Once the time interval allotted to bypass mode has been surpassed, the Cache Engine will begin to pick up bypassed traffic one bucket at a time. The time between the return, or pick-up, of each bucket is measured in seconds. The default is 60 seconds. The range is 4 to 600 seconds.
- Set the bypass entry expiration time in minutes. The number of minutes an idle client/server pair will remain on the bypass access list. The default value is ten minutes. The range is 1 to 1440 minutes.

Click **HELP** for information on configuring the bypass feature.

The Authentication Bypass feature is also located in this new GUI location. Some web sites, due to IP authentication, may not allow the Cache Engine to connect directly on behalf of the client. In order to avoid a disruption of service, the Cache can use Authentication Bypass to generate a dynamic access-list for these client/server pairs. Authentication Bypass triggers are also propagated upstream and downstream in the case of hierarchical caching. To enable Authentication Bypass on the Cache Engine, select the **On** radio button. To disable Authentication Bypass without losing your settings, select the **Off** radio button. The default value is **Off**.

The packets could be bypassed by Authentication Bypass even if load bypass is not enabled. Once a client/server pair goes into Authentication Bypass, it is bypassed for a configurable amount of time (ten minutes by default).

The Tunnel Bypass option is no longer available. This option was for debugging purposes to force all WCCP-redirected traffic to bypass the Cache Engine.

Command-Line-Interface Changes and Additions

- To configure the bypass feature using the CLI, use the **bypass** global configuration command. To disable the bypass feature, use the **no** form of this command.

  bypass {**auth-traffic enable | list timer** *minutes* **| load {enable | in-interval** *seconds* **|**
  out-interval *seconds* **| time-interval** *minutes*}

Note The bypass feature is only available when WCCP Version 2 is enabled. The Cache Engine can only bypass WCCP-redirected traffic, not proxy-style requests.

- To display Authentication Bypass and Load Bypass statistics, use the **show bypass** command.

  show bypass statistics {**auth-traffic** | **load**}

- The global configuration command **wccp tunnel-bypass**, **wccp auth-bypass**, and **wccp load-bypass** are no longer available.

Note The **auth-bypass** option is now called **auth-traffic** option. Bypass options are now configured through the **bypass** global command rather than the **wccp** global command.

For more information on these commands, refer to the section “Related Documentation” for CCO location for the updated Appendix A, “Command Reference” in the *Cisco Cache Engine User Guide, Version 2.0.0* publication.

TCP Stack Improvement

Implementation of enhancements to the TCP stack that improve network responsiveness, particularly in high-latency networks (for example, satellite). Satellite providers need these improvements to fully utilize their satellite links. They want to distribute content to many distributed caches.

Command-Line-Interface Changes and Additions

The global configuration command **tcp** has been updated to include TCP client and server maximum segment size (**client-mss** and **server-mss**) and TCP satellite (**client-satellite** and **server-satellite**) options. Using this command you can configure TCP parameters. To disable TCP parameters, use the **no** form of this command.

tcp {**client-mss** *size* | **client-receive-buffer** *kbytes* | **client-rw-timeout** *seconds* | **client-satellite** | **client-send-buffer** *kbytes* | **cwnd-base** *factor* | **init-ssthresh** *value* | **keepalive-probe-cnt** *count* | **keepalive-probe-interval** *seconds* | **keepalive-timeout** *seconds* | **listen-queue** *length* **server-receive-buffer** *kbytes* | **server-mss** *size* | **server-rw-timeout** *seconds* | **server-satellite** | **server-send-buffer** *kbytes*}

no tcp {**client-mss** *size* | **client-receive-buffer** *kbytes* | **client-rw-timeout** *seconds* | **client-satellite** | **client-send-buffer** *kbytes* | **cwnd-base** *factor* | **init-ssthresh** *value* | **keepalive-probe-cnt** *count* | **keepalive-probe-interval** *seconds* | **keepalive-timeout** *seconds* | **listen-queue** *length* **server-receive-buffer** *kbytes* | **server-mss** *size* | **server-rw-timeout** *seconds* | **server-satellite** | **server-send-buffer** *kbytes*}

The **show tcp** command TCP configuration output has been updated to show the new TCP setting options:

```
Console# show tcp
==TCP Configuration==
TCP keepalive timeout 300 sec
TCP keepalive probe count 4
TCP keepalive probe interval 75 sec
TCP client max segment size 1460
TCP server max segment size 1460
TCP client satellite (RFC1323) disable
TCP server satellite (RFC1323) disable
TCP server R/W timeout 120 sec
TCP client R/W timeout 120 sec
TCP server send buffer 8 k
TCP server receive buffer 32 k
TCP client send buffer 32 k
TCP client receive buffer 8 k
TCP Listen Queue 200
TCP init ssthresh 65536
TCP cwnd base 2
```

For more information on these commands, refer to the section “Related Documentation” for CCO location for the updated Appendix A, “Command Reference” in the *Cisco Cache Engine User Guide, Version 2.0.0* publication.

Customizing URL Blocked Message

Using this feature you can customize the blocked message that is sent back to a user when a request from the client matches a blocked URL. You can create your own HTML page called block.html and place it in the /local/etc/ directory. If you want to embed graphics into the HTML page, place the corresponding graphics gif/jpeg file in the /local/lib/gui/pub directory.

Following is an example of the block.html file:

```
<HTML>
<HEAD>
<TITLE>
URL Blocked
</TITLE>
</HEAD>
<BODY>
The site you are trying to view is blocked. Please contact your system administrator if
you need to unblock this site <IMG_SRC = /local/lib/gui/pub/stop.gif width=492
height=94 border=0>
</BODY>
</HTML>
```

Once you have created your customized block.html page, you can turn on this feature from the CLI or GUI.

Cache Engine Management Interface GUI Changes and Additions

On the Cache Engine Management Interface GUI, **CACHING** menu, **URL Filtering** option, a **Display customized URL blocking message (/local/etc/block.html)** checkbox has been added. Check this box to turn on or off the customized URL block message.

Command-Line-Interface Changes and Additions

The global configuration command **url-filter** has been updated to support this feature. Using this command you can enable URL blocking.

To turn on the customized URL blocking message, enter:

url-filter bad-sites-allow [custom-message]

url-filter good-sites-allow [custom-message]

To turn off the customized URL blocking message, enter:

url-filter bad-sites-allow

url-filter good-sites-allow

To disable URL blocking, use the **no** form of this command.

Refer to the section “Related Documentation” for CCO location for the updated Appendix A, “Command Reference” in the *Cisco Cache Engine User Guide, Version 2.0.0* publication.

Installation Changes

Refer to the section “Related Documentation” for CCO location for the updated Chapter 2, “Installing the Cache Engine” in the *Cisco Cache Engine User Guide, Version 2.0.0* publication. The following changes are described in the updated chapter:

Section “Enabling Cache Support on the Router” starting on page 2-10.

- Ensure that the router is running a release of the Cisco IOS software that includes WCCP. You must upgrade the Cisco IOS software if it does not have this support before you can continue.

  IOS versions before 12.0(3)T support only WCCP Version 1. IOS versions between 12.0(3)T and 12.0(5)T support only WCCP Version 2. IOS version 12.0(5)T or later support both WCCP Version 1 and Version 2. In IOS version 12.0(5)T or later, the default WCCP version is Version 2. You can override the WCCP default, by using the global configuration command **ip wccp version 1**.

  If you have WCCP Version 1 configured and attempt to configure any WCCP Version 2 specific features, you will receive a configuration error.

- To enable cache support on the router for WCCP Version 1, enter:

  `ip wccp enable`

  To have the interface redirect packets for port 80 to the Cache Engine, enter the following command for each interface:

  `ip web-cache redirect`

- To enable cache support on the router for WCCP Version 2, enter:

  ip wccp {**web-cache |** *services*}

  `where` *services* `is the number of predefined services (0 to 99)`

  To have the interface redirect packets for port 80 to the Cache Engine, enter the following command for each interface:

  ip wccp {**web-cache |** *services*} **redirect out**

Hardware Caveats

- The SCSI-LVD only port, located on the front of the Cache Engine, is reserved for future use and is not supported in the current versions of the Cache Engine.
- The Ethernet 1 port, located on the front of the Cache Engine, is reserved for future use and is not supported on current versions of the Cache Engine.

Resolved Caveats

- Cache Engine crashes due to possible disk failure. [CSCdm94083]
- The custom-web-cache option which formerly supported ports 1 to 1,600 has been expanded to support ports 1 to 65,535.[CSCdp04443]
- URL blocking not according to intent. The Bad URL list does simple pattern matching that contradicts the intent of blocking. It needs to be able to block the domain part of an URL, but not the file part or subset of an URL. [CSCdp01923]
- The custom-web-cache option does not allow for full flexibility. [CSCdp04440]
- IP routes fail to save running configuration with 200+ routes to NVRAM. [CSCdp00278]
- Cannot remove IP route 0.0.0.0 0.0.0.0. [CSCdp04758]
- Error msg: (tNetTask): arptnew failed on a010121. [CSCdm64310]
- Host line in header causes stale served pages. [CSCdp06214]

Unresolved Caveats

- The Cache Engine allows idle persistent connections to outlive the specified max-idle parameter set in the CLI or the GUI. [CSCdm39593]
- When using the global configuration command **logging**, make sure to complete the command string before pressing Enter. The parser will interpret an incomplete command string as the hostname keyword, blocking access to the command line interface until the search for the “host” times out. For example, the command **logging console alerts** executes correctly, while **logging console** starts a search for the IP host named “console” [CSCdm67986].

```
console#config
Enter configuration commands, one per line. End with CNTL/Z

console(config)#logging console alerts
console(config)#
console(config)#logging console
Translating "console" using configured ip name-server(s)...Failed

% Incomplete command.
console(config)#
```

- The following HTTP statistics counters displayed by the **show statistics http err** command do not increment correctly [CSCdm54304]:
  - — HTTP Parse Request Error
  - — HTTP TimeOut Error
  - — HTTP Connection Refused Error
- The following HTTP statistics counters displayed by the **show statistics http ims** command do not increment correctly [CSCdm54322]:
  - — Revalidated
  - — Cache to server
  - — IMS Issued
  - — Due to Client IMS
  - — Due to Expiration
- The following HTTP statistics counters displayed by the **show statistics http requests** command do not increment correctly [CSCdm64206]:
  - — Forced Reloads
  - — Server Errors
- When error-handling is set to **error-handling send-cache-error**, the Cache Engine generates an erroneous error message upon receipt of a non-HTTP request.[CSCdm69975]

Related Documentation

- The *Cisco Cache Engine User Guide, Version 2.0.0* publication that ships with the Cache Engine is available on Cisco Connection Online (CCO) at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/webcache/ce20/ver20/index.htm

- The updated Chapter 2 “Installing the Cache Engine” in the *Cisco Cache Engine User Guide, Version 2.0.0* publication is available on Cisco Connection Online (CCO) at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/webcache/ce20/ver20/wc202ins.htm

- The updated Appendix A “Command Reference” in the *Cisco Cache Engine User Guide, Version 2.0.0* publication is available on Cisco Connection Online (CCO) at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/webcache/ce20/ver20/wc202cli.htm

- The updated Appendix C “Web Cache Communication Protocol Version 2” of the *Cisco Cache Engine User Guide, Version 2.0.0* publication is available on Cisco Connection Online (CCO) at the following URL:

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/webcache/ce20/ver20/wc20wcc2.htm

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

Note Always check the following URLs for the latest software updates and documentation updates to ensure that you have the latest version of software and related documentation.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

CD-ROM Documentation

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

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

This document is to be used in conjunction with the *Cisco Cache Engine User Guide, Version 2.0.0* publication.