



# Release Notes for Cisco Cache Engine 500 Series, Software Version 2.1.0

---

**April 7, 2000**

These release notes provide the current open caveats for the Cisco Cache Engine 500 series software version 2.1.0.



---

The most current Cisco Documentation is on Cisco Connection Online 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:

- Introduction, page 1
- System Requirements, page 2
- New Features in Software Release 2.1.0, page 2
- Important Notes, page 7
- Open Caveats, page 7
- Obtaining Documentation, page 8
- Obtaining Technical Assistance, page 9

## Introduction

The Cisco Systems next-generation Cache Engine 500 series solutions enable service providers and enterprises to accelerate web content delivery, optimize WAN bandwidth utilization, and control access to content. The Cisco network caching solution is architected and optimized to work as a single caching system by pairing the following:



- Content-aware internetworking equipment, running Cisco IOS software with WCCP Version 2
- Network-integrated Cache Engine 500 series products that are managed and designed like networking products and can be transparently inserted into the network

## System Requirements

### Hardware Supported

As of the printing of this release note, Cache Engine software version 2.1.0 can operate with the following models of the Cache Engine:

- Cisco Cache Engine 505—Entry-level Cache Engine for small enterprise branch offices with T1/E1 uplinks
- Cisco Cache Engine 550—Mid-range Cache Engine for regional offices with WAN uplink bandwidth up to 11 Mbps
- Cisco Cache Engine 570—Mid-range Cache Engine for small service provider points of presence and medium-sized enterprises with WAN uplink bandwidth up to 22 Mbps

### Determining the Software Version

**Note**

---

Cisco recommends that you install the most recent software version available for your model of the Cache Engine.

---

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

### Downloading Cache Engine Software

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

<http://www.cisco.com/cgi-bin/tablebuild.pl/cache-engine>

## New Features in Software Release 2.1.0

Software Release 2.1.0 introduces the following new features:

### Cisco Cache Engine 570 Hardware Support

The Cisco Cache Engine 570 is designed to handle up to 400 TPS at a transmission speed of 22 Mb/s.

## Cacheable Object Size Configuration

Cache Engine Software Release 2.1.0 permits the administrator to define the maximum size of objects to cache. Objects above the specified size are not cached.

### Command-Line-Interface Changes and Additions

The **object** parameter has been added to the **http** global configuration command.

The **object** parameter has been added to the **show http** EXEC command.

The **object** parameter has been added to the **show statistics http** EXEC command.

### Cache Engine Management Interface GUI Changes and Additions

On the Cache Engine Management Interface GUI, the **Maximum size a cacheable object** option has been added to the **HTTP Freshness** page in the **CACHING** menu. With this feature the user can either specify the size limit of cacheable object or specify no limit.

## Denial-of-Service Attack Resistance

Denial-of-Service (DoS) attacks can disable a host or a network by consuming critical resources, altering configuration information, or by destruction of physical network components. The Cache Engine protects against the well-known DoS attacks listed in Table 1.

*Table 1 Cache Engine DoS Defense*

Type of DoS Attack Prevented	Description of Attack
Bonk	Uses IP and bad packet construction
Fraggle	Uses UDP and spoofed IP address (variant of Smurf)
LAND	Uses TCP and spoofed IP addresses
Ping-of-Death	Uses ICMP and huge IP packet size
Ping-Pong	Uses UDP and spoofed IP address
Smurf	Uses ICMP and spoofed IP address
SYN Flooding	Uses TCP and excessive connection requests
Tear-Drop	Uses IP and bad packet construction

### Command-Line-Interface Changes and Additions

New statistics were added to the **show statistics tcp** as follows:

```

console#show statistics tcp
...
0 half open connections dropped
  0 dropped due to rexmit thresh exceeded
  0 dropped due to bad foreign address
  5 good address hash count
  0 good address hash collisions
  0 good address hash deletions
...

```

DoS Related TCP Statistic	Explanation
dropped due to rexmit thresh exceeded	Half-open connections dropped from a full queue due to exceeded retransmission threshold.
dropped due to bad foreign address	Half-open connections dropped from a full queue due to foreign address not in good address table.
good address hash count	Entries in good address table currently in use.
good address hash collisions	Number of times an entry collision occurred during insertion into good address table.
good address hash deletions	Number of times an entry was explicitly removed from the good address table.

## Exporting Transaction Logs to External FTP Server

A Cache Engine can now export transaction logs to external servers, or multiple Cache Engines can export their transaction log files to the same server. Up to four external FTP servers can be configured. Transaction log files are transferred by FTP.

### Command-Line-Interface Changes and Additions

The universal configuration command **transaction-logs** has been changed. The **show transaction-logging** command has been updated to display information on exported log files. The **export** option has been added to the **show statistics transaction-log** command to display the status of logging attempts to export servers.

### Cache Engine Management Interface GUI Changes and Additions

In the **CACHING** menu on the **Transaction Logs** page, up to four FTP servers can be configured to accept transaction log files. To disable the export of transaction logs while saving the current configuration, click the **Off** Radio button in the **Transaction Log FTP Export** field.

## QoS Interoperability

Cache Engine software version 2.1.0 can now transparently pass Type of Service (ToS) information between a client and a remote server. The incoming ToS of packets received from the client request to the Cache Engine is used as the outgoing ToS in packets sent to the server. There are no command line or graphic user interface changes for this feature.

## Sanitized Transaction Log Files

A sanitized transaction log disguises the network identity of a client by changing the IP address and username (if applicable) in the transaction logs. The IP address is changed to 0.0.0.0.

#### Command-Line-Interface Changes and Additions

The **sanitized** parameter has been added to the **transaction-logs** global configuration command.

#### Cache Engine Management Interface GUI Changes and Additions

In the **Transaction Logs** page in the **CACHING** menu, a radio button is provided to enable and disable the **Sanitize transaction logs** feature.

## Selective Abort of Cacheable Objects

Client abort processing occurs when a client of the Cache Engine aborts the download of a cacheable object before the download is complete. Typically a client aborts a download by clicking the Stop icon on the browser, or by closing the browser during a download. Release 2.1.0 provides user-defined thresholds to determine whether or not the Cache Engine will complete the download. When the download of an object aborts before being completed, the object is not stored on the Cache Engine or counted in the hit-rate statistics.

#### Command-Line-Interface Changes and Additions

The **cache-on-abort** option has been added to the **http** global configuration command.

The **cache-on-abort** option was added to the **show http** global configuration command.

#### Cache Engine Management Interface GUI Changes and Additions

The **Cache on Abort** page has been added to the of the **CACHING** menu of the management GUI.

## Selective RADIUS Authentication

With this feature users can specify an exclusion list of IP addresses or domain names (in the form mydomain.com), for which the Cache Engine will not perform RADIUS authentication. The maximum number of excluded domains is 64. The Selective Radius Authentication feature can be disabled without deleting the domains.

The Cache Engine currently supports Remote Authentication Dial-In User Service (RADIUS) authentication. RADIUS clients run on Cisco Cache Engines. When enabled, these clients send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. Selective RADIUS authentication allows users to access intranet servers without requiring authentication, and can limit RADIUS authentication to those users that access external web servers.

#### Command-Line-Interface Changes and Additions

The **radius** universal configuration command has been changed.

The **show radius** command has been updated to display the list of local domains excluded from RADIUS authentication.

#### Cache Engine Management Interface GUI Changes and Additions

On the Cache Engine Management Interface GUI, on the **CACHING** menu, under the **RADIUS** option, a **Do not perform RADIUS Authentication for the following domains** checkbox has been added. Click this box to exclude the domains entered in the adjacent list box from RADIUS authentication. Each IP address or domain name in the list box should be delimited by a carriage-return.

## Static Bypass Lists

This feature permits traffic from specified sources to bypass the Cache Engine. The type of traffic sources are as follows:

- specific web client to a specific web server
- specific web client to any web server
- any web client to a specific web server

Wildcarding of either the source or destination field is not supported.

A statically configurable list of source and destination addresses helps to isolate instances of misbehaving clients and servers.

### Command-Line-Interface Changes and Additions

The global configuration command **bypass static** has been added.

To display static configuration list items, use the **show bypass list** command.

The total number of entries in the bypass list is now reported in the **show bypass summary** command.

To clear all Static Configuration lists and counters, use the **clear bypass** command.

### Cache Engine Management Interface GUI Changes and Additions

The static bypass configuration list feature is not implemented in software version 2.1.0.

## URL Filtering with the Websense Server

Software version 2.1.0 enables a Cache Engine to use either a UNIX or Windows NT Websense server as a filtering engine. The Cache Engine can then enforce the filtering policy configured on the Websense server. Refer to the Websense documentation for further information on Websense filtering policies.

### Command-Line-Interface Changes and Additions

The **websense** option has been added to the **url-filter** global configuration command.

### Cache Engine Management Interface GUI Changes and Additions

Websense configuration options have been added to the **URL Filtering** page of the **CACHING** menu.

## WCCP Clean Shutdown

To prevent broken TCP connection, software version 2.1.0 implements a clean shutdown of WCCP. After a **reload** or **wccp version** command the Cache Engine continues servicing the flows it is handling and starts to bypass new flows. When the number of existing flows go down to zero, the Cache Engine takes itself out of the cluster by informing the lead Cache Engine to redistribute the buckets it was handling. This prevents broken connections as the Cache Engine shuts down. The connections will still be broken if the Cache Engine crashes or is rebooted without WCCP being cleanly shutdown. The clean shutdown can be aborted while in progress.

### Command-Line-Interface Changes and Additions

The **wccp cleanshutdown** global configuration command has been added.

### Cache Engine Management Interface GUI Changes and Additions

The **Enable WCCP** page of the **WCCP** menu provides clean shutdown options.

## WCCP Slow Start

Within a cluster of Cache Engines TCP connections are redirected to other Cache Engine as units are added or removed. A Cache Engine can be overloaded if too quickly reassigned new traffic or introduced abruptly into a fat pipe. The WCCP slow start performs the following tasks to prevent a Cache Engine from being overwhelmed when it comes online or is reassigned new traffic:

- TCP flow protection when WCCP 2 is enabled and a Cache Engine is introduced into the cluster.
- TCP flow protection when WCCP 2 is disabled and a Cache Engine is leaving the cluster.
- Load is given to the Cache Engine in slow increments rather than the full load at bringup time.

Slow start is applicable only in the following cases:

- Initial bring up when there is no Cache Engine yet present in the server farm.
- New Cache Engine is added to a cluster that is not handling the full load. For example, when there are some buckets that are being shed by the cluster.

In all other cases Slow Start is not necessary and all the Cache Engines could be assigned their share of the buckets right away.

### Command-Line-Interface Changes and Additions

Enable slow start with the **wccp slow-start** global configuration command.

### Cache Engine Management Interface GUI Changes and Additions

There is no GUI configurable option for the WCCP slow start feature in release 2.1.0.

## Important Notes

### Erroneous CPU Fan Failure Message

The Cache Engine 570 may log an erroneous CPU fan failure message in the syslog file. For example,

```
Tue Apr 11 15:17:27 2000 ... web-cache-2.ce.ca 73:CPU Fan Failed!
```

If the Cache Engine is functioning, ignore the message. It does not indicate a danger to the continued, safe operation of the Cache Engine.

## Open Caveats

The following are open caveats for software version 2.1.0:

- CSCdr24301, Erroneous HTTP Statistics Reporting  
The **show statistics http performance** command might display erroneous statistics.
- CSCdr13225 No WCCP Hash Allotment to some Cache Engines in Farm

Cisco Systems has observed that in topologies with 20 or more routers configured to service multiple Cache Engines, some of the Cache Engines do not receive hash allotments, and thus receive no redirected traffic from the routers. The routers can be configured either in unicast or multicast mode.

**Workaround:** To correct this condition, reboot each Cache Engine or stop and start WCCP on each Cache Engine using the Cache Engine global configuration command **wccp**.

For example, to reset WCCP on a Cache Engine in the farm configured only with basic web caching, issue the following commands:

```
console(config)# no wccp web-cache
console(config)# wccp web-cache router 1
```



---

**Note** Wait 30 seconds between stopping and starting WCCP. The **wccp** keywords and options apply to the example Cache Engine only. Use the keywords and options appropriate to the configuration of each Cache Engine.

---

Display the hash allotments for Cache Engines by using the **show ip wccp web-cache detail** router command.

## Obtaining Documentation

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <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. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

### Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at <http://www.cisco.com/cgi-bin/subcat/kaojump.cgi>.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).



# Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

## Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online 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.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, 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 CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: [www.cisco.com](http://www.cisco.com)
- Telnet: [cco.cisco.com](http://cco.cisco.com)
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to [cco-team@cisco.com](mailto:cco-team@cisco.com).

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use [www.cisco.com/techsupport](http://www.cisco.com/techsupport).

To contact by e-mail, use one of the following:

Language	E-mail Address
English	<a href="mailto:tac@cisco.com">tac@cisco.com</a>
Hanzi (Chinese)	<a href="mailto:chinese-tac@cisco.com">chinese-tac@cisco.com</a>
Kanji (Japanese)	<a href="mailto:japan-tac@cisco.com">japan-tac@cisco.com</a>

Language	E-mail Address
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site:  
<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>.

---

This document is to be used in conjunction with the documents listed in the “Obtaining Documentation” section.

Access Registrar, AccessPath, Any to Any, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, RateMUX, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, SVX, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Voice Line, VisionWay, VlanDirector, Voice LAN, Wavelength Router, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (0003R)

Copyright © 2000, Cisco Systems, Inc.  
All rights reserved.

