IP Application Services Configuration Guide, Cisco IOS XE Release 3SG

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice.

In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.
CONTENTS

WCCP Version 2 1
Finding Feature Information 1
Prerequisites for WCCP Version 2 1
Restrictions for WCCP Version 2 2
Information About WCCP Version 2 3
   WCCPv2 Overview 3
   WCCPv2 Configuration 5
   WCCPv2 Support for Services Other Than HTTP 6
   WCCPv2 Support for Multiple Routers 6
   WCCPv2 MD5 Security 6
   WCCPv2 Web Cache Packet Return 6
   WCCPv2 Load Distribution 7
   WCCP Troubleshooting Tips 7
How to Configure WCCP Version 2 7
   Configuring WCCP 7
   Verifying and Monitoring WCCP Configuration Settings 10
Configuration Examples for WCCP Version 2 11
   Example: Changing the Version of WCCP on a Router 11
   Example: Configuring a General WCCPv2 Session 11
Additional References 11
Feature Information for WCCP Version 2 12

WCCP—Configurable Router ID 15
Finding Feature Information 15
Information About WCCP—Configurable Router ID 15
   WCCP—Configurable Router ID Overview 15
How to Configure WCCP—Configurable Router ID 16
   Configuring a Preferred WCCP Router ID 16
Configuration Examples for WCCP—Configurable Router ID 17
   Example: Configuring a Preferred WCCP Router ID 17
WCCP Version 2

The Web Cache Communication Protocol (WCCP) is a Cisco-developed content-routing technology that intercepts IP packets and redirects those packets to a destination other than that specified in the IP packet. Typically the packets are redirected from their destination web server on the Internet to a content engine that is local to the client. In some WCCP deployment scenarios, redirection of traffic may also be required from the web server to the client. WCCP enables you to integrate content engines into your network infrastructure.

Cisco IOS Release 12.1 and later releases allow the use of either WCCP Version 1 (WCCPv1) or Version 2 (WCCPv2).

The tasks in this document assume that you have already configured content engines on your network. For specific information on hardware and network planning associated with Cisco Content Engines and WCCP, see the Cisco Content Engines documentation at the following URL:

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

- Finding Feature Information, page 1
- Prerequisites for WCCP Version 2, page 1
- Restrictions for WCCP Version 2, page 2
- Information About WCCP Version 2, page 3
- How to Configure WCCP Version 2, page 7
- Configuration Examples for WCCP Version 2, page 11
- Additional References, page 11
- Feature Information for WCCP Version 2, page 12

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for WCCP Version 2

- IP must be configured on the interface connected to the Internet and another interface must be connected to the content engine.
The interface connected to the content engine must be a Fast Ethernet or Gigabit Ethernet interface.

Only Catalyst 6500 series switches with a PFC4 support the following hardware capabilities:

- WCCP generic routing encapsulation (GRE) decapsulation in hardware
- WCCP egress mask assignment in hardware
- WCCP exclude capability in hardware

Restrictions for WCCP Version 2

General

The following limitations apply to WCCPv2:

- WCCP works only with IPv4 networks.
- WCCP bypasses Network Address Translation (NAT) when Cisco Express Forwarding is enabled.

WCCPv2

- WCCP works only with IPv4 networks.
- For routers servicing a multicast cluster, the Time To Live (TTL) value must be set at 15 or fewer.
- Service groups can comprise up to 32 content engines and 32 routers.
- All content engines in a cluster must be configured to communicate with all routers servicing the cluster.
- Multicast addresses must be from 224.0.0.0 to 239.255.255.255.

Cisco Catalyst 4500 Series Switches

- Up to eight service groups are supported at the same time on the same client interface.
- The Layer 2 (L2) rewrite forwarding method is supported, but generic routing encapsulation (GRE) is not.
- Direct L2 connectivity to content engines is required; Layer 3 (L3) connectivity of one or more hops away is not supported.
- Ternary content addressable memory (TCAM)-friendly mask-based assignment is supported, but the hash bucket-based method is not.
- Redirect access control list (ACL) for WCCP on a client interface is not supported.
- Incoming traffic redirection on an interface is supported, but outgoing traffic redirection is not.
- When TCAM space is exhausted, traffic is not redirected; it is forwarded normally.
- The WCCP version 2 standard allows for support of up to 256 distinct masks. However, a Catalyst 4500 series switch supports only mask assignment tables with a single mask.

Cisco Catalyst 6500 Series Switches

The following limitation apply to Cisco Catalyst 6500 series switches:

- With a Policy Feature Card 2 (PFC2), Cisco IOS Release 12.2(17d)SXB and later releases support WCCP.
- With a PFC3, Cisco IOS Release 12.2(18)SXD1 and later releases support WCCP.
- With a PFC4, Cisco IOS Release 12.2(50)SY and later releases support WCCP and introduce support for WCCP GRE decapsulation, WCCP mask assignment, and WCCP exclude capability in hardware.
To use the WCCP Layer 2 PFC redirection feature, configure WCCP on the Catalyst 6500 series switch and configure accelerated WCCP on the cache engine as described in the Transparent Caching document.

Cisco Application and Content Networking System (ACNS) software releases later than Release 4.2.2 support WCCP Layer 2 Policy Feature Card (PFC) redirection hardware acceleration.

A content engine configured for mask assignment that tries to join a farm where the selected assignment method is hash remains out of the farm as long as the cache engine assignment method does not match that of the existing farm.

When WCCP Layer 2 PFC redirection is the forwarding method for a service group, the packet counters in the `show ip wccp service-number` command output display flow counts instead of packet counts.

**Catalyst 6500 Series Switches and Cisco 7600 Series Routers Access Control Lists**

When WCCP is using mask assignment, any redirect list is merged with the mask information from the appliance and the resulting merged ACL is passed down to the Catalyst 6500 series switch or Cisco 7600 series router hardware. Only Permit or Deny ACL entries from the redirect list in which the protocol is IP or exactly matches the service group protocol are merged with the mask information from the appliance.

The following restrictions apply to the redirect-list ACL:

- The ACL must be an IPv4 simple or extended ACL.
- Only individual source or destination port numbers may be specified; port ranges cannot be specified.
- The only valid matching criteria in addition to individual source or destination port numbers are `dscp` or `tos`.
- The use of `fragments`, `time-range`, or `options` keywords, or any TCP flags is not permitted.

If the redirect ACL does not meet the restrictions shown, the system will log the following error message:

```
WCCP-3-BADACE: Service <service group>, invalid access-list entry (seq:<sequence>, reason:<reason>)
```

WCCP continues to redirect packets, but the redirection is carried out in software (NetFlow Switching) until the access list is adjusted.

**Information About WCCP Version 2**

- WCCPv2 Overview, page 3
- WCCPv2 Configuration, page 5
- WCCPv2 Support for Services Other Than HTTP, page 6
- WCCPv2 Support for Multiple Routers, page 6
- WCCPv2 MD5 Security, page 6
- WCCPv2 Web Cache Packet Return, page 6
- WCCPv2 Load Distribution, page 7
- WCCP Troubleshooting Tips, page 7

**WCCPv2 Overview**

WCCP uses Cisco Content Engines (or other content engines running WCCP) to localize web traffic patterns in the network, enabling content requests to be fulfilled locally. Traffic localization reduces transmission costs and download time.
WCCP enables Cisco IOS XE routing platforms to transparently redirect content requests. The main benefit of transparent redirection is that users need not configure their browsers to use a web proxy. Instead, they can use the target URL to request content, and have their requests automatically redirected to a content engine. The word "transparent" in this case means that the end user does not know that a requested file (such as a web page) came from the content engine instead of from the originally specified server.

A content engine receiving a request attempts to service it from its own local cache. If the requested information is not present, the content engine issues its own request to the originally targeted server to get the required information. A content engine retrieving the requested information forwards it to the requesting client and caches it to fulfill future requests, thus maximizing download performance and substantially reducing transmission costs.

WCCP enables a series of content engines, called a content engine cluster, to provide content to a router or multiple routers. Network administrators can easily scale their content engines to manage heavy traffic loads through these clustering capabilities. Cisco clustering technology enables each cluster member to work in parallel, resulting in linear scalability. Clustering content engines greatly improves the scalability, redundancy, and availability of your caching solution. You can cluster up to 32 content engines to scale to your desired capacity.

The WCCP Version 2 feature provides several enhancements and features to the WCCP protocol, including:

- The ability of multiple routers to service a content engine cluster.
- Redirection of traffic other than HTTP (TCP port 80 traffic), including a variety of UDP and TCP traffic.
- Optional authentication that enables you to control which routers and content engines become part of the service group using passwords and the HMAC MD5 standard.
- A check on packets that determines which requests have been returned from the content engine unserviced.
- Load adjustments for individual content engines to provide an effective use of the available resources while helping to ensure high quality of service (QoS) to the clients.
WCCPv2 Configuration

Multiple routers can use WCCPv2 to service a content engine cluster. In WCCPv1, only one router could redirect content requests to a cluster. The figure below illustrates a sample configuration using multiple routers.

The subset of content engines within a cluster and routers connected to the cluster that are running the same service is known as a service group. Available services include TCP and UDP redirection.

In WCCPv1, the content engines were configured with the address of the single router. WCCPv2 requires that each content engine be aware of all the routers in the service group. To specify the addresses of all the routers in a service group, you must choose one of the following methods:

- **Unicast**—A list of router addresses for each of the routers in the group is configured on each content engine. In this case the address of each router in the group must be explicitly specified for each content engine during configuration.
- **Multicast**—A single multicast address is configured on each content engine. In the multicast address method, the content engine sends a single-address notification that provides coverage for all routers in the service group. For example, a content engine could indicate that packets should be sent to a multicast address of 224.0.0.100, which would send a multicast packet to all routers in the service group configured for group listening using WCCP (see the `ip wccp group-listen` or the `ipv6 wccp group-listen` interface configuration command for details).

The multicast option is easier to configure because you need only specify a single address on each content engine. This option also allows you to add and remove routers from a service group dynamically, without needing to reconfigure the content engines with a different list of addresses each time.

The following sequence of events details how WCCPv2 configuration works:

1. Each content engine is configured with a list of routers.
2 Each content engine announces its presence and a list of all routers with which it has established communications. The routers reply with their view (list) of content engines in the group.
3 When the view is consistent across all content engines in the cluster, one content engine is designated as the lead and sets the policy that the routers need to deploy in redirecting packets.

**WCCPv2 Support for Services Other Than HTTP**

WCCPv2 allows redirection of traffic other than HTTP (TCP port 80 traffic), including a variety of UDP and TCP traffic. WCCPv1 supported the redirection of HTTP (TCP port 80) traffic only. WCCPv2 supports the redirection of packets intended for other ports, including those used for proxy-web cache handling, File Transfer Protocol (FTP) caching, FTP proxy handling, web caching for ports other than 80, and Real Audio, video, and telephony applications.

To accommodate the various types of services available, WCCPv2 introduced the concept of multiple service groups. Service information is specified in the WCCP configuration commands using dynamic services identification numbers (such as 98) or a predefined service keyword (such as `web-cache`). This information is used to validate that service group members are all using or providing the same service.

The content engines in a service group specify traffic to be redirected by protocol (TCP or UDP) and up to eight source or destination ports. Each service group has a priority status assigned to it. The priority of a dynamic service is assigned by the content engine. The priority value is in the range of 0 to 255 where 0 is the lowest priority. The predefined web-cache service has an assigned priority of 240.

**WCCPv2 Support for Multiple Routers**

WCCPv2 allows multiple routers to be attached to a cluster of cache engines. The use of multiple routers in a service group allows for redundancy, interface aggregation, and distribution of the redirection load. WCCPv2 supports up to 32 routers per service group. Each service group is established and maintained independently.

**WCCPv2 MD5 Security**

WCCPv2 provides optional authentication that enables you to control which routers and content engines become part of the service group using passwords and the Hashed Message Authentication Code—Message Digest (HMAC MD5) standard. Shared-secret MD5 one-time authentication (set using the `ip wccp [password 0 | 7] password` global configuration command) enables messages to be protected against interception, inspection, and replay.

**WCCPv2 Web Cache Packet Return**

If a content engine is unable to provide a requested object it has cached due to error or overload, the content engine will return the request to the router for onward transmission to the originally specified destination server. WCCPv2 provides a check on packets that determines which requests have been returned from the content engine unserviced. Using this information, the router can then forward the request to the originally targeted server (rather than attempting to resend the request to the content engine cluster). This process provides error handling transparency to clients.

Typical reasons why a content engine would reject packets and initiate the packet return feature include the following:

- Instances when the content engine is overloaded and has no room to service the packets
- Instances when the content engine is filtering for certain conditions that make caching packets counterproductive (for example, when IP authentication has been turned on)
WCCPv2 Load Distribution

WCCPv2 can be used to adjust the load being offered to individual content engines to provide an effective use of the available resources while helping to ensure high quality of service (QoS) to the clients. WCCPv2 allows the designated content engine to adjust the load on a particular content engine and balance the load across the content engines in a cluster. WCCPv2 uses three techniques to perform load distribution:

- **Hot spot handling**—Allows an individual hash bucket to be distributed across all the content engines. Prior to WCCPv2, information from one hash bucket could go to only one content engine.
- **Load balancing**—Allows the set of hash buckets assigned to a content engine to be adjusted so that the load can be shifted from an overwhelmed content engine to other members that have available capacity.
- **Load shedding**—Enables the router to selectively redirect the load to avoid exceeding the capacity of a content engine.

The use of these hashing parameters prevents one content engine from being overloaded and reduces the potential for bottlenecks.

WCCP Troubleshooting Tips

CPU usage may be very high when WCCP is enabled. The WCCP counters enable a determination of the bypass traffic directly on the router and can indicate whether the cause is high CPU usage due to enablement of WCCP. In some situations, 10 percent bypass traffic may be normal; in other situations, 10 percent may be high. However, any figure above 25 percent should prompt a closer investigation of what is occurring in the web cache.

If the counters suggest that the level of bypass traffic is high, the next step is to examine the bypass counters in the content engine and determine why the content engine is choosing to bypass the traffic. You can log in to the content engine console and use the CLI to investigate further. The counters allow you to determine the percent of traffic being bypassed.

You can use the `clear ipv6 wccp` command to remove the IPv6 Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the router for a particular service.

You can use the `clear wccp` command to remove all (IPv4 and IPv6) Web Cache Communication Protocol (WCCP) statistics (counts) maintained on the router for a particular service.

You can use the `show ipv6 wccp` command to display the IPv6 Web Cache Communication Protocol (WCCP) global statistics (counts).

You can use the `show wccp` command to display all (IPv4 and IPv6) Web Cache Communication Protocol (WCCP) global statistics (counts).

How to Configure WCCP Version 2

- Configuring WCCP, page 7
- Verifying and Monitoring WCCP Configuration Settings, page 10

Configuring WCCP

Perform this task to configure WCCP.
Until you configure a WCCP service using the `ip wccp {web-cache | service-number}` global configuration command, WCCP is disabled on the router. The first use of a form of the `ip wccp` command enables WCCP. By default WCCPv2 is used for services, but you can use WCCPv1 functionality instead. To change the running version of WCCP from Version 2 to Version 1, or to return to WCCPv2 after an initial change, use the `ip wccp version` command in global configuration mode.

If a function is not allowed in WCCPv1, an error prompt will be printed to the screen. For example, if WCCPv1 is running on the router and you try to configure a dynamic service, the following message will be displayed: “WCCP V1 only supports the web-cache service.” The `show ip wccp` EXEC command will display the WCCP protocol version number that is running on your router.

Use the `ip wccp web-cache password` command to set a password for a router and the content engines in a service group. MD5 password security requires that each router and content engine that wants to join a service group be configured with the service group password. The password must be up to eight characters in length. Each content engine or router in the service group will authenticate the security component in a received WCCP packet immediately after validating the WCCP message header. Packets failing authentication will be discarded.

**SUMMARY STEPS**

1. enable
2. configure terminal
3. ip wccp version {1 | 2}
4. ip wccp [vrf vrf-name] {web-cache | service-number} [group-address multicast-address] [redirect-list access-list] [group-list access-list] [password password [0 | 7]]
5. interface type number
6. ip wccp [vrf vrf-name] {web-cache | service-number} redirect {in | out}
7. exit
8. interface type number
9. ip wccp redirect exclude in

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| **Step 3** ip wccp version \{1 | 2\} | Specifies which version of WCCP to configure on a router.  
  • WCCPv2 is the default running version. |
| **Example:** | Router(config)# ip wccp version 2 |
| **Step 4** ip [vrf vrf-name] \{web-cache | service-number\} [group-address multicast-address] [redirect-list access-list] [group-list access-list] [password password [0 | 7\}] | Specifies a web-cache or dynamic service to enable on the router, specifies a VRF-name to associate with the service group, specifies the IP multicast address used by the service group, specifies any access lists to use, specifies whether to use MD5 authentication, and enables the WCCP service. |
| **Example:** | Router(config)# ip wccp web-cache password password1 |
| **Step 5** interface type number | Targets an interface number for which the web cache service will run, and enters interface configuration mode. |
| **Example:** | Router(config)# interface ethernet0/0 |
| **Step 6** ip [vrf vrf-name] \{web-cache | service-number\} redirect \{in | out\} | Enables packet redirection on an outbound or inbound interface using WCCP.  
  • As indicated by the out and in keyword options, redirection can be specified for outbound interfaces or inbound interfaces. |
| **Example:** | Router(config-if)# ip wccp web-cache redirect in |
| **Step 7** exit | Exits interface configuration mode. |
| **Example:** | Router(config-if)# exit |
| **Step 8** interface type number | Targets an interface number on which to exclude traffic for redirection, and enters interface configuration mode. |
| **Example:** | Router(config)# interface GigabitEthernet 0/2/0 |
| **Step 9** ip wccp redirect exclude in | (Optional) Excludes traffic on the specified interface from redirection. |
| **Example:** | Router(config-if)# ip wccp redirect exclude in |
Verifying and Monitoring WCCP Configuration Settings

SUMMARY STEPS

1. enable
2. show ip wccp [vrf vrf-name] [web-cache] [service-number] [detail view]
3. show ip interface
4. more system:running-config

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td>Step 2 show ip wccp [vrf vrf-name] [web-cache] [service-number] [detail view]</td>
<td>Displays global information related to WCCP, including the protocol version running, the number of content engines in the router service group, which content engine group is allowed to connect to the router, and which access list is being used.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show ip wccp 24 detail</td>
<td></td>
</tr>
<tr>
<td>Step 3 show ip interface</td>
<td>Displays status about whether any ip wccp redirection commands are configured on an interface; for example, “Web Cache Redirect is enabled / disabled.”</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# show ip interface</td>
<td></td>
</tr>
<tr>
<td>Step 4 more system:running-config</td>
<td>(Optional) Displays contents of the running configuration file (equivalent to the show running-config command).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# more system:running-config</td>
<td></td>
</tr>
</tbody>
</table>
Configuration Examples for WCCP Version 2

- Example: Changing the Version of WCCP on a Router, page 11
- Example: Configuring a General WCCPv2 Session, page 11

Example: Changing the Version of WCCP on a Router

The following example shows how to change the WCCP version from the default of WCCPv2 to WCCPv1, and enabling the web-cache service in WCCPv1:

```
Router# show ip wccp
% WCCP version 2 is not enabled
Router# configure terminal
Router(config)# ip wccp version 1
Router(config)# end
Router# show ip wccp
% WCCP version 1 is not enabled
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# end
Router# show ip wccp
Global WCCP information:
   Router information:
      Router Identifier:                   10.4.9.8
      Protocol Version:                    1.0
```

Example: Configuring a General WCCPv2 Session

```
Router# configure terminal
Router(config)# ip wccp web-cache group-address 224.1.1.100 password password1
Router(config)# ip wccp source-interface GigabitEthernet 0/1/0
Router(config)# ip wccp check services all
   Configures a check of all WCCP services.
Router(config-if)# ip wccp web-cache redirect in
Router(config-if)# exit
Router(config)# interface GigabitEthernet 0/2/0
Router(config-if)# ip wccp redirect exclude in
Router(config-if)# exit
```

Additional References

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 addressing and connectivity</td>
<td>IPv6 Configuration Guide</td>
</tr>
</tbody>
</table>
Feature Information for WCCP Version 2

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
### Table 1  Feature Information for WCCP Version 2

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCCP Version 2</td>
<td>Cisco IOS XE Release 2.2</td>
<td>The WCCP Version 2 feature provides several enhancements and features to the WCCP protocol, including:</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.3SG</td>
<td>- The ability of multiple routers to service a content engine cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Redirection of traffic other than HTTP (TCP port 80 traffic), including a variety of UDP and TCP traffic.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Optional authentication that enables you to control which routers and content engines become part of the service group using passwords and the HMAC MD5 standard.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- A check on packets that determines which requests have been returned from the content engine unserviced.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Load adjustments for individual content engines to provide an effective use of the available resources while helping to ensure high quality of service (QoS) to the clients.</td>
</tr>
</tbody>
</table>

The following commands were introduced or modified by this feature: `clear ip wccp`, `ip wccp`, `ip wccp group-listen`, `ip wccp redirect`, `ip wccp redirect exclude in`, `ip wccp version`, `show ip wccp`.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,
and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.
WCCP—Configurable Router ID

The WCCP—Configurable Router ID feature enables the configuration of a Web Cache Communication Protocol (WCCP) source interface. The IP address of this configured source interface is then used as the preferred WCCP router ID and WCCP GRE source address. When a WCCP router ID is manually configured, router IDs are no longer automatically generated when the current router ID is no longer valid and the router ID does not change when another IP address is added to the system.

- Finding Feature Information, page 15
- Information About WCCP—Configurable Router ID, page 15
- How to Configure WCCP—Configurable Router ID, page 16
- Configuration Examples for WCCP—Configurable Router ID, page 17
- Additional References, page 17
- Feature Information for WCCP—Configurable Router ID, page 18

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About WCCP—Configurable Router ID

- WCCP—Configurable Router ID Overview, page 15

WCCP—Configurable Router ID Overview

WCCP uses a router ID in its control messages that a WCCP client can use to uniquely identify a particular WCCP server. The router ID is an IP address and is used as the source address of any WCCP-generated Generic Routing Encapsulation (GRE) frames. Prior to the WCCP—Configurable Router ID feature, WCCP selected a router ID using an automatic mechanism; the highest reachable IP address on the system (or the highest loopback IP address, if there is one) was used as the WCCP router ID. The highest IP address on the system is not always the best choice as the router ID or as the source address of GRE frames. A change in addressing information on the system may cause the WCCP router ID to change...
unexpectedly. During this changeover period, WCCP clients briefly advertise the existence of two routers (the old router ID and the new router ID) and GRE frames are sourced from a different address.

The WCCP—Configurable Router ID feature enables you to define a WCCP source interface from which the router ID will be obtained. The IP address of this configured source interface is then used as the preferred WCCP router ID and WCCP GRE source address. When a WCCP router ID is manually configured, the router ID does not change when another IP address is added to the system. The router ID changes only when a new router ID is manually configured using the `ip wccp source-address` or the `ipv6 wccp source-address` command, or when the address on the manually configured interface is no longer valid.

How to Configure WCCP—Configurable Router ID

- Configuring a Preferred WCCP Router ID, page 16

Configuring a Preferred WCCP Router ID

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `ip wccp [vrf vrf-name] source-interface source-interface`
4. `exit`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1  enable</strong></td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: Device&gt; enable</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2  configure terminal</strong></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example: Device# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3  ip wccp [vrf vrf-name] source-interface source-interface</strong></td>
<td>Configures a preferred WCCP router ID.</td>
</tr>
<tr>
<td>Example: Device(config)# ip wccp source-interface GigabitEthernet 0/0/0</td>
<td></td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 4</th>
<th>exit</th>
</tr>
</thead>
</table>

**Purpose**

Exits global configuration mode and returns to privileged EXEC mode.

**Example:**

Device(config)# exit

---

### Configuration Examples for WCCP—Configurable Router ID

- **Example: Configuring a Preferred WCCP Router ID, page 17**

### Example: Configuring a Preferred WCCP Router ID

The following example displays the configuration for a preferred WCCP router ID:

```plaintext
! Configure a preferred WCCP router ID
ip wccp source-interface GigabitEthernet 0/0/0
```

---

### Additional References

#### Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
</tbody>
</table>
| IP addressing and services commands and configuration tasks | • Cisco IOS IP Addressing Services Configuration Guide  
• Cisco IOS IP Addressing Services Command Reference |
| WCCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | Cisco IOS IP Application Services Command Reference |
Feature Information for WCCP—Configurable Router ID

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2  Feature Information for WCCP—Configurable Router ID

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>WCCP—Configurable Router ID</td>
<td>15.1(1)SG, 15.2(3)T</td>
<td>The WCCP—Configurable Router ID feature enables the configuration of a Web Cache Communication Protocol (WCCP) source interface. The IP address of this configured source interface is then used as the preferred WCCP router ID and WCCP GRE source address. When a WCCP router ID is manually configured, router IDs are no longer automatically generated when the current router ID is no longer valid and the router ID does not change when another IP address is added to the system. The following command was added: <strong>ip wccp source-interface.</strong></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.1S</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco IOS XE Release 3.3SG</td>
<td></td>
</tr>
</tbody>
</table>
WCCP—Fast Timers

The Web Cache Communication Protocol (WCCP)—Fast Timers feature enables WCCP to establish redirection using a configurable message interval when a WCCP client is added to a service group or when a WCCP client fails.

The WCCP message interval capability introduced by the WCCP-Fast Timers feature defines the transmission interval that WCCP clients and WCCP routers use when sending keepalive messages and defines a scaling factor used when calculating the timeout value. The WCCP router uses the timeout value to determine if a WCCP client is no longer available and to redirect traffic as a result.

Finding Feature Information, page 21
Information About WCCP—Fast Timers, page 21
How to Configure WCCP—Fast Timers, page 22
Configuration Examples for WCCP—Fast Timers, page 23
Additional References, page 23
Feature Information for WCCP—Fast Timers, page 24

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Information About WCCP—Fast Timers

WCCP—Fast Timers Overview, page 21

WCCP—Fast Timers Overview

The WCCP—Fast Timers feature enables WCCP to establish redirection using a configurable message interval when a WCCP client is added to a service group or when a WCCP client fails. WCCP routers and WCCP clients exchange keepalive messages at a fixed interval. Prior to the introduction of the WCCP—Fast Timers feature, the WCCP message interval was fixed at 10 seconds. The WCCP—Fast Timers feature enables use of message intervals ranging from 0.5 seconds to 60 seconds and a timeout value scaling factor of 1 to 5. The default is 10 seconds. The timer interval is driven by the WCCP client which is being
redirected to. The WCCP clients must support variable message interval timers in order for the WCCP—Fast Timers feature to function correctly.

The WCCP message interval capability introduced by the WCCP—Fast Timers feature defines the transmission interval that WCCP clients and WCCP routers use when sending keepalive messages and defines a scaling factor used when calculating the timeout value. The WCCP router uses the timeout value to determine if a WCCP client is no longer available and to redirect traffic as a result. The WCCP router enforces a single message interval per service group. WCCP clients with incompatible message intervals are prevented from joining a service group. If a default message interval that is smaller than the default 10 seconds is used, CPU usage will increase.

You can use the `show ip wccp service service-number detail` command to display information about the message interval.

How to Configure WCCP—Fast Timers

• Displaying WCCP—Fast Timers Information, page 22

Displaying WCCP—Fast Timers Information

**SUMMARY STEPS**

1. `enable`
2. `show ip wccp [service-number][detail]`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example:</td>
<td>• Enter your password if prompted.</td>
</tr>
<tr>
<td>Device&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> <code>show ip wccp [service-number][detail]</code></td>
<td>Displays WCCP client information that includes the message interval information.</td>
</tr>
<tr>
<td>Example:</td>
<td>• The message interval is the fixed time interval between successive keepalive messages sent from a WCCP client to a WCCP router. The default time interval is 10 seconds. If the default time interval is configured, the &quot;Message Interval&quot; field is not displayed.</td>
</tr>
<tr>
<td>Device# show ip wccp 24 detail</td>
<td>Note  You configure the time interval on the WCCP client device. Details of the client configuration are specific to each type of client, so you should consult the documentation of your WCCP client device. Client devices may choose not support the full range of settings that are supported by the router.</td>
</tr>
</tbody>
</table>
Configuration Examples for WCCP—Fast Timers

- Example: Displaying WCCP-Fast Timers Information, page 23

Example: Displaying WCCP-Fast Timers Information

The following example displays WCCP client information that includes the message interval information:

Device# show ip wccp 91 detail

WCCP Client information:
WCCP Client ID: 10.1.1.14
Protocol Version: 2.0
State: Usable
Redirection: GRE
Packet Return: GRE
Assignment: MASK

Message Interval: 2.500 seconds (2.354 since last message)
Client timeout: 15 seconds
Assignment timeout: 25 seconds
Packets Redirected: 0
Connect Time: 00:01:56
Bypassed Packets
Process: 0
CEF: 0

Additional References

Related Documents

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS commands</td>
<td>Cisco IOS Master Commands List, All Releases</td>
</tr>
<tr>
<td>IP addressing and services commands and configuration tasks</td>
<td>• Cisco IOS XE IP Addressing Services Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>• Cisco IOS IP Addressing Services Command Reference</td>
</tr>
<tr>
<td>WCCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples</td>
<td>Cisco IOS IP Application Services Command Reference</td>
</tr>
</tbody>
</table>
Technical Assistance

<table>
<thead>
<tr>
<th>Description</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.</td>
<td><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></td>
</tr>
</tbody>
</table>

Feature Information for WCCP—Fast Timers

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
The Web Cache Communication Protocol (WCCP)—Fast Timers feature enables WCCP to establish redirection using a configurable message interval when a WCCP client is added to a service group or when a WCCP client fails.

The WCCP message interval capability introduced by the WCCP-Fast Timers feature defines the transmission interval that WCCP clients and WCCP routers use when sending keepalive messages and defines a scaling factor used when calculating the timeout value. The WCCP router uses the timeout value to determine if a WCCP client is no longer available and to redirect traffic as a result.

The following command were modified: `show ip wccp`.

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.