



Configuring Web Cache Services Using WCCP

This chapter describes how to configure the Cisco 7600 series routers to redirect traffic to cache engines (web caches) using the Web Cache Communication Protocol (WCCP), and describes how to manage cache engine clusters (cache farms).



Note

- For complete syntax and usage information for the commands used in this chapter, refer to the Cisco 7600 Series Routers Command References at this URL:
http://www.cisco.com/en/US/products/hw/routers/ps368/prod_command_reference_list.html
- The PFC supports WCCP.
- To use the WCCP Layer 2 PFC redirection feature, configure WCCP on the Cisco 7600 series router as described in this chapter and configure accelerated WCCP on the cache engine as described in the following publication:
<http://www.cisco.com/univercd/cc/td/doc/product/webscale/uce/acns42/cnfg42/transprt.htm#xtocid34>
- A cache 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.
- With WCCP Layer 2 PFC redirection as the forwarding method for a service group, the packet counters in the **show ip wccp service_name** command output displays flow counts instead of packet counts.

This chapter consists of these sections:

- [Understanding WCCP, page 60-2](#)
- [Restrictions for WCCPv2, page 60-7](#)
- [Configuring WCCP, page 60-8](#)
- [Verifying and Monitoring WCCP Configuration Settings, page 60-12](#)
- [WCCP Configuration Examples, page 60-12](#)
- [VRF Support on WCCP, page 60-16](#)

**Note**

The tasks in this chapter assume that you have already configured cache engines on your network. For specific information on hardware and network planning associated with Cisco Cache Engines and WCCP, see the Product Literature and Documentation links available on the Cisco.com Web Scaling site.

Understanding WCCP

These sections describe WCCP:

- [WCCP Overview, page 60-2](#)
- [Hardware Acceleration, page 60-3](#)
- [Understanding WCCPv1 Configuration, page 60-4](#)
- [Understanding WCCPv2 Configuration, page 60-5](#)
- [WCCPv2 Features, page 60-6](#)

WCCP Overview

The Web Cache Communication Protocol (WCCP) is a Cisco-developed content-routing technology that allows you to integrate cache engines (such as the Cisco Cache Engine 550) into your network infrastructure.

**Note**

Cisco Systems replaced the Cache Engine 500 Series platforms with Content Engine Platforms in July 2001. Cache Engine Products were the Cache Engine 505, 550, 570, and 550-DS3. Content Engine Products are the Content Engine 507, 560, 590, and 7320.

The Cisco IOS WCCP feature allows use of Cisco Cache Engines (or other caches 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 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 cache 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 cache engine instead of from the originally specified server.

When a cache engine receives a request, it attempts to service it from its own local cache. If the requested information is not present, the cache engine issues its own request to the originally targeted server to get the required information. When the cache engine retrieves the requested information, it 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 cache engines, called a *cache engine cluster*, to provide content to a router or multiple routers. Network administrators can easily scale their cache engines to handle heavy traffic loads through these clustering capabilities. Cisco clustering technology enables each cache member to work in parallel, resulting in linear scalability. Clustering cache engines greatly improves the scalability, redundancy, and availability of your caching solution. You can cluster up to 32 cache engines to scale to your desired capacity.

Hardware Acceleration

Cisco 7600 series routers provide WCCP Layer 2 PFC redirection hardware acceleration for directly connected Cisco Cache Engines, which is more efficient than Layer 3 redirection in software on the MSFC with generic route encapsulation (GRE).

WCCP Layer 2 PFC redirection allows Cisco Cache Engines to use hardware-supported Layer 2 redirection. A directly connected Cache Engine can be configured to negotiate use of the WCCP Layer 2 PFC Redirection feature. The WCCP Layer 2 PFC redirection feature requires no configuration on the MSFC. The **show ip wccp web-cache detail** command displays which redirection method is in use for each cache.

The following guidelines apply to WCCP Layer 2 PFC redirection:

- The WCCP Layer 2 PFC redirection feature sets the IP flow mask to full-flow mode.
- You can configure the Cisco Cache Engine software release 2.2 or later releases to use the WCCP Layer 2 PFC redirection feature.
- Layer 2 redirection takes place on the PFC and is not visible to the MSFC. The **show ip wccp web-cache detail** command on the MSFC displays statistics for only the first packet of a Layer 2 redirected flow, which provides an indication of how many flows, rather than packets, are using Layer 2 redirection. Entering the **show mls entries** command displays the other packets in the Layer 2 redirected flows.



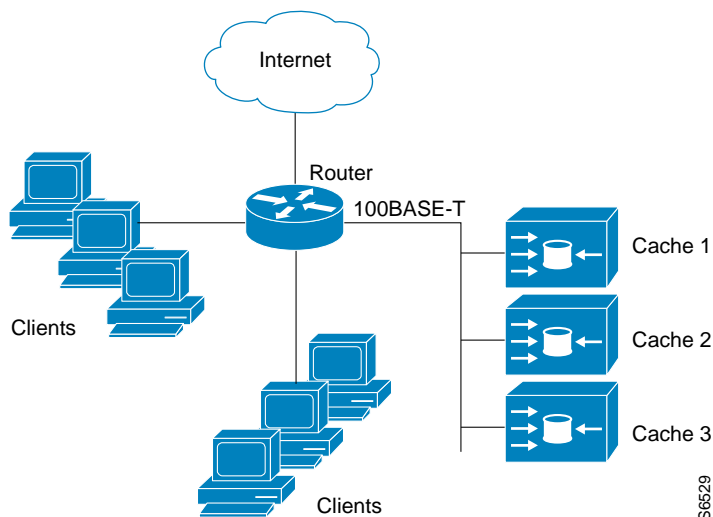
Note

- The PFC provides hardware acceleration for generic route encapsulation (GRE). If you use WCCP Layer 3 redirection with generic route encapsulation (GRE), there is hardware support for encapsulation, but the PFC3 does not provide hardware support for decapsulation of WCCP GRE traffic.
- Releases of Cisco Application and Content Networking System (ACNS) software later than Release 4.2.1 support the **accelerated** keyword.

Understanding WCCPv1 Configuration

With WCCP-Version 1, only a single router services a cluster. In this scenario, this router is the device that performs all the IP packet redirection. [Figure 60-1](#) illustrates how this configuration appears.

Figure 60-1 Cisco Cache Engine Network Configuration Using WCCP-Version 1



Content is not duplicated on the cache engines. The benefit of using multiple caches is that you can scale a caching solution by clustering multiple physical caches to appear as one logical cache.

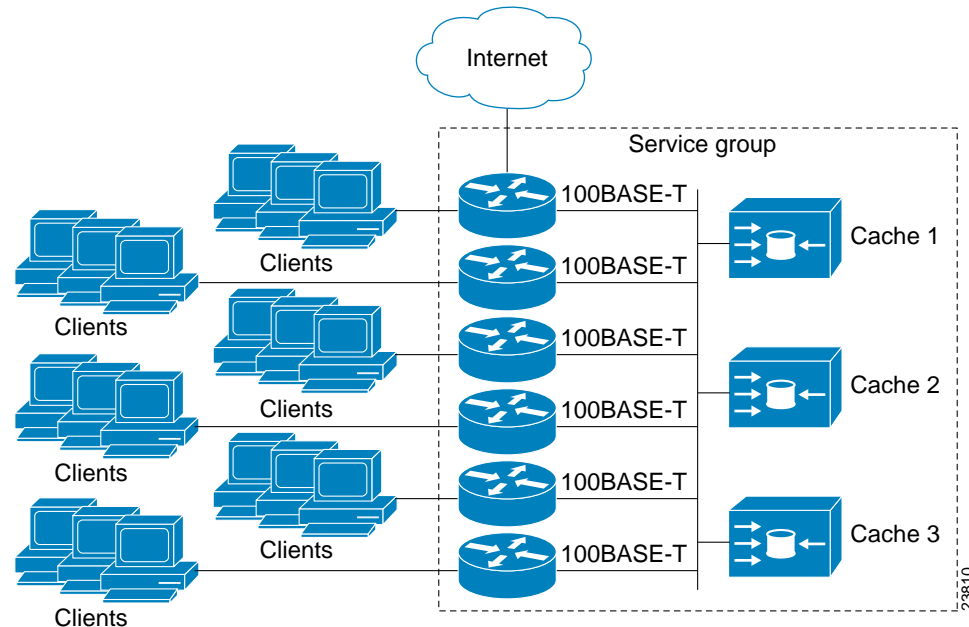
The following sequence of events details how WCCPv1 configuration works:

1. Each cache engine is configured by the system administrator with the IP address of the control router. Up to 32 cache engines can connect to a single control router.
2. The cache engines send their IP addresses to the control router using WCCP, indicating their presence. Routers and cache engines communicate to each other via a control channel; this channel is based on UDP port 2048.
3. This information is used by the control router to create a cluster view (a list of caches in the cluster). This view is sent to each cache in the cluster, essentially making all the cache engines aware of each other. A stable view is established after the membership of the cluster remains the same for a certain amount of time.
4. Once a stable view has been established, one cache engine is elected as the lead cache engine. (The lead is defined as the cache engine seen by all the cache engines in the cluster with the lowest IP address). This lead cache engine uses WCCP to indicate to the control router how IP packet redirection should be performed. Specifically, the lead cache engine designates how redirected traffic should be distributed across the cache engines in the cluster.

Understanding WCCPv2 Configuration

Multiple routers can use WCCPv2 to service a cache cluster. This is in contrast to WCCPv1 in which only one router could redirect content requests to a cluster. [Figure 60-2](#) illustrates a sample configuration using multiple routers.

Figure 60-2 Cisco Cache Engine Network Configuration Using WCCP v2



The subset of cache 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 User Datagram Protocol (UDP) redirection.

Using WCCPv1, the cache engines were configured with the address of the single router. WCCPv2 requires that each cache 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 cache engine. In this case the address of each router in the group must be explicitly specified for each cache engine during configuration.
- **Multicast**—A single multicast address is configured on each cache engine. In the multicast address method, the cache engine sends a single-address notification that provides coverage for all routers in the service group. For example, a cache 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** interface configuration command for details).

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

The following sequence of events details how WCCPv2 configuration works:

1. Each cache engine is configured with a list of routers.

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

The following sections describe how to configure WCCPv2 on routers so they may participate in a service group.

WCCPv2 Features

These sections describe WCCPv2 features:

- [Support for Non-HTTP Services](#)
- [Support for Multiple Routers](#)
- [MD5 Security](#)
- [Web Cache Packet Return](#)
- [Load Distribution](#)

Support for Non-HTTP Services

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 introduces 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 keywords (such as “web-cache”). This information is used to validate that service group members are all using or providing the same service.

The cache engines in service group specify traffic to be redirected by protocol (TCP or UDP) and port (source or destination). Each service group has a priority status assigned to it. Packets are matched against service groups in priority order.

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.

MD5 Security

WCCPv2 provides optional authentication that enables you to control which routers and cache engines become part of the service group using passwords and the 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.

Web Cache Packet Return

If a cache engine is unable to provide a requested object it has cached due to error or overload, the cache 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 cache engine unserved. Using this information, the router can then forward the request to the originally targeted server (rather than attempting to resend the request to the cache cluster). This provides error handling transparency to clients.

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

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

Load Distribution

WCCPv2 can be used to adjust the load being offered to individual cache 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 cache to adjust the load on a particular cache and balance the load across the caches 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 cache engines. Prior to WCCPv2, information from one hash bucket could only go to one cache engine.
- **Load Balancing**—Allows the set of hash buckets assigned to a cache engine to be adjusted so that the load can be shifted from an overwhelmed cache 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 cache engine.

By using these hashing parameters, you can prevent one cache from being overloaded and reduce the potential for congestion.

Restrictions for WCCPv2

The following limitations apply to WCCP v2:

- WCCP works only with IP networks.
- For routers servicing a multicast cluster, the time to live (TTL) value must be set at 15 or fewer.
- Because the messages may now be IP multicast, members may receive messages that will not be relevant or are duplicates. Appropriate filtering needs to be performed.
- Service groups can comprise up to 32 cache engines and 32 routers.
- All cache 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.

Configuring WCCP

The following configuration tasks assume that you have already installed and configured the cache engines you want to include in your network. You must configure the cache engines in the cluster before configuring WCCP functionality on your routers. Refer to the [Cisco Cache Engine Configuration Guide](#) for cache engine configuration and setup tasks.

IP must be configured on the router interface connected to the cache engines and on the router interface connected to the Internet. Cisco Cache Engines require use of a Fast Ethernet interface for a direct connection. Examples of router configuration tasks follow this section. For complete descriptions of the command syntax, refer to the Release 12.2 *Cisco IOS Configuration Fundamentals Command Reference*.

These sections describe how to configure WCCP:

- [Specifying a Version of WCCP, page 60-8](#) (Optional)
- [Configuring a Service Group Using WCCPv2, page 60-8](#) (Required)
- [Excluding Traffic on a Specific Interface from Redirection, page 60-10](#) (Optional)
- [Registering a Router to a Multicast Address, page 60-10](#) (Optional)
- [Using Access Lists for a WCCP Service Group, page 60-11](#) (Optional)
- [Setting a Password for a Router and Cache Engines, page 60-11](#) (Optional)

Specifying a Version of 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, perform this task in EXEC mode:

Command	Purpose
Router# ip wccp version {1 2}	Specifies which version of WCCP to configure on a router. WCCPv2 is the default version.

WCCPv1 does not use the WCCP commands from earlier Cisco IOS versions. Instead, use the WCCP commands documented in this chapter. 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 currently running on your router.

Configuring a Service Group Using WCCPv2

WCCPv2 uses service groups based on logical redirection services, deployed for intercepting and redirecting traffic. The standard service is web cache, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the cache engines. This service is referred to as a *well-known service*, because the

characteristics of the web cache service are known by both the router and cache engines. A description of a well-known service is not required beyond a service identification (in this case, the command line interface (CLI) provides a **web-cache** keyword in the command syntax).

In addition to the web cache service, there can be up to seven dynamic services running concurrently in a service group.

**Note**

More than one service can run on a router at the same time, and routers and cache devices can be part of multiple service groups at the same time.

The dynamic services are defined by the cache engines; the cache instructs the router which protocol or ports to intercept, and how to distribute the traffic. The router itself does not have information on the characteristics of the dynamic service group's traffic, because this information is provided by the first web cache to join the group. In a dynamic service, up to eight ports can be specified within a single protocol.

Cisco Cache Engines, for example, use dynamic service 99 to specify a reverse-proxy service. However, other cache devices may use this service number for some other service. The following configuration information deals with enabling general services on Cisco routers. Refer to the cache server documentation for information on configuring services on cache devices.

To enable a service on a Cisco 7600 series router, perform this task:

	Command	Purpose
Step 1	Router(config)# ip wccp { web-cache <i>service-number</i> } [accelerated] [group-address <i>groupaddress</i>] [redirect-list <i>access-list</i>] [group-list <i>access-list</i>] [password <i>password</i>]	Specifies a web cache or dynamic service to enable on the router, 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.
Step 2	Router(config)# interface <i>type number</i>	Specifies an interface to configure and enters interface configuration mode.
Step 3	Router(config-if)# ip wccp { web-cache <i>service-number</i> } redirect { out in }	Enables WCCP redirection on the specified interface.

**Note**

A future release of Cisco Application and Content Networking System (ACNS) software (Release 4.2.2 or later) supports the **ip wccp service accelerated** command.

As indicated by the **out** and **in** keyword options in the **ip wccp service redirect** command, redirection can be specified for outbound interfaces or inbound interfaces.

Inbound traffic can be configured to use Cisco Express Forwarding (CEF), distributed Cisco Express Forwarding (dCEF), Fast Forwarding, or Process Forwarding.

Configuring WCCP for redirection for inbound traffic on interfaces allows you to avoid the overhead associated with CEF forwarding for outbound traffic. Setting an output feature on any interface results in the slower switching path of the feature being taken by all packets arriving at all interfaces. Setting an input feature on an interface results in only those packets arriving at that interface taking the configured feature path; packets arriving at other interfaces will use the faster default path. Configuring WCCP for inbound traffic also allows packets to be classified before the routing table lookup, which provides faster redirection of packets.

Specifying a Web Cache Service

To configure a web-cache service, perform this task:

	Command	Purpose
Step 1	Router(config)# ip wccp web-cache	Enables the web cache service on the router.
Step 2	Router(config)# interface <i>type number</i>	Targets an interface number for which the web cache service will run, and enters interface configuration mode.
Step 3	Router(config-if)# ip wccp web-cache redirect {out in}	Enables the check on packets to determine if they qualify to be redirected to a web cache, using the interface specified in Step 2.

Excluding Traffic on a Specific Interface from Redirection

To exclude any interface from redirecting inbound traffic, perform this task in global configuration mode:

	Command	Purpose
Step 1	Router(config)# interface <i>type number</i>	Specifies an interface to configure, and enters interface configuration mode.
Step 2	Router(config-if)# ip wccp redirect exclude in	Allows inbound packets on this interface to be excluded from redirection.

Registering a Router to a Multicast Address

If you decide to use the multicast address option for your service group, you must configure the router to listen for the multicast broadcasts on an interface. To configure the router, perform this task:

	Command	Purpose
Step 1	Router(config)# ip wccp {web-cache service-number} group-address <i>groupaddress</i>	Specifies the multicast address for the service group.
Step 2	Router(config)# interface <i>type number</i>	Specifies the interface to be configured for multicast reception.
Step 3	Router(config-if)# ip wccp {web-cache service-number} group-listen	Enables the reception of IP multicast packets (content originating from the cache engines) on the interface specified in Step 2.

For network configurations where redirected traffic needs to traverse an intervening router, the router being traversed must be configured to perform IP multicast routing. You must configure the following two components to enable traversal over an intervening router:

- Enable IP multicast routing using the **ip multicast routing** interface configuration command.
- Enable the interfaces to which the cache engines will connect to receive multicast transmissions using the **ip wccp group-listen** interface configuration command (note that earlier Cisco IOS versions required the use of the **ip pim** interface configuration command).

Using Access Lists for a WCCP Service Group

To configure the router to use an access list to determine which traffic should be directed to which cache engines, perform this task in global configuration mode:

	Command	Purpose
Step 1	Router(config)# access-list <i>access-list</i> permit ip host <i>host-address</i> [<i>destination-address</i> <i>destination-host</i> any]	Creates an access list that enables or disables traffic redirection to the cache engine.
Step 2	Router(config)# ip wccp web-cache group-list <i>access-list</i>	Indicates to the router from which IP addresses of cache engines to accept packets.

To disable caching for certain clients, perform this task in global configuration mode:

	Command	Purpose
Step 1	Router(config)# access-list <i>access-list</i> permit ip host <i>host-address</i> [<i>destination-address</i> <i>destination-host</i> any]	Creates an access list that enables or disables traffic redirection to the cache engine.
Step 2	Router(config)# ip wccp web-cache redirect-list <i>access-list</i>	Sets the access list used to enable redirection.

Setting a Password for a Router and Cache Engines

MD5 password security requires that each router and cache engine that wants to join a service group be configured with the service group password. The password can consist of up to seven characters. Each cache 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.

To configure an MD5 password for use by the router in WCCP communications, perform this task in global configuration mode:

Command	Purpose
Router(config)# ip wccp web-cache password <i>password</i>	Sets an MD5 password on the router.

Verifying and Monitoring WCCP Configuration Settings

To verify and monitor the configuration settings for WCCP, use the following commands in EXEC mode:

Command	Purpose
Router# show ip wccp [web-cache <i>service-number</i>]	Displays global information related to WCCP, including the protocol version currently running, the number of cache engines in the routers service group, which cache engine group is allowed to connect to the router, and which access list is being used.
Router# show ip wccp { web-cache <i>service-number</i> } detail	Queries the router for information on which cache engines of a specific service group the router has detected. The information can be displayed for either the web cache service or the specified dynamic service.
Router# show ip interface	Displays status about whether any ip wccp redirection commands are configured on an interface. For example, “Web Cache Redirect is enabled / disabled.”
Router# show ip wccp { web-cache <i>service-number</i> } view	Displays which devices in a particular service group have been detected and which cache engines are having trouble becoming visible to all other routers to which the current router is connected. The view keyword indicates a list of addresses of the service group. The information can be displayed for either the web cache service or the specified dynamic service. For further troubleshooting information, use the show ip wccp { web-cache <i>service number</i> } service command.

WCCP Configuration Examples

This section provides the following configuration examples:

- [Changing the Version of WCCP on a Router Example, page 60-13](#)
- [Performing a General WCCPv2 Configuration Example, page 60-13](#)
- [Running a Web Cache Service Example, page 60-13](#)
- [Running a Reverse Proxy Service Example, page 60-14](#)
- [Registering a Router to a Multicast Address Example, page 60-14](#)
- [Using Access Lists Example, page 60-14](#)
- [Setting a Password for a Router and Cache Engines Example, page 60-15](#)
- [Verifying WCCP Settings Example, page 60-15](#)

Changing the Version of WCCP on a Router Example

The following example shows the process of changing 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# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
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
  . . .
```

Performing a General WCCPv2 Configuration Example

The following example shows a general WCCPv2 configuration session:

```
Router# configure terminal
Router(config)# ip wccp web-cache group-address 224.1.1.100 password alaska1
Router(config)# interface vlan 20
Router(config-if)# ip wccp web-cache redirect out
```

Running a Web Cache Service Example

The following example shows a web cache service configuration session:

```
router# configure terminal
router(config)# ip wccp web-cache
router(config)# interface vlan 20
router(config-if)# ip wccp web-cache redirect out
Router(config-if)# ^Z
Router# copy running-config startup-config
```

The following example shows a configuration session in which redirection of HTTP traffic arriving on VLAN interface 30 is enabled:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface vlan 30
Router(config-if)# ip wccp web-cache redirect in
Router(config-if)# ^Z
Router# show ip interface vlan 30 | include WCCP Redirect
WCCP Redirect inbound is enabled
WCCP Redirect exclude is disabled
```

Running a Reverse Proxy Service Example

The following example assumes you are configuring a service group using Cisco Cache Engines, which use dynamic service 99 to run a reverse proxy service:

```
router# configure terminal
router(config)# ip wccp 99
router(config)# interface vlan 40
router(config-if)# ip wccp 99 redirect out
```

Registering a Router to a Multicast Address Example

The following example shows how to register a router to a multicast address of 224.1.1.100:

```
Router(config)# ip wccp web-cache group-address 224.1.1.100
Router(config)# interface vlan 50
Router(config-if)# ip wccp web-cache group-listen
```

The following example shows a router configured to run a reverse proxy service, using the multicast address of 224.1.1.1. Redirection applies to packets outgoing through VLAN interface 60:

```
Router(config)# ip wccp 99 group-address 224.1.1.1
Router(config)# interface vlan 60
Router(config-if)# ip wccp 99 redirect out
```

Using Access Lists Example

To achieve better security, you can use a standard access list to notify the router which IP addresses are valid addresses for a cache engine attempting to register with the current router. The following example shows a standard access list configuration session where the access list number is 10 for some sample hosts:

```
router(config)# access-list 10 permit host 11.1.1.1
router(config)# access-list 10 permit host 11.1.1.2
router(config)# access-list 10 permit host 11.1.1.3
router(config)# ip wccp web-cache group-list 10
```

To disable caching for certain clients, servers, or client/server pairs, you can use WCCP access lists. The following example shows that any requests coming from 10.1.1.1 to 12.1.1.1 will bypass the cache and that all other requests will be serviced normally:

```
Router(config)# ip wccp web-cache redirect-list 120
Router(config)# access-list 120 deny tcp host 10.1.1.1 any
Router(config)# access-list 120 deny tcp any host 12.1.1.1
Router(config)# access-list 120 permit ip any any
```

The following example configures a router to redirect web-related packets received through VLAN interface 70, destined to any host except 209.165.196.51:

```
Router(config)# access-list 100 deny ip any host 209.165.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp web-cache redirect-list 100
Router(config)# interface vlan 70
Router(config-if)# ip wccp web-cache redirect in
```

Setting a Password for a Router and Cache Engines Example

The following example shows a WCCPv2 password configuration session where the password is alaska1:

```
router# configure terminal
router(config)# ip wccp web-cache password alaska1
```

Verifying WCCP Settings Example

To verify your configuration changes, use the **more system:running-config** EXEC command. The following example shows that the both the web cache service and dynamic service 99 are enabled on the router:

```
router# more system:running-config

Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname router4
!
enable secret 5 $1$nSVy$faliJsVQXVPW.KuCxZNTh1
enable password alabama1
!
ip subnet-zero
ip wccp web-cache
ip wccp 99
ip domain-name cisco.com
ip name-server 10.1.1.1
ip name-server 10.1.1.2
ip name-server 10.1.1.3
!
!
!
interface Vlan200
ip address 10.3.1.2 255.255.255.0
no ip directed-broadcast
ip wccp web-cache redirect out
ip wccp 99 redirect out
no ip route-cache
no ip mroute-cache
!

interface Vlan300
ip address 10.4.1.1 255.255.255.0
no ip directed-broadcast
ip wccp 99 redirect out
no ip route-cache
no ip mroute-cache
!
interface Serial0
no ip address
no ip directed-broadcast
no ip route-cache
```

```

no ip mroute-cache
shutdown
!
interface Serial1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
!
ip default-gateway 10.3.1.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.3.1.1
no ip http server
!
!
!
line con 0
transport input none
line aux 0
transport input all
line vty 0 4
password alaska1
login
!
end

```

VRF Support on WCCP

Virtual Routing and Forwarding (VRF) is an IP technology that allows multiple instances of a routing table to coexist on the same router at the same time. Before Cisco IOS 15.1(3)S, VRF was not supported as a part of Web Cache Communication Protocol (WCCP). Service groups that defines the nature of the traffic for redirection were configured globally. The VRF support on WCCP enhances the existing WCCP protocol by allowing implementing support for VRF and allows you to configure service groups for each VRF. Both the service identifier and the VRF identifier of WCCP protocol packets are used to associate cache engines with a configured service group.

Configuring VRF Support on WCCP

Complete these steps to configure VRF support on WCCP.

Summary Steps

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **exit**
6. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number* | **source-interface** *source-interface*} [**group-address** *group-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]

7. **interface** *type number*
8. **ip vrf forwarding** *vrf-name*
9. **ip address** *ip-address subnet-mask*
10. **ip wccp** [*vrf vrf-name*] {**web-cache** | **service-number**} **redirect** {**out** | **in**}
11. **end**

Detailed Steps

	Command	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	configure terminal Example: Router(config)# terminal	Enters global configuration mode.
Step 3	ip vrf <i>vrf-name</i> Example: Router(config)# ip vrf vrf1	Enters VRF configuration sub mode to configure the variables associated with the VRF.
Step 4	rd <i>route-distinguisher</i> Example: Router(config-vrf)# rd 100:1	Specifies the eight-byte route distinguisher (RD). route-distinguisher- The route distinguisher (RD) is a number which helps to identify a VPN in a provider's network. Enter either an autonomous system (AS) number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y).
Step 5	exit Example: Router(config-vrf)# exit	exits the VRF configuration mode.

	Command	Purpose
Step 6	<pre>ip wccp vrf vrf-name {web-cache service-number source-interface source-interface} [accelerated] [group-address group-address] [redirect-list redirect-list] [group-list group-list] [password password]</pre> <p>Example:</p> <pre>Router(config)# ip wccp vrf vrf1 web-cache</pre>	<p>Enables the WCCP service.</p> <ul style="list-style-type: none"> • vrf-name — Specifies a VRF name to associate with the service group. • service-number — Specifies a dynamic service number. You can specify a number from 0 to 255. • source-interface — Specifies the interface that WCCP use as the preferred router ID. • group-address — Specifies the IP multicast address used by the service group. • redirect-list — Specifies the access-list for redirecting traffic. • group-list — Specifies the access-list for filtering data traffic. • password — Specifies the authentication password
Step 7	<pre>interface gigabitethernet slot/port or interface tengigabitethernet slot/port</pre> <p>Example:</p> <pre>Router(config)# interface gigabit ethernet 1/1</pre>	<p>Specifies the interface to configure VRF support on WCCP.</p> <p>slot/port — Specifies the location of the interface.</p>
Step 8	<pre>ip vrf forwarding vrf-name</pre> <p>Example:</p> <pre>Router(config)# ip vrf forwarding vrf1</pre>	<p>Applies the specified VRF on the interface.</p>
Step 9	<pre>ip address ip-address subnet-mask</pre> <p>Example:</p> <pre>Router(config)# ip address 10.1.1.0 255.255.255.0</pre>	<p>Specifies an IP address to the interface.</p>
Step 10	<pre>ip wccp vrf vrf-name {web-cache service-number} redirect {out in}</pre> <p>Example:</p> <pre>Router(config-if)# ip wccp vrf vrf1 web-cache redirect in</pre>	<p>Enables redirection on an inbound or outbound interface using WCCP.</p>
Step 11	<pre>end Router(config-if)# end</pre>	<p>Closes the configuration session.</p>

Examples

This example shows how to configure a web-cache service on an interface with VRF.

```

Router# enable
Router# configure terminal
Router(config)# ip vrf vrf1
Router(config-vrf1)# rd 100:1
Router(config)# ip wccp vrf vrf1 web-cache
Router(config)# interface gigabitethernet 1/1
Router(config-if)# ip vrf forwarding vrf1
Router(config-if)# ip address 100.1.1.1 255.255.0.0
Router(config-if)# ip wccp vrf vrf1 web-cache redirect in
Router(config-if)# end

```

This example shows how to configure a web-cache service on an interface with VRF and ACL configured.

```

Router# enable
Router# configure terminal
Router(config)# ip vrf vrf2
Router(config-vrf2)# rd 200:1
Router(config)# ip wccp vrf vrf2 web-cache
Router(config)# ip access-list extended wccp_acl
Router(config-ext-nacl)# 10 deny tcp any eq www any eq www
Router(config-ext-nacl)# 20 permit ip any any
Router(config)# ip wccp vrf vrf2 web-cache redirect-list wccp_acl
Router(config)# interface gigabitethernet 1/2
Router(config-if)# ip vrf forwarding vrf2
Router(config-if)# ip address 200.1.1.1 255.255.0.0
Router(config-if)# ip wccp vrf vrf2 web-cache redirect in
Router(config-if)# end

```

Verification

Use the **show ip wccp summary** command to display the summary of all WCCP services including VRF specific WCCP configuration.

```

Router# show ip wccp summary
WCCP version 2 enabled, 2 services

```

Service	Clients	Routers	Assign	Redirect	Bypass
-----	-----	-----	-----	-----	-----
Default routing table (Router Id: 15.0.0.2):					
web-cache	1	1	MASK	L2	L2
VRF vrf1 (Router Id: 6.6.6.5):					
web-cache	1	1	MASK	L2	L2

Use the **show ip wccp vrf vrf-id** command to display the VRF specific WCCP configuration.

```

Router# show ip wccp vrf vrf1
VRF RED WCCP information:
  Router information:
    Router Identifier:      80.20.1.3
    Protocol Version:      2.0

  Service Identifier: web-cache
    Number of Service Group Clients: 1
    Number of Service Group Routers: 1
    Total Packets Redirected: 0
    Process: 0
    CEF: 0
    Service mode: Open

```

```

Service Access-list:                -none-
Total Packets Dropped Closed:      0
Redirect access-list:              -none-
Total Packets Denied Redirect:     0
Total Packets Unassigned:          0
Group access-list:                 -none-
Total Messages Denied to Group:    0
Total Authentication failures:      0
Total GRE Bypassed Packets Received: 0
    Process:                        0
    CEF:                            0
    
```

Troubleshooting Tips

Command	Purpose
<code>debug ip wccp vrf <i>vrf-id</i></code>	Displays information about significant WCCP events or each WCCP packet sent or received by the router.

WCCPv2 IPv6 Support on the Cisco 7600 Series Router

The Web Cache Communication Protocol (WCCP) is a content-routing technology that intercepts IP packets and redirects those packets to a destination other than the specified destination in the IP packet. Earlier, WCCP support was available only for IPv4 networks on Cisco 7600 series routers. Effective with Cisco IOS release 15.3(1)S, WCCP also supports IPv6 networks on Cisco 7600 series routers.

For more information about WCCP, see [“Understanding WCCP” section on page 60-2](#).

Restrictions and Usage Guidelines

Following restrictions apply while configuring WCCPv2 IPv6 feature on the Cisco 7600 series routers.

- Supports only these WCCP features:
 - Layer 2 redirection
 - Layer 2 return
 - Mask assignment
- VRF is not supported.
- Redirection is supported only in the ingress direction and egress redirection is not supported.
- Hash assignment is not supported.
- GRE redirection and return are not supported.
- These WCCP commands are disabled for the WCCPv2 IPv6 feature:
 - **ipv6 wccp check acl outbound**
 - **ipv6 wccp check services all**
 - **ip wccp redirect exclude in**

Configuring WCCPv2 IPv6 Support

Complete these steps to configure WCCPv2 IPv6 support on Cisco 7600 routers.

Summary Steps

1. **enable**
2. **configure terminal**
3. **ipv6 wccp** {**web-cache** | *service-number* | **source-interface** *source-interface*} [**group-address** *group-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
4. **ipv6 unicast-routing**
5. **mls ipv6 acl compress address unicast**
6. **interface** *type number*
7. **ipv6 enable**
8. **ipv6 address** *ipv6-address/prefix*
9. **ipv6 wccp** {**web-cache** | *service-number*} **redirect in**

10. end

Detailed Steps

	Command	Purpose
Step 1	enable Example: Router# enable	Enables privileged EXEC mode. If prompted, enter your password.
Step 2	configure terminal Example: Router(config)# terminal	Enters global configuration mode.
Step 3	ipv6 wccp {web-cache service-number source-interface source-interface} [accelerated] [group-address group-address] [redirect-list redirect-list] [group-list group-list] [password password] Example: Router(config)# ipv6 wccp web-cache	Enables the WCCP service. <ul style="list-style-type: none"> • service-number — Specifies a dynamic service number. You can specify a number from 0 to 255. • source-interface — Specifies the interface that WCCP use as the preferred router ID. • group-address — Specifies the IP multicast address used by the service group. • redirect-list — Specifies the access-list for redirecting traffic. • group-list — Specifies the access-list for filtering data traffic. • password — Specifies the authentication password
Step 4	ipv6 unicast-routing Example: Router(config)# ipv6 unicast-routing	Enables the forwarding of IPv6 unicast datagrams.
Step 5	mls ipv6 acl compress address unicast Example: Router(config)# mls ipv6 acl compress address unicast	Enables the compression of compressible IPv6 addresses.

	Command	Purpose
Step 6	interface <i>type number</i> Example: Router(config)# interface gigabitethernet 1/1	Specifies the interface to configure WCCP.
Step 7	ipv6 enable Example: Router(config-if)# ipv6 enable	Enables IPv6 on the interface.
Step 8	ipv6 address <i>ipv6-address/prefix</i> Example: Router(config-if)# ipv6 address 3FFE:2002::A8BB:CCFF:FE01:2C01/112	Specifies an IPv6 address to the interface.
Step 9	ipv6 wccp { <i>web-cache</i> <i>service-number</i> } redirect in Example: Router(config-if)# ipv6 wccp web-cache redirect in	Enables redirection on an inbound interface using WCCP.
Step 10	end Example: Router(config-if)# end	Closes the configuration session.

Examples

This example shows how to configure web-cache service on an interface with IPv6 address.

```
Router# enable
Router# configure terminal
Router(config)# ipv6 wccp web-cache
Router(config)# ipv6 unicast-routing
Router(config)# mls ipv6 acl compress address unicast
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# ipv6 enable
Router(config-if)# ipv6 address 3FFE:2002::A8BB:CCFF:FE01:2C01/112
Router(config-if)# ipv6 wccp web-cache redirect in
Router(config-if)# end
```

Verification

Use these commands to verify the WCCPv2 IPv6 support feature.

Command	Purpose
<code>show ipv6 wccp [web-cache service-number]</code>	Displays information related to WCCP including the protocol version, number of cache engines and access list in use.
<code>show ipv6 wccp {web-cache service-number} detail</code>	Displays web cache engine information and WCCP router statistics for the web cache service or client service information, and WCCP router statistics for the specified dynamic service.
<code>show ipv6 wccp summary</code>	Displays information on the configured WCCP services and a summary of their current state.
<code>show ipv6 wccp capabilities</code>	Displays information about WCCP platform capabilities.
<code>show tcam interface type number acl in ipv6 module module_numbers</code>	Displays information about the interface-based Ternary Content Addressable Memory (TCAM) for the specified module.

This is a sample output of the `show ipv6 wccp capabilities` command.

```
Router #show ipv6 wccp capabilities
WCCP Platform Capability Settings
```

Capability	Setting
Supported forwarding methods	L2
Supported return methods	L2
Supported assignment methods	Mask
Accelerated forwarding methods	L2
Accelerated return methods	L2
Accelerated assignment methods	Mask
Accelerated Mode CLI	On, CLI Disabled
Supported redirection types	Input
Check Outbound ACL CLI	Off, CLI Disabled
Check All Services CLI	On, CLI Disabled
Closed Service Support	Unsupported
VRF Support	Unsupported
Supported service groups	256

Troubleshooting Tips

Command	Purpose
<code>debug fm ipv6 wccp [all events inband vmr]</code>	Enables debugging information for WCCPv2 IPv6 support.