

Configuring WCCP Version 2 Services

**Note**

WCCP v2 is *not* supported on Supervisor Engine 6-E.

This chapter describes how to configure the Catalyst 4500 series switches to redirect traffic to content engines (web caches) using the Web Cache Communication Protocol (WCCP) version 2

**Note**

Throughout this chapter, WCCP refers to WCCP version 2. Version 1 is *not* supported.

This chapter consists of these sections:

- [Understanding WCCP, page 52-1](#)
- [Restrictions for WCCP, page 52-5](#)
- [Configuring WCCP, page 52-5](#)
- [Verifying and Monitoring WCCP Configuration Settings, page 52-8](#)
- [WCCP Configuration Examples, page 52-8](#)

**Note**

The tasks in this chapter 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 Product Literature and Documentation links available on the Cisco.com Web Scaling site at this location:

<http://www.cisco.com/warp/public/cc/pd/exsr/ces/index.shtml>.

Understanding WCCP

These sections describe WCCP:

- [WCCP Overview, page 52-2](#)
- [Hardware Acceleration, page 52-2](#)
- [Understanding WCCP Configuration, page 52-2](#)
- [WCCP Features, page 52-4](#)

WCCP Overview

WCCP is a Cisco-developed content-routing technology that enables you to integrate content engines into your network infrastructure.

The Cisco IOS WCCP feature enables use of 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 routing platforms to transparently redirect content requests. The main benefit of transparent redirection of HTTP requests 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.

When a content engine receives a request, it attempts to service it from its own local content. If the requested information is not present, the content engine issues its own request to the originally targeted server to get the required information. When the content 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 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 handle heavy traffic loads through these clustering capabilities. Cisco clustering technology enables each content 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.

Hardware Acceleration

Catalyst 4500 series switches provide hardware acceleration for directly connected Cisco Content Engines, which is more efficient than Layer 3 redirection in the software.

You must configure a directly connected Content Engine to negotiate use of the WCCP Layer 2 Redirection feature with load balancing based on the mask assignment table. The **show ip wccp web-cache detail** command displays which redirection method is in use for each cache.

**Note**

You can configure the Cisco Content Engine software release 2.2 or later releases to use the WCCP Layer 2 redirection feature along with the mask assignment table.

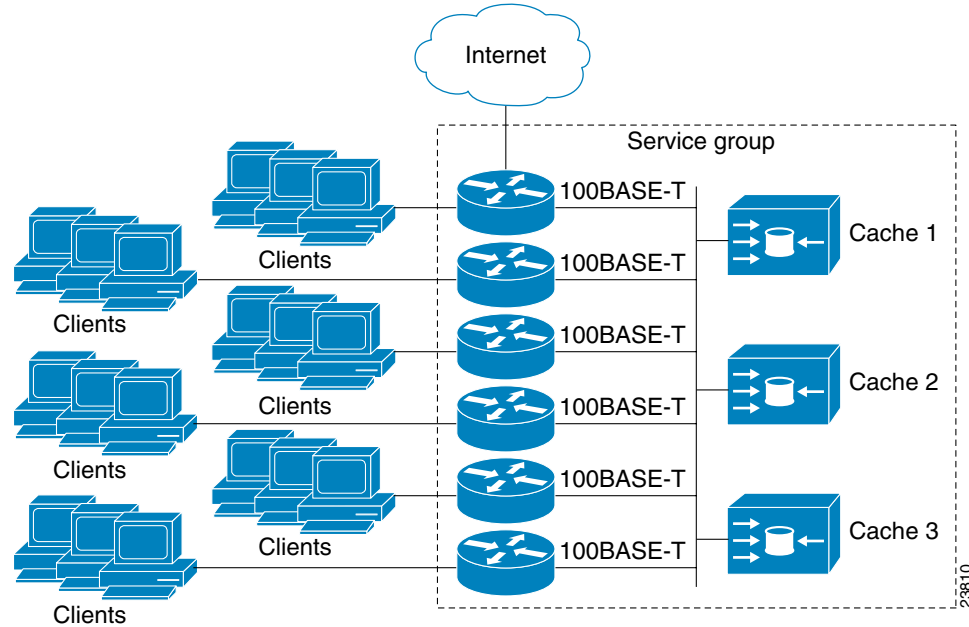
Understanding WCCP Configuration

**Note**

WCCPv1 is not supported.

Multiple routers can use WCCP to service a cache cluster. [Figure 52-1](#) illustrates a sample configuration using multiple routers.

Figure 52-1 Cisco Content Engine Network Configuration Using WCCP



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 User Datagram Protocol (UDP) redirection.

WCCP 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** 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 enables 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 shows how WCCP 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. Once 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.

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

WCCP Features

These sections describe WCCP features:

- [Support for HTTP and Non-HTTP Services](#)
- [Support for Multiple Routers](#)
- [MD5 Security](#)
- [Web Content Packet Return](#)

Support for HTTP and Non-HTTP Services

WCCP enables redirection of HTTP traffic (TCP port 80 traffic), as well as non-HTTP traffic (TCP and UDP). WCCP 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, WCCP 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.

**Note**

The Catalyst 4500 series switch supports up to eight service groups.

For information on supported WCCP version 2 services with ACNS version 5.2 software, refer to the *Release Notes for Cisco ACNS Software, Release 5.2.3*.

The content 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 level assigned to it. Packets are matched against service groups in priority order and redirected by the highest priority service group that matches traffic characteristics.

Support for Multiple Routers

WCCP enables you to attach multiple routers to a cluster of cache engines. The use of multiple routers in a service group enables redundancy, interface aggregation, and distribution of the redirection load.

MD5 Security

WCCP provides 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. 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 Content Packet Return

If a content engine is unable to provide a requested object it has cached due to error or overload, the content engine returns the request to the router for onward transmission to the originally specified destination server. WCCP verifies which requests have been returned from the content 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 content cluster). This 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 (such as, when IP authentication has been turned on).

Restrictions for WCCP

The following limitations apply to WCCP:

- 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 are not relevant or duplicates. Appropriate filtering needs to be performed.
- A service group 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.
- Up to 8 service groups are supported at the same time on the same client interface.
- The L2 rewrite forwarding method is supported, but GRE encapsulation is not.
- Direct L3 connectivity to content engines is required; L3 connectivity of one or more hops away is not supported.
- Layer 2 redirection requires that content engines and clients I/Fs be directly connected to a router and should be on separate IP subnetworks
- The TCAM friendly mask-based assignment is supported, but the hash bucket-based method is not.
- Redirect ACL for WCCP on a client interface is not supported.
- Incoming traffic redirection on an interface is supported, but outgoing traffic re-direction is not.
- When TCAM space is exhausted, traffic is not redirected; it is forwarded normally.
- WCCP version 2 standard allows for support of up to 256 distinct masks. However, a Catalyst 4500 series switch only supports mask assignment table with a single mask.

Configuring WCCP

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

IP must be configured on the router interface connected to the cache engines. Examples of router configuration tasks follow this section. For complete descriptions of the command syntax, refer to the *Cisco IOS Configuration Fundamentals Command Reference, Cisco IOS Release 12.3*.

These sections describe how to configure WCCP:

- [Configuring a Service Group Using WCCP, page 52-6](#) (Required)
- [Using Access Lists for a WCCP Service Group, page 52-7](#) (Optional)
- [Setting a Password for a Router and Cache Engines, page 52-7](#) (Optional)

Configuring a Service Group Using WCCP

WCCP uses service groups based on logical redirection services, deployed for intercepting and redirecting traffic. The standard service is the content engine, which intercepts TCP port 80 (HTTP) traffic and redirects that traffic to the content 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 content 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).

For information on supported WCCP services with ACNS version 5.2 software, refer to the *Release Notes for Cisco ACNS Software, Release 5.2.3*.

In addition to the web cache service, there can be up to seven dynamic services running concurrently on the switch.



Note

More than one service can run on a switch at the same time, and routers and content engines can be part of multiple service groups at the same time.

The dynamic services are defined by the content engines; the content engine 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 content engine to join the group. In a dynamic service, up to eight ports can be specified within a single protocol TCP or UDP).

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

To enable a service on a Catalyst 4500 series switch, perform this task:

| | Command | Purpose |
|--------|---|---|
| Step 1 | Switch(config)# ip wccp { web-cache <i>service-number</i> } [group-address <i>groupaddress</i>] [group-list <i>access-list</i>] [password <i>password</i>] | Specifies a dynamic service to enable on the switch, specifies the IP multicast address used by the service group (optional), group list to use for content engine membership (optional), specifies whether to use MD5 authentication (optional), and enables the WCCP service. |
| Step 2 | Switch(config)# interface <i>type number</i> | Specifies a client interface to configure and enters interface configuration mode. |
| Step 3 | Switch(config-if)# ip wccp { web-cache <i>service-number</i> } redirect in | Enables WCCP redirection for ingress traffic on the specified client interface. |

| | Command | Purpose |
|--------|--|---|
| Step 4 | Switch(config)# interface <i>type number</i> | (Only needed to run the multicast feature) Specifies the content engine interface to be configured for multicast reception. |
| Step 5 | Switch(config-if)# ip wccp { web-cache <i>service-number</i> } group-listen | (Only needed to run the multicast feature) Enables the reception of IP multicast packets (WCCP protocol packets originating from the content engines) on the interface specified in Step 4. |

Specifying a Web Cache Service

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

| | Command | Purpose |
|--------|---|---|
| Step 1 | Switch(config)# ip wccp web-cache | Enables the web cache service on the switch. |
| Step 2 | Switch(config)# interface <i>type number</i> | Targets a client interface number for which the web cache service runs, and enters interface configuration mode. |
| Step 3 | Switch(config-if)# ip wccp web-cache redirect in | Enables the check on packets to determine if they qualify to be redirected to a content engine, using the client interface specified in Step 2. |

Using Access Lists for a WCCP Service Group

A Catalyst 4500 series switch can use an access list to restrict the content engines that can join a service group.

To restrict a content engine, perform this task:

| | Command | Purpose |
|--------|--|--|
| Step 1 | Switch(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 based on the unicast address of the content engines. |
| Step 2 | Switch(config)# ip wccp web-cache group-list <i>access-list</i> | Indicates to the switch which content engines are allowed or disallowed to form a service group. |

Setting a Password for a Router and Cache Engines

MD5 password security requires that each content engine and Catalyst 4500 series switch that wants to join a service group be configured with the service group password. The password can consist of up to seven characters. Each content engine or Catalyst 4500 series switch in the service group authenticates the security component in a received WCCP packet immediately after validating the WCCP message header. Packets failing authentication are discarded.

To configure an MD5 password for use by the Catalyst 4500 series switch in WCCP communications, perform this task:

| Command | Purpose |
|---|--|
| Switch(config)# ip wccp web-cache password <i>password</i> | Sets an MD5 password on the Catalyst 4500 series switch. |

Verifying and Monitoring WCCP Configuration Settings

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

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

WCCP Configuration Examples

This section provides the following configuration examples:

- [Performing a General WCCP Configuration Example, page 52-9](#)
- [Running a Web Cache Service Example, page 52-9](#)
- [Running a Reverse Proxy Service Example, page 52-9](#)
- [Using Access Lists Example, page 52-9](#)

- [Setting a Password for a Switch and Content Engines Example, page 52-10](#)
- [Verifying WCCP Settings Example, page 52-10](#)

Performing a General WCCP Configuration Example

The following example shows a general WCCP configuration session. VLAN 20 is for the client interface. VLAN 50 is for the content engine interface.

```
Switch# configure terminal
Switch(config)# ip wccp web-cache group-address 224.1.1.100 password alaska1
Switch(config)# interface vlan 20
Switch(config-if)# ip wccp web-cache redirect in
Switch(config)# interface vlan 50
Switch(config-if)# ip wccp web cache group-listen
```

Running a Web Cache Service Example

The following example shows a web cache service configuration session:

```
Switch# configure terminal
Switch(config)# ip wccp web-cache
Switch(config)# interface vlan 20
Switch(config-if)# ip wccp web-cache redirect in
Switch(config-if)# ^Z
Switch# copy running-config startup-config
Switch# show ip interface vlan 20 | 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 Content Engines, which use dynamic service 99 to run a reverse proxy service:

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

Using Access Lists Example

To achieve better security, you can use a standard access list to notify the Catalyst 4500 series switch to which IP addresses are valid addresses for a content engine attempting to register with the current switch. 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
```

Setting a Password for a Switch and Content Engines Example

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

```
Switch# 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 Catalyst 4500 series switch:

```
Switch# more system:running-config

Building configuration...
Current configuration:
!
version 12.2
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.KuCxZNT1
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 in
ip wccp 99 redirect in
no ip route-cache
no ip mroute-cache
!
interface Vlan300
ip address 10.4.1.1 255.255.255.0
!
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
```

