



Web Cache Communication Protocol Version 2

This chapter describes the Web Cache Communication Protocol (WCCP) Version 2 feature. (WCCP is also known as Web Cache Control Protocol and Web Cache Coordination Protocol.) This chapter includes information on the benefits of this feature, supported platforms, and other information you may need to work with WCCP Version 2. This chapter includes the following sections:

- [Feature Overview, page B-2](#)
- [Prerequisites, page B-7](#)
- [Configuration Tasks, page B-8](#)
- [Monitoring and Maintaining WCCP Version 2, page B-12](#)
- [Configuration Examples, page B-13](#)
- [Command Reference, page B-16](#)



Note

This chapter may include descriptions of WCCP Version 2 features that may not be supported in your release of the Cisco Cache software. Refer to the release notes for your release of the Cache software for further information.

Feature Overview

Cisco developed the Web Cache Communication Protocol (WCCP) within Cisco IOS software to enable routers or switches to transparently redirect packets to network caches. It does not interfere with normal router or switch operations. Using WCCP, the router redirects requests on configured TCP ports to network caches rather than to intended host sites. It also balances traffic load across a cache cluster and ensures fault-tolerant and fail-safe operation. As Content Engines are added to or deleted from a cache cluster, the WCCP-aware router or switch dynamically adjusts its redirection map to reflect the currently available caches, resulting in maximized performance and content availability.

WCCP Version 2 contains the following features:

- Multiple router support
- Improved security
- Faster throughput
- Redirection of multiple TCP port-destined traffic
- Load-distributing applications capability
- Client IP addressing transparency

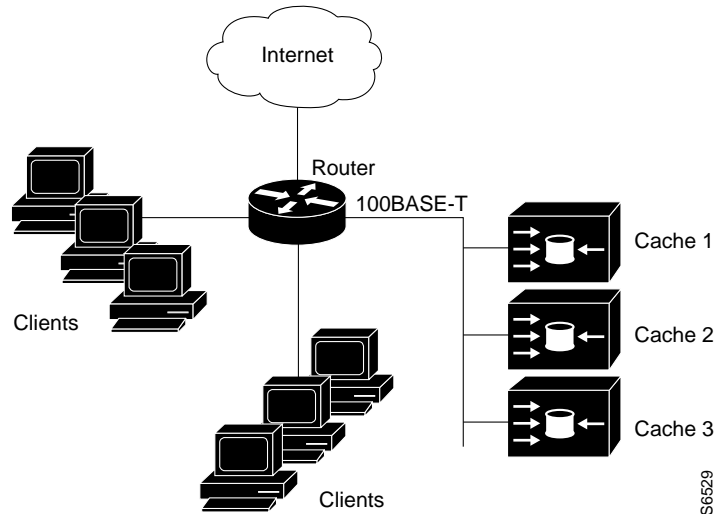
Multirouter Support

WCCP Version 2 enables a series of Content Engines, called a *Content Engine cluster*, to connect to multiple routers. This feature provides redundancy and a more distributed architecture for instances when a Content Engine needs to connect to a large number of interfaces. This strategy also has the benefit of keeping all the Content Engines in a single cluster, avoiding unnecessary duplication of web pages across several clusters.

How Version 1 Works

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

Figure B-1 Content Engine Network Configuration Using WCCP Version 1



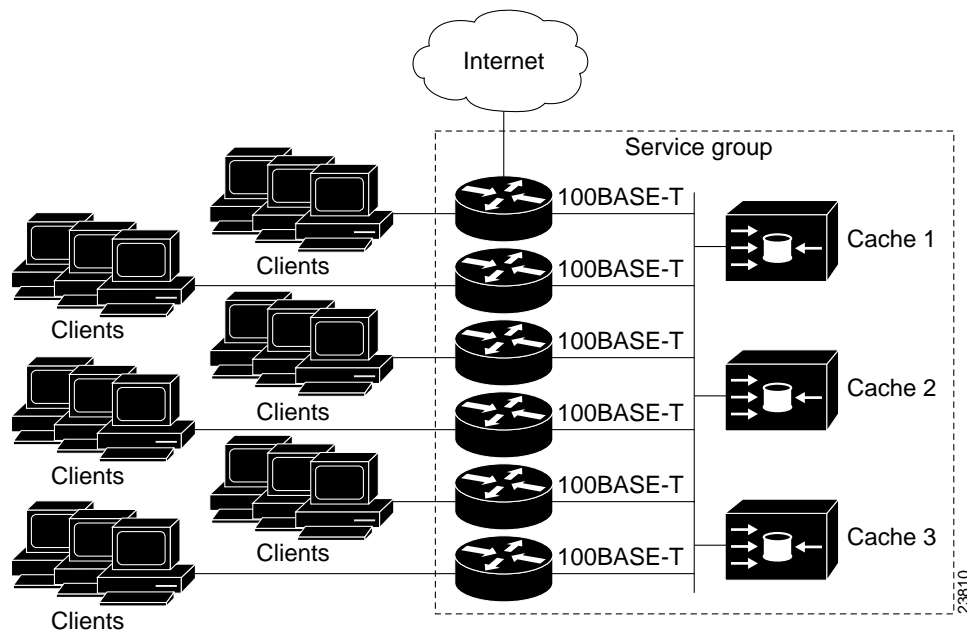
The following sequence of events details how this process works:

1. Each Content Engine records the IP address of the router servicing the cluster.
2. The Content Engines then transmit their IP addresses to the router, indicating their presence to one another in the cluster.
3. The router then replies to the Content Engines, establishing that each can connect to others in the cluster, and providing a *view* (a list) of Content Engine addresses in the cluster, indicating that all can recognize one another.
4. Once the view has been established, one Content Engine is designated the lead and indicates to the router how IP packet redirection should be performed. The lead Content Engine is defined as one seen by all the routers in the service group and that has the lowest IP address.

How Version 2 Works

With WCCP Version 2, multiple routers can service a cluster. This allows any of the available routers in a service group to redirect packets to each of the Content Engines in the cluster. [Figure B-2](#) illustrates how this configuration appears.

Figure B-2 Content Engine Network Configuration Using WCCP Version 2



You can configure the router to run one of the following cache-related services:

- Web cache—A global service that sends content to a large collection of destination World Wide Web servers
- Reverse proxy—A local service that sends content to a small number of destination World Wide Web servers
- Custom web cache—A service that permits routers to redirect HTTP traffic to Content Engines on a port other than port 80
- Dynamic web service—Service in which port numbers 90 to 97 can be configured to redirect traffic to the Content Engine

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.

Using WCCP Version 1, the Content Engines were configured with the address of the single router. WCCP Version 2 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 packets should be sent to a multicast address of 224.0.0.100, which in turn would send a multicast packet to all routers in the service group configured for group listening using WCCP. (See the **ip wccp group-listen** command for details.)

The multicast option is easier to configure because you have to specify only a single address on each Content Engine. This option also allows you to add and remove routers from a service group dynamically, without having to reconfigure the Content Engines with a different list of addresses each time.

The following sequence of events details how WCCP Version 2 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 the lead and sets the policy that the routers need to deploy in redirecting packets.

You must also perform these tasks to configure the routers that will become members of the service group:

- Configure an IP multicast address for use by the cluster.
- Enable the **ip wccp** command.

For network configurations in which the Content Engine sends to a target router a packet that needs to traverse an intervening router, the router being traversed must be configured to perform IP multicast routing. You must configure two components to enable traversal over an intervening router:

- Enable IP multicast routing using the **ip multicast routing** command.
- Enable the interfaces to which the Content Engines will connect to receive multicast transmissions using the **ip pim** command.

How Routers and Content Engines Communicate

Routers and Content Engines become aware of one another and form a service group using a management protocol. Once the service group has been established, one of the Content Engines is designated to determine load assignments among the Content Engines.

If there is a group of Content Engines, the one seen by all routers and the one that has the lowest IP address becomes the lead Content Engine. The role of this Content Engine is to determine how traffic should be allocated across Content Engines. The assignment information is passed to the entire service group from the designated Content Engine so that the routers of the group can redirect the packets properly and the Content Engines of the group can manage their load better.

Improved Security

WCCP Version 2 provides authentication that enables you to control which routers and Content Engines become part of the service group. You use passwords and the HMAC MD5 standard set by the **ip wccp [password [0-7] password]** command to control service group membership.

Faster Throughput

Cisco Express Forwarding (CEF) has been integrated into WCCP Version 2 and provides fast packet redirection.

Redirection for Multiple TCP Port-Destined Traffic

WCCP Version 2 enables more TCP ports to have traffic redirected to the Content Engine. Previously, web-cached information could be redirected only if it was destined for TCP port 80. Many applications require packets intended for other ports to be redirected, for example, proxy web cache handling, FTP caching, FTP proxy handling, web caching for ports other than 80, and RealAudio, video, and telephony applications.

Packets that the Content Engines do not service are tunneled back to the same router from which they were received. When a router receives a formerly redirected packet, it knows not to redirect it again.

The criteria for determining whether to redirect the traffic are:

- IP protocol
- Ports
- Priority
- Distribution scheme
- Default handling

Note that service information has been added to the protocol to indicate which service the WCCP messages refer to. This information is used to help verify that service group members are all using or providing the same service.

Web Cache Packet Return

WCCP Version 2 filters packets to determine which redirected packets have been returned from the Content Engine and which ones have not. It does not redirect the ones that have been returned, because the Content Engine has determined that the packets should not be cached. WCCP Version 2 returns packets that the Content Engine does not service to the same router from which they were transmitted. Typical reasons why a Content Engine would reject packets and initiate packet return are:

- The Content Engine is overloaded and has no room to service the packets.
- The Content Engine is filtering certain conditions that make caching packets counterproductive, for example, when IP authentication has been turned on.

Load-Distributing Applications

WCCP Version 2 has the capability to adjust the load being offered to individual Content Engines to provide more effective use of the resources available and at the same time help to ensure high quality of service to the clients. It uses three techniques to perform this task:

- Hot spot handling allows an individual hash bucket, or a pool of IP addresses to which routers are mapped, to be distributed across all the Content Engines.
- 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 Content Engines that have available capacity.
- Load shedding enables the router to selectively redirect the load to avoid exceeding the capacity of the Content Engines.

Client IP Address Transparency

The Content Engine accepts traffic and establishes the connection with the client, acting as if it were the original destination server. Once the connection is established, if the object being requested is not available on the Content Engine, the engine then establishes its own connection out to the original destination server.

Restrictions

The following limitations apply to WCCP Version 2:

- The Time To Live (TTL) value of routers servicing a cluster must be 15 seconds or less.
- The protocol needs to include the list of routers in the service group as part of its messages to properly depict the view.
- Because the messages may now be IP multicasted, 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 Content Engines and 32 routers.
- All Content Engines in a cluster must include all routers servicing the cluster in its configuration. If a Content Engine within a cluster does not include one or more of the routers in its configuration, the service group will detect the inconsistency and the Content Engine will not be allowed to operate within the service group.
- Multicast addresses must be between 224.0.0.0 and 239.255.255.255.
- WCCP works with IP networks only.

Related Documents

- *Cisco IOS Configuration Fundamentals Configuration Guide*
- *Cisco IOS Configuration Fundamentals Command Reference*

Prerequisites

Before you use WCCP Version 2, you must complete the following tasks:

- Properly install and configure a cache cluster connected to one or more routers.
- Configure IP on the interface connected to the Internet and the interface connected to the Content Engine. The interface connected to the Content Engine must be an Ethernet or Fast Ethernet interface.

Configuration Tasks

You can configure a router to run the web cache, custom web cache, and reverse proxy services associated with WCCP Version 2. The services can be configured simultaneously. Perform the following tasks to configure a cluster with multiple routers.

- [Configuring a Service Group Using WCCP Version 2, page B-8](#)
- [Running the Web Cache Service, page B-8](#)
- [Running the Reverse Proxy Service, page B-9](#)
- [Running a Custom Web Cache Service, page B-9](#)
- [Running a Dynamic Web Cache Service, page B-9](#)
- [Registering a Router to a Multicast Address, page B-9](#)
- [Informing a Router of Valid IP Addresses, page B-10](#)
- [Setting a Password for a Router and Content Engines, page B-10](#)
- [Disabling Caching for Certain Clients, page B-10](#)

Configuring a Service Group Using WCCP Version 2

	Command	Purpose
Step 1	Router(config)# ip wccp {web-cache service-number} [group-address groupaddress] [redirect-list access-list] [group-list access-list] [password [0-7] password]	Turns the WCCP feature on or off for the specified service.
Step 2	Router(config)# interface type number	Specifies an interface to configure and enters interface configuration mode.
Step 3	Router(config-if)# ip wccp {web-cache service-number} redirect {out in}	Enables WCCP redirection on the specified interface.
Step 4	Router(config-if)# ip wccp redirect exclude in	Allows inbound packets on this interface to be excluded from redirection.

Running the Web Cache Service

	Command	Purpose
Step 1	Router(config)# ip wccp web-cache	Turns on the protocol for web caching.
Step 2	Router(config)# interface type number	Specifies an interface for web caching.
Step 3	Router(config-if)# ip wccp web-cache redirect out	Enables the check on packets to determine whether they need to be redirected to a web cache.

Running the Reverse Proxy Service

	Command	Purpose
Step 1	Router(config)# ip wccp 99	Turns the WCCP feature on or off for the reverse proxy service. The service number for reverse proxy is 99.
Step 2	Router(config)# interface <i>type number</i>	Specifies an interface for the reverse proxy service.
Step 3	Router(config-if)# ip wccp 99 redirect out	Specifies “out” for the reverse proxy service.

Running a Custom Web Cache Service

	Command	Purpose
Step 1	Router(config)# ip wccp 98	Turns the WCCP feature on or off for the custom web cache service. The service number for custom web cache is 98.
Step 2	Router(config)# interface <i>type number</i>	Specifies an interface on which the custom web cache service will run.
Step 3	Router(config-if)# ip wccp 98 redirect out	Specifies “out” for the custom web cache service.

Running a Dynamic Web Cache Service

	Command	Purpose
Step 1	Router(config)# ip wccp 90	Turns the WCCP feature on or off for the generic web cache service. The service numbers for generic web cache services are 90 to 97.
Step 2	Router(config)# interface <i>type number</i>	Specifies an interface on which the reverse proxy service will run.
Step 3	Router(config-if)# ip wccp 90 redirect out	Specifies “out” for the custom web cache service.

Registering a Router to a Multicast Address

	Command	Purpose
Step 1	Router(config)# ip wccp web-cache group-address <i>groupipaddress</i>	Configures the group address for the service group.
Step 2	Router(config)# interface <i>type number</i>	Specifies an interface that will listen for the multicast address.
Step 3	Router(config-if)# ip wccp web-cache group-listen	Configures an interface on a router to enable or disable the reception of IP multicast packets for WCCP.

Informing a Router of Valid IP Addresses

	Command	Purpose
Step 1	Router(config)# ip wccp web-cache group-list access-list	Indicates to the router which Content Engine IP addresses to allow packets from.
Step 2	Router(config)# access-list <i>access-list number</i> permit host <i>host-address</i>	Creates an access list that enables or disables traffic redirection to the Content Engine.

Setting a Password for a Router and Content Engines

	Command	Purpose
Step 1	Router(config)# ip wccp web-cache password [0-7] <i>password</i>	Sets a password for the Content Engine that the router is trying to access.

Disabling Caching for Certain Clients

	Command	Purpose
Step 1	Router(config)# ip wccp web-cache redirect-list <i>access-list number</i>	Sets the access list used to enable redirection.
Step 2	Router(config)# access-list <i>access-list number</i> deny host <i>host-address</i>	Creates an access list that enables or disables traffic redirection to the Content Engine.

Verifying WCCP Configuration Settings

Step 1 To view the configuration, enter the **show running-config** command.

A sample configuration follows:

```

Console# show 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.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 Ethernet0
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 Ethernet1
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
```

- Step 2** To view values associated with WCCP variables, enter the **show ip wccp** command. Output similar to the following is displayed:

```

Console# show ip wccp

Global WCCP Information:
Service Name: web-cache:
Number of Content Engines:1
Number of Routers:1
Total Packets Redirected:213
Redirect access-list:no_linux
Total Packets Denied Redirect:88
Total Packets Unassigned:-none-
Group access-list:0
Total Messages Denied to Group:0
Total Authentication failures:0

Service Name: 99
Number of Content Engines:1
Number of Routers:2
Total Packets Redirected:198
Redirect access-list:-none-
Total Packets Denied Redirect:0
Total Packets Unassigned:0
Group access-list:11
Total Messages Denied to Group:0
Total Authentication failures:0

```

Monitoring and Maintaining WCCP Version 2

Command	Purpose
Router# show ip wccp	Displays global statistics related to WCCP.
or	
Router# show ip wccp {web-cache 99}	Queries the router for information about which Content Engines the router has detected in a specific service group. The information can be displayed for either a web cache or the reverse proxy service, which is indicated by a value of 99.
Router# show ip wccp {web-cache 99} detail	
Router# show ip interface	Shows whether any ip wccp direct commands are configured on an interface.
Router# show ip wccp {web-cache 99} view	Displays which devices in a particular service group have been detected and which Content Engines are not visible to all other routers to which the current router is connected. The information can be displayed for either a web cache or the reverse proxy service, which is indicated by a value of 99.

Configuration Examples

This section provides the following configuration examples:

- [Performing a General WCCP Version 2 Configuration, page B-13](#)
- [Running the Web Cache Service, page B-13](#)
- [Running the Reverse Proxy Service, page B-13](#)
- [Running the Custom Web Cache Service, page B-14](#)
- [Running a Generic Web Cache Service, page B-14](#)
- [Registering a Router to a Multicast Address, page B-14](#)
- [Informing a Router of Valid IP Addresses, page B-14](#)
- [Setting a Password for a Router and Content Engines, page B-14](#)
- [Bypassing the Cache with Router Access Lists, page B-15](#)
- [Displaying WCCP Settings, page B-15](#)

Performing a General WCCP Version 2 Configuration

The following example shows a general WCCP Version 2 configuration session:

```
ip wccp web-cache group-address 224.1.1.100 password alabama1
interface ethernet0
ip wccp web-cache redirect out
```

Running the Web Cache Service

The following example shows a web cache service configuration session:

```
configure terminal
ip wccp web-cache
interface ethernet 0
ip wccp web-cache redirect out
```

Running the Reverse Proxy Service

The following example shows a reverse proxy service configuration session:

```
configure terminal
ip wccp 99
interface ethernet 0
ip wccp 99 redirect out
```

Running the Custom Web Cache Service

The following example shows a custom web cache configuration session:

```
configure terminal
ip wccp 98
interface ethernet 0
ip wccp 98 redirect out
```

Running a Generic Web Cache Service

The following example shows a generic web cache configuration session:

```
configure terminal
ip wccp 91
interface ethernet 0
ip wccp 91 redirect out
```

Registering a Router to a Multicast Address

The following example shows how to register a router to a multicast address of 192.168.0.0:

```
configure terminal
ip wccp web-cache group-address 172.168.0.0
interface ethernet 0
ip wccp web-cache group-listen
```

Informing a Router of Valid IP Addresses

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

```
configure terminal
access-list 10 permit host 10.1.1.1
access-list 10 permit host 10.1.1.2
access-list 10 permit host 10.1.1.3
ip wccp web-cache group-list 10
```

Setting a Password for a Router and Content Engines

The following example shows a WCCP Version 2 password configuration session in which the password is alabama2:

```
configure terminal
ip wccp web-cache password alabama2
```

Bypassing the Cache with Router Access Lists

The router can be configured with access lists to permit or deny redirection of traffic to the Content Engine. In the following example, traffic conforming to the following criteria is not redirected by the router to the Content Engine:

- Originating from the host 10.1.1.1 destined for any other host
- Originating from any host destined for the host 10.255.1.1

```
router# configure terminal
router(config)# ip wccp web-cache redirect-list 120
router(config)# access-list 120 deny ip host 10.1.1.1 any
router(config)# access-list 120 deny ip any host 10.255.1.1
router(config)# access-list 120 permit ip any any
```

Traffic not explicitly permitted is implicitly denied redirection.

The `access-list 120 permit ip any any` command explicitly permits all traffic (from any source en route to any destination) to be redirected to the Content Engine. Because criteria matching occurs in the order by which the commands are entered, the global permit command is the last command entered. For further information on access lists, refer to Cisco IOS software documentation.

Displaying WCCP Settings

The following example displays WCCP settings, using the `show running-config` command:

```
Console# show 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.KuCxZNT1
enable password alabamal
!
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 Ethernet0
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 Ethernet1
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

```

Command Reference

This section documents new or modified commands that configure the WCCP Version 2 feature.

- [clear ip wccp](#)
- [ip wccp](#)
- [ip wccp group-listen](#)
- [ip wccp redirect exclude in](#)
- [ip wccp redirect](#)
- [ip wccp version](#)
- [show ip interface](#)
- [show ip wccp](#)

In Cisco IOS Release 12.0(1)T or a later version of Release 12.0 T, you can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (|), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search or filter on:

```
command | { begin | include | exclude } regular-expression
```

Following is an example of the **show atm vc** command in which you want the command output to begin with the first line where the expression “PeakRate” appears:

```
show atm vc | begin PeakRate
```

For more information on the search and filter functionality, refer to the Cisco IOS Release 12.0(1)T feature module titled *CLI String Search*.

clear ip wccp

To remove Web Cache Communication Protocol (WCCP) statistics maintained on the router either for a particular service or for all the services, use the **clear ip wccp** EXEC command.

```
clear ip wccp { web-cache | service-number }
```

Syntax Description	web-cache	Directs the router to remove statistics for the web cache service.
	<i>service-number</i>	Directs the router to remove statistics for a specified web cache service. The number can be from 0 to 99. The reverse proxy service is indicated by a value of 99.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	11.1 CA	This command was introduced.
	11.2 P	This command was introduced.
	12.0(3)T	This command has been expanded to be explicit about service.

Usage Guidelines Use the **show ip wccp** and **show ip wccp detail** commands to display WCCP statistics.

Examples

```
clear ip wccp web cache
```

Related Commands	Command	Description
	ip wccp	Directs a router to enable or disable the support for a service group.
	show ip wccp	Displays global statistics related to the WCCP feature.

ip wccp

To direct a router to enable or disable the support for a Content Engine service group, use the **ip wccp** global configuration command. To remove the ability of a router to control support for a service group, use the **no** form of this command.

```
ip wccp { web-cache | service-number } [group-address groupaddress] [redirect-list access-list]
[group-list access-list] [password [0-7] password]
```

```
no ip wccp { web-cache | service-number } [group-address groupaddress] [redirect-list
access-list] [group-list access-list] [password [0-7] password]
```

Syntax Description

web-cache	Enables the web cache service.
<i>service-number</i>	Identification number of the Web Cache Communication Protocol (WCCP) service being controlled by a router. The number can be from 0 to 99. The reverse proxy service is indicated by a value of 99.
group-address	(Optional.) Directs the router to use a specified multicast IP address for communication with the WCCP service group.
<i>groupaddress</i>	(Optional.) Multicast address used by the router to determine which Content Engine should receive redirected messages.
redirect-list	(Optional.) Directs the router to use an access list to control traffic redirected to this service group.
<i>access-list</i>	(Optional.) String (not to exceed 64 characters) that is the name of the access list that determines which traffic is redirected to a Content Engine.
group-list	(Optional.) Directs the router to use an access list to determine which Content Engines are allowed to participate in the service group.
<i>access-list</i>	(Optional.) String (not to exceed 64 characters) that is the name of the access list that determines which Content Engines are allowed to participate in the service group.
password	(Optional.) String that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. Messages that are not accepted by the authentication are discarded.
<i>0-7</i>	(Optional.) Value that indicates the HMAC MD5 algorithm used to encrypt the password. This value is generated when an encrypted password is created for the Content Engine.
<i>password</i>	(Optional.) Password name that is combined with the HMAC MD5 value to create security for the connection between the router and the Content Engine.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.

Examples

The following example shows a router configured to run WCCP reverse proxy service, using (listening to) the multicast address 172.168.0.0:

```
ip wccp 99 group-address 172.168.0.0
```

Related Commands

Command	Description
ip wccp group-listen	Configures an interface on a router to enable or disable the reception of IP multicast packets for the WCCP feature.

ip wccp group-listen

To configure an interface on a router to enable or disable the reception of IP multicast packets for the Web Cache Communication Protocol (WCCP) feature, use the **ip wccp group-listen** interface configuration command. To remove control of the reception of IP multicast packets for the WCCP feature, use the **no** form of this command.

ip wccp {web-cache | service-number} group-listen

no ip wccp {web-cache | service-number} group-listen

Syntax Description	web-cache	Directs the router to transmit packets to the web cache service.
	<i>service-number</i>	Identification number of the Content Engine service group being controlled by a router. The number can be from 0 to 99. The reverse proxy service is indicated by a value of 99.

Defaults This command is disabled by default.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Examples The following example shows that multicast packets have been enabled for a web cache with an address of 192.168.0.0.

```
configure terminal
ip wccp web-cache group-address 192.168.0.0
interface ethernet 0
ip wccp web cache group-listen
```

Related Commands	Command	Description
	ip wccp	Directs a router to enable or disable the support for a service group.
	ip wccp redirect out	Configures an interface to enable or disable the exclusion of a redirection check for packets that were received on the interface.

ip wccp redirect exclude in

To configure an interface to enable or disable excluding packets received on an interface from being redirected to a Content Engine, use the **ip wccp redirect exclude in** interface configuration command. To disable a router's ability to verify that only appropriate packets are being redirected to a Content Engine, use the **no** form of this command.

ip wccp redirect exclude in

no ip wccp redirect exclude in

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Interface configuration

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines Note that the command is global to all the services and should be applied to any inbound interface that has been configured to be excluded from redirection on an outbound interface that the traffic will traverse.

Examples

```
configure terminal
ip wccp 99
interface ethernet0
ip wccp redirect exclude in
```

Related Commands	Command	Description
	ip wccp	Directs a router to enable or disable the support for a service group.
	ip wccp redirect out	Configures an interface to enable or disable the exclusion of a redirection check for packets that were received on the interface.

ip wccp redirect

To enable packet redirection on an outbound or inbound interface using Web Cache Communication Protocol (WCCP), use the **ip wccp redirect** interface configuration command. To disable WCCP redirection, use the no form of this command.

```
ip wccp { web-cache | service-number } redirect { out | in }
```

```
no ip wccp { web-cache | service-number } redirect { out | in }
```

Syntax Description

web-cache	Enables the web cache service.
<i>service-number</i>	Identification number of the Content Engine service group being controlled by a router. The number can be from 0 to 99. The reverse proxy service is indicated by a value of 99.
redirect	Enables packet redirection checking on an outbound or inbound interface.
out	Specifies packet redirection on an outbound interface.
in	Specifies packet redirection on an inbound interface.

Defaults

Redirection checking on the interface is disabled.

Command Types

Interface configuration

Usage Guidelines

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 translates into faster redirection of packets.



Note This command has the potential to affect the **ip wccp redirect exclude in** command. If you have **ip wccp redirect exclude in** set on an interface and you subsequently configure the **ip wccp redirect in** command, the **exclude in** command is overridden. The opposite is also true: configuring the **exclude in** command overrides the **redirect in** command.

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(11)S	The in keyword was added to the 12.0 S release train
12.1(3)T	The in keyword was added to the 12.1 T release train

Examples

The following example shows a configuration session in which reverse proxy packets on Ethernet interface 0 are being checked for redirection and redirected to a Cisco Content Engine:

```
Router# configure terminal
Router(config)# ip wccp 99
Router(config)# interface ethernet 0
Router(config-if)# ip wccp 99 redirect out
```

The following example shows a configuration session in which HTTP traffic arriving on interface 0/1 is redirected to a Cisco Cache Engine:

```
Router# configure terminal
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/1
Router(config-if)# ip wccp web-cache redirect in
```

Related Commands

Command	Description
ip wccp redirect exclude in	Configures an interface to enable or disable excluding packets received on an interface from being cached.

ip wccp version

To configure the WCCP version number, use the **ip wccp version** global configuration command. The default WCCP version is Version 2. Use this command to override the default.

ip wccp version { 1 | 2 }

Syntax	Description
1	Enables WCCP Version 1
2	Enables WCCP Version 2

Defaults The default is Version 2.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Examples `ip wccp version 1`

show ip interface

To display status about any **ip wccp direct** commands configured on an interface, use the **show ip interface EXEC** command.

```
show ip interface [type-number]
```

Syntax Description	<i>type-number</i> (Optional.) The interface number whose status is being displayed.
---------------------------	--

Defaults	No default behavior or values
-----------------	-------------------------------

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	10.0	This command was introduced.
	12.0	This command was enhanced.
	12.0(3)T	This command was enhanced to include status of ip wccp redirect out and ip wccp redirect exclude in commands.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable. A usable interface is one through which the software can send and receive packets. If the software determines that an interface is not usable, it removes the directly connected routing entry from the routing table. Removing the entry allows the software to use dynamic routing protocols to determine backup routes to the network (if any).

If the interface can provide two-way communication, the line protocol is indicated to be up. If the interface hardware is usable, the interface is indicated to be up.

If you specify an optional interface type, you will see information on that specific interface only.

If you specify no optional arguments, you will see information on all the interfaces.

When an asynchronous interface is encapsulated with Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

Examples

The following example displays output from the **show ip interface** command, using the interface e3/0:

```
show ip interface e3/0

Ethernet3/0 is up
Internet address is 17.1.1.38/24
Broadcast address is 255.255.255.255
Address determined by non-volatile memory
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is enabled
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
Split horizon is enabled
ICMP redirects are always sent
ICMP unreachable are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP fast switching on the same interface is disabled
IP Optimum switching is enabled
IP multicast fast switching is enabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Gateway Discovery is disabled
Policy routing is disabled
Network address translation is disabled
WCCP Redirect outbound is enabled
WCCP Redirect exclude is disabled
```

Table B-1 describes the fields shown in the display.

Table B-1 Field Descriptions—*show ip interface* Command

Field	Description
Ethernet 3/0 is up	Indicates the status of an interface. If the interface hardware is usable, the interface is marked “up.” For an interface to be usable, both the interface hardware and line protocol must be up.
Internet address	Shows the IP address of the interface.
Broadcast address	Shows the broadcast address.
Address determined by	Indicates how the IP address of the interface was determined.
MTU	Shows the maximum transmission unit (MTU), or the maximum size of packets allowed to be transmitted from the router to a Content Engine.
Helper address	Shows a helper address, if one has been set.
Directed broadcast forwarding	Shows a secondary address, if one has been set.
Outgoing access list	Indicates whether the interface has an outgoing access list set.
Inbound access list	Indicates whether the interface has an incoming access list set.
Proxy ARP	Specifies the IP Security Option (IPSO) security level set for this interface.

Table B-1 Field Descriptions—*show ip interface Command (continued)*

Field	Description
Security level	Specifies the default IPSO security level for this interface.
Split horizon	Specifies that routing updates sent to a particular neighbor router should not contain information about routes that were learned from that neighbor.
ICMP redirects	Indicates whether Internet Control Message Protocol (ICMP) redirects will be sent on this interface.
ICMP unreachable	Indicates whether unreachable messages will be sent on this interface.
ICMP mask replies	Specifies whether mask replies will be sent on this interface.
IP fast switching	Indicates whether fast switching has been enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP fast switching on the same interface	Indicates whether fast switching has been disabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Optimum switching	Indicates whether the IP optimum switching feature has been turned on.
IP multicast fast switching	Indicates whether the IP multicast fast switching feature has been turned on.
Router Discovery	Indicates whether the Cisco Discovery Protocol has been turned off.
IP output packet accounting	Indicates whether the output packet counter has been turned off.
IP access violation accounting	Indicates whether the feature that counts unauthorized access events on the router has been turned off.
TCP/IP header compression	Indicates whether compression is enabled or disabled.
Probe proxy name replies	Indicates whether HP Probe proxy name replies are generated.
Gateway Discovery	Indicates whether the gateway discovery option has been turned off.
Policy routing	Indicates whether the policy routing option has been turned off.
Network address translation	Indicates whether the status of the network address translation feature has been enabled or disabled.
WCCP Redirect outbound	Indicates whether packets received on an interface are redirected to a Content Engine. This field can be enabled or disabled.
WCCP Redirect exclude	Indicates whether packets targeted for an interface will be excluded from being redirected to a Content Engine. This field can be enabled or disabled.

Related Commands

Command	Description
show ip wccp	Displays global statistics related to the Web Cache Communication Protocol feature.

show ip wccp

To display global statistics related to the Web Cache Communication Protocol (WCCP) feature, use the **show ip wccp** EXEC command.

```
show ip wccp { web-cache | service-number } [view | detail]
```

Syntax Description	web-cache	Directs the router to display statistics for the web cache service.
	<i>service-number</i>	Identification number of the Content Engine service group being controlled by a router. The number can be from 0 to 99. The reverse proxy service is indicated by a value of 99. The custom web cache is indicated by a value of 98.
	view	(Optional.) Directs the router to display statistics for the WCCP view configuration.
	detail	(Optional.) Directs the router to display statistics for the WCCP detail configuration.

Defaults No default behavior or values

Command Modes EXEC

Command History	Release	Modification
	11.1 CA and 11.2 P	This command was introduced.
	12.0(3)T	The user was allowed to query the router for the current global configuration information in use by either a single service or all services.

Usage Guidelines Use the **clear ip wccp** command to reset the counter for the “Packets Redirected” information.

Examples

The following example displays output from the **show ip wccp** command:

```
show ip wccp

Global WCCP Information:
Service Name: web-cache:
Number of Content Engines:1
Number of Routers:1
Total Packets Redirected:213
Redirect access-list: no_linux
Total Packets Denied Redirect:88
Total Packets Unassigned:-none-
Group access-list:0
Total Messages Denied to Group:0
Total Authentication failures:0

Service Name: 1
Number of Content Engines:1
Number of Routers:2
Total Packets Redirected:198
Redirect access-list:-none-
Total Packets Denied Redirect:0
Total Packets Unassigned:0
Group access-list:11
Total Messages Denied to Group:0
Total Authentication failures:0
```

[Table B-2](#) describes the fields shown in the display.

Table B-2 *Field Descriptions—show ip wccp Command*

Field	Description
Service Name	Service that is detailed in the display output.
Number of Content Engines	Number of Content Engines using the router as their home router.
Number of Routers	Number of routers in the service group.
Total Packets Redirected	Total number of packets redirected by the router.
Redirect access-list	Name or number of the access list that determines which packets will be redirected.
Total Packets Denied Redirect	Total number of packets that were not redirected because they did not match the access list.
Total Packets Unassigned	Number of packets that were not redirected because they were not assigned to any Content Engine. Packets may not be assigned during initial discovery of Content Engines or when a Content Engine is dropped from a cluster.
Group access-list	Content Engine that is allowed to connect to the router.
Total Messages Denied to Group	Number of messages disallowed by the router because they did not meet all the requirements of the service group.
Total Authentication failures	Number of password authentication failures.

The following example displays output from the **show ip wccp web-cache detail EXEC** command. This command displays Content Engine and WCCP router statistics for a particular service group:

```
show ip wccp web-cache detail
```

```
WCCP Router information:
IP Address 172.31.88.10
Protocol Version:2.0

WCCP Cache-Engine Information
IP Address:172.31.88.11
Protocol Version:2.0
State:Usable
Initial Hash Info:AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAA
Assigned Hash Info:FFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFF
Hash Allotment:256 (100.00%)
Packets Redirected:21345
Connect Time:00:13:46
```

Table B-3 describes the fields shown in the display.

Table B-3 Field Descriptions—show ip wccp web-cache detail Command

Field	Description
WCCP Router information	Header for the area that contains fields for the IP address and version of WCCP associated with the router connected to the Content Engine in the service group.
IP Address	IP address of the router connected to the Content Engine in the service group.
Protocol Version	Version of WCCP being used by the router in the service group.
WCCP Cache-Engine information	Fields for information on Content Engines.
IP Address	IP address of the Content Engine in the service group.
Protocol Version	Version of WCCP being used by the Content Engine in the service group.
State	Indicates whether the Content Engine is operating properly and can be contacted by a router and other Content Engines in the service group.
Initial Hash Info	Initial state of the hash bucket assignment.
Assigned Hash Info	Current state of the hash bucket assignment.
Hash Allotment	Percentage of buckets assigned to the current Content Engine. Both a value and a percentage figure are displayed.
Packets Redirected	Number of packets that have been redirected to the Content Engine.
Connect Time	Length of time the Content Engine has been connected.

■ show ip wccp

The following is sample output from the **show ip wccp view EXEC** command. In this case, the service number 1 has been specified.

```
show ip wccp service 1 view
```

```
WCCP Router Informed of:
```

```
192.168.88.10
```

```
192.168.88.20
```

```
WCCP Content Engines Visible
```

```
192.168.88.11
```

```
192.168.88.12
```

```
WCCP Content Engines Not Visible:
```

```
-none-
```

If any Content Engine is displayed under the WCCP Content Engines Not Visible field, the Content Engine needs to be reconfigured to add this router to it.

[Table B-4](#) describes the fields shown in the display.

Table B-4 *Field Descriptions—show ip wccp service Command*

Field	Description
WCCP Routers Informed of	List of routers detected by the current router.
WCCP Content Engines Visible	List of Content Engines that are visible to the router and other Content Engines in the service group.
WCCP Content Engines Not Visible	List of Content Engines in the service group that are not visible to the router and other Content Engines in the service group.

Related Commands

Command	Description
ip wccp detail	Directs a router to enable or disable the support for a service group.