



Configuring WCCP

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

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

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

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

- [Finding Feature Information, page 1](#)
- [Prerequisites for WCCP, page 2](#)
- [Restrictions for WCCP, page 2](#)
- [Information About WCCP, page 4](#)
- [How to Configure WCCP, page 16](#)
- [Configuration Examples for WCCP, page 28](#)
- [Additional References, page 32](#)
- [Feature Information for WCCP, page 33](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for WCCP

- To use WCCP, IP must be configured on the interface connected to the Internet and another interface must be connected to the content engine.
- The interface connected to the content engine must be a Fast Ethernet or Gigabit Ethernet interface.
- Only Catalyst 6500 series switches with a PFC4 support the following hardware capabilities:
 - WCCP generic routing encapsulation (GRE) decapsulation in hardware
 - WCCP Egress Mask assignment in hardware
 - WCCP Exclude capability in hardware

Restrictions for WCCP

General

The following limitations apply to Web Cache Communication Protocol version1 (WCCPv1) and WCCP version 2 (WCCPv2):

- WCCP works only with IPv4 networks.
- WCCP bypasses Network Address Translation (NAT) when Cisco Express Forwarding is enabled.
- WCCP interoperability with Network Address Translation (NAT) in conjunction with Zone-Based Firewall (ZBF) is not supported.

WCCPv1

The following limitations apply to WCCPv1:

- WCCPv1 supports the redirection of HTTP (TCP port 80) traffic only.
- WCCPv1 does not allow multiple routers to be attached to a cluster of content engines.

WCCPv2

The following limitations apply to WCCPv2:

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

WCCP VRF Support

In Cisco IOS Release 12.2(33)SRE, this feature is supported only on Cisco 7200 NPE-G2 and Cisco 7304-NPE-G100 routers.

This feature is supported in Cisco IOS Release 12.2(50)SY on Catalyst 6000 series switches with a PFC4.

Layer 2 Forwarding and Return

The following limitations apply to WCCP Layer 2 Forwarding and Return:

In a Cisco Wide Area Application Services (WAAS) and Cisco IOS XE firewall configuration, all packets processed by a Wide Area Application Engine (WAE) device must go over the Cisco IOS XE firewall in both directions to support the Web Cache Coordination Protocol (WCCP) generic routing encapsulation (GRE) redirect. This situation occurs when a Layer 2 redirect is not available. If a Layer 2 redirect is configured on the WAE, the system defaults to the GRE redirect to continue to function.

The client device and a WAE device or a cache engine cannot be connected to a Cisco device with the same interface and WCCP redirect configured on the interface.

The following two configurations are supported:

- 1 For WCCP Layer 2 return, the client and WAE are connected to a Cisco device with same interface and WCCP output is configured on the interface.
- 2 For WCCP Layer 2 return, the client and WAE are connected to a Cisco device with same physical interface but in different VLANs and sub-interfaces.

Cisco Catalyst 4500 Series Switches

The following limitations apply to Cisco Catalyst 4500 series switches:

- Catalyst 4500 series switches do not support WCCPV1.
- Up to eight service groups are supported at the same time on the same client interface.
- The Layer 2 (L2) rewrite forwarding method is supported, but generic routing encapsulation (GRE) is not.
- Direct L2 connectivity to content engines is required; Layer 3 (L3) connectivity of one or more hops away is not supported.
- Ternary content addressable memory (TCAM) friendly mask-based assignment is supported, but the hash bucket-based method is not.
- Redirect ACL for WCCP on a client interface is not supported.
- Incoming traffic redirection on an interface is supported, but outgoing traffic redirection is not.
- When TCAM space is exhausted, traffic is not redirected; it is forwarded normally.
- The WCCP version 2 standard allows for support of up to 256 distinct masks. However, a Catalyst 4500 series switch supports only mask assignment tables with a single mask.

Cisco Catalyst 6500 Series Switches

The following limitation apply to Cisco Catalyst 6500 series switches:

- With a Policy Feature Card 2 (PFC2), Cisco IOS Release 12.2(17d)SX and later releases support WCCP.

- With a PFC3, Cisco IOS Release 12.2(18)SXD1 and later releases support WCCP.
- With a PFC4, Cisco IOS Release 12.2(50)SY and later releases support WCCP and introduce support for WCCP GRE decapsulation, WCCP mask assignment, and WCCP exclude capability in hardware.
- To use the WCCP Layer 2 PFC redirection feature, configure WCCP on the Catalyst 6500 series switch and configure accelerated WCCP on the cache engine as described in the [Transparent Caching](#) document.
- Cisco Application and Content Networking System (ACNS) software releases later than Release 4.2.2 support WCCP Layer 2 Policy Feature Card (PFC) redirection hardware acceleration.
- A content engine configured for mask assignment that tries to join a farm where the selected assignment method is hash remains out of the farm as long as the cache engine assignment method does not match that of the existing farm.
- When WCCP Layer 2 PFC redirection is the forwarding method for a service group, the packet counters in the `show ip wccp service-number` command output display flow counts instead of packet counts.

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

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

The following restrictions apply to the redirect-list ACL:

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

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

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

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

Information About WCCP

WCCP Overview

WCCP uses Cisco Content Engines (or other content engines running WCCP) to localize web traffic patterns in the network, enabling content requests to be fulfilled locally. Traffic localization reduces transmission costs and download time.

WCCP enables routing platforms to transparently redirect content requests. The main benefit of transparent redirection is that users need not configure their browsers to use a web proxy. Instead, they can use the target URL to request content, and have their requests automatically redirected to a content engine. The word

"transparent" in this case means that the end user does not know that a requested file (such as a web page) came from the content engine instead of from the originally specified server.

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

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

Layer 2 Forwarding Redirection and Return

WCCP uses either generic routing encapsulation (GRE) or Layer 2 (L2) to redirect or return IP traffic. When WCCP forwards traffic via GRE, the redirected packets are encapsulated within a GRE header. The packets also have a WCCP redirect header. When WCCP forwards traffic using L2, the original MAC header of the IP packet is overwritten and replaced with the MAC header for the WCCP client.

Using L2 as a forwarding method allows direct forwarding to the content engine without further lookup. Layer 2 redirection requires that the router and content engines are directly connected, that is, on the same IP subnetwork.

When WCCP returns traffic via GRE, the returned packets are encapsulated within a GRE header. The destination IP address is the address of the router and the source address is the address of the WCCP client. When WCCP returns traffic via L2, the original IP packet is returned without any added header information. The router to which the packet is returned will recognize the source of the packet and prevent redirection.

The WCCP redirection method does not have to match the return method.

L2 forwarding, return, or redirection are typically used for hardware-accelerated platforms. Depending on your release, L2 forwarding, return, and redirection can also be used for software-switching platforms.

On Cisco ASR 1000 Series Aggregation Services Routers, both the GRE and L2 forward and return methods use the hardware. Therefore, there is no significant performance degradation between them.

For content engines running Application and Content Networking System (ACNS) software, use the **wccp custom-web-cache** command with the **l2-redirect** keyword to configure L2 redirection. For content engines running Cisco Wide Area Application Services (WAAS) software, use the **wccp tcp-promiscuous** command with the **l2-redirect** keyword to configure L2 redirection.



Note

Before configuring a GRE tunnel, configure a loopback interface (that is not attached to a VRF) with an IP address so that the internally created tunnel interface is enabled for IPv4 forwarding by unnumbering itself to this dummy loopback interface. You do not need to configure a loopback interface if the system has at least one interface that is not attached to a VRF and that is configured with an IPv4 address.

For information about Cisco ACNS commands used to configure Cisco Content Engines, see the [Cisco ACNS Software Command Reference](#).

For more information about WAAS commands used to configure Cisco Content Engines, see the [Cisco Wide Area Application Services Command Reference](#).

WCCP Mask Assignment

The WCCP Mask Assignment feature enables mask assignment as the load-balancing method (instead of the default hash assignment method) for a WCCP service.

For content engines running Application and Content Networking System (ACNS) software, use the **wccp custom-web-cache** command with the **mask-assign** keyword to configure mask assignment. For content engines running Cisco Wide Area Application Services (WAAS) software, use the **wccp tcp-promiscuous** command with the **mask-assign** keyword to configure mask assignment.

For information about Cisco ACNS commands used to configure Cisco Content Engines, see the [Cisco ACNS Software Command Reference](#).

For more information about WAAS commands used to configure Cisco Content Engines, see the [Cisco Wide Area Application Services Command Reference](#).

Hardware Acceleration

Catalyst 6500 series switches and Cisco 7600 series routers provide WCCP Layer 2 Policy Feature Card (PFC) redirection hardware acceleration. Hardware acceleration allows Cisco Content Engines to perform a L2 MAC address rewrite redirection method when directly connected to a compatible switch or router.

Redirection processing is accelerated in the switching or routing hardware, which is more efficient than L3 redirection with Generic Routing Encapsulation (GRE). L2 redirection takes place on the switch or router, and is not visible to the Multilayer Switch Feature Card (MSFC). The WCCP L2 PFC redirection feature requires no configuration on the MSFC. The **show ip wccp {service-number | web-cache} detail** command displays which redirection method is in use for each content engine.

In order for the router or switch to make complete use of hardware redirection, the content engine must be configured with L2 redirection and mask assignment.

Use the **ip wccp web-cache accelerated** command on hardware-based platforms to enforce the use of L2 redirection and mask assignment. Using this command configures the router to form a service group and redirect packets with an appliance only if the appliance is configured for L2 and mask assignment.

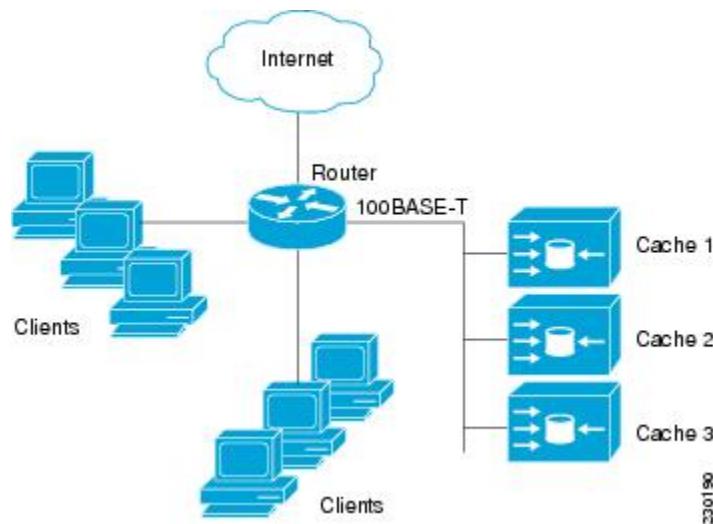
The following guidelines apply to WCCP Layer 2 PFC redirection:

- 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.
- L2 redirection takes place on the PFC and is not visible to the MSFC. The **show ip wccp {service-number | web-cache} detail** command on the MSFC displays statistics for only the first packet of an L2 redirected flow, which provides an indication of how many flows, rather than packets, are using L2 redirection. You can view information about L2 redirected flows by entering the **show platform flow ip** command. The PFC3 provides hardware acceleration for GRE. If you use WCCP Layer 3 redirection with GRE, there is hardware support for encapsulation, but the PFC3 does not provide hardware support for decapsulation of WCCP GRE traffic.

WCCPv1 Configuration

With WCCPv1, only a single router services a cluster. In this scenario, this router is the device that performs all the IP packet redirection. The figure below illustrates the WCCPv1 configuration.

Figure 1: WCCPv1 Configuration



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

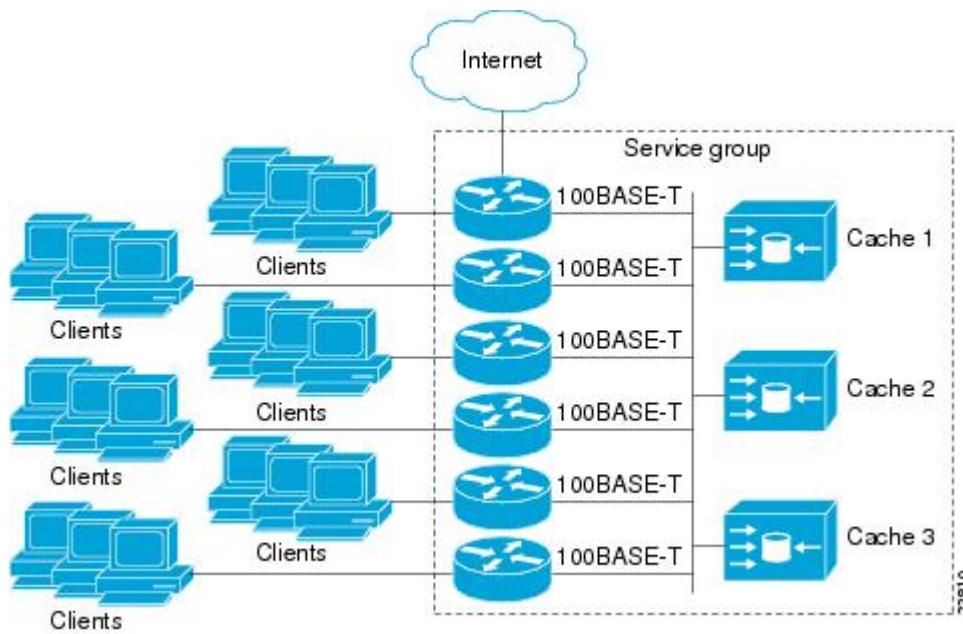
The following sequence of events details how WCCPv1 configuration works:

- 1 Each content engine is configured by the system administrator with the IP address of the control router. Up to 32 content engines can connect to a single control router.
- 2 The content engines send their IP addresses to the control router using WCCP, indicating their presence. Routers and content 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 content engine in the cluster, essentially making all the content 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 When a stable view has been established, one content engine is elected as the lead content engine. (The lead is defined as the content engine seen by all the content engines in the cluster with the lowest IP address). This lead content engine uses WCCP to indicate to the control router how IP packet redirection should be performed. Specifically, the lead content engine designates how redirected traffic should be distributed across the content engines in the cluster.

WCCPv2 Configuration

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

Figure 2: Cisco Content Engine Network Configuration Using WCCPv2



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

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

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

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

The following sequence of events details how WCCPv2 configuration works:

- 1 Each content engine is configured with a list of routers.

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

WCCPv2 Support for Services Other Than HTTP

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

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

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

WCCPv2 Support for Multiple Routers

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

WCCPv2 MD5 Security

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

WCCPv2 Web Cache Packet Return

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

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

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

WCCPv2 Load Distribution

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

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

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

WCCP Mask Assignment

The WCCP Mask Assignment feature enables mask assignment as the load-balancing method (instead of the default hash assignment method) for a WCCP service.

For content engines running Application and Content Networking System (ACNS) software, use the **wccp custom-web-cache** command with the **mask-assign** keyword to configure mask assignment. For content engines running Cisco Wide Area Application Services (WAAS) software, use the **wccp tcp-promiscuous** command with the **mask-assign** keyword to configure mask assignment.

For information about Cisco ACNS commands used to configure Cisco Content Engines, see the [Cisco ACNS Software Command Reference](#).

For more information about WAAS commands used to configure Cisco Content Engines, see the [Cisco Wide Area Application Services Command Reference](#).

WCCP VRF Support

The WCCP VRF Support feature enhances the WCCPv2 protocol by implementing support for virtual routing and forwarding (VRF).

The WCCP VRF Support feature allows service groups to be configured on a per-VRF basis in addition to those defined globally.

Along with the service identifier, the VRF of WCCP protocol packets arriving at the router is used to associate cache-engines with a configured service group.

The same VRF must have the interface on which redirection is applied, the interface which is connected to cache engine, and the interface on which the packet would have left if it had not been redirected.

WCCP VRF Tunnel Interfaces

In releases that support the WCCP VRF Support feature, the use of GRE redirection results in the creation of new tunnel interfaces. You can display these tunnel interfaces by entering the **show ip interface brief | include tunnel** command:

```
Device# show ip interface brief | include tunnel
```

| | | | | | |
|---------|------------|-----|-------|----|----|
| Tunnel0 | 172.16.0.1 | YES | unset | up | up |
| Tunnel1 | 172.16.0.1 | YES | unset | up | up |
| Tunnel2 | 172.16.0.1 | YES | unset | up | up |
| Tunnel3 | 172.16.0.1 | YES | unset | up | up |

Device#

The tunnel interfaces are automatically created in order to process outgoing GRE-encapsulated traffic for WCCP. The tunnel interfaces appear when a content engine connects and requests GRE redirection. The tunnel interfaces are not created directly by WCCP, but are created indirectly via a tunnel application programming interface (API). WCCP does not have direct knowledge of the tunnel interfaces, but can redirect packets to them, resulting in the appropriate encapsulation being applied to the packets. After the appropriate encapsulation is applied, the packet is then sent to the content engine.



Note

The tunnel interfaces are not used to connect with incoming WCCP GRE return packets.

One tunnel is created for each service group that is using GRE redirection. One additional tunnel is created to provide an IP address that allows the other tunnel group interfaces to be unnumbered but still enabled for IPv4.

You can confirm the connection between the tunnels and WCCP by entering the **show tunnel groups wccp** command:

```
Device# show tunnel groups wccp
```

```
WCCP : service group 0 in "Default", ver v2, assgnmnt: hash-table
    intf: Tunnel0, locally sourced
WCCP : service group 317 in "Default", ver v2, assgnmnt: hash-table
    intf: Tunnel3, locally sourced
WCCP : service group 318 in "Default", ver v2, assgnmnt: hash-table
    intf: Tunnel2, locally sourced
```

You can display additional information about each tunnel interface by entering the **show tunnel interface interface-number** command:

```
Device# show tunnel interface t0
```

```
Tunnel0
Mode:multi-GRE/IP, Destination UNKNOWN, Source 10.1.1.80
Application ID 2: WCCP : service group 0 in "Default", ver v2, assgnmnt: hash-table
Linestate - current up
Internal linestate - current up, evaluated up
```

```
Device# show tunnel interface t1
```

```
Tunnel1
Mode:multi-GRE/IP, Destination UNKNOWN, Source 172.16.0.1
Application ID 2: unspecified
Linestate - current up
Internal linestate - current up, evaluated up
```

```
Device# show tunnel interface t2
```

```

Tunnel2
Mode:multi-GRE/IP, Destination UNKNOWN, Source 10.1.1.80
Application ID 2: WCCP : service group 318 in "Default", ver v2, assgnmnt: hash-table
Linestate - current up
Internal linestate - current up, evaluated up

Device# show tunnel interface t3

Tunnel3
Mode:multi-GRE/IP, Destination UNKNOWN, Source 10.1.1.80
Application ID 2: WCCP : service group 317 in "Default", ver v2, assgnmnt: hash-table
Linestate - current up
Internal linestate - current up, evaluated up
Device#

```

Note that the service group number shown in the examples is the internal tunnel representation of the WCCP service group number. Group 0 is the web-cache service. To determine the dynamic services, subtract 256 from the displayed service group number to convert to the WCCP service group number. For interfaces that are used for redirection, the source address shown is the WCCP router ID.

You can display information about the connected content engines and encapsulation, including software packet counters, by entering the **show adjacency [tunnel-interface] [encapsulation] [detail] [internal]** command:

```

Device# show adjacency t0

Protocol Interface          Address
IP      Tunnel0             10.1.1.82(3)

Device# show adjacency t0 encapsulation

Protocol Interface          Address
IP      Tunnel0             10.1.1.82(3)
Encap length 28
4500000000000000FF2F7D2B1E010150
1E0101520000883E00000000
Provider: TUNNEL
Protocol header count in macstring: 3
HDR 0: ipv4
    dst: static, 10.1.1.82
    src: static, 10.1.1.80
    prot: static, 47
    ttl: static, 255
    df: static, cleared
    per packet fields: tos ident tl chksm
HDR 1: gre
    prot: static, 0x883E
    per packet fields: none
HDR 2: wccpv2
    dyn: static, cleared
    sGID: static, 0
    per packet fields: alt altB priB

Device# show adjacency t0 detail

Protocol Interface          Address
IP      Tunnel0             10.1.1.82(3)
connectionid 1
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 1
Encap length 28
4500000000000000FF2F7D2B1E010150
1E0101520000883E00000000
Tun endpt
Next chain element:
    IP adj out of Ethernet0/0, addr 10.1.1.82

Device# show adjacency t0 internal

Protocol Interface          Address
IP      Tunnel0             10.1.1.82(3)

```

```

connectionid 1
0 packets, 0 bytes
epoch 0
sourced in sev-epoch 1
Encap length 28
450000000000000FF2F7D2B1E010150
1E0101520000883E00000000
Tun endpt
Next chain element:
    IP adj out of Ethernet0/0, addr 10.1.1.82
    parent oce 0x4BC76A8
    frame originated locally (Null0)
L3 mtu 17856
Flags (0x2808C4)
Fixup enabled (0x40000000)
    GRE WCCP redirection
HWIDB/IDB pointers 0x55A13E0/0x35F5A80
IP redirect disabled
Switching vector: IPv4 midchain adj oce
IP Tunnel stack to 10.1.1.82 in Default (0x0)
    nh tracking enabled: 10.1.1.82/32
    IP adj out of Ethernet0/0, addr 10.1.1.82
Adjacency pointer 0x4BC74D8
Next-hop 10.1.1.82
Device#

```

WCCP Bypass Packets

WCCP intercepts IP packets and redirects those packets to a destination other than the destination that is specified in the IP header. Typically the packets are redirected from a web server on the Internet to a web cache that is local to the destination.

Occasionally a web cache cannot manage the redirected packets appropriately and returns the packets unchanged to the originating router. These packets are called bypass packets and are returned to the originating router using either Layer 2 forwarding without encapsulation (L2) or encapsulated in generic routing encapsulation (GRE). The router decapsulates and forwards the packets normally. The VRF associated with the ingress interface (or the global table if there is no VRF associated) is used to route the packet to the destination.

GRE is a tunneling protocol developed by Cisco that encapsulates packet types from a variety of protocols inside IP tunnels, creating a virtual point-to-point link over an IP network.

WCCP Closed Services and Open Services

In applications where packets are intercepted and redirected by a Cisco IOS router to external WCCP client devices, it may be necessary to block the packets for the application when a WCCP client device is not available. This blocking is achieved by configuring a WCCP closed service. When a WCCP service is configured as closed, the packets that fulfill the services, but do not have an active client device, are discarded.

By default, WCCP operates as an open service, wherein communication between clients and servers proceeds normally in the absence of an intermediary device.

The **ip wccp service-list** or the **ipv6 wccp service-list** command can be used for both closed-mode and open-mode services. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number. Use the **mode** keyword to select an open or closed service.

WCCP Service Groups

WCCP is a component of Cisco IOS software that redirects traffic with defined characteristics from its original destination to an alternative destination. The typical application of WCCP is to redirect traffic bound for a remote web server to a local web cache to improve response time and optimize network resource usage.

The nature of the selected traffic for redirection is defined by service groups (see figure below) specified on content engines and communicated to routers by using WCCP. The maximum number of service groups allowed across all VRFs is 256.

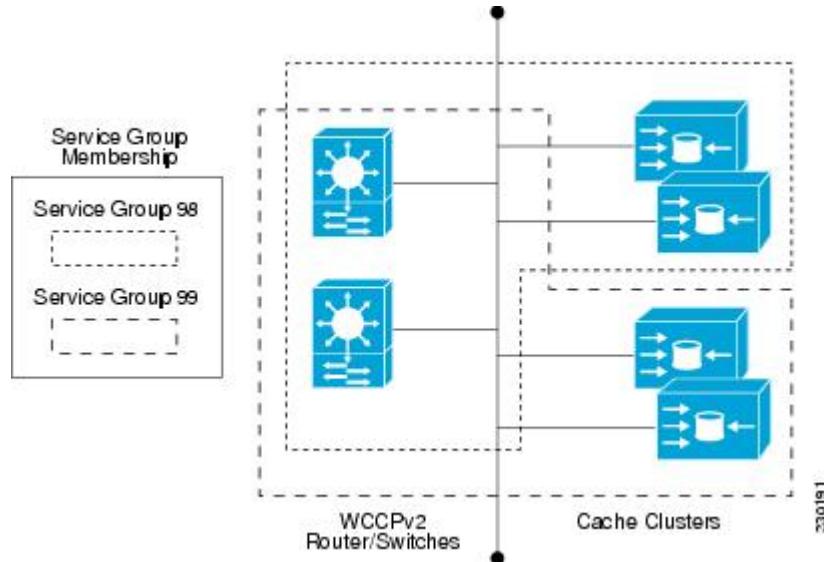
WCCPv2 supports up to 32 routers per service group. Each service group is established and maintained independently.

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 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. To specify the standard web cache service, use the **ip wccp** or the **ipv6 wccp** command with the **web-cache** keyword.



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

Figure 3: WCCP Service Groups



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.

Cisco Content Engines, for example, use dynamic service 99 to specify a reverse-proxy service. However, other content engine devices may use this service number for some other service.

WCCP—Check All Services

An interface may be configured with more than one WCCP service. When more than one WCCP service is configured on an interface, the precedence of a service depends on the relative priority of the service compared to the priority of the other configured services. Each WCCP service has a priority value as part of its definition. When an interface is configured with more than one WCCP service, the precedence of the packets is matched against service groups in priority order.

**Note**

The priority of a WCCP service group cannot be configured via Cisco IOS software.

With the **ip wccp check services all** or the **ipv6 wccp check services all** command, WCCP can be configured to check all configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by a redirect ACL and by the service priority.

If no WCCP services are configured with a redirect ACL, the services are considered in priority order until a service is found that matches the IP packet. If no services match the packet, the packet is not redirected. If a service matches the packet and the service has a redirect ACL configured, then the IP packet will be checked against the ACL. If the packet is rejected by the ACL, the packet will not be passed down to lower priority services unless the **ip wccp check services all** or the **ipv6 wccp check services all** command is configured. When the **ip wccp check services all** or the **ipv6 wccp check services all** command is configured, WCCP will continue to attempt to match the packet against any remaining lower priority services configured on the interface.

WCCP Interoperability with NAT

To redirect traffic using WCCP to a router running WAAS software that is also configured with NAT, enable the **ip nat inside** or the **ipv6 nat inside** command on the WAAS interface. If you are not able to configure the **ip nat inside** or the **ipv6 nat inside** command on the WAAS interface, disable Cisco Express Forwarding. You must also update the WCCP redirect ACL to include a private address to ensure that pretranslated traffic is redirected.

WCCP Troubleshooting Tips

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

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

You can use the **clear ipv6 wccpservice-id** command to remove the IPv6 WCCP statistics (counts) maintained on the router for a particular service.

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

You can use the **show ipv6 wccp** command to display the IPv6 WCCP global statistics (counts).

You can use the **show wccp** command to display all (IPv4 and IPv6) WCCP global statistics (counts).

How to Configure 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 or switches. Refer to the [Cisco Cache Engine User Guide](#) for content engine configuration and setup tasks.

Configuring WCCP

Perform this task to configure WCCP.

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | ip wccp version {1 2} Example: Router(config)# ip wccp version 2 | Specifies which version of WCCP to configure on a router. • WCCPv2 is the default running version. |
| Step 4 | ip wccp [vrf vrf-name] {web-cache service-number} [group-address multicast-address] [redirect-list access-list] [group-list access-list] [password password [0 7]] Example: Router(config)# ip wccp web-cache password password1 | Specifies a web-cache or dynamic service to enable on the router, specifies a VRF-name to associate with the service group, specifies the IP multicast address used by the service group, specifies any access lists to use, specifies whether to use MD5 authentication, and enables the WCCP service. |
| Step 5 | interface type number Example: Router(config)# interface ethernet0/0 | Targets an interface number for which the web cache service will run, and enters interface configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 6 | ip wccp [vrf <i>vrf-name</i>] {web-cache service-number} redirect {in out} Example: Router(config-if)# ip wccp web-cache redirect in | Enables packet redirection on an outbound or inbound interface using WCCP. • As indicated by the out and in keyword options, redirection can be specified for outbound interfaces or inbound interfaces. |
| Step 7 | exit Example: Router(config-if)# exit | Exits interface configuration mode. |
| Step 8 | interface <i>type number</i> Example: Router(config)# interface GigabitEthernet 0/2/0 | Targets an interface number on which to exclude traffic for redirection, and enters interface configuration mode. |
| Step 9 | ip wccp redirect exclude in Example: Router(config-if)# ip wccp redirect exclude in | (Optional) Excludes traffic on the specified interface from redirection. |

Configuring Closed Services

Perform this task to specify the number of service groups for WCCP, to configure a service group as a closed or open service, and to optionally specify a check of all services.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Enter one of the following commands:
 - **ip wccp [vrf vrf-name] service-number [service-list service-access-list mode {open | closed}]**
 - or
 - **ip wccp [vrf vrf-name] web-cache mode {open | closed}**
4. **ip wccp check services all**
5. **ip wccp [vrf vrf-name] {web-cache | service-number}**
6. **exit**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | Enter one of the following commands: <ul style="list-style-type: none"> • ip wccp [vrf vrf-name] service-number [service-list service-access-list mode {open closed}] • or • ip wccp [vrf vrf-name] web-cache mode {open closed} Example: Device(config)# ip wccp 90 service-list 120 mode closed or Device(config)# ip wccp web-cache mode closed | Configures a dynamic WCCP service as closed or open. or Configures a web-cache service as closed or open. Note When configuring the web-cache service as a closed service, you cannot specify a service access list. Note When configuring a dynamic WCCP service as a closed service, you must specify a service access list. |
| Step 4 | ip wccp check services all | (Optional) Enables a check of all WCCP services. |

| | Command or Action | Purpose |
|---------------|--|---|
| | <p>Example:</p> <pre>Device(config)# ip wccp check services all</pre> | <ul style="list-style-type: none"> • Use this command to configure WCCP to check the other configured services for a match and perform redirection for those services if appropriate. The caches to which packets are redirected can be controlled by the redirect ACL and not just the service description. <p>Note The ip wccp check services all command is a global WCCP command that applies to all services and is not associated with a single service.</p> |
| Step 5 | <p>ip wccp [vrf vrf-name] {web-cache service-number}</p> <p>Example:</p> <pre>Device(config)# ip wccp 201</pre> | <p>Specifies the WCCP service identifier.</p> <ul style="list-style-type: none"> • You can specify the standard web-cache service or a dynamic service number from 0 to 255. • The maximum number of services that can be specified is 256. |
| Step 6 | <p>exit</p> <p>Example:</p> <pre>Device(config)# exit</pre> | Exits to privileged EXEC mode. |

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.

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** global 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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing [vrf *vrf-name*] [distributed]**
4. **ip wccp [vrf *vrf-name*] {web-cache | service-number} group-address *multicast-address***
5. **interface *type number***
6. **ip pim {sparse-mode | sparse-dense-mode | dense-mode [proxy-register {list access-list | route-map *map-name*}]}**
7. **ip wccp [vrf *vrf-name*] {web-cache | service-number} group-listen**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | ip multicast-routing [vrf <i>vrf-name</i>] [distributed] Example: Device(config)# ip multicast-routing | Enables IP multicast routing. |
| Step 4 | ip wccp [vrf <i>vrf-name</i>] {web-cache service-number} group-address <i>multicast-address</i> Example: Device(config)# ip wccp 99 group-address 239.1.1.1 | Specifies the multicast address for the service group. |
| Step 5 | interface <i>type number</i> Example: Device(config)# interface ethernet 0/0 | Enables the interfaces to which the content engines will connect to receive multicast transmissions for which the web cache service will run, and enters interface configuration mode. |
| Step 6 | ip pim {sparse-mode sparse-dense-mode dense-mode [proxy-register {list access-list route-map <i>map-name</i>}]} | (Optional) Enables Protocol Independent Multicast (PIM) on an interface. |

| | Command or Action | Purpose |
|---------------|---|---|
| | Example: <pre>Device(config-if)# ip pim dense-mode</pre> | Note To ensure correct operation of the ip wccp group-listen command on Catalyst 6500 series switches and Cisco 7600 series routers, you must enter the ip pim command in addition to the ip wccp group-listen command. |
| Step 7 | ip wccp [vrf vrf-name] {web-cache service-number} group-listen Example: <pre>Device(config-if)# ip wccp 99 group-listen</pre> | Configures an interface to enable or disable the reception of IP multicast packets for WCCP. |

Using Access Lists for a WCCP Service Group

Perform this task to configure the device to use an access list to determine which traffic should be directed to which content engines.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **access-list access-list-number remark remark**
4. **access-list access-list-number permit {source [source-wildcard] | any} [log]**
5. **access-list access-list-number remark remark**
6. **access-list access-list-number deny {source [source-wildcard] | any} | [log]**
7. Repeat some combination of Steps 3 through 6 until you have specified the sources on which you want to base your access list.
8. **ip wccp [vrf vrf-name] web-cache group-list access-list**
9. **ip wccp [vrf vrf-name] web-cache redirect-list access-list**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | access-list access-list-number remark remark Example: Device(config)# access-list 1 remark Give access to user1 | (Optional) Adds a user-friendly comment about an access list entry. • A remark of up to 100 characters can precede or follow an access list entry. |
| Step 4 | access-list access-list-number permit {source [source-wildcard] any} [log] Example: Device(config)# access-list 1 permit 172.16.5.22 0.0.0.0 | Creates an access list that enables or disables traffic redirection to the cache engine and permits the specified source based on a source address and wildcard mask. • Every access list needs at least one permit statement; it does not need to be the first entry. • Standard IP access lists are numbered 1 to 99 or 1300 to 1999. • If the <i>source-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. • Optionally use the keyword any as a substitute for the <i>source source-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. • In this example, host 172.16.5.22 is allowed to pass the access list. |
| Step 5 | access-list access-list-number remark remark Example: Device(config)# access-list 1 remark Give access to user1 | (Optional) Adds a user-friendly comment about an access list entry. • A remark of up to 100 characters can precede or follow an access list entry. |
| Step 6 | access-list access-list-number deny {source [source-wildcard] any} [log] Example: Device(config)# access-list 1 deny 172.16.7.34 0.0.0.0 | Denies the specified source based on a source address and wildcard mask. • If the <i>source-wildcard</i> is omitted, a wildcard mask of 0.0.0.0 is assumed, meaning match on all bits of the source address. • Optionally use the abbreviation any as a substitute for the <i>source source-wildcard</i> to specify the source and source wildcard of 0.0.0.0 255.255.255.255. • In this example, host 172.16.7.34 is denied passing the access list. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 7 | Repeat some combination of Steps 3 through 6 until you have specified the sources on which you want to base your access list. | Remember that all sources not specifically permitted are denied by an implicit deny statement at the end of the access list. |
| Step 8 | ip wccp [vrf <i>vrf-name</i>] web-cache group-list <i>access-list</i> <p>Example:</p> <pre>Device(config) ip wccp web-cache group-list 1</pre> | Indicates to the device from which IP addresses of content engines to accept packets. |
| Step 9 | ip wccp [vrf <i>vrf-name</i>] web-cache redirect-list <i>access-list</i> <p>Example:</p> <pre>Device(config)# ip wccp web-cache redirect-list 1</pre> | (Optional) Disables caching for certain clients. |

Enabling WCCP Interoperability with NAT

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **ip nat inside**
5. **ip wccp *service-number* redirect in**
6. **exit**
7. **interface *type number***
8. **ip nat outside**
9. **ip wccp *service-number* redirect in**
10. **exit**
11. **interface *type number***
12. **ip nat inside**
13. **ip wccp redirect exclude in**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | interface type number Example: Router(config)# interface ethernet 1 | Specifies an interface on which to enable NAT and enters interface configuration mode. • This is the LAN-facing interface. |
| Step 4 | ip nat inside Example: Router(config-if)# ip nat inside | Designates that traffic originating from or destined for the interface is subject to NAT and indicates that the interface is connected to the inside network (the network subject to NAT translation). |
| Step 5 | ip wccp service-number redirect in Example: Router(config-if)# ip wccp 61 redirect in | Enables packet redirection on an inbound interface using WCCP. |
| Step 6 | exit Example: Router(config-if)# exit | Exits interface configuration mode and returns to global configuration mode. |
| Step 7 | interface type number Example: Router(config)# interface ethernet 2 | Specifies an interface on which to enable NAT and enters interface configuration mode. • This is the WAN-facing interface. |
| Step 8 | ip nat outside Example: Router(config-if)# ip nat outside | Designates that traffic originating from or destined for the interface is subject to NAT and indicates that the interface is connected to the outside network. |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 9 | ip wccp service-number redirect in Example: Router(config-if)# ip wccp 62 redirect in | Enables packet redirection on an inbound interface using WCCP. |
| Step 10 | exit Example: Router(config-if)# exit | Exits interface configuration mode and returns to global configuration mode. |
| Step 11 | interface type number Example: Router(config)# interface ethernet 3 | Specifies an interface on which to enable NAT and enters interface configuration mode. • This is the WAAS-facing interface. |
| Step 12 | ip nat inside Example: Router(config-if)# ip nat inside | Designates that traffic originating from or destined for the interface is subject to NAT and indicates that the interface is connected to the inside network (the network subject to NAT translation). |
| Step 13 | ip wccp redirect exclude in Example: Router(config-if)# ip wccp redirect exclude in | Configures an interface to exclude packets received on an interface from being checked for redirection.. |

Verifying and Monitoring WCCP Configuration Settings

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | show ip wccp [vrf vrf-name] [web-cache service-number] [detail view] Example: Router# show ip wccp 24 detail | Displays global information related to WCCP, including the protocol version running, the number of content engines in the router service group, which content engine group is allowed to connect to the router, and which access list is being used. • vrf vrf-name —(Optional) Virtual routing and forwarding (VRF) instance associated with a service group. • service-number —(Optional) Dynamic number of the web-cache service group being controlled by the content engine. The range is from 0 to 99. For web caches that use Cisco Content Engines, the reverse proxy service is indicated by a value of 99. • web-cache —(Optional) statistics for the web-cache service. • detail —(Optional) other members of a particular service group or web cache that have or have not been detected. • view —(Optional) information about a router or all web caches. |
| Step 3 | show ip interface Example: 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.” |
| Step 4 | more system:running-config Example: Router# more system:running-config | (Optional) Displays contents of the running configuration file (equivalent to the show running-config command). |

Configuration Examples for WCCP

Example: Changing the Version of WCCP on a Router

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

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

Example: Configuring a General WCCPv2 Session

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

Example: Setting a Password for a Router and Content Engines

```
Router# configure terminal
Router(config)# ip wccp web-cache password password1
```

Example: Configuring a Web Cache Service

```
Device# configure terminal
Device(config)# ip wccp web-cache
Device(config)# interface GigabitEthernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# exit
Device# copy running-config startup-config
```

The following example shows how to configure a session in which redirection of HTTP traffic arriving on Gigabit Ethernet interface 0/1/0 is enabled:

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
Device(config-if)# exit
Device# show ip interface GigabitEthernet 0/1/0
.
.
.
WCCP Redirect inbound is enabled
WCCP Redirect exclude is disabled
.
.
.
```

Example: Running a Reverse Proxy Service

The following example assumes that 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 gigabitethernet 0/1/0
Router(config-if)# ip wccp 99 redirect out
```

Example: Registering a Router to a Multicast Address

```
Device# configure terminal
Device(config)# ip wccp web-cache group-address 224.1.1.100
Device(config)# interface gigabitethernet 0/1/0
Device(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 via Gigabit Ethernet interface 0/1/0:

```
Device# configure terminal
Device(config)# ip wccp 99 group-address 224.1.1.1
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp 99 redirect out
```

Example: Using Access Lists

Example: Using Access Lists

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

```
Device(config)# access-list 10 permit host 10.1.1.1
Device(config)# access-list 10 permit host 10.1.1.2
Device(config)# access-list 10 permit host 10.1.1.3
Device(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 10.3.1.1 will bypass the cache, and that all other requests will be serviced normally:

```
Device(config)# ip wccp web-cache redirect-list 120
Device(config)# access-list 120 deny tcp host 10.1.1.1 any
Device(config)# access-list 120 deny tcp any host 10.3.1.1
Device(config)# access-list 120 permit ip any any
```

The following example configures a device to redirect web-related packets received via Gigabit Ethernet interface 0/1/0, destined to any host except 209.165.200.224:

```
Device(config)# access-list 100 deny ip any host 209.165.200.224
Device(config)# access-list 100 permit ip any any
Device(config)# ip wccp web-cache redirect-list 100
Device(config)# interface gigabitethernet 0/1/0
Device(config-if)# ip wccp web-cache redirect in
```

Example: Enabling WCCP Interoperability with NAT

```
Router(config)# interface ethernet1 ! This is the LAN-facing interface
Router(config-if)# ip nat inside
Router(config-if)# ip wccp 61 redirect in
Router(config-if)# exit
Router(config)# interface ethernet2 ! This is the WAN-facing interface
Router(config-if)# ip nat outside
Router(config-if)# ip wccp 62 redirect in
Router(config-if)# exit
Router(config)# interface ethernet3 ! This is the WAAS-facing interface
Router(config-if)# ip nat inside
Router(config-if)# ip wccp redirect exclude in
```

Example: Verifying WCCP Settings

The following example shows how to verify your configuration changes by using the **more system:running-config** command in privileged EXEC mode. The following example shows that both the web cache service and dynamic service 99 are enabled on the device:

```
Device# 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$faIJSvQXVPW.KuCxZNTh1
enable password password1
!
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 GigabitEthernet0/1/1
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 GigabitEthernet0/1/0
ip address 10.4.1.1 255.255.255.0
no ip directed-broadcast
ip wccp 99 redirect in
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 password1
login
!
end

```

The following example shows how to display global statistics related to WCCP:

```

Device# show ip wccp web-cache detail

WCCP Client information:
WCCP Client ID:      10.1.1.2
Protocol Version:   2.0
State:              Usable
Redirection:        L2

```

Additional References

```

Packet Return:      L2
Packets Redirected: 0
Connect Time:       00:20:34
Assignment:         MASK
Mask   SrcAddr     DstAddr     SrcPort DstPort
----- -----
0000: 0x00000000 0x00001741 0x0000 0x0000
Value  SrcAddr     DstAddr     SrcPort DstPort CE-IP
----- -----
0000: 0x00000000 0x00000000 0x0000 0x0000 0x3C010102 (10.1.1.2)
0001: 0x00000000 0x00000001 0x0000 0x0000 0x3C010102 (10.1.1.2)
0002: 0x00000000 0x00000040 0x0000 0x0000 0x3C010102 (10.1.1.2)
0003: 0x00000000 0x00000041 0x0000 0x0000 0x3C010102 (10.1.1.2)
0004: 0x00000000 0x00000100 0x0000 0x0000 0x3C010102 (10.1.1.2)
0005: 0x00000000 0x00000101 0x0000 0x0000 0x3C010102 (10.1.1.2)
0006: 0x00000000 0x00000140 0x0000 0x0000 0x3C010102 (10.1.1.2)

```

For more information about the **show ip wccp web-cache** command, see the *Cisco IOS IP Application Services Command Reference*.

Additional References

Related Documents

| Related Topic | Document Title |
|---|--|
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Cisco ACNS software configuration information | <ul style="list-style-type: none"> • <i>Cisco ACNS Software Caching Configuration Guide, Release 4.2</i> • Cisco ACNS Software listing page on Cisco.com |
| IP access list overview, configuration tasks, and commands | <i>Cisco IOS Security Command Reference</i> |
| IP addressing and services commands and configuration tasks | <ul style="list-style-type: none"> • <i>Cisco IOS IP Addressing Services Configuration Guide</i> • <i>Cisco IOS IP Addressing Services Command Reference</i> |
| WCCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples | <i>Cisco IOS IP Application Services Command Reference</i> |

Standards

| Standard | Title |
|---|--------------|
| No new or modified standards are supported, and support for existing standards has not been modified. | — |

MIBs

| MIB | MIBs Link |
|---|---|
| No new or modified MIBs are supported, and support for existing MIBs has not been modified. | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

RFCs

| RFC | Title |
|---|--------------|
| No new or modified RFCs are supported, and support for existing RFCs has not been modified. | — |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for WCCP

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

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

Table 1: Feature Information for WCCP

| Feature Name | Releases | Feature Information |
|-------------------------|-----------------|--|
| WCCP Bypass Counters | 15.0(1)SY | <p>The WCCP Bypass Counters feature allows you to display a count of packets that have been bypassed by a web cache and returned to the originating router to be forwarded normally.</p> <p>The show ip wccp command was modified by this feature.</p> |
| WCCP Closed Services | 15.0(1)SY | <p>The WCCP Closed Services feature permits WCCP services to be configured so that WCCP always intercepts traffic for such services but, if no WCCP client (such as a content engine) has registered to receive this traffic, packets are discarded.</p> <p>This behavior supports Application-Oriented Network Services (AONS) applications, which require traffic to be transparently intercepted using WCCP but do not want the packets to be forwarded to their destination if the WCCP client is unavailable to perform its processing. (This is contrary to the traditional use of WCCP to assist caches where the absence of a cache does not change the behavior as observed by the user.)</p> <p>The ip wccp command was modified by this feature.</p> |
| WCCP Increased Services | 15.0(1)SY | <p>The WCCP Increased Services feature increases the number of services supported by WCCP to a maximum of 256 across all VRFs.</p> <p>The following commands were modified by this feature: ip wccp, ip wccp check services all, show ip wccp.</p> |

| Feature Name | Releases | Feature Information |
|--|-----------|--|
| WCCP L2 Return | 15.0(1)SY | <p>The WCCP L2 Return feature allows content engines to return packets to WCCP routers directly connected at Layer 2 by swapping the source and destination MAC addresses rather than tunneling packets back to the router inside a Layer 3 GRE tunnel.</p> <p>There are no new or modified commands associated with this feature.</p> |
| WCCP Mask Assignment | 15.0(1)SY | <p>The WCCP Mask Assignment feature introduces support for ACNS/WAAS devices using mask assignment as a cache engine assignment method.</p> <p>There are no new or modified commands associated with this feature.</p> |
| WCCP Redirection on Inbound Interfaces | 15.0(1)SY | <p>The WCCP Redirection on Inbound Interfaces feature enables interfaces to be configured for input redirection for a particular WCCP service. When this feature is enabled on an interface, all packets arriving at that interface are compared against the specified WCCP service. If the packets match, they will be redirected.</p> <p>The following commands were introduced or modified by this feature: ip wccp redirect-list.</p> |

| Feature Name | Releases | Feature Information |
|------------------|-----------|---|
| WCCP Version 2 | 15.0(1)SY | <p>The WCCP Version 2 feature provides several enhancements and features to the WCCP protocol, including:</p> <ul style="list-style-type: none"> • The ability of multiple routers to service a content engine cluster. • Redirection of traffic other than HTTP (TCP port 80 traffic), including a variety of UDP and TCP traffic. • Optional authentication that enables you to control which routers and content engines become part of the service group using passwords and the HMAC MD5 standard. • A check on packets that determines which requests have been returned from the content engine unserviced. • Load adjustments for individual content engines to provide an effective use of the available resources while helping to ensure high quality of service (QoS) to the clients. <p>The following commands were introduced or modified by this feature: clear ip wccp, ip wccp, ip wccp group-listen, ipwccp redirect, ip wccp redirect exclude in, ip wccp version, show ip wccp.</p> |
| WCCP VRF Support | 15.0(1)SY | <p>The WCCP VRF Support feature provides enhancements to the existing WCCPv2 protocol which support VRF awareness.</p> <p>The following commands were introduced or modified by this feature: clear ip wccp, debug ip wccp, ip wccp, ip wccp group-listen, ip wccp redirect, show ip wccp.</p> |

