Configuring WCCP

Last Updated: December 16, 2011

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 XE Release 2.2 supports only 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

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

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

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

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.

Restrictions for WCCP

- WCCP works only with IPv4 networks.
- WCCP does not redirect IP multicast packets.
- WCCP packet redirection on outbound interfaces is not supported in Cisco IOS XE releases prior to Cisco IOS XE Release 3.1S.
- There is no SNMP support and no MIB has been implemented for WCCPv2.
- Cisco ASR 1000 Series Routers do not support WCCPv1.
- Cisco ASR 1000 Series Routers do not support inter-VRF redirection.
- Service groups can comprise up to 32 content engines and 32 routers.
- WCCP does not support InService Software Upgrade (ISSU), stateful switchover (SSO) or nonstop forwarding (NSF).
- Transiting packets are lost in the event of a forwarding processor (FP) failover on a 6-rack-unit (6RU) and 13RU chassis.
- All content engines in a cluster must be configured to communicate with all routers servicing the cluster.
- Hash assignment as a load-balancing method for a WCCP service is not supported. As of Cisco IOS XE Release 3.1S, clients that send hash assignment will not be allowed by the router to come online. On Cisco ASR 1000 Series Routers, the **show ip wccp 61 detail** command displays that hash is an incompatible assignment method.
- For routers servicing a multicast cluster, the Time To Live (TTL) value must be set at 15 or lower.
- The **show ip wccp** command displays information about software-based (process, fast and Cisco Express Forwarding [CEF]) forwarding of WCCP packets. The Cisco ASR 1000 Series Routers implement WCCP in hardware, rather than in the CEF or process-switching paths. Implementing WCCP in hardware results in a packet count of 0 when the **show ip wccp** command is entered. Use the **show platform software wccp interface counters** or **show platform software wccp counters** commands to display global statistics related to WCCP on the Cisco ASR 1000 Series Routers.
- When the Cisco ASR 1000 Series Router and WCCP are used to redirect traffic to a WAE that is using WCCP GRE return as the egress method and the HTTP accelerator is enabled, the ASR router's handling of proxied HTTP connections may cause HTTP slowness. To work around this issue, on the ASR router, use the **ip wccp** [**vrf** *vrf-name*] **web-cache** command to create a web cache service in the same VRF as that of the 61/62 service.
- In Cisco IOS XE Release 3.1S, the **show ip wccp** command displays redirected WCCP packets.
- When the IP address of an interface that is being used as the router ID (highest IP address of the interfaces) is removed when a WCCP cache engine is connected via Generic Routing Encapsulation (GRE) adjacency, the source-IP address of the outer IP packet (of GRE) will continue to use the removed IP address. The traffic will continue to get redirected to the cache engine. This symptom is not visible, because the Cisco IOS XE software updates the router ID in the protocol messages to the cache engine, and the cache engine uses the new router ID when it returns packets to the router. Configure a loopback address and assign an IP address to the loopback address so that the assigned loopback address is used as the router ID. Removal of such a loopback IP address is unlikely, but

when the loopback address is removed, the source IP address of the GRE packet from the router to the cache engine will carry the removed IP address. Enter the **shutdown** command, followed by the **no shutdown** command on the cache engine interface that has the GRE redirect method configured to stop the interface from using the removed IP address.

- The following limitation applies to WCCP Layer 2 Forwarding and Return feature:
  Layer 2 redirection requires that content engines be directly connected to an interface on each WCCP router. WCCP configuration of the content engine must reference the directly connected interface IP address of the WCCP router and not a loopback IP address or any other IP address configured on the WCCP router.

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 Cisco IOS XE routing platforms to transparently redirect content requests. The main benefit of transparent redirection is that users do not need to configure their browsers to use a web proxy. Instead, they can use the target URL to request content, and have their requests automatically redirected to a content engine. The word "transparent" in this case means that the end user does not know that a requested file (such as a web page) came from the content engine instead of from the originally specified server.

When a content engine receives a request, it attempts to service it from its own local 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. When the content engine retrieves the requested information, it forwards it to the requesting client and caches it to fulfill future requests, thus maximizing download performance and substantially reducing transmission costs.

WCCP enables a series of content engines, called a content engine cluster, to provide content to a router or multiple routers. Network administrators can easily scale their content engines to 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 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. On Cisco ASR 1000 Series Routers, both the GRE and L2 forward/return methods use the hardware, so there is not any 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.

For more information on Cisco ACNS commands used to configure Cisco Content Engines, see the *Cisco ACNS Software Command Reference*, Release 5.5.13.

For more information on WAAS commands used to configure Cisco Content Engines, see the *Cisco Wide Area Application Services Command Reference (Software Versions 4.2.1)*.

WCCP Mask Assignment

The WCCP Mask Assignment feature enables mask assignment as the load-balancing method for a WCCP service.

For content engines running Application and Content Networking System (ACNS) software, use the **wccp web-cache** command with the **mask-assign**keywords 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 more information on Cisco ACNS commands used to configure Cisco Content Engines, see the *Cisco ACNS Software Command Reference*, Release 5.5.13.

For more information on WAAS commands used to configure Cisco Content Engines, see the Cisco Wide Area Application Services Command Reference (Software Versions 4.2.1).

Hardware Acceleration

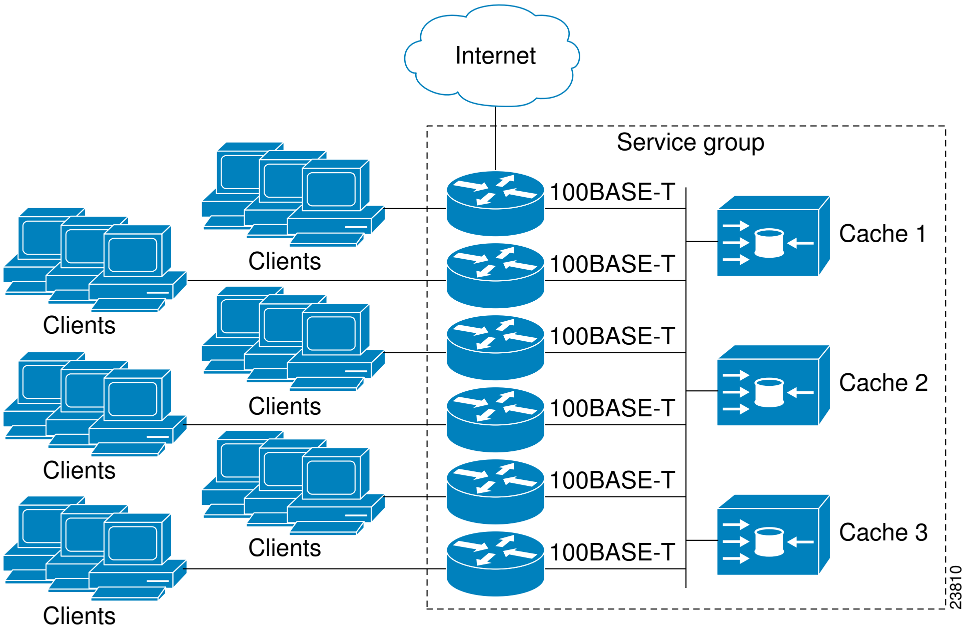
WCCP implementation on the Cisco ASR 1000 Series Routers is hardware accelerated by default.

You do not need to configure the **ip wccp web-cache accelerated** command on Cisco ASR routers to enable hardware acceleration.

WCCPv2 Configuration

Multiple routers can use WCCPv2 to service a content engine cluster. The figure below illustrates a sample configuration using multiple routers.

Figure 1 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.

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 the following method:

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

The multicast option is easier to configure because you need only specify a single address on each content engine. This option also 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 introduces the concept of multiple *service groups*. Service information is specified in the WCCP configuration commands using dynamic services identification numbers (such as 98) or a predefined service 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 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)

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 packet flows are intercepted and redirected by a Cisco IOS router to external WCCP client devices, it may be necessary to block the packet flows 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, WCCP discards packets that do not have a WCCP client registered to receive the redirected traffic.

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** command can only be used for closed-mode services. Use the **service-list** keyword and *service-access-list* argument to register an application protocol type or port number.

When there is a mismatch between the service-list ACL and the definition received from a cache engine, the service is not allowed to start.

WCCP Outbound ACL Check

When WCCP is enabled for redirection on an ingress interface, the packets are redirected by WCCP and instead egress on an interface other than the destination that is specified in the IP header. The packets are still subject to ACLs configured on the ingress interface. However, redirection can cause the packets to bypass the ACL configured on the original egress interface. Packets that would have been dropped because of the ACL configured on the original egress interface can be sent out on the redirect egress interface. This poses a possible security problem. Enabling the WCCP Outbound ACL check feature ensures that redirected packets are subject to any ACL conditions configured on the original egress interface.

WCCP Service Groups

WCCP is a component of Cisco IOS XE 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.

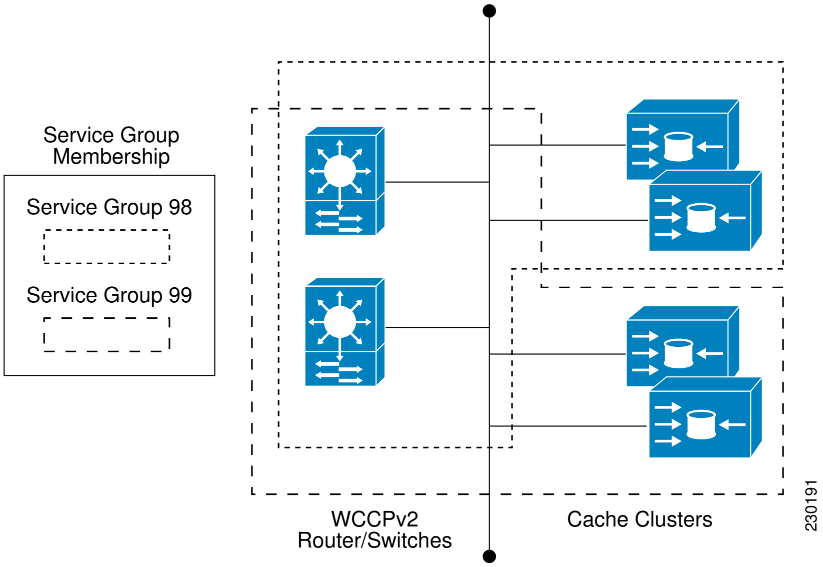
The nature of the selected traffic for redirection is defined by service groups specified on content engines and communicated to routers by using WCCP. The current implementation of WCCP in Cisco IOS XE software allows for a maximum of 256 service groups across all VRFs.

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** 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 2 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. The configuration information in this document deals with enabling general services on the Cisco ASR 1000 Series Routers.

WCCP Check Services All

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** 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 as well as 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** command is configured. When the **ip 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 Configurable Router ID

WCCP uses a router ID in its control messages and the router ID serves as a means by which a WCCP client can identify a particular WCCP server. The router ID is treated as an IPv4 address and may also be used as the source address of any WCCP-generated GRE frames. Prior to the WCCP Configurable Router ID feature, WCCP selects a router ID using an automatic mechanism; the highest reachable IPv4 address on the system is used as the WCCP router ID. The highest IPv4 address on the system is not always the best choice as the router ID or as the source address of GRE frames. A change in addressing information on the system may cause the WCCP router ID to change unexpectedly. During this changeover period, WCCP clients briefly advertise the existence of two routers (the old router ID and the new Router ID) and GRE frames are sourced from a different address.

The WCCP Configurable Router ID feature enables you to define a WCCP source interface. The IP address of this configured source interface is then used as the preferred WCCP router ID and WCCP GRE source address. When a WCCP router ID is manually configured, router IDs are not automatically generated when the current router ID is no longer valid and the router ID does not change when another IP address is added to the system. The router ID changes only when a new router ID is manually configured using the **ip wccp source-address** command.

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** command on the WAAS interface. If you are not able to configure the **ip 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

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 CLI to investigate further. The counters allow you to determine the percent of traffic being bypassed.

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.

Using the**ip wccp web-cache password** command, you can 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 can consist of up to eight characters. 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.

Note WCCPv1 is not supported on the Cisco ASR 1000 Series Routers.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} | [**group-address** *group-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*]
4. **ip wccp** [**vrf** *vrf-name*] **source-interface** *source-interface*
5. **interface** *type number*
6. **ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**out** | **in**}
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** [**vrf** *vrf-name*] {**web-cache** | *service-number*} | [**group-address** *group-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** *password*] **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 4	**ip wccp** [**vrf** *vrf-name*] **source-interface** *source-interface* **Example:** `Router (config)# ip wccp source-interface GigabitEthernet 0/0/0`	(Optional) Configures a preferred WCCP router ID.

	Command or Action	Purpose
Step 5	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet0/1/0`	Targets an interface number for which the web cache service will run, and enters interface configuration mode.

Step 6	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **redirect** {**out** | **in**}
	Example:
	`Router(config-if)# ip wccp web-cache redirect in`
		Enables packet redirection on an inbound or outbound interface using WCCP.

Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 8	**interface** *type number* **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. You can use this command in conjunction with the **ip wccp redirect out** command.

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:** `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	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**}
	Example:
	`Router(config)# ip wccp 90 service-list 120 mode closed`
	or
	`Router(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.

	Command or Action	Purpose
Step 4	**ip wccp check services all** **Example:** `Router(config)# ip wccp check services all`	(Optional) Enables a check of all WCCP services. • 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. **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.

Step 5	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*}
	Example:
	`Router(config)# ip wccp 201`
		Specifies the WCCP service identifier.
		• 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	**exit** **Example:** `Router(config)# exit`	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:** `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 multicast-routing** [**vrf** *vrf-name*] [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing.
Step 4	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-address** *multicast-address* **Example:** `Router(config)# ip wccp 99 group-address 239.1.1.1`	Specifies the multicast address for the service group.
Step 5	**interface** *type number* **Example:** `Router(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** *map-name*}]}
	Example:
	`Router(config-if)# ip pim dense-mode`
		(Optional) Enables Protocol Independent Multicast (PIM) on an interface.
		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.

	Command or Action	Purpose
Step 7	**ip wccp** [**vrf** *vrf-name*] {**web-cache** | *service-number*} **group-listen** **Example:** `Router(config-if)# ip wccp 99 group-listen`	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 router 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:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**access-list** *access-list-number* **remark** *remark* **Example:** `Router(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:** `Router(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 *source-wildcard* 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 *source source-wildcard* 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:** `Router(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:** `Router(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 *source-wildcard* 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 *source source-wildcard* 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.
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** *vrf-name*] **web-cache group-list** *access-list* **Example:** `Router(config) ip wccp web-cache group-list 1`	Indicates to the router from which IP addresses of content engines to accept packets.

	Command or Action	Purpose
Step 9	**ip wccp** [**vrf** *vrf-name*] **web-cache redirect-list** *access-list* **Example:** `Router(config)# ip wccp web-cache redirect-list 1`	(Optional) Disables caching for certain clients.

Enabling the WCCP Outbound ACL Check

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip wccp** [**vrf** *vrf-name*] {**web-cache** \| *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list***access-list*] [**password** *password*]
4. **ip wccp check acl outbound**
5. **exit**

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** [**vrf** *vrf-name*] {**web-cache** | *service-number*} [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list***access-list*] [**password** *password*] **Example:** `Router(config)# ip wccp web-cache`	Enables the support for a Cisco content engine service group or any content engine service group and configures a redirect ACL list or group ACL.

	Command or Action	Purpose
Step 4	**ip wccp check acl outbound** **Example:** `Router(config)# ip wccp check acl outbound`	Enables the ACL outbound check on the originating interface. **Note** The **ip wccp outbound-check-acl** command can also be configured.
Step 5	**exit** **Example:** `Router(config)# exit`	Exits global configuration.

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.

	Command or Action	Purpose
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

The **show ip wccp** command displays information about software-based (process, fast, and Cisco Express Forwarding [CEF]) forwarding of WCCP packets. The Cisco ASR 1000 Series Routers implement WCCP in hardware, rather than in the CEF or process-switching paths. Implementing WCCP in hardware results in a packet count of 0 when the **show ip wccp** command is entered in Cisco IOS XE releases prior to Cisco IOS XE Release 3.1S. To display global statistics related to WCCP in Cisco ASR 1000, use the **show platform software wccp** command. As of Cisco IOS XE Release 3.1S, the **show ip wccp** command displays redirected WCCP packets.

Use the following commands in privileged EXEC mode to verify and monitor the configuration settings for WCCP.

SUMMARY STEPS

1. **enable**
2. **debug ip wccp** {**default** | **vrf** *vrf-name* {**events** | **packets** [**control**]} | **events** | **packets** [**bypass** | **control** | **redirect**] | **platform** | **subblocks**}
3. **debug platform hardware qfp active feature wccp** {{**client** | **lib-client** {**all** | **error** | **info** | **trace** | **warning**}} | **datapath all**}
4. **debug platform software wccp** {**configuration** | **counters** | **detail** | **messages**}
5. **show platform software wccp** [*service-number* **counters** | [*slot* [*service-number* [**access-list**] | **cache-info** | **interface** | **statistics** | **web-cache** [**access-list**]] | **vrf** *vrf-identifier* {*service-number* [**access-list**] | **web-cache** [**access-list**]}]] | **interface counters** | **statistics** | [**vrf** *vrf-identifier* {*service-number* **counters** | **web-cache counters**}] | **web-cache counters**]
6. **show platform hardware qfp active feature wccp** [**vrf** *vrf-id*] **service id** *service-id*
7. **show ip wccp global** [**counters**]
8. **show ip interface**
9. **more system:running-config**
10. **configure terminal**
11. **platform trace runtime slot** *slot* **bay** *bay* **process forwarding-manager module wccp level** {*level*}

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**debug ip wccp** {**default** | **vrf** *vrf-name* {**events** | **packets** [**control**]} | **events** | **packets** [**bypass** | **control** | **redirect**] | **platform** | **subblocks**}
	Example:
	`Router# debug ip wccp events`
		Display information about WCCP services.

Step 3	**debug platform hardware qfp active feature wccp** {{**client** | **lib-client** {**all** | **error** | **info** | **trace** | **warning**}} | **datapath all**} **Example:** `Router# debug platform hardware qfp active feature wccp client all`	Enables debug logging for the WCCP client in the Cisco Quantum Flow Processor (QFP).

	Command or Action	Purpose
Step 4	**debug platform software wccp** {**configuration** | **counters** | **detail** | **messages**} **Example:** `Router# debug platform software wccp configuration`	Enables WCCP platform debug messages.
Step 5	**show platform software wccp** [*service-number* **counters** | [*slot* [*service-number* [**access-list**] | **cache-info** | **interface** | **statistics** | **web-cache** [**access-list**]] | **vrf** *vrf-identifier* {*service-number* [**access-list**] | **web-cache** [**access-list**]}]] | **interface counters** | **statistics** | [**vrf** *vrf-identifier* {*service-number* **counters** | **web-cache counters**}] | **web-cache counters**] **Example:** `Router# show platform software wccp 61 counters`	Displays global statistics related to WCCP on the Cisco ASR 1000 Series Routers.
Step 6	**show platform hardware qfp active feature wccp** [**vrf** *vrf-id*] **service id** *service-id* **Example:** `Router# show platform hardware qfp active feature wccp [vrf vrf-id] service id 1`	Displays WCCP service group information in the active QFP.
Step 7	**show ip wccp global** [**counters**] **Example:** `Router# show ip wccp global counters`	Displays global, nonservice WCCP information.
Step 8	**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 9	**more system:running-config** **Example:** `Router# more system:running-config`	(Optional) Displays contents of the currently running configuration file (equivalent to the **show running-config** command.)

	Command or Action	Purpose
Step 10	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 11	**platform trace runtime slot** *slot* **bay** *bay* **process forwarding-manager module wccp level** {*level*} **Example:** `Router(config)# platform trace runtime slot 1 bay 0 process forwarding-manager module wccp level debug`	Enables Forwarding Manager route processor and Embedded Service Processor trace messages for the WCCP process.

Configuration Examples for WCCP

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

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

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

```
Router# configure terminal
Router(config)# ip wccp web-cache group-address 224.1.1.100
Router(config)# interface gigabitethernet 0/1/0
Router(config-if)# ip wccp web cache group-listen
```

The following example shows a router configured to run a reverse proxy service, using the multicast address of 224.1.1.1. Redirection applies to packets outgoing via Gigabit Ethernet interface 0/1/0:

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

Example: Using Access Lists

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 where the access list number is 10 for some sample hosts:

```
Router(config)# access-list 10 permit host 10.1.1.1
Router(config)# access-list 10 permit host 10.1.1.2
Router(config)# access-list 10 permit host 10.1.1.3
Router(config)# ip wccp web-cache group-list 10
```

To disable caching for certain clients, servers, or client/server pairs, you can use WCCP access lists. The following example shows that any requests coming from 10.1.1.1 to 10.3.1.1 will bypass the cache, and that all other requests will be serviced normally:

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

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

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

Example: WCCP Outbound ACL Check Configuration

The following configuration example shows that the access list prevents traffic from network 10.0.0.0 leaving Gigabit Ethernet interface 0/1/0. Because the outbound ACL check is enabled, WCCP does not redirect that traffic. WCCP checks packets against the ACL before they are redirected.

```
Router(config)# ip wccp web-cache
Router(config)# ip wccp check acl outbound
Router(config)# interface gigabitethernet 0/1/0
Router(config-if)# ip access-group 10 out
Router(config-if)# exit
Router(config)# ip wccp web-cache redirect-list redirect-out
Router(config)# access-list 10 deny 10.0.0.0 0.255.255.255
Router(config)# access-list 10 permit any
```

If the outbound ACL check is disabled, the HTTP packets from network 10.0.0.0 would be redirected to a web cache. Users with that network address could retrieve web pages even though the network administrator wanted to prevent it.

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 router:

```
Router# more system:running-config
```

```
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname router4
!
enable secret 5 $1$nSVy$faliJsVQXVPW.KuCxZNTh1
enable password 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:

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

WCCP Client information:
WCCP Client ID:      10.1.1.2
Protocol Version:    2.0
State:               Usable
Redirection:         L2
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 ACNS software configuration information	• Cisco ACNS Software Caching Configuration Guide, Release 4.2 • http://www.cisco.com/en/US/products/sw/conntsw/ps491/products_installation_and_configuration_guides_list.html • Cisco ACNS Software listing page on Cisco.com
Deploying and Troubleshooting WCCP on Cisco ASR 1000 Series Routers	Deploying and Troubleshooting Web Cache Control Protocol Version 2 on Cisco ASR 1000 Series Aggregation Services Routers
IP Access List overview, configuration tasks, and commands	• *Cisco IOS XE Security Configuration Guide: Securing the Data Plane* • *Cisco IOS Security Command Reference*

Related Topic	Document Title
IP addressing and services commands and configuration tasks	• *Cisco IOS XE IP Addressing Services Configuration Guide* • *Cisco IOS IP Addressing Services Command Reference*
WCCP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Application Services Command Reference*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
None	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 by this feature, and support for existing RFCs has not been modified by this feature.	

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	Cisco IOS XE Release 2.2	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. The following commands were modified or introduced by this feature: **show ip wccp**, **show platform software wccp**.
WCCP: Check Services All	Cisco IOS XE Release 3.1S	The WCCP: Check Services All feature enables you to configure WCCP to search all service groups and redirect ACLs in priority order for a match. The following command was modified by this feature: **ip wccp check services all**

Feature Name	Releases	Feature Information
WCCP Closed Services	Cisco IOS XE Release 3.1S	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. This behavior supports AONS (Application-Oriented Network Services) 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 behavior 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.) The **ip wccp** command was modified by this feature.
WCCP--Configurable Router ID	Cisco IOS XE Release 3.1S	The WCCP--Configurable Router ID feature permits the router ID which WCCP uses to be configurable, rather than relying on the router’s selection mechanism. The **ip wccp source-interface** commands was introduced by this feature.
WCCP Egress Redirection Support	Cisco IOS XE Release 3.1S	The WCCP Egress Redirection Support feature enables WCCP based redirection applied to the outbound traffic on the outbound interface. The **ip wccp redirect** command was modified by this feature.

Feature Name	Releases	Feature Information
WCCP Exclude Interface	Cisco IOS XE Release 3.1S	The WCCP Exclude Interface feature enables you to configure an interface to exclude packets received on an interface from being checked for redirection by configuring the **ip wccp redirect exclude in**command in interface configuration mode. The following command was introduced by this feature: **ip wccp redirect exclude in**
WCCP Group List	Cisco IOS XE Release 3.1S	The WCCP Group List feature enables you to configure the IP addresses of cache engines from which a router accepts packets. Configuring a group list is used to validate the protocol packets received from the cache engine. Packets matching the address in a configured group-list are processed, others are discarded. The **ip wccp** command was introduced or modified by this feature.
WCCP--Group Listen and Multicast Service Support	Cisco IOS XE Release 3.1S	The WCCP--Group Listen and Multicast Service Support feature adds the ability to configure a multicast address per service group for sending and receiving protocol messages. In the multicast address method, the cache engine sends a single-address notification that provides coverage for all routers in the service group. • WCCPv2 Configuration, page 5 • Registering a Router to a Multicast Address, page 14 • Example: Registering a Router to a Multicast Address, page 25 • The **ip wccp group-listen**command was modified by this feature.

Feature Name	Releases	Feature Information
WCCP Increased Services	Cisco IOS XE Release 3.1S	The WCCP Increased Services feature increases the number of services supported by WCCP to a maximum of 256 across all VRFs. The following commands were modified by this feature: **ip wccp**, **ip wccp check services all**, **ip wccp outbound-acl-check, show ip wccp**.
WCCP Layer 2 Redirection / Forwarding	Cisco IOS XE Release 2.2	The WCCP Layer 2 Redirection/ Forwarding feature allows directly connected Cisco content engines to use Layer 2 redirection, which is more efficient than Layer 3 redirection via GRE encapsulation. You can configure a directly connected Cache Engine to negotiate use of the WCCP Layer 2 Redirection/ Forwarding feature. The WCCP Layer 2 Redirection/Forwarding feature requires no configuration on the router or switch. There are no new or modified commands associated with this feature.
WCCP L2 Return	Cisco IOS XE Release 2.2	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. There are no new or modified commands associated with this feature.

Feature Name	Releases	Feature Information
WCCP Mask Assignment	Cisco IOS XE Release 2.2	The WCCP Mask Assignment feature introduces support for ACNS/WAAS devices using mask assignment as a cache engine assignment method. There are no new or modified commands associated with this feature.
WCCP Outbound ACL Check	Cisco IOS XE Release 3.1S	The WCCP Outbound ACL Check feature enables you to ensure that traffic redirected by WCCP at an input interface is subjected to the outbound ACL checks that may be configured on the output interface prior to redirection. The following commands were introduced or modified by this feature: **ip wccp**, **ip wccp check acl outbound**.
WCCP Redirection on Inbound Interfaces	Cisco IOS XE Release 2.2	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. The following commands were introduced or modified by this feature: **ip wccp redirect**.

Feature Name	Releases	Feature Information
WCCP Version 2	Cisco IOS XE Release 2.2	The WCCP Version 2 feature provides several enhancements and features to the WCCP protocol, including: • The ability of multiple routers to service a content engine cluster. • Redirection of traffic other than HTTP (TCP port 80 traffic), including a variety of UDP and TCP traffic. • Optional authentication that enables you to control which routers and content engines become part of the service group using passwords and the HMAC MD5 standard. • A check on packets that determines which requests have been returned from the content engine unserviced. • Load adjustments for individual content engines to provide an effective use of the available resources while helping to ensure high quality of service (QoS) to the clients. The following commands were introduced or modified by this feature: **clear ip wccp**, **ip wccp**, **ip wccp group-listen**, **ip wccp redirect**, **ip wccp redirect exclude in**, **ip wccp version**, **show ip wccp**.
WCCP VRF Support	Cisco IOS XE Release 3.1S	The WCCP VRF Support feature provides enhancements to the existing WCCPv2 protocol, which supports VRF awareness. 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**