Configuring WCCPv2

This chapter contains the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your 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 "New and Changed Information"chapter or the Feature History table in this chapter.

Information About WCCPv2

WCCPv2 Overview

WCCPv2 enables the Cisco NX-OS router to transparently redirect packets to cache engines. WCCPv2 does not interfere with normal router operations. Using WCCPv2, the router can redirect requests on configured interfaces to cache engines rather than to intended host sites. With WCCPv2, the router can balance traffic loads across a cluster of cache engines (cache cluster) and ensure fault-tolerant and fail-safe operation in the cluster. As you add or delete cache engines from a cache cluster, WCCPv2 dynamically redirects the packets to the currently available cache engines.

WCCPv2 accepts the traffic at the cache engine and establishes the connection with the traffic originator (the client). The cache engine acts as if it were the original destination server. If the requested object is not available on the cache engine, the cache engine establishes its own connection out to the original destination server to retrieve the object.

Until Release 8.1(2), WCCPv2 is supported only on the Layer3 or SVI interfaces, for Cisco Nexus 7000 Series Switches.

WCCPv2 communicates between routers and cache engines on UDP port 2048.

By allowing a cache cluster to connect to multiple routers, WCCPv2 provides redundancy and a distributed architecture for instances when a cache engine must connect to many interfaces. In addition, WCCPv2 allows you to keep all the cache engines in a single cluster, which avoids the unnecessary duplication of web pages across several clusters.

WCCPv2 Service Types

A service is a defined traffic type that the router redirects to a cache engine with the WCCPv2 protocol.

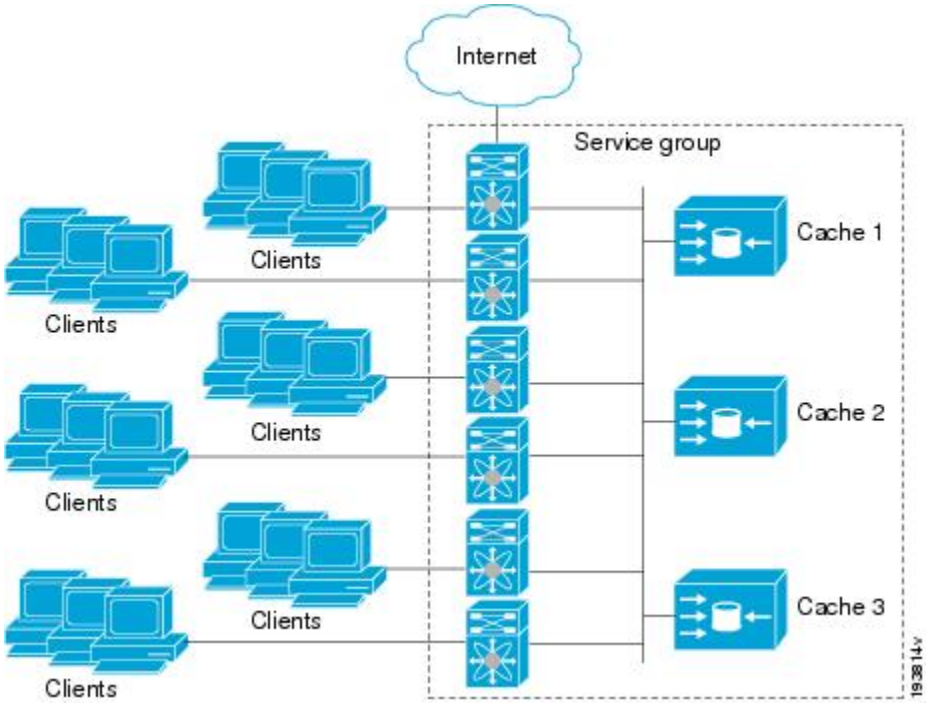
You can configure the router to run one of the following cache-related services:

- Well-known —The router and the cache engine know the traffic type, for example the web cache service on TCP port 80 for HTTP.
- Dynamic service—A service in which the cache engine describes the type of redirected traffic to the router.

WCCPv2 Service Groups

A service group is a subset of cache engines within a cluster and the routers connected to the cluster that are running the same service. The figure shows a service group within a cache cluster. The cache engines and the routers can be a part of multiple service groups.

Figure 1: WCCPv2 Cache Cluster and Service Group



You can configure a service group as open or closed. An open service group forwards traffic without redirection if there is no cache engine to redirect the traffic to. A closed service group drops traffic if there is no cache engine to redirect the traffic to.

The service group defines the traffic that is redirected to individual cache engines in that service group. The service group definition consists of the following:

- Service ID (0–255)
- Service Type
- Priority of the service group
- Protocol (TCP or UDP) of redirected traffic
- Service flags
- Up to eight TCP or UDP port numbers (either all source or all destination port numbers)

WCCPv2 Service Group Lists

WCCPv2 requires that each cache engine be aware of all the routers in the service group. You can configure a list of router addresses for each of the routers in the group on each cache engine.

The following sequence of events details how WCCPv2 configuration works:

1. You configure each cache engine with a list of routers.
2. Each cache engine announces its presence and generates a list of all routers with which it has established communications.

3. The routers reply with their view (list) of cache engines in the group.

The cache engines and routers exchange control messages every 10 seconds by default.

WCCPv2 Designated Cache Engine

WCCPv2 designates one cache engine as the lead. If there is a group of cache engines, the one seen by all routers and the one that has the lowest IP address becomes the designated cache engine. The designated cache engine determines how traffic should be allocated across cache engines. The traffic assignment method is passed to the entire service group from the designated cache engine so that the routers of the group can redirect the packets and the cache engines of the group can manage their traffic load better.

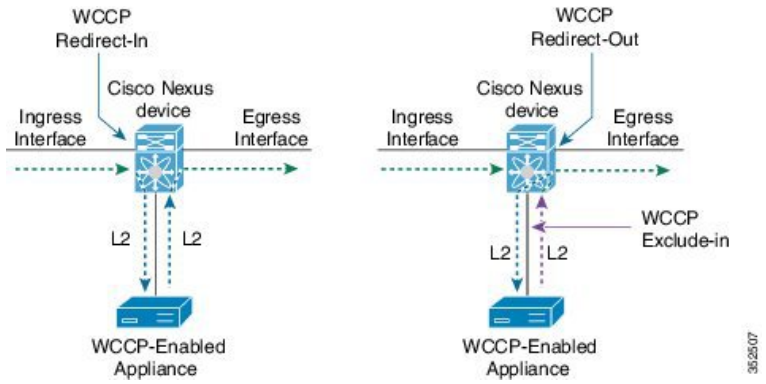
Cisco NX-OS uses the mask method to assign traffic. The designated cache engine assigns the mask and value sets to the router in the WCCP Redirect Assignment message. The router matches these mask and value sets to the source IP address, destination IP address, source port, and destination port of each packet. The router redirects the packet to the cache engine if the packet matches an assigned mask and value set. If the packet does not match an assigned mask and value set, the router forwards the packet without any redirection.

WCCPv2 Redirection

You can use an IP access list as a redirect list to specify a subset of traffic to redirect with WCCPv2. You can apply this access list for ingress or egress traffic on an interface. The figure shows how redirection applies to ingress or egress traffic.

You can also exclude ingress traffic on an interface but allow egress redirection on that interface.

Figure 2: WCCPv2 Redirection



Supported Modules for WCCPv2 Redirection

The following tables show the supported modules in Cisco NX-OS for WCCPv2 redirection.

Redirect-In

Table 1: Supported Modules for WCCPv2 Redirect-In—Same Module Type

Ingress module	Egress Module	Module used to connect to WCCPv2 enabled device
M	M	M
F2	F2	F2

Ingress module	Egress Module	Module used to connect to WCCPv2 enabled device
F2e	F2e	F2e
F3	F3	F3

Table 2: Supported Modules for WCCPv2 Redirect-In—Mixed Module Type

Ingress module	Egress Module	Module used to connect to WCCPv2 enabled device
M	F2e	F2e
M2/M3	M2/M3	F3
M2/M3	F3	M2/M3
F3	M2/M3	M2/M3
M2/M3	F3	F3
F3	M2/M3	F3
F3	F3	M2/M3
F2e	F2e	F3
F2e	F3	F2e
F3	F2e	F2e
F3	F3	F2e
F3	F2e	F3
F2e	F3	F3

Redirect-Out

Table 3: Supported Modules for WCCPv2 Redirect-Out—Same Module Type

Ingress module	Egress Module	Module used to connect to WCCPv2 enabled device
M	M	M
F2	F2 [1]	F2 [1]
F2e	F2e [1]	F2e [1]
F3	F3	F3

Note [1] Redirect-out and exclude-in are not supported on interface VLANs (SVIs).

Table 4: Supported Modules for WCCPv2 Redirect-Out—Mixed Module Type

Ingress module	Egress Module	Module used to connect to WCCPv2 enabled device
F2e	M	M
F2e	F2e	M
M	F2e	M
M2/M3	M2/M3	F3
F3 [2]	M2/M3	M2/M3
F3	M2/M3	F3
F2e [3]	F2e [4]	F3
F2e [3]	F3	F2e [5]
F3 [3]	F2e [4]	F2e [5]
F3 [3]	F3	F2e [5]
F3 [3]	F2e [4]	F3
F2e [3]	F3	F3

Note [2] Will not work if the F3 port is a FabricPath core port.

[3] WCCP redirect-out will not work if the ingress traffic is on a FabricPath VLAN.

[4] WCCP redirect-out is not supported on an F2e SVI.

[5] WCCP exclude-in is not supported on an F2e SVI.

WCCPv2 Authentication

WCCPv2 can authenticate a device before it adds that device to the service group. Message Digest (MD5) authentication allows each WCCPv2 service group member to use a secret key to generate a keyed MD5 digest string that is part of the outgoing packet. At the receiving end, a keyed digest of an incoming packet is generated. If the MD5 digest within the incoming packet does not match the generated digest, WCCP ignores the packet.

WCCPv2 rejects packets in any of the following cases:

- The authentication schemes differ on the router and in the incoming packet.

- The MD5 digests differ on the router and in the incoming packet.

You must configure the same authentication on all members of a WCCPv2 service group.

WCCPv2 Redirection Method

WCCPv2 negotiates the packet redirection method between the router and the cache engine. Cisco NX-OS uses this traffic redirection method for all cache engines in a service group.

WCCPv2 redirects packets using Layer 2 Destination MAC rewrite method, where WCCPv2 replaces the destination MAC address of the packet with the MAC address of the cache engine that needs to handle the packet. The cache engine and the router must be adjacent to Layer 2.

You can also configure an access control list (ACL), called a redirect list, for a WCCPv2 service group. This ACL can either permit a packet to go through the WCCPv2 redirection process or deny the WCCP redirection and send the packet through the normal packet forwarding procedure.

WCCPv2 Packet Return Method

WCCPv2 filters packets to determine which redirected packets have been returned from the cache engine and which packets have not. WCCPv2 does not redirect the returned packets, because the cache engine has determined that these packets should not be cached. WCCPv2 returns packets that the cache engine does not service to the router that transmitted them.

A cache engine may return a packet for one of the following reasons:

- The cache engine is overloaded and cannot service the packets.
- The cache engine is filtering certain conditions that make caching packets counterproductive, for example, when IP authentication has been turned on.

WCCPv2 negotiates the packet return method between the router and the cache engine. Cisco NX-OS uses this traffic return method for all cache engines in a service group.

WCCPv2 returns packets using the Destination MAC rewrite method, where WCCPv2 replaces the destination MAC address of the packet with the MAC address of the router that originally redirected the packet. The cache engine and the router must be adjacent to Layer 2.

High Availability for WCCPv2

WCCPv2 supports stateful restarts and stateful switchovers. A stateful restart occurs when the WCCPv2 process fails and is restarted. A stateful switchover occurs when the active supervisor switches to the standby supervisor. Cisco NX-OS applies the running configuration after a switchover.

Virtualization Support for WCCPv2

WCCPv2 supports virtual routing and forwarding (VRF) instances. VRFs exist within virtual device contexts (VDCs). By default, Cisco NX-OS places you in the default VDC and default VRF unless you specifically configure another VDC and VRF.

WCCP redirection occurs within a VRF. You must configure the WCCP cache engine so that the forward and return traffic to and from the cache engine occurs from interfaces that are a part of the same VRF.

The VRF used for the WCCP on an interface should match the VRF configured on that interface.

If you change the VRF membership of an interface, Cisco NX-OS removes all layer 3 configuration, including WCCPv2.

For more information, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

WCCPv2 Error Handling for SPM Operations

The Service Policy Manager (SPM) supervisor component acts as a data path manager for the WCCP Manager. The WCCP manager is shielded from the underlying platform specifics by the SPM and is portable to platform variations. The WCCP manager has a set of SPM APIs to pass the configurations that are mapped and programmed in the hardware. These APIs can process and parse the application data that is implemented and maintained in one single handler.

The interface redirects that failed to be programmed by the SPM are stored until there is a service group configuration change through the CLI or an RA message. The WCCP manager retries programming policies that failed previously.

The WCCP manager sends policy updates to the SPM in intervals to program TCAM entries in the hardware. These policy updates can be triggered by the CLI or through RA (Redirect-Assign) messages. When the WCCP is notified of an SPM error, a syslog message appears.

Licensing Requirements for WCCPv2

This feature does not require a license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

Prerequisites for WCCPv2

WCCPv2 has the following prerequisites:

- You must globally enable the WCCPv2 feature.
- You can only configure WCCPv2 on Layer 3 or VLAN interfaces (see the *Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*).
- If you configure VDCs, install the Advanced Services license and enter the desired VDC (see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*).

Guidelines and Limitations for WCCPv2

WCCPv2 has the following configuration guidelines and limitations:

- A WCCPv2 service group supports up to 32 routers and 32 cache engines.
- All cache engines in a cluster must include all routers that service the cluster in its configuration. If a cache engine within a cluster does not include one or more of the routers in its configuration, the service group detects the inconsistency and the cache engine is not allowed to operate within the service group.

- The cache engine cannot be on the same SVI with a redirect out statement.
- WCCPv2 works with IPv4 networks only.
- Any traffic that is coming from an M1-Series or M2-Series I/O module interface and going towards a Traffic Engineering (TE) Class-based Tunnel Selection (CBTS) tunnel will be dropped if you have configured the **ip wccp redirect exclude in** command on the inbound M1-Series or M2-Series I/O module interface or Switch Virtual Interface (SVI).
- WCCPv2 supports multiple service groups in the same direction (either inbound or outbound) on any Layer 3 interface, under the following conditions:
  - The access-list used must not have **deny ip any any** entry.
  - The access-list used for multiple service groups must not contain overlapping entries.

    The following is an example of an overlapping entry:

```
ip access-list wccp_acl1
 permit tcp 10.0.0.0/8 10.0.0.0/8
ip access-list wccp_acl2
 permit tcp 10.10.10.1/32 10.10.10.10/32
```

- Cisco NX-OS removes all Layer 3 configuration on an interface when you change the VDC, interface VRF membership, port-channel membership, or the port mode to Layer 2.
- Cisco NX-OS does not support WCCPv2 on tunnel interfaces.
- WCCPv2 is supported on all types of FEX devices.
- WCCP requires the client, server, and WCCP client to be on separate interfaces. If you migrate a topology from a Cisco Catalyst 6500 Series switch deployment, it might not be supported.
- F2 Series, F2e Series, M1 Series, and M2 Series modules support WCCPv2. However, F2 and F2e Series modules do not support egress WCCPv2 on an SVI including “exclude in” on SVI. F1 Series modules do not support WCCPv2.
- WCCPv2 redirect-in and redirect-out is fully supported in Cisco NX-OS Release 6.2 in non-mixed module VDCs. WCCPv2 is also support in mixed module VDC scenarios for most module combinations. For complete support details, see Supported Modules for WCCPv2 Redirection, on page 4
- For egress WCCPv2, traffic is not redirected when the ingress includes F2 series modules, and the next-hop is pointing to an SVI interface or subinterface of any module. If the egress WCCP policy is applied on a SVI or subinterface and if the packet ingresses on a F2 module, the same limitation applies.
- Beginning with Cisco NX-OS Release 5.2(4), policy-based routing and WCCPv2 are supported on the same interface. However, policy-based routing with statistics and WCCPv2 is supported on the same interface only if bank chaining is disabled.
- GRE redirection/return and hash assignment are not supported on a Cisco Nexus 7000 Series switch.
- Traffic might encounter a vPC loop and drop if you have Web Cache Control Protocol (WCCP) and vPC on your Cisco Nexus 7000 Series switch and the traffic migrates from a Cisco Nexus 65xx switch to your switch. Traffic that comes from a vPC member port and crosses a vPC peer-link is not permitted to egress any vPC member port. However, it can egress any other type of port, such a Layer 3 port or an orphan port. This behavior is expected.

  If traffic drops after you configure WCCP and vPC on your Nexus 7000 Series switch and based on your design, you can perform one of the following tasks to avoid the vPC loop:

- Configure a Layer 2 trunk to carry the traffic in question.
- Enable a peer gateway.
- Shut down one of the member ports in the vPC.

Refer Best Practices for Virtual Port Channels (vPC) on Cisco Nexus 7000 Series Switches for more details.

- If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.
- The following restrictions apply to the redirect-list, ACL:
  - Permit statements in the redirect ACL will consume more security TCAM entries compared to deny statements. Ensure the TCAM does not become oversubscribed.
  - The ACL must be an IPV4 simple ACL.
  - The protocol must be IP or TCP.
  - Only individual source or destination port numbers may be specified; port ranges cannot be specified.
  - The use of fragments or options is not permitted.

WCCPv2 Default Settings

Parameters	Default
Authentication	No authentication
WCCPv2	Disable

Configuring WCCPv2

To configure WCCPv2, perform these tasks in this chapter:

Procedure

Step 1 Enable the WCCPv2 feature.

Step 2 Configure a WCCPv2 service group.

Step 3 Apply WCCPv2 redirection to an interface.

Enabling and Disabling WCCPv2

Before you begin

- Enable the WCCPv2 feature.
- Ensure you are in the correct VDC (or use the **switchto vdc** command

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	(config)# [**no**] **feature wccp**	Enables or disables the WCCPv2 feature in a VDC. Use the **no** form of the command to disable the feature.
Step 3	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Configuring a WCCPv2 Service Group

Note You must enter the **ip wccp** command with all your required parameters. Any subsequent entry of the **ip wccp** command overwrites the earlier configuration.

Before you begin

- Enable the WCCPv2 feature.
- Ensure you are in the correct VDC (or use the **switchto vdc** command

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **ip wccp** {*service-number* | **web-cache**} [**mode** {**open** [**redirect-list** *acl-name*] | **closed service-list** *acl-name*}][**password** [**0-7**] *pwstring*]	Creates an open or closed mode service group. The service list identifies a named extended IP access list that defines the packets that will match the service. This list is required only when the service is defined as closed mode Optional parameters are as follows: • **mode**—Configures the service group in open or closed mode. On a service list, the mode controls the traffic type that the

	Command or Action	Purpose
		service group handles. The default is open. For closed mode, use this keyword to configure an IP access list to define the traffic type that matches this service. Closed mode for dynamic service groups requires a service list ACL that specifies the protocol and port information that is used for the service group. If there are no members in the service group, packets matching the service-list ACL are dropped. • **password**—Configures MD5 authentication for a service group. Use **password** *0 pwstring* to store the password in clear text. Use **password 7** *pwstring* to store the password in encrypted form. You can use the **password 7** keywords for an already encrypted password. • **redirect-list**—Configures a global WCCPv2 redirection list for the service group to control the traffic that is redirected to the cache engine. • **service-list**—Configures an IP access list that defines the traffic type redirected by the service group. • The *service-number* range is from 1 to 255. The *acl-name* can be any case-sensitive, alphanumeric string up to 64 characters. The *pwstring* can be any case-sensitive, alphanumeric string up to eight characters.
Step 3	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Applying WCCPv2 Redirection to an Interface

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **interface ethernet** *number*	Enters interface configuration mode.

	Command or Action	Purpose
Step 3	switch(config-if)# **ip wccp** {*service-number* **redirect**{**in** | **out**} | **web-cache** | **redirect** {**in** | **out**}}	Applies the specified type of WCCPv2 redirection to the interface. The command examples show the following: • WCCPv2 redirection applied on the ingress or egress traffic for this interface. • WCCPv2 redirection applied on the ingress or egress web cache traffic for this interface. • Ingress traffic excluded from WCCP redirection on this interface. **Note** **ip wccp web-cache redirect out** command is not supported in WCCP on BDI interface.
Step 4	switch(config)# **copy running-config startup-config**	(Optional) Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure a router to redirect web-related packets without a destination of 19.20.2.1 to the web cache:

```
switch(config)# access-list 100
switch(config-acl)# deny ip any host 192.0.2.1
switch(config-acl)# permit ip any any
switch(config-acl)# exit
switch(config)# ip wccp web-cache redirect-list 100
switch(config)# interface ethernet 2/1
switch(config-if)# ip wccp web-cache redirect out
```

This example shows sample configuration for un-supported features:

```
switch# configure terminal
switch(config)# interface Bdi555
switch(config-if)# ip wccp redirect exclude in
This will remove all redirect-in on the interface. Proceed (y/n)?  [no] y
ERROR: Exclude in not supported on BDI

switch(config-if)# ip wccp 62 redirect out
ERROR: Redirect out not supported on BDI
```

This example shows a running-configuration, followed by a verification command that displays the L3VNI-BDI configuration details. Replace the placeholders with relevant values for your setup. The example considers that interface 555 is configured for BDI.

```
switch (config)# show running-configuration interface bdi 555

!Command: show running-config wccp
!Time: Thu Sep 25 02:46:02 2017
```

```
version 8.2(1)
interface Bdi555
   description L3VNI-BDI
   no shutdown
   vrf member vrf5000
   no ip redirects
   ip forward
   ip pin sparse-mode
 ip wccp 61 redirect in
```

This example show running-configuration for WCCP configuration on BDI interface. Replace the placeholders with relevant values for your setup.

```
switch (config)# show running-configuration wccp

!Command: show running-config wccp
!Time: Thu Sep 25 02:46:02 2017

version 8.2(1)
feature wccp

vrf context vrf5000
   ip wccp web-cache
   ip wccp 61
   ip wccp 62

interface Bdi555
   vrf member vrf5000
   ip wccp 61 redirect in
```

Configuring WCCPv2 in a VRF

Note You must enter the **ip wccp** command with all your required parameters. Any subsequent entry of the **ip wccp** command overwrites the earlier configuration.

Before you begin

- Enable the WCCPv2 feature.
- Ensure you are in the correct VDC (or use the **switchto vdc** command

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **vrf context** *vrf-name*	Enters VRF configuration mode. The vrf-name can be any case-sensitive, alphanumeric string up to 63 characters.
Step 3	switch(config)# **ip wccp** {*service-number* | **web-cache**} [**mode** {**open** [**redirect-list**	Creates an open or closed mode service group. The service list identifies a named extended IP access list that defines the packets that will

	Command or Action	Purpose
	acl-name] | **closed service-list** *acl-name*}][**password** [**0-7**] *pwstring*]	match the service. This list is required only when the service is defined as closed mode Optional parameters are as follows: • **mode**—Configures the service group in open or closed mode. On a service list, the mode controls the traffic type that the service group handles. The default is open. For closed mode, use this keyword to configure an IP access list to define the traffic type that matches this service. Closed mode for dynamic service groups requires a service list ACL that specifies the protocol and port information that is used for the service group. If there are no members in the service group, packets matching the service-list ACL are dropped. • **password**—Configures MD5 authentication for a service group. Use **password** *0 pwstring* to store the password in clear text. Use **password 7** *pwstring* to store the password in encrypted form. You can use the **password 7** keywords for an already encrypted password. • **redirect-list**—Configures a global WCCPv2 redirection list for the service group to control the traffic that is redirected to the cache engine. • **service-list**—Configures an IP access list that defines the traffic type redirected by the service group. • The *service-number* range is from 1 to 255. The *acl-name* can be any case-sensitive, alphanumeric string up to 64 characters. The *pwstring* can be any case-sensitive, alphanumeric string up to eight characters.
Step 4	(Optional) switch(config-vrf)# **show ip wccp** [**vrf** *vrf-name*]	Displays information about WCCPv2. The vrf-name can be any case-sensitive, alphanumeric string up to 64 characters.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example shows how to configure WCCPv2 in VRF Red on interface Ethernet 2/1:

```
switch# configure terminal
switch(config)# vrf context Red
switch(config-vrf)# ip wccp web-cache password Test1 redirect-list httpTest
switch(config-vrf)# interface ethernet 2/1
switch(config-if)# vrf member Red
switch(config-if)# ip wccp web-cache redirect out
```

Verifying the WCCPv2 Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show ip wccp [**vrf** *vrf-name*] [*service-number* | **web-cache**]	Displays the WCCPv2 status for all groups or one group in a VRF.
show ip interface [*ethernet-number*]	Displays the WCCPv2 interface information.
show ip wccp [*service-number* | **web-cache**]	Displays the WCCPv2 service group status.
show ip wccp [*service-number* | **web-cache**] **detail**	Displays the clients in a WCCPv2 service group.
show ip wccp [*service-number* | **web-cache**] **mask**	Displays the WCCPv2 mask assignment.
show ip wccp [*service-number* | **web-cache**] **service**	Displays the WCCPv2 service group definition.
show ip wccp [*service-number* | **web-cache**] **view**	Displays the WCCPv2 group membership.

Configuration Examples for WCCPv2

This example shows how to configure WCCPv2 authentication on router redirect web-related packets without a destination of 192.0.2.1 to the web cache:

```
access-list 100
 deny ip any host 192.0.2.1
 permit ip any any
feature wccp
ip wccp web-cache password 0 Test1 redirect-list 100
interface ethernet 1/2
 ip wccp web-cache redirect out
 no shutdown
```

This example shows the sample output when WCCP is configuration in a VRF.

```
switch(config)# show ip wccp vrf vrf5000

VRF vrf5000 WCCP information:
    Router information:
        Router Identifier:                   50.50.50.1
        Protocol Version:                    2.0
```

```
    Service Identifier: web-cache
        Number of Service Group Clients:      1
        Number of Service Group Routers:      1
        Service mode:                         Open
        Service Access-list:                  -none-
        Redirect Access-list:                 -none-
    Service Identifier: 61
        Number of Service Group Clients:      1
        Number of Service Group Routers:      1
        Service mode:                         Open
        Service Access-list:                  -none-
        Redirect Access-list:                 -none-
    Service Identifier: 62
        Number of Service Group Clients:      1
        Number of Service Group Routers:      1
        Service mode:                         Open
        Service Access-list:                  -none-
        Redirect Access-list:                 -none-
```

The following example shows a verification command to display the kind of service for WCCP.

```
switch(config)# show ip wccp vrf vrf5000 61 service
WCCP service information definition:
    Type:          Dynamic
    Id:            61
    Priority:      34
    Protocol:      6
    Options:       0x00000501
    --------
        Mask/Value sets:  1
        Value elements :  16
        Ports:            -none-
```

The following example shows a verification command to display cache engine information, after the connection with the cache engine is established

```
switch(config)# show ip wccp vrf vrf5000 61 view

WCCP Router Informed of:
50.50.50.1

WCCP Cache Engines Visible:
10.10.10.3

WCCP Cache Engines Not Visible:
-none-
```

Related Documents for WCCPv2

Related Topic	Document Title
WCCPv2 CLI commands	*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*
IP ACLs	*Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x*

Standards for the WCCPv2

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

Feature History for WCCPv2

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

Feature Name	Release	Feature Information
WCCPv2 on BDI	8.2(1)	Added support on BDI interface.
WCCPv2 Redirection	7.3(0)DX(1)	Added support for M3 module.
WCCPv2	5.2(4)	Added support for policy-based routing and WCCPv2 on the same interface if bank chaining is disabled.
WCCPv2 Error Handling for SPM Operations	5.1(1)	This feature was added.
WCCPv2	4.2(1)	This feature was introduced.