



## Configuring the MSFC Cisco IOS Features

---

This chapter describes the Cisco IOS features that are used with the Catalyst operating system to provide feature functionality and parity between these operating systems.

These sections describe the Cisco IOS features that are used with the Catalyst operating system:

- [IP-in-IP Tunneling, page 56-1](#)
- [WCCP, page 56-2](#)

### IP-in-IP Tunneling

IP-in-IP tunneling allows a mobile host to move between networks without changing its IP address. IP-in-IP tunneling allows an IPv4 datagram to be encapsulated within another IPv4 datagram and carried as a payload to its destination. This IPv4 within IPv4 encapsulation is a type of Generic Routing Encapsulation (GRE) that is similar to GRE tunneling.

The PFC3 and DFC3s support the following tunnel commands:

- **tunnel destination**
- **tunnel mode gre**
- **tunnel mode ipip**
- **tunnel source**
- **tunnel ttl**
- **tunnel tos**

Other supported types of tunneling are run in the software on the MSFC3.

Enter the **tunnel ttl** command (default 255) to set the TTL of encapsulated packets.

Enter the **tunnel tos** command, if present, to set the ToS byte of a packet when it is encapsulated. If the **tunnel tos** command is not present and you do not enable QoS, the ToS byte of a packet sets the ToS byte of the packet when it is encapsulated. If the **tunnel tos** command is not present and you enable QoS, the ToS byte of a packet as modified by PFC QoS sets the ToS byte of the packet when it is encapsulated.

To configure GRE tunneling and IP-in-IP tunneling, refer to these URLs:

[http://www.cisco.com/en/US/docs/ios/12\\_2/interface/configuration/guide/icflogin.html](http://www.cisco.com/en/US/docs/ios/12_2/interface/configuration/guide/icflogin.html)

To configure the **tunnel tos** and **tunnel ttl** commands, refer to this URL:

[http://www.cisco.com/en/US/docs/ios/12\\_0s/feature/guide/12s\\_tos.html](http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/12s_tos.html)

## IP-in-IP Configuration Guidelines

This section describes the guidelines for configuring IP-in-IP tunneling:

- Each hardware-assisted tunnel must have a unique source.
- Hardware-assisted tunnels cannot share a source even if the destinations are different.
- Use secondary addresses on loopback interfaces or create multiple loopback interfaces.
- Each tunnel interface uses one internal VLAN.
- Each tunnel interface uses one additional router MAC address entry per router MAC address.
- The PFC3A does not support any PFC QoS features on tunnel interfaces.
- The PFC3B and PFC3BXL support PFC QoS features on tunnel interfaces.
- The PFC3 does not support GRE tunnel encapsulation and deencapsulation of multicast traffic.
- The MSFC3 supports tunnels that are configured with egress features on the tunnel interface. Examples of egress features are output Cisco IOS ACLs, NAT and PAT (for inside-to-outside translation), TCP intercept, context-based access control (CBAC), and encryption.

## WCCP

The Web Cache Communication Protocol (WCCP) allows you to redirect traffic to a cache engine (web caches) and manage cache engine clusters (cache farms).



### Note

- Release 12.2(17d)SXB1 and later releases support WCCP on Supervisor Engine 2.
- Release 12.2(18)SXD1 and later releases support WCCP on Supervisor Engine 720.
- To use the WCCP Layer 2 PFC redirection feature, configure WCCP on the Catalyst 6500 series switch as described in this chapter and configure accelerated WCCP on the cache engine as described in the following publication:  
[http://www.cisco.com/en/US/docs/app\\_ntwk\\_services/waas/acns/v42/configuration/guide/transprt.html](http://www.cisco.com/en/US/docs/app_ntwk_services/waas/acns/v42/configuration/guide/transprt.html)
- A future release of Cisco Application and Content Networking System (ACNS) software, Release 4.2.2 and later releases support the **ip wccp service accelerated** command with a PFC2.

Because the WCCP service group list is scanned in the order in which service groups are created, not by priority, with multiple dynamic WCCP services defined the traffic that matches the selection criteria for more than one service group is not redirected to the service group with the highest priority. This problem is resolved in Release 12.2(18)SXE.

In Release 12.2(18)SXE where caveat [CSCec55429](#) is resolved, after a number of Web Cache Communication Protocol (WCCP) “cache lost” and “cache found” events have occurred for all the caches in a service group, spurious memory accesses might occur, the addition and deletion of WCCP services might fail, and the **show ip wccp** command displays the WCCP service, but the output of the **show ip wccp service\_number** command does not show the WCCP service. This problem is resolved in Release 12.2(18)SXE.

Configuring WCCPv2 on a Supervisor Engine 720 causes high CPU utilization. This problem is resolved in Release 12.2(18)SXD4.

Network Address Translation (NAT) does not work with WCCP configured. This problem is resolved in Release 12.2(18)SXD1.

WCCP-redirectioned packets that have no next-hop ARP cache entry are process switched to generate an ARP request, but because of the WCCP redirection, no ARP request is sent and the ARP cache is never populated for the next hop and subsequent WCCP-redirectioned packets continue to be process switched. This problem is resolved in Release 12.2(17d)SXB2.

For more information about Web Cache Control Protocol (WCCP) support with Supervisor Engine 720, refer to this URL:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/wccp.html>

For more information about Web Cache Control Protocol (WCCP) that is supported only with Supervisor Engine 2, refer to this URL:

<http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2SXF/native/configuration/guide/wccp.html>

