

This article describes how to troubleshoot Web Cache Communication Protocol version 2 (WCCPv2) on Cisco NX-OS.

Guide Contents
Troubleshooting Overview
Troubleshooting Installs, Upgrades, and Reboots
Troubleshooting Licensing
Troubleshooting VDCs
Troubleshooting CFS
Troubleshooting Ports
Troubleshooting vPCs
Troubleshooting VLANs
Troubleshooting STP
Troubleshooting Routing
Troubleshooting Unicast Traffic
Troubleshooting WCCP (this section)
Troubleshooting Memory
Troubleshooting Packet Flow Issues
Troubleshooting FCoE
Before Contacting Technical Support
Troubleshooting Tools and Methodology

Contents

- [1 Information About Troubleshooting WCCP](#)
- [2 Problem Scenarios](#)
 - ◆ [2.1 Reasons For Service Group Startup Failure](#)
 - ◆ [2.2 Client Loss](#)
 - ◆ [2.3 Packet Redirect Counts Not Incrementing](#)
 - ◆ [2.4 Potential problems](#)

Information About Troubleshooting WCCP

The Web Cache Communication Protocol (WCCP) is a content-routing protocol that enables a Cisco NX-OS router to transparently redirect packets to cache engines. It has built-in load balancing, scaling, fault tolerance, and service-assurance (failsafe) mechanisms. WCCP version 2 (WCCPv2) is the only version supported on Cisco NX-OS devices.

See the [Configuring WCCPv2](#) chapter in the [Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide](#) for more information on WCCPv2.

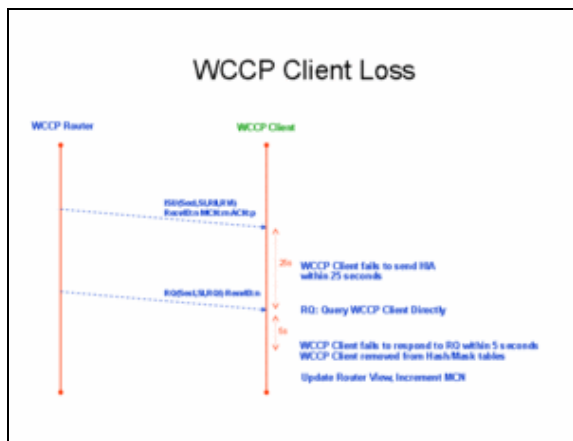
Problem Scenarios

Reasons For Service Group Startup Failure

- WCCP Client fails to see ISU messages and is stuck in the *NOT Usable* state.
 - ◆ Confirm by enabling the WCCP event debugging messages and looking for bad Receive ID messages.
 - ◆ The reason for the failure would in general be a connectivity problem and may be mismatched speed or duplex settings.
- The WCCP Client is requesting a capability which is not supported by the router probably because of platform limitations.
 - ◆ This can be confirmed by enabling WCCP event debugging and looking for Capability Mismatch messages.
- The WCCP Client is requesting a capability which is not supported by the service group.
 - ◆ This will occur if a service group is already formed and the WCCP Client configuration does not match the existing service.
 - ◆ This is a misconfiguration of the WCCP Client and can be confirmed by enabling WCCP event debugging and looking for Capability Mismatch messages.
- HIA event messages may indicate other reasons why the router rejected an incoming "Here I Am" message.
- Some WCCP clients don't adhere to the configured forward/return methods and prefer to always default to "GRE" forward/return. The Cisco Nexus 7000 requires L2 forward/return methods. ACNS, WAAS, etc. might need to be configured with the **assign-method-strict** option. This type of failure can be seen with packet traces. The client does not respond to the Cisco Nexus 7000 with a sent RXID but will keep sending HIA with a receive ID of 0.

Client Loss

A WCCP Client is removed from a service group when the router loses contact with the WCCP Client.



The reasons why this might occur include:

- The service group has been disabled on the WCCP Client.
 - ◆ Check the WCCP Client configuration.
- The service definition has been changed on the WCCP Client
 - ◆ Check the WCCP Client configuration.
- Loss of physical connectivity to the WCCP Client.
 - ◆ Verify connectivity using the **ping** command.
- Message loss between the router and WCCP Client perhaps because of a heavily utilized link or a flapping interface.
 - ◆ Enable WCCP packet debugging and confirm message exchange.

- WCCP Client loss from a service group is indicated by the console message:
%WCCP-1-SERVICELOST: Service *Service ID* lost on WCCP client *IP address*

Packet Redirect Counts Not Incrementing

- The WCCP service not present on the interface.
 - ◆ Verify using the **show running-config interface ifname** command.
- The WCCP service is not active.
 - ◆ Check the service state using the **show ip wccp web-cache | service-number detail** command.
 - ◆ Verify using the **show running-config wccp** command.
- The WCCP service definition does not match the traffic to be redirected.
 - ◆ Check the service definition using the **show ip wccp service-number service** command.
 - ◆ WCCP service mismatch is indicated by the console message:
%WCCP-1-SERVICEMISMATCH: Service *Service ID* mismatched on WCCP client *IP address*
- Matching traffic is excluded from redirection by the redirect ACL.
 - ◆ Monitor the redirect ACL count using the **show ip wccp service-number** command.
- No traffic matching the WCCP service is traversing the interface.
 - ◆ Define an extended IP access list to get an independent count of matching traffic.
- All traffic redirection is done by the platform hardware.

Potential problems

- Direct communication between WCCP client and host
 - ◆ The Cisco Nexus 7000 requires that the host running the browser, the WCCP clients, be attached to different L3 interfaces (the hosts cannot be present in the same subnet).
- Service definition mismatch
 - ◆ There is no mechanism on a Cisco WCCP Client to mark two services as complementary. This also appears to be true for third party vendors. This has the consequence that the two services can drift apart over time. On service startup there is usually no problem however, as WCCP clients leave and rejoin either of the services the assignments change independently meaning that an outgoing connection and the corresponding incoming connection may not be redirected to the same WCCP Client. If that happens the configuration is broken.
 - ◆ Check for this condition by comparing the assignments shown with the **show ip wccp [web-cache | service number] detail** command. The only way currently to correct the condition is to restart both services.
- Asymmetric routing
 - ◆ As long as the incoming connection returns to any router in the complementary service group that will happen automatically. Note that the connection does not have to go to the exact same router as the outgoing connection, just the same service group. In any given network the routes to a particular destination may be numerous which raises the possibility that traffic returning from an origin server may take a different route to the outgoing traffic and fail to hit routers in the complementary service group. In that case the connection will not be redirected and the configuration will be broken. There is no way round this other than to ensure that there is no asymmetric routing taking place.