

Troubleshoot Unicast IP Routing Involving CEF on Catalyst 6500/6000 Series Switches with a Supervisor Engine 2 and Running CatOS System Software

Document ID: 20626

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Overview of CEF

Forwarding Information Base (FIB)

- Adjacency Table

How to Read the FIB and Adjacency Table on PFC2

Troubleshooting Method

Case Study 1: Connectivity to a Host in a Directly Connected Network

- Troubleshooting Steps
- Remarks and Conclusions

Case Study 2: Connectivity to a Remote Network

- Troubleshooting Steps
- Remarks and Conclusions

Case Study 3: Load Balancing to Several Next Hops

Case Study 4: Default Routing

- Default Route Exists in the MSFC2 Routing Table
- No Default Route in the Routing Table

Other Troubleshooting Tips and Known Issues

- Issuing the show mls cef mac Command
- Shadow TCAM
- Default Routing Broken

Related Information

Introduction

This document should be used as a guide to troubleshoot unicast IP routing on Catalyst 6500/6000 switches with Supervisor Engine 2, Policy Feature Card 2 (PFC2), Multilayer Switch Feature Card 2 (MSFC2). Unicast routing on the Supervisor Engine 2 is done using Cisco Express Forwarding (CEF). This document only concerns IP routing on the Catalyst 6500/6000 series equipped with Supervisor Engine 2, PFC2, MSFC2. This document is not valid for a Catalyst 6500/6000 with Supervisor Engine 1 (or 1A) or for the Multilayer Switch Module (MSM). This document is valid only for switches running Catalyst OS (CatOS) system software on the Supervisor Engine, and not for the Cisco IOS® System Software.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Overview of CEF

CEF was originally a Cisco IOS Software switching technique designed to route packets faster. CEF is much more scalable than fast switching. (There is no need to send the first packet to process switching.) The Catalyst 6500 with Supervisor Engine 2 uses a hardware-based CEF forwarding mechanism implemented on the PFC2. CEF mainly uses two tables to store the information needed for routing: the Forwarding Information Base (FIB) and the adjacency table.

Forwarding Information Base (FIB)

CEF uses a FIB to make IP destination prefix-based switching decisions (longest match first). The FIB is conceptually similar to a routing table or information base. It maintains a mirror image of the forwarding information contained in the IP routing table. When routing or topology changes occur in the network, the IP routing table is updated, and those changes are reflected in the FIB. The FIB maintains the next hop address information based on the information in the IP routing table. Due to a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes and eliminates the need for route cache maintenance that is associated with switching paths, such as fast switching and optimum switching. There is always a match in the FIB, whether it be default or wildcard.

Adjacency Table

Nodes in the network are said to be adjacent if they can reach each other with a single hop across a link layer. In addition to the FIB, CEF uses adjacency tables to prepend Layer 2 (L2) addressing information. The adjacency table maintains L2 next hop addresses for all FIB entries. This means that a complete FIB entry contains a pointer to a location in the adjacency table that holds the L2 rewrite information for the next hop to reach the final IP destination. In order for the hardware CEF to work on the Catalyst 6500/Supervisor Engine 2 system, IP CEF needs to run on the MSFC2.

How to Read the FIB and Adjacency Table on PFC2

The FIB table of the PFC2 should be exactly the same as the FIB table on the MSFC2. On the PFC2, all IP prefixes in the FIB are stored in a ternary content addressable memory (TCAM) and are sorted by mask length, starting with the longest mask. This means that you first find all the entries with a mask of 32 (host entry); next, you find all entries with a mask length of 31, and so on, until you reach an entry with a mask length of 0. This is the default entry. The FIB is read sequentially, and the first hit is used as a match. Consider this sample FIB table on PFC2:

```
Cat6k> (enable) show mls entry cef
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
```

```

15 receive 0.0.0.0 255.255.255.255

!--- This is the first entry with mask length 32.

15 receive 255.255.255.255 255.255.255.255
15 receive 192.168.254.254 255.255.255.255
15 receive 10.48.72.237 255.255.255.255
15 receive 10.48.72.0 255.255.255.255
15 receive 10.48.72.255 255.255.255.255
15 receive 192.168.222.7 255.255.255.255
15 receive 192.168.100.254 255.255.255.255
15 receive 192.168.10.254 255.255.255.255
15 resolved 192.168.199.3 255.255.255.255 192.168.199.3 1
15 resolved 192.168.222.2 255.255.255.255 192.168.222.2 1
15 resolved 192.168.199.2 255.255.255.255 192.168.199.2 1
15 resolved 192.168.254.252 255.255.255.255 192.168.199.3 1

!--- This is the last entry with mask length 32.

15 connected 192.168.222.0 255.255.255.252

!--- This is the only entry with mask length 30.

15 receive 224.0.0.0 255.255.255.0

!--- This is the first entry with mask length 24.

15 connected 10.48.72.0 255.255.255.0
15 connected 192.168.10.0 255.255.255.0
15 connected 192.168.11.0 255.255.255.0
15 connected 192.168.100.0 255.255.255.0
15 connected 192.168.101.0 255.255.255.0
15 connected 192.168.199.0 255.255.255.0

!--- This is the last entry with mask length 24.

15 connected 127.0.0.0 255.0.0.0

!--- This is the entry with mask length 8.

15 wildcard 0.0.0.0 0.0.0.0

!--- This is the entry with mask length 0.

```

Each entry consists of the following fields:

- Mod The MSFC2 that installs the entry is either 15 or 16, dependent on which is the designated MSFC2.
- FIB-Type The type associated with this specific entry. The possible FIB-Types are:
 - ◆ receive The prefix associated with MSFC interfaces. This contains a prefix with a mask of 32 corresponding to the IP address of the MSFC interfaces and an IP address of the broadcast subnet.
 - ◆ resolved The prefix associated with a valid next hop address. This contains any prefix with a resolved adjacency for the next hop.
 - ◆ connected The prefix associated with a connected network.
 - ◆ wildcard This matches all entries (drop or MSFC redirect). This entry is only present if there is no default entry, and is present with a mask length of 0.
 - ◆ default The default route. As the wildcard entry, it matches all subnets and is present with a mask length of 0. It points to the next hop. This default CEF entry is only present if there is a default route present in the routing table.

- ◆ drop All packets matching an entry with a drop are dropped.
- Destination-IP The destination IP address or IP subnet concerned.
- Destination-Mask The mask associated with the entry. As you can see in the example above, the FIB is ranked starting with the longest mask (255.255.255.255), and ending with the shortest possible mask (0.0.0.0).
- Next-Hop IP Displays the next hop IP, if it exists.

You can view the complete adjacency table by entering this command:

```
Cat6k> (enable) show mls entry cef adjacency
Mod:15
Destination-IP : 192.168.98.2 Destination-Mask : 255.255.255.255
FIB-Type :resolved
AdjType NextHop-IP NextHop-Mac VLAN Encp Tx-Packets Tx-Octets
-----
connect 192.168.98.2 00-90-21-41-c5-57 98 ARPA 0 0
```

Note: This output contains an entry similar to that found in the sample FIB table, above, for each of the resolved (or default) CEF entries in the FIB.

Troubleshooting Method

Before providing some examples and details on troubleshooting, this section summarizes the methods that are followed to troubleshoot connectivity or reachability to a specific IP address. Keep in mind that the CEF table on the PFC2 mirrors the CEF table on the MSFC2. Therefore, PFC2 only holds the correct information to reach an IP address if the information known by the MSFC2 is also correct. As such, you always need to verify the information below.

From the MSFC2:

Complete these steps:

1. Verify that the information held in the IP routing on the MSFC2 table is correct by issuing the **show ip route** command (or the **show ip route x.x.x.x** command, to avoid browsing the complete routing table), then verifying that the output contains the expected next hop.

If not, you need to check your routing protocol, configuration, routing protocol neighbor, and any other troubleshooting that is relevant to the routing protocol that you are running.

2. Verify that the next hop (or the final destination for a connected network) has a correct resolved Address Resolution Protocol (ARP) entry on the MSFC2 by issuing the **show ip arp next_hop_ip_address** command, then verifying that the ARP is resolved and contains the correct MAC address.

If the MAC address is incorrect, you need to verify whether another device owns that IP address. Eventually, you need to track the switch level on the port that connects the device that owns that MAC address. If the ARP entry is incomplete, it means that you did not get any replies from that host. You need to verify that the host is up and running. A sniffer may be used on the host to see if it gets the ARP reply and if it answers correctly.

3. Verify that the CEF table on the MSFC2 contains the correct information and that adjacency is resolved by performing these steps:
 - a. Issue the **show ip cef destination_network** command to verify that the next hop in the CEF table matches the next hop in the IP routing table (from Step 1, above).
 - b. Verify that the adjacency is correct by issuing the **show adjacency detail | begin next_hop_ip_address** command.

This should contain the same MAC address of the ARP seen in Step 2, above.

If Steps 1 and 2, above, provide correct results, but Steps 3a or 3b are failing, you are facing a Cisco IOS Software CEF issue that is likely not related to the Catalyst 6500/6000. You must try to clear the ARP table and the IP routing table.

From the PFC2:

Complete these steps:

1. Verify that the FIB information stored on the PFC2 is correct and matches the information stored in the CEF table on the MSFC2 (as seen in Step 3, above) by issuing the **show mls entry cef ip destination_ip_network/destination_subnet_mask** command, then verifying that the next hop IP address is the one you expect.

If the information does not match the results in Step 3, above, it points to a communication problem between the MSFC2 and the PFC2 (internal to the Catalyst 6500/6000). Verify that there is not a known bug for the CatOS of the PFC2 or the Cisco IOS Software of the MSFC2 that you are running. You can restore the correct entry by issuing the **clear ip route** command on the MSFC2 .

2. Verify the adjacency table on the PFC2 by issuing the **show mls entry cef ip next_hop_ip_address/32 adjacency** command, then verifying that it contains the same MAC address as the one seen in Steps 2 and 3b of the From the MSFC2 section, above.

If the adjacency in the PFC2 does not match the adjacency for the next hop in Step 3b, you are probably facing an issue of internal communication between MSFC2 and PFC2. You can try clearing the adjacency to restore the correct information.

Case Study 1: Connectivity to a Host in a Directly Connected Network

This simple case provides a study of the connectivity between:

- host 1 in VLAN 10 with an IP address of 192.168.10.10
- host 2 in VLAN 199 with an IP address of 192.168.199.3

This is a sample of the MSFC2 configuration output:

```
interface VLAN 10
description Server VLAN
ip address 192.168.10.1 255.255.255.0
no ip redirects
!
interface VLAN 199
ip address 192.168.199.1 255.255.255.0
```

Note: It is important to note that the Catalyst 6500/6000 with Supervisor Engine 2 and MSFC2 is routing using CEF in hardware. There is nothing to configure for it. CEF cannot be disabled on the MSFC2.

Troubleshooting Steps

Follow the procedures highlighted in the Troubleshooting Method section of this document to verify the path to reach IP address 192.168.199.3.

1. Verify the IP routing table by issuing either of these commands:

```

◆ Cat6k-MSFC2# show ip route 192.168.199.3
Routing entry for 192.168.199.0/24
Known via "connected", distance 0, metric 0 (connected, via interface)
Routing Descriptor Blocks:
* directly connected, via VLAN 199
Route metric is 0, traffic share count is 1

```

or

```

◆ Cat6k-MSFC2# show ip route | include 192.168.199.0
C 192.168.199.0/24 is directly connected, VLAN 199

```

In both of these command outputs, you can see that the destination is in a directly connected subnet. As such, there is no next hop to the destination.

2. Verify the ARP entry on the MSFC2.

In this case, verify that there is an ARP entry for the destination IP address by issuing this command:

```

Cat6k-MSFC2# show ip arp 192.168.199.3
Protocol Address      Age (min) Hardware      Addr Type Interface
Internet 192.168.199.3 176          0030.7150.6800 ARPA VLAN 199

```

3. Verify the CEF and adjacency table on the MSFC2.

a. Verify the CEF table by issuing this command:

```

Cat6k-MSFC2# show ip cef 192.168.199.3
192.168.199.3/32, version 281, connected, cached adjacency 192.168.199.3
0 packets, 0 bytes
via 192.168.199.3, VLAN 199, 0 dependencies
next-hop 192.168.199.3, VLAN 199
valid cached adjacency

```

You can see that there is a valid CEF entry with a mask length of 32 and that there is valid cache adjacency.

b. Verify the adjacency table by issuing this command:

```

Cat6k-MSFC2# show adjacency detail | begin 192.168.199.3
IP VLAN 199 192.168.199.3(7)
0 packets, 0 bytes
003071506800

!--- This is the destination MAC address.

00D0003F8BFC0800
ARP00:58:35

```

As you can see from the above output, there is an adjacency. The destination MAC address of the adjacency is showing the same information as the MAC address in the ARP table of Step 2, above.

Note that the counters in Step 3b are almost always 0, as packets are Layer 3 (L3) switched in hardware. As such, they never reach the MSFC2 and are not counted on the MSFC2 CEF counters. The only way to see statistics on packets forwarded to a given destination is to look at statistics of the adjacency found on the PFC2 during Step 5.

4. Verify from the Supervisor Engine point of view that you have the correct CEF/FIB entry.

There are two interesting entries in the FIB, as follows:

a. An entry for the destination IP address, as shown here:

```

Cat6k> (enable) show mls entry cef ip 192.168.199.3/32

```

Mod	FIB-Type	Destination-IP	Destination-Mask	NextHop-IP	Weight
15	resolved	192.168.199.3	255.255.255.255	192.168.199.3	1

This entry is a host entry with an already known next hop (which, in this case, is the destination itself).

- b. An entry corresponding to the destination network, as shown here:

```
Cat6k> (enable) show mls entry cef ip 192.168.199.0/24
```

Mod	FIB-Type	Destination-IP	Destination-Mask	NextHop-IP	Weight
15	connected	192.168.199.0	255.255.255.0		

This entry is a connected FIB entry, which means that any packet hitting this entry is redirected to the MSFC2 for further processing (mainly sending ARP and waiting for ARP resolution).

Remember that the FIB is browsed sequentially, starting with the longest mask length. As such, if both the entries listed in Step 4, above, are present, you hit the first one with the mask 32 (host entry), and you do not go further down the FIB table. In the case where the /32 entry is not present, you hit the second entry, which is the entry for the network; as it is a connected entry, you redirect the packet to the MSFC2 for further processing. It is quite possible for the MSFC2 to send an ARP request for the destination mask. Once the ARP reply is received, the ARP table and adjacency table are completed for that host on the MSFC2.

5. Once you have the correct FIB entry with mask length 32, verify that the adjacency is correctly populated for that host by issuing this command:

```
Cat6k> (enable) show mls entry cef ip 192.168.199.3/32 adjacency
```

Mod:15	Destination-IP	Destination-Mask	FIB-Type	AdjType	NextHop-IP	NextHop-Mac	VLAN	Encp	TX-Packets	TX-Octets
	192.168.199.3	255.255.255.255	resolved	connect	192.168.199.3	00-30-71-50-68-00	199	ARPA	0	0

Note: The adjacency is populated and the NextHop-Mac field contains the valid MAC address of host 2 (as seen in Steps 2 and 3b).

At this point, all the output is correct, although the number of transmitted packets for this adjacency is still 0. In the next example, you send ten pings of 100 bytes from host 1 to host 2 and check the adjacency again.

```
Cat6k> (enable) show mls entry cef ip 192.168.199.3/32 adjacency
```

Mod:15	Destination-IP	Destination-Mask	FIB-Type	AdjType	NextHop-IP	NextHop-Mac	VLAN	Encp	TX-Packets	TX-Octets
	192.168.199.3	255.255.255.255	resolved	connect	192.168.199.3	00-30-71-50-68-00	199	ARPA	10	1000

You can now see that the number of TX-Packets is 10, which is consistent with the traffic that was sent.

Remarks and Conclusions

As mentioned in Step 4 of Troubleshooting Steps, above, you have two FIB entries that can be a good match, as explained below:

- the network entry (in this case, 192.168.199.0/24) This entry is always present and is coming directly from the routing and CEF table on the MSFC. You always have this network directly connected in the routing table.
- the destination host entry (in this case, 192.168.199.3/32) This entry is not necessarily present. If it is not, you hit the network entry, and these items occur:

1. The packet is forwarded to the MSFC2.
2. The host entry with mask length 32 is then created in the FIB table of the PFC. However, as you do not yet have a complete adjacency, the adjacency is created with the type being `frd drop` (which means force drop).
3. The subsequent packet for that destination hits the `/32 frd drop` entry, and the packet is dropped.
4. At the same time, the original packet sent to the MSFC2 triggers the MSFC2 to send an ARP request.
5. Once the ARP is resolved, the ARP entry is completed. The adjacency is completed on the MSFC2, and an adjacency update is sent to the Supervisor Engine to complete the existing `frd drop` adjacency.
6. The Supervisor Engine changes the host adjacency to reflect the rewrite MAC address, and the adjacency type is changed to `connect`.

This mechanism of installing an `frd drop` adjacency while you wait for the ARP to be resolved is called ARP throttle. ARP throttle is useful to avoid having all packets forwarded to the MSFC2 and generating multiple ARP requests. Only the first few packets are sent to the MSFC2, and the rest are dropped at the PFC2 until the adjacency is complete.

This also allows you to drop traffic directed to a nonexistent or nonresponding host in a directly connected network.

When troubleshooting connections between two users in two different VLANs, it is important to always keep in mind that you need to look at:

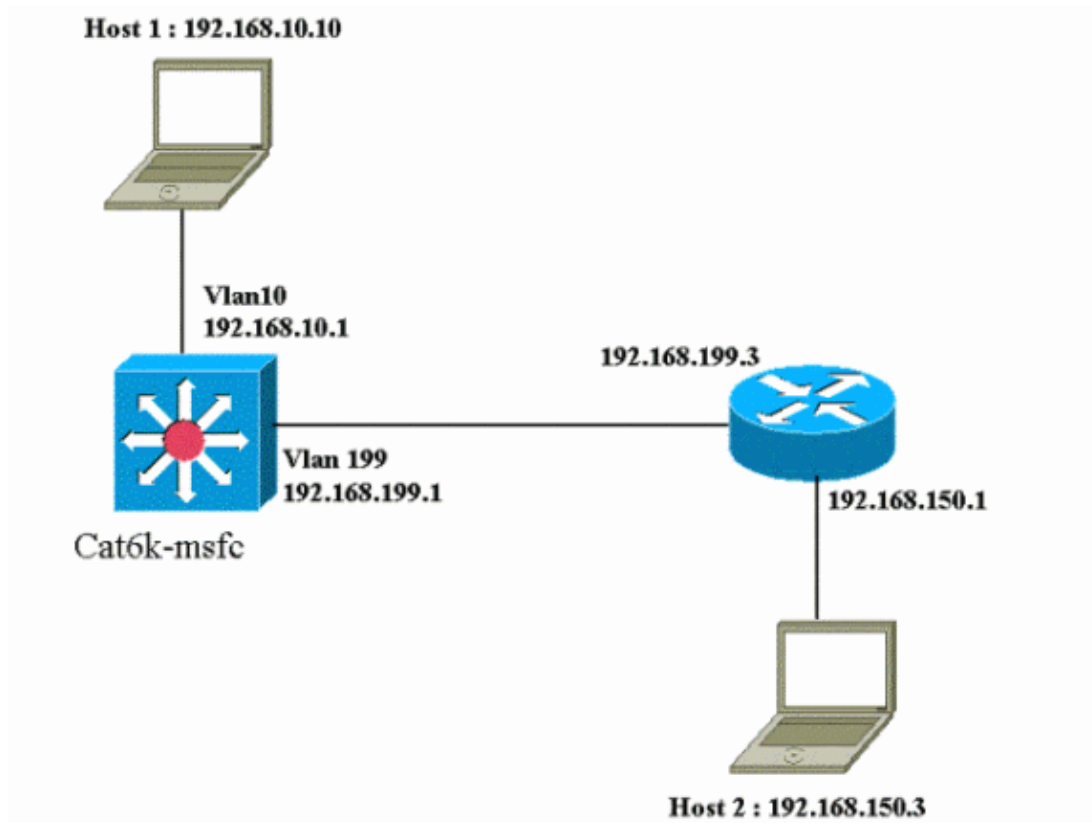
- traffic from host 1 to host 2 using the Troubleshooting Method, above, for making the destination IP address host 2
- traffic from host 2 to host 1 using the same method, but this time with the destination as host 1

It is also important to remember that the output needs to be taken on the default gateway of the source, which is not necessarily the same traffic from host 1 to host 2 and traffic from host 2 to host 1.

Note: The counters in Step 3b of Troubleshooting Steps, above, are almost always 0 as packets are L3 switched in hardware. As such, they never reach the MSFC2 and are not counted on the MSFC2 CEF counters. The only way to see statistics on packets forwarded to a given destination is to look at statistics of the adjacency found on the PFC2 during Step 5 of Troubleshooting Steps, above.

Case Study 2: Connectivity to a Remote Network

Consider the following diagram, in which host 1 with an IP address of 192.168.10.10 pings host 2 with an IP address of 192.168.150.3. However, this time, host 2 is located two routed hops away instead of being directly connected to Catalyst 6500/6000–MSFC2. The same method is used to follow the CEF routed path on the Catalyst 6500/6000–MSFC2.



Troubleshooting Steps

Complete these steps:

1. Check the routing table on the MSFC2 by issuing this command:

```
Cat6k-MSFC2# show ip route 192.168.150.3
Routing entry for 192.168.150.0/24
Known via "ospf 222", distance 110, metric 2, type intra area
Last update from 192.168.199.3 on VLAN 199, 00:12:43 ago
Routing Descriptor Blocks:
* 192.168.199.3, from 192.168.254.252, 00:12:43 ago, via VLAN 199
Route metric is 2, traffic share count is 1
Cat6k-MSFC2#sh ip route | include 192.168.150.0
O 192.168.150.0/24 [110/2] via 192.168.199.3, 00:13:00, VLAN 199
```

You can see from the output above that, to reach host 2 with IP address 192.168.150.3, you have an Open Shortest Path First (OSPF) route. It needs to be reached using IP address 192.168.199.3 in VLAN 199 as the next hop.

2. Check the ARP table on the MSFC2 by issuing the command below.

Note: Check the ARP entry for the next hop, not for the final destination.

```
Cat6k-MSFC2# show ip arp 192.168.199.3
Protocol Address      Age (min)  Hardware      Addr Type  Interface
Internet 192.168.199.3  217       0030.7150.6800 ARPA      VLAN 199
```

3. Check the CEF table and the adjacency table on the MSFC2 by issuing this command:

```
Cat6k-MSFC2# show ip cef 192.168.150.0
192.168.150.0/24, version 298, cached adjacency 192.168.199.3
0 packets, 0 bytes
via 192.168.199.3, VLAN 199, 0 dependencies
next-hop 192.168.199.3, VLAN 199
```

```
valid cached adjacency
```

You can see that there is a CEF entry for the destination network, and the next hop results match what you have in Step 1 from the routing table.

4. Check the adjacency table for the next hop by issuing this command:

```
Cat6k-MSFC2# show adjacency detail | begin 192.168.199.3
IP VLAN 199 192.168.199.3(9)
0 packets, 0 bytes
003071506800
00D0003F8BFC0800
ARP 00:17:48
```

There is a valid adjacency for the next hop, and the destination MAC address matches the ARP entry found in Step 2, above.

5. Check the FIB table on the Supervisor Engine (PFC2) by issuing this command:

```
Cat6k> (enable) show mls entry cef ip 192.168.150.0/24
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 resolved 192.168.150.0 255.255.255.0 192.168.199.3 1
```

The FIB reflects the same information found in Step 3, and you have the same next hop.

6. Check the adjacency on the Supervisor Engine (PFC2) by issuing this command:

```
Cat6k> (enable) show mls entry cef ip 192.168.150.0/24 adjacency
Mod:15
Destination-IP : 192.168.150.0 Destination-Mask : 255.255.255.0
FIB-Type : resolved
AdjType NextHop-IP NextHop-Mac VLAN Encp TX-Packets TX-Octets
-----
connect 192.168.199.3 00-30-71-50-68-00 199 ARPA 0 0
```

You can also verify that you have a connect adjacency that reflects the same MAC address as found in Steps 2 and 4, above.

Note: You can check the adjacency for the final destination when checking the adjacency on the PFC2. This is not possible with Cisco IOS Software on the MSFC2, with which you need to check adjacency for the next hop. The adjacency table on the PFC2 for the final destination shows both the next hop and the adjacency for the next hop (if it is resolved), all in one command output. On the MSFC2, you need to separately check the CEF entry to find the next hop and then look to the next hop adjacency itself.

Remarks and Conclusions

You can see in this example that the troubleshooting steps used to verify connectivity on a Catalyst 6500/6000-MSFC2 to reach a remote network are similar to the previous example found in the section Case Study 1: Connectivity to a Host in a Directly Connected Network. There are, however, a few differences:

- You check the final destination in the IP routing table, CEF table, and FIB (Steps 1, 3, and 5).
- You check the next hop information in the ARP table and adjacency table (Steps 2 and 4).
- In Step 6, you can directly check the adjacency for the final destination. The results display both the next hop from the FIB and the adjacency rewrite information from the adjacency table.

In this case, there is no entry in the FIB for the final destination, as shown below. (Only the network entry with mask length of 24 is present.)

```
Cat6k> (enable) show mls entry cef ip 192.168.150.3/32 adjacency
Cat6k> (enable)
```

Case Study 3: Load Balancing to Several Next Hops

This case study discusses what happens in the event that several next hops and several routes are available to reach the same destination network.

1. In a sample section of the routing table below, notice that there are three different routes and three different next hops available to reach the same destination IP address of 192.168.254.253.

```
O 192.168.254.253 [110/2] via 192.168.222.6, 00:42:45, POS8/2
[110/2] via 192.168.222.2, 00:42:45, VLAN 222
[110/2] via 192.168.199.2, 00:42:45, VLAN 199
```

2. Check the ARP entry for each of the three next hops, by following these steps:

- a. Check the CEF table for the destination.

Notice that the destination is also showing three different entries in the CEF table on MSFC2. Cisco IOS Software CEF is able to make load sharing between different routes.

```
cat6k-MSFC2# show ip cef 192.168.254.253
192.168.254.253/32, version 64, per-destination sharing
0 packets, 0 bytes
via 192.168.222.6, POS8/2, 0 dependencies
traffic share 1
next-hop 192.168.222.6, POS8/2
valid adjacency
via 192.168.222.2, VLAN 222, 0 dependencies
traffic share 1
next-hop 192.168.222.2, VLAN 222
valid adjacency
via 192.168.199.2, VLAN 199, 0 dependencies
traffic share 1
next-hop 192.168.199.2, VLAN 199
valid adjacency
0 packets, 0 bytes switched through the prefix
```

- b. Check the three adjacencies in the MSFC2 adjacency table.

They should match the ARP entry in Step 2, above.

3. Notice that three different FIB entries are installed for the same destination.

Hardware CEF on the PFC2 is able to load share up to six different paths for the same destination. You can see the weight used for each next hop in the weight field. The load sharing used by the PFC2 is only a per-flow load sharing. It is not enabling per-packet load sharing.

```
Cat6k> (enable) show mls entry cef ip 192.168.254.253/32
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 resolved 192.168.254.253 255.255.255.255 point2point 1
192.168.222.2 1
192.168.199.2 1
```

4. Check the adjacency for that destination entry by issuing this command:

```
cat6k> (enable) show mls entry cef ip 192.168.254.253/32 adjacency
Mod : 15
Destination-IP : 192.168.254.253 Destination-Mask : 255.255.255.255
FIB-Type : resolved
AdjType NextHop-IP NextHop-Mac VLAN Encp TX-Packets TX-Octets
-----
connect point2point 00-00-08-00-04-00 1025 ARPA 0 0
```

```

connect 192.168.222.2 00-90-21-41-c4-07 222 ARPA 0 0
connect 192.168.199.2 00-90-21-41-c4-17 199 ARPA 0 0

```

Case Study 4: Default Routing

Whatever the routing table looks like, there is always a FIB entry in the Supervisor Engine 2 to forward packets that do not match any other previous entry. You can see this entry by issuing this command:

```

Cat6k> (enable) show mls entry cef ip 0.0.0.0/0
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 default 0.0.0.0 0.0.0.0 192.168.98.2 1

```

As you can see, this is the only entry with a mask length of 0. This default can be of two types, as explained below in the sections Default Route Exists in the MSFC2 Routing Table and No Default Route in the Routing Table.

Default Route Exists in the MSFC2 Routing Table

First, determine how to verify if a default route is present in the MSFC2 routing table. You can either look for a route with a destination of 0.0.0.0 or look in the routing table. The default route is marked with an asterisk (*). (Here, it appears in boldface also.)

```

Cat6k-MSFC2# show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
Known via "rip", distance 120, metric 1, candidate default path
Redistributing via rip
Last update from 192.168.98.2 on VLAN 98, 00:00:14 ago
Routing Descriptor Blocks:
* 192.168.98.2, from 192.168.98.2, 00:00:14 ago, via VLAN 98
Route metric is 1, traffic share count is 1
Cat6k-MSFC2#sh ip ro | include 0.0.0.0
R* 0.0.0.0/0 [120/1] via 192.168.98.2, 00:00:22, VLAN 98

```

In this case, the default route is present in the MSFC2 routing table and is learned via the Routing Information Protocol (RIP). However, note that CEF behavior is the same no matter how this default route is learned (static, OSPF, RIP, and so on).

In this case, where you have a default route, you always have a CEF entry with a mask length of 0 and a FIB-Type of default that is used to forward all traffic not matching any other prefix.

```

Cat6k> (enable) show mls entry cef ip 0.0.0.0/0
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 default 0.0.0.0 0.0.0.0 192.168.98.2 1
Cat6k< (enable) show mls entry cef ip 0.0.0.0/0 adjacency
Mod : 15
Destination-IP : 0.0.0.0 Destination-Mask : 0.0.0.0
FIB-Type : default
AdjType NextHop-IP NextHop-Mac VLAN Encp TX-Packets TX-Octets
-----
connect 192.168.98.2 00-90-21-41-c5-57 98 ARPA 10433743 3052325803

```

As the FIB is browsed sequentially for each packet, beginning with longest match first, this default FIB is only used for packets for which no other match was found.

No Default Route in the Routing Table

```
Cat6k-MSFC2# show ip route 0.0.0.0
% Network not in table
```

If there are not any default routes in the routing table, there is still a FIB entry with mask length 0 in the Supervisor Engine 2. However, this entry now has a FIB-Type of wildcard. This wildcard FIB drops all packets hitting it and matches any packet that does not match any other entry in the FIB. It is useful to drop these packets, as you do not have any default routes. There is no need to forward these packets to the MSFC2, which would drop them anyway. By using this wildcard FIB, you are ensuring the drop of these useless packets in hardware.

```
Cat6k> (enable) show mls entry cef ip 0.0.0.0/0
Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight
-----
15 wildcard 0.0.0.0 0.0.0.0
```

Note: In the rare case in which the FIB table is full, the wildcard entry is still present but, instead of dropping packets that match it, they are forwarded to the MSFC2. This only occurs if you have more than a 256K prefix in the FIB and if you cannot store the complete routing table and ARP adjacency in the FIB. You then need to have the default mechanism sent to MSFC2 since the MSFC2 can have a routing entry that is not present in the FIB.

Other Troubleshooting Tips and Known Issues

Issuing the show mls cef mac Command

When the Supervisor Engine 2 gets a packet, it only considers it a potential L3 packet if the destination MAC address of the packet is the same as one of the MSFC2 MAC addresses. You can verify that these addresses are from the Supervisor Engine 2 point of view by issuing this command:

```
Cat6k> (enable) show mls cef mac
Module 15 : Physical MAC-Address 00-d0-00-3f-8b-fc
VLAN Virtual MAC-Address(es)
-----
10 00-00-0c-07-ac-0a
100 00-00-0c-07-ac-64
Module 15 is the designated MSFC for installing CEF entries
```

You can see the physical MAC address of the MSFC2. (Remember that all interfaces on the MSFC2 use the same MAC address; you cannot configure different MAC addresses on two different interfaces.) This MAC address needs to be the same as the one on the MSFC2.

```
Cat6k-MSFC2# show interface
VLAN1 is up, line protocol is up
Hardware is Cat6k RP Virtual Ethernet, address is 00d0.003f.8bfc (bia 00d0.003f.8bfc)
?..
```

The **show mls cef mac** command also displays all MAC addresses linked to Hot Standby Router Protocol (HSRP) groups, where the MSFC is active. The output from the **show mls cef mac** command, above, means that the MSFC is HSRP-active for VLAN 10 and for VLAN 100. You can verify that this is correct by issuing this command on the MSFC2:

```
Cat6k-MSFC2# show standby brief
P indicates configured to preempt.
|
Interface Grp Prio P State Active addr Standby addr Group addr
```

Vl110	10	200	P Active	local	192.168.10.2	192.168.10.254
Vl111	11	100	P Standby	192.168.11.1	local	192.168.11.254
Vl198	98	200	Standby	192.168.98.2	local	192.168.98.5
Vl199	99	200	Standby	192.168.99.2	local	192.168.99.5
Vl1100	100	200	P Active	local	192.168.100.2	192.168.100.254
Vl1101	101	100	P Standby	192.168.101.2	local	192.168.101.254

As you can see, the state is **Active** for only VLAN 10 and VLAN 100. The state is **Standby** for all other HSRP groups configured. If, for whatever reason, a state of **Active** begins for another VLAN, output of the **show mls cef mac** command should reflect that this additional VLAN is not active.

If there are inconsistencies between the **show mls cef mac** command output and what it should be, you can issue this command, which provides more information on the MAC addresses added and removed in the **show mls cef mac** command list:

```
Cat6k-MSFC2#Cat6k> (enable) show mls rlog 12
SWLOG at 82a7f410: magic 1008, size 51200, cur 82a81ca4, end 82a8bc20
Current time is: 12/28/01,17:09:15
1781 12/28/01,11:40:05:(RouterConfig)Router_cfg: router_add_mac_to_earl 00-d0-00-3f-8b-
fcadded for mod 15/1 VLAN 99 Earl AL =0
1780 12/28/01,11:40:05:(RouterConfig)Router_Cfg: process add(3) router intf for mNo 15/1
VLAN 99
1779 12/28/01,11:40:05:(RouterConfig)Router_cfg: router_add_mac_to_earl 00-d0-00-3f-8b-
fcadded for mod 15/1 VLAN 99 Earl AL =0
1778 12/28/01,11:40:05:(RouterConfig)Router_Cfg: process add(3) router intf for mNo 15/1
VLAN 99
1777 12/28/01,11:40:05:(RouterConfig)Router_cfg: router_add_mac_to_earl 00-d0-00-3f-8b-
fcadded for mod 15/1 VLAN 99 Earl AL =0
1776 12/28/01,11:40:05:(RouterConfig)Router_Cfg: Process add mls entry for mod 15/1
VLAN 99 i/f 1, proto 3, LC 0
1775 12/28/01,11:40:05:(RouterConfig)Router_cfg: router_add_mac_to_earl 00-d0-00-3f-8b-
fcadded for mod 15/1 VLAN 99 Earl AL =0
1774 12/28/01,11:40:05:(RouterConfig)Router_Cfg: Process add mls entry for mod 15/1
VLAN 99 i/f 1, proto 2, LC 0
```

This command provides a message each time you add or remove a MAC address in the **show mls cef mac** command table.

Shadow TCAM

This document has discussed how to check the **show mls entry cef** command table on the Supervisor Engine 2. This command does not accurately represent the real application-specific integrated circuit (ASIC) programming of the PFC2. It only represents a shadow copy of this ASIC setting. There have been some known issues in which the real hardware settings did not agree with what was displayed in the shadow TCAM, which caused some packets to be forwarded to the wrong next hop. These issues are documented in Cisco bug ID CSCdv49956 [☞](#) (registered customers only) and CSCdu85211 [☞](#) (registered customers only), which are both fixed in CatOS software versions 6.3(3), 7.1(1), and later.

Default Routing Broken

There was a bug found in early versions of code in which forwarding to the default route did not work with Enhanced Interior Gateway Routing Protocol (EIGRP) or with OSPF. This is documented in Cisco bug ID CSCdt54036 [☞](#) (registered customers only), and is fixed in CatOS software version 6.1(3) and later for the Supervisor Engine image, and in Cisco IOS Software Release 12.1(6)E1 for the MSFC2 image.

Related Information

- [Configuring and Troubleshooting IP MLS on Catalyst 6000 Switches with an MSFC](#)
 - [LAN Product Support Pages](#)
 - [LAN Switching Support Page](#)
 - [Tools and Utilities](#)
 - [Technical Support – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2014 – 2015 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jun 05, 2008

Document ID: 20626
