

Catalyst 6500/6000 Series Switches with Supervisor Engine 720 and Cisco IOS System Software Troubleshoot of Unicast IP Routing Problems That Involve CEF

Document ID: 64939

Contents

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Overview of CEF

- Adjacency Table

How to Read the FIB and Adjacency Table on the RP

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

- Troubleshooting Steps

Case Study 4: Default Routing

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

Other Troubleshooting Tips and Known Issues

- DFC-Based Line Cards
- Disable IP Routing
- Difference Between IP CEF and MLS CEF

Related Information

Introduction

This document serves as a guide to troubleshoot unicast IP routing on Cisco Catalyst 6500/6000 series switches with Supervisor Engine 720, Policy Feature Card 3 (PFC3), Multilayer Switch Feature Card 3 (MSFC3). Cisco Express Forwarding (CEF) is used to perform unicast routing on the Supervisor Engine 720. This document only concerns IP routing on the Catalyst 6500/6000 series switches with Supervisor Engine 720, PFC3, MSFC3. 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 that run Cisco IOS® Software on the Supervisor Engine. The document is not valid for Cisco Catalyst OS (CatOS) system software.

Note: You can also use this document in order to troubleshoot unicast IP routing on Catalyst 6500/6000 switches with Supervisor Engine 2 and MSFC2.

Note: This document uses the terms Route Processor (RP) and Switch Processor (SP) in place of MSFC and

PFC, respectively.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

Conventions

Refer to Cisco Technical Tips Conventions for more information on document 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 6500/6000 with Supervisor Engine 720 uses a hardware-based CEF forwarding mechanism that is implemented on the SP. CEF mainly uses two tables to store the information necessary for routing:

- Forwarding Information Base (FIB) table
- Adjacency table

CEF uses a FIB in order to make IP destination prefix-based switching decisions. CEF looks at the longest match first. The FIB is conceptually similar to a routing table or information base. The FIB maintains a mirror image of the forwarding information that the IP routing table contains. When routing or topology changes occur in the network, an update takes place in the IP routing table. The FIB reflects the changes. The FIB maintains the next hop address information on the basis of the information in the IP routing table. Because of a one-to-one correlation between FIB entries and routing table entries, the FIB contains all known routes. This 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 the match is 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. 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 6500/6000 with Supervisor Engine 720 system, IP CEF needs to run on the MSFC3.

How to Read the FIB and Adjacency Table on the RP

The FIB table of the SP must be exactly the same as the FIB table on the RP. On the RP, a ternary content addressable memory (TCAM) stores all IP prefixes in the FIB. The sort of the prefixes occurs by mask length and starts with the longest mask. So you first find all the entries with a mask of 32, which is the host entry. Next, you find all entries with a mask length of 31. You continue until you reach an entry with a mask length

of 0, which is the default entry. The FIB is read sequentially, and the first hit is used as a match. Consider this sample FIB table on the RP:

```
Cat6500-A#show ip cef
Prefix          Next Hop          Interface
0.0.0.0/0       14.1.24.1        FastEthernet2/48
0.0.0.0/32      receive
14.1.24.0/24    attached         FastEthernet2/48
14.1.24.0/32    receive
14.1.24.1/32    14.1.24.1        FastEthernet2/48
14.1.24.111/32  receive
14.1.24.179/32  14.1.24.179      FastEthernet2/48
14.1.24.255/32  receive
100.100.100.0/24 attached         TenGigabitEthernet6/1
100.100.100.0/32 receive
100.100.100.1/32 100.100.100.1    TenGigabitEthernet6/1
100.100.100.2/32  receive
100.100.100.255/32 receive
112.112.112.0/24 attached         FastEthernet2/2
112.112.112.0/32 receive
112.112.112.1/32 receive
112.112.112.2/32 112.112.112.2    FastEthernet2/2
112.112.112.255/32 receive
127.0.0.0/8      attached         EOBC0/0
127.0.0.0/32    receive
127.0.0.51/32   receive
127.255.255.255/32 receive
Prefix          Next Hop          Interface
222.222.222.0/24 100.100.100.1    TenGigabitEthernet6/1
223.223.223.1/32 100.100.100.1    TenGigabitEthernet6/1
224.0.0.0/4      drop
224.0.0.0/24    receive
255.255.255.255/32 receive
```

Each entry consists of these fields:

- **Prefix** The destination IP address or IP subnet that is concerned
- **Next Hop** The next hop that is associated with this Prefix

The possible Next Hop values are:

- ◆ **receive** The prefix that is associated with MSFC interfaces

This entry contains a prefix with a mask of 32 that corresponds to the IP address of the Layer 3 (L3) interfaces.

- ◆ **attached** The prefix that is associated with a connected network
- ◆ **The IP address of the next hop**
- ◆ **drop** All packets that match an entry with a drop are dropped.
- **Interface** The outgoing interface for that destination IP address or IP subnet

In order to view the complete adjacency table, issue this command:

```
Cat6500-A#show adjacency TenGigabitEthernet 6/1 detail
Protocol Interface          Address
IP          TenGigabitEthernet6/1  100.100.100.1(9)
                    5570157 packets, 657278526 bytes
                    00D0022D3800
                    00D0048234000800
                    ARP          03:43:51
                    Epoch: 0
```

Troubleshooting Method

This section provides troubleshooting examples and details. But first, this section summarizes the methods to troubleshoot connectivity or reachability to a specific IP address. Keep in mind that the CEF table on the SP mirrors the CEF table on the RP. Therefore, the SP only holds the correct information to reach an IP address if the information that is known by the RP is also correct. So you always need to verify this information.

From the RP

Complete these steps:

1. Verify that the information that is held in the IP routing on the RP table is correct.

Issue the **show ip route** command and verify that the output contains the expected next hop.

Note: If you issue the **show ip route x.x.x.x** command instead, you do not need to browse the complete routing table.

If the output does not contain the expected next hop, check your configuration and routing protocol neighbors. Also perform any other troubleshooting procedures that are relevant to the routing protocol that you run.

2. Verify that either the next hop or, for a connected network, the final destination has a correct, resolved Address Resolution Protocol (ARP) entry on the RP.

Issue the **show ip arp next_hop_ip_address** command. Verify the resolution of the ARP entry and that the entry 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 the MAC address. An incomplete ARP entry indicates that the RP has not received any replies from that host. Verify that the host is up and running. You can use a sniffer on the host to see if the host gets the ARP reply and answers correctly.

3. Verify that the CEF table on the RP contains the correct information and that adjacency is resolved.

Complete these steps:

- a. Issue the **show ip cef destination_network** command in order to verify that the next hop in the CEF table matches the next hop in the IP routing table.

This is the next hop from Step 1 of this section.

- b. Issue the **show adjacency detail | begin next_hop_ip_address** command in order to verify that the adjacency is correct.

The entry must contain the same MAC address of the ARP as in Step 2 of this section.

If Steps 1 and 2 of this section provide correct results, but Steps 3a or 3b fail, you face a Cisco IOS Software CEF issue. This issue is not likely a platform-specific issue that relates to the Catalyst 6500/6000. You must try to clear the ARP table and the IP routing table.

From the SP

Complete these steps:

1. Verify that the FIB information that the SP stores is correct and matches the information that the CEF table on the RP stores.

Note: The information in the CEF table is from Step 3 of the From the RP section.

Issue the **show mls cef lookup destination_ip_network detail** command and verify that there is an adjacency entry.

If the information does not exist, there is a communication problem between the RP and the SP. This issue relates to Catalyst 6500/6000 platform–specific functionality. Verify that there is no known bug for the specific Cisco IOS Software release that you run. In order to restore the correct entry, issue the **clear ip route** command on the RP.

2. In order to verify the adjacency table on the SP, issue the **show mls cef adjacency entry adjacency_entry_number detail** command.

Verify that the entry contains the same destination MAC address as the address that you saw in Steps 2 and 3b of the From the RP section.

If the adjacency in the SP does not match the adjacency for the next hop in Step 3b, you probably face an issue of internal communication between the RP and SP. Try to clear the adjacency in order 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 these hosts:

- Host A in network 112.112.112.0/24 with an IP address of 112.112.112.2
- Host B in network 222.222.222.0/24 with an IP address of 222.222.222.2

This is the relevant RP configuration:

```
interface TenGigabitEthernet4/1
 ip address 100.100.100.1 255.255.255.0

! interface GigabitEthernet5/5
 ip address 222.222.222.1 255.255.255.0
```

Important Note: The Catalyst 6500/6000 platform with Supervisor Engine 720 and MSFC3 performs routing with the use of CEF in hardware. There is no configuration requirement for CEF, and you cannot disable CEF on the MSFC3.

Troubleshooting Steps

Follow the procedures in the Troubleshooting Method section of this document in order to verify the path to reach IP address 222.222.222.2.

1. In order to verify the IP routing table, issue either of these two commands:

```
◆ Cat6500-B#show ip route 222.222.222.2
Routing entry for 222.222.222.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Redistributing via eigrp 100
  Routing Descriptor Blocks:
    * directly connected, via GigabitEthernet5/5
```

Route metric is 0, traffic share count is 1

or

```
◆ Cat6500-B#show ip route | include 222.222.222.0
C 222.222.222.0/24 is directly connected, GigabitEthernet5/5
```

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

2. Verify the ARP entry on the RP.

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

```
Cat6500-B#show ip arp 222.222.222.2
Protocol Address Age (min) Hardware Addr Type Interface
Internet 222.222.222.2 41 0011.5c85.85ff ARPA GigabitEthernet5/5
```

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

a. In order to verify the CEF table, issue this command:

```
Cat6500-B#show ip cef 222.222.222.2
222.222.222.2/32, version 10037, epoch 0, connected, cached adjacency
222.222.222.2
0 packets, 0 bytes
via 222.222.222.2, GigabitEthernet5/5, 0 dependencies
next hop 222.222.222.2, GigabitEthernet5/5
valid cached adjacency
```

You can see that there is a valid CEF entry with a mask length of 32. Also, you can see that there is valid cached adjacency.

b. In order to verify the adjacency table, issue this command:

```
Cat6500-B#show adjacency detail | begin 222.222.222.2
IP GigabitEthernet5/5 222.222.222.2(7)
481036 packets, 56762248 bytes
00115C8585FF
00D0022D38000800
ARP 03:10:29
Epoch: 0
```

This output shows that there is an adjacency. The destination MAC address of the adjacency shows the same information as the MAC address in the ARP table of Step 2 of this section.

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

There are two interesting entries in the FIB:

◆ An entry for the destination IP address, as this output shows:

```
Cat6500-B#show mls cef ip 222.222.222.2 detail

Codes: M - mask entry, V - value entry, A - adjacency index, P - priority
bit
D - full don't switch, m - load balancing modnumber, B - BGP Bucket
sel
V0 - Vlan 0,C0 - don't comp bit 0,V1 - Vlan 1,C1 - don't comp bit 1
RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(90 ): E | 1 FFF 0 0 0 0 255.255.255.255
V(90 ): 8 | 1 0 0 0 0 0 222.222.222.2 (A:327680 ,P:1,D:0,m:0 ,
B:0 )
```

This entry is a host entry with an already known next hop. In this case, the next hop is the destination itself.

- ◆ An entry that corresponds to the destination network, as this output shows:

```
Cat6500-B#show mls cef ip 222.222.222.0 detail
```

```
Codes: M - mask entry, V - value entry, A - adjacency index, P - priority
       bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket
       sel
       V0 - Vlan 0,C0 - don't comp bit 0,V1 - Vlan 1,C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(88      ): E | 1 FFF  0 0 0 0   255.255.255.255
V(88      ): 8 | 1 0    0 0 0 0   222.222.222.0      (A:13      ,P:1,D:0,m:0 ,
       B:0 )
M(3207    ): E | 1 FFF  0 0 0 0   255.255.255.0
V(3207    ): 8 | 1 0    0 0 0 0   222.222.222.0      (A:14      ,P:1,D:0,m:0 ,
       B:0 )
```

This entry is a connected FIB entry. Any packet that hits this entry is redirected to the RP for additional processing. This processing mainly involves the send of ARP and wait for ARP resolution.

Remember that FIB is browsed sequentially and starts with the longest mask length. So if you have both an entry for the destination IP address and an entry for the destination network, the SP uses the first entry with the mask 32. This entry is the host entry. There is no consideration of less-specific FIB table entries. If the /32 entry is not present, the SP uses the second entry, which is the entry for the destination network. As if this entry were a connected entry, the SP redirects the packet to the RP for further processing. The RP can send an ARP request for the destination mask. At the receipt of the ARP reply, the ARP table and adjacency table are complete for that host on the RP.

5. When you have the correct FIB entry with mask length 32, verify that the adjacency is correctly populated for that host.

Issue this command:

```
Cat6500-B#show mls cef adjacency entry 327680 detail
```

```
Index: 327680 smac: 00d0.022d.3800, dmac: 0011.5c85.85ff
mtu: 1518, vlan: 1021, dindex: 0x0, l3rw_vld: 1
format: MAC_TCP, flags: 0x8408
delta_seq: 0, delta_ack: 0
packets: 0, bytes: 0
```

Note: The adjacency is populated and the destination MAC (dmac) field contains the valid MAC address of host B. This address is the one you saw in Steps 2 and 3b of this section.

Note: The packets and bytes count is 0. If the ingress module has a Distributed Forwarding Card (DFC), you must log in to the module in order to get the packets/bytes count. The Other Troubleshooting Tips and Known Issues section discusses this process.

Remarks and Conclusions

As Step 4 of the Troubleshooting Steps mentions, there are two FIB entries that can be a good match. They are:

- The network entry, which is 222.222.222.0/24 in this case This entry is always present and comes directly from the routing and CEF table on the MSFC. This network always has direct connection in

the routing table.

- The destination host entry, which is 222.222.222.2/32 in this case This entry may not necessarily be present. If the entry is not present, the SP uses the network entry, and these events occur:
 1. The SP forwards the packet to the RP.
 2. The FIB table of the PFC creates the host entry with mask length 32. However, you do not yet have a complete CEF adjacency, so the adjacency is created with the type `drop`.
 3. The subsequent packet for that destination hits the `/32 drop` entry, and the packet drops.
 4. At the same time, the original packet that transmitted to the RP triggers the MSFC to send an ARP request.
 5. At the resolution of the ARP, the ARP entry is complete. The adjacency is complete on the RP. An adjacency update goes to the SP in order to complete the existing `drop` adjacency.
 6. The SP changes the host adjacency in order to reflect the rewrite MAC address. The adjacency type changes to the connected interface.

This mechanism to install a `drop` adjacency while you wait for the resolution of the ARP has the name "ARP throttle". ARP throttle is useful in order to avoid the forwarding of all packets to the RP and generation of multiple ARP requests. Only the first few packets transmit to the RP, and the PFC drops the rest until the adjacency is complete.

The ARP throttle also allows you to drop traffic that is directed to a nonexistent or nonresponsive host in a directly connected network.

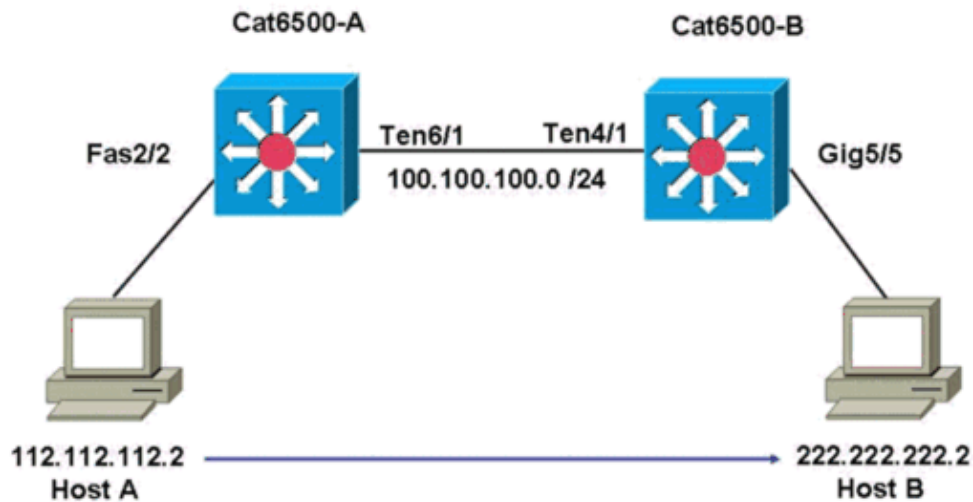
When you troubleshoot connections between two users in two different VLANs, always keep in mind that you need to look at:

- Traffic from host A to host B with the use of the Troubleshooting Method in order to make the destination IP address host B
- Traffic from host B to host A with the use of the same Troubleshooting Method, but with the destination as host A

Also remember to take the output on the default gateway of the source. This traffic from host A to host B and traffic from host B to host A are not necessarily the same.

Case Study 2: Connectivity to a Remote Network

In the diagram in this section, host A with an IP address of 112.112.112.2 pings host B with an IP address of 222.222.222.2. However, this time, host B does not have a direct connection to the Cat6500–A switch; host B is two routed hops away. You use the same method to follow the CEF routed path on the Cat6500–B switch.



Troubleshooting Steps

Complete these steps:

1. In order to check the routing table on the Cat6500-A, issue this command:

```
Cat6500-A#show ip route 222.222.222.2
Routing entry for 222.222.222.0/24
  Known via "ospf 100", distance 110, metric 2, type intra area
  Last update from 100.100.100.1 on TenGigabitEthernet6/1, 00:00:37 ago
  Routing Descriptor Blocks:
    * 100.100.100.1, from 222.222.222.1, 00:00:37 ago, via TenGigabitEthernet6/1
      Route metric is 2, traffic share count is 1
```

You can see from this output that, in order to reach host B with IP address 222.222.222.2, you have an Open Shortest Path First (OSPF) Protocol route. You need to reach the host with the use of IP address 100.100.100.1, with TenGigabitEthernet6/1 as the next hop.

2. In order to check the ARP table on the RP, issue this command:

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

```
Cat6500-A#show ip arp 100.100.100.1
Protocol Address Age (min) Hardware Addr Type Interface
Internet 100.100.100.1 27 00d0.022d.3800 ARPA TenGigabitEthernet6/1
```

3. In order to check the CEF table and the adjacency table on the RP, issue this command:

```
Cat6500-A#show ip cef 222.222.222.2
222.222.222.0/24, version 6876, epoch 0, cached adjacency 100.100.100.1
0 packets, 0 bytes
  via 100.100.100.1, TenGigabitEthernet6/1, 0 dependencies
    next hop 100.100.100.1, TenGigabitEthernet6/1
    valid cached adjacency
```

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

4. In order to check the adjacency table for the next hop, issue this command:

```
Cat6500-A#show adjacency detail | begin 100.100.100.1
IP TenGigabitEthernet6/1 100.100.100.1(9)
```

```
2731045 packets, 322263310 bytes
00D0022D3800
00D0048234000800
ARP          03:28:41
Epoch: 0
```

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

5. In order to check the FIB table on the SP, issue this command:

```
Cat6500-A#show mls cef ip lookup 222.222.222.2 detail
```

```
Codes: M - mask entry, V - value entry, A - adjacency index, P - priority bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket sel
       V0 - Vlan 0,C0 - don't comp bit 0,V1 - Vlan 1,C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(3203  ): E | 1 FFF  0 0 0 0   255.255.255.0
V(3203  ): 8 | 1 0    0 0 0 0   222.222.222.0      (A:163840 ,P:1,D:0,m:0 ,B:0 )
```

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

6. In order to check the adjacency on the SP, issue this command:

```
Cat6500-A#show mls cef adjacency entry 163840 detail
```

```
Index: 163840 smac: 00d0.0482.3400, dmac: 00d0.022d.3800
           mtu: 1518, vlan: 1018, dindex: 0x0, l3rw_vld: 1
           format: MAC_TCP, flags: 0x8408
           delta_seq: 0, delta_ack: 0
           packets: 726, bytes: 85668
```

Note: The packets and bytes counters are real-time. When the traffic stops, the counters return to 0.

Remarks and Conclusions

These Troubleshooting Steps verify connectivity on a Cat6500–A switch in order to reach a remote network. The steps are similar to the Troubleshooting Steps in the section Case Study 1: Connectivity to a Host in a Directly Connected Network. However, there are a few differences. In the Troubleshooting Steps for Case Study 2: Connectivity to a Remote Network, you need to:

- Check the final destination in the IP routing table, the CEF table, and the FIB.

You perform this check in Steps 1, 3, and 5.

- Check the next hop information in the ARP table and the adjacency table.

You perform this check in Steps 2 and 4.

- Check the adjacency for the final destination.

You perform this check in Step 6.

Case Study 3: Load Balancing to Several Next Hops

Troubleshooting Steps

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

1. Check the routing table in order to determine that there are different routes and different next hops available to reach the same destination IP address.

In a sample section of this routing table, there are two routes and two next hops available to reach destination IP address 222.222.222.2:

```
Cat6500-A#show ip route | begin 222.222.222.0
O    222.222.222.0/24
      [110/2] via 100.100.100.1, 00:01:40, TenGigabitEthernet6/1
      [110/2] via 111.111.111.2, 00:01:40, FastEthernet2/1
```

2. Check the ARP entry for each of the three next hops.

Complete these steps:

- a. Check the CEF table for the destination.

Notice that the destination also shows two different entries in the CEF table on the RP. Cisco IOS Software CEF is able to do load sharing between different routes.

```
Cat6500-A#show ip cef 222.222.222.2
222.222.222.0/24, version 6893, epoch 0
0 packets, 0 bytes
  via 100.100.100.1, TenGigabitEthernet6/1, 0 dependencies
    traffic share 1
    next hop 100.100.100.1, TenGigabitEthernet6/1
    valid adjacency
  via 111.111.111.2, FastEthernet2/1, 0 dependencies
    traffic share 1
    next hop 111.111.111.2, FastEthernet2/1
    valid adjacency
0 packets, 0 bytes switched through the prefix
tmstats: external 0 packets, 0 bytes
        internal 0 packets, 0 bytes
```

- b. Check the ARP entries for the two next hops.

```
Cat6500-A#show ip arp 100.100.100.1
Protocol Address          Age (min)  Hardware Addr  Type   Interface
Internet 100.100.100.1      13        00d0.022d.3800 ARPA   TenGigabitEthernet6/1

Cat6500-A#show ip arp 111.111.111.2
Protocol Address          Age (min)  Hardware Addr  Type   Interface
Internet 111.111.111.2      0         00d0.022d.3800 ARPA   FastEthernet2/1
```

- c. Check the two adjacencies in the RP adjacency table.

```
Cat6500-A#show adjacency detail
Protocol Interface          Address

IP       TenGigabitEthernet6/1 100.100.100.1(23)
62471910 packets, 7371685380 bytes
00D0022D3800
00D0048234000800
ARP      03:34:26
Epoch: 0

IP       FastEthernet2/1      111.111.111.2(23)
0 packets, 0 bytes
00D0022D3800
```

```
Address
00D0048234000800
ARP          03:47:32
Epoch: 0
```

The information in Steps 2b and 2c must match.

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

Hardware CEF on the PFC is able to load share up to 16 different paths for the same destination. The default is src_dst IP load sharing.

```
Cat6500-A#show mls cef ip 222.222.222.0

Codes: decap - Decapsulation, + - Push Label
Index  Prefix                Adjacency
3203   222.222.222.0/24      Te6/1          , 00d0.022d.3800 (Hash: 007F)
                               Fa2/1          , 00d0.022d.3800 (Hash: 7F80)
```

4. Check the exact route that is used to forward traffic.

Issue this command:

```
Cat6500-A#show ip cef exact-route 111.111.111.2 222.222.222.2
111.111.111.2 -> 222.222.222.2 : TenGigabitEthernet6/1 (next hop 100.100.100.1)
```

Case Study 4: Default Routing

Whatever the routing table looks like, there is always an FIB entry in the Supervisor Engine 720 to forward packets that do not match any other previous entry. In order to see this entry, issue this command:

```
Cat6500-A#show mls cef ip 0.0.0.0

Codes: decap - Decapsulation, + - Push Label
Index  Prefix                Adjacency
64     0.0.0.0/32           receive
134368 0.0.0.0/0            Fa2/48          , 000c.3099.373f
134400 0.0.0.0/0            drop
```

There are three entries. This default can be of two types:

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

Default Route Exists in the Routing Table

First, verify the presence of a default route in the RP 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, the default route also appears in boldface text.

```
Cat6500-A#show ip route 0.0.0.0
Routing entry for 0.0.0.0/0, supernet
  Known via "static", distance 1, metric 0, candidate default path
  Routing Descriptor Blocks:
    * 14.1.24.1
      Route metric is 0, traffic share count is 1
```

In this case, the default route is present in the RP routing table and is known via the "static" route that is configured.

Note: CEF behavior is the same no matter how this default route is learned, whether by static, OSPF, Routing Information Protocol (RIP), or another method.

Where you have a default route, you always have a CEF entry with a mask length of 0. This entry forwards all traffic that does not match any other prefix.

```
Cat6500-A#show mls cef ip 0.0.0.0

Codes: decap - Decapsulation, + - Push Label
Index  Prefix                Adjacency
64     0.0.0.0/32             receive
134368 0.0.0.0/0          Fa2/48           , 000c.3099.373f
134400 0.0.0.0/0             drop
```

The CEF browses the FIB sequentially for each packet and starts with the longest match first. Therefore, this default FIB is only for use with packets for which no other match is found.

No Default Route Exists in the Routing Table

```
Cat6500-B#show ip route 0.0.0.0
% Network not in table
```

If there are no default routes in the routing table, there is still an FIB entry with mask length 0 in the Supervisor Engine 720. This FIB entry is for use with a packet that does not match any other entry in the FIB and, as a result, is dropped. This drop is useful because you do not have any default routes. There is no need to forward these packets to the RP, which drops the packets anyway. If you use this FIB entry, you ensure the drop of these useless packets in hardware. This drop avoids needless utilization of the RP. However, if a packet is destined to IP address 0.0.0.0 specifically, that packet goes to the RP.

```
Cat6500-B#show mls cef ip 0.0.0.0

Codes: decap - Decapsulation, + - Push Label
Index  Prefix                Adjacency
67     0.0.0.0/32          receive
134400 0.0.0.0/0             drop
```

Note: In the rare case in which the FIB table is full, the FIB drop entry is still present. However, instead of a drop of packets that match the entry, the packets go to the RP. This only occurs when more than 256,000 prefixes are present in the FIB and there is insufficient space for the complete routing table.

Other Troubleshooting Tips and Known Issues

DFC–Based Line Cards

If the ingress module for traffic is a DFC–based line card, the forward decision is made locally on the module. In order to check the hardware packet counters, perform a remote login to the module. Then, issue the commands, as this section shows.

Use as an example Case Study 2: Connectivity to a Remote Network. For Cat6500–B, traffic comes into module 4, which has a DFC. Issue this command for a remote login to the module:

```
Cat6500-B#remote login module 4
Trying Switch ...
Entering CONSOLE for Switch
Type ^C^C^C to end this session
Cat6500-B-dfc4#
```

Then, you can check CEF FIB information on the module.

```
Cat6500-B-dfc4#show mls cef ip 222.222.222.2 detail
Codes: M - mask entry, V - value entry, A - adjacency index, P - priority bit
       D - full don't switch, m - load balancing modnumber, B - BGP Bucket sel
       V0 - Vlan 0,C0 - don't comp bit 0,V1 - Vlan 1,C1 - don't comp bit 1
       RVTEN - RPF Vlan table enable, RVTSEL - RPF Vlan table select
Format: IPV4_DA - (8 | xtag vpn pi cr recirc tos prefix)
Format: IPV4_SA - (9 | xtag vpn pi cr recirc prefix)
M(90   ): E | 1 FFF  0 0 0 0   255.255.255.255
V(90   ): 8 | 1 0   0 0 0 0   222.222.222.2   (A:294912 ,P:1,D:0,m:0 ,B:0 )
```

Next, you can check the adjacency information with the hardware counters.

```
Cat6500-B-dfc4#show mls cef adjacency entry 294912 detail
Index: 294912 smac: 00d0.022d.3800, dmac: 0011.5c85.85ff
mtu: 1518, vlan: 1021, dindex: 0x0, l3rw_vld: 1
format: MAC_TCP, flags: 0x8408
delta_seq: 0, delta_ack: 0
packets: 4281043, bytes: 505163074
```

Disable IP Routing

In Cisco IOS Software Release 12.1(20)E and later, the support for disablement of IP routing has been removed for Catalyst 6500 series switches. You cannot disable IP routing in these switches, as this example shows:

```
Cat6500(config)#no ip routing
Cannot disable ip routing on this platform
```

The **no ip routing** command is a Cisco IOS Software command which is used to disable IP routing on Cisco IOS routers. Usually, this command is used on low-end routers.

The **no ip routing** command is accepted only if the **service internal** command is already enabled on the switch. However, it is not saved to the configuration and is lost once the switch reloads. Cisco recommends not to disable the IP routing on the Catalyst 6000/6500 series switches that run Cisco IOS System software.

As a workaround to this issue, use the **ip route 0.0.0.0 0.0.0.0 a.b.c.d** command. In this command, *a.b.c.d* is the IP address of the default gateway. The routing process is not used if both these items are true:

- You use the **switchport** command in order to configure all the interfaces in the switch as L2 ports.
- There are no switched virtual interfaces (SVIs) (VLAN interfaces) configured in the switch.

Difference Between IP CEF and MLS CEF

The output of **show mls cef exact-route source-ip address dest-ip address** and **show ip cef exact-route source-ip address dest-ip address** is different because the packets are software switched when IP CEF is used, and the packets are hardware switched when MLS CEF is used. Because most of the packets are hardware switched, the best command to view the next-hop to reach a destination is **show mls cef exact-route source-ip address dest-ip address**.

Related Information

- **Troubleshoot Unicast IP Routing Involving CEF on Catalyst 6500/6000 Series Switches with a Supervisor Engine 2 and Running CatOS System Software**
- **Configuring and Troubleshooting IP MLS on Catalyst 6500/6000 Switches with an MSFC**

- **LAN Product Support Pages**
 - **LAN Switching Support Page**
 - **Tools & Resources**
 - **Technical Support & Documentation – 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: Dec 11, 2008

Document ID: 64939
