

对带有Supervisor 引擎 2且运行CatOS系统软件的Catalyst 6500/6000 系列交换机上涉及CEF的单播IP路由进行故障检修。

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[CEF概述](#)

[转发信息库 \(FIB\)](#)

[邻接表](#)

[如何读取PFC2上的FIB和邻接表](#)

[故障排除方法](#)

[案例分析 1：与直连网络中主机的连接](#)

[故障排除步骤](#)

[注解和结论](#)

[案例分析 2：到远程网络的连接](#)

[故障排除步骤](#)

[注解和结论](#)

[案例分析 3：负载均衡到多个下一跳](#)

[案例分析 4：默认路由](#)

[MSFC2路由表中存在默认路由](#)

[路由表中没有默认路由](#)

[其它故障排除提示和已知问题](#)

[发出show mls cef mac命令](#)

[Shadow TCAM](#)

[默认路由中断](#)

[相关信息](#)

简介

本文档应用于指南，以排除Catalyst 6500/6000交换机上单播IP路由故障，该交换机带有Supervisor引擎2、策略功能卡2(PFC2)、多层交换机功能卡2(MSFC2)。管理引擎2上的单播路由使用思科快速转发(CEF)完成。本文档仅涉及配备Supervisor引擎2、PFC2、MSFC2的Catalyst 6500/6000系列上的IP路由。本文档对带Supervisor引擎1 (或1A) 的Catalyst 6500/6000或多层交换模块(MSM)无效。本文档仅对在Supervisor引擎上运行Catalyst OS(CatOS)系统软件的交换机有效，对Cisco IOS®系统软件无效。

[先决条件](#)

[要求](#)

本文档没有任何特定的要求。

[使用的组件](#)

本文档不限于特定的软件和硬件版本。

[规则](#)

有关文件规则的更多信息请参见“Cisco技术提示规则”。

[CEF概述](#)

CEF最初是Cisco IOS软件交换技术，旨在更快地路由数据包。CEF比快速交换更具扩展性。（无需将第一个数据包发送到进程交换。）带Supervisor引擎2的Catalyst 6500使用在PFC2上实施的基于硬件的CEF转发机制。CEF主要使用两个表来存储路由所需的信息：转发信息库(FIB)和邻接表。

[转发信息库 \(FIB\)](#)

CEF使用FIB做出基于IP目标前缀的交换决策（最长匹配优先）。FIB是概念上和路由表或信息库类似。它维护IP路由表中包含的转发信息的镜像。当网络中发生路由或拓扑更改时，IP路由表将进行更新，然后这些更改将反映在FIB中。FIB根据IP路由表中的信息维护下一跳地址信息。由于FIB条目和路由表条目之间的一对一关联，FIB包含所有已知路由，并且无需维护与交换路径相关的路由缓存，例如快速交换和最佳交换。FIB中始终存在匹配项，无论是默认还是通配符。

[邻接表](#)

如果网络中的节点能通过链路层的单跳到达对方，则这些节点称为相邻节点。除FIB外，CEF还使用邻接表来预置第2层(L2)编址信息。邻接表维护所有FIB条目的L2下一跳地址。这意味着完整的FIB条目包含指向邻接表中某个位置的指针，该位置保存下一跳到达最终IP目标的L2重写信息。为了使硬件CEF在Catalyst 6500/Supervisor引擎2系统上工作，IP CEF需要在MSFC2上运行。

[如何读取PFC2上的FIB和邻接表](#)

PFC2的FIB表应与MSFC2上的FIB表完全相同。在PFC2上，FIB中的所有IP前缀都存储在三层内容可寻址存储器(TCAM)中，并按掩码长度排序，从最长掩码开始。这意味着您首先找到掩码为32（主机条目）的所有条目；接下来，您会找到掩码长度为31的所有条目，依此类推，直到您到达掩码长度为0的条目。这是默认条目。FIB被按顺序读取，并且第一次命中用作匹配。请考虑PFC2上的以下示例FIB表：

```
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.

```

每个条目包含以下字段：

- Mod — 安装该条目的MSFC2为15或16，具体取决于指定的MSFC2。
- FIB — 与此特定条目关联的类型。可能FIB包括：`receive` — 与MSFC接口关联的前缀。这包含一个前缀，其掩码为32，与MSFC接口的IP地址和广播子网的IP地址对应。`resolved` — 与有效下一跳地址关联的前缀。这包含具有下一跳已解析邻接关系的任何前缀。`connected` — 与已连接网络关联的前缀。`wildcard` — 匹配所有条目（丢弃或MSFC重定向）。此条目仅在没有默认条目时存在，且掩码长度为0。`default` — 默认路由。作为通配符条目，它匹配所有子网，掩码长度为0。它指向下一跳。仅当路由表中存在默认路由时，此默认CEF条目才存在。`drop` — 丢弃与条目匹配的所有数据包。
- Destination-IP — 相关的目标IP地址或IP子网。
- — 与条目关联的掩码。如上例所示，FIB从最长掩码(255.255.255.255)开始，以最短掩码(0.0.0.0)结束。
- Next-Hop IP — 显示下一跳IP（如果存在）。

您可以通过输入以下命令查看完整的邻接表：

```

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

```

注意：此输出包含一个与上面示例FIB表中找到的条目类似的条目，用于FIB中每个已解析（或默认）CEF条目。

故障排除方法

在提供故障排除的一些示例和详细信息之前，本节总结了排除特定IP地址的连通性或可达性故障所遵循的方法。请记住，PFC2上的CEF表镜像MSFC2上的CEF表。因此，如果MSFC2知道的信息也正确，PFC2仅保存到达IP地址的正确信息。因此，您始终需要验证以下信息。

从MSFC2:

请完成以下步骤：

1. 通过发出`show ip route`命令(或`show ip route x.x.x.x`命令，以避免浏览完整的路由表)，验证MSFC2表上IP路由中保存的信息是否正确，然后验证输出是否包含预期的下一跳。否则，您

需要检查路由协议、配置、路由协议邻居以及与您运行的路由协议相关的任何其他故障排除。

2. 通过发出`show ip arp next_hop_ip_address`命令，验证ARP已解析并包含正确的MAC地址，在MSFC2上验证下一跳（或已连接网络的最终目的地）是否具有正确的已解析地址解析协议（ARP）条目。如果MAC地址不正确，您需要验证另一台设备是否拥有该IP地址。最终，您需要跟踪连接拥有该MAC地址的设备的端口上的交换机级别。如果ARP条目不完整，则表示您未收到该主机的任何回复。您需要检验主机是否已启动并正在运行。主机上可能会使用嗅探器来查看它是否收到ARP应答以及它是否正确应答。
3. 验证MSFC2上的CEF表包含正确的信息，并通过执行以下步骤解析邻接关系：发出`show ip cef destination_network`命令，以验证CEF表中的下一跳是否与IP路由表中的下一跳匹配（从上面的步骤1开始）。通过发出`show adjacency detail`命令，验证邻接是否正确 | `begin next_hop_ip_address`命令。这应包含上面步骤2中所示的ARP的相同MAC地址。

如果上述步骤1和2提供正确的结果，但步骤3a或3b失败，则您面临的Cisco IOS软件CEF问题可能与Catalyst 6500/6000无关。您必须尝试清除ARP表和IP路由表。

从PFC2:

请完成以下步骤：

1. 通过发出`show mls entry cef ip destination_ip_network/destination_subnet_mask`命令，验证PFC2上存储的FIB信息是否正确，并与MSFC2上CEF表中存储的信息（如上面的步骤3所示）相匹配，然后验证下一跳IP地址是否是您期望的。如果信息与上面步骤3中的结果不匹配，则表明MSFC2和PFC2（Catalyst 6500/6000内部）之间存在通信问题。验证PFC2的CatOS或运行的MSFC2的Cisco IOS软件没有已知的Bug。您可以在MSFC2上发出`clear ip route`命令，以恢复正确的条目。
2. 通过发出`show mls entry cef ip next_hop_ip_address/32 adjacency`命令，然后验证其包含的MAC地址与上文“从MSFC2”部分步骤2和步骤3b中所示的MAC地址相同，以验证PFC2上的邻接表。如果PFC2中的邻接与步骤3b中下一跳的邻接不匹配，则您可能面临MSFC2和PFC2之间的内部通信问题。您可以尝试清除邻接以恢复正确的信息。

案例分析 1：与直连网络中主机的连接

此简单案例提供了以下之间连接的研究：

- IP地址为192.168.10.10的VLAN 10中的host 1
- IP地址为192.168.199.3的VLAN 199中的host 2

以下是MSFC2配置输出的示例：

```
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
```

注意：请注意，带Supervisor引擎2和MSFC2的Catalyst 6500/6000在硬件中使用CEF进行路由。没有要为其配置的内容。无法在MSFC2上禁用CEF。

故障排除步骤

按照本文档故障排除方法部分突出显示的步骤验证到达IP地址192.168.199.3的路径。

1. 发出以下任一命令来检验IP路由表：

```
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
```

或

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

在这两个命令输出中，您可以看到目的地位于直连子网中。因此，没有到达目的地的下一跳。

2. 检验MSFC2上的ARP条目。在这种情况下，请发出以下命令，验证目的IP地址是否有ARP条目：

```
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. 检验MSFC2上的CEF和邻接表。发出以下命令，验证CEF表：

```
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
```

您可以看到，存在掩码长度为32的有效CEF条目，并且存在有效的缓存邻接关系。发出以下命令验证邻接表：

```
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
```

从以上输出中可以看到，存在邻接关系。邻接的目的MAC地址显示的信息与上面步骤2的ARP表中的MAC地址相同。请注意，步骤3b中的计数器几乎总是0，因为数据包是在硬件中交换的第3层(L3)。因此，它们永远不会到达MSFC2，并且不计入MSFC2 CEF计数器。查看转发到给定目的地的数据包统计信息的唯一方法是查看步骤5中在PFC2上找到的邻接关系统计信息。

4. 从Supervisor引擎的角度验证您是否具有正确的CEF/FIB条目。FIB中有两个有趣的条目，如下所示：目标IP地址的条目，如下所示：

```
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
```

此条目是具有已知下一跳的主机条目（在本例中，它是目标本身）。与目的网络对应的条目，如下所示：

```
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
```

此条目是连接的FIB条目，这意味着到达此条目的任何数据包都会重定向到MSFC2以进行进一步处理（主要是发送ARP并等待ARP解析）。请记住，FIB是从最长掩码长度开始按顺序浏览的。因此，如果上面步骤4中列出的两个条目都存在，则您使用掩码32（主机条目）命中第一个条目，并且不会在FIB表中进一步。如果/32条存在，则点击第二个条目，即网络条目；由于它是连接条目，因此您将数据包重定向到MSFC2以进一步处理。MSFC2很可能会发送ARP请求来获取目的掩码。收到ARP应答后，MSFC2上该主机的ARP表和邻接表即会完成。

5. 一旦您有了掩码长度为32的正确FIB条目，请发出以下命令，验证该主机的邻接关系是否已正确填充：

```
Cat6k> (enable) show mls entry cef ip 192.168.199.3/32 adjacency
Mod:15
Destination-IP : 192.168.199.3 Destination-Mask : 255.255.255.255
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
```

注意：邻接关系已填充，NextHop-Mac 字段包含主机2的有效MAC地址（如步骤2和3b所示）。此时，所有输出都正确，但此邻接关系的已传输数据包数仍为0。在下一个示例中，您从主机1向主机2发送10个100字节的ping，然后再次检查邻接关系。

```
Cat6k> (enable) show mls entry cef ip 192.168.199.3/32 adjacency
Mod:15
Destination-IP : 192.168.199.3 Destination-Mask : 255.255.255.255
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      10          1000
```

您现在可以看到TX-Packets的数量为10，与发送的流量一致。

注解和结论

如上面的故障排除步骤第4步中所述，您有两个FIB条目可以很好地匹配，如下所述：

- network entry(本例中为192.168.199.0/24) — 此条目始终存在，并且直接来自MSFC上的路由和CEF表。路由表中始终直连此网络。
- 目标主机条目(本例中为192.168.199.3/32) — 此条目不一定存在。否则，您会点击网络条目，并出现以下项：数据包被转发到MSFC2。然后，在PFC的FIB表中创建掩码长度为32的主机条目。但是，由于您尚未建立完整的邻接关系，因此会创建邻接关系，其类型为 `frc drop`（这意味着强制丢弃）。该目的地的后续数据包命中 `/32 frc` 丢弃条目，并丢弃该数据包。同时，发送到MSFC2的原始数据包会触发MSFC2发送ARP请求。解析ARP后，ARP条目即完成。MSFC2上的邻接关系已完成，并且邻接更新已发送到Supervisor引擎以完成现有 `frc` 邻接。Supervisor引擎更改主机邻接关系以反映重写MAC地址，并且邻接类型更改为连接。在等待ARP解析时 `FRc` 丢弃邻接关系的这种机制称为ARP限制。ARP限制有助于避免将所有数据包转发到MSFC2并生成多个ARP请求。只有前几个数据包会发送到MSFC2，其余数据包会在PFC2上丢弃，直到邻接关系完成。这还允许您丢弃定向到直连网络中不存在或无响应主机的流量。

排除两个不同VLAN中两个用户之间的连接故障时，务必始终牢记您需要了解：

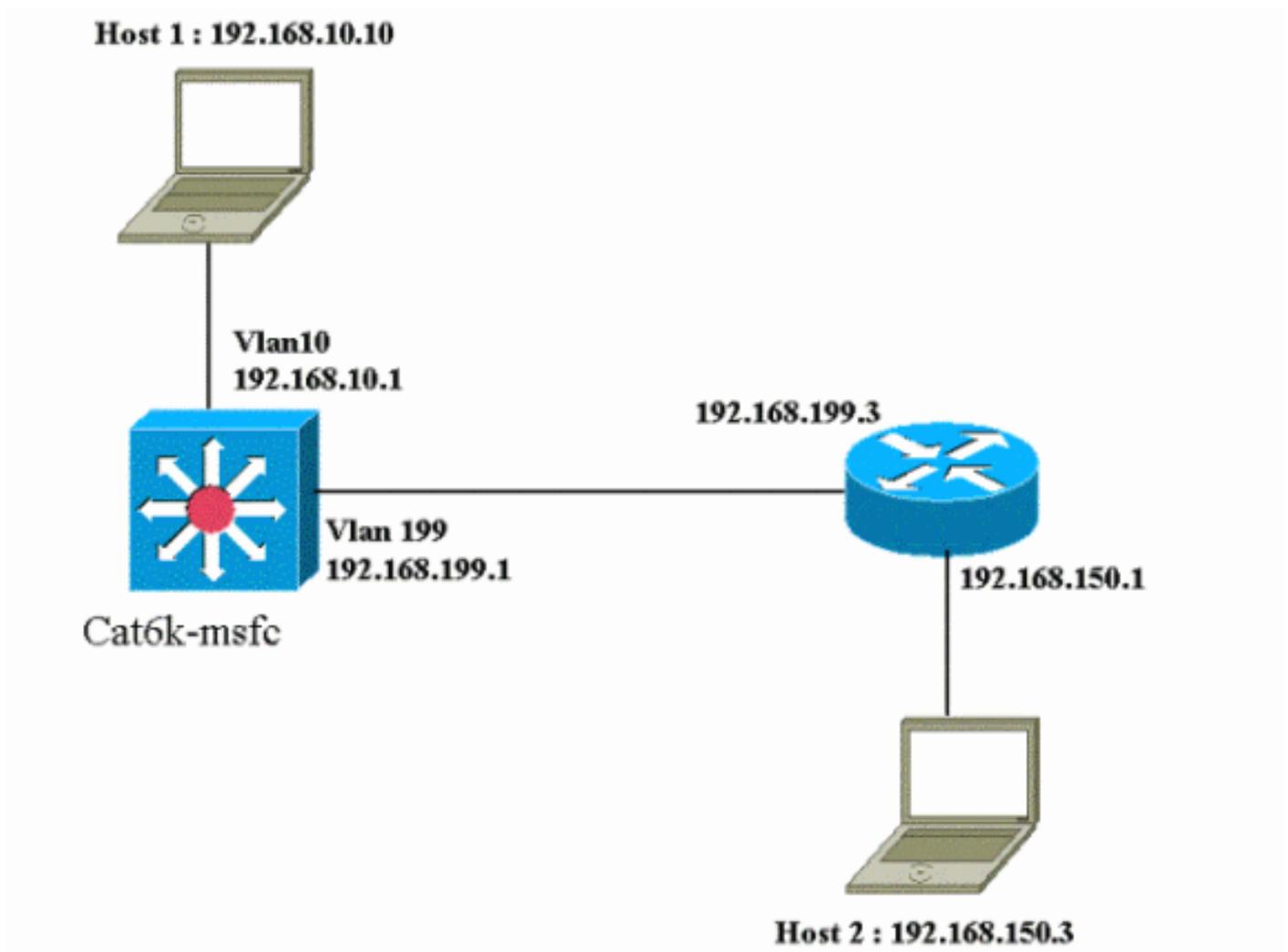
- 使用上述故障排除方法从主机1到主机2的流量，以[使目的IP地址为主机2](#)
- 使用相同方法从主机2到主机1的流量，但此次目标为主机1

还要记住，输出需要在源的默认网关上执行，这不一定与从主机1到主机2的流量以及从主机2到主机1的流量相同。

注意：由于数据包在硬件中进行L3交换，[因此](#)上述故障排除步骤步骤3b中的计数器几乎始终为0。因此，它们永远不会到达MSFC2，并且不计入MSFC2 CEF计数器。查看转发到给定目的地的数据包统计信息的唯一方法是在上述故障排除步骤步骤的步骤5期间查看在PFC2上找到的邻[接关系](#)的统计信息。

案例分析 2：到远程网络的连接

请看下图，其中IP地址为192.168.10.10 ping的主机1 IP地址为192.168.150.3的主机2。但是，这次，主机2位于两个路由跃点之外，而不是直接连接到Catalyst 6500/6000-MSFC2。在Catalyst 6500/6000-MSFC2上，使用相同方法遵循CEF路由路径。



故障排除步骤

请完成以下步骤：

1. 发出以下命令检查MSFC2上的路由表：

```
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
```

从上面的输出中可以看到，要到达IP地址为192.168.150.3的主机2，您有开放最短路径优先(OSPF)路由。需要使用VLAN 199中的IP地址192.168.199.3作为下一跳来到达它。

2. 发出以下命令，检查MSFC2上的ARP表。注意：检查ARP条目以查找下一跳，而不是最终目的地。

```
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. 发出以下命令，检查MSFC2上的CEF表和邻接表：

```
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
```

您可以看到目的网络有一个CEF条目，下一跳结果与您在第1步的路由表中的结果匹配。

4. 发出以下命令，检查下一跳的邻接表：

```
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
```

下一跳存在有效的邻接关系，且目的MAC地址与上述步骤2中找到的ARP条目匹配。

5. 发出以下命令，检查Supervisor引擎(PFC2)上的FIB表：

```
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
```

FIB反映的信息与步骤3中的信息相同，您的下一跳也相同。

6. 发出以下命令，检查Supervisor引擎(PFC2)上的邻接关系：

```
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
```

您还可以验证是否具有反映上述步骤2和4中所示相同MAC地址的连接邻接关系。

注意：在检查PFC2上的邻接关系时，可以检查最终目标的邻接关系。在MSFC2上的Cisco IOS软件中，这是不可能的，您需要使用该软件检查下一跳的邻接关系。PFC2上最终目的地的邻接表同时显示下一跳和下一跳的邻接（如果已解析），全部在一个命令输出中。在MSFC2上，您需要单独检查CEF条目以查找下一跳，然后查看下一跳邻接关系本身。

注解和结论

在本例中，您可以看到用于验证Catalyst 6500/6000-MSFC2上连接以到达远程网络的故障排除步骤与案例研究1部分中的上一个示例[类似：与直连网络中主机的连接](#)。然而，这里有一些不同：

- 在IP路由表、CEF表和FIB中检查最终目标（步骤1、3和5）。
- 您将检查ARP表和邻接表中的下一跳信息（步骤2和4）。
- 在步骤6中，您可以直接检查最终目标的邻接关系。结果显示来自FIB的下一跳和来自邻接表的邻接重写信息。

在这种情况下，FIB中没有最终目的地的条目，如下所示。（仅存在掩码长度为24的网络条目。）

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

案例分析 3：负载均衡到多个下一跳

本案例研究讨论当有多个下一跳和多条路由可用于到达同一目的网络时会发生什么情况。

1. 在下面的路由表示例部分中，请注意有三条不同的路由和三条不同的下一跳可用于到达同一目

的IP地址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
```

- 按照以下步骤检查ARP条目，查找下三跳中的每一跳：检查CEF表以查找目标。请注意，目标还在MSFC2的CEF表中显示了三个不同的条目。Cisco IOS软件CEF能够在不同路由之间进行负载共享。

```
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
```

检查MSFC2邻接表中的三项邻接关系。它们应与上述步骤2中的ARP条目匹配。

- 请注意，为同一目标安装了三个不同的FIB条目。PFC2上的硬件CEF能够为同一目标加载最多六个不同路径的共享。您可以在权重字段中查看用于每个下一跳的权重。PFC2使用的负载共享仅是每流负载共享。它不启用每数据包负载共享。

```
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
```

- 发出以下命令检查该目标条目的邻接关系：

```
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
```

案例分析 4：默认路由

无论路由表如何显示，Supervisor引擎2中始终有一个FIB条目，用于转发与任何其他先前条目不匹配的数据包。您可以通过发出以下命令来查看此条目：

```
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
```

如您所见，这是唯一掩码长度为0的条目。此默认路由可以分为两种类型，如[MSFC2路由表中存在默认路由和路由表中无默认路由部分](#)中所述。

MSFC2路由表中存在默认路由

首先，确定如何验证MSFC2路由表中是否存在默认路由。您可以查找目标为0.0.0.0的路由，也可以查找路由表。默认路由标有星号(*)。(此处也以粗体显示。)

```
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
```

在这种情况下，默认路由存在于MSFC2路由表中，并通过路由信息协议(RIP)获取。但是，请注意，无论如何获取此默认路由(静态、OSPF、RIP等)，CEF行为都是相同的。

在这种情况下，如果您有默认路由，则始终有掩码长度为0的CEF条目和FIB-Type 默认条目，用于转发与任何其他前缀不匹配的所有流量。

```
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
```

由于FIB按顺序浏览每个数据包(以最长匹配开头)，因此此默认FIB仅用于找不到其他匹配项的数据包。

路由表中没有默认路由

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

如果路由表中没有任何默认路由，则Supervisor引擎2中仍有掩码长度为0的FIB条目。但是，此条目现在具有FIB-Type通配符。此通配符FIB会丢弃所有到达它的数据包，并匹配与FIB中任何其他条目不匹配的任何数据包。丢弃这些数据包非常有用，因为您没有任何默认路由。无需将这些数据包转发到MSFC2,MSFC2会丢弃它们。通过使用此通配符FIB，您可以确保在硬件中丢弃这些无用数据包。

```
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
```

注意：在FIB表已满的极少数情况下，通配符条目仍然存在，但是，它们不会丢弃与其匹配的数据包，而是会转发到MSFC2。仅当FIB中有超过256K前缀，并且无法在FIB中存储完整的路由表和ARP时，才会发生这种情况。然后，您需要将默认机制发送到MSFC2，因为MSFC2可以具有FIB中

不存在的路由条目。

其它故障排除提示和已知问题

发出show mls cef mac命令

当Supervisor引擎2获取数据包时，它仅将其视为可能的第3层数据包，前提是数据包的目的MAC地址与其中一个MSFC2 MAC地址相同。您可以发出以下命令，验证这些地址是否来自Supervisor引擎2的视点：

```
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
```

您可以看到MSFC2的物理MAC地址。(请记住，MSFC2上的所有接口都使用相同的MAC地址；不能在两个不同的接口上配置不同的MAC地址。) 此MAC地址需要与MSFC2上的MAC地址相同。

```
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)
?..
```

show mls cef mac命令还显示链接到热备份路由器协议(HSRP)组(其中MSFC处于活动状态)的所有MAC地址。以上show mls cef mac命令的输出意味着MSFC对于VLAN 10和VLAN 100是HSRP活动的。您可以在MSFC2上发出以下命令来验证这是正确的：

```
Cat6k-MSFC2# show standby brief
P indicates configured to preempt.
|
Interface Grp Prio P State Active addr Standby addr Group addr
Vl10 10 200 P Active local 192.168.10.2 192.168.10.254
Vl11 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
```

如您所见，仅VLAN 10和VLAN 100的状态为Active。对于配置的所有其他HSRP组，状态Standby。如果由于任何原因，另一个VLAN的Active状态开始，则show mls cef mac命令的输出应会反映出此附加VLAN未处于活动状态。

如果show mls cef mac命令输出与应输出不一致，则可以发出以下命令，该命令提供有关在show mls cef mac命令列表中添加和删除的MAC地址的更多信息：

```
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-fc
added 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
```

每次在show mls cef mac命令表中添加或删除MAC地址时，此命令都会提供消息。

[Shadow TCAM](#)

本文档讨论了如何检查Supervisor引擎2上的show mls entry cef命令表。此命令不能准确表示PFC2的实际专用集成电路(ASIC)编程。它只表示此ASIC设置的卷影副本。已知存在一些问题，即实际硬件设置与影子TCAM中显示的内容不一致，导致某些数据包转发到错误的下一跳。这些问题记录在Cisco Bug ID [CSCdv49956 \(仅注册客户\)](#)和[CSCdu85211 \(仅注册客户\)](#)(在CatOS软件版本6.3(3)、7.1(1)中都已修复)中等会再说。

[默认路由中断](#)

在早期版本的代码中发现一个错误，在该错误中，转发到默认路由不能与增强型内部网关路由协议(EIGRP)或OSPF配合使用。这记录在Cisco Bug ID [CSCdt54036 \(仅注册客户\)](#)中，并在CatOS软件版本6.1(3)及更高版本中(用于Supervisor引擎映像)和Cisco IOS软件版本12.1(6)E1(用于MSFC2)中图像。

[相关信息](#)

- [带 MSFC 的 Catalyst 6000 交换机上的 IP MLS 的配置与故障排除](#)
- [LAN 产品支持页](#)
- [LAN 交换技术支持页](#)
- [工具和实用程序](#)
- [技术支持 - Cisco Systems](#)