

# 使用Supervisor Engine 2且執行CatOS系統軟體的Catalyst 6500/6000系列交換器上涉及CEF的單播IP路由疑難排解

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[CEF概述](#)

[轉送資訊庫\(FIB\)](#)

[鄰接表](#)

[如何讀取PFC2上的FIB和鄰接表](#)

[故障排除方法](#)

[案例研究1:連線到直連網路中的主機](#)

[疑難排解步驟](#)

[備註和結論](#)

[案例研究2:連線到遠端網路](#)

[疑難排解步驟](#)

[備註和結論](#)

[案例研究3:到下一跳的負載均衡](#)

[案例研究4:預設路由](#)

[MSFC2路由表中存在預設路由](#)

[路由表中沒有預設路由](#)

[其他疑難排解提示和已知問題](#)

[發出show mls cef mac命令](#)

[影子TCAM](#)

[預設路由已中斷](#)

[相關資訊](#)

## 簡介

本文應用作指南，對搭載Supervisor引擎2、原則功能卡2(PFC2)和多層交換器功能卡2(MSFC2)的Catalyst 6500/6000交換器上的單點傳播IP路由進行疑難排解。Supervisor Engine 2上的單播路由是使用Cisco Express Forwarding(CEF)完成的。本文只涉及配備了Supervisor Engine 2、PFC2和MSFC2的Catalyst 6500/6000系列上的IP路由。本檔案不適用於具備Supervisor Engine 1 (或1A)的Catalyst 6500/6000或多層交換器模組(MSM)。本檔案僅適用於在Supervisor Engine上執行Catalyst OS(CatOS)系統軟體的交換器，而不適用於Cisco IOS®系統軟體。

## 必要條件

### 需求

本文件沒有特定需求。

### 採用元件

本文件所述內容不限於特定軟體和硬體版本。

### 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## CEF概述

CEF最初是一種Cisco IOS軟體交換技術，旨在更快地路由資料包。CEF的可擴充性比快速交換強得多。（無需將第一個資料包傳送到進程交換。）搭載Supervisor Engine 2的Catalyst 6500使用在PFC2上實作的硬體CEF轉送機制。CEF主要使用兩個表來儲存路由所需的資訊：轉發資訊庫（FIB）和鄰接表。

### 轉送資訊庫(FIB)

CEF使用FIB作出IP目的地首碼型交換決定（最長匹配優先）。FIB在概念上類似於路由表或資訊庫。它維護IP路由表中包含的轉發資訊的映象。當網路中發生路由或拓撲更改時，IP路由表將更新，這些更改將反映在FIB中。FIB根據IP路由表中的資訊維護下一跳地址資訊。由於FIB條目和路由表條目之間是一對一的關聯，FIB包含所有已知路由，並且不需要與交換路徑相關聯的路由快取維護，例如快速交換和最佳交換。FIB中總有一個相符專案，無論是預設專案還是萬用字元專案。

### 鄰接表

如果網路中的節點能夠通過鏈路層的一跳到達彼此，則稱為相鄰節點。除FIB外，CEF還使用鄰接表來預置第2層(L2)編址資訊。鄰接表為所有FIB條目維護第2層下一跳地址。這表示完整的FIB條目包含指向鄰接表中位置的指標，該位置儲存了下一跳到達最終IP目標的L2重寫資訊。為了讓硬體CEF在Catalyst 6500/Supervisor Engine 2系統上工作，需要在MSFC2上運行IP CEF。

## 如何讀取PFC2上的FIB和鄰接表

PFC2的FIB表應該與MSFC2上的FIB表完全相同。在PFC2上，FIB中的所有IP字首都儲存在三重內容可定址儲存器(TCAM)中，並按掩碼長度排序，以最長掩碼開始。這表示首先找到遮罩為32的所有專案（主機專案）；接下來，查詢掩碼長度為31的所有條目，以此類推，直至找到掩碼長度為0的條目。這是預設條目。順序讀取FIB，並將第一次命中用作匹配。請考慮使用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.

```

每個條目包含以下欄位：

- Mod — 安裝條目的MSFC2為15或16，具體取決於哪個是指定的MSFC2。
- FIB-Type — 與此特定條目關聯的型別。可能的FIB包括：`receive` — 與MSFC介面關聯的字首。這包含與MSFC介面的IP地址和廣播子網的IP地址對應的掩碼為32的字首。`resolved` — 與有效下一跳地址關聯的字首。這包含具有下一躍點的已解析鄰接關係的任何字首。`connected` — 與已連線網路關聯的字首。`wildcard` — 此選項匹配所有條目（丟棄或MSFC重新導向）。此條目僅在沒有預設條目時存在，掩碼長度為0。`default` — 預設路由。作為萬用字元條目，它匹配所有子網，掩碼長度為0。它指向下一跳。僅當路由表中存在預設路由時，才會出現此預設CEF條目。`drop` — 丟棄與具有丟棄的條目匹配的所有資料包。
- Destination-IP — 相關的目標IP地址或IP子網。
- Destination-Mask — 與條目關聯的掩碼。如上例所示，FIB的排名從最長的掩碼（255.255.255.255）開始，並以最短的掩碼（0.0.0.0）結束。
- Next-Hop IP — 顯示下一跳IP（如果存在）。

您可以通過輸入以下命令檢視完整的鄰接表：

```

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

```

註：此輸出包含與上例FIB表中的條目類似的條目，用於FIB中每個已解析（或預設）的CEF條目。

## 故障排除方法

在提供故障排除的一些示例和詳細資訊之前，本節總結了對特定IP地址進行連線或可達性故障排除所遵循的方法。請記住，PFC2上的CEF表映象MSFC2上的CEF表。因此，如果MSFC2所知的資訊也正確，PFC2僅保留到達IP地址的正確資訊。因此，您始終需要驗證以下資訊。

### 在MSFC2上：

請完成以下步驟：

1. 發出`show ip route`命令(或`show ip route x.x.x.x`命令，避免瀏覽完整的路由表)以驗證

MSFC2表上IP路由中儲存的資訊是否正確，然後驗證輸出是否包含預期的下一跳。如果不是，您需要檢查您的路由協定、配置、路由協定鄰居以及與您正在運行的路由協定相關的任何其他故障排除。

2. 發出**show ip arp next\_hop\_ip\_address** 命令，確認下一個躍點（或所連網路的最終目的地）在MSFC2上是否有正確的已解析位址解析通訊協定(ARP)專案，然後確認ARP已解析且包含正確的MAC位址。如果MAC地址不正確，您需要驗證另一台裝置是否擁有該IP地址。最後，您需要在連線擁有該MAC地址裝置的埠上跟蹤交換機級別。如果ARP專案不完整，則表示您未從該主機獲得任何回覆。您需要驗證主機是否已啟動並正在運行。主機上可能會使用監聽器來檢查它是否收到了ARP回覆以及是否正確回應。
3. 驗證MSFC2上的CEF表包含正確的資訊，並通過執行以下步驟解決鄰接關係：發出**show ip cef destination\_network** 命令，確認CEF表中的下一跳與IP路由表中的下一跳匹配（來自上述步驟1）。發出**show adjacency detail**，確認鄰接關係是否正確 | **begin next\_hop\_ip\_address** 命令。它應包含上述步驟2中相同的ARP MAC地址。

如果上述步驟1和2提供正確結果，但步驟3a或3b失敗，則您會遇到可能與Catalyst 6500/6000無關的Cisco IOS軟體CEF問題。您必須嘗試清除ARP表和IP路由表。

## [在PFC2上：](#)

請完成以下步驟：

1. 通過發出**show mls entry cef ip destination\_ip\_network/destination\_subnet\_mask** 命令，驗證PFC2上儲存的FIB資訊是否正確並與MSFC2上CEF表中儲存的資訊（如上面的步驟3所示）匹配，然後驗證下一跳IP地址是否為您期望的地址。如果資訊與上述步驟3中的結果不匹配，則表明MSFC2和PFC2之間存在通訊問題（Catalyst 6500/6000內部）。確認您運行的PFC2的CatOS或MSFC2的Cisco IOS軟體沒有已知錯誤。您可以在MSFC2上發出**clear ip route**命令，以恢復正確的條目。
2. 發出**show mls entry cef ip next\_hop\_ip\_address/32 adjacency**命令以驗證PFC2上的鄰接表，然後驗證它包含的MAC地址是否與上面[從MSFC2](#)一節的步驟2和3b中顯示的相同。如果PFC2中的鄰接關係與步驟3b中下一跳的鄰接關係不匹配，則可能會面臨MSFC2和PFC2之間的內部通訊問題。您可以嘗試清除鄰接關係以還原正確的資訊。

## [案例研究1:連線到直連網路中的主機](#)

這個簡單的案例將研究以下各項之間的連通性：

- VLAN 10中的主機1,IP地址為192.168.10.10
- VLAN 199中的主機2,IP地址為192.168.199.3

以下是MSFC2配置輸出的示例：

```
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
```

**註：**請注意，搭載Supervisor Engine 2和MSFC2的Catalyst 6500/6000在硬體中使用CEF進行路由。沒有要配置的內容。無法在MSFC2上禁用CEF。

## 疑難排解步驟

請按照本檔案[故障排除方法](#)部分中突出顯示的步驟操作，驗證到達IP地址192.168.199.3的路徑。

### 1. 發出以下任一命令以驗證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
```

從這兩個命令輸出中，可以看到目標位於直連子網中。因此，沒有到達目的地的下一跳。

### 2. 檢驗MSFC2上的ARP條目。在這種情況下，發出以下命令以驗證目的IP地址是否存在ARP條目：

```
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. 驗證MSFC2上的CEF和鄰接表。發出以下命令以驗證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
```

您可以看到存在掩碼長度為32的有效CEF條目，並且存在有效的快取鄰接關係。發出以下命令驗證鄰接表：

```
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
```

從上面的輸出中您可以看到，存在鄰接關係。鄰接的目標MAC地址顯示的資訊與上面步驟2的ARP表中的MAC地址相同。請注意，步驟3b中的計數器幾乎一律為0，因為封包是在硬體中交換的第3層(L3)。因此，它們永遠不會到達MSFC2，並且不會計入MSFC2 CEF計數器。檢視轉發到給定目的地的資料包統計資訊的唯一方法是檢視步驟5期間在PFC2上發現的鄰接統計資訊。

### 4. 從Supervisor Engine的角度驗證您是否具有正確的CEF/FIB條目。FIB中有兩個有趣的條目，如下所示：目標IP地址的條目，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
```

此專案是包含已知下一躍點的主機專案（在本案例中是目的地本身）。與目的網路對應的條目，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
```

此條目是連線的FIB條目，這意味著遇到此條目的任何資料包都會重定向到MSFC2以進行進一步處理（主要傳送ARP並等待ARP解析）。請記住，FIB按順序瀏覽，從最長的掩碼長度開始。因此，如果上述步驟4中列出的兩個條目都存在，則您使用掩碼32（主機條目）擊中的第一個條目，並且不會進一步進入FIB表。如果沒有/32專案，則點選第二個專案，即網路的專案

；由於資料包是連線的條目，因此您需要將資料包重定向到MSFC2以進行進一步處理。MSFC2很可能傳送目標掩碼的ARP請求。收到ARP應答後，MSFC2上該主機的ARP表和鄰接表即完成。

5. 收到掩碼長度為32的正確FIB條目後，發出以下命令驗證該主機的鄰接關係是否正確填充：

```
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：**鄰接關係已填充，並且NextHop-Mac欄位包含主機2的有效MAC地址（如步驟2和3b所示）。此時，所有輸出都正確，儘管此鄰接的已傳輸資料包數仍為0。在下一個示例中，您將從主機1向主機2傳送十個100位元組的ping，並再次檢查鄰接關係。

```
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
```

現在您可以看到TX-Packets的數量為10，這與已傳送的流量一致。

## 備註和結論

正如上述疑難排解步驟的步驟4中所述，有兩個完全匹配的FIB條目，如下所示：

- network entry(本例中為192.168.199.0/24) — 此條目始終存在，並且直接來自MSFC上的路由和CEF表。在路由表中總是直接連線此網路。
- 目標主機條目(本例中為192.168.199.3/32) — 此條目不一定存在。如果失敗，您按一下網路專案，系統就會發生以下專案：資料包被轉發到MSFC2。掩碼長度為32的主機條目接著在PFC的FIB表中建立。但是，由於您尚未建立完全鄰接關係，因此建立鄰接關係的型別為frd drop（這意味著強制丟棄）。該目的地的後續封包會命中/32 frd drop，因此該封包會遭捨棄。同時，傳送到MSFC2的原始資料包觸發MSFC2傳送ARP請求。解析ARP後，ARP條目即完成。鄰接關係在MSFC2上完成，鄰接更新將傳送到Supervisor Engine以完成現有的frd接。Supervisor Engine更改主機鄰接關係以反映重寫MAC地址，並且鄰接型別更改為連線。在等待解析ARP時frd drop鄰接關係的這種機制稱為ARP限制。ARP限制對於避免將所有資料包轉發到MSFC2並生成多個ARP請求非常有用。僅將前幾個資料包傳送到MSFC2，其餘資料包在PFC2處丟棄，直到鄰接關係完成。此功能也允許您丟棄定向到直連網路中不存在或無響應主機的流量。

對兩個不同VLAN中的兩個使用者之間的連線進行故障排除時，請務必記住您需要檢視：

- 使用上述Troubleshooting Method從主機1到主機2的流量，用於使目標IP地址成為主機2
- 從主機2到主機1的流量使用相同方法，但這一次目的地為主機1

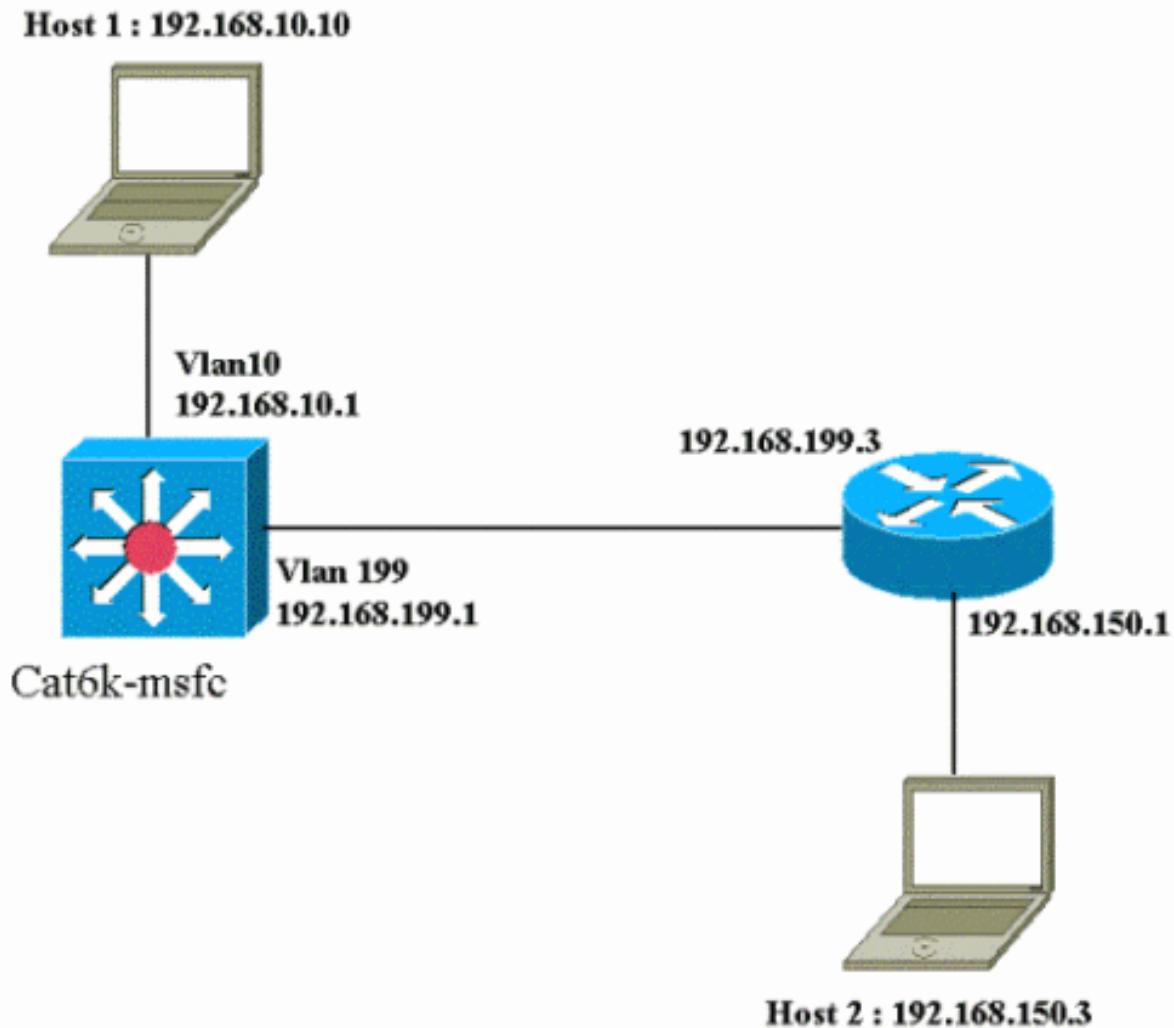
記住以下情況也很重要：輸出需要在源的預設網關上執行，從主機1到主機2以及從主機2到主機1的流量不一定相同。

**註：**上面的故障排除步驟的步驟3b中的計數器幾乎總是零，因為資料包是在硬體中進行第3層交換的。因此，它們永遠不會到達MSFC2，並且不會計入MSFC2 CEF計數器。檢視轉發到給定目的地的資料包統計資訊的唯一方法是檢視在上述故障排除步驟的步驟5中在PFC2上發現的鄰接統計資訊。

。

## 案例研究2:連線到遠端網路

請考慮以下圖表，其中IP位址為192.168.10.10的主機1對IP位址為192.168.150.3的主機2執行ping操作。但是，這一次，主機2位於兩個路由躍點之外，而不是直接連線到Catalyst 6500/6000-MSFC2。在Catalyst 6500/6000-MSFC2上，CEF路由路徑使用相同的方法。



### 疑難排解步驟

請完成以下步驟：

1. 發出以下命令檢查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
```

從上面的輸出中您可以看到，要到達IP地址為192.168.150.3的主機2，您有一條開放最短路徑優先(OSPF)路由。需要使用VLAN 199中的IP地址192.168.199.3作為下一跳到達。

2. 通過發出以下命令檢查MSFC2上的ARP表。注意：檢查ARP條目中是否有下一跳，而不是最終目的地。

```
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. 發出以下命令檢查MSFC2上的CEF表和鄰接表：

```
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
```

您可以看到有目的地網路的CEF專案，且下一躍點結果會與路由表中步驟1中的結果相符。

### 4. 發出以下命令檢查下一跳的鄰接表：

```
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
```

下一跳有一個有效的鄰接關係，目的MAC地址與上面步驟2中的ARP條目匹配。

### 5. 發出以下命令檢查Supervisor Engine(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反映了在步驟3中找到的相同資訊，並且您具有相同的下一跳。

### 6. 發出以下命令檢查Supervisor Engine(PFC2)上的鄰接關係：

```
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
```

您還可以驗證您是否有連線鄰接關係，該鄰接關係反映了上述步驟2和4中相同的MAC地址。

**注意：**在檢查PFC2上的鄰接關係時，您可以檢查最終目標的鄰接關係。在MSFC2上的Cisco IOS軟體中無法進行此操作，您需要用它檢查下一跳的鄰接關係。最終目標的PFC2上的鄰接表在一個命令輸出中同時顯示下一跳和下一跳的鄰接關係（如果已解析）。在MSFC2上，您需要分別檢查CEF條目以查詢下一跳，然後查詢下一跳鄰接本身。

## 備註和結論

在此範例中，您可以看到用於驗證Catalyst 6500/6000-MSFC2上連線到遠端網路的疑難排解步驟與案例研究1一節中的上一個範例相似：[連線到直連網路中的主機](#)。不過，兩者存在一些差異：

- 您檢查IP路由表、CEF表和FIB中的最終目的地（步驟1、3和5）。
- 您檢查ARP表和鄰接表中的下一跳資訊（步驟2和4）。
- 在步驟6中，可以直接檢查最終目標的鄰接關係。結果既顯示FIB的下一跳，也顯示鄰接表中的鄰接重寫資訊。

在這種情況下，FIB中沒有用於最終目的地的條目，如下所示。（僅存在掩碼長度為24的網路條目。）

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

## 案例研究3:到下一跳的負載均衡



本案例研究討論了有多個下一跳和多個路由可以到達同一目的網路時發生的情況。

1. 在以下路由表的示例部分中，請注意，到達同一目的IP地址192.168.254.253有三種不同的路由和三種不同的下一跳。

```
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. 按照以下步驟檢查三個下一躍點中的ARP條目：檢查CEF表以查詢目標。請注意，目的地也在MSFC2上的CEF表中顯示三個不同的條目。Cisco IOS軟體CEF能夠在不同的路由之間實現負載共用。

```
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
```

檢查MSFC2鄰接表中的三個鄰接關係。它們應與上面步驟2中的ARP條目匹配。

3. 請注意，為同一目標安裝了三個不同的FIB條目。PFC2上的硬體CEF最多可以為同一目標載入六個不同路徑。您可以在權重欄位中看到用於每個下一跳的權重。PFC2使用的負載共用只是每個流的負載共用。它沒有啟用每個資料包的負載共用。

```
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. 發出以下命令檢查該目標條目的鄰接關係：

```
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
```

## 案例研究4:預設路由

無論路由表看起來如何，Supervisor Engine 2中總有一個FIB條目用於轉發與之前任何條目都不匹配的資料包。發出以下命令可檢視此條目：

```
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
```

如您所見，這是掩碼長度為0的唯一條目。此預設路由可以分為兩種型別，如下面的[MSFC2路由表中預設路由存在](#)和路由表中無預設路由[一節所述](#)。

## [MSFC2路由表中存在預設路由](#)

首先，確定如何驗證MSFC2路由表中是否存在預設路由。您可以查詢目的地為0.0.0.0的路由，或者在路由表中查詢。預設路由標有星號(\*)。(此處也以粗體顯示。)

```
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
```

在這種情況下，預設路由存在於MSFC2路由表中，並通過路由資訊協定(RIP)獲知。但是請注意，無論如何獲知此預設路由(靜態、OSPF、RIP等)，CEF行為都是相同的。

這種情況下，如果您有預設路由，則始終會有一個CEF條目，其掩碼長度為0，並且FIB-Type為，用於轉發所有不匹配任何其他字首的流量。

```
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
```

由於按順序瀏覽每個資料包的FIB(首先從最長匹配開始)，此預設FIB僅用於找不到其他匹配的資料包。

## [路由表中沒有預設路由](#)

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

如果路由表中沒有任何預設路由，則Supervisor Engine 2中仍存在掩碼長度為0的FIB條目。但是，此條目現在有一個FIB-Type萬用字元。此萬用字元FIB會丟棄命中它的所有資料包，並匹配與FIB中任何其他條目不匹配的任何資料包。丟棄這些資料包非常有用，因為您沒有任何預設路由。無需將這些封包轉送到MSFC2,MSFC2無論如何都會捨棄這些封包。使用此萬用字元FIB，可以確保丟棄硬體中的這些無用資料包。

```
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表已滿的極少數情況下，萬用字元條目仍然存在，但不會丟棄與其匹配的資料包，而是將其轉發到MSFC2。僅當在FIB中有超過256K的字首並且無法在FIB中儲存完整的路由表和ARP鄰接關係時，才會出現這種情況。然後，您需要將預設機制傳送到MSFC2，因為MSFC2可以具有不在FIB中的路由條目。

## [其他疑難排解提示和已知問題](#)

### [發出show mls cef mac命令](#)

Supervisor引擎2收到資料包時，如果資料包的目的MAC地址與其中一個MSFC2 MAC地址相同，它只會將其視為潛在的第3層資料包。發出以下命令可以驗證這些地址是否來自Supervisor Engine 2的視點：

```
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。(請記住，MSFC2上的所有介面使用相同的MAC地址；不能在兩個不同的介面上配置不同的MAC地址。)此MAC地址需要與MSFC2上的相同。

```
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命令也會顯示連結到熱待命路由器協定(HSRP)組(其中MSFC處於活動狀態)的所有MAC地址。上述show mls cef mac命令的輸出表示，對於VLAN 10和VLAN 100,MSFC處於HSRP-active狀態。您可以在MSFC2上發出以下命令來驗證此命令是否正確：

```
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  
Vl100 100 200 P Active local 192.168.100.2 192.168.100.254  
Vl101 101 100 P Standby 192.168.101.2 local 192.168.101.254
```

您可以看到，只有VLAN 10和VLAN 100處於Active狀態。所有已配置的HSRP組的狀態為Standby。無論出於何種原因，如果另一個VLAN的Active狀態開始，show mls cef mac命令的輸出應反映此附加VLAN處於非活動狀態。

如果show mls cef mac命令輸出與它應顯示的內容不一致，您可以發出此命令，此命令將提供有關在show mls cef mac命令清單中新增和刪除的MAC地址的詳細資訊：

```
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
```

每次在**show mls cef mac**命令表中新增或刪除MAC地址時，此命令都會提供一條消息。

## 影子TCAM

本文討論了如何檢查Supervisor Engine 2上的**show mls entry cef**命令表。此命令不能準確表示PFC2的實際應用專用積體電路(ASIC)程式設計。它只表示此ASIC設定的卷影副本。出現了一些已知問題，其中實際硬體設定與影子TCAM中顯示的內容不一致，這導致某些資料包被轉發到錯誤的下一跳。這些問題記錄在Cisco錯誤ID [CSCdv49956](#) (僅註冊客戶)和[CSCdu85211](#) (僅註冊客戶)中，[這兩個問題都在CatOS軟體版本6.3\(3\)、7.1\(1\)和更新版本中修正。](#)

## 預設路由已中斷

在早期版本的代碼中發現一個錯誤，其中向預設路由的轉發不適用於增強型內部網關路由協定(EIGRP)或OSPF。此問題已記錄在Cisco錯誤ID [CSCdt54036](#) (僅限註冊客戶)，並在CatOS軟體版本6.1(3)及更高版本 (適用於Supervisor Engine映像) 和Cisco IOS軟體版本12.1(6)E1 (適用於MSFC2映像) 中。

## 相關資訊

- [在具有MSFC的Catalyst 6000交換機上配置並排除IP MLS故障](#)
- [LAN 產品支援頁面](#)
- [LAN 交換支援頁面](#)
- [工具與公用程式](#)
- [技術支援 - Cisco Systems](#)