

# ハイブリッドモードの Supervisor 2 を搭載する Catalyst 6000 スイッチでのユニキャスト IP ルーティング CEF のトラブルシューティング

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[CEFとは](#)

[転送情報ベース\(FIB\)](#)

[隣接テーブル](#)

[PFC 2のFIBおよび隣接テーブルの読み方](#)

[トラブルシューティングの方法](#)

[ケーススタディ 1:直接接続ネットワークのホストへの接続](#)

[トラブルシューティングの手順](#)

[考慮事項および結論](#)

[ケーススタディ 2:リモート ネットワークへの接続](#)

[トラブルシューティングの手順](#)

[考慮事項および結論](#)

[ケーススタディ 3:複数のネクスト ホップへの負荷分散](#)

[ケーススタディ 4:デフォルト ルーティング](#)

[MSFC 2 ルーティング テーブルにデフォルト ルートがある場合](#)

[ルーティング テーブルにデフォルト ルートがない場合](#)

[その他のトラブルシューティングのためのヒントおよび既知の問題](#)

[sh mls cef Mac コマンド](#)

[シャドウTCAM](#)

[デフォルト ルーティングの問題](#)

[関連情報](#)

## 概要

この資料は、Supervisor 2 (Sup 2) / Policy Feature Card 2 (PFC 2) / Multilayer Switch Feature Card 2 (MSFC 2)搭載のCatalyst 6000 スイッチ上でのユニキャストIPルーティングのトラブルシューティングガイドです。Sup 2のユニキャストルーティングは、Cisco Express Forwarding (CEF)を使用して実行されます。このドキュメントは、Supervisor Engine 2、PFC2、MSFC2を搭載したCatalyst 6500/6000シリーズでのIPルーティングにのみ関するものです。このドキュメントは、Supervisor Engine 1 (または1A) 搭載のCatalyst 6500/6000では0できません。また、ハイブリッドソフトウェアだけを対象にしているため、IOSモードを実行しているCatalyst 6000ファ

ミラー スイッチは対象外です。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

### 表記法

ドキュメント表記の詳細は、「[シスコ テクニカル ティップスの表記法](#)」を参照してください。

## CEFとは

CEF は、パケット ルーティングをより高速化するために設計された Cisco IOS ソフトウェア スイッチング テクノロジーです。CEF はファスト スイッチングに比べ、はるかにスケーラブルです。( プロセス スイッチングに最初のパケットを送信する必要はありません )。 Supervisor Engine 2を搭載したCatalyst 6500では、PFC 2に実装されたハードウェアベースのCEF転送メカニズムが使用されます。CEFでは、ルーティングに必要な情報を保存するために、主に2つのテーブルが使用されます。Forwarding Information Database ( FIB ) および隣接テーブル

### 転送情報ベース(FIB)

CEFは、FIBを使用してIP宛先のプレフィクスに基づくスイッチングを判断します ( 最長マッチを最優先 )。 FIB は概念的には、ルーティング テーブルや情報ベースに類似します。FIB は、IP ルーティング テーブルに含まれるフォワーディング情報のミラー イメージを維持します。ネットワークでルーティングまたはトポロジの変更が行われると、IP ルーティング テーブルが更新され、それらの変更が FIB に反映されます。FIBは、IPルーティング テーブルの情報に基づいて、ネクスト ホップのアドレス情報を保守します。FIBのエントリとルーティング テーブルのエントリは1対1で関連付けられているので、FIBにはすべての既知ルートが含まれています。したがって、ファスト スイッチングや最適スイッチングのように、スイッチング パスに関するルート キャッシュを保持する必要がありません。デフォルトであっても、ワイルドカードであっても、常に FIBに一致しています。

### 隣接テーブル

リンク層上でネットワーク内のノードが 1 ホップで相互に到達可能な場合、これらのノードは隣接関係にあると見なされます。CEFは、FIBのほかに、隣接テーブルを使用してレイヤ2 ( L2 ) アドレス情報を保持します。隣接テーブルには、すべてのFIBエントリのL2ネクスト ホップ アドレスが含まれています。つまり、完全なFIBエントリには隣接テーブル内にある、最終の宛先に到達するためのネクストホップL2情報の位置を示すポインタが含まれています。Catalyst 6500/Sup 2システムでハードウェアCEFを正常に動作させるには、MSFC 2上で IP CEF を実行する必要があります。

## PFC 2のFIBおよび隣接テーブルの読み方

PFC2のFIBテーブルは、MSFC2のFIBテーブルとまったく同じでなければなりません。PFC2では、FIBのすべてのIPプレフィックスはTernary Content Addressable Memory(TCAM)に格納され、マスク長で最長のマスクからソートされます。つまり、最初にマスク長 32 ( ホスト エントリ ) の全エントリ、次に、マスク長が31のエントリをすべて検索し、マスク長が0のエントリに到達します。これがデフォルトのエントリです。FIBは順次読み込まれるので、最初に一致したエントリが使用されます。次に、PFC 2のFIBテーブルの例を示します。

```
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.
各エントリには、次のフィールドがあります。
```

- Mod : エントリをインストールするMSFC2は、代表MSFC2に応じて15または16です。
- FIB-Type - 次の FIB-Type があります。receive - MSFC MSFCインターフェイスのIPアドレスおよびブロードキャスト サブネットのIPアドレスに対応するマスク長が32のプレフィックスです。resolved - 隣接関係が確認されたネクスト ホップのプレフィックスです。connected - wildcard - MSFC デフォルトのエントリが存在しない場合にのみ挿入される、マスク長が0のエントリです。default - wildcardエントリと同様に、すべてのサブネットが対象で、マスク長は0です。このエントリはネクスト ホップを宛先とします。デフォルトのCEFエントリが挿入されるのは、ルーティング テーブルにデフォルト ルートが設定されている場合だけです。
  - drop - drop
- Destination-IP - IP IP
- Destination-Mask - FIBのエントリは、最大マスク長 (255.255.255.255)から開始され、最小マスク長 (0.0.0.0)で終了します。
- Next-Hop IP - IP

完全な隣接テーブルを表示するには、次のコマンドを入力します。

```
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 : この出力には、FIBの解決済み ( またはデフォルト ) CEFエントリごとに、上記のサンプル

FIBテーブルに見つかったエントリに似たエントリが含まれています。

## トラブルシューティングの方法

トラブルシューティングの具体的な例および詳細を示す前に、ここでは特定のIPアドレスへの接続性または到達性のトラブルシューティングについて、簡単に説明します。PFC2のCEFテーブルは、MSFC 2のCEFテーブルをミラーリングしています。したがって、PFC2は、MSFC2で認識されている情報も正しい場合に、IPアドレスに到達するための正しい情報だけを保持します。したがって、常に、次の情報を確認する必要があります。

### MSFC2 を使用する場合：

次のステップを実行します。

1. `sh ip route` コマンド (または、ルーティング テーブルを部分的に検索する場合は `sh ip route x.x.x.x` コマンド) を入力し、正確なネクスト ホップが出力に含まれているか確認します。正確な情報が表示されない場合には、ルーティング プロトコル、コンフィギュレーション、ルーティング プロトコル ネイバを確認し、実行中のルーティング プロトコルに関するトラブルシューティングを行う必要があります。
2. `show ip arp next_hop_ip_address` コマンドを発行し、ARPが解決され、正しいMACアドレスが含まれていることを確認して、ネクストホップ (または接続されたネットワークの最終宛先) がMSFC2上で正しく解決されていることを確認します。MACアドレスが不正な場合には、他のデバイスがそのIPアドレスを所有しているかどうかを確認する必要があります。最終的には、そのMACアドレスを所有するデバイスの接続ポート上で、スイッチ レベルを確認します。ARPエントリが不完全な場合は、ホストから応答を得られなかったことを意味しています。ホストが起動し、アクティブかどうか確認する必要があります。必要ならばスニファを使用して、ARP応答が得られるかどうか、ホストが正しく応答するかどうかを確認します。
3. 次の手順で、MSFC 2のCEFテーブルに正しい情報が含まれていて、隣接関係が解決されていることを確認します。 `sh ip cef destination_network` コマンドを入力し、CEFテーブルでのネクスト ホップが、IPルーティング テーブルでのネクスト ホップ (手順 1 を参照) と一致しているか確認します。 `show adjacency detail | begin next_hop_ip_address` コマンドを発行します。手順 2 で確認したARPのMACアドレスが含まれている必要があります。

上記のステップ1と2で正しい結果が得られますが、ステップ3aまたは3bで障害が発生している場合は、Catalyst 6500/6000に関連していない可能性があるCisco IOSソフトウェアCEFの問題が発生しています。

### PFC 2での確認

次のステップを実行します。

1. `show mls entry cef ip destination_ip_network/destination_subnet_mask` コマンドを発行し、`show mls entry cef ip destination_ip_network/destination_subnet_mask` コマンドを発行して、PFC2に格納されているFIB情報が正しいこと、およびMSFC2のCEFテーブルに格納されている情報が一致していることを確認します。表示された情報が、手順 3 の結果と一致していない場合には、MSFC 2とPFC 2間の通信に問題があります (Catalyst 6000内部の問題)。実行中のPFC 2のCatOSまたはMSFC 2のIOSに既知の不具合がないかどうか調べてください。正しいエントリを復元するには、MSFC 2で `clear ip route` コマンドを実行しま

す。

2. `show mls entry cef ip next_hop_ip_address/32 adjacency` コマンドを入力し、上記の「[MSFC 2 を使用する場合](#)」セクションの手順 2 と 3b で確認したのと同じ MAC アドレスが含まれていることを確認して、PFC 2 の隣接関係テーブルを確認します。PFC2の隣接関係がステップ3bのネクストホップの隣接関係と一致しない場合、MSFC2とPFC2の間の内部通信の問題が発生している可能性があります。隣接関係をクリアすると、正しい情報が復元されます。

## ケーススタディ 1:直接接続ネットワークのホストへの接続

ここでは、次のホスト間の接続について検証します。

- VLAN 10に存在するIPアドレス 192.168.10.10 のホスト 1
- VLAN 199に存在するIPアドレス 192.168.199.3 のホスト 2

次に、MSFC 2の設定例を示します。

```
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：Supervisor Engine 2およびMSFC2を搭載したCatalyst 6500/6000は、ハードウェアでCEFを使用してルーティングを行っています。MSFC 2でCEFをディセーブルにすることはできません。トラブルシューティングの手順

### トラブルシューティングの手順

IP アドレス 192.168.199.3 に到達するパスを確認するには、このドキュメントの「[トラブルシューティングの方法](#)」の項で示されている手順に従ってください。

1. 次のいずれかのコマンドを入力して、IPルーティング テーブルを確認します。

```
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
```

または

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

これらのコマンドの出力から、宛先が、直接接続されたサブネット上にあることがわかります。つまり、宛先に到達するためのネクスト ホップは存在しません。

2. MSFC 2のARPエントリを確認します。次のコマンドを入力して、宛先IPアドレスに対応するARPエントリがあることを確認します。

```
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. MSFC 2のCEFテーブルおよび隣接テーブルを確認します。次のコマンドを入力して、CEFテーブルを確認します。

```
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
```

マスク長 32の有効なCEFエントリと、有効な隣接キャッシュが存在することがわかります。次のコマンドを入力して、隣接テーブルを確認します。

```
Cat6k-MSFC2# show adjacency detail | begin 192.168.199.3
IP VLAN 199192.168.199.3(7)
0 packets, 0 bytes
003071506800
!--- This is the destination MAC address. 00D0003F8BFC0800 ARP00:58:35
```

出力から、隣接関係が存在することがわかります。隣接関係の宛先 MAC アドレスには、上記の手順 2 の ARP テーブル内の MAC アドレスと同じ情報が表示されています。パケットはハードウェアのレイヤ 3 (L3) で切り替えられるので、手順 3b のカウンタはほとんどの場合 0 になることに注意してください。パケットはMSFC 2には到達しないので、MSFC 2のCEFカウンタの対象にはなりません。手順 5 の PFC 2 で見つかる隣接関係の統計を調べることによってのみ、特定の宛先に転送されるパケットの統計情報を確認できます。

4. スーパーバイザ上でCEF/FIBエントリが正しいかどうかを確認します。次に示すように、FIBには2つの関連エントリがあります。宛先IPアドレスのエントリ

```
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
```

ネクスト ホップ (この場合は宛先) がわかっているホスト エントリです。宛先ネットワークに対応するエントリ

```
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
```

接続先のFIBエントリです。このエントリにヒットするパケットはすべて、次の処理のためにMSFC 2に転送されます (主として、ARPを送信し、ARP解決を待機します)。FIBエントリは、最大マスク長のものから順番に検索されます。したがって、上記の両エントリが存在する場合には、マスク長32 (ホスト エントリ) が最初にヒットするので、次には進みません。/32 2 これは接続先エントリなので、パケットは MSFC 2 にリダイレクトされて処理されます。たとえば、MSFC 2から宛先マスクのARP要求が送信されます。ARP応答を受信すると、MSFC 2のARPテーブルと隣接テーブルに、そのホストの情報が保管されます。

5. マスク長32の正しいFIBエントリが作成されたら、次のコマンドを入力して、そのホストについて隣接関係が正しくポピュレートされているか確認する必要があります。

```
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：隣接関係が設定され、[NextHop-Mac]にはホスト2の有効なMACアドレスが含まれます (手順2と3bを参照)。この時点では、この隣接関係に対して送信されたパケットの数はまだ0ですが、すべての出力は正しいです。次の例では、100バイトのpingをホスト1からホスト2に送信し、もう一度隣接関係を確認します。**

```
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

TX-Packets の値が10になります。これは、送信したトラフィック数と一致しています。

## 考慮事項および結論

前述したように、一致するFIBエントリは2つあります。

- ネットワークエントリ(この場合は192.168.199.0/24) : このエントリは常に存在し、MSFCのルーティングおよびCEFテーブルから直接送信されます。ルーティング テーブル内の直接接続ネットワークです。
- destination host entry(この例では192.168.199.3/32) : このエントリは必ずしも存在しません。存在しない場合にはネットワーク エントリがヒットし、次の処理が行われます。パケットがMSFC 2に転送されます。PFCのFIBテーブルにマスク長32のホスト エントリが作成されます。ただし、完全な隣接関係はありません。隣接関係は、frc drop (force drop [強制廃棄]) タイプとして作成されます。宛先への以降のパケットが/32 frc drop エントリにヒットし、廃棄されます。同時に、MSFC 2に転送された最初のパケットにより、MSFC 2からARP要求が送信されます。ARPが解決されると、ARPエントリが完成します。MSFC 2で完全な隣接関係が作成され、スーパーバイザに更新情報が送信されます。既存のfrc drop 隣接関係は終了します。スーパーバイザにより、ホストの隣接関係が新しいMACアドレスに変更されます。隣接関係がconnectに変わります。ARPが解決されるまでの待機中にFRCドロップの隣接関係を設定するメカニズムは、ARPスロットルと呼ばれます。これにより、すべてのパケットがMSFC 2に転送され、複数のARP要求が送信されるのを防ぐことができます。MSFC 2に送信されるのは最初のいくつかのパケットだけで、以降のパケットは、隣接関係が完了するまで、PFC 2上で廃棄されます。また、この動作によって、直接接続ネットワーク内に存在しないホストまたは非応答ホストに宛てられたトラフィックを廃棄することもできます。

異なるVLANに属す2ユーザ間の接続のトラブルシューティングを行うには、常に、次の事項を確認する必要があります。

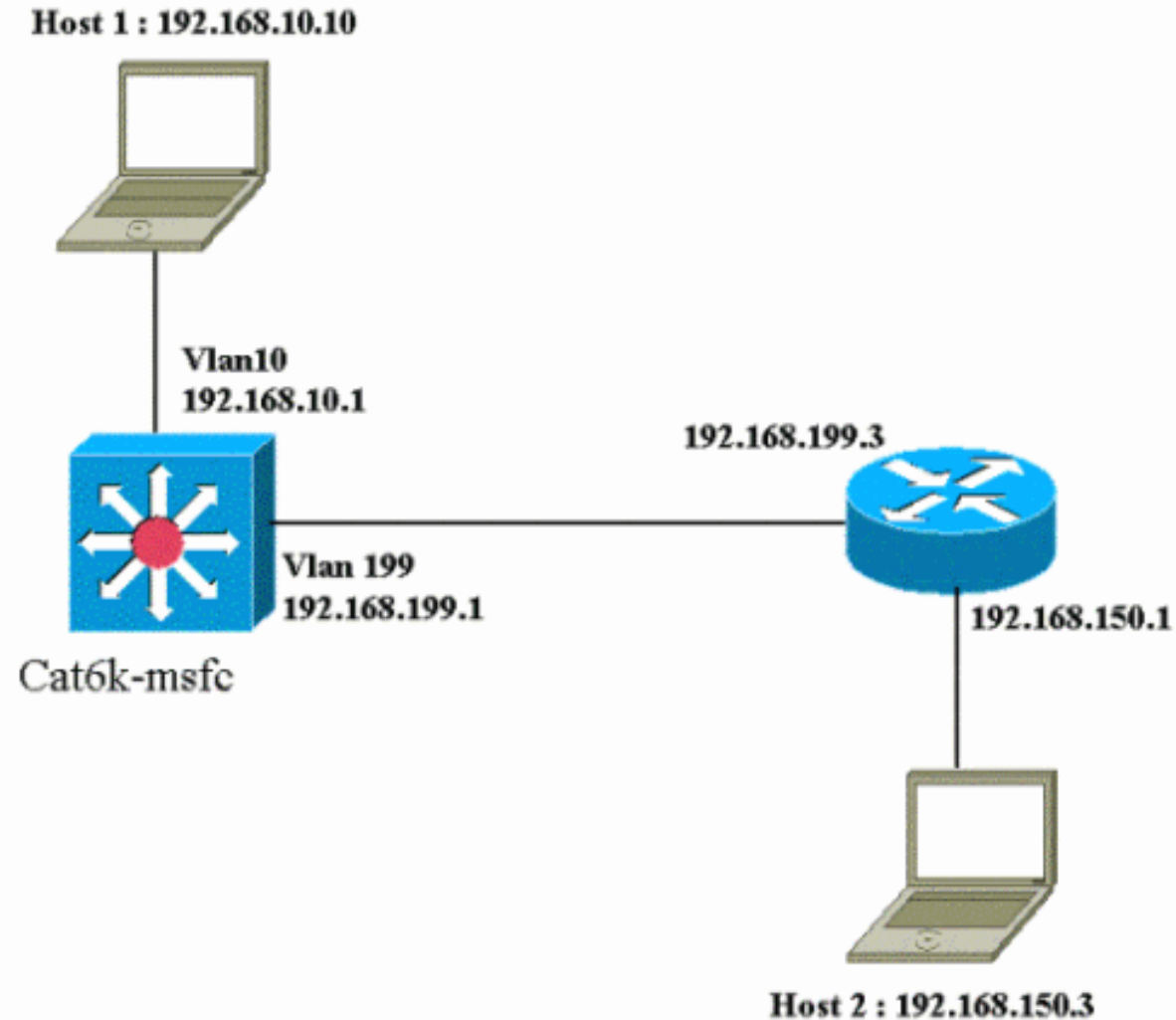
- ホスト1からホスト2へのトラフィックについては、宛先 IPアドレスをホスト2にし、前述した手順を実行します。
- ホスト2からホスト1へのトラフィックについては、同じ手順で宛先 IPアドレスをホスト1にします。

送信元のデフォルト ゲートウェイ上で出力を生成することも重要です。ホスト1からホスト2へのデフォルトゲートウェイと、ホスト2からホスト1へのデフォルトゲートウェイ双方が同じである必要はありません。

注 : 上記のトラブルシューティング手順のステップ3bのカウンタ<sup>2</sup>は、パケットがハードウェアでL3スイッチングされるため、ほぼ常に0です。パケットはMSFC 2には到達しないので、MSFC 2のCEFカウンタの対象にはなりません。上記の「[トラブルシューティングの手順](#)」の手順5のPFC 2で見つかる隣接関係の統計を調べることによってのみ、特定の宛先に転送されるパケットの統計情報を確認できます。

## ケーススタディ 2: リモート ネットワークへの接続

IPアドレス192.168.10.10のホスト1が、IPアドレス192.168.150.3のホスト2に対してpingを実行する次の図を考えてみましょう。ただし、今回は、Catalyst 6500/6000-MSFC2に直接接続する代わりに、2ホップ離れた場所にあります000-MSFC2



## トラブルシューティングの手順

次のステップを実行します。

1. 次のコマンドを入力して、MSFC 2のルーティング テーブルを確認します。

```
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
```

出力から、IPアドレス 192.168.150.3 のホスト2に到達するために、Open Shortest Path First (OSPF)ルートを使用することがわかります。ネクスト ホップとしてVLAN 199のIPアドレス 192.168.199.3 を使用する必要があります。

2. 次のコマンドを入力して、MSFC 2 の ARP テーブルを確認します。注：最終宛先ではなく、ネクストホップのARPエントリを確認します。

```
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. a. 次のコマンドを入力して、MSFC 2のCEFテーブルおよび隣接テーブルを確認します。

```
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
```

宛先ネットワークに CEF エントリがあることがわかります。ネクスト ホップの結果は、ルーティング テーブルの手順 1 の結果と一致します。

4. b. 次のコマンドを入力して、ネクスト ホップの隣接テーブルを確認します。

```
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
```

ネクスト ホップの有効な隣接関係が存在し、宛先の MAC アドレスは上記の手順 2 の ARP エントリと一致します。

5. 次のコマンドを入力して、スーパーバイザ (PFC 2) の FIB テーブルを確認します。

```
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 には手順 3 で確認したのと同じ情報が反映され、同じネクスト ホップがあります。

6. 次のコマンドを入力して、スーパーバイザ (PFC 2) の隣接関係を確認します。

```
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
```

上記の手順 2 および 4 と同じ MAC アドレスを反映する接続の隣接関係があることも確認できます。

注：PFC 2 の隣接関係をチェックする場合、最終宛先の隣接関係をチェックできます。MSFC 2 の Cisco IOS ソフトウェアでは、ネクストホップの隣接関係をチェックする必要がある場合は、これは不可能です。PFC 2 では、1 つのコマンドで出力される最終宛先の隣接テーブルに、ネクストホップとネクストホップの隣接関係 ( 解決されている場合 ) の両方が表示されます。MSFC 2 では、まずネクストホップの CEF エントリを確認してから、別途、ネクストホップの隣接関係を見る必要があります。

## [考慮事項および結論](#)

この例からわかるように、Catalyst 6000 MSFC 2 からリモート ネットワークへの接続を確認するためのトラブルシューティング手順は、セクション「[ケーススタディ 1 :](#)」にある例とほとんど同じです。[直接接続ネットワークのホストへの接続](#)」の項にあります。以下に、相違点をまとめます。

- IP ルーティング テーブル、CEF テーブル、FIB の最終的な宛先を確認します ( 手順 1、3、および 5 )。
- ARP テーブルおよび隣接テーブルでネクスト ホップ情報を確認します ( 手順 2 および 手順 3b )。
- 手順 5 では最終宛先の隣接関係を直接確認できます。FIB のネクスト ホップ情報と、隣接テーブルの隣接関係更新情報の両方が表示されます。

次に示すように、この例では、FIB に最終宛先のエントリはありません。( マスク長 24 のネットワーク エントリだけです )

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

## ケーススタディ 3:複数のネクスト ホップへの負荷分散

ここでは、同じ宛先ネットワークに到達する方法として、複数のネクスト ホップと複数のルートが存在するケースについて説明します。

1. 次のルーティング テーブルの例を見ると、宛先IPアドレス 192.168.254.253 への到達方法として、3つの異なるルートと3つの異なるネクスト ホップが存在することがわかります。

```
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. 次の手順で、3つのネクスト ホップについて、それぞれARPエントリを確認します。宛先のCEFテーブルを確認します。宛先には、MSFC 2のCEFテーブルの3つの異なるエントリも表示されています。Cisco IOSソフトウェアCEFでは、異なるルート間でロードシェアリングを行うことができます。

```
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
```

MSFC 2の隣接テーブルで、3つの隣接関係を確認します。これらは、上記の手順 2 の ARP エントリと一致する必要があります。

3. 同じ宛先について、3つの異なるFIBエントリが挿入されています。PFC 2のハードウェア CEFは、1つの宛先について最大6つの異なるルートに負荷を分散させることができます。各ネクスト ホップのウェイトは、Weightフィールドで確認できます。PFC 2がサポートしているのはフロー単位の負荷分散だけです。パケット単位の負荷分散はサポートされません。

```
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. 次のコマンドを入力して、宛先エントリの隣接関係を確認します。

```
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
```

## ケーススタディ 4 :デフォルト ルーティング

ルーティング テーブルの内容によらず、Sup 2には、他のどのエントリとも一致しないパケットを転送するためのFIBエントリが必ず存在します。このエントリは、次のコマンドで確認できます。

```
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
```

マスク長が0の唯一のエントリです。このデフォルトは、次のセクションで説明されているように、MSFC2のルーティングテーブルにデフォルトルートが存在し、ルーティングテーブルにデフォルトルートが存在しない2種類です。

### MSFC 2 ルーティング テーブルにデフォルト ルートがある場合

最初に、MSFC 2のルーティング テーブルにデフォルト ルートが存在するかどうかを確認します。宛先0.0.0.0のルートを表示するか、またはルーティング テーブル全体を確認します。デフォルトルートにはアスタリスク(\*)が付いています (ここでは、太字でも表示されます)。

```
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
```

この例では、MSFC 2ルーティング テーブルにデフォルト ルートが存在します。このルートはRouting Information Protocol (RIP)経由で学習されたものです。ただし、デフォルト ルートが何によって得られたか (スタティック、OSPF、RIPなど) に関係なく、CEFの動作は同じです。

この場合にはデフォルト ルートが存在するので、マスク長 0でFIB-TypeがdefaultであるCEFエントリが必ず存在し、他のどのプレフィクスとも一致しないすべてのトラフィックの転送に使用されます。

```
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
```

各パケットは、最大長のFIBから順番に照合されます。したがってデフォルトのFIBは、他のどのエントリとも一致しなかったパケットに対してのみ適用されます。

## ルーティング テーブルにデフォルト ルートがない場合

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

ルーティング テーブルにデフォルト ルートが設定されていなくても、Sup 2にはマスク長0の FIBエントリが存在します。ただし、このエントリのFIB-Typeは wildcard です。ワイルドカードのFIB-Typeは、ヒットしたすべてのパケット、すなわち、FIBの他のどのエントリとも一致しないすべてのパケットを廃棄します。デフォルト ルートが存在しない場合、これらのパケットは廃棄したほうが便利です。いずれにしても廃棄されるので、これらのパケットをMSFC 2に転送する必要はないからです。ワイルドカードFIBを使用することによって、ハードウェアで不要なパケットを確実に廃棄することができます。

```
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：まれには、FIBテーブルが満杯の場合、ワイルドカードエントリは存在しますが、一致するパケットをドロップする代わりにMSFC2に転送されます。これは、FIBに256Kのプレフィクスを超える場合に限られます。このような状況では、デフォルトでパケットをMSFC 2に転送する必要があります。MSFC 2に、FIBに保管できなかったルーティング エントリが設定されているからです。

## その他のトラブルシューティングのためのヒントおよび既知の問題

### sh mls cef Mac コマンド

Sup 2は、受信したパケットの宛先MACアドレスがMSFC 2 MACアドレスの1つと一致している場合に限り、潜在的にL3パケットであるとみなします。Sup 2が認識するアドレスは、次のコマンドによって確認できます。

```
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
```

MSFC2の物理MACアドレスが表示されます(MSFC2上のすべてのインターフェイスが同じMACアドレスを使用することに注意してください。異なるインターフェイスに異なる MAC アドレスを設定することはできません)。このMACアドレスは、MSFC 2上のアドレスと一致している必要があります。

```
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 コマンドでは、MSFC がアクティブである Hot Standby Router Protocol ( HSRP ) グループにリンクしている MAC アドレスも、すべて表示されます。上記の

show mls cef macコマンドの出力は、MSFCがVLAN 10およびVLAN 100に対してHSRPアクティブであることを示しています。これは、MSFC2で次のコマンドを発行することで正しいことを確認できます。

```
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
```

Activeに設定されているのは、VLAN 10 とVLAN 100だけです。他の設定済みHSRPグループはすべてStanbyです。何らかの理由で別のVLANをアクティブに変更した場合、sh mls cef Mac コマンドにそのVLANがアクティブであることが反映されないことがあります。

sh mls cef Macコマンドの出力と実際の設定が異なる場合には、次のコマンドを入力すると、sh mls cef Mac コマンド リストに追加された、またはリストから削除されたMACアドレスの詳細情報が表示されます。

```
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
```

このコマンドでは、sh mls cef Mac コマンドのテーブルでMACアドレスを追加/削除するごとにメッセージが表示されます。

## シャドウTCAM

このドキュメントでは、show mls entry cefコマンドテーブルをスーパーバイザエンジン2でチェックする方法について説明しました。このコマンドは、PFC2の実際の特用途向け集積回路(ASIC)プログラミングを正確に表していません。このASIC設定のシャドウコピーのみを表します。実際のハードウェア設定がシャドウTCAMの表示内容に反映されていない場合、一部の packets が不正なネクスト ホップに転送されることがあります。これらの問題は、Cisco Bug ID [CSCdv49956](#) (登録ユーザ専用) および [CSCdu85211](#) (登録ユーザ専用) に記載されています。これらの問題は、CatOSソフトウェアバージョン6.3(3)、7.1)で1で66331(1)、およびそれ以降。

## [デフォルト ルーティングの問題](#)

旧バージョンのソフトウェアで、Enhanced Interior Gateway Routing Protocol (EIGRP) または OSPFで、デフォルト ルートへの転送が正常に動作しないという問題が見つっています。この問題は、Cisco Bug ID [CSCdt54036](#) (登録ユーザ専用) に記載されて、スーパーバイザエンジン イメージのCatOSソフトウェアバージョン6.1(3)以降、およびMSFC2イメージのCisco IOSソフトウェアリリース12.1(6)E1で) ..

## [関連情報](#)

- [MSFC を使用する Catalyst 6000 スイッチの IP MLS の設定とトラブルシューティング](#)
- [LAN 製品に関するサポート ページ](#)
- [LAN スイッチングに関するサポート ページ](#)
- [ツールおよびユーティリティ](#)
- [テクニカルサポート - Cisco Systems](#)