

# 目次

[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](#)

[MSFC2 ルーティング テーブルで存在 する デフォルト ルート](#)

[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。ここでは、Sup 2、PFC 2、およびMSFC 2を搭載しているCatalyst 6000ファミリー スイッチのIPルーティングだけを取り上げています。Supervisor 1 (Sup 1) またはMultilayer Switch Module (MSM)搭載スイッチの情報は含まれていません。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ファミリー 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関する固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IOS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、はるかに効率的です。(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がありません。) Sup 2搭載Catalyst 6500は、PFC 2上で実現されるハードウェアベースのCEF転送メカニズムを採用しています。CEFでは、ルーティングに必要な情報を2つの主要テーブルに保管しています。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ー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

ネットワーク内の2つのノードが、リンクレイヤ上の1ホップで相互に到達できる場合、これらを隣接ノードと呼びます。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

PFC 2のFIBテーブルは、MSFC 2のFIBテーブルと完全に一致した内容になります。PFC 2では、FIBのすべてのIPプレフィクスはTernary Content Addressable Memory (TCAM)に保管され、マスク長によって最大マスク長から順番にソートされます。これは最初に32のマスクのすべてのエントリを検出することを意味します(ホストエントリ);0のマスク長さのエントリに達する

まで、次に、31のマスク長さのすべてのエントリを、等検出します。これはデフォルト 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 cefMod FIB-Type Destination-IP Destination-Mask NextHop-IP
Weight --- -----
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 0 !--- This is the entry with mask length 8.15 wildcard
0.0.0.0          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** か。エントリをインストールする MSFC2 は依存が指定 MSFC2 の 16 です、または 15。
- **FIB** か。この特殊標目記入と関連付けられる型。次の FIB-Type があります。か。MSFC インターフェイスと関連付けられるプレフィクス。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 のプレフィクスです。か。有効なネクストホップ アドレスと関連付けられるプレフィクス。隣接関係が確認されたネクスト ホップのプレフィクスです。か。接続ネットワークと関連付けられるプレフィクス。か。これはすべてのエントリと一致します (ドロップするか MSFC リダイレクト)。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。か。デフォルト ルート。ワイルドカード エントリとして、それはすべてのサブネットと一致し、0 のマスク 長さ とあります。それはネクスト ホップを指します。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。か。ドロップするにエントリをマッチさせるすべてのパケットは廃棄されます。
- **IP** か。かかわっている宛先 IP アドレスか IP サブネット。
- **か**。エントリと関連付けられるマスク。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。
- **IP** か。ネクスト ホップ IP を、存在 する だけ 表示 する。

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 adjacencyMod: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 FIB テーブルの resolved ( または default ) の各 CEF エントリについて、上記のような出力が表示されます。

## 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。PFC 2 の CEF テーブル

ルは、MSFC 2のCEFテーブルをミラーリングしたものであることに注意してください。すなわち、MSFC 2の情報が正確であれば、PFC 2に含まれているIPアドレスへの到達情報も正確だということです。したがって、常に、次の情報を確認する必要があります。

## MSFC2 から:

次の手順を実行します。

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. 次の手順で、ネクスト ホップ (または接続先ネットワークの最終宛先) について、MSFC 2に解決済みの正確なAddress Resolution Protocol (ARP)エントリが含まれているか確認します。`sh ip arp next_hop_ip_address` コマンドを入力して、ARPが解決され、正しいMAC (メディア アクセス制御)アドレスが得られているか確認します。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。隣接関係が `show adjacency` 詳細のことを発行によって正しいことを確認して下さい | `begin next_hop_ip_address` コマンド。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。

ステップ 1 および 2 が、上で、正しい結果を提供するが、ステップ 3a か 3b が失敗すれば、Catalyst 6500/6000 に本当らしい関係していない Cisco IOSソフトウェア CEF 問題に直面しています。ARP テーブルと IP ルーティング テーブルをクリアする必要があります。

## PFC 2での確認

次の手順を実行します。

1. 次の手順で、PFC 2のFIB情報が、MSFC 2のCEFテーブルの情報 (手順 3を参照) と一致しているかどうかを確認します。`show mls entry cef ip destination_ip_network/destination_subnet_mask` コマンドを入力し、ネクスト ホップのIPアドレスが正しいことを確認します。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 エントリ cef IP next_hop_ip_address/32 隣接関係` コマンドを発行すること、そして、[MSFC2 セクションからの](#)のステップ 2 および 3b で見られるものと同じ MAC アドレスが含まれていることの上で検証によって PFC2 の隣接テーブルを確認して下さい。PFC 2の隣接情報が、手順 3b で確認した隣接情報と異なる場合には、MSFC 2とPFC 2間の内部通信

に問題があります。隣接情報をクリアし、正しい情報を復元してください。

## 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。

```
Cat6k> (enable) show mls entry cef adjacencyMod: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Supervisor Engine 2 および MSFC2 の Catalyst 6500/6000 がハードウェアの CEF を使用してルーティングしていることに注意することは重要です。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

パスを IP アドレス 192.168.199.3 に達するために確認するようにこの資料の[トラブルシューティングの方法](#) セクションで強調表示される手順に従って下さい。

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 InterfaceInternet 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 192.168.199.30 packets, 0 bytesvia 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 bytes003071506800 *!--- 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 アドレスはステップ 2 の ARPテーブルで MAC アドレスと同じ情報を、上で示しています。パケットがハードウェアで切り替えられるレイヤ3 (L3) であるのでステップ 3b のカウンターがほとんど常に 0 であることに注目して下さい。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。所定のデスティネーションに転送されるパケットの統計情報を見る唯一の方法はステップ 5.の間に PFC2 で見つけられる隣接関係の統計情報を検知 することです。
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 -----
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 エントリがないケースでは、ネットワークのためのエントリである第2エントリを見つけます、;それが接続されたエントリであるので、これからのプロセスのためのMSFC2にパケットをリダイレクトします。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 注隣接関係は読み込まれ、NextHop<sub>Mac</sub> フィールドはホスト2の有効なMACアドレスが含まれています (ステップ2および3bに見られるように)。この時点で、すべての出力はこの隣接関係のための伝送パケットの数がまだ0であるが、正しいです。次に、ホスト1からホスト2に100バイトのpingを10回送信し、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 1000TX-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、192.168.199.0/24)? This エントリは常にあり、MSFC のルーティングおよびCEF表から直接来ています。ルーティングテーブル内の直接接続ネットワークです。
- 宛先ホスト エントリ (この場合、192.168.199.3/32)? This エントリは必ずしもありません。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スロツトルと呼ばれます。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。

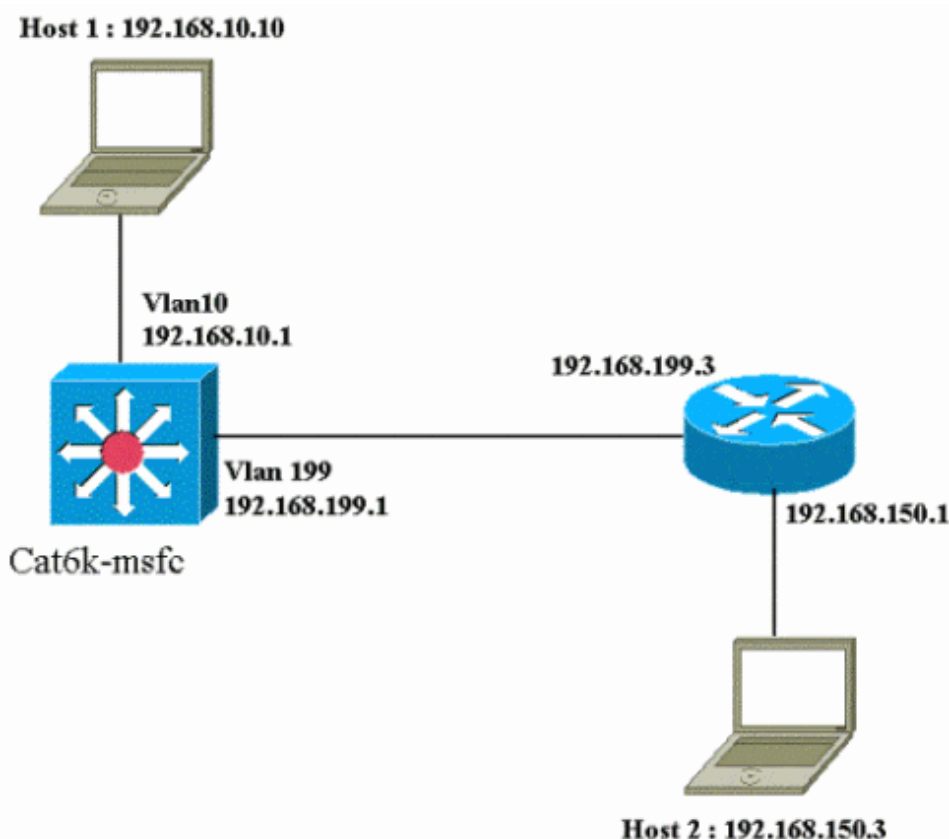
- [ホスト1からホスト2へのトラフィックについては、宛先 IPアドレスをホスト2にし、前述した手順を実行します。](#)
- ホスト2からホスト1へのトラフィックについては、同じ手順で宛先 IPアドレスをホスト1にします。

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[トラブルシューティング の手順](#)のステップ 3b のカウンターは、上で、パケットがハードウェアでレイヤ 3 (L3) スイッチドであるのでほとんど常に 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。所定のデスティネーションに転送されるパケットの統計情報を見る唯一の方法は上で[トラブルシューティング の手順](#)のステップ 5 の間に PFC2 で見つけられる隣接関係の統計情報を検知 することです。

## [ケーススタディ 2： リモート ネットワークへの接続](#)

次の図を参照してください。IPアドレス 192.168.10.10 のホスト1から、IPアドレス 192.168.150.3 のホスト2にpingを送信します。ただし、このホスト2は、Catalyst 6000 MSFC 2に直接接続しているネットワーク上ではなく、2ホップ先の位置にあります。ケーススタディ 1と同じ方法を使用して、Catalyst 6000 MSFC 2上のルーティング パスを確認します。



## トラブルシューティングの手順

次の手順を実行します。

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 192.168.150.0/24Known via "ospf 222", distance 110, metric 2, type intra areaLast 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. 下記のコマンドの発行によって MSFC2 の ARPテーブルをチェックして下さい。注最終宛先ではなくネクスト ホップのARPエントリをチェックする必要があります。Cat6k-MSFC2#  

```
show ip arp 192.168.199.3
```

Protocol Address Age (min) Hardware Addr Type  
InterfaceInternet 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  
ルーティング テーブルからのステップ 1である何が宛先ネットワークのための CEFエントリがある、ネクスト ホップは一致生じますことがわかり。
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 ホップのための有効な隣接があり、宛先 MAC アドレスはステップ 2 で検出される ARPエントリと上で一致します。
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 はステップ 3 で見つけれられる同じ情報を示し同じネクスト ホップを食べます。
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:15Destination-IP : 192.168.150.0  
Destination-Mask : 255.255.255.0FIB-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  
またステップ 2 および 4 に見られるように同じ MAC アドレスを反映する接続隣接関係が、上であることを確認できます。

注PFC2 の隣接関係をチェックするとき最終宛先があるように隣接関係を確認できます。MSFC 2のIOSでは最終宛先の確認はできないので、ネクスト ホップの隣接関係を見る必要があります。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

Catalyst 6500/6000-MSFC2 の接続を確認するのに使用されるリモートネットワークにアクセスするためにトラブルシューティング の手順がセクション [ケーススタディ 1](#) で見つけれられる前例に類似したであることがこの例でわかります: [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 表および FIB ( ステップ 1、3、および 5 ) の最終宛先をチェックします。
- 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。  

```
Cat6k> (enable) show mls entry cef ip 192.168.150.3/32 adjacency Cat6k> (enable)
```
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。この宛先について、MSFC 2のCEFテーブルに3つの異なるエントリがあることがわかります。IOS CEF は、異なるルートを使用した負荷分散をサポートしています。

```
cat6k-MSFC2# show ip cef 192.168.254.253192.168.254.253/32, version 64, per-destination sharing0 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。それらは上でステップ 2 の ARPエントリを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 192.168.254.253/32Mod FIB-Type Destination-IP Destination-Mask NextHop-IP Weight-----
```

Destination-IP	Destination-Mask	NextHop-IP	Weight
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 adjacencyMod : 15Destination-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 -----
```

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 --- -----
default 0.0.0.0 0.0.0.0 192.168.98.2 1
```

見てわかるように、これは0のマスキ長さの唯一のエントリです。このデフォルトは [MSFC2 ルーティング テーブルで存在 するセクション デフォルト ルート](#) および [ルーティング テーブルの デフォルト ルート](#) で後で説明されるように2つの型、である場合もありません。

## [MSFC2 ルーティング テーブルで存在 する デフォルト ルート](#)

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。(ここに、それは太字にまた現われます。)

```
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 ルートがない場合、今でも Supervisor Engine 2 のマスク 長さ0のFIBエントリがあります。ただし、このエントリに今のFIBがあります。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FIBテーブルが完全の稀なケースでは、ワイルドカード エントリはまだありますが、それを一致する 廃棄パケットの代わりに、それらはMSFC2に転送されます。すなわち、FIBに256K以上のプレフィクスが存在し、FIBにすべてのルーティング テーブルとARP隣接関係を保管できない場合です。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に保管できなかつたルーティング 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-fcVLAN 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
```

MSFC 2の物理MACアドレスが表示されます ( MSFC 2のインターフェイスはすべて同じMACアドレスを使用します。 MSFC2 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を ( 覚えて下さい; 2 つの異なるインターフェイスの異なる MAC アドレスを設定できません。 ) 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**はまた MSFC がアクティブである Hot Standby Router Protocol ( HSRP ) グループにリンクされるすべての MAC アドレスを表示する。 **show mls cef mac** コマンドからの出力は、上で、MSFC が VLAN 10 と VLAN 100 のための HSRP アクティブであることを意味します。 MSFC 2上で次のコマンドを入力すると、この情報が正しいかどうかを確認できます。

```
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
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
```

見てわかるように、状態は VLAN 10 および VLAN 100 だけのためにです。状態は設定される他のすべての HSRP グループのためにです。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/削除することにメッセージが表示されます。

## シャドウTCAM

この資料は Supervisor Engine 2 の show mls entry cef コマンド 表をチェックする方法を説明しました。このコマンドは正確に PFC2 の実質 application-specific integrated circuit (ASIC) プログラミングを表しません。表示されるのは、ASIC設定のシャドウコピーだけです。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、一部のパケット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 バグ ID [CSCdv49956](#) ( [登録ユーザのみ](#) ) および [CSCdu85211](#) ( [登録ユーザのみ](#) ) 、CatOS ソフトウェアバージョン 6.3(3)の両方とも固定である、で 7.1(1)、およびそれ以降 文書化されています。

## 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かっています。これらは [CSCdt54036](#) ( [登録ユーザのみ](#) ) に記述されているバグで、いずれもSup

## 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](#)