

スーパーバイザ エンジン 720 および Cisco IOS システム ソフトウェアを搭載した Catalyst 6500/6000 シリーズ スイッチでの、CEF が絡むユニキャスト IP ルーティング問題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](#)

[隣接テーブル](#)

[RP 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](#)

[トラブルシューティングの手順](#)

[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](#)

[DFC-Based ラインカード](#)

[IP ルーティングのディセーブル化](#)

[IP CEF および MLS CEF の違い](#)

[関連情報](#)

概要

このドキュメントは、Supervisor Engine 720、ポリシー フィーチャ カード 3 (PFC3)、マルチレイヤスイッチ フィーチャ カード 3 (MSFC3) 搭載の Cisco Catalyst 6500/6000 シリーズ スイッチ上でユニキャスト IP ルーティングをトラブルシューティングするためのガイドとして使用し

ます。 Supervisor Engine 720でユニキャストルーティングを実行するには、Cisco Express Forwarding(CEF)を使用します。このドキュメントは、Supervisor Engine 720、PFC3、MSFC3を搭載したCatalyst 6500/6000シリーズスイッチのIPルーティングにのみ関連します。 Supervisor Engine 1または1A、またはMultilayer Switch Module(MSM)を搭載した000。 このドキュメントは、スーパーバイザ エンジンで Cisco IOS® ソフトウェアが稼働するスイッチの場合にだけ有効です。ドキュメントは、Cisco Catalyst OS (CatOS) システム ソフトウェアには適用されません。

注：このドキュメントは、Supervisor Engine 2およびMSFC2を搭載したCatalyst 6500/6000スイッチでのユニキャストIPルーティングのトラブルシューティングにも使用できます。

注：このドキュメントでは、MSFCとPFCの代わりにルートプロセッサ(RP)とスイッチプロセッサ(SP)という用語をそれぞれ使用します。

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 720 を搭載した Catalyst 6500/6000 は、SP 上で実行されるハードウェアベースの CEF 転送メカニズムを使用します。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。

- 転送情報ベース (FIB) テーブル
- 隣接テーブル

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。CEF は最初に最長マッチを確認します。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。ルーティングまたはトポロジの変更がネットワークで発生すると、更新は IP ルーティング テーブルで発生します。FIB は変更を反映します。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 エントリとルーティング テーブルのエントリには 1 対 1 の相関関係があるため、FIB には既知のルートのすべてが含まれています。このため、高速スイッチングや最適スイッチングなどのスイッチング パスに関連するルート キャッシュのメンテナンスは不要になります。一致が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。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。Supervisor Engine 720 を搭載した Catalyst 6500/6000 システムでハードウェア CEF を正常に動作させるには、MSFC3 上で IP CEF を実行する必要があります。

RP の FIB および隣接テーブルの読み方

SP の FIB テーブルは、RP の FIB テーブルと完全に一致した内容になります。RP では、Ternary Content Addressable Memory (TCAM) は FIB にすべての IP プレフィックスを保存します。プレフィックスのソートはマスク長で行われ、最も長いマスクから開始されます。したがって、最初にホスト エントリである 32 マスクが設定されたすべてのエントリが表示されます。次に、マスク長が 31 のすべてのエントリが表示されます。マスク長が 0 のエントリ (デフォルトのエントリ) に到達するまで続行します。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。次の例は、RP の FIB テーブルの参考例です。

```
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
```

各エントリは、次のフィールドから構成されています。

- Prefix IP IP

- Next Hop 考えられる Next Hop receiveMSFC このエントリには、レイヤ 3 (L3) のインターフェイスの IP アドレスに対応するマスク長が 32 のプレフィックスが含まれています。
attachedネクスト ホップの IP アドレスdropdrop
- Interface IP IP

完全な隣接テーブルを表示するには、次のコマンドを発行します。

```
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
```

トラブルシューティングの方法

ここでは、トラブルシューティング例および詳細を提供します。最初に、ここでは特定の IP アドレスに対する接続または到達可能性をトラブルシューティングする方法を示します。SP の CEF テーブルは、RP 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。したがって、SP は RP によって認識されている情報が正しい場合のみ、IP アドレスに到達する正しい情報を保持します。したがって、この情報は必ず確認する必要があります。

RP から実行

次のステップを実行します。

1. RP テーブルの IP ルーティングに含まれている情報が正しいことを確認します。show ip route コマンドを発行し、予想されるネクスト ホップが出力に含まれていることを確認します。注：代わりに、show ip route x.x.x.x コマンドを発行すると、完全なルーティング テーブルを参照する必要はありません。予想されるネクスト ホップが出力に含まれていない場合は、設定およびルーティング プロトコル ネイバーを確認します。また、実行しているルーティング プロトコルに関する別のトラブルシューティング手順を実行します。
2. ネクスト ホップ、または接続されたネットワークの場合は最終的な宛先が正しい、RP 上の解決済みのアドレス解決プロトコル (ARP) エントリであることを確認します。show ip arp next_hop_ip_address コマンドを発行します。ARP エントリの解決を確認し、エントリに正しい MAC アドレスが含ま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、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。不完全な ARP エントリは、RP がホストから応答を受信しなかったことを示します。ホストが稼働中であることを確認します。ホストが ARP の応答を取得し、正しく応答するかどうかを確認するには、ホストにスニファを使用できます。
3. RP の CEF のテーブルに正しい情報が含まれていて、アジャセンシー関係が解決されることを確認します。次のステップを実行します。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 ホップと一致していることを確認するために、show ip cef destination_network コマンドを発行します。これは、この項のステップ 1 のネクスト ホップです。アジャセンシー関係が正しいことを確認するために、show adjacency detail | begin next_hop_ip_address コマンドを発行して、隣接関係が正しいことを確認します。エントリは、この項のステップ 2 と同じ ARP の MAC アドレスを含む必要があります。

この項のステップ 1 と 2 で正しい結果を得られたとしても、ステップ 3a または 3b に失敗すると

IOS CEF の問題が発生します。この問題は、Catalyst 6500/6000に関連するプラットフォーム固有の問題ではない可能性があります。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。

SP から実行

次のステップを実行します。

1. SP に保存された FIB 情報が正しく、RP に保存された CEF テーブルの情報と一致することを確認します。注：CEFテーブルの情報は、「RPから」セクションのステップ3に基づいています。show mls cef lookup *destination_ip_network detail* コマンドを発行し、隣接エントリがあることを確認します。情報が存在しない場合、RP と SP 間に通信の問題があります。この問題は、Catalyst 6500/6000 プラットフォーム固有の機能と関係があります。実行している特定の Cisco IOS ソフトウェア リリースの既知の不具合がないかどうかを確認してください。正しいエントリを復元するには、RP で clear ip route コマンドを発行します。
2. SP の隣接テーブルを確認するには、show mls cef adjacency entry *adjacency_entry_number detail* コマンドを発行します。エントリに、「RPから実行」の項にあるステップ2と3bで表示されるアドレスと同じ宛先 MAC アドレスが含まれていることを確認します。SP の隣接情報が、ステップ3bで確認した隣接情報と異なる場合には、RP と SP 間の内部通信に問題があります。正しい情報を復元するために、アジャセンシー関係をクリアしてみてください。

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。

- IP アドレスが 112.112.112.2 であるネットワーク 112.112.112.0/24 内のホスト A
 - IP アドレスが 222.222.222.2 であるネットワーク 222.222.222.0/24 内のホスト B
- 関連する RP コンフィギュレーションは、次のとおりです。

```
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
```

特記事項： Supervisor Engine 720 および MSFC3 を搭載した Catalyst 6500/6000 プラットフォームは、ハードウェアの CEF を使用してルーティングを実行します。CEF の設定要件はなく、MSFC3 で CEF を無効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

IP アドレス 222.222.222.2 に到達するパスを確認するには、このドキュメント「[トラブルシューティングの方法](#)」の項にある手順に従ってください。

1. IP ルーティング テーブルを確認するには、次の 2 つのコマンドのいずれか、または両方を発行します。

```
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
```

または

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

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. RP の ARP エントリを確認します。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。次のコマンドを実行します。

```
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. RP の CEF テーブルおよび隣接テーブルを確認します。CEF テーブルを確認するには、次のコマンドを発行します。

```
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
```

マスク長32の有効なCEFエントリが存在することがわかります。また、有効なキャッシュされた隣接関係が存在していることも確認できます。隣接テーブルを確認するには、次のコマンドを発行します。

```
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
```

この出力は、アジャセンシー関係があることを示しています。アジャセンシー関係の宛先 MAC アドレスには、この項のステップ 2 の ARP テーブル内の MAC アドレスと同じ情報が表示されます。

4. SP の観点から、CEF/FIB エントリが正しいかどうかを確認します。FIB には、次の 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は、次の出力のように表示されます

```
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 )
```

このエントリは既知のネクスト ホップを含むホスト エントリです。この場合、ネクスト ホップは宛先自体です。宛先ネットワークに対応するエントリは、次の出力のように表示されます。

```
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)

このエントリは接続された FIB エントリです。このエントリにヒットするパケットは、追加処理のために RP にリダイレクトされます。この処理は、主に ARP の送信と ARP の解決の待機を行います。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、宛先 IP アドレスのエントリと宛先ネットワークのエントリの両方がある場合、SP はマスク 32 の最初のエントリを使用します。このエントリがホストエントリです。より詳細な FIB テーブルエントリは考慮されません。/32 合、SP は宛先ネットワークのエントリである 2 番目のエントリを使用します。このエントリが接続されたエントリであるかのように、SP は次の処理のために RP にパケットをリダイレクトします。RP は宛先マスクの ARP の要求を送信できます。ARP の応答を受信すると、RP のホストの ARP テーブルと隣接テーブルが完全になります。

5. マスク長 32 の正しい FIB エントリが作成されたら、そのホストについてアジャセンシー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。次のコマンドを実行します。

```
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
```

注：隣接関係が設定され、宛先 MAC(d_{mac}) フィールドにはホスト B の有効な MAC アドレスが含まれます。このアドレスは、このセクションのステップ 2 と 3b で確認したアドレスです。

注：packets_{bytes} の数は 0 です。入力モジュールに Distributed Forwarding Card (DFC) がある場合は、パケット/バイト数を取得するためにモジュールにログインする必要があります。

[「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」](#)では、このプロセスについて説明します。

考慮事項および結論

[「トラブルシューティングの手順」](#)のステップ 4 で説明するように、優れた一致となる 2 つの FIB エントリがあります。その内容は次のとおりです。

- この場合は、222.222.222.0/24 のネットワーク エントリです。このエントリは常に存在し、MSFC のルーティング テーブルおよび CEF のテーブルから直接取得されます。このネットワークは、ルーティング テーブルで常に直接接続があります。
- 宛先ホストエントリ(この場合は 222.222.222.2/32)は、このエントリが存在するとは限りません。エントリが存在しない場合、SP はネットワーク エントリを使用し、次のイベントが発

生じます。SP によってパケットが RP に転送されます。PFCのFIBテーブルは、マスク長 32のホストエントリを作成します。ただし、CEFの完全な隣接関係はまだないため、タイプ `drop` します。宛先への以降のパケットが `/32 drop` 同時に、RP に転送された最初のパケットにより、MSFC から ARP 要求が送信されます。ARP の解決により、ARP エントリが完成します。RP のアジャセンシー関係が完成します。既存の `drop SP` SP は書き換えられた MAC アドレスを反映するため、ホストのアジャセンシー関係を変更します。アジャセンシー関係のタイプが接続されたインターフェイスに変更されます。ARP の解決を待つ間、`drop ARP throttle` ARP throttle は、すべてのパケットが RP に転送されて、複数の ARP 要求が生成されることを回避します。RP には最初のいくつかのパケットのみが転送され、PFC はアジャセンシー関係が完成するまで残りのパケットを廃棄します。また、ARP throttle は直接接続されたネットワーク上の存在または応答しないホストに宛てられているトラフィックを廃棄できるようにします。

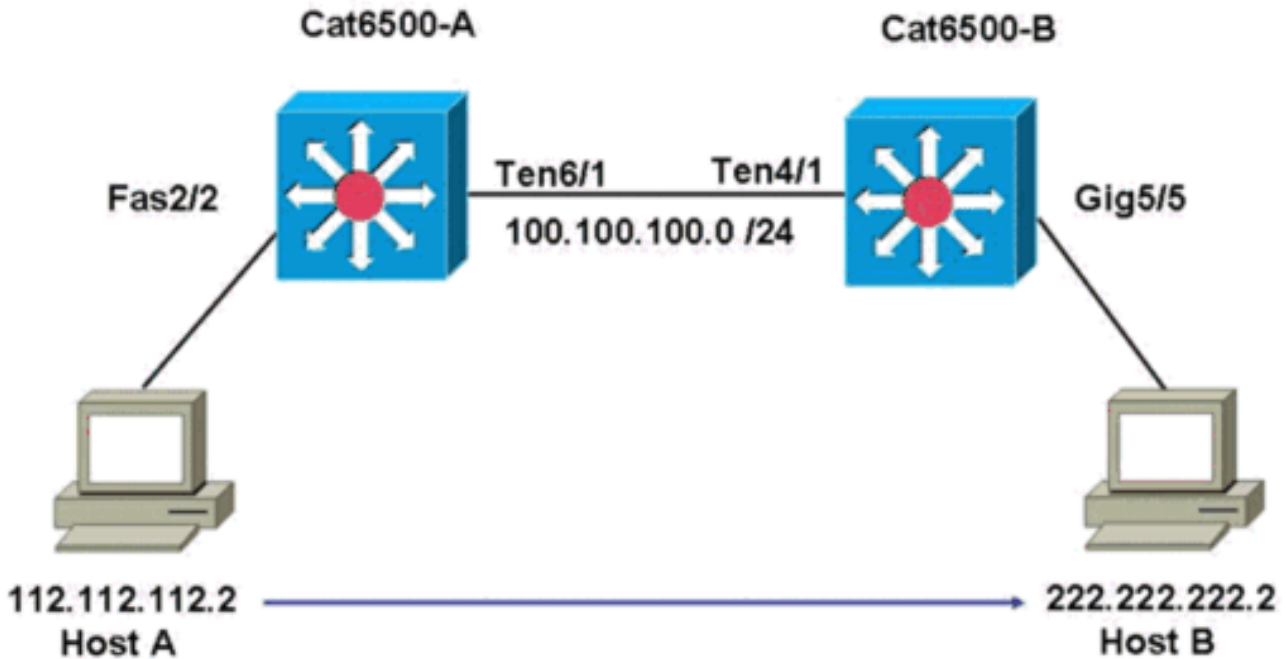
異なる VLAN に属す 2 ユーザ間の接続のトラブルシューティングを行うには、常に、次の事項を確認する必要があります。

- 「[トラブルシューティングの方法](#)」を使用して宛先 IP アドレスをホスト B にする、ホスト A からホスト B へのトラフィック
- 同じ「[トラブルシューティングの方法](#)」を使用しているが、宛先をホスト A にする、ホスト B からホスト A へのトラフィック

また、ソースのデフォルト ゲートウェイの出力を取得することも忘れないでください。このホスト A からホスト B へのトラフィックとホスト B からホスト A へのトラフィックは、必ずしも同じではありません。

[ケーススタディ 2: リモート ネットワークへの接続](#)

このセクションの図では、IPアドレスが112.112.112.2のホストAが、IPアドレスが222.222.222.2のホストBにpingを実行していますが、今回は、ホストBがCat6500-Aスイッチに直接接続していません。ホストBは、2ホップ離れた場所にルーティングされています。Cat6500-BスイッチでCEFのルーティングされたパスをたどるときと同じ方法を使用します。



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. Cat6500-A のルーティング テーブルを確認するには、次のコマンドを発行します。

```
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
```

この出力から、IPアドレス222.222.222.2のホストBに到達するために、Open Shortest Path First(OSPF)プロトコルルートがあることがわかります。TenGigabitEthernet6/1 をネクストホップとして、IP アドレス 100.100.100.1 を使用してホストに到達する必要があります。

2. RP の ARP テーブルを確認するには、次のコマンドを発行します。注：最後の宛先ではなく、ネクストホップのARPエントリを確認してください。

```
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. RP の CEF テーブルと隣接テーブルを確認するには、次のコマンドを発行します。

```
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
```

宛先ネットワークの CEF エントリがあることを確認できます。また、ネクストホップの結果はステップ1のルーティングテーブルにある内容と一致します。

4. ネクストホップの隣接テーブルを確認するには、次のコマンドを発行します。

```
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
```

ネクスト ホップの有効なアジャセンシー関係が存在し、宛先の MAC アドレスはステップ 2 の ARP エントリと一致します。

5. SP の FIB テーブルを確認するには、次のコマンドを発行します。

```
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 0 222.222.222.0 (A:163840 ,P:1,D:0,m:0 ,B:0 )
```

FIB にはステップ 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. SP の隣接テーブルを確認するには、次のコマンドを発行します。

```
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
```

注：パケットとバカウンタルタイムです。トラフィックが停止すると、カウンタは0に戻ります。

考慮事項および結論

次の「[トラブルシューティングの手順](#)」は、リモート ネットワークに到達するために Cat6500-A スイッチの接続を確認します。この手順は、「[トラブルシューティングの手順](#)」と似ています。これは、「[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](#)」の項にあります。以下に、相違点をまとめます。「[トラブルシューティングの手順](#)」、「[ケーススタディ 2：リモートネットワークへの接続](#)」では、次を行う必要があります。

- IP ルーティング テーブル、CEF テーブル、FIB テーブルの最終的な宛先を確認します。この確認は、ステップ 1、3、および 5 で実行します。
- ARP テーブルと隣接テーブルでネクスト ホップ情報を確認します。この確認は、ステップ 2 および 4 で実行します。
- 最終的な宛先の隣接テーブルを確認します。この確認は、ステップ 6 で実行します。

ケーススタディ 3：複数のネクスト ホップへの負荷分散

トラブルシューティングの手順

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. 同じ宛先 IP アドレスに到達するために使用できる異なるルートと異なるネクスト ホップがあることを調べるため、ルーティング テーブルをチェックします。このルーティング テー

ブルの例では、宛先 IP アドレス 222.222.222.2 に到達するために使用できる 2 つのルートおよび 2 つのネクスト ホップがあります。

```
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. 3 つのネクスト ホップについて、それぞれの ARP エントリを確認します。次のステップを実行します。宛先の CEF テーブルを確認します。宛先として、RP の CEF テーブル内の 2 つの異なるエントリが表示されます。Cisco IOS ソフトウェア 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。

```
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
```

2 つのネクスト ホップについて、ARP エントリを確認します。

```
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   TenGigabit
Ethernet6/1
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
```

RP の隣接テーブルで、2 つのアジャセンシー関係を確認します。

```
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
```

ステップ 2b および 2c の情報が一致する必要があります。

3. 同じ宛先について、2 つの異なる FIB エントリが挿入されています。PFC のハードウェア CEF は、1 つの宛先について最大 16 の異なるルートに負荷を分散させることができます。デフォルトは src_dst IP ロードシェアリングです。

```
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)
```

4. トラフィックの転送に使用する正確なルートを確認します。次のコマンドを実行します。

```
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)
```

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、Supervisor Engine 720 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。このエントリを表示するには、次のコマンドを発行します。

```
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
```

3 個のエントリがあります。デフォルトは、次の 2 つのタイプになります。

- [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](#)

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、RP ルーティング テーブルにデフォルト ルートが存在していることを確認します。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。また、デフォルト ルートは太字で表示されています。

```
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
```

この例では、RP ルーティング テーブルにデフォルト ルートが存在し、設定された「static

注：CEFの動作は、スタティック、OSPF、Routing Information Protocol(RIP)、または別の方法でデフォルトルートがどのように学習されても同じです。

デフォルトルートがある場合、常にマスク長0のCEFエントリがあります。このエントリは、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を転送します。

```
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
```

CEF は最初に最長マッチから開始し、各パケットについて FIB を順番に参照します。したがって

、このデフォルトの FIB は、他に一致しないパケットでのみ使用します。

ルーティング テーブルにデフォルト ルートがない場合

```
Cat6500-B#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、Supervisor Engine 720にはマスク長0の FIB エントリが残ります。この FIB エントリは、FIB 内の他のエントリと一致しないパケットで使用され、その結果ドロップされます。この廃棄はデフォルト ルートがないため、有用です。これらのパケットはどのみち RP で廃棄されるため、これらのパケットを RP に転送する必要はありません。この FIB エントリを使用すると、ハードウェアの不要なパケットを確実に廃棄できます。この廃棄は RP の無駄な使用率を回避します。ただし、具体的に IP アドレス 0.0.0.0 にパケットが宛てられた場合、そのパケットは RP に送られます。

```
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

注：まれには、FIB テーブルがいっぱいになっている場合でも、FIB ドロップ エントリは存在します。ただし、エントリに一致するパケットを廃棄する代わりに、パケットは RP に送られます。これは、FIB に 256,000 以上のプレフィックスが存在し、完全なルーティング テーブルに十分な領域がない場合にのみ発生します。

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

DFC-Based ラインカード

トラフィックの入力モジュールが DFC ベースのライン カードの場合、転送決定はモジュールでローカルに行われます。ハードウェアのパケット カウンタを調べるには、モジュールに対してリモート ログインを実行します。その後、この項で示すように、コマンドを発行します。

「[ケーススタディ 2：リモート ネットワークへの接続](#)」を例として使用します。Cat6500-B の場合、トラフィックは DFC があるモジュール 4 に入ります。モジュールにリモート ログインするには、次のコマンドを発行します。

```
Cat6500-B#remote login module 4
```

```
Trying Switch ...
```

```
Entering CONSOLE for Switch
```

```
Type "^C^C^C" to end this session
```

```
Cat6500-B-dfc4#
```

次に、モジュールで CEF FIB 情報を確認できます。

```
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 )
```

次に、ハードウェア カウンタで隣接情報を確認できます。

```
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
```

IP ルーティングのディセーブル化

Cisco IOS ソフトウェア リリース 12.1(20)E 以降では、Catalyst 6500 シリーズ スイッチの IP ルーティングをディセーブルにするサポートがなくなりました。次の例に示すように、これらのスイッチでは IP ルーティングをディセーブルにすることはできません。

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

no ip routing コマンドは、Cisco IOS ルータで IP ルーティングをディセーブルにするために使用される Cisco IOS ソフトウェア コマンドです。通常、このコマンドは、ローエンド ルータで使用されます。

no ip routing コマンドは、スイッチで **service internal** コマンドがすでにイネーブルになっている場合にのみ受け入れられます。ただし、設定には保存されず、スイッチのリロードすると失われます。シスコは、Cisco IOS システム ソフトウェアを実行する Catalyst 6000/6500 シリーズ スイッチで IP ルーティングをディセーブルにしないことを推奨します。

この問題の回避策として、**ip route 0.0.0.0 0.0.0.0 a.b.c.d** コマンドを使用します。このコマンドでは、a.b.c.d はデフォルト ゲートウェイの IP アドレスです。次の両方に当てはまる場合、ルーティング プロセスは使用されません。

- **switchport** コマンドを使用して、スイッチのすべてのインターフェイスを L2 ポートとして設定しました。
- スイッチでスイッチ仮想インターフェイス (SVI) (VLAN インターフェイス) が設定されていません。

IP CEF および MLS CEF の違い

show mls cef exact-route source-ip address dest-ip address と **show ip cef exact-route source-ip address dest-ip address** の出力は、パケットが IP CEF の使用時にはソフトウェアでスイッチングされ、MLS CEF の使用時にはハードウェアでスイッチングされるため、異なります。ほとんどのパケットはハードウェアでスイッチングされるため、宛先に到達するネクスト ホップを表示する最善のコマンドは、**show mls cef exact-route source-ip address dest-ip address** です。

関連情報

- [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](#)
- [MSFC を搭載した Catalyst 6500/6000 スイッチでの 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](#)
- [ツールとリソース](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)