Catalyst 5000 ルート スイッチ モジュール（RSM）および VLAN 間ルーティングのトラブルシューティング

目次

はじめに

このドキュメントでは、Catalyst 5000 ファミリ スイッチのルート スイッチ モジュール（RSM）を使用した VLAN 間ルーティングのトラブルシューティングに関する情報について説明します。 RSM のトラブルシューティングに関しては、まず RSM を単純な外部ルータとして想定する必要があります。 VLAN 間ルーティングが関与する場合、RSM 固有の問題が障害の原因になることは非常にまれです。 したがって、このドキュメントでは問題が生じる可能性のある次の 2 つの主な分野のみを取り扱います。

- **RSM ハードウェア関連の問題**: この資料は RSM アーキテクチャを導入し、トラッキングするために追加 RSM 関連のカウンターの詳細を説明します。
- **VLAN 間の設定に関連する問題**（大抵ルータとスイッチ間の相互対話に関する）: これはまた他の内部ルータ（マルチレイヤ・スイッチ フィーチャ・カード[MSFC]、Route Switch Feature Card [RSFC]のような、8510CSR、等）と頻繁に外部ルータに適用します。

注: この資料は Catalyst 4000，5000 および 6000 スイッチの VLAN 間ルーティングを設定することを取り扱っていません。 それらの詳細については、これらの文書を参照して下さい:

- Catalyst 4500/4000 ファミリー（WS-X4232-L3）用のルータモジュールの設定および外観
- Catalyst 4000 レイヤ3 サービス モジュールに関するインストール および 設定に関する 注意書きの *InterVLANルーティング セクションのためのモジュールの設定*
- CatOS システム ソフトウェアが稼働する Catalyst 5500/5000 および 6500/6000 スイッチでの内部ルータ（レイヤ 3 カード）を使用した VLAN 間ルーティングの設定

この資料は解決する基本的なルーティング プロトコルか Multilayer Switching （MLS）関連の問題を取り扱っていません。

前提条件

要件

このドキュメントに関しては個別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。

VLAN 間ルーティングとは何か。

VLAN 間ルーティングを論議する前に、この資料は VLAN 概念に焦点を合わせます。 これは VLAN のための必要の理論的な説明単にでが、VLAN がスイッチをどのように操作するか論議します。 スイッチ上に VLAN を作成すると、あたかもスイッチがいくつかの仮想ブリッジに分割され、それぞれが同じ VLAN に属するポートだけをブリッジするようになります。

このダイアグラムは 3 異なる VLAN に割り当てられる 9 つのポートとスイッチを表します:

これは 3 つの独立 したブリッジで構成されている次のネットワークと丁度同等です、:

このスイッチでは、各 VLAN が個別にブリッジを作成しているため、3 つの異なるブリッジが存在します。 各 VLAN が別のスパニング ツリー プロトコル（STP）例を作成するので、STP は 3 つの異なるフォワーディングテーブルを維持します。

2 番目の図から、同じ物理デバイスに接続されているにもかかわらず、異なる VLAN に属するポートはレイヤ 2（L2）で直接通信できないことは明白になります。 仮に可能だとしても、これは適切ではありません。 たとえば、接続されたポート 1 からポート 4、VLAN1 に VLAN2 を単にマージした場合。 この場合、2 つの別個の VLAN にする必要はありません。

VLAN の間でほしいと思う唯一の接続はレイヤ3（L3）でルータによって実現します。 これは VLAN 間ルーティングです。 更にダイアグラムを簡素化するために、VLAN は異なる物理的なイーサネット セグメントとしてスイッチによって提供される特定のブリッジング機能に実際に興味がないので、表されます。

このダイアグラムでは、2 VLAN は 2 つの異なるイーサネット セグメントとして考慮されます。

VLAN 間のトラフィックは外部ルータを通過する必要があります。 ホストA がホスト B と通信したいと思う場合デフォルト ゲートウェイとして一般的にルータを使用します。

RSM のアーキテクチャ

論理アーキテクチャ

RSM は、Catalyst 5000 スイッチの異なる VLAN に直接接続される複数のインターフェイスを持つ外部ルータとみなすことができます。

呼ばれるかわりにイーサネットインターフェイスと、これらのインターフェイスは接続する VLAN に従って指名されます。（インターフェイス VLAN1 は VLAN1 に直接、等接続されます。）

実装アーキテクチャ

RSM は Catalyst 5000 ラインカードのの中の Cisco 7500 Route スイッチ プロセッサ（RSP）ルータです。 それを設定し、解決するためにカードのアーキテクチャについてずいぶん確認する必要はありません。 ただし RSM がどのようにの正常な外部ルータと異なっているどのようにか理解する構築されたヘルプであるか、概念を持っています。 この知識は **show controller c5ip コマンドを**もたらすとき特に重要です。

このダイアグラムは RSM ラインカードで主要なコンポーネントを取付けます:

Catalyst 5000 インターフェイス プロセッサ

Catalyst 5000 Interface Processor（C5IP; Catalyst 5000 インターフェイス プロセッサ）は RSM の一部であり、Catalyst 5000 のスイッチング バスをネットワーク インターフェイスとして使用することにより、Catalyst 7500 システム の IP をエミュレートします。 C5IP には R4700 プロセッサ と 2 つの SAGE Application-Specific Integrated Circuit（ASIC; 特定用途集積回路）が含まれています。これらは Catalyst 5000 スイッチング バスへのアクセスを行います。

SAGE

これら 2 つの ASIC は、スイッチング バス間でパケットを授受し、これらをバッファリングします。 また、パケット内のデータとともに、スイッチ内のパケットの宛先を識別する索引も取得します。

宛先 VLAN インターフェイスは、パケット自体のコンテンツからは判別されませんが、この索引から導出されます。 パケットおよびインデックスは SAGE の中の 2 つの異なる FIFO で最初に保存されます。 索引が読み取られ、必要な共有メモリが宛先 VLAN の領域に予約されます。 パケットはこの後、SAGE への Direct Memory Access（DMA; ダイレクト メモリ アクセス）を使用して、memory device（MEMD; メモリ デバイス）の中にコピーされます。

ルータとスイッチングバスの間で通信するために並行してはたらく 2 SAGE はのパケットデリバリ順序が狂って原因となる場合があります。（たとえば、SAGE0 で受信された大きいパケットは SAGE1 による小さいパケットによって受け取った以降後送信できます。）これを回避するために、各 VLAN は任意の SAGE に静的に割り当てられています。 これは始動で自動的にされます。（ルータに従って、VLAN は 2 つの DMA チャネルの 1 つに、SAGE に導く全部関連付けられます。）任意の VLAN からのパケットは、常に順序どおりに配信されます。

MEMD

MEMD は、ルータがパケットの送受信に使用する共有メモリです。 RSM に設定されている各 VLAN インターフェイスに、利用可能な共有メモリの一部が割り当てられます。 設定した VLAN インターフェイスの数が多いほど、インターフェイス単位の共有メモリの量は減ります。 VLANインターフェイスは無効かシャットダウンされて時でさえ共用メモリの一部を保持します。 VLAN インターフェイスを管理上追加または削除した場合のみ、VLAN インターフェイス間の MEMD の区画の再設定が新たに行われます。

RSMに特有のトラブルシューティング

Cisco 通常 IOS® ルータドキュメンテーションでカバーされない主要な RSM 特有の問題は RSM のアクセスに関する問題、およびまたパフォーマンス上の問題です。

RSM へのアクセス

RSM には、次の 3 つの方法でアクセスできます。

- RSM への Telnet 接続
- セッション スイッチ スーパバイザからの RSM に
- 直接コンソール接続

RSM への Telnet 接続

RSM に Telnet するには、その VLAN インターフェイスの 1 つに割り当てられている IP アドレスを知る必要があります。 Telnet セッションは、通常の Cisco IOS ルータに接続を試行する場合とまったく同様に機能します。 Telnet およびゲイン イネーブル アクセスを実現するために VTY にパスワードを割り当てる必要がある場合もあります。

この例は Supervisor Engine から VLAN1 IP アドレスが 10.0.0.1 である RSM に Telnetセッションを示したものです:

```
sup> (enable) telnet 10.0.0.1
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
User Access Verification
Password: rsm> enable
Password: rsm# show run
!--- Output suppressed. ! hostname rsm ! enable password ww !--- An enable password is
configured. ! !--- Output suppressed. line vty 0 4 password ww login !--- Login is enabled. A
password must be configured on the vty. ! end
```

この方法は、他の外部ルータの Cisco IOS の設定に似ています。

セッション スイッチ スーパバイザからの RSM に

セッションを使用する Supervisor Engine からのスロット *X*.の RSM に *x コマンドは*接続します。

この方式は Telnet の方法と同じです。 RSM には隠れた VLAN0 インターフェイスがあり、この

IP アドレスは 127.0.0. (x+1) です。x は RSM が取り付けられたスロットを指しています。session コマンドにより、このアドレスに対して隠れた Telnet セッションが発行されます。

注: 今回、VTY およびイネーブル パスワードは RSM にフルアクセスを得る設定にあるなりません。

```
sup> (enable) show module
Mod Slot  Ports      Module-Type Model          Status
--- ---- ----- ------------------------ ------------------
1     1    0     Supervisor III WS-X5530          ok
2     2          Route Switch Ext Port
3     3    1     Route Switch WS-X5302            ok
4     4   24     10/100BaseTX Ethernet WS-X5225R  ok
5     5   12     10/100BaseTX Ethernet WS-X5203   ok
!--- Output suppressed. sup> (enable) session 3
Trying Router-3...
Connected to Router-3.
Escape character is '^]'.
rsm> enable
rsm#
```

RSM がスイッチにインストールされているスロットを識別するのに Supervisor Engine コマンド show module を使用します。 **session コマンドの**使用によって直接それにアクセスできます。

直接コンソール接続

RSM のシステムコンソールポートはシステムと設定し、通信することを可能にするデータターミナルを接続するための DB-25 ソケット DCE ポートです。 備え付けられたコンソール ケーブルを使用して、端末を RSM のコンソール ポートに接続します。 RSM のコンソール ポートは補助ポートの隣にあり、コンソールというラベルが付けられています。

コンソールポートを接続する前に、使用するターミナルのボーレートを判別するためにターミナルドキュメンテーションをチェックして下さい。 端末のボー レートは、デフォルトのボー レート (9600 ボー) に一致する必要があります。 ターミナルをとして設定して下さい: 9600 ボー、8 データ ビット、パリティなし、2 ストップ ビット (9600、8N2) 。

RSM にアクセスできない

RSM はいくつかの理由で切り離されることがあります。 RSM に接続できない場合でも、外側から確認できる表示があります。

- RSM の LED のステータスをチェックして下さい:CPU 停止 LED は以外のシステム検知しましたプロセッサハードウェア失敗をです。オレンジ ステータス LED —ディセーブルにされるモジュールは進行中の進行中、かシステム ブートをテストします。
- スイッチが RSM を見る場合があるかどうか Supervisor Engine を確認して下さい。 これを行うには、show module コマンドを発行します。

```
sup> (enable) show module
Mod Slot Ports    Module-Type Model              Status
--- ---- ----- ------------------------  ------------------
1    1    0    Supervisor III WS-X5530            ok
2    2         Route Switch Ext Port
3    3    1    Route Switch WS-X5302              ok
4    4   24    10/100BaseTX Ethernet WS-X5225R    ok
5    5   12    10/100BaseTX Ethernet WS-X5203     ok
!--- Output suppressed.
```

コンソール接続の試行が終るまでは、絶対に RSM が故障していると宣言しないでください。 、見たようにセッションおよび Telnetアクセスは両方 RSM に IP接続に頼っています。 RSM がまたは起動するか、たとえば、それにまたはセッション Telnet で接続することができません ROMMON モードでスタックされて。 しかし、これはきわめて正常なことです。

RSM に障害が起きているように見受けられる場合であっても、コンソールに接続を試みてください。 そうすることで、コンソールに表示されるエラー メッセージが見える可能性があります。

パフォーマンスの問題

RSM と関連しているパフォーマンス上の問題のほとんどは正常な Cisco IOS ルータと同様に同じように解決することができます。 このセクションは C5IP である RSM 実装の特定の一部に焦点を合わせます。 コマンド **show controller c5ip は** C5IP のオペレーションに関する情報を与えることができます。 この出力はいくつかの最も重要なフィールドを解説したものです:

```
RSM# show controllers c5ip
DMA Channel 0 (status ok) 51 packets, 3066 bytes One minute rate, 353 bits/s, 1 packets/s Ten
minute rate, 36 bits/s, 1 packets/s Dropped 0 packets Error counts, 0 crc, 0 index, 0 dmac-
length, 0 dmac-synch, 0 dmac-timeout Transmitted 42 packets, 4692 bytes One minute rate, 308
bits/s, 1 packets/s Ten minute rate, 32 bits/s, 1 packets/s DMA Channel 1 (status ok) Received
4553 packets, 320877 bytes One minute rate, 986 bits/s, 2 packets/s Ten minute rate, 1301
bits/s, 3 packets/s Dropped 121 packets 0 ignore, 0 line-down, 0 runt, 0 giant, 121 unicast-
flood Last drop (0xBD4001), vlan 1, length 94, rsm-discrim 0, result-bus 0x5 Error counts, 0
crc, 0 index, 0 dmac-length, 0 dmac-synch, 0 dmac-timeout Transmitted 182 packets, 32998 bytes
One minute rate, 117 bits/s, 1 packets/s Ten minute rate, 125 bits/s, 1 packets/s Vlan Type DMA
Channel Method 1 ethernet 1 auto 2 ethernet 0 auto Inband IPC (status running) Pending messages,
0 queued, 0 awaiting acknowledgment Vlan0 is up, line protocol is up Hardware is Cat5k Virtual
Ethernet, address is 00e0.1e91.c6e8 (bia 00e0.1e91.c6e8) Internet address is 127.0.0.4/8 MTU
1500 bytes, BW 100000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:00,
output 00:00:00, output hang never Last clearing of "show interface" counters never Queueing
strategy: fifo Output queue 0/40, 0 drops; input queue 0/75, 0 drops 5 minute input rate 0
bits/sec, 1 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 53 packets input, 3186
bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC,
0 frame, 0 overrun, 0 ignored RSM#
```

DMA Channel 0/1

RSM 内部の RSP ルータは、（2 つの SAGE ASIC につながっている）2 つの別個の DMA チャネルを介して、スイッチとの通信を行います。 各 VLAN インターフェイスは、これらの DMA チャネルの 1 つに自動的に関連付けられます。 show controllers c5ip コマンドは、2 つの別個のセクションでそれぞれに関する情報を表示します。

Received/Transmitted

これらの統計情報は、異なる DMA チャネルの負荷を判別する際に使用します。 他方の DMA チャネルと比べて、一貫して過負荷になっている DMA チャネルを探します。 これはすべてのトラフィック集中型 VLAN が同じ DMA チャネルに割り当てられる場合発生するかもしれません。 必要な場合は、インターフェイス コマンド dma-channel を使用して、手動で VLAN インターフェイスを特定の DMA チャネルに割り当てることができます。

Dropped

これは RSM が受け取ったが、廃棄したパケットの数を示します。 これは、パケットとともに受

信されたインデックスが、パケットの具体的な宛先を RSM に示していない場合に発生します。

Error Counts

- **crc** – Cycle Redundancy Check（CRC; 巡回冗長検査）エラーは、RSM によって不正な CRC が検出された場合に発生します。 バックプレーンの悪い CRC のパケットがないはずであるしいくつかのラインカードか他のバックプレーン接続されたデバイスがきちんとはたらいていないことをこれらを検出する RSM は示します。**注:** CRC エラーは、ISL トランクを経由して接続されているリモート デバイスが原因であることもあります。 ほとんどの Catalyst ラインカードでは、バックプレーンから受信したパケットや、トランクでフォワーディングするパケットの CRC をチェックしていません。
- **index** – インデックス エラーはインデックスが正確ではないと発生します。 C5IP はこのパケットをなぜ受信したかに気づいていません。 索引エラーによって dropped カウンタも増分されます。
- **DMAC** —これらのエラーは SAGE ASIC は探知されていなかったらルータ共用メモリを破損しよう最大伝送ユニット（MTU）サイズをオーバーランすることを C5IP インターフェイスが防いだときに発生します。
- **dmac** — SAGE ASIC がパケットを廃棄する場合、パケット FIFO およびインデックス FIFO は同期化からなります。 このエラーは発生すると、自動的に検出され、dmac-synch のカウンタが増分されます。 これが発生することはまずないです、パフォーマンス影響は極端に低いです。
- **DMAC** —このカウンターは Cisco IOS ソフトウェア リリース 11.2(16)P および 12.0(2) の **show controllers c5ip コマンド**に追加されました。 このカウンタは、起こりうる最長の転送に必要とされる最大時間内で、DMA 転送が完了しなかった場合に増分されます。 それはハードウェア障害を示し、このカウンターのゼロ以外の値を表示する RSM は置換用のよい候補です。
- **ignore** –無視はルータがインプットパケットのための MEMD バッファを使い果たすと行われます。 これは入っている程に CPU がファースト パケットを処理していないと起こります。 CPU をビジー状態にしているものが原因であると考えられます。
- —ラインダウンは行プロトコル VLAN に向かうパケットが廃棄されたことを示します。 C5IP はダウンすると信じる VLANインターフェイスのためのパケットを受信しました。 これはスイッチがダウンしている RSM インターフェイスにパケットを転送することを止める必要があるので起こるべきではありません。 しかし、RSM がインターフェイスのダウンを宣言してからスイッチにそれが通知されるまでのタイミングが原因で、インターフェイスがダウンしているにもかかわらず RSMインターフェイスにパケットがフォワーディングされることがまれにあります。
- /—このカウンタは無効サイズのパケットを追跡記録します。
- —ユニキャスト フラッディング パケットは特定の MAC アドレスに送信されるパケットです。 Catalyst 5000 の CAM テーブルでは、どのポートに MAC アドレスがあるかわからないため、VLAN のすべてのポートにこのパケットを フラッディングします。 RSM はまたこれらのパケットを受信します、その VLAN のブリッジングのために設定されなければ、自身の MAC アドレスを一致するパケットに興味がありません。 RSM はこれらのパケットを廃棄します。 これは、イーサネット インターフェイス チップ内にあり、その他の MAC アドレス宛のパケットを無視するようにプログラムされている、実際のイーサネット インターフェイスで発生する状況に匹敵します。 RSM では、これは C5IP ソフトウェアで行われます。 廃棄されるパケットのほとんどはユニキャストフラッディング パケットです。
- **drop** –このカウンターは最後の破棄された パケットについての特定の情報を明らかにします。 これはこの資料の範囲外にある低レベル情報です。

DMA チャネル間の VLAN ディストリビューション

下記に、10 個の VLAN インターフェイスが設定された RSM 上の show controllers c5ip コマンドの出力の一部を示します。

```
RSM# show controllers c5ip
DMA Channel 0 (status ok) 51 packets, 3066 bytes One minute rate, 353 bits/s, 1 packets/s Ten minute rate, 36 bits/s, 1 packets/s Dropped 0 packets Error counts, 0 crc, 0 index, 0 dmac-length, 0 dmac-synch, 0 dmac-timeout Transmitted 42 packets, 4692 bytes One minute rate, 308 bits/s, 1 packets/s Ten minute rate, 32 bits/s, 1 packets/s DMA Channel 1 (status ok) Received 4553 packets, 320877 bytes One minute rate, 986 bits/s, 2 packets/s Ten minute rate, 1301 bits/s, 3 packets/s Dropped 121 packets 0 ignore, 0 line-down, 0 runt, 0 giant, 121 unicast-flood Last drop (0xBD4001), vlan 1, length 94, rsm-discrim 0, result-bus 0x5 Error counts, 0 crc, 0 index, 0 dmac-length, 0 dmac-synch, 0 dmac-timeout Transmitted 182 packets, 32998 bytes One minute rate, 117 bits/s, 1 packets/s Ten minute rate, 125 bits/s, 1 packets/s Vlan Type DMA Channel Method 1 ethernet 1 auto 2 ethernet 0 auto Inband IPC (status running) Pending messages, 0 queued, 0 awaiting acknowledgment Vlan0 is up, line protocol is up Hardware is Cat5k Virtual Ethernet, address is 00e0.1e91.c6e8 (bia 00e0.1e91.c6e8) Internet address is 127.0.0.4/8 MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:00, output 00:00:00, output hang never Last clearing of "show interface" counters never Queueing strategy: fifo Output queue 0/40, 0 drops; input queue 0/75, 0 drops 5 minute input rate 0 bits/sec, 1 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 53 packets input, 3186 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored RSM#
```

この出力結果から、任意の VLAN インターフェイスがどの DMA チャネルに割り当てられているかがわかります。 1.を必要ならばチャネリングするために VLAN がリンクされる一方奇数の VLAN がインターフェイスコンフィギュレーションコマンド dma **チャネル**を使用してハードにこの対応をコードできる 0 をチャネリングすることを行くことがわかります。 この例に DMA チャネル 0 に RSM のインターフェイス VLAN1 を割り当てる方法を示されています:

```
RSM# show controllers c5ip
!--- Output suppressed. Vlan Type DMA Channel Method 1 ethernet 1 auto 2 ethernet 0 auto !--- Output suppressed. RSM# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RSM(config)# interface vlan 1
RSM(config-if)# dma-channel 0
RSM(config-if)# ^Z
RSM#
RSM# show controllers c5ip
!--- Output suppressed. Vlan Type DMA Channel Method 1 ethernet 0 configured 2 ethernet 0 auto
!--- Output suppressed.
```

VLAN0 の情報

VLAN0 の主な目的はスイッチの Supervisor Engine へ有効な通信を確認することです。 VLAN0 は隠されたインターフェイスであるため、単純な show interface vlan0 コマンドを使用してこれに関する統計情報を表示することはできません。

VLAN 間ルーティング よくある 問題

RSM Autostate 機能の使用

ブリッジングで頻発する問題は、切断されたリンクが L2 ネットワークを容易に 2 つの断片に分割できてしまうことです。 この状況はあらゆる価格で非近接 ネットワークがルーティングを壊す

ので陥らないようにする必要があります。（これは通常冗長リンクの展開によって実現します。）

スイッチ 2 で接続されるクライアントがスイッチ 1 で接続されるサーバと通信するこの例を参照して下さい、:

クライアントからサーバへのトラフィックだけを考察します。 VLAN3 では、クライアントからの着信トラフィックは RSM2 によってルートされます。RSM2 は、インターフェイス VLAN2 を経由してサーバのサブネットに直接接続できます。 紫色の矢印は、経路を示しています。

スイッチ 1 とスイッチ 2 の間の VLAN1 用のリンクが切断されたと仮定します。 ここの主要な問題は、RSM2 の視点から、何もネットワークで変更しなかったことです。 RSM2 には依然として VLAN1 に直接接続されたインターフェイスがあり、このパスを通じてクライアントからサーバにトラフィックを転送し続けています。 トラフィックはスイッチ 2 で損失され、クライアントとサーバ間の接続は切断されます。

RSM Autostate 機能は、この問題に対処するために設計されたものです。 スイッチの特定の VLAN 用にアップしたポートがない場合、RSM の対応する VLAN インターフェイスがダウンします。

例の場合には、スイッチ 1 とスイッチ 2 間の VLAN のリンクが失敗するとき、スイッチ 2 の VLAN1 の唯一のポートはダウン状態になっています（リンク）。 RSM Autostate 機能は、RSM2 のインターフェイス VLAN1 をディセーブルします。 インターフェイス VLAN1 がダウンしているので、RSM2 はルーティング プロトコルをこのダイアグラムに示すように別のインターフェイスによってサーバおよび結局順方向にトラフィックに、宛てたパケットのための別のパスを見つけ出すのに使用できます:

RSM autostate は VLAN に他のポート アップがない場合その時だけはたらきます。 たとえば定義されたインターフェイス VLAN1 が付いているシャーシの 2 を切り替えるために接続された VLAN1 で他のクライアントがあったらまたは RSM インターフェイス VLAN1 は無効ではないですスイッチ 1 とスイッチ 2 間のリンクが失敗した場合。 したがって、トラフィックは再び混乱します。

RSM Autostate 機能はデフォルトでイネーブルにされています。 もし必要なら、それは Supervisor Engine の set rsmautostate コマンドを使用して手動でディセーブルにすることができます:

```
sup> (enable) show rsmautostate
RSM Auto port state: enabled
sup> (enable) set rsmautostate disable
sup> (enable) show rsmautostate
RSM Auto port state: disabled
```

フォールバック ブリッジング

フォールバックブリッジングは VLAN 間のブリッジングプロトコルでいくつかの他をルーティングしている間構成されています。 可能であれば、この種の設定は避けて、一時的なマイグレーションの期間にのみ使用してください。 通常、これは別の VLAN の異なる IP サブネットのネットワークを、それぞれセグメント化したが、いくつかの古いルーティング 不可能なプロトコル（ローカルエリア転送[LAT]繋ぎ続けたいと思う時必要たとえばです）。 このような場合は、RSM を IP 用のルータとして、ただしその他のプロトコルに対してはブリッジとして使用する必要があります。 これは、IP アドレスはそのままにして、RSM インターフェイスにブリッジングを設定するだけでできます。 次の例では、フォールバック ブリッジングを使用した非常に単純なネットワ

ークと、この種の設定で最も一般的な問題を説明します。

この非常に単純なネットワークは、異なる 2 つの IP サブネットに対応する 2 つの VLAN で構成されています。 ある特定の VLAN のホストはデフォルト ゲートウェイ（また更に両方として Hot Standby Router Protocol [HSRP]を使用して）の 2 RSM 使用、他の VLAN のホストとこうして通信できます。 ネットワークは以下のようになります：

また、両方の RSM は、各自のインターフェイス間（VLAN1 と VLAN2）のその他のプロトコルをブリッジするように設定されています。 LAT サービスを提供するホストおよびそれらを使用しているクライアントがあることを仮定して下さい。 ネットワークはこのようになります:

このダイアグラムに関しては、各 Catalyst は 2 つの異なるブリッジ（各 VLAN のための 1）に分割されます。 2 VLAN の間のブリッジングが 2 VLAN の合併という結果に終ったことがわかります。 ブリッジドプロトコルに関する限りでは、1 VLAN がありただ、LAT サーバおよびクライアントは直接通信できます。 当然、これはまたネットワークでループがあること、そして STP が 1 つのポートをブロックしなければならないことを意味します。

図を見てわかるとおり、問題はこのポートのブロッキング ポートから発生します。 スイッチは純粋な L2 デバイスで、IP と LATトラフィックを区別できません。 それ故に、スイッチ 2 が 1 つのポートをブロックすれば、次上記のダイアグラム、すべてのトラフィックの種類を（IP、LAT、または他）ブロックします。 このような理由で、このようにネットワークな:

VLAN2 は 2 人の部に分割され、隣接しないサブネット 10.2.0.0 があります。 この設定では、ホスト 10.2.0.10 は、同じサブネットおよび VLAN 上にあるにもかかわらずホスト 10.2.0.20 に通信できません。

解決策は、ブロックされたポートを L2 トラフィックと L3 トラフィックを区別できる唯一のデバイスに移動させることです。 そのデバイスが RSM です。 これを行う方法には主に次の 2 つがあります。

- **STP パラメータのチューニング：** RSM1 か RSM2 にように、結局、ブロッキング状態のポートいます 1 つのまたは複数のデバイスのコストを増加する必要があります。 この方式にはあまり柔軟性がないため、STP 設定は非常に厳密になることを意味します。 スイッチを追加するによりまたはリンクの帯域幅を変更することは（Fast EtherChannel またはギガビットイーサネット（802.3z））調整の完全な修正作業を引き起こすかもしれません。
- **RSM で別のスパニングツリー アルゴリズム（STA）を使用：** スイッチは IEEE STA だけを実行し、DEC STP に対して完全に透過的です。 両方の RSM の DEC STP を設定する場合、それらは直接接続された、それらの 1 つはブロックしますようにはたらき。 このダイアグラムはこれを説明します:

一時的なブラック ホール（ST コンバージェンス）

障害時にネットワークの再構成の速度をテストするお客様は、STP に関する設定問題に対処する場合が頻繁にあります。 次に示すネットワークで、クライアントは異なる 2 つのパスを経由してサーバにアクセスしています。 デフォルトにより、クライアントからサーバへのトラフィックは、RSM2 によってインターフェイス VLAN2 経由でルーティングされます。

ユーザはテストを実行するために、スイッチ 2 とスイッチ 3 の間のリンクを切断します。対応するポートは即時ダウンし、RSM Autostate 機能によって RSM2 上のインターフェイス VLAN2 はダウンします。 このサーバの直接接続されたルートは、RSM2 のルーティング テーブルから消去されます。そしてこのテーブルはすぐに RSM1 経由で新しいルートを学習します。 Open

Shortest Path First（OSPF）または拡張内部ゲートウェイ ルーティング プロトコル（EIGRP）のような効率的なルーティング プロトコルによって、統合はこのオペレーションの間にほとんど ping を失わないほどファーストです。

障害が発生した場合、2 つのパス（黄色の VLAN2 と緑色の VLAN3）間の切り替えは即時です。ユーザがスイッチ 2 間のリンクを再確立し、スイッチ 3、しかし、クライアントは約 30 秒のサーバに接続切断を経験します。

この理由も STA に関連しています。 STA の実行時には、新しく接続されたポートはまずリスニング段階とラーニング段階に入り、その後で最終的なフォワーディング モードになります。 最初の 2 つの 15 第 2 ステージの間に、ポートは稼働していますが、トラフィックを送信しません。これはリンクが接続されるとすぐ、RSM autostate 機能はすぐに RSM2 のインターフェイス VLAN2 を再び有効にする、トラフィックはスイッチ 2 およびスイッチ 3 範囲の間で転送ステージまでリンクのポート行くことができませんことを意味します。 これは、クライアントとサーバ間の一時接続が失われることの説明です。 スイッチ 1 とスイッチ 2 の間のリンクがトランクでない場合は、PortFast 機能をイネーブルにしてリスニング段階とラーニング段階をとばし、ただちにコンバージすることができます。

注: PortFast はトランク ポートでは動作しません。 詳細は、『PortFast と他のコマンドを使用したワークステーションの接続始動遅延の修復』を参照してください。

結論

この資料はいくつかの RSM 特有の問題に焦点を合わせます、また非常によくある VLAN 間ルーティングは発行します。 この情報はすべての正常な Cisco IOS ルータ トラブルシューティング手順が試みられたらだけ役立ちます。 RSM によってルーティングされる間違ったルーティング テーブルが理由でパケットの半分が失われる場合、DMA チャネル統計情報を解読することを試みるのを助けません。 一般の VLAN 間ルーティング問題は高度なトピックで、頻繁に発生しません。 大半の場合、RSM（またはスイッチ内に組み込まれたその他のルーティング デバイス）を単純な外部 Cisco IOS ルータと考えれば、スイッチ環境でのルーティング問題のトラブルシューティングは十分に可能です。

関連情報

- IP ルーティング プロトコルに関するサポート ページ
- IP マルチレイヤ スイッチングのトラブルシューティング
- InterVLAN ルーティングの設定
- PortFast と他のコマンドを使用したワークステーションの接続始動遅延の修復
- 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
- テクニカル サポートとドキュメント – Cisco Systems