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

内容

概要

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**:このドキュメントでは、RSMアーキテクチャを紹介し、追跡する追加のRSM関連カウンタの詳細を説明します。
- **VLAN間設定固有の問題**（主にルータとスイッチ間のインタラクションに関連）:これは、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)、ルートスイッチフィーチャカード(RSFC)、8510CSRなど)にも適用され、多くの場合、外部ルータにも適用されます。

注：このドキュメントでは、Catalyst 4000、5000、および6000スイッチでのインターVLANルーティングの設定については説明しません。詳細については、次のドキュメントを参照してくださ

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のインストールと設定ノート』の「インターVLANルーティング用モジュールの設定」セクション
- 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）を使用したインター VLAN ルーティングの設定

このドキュメントでは、基本的なルーティングプロトコルのトラブルシューティング、またはマルチレイヤスイッチング(MLS)関連の問題については説明しません。

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。

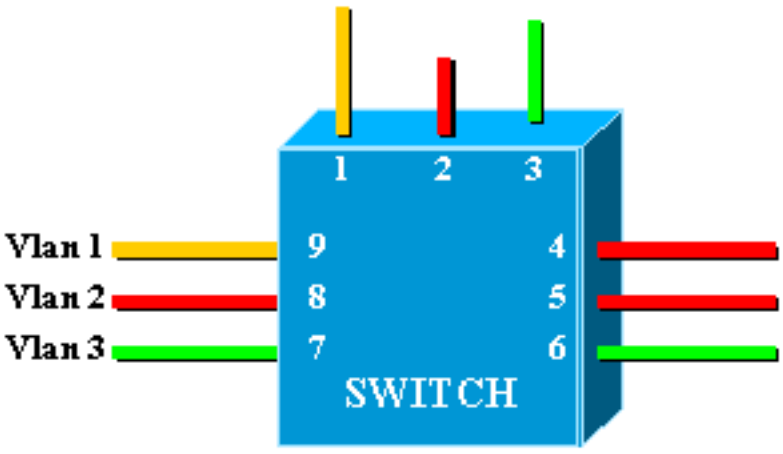
表記法

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。

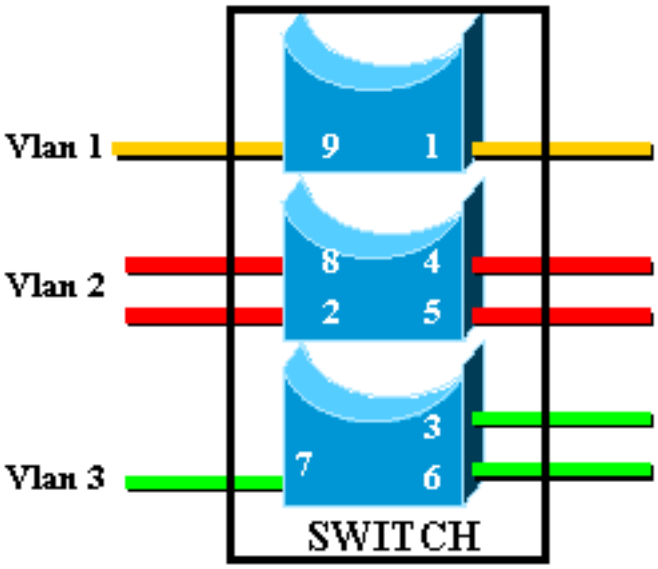
VLAN間ルーティングとは

VLAN間ルーティングについて説明する前に、このドキュメントではVLANの概念に焦点を当てています。これは、VLANの必要性に関する理論的な説明ではなく、単にVLANがスイッチでどのように動作するかについて説明します。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。

次の図は、9つのポートが3つの異なるVLANに割り当てられているスイッチを示しています。



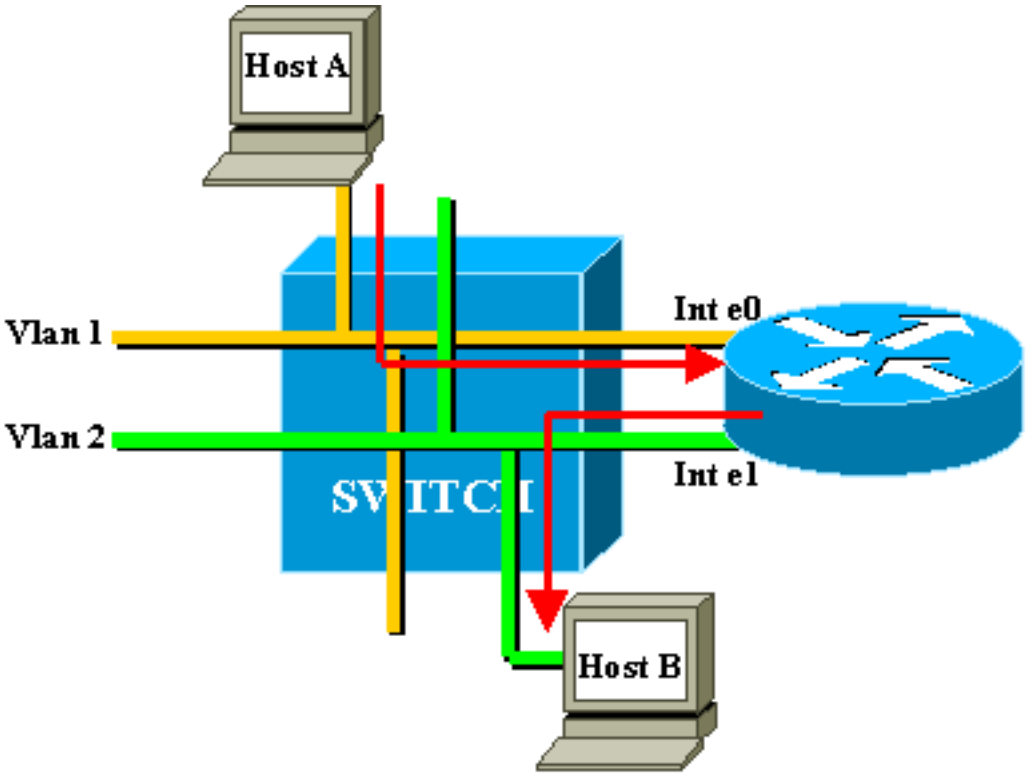
これは、次の3つの独立したブリッジで構成されるネットワークとまったく同じです。



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は個別のスパニングツリープロトコル(STP)インスタンスを作成するため、STPは3つの異なる転送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、ポート1をポート4に接続した場合は、VLAN1をVLAN2にマージするだけです。この場合、2つのVLANを別々に設定する理由はありません。

VLAN間で必要な唯一の接続は、ルータによってレイヤ3(L3)で実現されます。これはVLAN間ルーティングです。図をさらに簡素化するために、VLANは異なる物理イーサネットセグメントとして表されます。スイッチが提供する特定のブリッジング機能に特に関心がないためです。



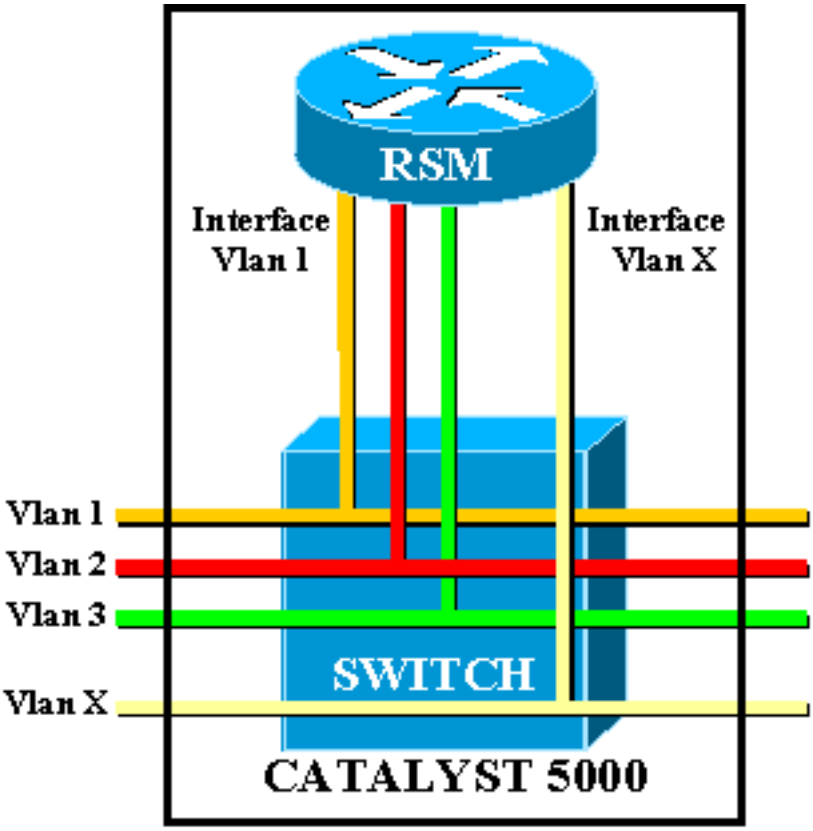
この図では、2つのVLANは2つの異なるイーサネットセグメントと見なされます。VLAN間トラフィックは、外部ルータを通過する必要があります。ホストAがホストBと通信する場合、通常はルータをデフォルトゲートウェイとして使用します。

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。

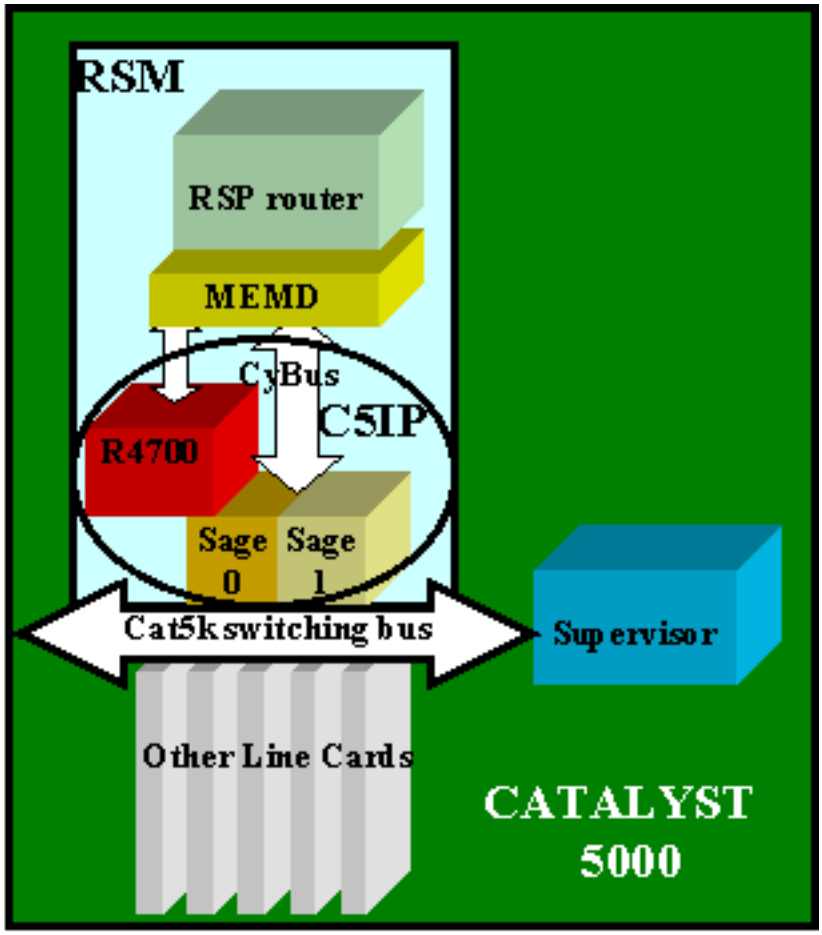
これらのインターフェイスは、イーサネットインターフェイスと呼ばれるのではなく、接続先のVLANに従って名前が付けられます。（インターフェイスVLAN1はVLAN1に直接接続されている、など）。



実装アーキテクチャ

RSMは、Catalyst 5000ラインカード内部のCisco 7500ルートスイッチプロセッサ(RSP)ルータです。カードの設定とトラブルシューティングを行うために、カードのアーキテクチャに関する知識は必要ありません。ただし、RSMの構築方法を理解しておくと、通常の外部ルータとの違いを理解するのに役立ちます。この知識は、**show controller c5ipコマンドを導入する際に特に重要です**。

次の図は、RSMラインカードの主要コンポーネントを示しています。

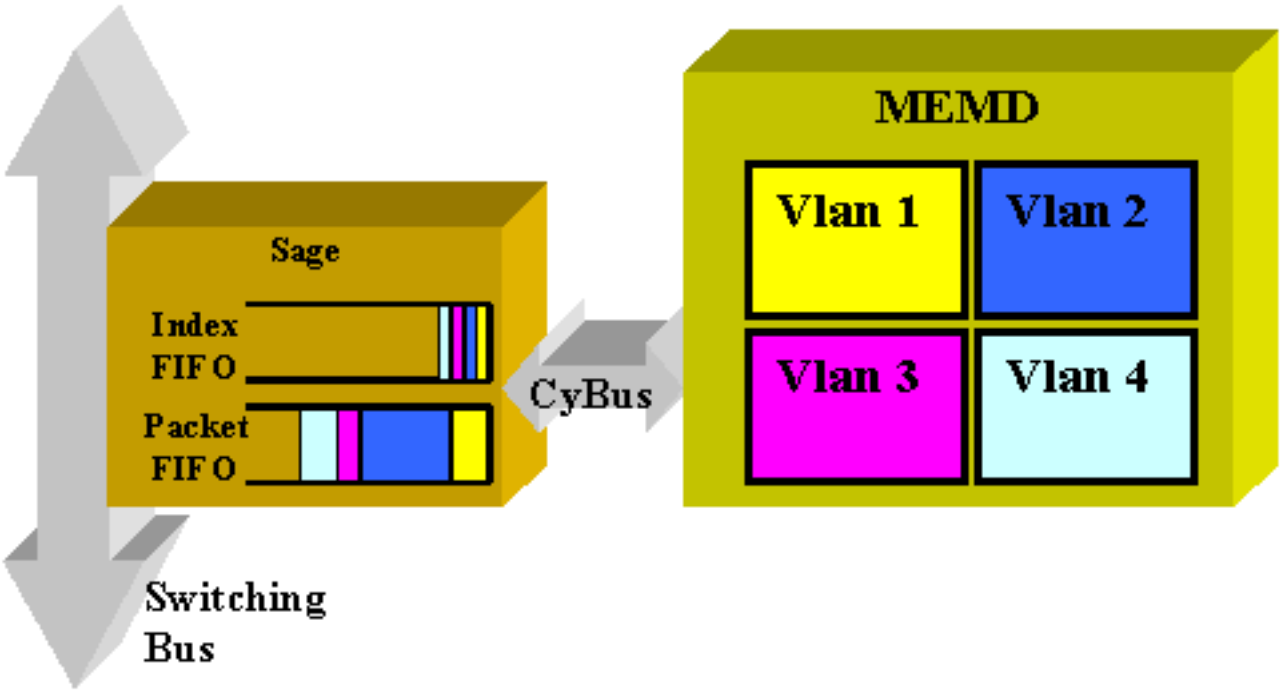


Catalyst 5000 インターフェイス プロセッサ

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。パケットとインデックスは、最初にSAGE内の2つの異なるFIFOに格納されます。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の通信に並行して動作する2つのSAGEは、パケット配信の順序が正しくないことがあります。 (たとえば、SAGE0で受信した大きなパケットは、後でSAGE1で受信した小さなパケットの後に送信できます)。 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。これは起動時に自動的に行われます。 (ルータによると、VLANは2つのDMAチャネルの1つに関連付けられ、それぞれがSAGEに接続されます)。 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、無効またはシャットダウンされても、共有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固有のトラブルシューティング

通常のCisco IOS®ルータに関するドキュメントでは扱っていないRSM固有の主な問題は、RSMへのアクセスに関する問題と、パフォーマンスの問題です。

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

- スイッチスーパーバイザからRSMへのセッションイン
- 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を実行してイネーブルアクセスを取得するには、vtyにパスワードを割り当てる必要があります。

次の例は、スーパーバイザエンジンからRSMへのTelnetセッションを示しています。VLAN1のIPアドレスは10.0.0.1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。

スイッチスーパーバイザからRSMへのセッションイン

スーパーバイザエンジンから*session x*コマンドを使用して、スロットxのRSMに接続します。

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：今回は、vtyおよびイネーブルパスワードがRSMに完全にアクセスするために設定内にある必要はありません。

```
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#
```

スーパーバイザエンジンのコマンドshow moduleを使用して、スイッチにRSMが取り付けられているスロットを識別します。sessionコマンドを使用して、直接アクセスできます。

直接コンソール接続

RSMのシステムコンソールポートは、データ端末を接続するためのDB-25レセプタクルDCEポートで、システムの設定と通信が可能です。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。

コンソールポートに接続する前に、使用する端末のボーレートを確認するために、端末のマニュアルを参照してください。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。 ターミナルを次のように設定します。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の状態を確認します。CPU Halt LED is OFF：システムがプロセッサハードウェアの障害を検出しました。オレンジ色のSTATUS LED：モジュールが無効、テスト中、またはシステムのブート中。
- スーパーバイザエンジンをチェックして、スイッチでRSMが認識できるかどうかを確認します。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。ご覧のように、セッションとTelnetアクセスの両方がRSMへのIP接続に依存しています。たとえば、RSMがブート中またはROMMONモードでスタックしている場合、Telnetやセッションを実行することはできません。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に関連するパフォーマンスの問題のほとんどは、通常のCisco IOSルータとまったく同じ方法でトラブルシューティングできます。このセクションでは、C5IPであるRSM実装の特定の部分に焦点を当てています。コマンド**show controller c5ip**は、C5IPの動作に関する情報を提供できます。次の出力は、最も重要なフィールドの一部を示しています。

```
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#
```

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、トラフィックを大量に消費するすべてのVLANが同じDMAチャネルに割り当てられている場合に発生する可能性があります。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が受信したがドロップ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**:RSMによって不正なCRCが検出されると、巡回冗長周期(CRC)エラーが発生します。バックプレーンに不正なCRCを持つパケットが存在してはなりません。これらのパケットを検出したRSMは、ラインカードやその他のバックプレーンに接続されたデバイスが正しく動作していないことを示しています。**注：CRCエラー**は、ISLトランク経由で接続されたリモートデバイスからも発生する可能性があります。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**：インデックスが正確でない場合にインデックスエラーが発生します。C5IPはこのパケットを受信した理由を認識していません。索引エラーによって dropped カウンタも増分されます。
- **dmac-length**：このエラーは、C5IPインターフェイスがSAGE ASICが最大伝送ユニット(MTU)サイズを超過するのを防いだ場合に発生します。このサイズが未検出の場合は、ルータの共有メモリが破損します。
- **dmac-synch**:SAGE ASICがパケットをドロップすると、パケットのFIFOとインデックスのFIFOが同期しなくなります。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。この問題が発生する可能性は低いですが、発生する場合はパフォ

ーマンスへの影響が非常に低くなります。

- **dmac-timeout**：このカウンタは、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。これはハードウェアの障害を示しており、このカウンタに0以外の値が示されているRSMは交換に適しています。
- **ignore**：ルータが入力パケットのMEMDバッファを使い果たした場合、無視されます。これは、CPUがパケットの受信速度よりも速くパケットを処理していない場合に発生します。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。
- **line-down**:line-downは、回線プロトコルダウンVLAN宛てのパケットがドロップされたことを示します。C5IPは、ダウンしていると思われるVLANインターフェイスのパケットを受信しました。スイッチはダウンしているRSMインターフェイスへのパケットの転送を停止する必要があるため、これは発生しません。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。
- **runt/giant：このカウンタは無効なサイズのパケットを追跡します。**
- **unicast-flood**：ユニキャストフラッドパケットは、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もこれらのパケットを受信しますが、そのVLANでブリッジングするように設定されていない限り、自身のMACアドレスに一致しないパケットには関心がありません。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。
- **Last drop**：このカウンタは、最後にドロップされたパケットに関する特定の情報を示します。これは、このドキュメントの範囲外の低レベルの情報です。

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。

```
Vlan Type DMA Channel Method
1 ethernet 1 auto
2 ethernet 0 auto
3 ethernet 1 auto
4 ethernet 0 auto
5 ethernet 1 auto
6 ethernet 0 auto
7 ethernet 1 auto
8 ethernet 0 auto
9 ethernet 1 auto
10 ethernet 0 auto
```

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。奇数のVLANはチャネル0に移動し、偶数のVLANはチャネル1にリンクされていることがわかります。必要に応じて、インターフェイスコンフィギュレーションコマンド**dma-channelを使用して、この対応をハードコードできます。**次の例は、RSMのインターフェイスVLAN1をDMAチャネル0に割り当てる方法を示しています。

```
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

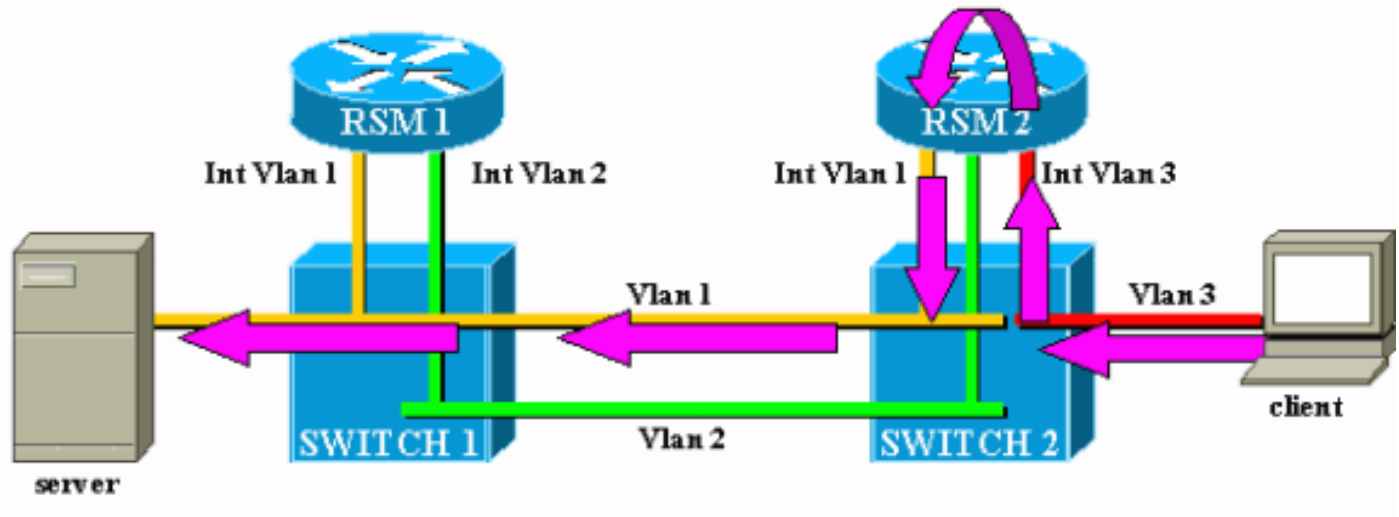
VLAN0の主な目的は、スイッチのスーパーバイザエンジンへの効果的な通信を確保することです。VLAN0 は隠されたインターフェイスであるため、単純な show interface vlan0 コマンドを使用してこれに関する統計情報を表示することはできません。

VLAN間ルーティングの一般的な問題

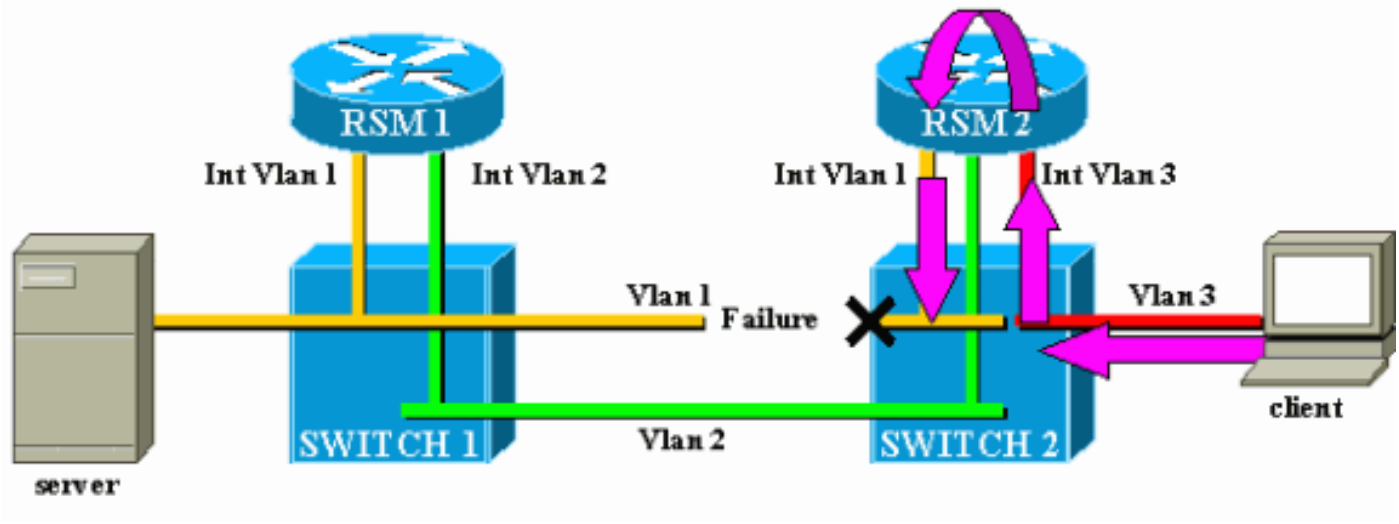
RSM Autostate 機能の使用

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。不連続ネットワークがルーティングを切断するため、この状況は任意の価格で回避する必要があります。（これは通常、冗長リンクを展開することによって実現されます）。

スイッチ2に接続されたクライアントがスイッチ1に接続されたサーバと通信する例を次に示します。



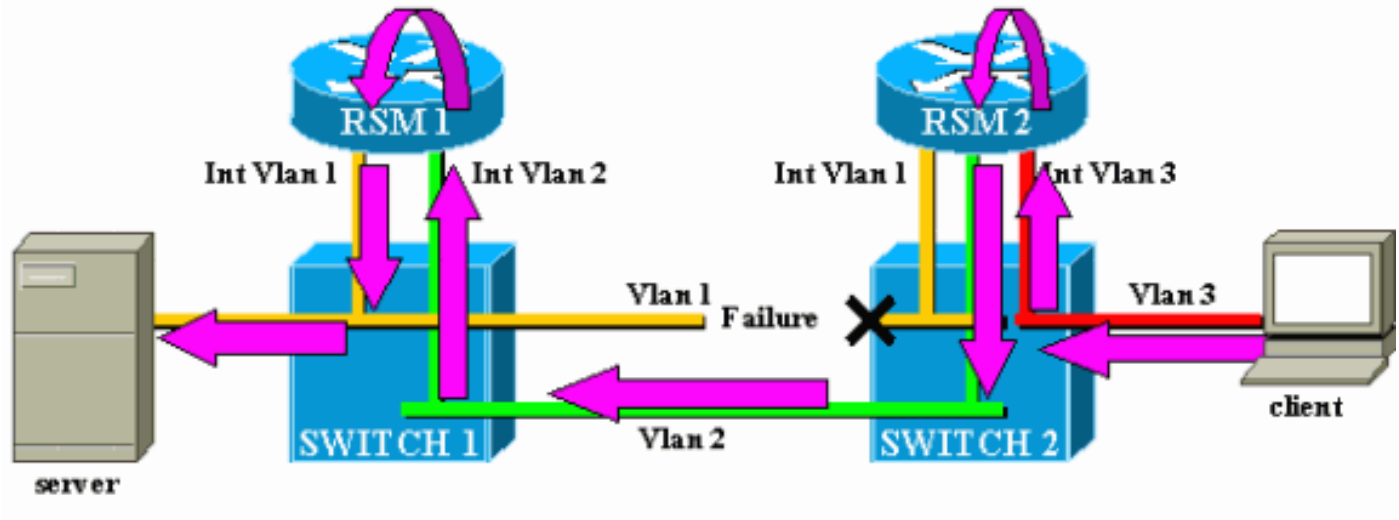
クライアントからサーバへのトラフィックだけを考察します。VLAN3のクライアントからの着信トラフィックはRSM2によってルーティングされます。RSM2は、インターフェイスVLAN2経由でサーバのサブネットに直接接続されています。紫色の矢印は、次のパスを表します。



スイッチ1とスイッチ2の間のリンクがVLAN1に対して壊れていると仮定します。ここでの主な問題は、RSM2の観点から見ると、ネットワークで何も変更されていないことです。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。

この例では、スイッチ1とスイッチ2の間のVLAN内のリンクに障害が発生すると、スイッチ2のVLAN1内の唯一のポートがダウンします（リンクダウン）。 RSM autostate機能は、RSM2のインターフェイスVLAN1を無効にします。インターフェイスVLAN1がダウンした場合、RSM2はルーティングプロトコルを使用して、サーバ宛のパケットに別のパスを見つけ、最終的には別のインターフェイスを介してトラフィックを転送できます。



RSM autostateは、VLAN内に他のポートがアップしていない場合にのみ動作します。たとえば、VLAN1内の別のクライアントがスイッチ2に接続されている場合、またはインターフェイスVLAN1が定義されたシャーシ内のRSMがある場合、スイッチ1とスイッチ2の間のリンクに障害が発生しても、インターフェイスVLAN1は無効になりません。したがって、トラフィックは再び混乱します。

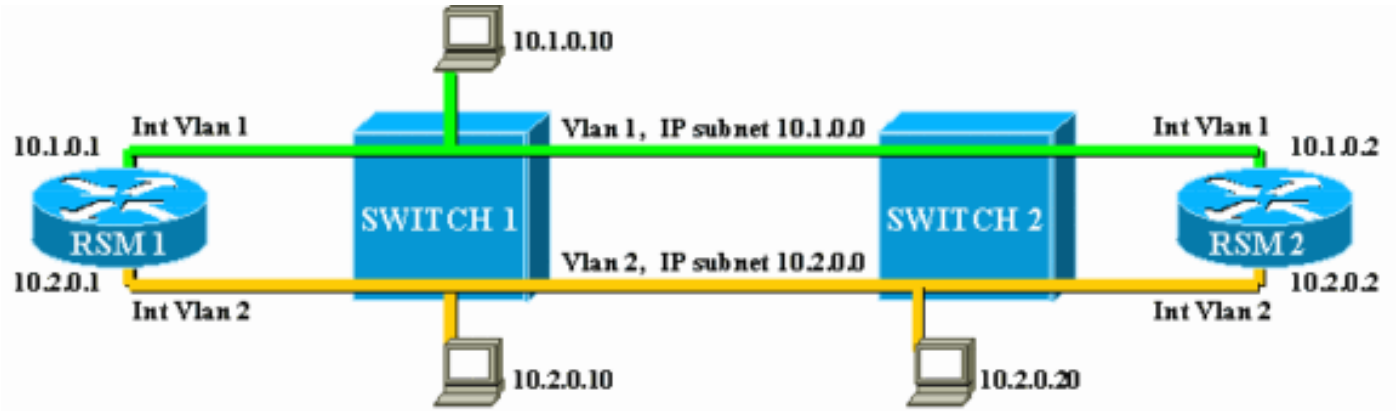
RSM Autostate 機能はデフォルトでイネーブルにされています。必要に応じて、スーパーバイザエンジンでset rsmautostateコマンドを使用して、手動で無効にできます。

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

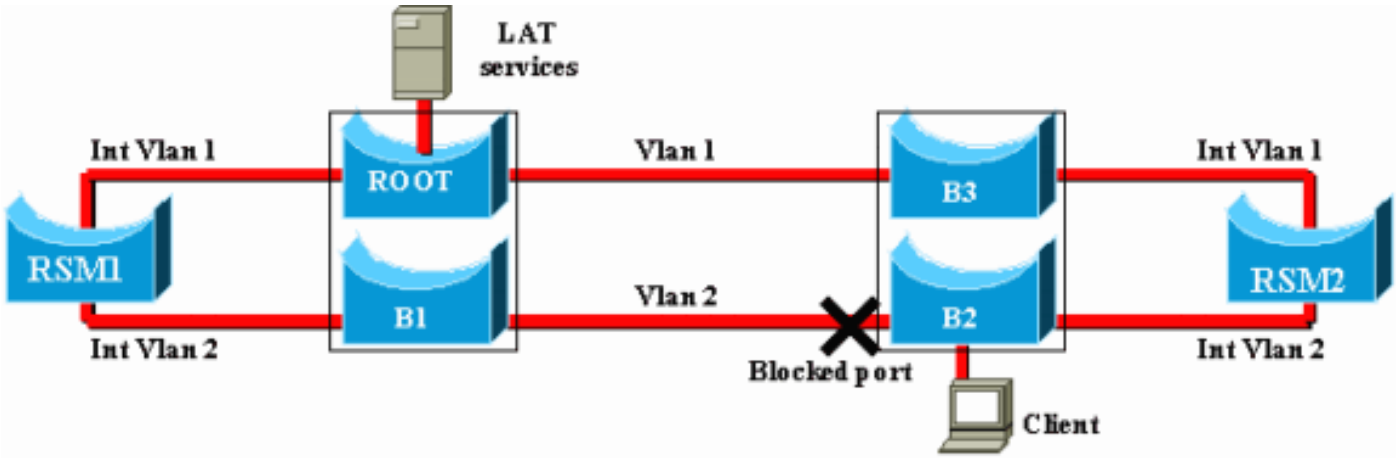
フォールバック ブリッジング

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構成され、その他のプロトコルはルーティングされます。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、異なるVLAN上の異なるIPサブネットを持つネットワークをセグメント化し、古いルーティング不可能なプロトコル(ローカルエリアトランスポート(LAT)など)のブリッジングを継続する場合に必要です。 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。特定のVLAN内のホストは、2つのRSMのいずれかをデフォルトゲートウェイとして使用できます(Hot Standby Router Protocol（HSRP；ホットスタンバイルータプロトコル）を使用して両方とも使用できます)。ネットワークは以下のようになります：



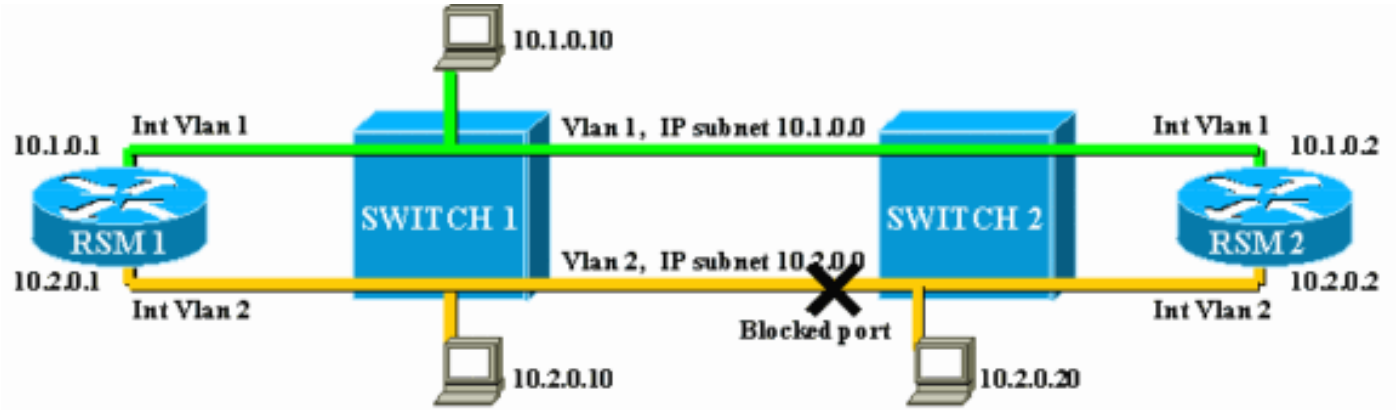
両方のRSMも、インターフェイスVLAN1とVLAN2の間で他のプロトコルをブリッジするように設定されています。LATサービスを提供するホストとそれらを使用するクライアントがあるとします。ネットワークは次のようになります。



この図では、各Catalystが2つの異なるブリッジ（VLANごとに1つ）に分割されています。 2つのVLAN間のブリッジングにより、2つのVLANが統合されていることがわかります。ブリッジプロ

トコルに関する限り、VLANは1つしかなく、LATサーバとクライアントは直接通信できます。もちろん、これは、ネットワークにループがあり、STPが1つのポートをブロックする必要があることを意味します。

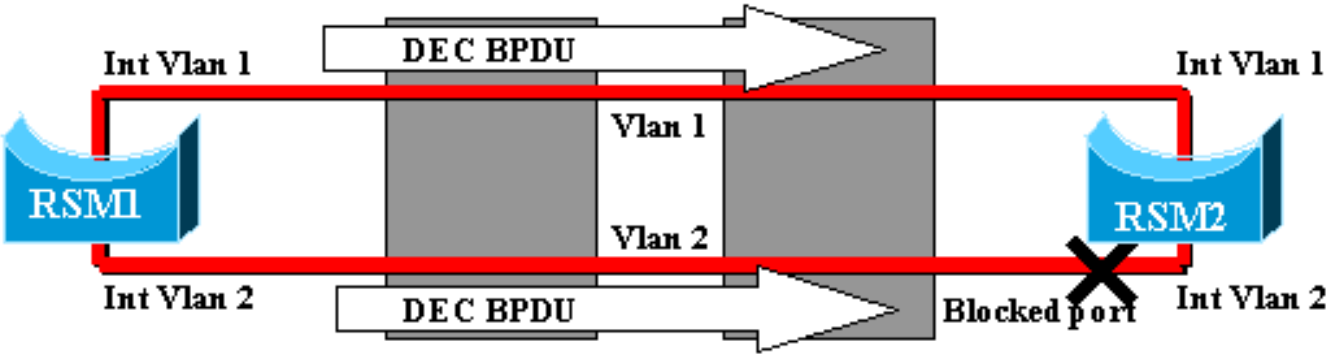
図を見てわかるとおり、問題はこのポートのブロッキング ポートから発生します。スイッチは純粋なL2デバイスであり、IPトラフィックとLATトラフィックを区別できません。したがって、上記の図のように、スイッチ2が1つのポートをブロックすると、すべてのタイプのトラフィック（IP、LAT、またはその他）がブロックされます。 このため、ネットワークは次のようになります。



VLAN2は2つの部分に分割され、不連続のサブネット10.2.0.0が存在します。この設定では、ホスト10.2.0.10は同じサブネットとVLAN上にありますが、ホスト10.2.0.20と通信できません。

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。

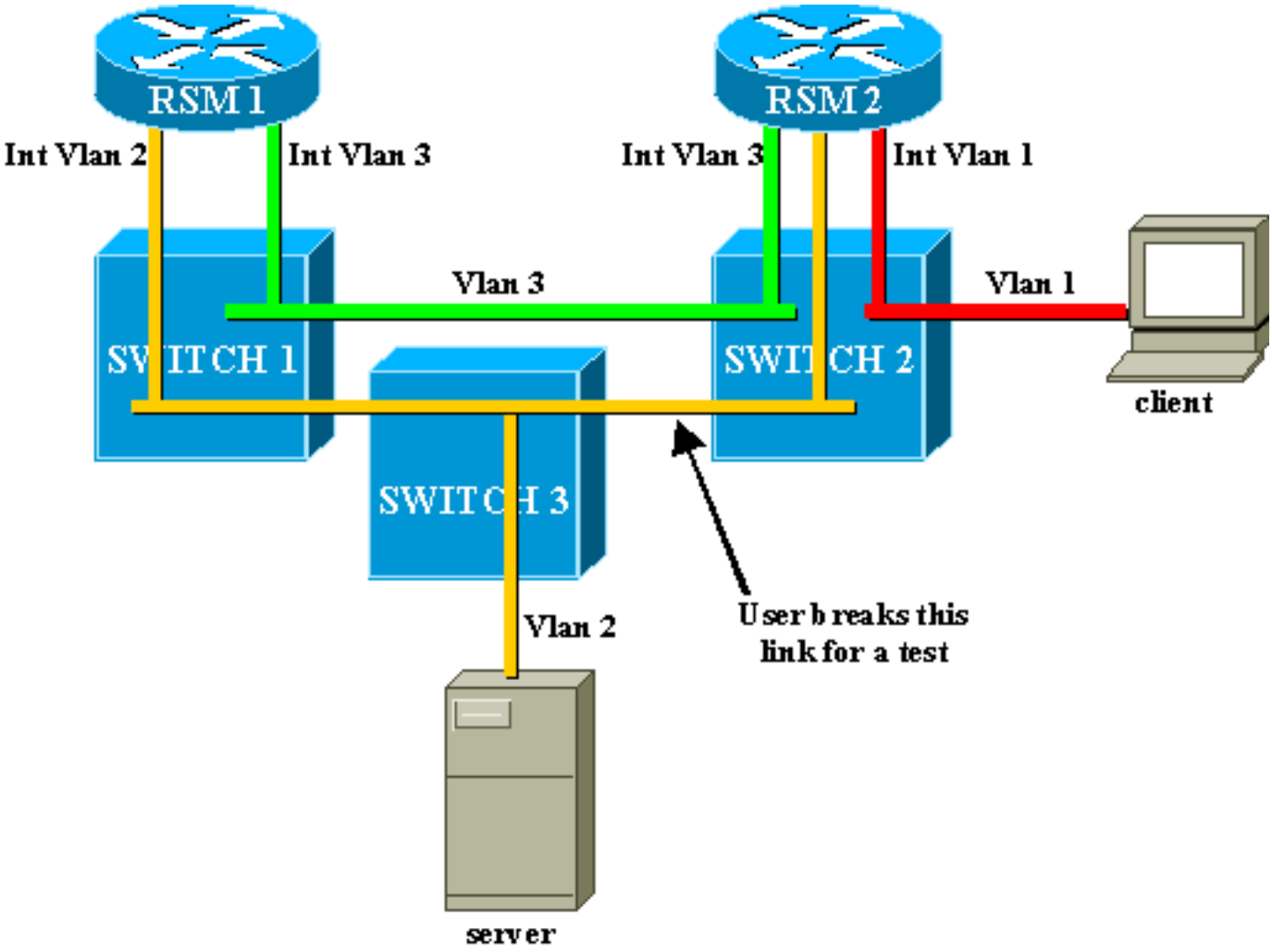
- **STP パラメータのチューニング**：最終的にブロッキングポートがRSM1またはRSM2に配置されるように、1つまたは複数のデバイスのコストを増やす必要があります。この方法は柔軟性が低く、非常に厳密なSTP設定を意味します。スイッチを追加したり、リンクの帯域幅を変更したりすると（Fast EtherChannelまたはギガビットイーサネット）、チューニングが完全に変更されることがあります。
- **RSM で別のスパニングツリー アルゴリズム（STA）を使用**：スイッチはIEEE STAのみを実行し、DEC STPに対して完全に透過的です。両方のRSMでDEC STPを設定すると、それらが直接接続されているかのように動作し、そのうちの1つがブロックされます。次の図に、これを示します。



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。



テストを実行するために、ユーザはスイッチ2とスイッチ3の間のリンクを切断します。対応するポートがダウンし、RSM autostate機能によってRSM2のインターフェイスVLAN2がダウンします。サーバに直接接続されたルートは、RSM1経由で新しいルートを学習します。 ospf)またはEnhanced Interior Gateway Routing Protocol(EIGRP)では、コンバージェンスが非常に高速であるため、この操作中にpingが失われにくくなります。

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。ただし、ユーザがスイッチ2とスイッチ3の間のリンクを再確立すると、クライアントは約30秒間、サーバへの接続を失います。

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秒の段階では、ポートはアップしていますが、トラフィックは送信しません。これは、リンクが接続されるとすぐに、RSM autostate機能がRSM2のインターフェイスVLAN2を再度有効にしますが、スイッチ2とスイッチ3の間のリンク上のポートがフォワーディングステージに達するまで、トラフィックは通過できないことを意味します。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。詳細については、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 [英語] を参照してください。

結論

このドキュメントでは、RSM固有の問題と、非常に一般的なVLAN間ルーティングの問題について説明します。この情報が役立つのは、通常のCisco IOSルータのトラブルシューティング手順がすべて試行されている場合だけです。RSMによってルーティングされたパケットの半分が、誤ったルーティングテーブルのために失われた場合、DMAチャネルの統計情報を解釈しようとしても役に立ちません。一般的なVLAN間ルーティングの問題でさえ高度なトピックであり、あまり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