Troubleshooting do Módulo Switch de Rota (RSM - Route Switch Module) Catalyst 5000 e Roteamento entre VLANs

Contents

Introduction

Este documento fornece informações sobre como solucionar problemas de roteamento entre VLANs com um Route Switch Module (RSM) em um switch da família Catalyst 5000. Quando se trata de Troubleshoot RSM, a primeira coisa a ser feita é considerá-lo um roteador externo simples. É muito raro um problema específico de RSM estar causando um problema quando o roteamento entre VLANs está relacionado. Portanto, este documento abrange apenas as duas principais áreas em que isso pode ocorrer:

- **Problemas relacionados ao hardware RSM**: Este documento apresenta a arquitetura RSM e fornece detalhes sobre os contadores adicionais relacionados a RSM a serem rastreados.
- **Problemas específicos de configuração entre VLANs** (principalmente relacionados à interação entre roteadores e switches): Isso também se aplica a outros roteadores internos (como o Multilayer Switch Feature Card [MSFC], Route Switch Feature Card [RSFC], 8510CSR e assim por diante), e frequentemente a roteadores externos.

Observação: este documento não abrange a configuração do roteamento entre VLANs em

switches Catalyst 4000, 5000 e 6000. Para obter esses detalhes, consulte estes documentos:

- Configuração e visão geral do módulo do roteador para a família Catalyst 4500/4000 (WS-X4232-L3)
- *Configurando o módulo para roteamento entre VLANs* seção de Nota de instalação e configuração para o Módulo de Serviços da Camada 3 do Catalyst 4000
- Configuração do Roteamento entre VLANs utilizando um Roteador Interno (Placa de Camada 3) em Switches Catalyst 5500/5000 e 6500/6000 que Executam o Software do Sistema do CatOS

Este documento não aborda a solução básica de problemas de protocolo de roteamento ou de comutação multicamada (MLS).

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

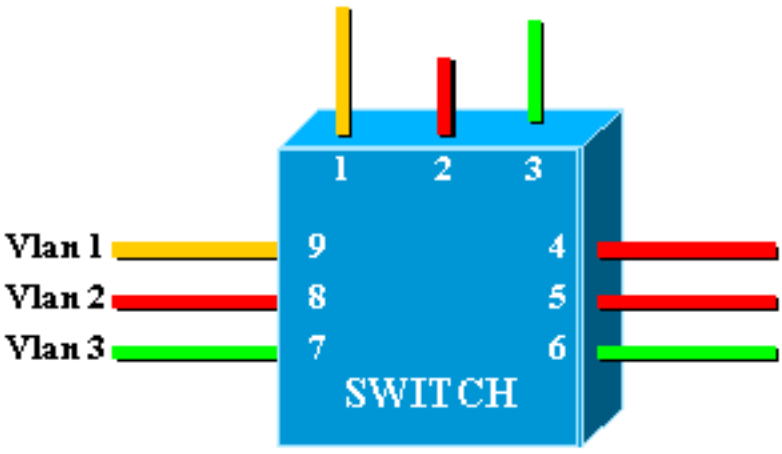
Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

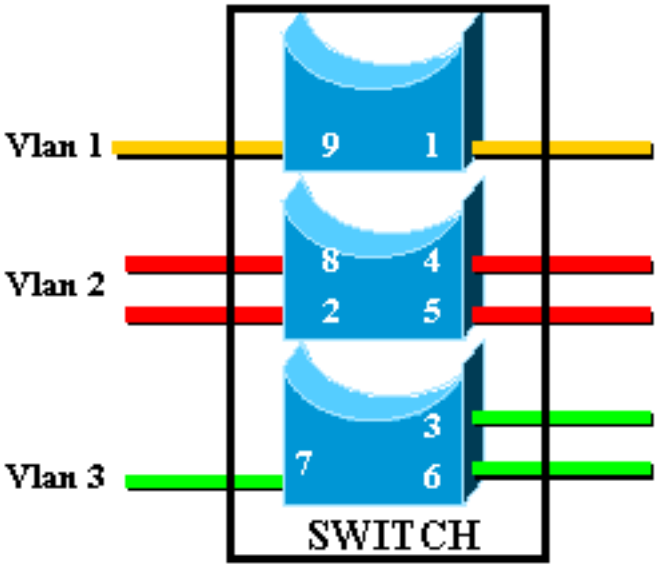
O que é roteamento entre VLANs?

Antes de discutir o roteamento entre VLANs, este documento concentra-se no conceito de VLAN. Esta não é uma discussão teórica sobre a necessidade de VLANs, mas simplesmente discute como as VLANs operam em um switch. When you create VLANs on your Switch, it is as though you split your Switch into several virtual bridges, with each one only bridging ports belonging to the same VLAN.

Este diagrama representa um switch com nove portas atribuídas a três VLANs diferentes:



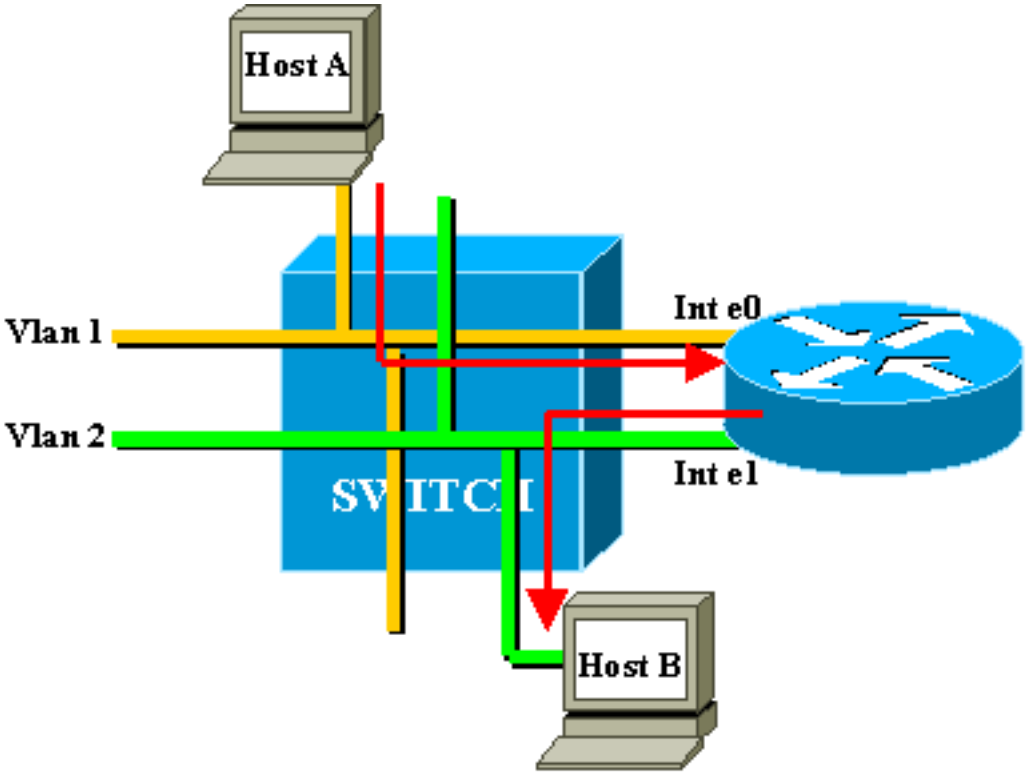
Isso é exatamente equivalente à seguinte rede, que consiste em três pontes independentes:



In the Switch, there are three different bridges, due to each VLAN creating a separate bridge. Como cada VLAN cria uma instância separada do Spanning Tree Protocol (STP), o STP mantém três tabelas de encaminhamento diferentes.

Usando o segundo diagrama, torna-se óbvio que, embora conectadas ao mesmo dispositivo físico, as portas pertencentes a diferentes VLANs não podem se comunicar diretamente na Camada 2 (L2). Mesmo se fosse possível, isto não seria apropriado. Por exemplo, se você conectasse a porta 1 à porta 4, simplesmente mesclaria VLAN1 à VLAN2. Nesse caso, não há motivo para ter duas VLANs diferentes.

A única conectividade que você deseja entre VLANs é obtida na Camada 3 (L3) por um roteador. Esse é o roteamento entre VLANs. Para simplificar ainda mais os diagramas, as VLANs são representadas como diferentes segmentos físicos Ethernet, já que você não está realmente interessado nas funções específicas de bridging fornecidas pelo switch.



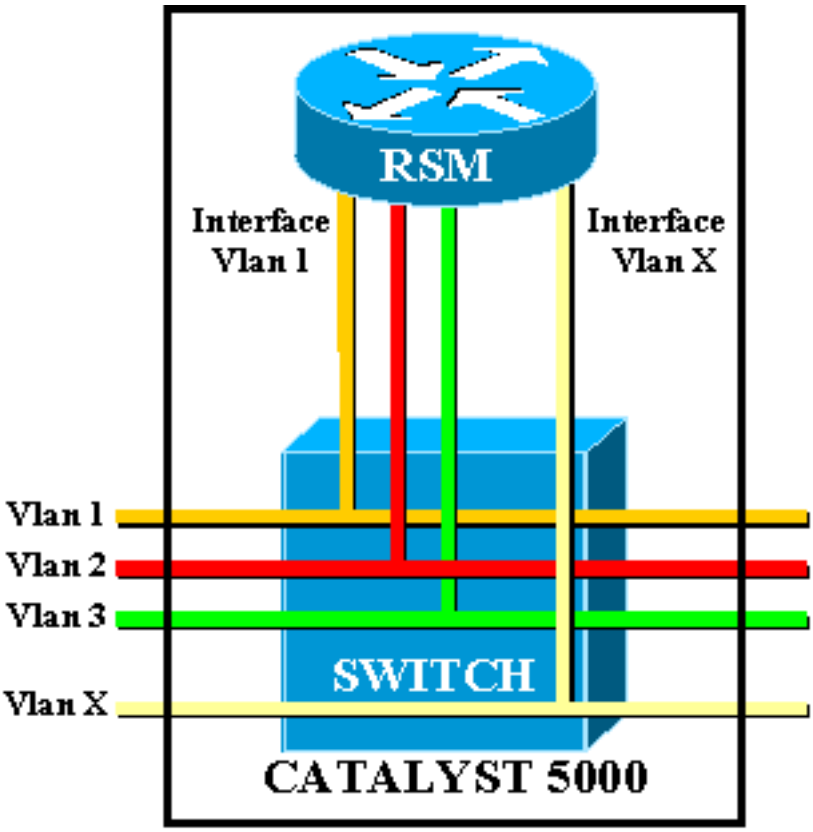
Neste diagrama, as duas VLANs são consideradas como dois segmentos Ethernet diferentes. O tráfego entre VLANs precisa passar pelo roteador externo. Se o host A deseja se comunicar com o host B, ele normalmente usa o roteador como um gateway padrão.

Arquitetura RSM

Arquitetura lógica

Você pode ver um RSM como um roteador externo que tem várias interfaces diretamente conectadas às diferentes VLANs de um switch Catalyst 5000.

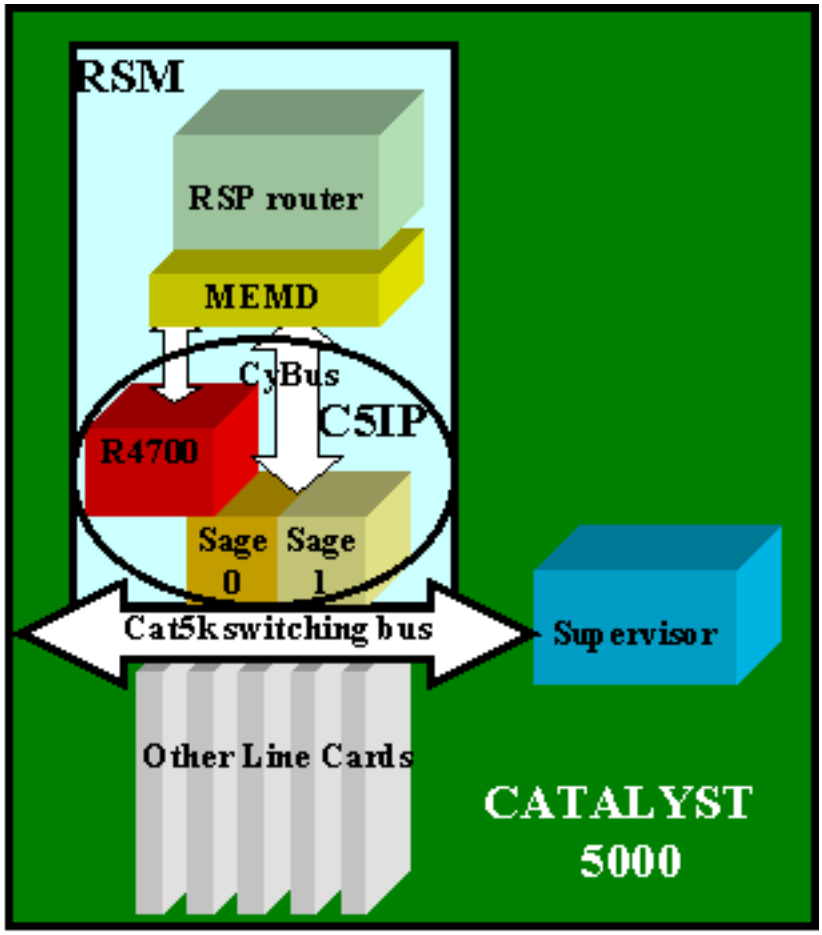
Em vez de serem chamadas de interface Ethernet, essas interfaces são nomeadas de acordo com a VLAN à qual se conectam. (A interface VLAN1 está diretamente conectada à VLAN1 e assim por diante.)



Arquitetura implementada

O RSM é um roteador Cisco 7500 Route Switch Processor (RSP) dentro de uma placa de linha Catalyst 5000. Você não precisa saber muito sobre a arquitetura da placa para configurá-la e solucioná-la. No entanto, ter uma ideia de como o RSM é criado ajuda a entender como ele é diferente de um roteador externo normal. Esse conhecimento é especialmente importante ao apresentar o comando **show controller c5ip**.

Este diagrama localiza os principais componentes na placa de linha RSM:

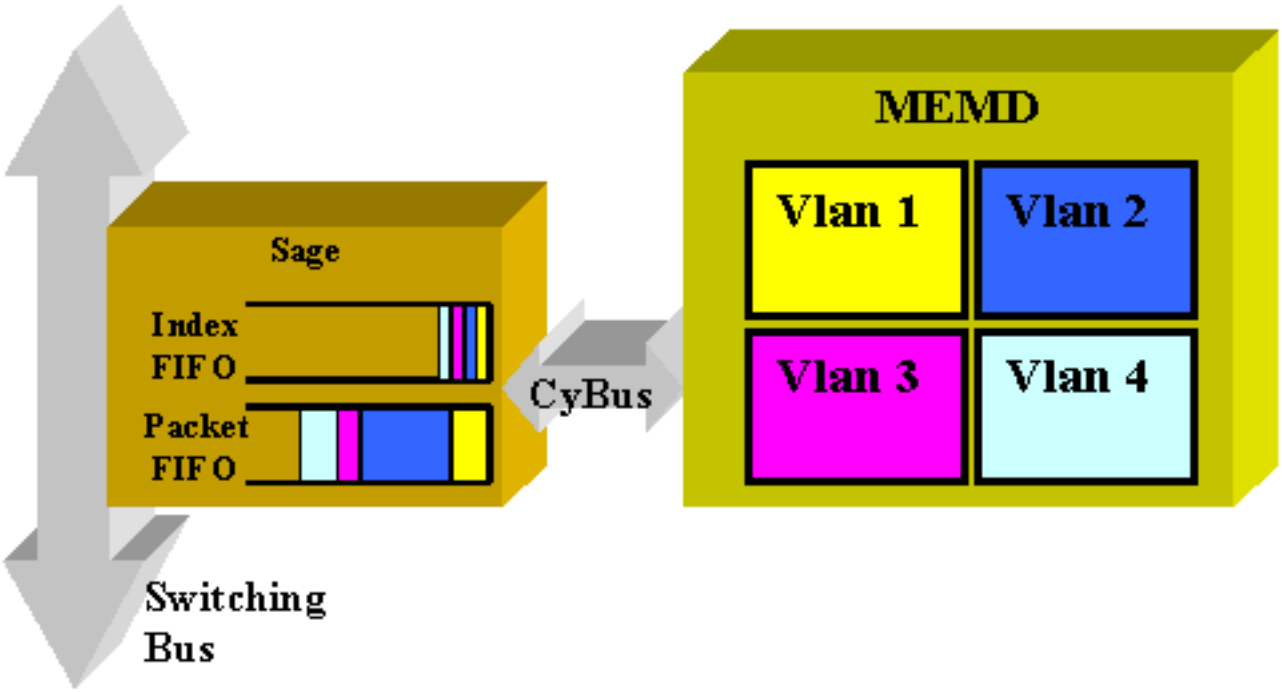


Processador de interface Catalyst 5000

O Processador de Interface Catalyst 5000 (C5IP) é a parte do RSM que emula um IP de sistema Catalyst 7500, com o barramento de switching Catalyst 5000 como interface de rede. O C5IP inclui um processador R4700 junto com dois SAGE Application-Specific Integrated Circuits (ASICs), responsáveis pelo acesso ao barramento de switching do Catalyst 5000.

SAGE

Esses dois ASICs obtêm pacotes de/para o barramento de switching e os armazenam em buffer. Along with the data in the packet, they also get an index identifying the destination of the packet in the Switch.



A interface VLAN de destino não é determinada do conteúdo do próprio pacote, mas deriva do índice. O pacote e o índice são armazenados primeiro em dois FIFOs diferentes dentro do SAGE. O índice é lido e a memória compartilhada necessária é reservada na área da VLAN de destino. Em seguida, o pacote é copiado para o dispositivo de memória (MEMD), usando um Acesso direto à memória (DMA) para o SAGE.

Dois SAGEs trabalhando em paralelo para se comunicar entre o roteador e o barramento de switching podem levar a uma entrega de pacotes fora de sequência. (Por exemplo, um pacote grande recebido no SAGE0 pode ser transmitido após um pacote pequeno recebido posteriormente pelo SAGE1.) Para evitar isso, cada VLAN é estaticamente atribuída a um determinado SAGE. Isso é feito automaticamente na inicialização. (De acordo com o roteador, uma VLAN é associada a um dos dois canais DMA, cada um deles levando a um SAGE.) Os pacotes de uma dada VLAN são sempre entregues em seqüência.

MEMD

MEMD é a memória compartilhada usada pelo roteador para enviar e receber pacotes. Cada interface de VLAN configurada no RSM recebe uma parte da memória compartilhada disponível. Quanto maior for o número de interfaces VLAN configuradas, menor será a memória compartilhada por interface. As interfaces VLAN mantêm sua parte da memória compartilhada mesmo quando desabilitadas ou desligadas. Adicionar ou remover apenas administrativamente uma interface VLAN ativa uma nova repartição do MEMD entre as interfaces VLAN.

Solução de problemas específica de RSM

Os principais problemas específicos de RSM que não são abordados na documentação normal do roteador Cisco IOS® são problemas de acesso ao RSM e também problemas de desempenho.

Acessando um RSM

O RSM pode ser acessado de três maneiras diferentes:

- Telnet para o RSM
- Sessão de Entrada no RSM do Supervisor do Switch
- Conexão direta do console

Telnet para o RSM

Para efetuar login via Telnet no RSM, você precisa conhecer o endereço IP atribuído a uma de suas interfaces VLAN. A sessão de Telnet funciona exatamente da mesma forma que se você estivesse tentando se conectar a um roteador Cisco IOS normal. Você pode precisar atribuir uma senha ao vty para obter Telnet e obter acesso de ativação.

Este exemplo mostra uma sessão Telnet de um Supervisor Engine para um RSM, na qual o endereço IP da VLAN1 é 10.0.0.1:

```
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
```

Isso é semelhante às outras configurações de roteadores externos do Cisco IOS.

Sessão de Entrada no RSM do Supervisor do Switch

O uso do comando **session *x*** do Supervisor Engine o conecta ao RSM no slot *x*.

O processo é o mesmo que o anterior: O RSM possui uma interface VLAN0 oculta que tem o endereço IP 127.0.0.(x+1), onde x é o slot em que o RSM está instalado. O comando **session** emite uma sessão Telnet oculta para este endereço.

Observação: desta vez, as senhas vty e enable não precisam estar na configuração para obter acesso total ao RSM.

```
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#
```

Use o comando Supervisor Engine **show module** para identificar o slot no qual seu RSM está instalado no switch. Você pode acessá-lo diretamente usando o comando **session**.

Conexão direta do console

A porta de console do sistema no RSM é uma porta DCE de receptáculo DB-25 para conectar um terminal de dados, que permite que você configure e se comunique com seu sistema. Use o cabo de console fornecido para conectar o terminal à porta de console no RSM. A porta do console está localizada no RSM próximo à porta auxiliar e está rotulada como 'console'.

Antes de conectar a porta de console, verifique a documentação do terminal para determinar a taxa de baud do terminal que você usará. A taxa de baud do terminal deve corresponder à taxa de baud padrão (9600 baud). Configure o terminal como: 9600 baud, oito bits de dados, sem paridade e dois bits de parada (9600,8N2).

Não é possível acessar o RSM

O RSM pode estar isolado por vários motivos. Mesmo sem estar apto a fazer a conexão, há alguns sinais de vida que podem ser verificados de fora.

- Verifique o status dos LEDS no RSM:O LED de parada da CPU está DESLIGADO—O sistema detectou uma falha de hardware do processador.LED de STATUS laranja—Módulo desabilitado, teste em andamento ou inicialização do sistema em andamento.
- Verifique o Supervisor Engine para ver se o switch pode ver o RSM. Para fazer isso, emita o comando **show module**:

```
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.
```

Nunca declare seu RSM como inativo antes de ter tentado a conexão do console. Como você viu, tanto a sessão como o acesso Telnet estão confiando em uma conexão IP com o RSM. Se o RSM estiver inicializando ou travado no modo ROMMON, por exemplo, você não poderá executar telnet ou sessão nele. Entretanto, isto é bastante normal.

Mesmo que o RSM pareça estar com defeito, tente se conectar ao console. Ao fazer isso, você poderá ver algumas mensagens de erro, que serão exibidas ali.

Problemas de desempenho

A maioria dos problemas de desempenho relacionados ao RSM pode ser solucionada exatamente da mesma forma que com um roteador Cisco IOS normal. Esta seção se concentra na parte específica da implementação de RSM que é o C5IP. O comando **show controller c5ip** pode fornecer informações sobre a operação do C5IP. Esta saída descreve alguns de seus campos mais importantes:

```
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#
```

Canal DMA 0/1

O roteador de RSP dentro do RSM está se comunicando com o Switch através de dois canais DMA distintos (indo para os dois SAGE ASICs). Cada interface VLAN é automaticamente associada a um desses canais DMA. O comando show controllers c5ip exibe informações sobre cada um em duas seções distintas.

Recebido/Transmitido

Essas estatísticas ajudam a identificar a carga em diferentes canais DMA. Procure um canal DMA que esteja continuamente sobrecarregado em comparação com os outros. Isso pode ocorrer se todas as VLANs com tráfego intenso forem atribuídas ao mesmo canal DMA. Se necessário, você pode atribuir manualmente interfaces VLAN a um canal DMA específico usando o canal dma do comando de interface.

Descartado

Isso indica o número de pacotes que o RSM recebeu, mas descartou. Isto acontece quando o índice recebido junto com o pacote não fornece o RSM do destino especificado no pacote.

Contagens de erro

- **crc** —Erros de ciclo de redundância cíclica (CRC) ocorrem quando um CRC inválido é detectado pelo RSM. Não deve haver nenhum pacote com CRCs defeituosos no backplane, e a detecção de RSM indica que algumas placas de linha ou outros dispositivos conectados ao backplane não estão funcionando corretamente.**Observação:** erros de CRC também podem vir de um dispositivo remoto conectado por um tronco ISL. A maioria das placas de linha Catalyst não verifica o CRC de um pacote que recebem do painel traseiro e encaminham em um tronco.
- **index** — Erros de índice ocorrem quando o índice não é preciso. O C5IP não sabe por que recebeu esse pacote. Isso também incrementa o contador descartado.
- **dmac-length** —Esses erros ocorrem quando a interface C5IP impediu que o SAGE ASIC sobrecarregasse um tamanho de MTU (Maximum Transmission Unit, unidade de transmissão máxima) que, se não detectado, teria corrompido a memória compartilhada do roteador.
- **dmac-synch** — Se um SAGE ASIC descarta um pacote, o FIFO do pacote e o índice FIFO ficam fora de sincronização. Se esse erro ocorrer, será automaticamente detectado e o

contador dmac-synch será incrementado. É improvável que isso ocorra, mas se acontecer, o impacto no desempenho é extremamente baixo.

- **dmac-timeout** —Este contador foi adicionado ao comando **show controllers c5ip** nas versões 11.2(16)P e 12.0(2) do software Cisco IOS. Ela é incrementada quando uma transferência de DMA não é concluída dentro do tempo máximo necessário para a transferência mais longa possível. Indica uma falha de hardware e um RSM mostrando um valor diferente de zero para esse contador é um bom candidato para substituição.
- **ignore** —Os ignorantes ocorrem quando o roteador fica sem buffers MEMD para pacotes de entrada. Isso acontece quando a CPU não está processando pacotes tão rápido quanto está entrando. Isso é provável devido ao que está mantendo a CPU ocupada.
- **line-down** —Line-down indica que os pacotes destinados a um protocolo de linha abaixo da VLAN foram descartados. O C5IP recebeu um pacote para uma interface VLAN que acredita estar inativa. Isso não deve acontecer, já que o switch deve parar de encaminhar pacotes para uma interface RSM que esteja inativa. Além disso, você pode ver alguns pacotes quando a interface se torna inativa, devido à temporização entre o RSM, que declara que a interface está inativa, e o Switch que está sendo notificado.
- **runt/giant** —Este contador rastreia pacotes de tamanho inválido.
- **unicast-flood** —pacotes unicast-flood são pacotes enviados a um endereço MAC específico. A tabela da CAM (Memória endereçável de conteúdo) do Catalyst 4000 não sabe em que porta o endereço MAC está localizado, portanto, inunda o pacote de todas as portas do VLAN. O RSM também recebe esses pacotes, mas a menos que esteja configurado para bridging nessa VLAN, não está interessado em pacotes que não correspondam ao seu próprio endereço MAC. O RSM descarta esses pacotes. Isso é o equivalente ao que acontece em uma interface Ethernet real no chip da interface Ethernet, que é programado para ignorar pacotes para outros endereços MAC. No RSM, isso é feito no software C5IP. A maioria dos pacotes descartados são pacotes unicast-flood.
- **Última queda** — Este contador revela informações específicas sobre o último pacote descartado. Estas são informações de baixo nível que estão fora do escopo deste documento.

Distribuição de VLAN entre canais DMA

Aqui está parte da saída do comando show controllers c5ip em um RSM tendo dez interfaces VLAN configuradas:

```
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
```

Esta saída mostra a qual canal DMA determinada interface VLAN é atribuída. Você pode ver que as VLANs ímpares vão para o canal 0, enquanto mesmo as VLANs estão vinculadas ao canal 1. Se necessário, você pode codificar essa correspondência usando o comando de configuração de interface **dma-channel**. Este exemplo mostra como atribuir a interface VLAN1 de um RSM ao

canal DMA 0:

```
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.
```

Informações da VLAN0

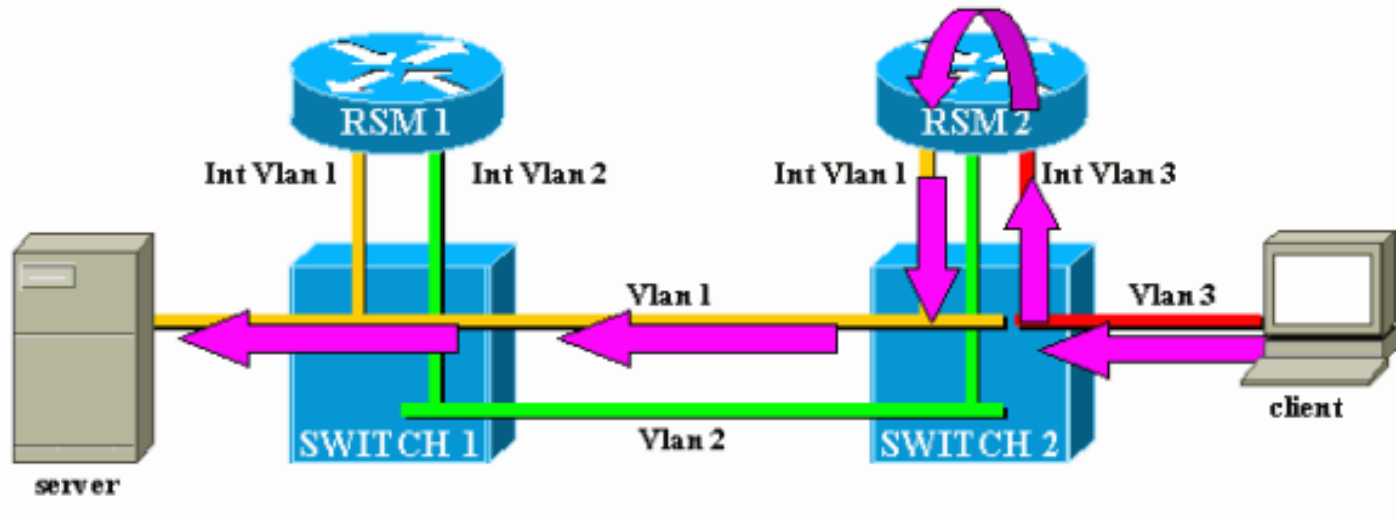
O principal objetivo da VLAN0 é garantir uma comunicação efetiva com o Supervisor Engine do switch. Como essa é uma interface oculta, não é possível utilizar um comando simple show interface vlan0 para ver as estatísticas sobre ela.

Problemas comuns de roteamento entre VLANs

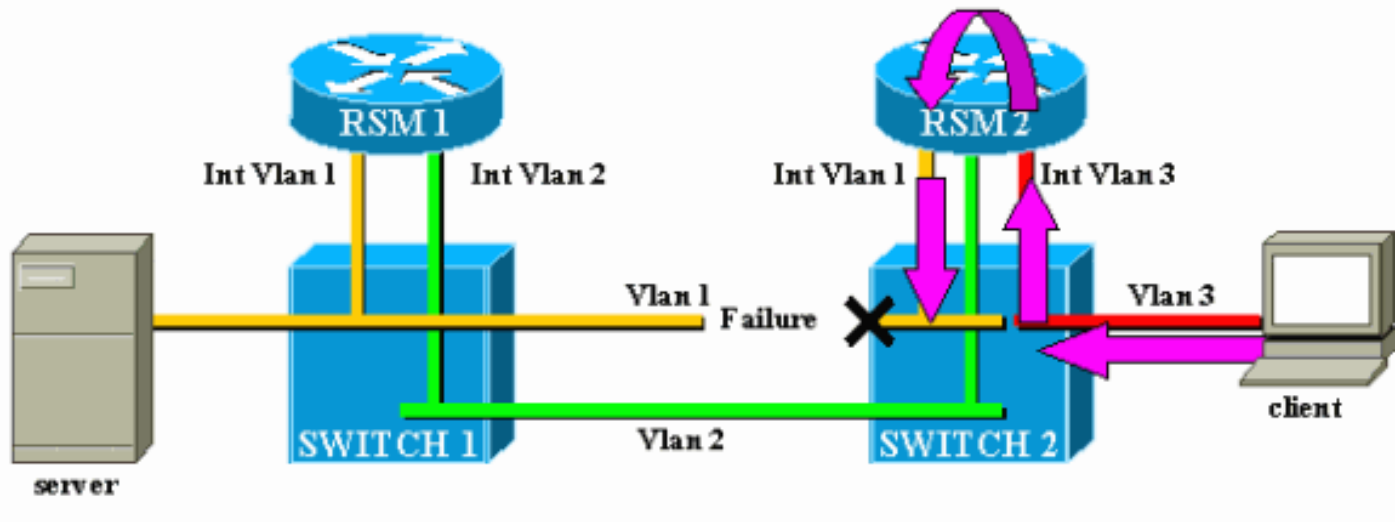
Usando o recurso RSM Autostate

Um problema freqüente com Bridging é que um link quebrado pode dividir facilmente uma rede L2 em duas partes. Essa situação deve ser evitada a qualquer preço, já que uma rede não contígua quebra o roteamento. (Isso geralmente é obtido com a implantação de links redundantes.)

Considere este exemplo, onde um cliente conectado ao Switch 2 se comunica com um servidor conectado ao Switch 1:



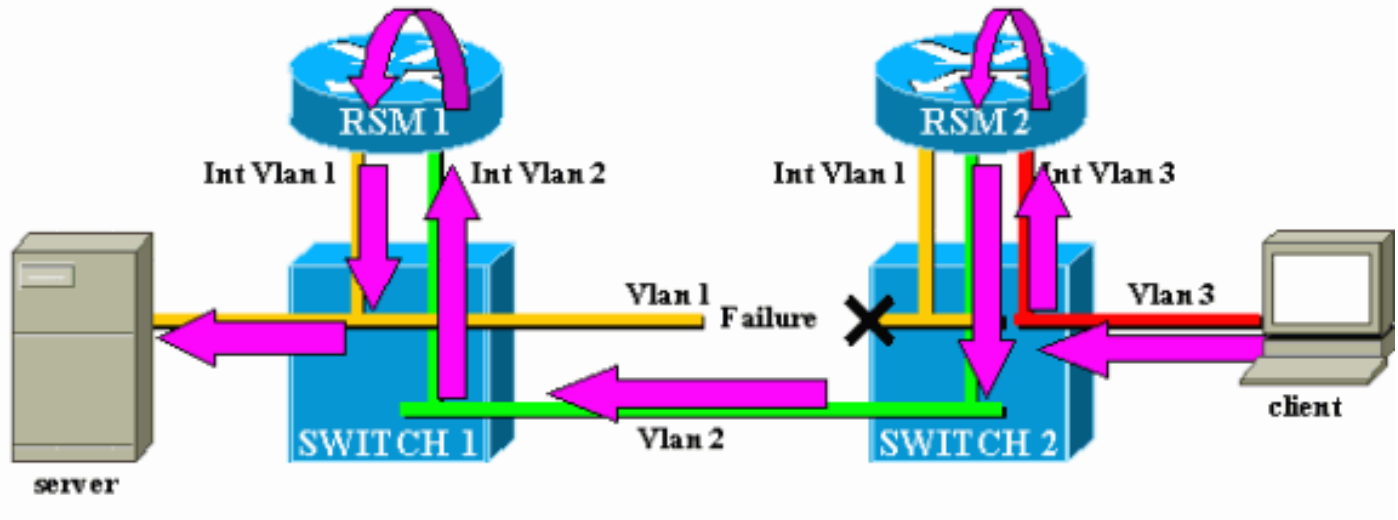
Considere apenas o tráfego do cliente para o servidor. O tráfego de entrada do cliente na VLAN3 é roteado pelo RSM2, que tem uma conexão direta com a sub-rede do servidor através de sua interface VLAN2. As setas roxas representam o caminho seguido:



Suponha que o link entre o Switch 1 e o Switch 2 se rompa para VLAN1. O principal problema aqui é que, do ponto de vista do RSM2, nada mudou na rede. O RSM2 ainda tem uma interface diretamente conectada à VLAN1 e mantém o tráfego de encaminhamento do cliente para o servidor através desse caminho. Ocorre perda do tráfego no Switch 2 e da conectividade entre o cliente e o servidor.

O recurso de estado automático RSM foi projetado para lidar com isso. If there is no port up for a specific VLAN on a Switch, the corresponding VLAN interface of the RSM is brought down.

No caso do exemplo, quando o link na VLAN entre o Switch 1 e o Switch 2 falha, a única porta na VLAN1 no Switch 2 está ficando inativa (link inativo). O recurso de estado automático RSM desativa a interface VLAN1 em RSM2. Agora que a interface VLAN1 está inoperante, o RSM2 pode usar um protocolo de roteamento para encontrar outro caminho para os pacotes destinados ao servidor e, eventualmente, encaminhar o tráfego através de outra interface, como mostrado neste diagrama:



O estado automático de RSM só funciona se não houver outra porta ativa na VLAN. Por exemplo, se você tivesse outro cliente na VLAN1 conectado ao Switch 2 ou RSM no chassi com uma interface VLAN1 definida, a interface VLAN1 não seria desabilitada se o link entre o Switch 1 e o Switch 2 falhasse. O tráfego seria então interrompido novamente.

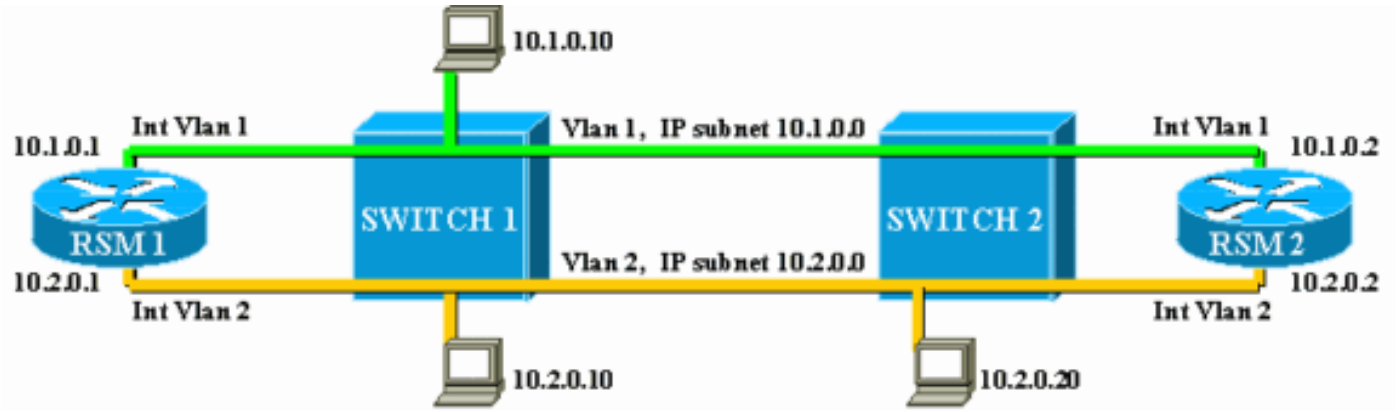
O recurso autostate do RSM é habilitado por padrão. Se necessário, ele pode ser desabilitado manualmente usando o comando set rsmautostate no Supervisor Engine:

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

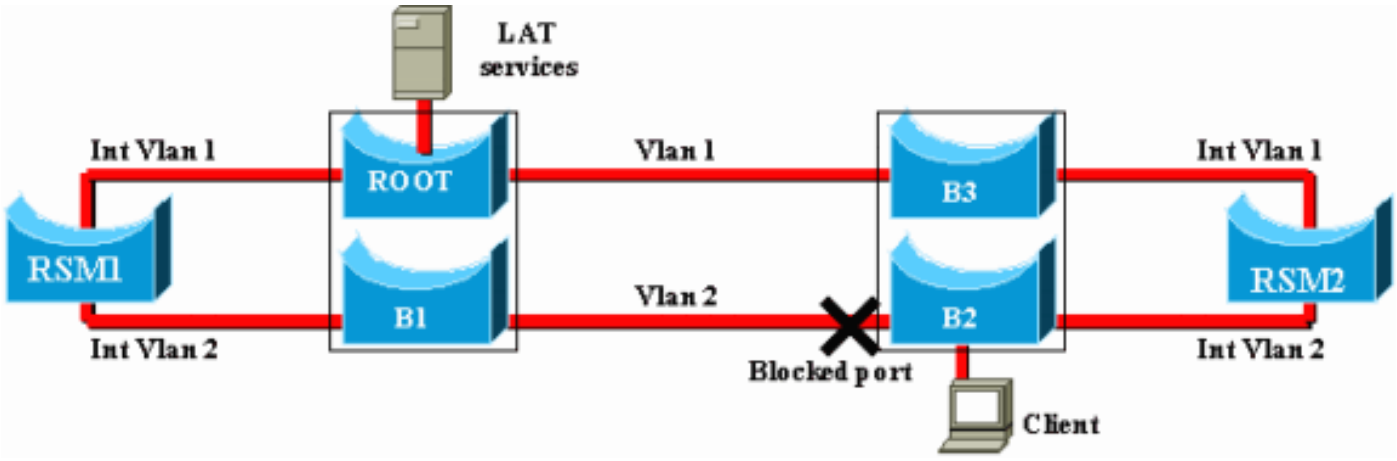
Fall-Back Bridging

O Fall-Back Bridging consiste em protocolos de bridging entre VLANs, enquanto roteia outras. Se possível, você deve evitar esse tipo de configuração e usá-la apenas durante um período de migração transitória. Normalmente, isso é necessário quando você segmentou sua rede com sub-redes IP diferentes, cada uma em uma VLAN diferente, mas deseja manter a ponte de alguns protocolos não roteáveis antigos (transporte de área local [LAT], por exemplo). Neste caso, use o seu RSM como roteador de IP, mas como uma ponte para os demais protocolos. Isto é obtido simplesmente através da configuração do Briding nas interfaces RSM, enquanto os IP Addresses são mantidos. O exemplo a seguir ilustra uma rede muito simples usando Fall-Back Bridging, juntamente com o problema mais comum que pode acorrer com esse tipo de configuração.

Essa rede muito simples é feita de duas VLANs, correspondendo a duas sub-redes IP diferentes. Os hosts em uma determinada VLAN podem usar qualquer um dos dois RSMs como um gateway padrão (ou mesmo ambos, usando o Protocolo de Roteador de Hot Standby [HSRP - Hot Standby Router Protocol]), e assim podem se comunicar com os hosts na outra VLAN. A rede é assim:



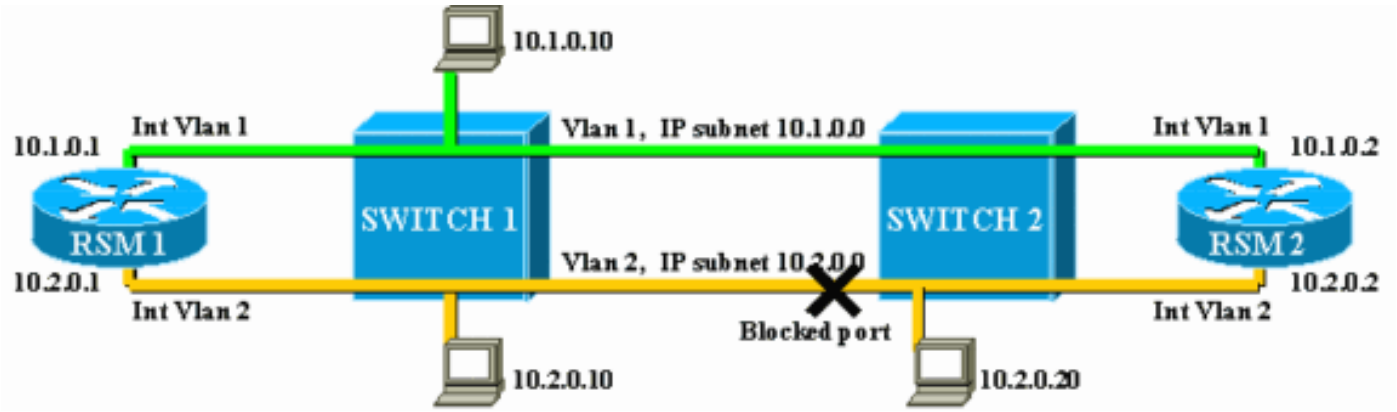
Os dois RSMs também são configurados para fazer a ponte com outros protocolos entre suas interfaces, VLAN1 e VLAN2. Suponha que você tenha um host que ofereça serviços LAT e um cliente que os esteja usando. Sua rede será semelhante a esta:



Para este diagrama, cada Catalyst é dividido em duas bridges diferentes (uma para cada VLAN). Você pode ver que o bridging entre as duas VLANs resultou em uma fusão das duas VLANs. No

que diz respeito aos protocolos interligados, você tem apenas uma VLAN, e o servidor e o cliente LAT podem se comunicar diretamente. Claro, isso também implica que você tem um loop na rede e que o STP tem que bloquear uma porta.

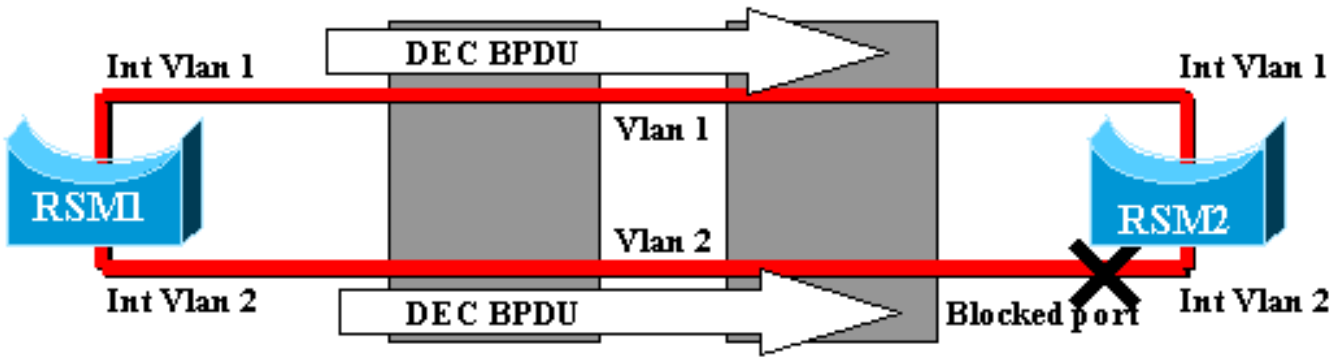
Como você pode ver, um problema resultará dessa porta de bloqueio. Um switch é um dispositivo L2 puro e não consegue diferenciar o tráfego IP do LAT. Portanto, se o Switch 2 bloqueia uma porta, como no diagrama acima, ele bloqueia todos os tipos de tráfego (IP, LAT ou outro). Por causa disso, sua rede se parece com isto:



A VLAN2 é dividida em duas partes e você tem uma sub-rede não contígua 10.2.0.0. Com essa configuração, o host 10.2.0.10 não pode se comunicar com o host 10.2.0.20, embora eles estejam na mesma sub-rede e VLAN.

A solução é mover a porta bloqueada para o único dispositivo que pode diferenciar o tráfego de L2 e L3. Aquele dispositivo é o RSM. Há duas maneiras principais de conseguir isto:

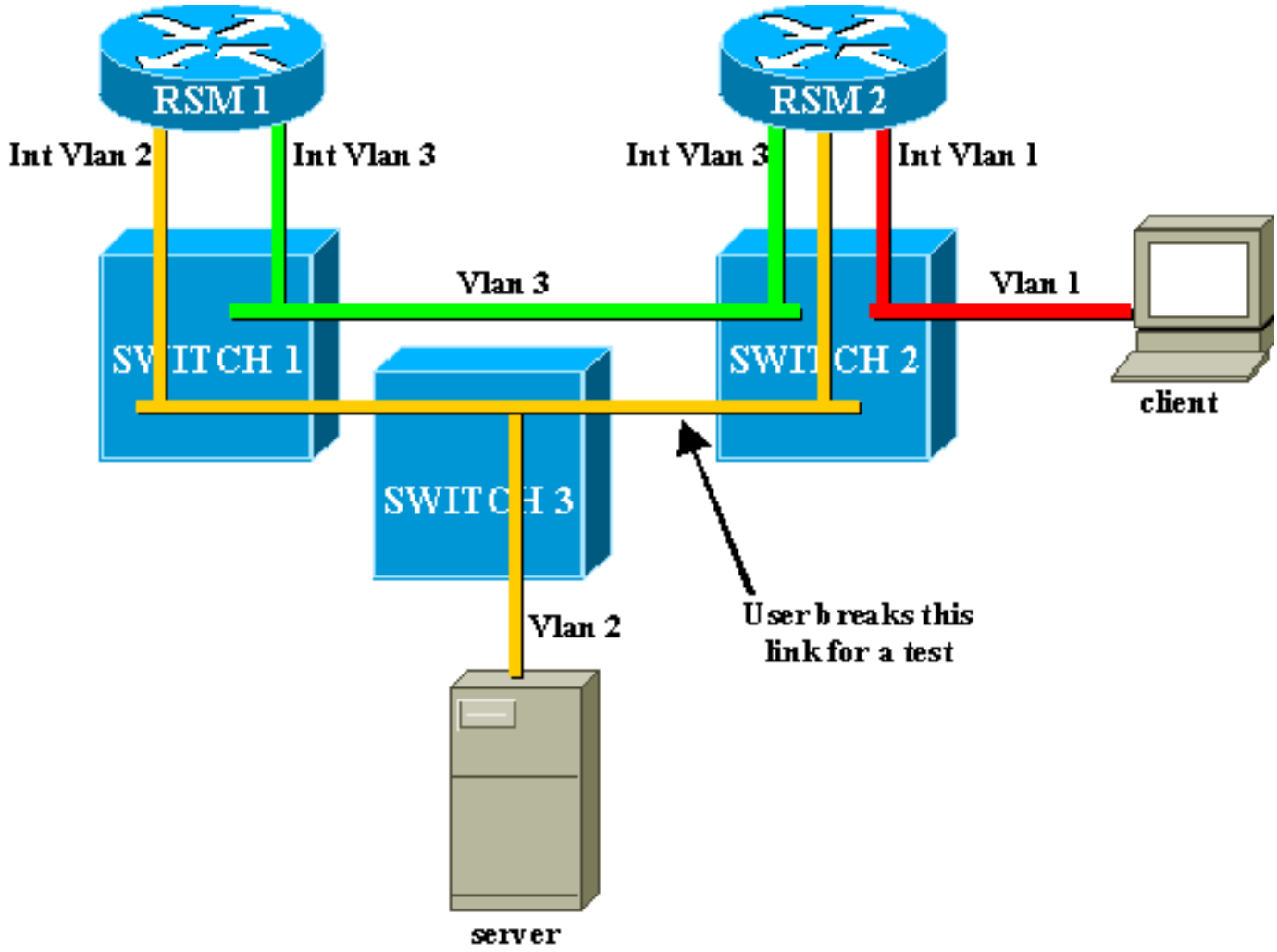
- **Ao ajustar os parâmetros de STP:** Você precisa aumentar o custo em um ou mais dispositivos para que, eventualmente, a porta de bloqueio esteja localizada em RSM1 ou RSM2. Este método não é muito flexível e implica em uma configuração de STP muito estrita. Adicionar um switch ou alterar a largura de banda de um link (Fast EtherChannel ou Gigabit Ethernet) pode causar um retrabalho completo do ajuste.
- **Usando um Spanning Tree Algorithm (STA) diferente no RSM:** Os switches executam apenas o IEEE STA e são completamente transparentes para o DEC STP. Se você configurar o DEC STP em ambos os RSMs, eles funcionarão como se estivessem diretamente conectados, e um deles será bloqueado. Este diagrama ilustra
  isto:



Buraco negro temporário (convergência ST)

Os clientes que testam a velocidade de reconfiguração da rede no caso de falha em geral lidam

com problemas de configuração relacionados com o STP. Considere a seguinte rede, onde um cliente acessa um servidor por dois caminhos diferentes. Por padrão, o tráfego do cliente ao servidor é roteado via interface VLAN2 por RSM2:



Para executar um teste, um usuário quebra o link entre o Switch 2 e o Switch 3. Imediatamente, a porta correspondente fica inativa e o recurso de estado automático RSM desativa a interface VLAN2 no RSM2. A rota diretamente conectada para o servidor desaparece da tabela de roteamento de RSM2, que aprende rapidamente uma nova rota via RSM1. Com protocolos de roteamento eficientes, como OSPF (Open Shortest Path First) ou EIGRP (Enhanced Interior Gateway Routing Protocol), a convergência é tão rápida que quase não se perde um ping durante essa operação.

Se houver falha, o switchover entre os dois caminhos (VLAN2 amarelo e VLAN3 verde) tem sido imediata. No entanto, se o usuário restabelecer o link entre o Switch 2 e o Switch 3, o cliente experimentará uma perda de conectividade com o servidor por cerca de 30 segundos.

O motivo para isso também está relacionado ao STA. Durante a execução do STA, uma porta recém-conectada passa primeiro pelos estágios de escuta e aprendizagem, antes de entrar no modo de encaminhamento. Durante os dois primeiros estágios de 15 segundos, a porta está ativa, mas não transmite tráfego. Isso significa que assim que o link é conectado, o recurso de estado automático RSM imediatamente reativa a interface VLAN2 no RSM2, mas o tráfego não pode passar até que as portas no link entre o Switch 2 e o Switch 3 atinjam o estágio de encaminhamento. Isso explica a perda de conectividade temporária entre o cliente e o servidor. If the link between Switch 1 and Switch 2 is not a trunk, you can enable the portfast feature to skip the listening and learning stages and converge immediately.

Observação: o PortFast não funciona em portas de tronco. Consulte Uso do PortFast e de Outros Comandos para Corrigir Atrasos de Conectividade de Inicialização da Estação de Trabalho para obter mais informações.

Conclusão

Este documento enfatiza alguns problemas específicos de RSM, bem como alguns problemas muito comuns de roteamento entre VLANs. Essas informações só são úteis quando todos os procedimentos normais de identificação e solução de problemas do roteador Cisco IOS tiverem sido tentados. Se metade dos pacotes roteados por um RSM forem perdidos devido à tabela de roteamento errada, isso não ajudará a tentar interpretar as estatísticas do canal DMA. Mesmo os problemas gerais de roteamento entre VLANs são tópicos avançados e não ocorrem com muita frequência. Na maioria dos casos, é suficiente considerar o RSM (ou qualquer outro dispositivo de roteamento integrado em um Switch) como um simples roteador externo do Cisco IOS para fazer Troubleshooting de roteamento em um ambiente comutado.

Informações Relacionadas

- Página de suporte aos protocolos de roteamento IP
- Troubleshooting de IP Multilayer Switching
- Configurando o roteamento entre VLANs
- Utilização de Portfast e outros comandos para reparar retardos de conectividade da inicialização de estação de trabalho
- Páginas de Suporte de Produtos de LAN
- Página de suporte da switching de LAN
- Suporte Técnico e Documentação - Cisco Systems