Catalyst 5000 RSM(Route Switch Module) 및 InterVLAN 라우팅 문제 해결

목차

소개

이 문서에서는 Catalyst 5000 제품군 스위치에서 RSM(Route Switch Module)을 사용하여 VLAN 간 라우팅의 문제 해결에 대한 정보를 제공합니다. RSM의 문제 해결에 있어서 가장 먼저 해야 할 일은 간단한 외부 라우터로 생각하는 것입니다. VLAN 간 라우팅과 관련된 경우 RSM 관련 문제로 인해 문제가 발생하는 경우는 거의 없습니다. 따라서 이 문서에서는 이러한 문제가 발생할 수 있는 두 가지 주요 영역만 다룹니다.

- **RSM 하드웨어 관련 문제**: 이 문서에서는 RSM 아키텍처를 소개하고 추적할 추가 RSM 관련 카운터에 대한 세부 정보를 제공합니다.
- **VLAN 간 컨피그레이션 관련 문제**(대부분 라우터와 스위치 간의 상호 작용과 관련): 이는 다른 내부 라우터(예: MSFC[Multilayer Switch Feature Card], RSFC[Route Switch Feature Card], 8510CSR 등)와 외부 라우터에도 적용됩니다.

참고: 이 문서에서는 Catalyst 4000, 5000 및 6000 스위치에서 interVLAN 라우팅 구성을 다루지 않습니다. 자세한 내용은 다음 문서를 참조하십시오.

- Catalyst 4500/4000 제품군용 라우터 모듈 구성 및 개요(WS-X4232-L3)
- Catalyst 4000 Layer 3 Services Module의 설치 및 구성 참고 사항의 InterVLAN Routing *모듈*

구성 섹션
- CatOS 시스템 소프트웨어를 실행하는 Catalyst 5500/5000 및 6500/6000 스위치에서 내부 라우터(레이어 3 카드)를 사용하여 InterVLAN 라우팅 구성

이 문서에서는 기본적인 라우팅 프로토콜 문제 해결 또는 MLS(Multilayer Switching) 관련 문제를 다루지 않습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

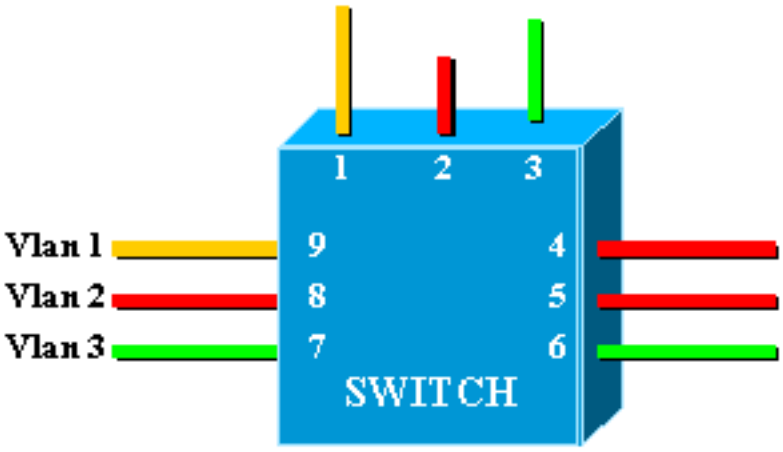
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

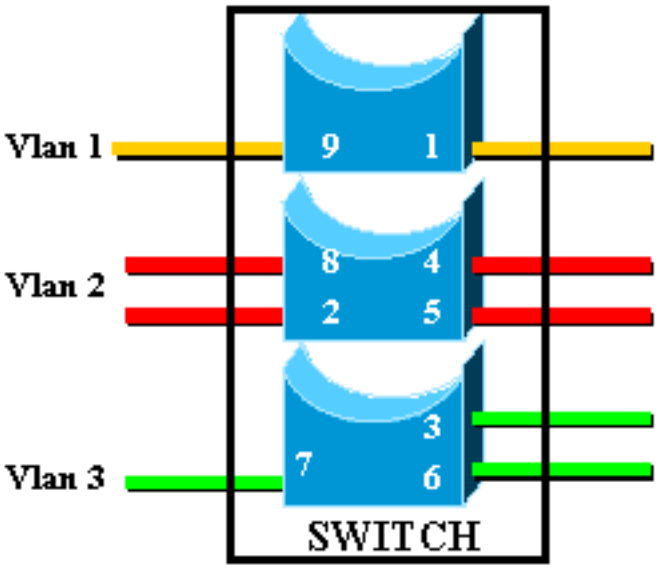
InterVLAN 라우팅이란?

이 문서에서는 interVLAN 라우팅을 논의하기 전에 VLAN 개념에 초점을 맞춥니다. 이는 VLAN의 필요성에 대한 이론적인 논의가 아니라 스위치에서 VLAN이 작동하는 방식에 대해 설명합니다. 스위치에서 VLAN을 생성할 때 스위치를 여러 가상 브리지로 분할하는 것과 같습니다. 각 브리징 포트는 동일한 VLAN에 속하는 유일한 브리징 포트입니다.

이 다이어그램은 세 개의 서로 다른 VLAN에 9개의 포트가 할당된 스위치를 나타냅니다.



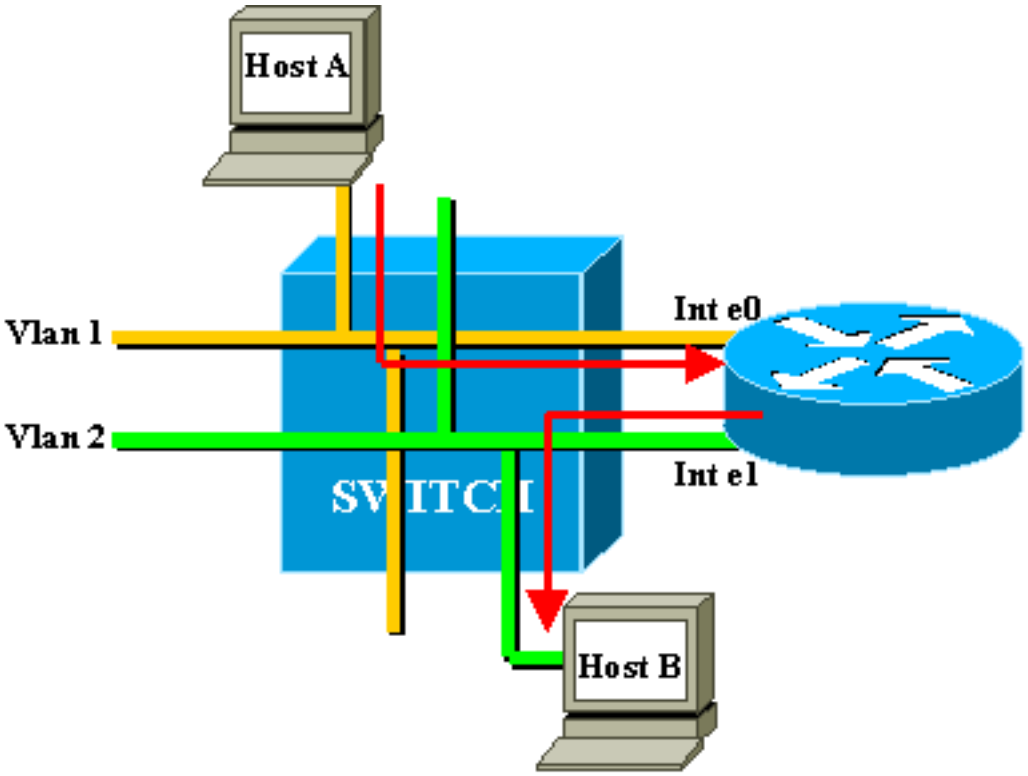
이는 3개의 독립적인 브리지로 구성된 다음 네트워크와 동일합니다.



스위치에는 각 VLAN이 별도의 브리지를 생성하므로 세 개의 서로 다른 브리지가 있습니다. 각 VLAN은 별도의 STP(Spanning Tree Protocol) 인스턴스를 생성하므로 STP는 세 개의 서로 다른 포워딩 테이블을 유지합니다.

두 번째 다이어그램을 사용하면 동일한 물리적 디바이스에 연결되었지만 서로 다른 VLAN에 속하는 포트는 레이어 2(L2)에서 직접 통신할 수 없다는 것이 분명해집니다. 가능하더라도 이것은 적절하지 않을 것이다. 예를 들어 포트 1을 포트 4에 연결한 경우 VLAN1을 VLAN2에 병합하면 됩니다. 이 경우 별도의 VLAN이 두 개 있을 필요는 없습니다.

VLAN 간에 원하는 유일한 연결은 라우터가 레이어 3(L3)에서 수행합니다. 이는 interVLAN 라우팅입니다. 다이어그램을 더욱 간소화하기 위해 VLAN은 스위치에서 제공하는 특정 브리징 기능에는 관심이 없으므로 서로 다른 물리적 이더넷 세그먼트로 표시됩니다.



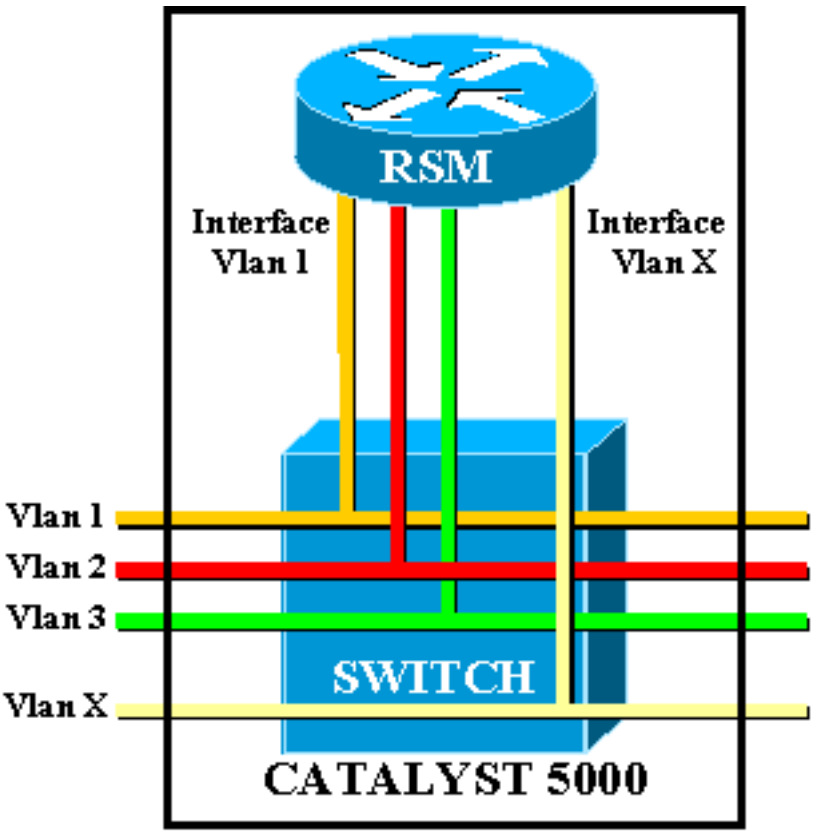
이 다이어그램에서 두 VLAN은 서로 다른 두 이더넷 세그먼트로 간주됩니다. InterVLAN 트래픽은 외부 라우터를 통과해야 합니다. 호스트 A가 호스트 B와 통신하려는 경우 일반적으로 라우터를 기본 게이트웨이로 사용합니다.

RSM 아키텍처

논리적 아키텍처

RSM을 Catalyst 5000 스위치의 서로 다른 VLAN에 직접 연결된 여러 인터페이스가 있는 외부 라우터로 볼 수 있습니다.

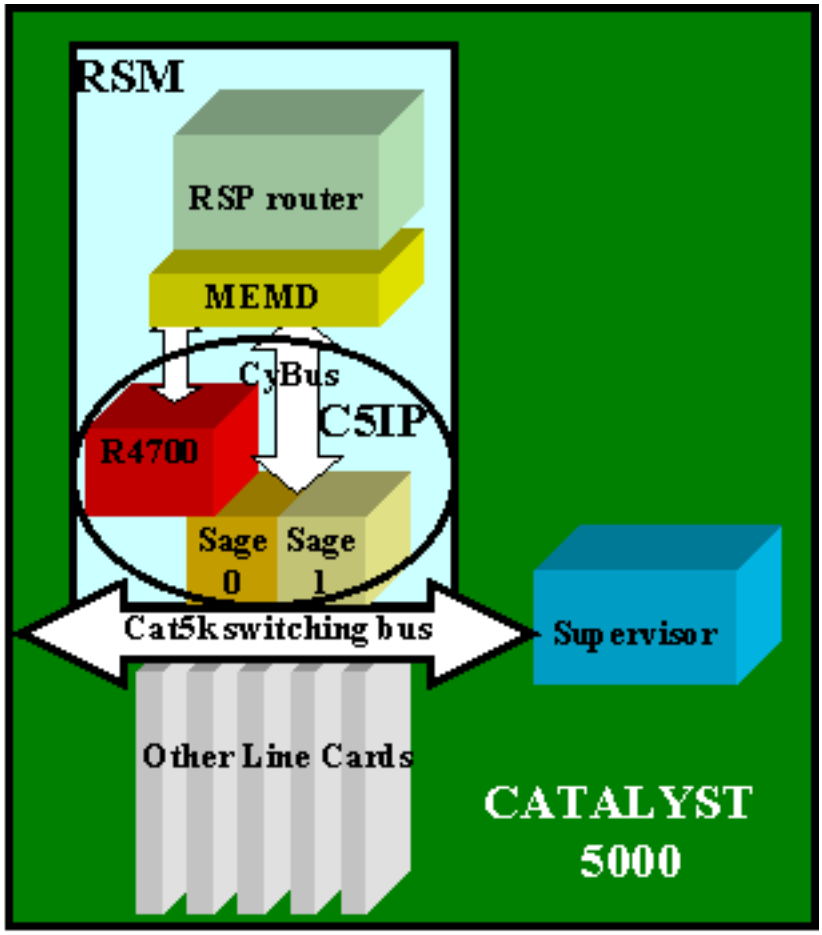
이러한 인터페이스의 이름은 이더넷 인터페이스라고 하는 대신 연결된 VLAN에 따라 지정됩니다. (인터페이스 VLAN1은 VLAN1에 직접 연결됨 등)



아키텍처 구현

RSM은 Catalyst 5000 라인 카드 내부의 Cisco 7500 RSP(Route Switch Processor) 라우터입니다. 구성 및 트러블슈팅을 위해 카드의 아키텍처에 대해 많이 알지 않아도 됩니다. 그러나 RSM이 어떻게 구축되는지 아는 것은 일반 외부 라우터와 어떻게 다른지를 파악하는 데 도움이 됩니다. 이 정보는 **show controller c5ip** 명령을 도입할 때 특히 중요합니다.

이 다이어그램은 RSM 라인 카드에서 기본 구성 요소를 찾습니다.

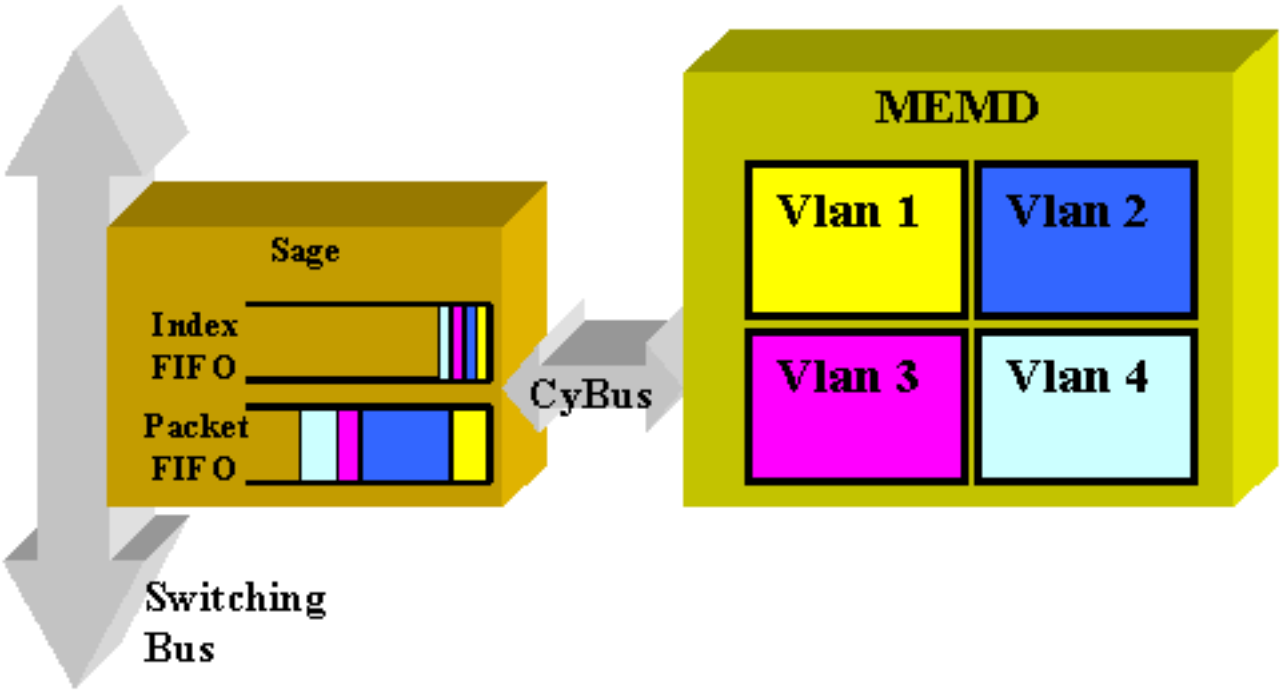


Catalyst 5000 Interface Processor

Catalyst 5000 Interface Processor(C5IP)는 Catalyst 7500 시스템 IP를 에뮬레이트하는 RSM의 일부이며, Catalyst 5000 스위칭 버스를 네트워크 인터페이스로 사용합니다. C5IP에는 R4700 프로세서와 Catalyst 5000 스위칭 버스 액세스를 담당하는 2개의 SAGE ASIC(Application-Specific Integrated Circuits)가 포함되어 있습니다.

세이지

이 두 ASIC는 스위칭 버스에서/로 패킷을 가져오고 버퍼링합니다. 패킷의 데이터와 함께 스위치에서 패킷의 대상을 식별하는 인덱스도 가져옵니다.



대상 VLAN 인터페이스는 패킷 자체의 콘텐츠에서 결정되지 않지만 인덱스에서 파생됩니다. 패킷과 인덱스는 먼저 SAGE 내의 서로 다른 두 FIFO에 저장됩니다. 인덱스가 읽혀지고 필요한 공유 메모리가 대상 VLAN 영역에 예약됩니다. 그런 다음 DMA(Direct Memory Access)를 사용하여 MEMD(메모리 디바이스)에 패킷이 복사됩니다.

라우터와 스위칭 버스 간에 통신하기 위해 병렬로 작동하는 두 SAGE는 순서가 틀린 패킷 전달을 초래할 수 있습니다. (예를 들어, SAGE0에서 수신된 큰 패킷은 나중에 SAGE1에서 수신한 작은 패킷 후에 전송할 수 있습니다.) 이를 방지하기 위해 각 VLAN은 지정된 SAGE에 정적으로 할당됩니다. 이 작업은 시작 시 자동으로 수행됩니다. (라우터에 따르면 VLAN은 두 DMA 채널 중 하나에 연결되며 각각 SAGE로 연결됩니다.) 지정된 VLAN의 패킷은 항상 순서대로 전달됩니다.

MEMD

MEMD는 라우터가 패킷을 보내고 받기 위해 사용하는 공유 메모리입니다. RSM에서 구성된 각 VLAN 인터페이스는 사용 가능한 공유 메모리의 일부로 할당됩니다. VLAN 인터페이스가 더 구성될수록 인터페이스당 공유 메모리는 더 적습니다. VLAN 인터페이스는 비활성화되거나 종료된 경우에도 공유 메모리의 일부를 유지합니다. 관리상 VLAN 인터페이스를 추가 또는 제거하기만 하면 VLAN 인터페이스 간에 MEMD의 새 재파티션이 트리거됩니다.

RSM 관련 문제 해결

일반적인 Cisco IOS® 라우터 설명서에서 다루지 않는 RSM 관련 주요 문제는 RSM 액세스 문제 및 성능 문제입니다.

RSM 액세스

RSM은 다음 세 가지 방법으로 액세스할 수 있습니다.

- RSM에 텔넷
- 스위치 수퍼바이저에서 RSM에 세션 인
- 직접 콘솔 연결

RSM에 텔넷

RSM에 텔넷하려면 VLAN 인터페이스 중 하나에 할당된 IP 주소를 알아야 합니다. 텔넷 세션은 일반 Cisco IOS 라우터에 연결하려고 했던 것과 동일하게 작동합니다. 텔넷을 달성하고 액세스 권한을 얻기 위해 vty에 비밀번호를 할당해야 할 수 있습니다.

다음 예에서는 VLAN1 IP 주소가 10.0.0.1인 Supervisor Engine에서 RSM으로의 텔넷 세션을 보여줍니다.

```
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
```

이는 다른 외부 라우터 Cisco IOS 컨피그레이션과 유사합니다.

스위치 수퍼바이저에서 RSM에 세션 인

Supervisor Engine에서 **session *x* 명령**을 사용하면 슬롯 *x*의 RSM에 연결됩니다.

방법은 이전 방법과 동일합니다. RSM에는 IP 주소가 127.0.0.(x+1)인 숨겨진 VLAN0 인터페이스가 있습니다. 여기서 x는 RSM이 설치된 슬롯입니다. session 명령은 이 주소에 대한 숨겨진 텔넷 세션을 실행합니다.

참고: 이번에는 RSM에 대한 전체 액세스 권한을 얻기 위해 vty 및 enable 비밀번호가 컨피그레이션에 있을 필요는 없습니다.

```
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#
```

Supervisor Engine 명령 show module을 사용하여 스위치에 RSM이 설치된 슬롯을 식별합니다. **session** 명령을 사용하여 직접 액세스할 수 있습니다.

직접 콘솔 연결

RSM의 시스템 콘솔 포트는 데이터 터미널을 연결하기 위한 DB-25 콘센트 DCE 포트이며, 이를 통해 시스템을 구성하고 시스템과 통신할 수 있습니다. 제공된 콘솔 케이블을 사용하여 터미널을

RSM의 콘솔 포트에 연결합니다. 콘솔 포트는 보조 포트 옆의 RSM에 있으며 콘솔 레이블이 지정됩니다.

콘솔 포트를 연결하기 전에 터미널 설명서를 참조하여 사용할 터미널의 전송 속도를 확인하십시오. 터미널의 전송 속도는 기본 전송 속도(보드 9600)와 일치해야 합니다. 터미널을 다음과 같이 설정합니다. 9600baud, 8개의 데이터 비트, 패리티 없음, 2개의 정지 비트(9600,8N2)

RSM에 액세스할 수 없음

RSM은 여러 가지 이유로 격리될 수 있습니다. 연결할 수 없어도 외부에서 확인할 수 있는 생명의 징후가 있습니다.

- RSM에서 LED의 상태를 확인합니다.CPU Halt LED is OFF(CPU Halt LED is OFF) - 시스템에서 프로세서 하드웨어 오류를 감지했습니다.주황색 STATUS LED - 모듈이 비활성화되었거나, 테스트가 진행 중이거나, 시스템 부팅이 진행 중입니다.
- Supervisor Engine에서 스위치가 RSM을 볼 수 있는지 확인합니다. 이렇게 하려면 **show module** 명령을 실행합니다.

```
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.
```

콘솔 연결을 시도하기 전에 RSM 데드를 선언하지 마십시오. 지금까지 살펴본 것처럼, 세션 및 텔넷 액세스 모두 RSM에 대한 IP 연결에 의존합니다. 예를 들어 RSM이 부팅 중이거나 ROMMON 모드에서 고착 상태인 경우 텔넷 또는 세션을 시작할 수 없습니다. 그러나 이것은 꽤 정상이다.

RSM에 결함이 있는 것처럼 보이는 경우에도 콘솔에 연결해 보십시오. 이렇게 하면 오류 메시지가 표시될 수 있습니다.

성능 문제

RSM과 관련된 대부분의 성능 문제는 일반적인 Cisco IOS 라우터와 동일한 방식으로 트러블슈팅할 수 있습니다. 이 섹션에서는 C5IP인 RSM 구현의 특정 부분에 대해 중점적으로 설명합니다. **show controller c5ip** 명령은 C5IP 작업에 대한 정보를 제공할 수 있습니다. 이 출력은 가장 중요한 필드 중 일부를 설명합니다.

```
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 채널 0/1

RSM 내의 RSP 라우터는 두 개의 서로 다른 DMA 채널을 통해 스위치와 통신합니다(두 SAGE ASIC로 이동). 각 VLAN 인터페이스는 이러한 DMA 채널 중 하나와 자동으로 연결됩니다. show **controllers c5ip** 명령은 두 개의 개별 섹션에 각 섹션에 대한 정보를 표시합니다.

수신/전송

이러한 통계는 서로 다른 DMA 채널의 로드를 식별하는 데 도움이 됩니다. 다른 채널에 비해 지속적으로 오버로드되는 DMA 채널을 찾습니다. 이는 모든 트래픽 집약형 VLAN이 동일한 DMA 채널에 할당된 경우 발생할 수 있습니다. 필요한 경우 interface 명령 dma-**channel**을 사용하여 특정 DMA 채널에 VLAN 인터페이스를 수동으로 할당할 수 있습니다.

삭제됨

이는 RSM이 수신했지만 삭제된 패킷 수를 나타냅니다. 패킷과 함께 수신된 인덱스가 RSM을 패킷의 특정 대상으로 제공하지 않을 경우 이러한 현상이 발생합니다.

오류 수

- **crc** - RSM에서 잘못된 CRC를 탐지하면 CRC(Cyclic Redundancy Cycle) 오류가 발생합니다. 백플레인에 잘못된 CRC가 있는 패킷은 없어야 하며, RSM에서 이를 탐지하는 경우 일부 라인 카드나 다른 백플레인에 연결된 디바이스가 제대로 작동하지 않음을 나타냅니다.**참고:** CRC 오류는 ISL 트렁크를 통해 연결된 원격 디바이스에서도 발생할 수 있습니다. 대부분의 Catalyst 라인 카드는 백플레인에서 수신한 패킷의 CRC를 확인하고 트렁크에서 전달하지 않습니다.
- **index** —인덱스가 정확하지 않을 때 인덱스 오류가 발생합니다. C5IP는 이 패킷을 수신한 이유를 알지 못합니다. 이렇게 하면 Dropped 카운터도 증가합니다.
- **dmac-length**—C5IP 인터페이스가 SAGE ASIC에서 MTU(Maximum Transmission Unit) 크기를 오버실행하지 못하도록 할 때 이러한 오류가 발생합니다. 탐지되지 않은 경우 라우터 공유 메모리가 손상될 수 있습니다.
- **dmac-synch** —SAGE ASIC에서 패킷을 삭제하면 패킷 FIFO 및 인덱스 FIFO가 동기화되지 않습니다. 이 오류가 발생하면 자동으로 감지되고 dmac 카운터가 증가합니다. 이러한 상황이 발생할 가능성은 낮지만, 발생할 경우 성능에 미치는 영향이 매우 낮습니다.
- **dmac-timeout** - 이 카운터는 Cisco IOS Software 릴리스 11.2(16)P 및 12.0(2)의 **show controllers c5ip** 명령에 추가되었습니다. DMA 전송이 가능한 가장 긴 전송에 필요한 최대 시간 내에 완료되지 않을 경우 증가합니다. 하드웨어 오류를 나타내며, 이 카운터에 0이 아닌 값을 표시하는 RSM이 교체에 적합합니다.
- **ignore** —라우터가 입력 패킷에 대한 MEMD 버퍼가 부족하면 무시됩니다. 이는 CPU가 들어오는 패킷만큼 빠르게 패킷을 처리하지 않을 때 발생합니다. 이는 CPU를 계속 사용할 수 있기 때문일 가능성이 높습니다.
- **line-down** - Line-down은 라인 프로토콜로 향하는 패킷이 다운 VLAN으로 삭제되었음을 나타냅니다. C5IP가 중단된 것으로 간주되는 VLAN 인터페이스에 대해 패킷을 받았습니다. 스위치가 다운된 RSM 인터페이스로 패킷을 전달하는 것을 중지해야 하므로 이러한 작업은 발생하지 않

습니다. 그러나 RSM이 인터페이스를 다운한다고 선언하는 시간과 알림을 받는 스위치 간의 타이밍 때문에 인터페이스가 다운될 때 몇 가지를 볼 수 있습니다.

- **runt/giant**—이 카운터는 잘못된 크기의 패킷을 추적합니다.
- **unicast-flood** - 유니캐스트 플러드 패킷은 특정 MAC 주소로 전송되는 패킷입니다. Catalyst 5000 CAM(Content Addressable Memory) 테이블은 MAC 주소가 어떤 포트에 있는지 알지 못하므로 VLAN의 모든 포트에 패킷을 플러딩합니다. RSM은 또한 이러한 패킷을 수신하지만, 해당 VLAN에서 브리징을 위해 구성되지 않는 한 자체 MAC 주소와 일치하지 않는 패킷에는 관심이 없습니다. RSM은 이러한 패킷을 버립니다. 이는 다른 MAC 주소에 대한 패킷을 무시하도록 프로그래밍된 이더넷 인터페이스 칩의 실제 이더넷 인터페이스에서 발생하는 것과 같습니다. RSM에서는 C5IP 소프트웨어에서 이 작업을 수행합니다. 삭제된 패킷의 대부분은 유니캐스트 플러드 패킷입니다.
- **Last drop( )** - 이 카운터는 마지막으로 삭제된 패킷에 대한 특정 정보를 표시합니다. 이 문서의 범위를 벗어난 하위 수준 정보입니다.

DMA 채널 간 VLAN 배포

다음은 10개의 VLAN 인터페이스가 구성된 RSM에서 **show controllers c5ip** 명령 출력의 일부입니다.

```
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
```

이 출력은 지정된 VLAN 인터페이스가 할당된 DMA 채널을 보여줍니다. 홀수 VLAN은 채널 0으로 이동하는 반면 VLAN도 채널 1에 연결되어 있습니다. 필요한 경우 interface configuration 명령 **dma-channel**을 사용하여 이 서신에 대해 하드 코딩할 수 있습니다. 다음 예에서는 RSM의 인터페이스 VLAN1을 DMA 채널 0에 할당하는 방법을 보여줍니다.

```
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 정보

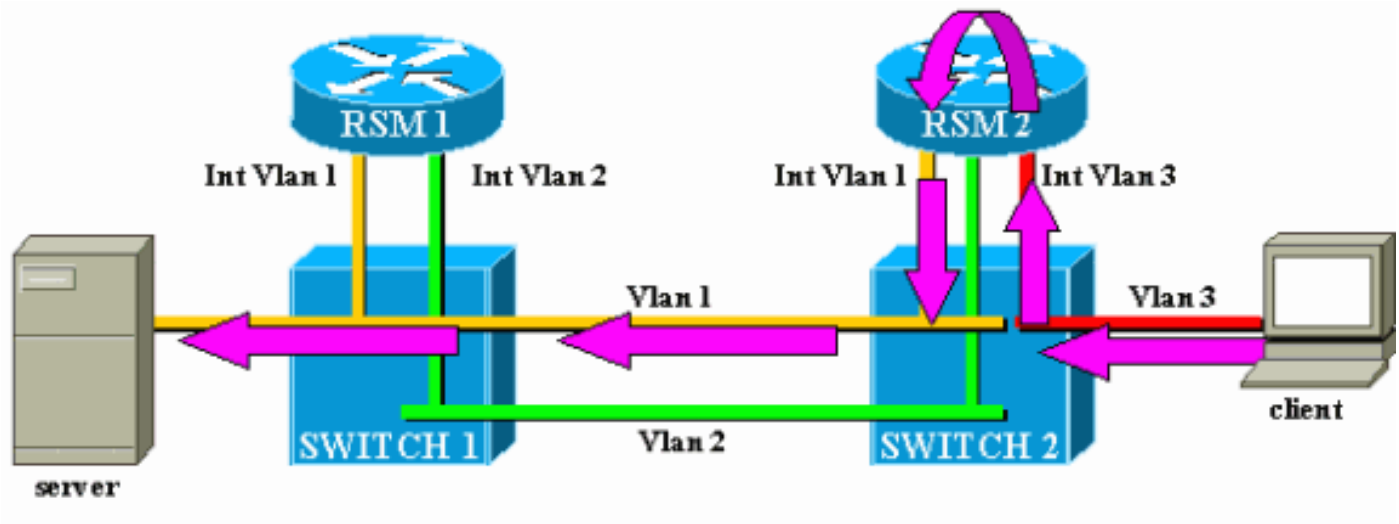
VLAN0의 주요 목적은 스위치의 Supervisor Engine과 효과적으로 통신하는 것입니다. 이 인터페이스는 숨겨진 인터페이스이므로 간단한 **show interface vlan0** 명령을 사용하여 통계를 볼 수 없습니다.

VLAN 간 라우팅 공통 문제

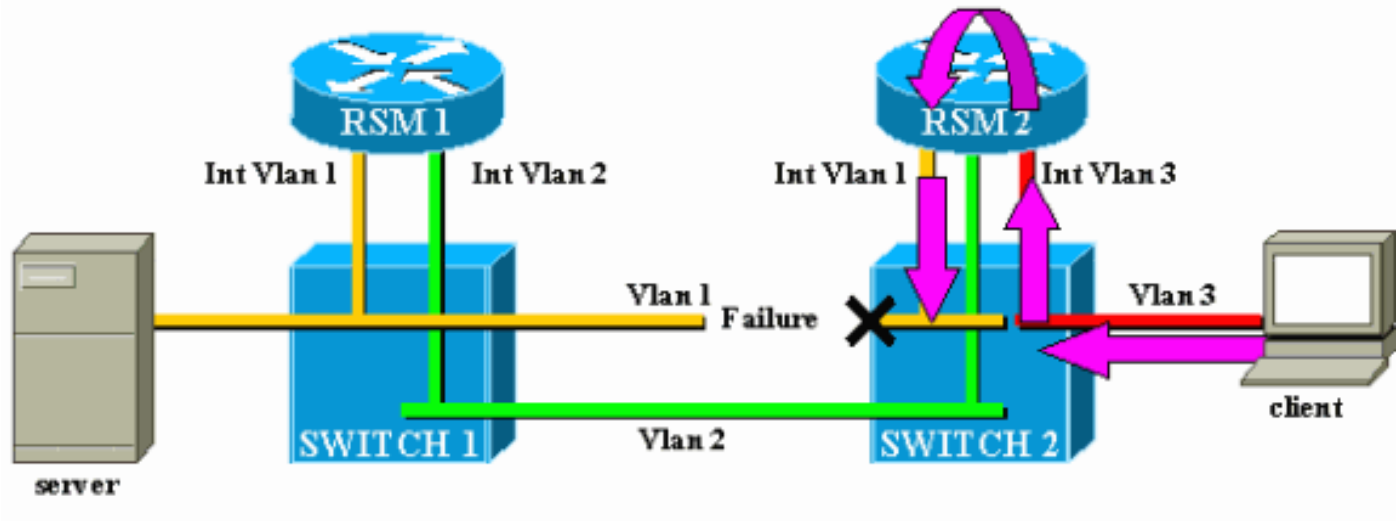
RSM 자동 상태 기능 사용

브리징과 관련하여 자주 발생하는 문제는 연결이 끊어지면 L2 네트워크를 쉽게 두 조각으로 분할할 수 있다는 것입니다. 연속되지 않은 네트워크가 라우팅을 중단하므로 이 상황은 어떠한 비용으로도 피해야 합니다. (일반적으로 이중 링크를 구축하면 이 작업을 수행할 수 있습니다.)

스위치 2에 연결된 클라이언트가 스위치 1에 연결된 서버와 통신하는 이 예를 들어 보겠습니다.



클라이언트에서 서버로의 트래픽만 고려하십시오. VLAN3의 클라이언트에서 들어오는 트래픽은 RSM2에 의해 라우팅됩니다. RSM2는 인터페이스 VLAN2를 통해 서버의 서브넷에 직접 연결됩니다. 보라색 화살표는 다음에 오는 경로를 나타냅니다.

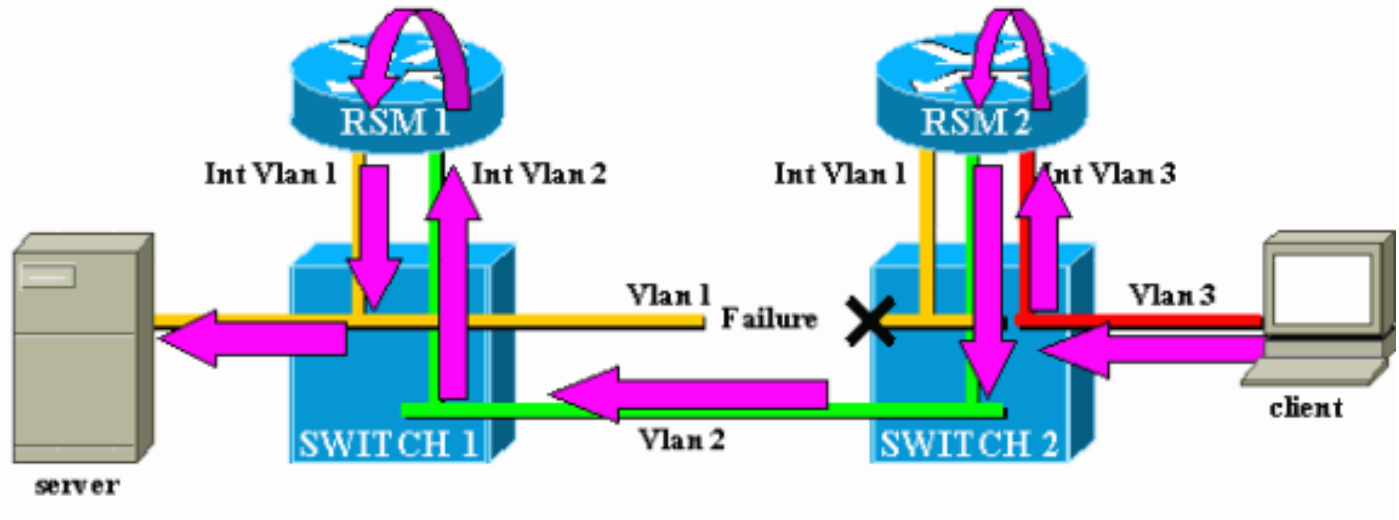


VLAN1에 대해 스위치 1과 스위치 2 간의 링크가 끊어진다고 가정해 보십시오. 여기서 가장 큰 문제는 RSM2의 관점에서 네트워크에서 아무것도 변경되지 않았다는 것입니다. RSM2는 여전히 VLAN1에 직접 연결된 인터페이스를 가지고 있으며, 이 경로를 통해 클라이언트에서 서버로 트래픽을 포워딩합니다. 스위치 2에서 트래픽이 손실되고 클라이언트와 서버 간의 연결이 끊어집니다.

RSM 자동 상태 기능은 이를 해결하도록 설계되었습니다. 스위치에서 특정 VLAN에 대한 포트가 없는 경우 RSM의 해당 VLAN 인터페이스가 중단됩니다.

예를 들어, 스위치 1과 스위치 2 간의 VLAN에 있는 링크가 실패하면 스위치 2의 VLAN1에 있는 유

일한 포트가 다운(링크 다운)됩니다. RSM 자동 상태 기능은 RSM2에서 인터페이스 VLAN1을 비활성화합니다. 인터페이스 VLAN1이 다운되었으므로 RSM2는 라우팅 프로토콜을 사용하여 서버로 향하는 패킷의 다른 경로를 찾고 궁극적으로는 다른 인터페이스를 통해 트래픽을 전달할 수 있습니다. 이 다이어그램은 다음과 같습니다.



RSM 자동 상태는 VLAN에 다른 포트가 없는 경우에만 작동합니다. 예를 들어, VLAN1의 다른 클라이언트가 스위치 2에 연결되었거나 인터페이스 VLAN1이 정의된 섀시의 RSM에 연결된 경우 스위치 1과 스위치 2 간의 링크가 실패한 경우 인터페이스 VLAN1이 비활성화되지 않습니다. 그러면 트래픽이 다시 중단될 것입니다.

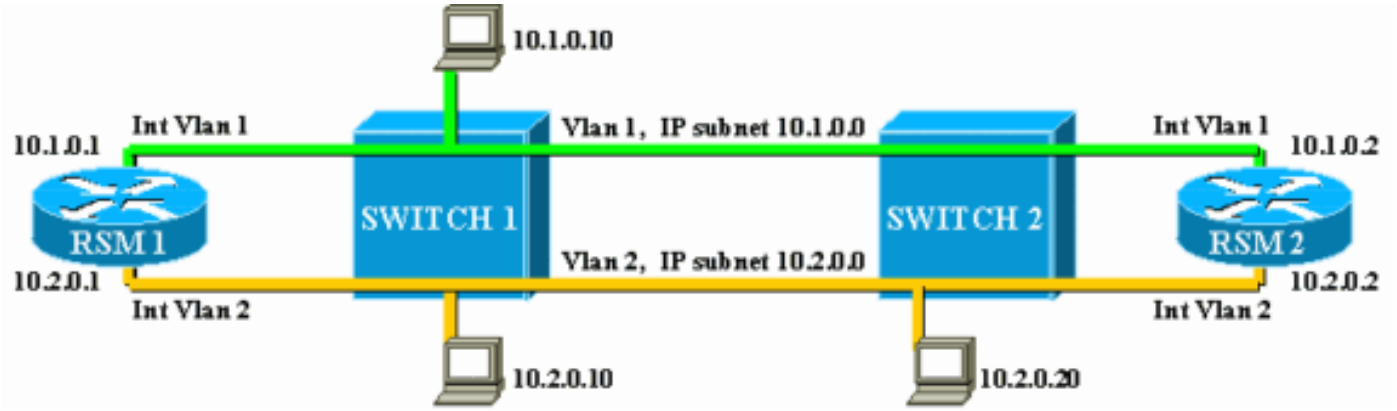
RSM 자동 상태 기능은 기본적으로 활성화되어 있습니다. 필요한 경우 Supervisor Engine에서 set rsmautostate 명령을 사용하여 수동으로 비활성화할 수 있습니다.

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

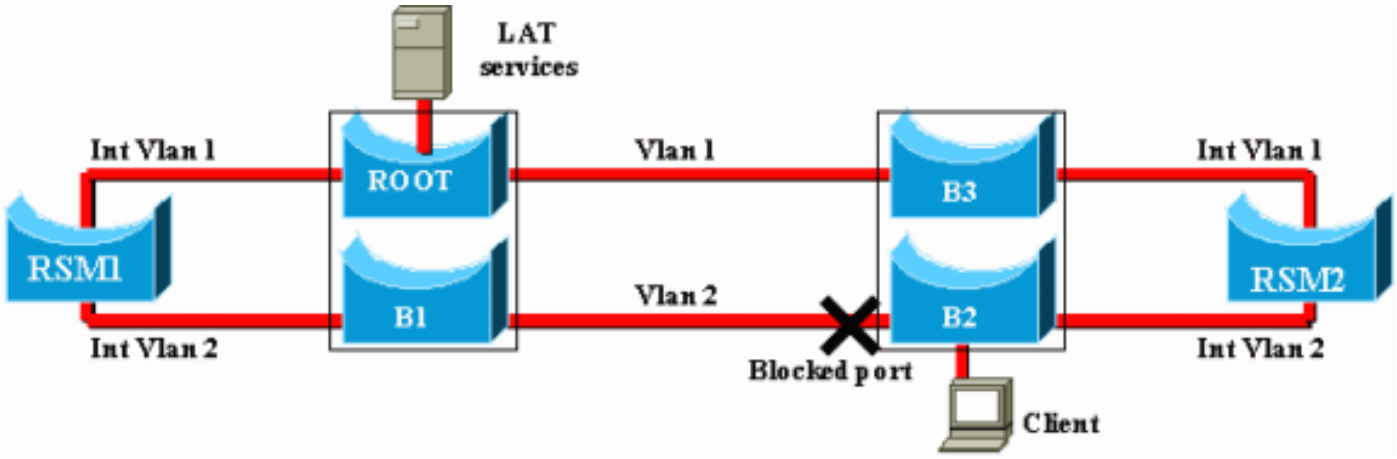
폴백 브리징

폴백 브리징은 VLAN 간 브리징 프로토콜과 다른 일부 라우팅을 통해 구성됩니다. 가능한 경우 이러한 종류의 컨피그레이션은 피하고 일시적인 마이그레이션 기간 동안에만 사용해야 합니다. 일반적으로 서로 다른 VLAN에 각각 다른 IP 서브넷을 사용하여 네트워크를 분할했지만, 라우팅 불가능한 일부 오래된 프로토콜(예: LAT[local area transport])을 계속 브리징하려는 경우 이 방법이 필요합니다. 이 경우 RSM을 IP용 라우터로 사용하되 다른 프로토콜의 브리지로 사용하려고 합니다. 이는 단순히 RSM 인터페이스에서 브리징을 구성하고 IP 주소를 유지함으로써 가능합니다. 다음 예에서는 폴백 브리징을 사용하는 매우 단순한 네트워크와 이러한 컨피그레이션에서 발생할 수 있는 가장 일반적인 문제를 보여줍니다.

이 매우 단순한 네트워크는 두 개의 서로 다른 IP 서브넷에 해당하는 두 개의 VLAN으로 구성됩니다. 지정된 VLAN의 호스트는 두 RSM 중 하나를 기본 게이트웨이(또는 HSRP[Hot Standby Router Protocol] 사용 둘 다)로 사용할 수 있으므로 다른 VLAN의 호스트와 통신할 수 있습니다. 네트워크는 다음과 같습니다.

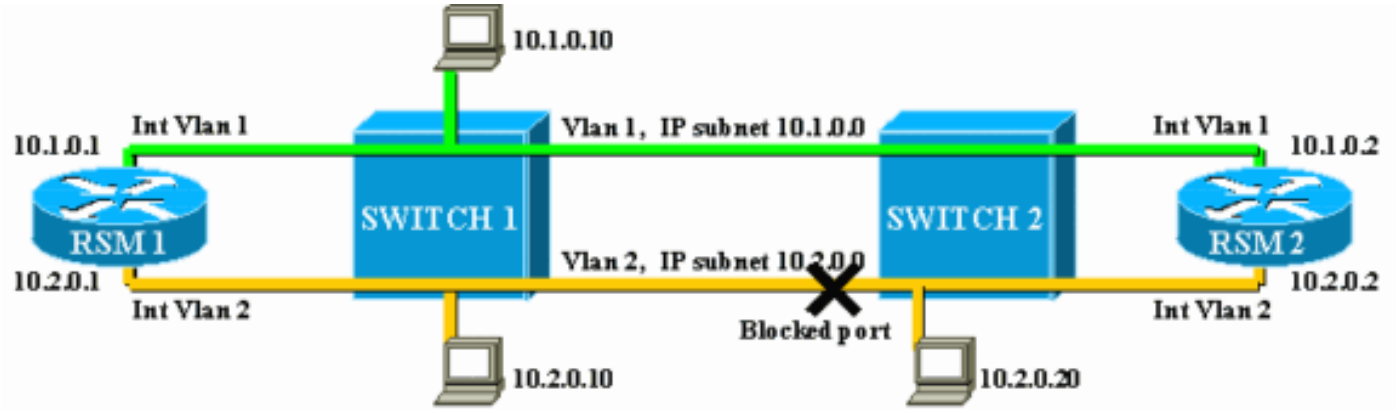


두 RSM 모두 VLAN1과 VLAN2 인터페이스 간에 다른 프로토콜을 연결하도록 구성됩니다. LAT 서비스를 제공하는 호스트와 이를 사용하는 클라이언트가 있다고 가정합니다. 네트워크는 다음과 같습니다.



이 다이어그램에서는 각 Catalyst가 두 개의 서로 다른 브리지(각 VLAN에 하나씩)로 분할됩니다. 두 VLAN 간의 브리징으로 인해 두 VLAN이 통합되었음을 알 수 있습니다. 브리지 프로토콜에 관한 한 VLAN은 하나만 있고 LAT 서버와 클라이언트는 직접 통신할 수 있습니다. 물론 이는 네트워크에 루프가 있으며 STP가 하나의 포트를 차단해야 한다는 것을 의미합니다.

보시다시피 이 차단 포트에서 문제가 발생할 것입니다. 스위치는 순수 L2 디바이스이며 IP와 LAT 트래픽을 구별할 수 없습니다. 따라서 스위치 2가 위 다이어그램과 같이 한 포트를 차단하는 경우 모든 트래픽 유형(IP, LAT 또는 기타)을 차단합니다. 이로 인해 네트워크는 다음과 같습니다.

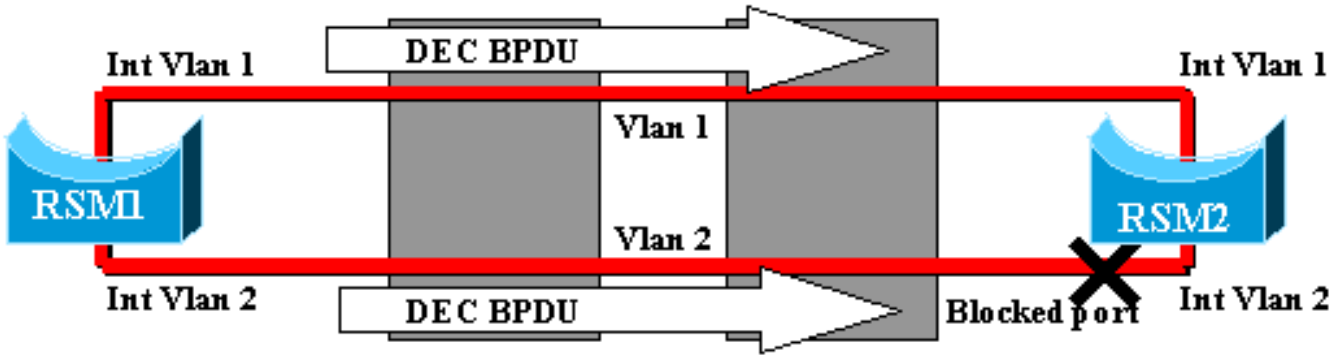


VLAN2는 두 부분으로 분할되며 연속되지 않는 서브넷 10.2.0.0이 있습니다. 이 구성에서는 호스트 10.2.0.10이 동일한 서브넷 및 VLAN에 있지만 호스트 10.2.0.20과 통신할 수 없습니다.

이 솔루션은 L2 및 L3 트래픽을 구별할 수 있는 유일한 디바이스에서 차단된 포트를 이동하는 것입니다. 해당 디바이스가 RSM입니다. 이를 실현하는 두 가지 주요 방법은 다음과 같습니다.

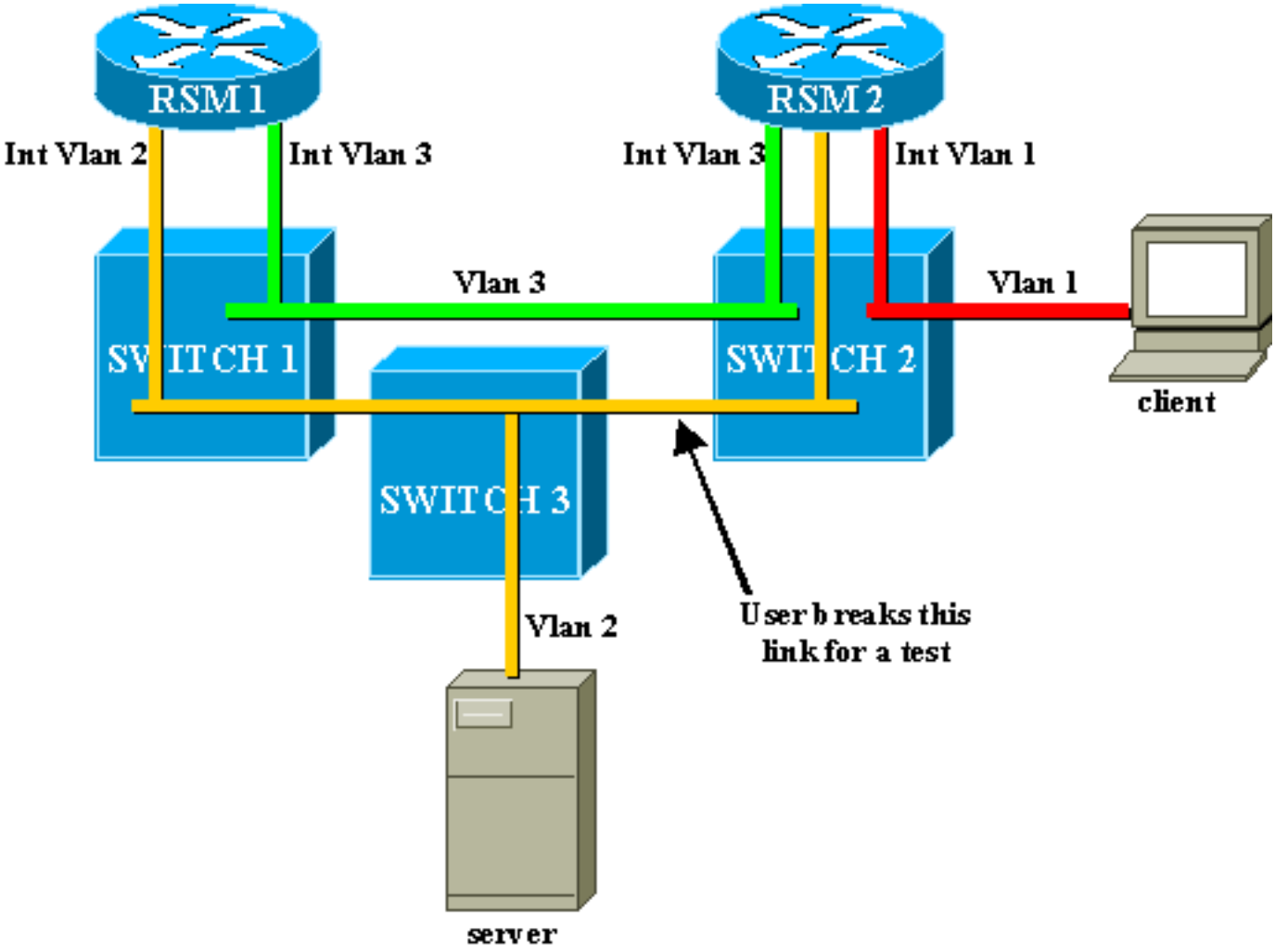
- **STP 매개변수를 튜닝하여 다음을 수행합니다.** 차단 포트가 RSM1 또는 RSM2에 위치하도록 하나 또는 여러 디바이스의 비용을 늘려야 합니다. 이 방법은 유연하지 않으며 매우 엄격한 STP 구성을 의미합니다. 스위치를 추가하거나 링크 대역폭(Fast EtherChannel 또는 기가비트 이더넷)을 변경하면 튜닝이 완전히 재작업될 수 있습니다.
- **RSM에서 다른 STA(Spanning Tree Algorithm)를 사용하여 다음을 수행합니다.** 이 스위치는 IEEE STA만 실행하며 DEC STP에 완전히 투명합니다. 두 RSM에서 DEC STP를 구성하는 경우, RSM은 직접 연결된 것처럼 작동하며, 그중 하나가 차단됩니다. 이 다이어그램은 다음과 같습니다

.



임시 블랙홀(ST 컨버전스)

장애 발생 시 네트워크 재구성 속도를 테스트하는 고객은 STP와 관련된 구성 문제를 처리하는 경우가 많습니다. 클라이언트가 서로 다른 두 경로를 통해 서버에 액세스하는 다음 네트워크를 고려하십시오. 기본적으로 클라이언트에서 서버로의 트래픽은 RSM2에 의해 인터페이스 VLAN2를 통해 라우팅됩니다.



테스트를 수행하기 위해 사용자는 스위치 2와 스위치 3 간의 링크를 끊습니다. 즉시 해당 포트가 다운되고 RSM 자동 상태 기능이 RSM2의 인터페이스 VLAN2를 다운합니다. 서버에 대해 직접 연결된 경로는 RSM2의 라우팅 테이블에서 사라지며, RSM1을 통해 새 경로를 빠르게 학습합니다. OSPF(Open Shortest Path First) 또는 IGRP Interiwan Routing Protocol(Enhanced Interigrp Routing Protocol)과 같은 효율적인 라우팅 프로토콜을 사용합니다. 컨버전스가 너무 빠르므로 이 작업 중에 ping을 거의 잃을 수 없습니다.

장애 발생 시 두 경로(노란색 VLAN2 및 녹색 VLAN3) 간의 전환이 즉시 이루어집니다. 그러나 사용자가 스위치 2와 스위치 3 간의 링크를 다시 설정하면 클라이언트는 약 30초 동안 서버와의 연결이 끊깁니다.

그 이유는 STA와도 관련이 있습니다. STA를 실행할 때 새로 연결된 포트가 먼저 수신 및 학습 단계를 거쳐 전달 모드로 끝납니다. 처음 두 15초 단계 동안 포트가 작동하지만 트래픽을 전송하지는 않습니다. 즉, 링크가 연결되자마자 RSM 자동 상태 기능은 RSM2에서 인터페이스 VLAN2를 즉시 다시 활성화하지만, 스위치 2와 스위치 3 사이의 링크의 포트가 전달 단계에 도달할 때까지 트래픽은 통과할 수 없습니다. 이렇게 하면 클라이언트와 서버 간의 임시 연결이 끊길 수 있습니다. 스위치 1과 스위치 2 간의 링크가 트렁크가 아닌 경우 PortFast 기능을 활성화하여 수신 및 학습 단계를 건너뛰고 즉시 통합할 수 있습니다.

참고: PortFast는 트렁크 포트에서 작동하지 않습니다. 자세한 내용은 PortFast 및 기타 명령을 사용하여 워크스테이션 시작 연결 지연 문제 해결을 참조하십시오.

결론

이 문서에서는 일부 RSM 관련 문제와 매우 일반적인 VLAN 간 라우팅 문제에 대해 중점적으로 설명합니다. 이 정보는 일반적인 모든 Cisco IOS 라우터 문제 해결 절차를 시도했을 때만 유용합니다. RSM에서 라우팅한 패킷의 절반이 잘못된 라우팅 테이블 때문에 손실된 경우 DMA 채널 통계를 해석하는 데 도움이 되지 않습니다. 일반적인 interVLAN 라우팅 문제도 고급 주제이며 자주 발생하지 않습니다. 대부분의 경우, RSM(또는 스위치 내의 다른 통합 라우팅 디바이스)을 단순한 외부 Cisco IOS 라우터로 간주하면 스위치드 환경에서 라우팅 문제를 해결할 수 있습니다.

관련 정보

- IP 라우팅 프로토콜 지원 페이지
- IP 멀티레이어 스위칭 문제 해결
- InterVLAN 라우팅 구성
- PortFast 및 기타 명령을 사용하여 워크스테이션 시작 연결 지연 수정
- LAN 제품 지원 페이지
- LAN 스위칭 지원 페이지
- 기술 지원 및 문서 – Cisco Systems