Fehlerbehebung für das Catalyst 500 Route Switch Module (RSM) und InterVLAN Routing

Inhalt

Einführung

Dieses Dokument enthält Informationen zur Fehlerbehebung beim VLAN-übergreifenden Routing mit einem Route Switch Module (RSM) auf einem Switch der Catalyst 5000-Familie. Wenn es um die Fehlerbehebung des RSM geht, ist es zunächst, es als einfachen externen Router zu betrachten. Es ist sehr selten, dass ein RSM-spezifisches Problem ein Problem beim Inter-VLAN-Routing verursacht. Daher werden in diesem Dokument nur die beiden Hauptbereiche behandelt, in denen dies auftreten könnte:

- **Hardwarebezogene Probleme mit RSM**: In diesem Dokument wird die RSM-Architektur vorgestellt und es werden Einzelheiten zu den zusätzlichen RSM-bezogenen Zählern für die Nachverfolgung aufgeführt.
- **Spezifische Fragen zur Inter-VLAN-Konfiguration** (hauptsächlich im Zusammenhang mit der Interaktion zwischen Routern und Switches): Dies gilt auch für andere interne Router (z. B. die Multilayer Switch Feature Card [MSFC], Route Switch Feature Card [RSFC], 8510CSR usw.) und häufig auch für externe Router.

Hinweis: Dieses Dokument behandelt nicht die Konfiguration von Inter-VLAN-Routing auf Catalyst Switches der Serien 4000, 5000 und 6000. Weitere Informationen finden Sie in den folgenden

Dokumenten:

- Konfiguration und Übersicht des Routermoduls für die Catalyst 4500/4000-Familie (WS-X4232-L3)
- *Konfigurieren des Moduls für InterVLAN Routing* im Abschnitt Installations- und Konfigurationshinweise für das Catalyst 4000 Layer 3 Services Module
- Konfigurieren von Inter-VLAN-Routing mithilfe eines internen Routers (Layer-3-Karte) auf Catalyst Switches der Serien 5500/5000 und 6500/6000, auf denen CatOS-Systemsoftware ausgeführt wird

Dieses Dokument behandelt weder grundlegende Probleme mit Routing-Protokollen noch Probleme im Zusammenhang mit Multilayer Switching (MLS).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

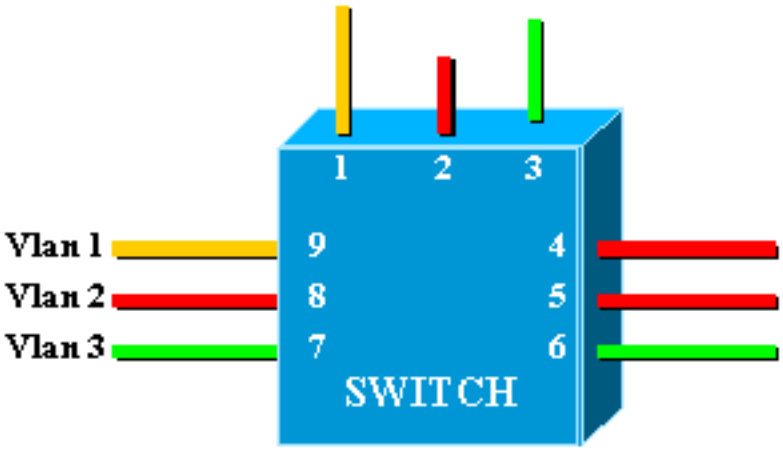
Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

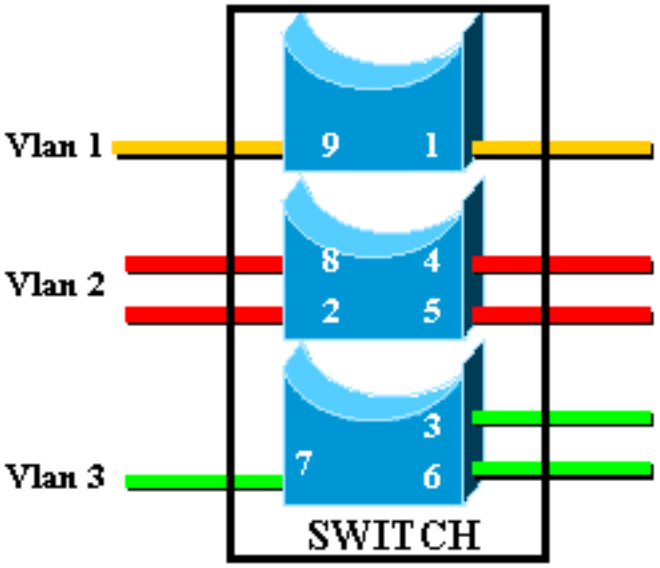
Was ist Inter-VLAN-Routing?

Bevor Sie Inter-VLAN-Routing besprechen, konzentriert sich dieses Dokument auf das VLAN-Konzept. Dies ist keine theoretische Diskussion über die Notwendigkeit von VLANs, sondern erläutert lediglich die Funktionsweise von VLANs auf einem Switch. Wenn Sie VLANs auf Ihrem Switch erstellen, ist es so, als ob Sie Ihren Switch in mehrere virtuelle Bridges aufteilen, wobei jeder einzelne nur Bridging-Ports zum gleichen VLAN gehört.

Dieses Diagramm stellt einen Switch dar, dem drei verschiedene VLANs neun Ports zugewiesen sind:



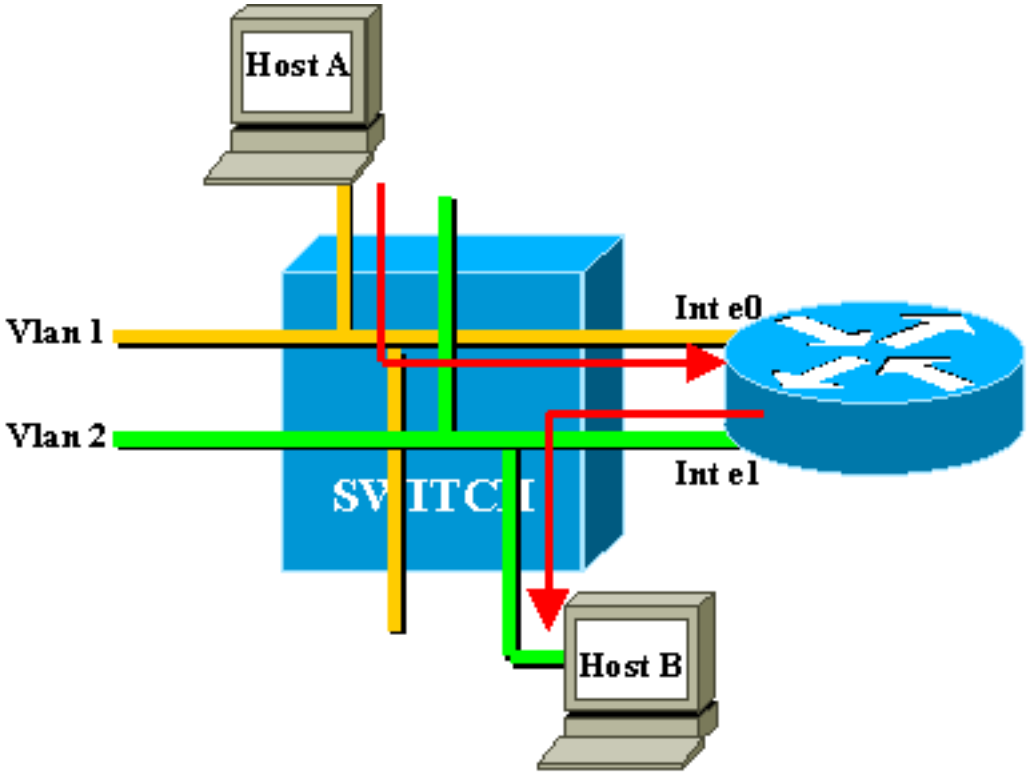
Dies entspricht genau dem folgenden Netzwerk, das aus drei unabhängigen Bridges besteht:



Im Switch gibt es drei verschiedene Bridges, da jedes VLAN eine separate Bridge erstellt. Da jedes VLAN eine separate STP-Instanz (Spanning Tree Protocol) erstellt, unterhält STP drei verschiedene Weiterleitungstabellen.

Im zweiten Diagramm wird deutlich, dass Ports, die zu unterschiedlichen VLANs gehören, zwar mit demselben physischen Gerät verbunden sind, jedoch nicht direkt auf Layer 2 (L2) kommunizieren können. Auch wenn dies möglich wäre, wäre dies nicht angemessen. Wenn Sie beispielsweise Port 1 mit Port 4 verbinden, müssen Sie einfach VLAN1 mit VLAN2 verbinden. In diesem Fall gibt es keinen Grund für zwei separate VLANs.

Die einzige Verbindung, die Sie zwischen VLANs wünschen, wird auf Layer 3 (L3) durch einen Router erreicht. Dies ist Inter-VLAN-Routing. Zur weiteren Vereinfachung der Diagramme werden VLANs als unterschiedliche physische Ethernet-Segmente dargestellt, da Sie nicht wirklich an den spezifischen Bridging-Funktionen interessiert sind, die der Switch bereitstellt.



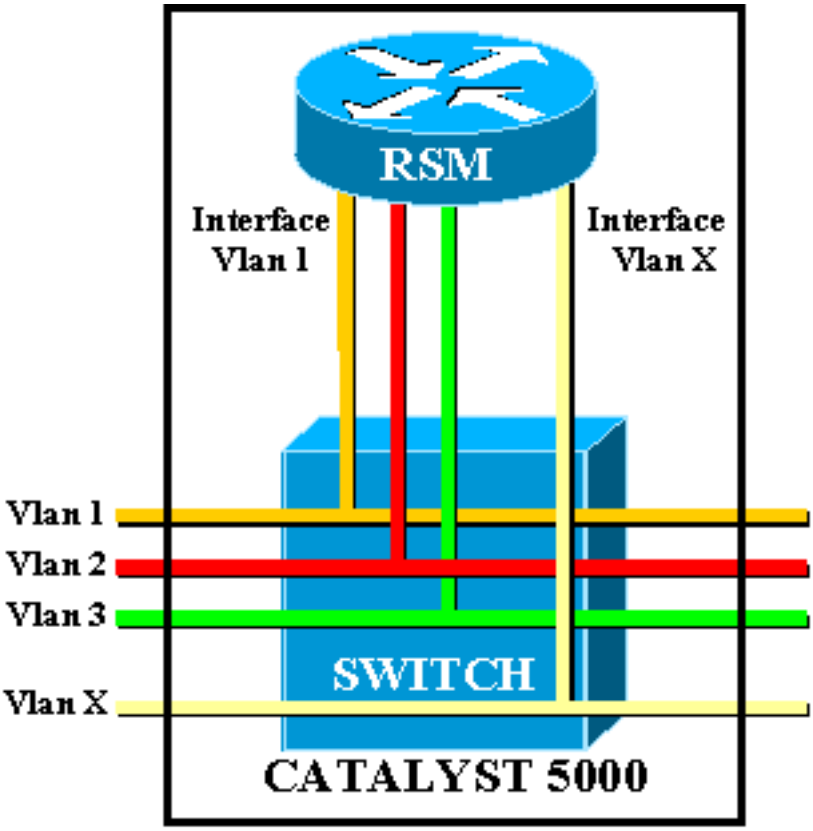
In diesem Diagramm werden die beiden VLANs als zwei verschiedene Ethernet-Segmente betrachtet. Der VLAN-übergreifende Datenverkehr muss über den externen Router geleitet werden. Wenn Host A mit Host B kommunizieren möchte, verwendet er in der Regel den Router als Standard-Gateway.

RSM-Architektur

Logische Architektur

Sie können ein RSM als externen Router anzeigen, der über mehrere Schnittstellen verfügt, die direkt mit den verschiedenen VLANs eines Catalyst 5000-Switches verbunden sind.

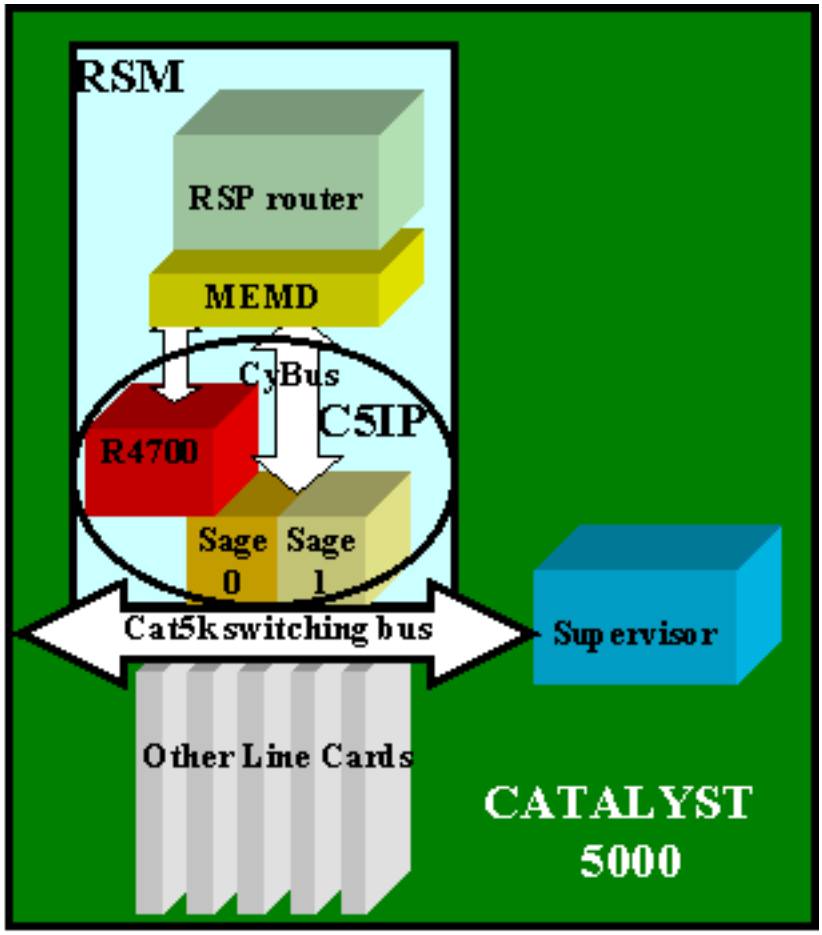
Anstatt als Ethernet-Schnittstelle bezeichnet zu werden, werden diese Schnittstellen nach dem VLAN benannt, mit dem sie verbunden sind. (Schnittstelle VLAN1 ist direkt mit VLAN1 verbunden usw.)



Implementierung der Architektur

Das RSM ist ein Cisco 7500 Route Switch Processor (RSP)-Router innerhalb einer Catalyst 5000 Line Card. Sie müssen nicht viel über die Architektur der Karte wissen, um sie zu konfigurieren und Fehler zu beheben. Eine Vorstellung davon, wie das RSM aufgebaut ist, hilft jedoch zu verstehen, wie es sich von einem normalen externen Router unterscheidet. Dieses Wissen ist besonders wichtig, wenn der Befehl **show controller c5ip** eingeführt wird.

In diesem Diagramm sind die Hauptkomponenten der RSM-Linecard aufgeführt:

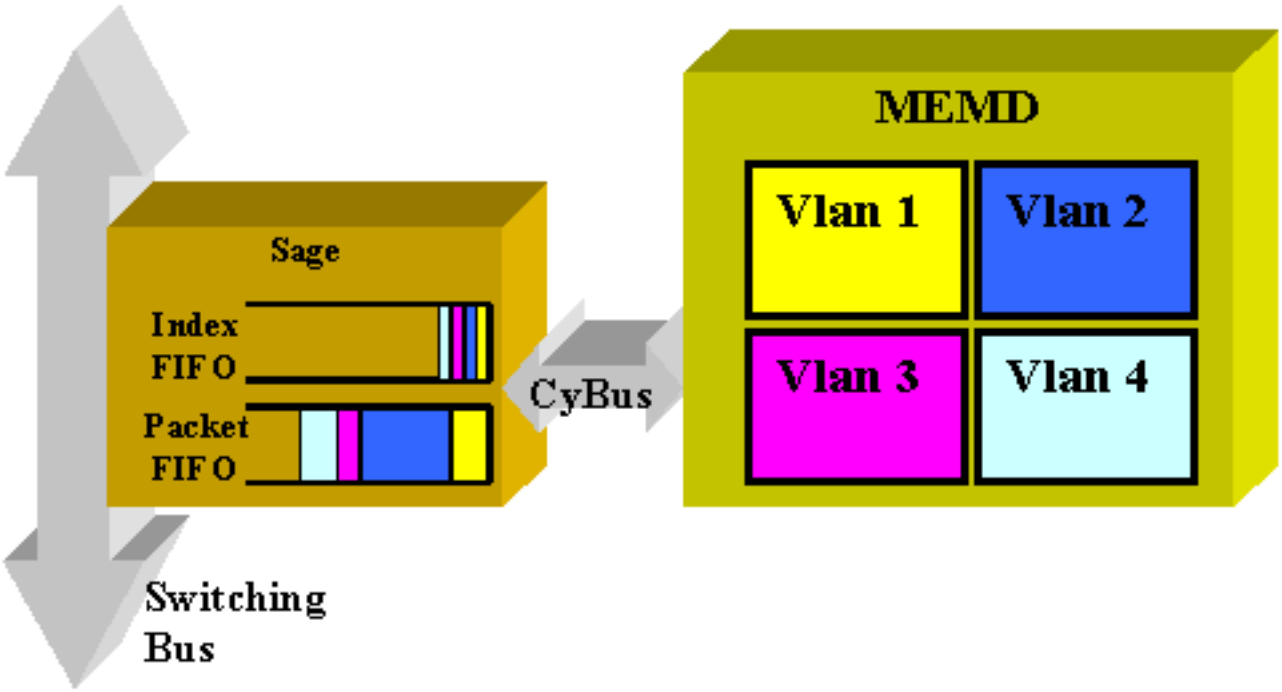


Catalyst 5000-Schnittstellenprozessor

Der Catalyst 5000 Interface Processor (C5IP) ist der Teil des RSM, der eine Catalyst 7500-System-IP emuliert, wobei der Catalyst 5000-Switching-Bus die Netzwerkschnittstelle darstellt. Der C5IP umfasst einen R4700-Prozessor sowie zwei ASICs (Application-Specific Integrated Circuits) von SAGE, die für den Zugriff auf den Catalyst 5000-Switching-Bus verantwortlich sind.

SAGE

Diese beiden ASICs empfangen Pakete vom/zum Switching-Bus und puffern sie. Neben den Daten im Paket erhalten sie auch einen Index, der das Ziel des Pakets im Switch identifiziert.



Die Ziel-VLAN-Schnittstelle wird nicht vom Inhalt des Pakets selbst bestimmt, sondern vom Index abgeleitet. Das Paket und der Index werden zunächst in zwei verschiedenen FIFOs im SAGE gespeichert. Der Index wird gelesen, und der erforderliche gemeinsam genutzte Speicher ist im Bereich des Ziel-VLANs reserviert. Das Paket wird dann mithilfe eines Direct Memory Access (DMA) in das Speichergerät (MEMD) kopiert.

Zwei SAGEs, die parallel arbeiten, um zwischen Router und Switching-Bus zu kommunizieren, können zu einer Paketübermittlung außerhalb der Sequenz führen. (Beispielsweise könnte ein großes Paket, das auf SAGE0 empfangen wurde, nach einem kleinen Paket übertragen werden, das später von SAGE1 empfangen wurde.) Um dies zu vermeiden, wird jedes VLAN einem bestimmten SAGE statisch zugewiesen. Dies erfolgt automatisch beim Start. (Dem Router zufolge ist ein VLAN einem der beiden DMA-Kanäle zugeordnet, von denen jeder zu einem SAGE führt.) Pakete aus einem bestimmten VLAN werden immer nacheinander geliefert.

MITGLIED

MEMD ist der freigegebene Speicher, der vom Router zum Senden und Empfangen von Paketen verwendet wird. Jeder konfigurierten VLAN-Schnittstelle im RSM wird ein Teil des verfügbaren gemeinsamen Speichers zugewiesen. Je mehr VLAN-Schnittstellen konfiguriert werden, desto weniger gemeinsam genutzter Arbeitsspeicher pro Schnittstelle. Die VLAN-Schnittstellen halten ihren Teil des gemeinsam genutzten Speichers auch dann, wenn sie deaktiviert oder heruntergefahren werden. Nur beim administrativen Hinzufügen oder Entfernen einer VLAN-Schnittstelle wird eine neue Trennung des MEMD zwischen den VLAN-Schnittstellen ausgelöst.

RSM-spezifische Fehlerbehebung

Die wichtigsten RSM-spezifischen Probleme, die in der Cisco IOS® Router-Dokumentation nicht behandelt werden, sind Probleme beim Zugriff auf das RSM sowie Leistungsprobleme.

Zugriff auf das RSM

Der Zugriff auf das RSM erfolgt auf drei verschiedene Arten:

Telnet zum RSM

Um Telnet in das RSM einbinden zu können, müssen Sie die IP-Adresse kennen, die einer der VLAN-Schnittstellen zugewiesen ist. Die Telnet-Sitzung funktioniert genau so, als ob Sie versucht hätten, eine Verbindung zu einem normalen Cisco IOS-Router herzustellen. Möglicherweise müssen Sie dem VTY ein Kennwort zuweisen, um Telnet zu erreichen und den Zugriff zu aktivieren.

Dieses Beispiel zeigt eine Telnet-Sitzung von einer Supervisor Engine zu einem RSM, in der die IP-Adresse von VLAN1 10.0.0.1 lautet:

```
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
```

Dies ähnelt anderen Cisco IOS-Konfigurationen für externe Router.

Sitzung wird vom Switch-Supervisor in das RSM übernommen

Mit dem Befehl **session *x*** von der Supervisor Engine wird eine Verbindung zum RSM in Steckplatz *x hergestellt*.

Die Methode ist die gleiche wie die vorherige: Das RSM verfügt über eine versteckte VLAN0-Schnittstelle mit der IP-Adresse 127.0.0 (x+1), wobei x der Steckplatz ist, in dem das RSM installiert ist. Der Befehl **session** gibt eine ausgeblendete Telnet-Sitzung an diese Adresse aus.

Hinweis: vty und enable passwords müssen nicht in der Konfiguration enthalten sein, um vollständigen Zugriff auf das RSM zu erhalten.

```
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#
```

Mit dem Supervisor Engine-Befehl **show module** können Sie den Steckplatz identifizieren, in dem das RSM im Switch installiert ist. Sie können direkt mit dem Befehl **session** darauf zugreifen.

Direkte Konsolenverbindung

Der Systemkonsolen-Port des RSM ist ein DB-25-Steckplatz-DCE-Port zum Anschluss eines Datenterminal, über den Sie ein Datenterminal konfigurieren und mit Ihrem System kommunizieren können. Verwenden Sie das mitgelieferte Konsolenkabel, um das Terminal mit dem Konsolenport am RSM zu verbinden. Der Konsolenport befindet sich im RSM neben dem AUX-Port und ist als Konsole gekennzeichnet.

Überprüfen Sie vor dem Anschließen des Konsolenports in der Terminaldokumentation die Baudrate des Terminals, das Sie verwenden werden. Die Baudrate des Terminals muss der Standardbaudrate (9600 Baud) entsprechen. Richten Sie das Terminal wie folgt ein: 9600 Baud, acht Datenbits, keine Parität und zwei Stoppbits (9600,8N2).

Zugriff auf das RSM nicht möglich

Das RSM kann aus mehreren Gründen isoliert werden. Auch wenn man keine Verbindung dazu hat, kann man von außen einige Lebenszeichen erkennen:

- Überprüfen Sie den Status der LEDS im RSM:CPU Halt LED is OFF (CPU-Halt-LED leuchtet nicht) - System hat einen Prozessor-Hardwarefehler erkannt.Orangefarbene STATUS-LED - Modul deaktiviert, Test wird ausgeführt oder System wird gestartet.
- Überprüfen Sie die Supervisor Engine, ob der Switch das RSM sehen kann. Führen Sie dazu den Befehl **show module aus**:

```
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.
```

Deklarieren Sie das RSM niemals als tot, bevor Sie versucht haben, die Konsolenverbindung herzustellen. Wie Sie gesehen haben, beruht der Zugriff auf Sitzungen und Telnet auf einer IP-Verbindung mit dem RSM. Wenn das RSM bootet oder beispielsweise im ROMMON-Modus feststeckt, können Sie keine Telnet- oder Sitzungsverbindung herstellen. Das ist jedoch ganz normal.

Selbst wenn das RSM fehlerhaft zu sein scheint, versuchen Sie, eine Verbindung zu seiner Konsole herzustellen. Dadurch können Sie möglicherweise einige Fehlermeldungen sehen, die dort angezeigt werden.

Leistungsprobleme

Die meisten Leistungsprobleme im Zusammenhang mit dem RSM können auf die gleiche Weise behoben werden wie bei einem normalen Cisco IOS-Router. In diesem Abschnitt wird der spezifische Teil der RSM-Implementierung (C5IP) behandelt. Der Befehl **show controller c5ip** kann Informationen zum Betrieb des C5IP liefern. In dieser Ausgabe werden einige der wichtigsten Felder beschrieben:

```
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-Kanal 0/1

Der RSP-Router im RSM kommuniziert mit dem Switch über zwei verschiedene DMA-Kanäle (zu den beiden SAGE-ASICs). Jede VLAN-Schnittstelle wird automatisch einem dieser DMA-Kanäle zugeordnet. Der Befehl **show controller c5ip** zeigt Informationen zu jedem einzelnen in zwei verschiedenen Abschnitten an.

Empfangen/übertragen

Diese Statistiken helfen, die Last auf den verschiedenen DMA-Kanälen zu identifizieren. Suchen Sie nach einem DMA-Kanal, der im Vergleich zu den anderen ständig überlastet ist. Dies kann auftreten, wenn alle datenintensiven VLANs demselben DMA-Kanal zugewiesen sind. Bei Bedarf können Sie VLAN-Schnittstellen einem bestimmten DMA-Kanal manuell mit dem Schnittstellenbefehl **dma-channel** zuweisen.

Verworfen

Dies gibt die Anzahl der Pakete an, die das RSM empfangen, aber verworfen hat. Dies geschieht, wenn der mit dem Paket empfangene Index das RSM nicht als spezifisches Ziel des Pakets angibt.

Fehlerzählungen

- **crc**: CRC-Fehler (Cyclical Redundancy Cycle) treten auf, wenn ein fehlerhaftes CRC vom RSM erkannt wird. Auf der Backplane sollten keine Pakete mit fehlerhaften CRCs vorhanden sein, und das RSM, das diese erkennt, weist darauf hin, dass einige Linecards oder andere mit der Backplane verbundene Geräte nicht ordnungsgemäß funktionieren.**Hinweis:** CRC-Fehler können auch von einem Remote-Gerät verursacht werden, das über einen ISL-Trunk angeschlossen ist. Die meisten Catalyst Line Cards überprüfen nicht das CRC eines Pakets, das sie von der Backplane empfangen, und leiten es auf einem Trunk weiter.
- **index** - Indexfehler treten auf, wenn der Index nicht korrekt ist. Der C5IP ist sich nicht bewusst, warum er dieses Paket erhalten hat. Dadurch wird auch der Dropped-Zähler erhöht.

- **dmac-length** - Diese Fehler treten auf, wenn die C5IP-Schnittstelle verhindert, dass der SAGE ASIC eine MTU-Größe (Maximum Transmission Unit) überläuft, die, wenn sie nicht erkannt wurde, den gemeinsamen Speicher des Routers beschädigt hätte.
- **dmac-synch**: Wenn ein SAGE-ASIC ein Paket verwirft, werden FIFO-Paket und FIFO-Index nicht synchronisiert. Wenn dieser Fehler auftritt, wird er automatisch erkannt und der Zähler `dmac-synch` erhöht. Es ist unwahrscheinlich, dass dies geschieht, aber wenn dies der Fall ist, sind die Auswirkungen auf die Leistung extrem gering.
- **dmac-timeout** - Dieser Zähler wurde dem Befehl **show controller c5ip** in den Cisco IOS Software Releases 11.2(16)P und 12.0(2) hinzugefügt. Es erhöht sich, wenn eine DMA-Übertragung nicht innerhalb der für die längstmögliche Übertragung erforderlichen maximalen Zeit abgeschlossen wird. Sie weist auf einen Hardwarefehler hin, und ein RSM mit einem Wert von 0 (null) für diesen Leistungsindikator ist ein geeigneter Ersatz.
- **ignore** - Ignorieren tritt auf, wenn dem Router die MEMD-Puffer für Eingabepakete ausgehen. Dies geschieht, wenn die CPU Pakete nicht so schnell verarbeitet, wie sie eingehen. Dies liegt wahrscheinlich daran, dass die CPU immer ausgelastet ist.
- **line-down** - Die Line-Down-Funktion gibt an, dass Pakete, die für ein Line Protocol Down VLAN bestimmt sind, verworfen wurden. Der C5IP hat ein Paket für eine VLAN-Schnittstelle empfangen, von der angenommen wird, dass sie ausgefallen ist. Dies sollte nicht passieren, da der Switch die Weiterleitung von Paketen an eine ausgefallene RSM-Schnittstelle beenden soll. Sie sehen jedoch möglicherweise einige wenige, wenn eine Schnittstelle ausfällt. Dies liegt an der Zeitangabe zwischen dem RSM, in dem die Schnittstelle deaktiviert wurde, und dem Switch, der benachrichtigt wird.
- **runt/gigant**: Dieser Zähler verfolgt Pakete ungültiger Größe.
- **Unicast-Flood**: Unicast-Flood-Pakete sind Pakete, die an eine bestimmte MAC-Adresse gesendet werden. Die Catalyst 5000 Content Addressable Memory (CAM)-Tabelle weiß nicht, an welchem Port sich die MAC-Adresse befindet, sodass das Paket an alle Ports im VLAN überflutet wird. Das RSM empfängt diese Pakete ebenfalls. Wenn es jedoch nicht für das Bridging in diesem VLAN konfiguriert ist, ist es nicht an Paketen interessiert, die nicht mit seiner eigenen MAC-Adresse übereinstimmen. Das RSM wirft diese Pakete weg. Dies entspricht dem, was auf einer echten Ethernet-Schnittstelle im Ethernet-Schnittstellenchip geschieht, der so programmiert ist, dass Pakete für andere MAC-Adressen ignoriert werden. Im RSM erfolgt dies über die C5IP-Software. Die meisten der verworfenen Pakete sind Unicast-Flood-Pakete.
- **Last drop** - Dieser Zähler zeigt spezifische Informationen über das zuletzt verworfene Paket an. Dies sind Informationen auf niedriger Ebene, die nicht in den Anwendungsbereich dieses Dokuments fallen.

VLAN-Verteilung zwischen DMA-Kanälen

Dies ist ein Teil der Ausgabe des Befehls **show controller c5ip** auf einem RSM mit zehn konfigurierten VLAN-Schnittstellen:

```
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
```

Diese Ausgabe zeigt, welchem DMA-Kanal eine bestimmte VLAN-Schnittstelle zugewiesen ist. Sie sehen, dass ungerade VLANs zu Kanal 0 gehen, während selbst VLANs mit Kanal 1 verbunden sind. Bei Bedarf können Sie diese Entsprechung mit dem Schnittstellenkonfigurationsbefehl **dma-channel** festschreiben. Dieses Beispiel zeigt, wie die Schnittstelle VLAN1 eines RSM dem DMA-Kanal 0 zugewiesen wird:

```
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-Informationen

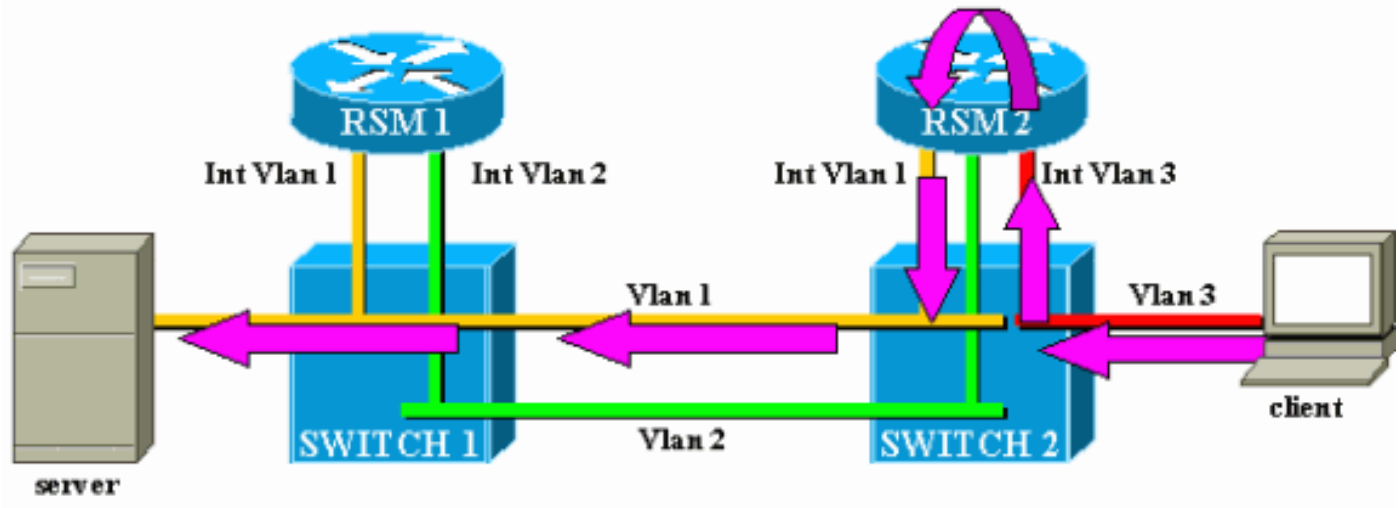
Der Hauptzweck von VLAN0 besteht in der Sicherstellung einer effektiven Kommunikation mit der Supervisor Engine des Switches. Da es sich um eine versteckte Schnittstelle handelt, können Sie mit dem Befehl **show interface vlan0** Statistiken darüber nicht anzeigen.

Häufige Probleme beim VLAN-Routing

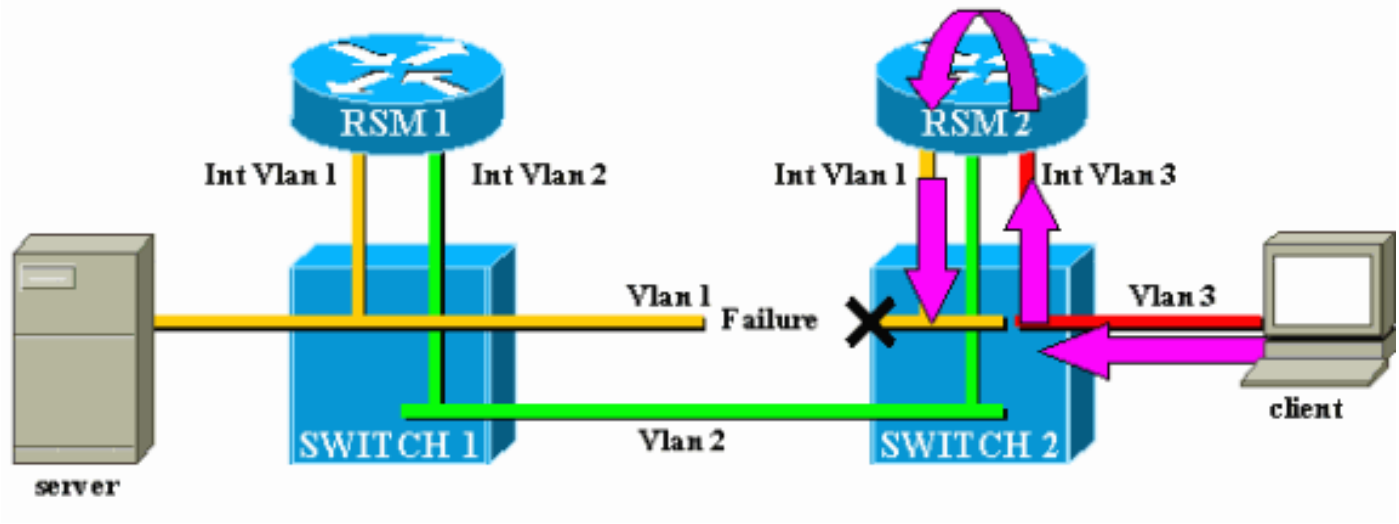
Verwenden der RSM Autostate-Funktion

Ein häufiges Problem bei der Überbrückung besteht darin, dass eine unterbrochene Verbindung ein L2-Netzwerk problemlos in zwei Teile aufteilen kann. Diese Situation sollte um jeden Preis vermieden werden, da ein unzusammenhängendes Netzwerk das Routing unterbricht. (Dies wird in der Regel durch die Bereitstellung redundanter Links erreicht.)

In diesem Beispiel kommuniziert ein an Switch 2 angeschlossener Client mit einem an Switch 1 angeschlossenen Server:



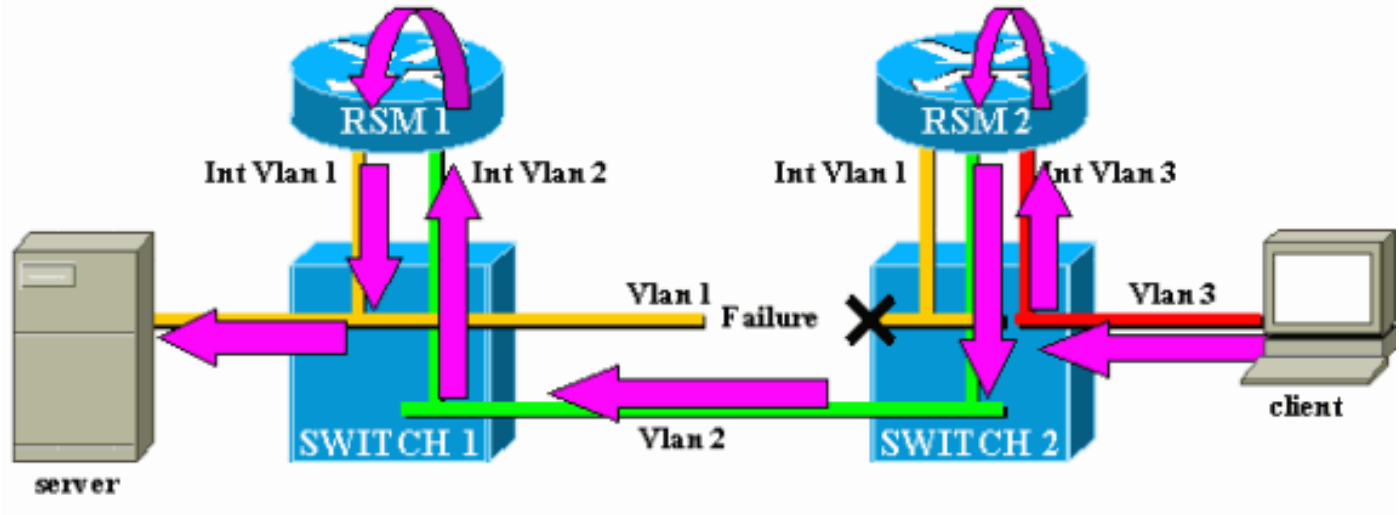
Berücksichtigen Sie nur den Datenverkehr vom Client zum Server. Eingehender Datenverkehr vom Client in VLAN3 wird von RSM2 geroutet, das über seine Schnittstelle VLAN2 eine direkte Verbindung zum Subnetz des Servers hat. Die lila Pfeile stellen den folgenden Pfad dar:



Angenommen, die Verbindung zwischen Switch 1 und Switch 2 bricht für VLAN1. Das Hauptproblem dabei ist, dass sich aus Sicht von RSM2 nichts im Netzwerk verändert hat. RSM2 verfügt weiterhin über eine Schnittstelle, die direkt mit VLAN1 verbunden ist. Über diesen Pfad wird der Datenverkehr vom Client zum Server weitergeleitet. In Switch 2 geht Datenverkehr verloren, und die Verbindung zwischen Client und Server ist unterbrochen.

Die RSM-Autostate-Funktion wurde entwickelt, um dies zu erreichen. Wenn auf einem Switch kein Port für ein bestimmtes VLAN vorhanden ist, wird die entsprechende VLAN-Schnittstelle des RSM deaktiviert.

Wenn im Beispiel die Verbindung im VLAN zwischen Switch 1 und Switch 2 ausfällt, fällt der einzige VLAN1-Port auf Switch 2 aus (Link Down). Die RSM-Autostate-Funktion deaktiviert die Schnittstelle VLAN1 auf RSM2. Nachdem die Schnittstelle VLAN1 ausgefallen ist, kann RSM2 ein Routing-Protokoll verwenden, um einen anderen Pfad für Pakete zu finden, die für den Server bestimmt sind, und den Datenverkehr schließlich über eine andere Schnittstelle weiterleiten, wie in diesem Diagramm gezeigt:



Der automatische RSM-Status funktioniert nur, wenn im VLAN kein anderer Port vorhanden ist. Wenn beispielsweise ein anderer Client in VLAN1 an Switch 2 oder ein RSM im Chassis angeschlossen ist und eine Schnittstelle für VLAN1 definiert ist, wird die Schnittstelle VLAN1 nicht

deaktiviert, wenn die Verbindung zwischen Switch 1 und Switch 2 fehlschlägt. Der Datenverkehr würde dann wieder unterbrochen.

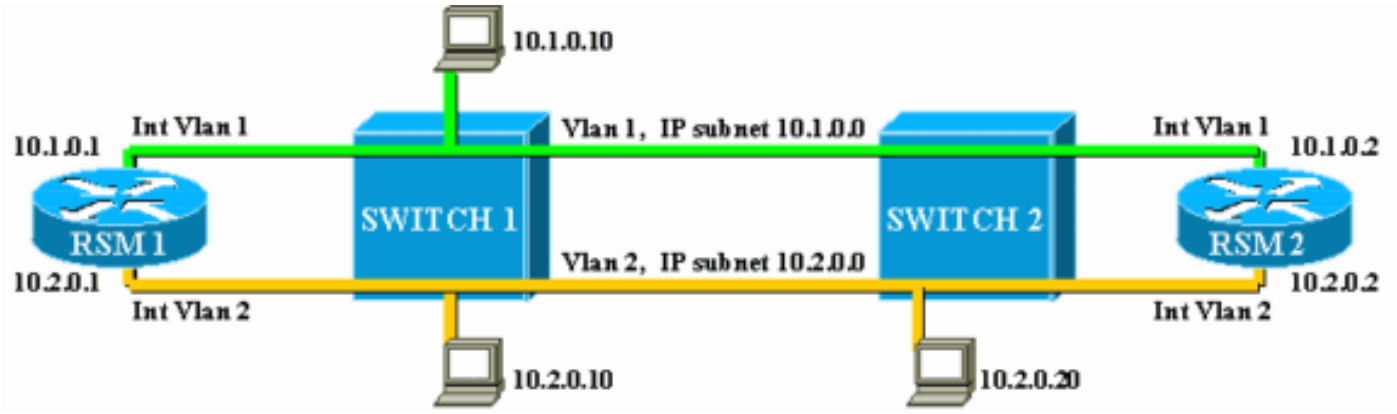
Die RSM-Autostate-Funktion ist standardmäßig aktiviert. Bei Bedarf kann sie manuell mithilfe des Befehls **set rsmautostate** auf der Supervisor Engine deaktiviert werden:

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

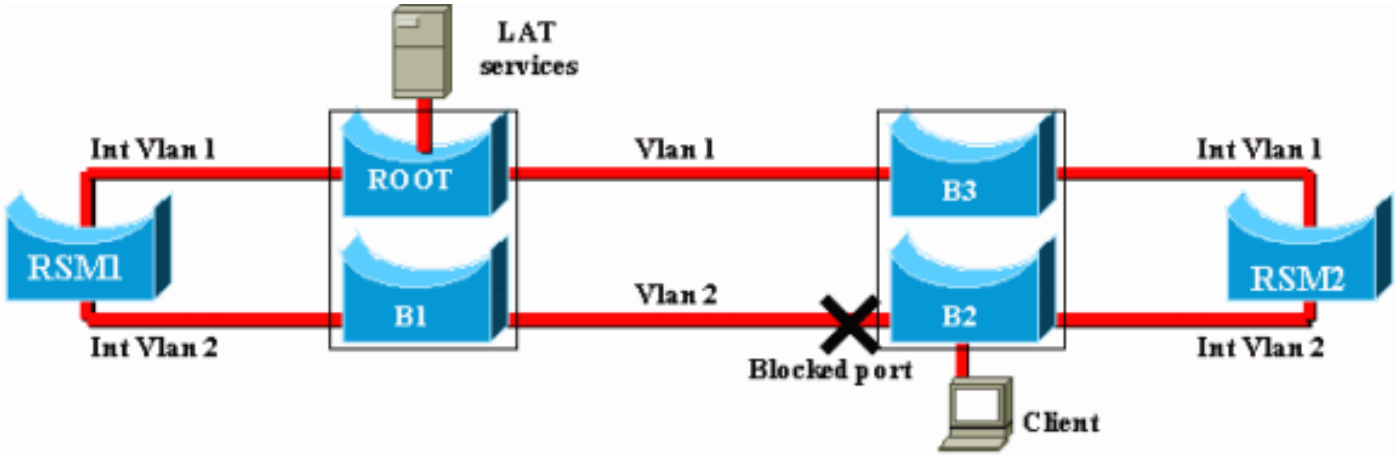
Fall-Back-Bridging

Das Fall-Back-Bridging besteht aus Bridging-Protokollen zwischen VLANs, während einige andere weitergeleitet werden. Wenn möglich, sollten Sie diese Konfiguration vermeiden und nur während einer Übergangszeit verwenden. In der Regel ist dies erforderlich, wenn Sie Ihr Netzwerk mit unterschiedlichen IP-Subnetzen in einem anderen VLAN segmentiert haben, aber weiterhin einige alte, nicht routbare Protokolle (z. B. Local Area Transport [LAT]) überbrücken möchten. In diesem Fall möchten Sie das RSM als Router für IP, aber als Bridge für andere Protokolle verwenden. Dies wird durch die Konfiguration von Bridging auf den RSM-Schnittstellen und die Beibehaltung von IP-Adressen erreicht. Das folgende Beispiel zeigt ein sehr einfaches Netzwerk, das eine Fallback-Bridging-Funktion verwendet, zusammen mit dem häufigsten Problem, das bei einer solchen Konfiguration auftreten kann.

Dieses sehr einfache Netzwerk besteht aus zwei VLANs, die zwei verschiedenen IP-Subnetzen entsprechen. Hosts in einem VLAN können eines der beiden RSMs als Standard-Gateway (oder sogar beide, unter Verwendung von Hot Standby Router Protocol [HSRP]) verwenden und so mit Hosts im anderen VLAN kommunizieren. Das Netzwerk sieht wie folgt aus:

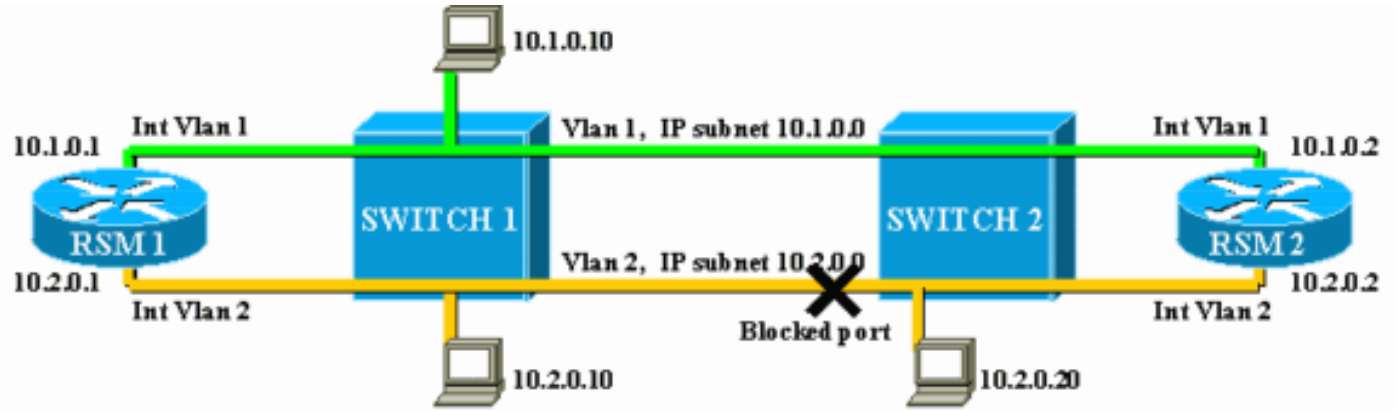


Beide RSMs sind auch so konfiguriert, dass sie andere Protokolle zwischen ihren Schnittstellen, VLAN1 und VLAN2, überbrücken. Angenommen, Sie haben einen Host, der LAT-Services anbietet, und einen Client, der diese Dienste verwendet. Ihr Netzwerk sieht wie folgt aus:



Für dieses Diagramm ist jeder Catalyst in zwei verschiedene Bridges aufgeteilt (eine für jedes VLAN). Sie sehen, dass die Überbrückung zwischen den beiden VLANs zu einer Fusion der beiden VLANs führte. Was überbrückte Protokolle angeht, so verfügen Sie nur über ein VLAN, und der LAT-Server und -Client können direkt miteinander kommunizieren. Natürlich impliziert dies auch, dass Sie eine Schleife im Netzwerk haben und dass STP einen Port blockieren muss.

Wie Sie sehen, wird ein Problem durch diesen blockierenden Port entstehen. Ein Switch ist ein reines L2-Gerät und kann nicht zwischen IP- und LAT-Datenverkehr unterscheiden. Wenn Switch 2 einen Port blockiert, wie im obigen Diagramm gezeigt, blockiert er daher alle Arten von Datenverkehr (IP, LAT oder andere). Aus diesem Grund sieht Ihr Netzwerk wie folgt aus:

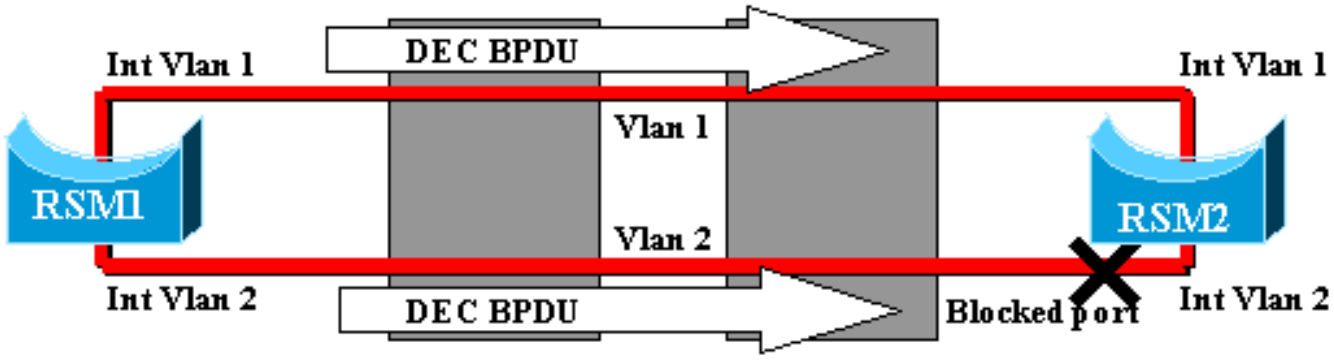


VLAN2 ist in zwei Teile unterteilt, und Sie haben ein nicht zusammenhängendes Subnetz 10.2.0.0. Bei dieser Konfiguration kann Host 10.2.0.10 nicht mit Host 10.2.0.20 kommunizieren, obwohl sie sich im gleichen Subnetz und VLAN befinden.

Die Lösung besteht darin, den blockierten Port auf dem einzigen Gerät zu verschieben, das L2- und L3-Datenverkehr unterscheiden kann. Dieses Gerät ist das RSM. Es gibt zwei Hauptmethoden, um dies zu erreichen:

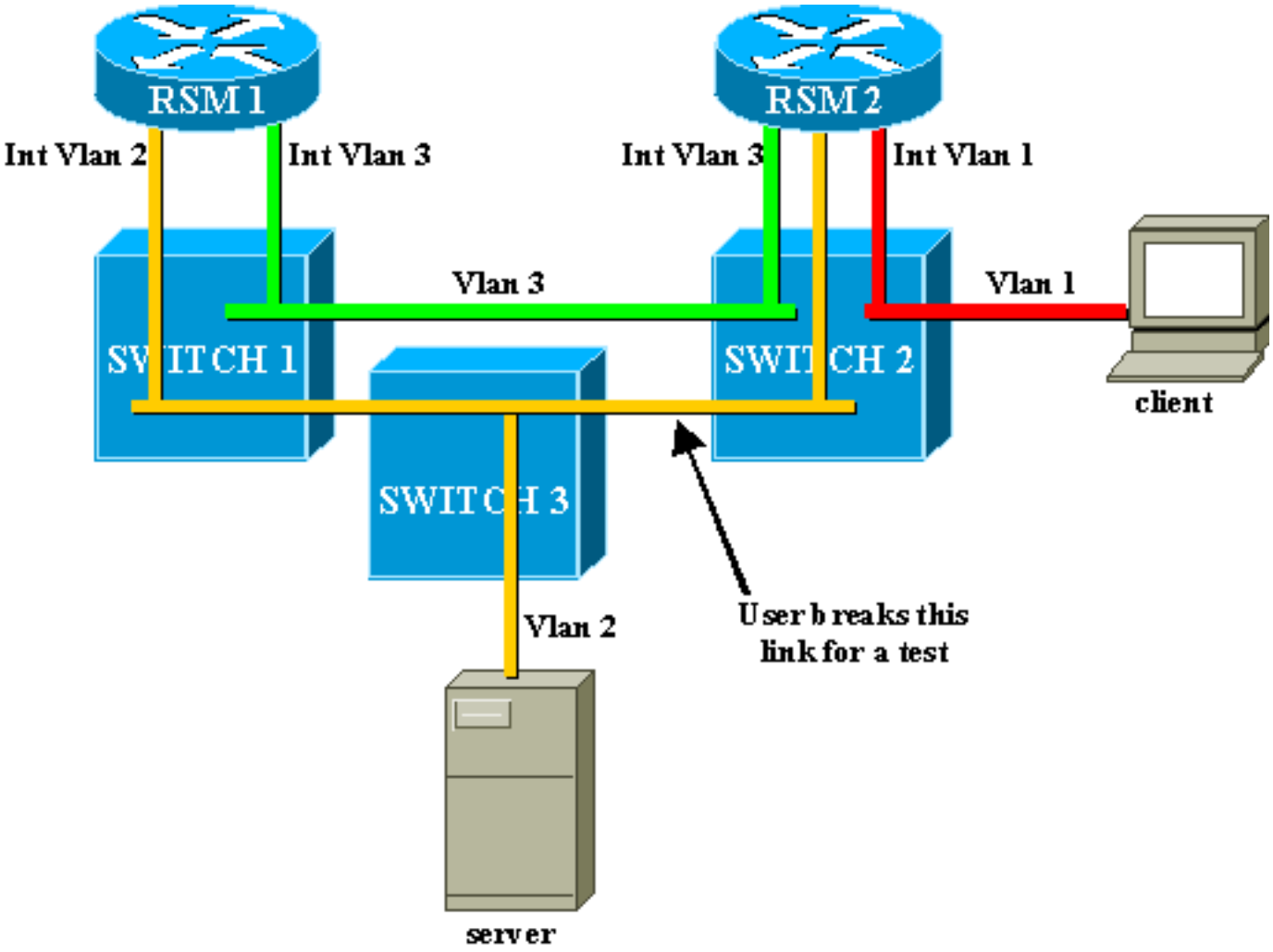
- **Durch Einstellen der STP-Parameter:** Sie müssen die Kosten für ein oder mehrere Geräte erhöhen, damit sich der blockierende Port schließlich auf RSM1 oder RSM2 befindet. Diese Methode ist nicht sehr flexibel und impliziert eine sehr strenge STP-Konfiguration. Das Hinzufügen eines Switches oder das Ändern der Bandbreite einer Verbindung (Fast EtherChannel oder Gigabit Ethernet) kann zu einer vollständigen Neuüberarbeitung der Einstellung führen.
- **Durch Verwendung eines anderen Spanning Tree Algorithm (STA) im RSM:** Die Switches führen nur den IEEE STA aus und sind für DEC STP vollständig transparent. Wenn Sie DEC STP auf beiden RSMs konfigurieren, funktionieren diese so, als wären sie direkt miteinander

verbunden, und einer von ihnen blockiert. Dieses Diagramm veranschaulicht dies:



Temporäre Black Hole (ST-Konvergenz)

Kunden, die die Geschwindigkeit der Neukonfiguration ihres Netzwerks bei einem Ausfall testen, befassen sich häufig mit Konfigurationsproblemen im Zusammenhang mit STP. Betrachten Sie das folgende Netzwerk, in dem ein Client über zwei verschiedene Pfade auf einen Server zugreift. Standardmäßig wird der Datenverkehr vom Client zum Server über die Schnittstelle VLAN2 von RSM2 geroutet:



Um einen Test durchzuführen, unterbricht ein Benutzer die Verbindung zwischen Switch 2 und Switch 3. Der entsprechende Port wird sofort deaktiviert, und die RSM Autostate-Funktion führt zum Ausfall der Schnittstelle VLAN2 auf RSM2. Die direkt verbundene Route für den Server verschwindet aus der Routing-Tabelle von RSM2, die schnell eine neue Route über RSM1 erfährt.

Dank effizienter Routing-Protokolle wie Open Shortest Path First (OSPF) oder Enhanced Interior Gateway Routing Protocol (EIGRP) ist die Konvergenz so schnell, dass Sie bei diesem Vorgang kaum einen Ping verlieren.

Bei einem Ausfall erfolgt der Switchover zwischen den beiden Pfaden (gelbes VLAN2 und grünes VLAN3) sofort. Wenn der Benutzer die Verbindung zwischen Switch 2 und Switch 3 wiederherstellt, geht die Verbindung zum Server für etwa 30 Sekunden verloren.

Der Grund dafür ist auch mit der STA verbunden. Bei der Ausführung von STA durchläuft ein neu verbundener Port zunächst die Phasen "Zuhören" und "Lernen", bevor er im Weiterleitungsmodus endet. In den ersten beiden 15-Sekunden-Phasen ist der Port aktiv, überträgt jedoch keinen Datenverkehr. Das bedeutet, dass die RSM-Autostate-Funktion, sobald die Verbindung angeschlossen ist, das Interface VLAN2 auf RSM2 sofort wieder aktiviert. Der Datenverkehr kann jedoch erst dann durchlaufen, wenn die Ports an der Verbindung zwischen Switch 2 und Switch 3 die Weiterleitungsphase erreichen. Dies erklärt den Verlust der temporären Verbindung zwischen dem Client und dem Server. Wenn die Verbindung zwischen Switch 1 und Switch 2 kein Trunk ist, können Sie die PortFast-Funktion aktivieren, um die Phasen des Abhörens und Lernens zu überspringen und sofort eine Konvergenz herzustellen.

Hinweis: PortFast funktioniert nicht auf Trunk-Ports. Weitere Informationen finden Sie unter Verwenden von PortFast und anderen Befehlen zum Beheben von Workstation-Startverbindungsverzögerungen.

Schlussfolgerung

Dieses Dokument konzentriert sich auf einige RSM-spezifische Probleme sowie einige sehr häufige Probleme beim VLAN-Routing. Diese Informationen sind nur nützlich, wenn alle üblichen Fehlerbehebungsverfahren für Cisco IOS-Router durchgeführt wurden. Wenn die Hälfte der von einem RSM gerouteten Pakete aufgrund der falschen Routing-Tabelle verloren geht, hilft dies nicht, die Statistiken zum DMA-Kanal zu interpretieren. Selbst die allgemeinen Probleme beim VLAN-übergreifenden Routing sind komplexe Themen und treten nicht sehr häufig auf. In den meisten Fällen reicht die Betrachtung Ihres RSM (oder eines anderen integrierten Routing-Geräts innerhalb eines Switches) als einfachen externen Cisco IOS-Router aus, um Routing-Probleme in einer Switching-Umgebung zu beheben.

Zugehörige Informationen

- Support-Seite für IP Routed Protocols
- Fehlerbehebung: IP Multilayer Switching
- Konfigurieren von Inter-VLAN-Routing
- Verwenden von PortFast und anderen Befehlen zum Beheben von Verzögerungen bei der Workstation-Startverbindung
- Support-Seiten für LAN-Produkte
- Support-Seite für LAN-Switching
- Technischer Support und Dokumentation - Cisco Systems