Probleemoplossing voor Catalyst 5000 routemodule (RSM) en InterVLAN-routing

Inhoud

Inleiding

Dit document bevat informatie over het opsporen en verhelpen van interVLAN-routing met een routeswitchmodule (RSM) op een Catalyst 5000 Series switch. Wanneer het aankomt op het oplossen van RSM, is het eerste wat te doen het als eenvoudige externe router te zien. Het is zeer zelden dat een RSM-specifiek probleem een probleem veroorzaakt wanneer het de routing tussen VLAN betreft. Dit document heeft derhalve slechts betrekking op de twee hoofdgebieden waar dit zou kunnen gebeuren:

- **RSM-gerelateerde problemen**: Dit document introduceert de RSM-architectuur en geeft details over de extra RSM-gerelateerde tellers om te volgen.
- **InterVLAN-configuratiespecifieke problemen** (vooral gerelateerd aan de interactie tussen routers en switches): Dit is ook van toepassing op andere interne routers (zoals de functiekaart voor meerlaagse Switch [MSFC], routefunctiekaart voor Switch [RSFC], 8510CSR enzovoort) en vaak op externe routers.

Opmerking: Dit document is niet van toepassing op het configureren van routing tussen VLAN's op Catalyst 4000, 5000 en 6000 switches. Raadpleeg voor deze informatie de volgende documenten:

- Configuratie en Overzicht van de routermodule voor de Catalyst 4500/4000, hele reeks (WS-X4232-L3)
- *Het configureren van de module voor InterVLAN-routing* van installatie- en configuratienoot voor Catalyst 4000 Layer 3 servicesmodule
- InterVLAN-routing met behulp van een interne router (Layer 3-kaart) op Catalyst 500/5000 en 6500/6000 Switches die CatOS-systeemsoftware uitvoeren

Dit document heeft geen betrekking op problemen die te maken hebben met basisroutingprotocol, of problemen die te maken hebben met meerlaagse switching (MLS).

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

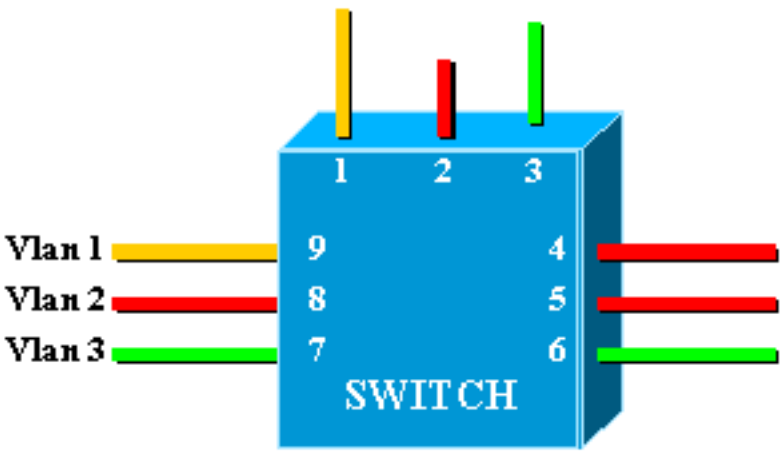
Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

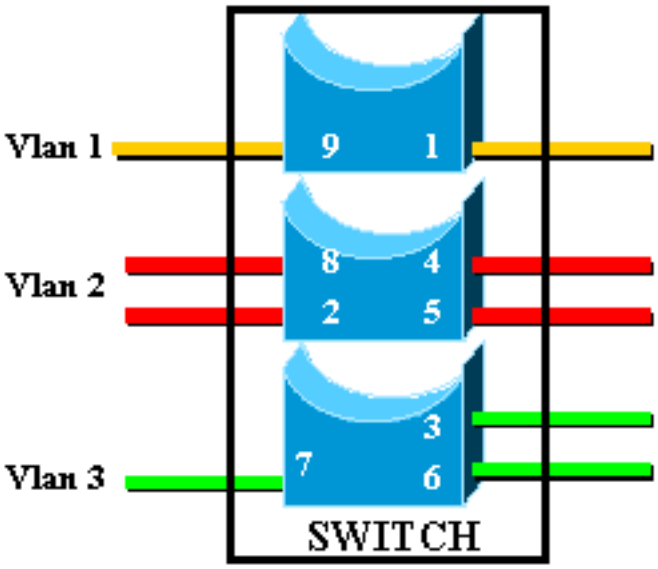
Wat is InterVLAN-routing?

Voordat u de routing tussen VLAN's bespreekt, richt dit document zich op het VLAN-concept. Dit is geen theoretische discussie over de noodzaak van VLAN's, maar bespreekt eenvoudig hoe VLAN's op een switch werken. Wanneer u VLAN's op uw switch maakt, is het alsof u uw switch in verscheidene virtuele bruggen splitst, waarbij elk slechts overbruggingshavens tot hetzelfde VLAN behoren.

Dit diagram vertegenwoordigt een switch met negen poorten die aan drie verschillende VLAN's zijn toegewezen:



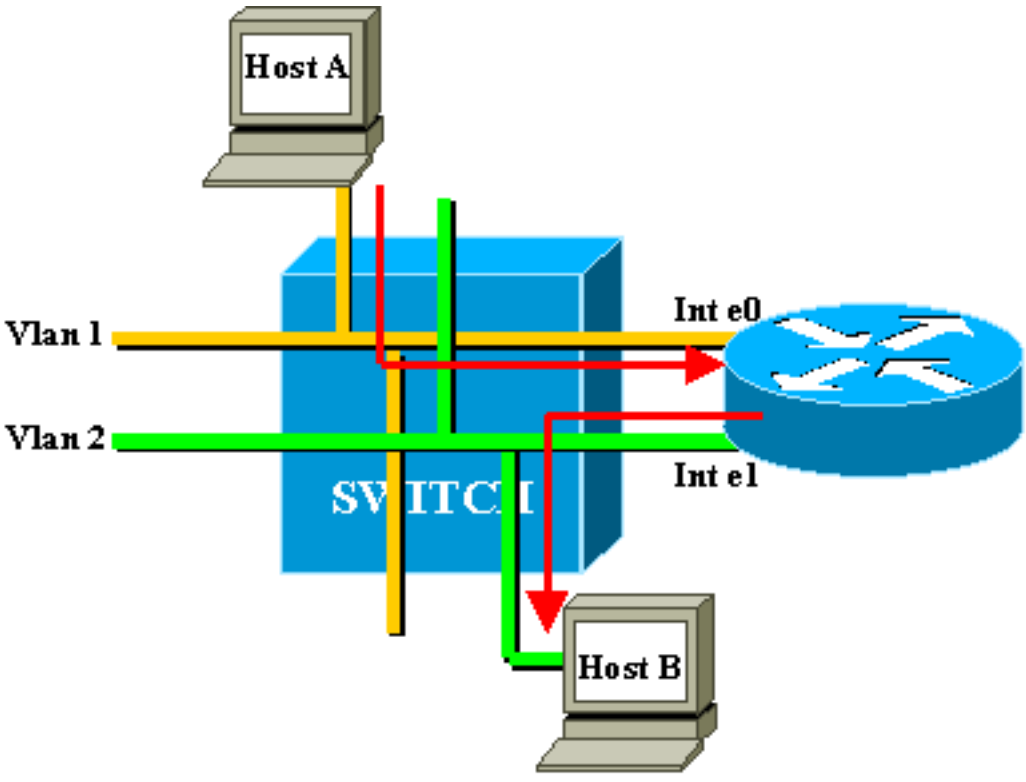
Dit is precies hetzelfde als het volgende netwerk, dat bestaat uit drie onafhankelijke bruggen:



In de switch zijn er drie verschillende bruggen, door elk VLAN dat een aparte brug maakt. Aangezien elk VLAN een afzonderlijk Spanning Tree Protocol (STP)-instantie maakt, houdt STP drie verschillende verzendtabellen bij.

Met gebruik van het tweede diagram wordt het duidelijk dat, alhoewel verbonden met het zelfde fysieke apparaat, havens die tot verschillende VLAN's behoren niet direct op Layer 2 (L2) kunnen communiceren. Zelfs indien mogelijk zou dit niet passend zijn. Bijvoorbeeld, als u haven 1 aan haven 4 verbonden hebt, zou u eenvoudig VLAN1 aan VLAN2 samenvoegen. In dit geval, zou er geen reden zijn om twee afzonderlijke VLANs te hebben.

De enige connectiviteit die u tussen VLAN's wilt wordt bereikt bij Layer 3 (L3) door een router. Dit is routing tussen VLAN’s. Om de diagrammen verder te vereenvoudigen, worden VLAN’s weergegeven als verschillende fysieke Ethernet-segmenten, omdat u niet echt geïnteresseerd bent in de specifieke overbruggingsfuncties die de switch biedt.



In dit diagram worden de twee VLAN’s gezien als twee verschillende Ethernet-segmenten.

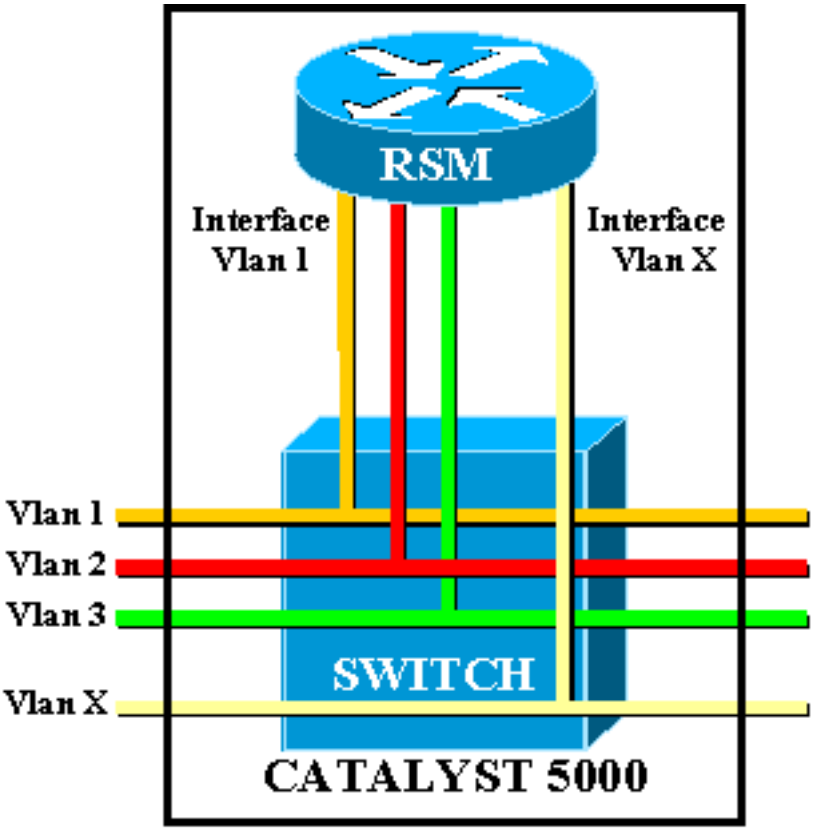
InterVLAN-verkeer moet door de externe router gaan. Als host A wil communiceren met host B, gebruikt het de router doorgaans als een standaardgateway.

RSM-architectuur

Logische architectuur

U kunt een RSM als een externe router bekijken die verschillende interfaces direct verbonden heeft met de verschillende VLAN's van een Catalyst 5000 switch.

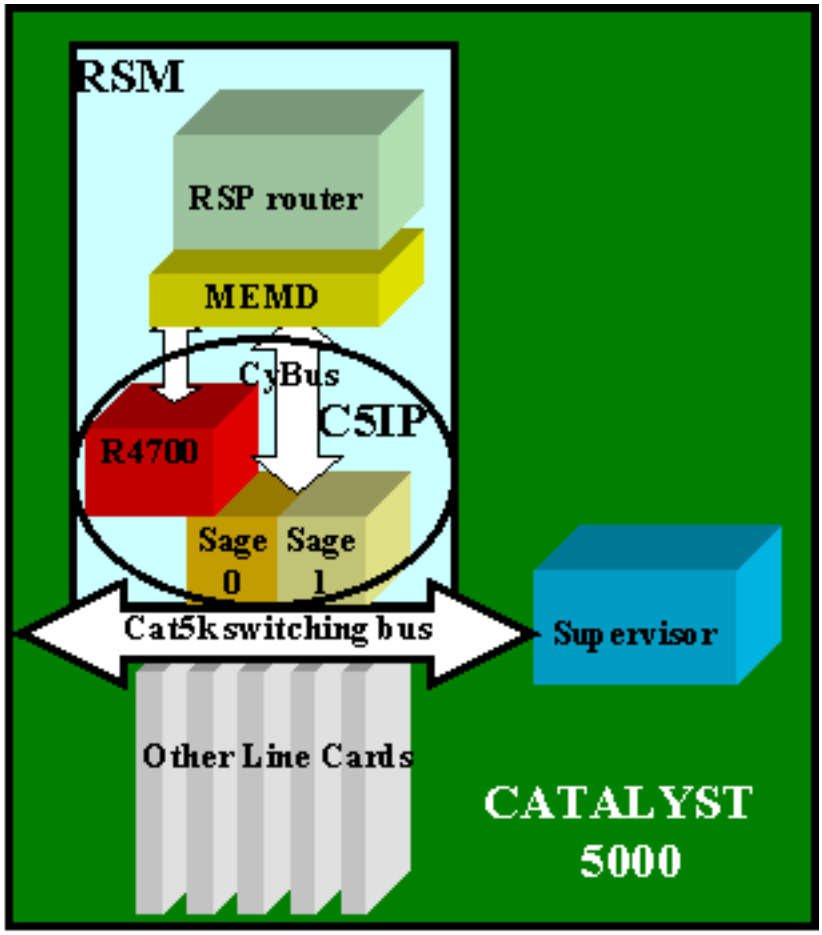
In plaats van een Ethernet interface te worden genoemd, worden deze interfaces genoemd volgens het VLAN waaraan zij zich verbinden. (Interface VLAN1 wordt direct aangesloten op VLAN1, etc.).



Geïmplementeerde architectuur

RSM is een Cisco 7500 Route Switch Processor (RSP)-router binnen een Catalyst 5000 lijnkaart. U hoeft niet veel te weten over de architectuur van de kaart om de kaart te configureren en op te lossen. Maar het hebben van een idee van hoe RSM gebouwd wordt helpt te begrijpen hoe het van een normale externe router verschillend is. Deze kennis is met name belangrijk bij de introductie van de **showcontroller c5ip-**opdracht.

In dit schema worden de belangrijkste onderdelen van de RSM-lijnkaart aangegeven:

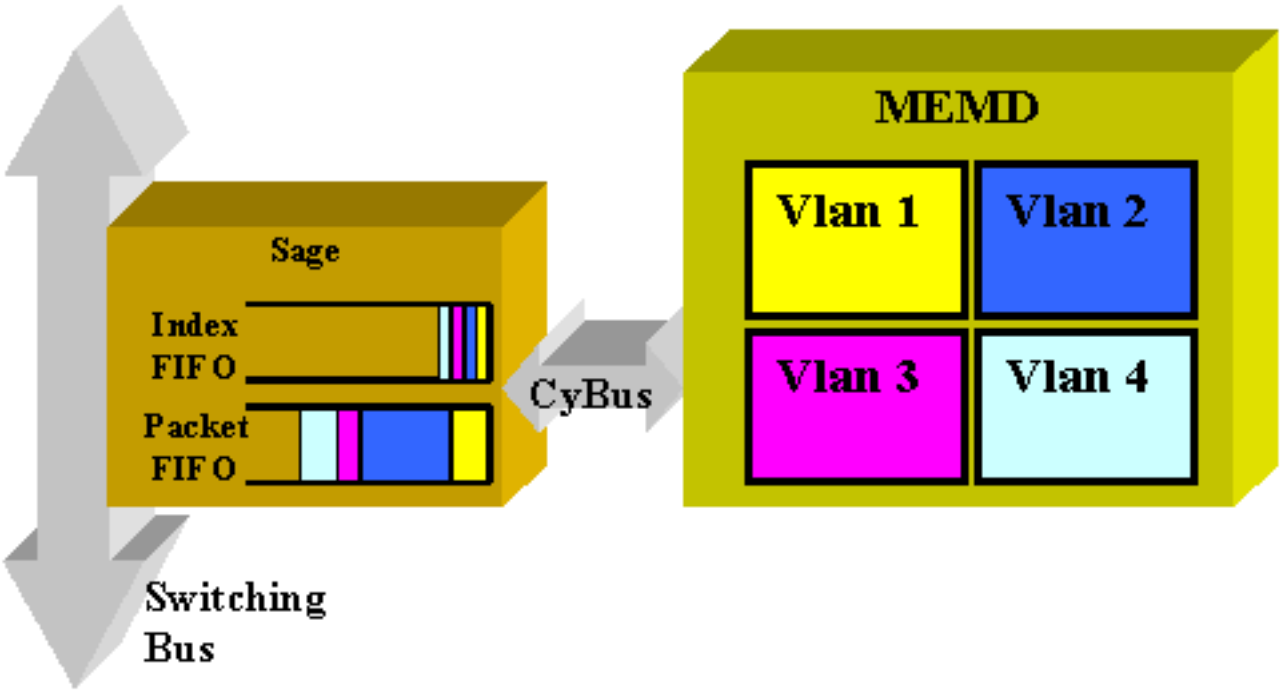


Catalyst 5000 interfaceprocessor

Catalyst 5000 interfaceprocessor (C5IP) is het deel van RSM dat een Catalyst 7500 systeem IP emuleert met de Catalyst 5000 switchbus als netwerkinterface. Het C5IP bevat een R4700-processor samen met twee SAGE Application-Specific Integrated Circuits (ASIC's), die verantwoordelijk zijn voor de toegang tot de Catalyst 5000-switchbus.

SAMENVOEGEN

Deze twee ASIC's krijgen pakketten van/naar de switchbus en bufferen ze. Samen met de gegevens in het pakket krijgen ze ook een index die de bestemming van het pakket in de switch identificeert.



De interface van het bestemming VLAN wordt niet bepaald van de inhoud van het pakket zelf, maar komt van de index voort. Het pakket en de index worden eerst opgeslagen in twee verschillende FIFO's in de SAGE. De index wordt gelezen en het benodigde gedeelde geheugen is gereserveerd in het gebied van het doelVLAN. Het pakket wordt vervolgens gekopieerd in het geheugen (MEMD), met behulp van een Direct Memory Access (DMA) tot de SAGE.

Twee SAGEs die parallel werken om tussen de router en de switchbus te communiceren kunnen tot een uit reeks pakketlevering leiden. (Een groot pakket dat op SAGE0 is ontvangen, kan bijvoorbeeld worden verzonden na een klein pakket dat later door SAGE1 wordt ontvangen.) Om dit te vermijden, wordt elk VLAN statistisch toegewezen aan een bepaalde SAGE. Dit gebeurt automatisch bij het opstarten. (Volgens de router wordt een VLAN gekoppeld aan een van de twee DMA-kanalen, en leidt elk van deze tot een SAGE.) Packets van een bepaald VLAN worden altijd achter elkaar geleverd.

MEMD

MEMD is het gedeelde geheugen dat door de router wordt gebruikt om pakketten te verzenden en ontvangen. Elke geconfigureerde VLAN-interface in RSM wordt een deel van het beschikbare gedeelde geheugen toegewezen. Hoe meer VLAN-interfaces, hoe minder gedeeld geheugen per interface. VLAN-interfaces houden hun deel van het gedeelde geheugen vast, zelfs wanneer uitgeschakeld of uitgeschakeld wordt. Alleen het toevoegen of verwijderen van een VLAN-interface leidt tot een nieuwe herverdeling van de MEMD tussen VLAN-interfaces.

RSM-specifieke probleemoplossing

De belangrijkste RSM-specifieke kwesties die niet worden behandeld in de gebruikelijke Cisco IOS® routerdocumentatie zijn problemen met de toegang tot RSM, en ook prestatiekwesties.

Toegang tot RSM

RSM kan op drie verschillende manieren worden benaderd:

- Telnet aan RSM
- Session in voor RSM van de Switch supervisor
- Direct Console-verbinding

Telnet aan RSM

Om in RSM te tellen, moet u het IP adres kennen dat aan één van zijn interfaces van VLAN is toegewezen. De Telnet-sessie werkt precies hetzelfde als als wanneer u probeert verbinding te maken met een normale Cisco IOS-router. U moet mogelijk een wachtwoord aan de Vty toewijzen om telnet te bereiken en toegang te verkrijgen.

Dit voorbeeld toont een zitting van Telnet van een Supervisor Engine aan een RSM, waarin het VLAN1 IP adres 10.0.0.1 is:

```
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
```

Dit is gelijk aan andere externe router Cisco IOS-configuraties.

Session in voor RSM van de Switch supervisor

Het gebruiken van de opdracht **sessie *x*** van de Supervisor Engine sluit u aan op RSM in sleuf *x*.

De methode is dezelfde als de vorige: RSM heeft een verborgen VLAN0 interface met een IP-adres 127.0.0(x+1), waar x de sleuf is waar RSM is geïnstalleerd. De opdracht **voor** de **sessie** geeft een verborgen Telnet-sessie aan dit adres uit.

N.B.: In dit geval hoeven de wachtwoorden niet in de configuratie te zijn geplaatst om volledige toegang tot de RSM te verkrijgen.

```
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#
```

U gebruikt de opdracht Supervisor Engine **module** om de sleuf te identificeren waarin uw RSM in de switch is geïnstalleerd. U kunt de **sessie** rechtstreeks benaderen via de opdracht **sessie**.

Direct Console-verbinding

De systeemconsole poort op RSM is een DB-25 container DCE poort voor het aansluiten van een gegevensterminal, die u toestaat om met uw systeem te vormen en te communiceren. Gebruik de console kabel die wordt meegeleverd om de terminal aan de console poort op RSM aan te sluiten. De troostpoort bevindt zich op RSM naast de hulphaven en wordt geëtiketteerd console.

Voordat u de console poort aansluit, controleert u uw terminaldocumentatie om de basissnelheid van de terminal te bepalen die u gebruikt. Het basistarief van de terminal moet overeenkomen met het standaardbasistarief (9600 baud). Stel de terminal in als volgt: 9600 baud, acht gegevensbits, geen pariteit en twee stoppen bits (9600,8N2).

Kan geen toegang krijgen tot RSM

Het RSM kan om verschillende redenen worden geïsoleerd. Zelfs zonder er verbinding mee te kunnen maken, zijn er enkele tekens van leven die je van buitenaf kunt controleren:

- Controleer de status van de LEDS op de RSM:CPU Halt LED is uitgeschakeld—systeem heeft een hardware-storing van de processor gedetecteerd.Oranje STATUS LED-module uitgeschakeld, testend in uitvoering of systeemstart in uitvoering.
- Controleer de Supervisor Engine om te zien of de switch RSM kan zien. Om dit te doen, geef de **opdracht** van de **showmodule** uit:

```
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.
```

Zeg nooit uw RSM dood voordat u de consoleverbinding hebt geprobeerd. Zoals u hebt gezien, vertrouwen zowel zitting als de toegang van het telnet op een IP verbinding met RSM. Als RSM op RSM start of in de ROMMON-modus zit, kunt u bijvoorbeeld niet tellen of er geen sessie aan geven. Dat is echter heel normaal.

Zelfs als RSM defect lijkt te zijn, probeer dan verbinding te maken met de console. Hierdoor kunt u een aantal foutmeldingen zien die hier weergegeven worden.

Prestatieproblemen

De meeste prestatiekwesties die aan RSM gerelateerd zijn kunnen op precies de zelfde manier als met een normale Cisco IOS router worden opgelost. Dit deel is gericht op het specifieke deel van de RSM-implementatie dat de C5IP is. De opdracht **toont controller c5ip** kan informatie geven over de werking van C5IP. Deze output beschrijft een aantal van de belangrijkste velden:

```
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-kanaal 1/1

De RSP-router binnen RSM communiceert met de switch via twee verschillende DMA-kanalen (naar de twee SAGE ASIC's). Elke VLAN-interface wordt automatisch gekoppeld aan een van deze DMA-kanalen. De **show control c5ip** opdracht geeft informatie over elk in twee verschillende secties weer.

Ontvangen/verzonden

Deze statistieken helpen de lading op de verschillende DMA kanalen te identificeren. Zoek een DMA-kanaal dat gestaag overbelast is in vergelijking met de andere. Dit kan voorkomen als alle verkeersintensieve VLAN's aan het zelfde DMA kanaal worden toegewezen. Indien nodig kunt u VLAN-interfaces handmatig aan een specifiek DMA-kanaal toewijzen met behulp van het **dma-kanaal** van de interfaceopdracht.

Gestopt

Dit wijst op het aantal pakketten dat RSM ontving maar liet vallen. Dit gebeurt wanneer de ontvangen index samen met het pakket niet RSM als specifieke bestemming van het pakket geeft.

Fouttellingen

- **crc**-**cyclische** redundantie-cyclus (CRC) fouten voorkomen wanneer een slechte CRC door het RSM wordt gedetecteerd. Er moeten geen pakketten zijn met slechte CRC's op het backplane. Het RSM-detecterende signaal geeft aan dat sommige lijnkaarten of andere backplane-aangesloten apparaten niet goed werken.**Opmerking:** CRC-fouten kunnen ook afkomstig zijn van een op een ISL-romp aangesloten apparaat. De meeste Catalyst lijnkaarten controleren niet CRC van een pakket dat zij van de backplane en voorwaarts op een boomstam ontvangen.
- **index**—indexfouten komen voor als de index niet nauwkeurig is. De C5IP is niet op de hoogte van waarom het dit pakket heeft ontvangen. Dit verhoogt ook de teller.
- **dmac-length**—Deze fouten gebeuren wanneer de C5IP interface voorkomt dat de SAGE ASIC een maximale grootte van een transmissieeenheid (MTU) overschrijdt die, indien niet gedetecteerd, het gedeelde geheugen van de router zou hebben beschadigd.
- **dmac-synch**-Als een SAGE ASIC een pakje verlaat, worden het pakje FIFO en de index FIFO uit de synch. Als deze fout optreedt, wordt deze automatisch gedetecteerd en wordt de `dmac-synch` teller verhoogd. Het is onwaarschijnlijk dat dit zal gebeuren, maar als het wel gebeurt is de impact op de prestaties extreem laag.

- **dmac-timeout**-Deze teller is toegevoegd aan de **show controllers c5ip** opdracht in Cisco IOS-softwarereleases 11.2(16)P en 12.0(2). Het wordt verhoogd wanneer een DMA-overdracht niet binnen de maximale tijd die nodig is voor de langst mogelijke overdracht voltooid is. Het wijst op een hardware fout, en een RSM die een niet nul waarde voor deze teller toont is een goede kandidaat voor vervanging.
- **negeren** —Negeer gebeurt wanneer de router geen buffers voor MEMD heeft voor ingangspakketten. Dit gebeurt wanneer de CPU-pakketten niet zo snel verwerkt als zij worden ingevoerd. Dit is waarschijnlijk te wijten aan wat de CPU bezig houdt.
- **lijn-down**-lijn betekent dat de pakketten die aan een lijnprotocol beneden VLAN zijn voorbestemd zijn gedaald. C5IP heeft een pakket voor een VLAN-interface ontvangen waarvan het gelooft dat het is weggevallen. Dit zou niet moeten gebeuren, aangezien de switch zou moeten ophouden pakketten naar een RSM interface te verzenden dat is neergezet. Toch kunt u er een paar zien wanneer een interface naar beneden gaat, door de timing tussen de RSM die de interface afschrijft en de switch die wordt aangemeld.
- **runt/reus** - Deze teller volgt ongeldige groote pakketten.
- **unicast-overstroming**-Unicast-overstroompakketten worden verzonden naar een specifiek MAC-adres. De Catalyst 5000 Content Adressable Memory (CAM)-tabel weet niet welke poort het MAC-adres is geactiveerd, zodat het pakket met alle poorten op VLAN wordt overspoeld. RSM ontvangt ook deze pakketten, maar tenzij het voor het overbruggen op dat VLAN wordt gevormd, is het niet geïnteresseerd in pakketten die niet zijn eigen MAC-adres aanpassen. RSM gooit deze pakketten weg. Dit is het equivalent van wat op een echte Ethernet interface in de Ethernet interfacechip gebeurt, die geprogrammeerd wordt om pakketten voor andere MAC-adressen te negeren. In de RSM, gebeurt dit in de C5IP-software. De meeste gedropt pakketten zijn pakketten van de overstroming van eenmalig.
- **Laatste daling** - Deze teller onthult specifieke informatie over het laatste ingetrokken pakket. Dit is laagwaardige informatie die buiten het toepassingsgebied van dit document valt.

VLAN-distributie onder DMA-kanalen

Hier is een deel van de uitvoer van de **show controllers c5ip** opdracht op een RSM met tien VLAN-interfaces geconfigureerd:

```
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
```

Deze uitvoer toont aan welk DMA kanaal een bepaalde interface van VLAN wordt toegewezen aan. U kunt zien dat vreemd VLAN's naar kanaal 0 gaan, terwijl zelfs VLAN's aan kanaal 1 zijn verbonden. Indien nodig kunt u deze correspondentie hard coderen met het **dma-kanaal** van de interfaceconfiguratie. Dit voorbeeld toont hoe de interface VLAN1 van een RSM aan DMA kanaal 0 toe te wijzen:

```
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-informatie

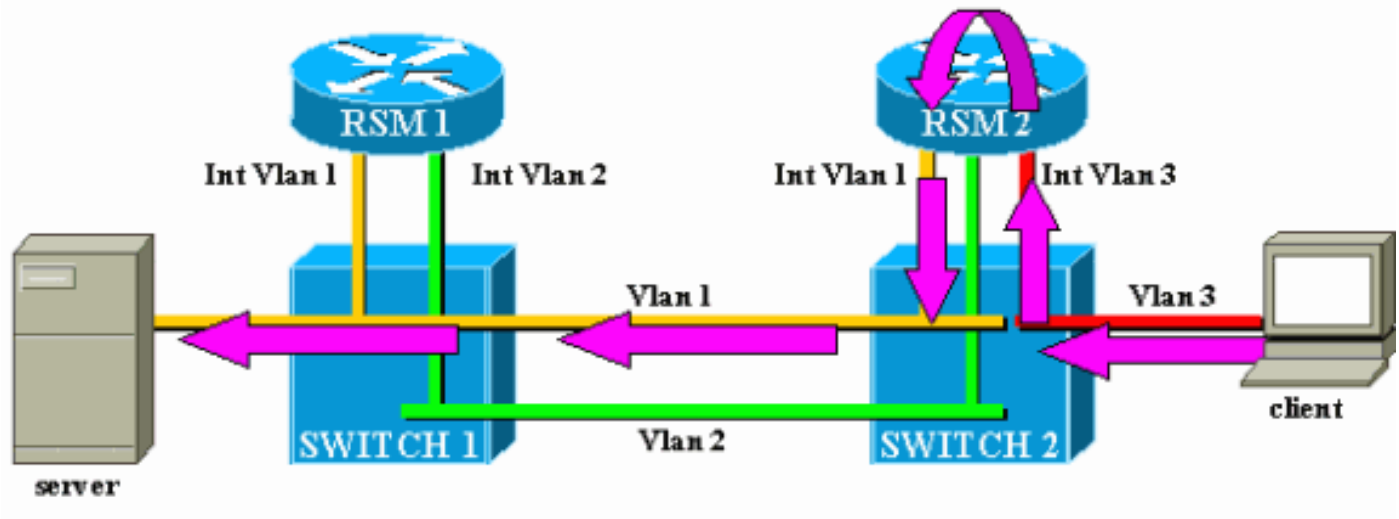
Het belangrijkste doel van VLAN0 is doeltreffende communicatie aan de Supervisor Engine van de switch te verzekeren. Aangezien dit een verborgen interface is, kunt u geen eenvoudig **show interface VLAN0** gebruiken om statistieken over het te zien.

InterVLAN-routing gemeenschappelijke problemen

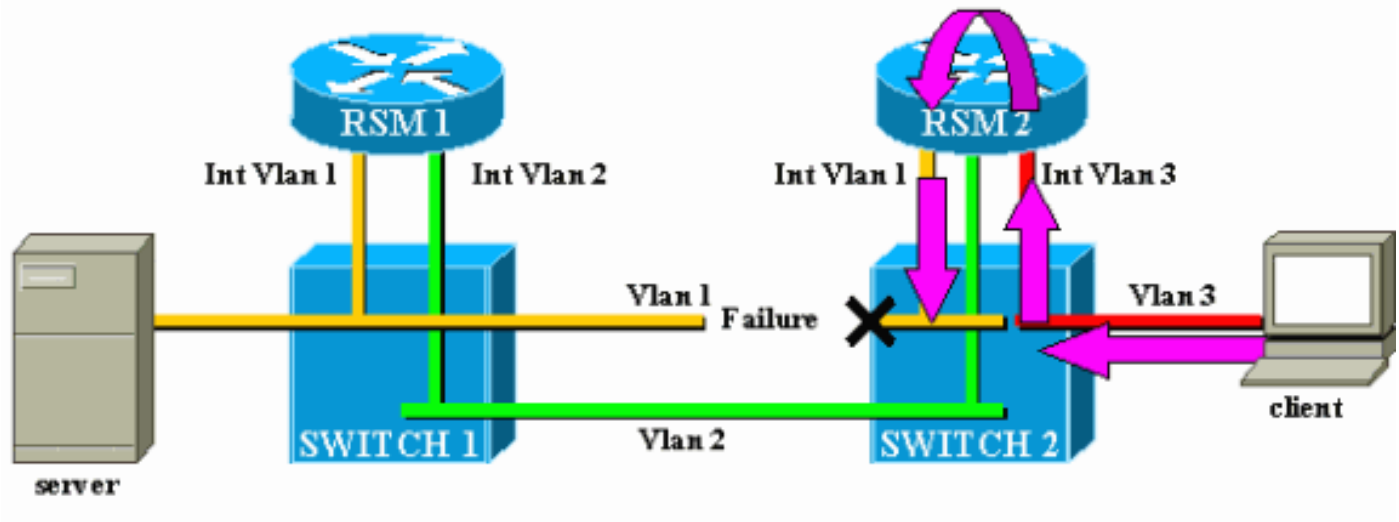
De automatische staatsfunctie van RSM gebruiken

Een regelmatig probleem met overbrugging is dat een verbroken link een L2 netwerk gemakkelijk in twee stukken kan splitsen. Deze situatie zou tegen om het even welke prijs moeten worden vermeden, aangezien een distiguous netwerk de routing breekt. (Dit wordt meestal bereikt door redundante links in te zetten.)

Neem dit voorbeeld, waar een client verbonden op Switch 2 communiceert met een server verbonden op Switch 1:



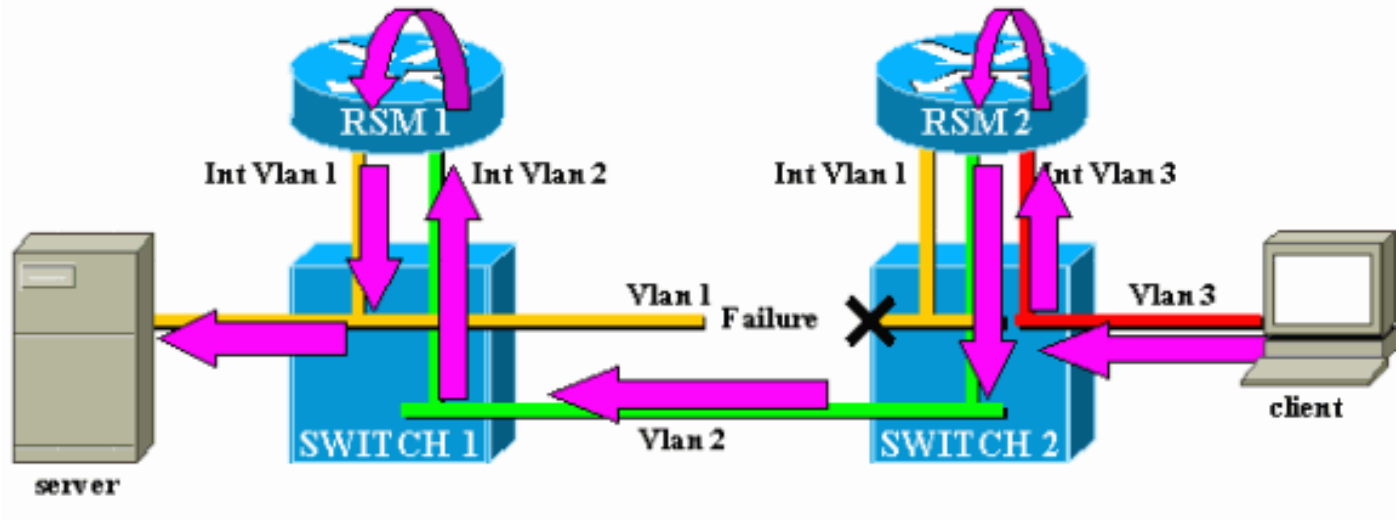
Denk alleen aan het verkeer van de client naar de server. Het inkomende verkeer van de client in VLAN3 wordt routed door RSM2, dat een directe verbinding met Subnet van de server via zijn interface VLAN2 heeft. De paarse pijlen vertegenwoordigen het volgende pad:



Stel dat het verband tussen Switch 1 en Switch 2 breekt voor VLAN1. Het belangrijkste probleem hier is dat, vanuit het standpunt van RSM2, niets in het netwerk veranderde. RSM2 heeft nog steeds een interface direct verbonden aan VLAN1, en het blijft verkeer van de client naar de server via dit pad doorsturen. Het verkeer gaat verloren in Switch 2 en de verbinding tussen de client en de server is verbroken.

De automatische status van RSM werd ontworpen om dit aan te pakken. Als er geen poort naar boven is voor een specifiek VLAN op een switch, wordt de corresponderende VLAN-interface van RSM verlaagd.

In het geval van het voorbeeld, wanneer de verbinding in het VLAN tussen Switch 1 en Switch 2 mislukt, gaat de enige poort in VLAN1 op Switch 2 naar beneden (link onderaan). De autostate optie RSM schakelt de interface VLAN1 op RSM2 uit. Nu de interface VLAN1 is gedaald, kan RSM2 een routeringsprotocol gebruiken om een ander pad voor pakketten te vinden die voor de server bestemd zijn en uiteindelijk verkeer via een andere interface te verzenden, zoals in dit diagram wordt getoond:



RSM autostate werkt alleen als er geen andere poort in het VLAN is. Als u bijvoorbeeld een andere client in VLAN1 aan Switch 2 gekoppeld had, of RSM in het chassis met een interface VLAN1 gedefinieerd, wordt de interface VLAN1 niet uitgeschakeld als de link tussen Switch 1 en Switch 2 mislukt is. Het verkeer zou dan weer worden verstoord.

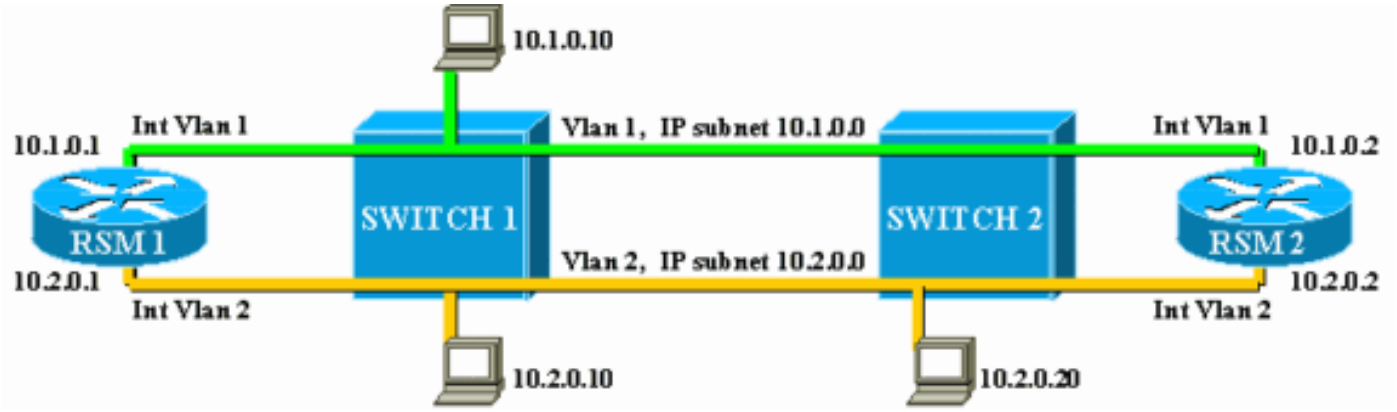
De optie RSM autostate is standaard ingeschakeld. Indien nodig kan het handmatig worden uitgeschakeld met behulp van de ingestelde rsmautostate opdracht op de Supervisor Engine:

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

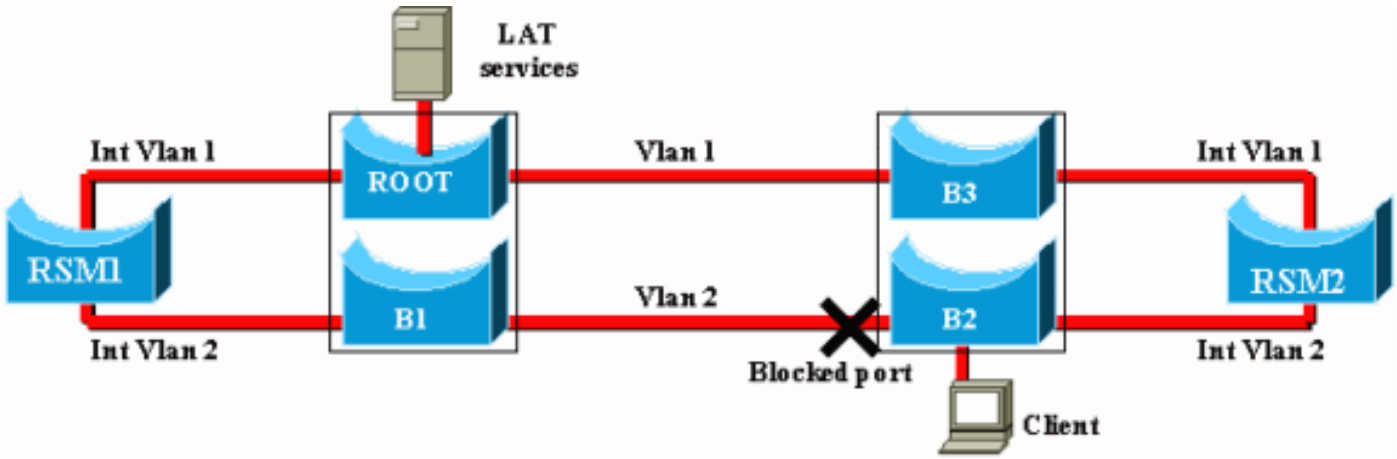
Back-uplijn

Back-uplijn bestaat uit het overbruggen van protocollen tussen VLAN's en het routeren van andere. Indien mogelijk dient u dit soort configuratie te vermijden en alleen te gebruiken tijdens een tijdelijke migratieperiode. Meestal is dit nodig als u uw netwerk met verschillende IP-subnetten, elk op een ander VLAN hebt gesegmenteerd, maar u wilt doorgaan met het overbruggen van oude niet routeerbare protocollen (lokaal gebiedstransport [LAT], bijvoorbeeld). In dit geval, wilt u uw RSM als router voor IP gebruiken, maar als brug voor andere protocollen. Dit wordt eenvoudigweg bereikt door het configureren van overbrugging op de RSM interfaces, terwijl u IP adressen bijhoudt. Het volgende voorbeeld illustreert een zeer eenvoudig netwerk dat gebruik maakt van fall-back-overbrugging, samen met het meest voorkomende probleem dat kan gebeuren met dit soort configuratie.

Dit zeer eenvoudige netwerk is gemaakt van twee VLAN's, die overeenkomen met twee verschillende IP subnetten. Hosten in een bepaald VLAN kunnen om het even welk van de twee RSM's als standaardgateway (of zelfs beide, die het HSRP protocol van de HSRP van de KREUK gebruiken) gebruiken, en kunnen dus met hosts op het andere VLAN communiceren. Het netwerk ziet er zo uit:

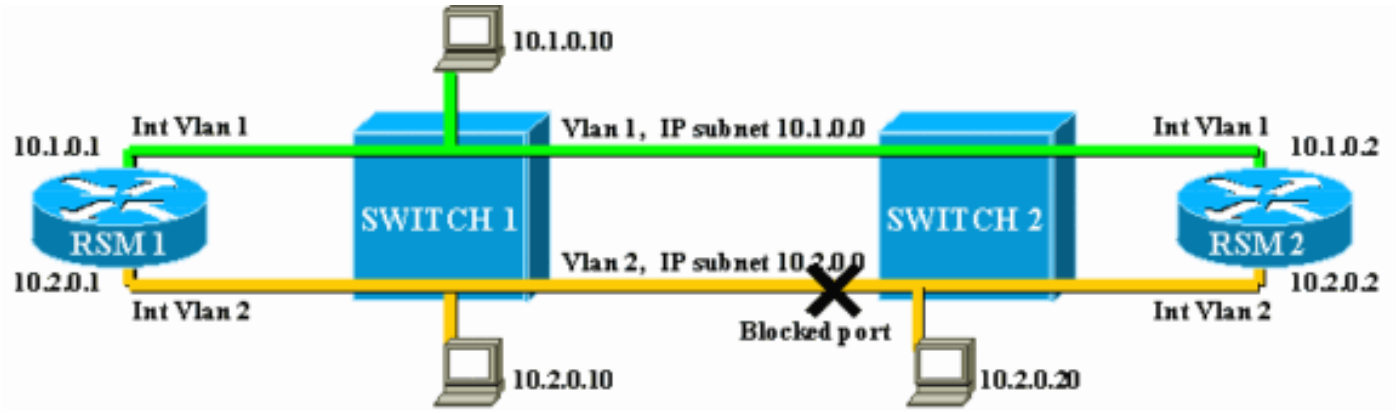


Beide RSM's zijn ook geconfigureerd om andere protocollen tussen hun interfaces, VLAN1 en VLAN2 te overbruggen. Stel dat u een host hebt die LAT-services aanbiedt en een client die deze services gebruikt. Uw netwerk zal er als volgt uitzien:



Voor dit diagram wordt elke Catalyst gesplitst in twee verschillende bruggen (één voor elk VLAN). U kunt zien dat het overbruggen tussen de twee VLAN's heeft geleid tot een fusie van de twee VLAN's. Wat overbrugde protocollen betreft, hebt u slechts één VLAN en de LAT server en client kunnen direct communiceren. Dit impliceert natuurlijk ook dat je een lus in het netwerk hebt en dat STP één poort moet blokkeren.

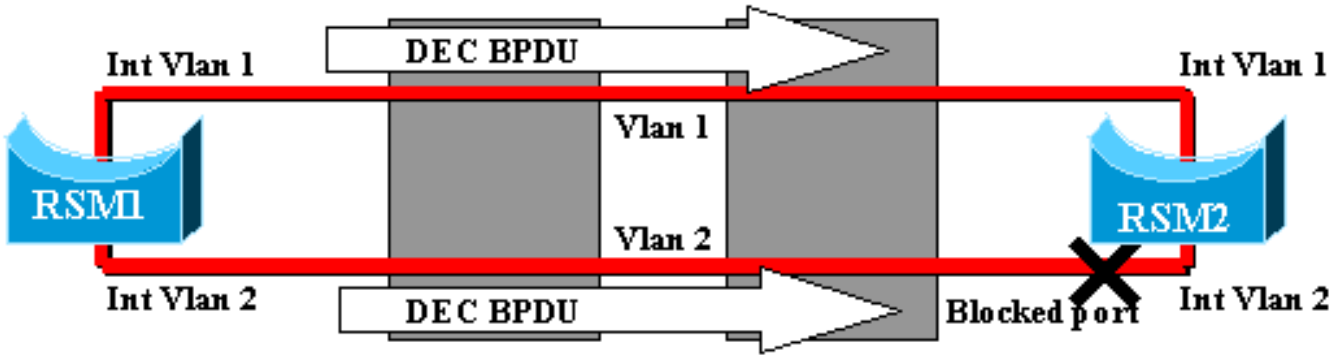
Zoals u ziet, zal er een probleem ontstaan uit deze blokkerende haven. Een switch is een zuiver L2 apparaat en kan geen verschil maken tussen IP en LAT verkeer. Als Switch 2 één poort blokkeert, zoals in het bovenstaande diagram, blokkeert het alle soorten verkeer (IP, LAT of andere). Daarom ziet uw netwerk er zo uit:



VLAN2 is verdeeld in twee delen, en u hebt een distiguous Subnet 10.2.0.0. Met deze configuratie, kan host 10.2.0.10 niet met host 10.2.0.20 communiceren, alhoewel ze op hetzelfde net en VLAN zijn.

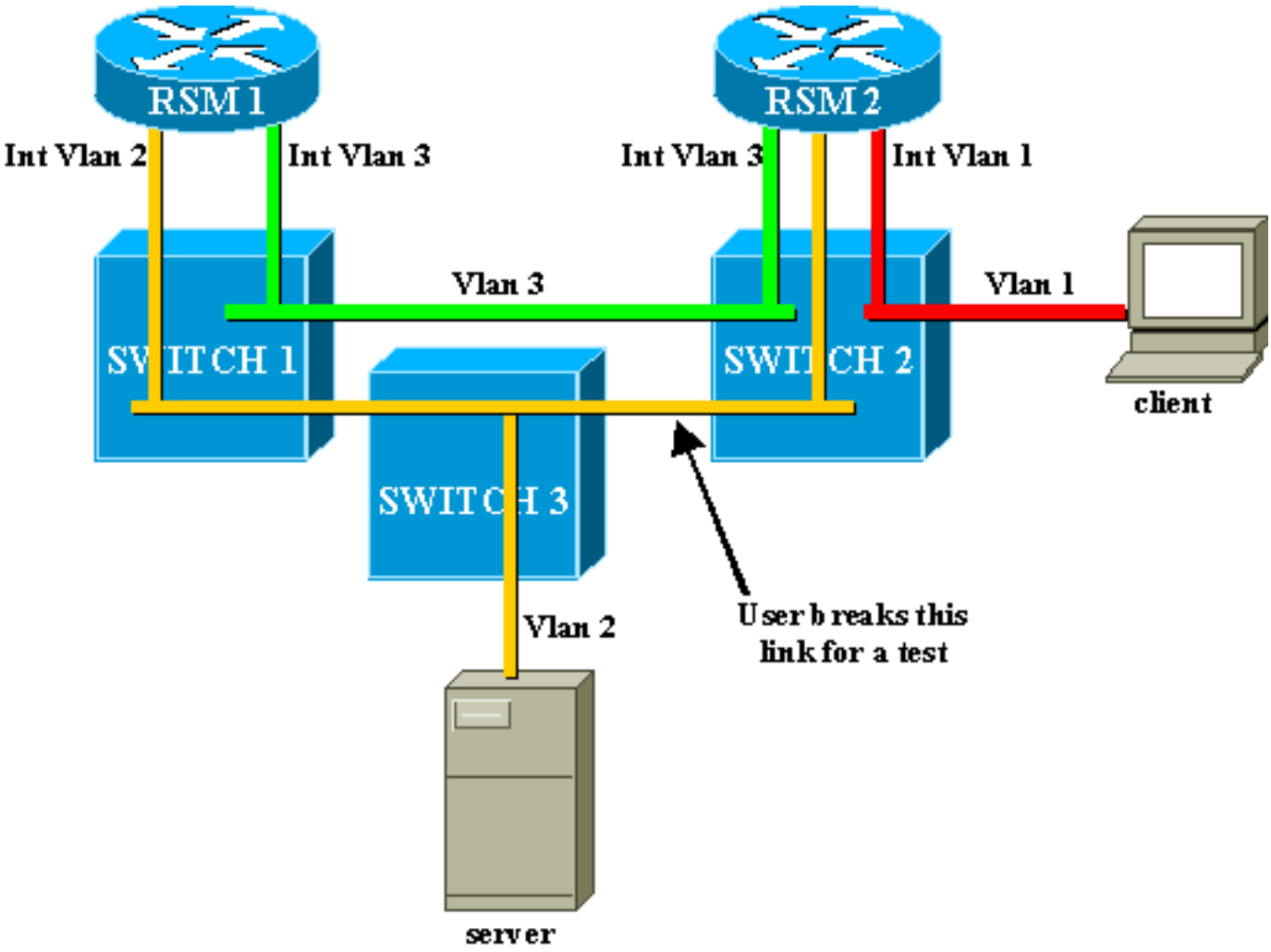
De oplossing is om de geblokkeerde poort te verplaatsen op het enige apparaat dat L2 en L3 verkeer kan onderscheiden. Dat apparaat is de RSM. Er zijn twee belangrijke manieren om dit te bereiken:

- **Door STP-parameters in te stellen:** U moet de kosten voor een of meer apparaten verhogen zodat, uiteindelijk, de blokkerende poort zich op RSM1 of RSM2 bevindt. Deze methode is niet erg flexibel en impliceert een zeer strikte STP-configuratie. Wanneer u een switch toevoegt of de bandbreedte van een link wijzigt (Fast EtherChannel of Gigabit Ethernet), kan dit een volledig opnieuw werk van de tuning tot gevolg hebben.
- **Door een ander Spanning Tree Algorithm (STA) op RSM te gebruiken:** De switches voeren alleen de IEEE STA uit en zijn volledig transparant in het DEC STP. Als u DEC STP op beide RSM's vormt, werken ze alsof ze direct verbonden waren en één van hen blokkeert. In dit schema wordt het volgende
  aangegeven:



Tijdelijk zwart gat (ST-conversie)

Klanten die de snelheid van het opnieuw configureren van hun netwerk testen in het geval van een storing hebben vaak te maken met configuratieproblemen in verband met STP. Denk aan het volgende netwerk, waar een client toegang heeft tot een server via twee verschillende paden. Standaard wordt verkeer van de client naar de server via interface VLAN2 door RSM2 routeerd:



Om een test uit te voeren breekt een gebruiker de verbinding tussen Switch 2 en Switch 3. Onmiddellijk gaat de overeenkomstige poort naar beneden, en de autostate optie RSM brengt interface VLAN2 op RSM2 neer. De direct verbonden route voor de server verdwijnt uit de routingtabel van RSM2, die snel een nieuwe route via RSM1 leert. Met efficiënte routingprotocollen zoals Open Shortest Path First (OSPF) of Enhanced Interior Gateway Routing Protocol (DHCP), is convergentie zo snel dat u nauwelijks een pingelen tijdens deze operatie verliest.

In het geval van mislukking is de omschakeling tussen de twee paden (geel VLAN2 en groen VLAN3) onmiddellijk geweest. Als de gebruiker het verband tussen Switch 2 en Switch 3 opnieuw bevestigt, ervaren de cliënt een verlies van connectiviteit aan de server voor ongeveer 30 seconden.

De reden hiervoor houdt ook verband met de STA. Wanneer STA wordt uitgevoerd, gaat een pas aangesloten poort eerst door de luisteraar en de leerfasen alvorens in expedentiële modus te eindigen. Tijdens de eerste twee 15-seconden stappen, is de haven omhoog, maar brengt geen verkeer over. Dit betekent dat zodra de verbinding wordt aangesloten, de autostate optie van RSM onmiddellijk interface VLAN2 op RSM2 opnieuw toelaat, maar het verkeer kan niet door gaan tot de havens op de verbinding tussen Switch 2 en Switch 3 het expedentiatiefase bereiken. Dit verklaart het verlies van tijdelijke connectiviteit tussen de client en de server. Als het verband

tussen Switch 1 en Switch 2 geen boomstam is, kunt u de eigenschap PortFast toestaan om de luisters en de leerfasen over te slaan en onmiddellijk samen te vallen.

Opmerking: PortFast werkt niet op boomstampoorten. Raadpleeg PortFast of Andere opdrachten om de connectiviteitsvertraging bij het opstarten van het werkstation voor meer informatie op te heffen.

Conclusie

Dit document concentreert zich op sommige RSM-specifieke kwesties, evenals sommige zeer vaak voorkomende interVLAN routeringskwesties. Deze informatie is alleen nuttig wanneer alle normale Cisco IOS-procedures voor het opsporen en verhelpen van routers zijn geprobeerd. Als de helft van de pakketten die door RSM worden routeerd wegens de verkeerde routingtabel verloren gaat, helpt het niet om de DMA-kanaalstatistieken te interpreteren. Zelfs de algemene interVLAN routeringskwesties zijn geavanceerde onderwerpen en komen niet zeer vaak voor. In de meeste gevallen is het overwegen van uw RSM (of een ander geïntegreerd routingapparaat binnen een switch) als eenvoudige externe Cisco IOS router genoeg om het routeren van problemen in een geschakeld milieu te voorzien.

Gerelateerde informatie

- Ondersteuningspagina voor IP-routeringsprotocollen
- IP-meerlaagse switching voor probleemoplossing
- InterVLAN-routing configureren
- Gebruik van PortFast en andere opdrachten voor het repareren van de connectiviteit van het werkstation
- Productondersteuningspagina's voor LAN
- Ondersteuningspagina voor LAN-switching
- Technische ondersteuning en documentatie – Cisco Systems