Resolver problemas el (RSM) y el InterVLAN Routing de la módulo Catalyst 5000 RouteSwitch

Contenido

Introducción

Este documento proporciona la información sobre el InterVLAN Routing del troubleshooting con un (RSM) del Route Switch Module en un Catalyst 5000 Family Switch. En lo que respecta a solucionar problemas en el RSM, la primera medida es considerarlo como un simple router externo. Es muy raramente que un problema Específico del RS está causando un problema cuando se refiere el InterVLAN Routing. Por lo tanto, este documento cubre solamente las dos áreas principales en donde éste podría ocurrir:

- **Asuntos relacionados con el hardware RS**: Este documento introduce la arquitectura de RSM y da los detalles en los contadores RS-relacionados adicionales para seguir.
- **Problemas específicos de la configuración del interVLAN** (relacionados sobre todo con la interacción entre el Routers y el Switches): Esto también se aplica a otros routeres internos (tales como la Multilayer Switch Feature Card [MSFC], Route Switch Feature Card [RSFC], 8510CSR, y así sucesivamente), y a menudo a los routeres externos.

Note: Este documento no cubre configurar el InterVLAN Routing en el Catalyst 4000, 5000, and 6000 switches. Para esos detalles, refiera a estos documentos:

- Configuración y descripción del módulo del router para la familia del Catalyst 4500/4000 (WS-X4232-L3)
- *Configurando el módulo para la sección de ruteo de InterVLAN de la* nota de instalación y configuración para el Catalyst 4000 acode el Módulo de servicios 3
- Configuración del Ruteo InterVLAN Mediante un Router Interno (Tarjeta Capa 3) en Switches Catalyst 5500/5000 y 6500/6000 que Ejecutan CatOS System Software

Este documento no cubre el troubleshooting básico del Routing Protocol, o el Multilayer Switching (MLS) - los asuntos relacionados.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

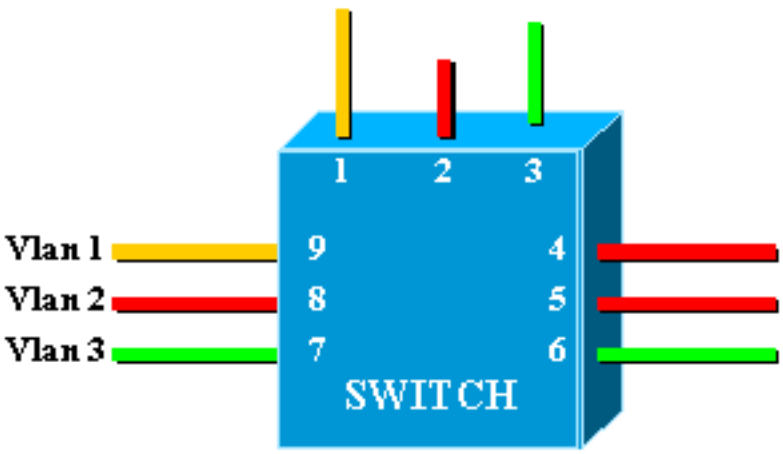
Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

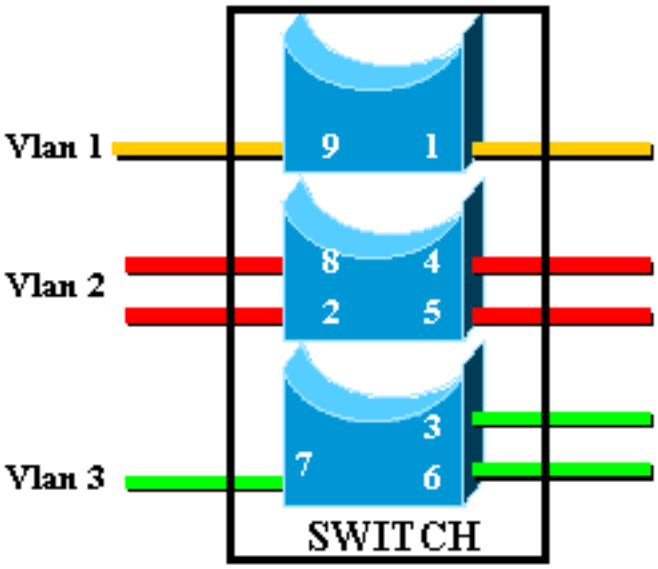
¿Cuál es InterVLAN Routing?

Antes de discutir el InterVLAN Routing, este documento se centra en el concepto de VLAN. Esto no es un debate teórico en la necesidad de los VLA N, sino discute simplemente cómo los VLA N actúan encendido un Switch. Cuando crea VLAN en su switch, es como si dividiera su switch en varios puentes virtuales, cada uno de los cuales conecta sólo los puertos que pertenecen a la misma VLAN.

Este diagrama representa un Switch con nueve puertos asignados a tres diversos VLA N:



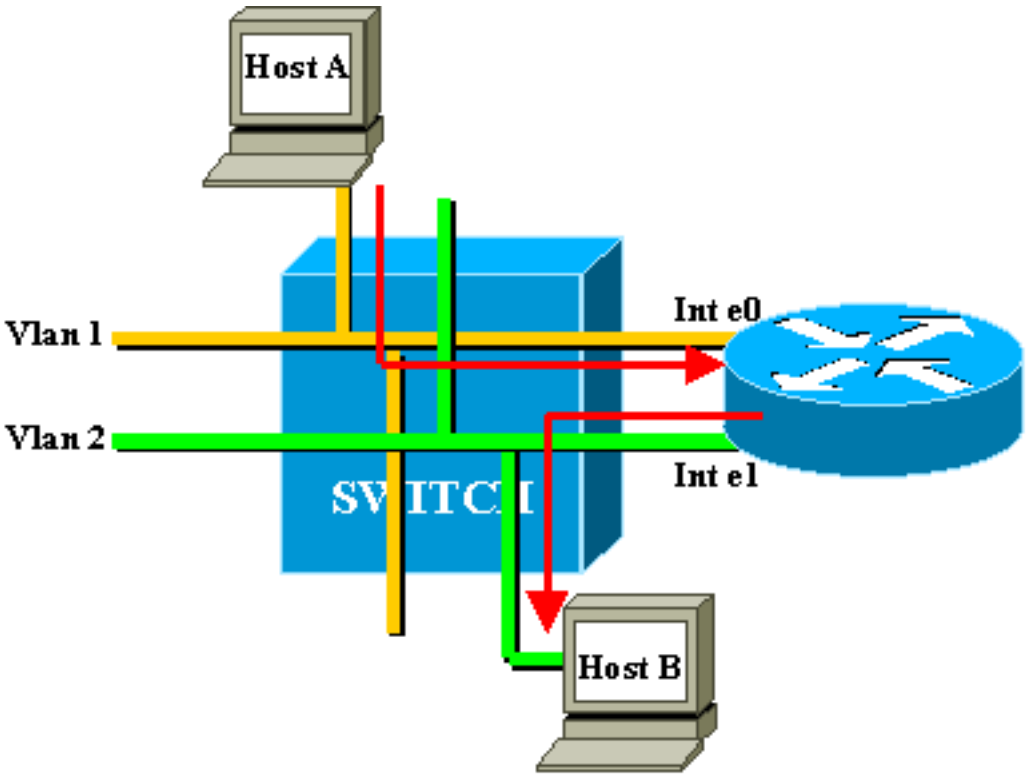
Esto es exactamente equivalente a la red siguiente, que consiste en tres Bridges independientes:



En el switch, hay tres puentes diferentes debido a que cada VLAN crea un puente separado. Puesto que cada VLA N crea un caso del protocolo del árbol de expansión separado (STP), el STP mantiene tres diversas tablas de reenvío.

Usando el segundo diagrama, llega a ser obvio que aunque estén conectados con el mismo dispositivo físico, los puertos que pertenecen a diversos VLA N no pueden comunicar directamente en la capa 2 (L2). Aún cuando fuera posible, esto sería inapropiado. Por ejemplo, si usted el puerto conectado 1 al puerto 4, usted combinaría simplemente el VLAN1 al VLAN2. En este caso, no sería necesario tener dos VLAN separadas.

La única Conectividad que usted quiere entre los VLA N es alcanzada en la capa 3 (L3) por un router. Éste es InterVLAN Routing. Para simplificar más lejos los diagramas, los VLA N se representan como diversos segmentos Ethernet físicos, pues usted no está realmente interesado en las funciones de Bridging específicas proporcionadas por el Switch.



En este diagrama, los dos VLA N se consideran como dos diversos segmentos Ethernet. El tráfico

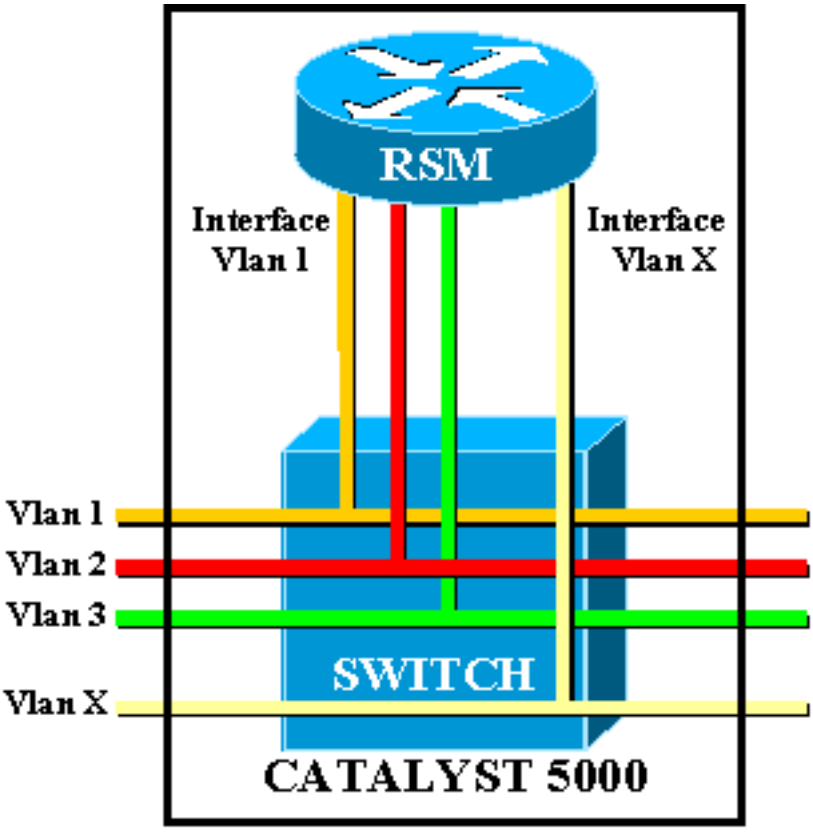
del interVLAN necesita pasar a través del router externo. Si el host A quiere comunicar con el host B, utiliza típicamente al router como default gateway.

Arquitectura de RSM

Arquitectura lógica

Usted puede ver un RS como router externo que tenga varias interfaces conectadas directamente en los diversos VLA N de un Catalyst 5000 Switch.

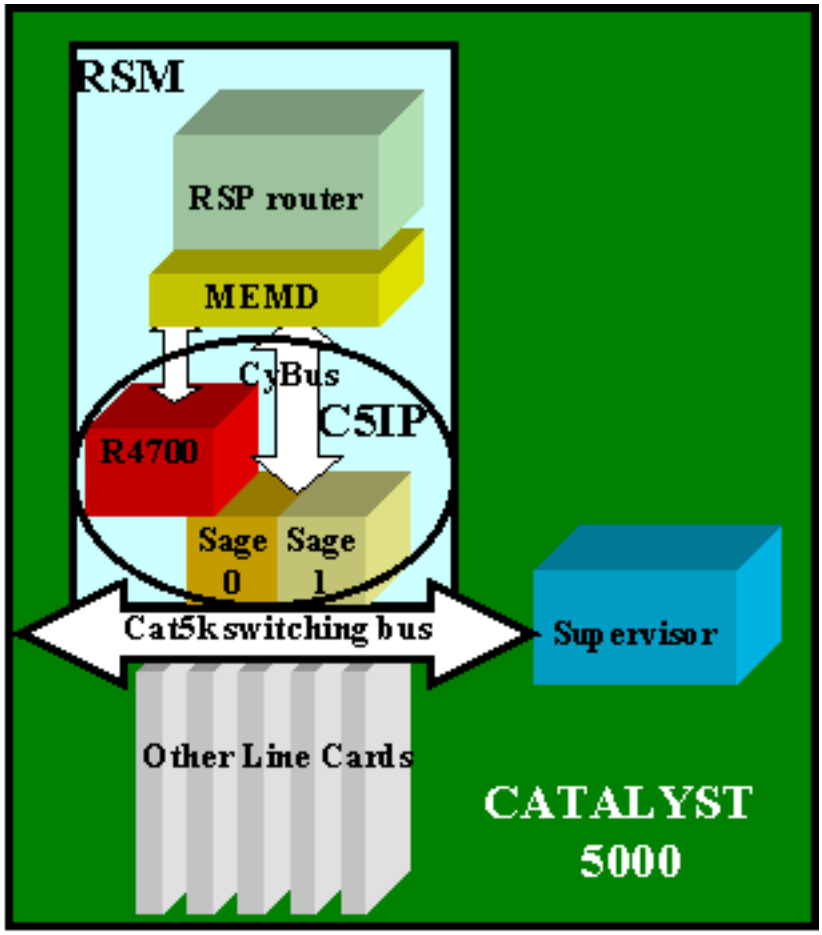
En vez de la llamada una interfaz de Ethernet, estas interfaces se nombran según el VLA N con el cual conectan. (el VLAN1 de la interfaz está conectado directamente con el VLAN1, y así sucesivamente.)



Arquitectura implementada

El RS es un router de la Cisco 7500 ruta Switch Processor (RSP) dentro de un linecard del Catalyst 5000. Usted no necesita saber mucho sobre la arquitectura del indicador luminoso LED amarillo de la placa muestra gravedad menor para configurarlo y para resolver problemas. Sin embargo, teniendo una idea de cómo el RS es ayudas construidas para entender cómo es diferente de un router externo normal. Este conocimiento es especialmente importante al presentar al **comando show controller c5ip**.

Este diagrama establece a los componentes principales en el linecard RS:

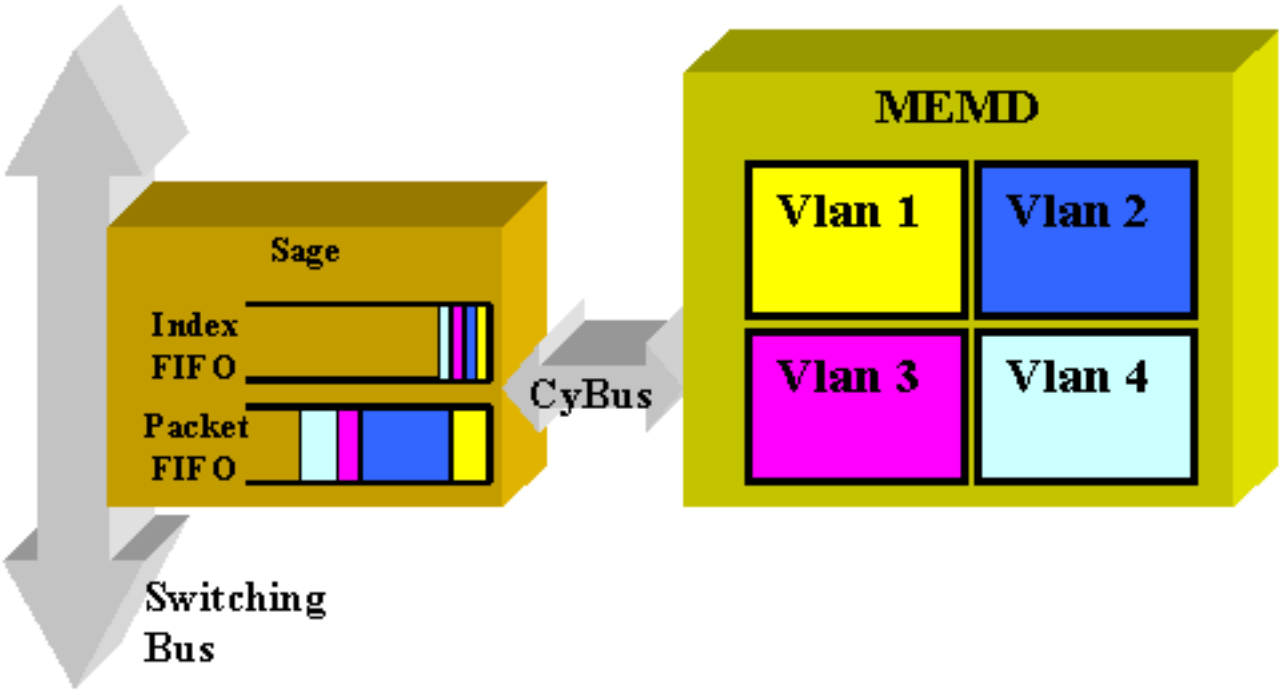


Catalyst 5000 Interface Processor

El Catalyst 5000 Interface Processor (C5IP) es la parte del RS que emula a un sistema IP del Catalyst 7500, con el Switching Bus del Catalyst 5000 como la interfaz de la red. El C5IP incluye un procesador R4700 junto con dos circuitos específicos de la aplicación SABIOS (Asics), que son responsables del acceso al Switching Bus del Catalyst 5000.

SAGE.

Este dos Asics consiguen los paquetes desde/hasta el Switching Bus y los mitigan. Junto con los datos contenidos en el paquete, también obtienen un índice que identifica el destino del paquete en el switch.



La interfaz del VLAN de destino no se determina del contenido del paquete sí mismo, sino se deriva del índice. El paquete y el índice primero se salvan en dos diversos (Primero en Entrar, Primero en Salir FIFO) dentro del SABIO. Se lee el índice y se reserva la memoria compartida necesaria en el área de la VLAN de destino. Luego el paquete se copia al dispositivo de memoria (MEMD), mediante un Acceso de memoria directo (DMA) al SAGE.

Dos SAGE que trabajan paralelamente para comunicar entre el router y el Switching Bus pueden llevar al fuera de la entrega del paquete de la secuencia. (Por ejemplo, un paquete grande recibido en el SAGE0 podría ser transmitido después de que un pequeño paquete recibido más adelante por el SAGE1.) Para evitar esto, cada VLA N se asigna estáticamente a un SABIO dado. Esto se hace automáticamente en el lanzamiento. (Según el router, un VLA N se asocia a uno de los dos canales DMA, cada uno de ellos que llevan a un SABIO.) Los paquetes que llegan de una VLAN determinada siempre se entregan en secuencia.

MEMD

El MEMD es memoria compartida usada por el router para enviar y para recibir los paquetes. Cada interfaz del VLAN configurado en el RS se afecta un aparato a una parte de memoria compartida disponible. Mientras haya más interfaces VLAN configuradas, habrá una menor cantidad de memoria compartida por interfaz. Las interfaces VLAN llevan a cabo a su parte de memoria compartida incluso cuando es discapacitado o apagado. Solamente administrativo agregar o la eliminación de una interfaz VLAN acciona un nuevo reparto del MEMD entre las interfaces VLAN.

Troubleshooting de RSM Específico

Los problemas Específicos del RS principales que no se cubren en la documentación del router usual de Cisco IOS® son problemas con acceder el RS, y también problemas de rendimiento.

Acceso a RSM

El RS se puede acceder en tres maneras diferentes:

- Telnet al RSM
- Sesión adentro al RS del supervisor del Switch
- Conexión de consola directa

Telnet al RSM

Para establecer una conexión de Telnet hacia el RSM, debe conocer la dirección IP asignada a una de sus interfaces VLAN. La sesión Telnet funciona de la misma manera que si intentara conectarse a un router normal de Cisco IOS. Usted puede necesitar asignar una contraseña al vty para alcanzar Telnet y el acceso del permiso del aumento.

Este ejemplo muestra a una sesión telnet de un Supervisor Engine a un RS, en el cual la dirección IP del VLAN1 es 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
```

Esto es similar a las otras configuraciones externas del router IOS de Cisco.

Sesión adentro al RS del supervisor del Switch

Usando del Supervisor Engine le conecta con el RS en el slot *x.*

El método es el mismo que el anterior: el RSM tiene una interfaz VLAN0 oculta que tiene una dirección IP 127.0.0.(x+1), donde x es la ranura donde el RSM se instala. **El comando session** publica a una sesión telnet ocultada a este direccionamiento.

Note: Esta vez, vty y contraseñas habilitadas no tienen que estar en la configuración para ganar el acceso total al RS.

```
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#
```

Usted utiliza el Supervisor Engine Usted puede accederlo directamente usando el **comando session**.

Conexión de consola directa

El puerto de consola del sistema en el RS es DB-25 un puerto del receptáculo DCE para conectar un terminal de datos, que permite que usted configure y que comunique con su sistema. Utilice el cable de la consola proporcionado para conectar la terminal con el puerto de la consola en el RS. El puerto de consola se ubica en el RSM próximo al puerto auxiliar y se etiqueta como consola.

Antes de conectar el puerto de la consola, marque su documentación de la terminal para determinar la velocidad en baudios de la terminal que usted utilizará. La velocidad en baudios de la terminal debe hacer juego la velocidad en baudios predeterminada (9600 baudios). Configure la terminal como: 9600 baudios, ocho bits de datos, ninguna paridad, y dos bits de detención (9600,8N2).

No puede acceder el RS

El RSM puede aislarse por varios motivos. Aun sin ser capaz de conectarlo, hay algunos signos de vida que puede verificar desde afuera:

- Marque el estatus del LED en el RS:El alto LED CPU está apagado — El sistema detectó un error de hardware del procesador.LED DE ESTADO anaranjado — El módulo inhabilitó, prueba en curso, o arranque del sistema en curso.
- Marque el Supervisor Engine para ver si el Switch puede considerar el RS. Para hacer esto, publique el **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 dé por muerto a su RSM antes de haber intentado la conexión de consola. Como usted ha visto, la sesión y el acceso de Telnet están confiando en una conexión IP al RS. Si el RS está iniciando o pegado en el modo ROMMON, por ejemplo, usted no puede Telnet o sesión a ella. Sin embargo, esto es bastante normal.

Incluso si el RS aparece ser defectuoso, intente conectar con su consola. De esta manera, usted puede poder ver algunos mensajes de error, que serán visualizados allí.

Problemas de rendimiento

La mayor parte de los problemas de rendimiento que se relacionan con el RS se pueden localizar averías de la misma manera como con un router normal del Cisco IOS. Esta sección se centra en la parte de específica la implementación de RSM que es los C5IP. El comando show controller c5ip puede dar la información con respecto a la operación del C5IP. Esta salida describe algunos de sus campos más 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 0/1 de DMA

El router RSP dentro del RSM se está comunicando con el switch a través de dos canales DMS diferentes (que van a los dos ASIC SAGE). Cada interfaz VLAN se asocia automáticamente a uno de estos canales DMA. El comando show controllers c5ip muestra información sobre cada uno en dos secciones diferenciadas.

Recibido/transmitido

Estas estadísticas ayudan a identificar la carga en los diferentes canales DMA. Busque un canal DMA que constantemente se sobrecargue comparado a los otros. Esto puede ocurrir si todos los VLA N tráfico-intensivos se asignan al mismo canal DMA. Si fuera necesario, puede asignar manualmente las interfaces VLAN a un canal DMA específico con el comando de interfaz dma-channel.

Suprimidos

Esto indica el número de paquetes que el RS recibió pero cayó. Esto sucede cuando el índice que se recibe junto con el paquete no da el RSM como destino específico del paquete.

Conteos de errores

- **crc** — Los errores del ciclo de la redundancia cíclica (CRC) ocurren cuando un mún CRC es detectado por el RS. No debe haber ninguna paquetes con los malos CRC en el backplane, y el RS que detecta éstos indica que el algún linecards o el otro dispositivo backplane-asociado no está trabajando correctamente.**Note**: Los errores CRC pueden también venir de un dispositivo remoto asociado vía un troncal ISL. La mayoría de las tarjetas de línea Catalyst no verifican la CRC de los paquetes que reciben de la placa de interconexiones y reenvían en un enlace troncal.
- **índice** — Los errores de indexación ocurren cuando el índice no es exacto. El C5IP no es consciente de porqué recibió este paquete. Esto también incrementa el contador descartado.
- **DMAC-longitud** — Estos errores ocurren cuando la interfaz C5IP evitó que el SAGE ASIC sobrara un Tamaño de la unidad máxima de transmisión (MTU) que, si es desapercibido, habría corrompido memoria compartida del router.
- **DMAC-synch** — Si un SAGE ASIC cae un paquete, el paquete (Primero en Entrar, Primero en Salir FIFO) y el índice (Primero en Entrar, Primero en Salir FIFO) se convierten fuera del

synch. Si ocurre este error, se detecta automáticamente y se incrementa el contador dmac-synch. Es poco probable que esto ocurra, pero si lo hace, el impacto del rendimiento es extremadamente - bajo.

- **DMAC-descanso** — Este contador fue agregado al **comando show controllers c5ip** en los Cisco IOS Software Releases 11.2(16)P y 12.0(2). Incrementa cuando una transferencia DMA no completa dentro del tiempo máximo requerido para la transferencia posible más larga. Indica un desperfecto de hardware, y un RS que muestra un valor distinto a cero para este contador es buen candidato para reemplazo.
- **ignore** — Ignores ocurre cuando el router se ejecuta de los buffers MEMD para los paquetes de entrada. Esto sucede cuando el CPU no está procesando los paquetes tan rápidamente como están viniendo adentro. Probablemente, esto se deba a aquello que mantiene ocupada a la CPU.
- **línea-abajo** — La línea-abajo indica que los paquetes destinados a un VLA N del Line Protocol abajo fueron caídos. El C5IP recibió un paquete para una interfaz VLAN que cree estar abajo. Esto no debe suceder, puesto que el Switch debe parar el remitir de los paquetes a una interfaz RS que esté abajo. A pesar de eso, se pueden ver algunos cuando una interfaz cae, debido a la sincronización entre la RSM que declara la caída de la interfaz y el switch que está siendo notificado.
- **runt/gigante** — Este contador sigue los paquetes del inválido-tamaño.
- **unicast-inundación** — Los paquetes de inundación de unidifusión son paquetes enviados a una dirección MAC específica. La tabla de Memoria direccionable por contenido (CAM) de Catalyst 5000 no sabe en qué puerto está ubicada la dirección MAC; por lo tanto, inunda el paquete en todos los puertos en la VLAN. El RS también recibe estos paquetes, pero a menos que se configure para el bridging en ese VLA N, no está interesado en los paquetes que no hacen juego su propia dirección MAC. El RS lanza estos paquetes lejos. Éste es el equivalente de qué sucede en una interfaz de Ethernet real en el chip de la interfaz de Ethernet, que se programa ignorar los paquetes para otras direcciones MAC. En el RSM, esto se realiza en el software C5IP. La mayor parte de los paquetes perdidos son paquetes de inundación de unidifusión.
- **El descenso más reciente** — Este contador revela la información específica sobre el paquete perdidos más reciente. Ésta es la información de bajo nivel que está fuera del ámbito de este documento.

Distribución de VLAN entre canales DMA

A continuación se incluye parte de la salida del comando show controllers c5ip en un RSM que tiene diez interfaces de 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
```

Este resultado muestra a qué canal DMA se asignó una determinada VLAN. Usted puede ver que

los VLAN impares van a canalizar 0, mientras que incluso los VLA N se conectan para canalizar 1. en caso necesario, usted pueden cifrar difícilmente esta correspondencia usando el DMA-**canal del** comando interface configuration. Este ejemplo muestra cómo asignar el VLAN1 de la interfaz de un RS al 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.
```

Información VLAN0

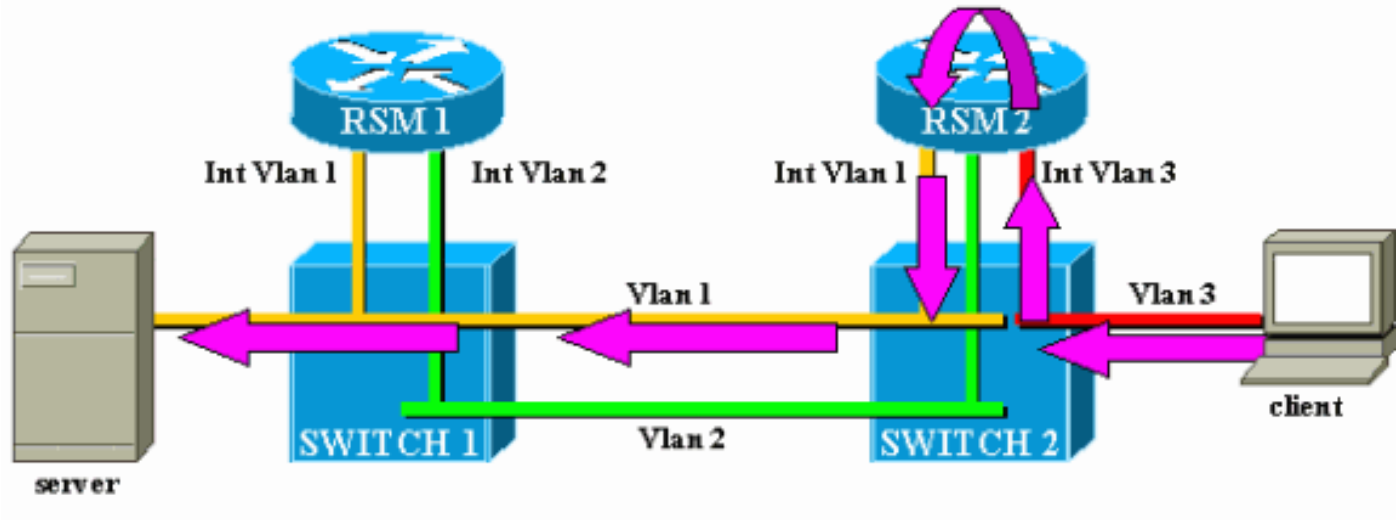
El propósito principal del VLAN0 es asegurar la comunicación efectiva al Supervisor Engine del Switch. Como esta es una interfaz oculta, no puede utilizar un comando simple show interface vlan0 para ver las estadísticas al respecto.

Problemas frecuentes del InterVLAN Routing

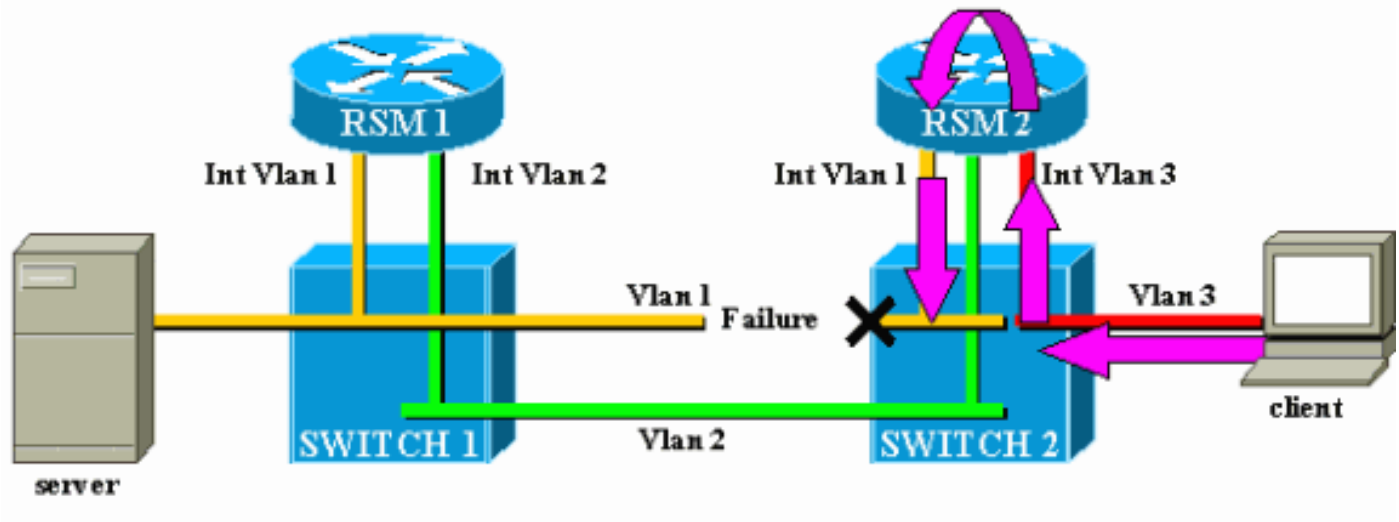
Uso de la característica RSM Autostate

Un problema frecuente con la conexión en puente es que un link dañado puede dividir fácilmente una red L2 en dos partes. Esta situación se debe evitar en cualquier precio, pues una red no contigua rompe la encaminamiento. (Esto es alcanzada generalmente desplegando los links redundantes.)

Considere este ejemplo, donde un cliente asociado en el Switch2 comunica con un servidor conectado en el Switch1:



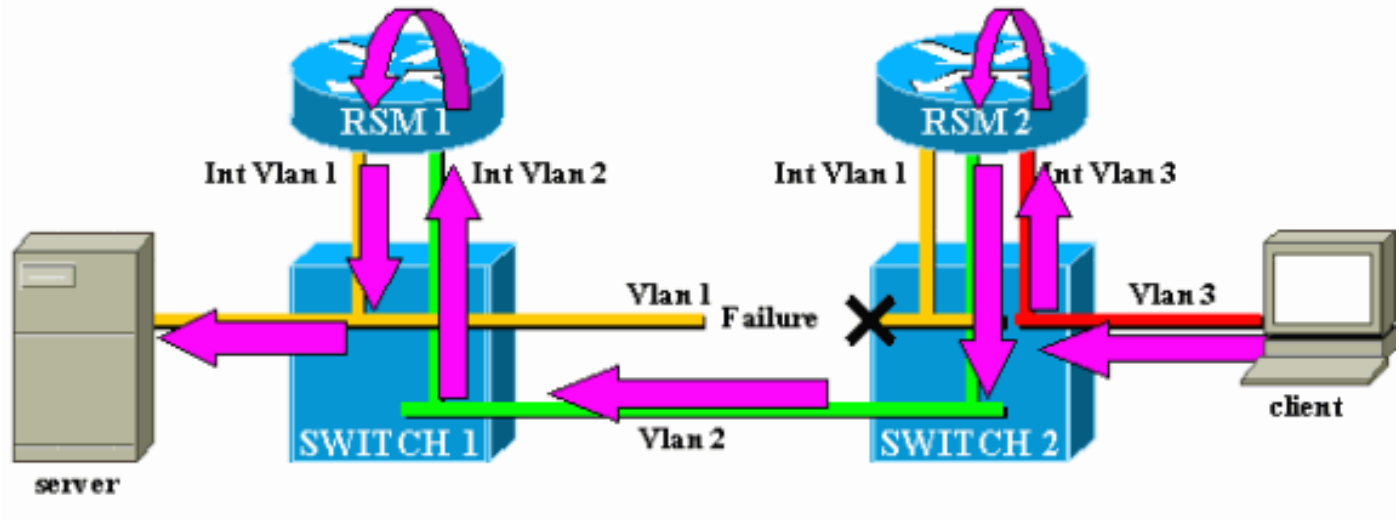
Considere el tráfico del cliente al servidor solamente. El tráfico entrante del cliente en el VLAN3 es ruteado por el RSM2, que tiene una conexión directa a la subred del servidor vía su interfaz VLAN2. Las flechas violetas representan la ruta seguida:



Suponga que el link entre el Switch1 y el Switch2 se rompe para el VLAN1. El problema principal aquí es que, desde el punto de vista del RSM2, nada cambió en la red. El RSM2 todavía tiene una interfaz asociada directamente al VLAN1, y guarda el tráfico de reenvío del cliente al servidor vía esta trayectoria. El tráfico está perdido en el Switch 2 y la conectividad entre el cliente y el servidor se quebró.

La función de estado automático RSM se diseñó para tratar esto. Si no existe un puerto activo para una VLAN específica en el switch, se desactiva la interfaz VLAN correspondiente de RSM.

En el caso del ejemplo, cuando el link en el VLA N entre el Switch1 y el Switch2 falla, el único puerto en el VLAN1 en el Switch2 va abajo (link abajo). Función Autostate de rsm inhabilita el VLAN1 de la interfaz en el RSM2. Ahora que el VLAN1 de la interfaz está abajo, el RSM2 puede utilizar un Routing Protocol para encontrar otra trayectoria para paquetes destinada para el servidor y adelante para traficar eventual vía otra interfaz, tal y como se muestra en de este diagrama:



Autostate de rsm trabaja solamente si no hay otro puerto para arriba en el VLA N. Por ejemplo, si usted tuviera otro cliente en el VLAN1 asociado al Switch2, o RS en el chasis con un VLAN1 de la interfaz definido, el VLAN1 de la interfaz no sería inhabilitado si el link entre el Switch1 y el Switch2 falló. El tráfico se vería interrumpido nuevamente.

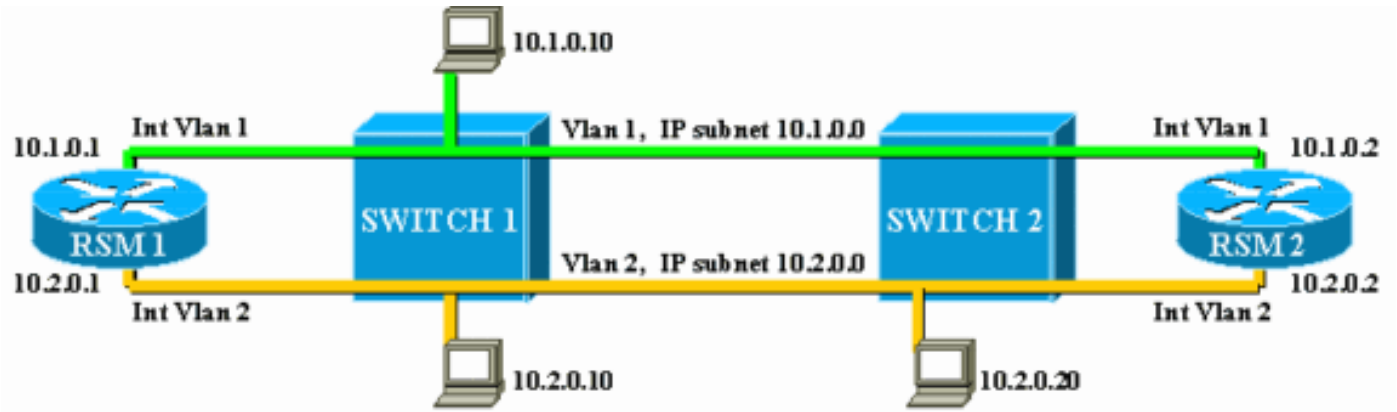
La función RSM autostate está activada de manera predeterminada. Si es necesario, puede ser inhabilitado manualmente usando el comando set rsmautostate en el Supervisor Engine:

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

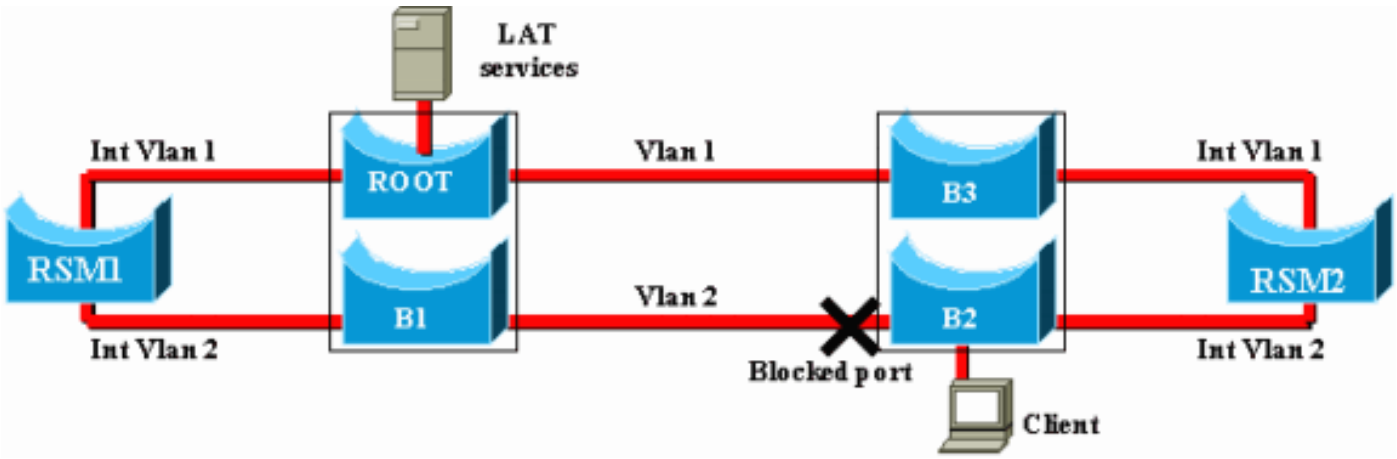
Conexión en puente de despliegue

El Fall-Back Bridging consiste en el interligar de los protocolos entre los VLA N, mientras que rutea algunos otros. Si es posible, debe evitar este tipo de configuración y sólo utilizarla durante un período de migración transitorio. Típicamente, esto es necesario cuando usted ha dividido su red en segmentos con diversas subredes IP, cada uno en un diverso VLA N, pero usted quiere guardar el interligar de algunos viejos protocolos no enrutables ([LAT] del transporte de área local, por ejemplo). En este caso, quiere usar su router RSM como router para IP, pero como puente para otros protocolos. Esto se logra simplemente configurando la conexión en puente de las interfaces RSM, a la vez que se mantienen las direcciones IP. El siguiente ejemplo ilustra una red muy simple con conexión en puente de repliegue, junto con el problema más común que puede ocurrir con este tipo de configuración.

Esta misma red simple se hace de dos VLA N, correspondiente a dos diversas subredes IP. Los host en un VLA N dado pueden utilizar los dos RS uces de los como un default gateway (o aún ambos, usando el protocolo del router de la espera en caliente [HSRP]), y pueden comunicar así con los host en el otro VLA N. La red parece esto:



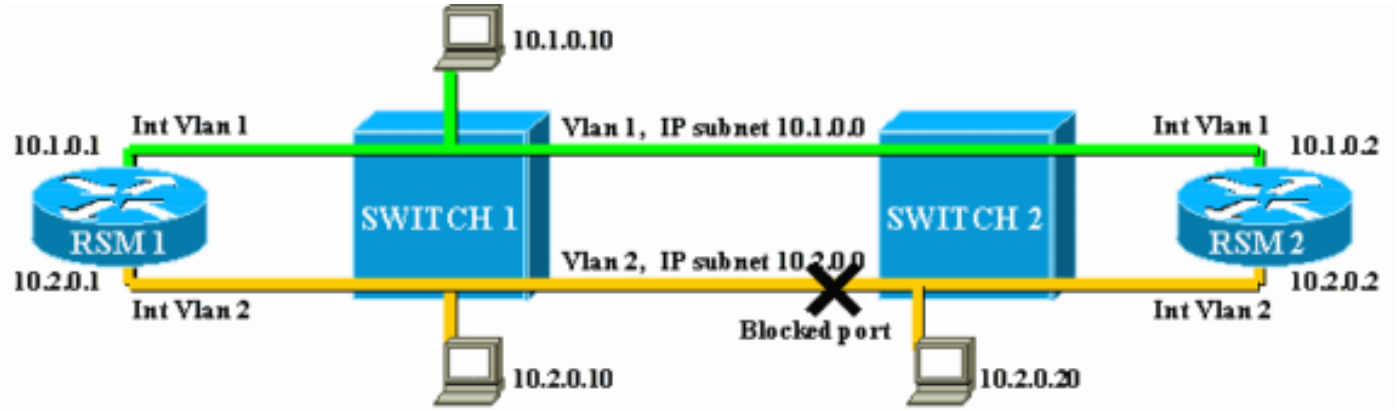
Los dos RSM también están configurados para realizar una conexión en puente de otros protocolos entre sus interfaces, VLAN1 y VLAN2. Suponga que usted tiene los servicios de ofrecimiento de un LAT del host y un cliente que los usa. Su red parecerá esto:



Para este diagrama, cada Catalyst está partido en dos diversos Bridges (uno para cada VLA N).

Usted puede ver que el interligar entre los dos VLA N dio lugar a una fusión de los dos VLA N. Por lo que los Bridged Protocol, usted tiene solamente un VLA N, y el servidor LAT y el cliente pueden comunicar directamente. Por supuesto, esto también implica que usted tiene un loop en la red y que el STP tiene que bloquear un puerto.

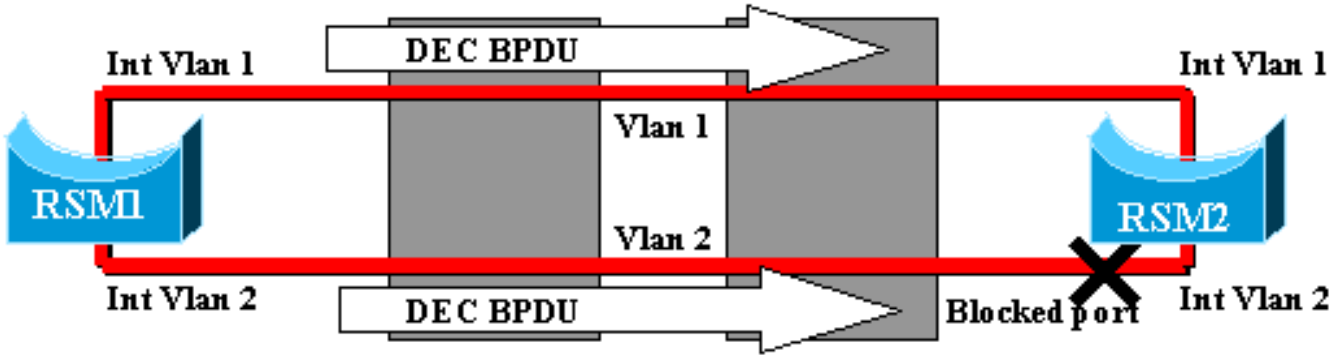
Como puede ver, va a surgir un problema desde este puerto de bloqueo. Un Switch es un dispositivo puro L2 y no puede distinguir entre el IP y el tráfico LAT. Por lo tanto, si el Switch2 bloquea un puerto, como en el diagrama antedicho, bloquea todos los tipos de tráfico (IP, LAT, u otro). Debido a esto, su red parece esto:



El VLAN2 está partido en dos porciones, y usted tiene una subred discontinua 10.2.0.0. Con esta configuración, el host 10.2.0.10 no puede comunicarse con el 10.2.0.20, aunque estén en la misma subred y VLAN.

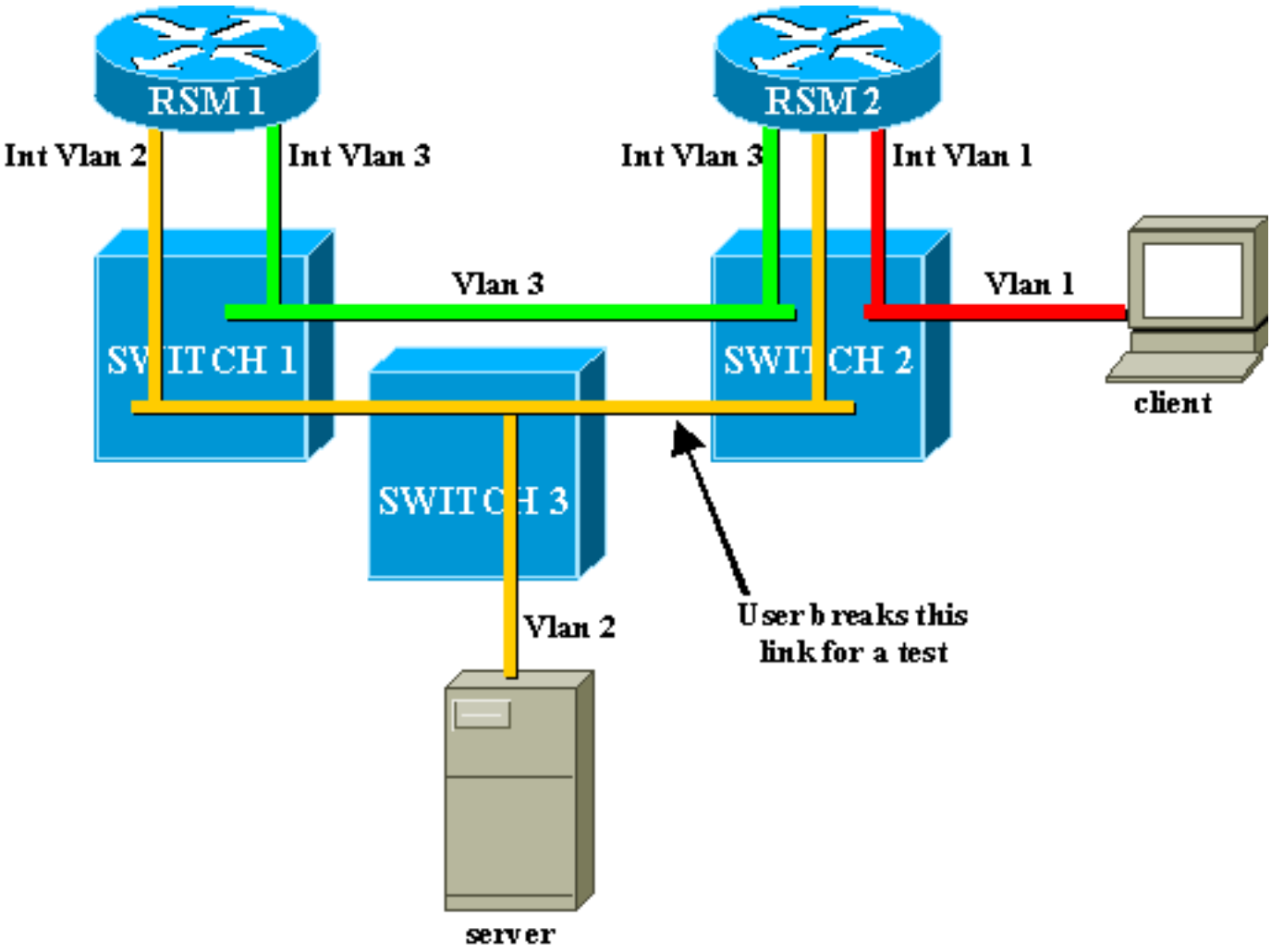
La única solución es mover el puerto bloqueado en el único dispositivo que puede distinguir el tráfico L2 y L3. Ese dispositivo es el RSM. Existen dos maneras principales para lograr esto:

- **Ajuste de parámetros STP:** Usted necesita aumentar el coste en un o vario dispositivos de modo que, eventual, el puerto de bloqueo está situado en el RSM1 o el RSM2. Este método es poco flexible e implica una configuración STP muy estricta. Agregar un Switch o el cambio del ancho de banda de un link (Fast EtherChannel o Gigabit Ethernet) puede causar un retrabajo completo de ajustar.
- **Al utilizar un algoritmo de árbol de expansión (STA) en el RSM:** El Switches ejecuta solamente el IEEE STA y es totalmente transparente al DEC STP. Si usted configura el DEC STP en ambos RS, él trabaja como si él fuera conectado directamente junto, y uno de ellos bloqueará. Este diagrama ilustra
  esto:



Agujero negro temporal (convergencia ST)

En general, los clientes que verifican la velocidad de la reconfiguración de su red en caso de falla experimentan problemas de configuración relacionados con STP. Considere la red siguiente, donde los accesos al cliente un servidor vía dos diversas trayectorias. La opción predeterminada es rutear el tráfico desde el cliente al servidor a través de la interfaz VLAN2 por RSM2:



Para realizar una prueba, el usuario interrumpe el link entre el switch 2 y el switch 3. Inmediatamente, se cae el puerto correspondiente y la función RSM autostate hace caer la interfaz VLAN2 en RSM2. La ruta para el servidor conectada directamente desaparece de la tabla de ruteo de RSM2 que rápidamente aprende una nueva ruta a través de RSM1. Con los protocolos del ruteo eficaz como el Open Shortest Path First (OSPF) o el Enhanced Interior Gateway Routing Protocol (EIGRP), la convergencia es tan rápidamente que usted pierde apenas un ping durante esta operación.

En caso de alguna falla, el intercambio entre los dos trayectos (VLAN2 amarilla y VLAN3 verde) ha sido inmediato. Si el usuario restablece el link entre el Switch2 y el Switch 3, sin embargo, el cliente experimenta una pérdida de conectividad al servidor por cerca de 30 segundos.

La razón de esto está también relacionada con STA. Al ejecutar STA, un puerto recién conectado primero pasa por los pasos de escucha y aprendizaje antes de terminar en el modo de reenvío. Durante las primeras dos etapas 15-second, el puerto está para arriba, pero no transmite el tráfico. Esto significa que tan pronto como el link esté conectado, Función Autostate de rsm vuelve a permitir inmediatamente la interfaz VLAN2 en el RSM2, pero el tráfico no puede ir a través hasta que los puertos en el link entre el Switch2 y el Switch 3 alcancen la etapa de la expedición. Esto explica la pérdida de conectividad temporal entre el cliente y el servidor. Si el link entre el Switch 1 y 2 no es un tronco, puede activar la función portfast para saltear los pasos de

escucha y aprendizaje y convergir de forma inmediata.

Note: Portfast no funciona en los puertos troncales. Consulte Uso de Portfast y de Otros Comandos de Reparar Demoras en la Conectividad de Inicialización de Estaciones de Trabajopara obtener más información.

Conclusión

Este documento se centra en algunos problemas Específicos del RS, así como un cierto InterVLAN Routing muy común publica. Esta información es solamente útil cuando se han intentado todos los procedimientos deTroubleshooting normales del router del Cisco IOS. Si la mitad de los paquetes ruteados por un RS se pierde debido a la tabla de ruteo incorrecta, no ayuda a intentar interpretar las estadísticas del DMA-canal. Incluso los problemas generales del InterVLAN Routing son temas más complejos y no ocurren muy a menudo. En la mayoría de los casos, si considera su RSM (o cualquier otro dispositivo de ruteo integrado dentro de un switch) como un simple router externo del Cisco IOS, es suficiente para solucionar problemas relacionados con el ruteo en un entorno conmutado.

Información Relacionada

- Página de Soporte de IP Routed Protocols
- Resolver problemas el IP MultiLayer Switching
- Configurar el InterVLAN Routing
- Utilización de Portfast y Otros Comandos para Solucionar Demoras al Iniciar la Conectividad de la Estación de Trabajo
- Páginas de Soporte de Productos de LAN
- Página de Soporte de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems