Risoluzione dei problemi di modulo Catalyst 5000 Route Switch (RSM) e routing tra VLAN

Sommario

Introduzione

In questo documento viene illustrato come risolvere i problemi di routing tra VLAN con un Route Switch Module (RSM) su uno switch della famiglia Catalyst 5000. Quando si tratta di risolvere i problemi dell'RSM, la prima cosa da fare è considerarlo un semplice router esterno. Molto raramente un problema specifico del modulo RSM causa un problema di routing tra VLAN. Il presente documento copre pertanto solo i due settori principali in cui ciò potrebbe verificarsi:

- **Problemi correlati all'hardware RSM**: In questo documento viene introdotta l'architettura RSM e vengono forniti dettagli sui contatori RSM aggiuntivi di cui tenere traccia.
- **Problemi specifici di configurazione tra VLAN** (per lo più relativi all'interazione tra router e switch): Ciò vale anche per altri router interni, ad esempio Multilayer Switch Feature Card (MSFC), Route Switch Feature Card (RSFC), 8510CSR e così via, e spesso per router esterni.

Nota: questo documento non descrive la configurazione del routing tra VLAN sugli switch Catalyst 4000, 5000 e 6000. Per ulteriori informazioni, fare riferimento ai seguenti documenti:

- Configurazione e panoramica del modulo router per la famiglia Catalyst 4500/4000 (WS-

X4232-L3)

- Nota *sulla configurazione del modulo per il routing tra* VLAN in Installazione e configurazione del modulo dei servizi Catalyst 4000 Layer 3
- Configurazione del routing tra VLAN con un router interno (scheda layer 3) sugli switch Catalyst 5500/5000 e 6500/6000 con software CatOS

Questo documento non descrive la risoluzione dei problemi di base dei protocolli di routing o i problemi relativi alla commutazione multilivello (MLS).

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

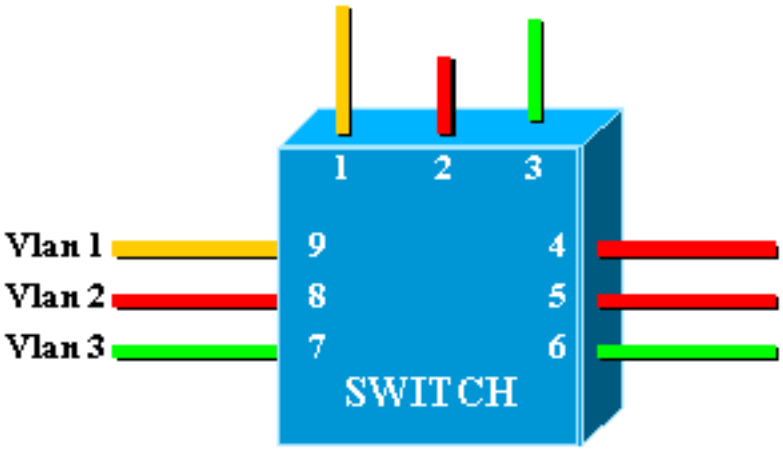
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

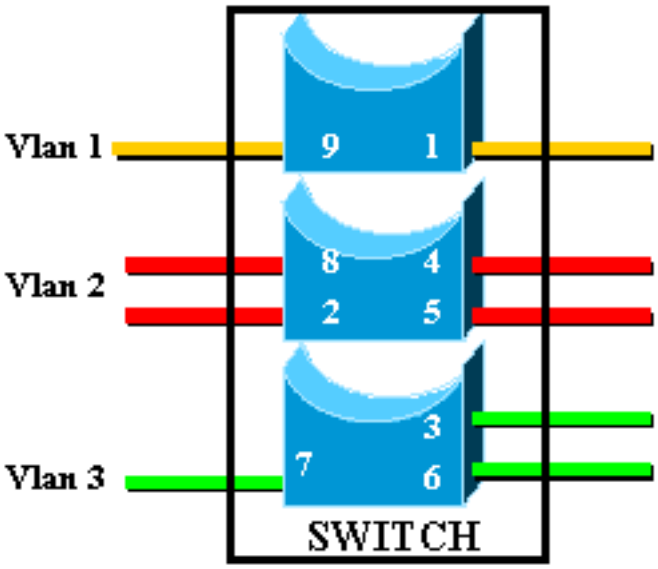
Cos'è il routing tra VLAN?

Prima di parlare del routing tra VLAN, questo documento si concentra sul concetto di VLAN. In questo corso non si parla teoricamente della necessità di avere VLAN, ma si parla semplicemente del funzionamento delle VLAN su uno switch. Quando si creano le VLAN sullo switch, è come suddividere lo switch in più bridge virtuali, ciascuno con solo porte di bridging appartenenti alla stessa VLAN.

Il diagramma mostra uno switch con nove porte assegnate a tre VLAN diverse:



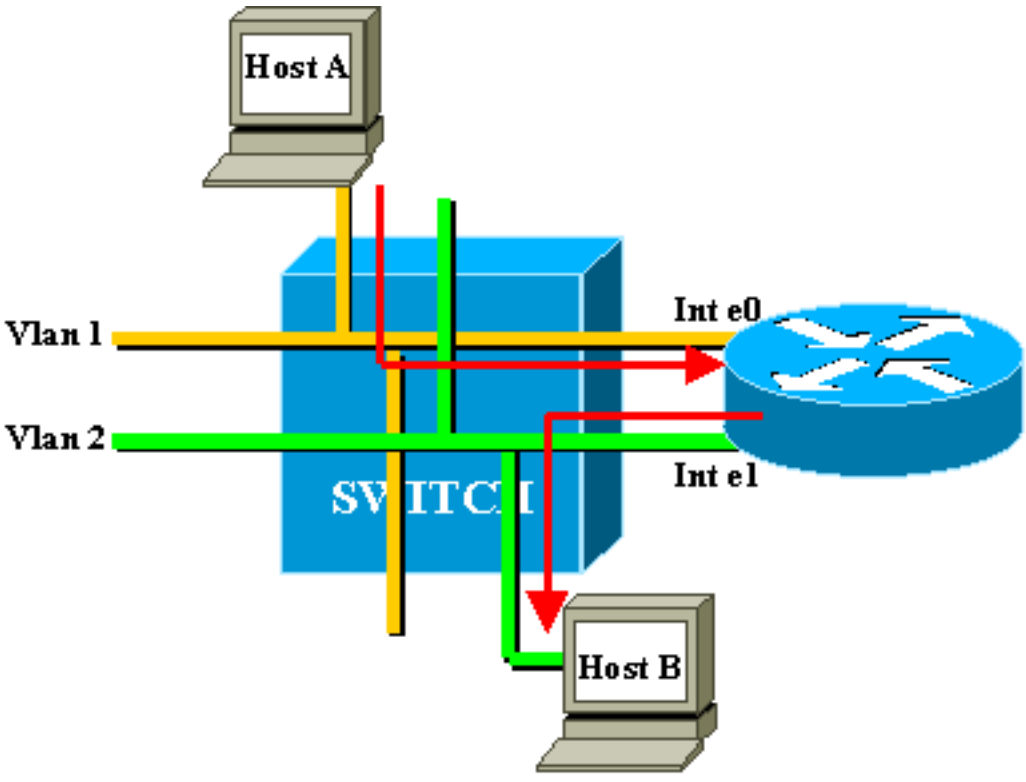
Ciò è esattamente equivalente alla seguente rete, costituita da tre ponti indipendenti:



Nello switch, sono presenti tre bridge diversi, perché ciascuna VLAN crea un bridge separato. Poiché ciascuna VLAN crea un'istanza STP (Spanning Tree Protocol) separata, STP mantiene tre tabelle di inoltro diverse.

Utilizzando il secondo diagramma, è evidente che, sebbene connesse allo stesso dispositivo fisico, le porte appartenenti a VLAN diverse non possono comunicare direttamente al layer 2 (L2). Anche se possibile, ciò non sarebbe appropriato. Ad esempio, se si collega la porta 1 alla porta 4, è sufficiente unire la VLAN1 alla VLAN2. In questo caso, non è necessario avere due VLAN separate.

L'unica connettività desiderata tra le VLAN è garantita al layer 3 (L3) da un router. Questo è il routing tra VLAN. Per semplificare ulteriormente i diagrammi, le VLAN sono rappresentate come segmenti Ethernet fisici diversi, in quanto l'utente non è realmente interessato alle funzioni di bridging specifiche fornite dallo switch.



In questo diagramma, le due VLAN sono considerate due segmenti Ethernet diversi. Il traffico tra

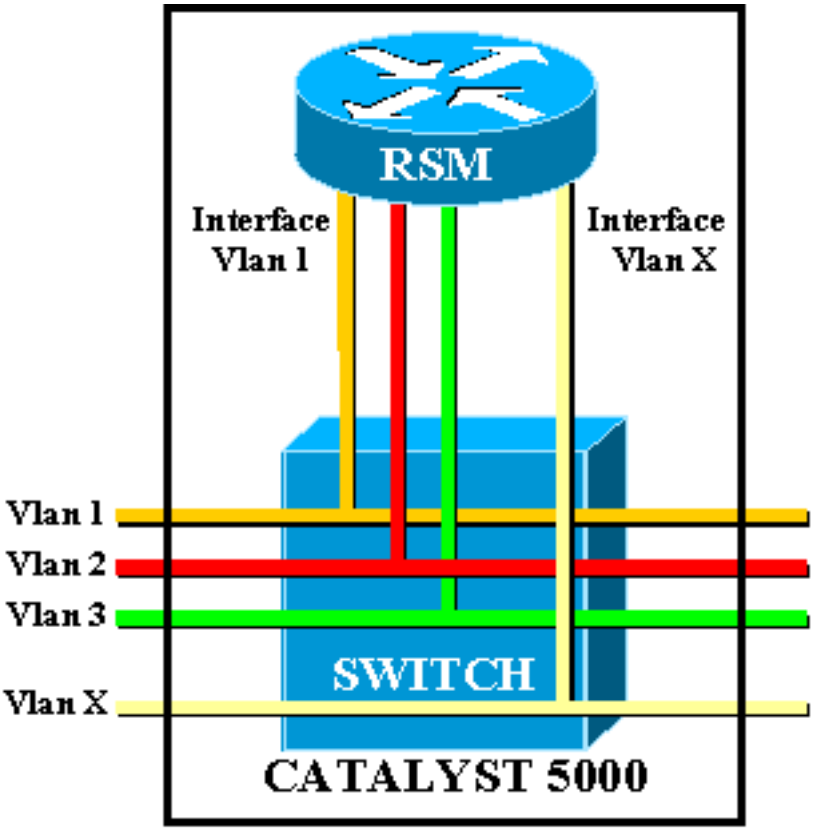
VLAN deve passare attraverso il router esterno. Se l'host A desidera comunicare con l'host B, in genere utilizza il router come gateway predefinito.

Architettura RSM

Architettura logica

Èpossibile visualizzare un modulo RSM come router esterno con diverse interfacce collegate direttamente alle diverse VLAN di uno switch Catalyst 5000.

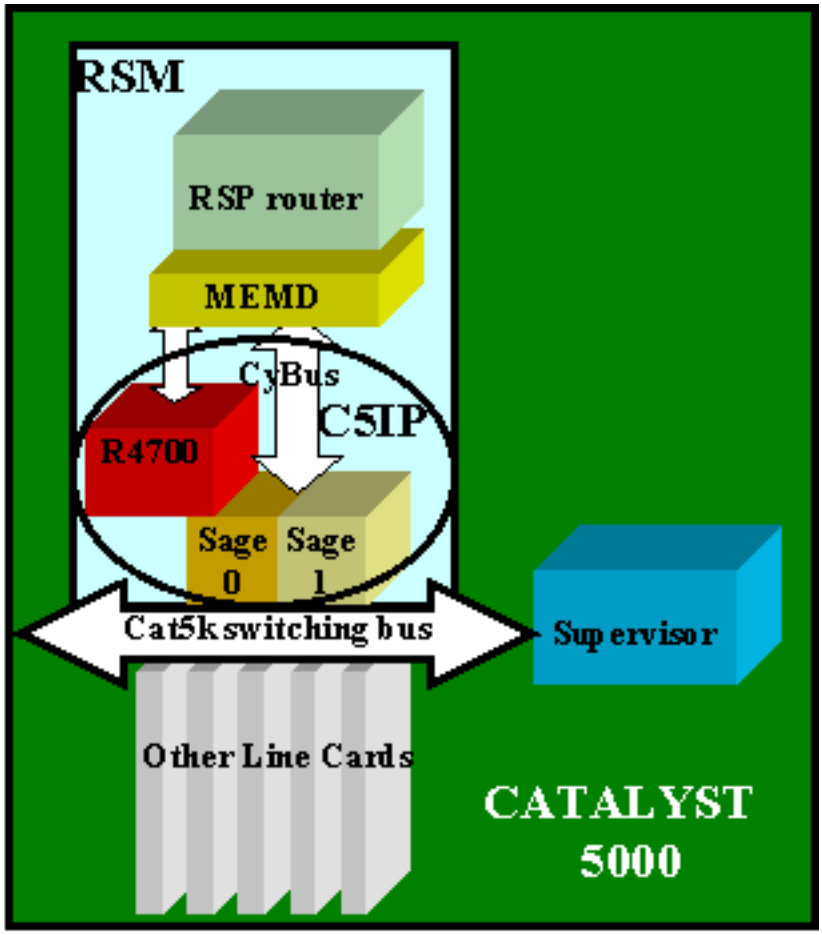
Anziché essere chiamate interfacce Ethernet, queste interfacce sono denominate in base alla VLAN a cui si connettono. (l'interfaccia VLAN1 è collegata direttamente alla VLAN1, e così via).



Implementazione dell'architettura

Il modulo RSM è un router Cisco 7500 Route Switch Processor (RSP) all'interno di una scheda di linea Catalyst 5000. Non è necessario conoscere molto sull'architettura della scheda per configurarla e risolverla. Tuttavia, avere un'idea di come è costruito l'RSM aiuta a capire le differenze con un normale router esterno. Questa conoscenza è particolarmente importante quando si introduce il comando **show controller c5ip**.

Il diagramma mostra i componenti principali della scheda di linea dell'RSM:

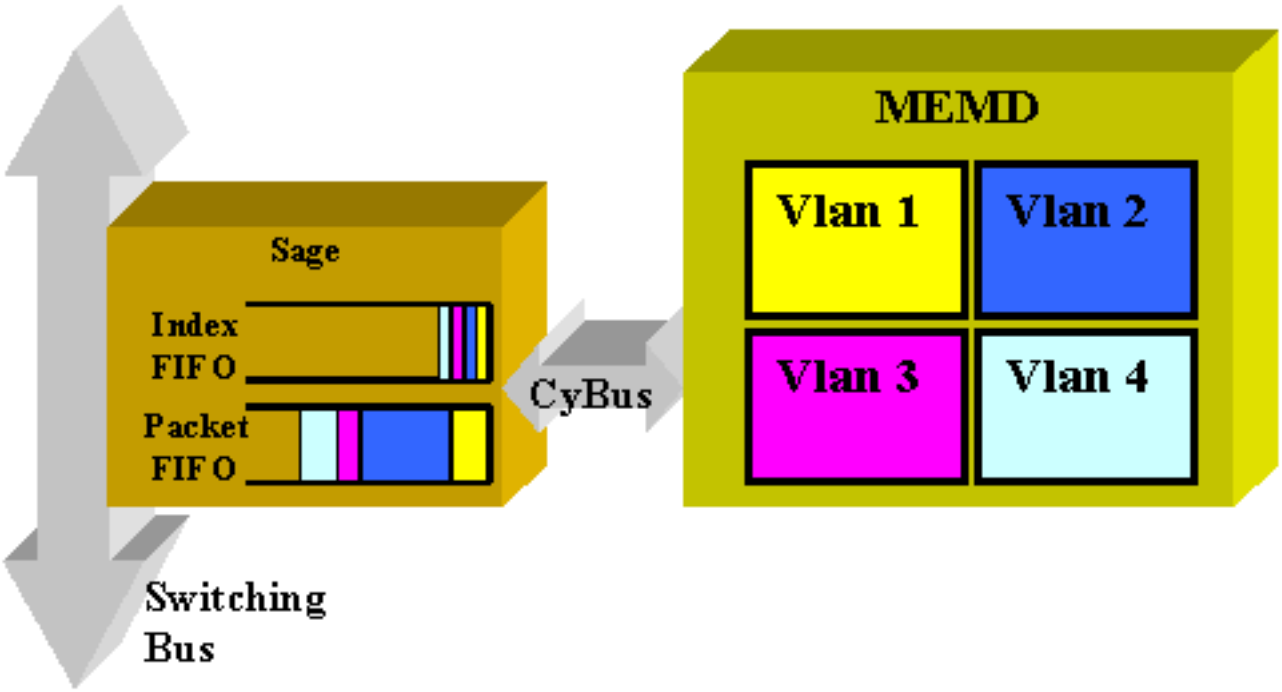


[Catalyst 5000 Interface Processor]

Il processore di interfaccia Catalyst 5000 (C5IP) è la parte del modulo RSM che emula un IP di sistema Catalyst 7500, con il bus di switching Catalyst 5000 come interfaccia di rete. Il C5IP include un processore R4700 e due ASIC (Application-Specific Integrated Circuit) SAGE, responsabili dell'accesso al bus di switching Catalyst 5000.

[SALVIA]

I due ASIC ricevono i pacchetti dal/al bus di switching e li inseriscono nel buffer. Insieme ai dati nel pacchetto, ottengono anche un indice che identifica la destinazione del pacchetto nello switch.



L'interfaccia VLAN di destinazione non viene determinata dal contenuto del pacchetto ma viene derivata dall'indice. Il pacchetto e l'indice vengono inizialmente archiviati in due FIFO diverse all'interno di SAGE. L'indice viene letto e la memoria condivisa necessaria viene riservata nell'area della VLAN di destinazione. Il pacchetto viene quindi copiato nel dispositivo di memoria (MEMD), utilizzando un DMA (Direct Memory Access) per SAGE.

Due SAGE che lavorano in parallelo per comunicare tra il router e il bus di commutazione possono causare una consegna di pacchetti fuori sequenza. (Ad esempio, un pacchetto grande ricevuto su SAGE0 potrebbe essere trasmesso dopo un pacchetto piccolo ricevuto successivamente da SAGE1). Per evitare questo problema, ciascuna VLAN è assegnata in modo statico a un determinato SAGE. Questa operazione viene eseguita automaticamente all'avvio. (A seconda del router, una VLAN è associata a uno dei due canali DMA, ciascuno dei quali porta a un SAGE). I pacchetti di una determinata VLAN vengono sempre consegnati in sequenza.

MEMD

MEMD è la memoria condivisa utilizzata dal router per inviare e ricevere pacchetti. A ciascuna interfaccia VLAN configurata sull'RSM viene assegnata una parte della memoria condivisa disponibile. Maggiore è il numero di interfacce VLAN configurate, minore sarà la memoria condivisa per interfaccia. Le interfacce VLAN conservano la loro parte di memoria condivisa anche quando sono disabilitate o spente. L'aggiunta o la rimozione amministrativa di un'interfaccia VLAN determina solo una nuova ripartizione del MEMD tra le interfacce VLAN.

Risoluzione dei problemi specifici di RSM

I principali problemi specifici dell'RSM non trattati nella documentazione usuale dei router Cisco IOS® sono i problemi di accesso all'RSM e i problemi di prestazioni.

Accesso al modulo RSM

Èpossibile accedere al modulo RSM in tre modi:

- Telnet su RSM
- Sessione nell'RSM dal Supervisor dello switch
- Connessione diretta console

Telnet su RSM

Per connettersi all'RSM in modalità Telnet, è necessario conoscere l'indirizzo IP assegnato a una delle interfacce VLAN. Il funzionamento della sessione Telnet è identico a quello di un router Cisco IOS normale. Potrebbe essere necessario assegnare una password al vty per ottenere Telnet e ottenere l'accesso abilitato.

Nell'esempio viene mostrata una sessione Telnet da un Supervisor Engine a un modulo RSM, in cui l'indirizzo IP della VLAN1 è 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
```

Analogamente ad altre configurazioni di Cisco IOS per i router esterni.

Sessione nell'RSM dal Supervisor dello switch

L'uso del comando **session *x*** del Supervisor Engine permette di connettersi all'RSM nello slot *x*.

Il metodo è lo stesso del precedente: l'RSM ha un'interfaccia VLAN0 nascosta con un indirizzo IP 127.0.0(x+1), dove x è lo slot in cui è installato l'RSM. Il comando **session** invia una sessione Telnet nascosta a questo indirizzo.

Nota: questa volta, non è necessario che le password vty e enable siano nella configurazione per ottenere l'accesso completo all'RSM.

```
sup> (enable) show module
Mod Slot  Ports      Module-Type Model          Status
--- ---- ----- ------------------------ ------------------
1     1    0     Supervisor III WS-X5530          ok
2     2          Route Switch Ext Port
3     3    1     Route Switch WS-X5302            ok
4     4   24     10/100BaseTX Ethernet WS-X5225R  ok
5     5   12     10/100BaseTX Ethernet WS-X5203   ok
!--- Output suppressed. sup> (enable) session 3
Trying Router-3...
Connected to Router-3.
Escape character is '^]'.
rsm> enable
rsm#
```

Il comando **show module** del Supervisor Engine consente di identificare lo slot in cui è installato il modulo RSM nello switch. È possibile accedervi direttamente utilizzando il comando **session**.

Connessione diretta console

La porta console di sistema sull'RSM è una porta DCE di ricezione DB-25 per il collegamento di un terminale dati, che consente di configurare e comunicare con il sistema. Utilizzare il cavo console fornito per collegare il terminale alla porta console sull'RSM. La porta console si trova sull'RSM accanto alla porta ausiliaria ed è denominata console.

Prima di collegare la porta console, consultare la documentazione del terminale per determinare la velocità in baud del terminale che si desidera utilizzare. La velocità in baud del terminale deve corrispondere alla velocità in baud predefinita (9600 baud). Impostare il terminale come: 9600 baud, otto bit di dati, nessuna parità e due bit di stop (9600,8N2).

Impossibile accedere al modulo RSM

Il modulo RSM può essere isolato per diversi motivi. Anche senza essere in grado di collegarsi ad esso, ci sono alcuni segni di vita che si può controllare dall'esterno:

- Controllare lo stato dei LED sull'RSM:Il LED di arresto CPU è spento: il sistema ha rilevato un errore hardware del processore.LED di stato arancione: modulo disabilitato, test in corso o avvio del sistema in corso.
- Controllare il Supervisor Engine per verificare se lo switch può vedere l'RSM. A tale scopo, usare il 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.
```

Non dichiarare mai inattivo il modulo RSM prima di aver tentato la connessione alla console. Come si è visto, sia la sessione che l'accesso Telnet si basano su una connessione IP al modulo RSM. Ad esempio, se il modulo RSM si sta avviando o è bloccato in modalità ROMMON, non è possibile eseguire una sessione Telnet su di esso. Si tratta tuttavia di un comportamento normale.

Anche se il modulo RSM sembra essere difettoso, provare a collegarsi alla relativa console. In questo modo, è possibile che vengano visualizzati alcuni messaggi di errore.

Problemi di prestazioni

La maggior parte dei problemi di prestazioni relativi all'RSM possono essere risolti esattamente come con un normale router Cisco IOS. Questa sezione si concentra sulla parte specifica dell'implementazione RSM che è il C5IP. Il comando **show controller c5ip** può fornire informazioni sul funzionamento del C5IP. Questo output descrive alcuni dei campi più importanti:

```
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#
```

Canale DMA 0/1

Il router RSP all'interno del modulo RSM sta comunicando allo switch tramite due canali DMA distinti (attraverso i due ASIC SAGE). Ogni interfaccia VLAN viene associata automaticamente a uno di questi canali DMA. Il comando **show controller c5ip** visualizza le informazioni su ciascuno di essi in due sezioni distinte.

Ricevuto/Trasmesso

Queste statistiche consentono di identificare il carico sui diversi canali DMA. Cercare un canale DMA costantemente sovraccarico rispetto agli altri. Questo problema può verificarsi se tutte le VLAN a traffico elevato sono assegnate allo stesso canale DMA. Se necessario, è possibile assegnare manualmente le interfacce VLAN a un canale DMA specifico utilizzando il comando interface **dma-channel**.

Eliminato

Indica il numero di pacchetti ricevuti ma scartati dall'RSM. Questo si verifica quando l'indice ricevuto insieme al pacchetto non fornisce l'RSM come destinazione specifica del pacchetto.

Conteggi errori

- **crc** - Gli errori CRC (Cyclic Redundancy Cycle) si verificano quando l'RSM rileva un CRC errato. Sul backplane non devono essere presenti pacchetti con CRC errati e il modulo RSM che rileva questi problemi indica che alcune schede di linea o altri dispositivi collegati al backplane non funzionano correttamente.**Nota:** gli errori CRC possono provenire anche da un dispositivo remoto collegato tramite un trunk ISL. La maggior parte delle schede di linea Catalyst non controlla il CRC di un pacchetto ricevuto dal backplane e inoltrato su un trunk.
- **indice** - Gli errori dell'indice si verificano quando l'indice non è accurato. Il C5IP non è a conoscenza del motivo per cui ha ricevuto il pacchetto. In questo modo viene incrementato anche il contatore Eliminato.
- **dmac-length**: questi errori si verificano quando l'interfaccia C5IP impedisce all'ASIC SAGE di sovraccaricare una dimensione MTU (Maximum Transmission Unit) che, se non rilevata, danneggerebbe la memoria condivisa del router.
- **dmac-synch**: se un SAGE ASIC scarta un pacchetto, il pacchetto FIFO e l'indice FIFO non sono più sincronizzati. Se si verifica questo errore, viene rilevato automaticamente e il contatore `dmac-synch` viene incrementato. È improbabile che ciò avvenga, ma se ciò accade, l'impatto sulle prestazioni è estremamente basso.

- **dmac-timeout**: questo contatore è stato aggiunto al comando **show controller c5ip** nel software Cisco IOS versione 11.2(16)P e 12.0(2). Aumenta quando un trasferimento DMA non viene completato entro il tempo massimo richiesto per il trasferimento più lungo possibile. Indica un errore hardware e un modulo RSM con un valore diverso da zero per questo contatore è un buon candidato per la sostituzione.
- **ignore**: questa opzione viene ignorata quando il router esaurisce i buffer MEMD per i pacchetti di input. Questo si verifica quando la CPU non elabora i pacchetti alla stessa velocità con cui arrivano. Ciò è probabilmente dovuto a ciò che sta tenendo occupata la CPU.
- **line-down**: l'opzione Line-down indica che i pacchetti destinati a una VLAN del protocollo di linea sono stati scartati. Il C5IP ha ricevuto un pacchetto per un'interfaccia VLAN che ritiene non attivo. Questa condizione non deve verificarsi, in quanto lo switch deve interrompere l'inoltro dei pacchetti a un'interfaccia RSM non attiva. Tuttavia, è possibile riscontrarne alcuni quando un'interfaccia non è disponibile, a causa del tempo che intercorre tra l'RSM che dichiara l'interfaccia non attiva e lo switch che viene notificato.
- **runt/giant**: questo contatore consente di tenere traccia dei pacchetti di dimensioni non valide.
- **unicast-flood**: i pacchetti unicast-flood vengono inviati a un indirizzo MAC specifico. La tabella Catalyst 5000 Content Addressable Memory (CAM) non sa su quale porta si trova l'indirizzo MAC, quindi instrada il pacchetto verso tutte le porte della VLAN. Anche l'RSM riceve questi pacchetti, ma a meno che non sia configurato per il bridging sulla VLAN, non è interessato ai pacchetti che non corrispondono al proprio indirizzo MAC. Il modulo RSM scarta questi pacchetti. Questo è l'equivalente di quello che succede su una vera interfaccia Ethernet nel chip dell'interfaccia Ethernet, che è programmato per ignorare i pacchetti per altri indirizzi MAC. Nell'RSM, questa operazione viene eseguita nel software C5IP. La maggior parte dei pacchetti ignorati sono pacchetti unicast-flood.
- **Last drop**: questo contatore rivela informazioni specifiche sull'ultimo pacchetto perso. Si tratta di informazioni di basso livello che esulano dall'ambito del presente documento.

Distribuzione della VLAN tra i canali DMA

Di seguito è riportata parte dell'output del comando **show controller c5ip** su un modulo RSM con dieci interfacce VLAN configurate:

```
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
```

Questo output mostra a quale canale DMA è assegnata una determinata interfaccia VLAN. È possibile vedere come le VLAN dispari passino al canale 0, mentre le VLAN pari sono collegate al canale 1. Se necessario, è possibile codificare questa corrispondenza utilizzando il comando di configurazione interfaccia **dma-channel**. Nell'esempio viene mostrato come assegnare l'interfaccia VLAN1 di un modulo RSM al canale 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.
```

Informazioni VLAN0

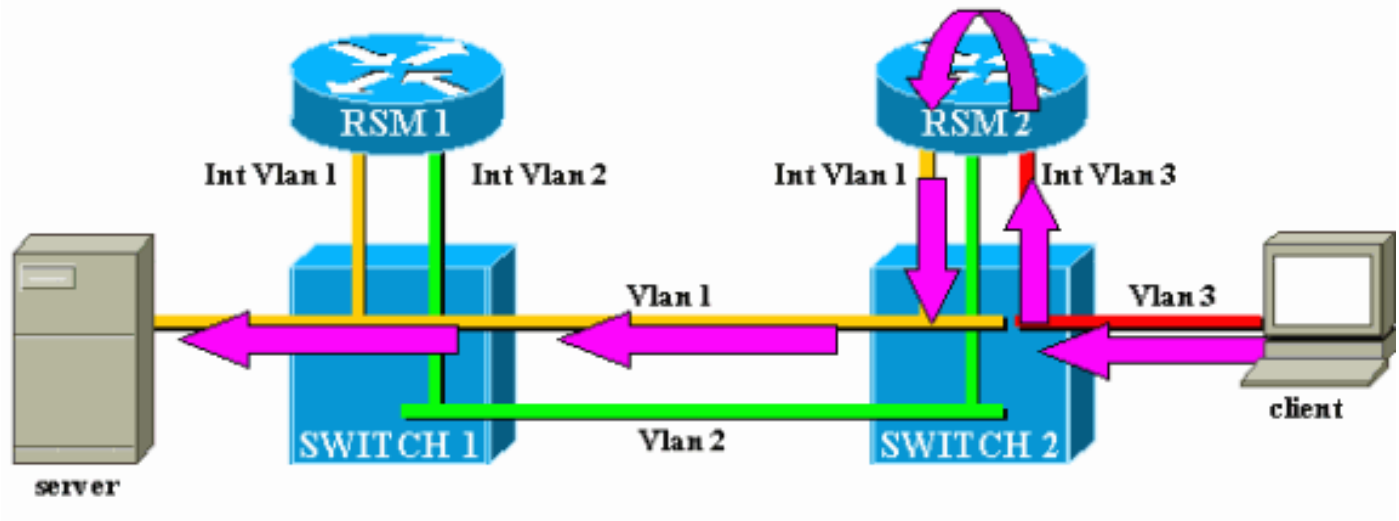
Lo scopo principale della VLAN0 è quello di garantire una comunicazione efficace con il Supervisor Engine dello switch. Poiché si tratta di un'interfaccia nascosta, non è possibile utilizzare un semplice comando **show interface vlan0** per visualizzare le statistiche relative.

Problemi comuni di routing tra VLAN

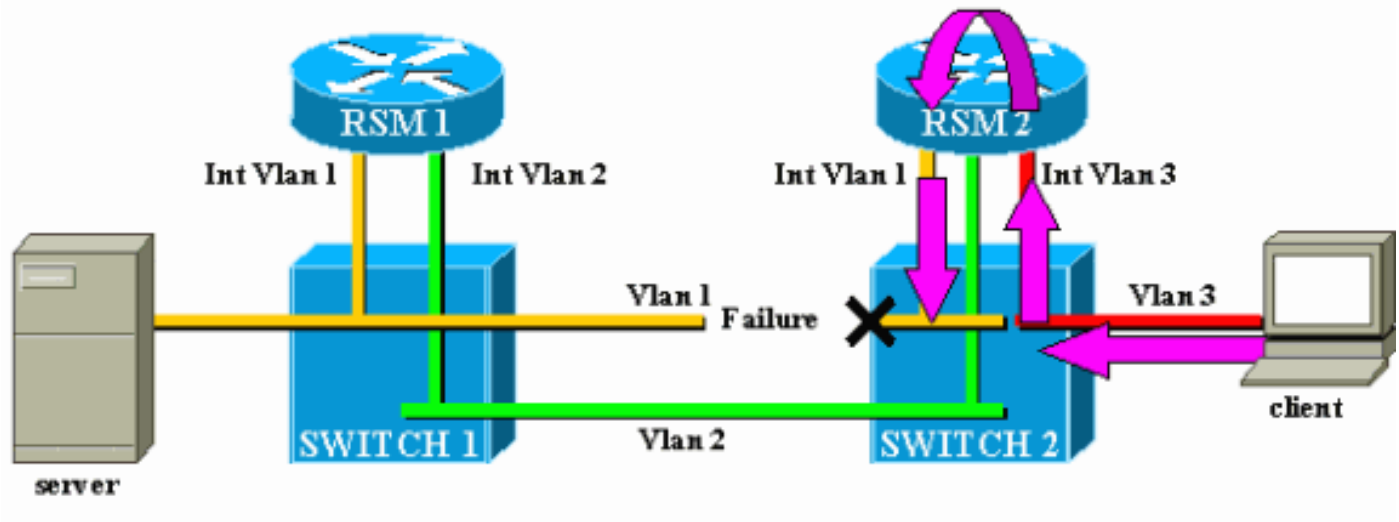
Utilizzo della funzione di autogestione del modulo RSM

Un problema frequente del bridging è che un collegamento interrotto può facilmente suddividere una rete L2 in due parti. Questa situazione deve essere evitata ad ogni prezzo, poiché una rete non contigua interrompe il routing. (ciò si ottiene generalmente installando collegamenti ridondanti).

Si consideri questo esempio, in cui un client collegato allo switch 2 comunica con un server connesso allo switch 1:



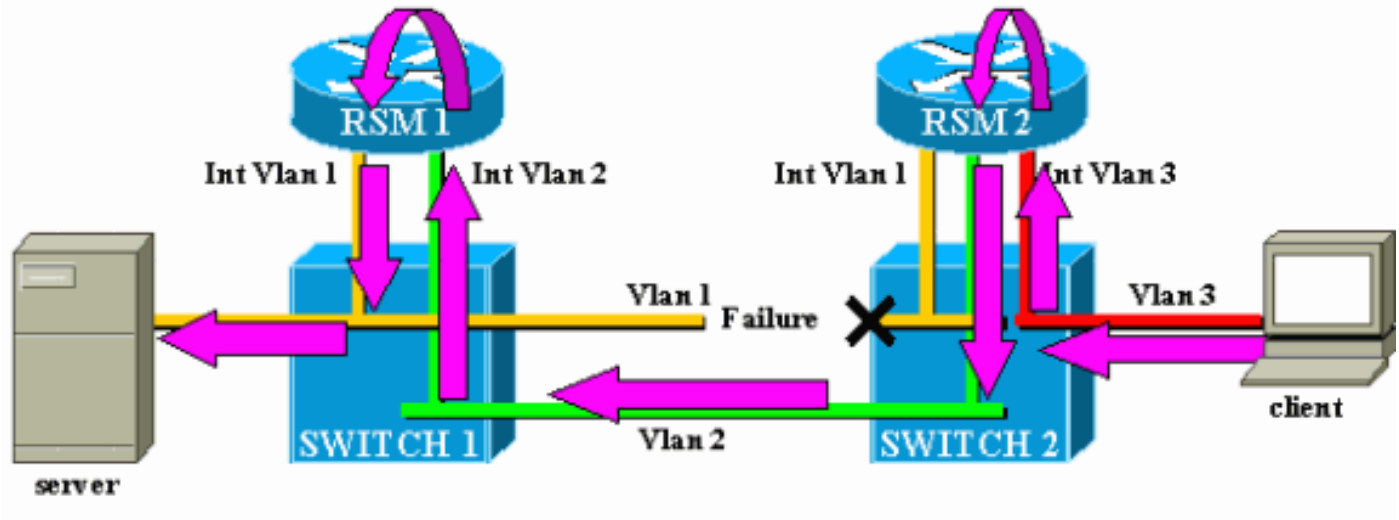
Considerare solo il traffico dal client al server. Il traffico in entrata dal client nella VLAN3 viene instradato dall'RSM2, che ha una connessione diretta alla subnet del server tramite l'interfaccia VLAN2. Le frecce viola rappresentano il percorso seguito:



Si supponga che il collegamento tra lo switch 1 e lo switch 2 si interrompa per la VLAN1. Il problema principale è che, dal punto di vista dell'RSM2, nella rete non vi sono modifiche. L'RSM2 ha ancora un'interfaccia collegata direttamente alla VLAN1 e continua a inoltrare il traffico dal client al server tramite questo percorso. Nello switch 2 il traffico viene perso e la connettività tra il client e il server viene interrotta.

Per risolvere questo problema, è stata progettata la funzionalità di automazione RSM. Se non vi sono porte attive per una VLAN specifica su uno switch, l'interfaccia VLAN corrispondente dell'RSM viene disabilitata.

Nel caso dell'esempio, quando il collegamento nella VLAN tra lo switch 1 e lo switch 2 ha esito negativo, l'unica porta nella VLAN1 sullo switch 2 sta diventando inattiva (collegamento non attivo). La funzione di autostazione dell'RSM disabilita l'interfaccia VLAN1 sull'RSM2. Ora che l'interfaccia VLAN1 è inattiva, l'RSM2 può utilizzare un protocollo di routing per trovare un altro percorso per i pacchetti destinati al server e inoltrare il traffico tramite un'altra interfaccia, come mostrato nel diagramma:



La funzionalità di autostazione del modulo RSM è disponibile solo se la VLAN non è dotata di altre porte attive. Ad esempio, se si dispone di un altro client nella VLAN1 collegato allo switch 2 o di un modulo RSM nello chassis con un'interfaccia VLAN1 definita, l'interfaccia VLAN1 non verrà disabilitata se il collegamento tra lo switch 1 e lo switch 2 ha esito negativo. Il traffico verrebbe quindi nuovamente interrotto.

Per impostazione predefinita, la funzione di autostazione del modulo RSM è attivata. Se

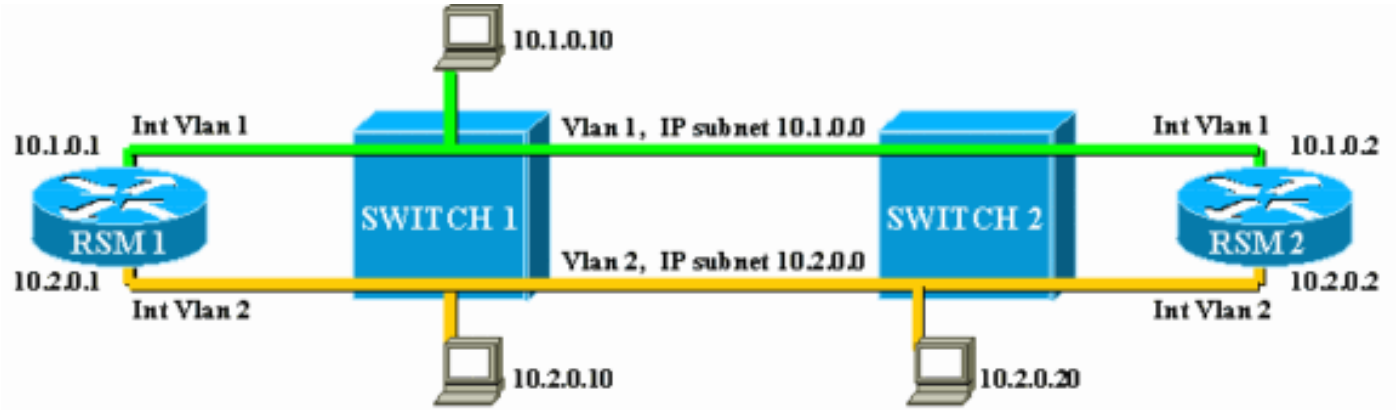
necessario, è possibile disabilitarlo manualmente con il comando set rsmautostate sul Supervisor Engine:

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

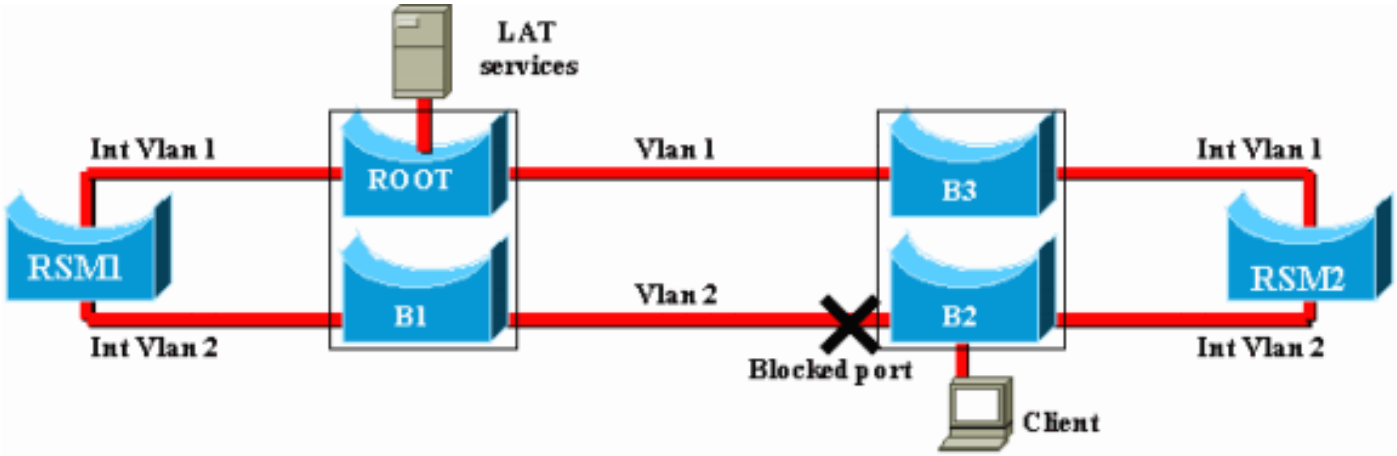
Bridging Fall-Back

Il bridging di fallback è costituito da protocolli di bridging tra VLAN e dal routing di alcune altre VLAN. Se possibile, evitare questo tipo di configurazione e utilizzarla solo durante un periodo di migrazione transitorio. In genere, questa condizione è necessaria quando la rete è stata segmentata con subnet IP diverse, ognuna su una VLAN diversa, ma si desidera continuare a creare il bridging di alcuni protocolli non instradabili meno recenti (ad esempio, Local Area Transport [LAT]). In questo caso, si desidera utilizzare il modulo RSM come router per l'IP e come bridge per altri protocolli. A tale scopo, è sufficiente configurare il bridging sulle interfacce del modulo RSM mantenendo gli indirizzi IP. Nell'esempio seguente viene illustrata una rete molto semplice che utilizza il bridging di fallback e viene illustrato il problema più comune che può verificarsi con questo tipo di configurazione.

Questa rete molto semplice è costituita da due VLAN, corrispondenti a due subnet IP diverse. Gli host di una determinata VLAN possono usare uno qualsiasi dei due RSM come gateway predefinito (o anche entrambi, utilizzando il protocollo HSRP (Hot Standby Router Protocol)), e quindi possono comunicare con gli host dell'altra VLAN. La rete avrà il seguente aspetto:

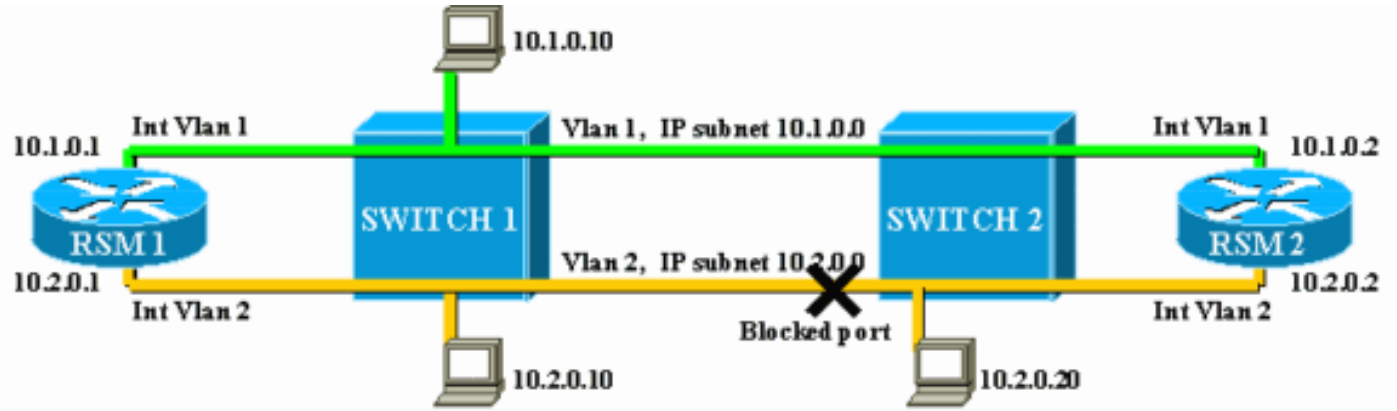


Entrambi i moduli RSM sono configurati anche per collegare altri protocolli tra le rispettive interfacce, VLAN1 e VLAN2. Si supponga di avere un host che offre servizi LAT e un client che li utilizza. La rete avrà il seguente aspetto:



Per questo diagramma, ciascun Catalyst è suddiviso in due bridge diversi (uno per ciascuna VLAN). Si noti che il bridging tra le due VLAN ha determinato la fusione delle due VLAN. Per quanto riguarda i protocolli con bridging, si dispone di una sola VLAN e il server e il client LAT possono comunicare direttamente. Naturalmente, ciò implica anche che si ha un loop nella rete e che STP deve bloccare una porta.

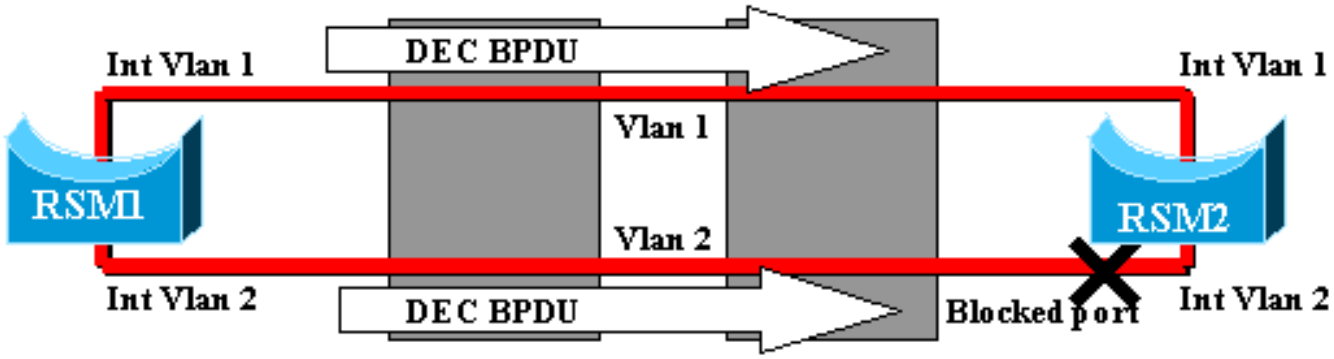
Come potete vedere, da questa porta bloccante sorgerà un problema. Uno switch è un dispositivo L2 puro e non è in grado di distinguere tra traffico IP e traffico LAT. Pertanto, se lo switch 2 blocca una porta, come nel diagramma precedente, vengono bloccati tutti i tipi di traffico (IP, LAT o altro). Per questo motivo, la rete avrà il seguente aspetto:



La VLAN2 è divisa in due parti e la subnet 10.2.0.0 non è contigua. Con questa configurazione, l'host 10.2.0.10 non può comunicare con l'host 10.2.0.20, anche se si trovano sulla stessa subnet e VLAN.

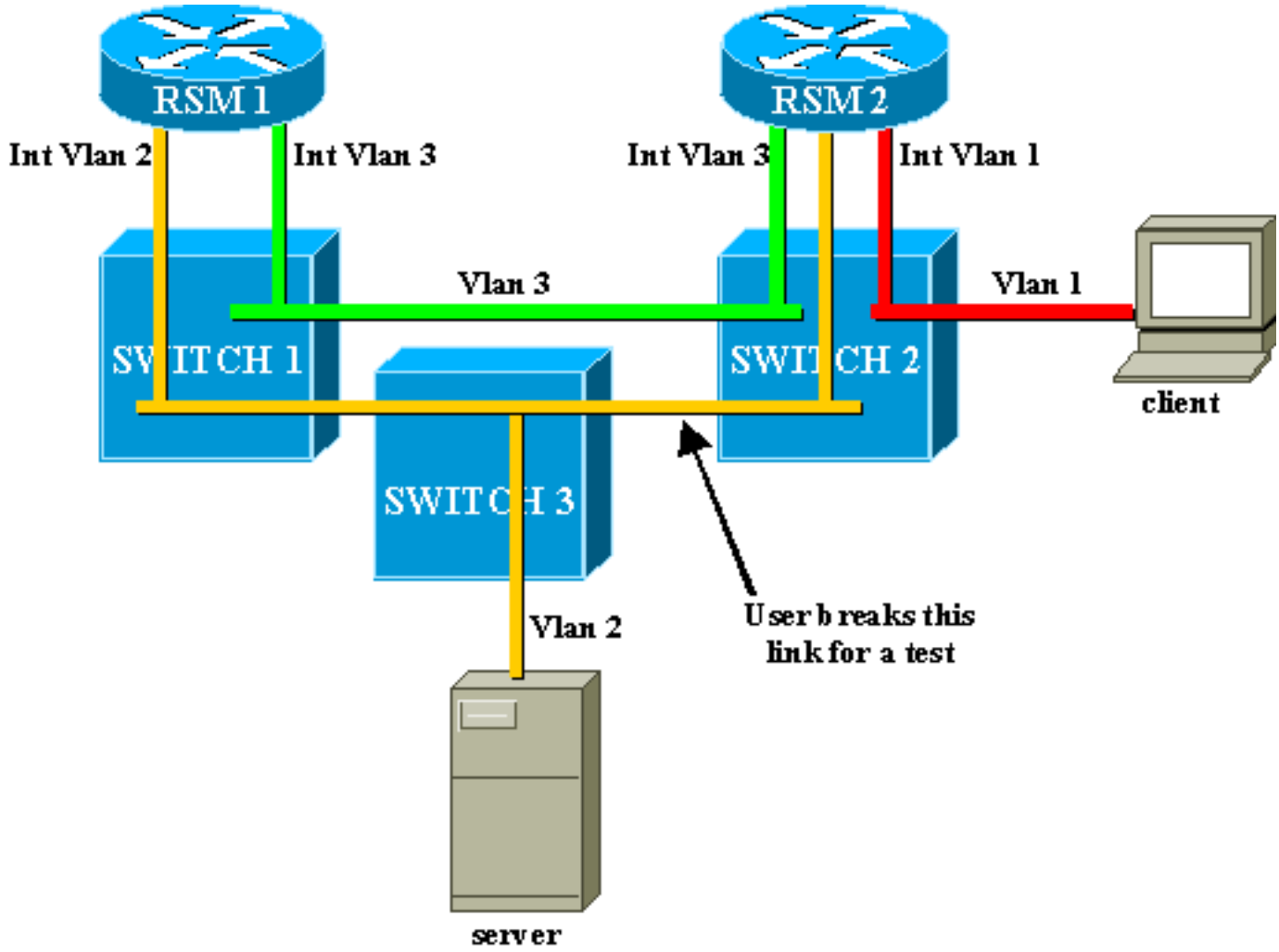
La soluzione è spostare la porta bloccata sull'unico dispositivo in grado di distinguere il traffico L2 e L3. Il dispositivo è l'RSM. Esistono due modi principali per raggiungere questo obiettivo:

- **Regolazione dei parametri STP** È necessario aumentare il costo di uno o più dispositivi in modo che, alla fine, la porta di blocco si trovi su RSM1 o RSM2. Questo metodo non è molto flessibile e implica una configurazione STP molto rigida. L'aggiunta di uno switch o la modifica della larghezza di banda di un collegamento (Fast EtherChannel o Gigabit Ethernet) può causare una rielaborazione completa della sintonizzazione.
- **Utilizzando un algoritmo STA (Spanning Tree Algorithm) diverso sull'RSM:** Gli switch eseguono solo IEEE STA e sono completamente trasparenti per il DEC STP. Se si configura DEC STP su entrambi gli RSM, questi funzionano come se fossero collegati direttamente tra loro e uno di essi si bloccherà. Il diagramma mostra quanto
  segue:



Foro nero temporaneo (convergenza ST)

I clienti che testano la velocità di riconfigurazione della rete in caso di guasto spesso gestiscono problemi di configurazione relativi a STP. Si consideri la rete seguente, in cui un client accede a un server tramite due percorsi diversi. Per impostazione predefinita, il traffico tra il client e il server viene instradato tramite l'interfaccia VLAN2 da RSM2:



Per eseguire un test, un utente interrompe il collegamento tra lo switch 2 e lo switch 3. Immediatamente, la porta corrispondente si interrompe e la funzione di autostazione RSM disattiva l'interfaccia VLAN2 su RSM2. Il percorso direttamente connesso al server scompare dalla tabella di routing di RSM2, che impara rapidamente un nuovo percorso tramite RSM1. Con protocolli di routing efficienti, quali Open Shortest Path First (OSPF) o Enhanced Interior Gateway Routing Protocol (EIGRP), la convergenza è così rapida che durante questa operazione non si perde quasi mai il ping.

In caso di guasto, lo switch tra i due percorsi (VLAN2 gialla e VLAN3 verde) è stato immediato. Tuttavia, se l'utente ristabilisce il collegamento tra lo switch 2 e lo switch 3, il client subisce una perdita di connettività al server per circa 30 secondi.

Il motivo è legato anche al STA. Quando si esegue STA, una porta appena connessa passa attraverso le fasi di ascolto e apprendimento prima di finire in modalità di inoltro. Durante le prime due fasi, la porta è attiva ma non trasmette il traffico. Ciò significa che, non appena il collegamento è connesso, la funzione di autostazione dell'RSM riattiva immediatamente l'interfaccia VLAN2 sull'RSM2, ma il traffico non può passare finché le porte sul collegamento tra lo switch 2 e lo switch 3 non raggiungono la fase di inoltro. Questo spiega la perdita di connettività temporanea tra il client e il server. Se il collegamento tra lo switch 1 e lo switch 2 non è un trunk, è possibile abilitare la funzionalità PortFast per saltare le fasi di ascolto e apprendimento e convergere immediatamente.

Nota: PortFast non funziona sulle porte trunk. Per ulteriori informazioni, fare riferimento a Utilizzo di PortFast e di altri comandi per correggere i ritardi della connettività di avvio della workstation.

Conclusioni

Questo documento si concentra su alcuni problemi specifici dei moduli RSM e alcuni problemi molto comuni di routing tra VLAN. Queste informazioni sono utili solo quando sono state tentate tutte le normali procedure di risoluzione dei problemi dei router Cisco IOS. Se metà dei pacchetti instradati da un modulo RSM vengono persi a causa di una tabella di routing errata, non è possibile interpretare le statistiche del canale DMA. Anche i problemi generali di routing tra VLAN sono argomenti avanzati e non si verificano molto spesso. Nella maggior parte dei casi, considerare il proprio RSM (o qualsiasi altro dispositivo di routing integrato all'interno di uno switch) come un semplice router Cisco IOS esterno è sufficiente per risolvere i problemi di routing in un ambiente commutato.

Informazioni correlate

- Pagina di supporto per i protocolli di routing IP
- Risoluzione dei problemi di switching multilayer IP
- Configurazione del routing tra VLAN
- Utilizzo di PortFast e di altri comandi per correggere i ritardi di connettività all'avvio della postazione di lavoro
- Pagine di supporto dei prodotti LAN
- Pagina di supporto dello switching LAN
- Documentazione e supporto tecnico – Cisco Systems