Nozioni base sullo switching Token Ring

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Convenzioni](#)
[TrBRF e TrCRF](#)
[Modalità di switching](#)
[Bridging trasparente](#)
[Switching Origine-Route](#)
[Bridging origine-route e trasparente origine-route](#)
[Collegamento tra switch](#)
[Spanning-Tree](#)
[Protocollo VLAN Trunking](#)
[Eliminazione VTP](#)
[Protocollo ad anello duplicato](#)
[VLAN HSRP e Token Ring](#)
[Informazioni correlate](#)

Introduzione

Per iniziare a comprendere i concetti della commutazione Token Ring, è molto importante comprendere il bridging trasparente, il bridging origine-route e lo Spanning-Tree. Catalyst 3900 e Catalyst 5000 utilizzano nuovi concetti, come descritto nell'allegato K dello standard IEEE 802.5. Questi concetti sono alla base delle VLAN Token Ring. Questo documento spiega i diversi concetti di bridging e il loro funzionamento:

- Trunking ISL (Inter-Switch Link)
- Spanning-Tree
- Protocollo VLAN Trunking Protocol (VTP)
- Protocollo DRiP (Duplicate Ring Protocol)

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

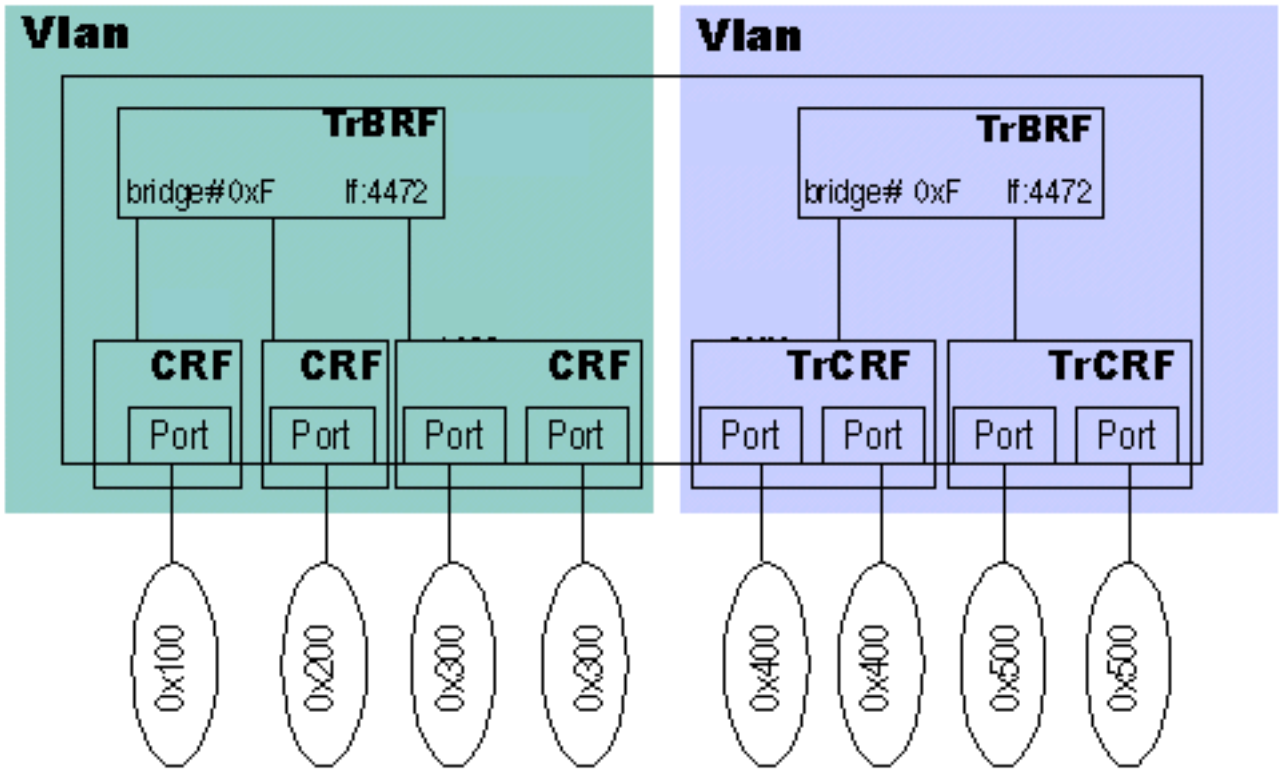
Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

TrBRF e TrCRF

La funzione TrBRF (Token Ring Bridge Relay Function) e la funzione TrCRF (Token Ring Concentrator Relay Function) sono i componenti fondamentali dell'architettura di Catalyst 3900 e della funzionalità Catalyst 5000. TrBRF è semplicemente la funzione bridge dello switch, mentre TrCRF è la funzione di concentrazione dello switch. È importante comprendere che il bridging si verifica a entrambi i livelli perché, in Token Ring, verranno discussi tre diversi tipi di bridging.

La funzionalità TrBRF dello switch controlla la commutazione del traffico ponte origine-route, come il bridging origine-route (SRB) e il bridging trasparente origine-route (SRT). La tecnologia TrCRF copre le funzionalità di switching origine-route (SRS) e bridging trasparente (TB). Ad esempio, è possibile avere uno switch Catalyst 3900 con un solo TrBRF e un solo TrCRF e tutte le porte dello switch si trovano nello stesso TrCRF. In questo modo, lo switch può eseguire solo SRS e TB. Se sono stati definiti dieci TrCRF diversi nello stesso TrBRF padre, il traffico proveniente dalle porte connesse allo stesso TrCRF verrà inoltrato tramite la funzionalità TrCRF di SRS o TB. Il traffico diretto agli altri TrCRF nello switch utilizzerebbe la funzionalità TrBRF dello switch e sarebbe un traffico di bridging tra origine e route o un traffico di bridging trasparente tra origine e route. I diversi meccanismi di commutazione saranno illustrati più avanti in questo documento.

Il diagramma mette in relazione il TrBRF e il TrCRF con il mondo fisico:



Èpossibile notare che ogni TrCRF è collegato a un anello specifico. Un TrCRF può compromettere più porte e queste porte comprometterebbero lo stesso numero di anello. Il TrBRF collega i TrCRF.

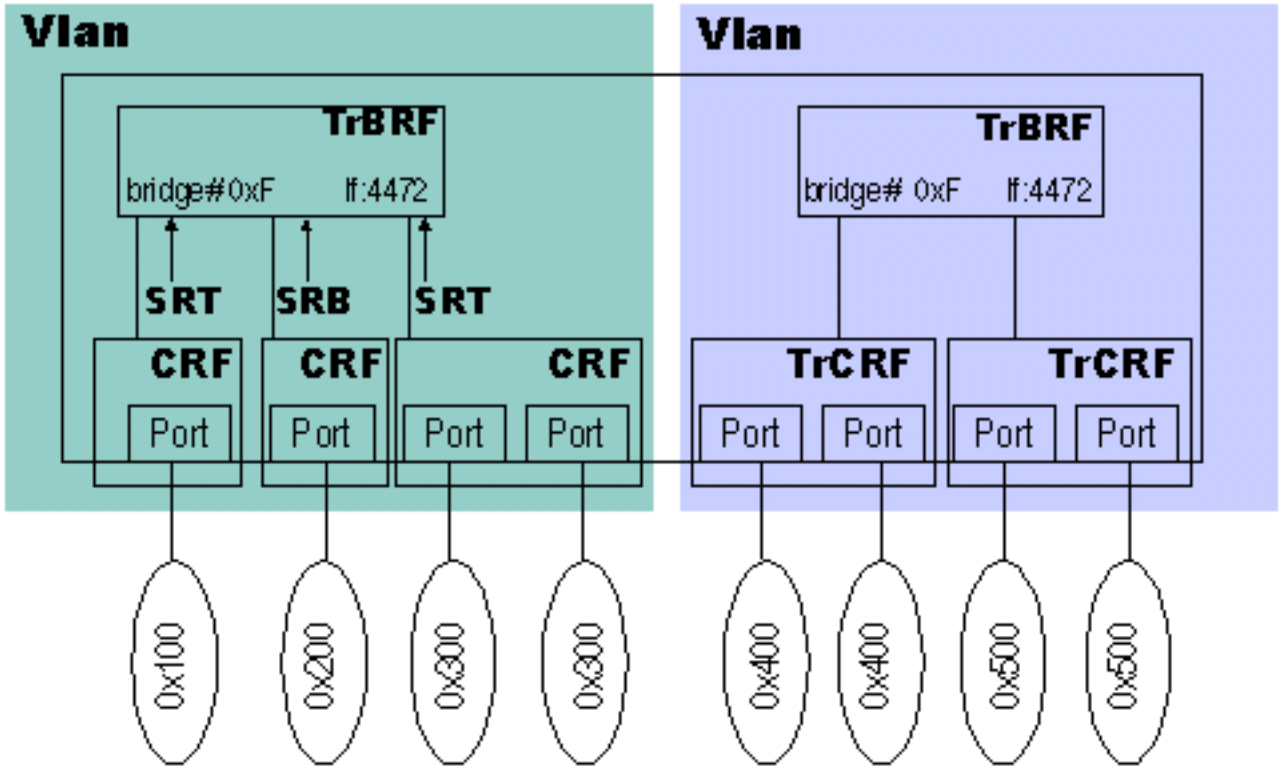
Una TrCRF e una TrBRF sono di per sé una VLAN diversa. Quindi, nel Token Ring, è possibile creare un bridge tra VLAN. Il bridging tra VLAN Token Ring segue due regole:

- Il bridging tra due VLAN TrBRF può essere eseguito solo da un dispositivo esterno, ad esempio un router o un Route Switch Module (RSM).
- Il bridging tra VLAN TrCRF può essere eseguito solo con VLAN TrCRF figli della stessa VLAN TrBRF padre.

Questa operazione è molto importante da tenere a mente per le VLAN Token Ring, perché rompe il paradigma Ethernet. Per riepilogare, una VLAN Ethernet è data dalla somma di un TrBRF e dei relativi TrCRF figlio. Poiché è possibile effettuare il bridging tra determinate VLAN in Token Ring, è necessario comprendere come si verifica questo bridging.

Nota: per semplificare la comprensione delle VLAN Token Ring in relazione alle VLAN Ethernet, tenere presente che la combinazione di TrCRF e TrBRF rende la VLAN in sé.

In questo diagramma è illustrato come la funzione TrCRF determini la modalità di bridging tra la funzione TrCRF e la TrBRF.



I singoli TrCRF hanno configurato il tipo di bridging che eseguiranno nei TrBRF. Questa operazione è importante perché si possono avere VLAN TrCRF che eseguiranno il bridging tra l'origine e la route verso altri TrCRF, ma non sui frame non indirizzati all'origine. Nel diagramma precedente, un TrCRF è configurato per la modalità SRB e due per la modalità SRT. Ciò significa che il traffico SRB può passare tra tutti e tre i TrCRF, ma che il traffico SRT può passare solo tra i due in modalità SRT. In questo modo è possibile impostare in modo granulare il flusso del traffico tra i TrCRF. Se la modalità bridging è stata impostata sul TrBRF, influirebbe su tutti i figli TrCRF della VLAN.

Modalità di switching

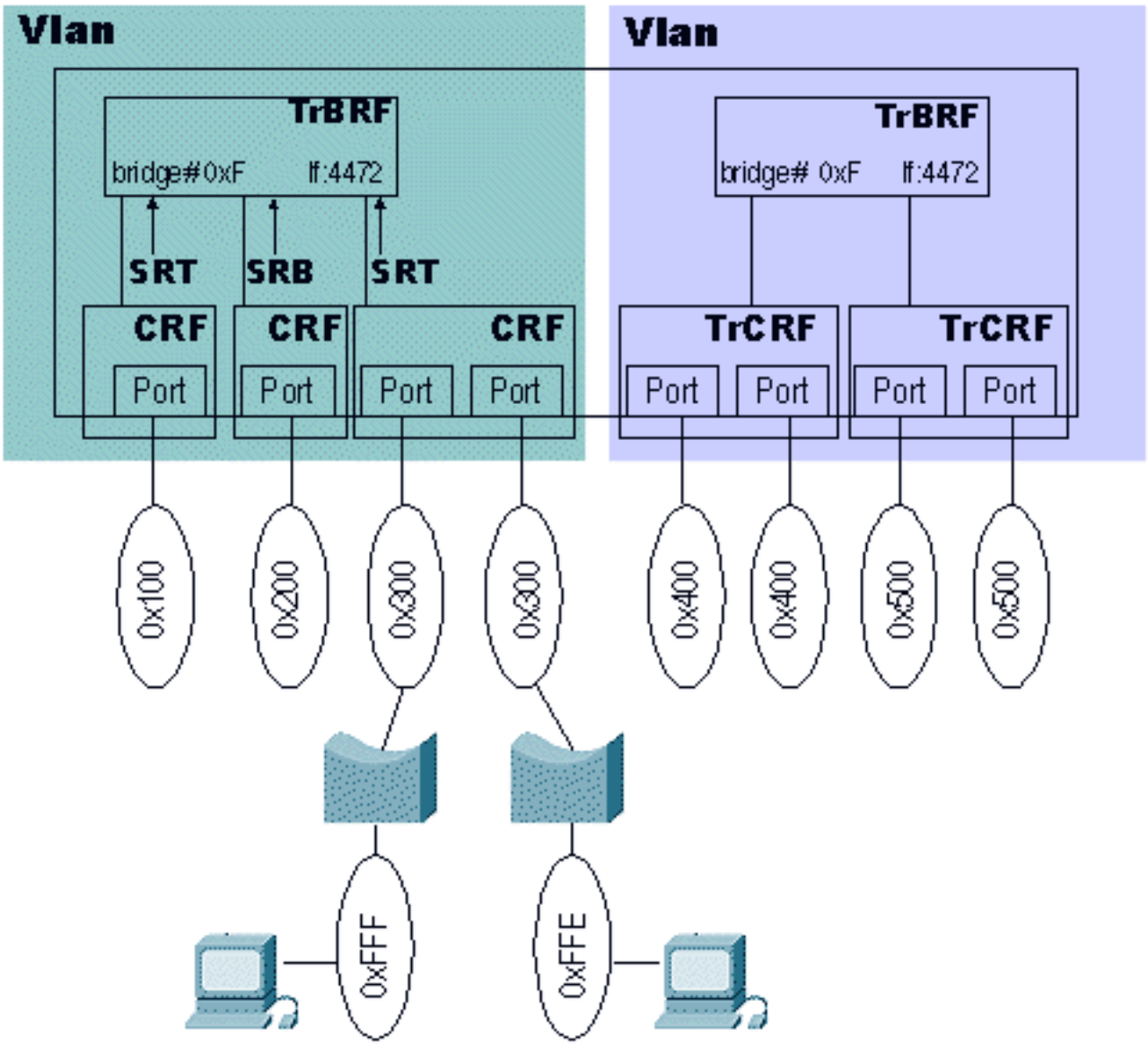
Configurazione predefinita, Catalyst 3900 include un TrBRF e un TrCRF. A tutte le porte viene assegnata la VLAN 1003 TrCRF predefinita. Lo stesso vale per il blade Catalyst 5000 Token Ring. Questa operazione è importante in quanto fornisce alla confezione un certo tipo di plug-and-play??? funzionalità. Questi switch possono eseguire l'inoltro in base alla commutazione origine-percorso e al bridging trasparente. Nelle sezioni seguenti vengono fornite informazioni dettagliate su queste tecnologie.

Bridging trasparente

Il Bridging trasparente è il più semplice di tutti i meccanismi di switching ed è basato sull'indirizzo MAC di destinazione dei frame nella rete. Questo è il meccanismo di inoltro delle reti Ethernet. Ogni volta che uno switch riceve un frame, registra l'indirizzo MAC di origine (SMAC) del frame come uno che appartiene a quella porta e, da quel momento in poi, inoltra il traffico destinato a quel MAC a quella porta. Se, durante la procedura di apprendimento, uno switch non è a conoscenza di un indirizzo MAC, il pacchetto verrà inoltrato a tutte le porte in stato di inoltro.

Switching Origine-Route

La commutazione origine-route è un meccanismo di inoltro necessario quando alle porte è assegnato un solo TrCRF e lo switch riceve pacchetti con campi di informazioni di routing (RIF, Routing Information Fields). Poiché lo switch non modifica il RIF del frame (in quanto non lo passa al TrBRF), la rete deve essere in grado di prendere decisioni sull'inoltro, con il RIF, senza modifiche. Considerare questo diagramma di rete che mostra SRS:



Il traffico che va dall'anello 0xFFF all'anello 0xFFE deve passare attraverso lo switch. Questo traffico sarebbe traffico ponte origine-route. Questa è la sequenza di avvio della comunicazione tra i due client:

1. Una stazione invia un pacchetto explorer all'anello in cui risiede. Si supponga che il client sul ring 0xFFF invii il pacchetto; ha il seguente aspetto (esadecimale):
   `0000 00c1 2345 8000 0c11 1111 C270`
   Nota: le informazioni sul pacchetto mostrano solo le informazioni DMAC, SMAC e RIF.
2. Quando il pacchetto raggiunge il bridge di origine e inoltra il frame al cavo, il pacchetto ha il seguente aspetto:
   `0000 00C1 2345 8000 0c11 1111 C670 FFF1 3000`
   `C670` è il campo di controllo di routing e `FFF1 3000` è anello 0xFFF, ponte 0x1, anello 0x300.
3. Ora il pacchetto colpisce lo switch. Poiché lo switch vede il pacchetto proveniente da un anello lontano, impara il descrittore del percorso. In questo caso, lo switch ora sa che il ring 0xFFF tramite il bridge 0x1 si trova sulla porta 3.
4. Poiché il pacchetto è un pacchetto del navigatore, lo switch inoltra il frame a tutte le porte nello stesso TrCRF. Se l'elenco delle cartelle deve passare a porte in TrCRF diverse, il frame verrà consegnato al TrBRF, che fornirà la funzionalità bridge. Se ci sono porte nello stesso TrCRF, inoltrerà il frame in uscita senza modifiche.
5. La stazione nel ring 0xFFE dovrebbe ottenere l'explorer e rispondere ad esso. Si supponga

che il client risponda con un frame diretto. Il frame indirizzato ha il seguente aspetto:
`0000 0C11 1111 8000 00C1 2345 08E0 FFF1 3001 FFE0`
`08E0` è il campo di controllo routing e `FFF1 3001 FFE0` è anello 0xFFF, ponte 0x1, anello 0x300, ponte 0x1, anello 0xFFE.

6. Infine, lo switch scopre che il ring 0xFFE si trova sulla porta 4 e conserva il descrittore della route.

D'ora in poi, lo switch sa di questi anelli. Se si osservano le tabelle, si dovrebbe notare che lo switch ha appreso il numero del ponte e il numero ad anello. Qualsiasi altro anello dopo l'anello 0xFFF e l'anello 0xFFE non sono necessari, perché devono passare attraverso l'anello 0xFFF o l'anello 0xFFE per raggiungere lo switch.

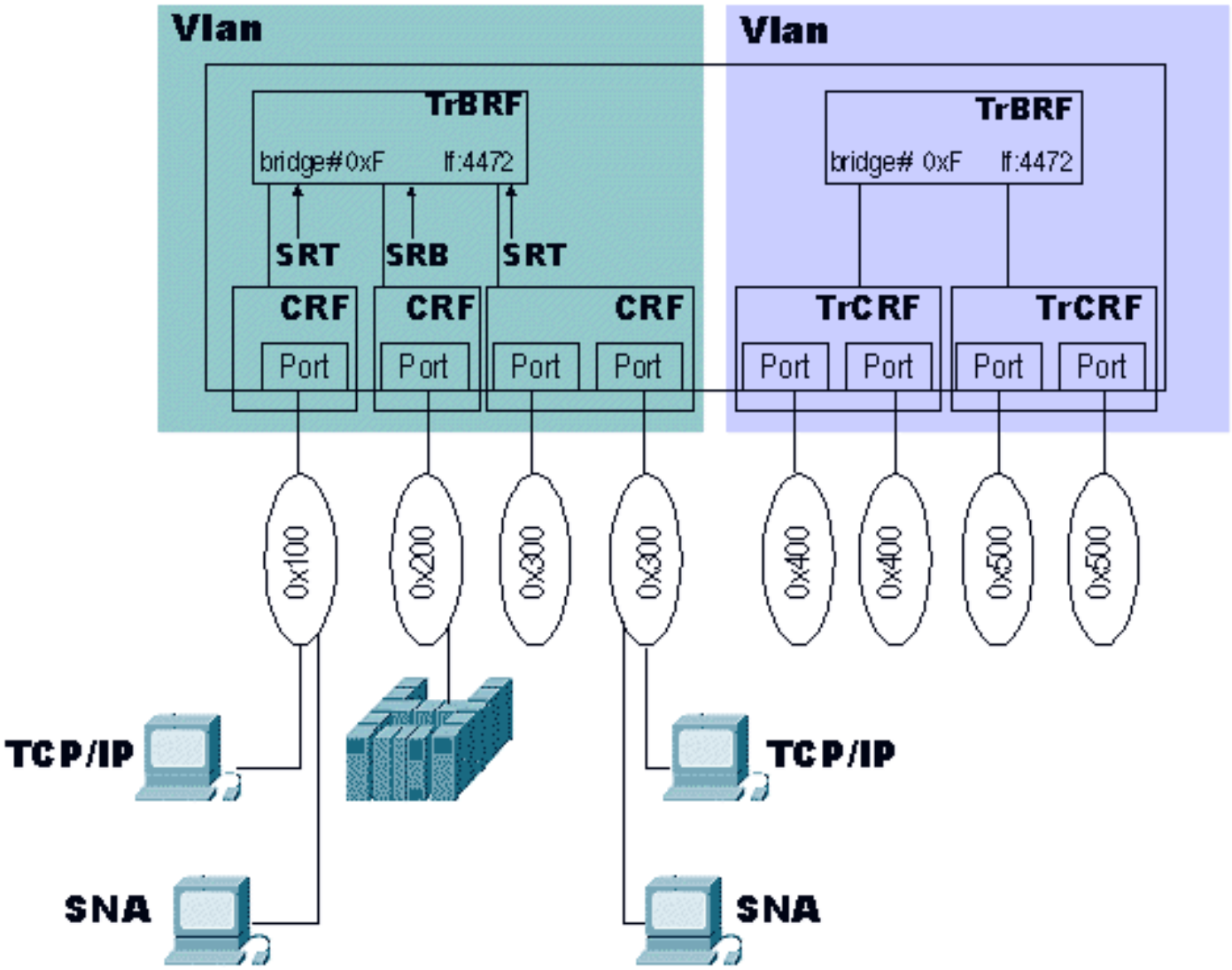
SRS è un inoltro di base di pacchetti basati su RIF senza funzionalità SRB, come nel caso di TrCRF.

Nota: per visualizzare la tabella delle informazioni di routing in Catalyst 5000, usare il comando **show rif**.

Bridging origine-route e trasparente origine-route

Tutte le funzionalità di bridging source-route si trovano nella logica TrBRF. La funzione TrCRF comanda la modalità di bridging della funzione TrBRF. Quindi, se la TrCRF è configurata per la modalità SRB su TrBRF, quando la TrCRF riceve un frame NSR (non source-routing), lo switch non la inoltra alla logica TrBRF.

Questa opzione può essere utilizzata se non si desidera che determinati tipi di traffico colpiscano o lascino un determinato anello. Il diagramma mostra un esempio:



Se i client TCP/IP non sono in grado di inviare pacchetti con RIF, lo switch non inserirà tali frame nello stesso anello del mainframe (0x200). Tuttavia, i frame SNA all'host (che solitamente hanno un RIF) raggiungerebbero il mainframe. Questo è un modo molto rudimentale di filtrare i frame in una rete a commutazione.

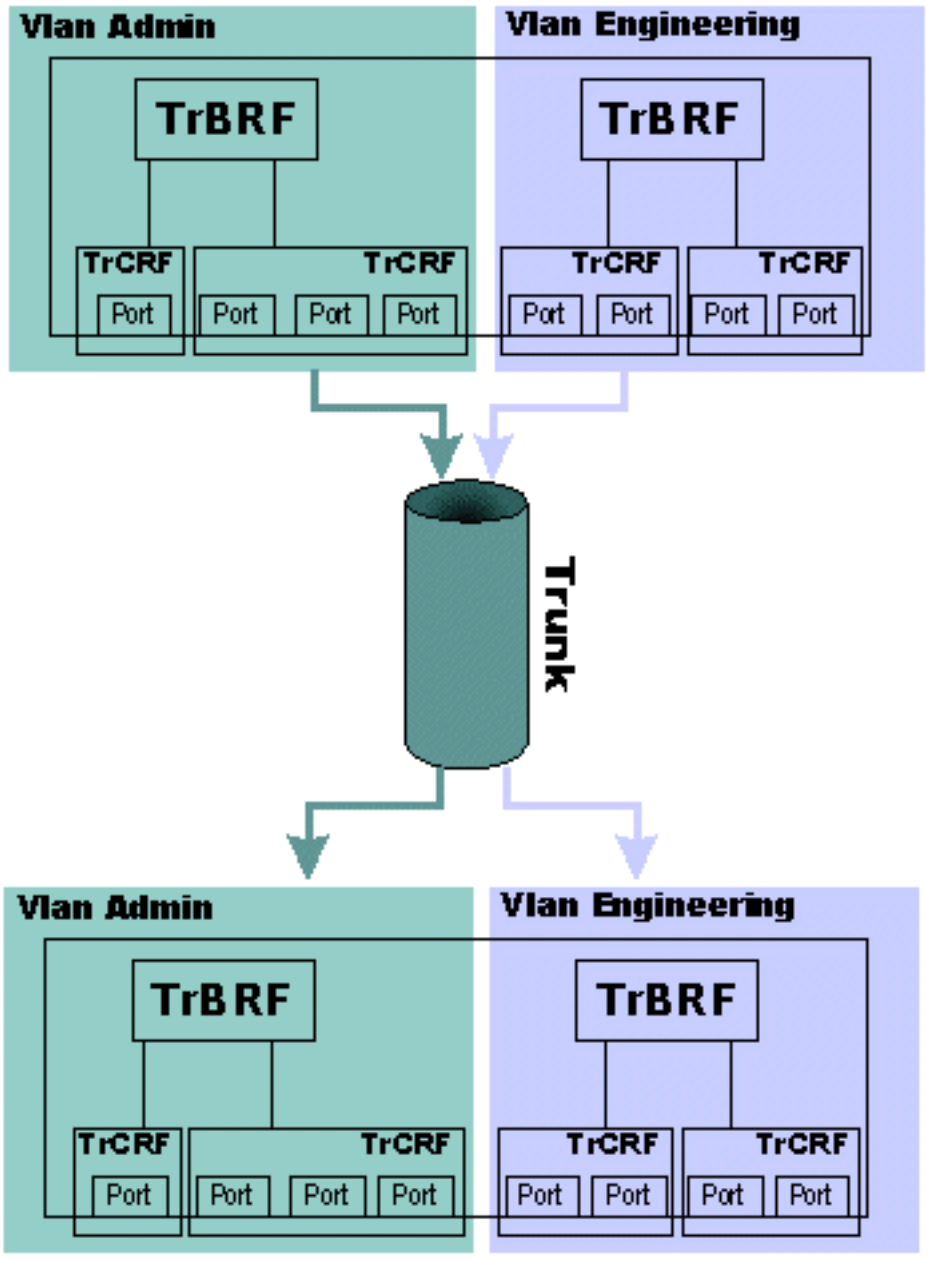
Questa è la sequenza che lo switch segue per inoltrare un frame con bridging source-route attraverso il TrBRF:

1. La stazione SNA sul ring 0x300 (porta 4) invia un esploratore per raggiungere il mainframe.
2. Quando il pacchetto explorer colpisce lo switch, inoltra l'explorer, senza modifiche, nello stesso TrCRF; quindi ne invia una copia al TrBRF per inoltrarla al resto dei TrCRF. In questo caso, poiché il pacchetto ha un RIF, passa attraverso il percorso SRB. Lo switch deve anche conoscere il percorso.
3. Lo switch conoscerà lo SMAC del frame, perché il pacchetto indica come proveniente dall'anello locale a cui è connesso lo switch. Infatti, in una combinazione di TrCRF a più porte, il RIF mostra l'anello di destinazione, ma lo switch deve sapere quale porta del TrCRF. Pertanto, lo switch apprende lo SMAC dei frame che entrano a livello TrCRF.
4. Il pacchetto viene inviato a tutti gli altri TrCRF, modificati con le rispettive combinazioni di numeri bridge ring.
5. Una volta che l'host risponde con il frame SRB, lo switch apprende lo SMAC dell'host per quel TrCRF e lo invia alla porta in uscita. Il traffico tra le due reti scorre poi avanti e indietro.

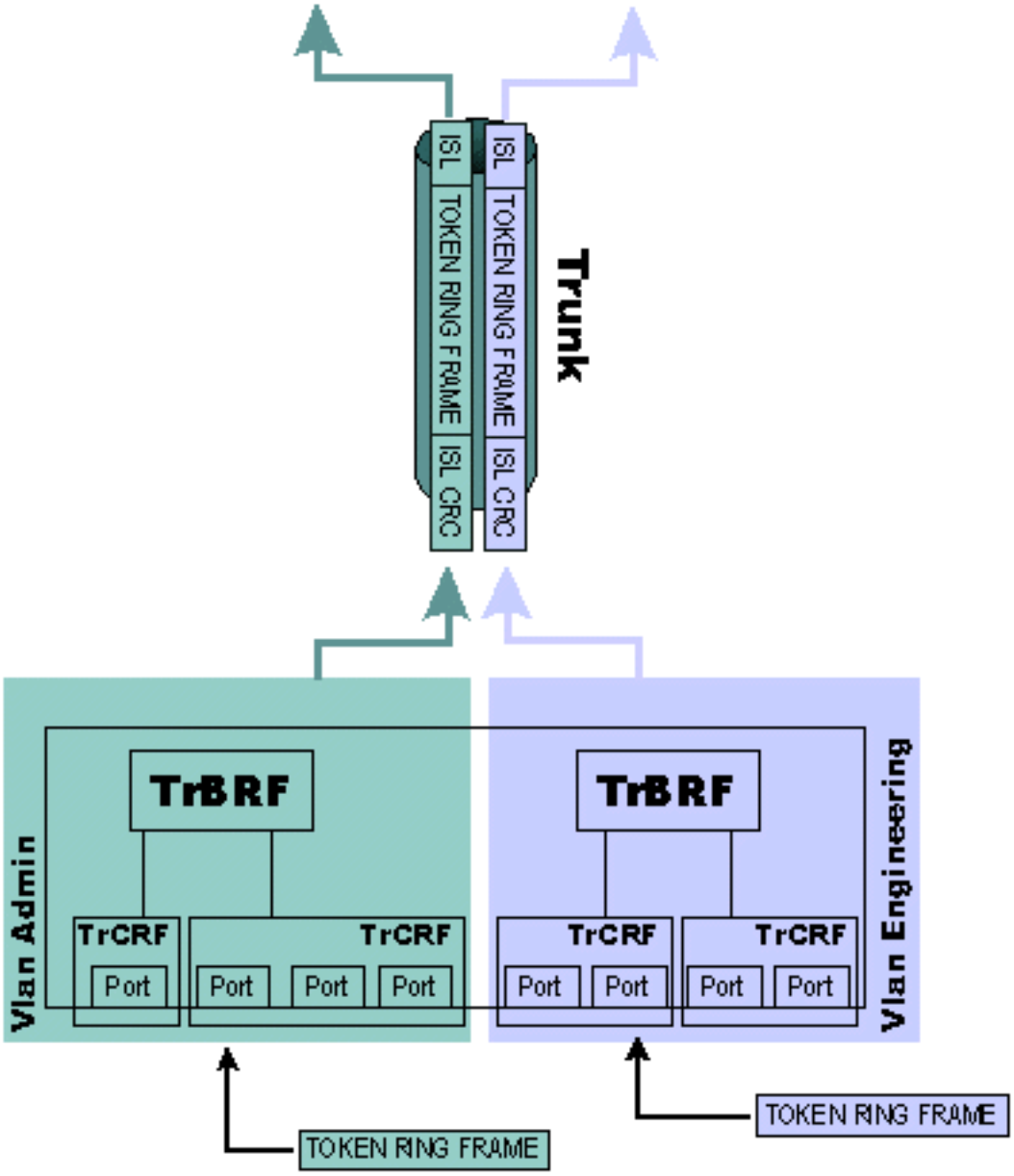
Nota: per controllare la tabella degli indirizzi MAC su Catalyst 5000, usare il comando **show cam**.

Collegamento tra switch

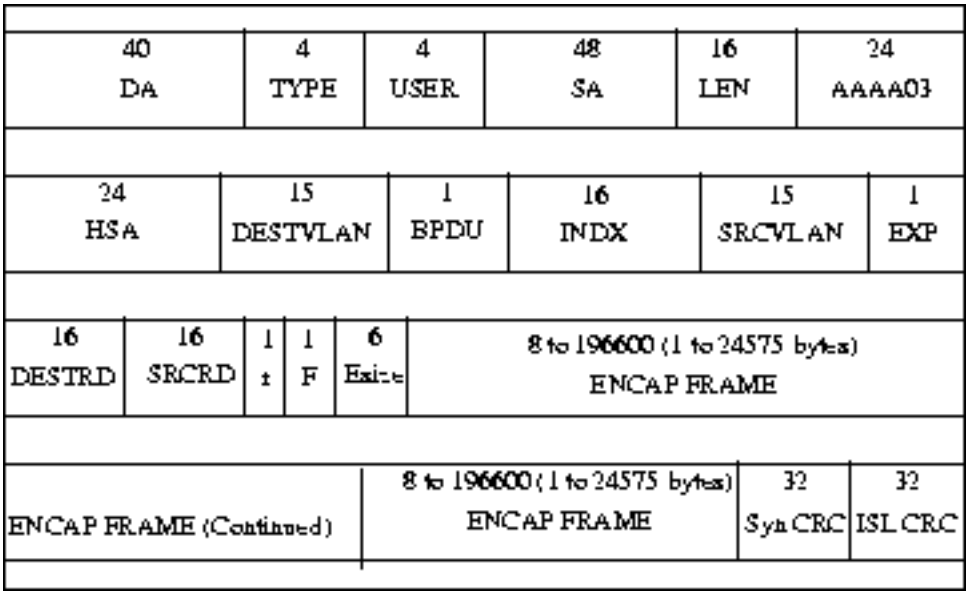
Inter-Switch Link è un protocollo molto semplice. Fondamentalmente, i frame che passano attraverso un trunk ISL sono incapsulati in un frame ISL che indica all'altro lato a cui appartengono i frame VLAN. Per questo motivo, le informazioni sulla VLAN devono essere condivise manualmente o automaticamente tra gli switch. Questo processo può essere gestito con un protocollo noto come VLAN Trunking Protocol (VTP). Per le VLAN Token Ring, è necessario eseguire il VTP V2 nella rete. Prendiamo in considerazione il seguente diagramma:



In questo caso, è stato creato un singolo trunk ISL per trasportare le VLAN di progettazione e le VLAN di amministrazione. Dopo aver attraversato il trunk, il traffico in una delle due VLAN non viene misto. Il diagramma mostra il modo in cui viene realizzata la separazione:



Ogni frame delle VLAN che deve attraversare il trunk è incapsulato in un frame ISL e la relativa VLAN è inclusa nel frame. Ciò consente allo switch ricevente di indirizzare correttamente il frame alla relativa VLAN specifica. Il frame ISL Token Ring (TRISL) ha alcuni campi in più rispetto a un frame ISL normale. Il diagramma mostra il layout di un frame TRISL:



Nota: anche se il protocollo TRISL viene eseguito su interfacce Fast Ethernet, i pacchetti contengono un frame Token Ring standard e le informazioni VLAN associate a tale frame, in una certa misura. Le VLAN Token Ring permettono di usare frame di dimensioni fino a 18k, come gli ISL. Ciò *non* è possibile attraverso la frammentazione del frame. L'intero frame è incapsulato in un frame ISL in un intero frammento e inviato attraverso il collegamento. L'idea errata è che ISL sia Ethernet e che la sua dimensione massima del frame sia 1500 byte.

Su Catalyst 5000, un protocollo noto come DTP (Dynamic Trunking Protocol) è diventato disponibile nella versione 4.x. Il DTP è il sostituto strategico di Dynamic ISL (DISL) perché include il supporto per la negoziazione del trunking 802.1Q. La funzione di DISL?? consiste nel negoziare, solo per ISL, se un collegamento tra due dispositivi debba o meno essere trunking. Il DTP è in grado di negoziare il tipo di incapsulamento di trunking che verrà utilizzato tra i trunk VLAN ISL e IEEE 802.1Q. Questa funzionalità è interessante, in quanto alcuni dispositivi Cisco supportano solo ISL o 802.1Q, mentre altri possono eseguire entrambi.

Questi sono i cinque stati diversi per cui è possibile configurare il DTP:

- Auto - In modalità Auto, la porta resta in ascolto di frame DTP dallo switch adiacente. Se lo switch adiacente indica che vorrebbe essere un trunk, o si tratta di un trunk, la modalità Auto crea il trunk con lo switch adiacente. Questo si verifica quando la porta adiacente è impostata sulla modalità On o Desirable.
- Desirable (Desiderabile) - La modalità Desirable (Desiderabile) indica allo switch adiacente che può essere un trunk ISL e che desidera che anche lo switch adiacente sia un trunk ISL. La porta diventa una porta trunk se la porta adiacente è impostata su On, Desirable o Auto.
- On: la modalità On attiva automaticamente il trunking ISL sulla porta, indipendentemente dallo stato dello switch adiacente. Rimane un trunk ISL a meno che non riceva un pacchetto ISL che disabiliti esplicitamente il trunk ISL.
- Non negoziazione: la modalità non negoziazione abilita automaticamente il trunking ISL sulla sua porta, indipendentemente dallo stato dello switch adiacente, ma non consente alla porta di generare frame DTP.
- Off: in modalità Off, ISL non è consentito su questa porta indipendentemente dalla modalità DTP configurata sull'altro switch.

La famiglia di switch Catalyst 5000 è in genere utilizzata per fornire la backbone ISL. Successivamente, è possibile collegare lo switch Catalyst 3900 a questa backbone tramite il modulo di espansione ISL dual 100 Mbps. Lo switch Catalyst 3900 Token Ring non supporta altre

modalità oltre all'ISL, quindi è sempre trunked. Inoltre, i moduli Catalyst 3900 ISL supportano solo connessioni a 100 Mbps e per impostazione predefinita sono full duplex.

Prestare particolare attenzione quando si collega uno switch Catalyst 3900 e uno switch Catalyst 5000 tramite il collegamento ISL. Il problema principale è che Catalyst 3900 non supporta la negoziazione multimediale Fast Ethernet. Per questo motivo, se Catalyst 5000 è configurato per la modalità automatica, per impostazione predefinita viene impostato su 100 Mbps half-duplex. Questo causa problemi come il passaggio della porta dal trunk al non trunk e la perdita di pacchetti.

Per collegare la porta ISL di Catalyst 3900 alla porta ISL di uno switch Catalyst 5000, è necessario configurare manualmente la porta ISL su Catalyst 5000:

1. Eseguire il comando **set port speed** per impostare su 100 Mbps:

   ```
   set port speed mod/port {4 | 10 | 16 | 100 | auto}
   ```

2. Eseguire il comando **set port duplex** per impostare la modalità full duplex:

   ```
   set port duplex mod/port {full | half}
   ```

Per forzare la porta di uno switch alla modalità trunk, usare il comando **set trunk** (su una riga):

```
set trunk mod/port {on | off | desirable | auto | nonegotiate} [vlans] [trunk_type]
```

Nel comando precedente, il valore delle vlan è compreso tra 1 e 1005 (ad esempio, 2-10 o 1005) e il valore di trunk_type è isl, dot1q, dot10, lane o negotiation.

Una volta attivate le porte trunk sugli switch, è possibile usare il comando **show trunk** per verificare che le porte trunk siano attive.

```
Pteradactyl-Sup> (enable) show trunk

Port      Mode         Encapsulation  Status        Native vlan
--------  -----------  -------------  ------------  -----------
 5/1      on           isl            trunking      1
10/1      on           isl            trunking      1

Port      Vlans allowed on trunk
--------  ---------------------------------------------------------------------
 5/1      1-1005
10/1      1-1005

Port      Vlans allowed and active in management domain
--------  ---------------------------------------------------------------------
 5/1
10/1      1

Port      Vlans in spanning tree forwarding state and not pruned
--------  ---------------------------------------------------------------------
 5/1
10/1      1
```

Un comando importante da utilizzare per osservare i trunk ISL è il comando **show cdp neighbors detail**. Questo comando consente inoltre di comprendere la topologia di rete.

```
Pteradactyl-Sup> (enable) show cdp neighbors detail

Port (Our Port): 10/1
Device-ID: 000577:02C700
Device Addresses:
Holdtime: 164 sec
Capabilities: SR_BRIDGE SWITCH
Version:
  Cisco Catalyst 3900 HW Rev 002; SW Rev 4.1(1)
  (c) Copyright Cisco Systems, Inc., 1995-1999  - All rights reserved.
  8 Megabytes System Memory
  2 Megabytes Network memory
Platform: CAT3900
Port-ID (Port on Neighbors's Device): 1/21
VTP Management Domain: unknown
Native VLAN: unknown
Duplex: unknown
```

Da questo output, è possibile vedere chiaramente che un Catalyst 3900 è collegato alla porta 10/1. Quando si controlla la porta 10/1 nell'output del precedente comando **show trunk**, è possibile stabilire che si tratta di una porta trunk.

Spanning-Tree

Lo Spanning-Tree negli ambienti Token Ring può diventare molto complicato perché si possono eseguire contemporaneamente tre diversi protocolli Spanning-Tree. In un ambiente tipico, ad esempio, IBM Spanning-Tree viene eseguito a livello TrBRF e IEEE (802.1d) o Cisco a livello TrCRF. Pertanto, Spanning-Tree è un po' più complicato da risolvere.

In questa tabella viene descritto ciò che accade in base ai diversi tipi di configurazioni possibili:

Modalità Bridging TrCRF	TrCRF	TrBRF
SRB	Esegue IEEE Spanning-Tree.	Viene eseguito come bridge source-route.
	Elabora il protocollo IBM Spanning-Tree Bridge Protocol Data Unit (BPDU) da bridge esterni.	Esegue i protocolli Spanning-Tree IBM su bridge esterni.
		Elimina i BPDU trasparenti

		del protocollo IEEE Spanning-Tree della TrCRF.
SRT	Esegue il protocollo Cisco Spanning-Tree.	Viene eseguito come bridge trasparente e source-route.
	Sostituisce il campo dell'indirizzo del gruppo di bridge di destinazione con un indirizzo di gruppo specifico di Cisco, in modo che i bridge esterni non analizzino i BPDU TrCRF.	Inoltra il traffico trasparente e il traffico dell'origine.
	Generare BPDU, con il bit RIF impostato nel campo dell'indirizzo di origine nel frame in uscita e un RIF di 2 byte aggiunto. Questo formato di frame garantisce che il TrCRF rimanga locale rispetto all'anello logico e non venga collegato in modo trasparente o inviato ad altre LAN. Solo i TrCRF connessi tramite loop fisici ricevono i BPDU.	Inoltra il traffico origine-route a tutti gli altri TrCRF nel TrBRF, sia in modalità SRT che SRB.
	Elaborazione delle BPDU IEEE Spanning-Tree da bridge esterni.	

Protocollo VLAN Trunking

Poiché con l'ISL, la VLAN determina la destinazione di un pacchetto, è importante che ciascuno switch sia a conoscenza delle VLAN nella rete. Lo scopo del VTP è quello di propagare le informazioni sulla VLAN sugli switch. Il VTP non funziona nei router, perché devono terminare la rete VLAN. Ciascuno switch della rete deve eseguire il VTP. In caso contrario, lo switch esegue in genere una sola VLAN (generalmente VLAN 1) e non esegue ISL su quel collegamento, perché non è necessario. Il VTP semplifica notevolmente la creazione delle VLAN, in quanto è possibile configurare le VLAN in uno switch e le VLAN possono propagarsi attraverso la rete. Ovviamente, ciò comporta dei problemi.

Il VTP non è un sistema solido, come il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol) o il protocollo di routing OSPF (Open Shortest Path First). È molto più semplice e si basa su un concetto molto importante: revisioni. Nel VTP, sono disponibili tre tipi di dispositivi VTP: client, server e dispositivi trasparenti. I dispositivi VTP client accettano semplicemente le informazioni sulla VLAN provenienti dai dispositivi server e non possono modificare queste informazioni. I server, tuttavia, possono modificare le informazioni VTP su uno qualsiasi dei server VTP. Per questo motivo, il VTP ha un sistema di revisione. Ogni server VTP che modifica o

aggiorna il database VLAN dichiara che si tratta della revisione più recente. Per questo motivo, è necessario procedere con estrema cautela, poiché lo switch con la revisione più recente avrà la priorità?????? e le relative informazioni sulla VLAN saranno quelle valide. Ad esempio, se si modifica un server VTP per comunicare che la VLAN 100 TrBRF eseguirà lo spanning-tree IEEE, si verificheranno problemi tra tutti gli switch, in quanto potrebbe causare agli switch (come lo switch Catalyst 3900) il blocco delle porte e quindi la protezione dagli loop. Inoltre, fare attenzione quando si introducono nuovi switch nella rete, in quanto potrebbero avere revisioni VTP superiori. In modalità trasparente, i pacchetti VTP ricevuti su un trunk vengono propagati automaticamente, senza modifiche, a tutti gli altri trunk sul dispositivo; ma vengono ignorati sul dispositivo stesso.

Quando si configura il VTP con gli switch Token Ring, è necessario eseguire il VTP V2. Se gli switch hanno sia VLAN Ethernet che Token Ring, è necessario aggiornare il VTP, anche per le VLAN Ethernet. *Non* è *possibile* avere due domini VTP diversi (ad esempio, non è possibile averne uno per Ethernet e uno per Token Ring).

Eliminazione VTP

Uno dei problemi del trunking VLAN è che le informazioni broadcast di una VLAN si propagano su tutti i trunk, perché gli switch non sanno quali VLAN esistono in uno switch remoto. Per questo motivo è stata creata l'eliminazione VTP. Consente agli switch di negoziare le VLAN assegnate alle porte all'altra estremità del trunk e, quindi, di eliminare le VLAN non assegnate in remoto. Sugli switch Catalyst 3900 e Catalyst 5000, l'eliminazione è disabilitata per impostazione predefinita.

Nota: l'eliminazione VTP è supportata sullo switch Catalyst 3900 nella versione 4.1(1).

Ciascuno dei messaggi di eliminazione VTP contiene informazioni sulle VLAN in questione e un bit che indica se la VLAN deve essere eliminata o meno per il trunk (il valore `1` indica che non deve essere eliminata). Se l'eliminazione è abilitata, il traffico VLAN normalmente non viene inviato attraverso il collegamento trunk, a meno che il collegamento trunk non riceva un messaggio di join appropriato con il bit della VLAN?? corrispondente abilitato. Questa operazione è molto importante perché indica che, quando si utilizza l'eliminazione VTP, è necessario verificare che le informazioni e la configurazione siano corrette e che tutti gli switch siano in esecuzione. se uno switch non invia messaggi di join a un altro switch sul trunk, potrebbe spegnersi per una particolare VLAN o VLAN. Al termine della negoziazione di eliminazione, la VLAN terminerà in stato eliminato o unito per il trunk.

Una funzione molto importante dell'eliminazione VTP consente di configurare una VLAN in modo che possa o meno eseguire l'eliminazione. Questa funzione indica agli switch con eliminazione VTP di non eliminare la VLAN. Quando si abilita l'eliminazione VTP, le VLAN da 2 a 1000 eseguono l'eliminazione delle VLAN idonee per impostazione predefinita. Pertanto, l'attivazione della eliminazione ha effetto su tutte le VLAN per impostazione predefinita. la VLAN 1, il TrCRF predefinito (1003), il TrBRF predefinito (1005) e i TrCRF sono sempre non idonei per l'eliminazione; di conseguenza, il traffico proveniente da queste VLAN non può essere eliminato.

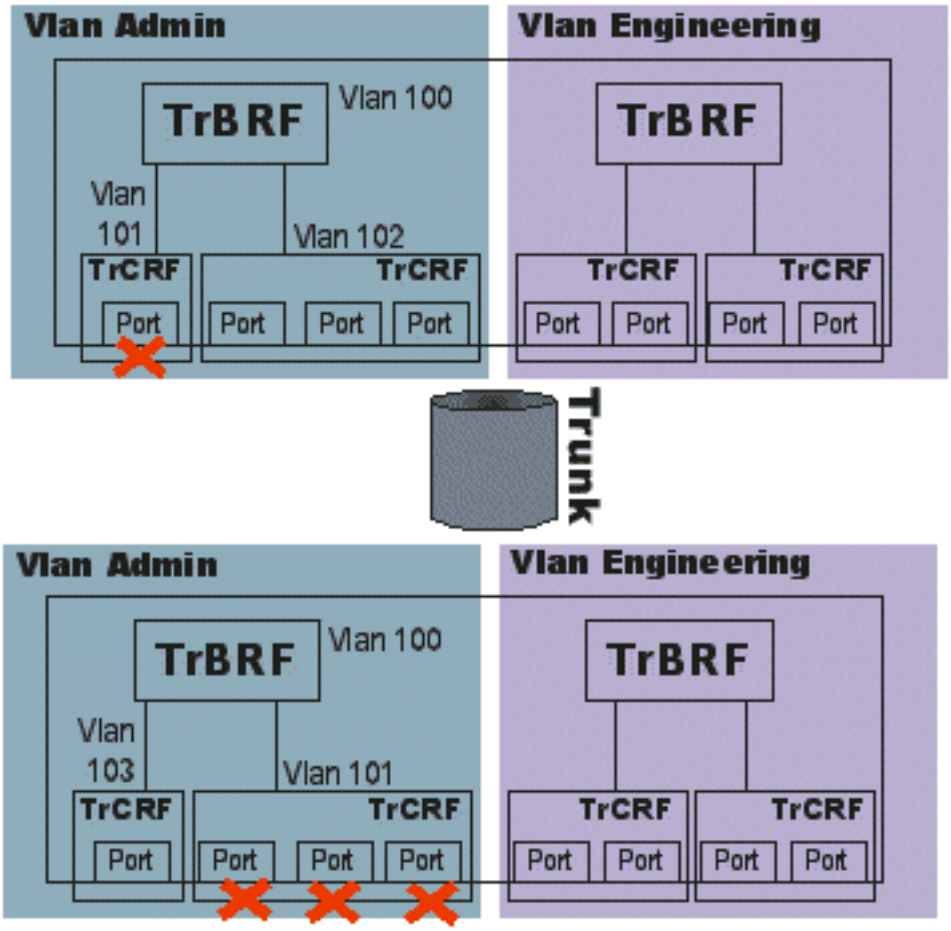
Protocollo ad anello duplicato

Il protocollo Token Ring è progettato per essere eseguito sugli switch con VLAN Token Ring. Il suo compito è quello di garantire la corretta configurazione delle VLAN Token Ring e di ridurre il numero di esploratori. Il protocollo DRiP utilizza il protocollo VTP per sincronizzare le informazioni del database VLAN, ma non è necessario per il funzionamento del protocollo DRiP (il database

VLAN può essere stabilito manualmente). Un'idea sbagliata è che DRiP comprenda i numeri ad anello; questo non è vero. Il DRiP si basa sull'univocità delle VLAN configurate in una rete e sulla configurazione di tale database VLAN.

Una delle caratteristiche più importanti di DRiP è l'implementazione della distribuzione TrCRF. Nel mondo dei Token Ring, è molto pericoloso distribuire qualsiasi VLAN diversa dalla 1003, a causa di problemi di spanning. Per questo motivo, se viene distribuito un TrCRF diverso dalla VLAN 1003, tutte le porte a cui tale VLAN è associata vengono disabilitate da DRiP.

Nell'esempio viene illustrato questo concetto:

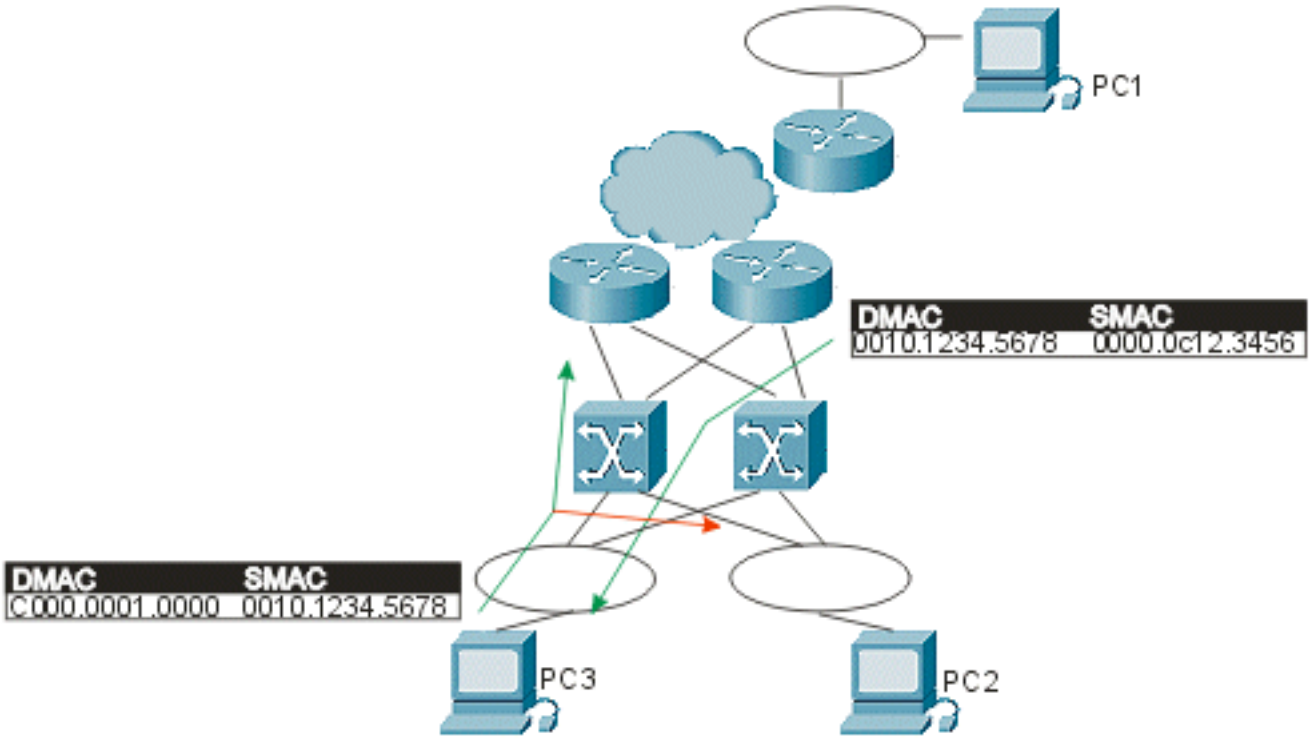


Nell'esempio, due switch diversi hanno una porta assegnata alla VLAN 101. Lo switch, tramite DRiP, sposta lo spanning-tree della porta per disabilitare e arrestare l'inoltro del traffico. In questo modo lo switch viene protetto da eventuali condizioni di loop.

Se non viene apportata alcuna modifica, DRiP annuncia lo stato TrCRF a tutte le porte trunk ogni 30 secondi. Qualsiasi modifica apportata tramite CLI (Command Line Interface) o SNMP invierebbe immediatamente un aggiornamento a tutte le porte. Questi annunci sono frame ISL di tipo 0 e vengono trasmessi sulla VLAN predefinita 1. Poiché il protocollo DRiP ne annuncia gli effetti solo per le VLAN, è importante che negli switch connessi tramite ISL siano presenti le informazioni VLAN corrette. Questa operazione viene eseguita tramite VTP. Se il VTP è disabilitato, questa funzione deve essere gestita manualmente su tutti gli switch che condividono le stesse VLAN. Gli annunci DRiP esistono solo sui collegamenti ISL. Non esistono su ATM, Token Ring, Ethernet o FDDI. In DRiP non sono presenti alberi della topologia.

VLAN HSRP e Token Ring

Uno dei maggiori problemi con HSRP è l'uso dell'indirizzo multicast nella rete. Poiché nessuno in rete ricerca i pacchetti con questo indirizzo MAC virtuale, gli switch non imparano mai questi indirizzi MAC. e inondano i frame su tutta la rete. Per questo motivo, è stato richiesto l'uso della funzione **use-bia** di **standby** dell'HSRP per inviare pacchetti che usavano l'indirizzo MAC incorporato dell'interfaccia del router HSRP attiva. Il problema principale di questo scenario è che, quando i router HSRP commutano, dovranno inviare un protocollo ARP (Broadcast Address Resolution Protocol; gratuite ARP) a tutte le stazioni del cavo, in modo che le stazioni possano conoscere il nuovo indirizzo MAC del gateway. Anche se questo processo dovrebbe funzionare in base alle specifiche IP, ci sono stati alcuni problemi noti con esso. A causa delle continue richieste provenienti dal campo, HSRP è stato modificato in modo da poter disporre dell'indirizzo multicast e anche essere in grado di utilizzare HSRP senza **use-bia di standby**. Questa modifica è stata introdotta nel software Cisco IOS versione 11.3(7) e 12.0(3) e successive.



Nel diagramma precedente è in corso la comunicazione tra PC1 e PC3. Il problema è che il traffico IP dal client al router predefinito in questa immagine utilizza un indirizzo di destinazione multicast. Poiché nessuno può ricevere il pacchetto da quell'indirizzo, gli switch non vengono mai a conoscenza dell'indirizzo e inondano sempre i pacchetti. Il DMAC tradizionale che dipende dai gruppi è C000.000X.0000, che non può mai essere uno SMAC in Token Ring. Tutti i pacchetti destinati da PC3 a PC1 tramite il gateway predefinito vengono ora visualizzati da PC2. In una rete con molti bridge, questo può moltiplicarsi molto rapidamente e causare ciò che sembrerebbe una trasmissione di tempeste, ma che in realtà è una grande quantità di traffico multicast.

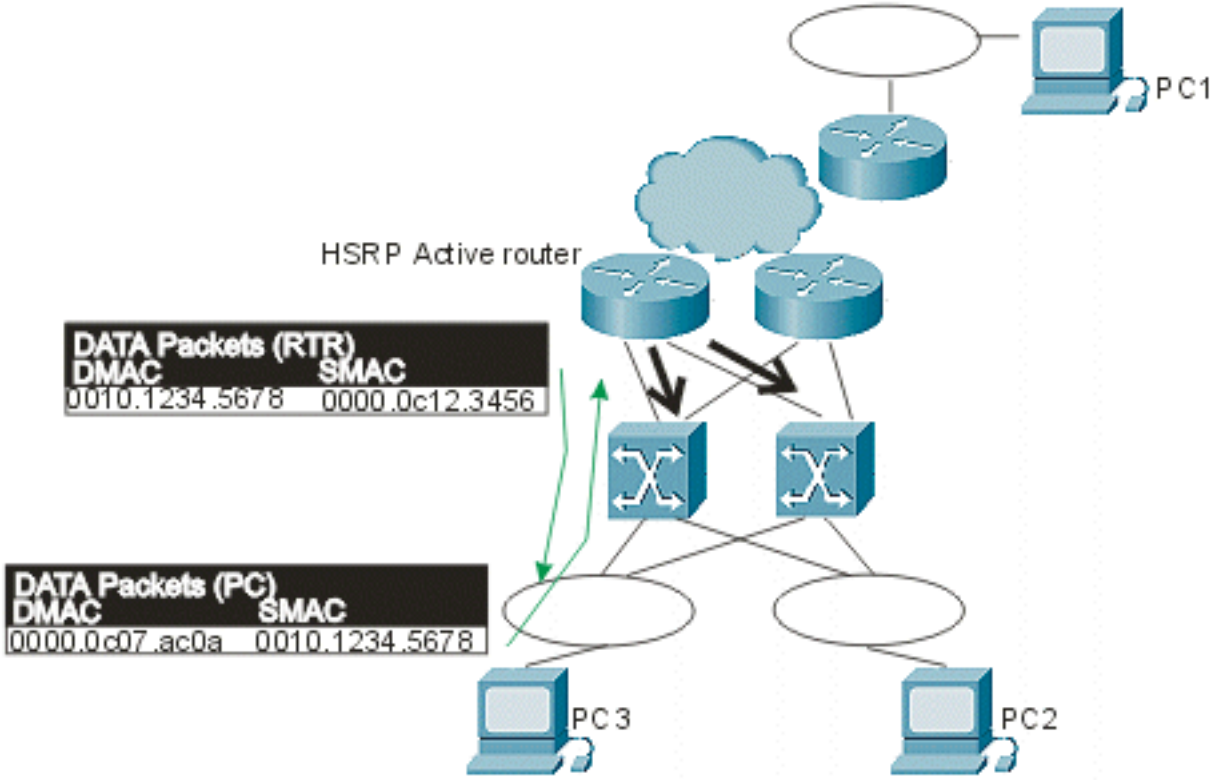
Per risolvere questo problema, è necessario utilizzare un indirizzo MAC che possa essere effettivamente utilizzato come SMAC dai router negli helper HSRP. Questo consente agli switch di conoscere questo indirizzo e, quindi, di commutare i pacchetti in modo appropriato. A tale scopo, configurare un nuovo indirizzo MAC virtuale nei router. I client devono inviare i pacchetti al DMAC di questo nuovo indirizzo virtuale. Questo è l'output di esempio di un comando **show standby**:

```
vdtl-rsm# show standby

Vlan500 - Group 10
Local state is Active, priority 100
Hellotime 3 holdtime 10
```

```
Next hello sent in 00:00:01.224
Hot standby IP address is 1.1.1.100 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac0a
```

In questo output, è stato creato un gruppo di standby 10 (standby IP 1.1.100). L'indirizzo MAC (`0000.0c07.ac0a`) è il nuovo indirizzo MAC virtuale e l'ultimo byte è il gruppo (0xA = 10). Con questa nuova configurazione, il traffico viene strutturato in modo da evitare sovraccarichi del traffico:



Ora, poiché il router sta inviando i pacchetti al DMAC del MAC virtuale HSRP, gli switch apprendono questo indirizzo MAC e inoltrano i pacchetti solo al router HSRP attivo. Se il router HSRP attivo si guasta e il sistema di standby diventa attivo, il nuovo router attivo inizierà a inviare gli hellop HSRP con lo stesso SMAC, in modo che le tabelle degli indirizzi MAC dello switch passino le voci apprese alla nuova porta dello switch e al nuovo trunk.

A causa del multireframe, è necessario eseguire un'operazione aggiuntiva per garantire che il RIF cambi effettivamente durante la transizione (anche se si tratta dello stesso indirizzo MAC). La funzione di multireframe consente al router di associare un RIF a un indirizzo MAC, proprio come una stazione terminale. I router necessitano di più collegamenti negli ambienti in cui esistono bridge SRB, in modo che i pacchetti possano attraversarli per raggiungere le stazioni terminali.

Nello stesso esempio vengono illustrati i passaggi aggiuntivi necessari al client per connettersi al nuovo router HSRP attivo:

1. Il router attivo smette di funzionare.
2. Quando il router in standby rileva una perdita di helper HSRP, avvia il processo per diventare il router HSRP attivo.
3. Il router invia un ARP gratuito dallo stesso SMAC come in precedenza, sia a livello MAC che a livello ARP.
4. Il PC ora invia il frame destinato allo stesso indirizzo MAC, ma con il nuovo RIF.
5. Una volta ricevuto il frame (destinato all'indirizzo MAC dell'HSRP), il router invia una richiesta

ARP direttamente al client, in quanto *non* include l'indirizzo MAC del client nella relativa tabella ARP.
6. Dopo aver ricevuto la risposta al pacchetto ARP, il router può inviare i pacchetti al client di destinazione.

Informazioni correlate

- Switch - Supporto dei prodotti
- Supporto della tecnologia di switching LAN
- Documentazione e supporto tecnico – Cisco Systems