Conceptos del Token Ring Switching

Contenido

Introducción

Para comenzar a entender los conceptos de Token Ring Switching, es muy importante que usted entiende Puente transparente, el Source-Route Bridging, y el Spanning-tree. El Catalyst 3900 y el Catalyst 5000 utilizan los conceptos nuevos, según lo descrito en IEEE802.5 el anexo K. Estos conceptos son los bloques de construcción para los VLAN Token Ring. Este documento explica los diversos conceptos de Bridging y cómo éstos trabajan:

- Enlace del Inter-Switch Link (ISL)
- Spanning-tree
- VLAN Trunking Protocol (VTP)
- Protocolo de anillo duplicado (DRiP)

Este documento también explica algunos de los problemas que ocurren cuando usted ejecuta el Hot Standby Router Protocol (HSRP) sobre los VLAN Token Ring, y sus soluciones alternativas.

Nota: Para la definición de las siglas del Token Ring que se utilizan en este documento, refiera a las siglas del Token Ring Switching.

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.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

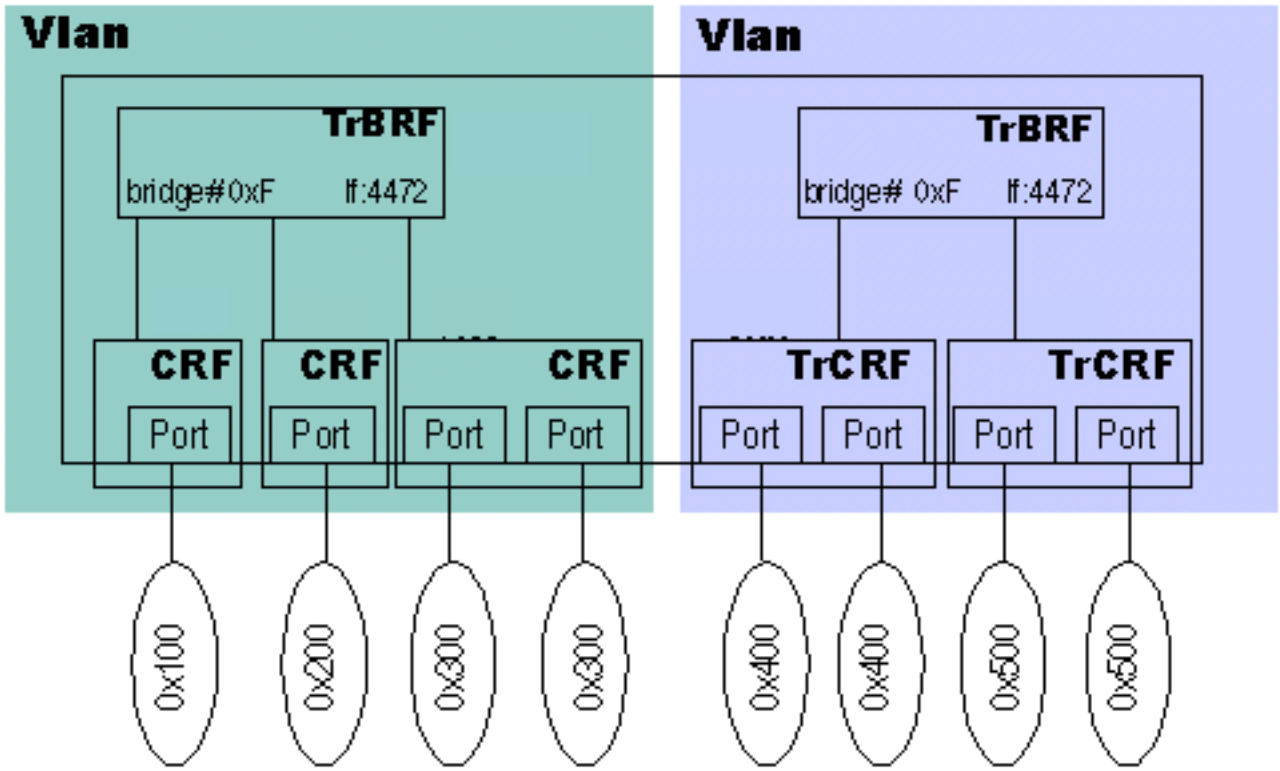
Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

TrBRF y TrCRF

La función de Token Ring Bridge Relay (TrBRF) y la función de retransmisión de concentrador Token Ring (TrCRF) son los bloques de construcción de la arquitectura del Catalyst 3900 y de las funciones del Catalyst 5000. El TrBRF es simplemente la función de Bridge del Switch, y el TrCRF es la función del concentrador del Switch. Es importante entender que el interligar sucede en ambas capas porque, en el Token Ring, discutirán tres diversos tipos de bridging.

La funcionalidad de TrBRF del Switch controla la transferencia del tráfico interligado por Source Route, como el (SRB) y el Source-Route Transparent Bridging (SRT) del Source-Route Bridging. El TrCRF cubre las funciones del Source-Route Switching (SRS) y del transparent bridging (TB). Por ejemplo, es posible tener un Catalyst 3900 Switch que tenga solamente un TrBRF y un TrCRF y todos los puertos del Switch están en el mismo TrCRF. Esto hace el Switch solamente poder hacer el SRS y el TB. Si usted definiera diez diversos TrCRFs bajo el mismo TrBRF del padre, después el tráfico de los puertos que están conectados con el mismo TrCRF sería remitido vía la funcionalidad de TrCRF del SRS o del TB. El tráfico que va al otro TrCRFs en el Switch utilizaría la funcionalidad de TrBRF del Switch y sería Source-Route interligado o Source-Route transparente interligado. Los diversos mecanismos de Switching serán discutidos más adelante en este documento.

Este diagrama se relaciona el TrBRF y el TrCRF con el mundo físico:



Usted puede ver que cada TrCRF está conectado con un timbre específico. Un TrCRF puede comprometer los puertos múltiples, y estos puertos comprometerían el mismo número de anillo. El TrBRF conecta el TrCRFs junto.

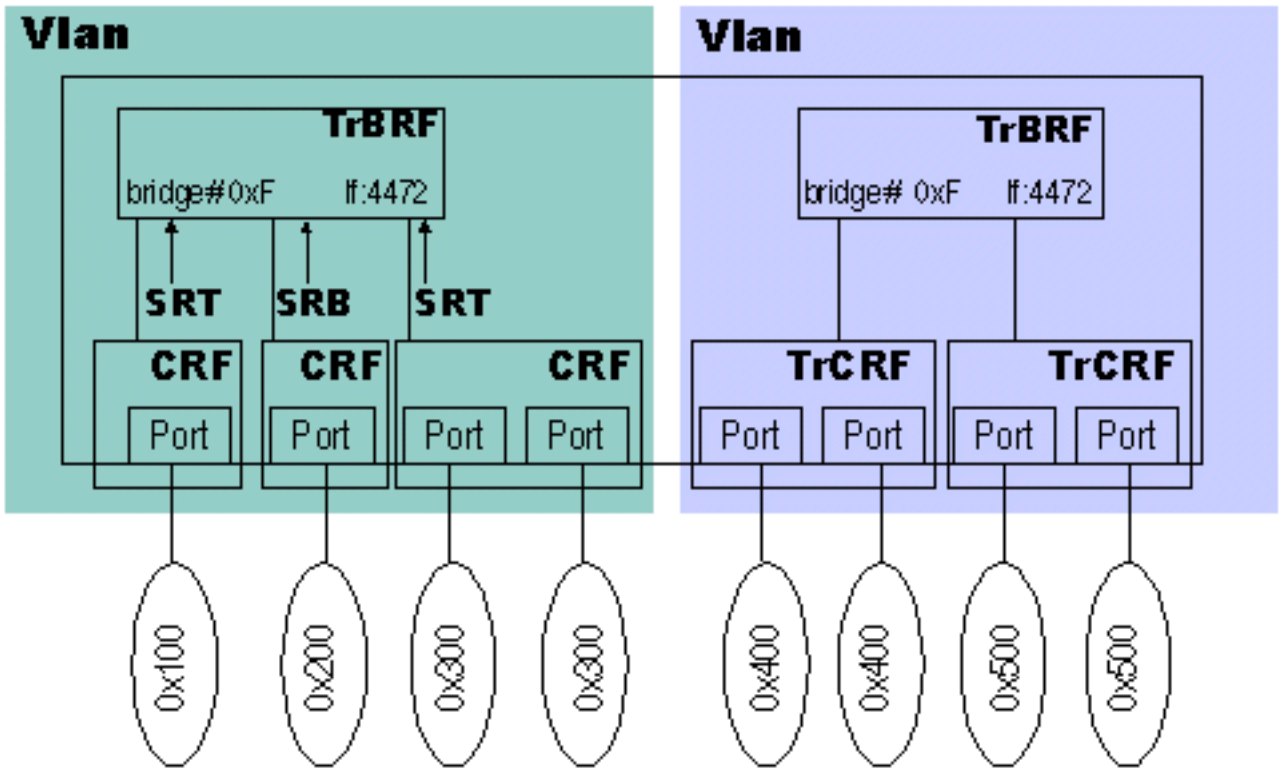
Un TrCRF y un TrBRF en sí mismo es un diverso VLA N. Así pues, en el Token Ring, usted puede interligar entre los VLA N. El bridging entre los VLAN Token Ring sigue dos reglas:

- El bridging entre dos VLA N del TrBRF se puede lograr solamente por un dispositivo externo, como un router o un (RSM) del Route Switch Module.
- El bridging entre los VLA N del TrCRF se puede lograr solamente con los VLA N del TrCRF que son niños del mismo VLA N del TrBRF del padre.

Esto es muy importante tener presente para los VLAN Token Ring, porque rompe el paradigma Ethernet. Para resumir, qué parecerían las redes Ethernet VLAN es la suma de un TrBRF y de su TrCRF de los niños. Porque usted puede interligar entre ciertos VLA N en el Token Ring, usted debe entender cómo ocurre este bridging.

Nota: Para hacerla más fácil entender los VLAN Token Ring en relación con las redes Ethernet VLAN, recuerde que la combinación de TrCRF y de TrBRF hace un VLA N en sí mismo.

En este diagrama, usted puede ver que el TrCRF decide al Bridging Mode entre el TrCRF y el TrBRF.



El TrCRFs individual ha configurado qué tipo de bridging harán al TrBRF. Esto es importante porque usted puede tener VLA N del TrCRF que hagan el Source-Route Bridging al otro TrCRFs pero no hará los Non-Source-Routed Frame. En el diagrama anterior, un TrCRF se configura para el modo SRB y dos están en el modo SRT. Esto significa que el tráfico SRB puede fluir entre los tres TrCRFs, pero el SRT puede fluir solamente entre los dos que están en el modo SRT. Esto permite que usted granularly fije cómo el tráfico debe fluir entre el TrCRFs. Si el Bridging Mode fuera fijado en el TrBRF, afectaría a todos los niños del TrCRF de ese VLA N.

Modos de Switching

El cuadro de los, el Catalyst 3900 se configura con un TrBRF y un TrCRF. Todos los puertos se asignan al VLA N predeterminado 1003 del TrCRF. Lo mismo se aplica al Token Ring Blade del Catalyst 5000. ¿Esto es importante porque da el cuadro seguro??? ¿función Plug and Play??? funciones. El cuadro de los, este Switches puede hacer la expedición basada en el Source-Route Switching y Puente transparente. Las siguientes secciones proporcionan los detalles sobre estas Tecnologías.

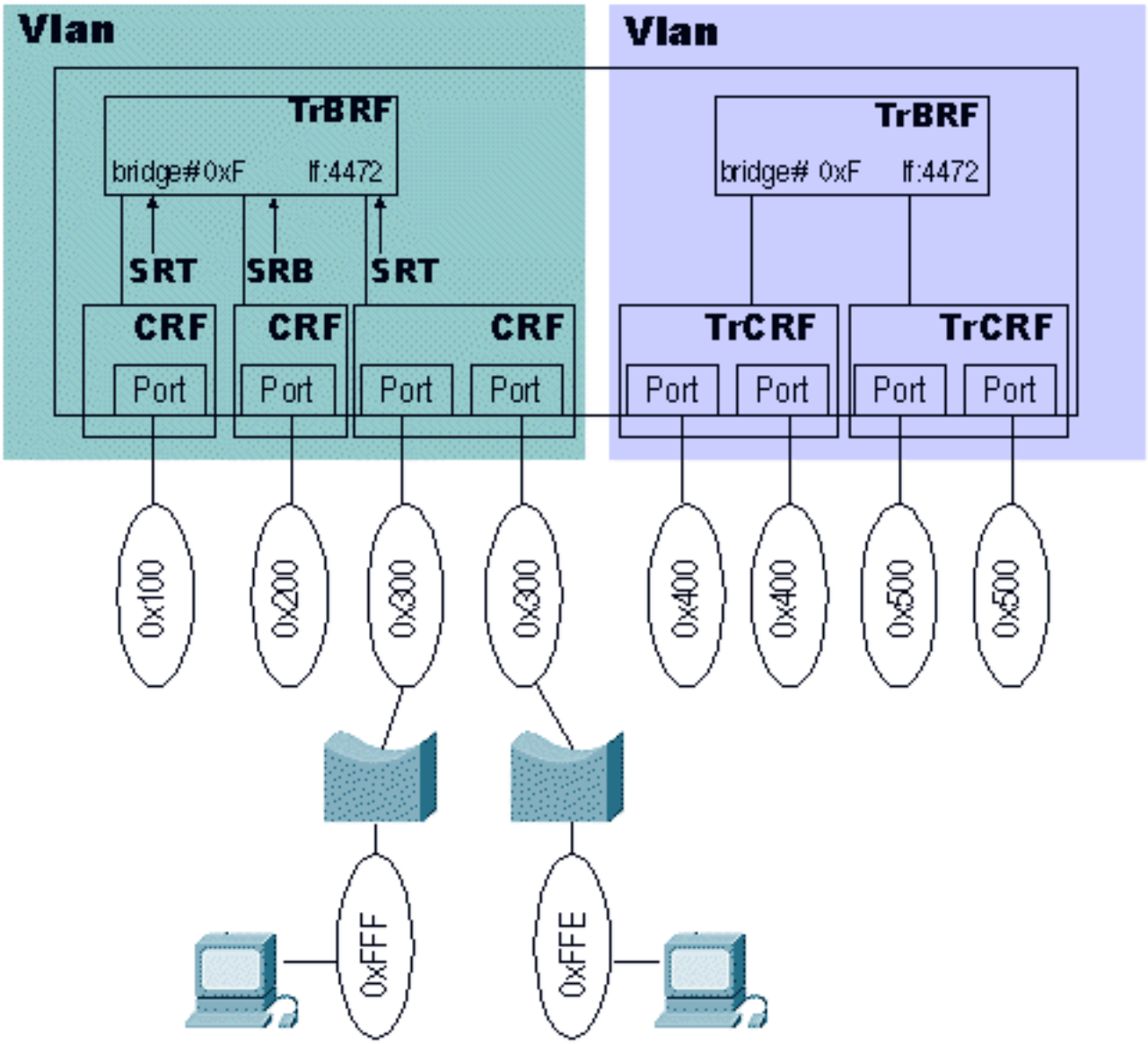
Uso de puente transparente

Puente transparente es el más básico de todos los mecanismos de Switching y se basa en el direccionamiento del MAC de destino (DMAC) de los bastidores en la red. Éste es el mecanismo de reenvío de las redes Ethernet. Un Switch recibe en cualquier momento una trama, registra MAC de origen (SMAC) el direccionamiento del bastidor como uno que pertenezca a ese puerto y, en adelante, adelante trafica que se destina a ese MAC a ese puerto. Si, en el proceso de aprendizaje, un Switch no sabe sobre una dirección MAC, inundará ese paquete a todos los puertos en el estado de reenvío.

Source-Route Switching

El Source-Route Switching es un mecanismo de reenvío que es necesario cuando hay solamente

un TrCRF asignado a los puertos y el Switch recibe los paquetes con los campos routing informationes (RIF) en ellos. Porque el Switch no modificará el RIF del bastidor (porque no lo pasará al TrBRF), la red debe poder tomar las decisiones en la expedición, con el RIF, sin las modificaciones. Considere este diagrama de la red que muestre el SRS:



El tráfico que va del timbre 0xFFF a sonar 0xFFE necesita pasar a través del Switch. Este tráfico sería tráfico de source-route bridge. Ésta es la Secuencia de inicio de la comunicación entre estos dos clientes:

1. Una estación envía un paquete explorador al timbre en el cual reside. Asuma que el cliente en el timbre 0xFFF envía el paquete; mira algo similar (en el hexadecimal):`0000 00c1 2345 8000 0c11 1111 C270`**Nota:** Esa información del paquete muestra solamente el DMAC, el S AC, y la información RIF.
2. Una vez que el paquete alcanza el Source-Route Bridge y adelante la trama al alambre, el paquete parece esto:`0000 00C1 2345 8000 0c11 1111 C670 FFF1 3000C670` es el campo de Routing Control y el `FFF1 3000` es el timbre 0xFFF, el Bridge 0x1, el timbre 0x300. Para más información sobre decodificar los RIF, refiera a configurar el Source-Route Bridging.
3. Ahora, el paquete golpea el Switch. Porque el Switch considera el paquete el venir lejos de un sonido, aprende al descriptor de Route. En este caso, el Switch ahora sabe que el timbre 0xFFF vía el Bridge 0x1 está situado en el puerto 3.

4. Porque el paquete es un paquete explorador, el Switch adelante la trama a todos los puertos bajo el mismo TrCRF. Si el explorador necesita ir a los puertos en diverso TrCRFs, entregará la trama al TrBRF, que harán sus funciones del Bridge. Si hay puertos en el mismo TrCRF, remitirá la trama saliente sin la modificación.
5. La estación en el timbre 0xFFE debe conseguir al explorador y responder a ella. Asuma que el cliente responde con un directed frame. Este directed frame parece esto:`0000 0C11 1111 8000 00C1 2345 08E0 FFF1 3001 FFE008E0` es el campo de Routing Control y el `FFF1 3001 FFE0` es el timbre 0xFFF, el Bridge 0x1, el timbre 0x300, el Bridge 0x1, el timbre 0xFFE.
6. Finalmente, el Switch aprende que el timbre 0xFFE está situado en el puerto 4 y guarda al descriptor de Route.

En adelante, el Switch sabe sobre esos timbres. Si usted mira las tablas, usted debe ver que el Switch ha aprendido sobre el número de Bridge y el número de anillo. Cualquier otros timbres después de que el timbre 0xFFF y el timbre 0xFFE no sean necesarios, porque tienen que pasar a través del timbre 0xFFF o sonar 0xFFE para alcanzar el Switch.

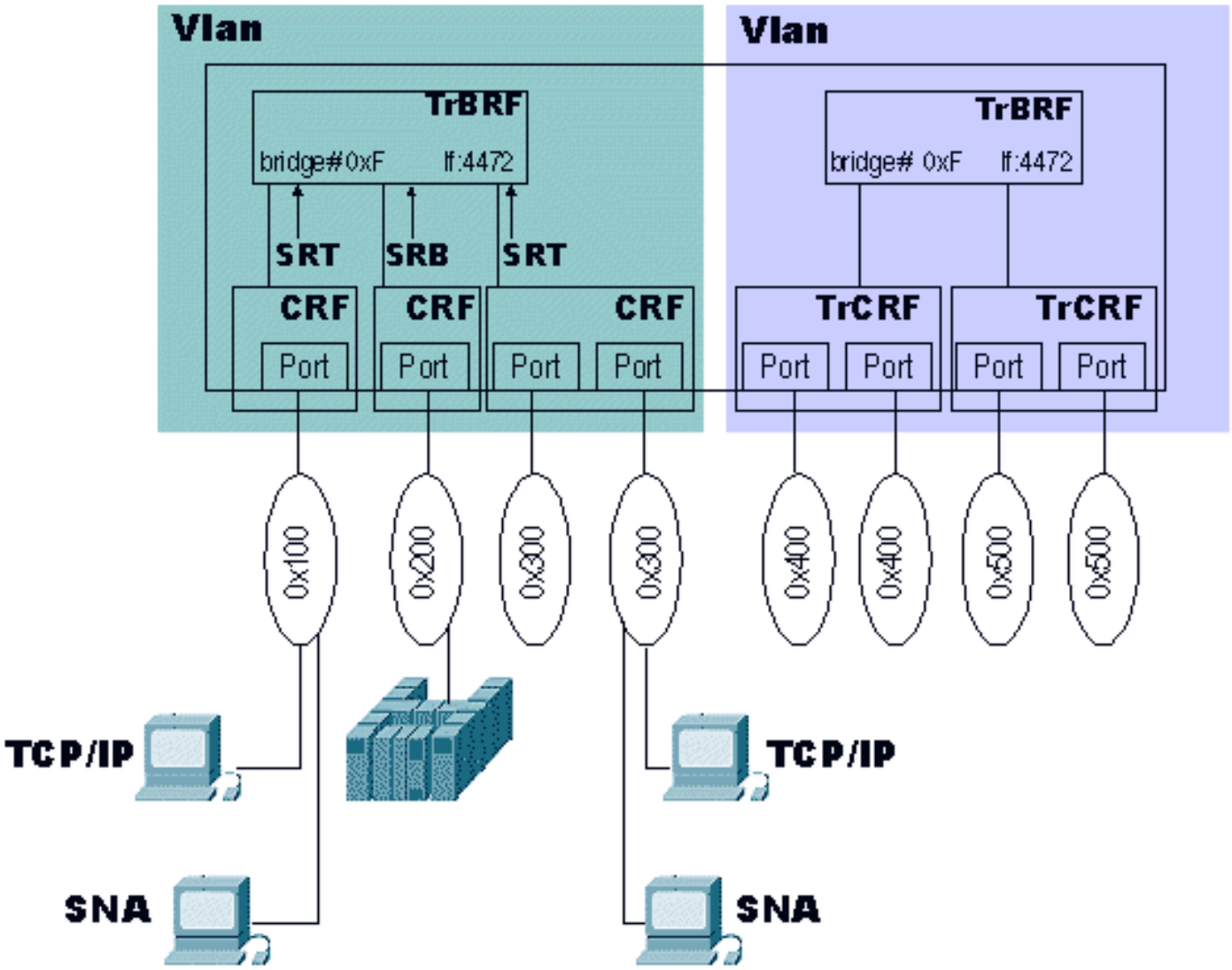
El SRS es una expedición básica de los paquetes RIF-basados sin la funcionalidad SRB, como en el caso del TrCRF.

Nota: Para ver la tabla de la información de ruteo en el Catalyst 3900, refiera al Route Descriptor Table de la visión para cada VLA N en el manejo del Catalyst 3900. Para el Catalyst 5000, publique el **comando show rif**.

Source-Route Bridging y ruta de origen transparente

Todas las funciones del Source-Route Bridging están situadas en la lógica TrBRF. El TrCRF es el que va a ordenar el Bridging Mode al TrBRF. Así pues, si el TrCRF entonces se configura para el modo SRB al TrBRF, cuando el TrCRF recibe una trama NSR (NON-fuente-ruteado), el Switch no le transmite la lógica TrBRF.

Esto puede ser utilizada si usted no quisiera que los tipos determinados de tráfico golpeen o que dejaran un timbre específico. Este diagrama muestra un ejemplo:



Si los clientes TCP/IP no tuvieran la capacidad de enviar los paquetes con los RIF, el Switch no pondría esas tramas en el mismo timbre con la unidad central (0x200). Sin embargo, las tramas SNA al host (que tienen generalmente un RIF) alcanzarían la unidad central. Esto es mismo una forma rudimentaria de filtrar las tramas en una red de switch.

Ésta es la secuencia que el Switch sigue para remitir a una trama Bridged del Source-Route a través del TrBRF:

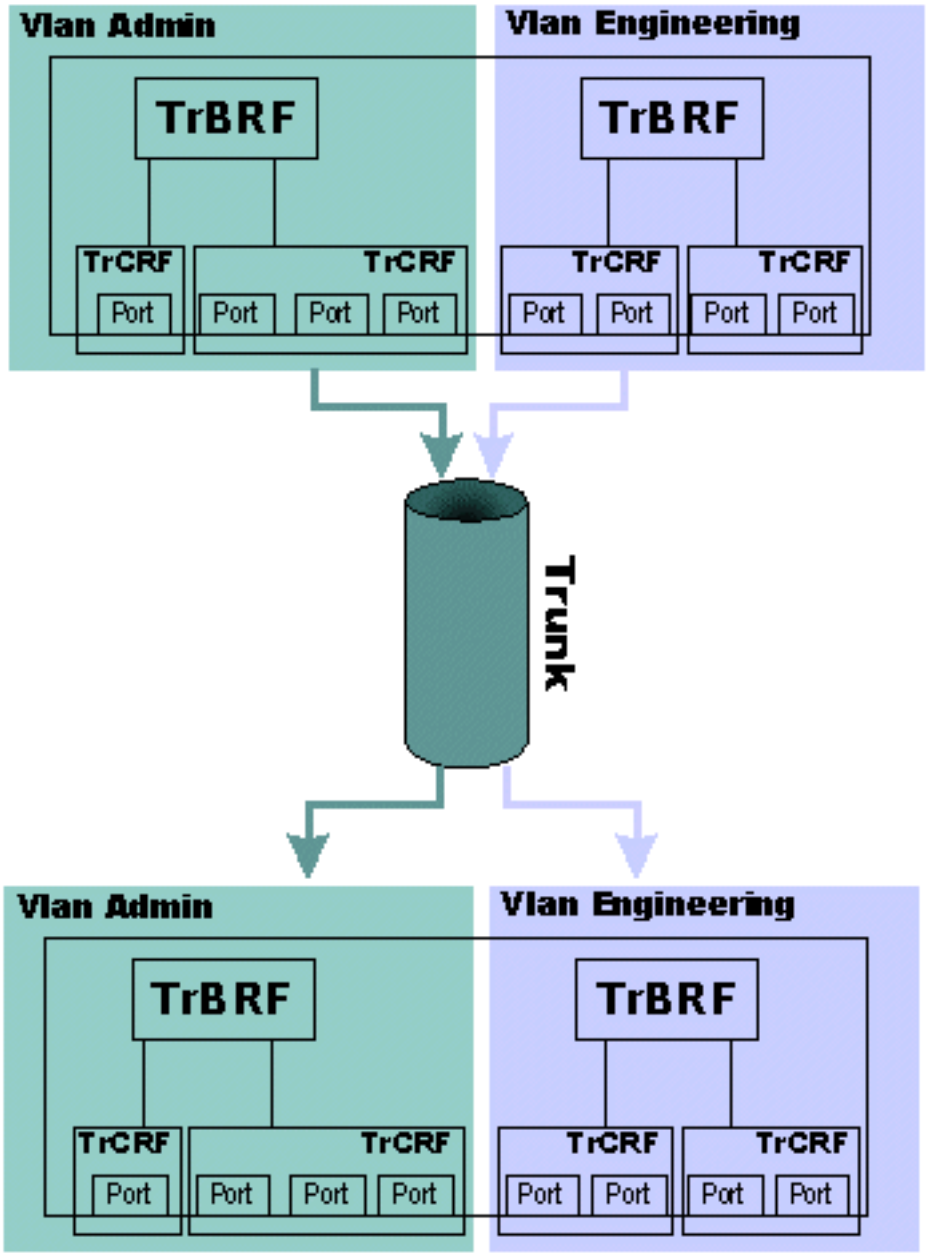
1. La estación SNA en el timbre 0x300 (el puerto 4) envía a un explorador para alcanzar la unidad central.
2. Cuando el paquete explorador golpea el Switch, él adelante el explorador, sin la modificación, en el mismo TrCRF; entonces envía una copia al TrBRF para remitir al resto del TrCRFs. En este caso, porque el paquete tiene un RIF, pasa a través del trayecto de SRB. El Switch también necesita aprender la ruta.
3. El Switch va a aprender el S AC del bastidor, porque el paquete muestra como originando en el anillo local con el cual el Switch está conectado. Esto es porque, en una combinación TrCRF del puerto múltiple, el RIF muestra el anillo de destino, solamente las necesidades del Switch de conocer cuál puerto en el TrCRF. Por lo tanto, el Switch aprende el S AC de los bastidores que están viniendo adentro en el TrCRF llano.
4. El paquete sale a todo el resto del TrCRFs, modificado con sus combinaciones respectivas de número de Bridge Ring.
5. El host responde una vez con la trama SRB, el Switch aprende el S AC del host para ese

TrCRF y lo envía al puerto de egreso. El tráfico entonces fluye hacia adelante y hacia atrás entre los dos.

Nota: Para marcar la tabla de la dirección MAC en el Catalyst 3900, refiera a ver la tabla de direcciones principal en el manejo del Catalyst 3900. Para el Catalyst 5000, publique el **comando show cam**.

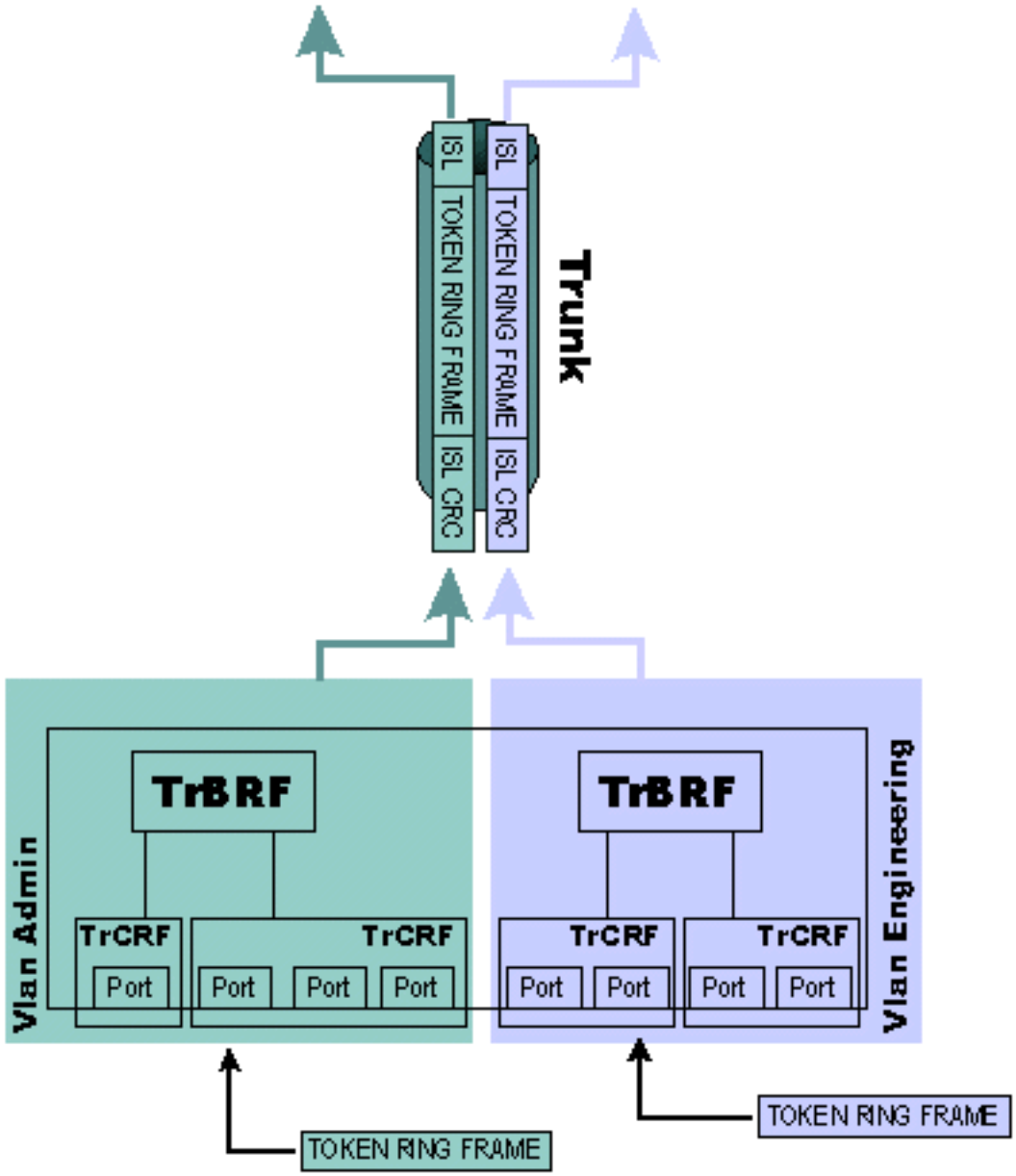
Link entre switches

El link entre switches es mismo un protocolo sencillo. Básicamente, las tramas que van a través de un troncal ISL se encapsulan en un ISL frame que dice el otro lado a qué VLA N pertenecen las tramas. Debido a esto, la información de VLAN se debe compartir manualmente o automáticamente entre el Switches. Un protocolo conocido como VLAN Trunking Protocol (VTP) puede manejar esta tarea. Para los VLAN Token Ring, usted debe ejecutar VTP V2 en la red. Considere este diagrama:

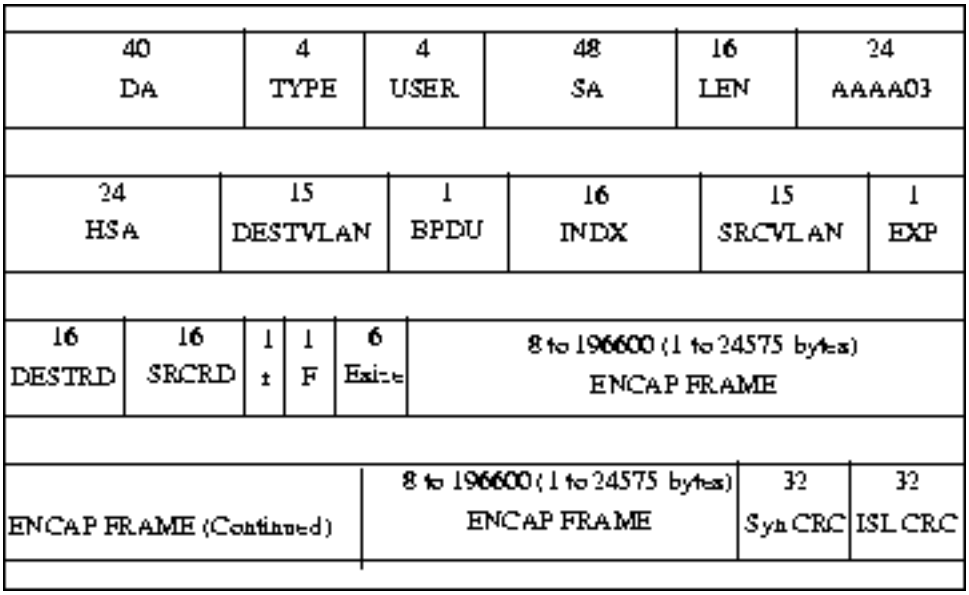


En este caso, un solo troncal ISL se ha creado para llevar, en sí mismo, los VLA N de la ingeniería y los VLA N admin. Ninguno del tráfico en cualquier VLA N se mezcla después de que

pase a través del trunk. Este diagrama muestra la manera que esta separación se alcanza:



Cada trama de esos VLA N que necesita ir a través del trunk se encapsula en un ISL frame y su VLA N se incluye en la trama. Esto permite que el Switch de recepción rutee correctamente la trama a su VLA N específico. La trama del ISL de Token Ring (TRISL) tiene algunos más campos que un ISL frame regular. Este diagrama muestra la disposición de un bastidor TRISL:



Nota: Aunque el TRISL funciona con encima las interfaces Fast Ethernet, los paquetes contienen una trama Token Ring estándar y la información de VLAN asociadas a esa trama, hasta cierto punto. Los VLAN Token Ring permiten hasta los tamaños de trama 18k, al igual que ISL. Esto no se alcanza con la fragmentación del bastidor. El toda la trama se encapsula en un ISL frame en un pedazo entero y se envía a través del link. Hay un concepto erróneo común que el ISL es Ethernet y que su tamaño máximo del marco es 1500 bytes.

En el Catalyst 5000, un protocolo conocido como Dynamic Trunking Protocol (DTP) estaba disponible en la versión 4.x. DTP es el reemplazo estratégico del ISL dinámico (DISL) porque incorpora el soporte para la negociación de trunking 802.1Q. ¿DISL??? la función s es negociar, para el ISL solamente, independientemente de si un link entre dos dispositivos debe ser enlace. El DTP puede negociar la encapsulación de la clase de conexión troncal que será utilizada entre los troncales VLAN ISL y del IEEE 802.1Q. Esto es una característica interesante, pues algunos dispositivos de Cisco soportan solamente el ISL o el 802.1Q, mientras que algunos pueden ejecutar ambos.

Éstos son los cinco diversos estados para los cuales usted puede configurar el DTP:

- ¿Auto??? En el modo automático, el puerto está atentas las tramas DTP del switch de vecindad. ¿Si el switch de vecindad indica que quisiera ser un trunk??? ¿o es un trunk??? entonces el modo automático crea el trunk con el switch de vecindad. Esto sucede cuando el puerto de vecindad se fija a encendido o desirable mode.
- ¿Deseable??? El desirable mode indica al switch de vecindad que es puede ser un troncal ISL y que como el switch de vecindad también sería un troncal ISL. El puerto se convierte en un puerto trunk si el puerto vecino está en modo encendido, deseable o automático.
- ¿En??? Encendido el modo habilita automáticamente la conexión troncal de ISL en su puerto, sin importar el estado de su switch de vecindad. Sigue siendo un troncal ISL, a menos que reciba un paquete ISL que inhabilite explícitamente el troncal ISL.
- ¿Nonegocie??? ¿El modo de no negociación habilita automáticamente la conexión troncal de ISL en su puerto??? ¿sin importar el estado de su switch de vecindad??? pero no permite que el puerto genere las tramas DTP.
- ¿De??? En el modo desconectado, el ISL no se permite en este puerto sin importar el modo DTP que se configura en el otro Switch.

El Catalyst 5000 Family del Switches se utiliza típicamente para proporcionar la estructura básica de ISL. El Catalyst 3900 Switch se puede entonces conectar con esta estructura básica vía el

módulo de extensión dual del 100 Mbps ISL. El Catalyst 3900 Token Ring Switch no soporta ningún otro modo que el ISL, así que es siempre trunked. También, los módulos ISL del Catalyst 3900 soportan solamente las conexiones del 100 Mbps y omiten por completo - el duplex.

Tenga muy cuidado cuando usted conecta un Catalyst 3900 y un Catalyst 5000 Switch vía el link ISL. El problema principal es que el Catalyst 3900 no soporta la negociación de medios de los fast ethernet. Por este motivo, si el Catalyst 5000 se configura para el modo automático, después omite el 100 Mbps semidúplex. Esto causa los problemas como el puerto que va del trunk al NON-trunk y a la pérdida del paquete.

Si usted quiere asociar el puerto del Catalyst 3900 ISL al puerto ISL de un Catalyst 5000, usted debe configurar manualmente el puerto ISL en el Catalyst 5000:

1. Publique el **comando set port speed** de fijar al 100 Mbps:
   set port speed *mod/port* **{4 | 10 | 16 | 100 | auto}**
2. Publique el **comando set port duplex** de fijar por completo - al duplex:
   set port duplex *mod/port* **{full | half}**

Si usted quiere forzar el puerto de un Switch al modo tronco, publique el **comando set trunk** (en una línea):

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

En el comando anterior, el *vlans* es un valor a partir de la 1 hasta el 1005 (por ejemplo, de **2-10** o de **1005**) y el *trunk_type* se fija al **isl**, **dot1q**, **dot10**, **carril**, o **negocie**.

Una vez que los puertos troncales son activos en el Switches, usted puede publicar el **comando show trunk** de ver que estos puertos trunked son activos.

```
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 de utilizar para observar los troncales ISL es el **comando show cdp neighbors detail**. Este comando también le ayuda a entender la topología de red.

```
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
```

De esa salida, usted puede ver claramente que un Catalyst 3900 está conectado con el puerto 10/1. Cuando usted examina el puerto 10/1 en la salida del **comando show trunk** anterior, usted puede decir que es un puerto troncal.

Spanning-tree

El Spanning-tree en los entornos Token Ring puede conseguir muy complicado porque uno puede funcionar con simultáneamente un total de tres diversos protocolos del Spanning-tree. Por ejemplo, un árbol de expansión IBM típico de los funcionamientos del entorno en el nivel y los funcionamientos IEEE (802.1d) del TrBRF o Cisco en el TrCRF llano. Por lo tanto, el Spanning-tree es un poco más complicado resolver problemas.

Esta tabla le dice qué sucede basado en los diversos tipos de configuraciones posibles:

Bridging Mode del TrCRF	TrCRF	TrBRF
SRB	Funciona con el árbol de expansión IEEE.	Se realiza como Source-Route Bridge.
	Unidades del protocolo IBM Spanning-Tree de los procesos (BPDU) de los Bridge externo.	Funciona con los protocolos IBM Spanning-Tree a los Bridge externo.
		Cae el IEEE Spanning-Tree Protocol transparente BPDU

		del TrCRF.
SRT	Funciona con el protocolo del Cisco SPANNING-TREE.	Se realiza como Bridge de la ruta de origen transparente.
	Direccionamiento del Grupo de Bridge de los reemplaces del campo dirección de destino con un grupo de dirección del Cisco específico, de modo que los Bridge externo no analicen el TrCRF BPDU.	Adelante transparente y tráfico de Source Route.
	Genere los BPDU, con el conjunto de bits RIF en el campo de dirección de origen en la trama de salida y el byte RIF del a2 agregados. Este formato de trama se asegura de que TrCRF siga siendo local al anillo lógico y es transparente no interligado o Source Routed a otros LAN. Solamente el TrCRFs conectado vía los loopes físicos recibe los BPDU.	Adelante tráfico de Source Route al resto del TrCRFs en el TrBRF, si estén en el SRT o el modo SRB.
	Árbol de expansión IEEE de proceso BPDU de los Bridge externo.	

Para más información, refiera al Spanning-Tree Protocol en los VLAN Token Ring y los protocolos relacionados.

VLAN Trunking Protocol

Porque, con el ISL, el VLA N determina donde un paquete debe ir, es importante que cada Switch sabe sobre los VLA N en la red. ¿VTP??? el propósito s en la vida es propagar la información de VLAN a través del Switches. El VTP no se ejecuta en el Routers, porque él debe terminar la red VLAN. Cada Switch en la red debe ejecutar el VTP. Si no, entonces el Switch ejecuta generalmente solamente un VLA N (generalmente el VLA N 1) y no ejecutaría el ISL en ese link, porque no hay necesidad. El VTP hace la creación de los VLA N una tarea mucho más fácil, porque usted podría configurar los VLA N en un Switch y propagarían a través de la red. Por supuesto, eso viene con los problemas.

El VTP no es un sistema robusto, como el Enhanced Interior Gateway Routing Protocol (EIGRP) o el Routing Protocol del Open Shortest Path First (OSPF). Es mucho más simple y actúa encendido un concepto muy importante: revisiones. En el VTP, hay tres tipos de dispositivos VTP: clientes, servidores, y dispositivos transparentes. Los dispositivos VTP cliente básicamente apenas validan la información de VLAN de los dispositivos del servidor y no pueden modificar esta información. Los servidores, sin embargo, pueden modificar la información VTP en los servidores VTP uces de los. Por este motivo, el VTP tiene un sistema de revisión. Cualquier servidor VTP que modifique o pone al día la base de datos de VLAN demanda que es la última revisión. ¿Por este motivo, la precaución extrema debe ser utilizada, porque el Switch con la más

reciente revisión lo va a hacer??? ¿triunfo??? y su información de VLAN será la válida. Por ejemplo, si usted modifica a un servidor VTP para decir que el VLAN 100 del TrBRF va a hacer el árbol de expansión IEEE, esto haría el estrago entre todo el Switches, porque podría hacer el Switches (como el Catalyst 3900) poner los puertos en el modo de bloqueo, para protegerse contra los loopes. También, tenga cuidado cuando usted introduce los nuevos cambios en la red, porque podrían tener revisiones VTP mayores. En el modo transparente, los paquetes VTP recibidos en un trunk se propagan automáticamente, sin los cambios, al resto de los trunks en el dispositivo; pero, se ignoran en el dispositivo sí mismo.

Cuando usted configura el VTP con los switches de red Token Ring, usted debe ejecutar VTP V2. Si usted va a tener Switches que ejecute los Ethernetes y los VLAN Token Ring, después usted debe actualizar el VTP, incluso para las redes Ethernet VLAN. Usted *no puede* tener dos diversos dominios VTP (por ejemplo, usted no puede tener uno para los Ethernetes y uno para el Token Ring).

Para más información, refiera al protocolo VLAN trunking en los VLAN Token Ring y los protocolos relacionados.

Recorte VTP

Un problema con el VLAN Trunking es que la información del broadcast a partir de un VLA N propaga a través de todos los trunks, porque el Switches no sabe qué VLA N existen en un switch remoto. El recorte VTP fue creado por este motivo. Permite que el Switches negocie qué VLA N se asignan a los puertos en el otro extremo de un trunk y, por lo tanto, podar los VLA N que no se asignan remotamente. La poda se inhabilita por abandono en el Switches del Catalyst 3900 y Catalyst 5000.

Nota: El recorte VTP se soporta en el Catalyst 3900 Switch en la versión 4.1(1).

Cada uno de los mensajes del recorte VTP contiene la información sobre los VLA N en la pregunta y contiene un bit que indique independientemente de si este VLA N se debe podar para este trunk (el a1 indica que no debe ser podado). ¿Con la poda habilitada, el tráfico VLAN no se envía normalmente a través del link de troncal, a menos que el link de troncal reciba un mensaje de incorporación apropiado con el VLAN correspondiente??? s mordido habilitado. Esto es muy importante porque le dice eso, cuando usted utiliza el recorte VTP, usted debe aseegurarse que existe la información y la configuración correctas y que todo el Switches está ejecutando la poda; si un Switch no envía los mensajes de incorporación a otro Switch a través del trunk, podría conseguir apagado para un VLAN determinado o los VLA N. Cuando la negociación de la poda es completa, el VLA N acabará en la pasa o el estado unido para ese trunk.

Una característica muy importante de recorte VTP permite que usted configure un VLA N para ser poda elegible o no. Esta característica dice el Switches que está funcionando con el recorte VTP para no podar este VLA N. Cuando usted habilita el recorte VTP, los VLA N 2 a 1000 son VLA N elegibles de la poda por abandono. Así pues, cuando usted gira la poda, afecta a todos los VLA N por abandono. El VLAN1, el TrCRF predeterminado (1003), el TrBRF predeterminado (1005), y el TrCRFs son siempre poda-inelegibles; por lo tanto, el tráfico de estos VLA N no puede ser podado.

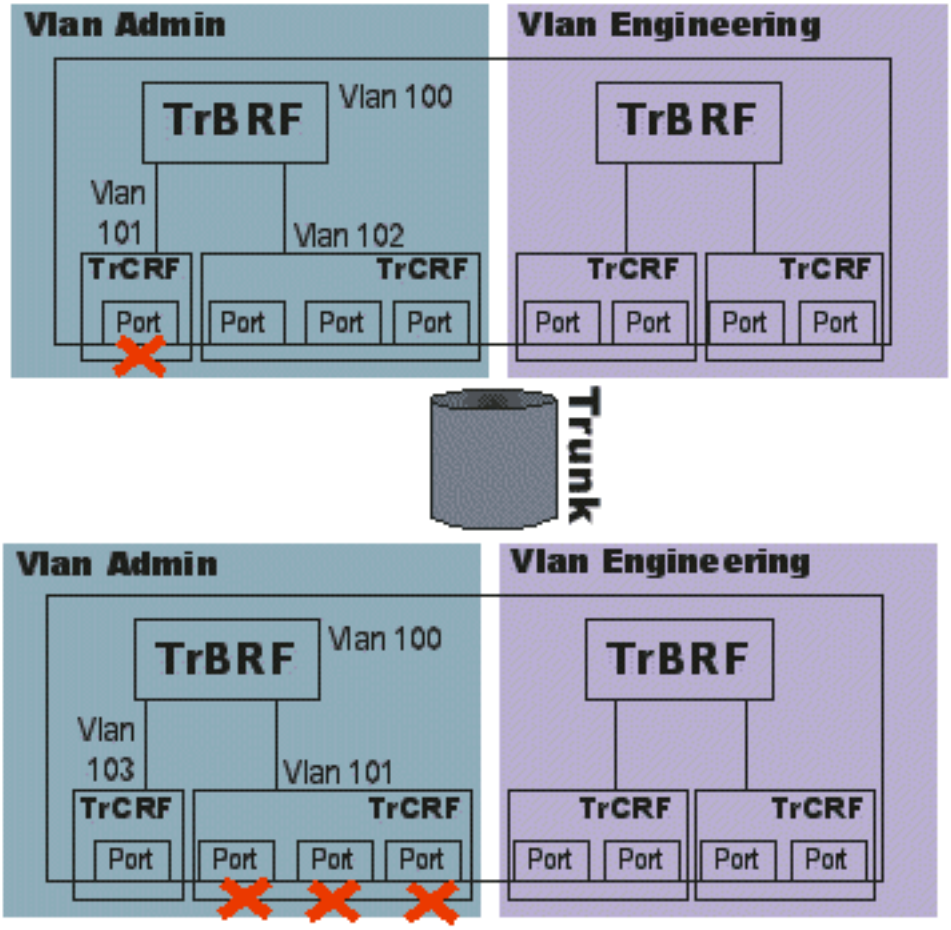
Para más información, refiera al recorte VTP en comprensión del Token Ring Switching.

Duplicate Ring Protocol

El Duplicate Ring Protocol se diseña para ejecutarse en el Switches que ejecuta los VLAN Token Ring. Su trabajo es asegurar la configuración correcta de la red VLAN en anillo y crear la reducción del explorador. El DRiP utiliza el VTP para sincronizar su información de la base de datos de VLAN, pero no se requiere para que el DRiP trabaje (la base de datos de VLAN se puede establecer manualmente). Una idea falsa es que el DRiP entiende los números de anillo; esto no es verdad. El DRiP confía en la unicidad de los VLA N configurados en una red y esa configuración de la base de datos de VLAN.

Una de las características más importantes del DRiP es aplicar la distribución TrCRF. En el mundo del Token Ring, es muy peligroso distribuir cualquier VLA N con excepción de 1003, debido a los problemas de expansión. Por este motivo, si un TrCRF con excepción del VLA N 1003 se distribuye, todos los puertos a las cuales ese VLA N es asociado son inhabilitados por el DRiP.

Este ejemplo ilustra este concepto:



En ese ejemplo, dos diverso Switches tiene un puerto que se asigne al VLAN 101. El Switch, vía el DRiP, mueve el atravesar-árbol del puerto para inhabilitar y para el tráfico de reenvío. Esto salvaguarda el Switch contra una condición de Loop posible.

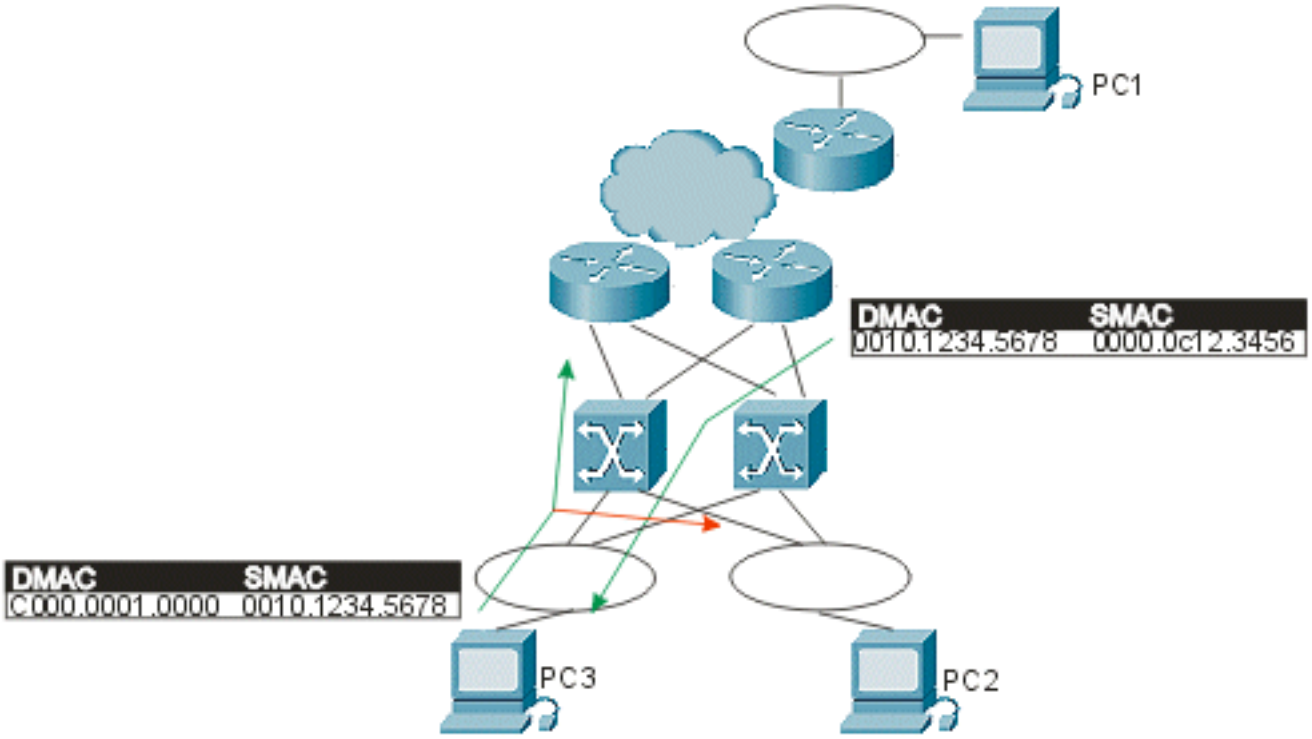
Si no hay cambio, el DRiP hace publicidad del estado TrCRF a todos sus puertos troncales cada 30 segundos. Ningunos cambian hecho con el CLI (interfaz de línea de comando) o el SNMP enviaría inmediatamente una actualización a todos los puertos. Estos anuncios son tramas del tipo 0 ISL y fluyen en el VLAN predeterminado 1. Porque el DRiP hace publicidad solamente de sus efectos para los VLA N, es importante que la información de VLAN correcta existe en el Switches que está conectado vía el ISL. Esto se hace vía el VTP. Si se inhabilita el VTP, después esta función se debe mantener manualmente a través de todo el Switches que comparta los mismos VLA N. Los anuncios del DRiP existen solamente en los links ISL. No existen en la

atmósfera, el Token Ring, los Ethernetes, o el FDDI. No hay árboles de topología mantenidos el DRiP.

Para más información, refiera al Duplicate Ring Protocol en los VLAN Token Ring y la guía de los protocolos relacionados.

HSRP y VLAN Token Ring

Uno de los problemas más grandes con el HSRP es el uso de la dirección Multicast en la red. Porque nadie en de la red las generas paquetes realmente con esta dirección MAC virtual, el Switches nunca aprende estas direcciones MAC. Por lo tanto, ellas tramas de inundación en la red. Debido a esto, el uso de la función **espera uso-BIA del** HSRP fue requerido para enviar los paquetes que utilizaron el Burned-In MAC Address de la interfaz del router HSRP activo. El problema principal con este escenario es que, cuando el Switch de los routers del HSRP, ellos tendría que enviar un protocolo Protocolo de resolución de la dirección (ARP) del broadcast (ARP; ARP gratuito) a todas las estaciones en el alambre, de modo que las estaciones aprendan la nueva dirección MAC del gateway. Aunque este proceso debe trabajar basado en las especificaciones IP, ha habido algunos problemas conocidos con él. Debido a las peticiones continuas del campo, el HSRP fue cambiado de modo que usted pueda tener la dirección Multicast y también poder utilizar el HSRP sin el uso-**BIA espera**. Este cambio fue implementado en CSCdk55937 y liberado en el Cisco IOS Software Release 11.3(7) y 12.0(3) y posterior.



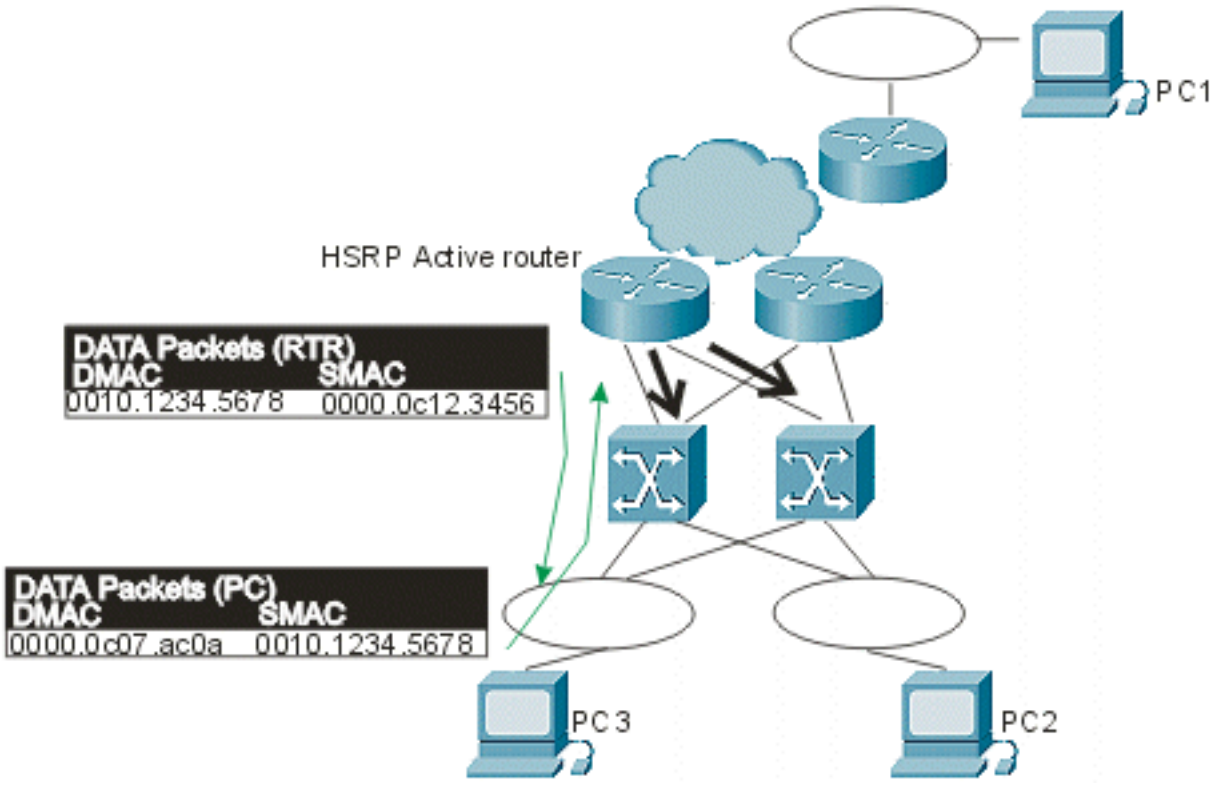
En el diagrama anterior, la comunicación está ocurriendo entre el PC1 y el PC3. El problema es que el tráfico IP del cliente al router predeterminado en esta imagen utiliza a una dirección de destino de Multicast. Porque puede nadie fuente este paquete de ese direccionamiento, el Switches nunca aprende este direccionamiento e inunda siempre los paquetes. El DMAC tradicional que depende de los grupos es C000.000X.0000, que puede nunca ser un S AC en el Token Ring. Tan todos los paquetes destinados del PC3 al PC1 vía el default gateway ahora son vistos por el PC2. En una red con muchos Bridges, esto puede multiplicarse muy rápidamente y causar qué parecerían como las tormentas de broadcast pero cuál está realmente una gran cantidad de tráfico Multicast.

Para superar este problema, usted debe utilizar una dirección MAC que se pueda utilizar realmente como S AC por el Routers en el hellos del HSRP. Esto permite que el Switches aprenda este direccionamiento y, por lo tanto, conmute los paquetes apropiadamente. Para hacer esto, configure una nueva dirección MAC virtual en el Routers. Los clientes necesitan enviar los paquetes al DMAC de esta nueva dirección virtual. Ésta es salida de ejemplo de 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
```

En esa salida, se ha creado un grupo en espera 10 (IP espera 1.1.1.100). La dirección MAC (`0000.0c07.ac0a`) es la nueva dirección MAC virtual y el byte más reciente es el grupo (0xA = 10). Una vez que usted tiene esta nueva configuración, usted ahora tendría este patrón de tráfico, que evita las inundaciones de tráfico:



Ahora, porque el router es paquetes de la compra de componentes con el DMAC del MAC virtual HSRP, el Switches aprende esta dirección MAC y remite solamente los paquetes al router HSRP activo. Si el router HSRP activo falla y va el recurso seguro active, el nuevo router activo comenzará a enviar el hellos del HSRP con el mismo S AC, que hace las tablas de la dirección MAC del Switch cambiar sus entradas aprendidas al nuevos puerto del switch y trunk.

Debido a multiring, la operación adicional necesita tomar el efecto para asegurarse de que el RIF cambia realmente durante la transición (aunque es la misma dirección MAC). Multiring es la capacidad del router para asociar un RIF a una dirección MAC, apenas como una estación terminal. El Routers necesita multiring en los entornos donde existen los Bridges SRB, de modo que los paquetes puedan atravesarlos para alcanzar las estaciones terminales.

En el mismo ejemplo que antes, usted puede ver los pasos adicionales requeridos para que el cliente conecte con el nuevo router HSRP activo:

1. El router activo para el trabajar.
2. Una vez que el router en espera detecta la pérdida de saludos de HSRP, inicia el proceso para sentir bien al router HSRP activo.
3. El router envía un ARP gratuito del mismo S AC que antes, en de las capas MAC y en la capa ARP.
4. El PC ahora envía la trama destinada a la misma dirección MAC, pero con el nuevo RIF.
5. Una vez que el router recibe esta trama (destinada al HSRP MAC), envía un pedido ARP al cliente directamente, porque no tiene la dirección MAC de ese cliente en su tabla ARP.
6. La respuesta al paquete ARP se recibe una vez, el router puede enviar los paquetes al cliente de destino.

Información Relacionada

- Comprensión del Token Ring Switching
- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems