Conceptos de Switching Token Ring

Contenido

Introducción

Para empezar a entender los conceptos de conmutación Token Ring, es muy importante que entienda el bridging transparente, el bridging de ruta de origen y el árbol de expansión. El Catalyst 3900 y el Catalyst 5000 utilizan nuevos conceptos, como se describe en el IEEE 802.5 anexo K. Estos conceptos son los bloques de creación para las VLAN Token Ring. Este documento explica los diferentes conceptos de conexión en puente y cómo funcionan:

- Enlace troncal entre switches (ISL)
- spanning-tree
- Protocolo de enlace troncal VLAN (VTP)
- Protocolo de anillo duplicado (DRiP)

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

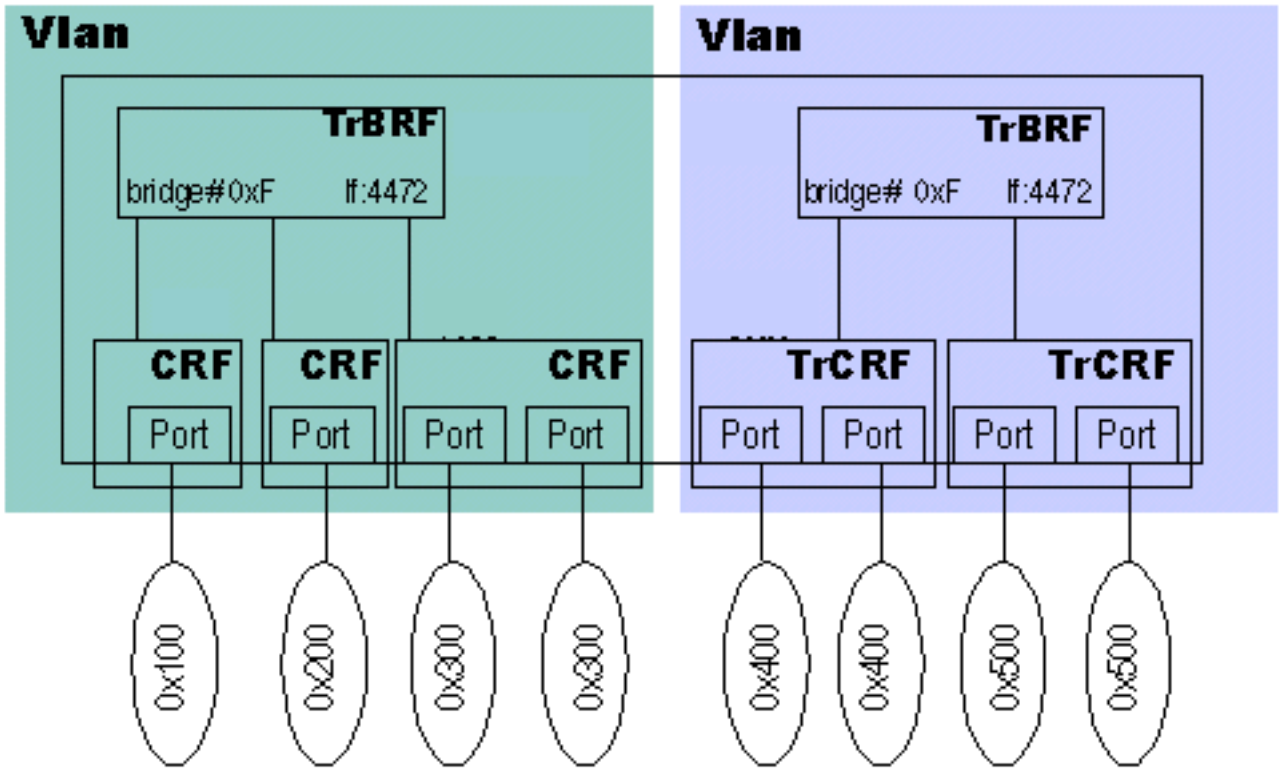
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

TrBRF y TrCRF

La función de retransmisión de puente Token Ring (TrBRF) y la función de retransmisión de concentrador Token Ring (TrCRF) son los bloques de creación de la arquitectura de la funcionalidad Catalyst 3900 y Catalyst 5000. TrBRF es simplemente la función de puente del switch, y TrCRF es la función de concentrador del switch. Es importante entender que el bridging ocurre en ambas capas porque, en Token Ring, se discutirán tres tipos diferentes de bridging.

La funcionalidad TrBRF del switch controla el switching del tráfico puenteado de ruta de origen, como el puente de ruta de origen (SRB) y el puente transparente de ruta de origen (SRT). El TrCRF cubre la funcionalidad de switching de ruta de origen (SRS) y conexión en puente transparente (TB). Por ejemplo, es posible tener un switch Catalyst 3900 que sólo tenga un TrBRF y un TrCRF y todos los puertos del switch estén en el mismo TrCRF. Esto hace que el switch sólo pueda hacer SRS y TB. Si definió diez TrCRF diferentes bajo el mismo TrBRF primario, entonces el tráfico de los puertos que están conectados al mismo TrCRF se reenviaría a través de la funcionalidad TrCRF de SRS o TB. El tráfico que se dirige a los otros TrCRF en el switch utilizaría la funcionalidad TrBRF del switch y se puentearía con puente de ruta de origen o con puente transparente de ruta de origen. Los diferentes mecanismos de conmutación se discutirán más adelante en este documento.

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



Puede ver que cada TrCRF está conectado a un anillo específico. Un TrCRF puede comprometer varios puertos y estos puertos comprometerían el mismo número de anillo. El TrBRF conecta los TrCRFs.

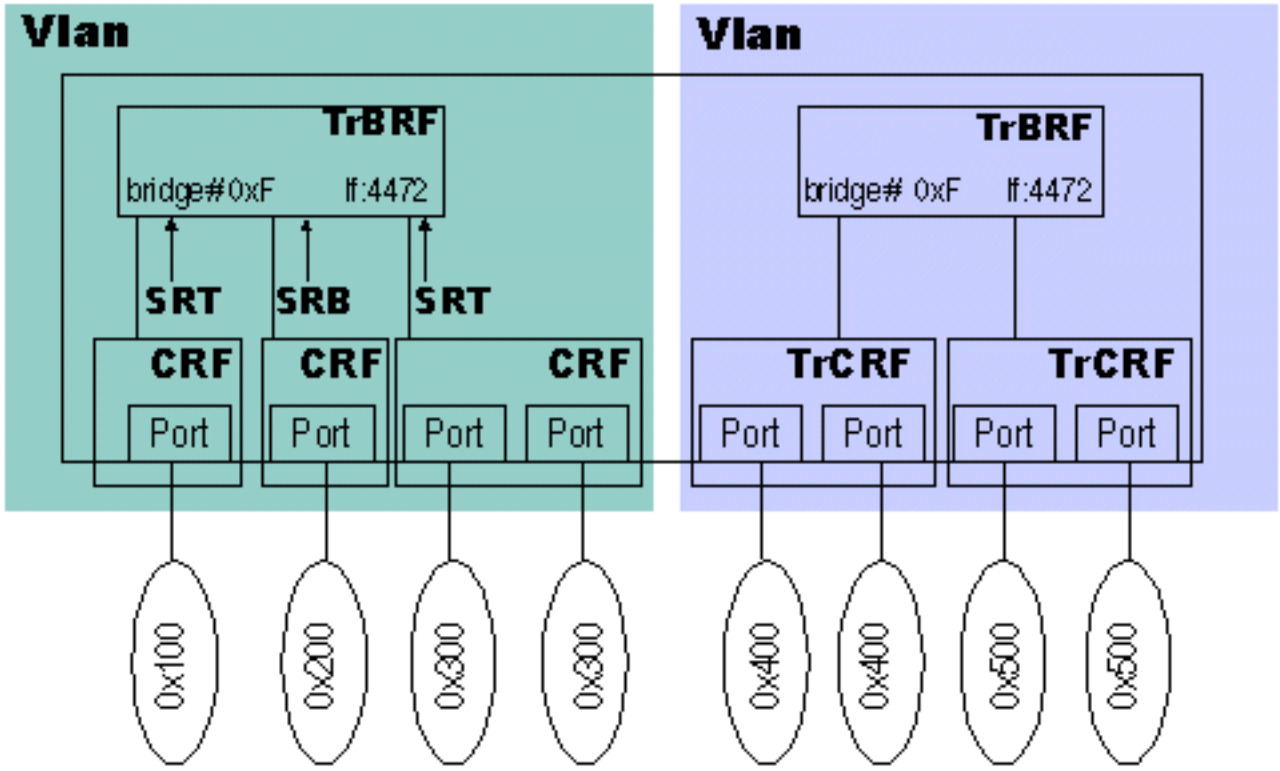
Un TrCRF y un TrBRF en sí mismos es una VLAN diferente. Por lo tanto, en Token Ring, puede establecer un puente entre las VLAN. El puente entre las VLAN Token Ring sigue dos reglas:

- La conexión en puente entre dos VLAN TrBRF sólo puede realizarse mediante un dispositivo externo, como un router o un Módulo de switch de ruta (RSM).
- El puente entre las VLAN TrCRF sólo se puede lograr con las VLAN TrCRF que son hijos de la misma VLAN TrBRF primaria.

Esto es muy importante para tener en cuenta para las VLANs Token Ring, porque rompe el paradigma Ethernet. En resumen, lo que parece una VLAN Ethernet es la suma de un TrBRF y sus hijos TrCRF. Debido a que puede establecer un puente entre ciertas VLAN en Token Ring, debe entender cómo ocurre este puente.

Nota: Para facilitar la comprensión de las VLAN Token Ring en relación con las VLAN Ethernet, recuerde que la combinación de TrCRF y TrBRF hace una VLAN en sí misma.

En este diagrama, puede ver que el TrCRF decide el modo de conexión en puente entre el TrCRF y el TrBRF.



Los TrCRF individuales han configurado qué tipo de conexión en puente le estarán haciendo al TrBRF. Esto es importante porque puede tener VLAN TrCRF que hagan el bridging de ruta de origen a otros TrCRFs pero no hagan tramas no ruteadas de origen. 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 TrCRF, pero SRT sólo puede fluir entre los dos que están en modo SRT. Esto le permite establecer de forma granular cómo debe fluir el tráfico entre los TrCRF. Si el modo de conexión en puente se configuró en el TrBRF, afectaría a todos los hijos de TrCRF de esa VLAN.

Modos de Switching

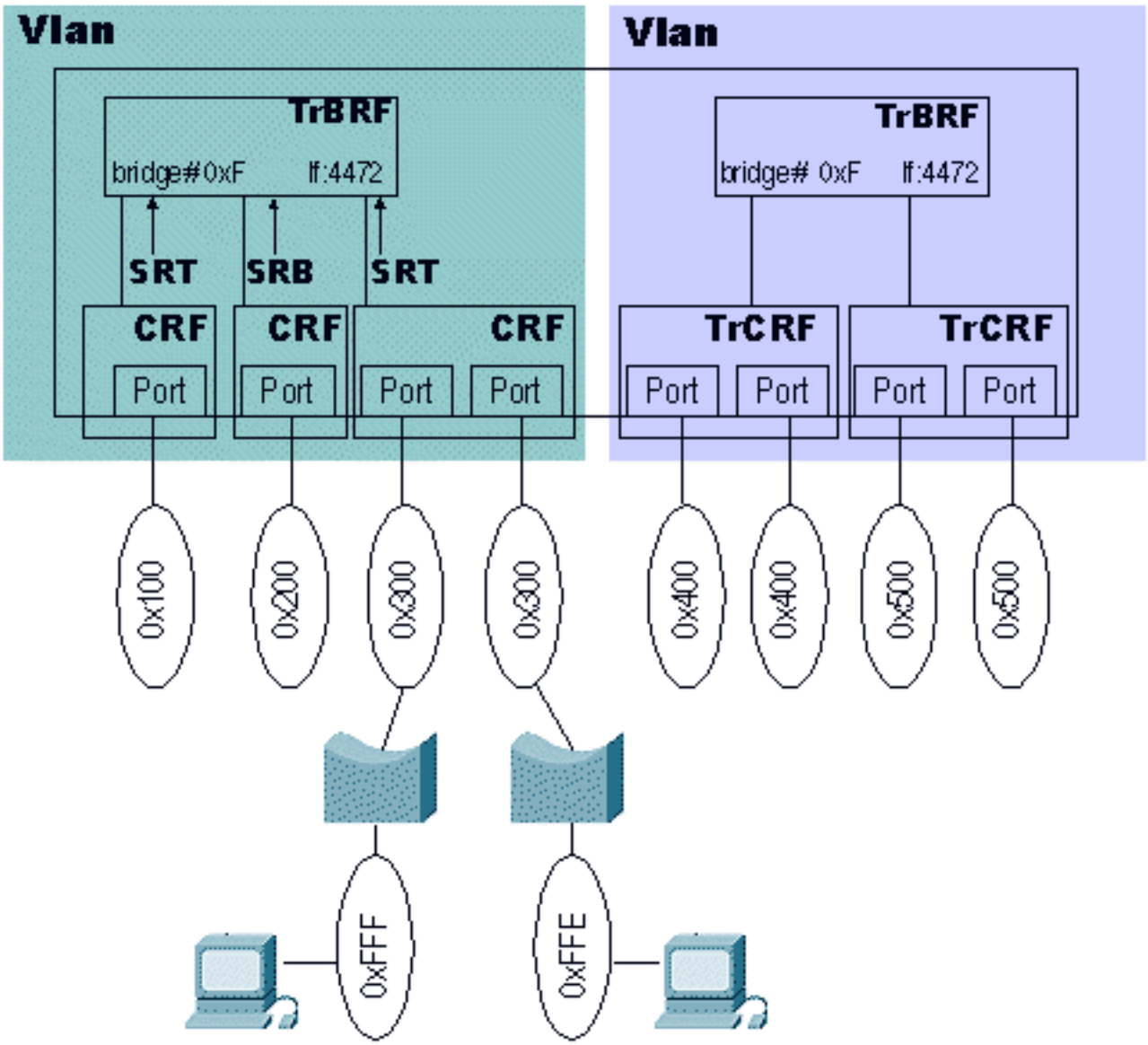
De forma inmediata, el Catalyst 3900 se configura con un TrBRF y un TrCRF. Todos los puertos se asignan a la VLAN 1003 TrCRF predeterminada. Lo mismo se aplica al servidor blade Catalyst 5000 Token Ring. Esto es importante porque le da a la caja seguridad ???plug-and-play???? funcionalidad. De forma inmediata, estos switches pueden realizar el reenvío en función del switching de ruta de origen y el bridging transparente. En las secciones siguientes se proporcionan detalles sobre estas tecnologías.

Uso de puente transparente

Transparent Bridging es el más básico de todos los mecanismos de switching y se basa en la dirección MAC de destino (DMAC) de las tramas de la red. Este es el mecanismo de reenvío de las redes Ethernet. Cada vez que un switch recibe una trama, registra la dirección MAC de origen (SMAC) de la trama como una que pertenece a ese puerto y, en lo sucesivo, reenvía el tráfico destinado a esa MAC a ese puerto. Si, en el proceso de aprendizaje, un switch no conoce una dirección MAC, inundará ese paquete en todos los puertos en estado de reenvío.

Source-Route Switching

El switching de ruta de origen es un mecanismo de reenvío que se necesita cuando sólo hay un TrCRF asignado a los puertos y el switch recibe paquetes con campos de información de routing (RIF) en ellos. Debido a que el switch no modificará el RIF de la trama (porque no lo pasará al TrBRF), la red debe ser capaz de tomar decisiones sobre el reenvío, con el RIF, sin modificaciones. Considere este diagrama de red que muestra SRS:



El tráfico que va del anillo 0xFFF al anillo 0xFFE debe atravesar el switch. Este tráfico sería tráfico de puente de ruta de origen. Esta es la secuencia de inicio de la comunicación entre estos dos clientes:

1. Una estación envía un paquete del explorador al anillo en el que reside. Suponga que el cliente en el anillo 0xFFF envía el paquete; se ve algo así (en hexadecimal):
   `0000 00c1 2345 8000 0c11 1111 C270`
   Nota: Esa información del paquete sólo muestra información de DMAC, SMAC y RIF.
2. Una vez que el paquete alcanza el bridge de ruta de origen y reenvía la trama al cable, el paquete tiene el siguiente aspecto:
   `0000 00C1 2345 8000 0c11 1111 C670 FFF1 3000`
   `C670` es el campo de control de ruteo y `FFF1 3000` es el anillo 0xFFF, bridge 0x1, ring 0x300.
3. Ahora, el paquete llega al switch. Debido a que el switch ve el paquete proveniente de un anillo lejano, aprende el descriptor de ruta. En este caso, el switch ahora sabe que el anillo 0xFFF a través del puente 0x1 está ubicado en el puerto 3.
4. Debido a que el paquete es un paquete del explorador, el switch reenvía la trama a todos los puertos bajo el mismo TrCRF. Si el explorador necesita ir a puertos en diferentes TrCRF, entregará la trama al TrBRF, que hará su funcionalidad de puente. Si hay puertos en el mismo TrCRF, reenviará la trama saliente sin modificación.
5. La estación en el anillo 0xFFE debe obtener el explorador y responder a él. Suponga que el

cliente responde con una trama dirigida. Esta trama dirigida tiene el siguiente aspecto:
`0000 0C11 1111 8000 00C1 2345 08E0 FFF1 3001 FFE0`
`08E0` es el campo de control de ruteo y `FFF1 3001 FFE0` es timbre 0xFFF, puente 0x1, anillo 0x300, puente 0x1, anillo 0xFFE.

6. Finalmente, el switch se entera de que el anillo 0xFFE se encuentra en el puerto 4 y mantiene el descriptor de ruta.

A partir de ahora, el switch sabe de esos anillos. Si observa las tablas, debe ver que el switch ha aprendido sobre el número de puente y el número de anillo. Los demás anillos después del anillo 0xFFF y del anillo 0xFFE no son necesarios, ya que deben pasar a través del anillo 0xFFF o del anillo 0xFFE para alcanzar el switch.

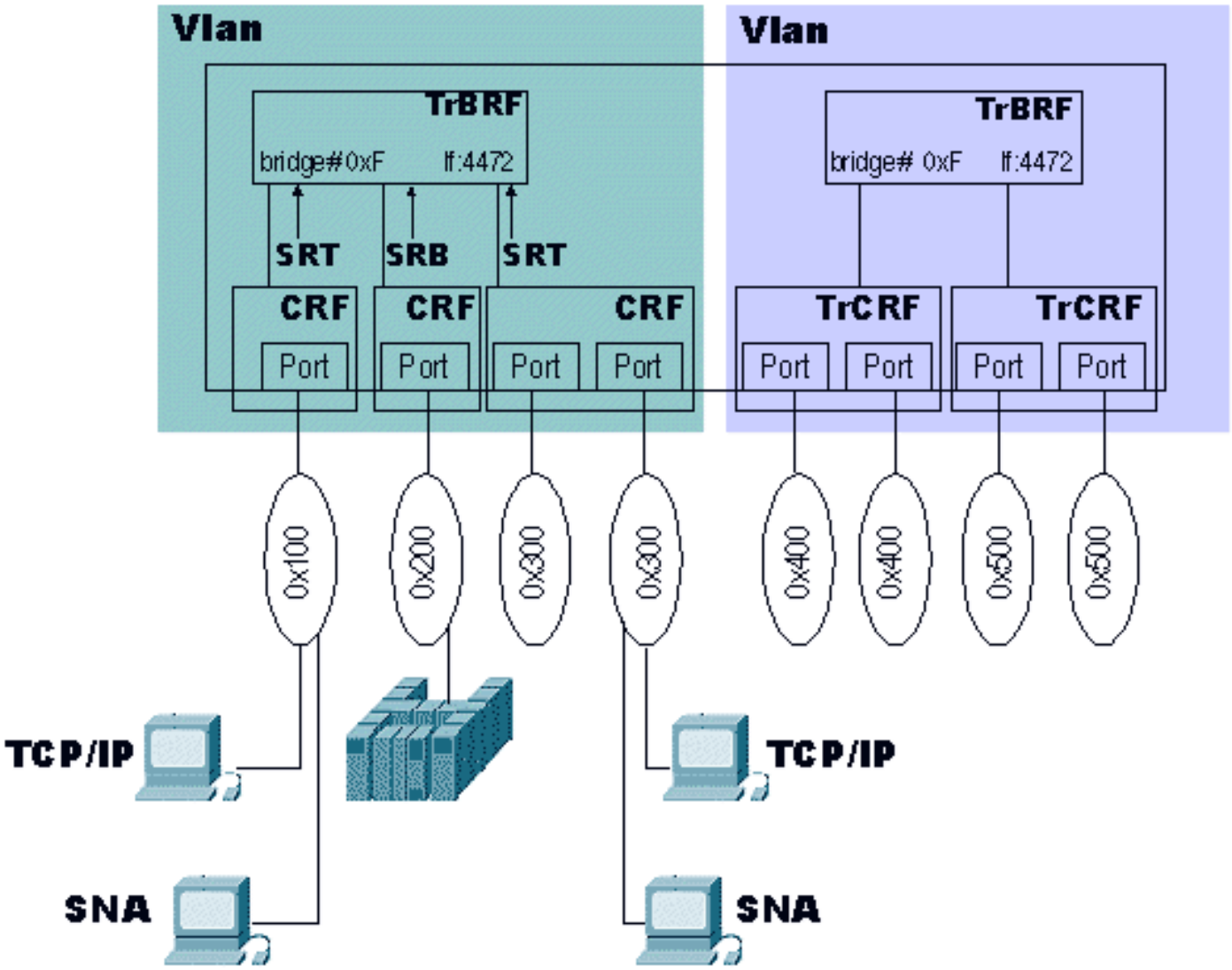
SRS es un reenvío básico de paquetes basados en RIF sin funcionalidad SRB, como ocurre con el TrCRF.

Nota: Para ver la tabla de información de ruteo en el Catalyst 5000, ejecute el comando **show rif**.

Source-Route Bridging y Source-Route Transparente

Toda la funcionalidad de puente de ruta de origen se encuentra en la lógica TrBRF. El TrCRF es el que va a ordenar el modo de conexión en puente al TrBRF. Por lo tanto, si el TrCRF se configura para el modo SRB en el TrBRF entonces, cuando el TrCRF recibe una trama NSR (no enrutada por origen), el switch no la reenviará a la lógica TrBRF.

Esto se puede utilizar si no desea que ciertos tipos de tráfico lleguen o salgan de un anillo específico. Este diagrama muestra un ejemplo:



Si los clientes TCP/IP no tenían la capacidad de enviar paquetes con RIF, el switch no colocaría esas tramas en el mismo anillo con el mainframe (0x200). Sin embargo, las tramas SNA al host (que normalmente tienen un RIF) llegarían al mainframe. Esta es una manera muy rudimentaria de filtrar tramas en una red conmutada.

Esta es la secuencia que el switch sigue para reenviar una trama puenteada de ruta de origen a través del TrBRF:

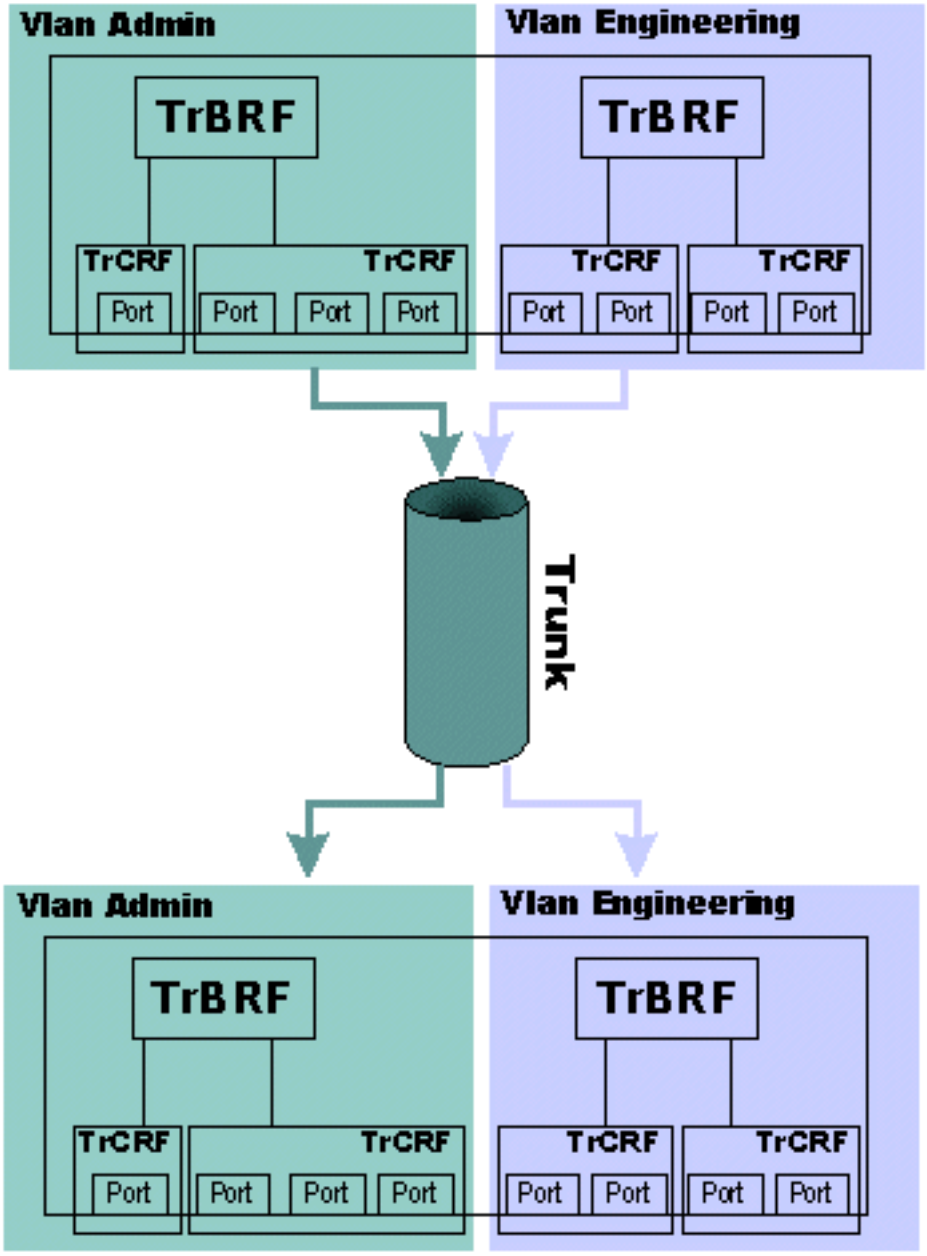
1. La estación SNA en el anillo 0x300 (puerto 4) envía un explorador para alcanzar el mainframe.
2. Cuando el paquete del explorador llega al switch, reenvía el explorador, sin modificación, en el mismo TrCRF; luego envía una copia al TrBRF para reenviarla al resto de los TrCRF. En este caso, debido a que el paquete tiene un RIF, pasa a través del trayecto SRB. El switch también necesita aprender la ruta.
3. El switch va a aprender el SMAC de la trama, porque el paquete se muestra como originado en el anillo local al que está conectado el switch. Esto se debe a que, en una combinación TrCRF de varios puertos, el RIF muestra el anillo de destino, pero el switch necesita saber qué puerto en el TrCRF. Por lo tanto, el switch aprende el SMAC de las tramas que ingresan en el nivel TrCRF.
4. El paquete sale a todos los demás TrCRF, modificados con sus respectivas combinaciones de números de anillo de puente.
5. Una vez que el host responde con la trama SRB, el switch aprende el SMAC del host para

ese TrCRF y lo envía al puerto de salida. El tráfico entonces fluye de ida y vuelta entre los dos.

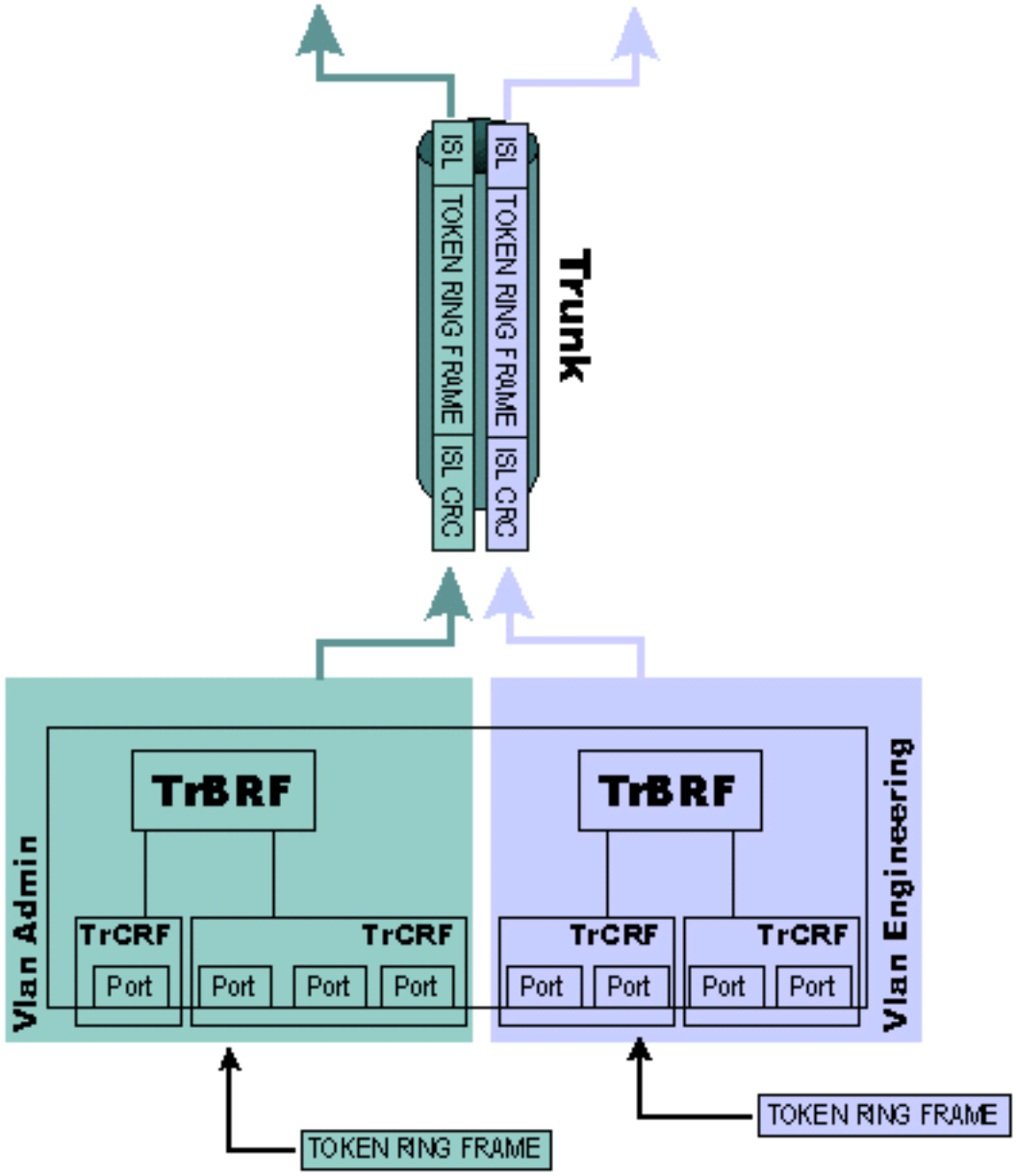
Nota: Para verificar la tabla de direcciones MAC en el Catalyst 5000, ejecute el **comando show cam**.

Inter-Switch Link

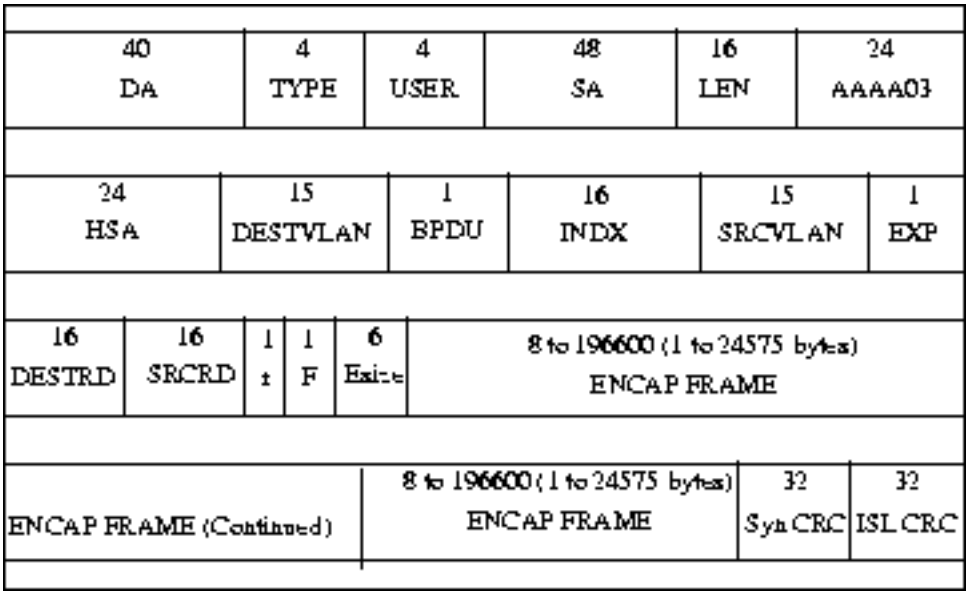
Inter-Switch Link es un protocolo muy simple. Básicamente, las tramas que atraviesan un tronco ISL se encapsulan en una trama ISL que indica al otro lado a qué VLAN pertenecen las tramas. Debido a esto, la información de VLAN se debe compartir de forma manual o automática entre los switches. Un protocolo conocido como VLAN Trunking Protocol (VTP) puede manejar esta tarea. Para las VLAN Token Ring, debe ejecutar VTP V2 en la red. Considere este diagrama:



En este caso, se ha creado un único tronco ISL para transportar, por sí mismo, las VLAN de ingeniería y las VLAN de administración. Ninguno del tráfico en ninguna de las VLAN se mezcla después de pasar por el tronco. Este diagrama muestra cómo se logra esta separación:



Cada trama de esas VLAN que necesita atravesar el tronco se encapsula en una trama ISL y su VLAN se incluye en la trama. Esto permite al switch receptor rutear correctamente la trama a su VLAN específica. La trama ISL Token Ring (TRISL) tiene unos pocos campos más que una trama ISL normal. Este diagrama muestra el diseño de una trama TRISL:



Nota: Aunque TRISL se ejecuta sobre interfaces Fast Ethernet, los paquetes contienen una trama estándar Token Ring y la información de VLAN asociada con esa trama, en cierta medida. Las VLAN Token Ring permiten hasta 18k tamaños de trama, al igual que ISL. Esto *no* se logra mediante la fragmentación del marco. La trama completa se encapsula en una trama ISL en toda una pieza y se envía a través del link. Hay un concepto erróneo común de que ISL es Ethernet y que su tamaño máximo de trama es de 1500 bytes.

En Catalyst 5000, un protocolo conocido como protocolo de enlace troncal dinámico (DTP) estuvo 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. La función de DISL?? es negociar, sólo para ISL, si un link entre dos dispositivos debe ser trunking o no. DTP puede negociar el tipo de encapsulación de troncal que se utilizará entre ISL y los troncales VLAN IEEE 802.1Q. Se trata de una función interesante, ya que algunos dispositivos de Cisco sólo admiten ISL o 802.1Q, mientras que otros pueden ejecutar ambos.

Estos son los cinco estados diferentes para los que puede configurar DTP:

- Auto - En el modo Auto, el puerto escucha las tramas DTP del switch vecino. Si el switch vecino indica que le gustaría ser un tronco - o un tronco - entonces el modo automático crea el tronco con el switch vecino. Esto sucede cuando el puerto vecino está configurado en el modo On o Desirable.
- Deseable - El modo Deseable indica al switch vecino que puede ser un trunk ISL y que le gustaría que el switch vecino también fuera un trunk ISL. El puerto se convierte en un puerto trunk si el puerto vecino está en modo encendido, deseable o automático.
- On - El modo On habilita automáticamente el trunking ISL en su puerto, independientemente del estado de su switch vecino. Sigue siendo un tronco ISL, a menos que reciba un paquete ISL que inhabilita explícitamente el troncal ISL.
- Nonegotiate - El modo Nonegotiate habilita automáticamente el trunking ISL en su puerto - independientemente del estado de su switch vecino - pero no permite que el puerto genere tramas DTP.
- Off - En el modo Off, ISL no está permitido en este puerto independientemente del modo DTP configurado en el otro switch.

La familia de switches Catalyst 5000 se utiliza normalmente para proporcionar la estructura básica ISL. El switch Catalyst 3900 se puede conectar a esta estructura básica a través del módulo de expansión ISL dual de 100 Mbps. El switch Catalyst 3900 Token Ring no soporta ningún otro

modo que no sea ISL, por lo que siempre es trunked. Además, los módulos ISL Catalyst 3900 sólo admiten conexiones de 100 Mbps y de forma predeterminada dúplex completo.

Tenga mucho cuidado cuando conecte un switch Catalyst 3900 y un switch Catalyst 5000 a través del link ISL. El problema principal es que el Catalyst 3900 no admite la negociación de medios Fast Ethernet. Por esta razón, si el Catalyst 5000 se configura para el modo Auto, entonces se configura de forma predeterminada en 100 Mbps semidúplex. Esto causa problemas como que el puerto pase del trunk al non-trunk y que se pierda el paquete.

Si desea conectar el puerto ISL Catalyst 3900 al puerto ISL de un Catalyst 5000, debe configurar manualmente el puerto ISL en el Catalyst 5000:

1. Ejecute el comando **set port speed** para establecer en 100 Mbps:

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

2. Ejecute el comando **set port duplex** para establecer en dúplex completo:

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

Si desea forzar el puerto de un switch al modo trunk, ejecute el comando **set trunk** (en una línea):

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

En el comando anterior, vlan es un valor entre 1 y 1005 (por ejemplo, 2-10 o 1005) y trunk_type se configura en isl, dot1q, dot10, lane o negocia.

Una vez que los puertos troncales están activos en los switches, puede ejecutar el comando **show trunk** para ver que estos puertos troncales están 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 que se debe 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
```

A partir de esa salida, puede ver claramente que un Catalyst 3900 está conectado al puerto 10/1. Cuando inspecciona el puerto 10/1 en la salida del anterior comando **show trunk**, puede decir que es un puerto trunk.

spanning-tree

El árbol de expansión en entornos Token Ring puede complicarse mucho porque se puede ejecutar simultáneamente un total de tres protocolos de árbol de expansión diferentes. Por ejemplo, un entorno típico ejecuta IBM Spanning-Tree en el nivel TrBRF y ejecuta IEEE (802.1d) o Cisco en el nivel TrCRF. Por lo tanto, el árbol de expansión es un poco más complicado de resolver problemas.

Esta tabla le indica lo que sucede en función de los diferentes tipos de configuraciones posibles:

Modo de Bridging TrCRF	TrCRF	TrBRF
SRB	Ejecuta el árbol de expansión IEEE.	Se desempeña como un puente de ruta de origen.
	Procesa las Unidades de datos (BPDU) del protocolo de árbol de extensión de IBM desde los bridges externos.	Ejecuta los protocolos IBM Spanning-Tree a los bridges externos.
		Descarta

		BPDU transparentes del protocolo IEEE Spanning-Tree del TrCRF.
SRT	Ejecuta el protocolo de árbol de extensión de Cisco.	Se desempeña como un puente transparente de ruta de origen.
	Reemplaza la dirección de grupo de bridge del campo de dirección de destino con una dirección de grupo específica de Cisco, de modo que los bridges externos no analicen las BPDU de TrCRF.	Reenvía tráfico transparente y de ruta de origen.
	Genere BPDU, con el bit RIF configurado en el campo de dirección de origen en la trama saliente y un RIF de 2 bytes agregado. Este formato de trama garantiza que el TrCRF permanezca local al anillo lógico y no se puentee de forma transparente o se rutee el origen a otras LAN. Sólo los TrCRF conectados a través de loops físicos reciben las BPDU.	Reenvía el tráfico de ruta de origen a todos los otros TrCRF en el TrBRF, ya estén en modo SRT o SRB.
	Procese BPDU de árbol de extensión IEEE desde bridges externos.	

VLAN Trunking Protocol

Porque, con ISL, la VLAN determina adónde debe ir un paquete, es importante que cada switch conozca las VLAN en la red. El propósito de VTP en la vida es propagar la información de VLAN a través de los switches. VTP no se ejecuta en los routers, porque deberían terminar la red VLAN. Cada switch de la red debe ejecutar VTP. Si no es así, el switch generalmente sólo ejecuta una VLAN (normalmente VLAN 1) y no ejecuta ISL en ese link, porque no hay necesidad. VTP hace que la creación de VLAN sea una tarea mucho más fácil, ya que podría configurar las VLAN en un switch y se propagarían a través de la red. Por supuesto, eso conlleva problemas.

VTP no es un sistema robusto, como el protocolo de routing de gateway interior mejorado (EIGRP) o el protocolo de routing Open Shortest Path First (OSPF). Es mucho más simple y se basa en un concepto muy importante: revisiones. En VTP, hay tres tipos de dispositivos VTP: clientes, servidores y dispositivos transparentes. Los dispositivos VTP del cliente básicamente sólo aceptan la información de VLAN de los dispositivos del servidor y no pueden modificar esta información. Sin embargo, los servidores pueden modificar la información VTP en cualquiera de

los servidores VTP. Por esta razón, VTP tiene un sistema de revisión. Cualquier servidor VTP que modifique o actualice la base de datos VLAN asegura que es la última revisión. Por esta razón, se debe tener extrema precaución, porque el switch con la revisión más alta ganará ?????? y su información de VLAN será la válida. Por ejemplo, si modifica un servidor VTP para decir que la VLAN 100 TrBRF realizará el árbol de expansión IEEE, esto causaría estragos entre todos los switches, porque podría hacer que los switches (como el Catalyst 3900) pusieran los puertos en modo de bloqueo, para protegerse de los loops. Además, tenga cuidado al introducir nuevos switches en la red, ya que podrían tener revisiones VTP más altas. En el modo transparente, los paquetes VTP recibidos en un tronco se propagan automáticamente, sin cambios, a todos los demás troncales del dispositivo; pero, se ignoran en el propio dispositivo.

Cuando configura VTP con switches Token Ring, debe ejecutar VTP V2. Si va a tener switches que ejecutan tanto VLAN Ethernet como Token Ring, debe actualizar VTP, incluso para las VLAN Ethernet. *No puede* tener dos dominios VTP diferentes (por ejemplo, no puede tener uno para Ethernet y otro para Token Ring).

Recorte VTP

Un problema con el enlace troncal VLAN es que la información de broadcast de una VLAN se propaga a través de todos los troncales, porque los switches no saben qué VLAN existen en un switch remoto. Por este motivo se creó el recorte de VTP. Permite a los switches negociar qué VLAN se asignan a los puertos en el otro extremo de un tronco y, por lo tanto, eliminar las VLAN que no se asignan remotamente. El recorte está desactivado de forma predeterminada en los switches Catalyst 3900 y Catalyst 5000.

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

Cada uno de los mensajes de recorte de VTP contiene información sobre las VLAN en cuestión y contiene un bit que indica si esta VLAN debe o no ser recortada para este tronco (un `1` indica que no debe ser recortada). Con el recorte habilitado, el tráfico VLAN no se envía normalmente a través del link troncal, a menos que el link troncal reciba un mensaje de unión apropiado con el bit VLAN?? correspondiente habilitado. Esto es muy importante porque le indica que, cuando utiliza el recorte de VTP, debe asegurarse de que existe la información y configuración correctas y que todos los switches están ejecutando el recorte; si un switch no envía mensajes de unión a otro switch a través del tronco, podría apagarse para una VLAN o VLAN concretas. Cuando se completa la negociación de recorte, la VLAN finalizará en estado de separación o de unión para ese tronco.

Una característica muy importante de la poda VTP le permite configurar una VLAN para que sea elegible o no para la poda. Esta función indica a los switches que ejecutan el recorte VTP que no borren esta VLAN. Cuando habilita el recorte de VTP, las VLAN 2 a 1000 están recortando las VLAN elegibles de forma predeterminada. Por lo tanto, cuando activa el recorte, afecta a todas las VLAN de forma predeterminada. VLAN 1, el TrCRF predeterminado (1003), el TrBRF predeterminado (1005) y los TrCRF siempre son inelegibles para el recorte; por lo tanto, el tráfico de estas VLAN no se puede recortar.

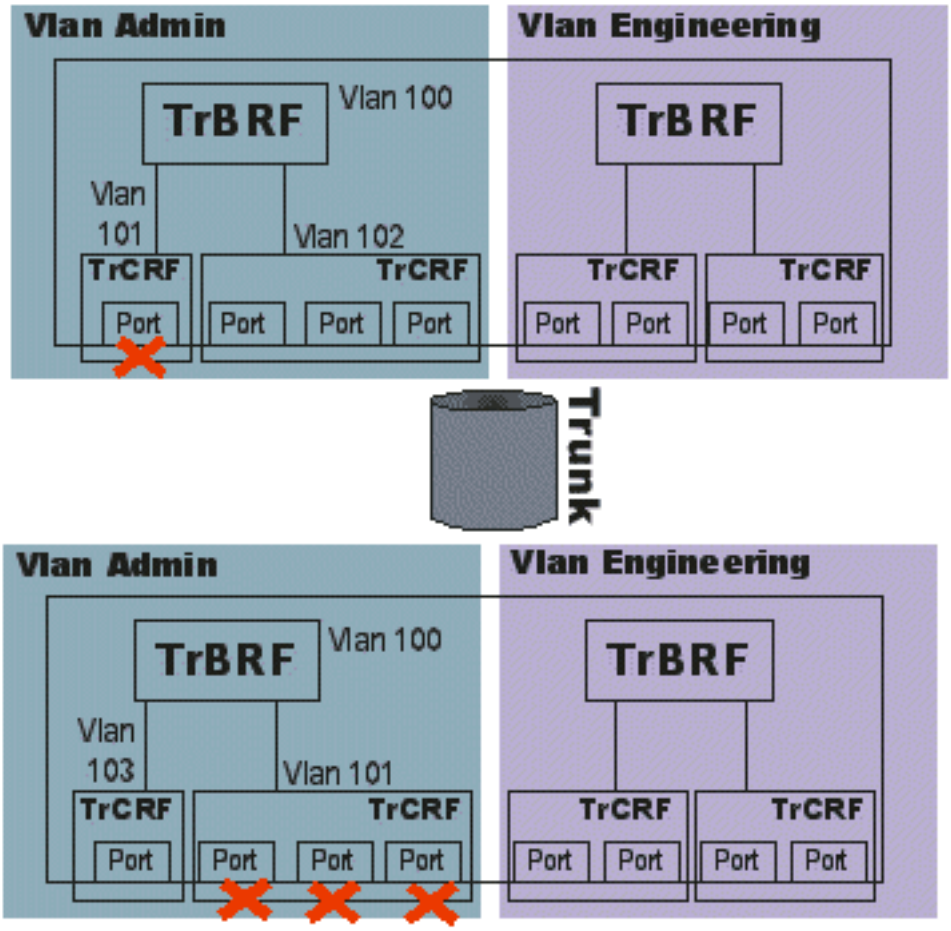
Duplicate Ring Protocol

Duplicate Ring Protocol está diseñado para ejecutarse en los switches que ejecutan las VLAN Token Ring. Su trabajo es asegurar la configuración adecuada de las VLAN Token Ring y crear una reducción del explorador. DRiP utiliza VTP para sincronizar su información de base de datos

de VLAN, pero no es necesario que DRiP funcione (la base de datos de VLAN se puede establecer manualmente). Un concepto erróneo es que DRiP entiende los números de timbre; esto no es verdadero. El DRiP depende de la unicidad de las VLAN configuradas en una red y de la configuración de la base de datos de VLAN.

Una de las características más importantes de DRiP es aplicar la distribución de TrCRF. En el mundo de Token Ring, es muy peligroso distribuir cualquier VLAN que no sea 1003, debido a problemas de expansión. Por esta razón, si se distribuye un TrCRF que no sea VLAN 1003, todos los puertos a los que se asocia esa VLAN son inhabilitados por DRiP.

Este ejemplo ilustra este concepto:

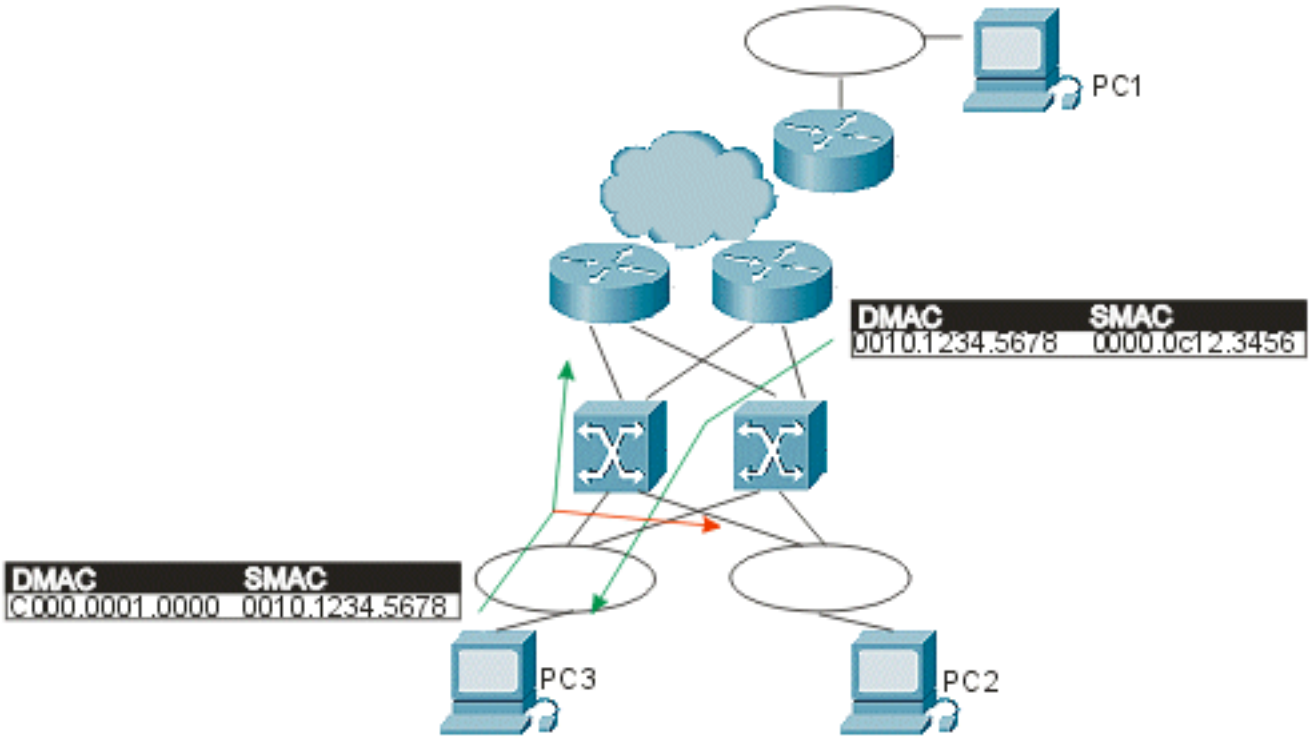


En ese ejemplo, dos switches diferentes tienen un puerto asignado a VLAN 101. El switch, a través de DRiP, mueve el árbol de expansión del puerto para inhabilitar y detener el reenvío de tráfico. Esto protege el switch contra una posible condición de loop.

Si no hay ningún cambio, DRiP anuncia el estado de TrCRF a todos sus puertos troncales cada 30 segundos. Cualquier cambio realizado a través de la CLI (interfaz de línea de comandos) o SNMP enviaría inmediatamente una actualización a todos los puertos. Estos anuncios son tramas ISL de tipo 0 y fluyen en la VLAN 1 predeterminada. Debido a que DRiP sólo anuncia sus efectos para las VLAN, es importante que exista la información de VLAN correcta en los switches que se conectan a través de ISL. Esto se realiza a través de VTP. Si se inhabilita VTP, esta función se debe mantener manualmente en todos los switches que comparten las mismas VLAN. Los anuncios DRiP sólo existen en los links ISL. No existen en ATM, Token Ring, Ethernet o FDDI. No hay árboles de topología guardados en DRiP.

VLAN HSRP y Token Ring

Uno de los mayores problemas con HSRP es el uso de la dirección multicast en la red. Dado que nadie en la red realmente origina paquetes con esta dirección MAC virtual, los switches nunca aprenden estas direcciones MAC. Por lo tanto, inundan las tramas en toda la red. Debido a esto, el uso de la función **standby use-bia** de HSRP fue necesario para enviar paquetes que usaban la dirección MAC impresa a fuego de la interfaz del router HSRP activo. El problema principal con este escenario es que, cuando los routers HSRP se conmuten, tendrían que enviar un protocolo de resolución de direcciones (ARP; ARP gratuito) a todas las estaciones del cable, de modo que las estaciones aprendan la nueva dirección MAC del gateway. Aunque este proceso debería funcionar según las especificaciones de IP, ha habido algunos problemas conocidos con él. Debido a las continuas solicitudes desde el campo, HSRP se cambió para que usted pueda tener la dirección multicast y también poder usar HSRP sin **standby use-bia**. Este cambio se lanzó en Cisco IOS Software Release 11.3(7) y 12.0(3) y posteriores.



En el diagrama anterior, la comunicación se produce entre PC1 y PC3. El problema es que el tráfico IP del cliente al router predeterminado en esta imagen utiliza una dirección de destino multicast. Debido a que nadie puede obtener este paquete de esa dirección, los switches nunca aprenden esta dirección y siempre inundan los paquetes. El DMAC tradicional que depende de los grupos es C000.000X.0000, que nunca puede ser un SMAC en Token Ring. Por lo tanto, todos los paquetes destinados de PC3 a PC1 a través de la gateway predeterminada ahora son vistos por PC2. En una red con muchos puentes, esto puede multiplicarse muy rápidamente y provocar lo que parecería tormentas de difusión, pero lo que en realidad es una gran cantidad de tráfico de multidifusión.

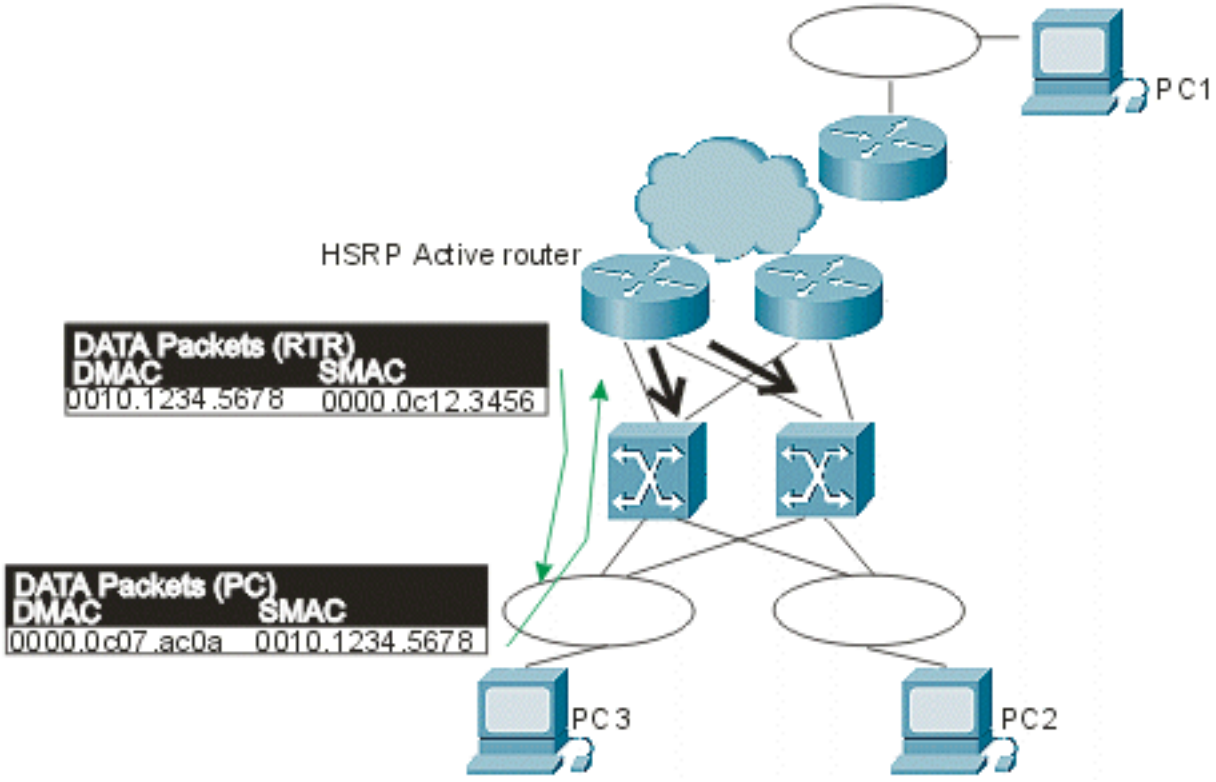
Para superar este problema, debe utilizar una dirección MAC que los routers de los saludos HSRP puedan utilizar realmente como SMAC. Esto permite que los switches aprendan esta dirección y, por lo tanto, conmuten los paquetes apropiadamente. Para ello, configure una nueva dirección MAC virtual en los routers. Los clientes deben enviar paquetes al DMAC de esta nueva dirección virtual. Este es un ejemplo de salida 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 ese resultado, se ha creado un grupo en espera 10 (IP en espera 1.1.1.100). La dirección MAC (`000.0c07.ac0a`) es la nueva dirección MAC virtual y el último byte es el grupo (0xA = 10). Una vez que tenga esta nueva configuración, ahora tendrá este patrón de tráfico, que evita las inundaciones de tráfico:



Ahora, debido a que el router está suministrando paquetes con el DMAC del HSRP virtual MAC, los switches aprenden esta dirección MAC y sólo reenvían los paquetes al router HSRP activo. Si el router HSRP activo falla y el standby se activa, el nuevo router activo comenzará a enviar saludos HSRP con el mismo SMAC, lo que hace que las tablas de direcciones MAC del switch conmuten sus entradas aprendidas al nuevo puerto del switch y al tronco.

Debido a la multiring, es necesario que surta efecto una operación adicional para asegurarse de que el RIF cambie realmente durante la transición (aunque sea la misma dirección MAC). La multidifusión es la capacidad del router para asociar un RIF con una dirección MAC, al igual que una estación final. Los routers necesitan varios anillos en entornos donde existen puentes SRB, de modo que los paquetes puedan atravesarlos para llegar a las estaciones finales.

En el mismo ejemplo que antes, puede ver los pasos adicionales necesarios para que el cliente se conecte al nuevo router HSRP activo:

1. El router activo deja de funcionar.
2. Una vez que el router en espera detecta la pérdida de saludos HSRP, inicia el proceso para convertirse en el router HSRP activo.
3. El router envía un ARP gratuito desde el mismo SMAC que antes, tanto en las capas MAC como en la capa ARP.
4. La 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 a HSRP MAC), envía una solicitud ARP al cliente directamente, porque *no* tiene la dirección MAC de ese cliente en su tabla ARP.
6. Una vez recibida la respuesta al paquete ARP, el router puede enviar paquetes al cliente de destino.

Información Relacionada

- Soporte de Productos de Switches
- Soporte de Tecnología de LAN Switching
- Soporte Técnico y Documentación - Cisco Systems