

Conceitos de Comutação Token Ring

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[TrBRF e TrCRF](#)

[Modos de switching](#)

[Bridging Transparente](#)

[Switching de rota de origem](#)

[Source-Route Bridging e Source-Route Transparent](#)

[Link entre switches](#)

[Árvore de abrangência](#)

[Protocolo de truncamento VLAN](#)

[Poda de VTP](#)

[Protocolo de toque duplicado](#)

[VLANs HSRP e Token Ring](#)

[Informações Relacionadas](#)

Introduction

Para começar a entender os conceitos de switching Token Ring, é muito importante que você entenda o bridging transparente, o bridging de rota de origem e o Spanning Tree. O Catalyst 3900 e o Catalyst 5000 usam novos conceitos, conforme descrito no IEEE 802.5 anexo K. Esses conceitos são os componentes para VLANs Token Ring. Este documento explica os diferentes conceitos de bridging e como eles funcionam:

- Entroncamento de ISL (Inter-Switch Link)
- Árvore de abrangência
- VLAN Trunking Protocol (VTP)
- Protocolo de anel duplicado (DRiP)

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Conventions

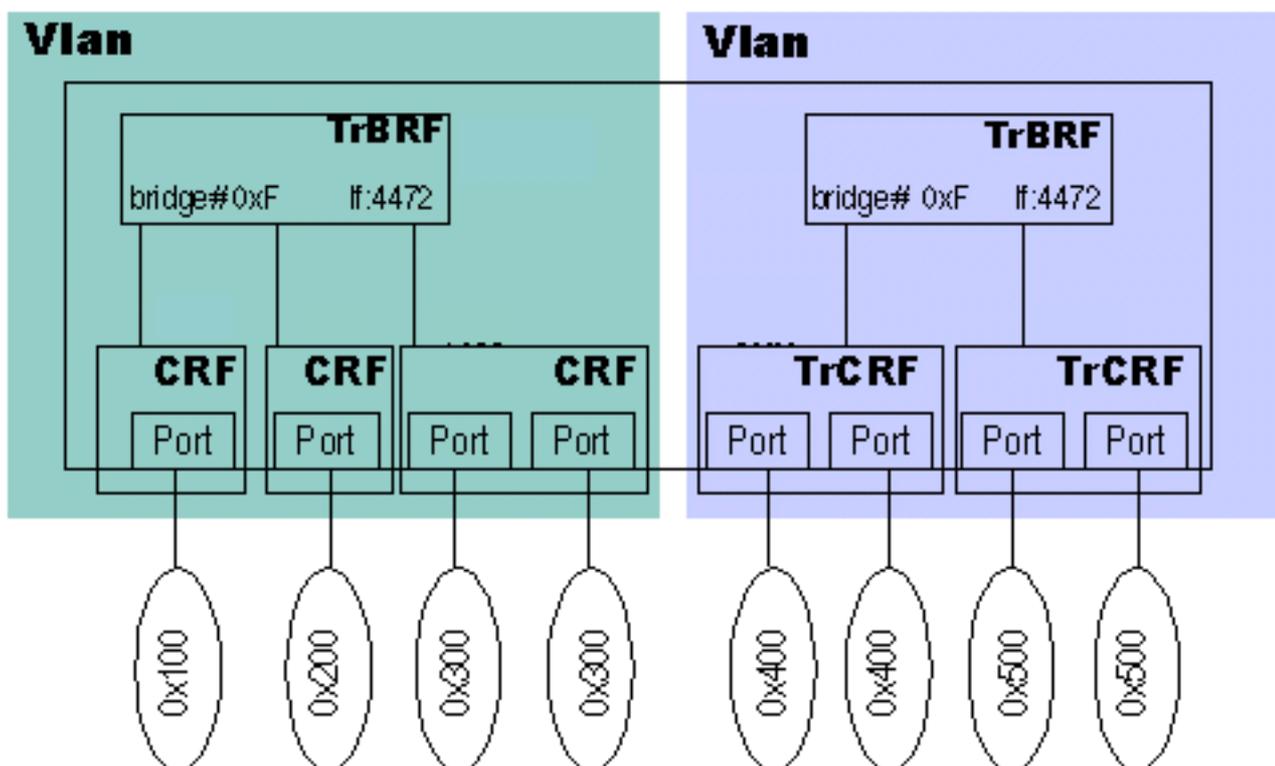
For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

TrBRF e TrCRF

A Token Ring Bridge Relay Function (TrBRF) e a Token Ring Concentrator Relay Function (TrCRF) são os blocos de construção da arquitetura do Catalyst 3900 e da funcionalidade do Catalyst 5000. TrBRF é simplesmente a função de bridge do switch, e TrCRF é a função de concentrador do switch. É importante entender que o bridging acontece em ambas as camadas porque, no Token Ring, três tipos diferentes de bridging serão discutidos.

A funcionalidade TrBRF do switch controla a comutação do tráfego de ponte de rota de origem, como o Source-Route Bridging (SRB) e o Source-Route transparent Bridging (SRT). O TrCRF cobre a funcionalidade de switching de rota de origem (SRS) e bridging transparente (TB). Por exemplo, é possível ter um switch Catalyst 3900 que tenha apenas um TrBRF e um TrCRF e todas as portas do switch estejam no mesmo TrCRF. Isso faz com que o switch só possa fazer SRS e TB. Se você definiu dez TrCRFs diferentes no mesmo TrBRF pai, o tráfego de portas conectadas ao mesmo TrCRF será encaminhado através da funcionalidade TrCRF do SRS ou TB. O tráfego que vai para os outros TrCRFs no switch usaria a funcionalidade TrBRF do switch e seria uma rota de origem interligada ou uma rota de origem transposta de forma transparente. Os diferentes mecanismos de comutação serão discutidos posteriormente neste documento.

Este diagrama relaciona o TrBRF e o TrCRF ao mundo físico:



Você pode ver que cada TrCRF está conectado a um anel específico. Um TrCRF pode

comprometer várias portas, e essas portas comprometem o mesmo número de anel. O TrBRF conecta os TrCRFs.

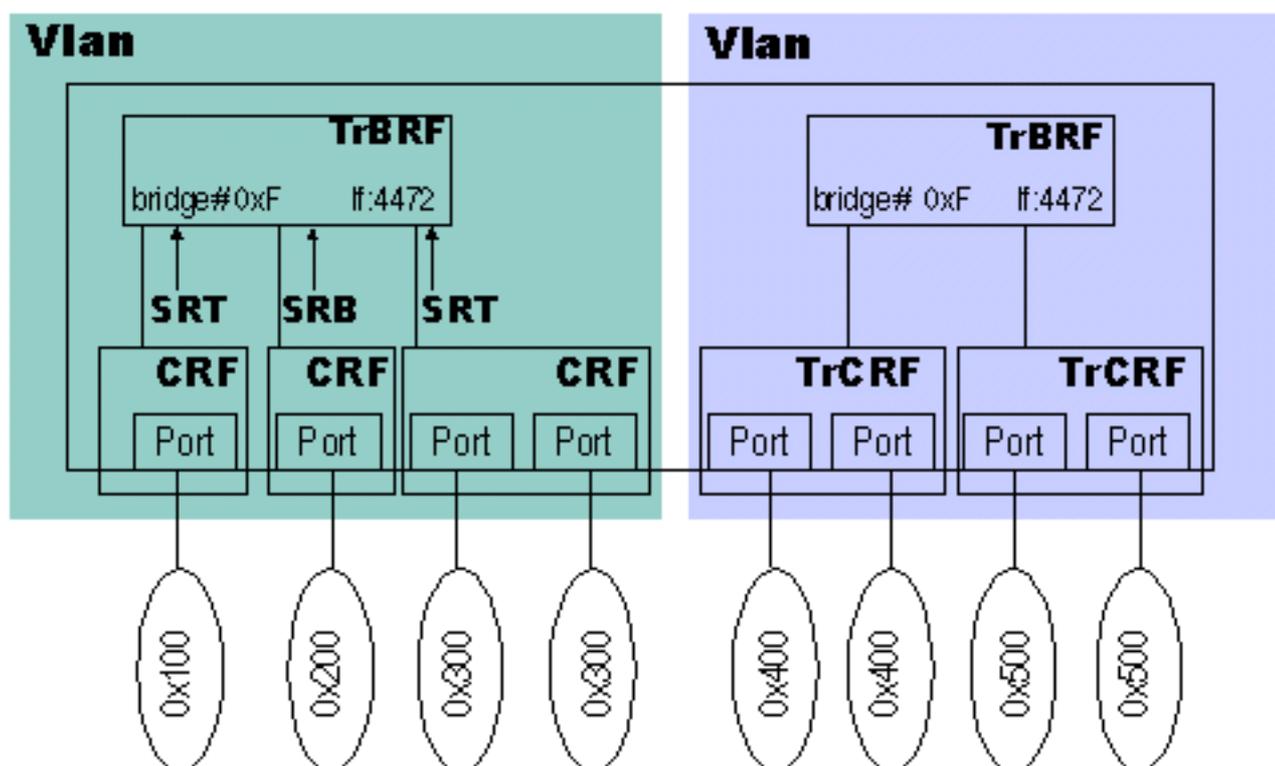
Um TrCRF e um TrBRF em si são uma VLAN diferente. Assim, em Token Ring, você pode fazer a ponte entre VLANs. O Bridging entre VLANs Token Ring segue duas regras:

- A conexão entre duas VLANs TrBRF só pode ser realizada por um dispositivo externo, como um roteador ou um Route Switch Module (RSM).
- A ponte entre VLANs TrCRF só pode ser realizada com VLANs TrCRF que sejam filhos da mesma VLAN TrBRF pai.

Isso é muito importante ter isso em mente para VLANs Token Ring, pois quebra o paradigma Ethernet. Resumindo, o que se pareceria com uma VLAN Ethernet é a soma de um TrBRF e seu TrCRF filho. Como você pode fazer a ponte entre determinadas VLANs em Token Ring, você deve entender como essa ponte ocorre.

Observação: para facilitar a compreensão das VLANs Token Ring em relação às VLANs Ethernet, lembre-se de que a combinação de TrCRF e TrBRF faz uma VLAN em si mesma.

Neste diagrama, você pode ver que o TrCRF decide o modo de bridging entre o TrCRF e o TrBRF.



Os TrCRFs individuais configuraram que tipo de bridging eles estarão fazendo com o TrBRF. Isso é importante porque você pode ter VLANs TrCRF que farão o bridging de rota de origem para outros TrCRFs, mas não farão quadros roteados não-origem. No diagrama anterior, um TrCRF é configurado para o modo SRB e dois estão no modo SRT. Isso significa que o tráfego SRB pode fluir entre os três TrCRFs, mas o SRT só pode fluir entre os dois que estão no modo SRT. Isso permite definir de forma granular como o tráfego deve fluir entre os TrCRFs. Se o modo de bridging fosse definido no TrBRF, ele afetaria todos os filhos TrCRF dessa VLAN.

Modos de switching

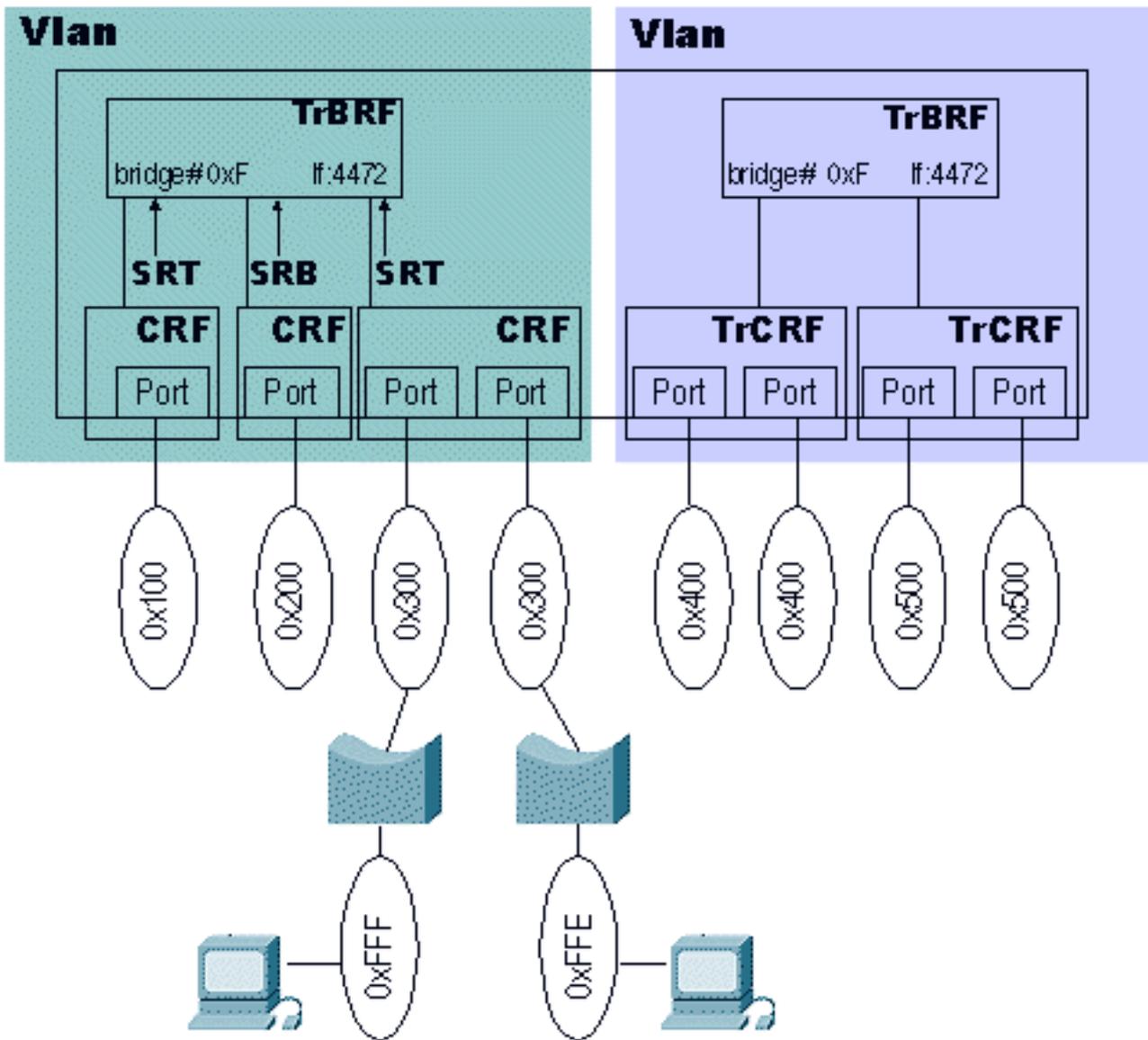
O Catalyst 3900 está configurado com um TrBRF e um TrCRF. Todas as portas são atribuídas à VLAN 1003 TrCRF padrão. O mesmo se aplica ao blade Token Ring do Catalyst 5000. Isso é importante porque dá à caixa um certo ???plug-and-play?? funcionalidade. De imediato, esses switches podem fazer o encaminhamento com base na comutação de rota de origem e no bridging transparente. As próximas seções fornecem detalhes sobre essas tecnologias.

Bridging Transparente

O Transparent Bridging é o mais básico de todos os mecanismos de comutação e é baseado no endereço MAC de destino (DMAC) dos quadros na rede. Esse é o mecanismo de encaminhamento de redes Ethernet. Sempre que um switch recebe um quadro, ele registra o endereço MAC de origem (SMAC) do quadro como um que pertence a essa porta e, a partir daí, encaminha o tráfego destinado a esse MAC para essa porta. Se, no processo de aprendizado, um switch não souber sobre um endereço MAC, ele inundará esse pacote para todas as portas no estado de encaminhamento.

Switching de rota de origem

O switching de rota de origem é um mecanismo de encaminhamento necessário quando há apenas um TrCRF atribuído às portas e o switch recebe pacotes com Campos de Informações de Roteamento (RIFs) nelas. Como o switch não modificará o RIF do quadro (porque não o passará para o TrBRF), a rede deve ser capaz de tomar decisões sobre encaminhamento, com o RIF, sem modificações. Considere este diagrama de rede que mostra o SRS:



O tráfego que vai do anel 0xFFFF ao anel 0xFFE precisa passar pelo switch. Esse tráfego seria o tráfego de bridge de rota de origem. Esta é a sequência de inicialização da comunicação entre estes dois clientes:

1. Uma estação envia um pacote explorador ao anel em que reside. Suponha que o cliente no anel 0xFFFF envie o pacote; parece algo assim (em hexadecimal):

```
0000 00c1 2345 8000 0c11 1111 c270
```

Observação: essas informações de pacote mostram apenas informações de DMAC, SMAC e RIF.

2. Quando o pacote chega à ponte de rota de origem e encaminha o quadro para o fio, o pacote se parece com isto:

```
0000 00C1 2345 8000 0c11 1111 C670 FFF1 3000
```

c670 é o campo de controle de roteamento e FFF1 3000 é ring 0xFFFF, bridge 0x1, ring 0x300.

3. Agora, o pacote atinge o switch. Como o switch vê o pacote vindo de um anel distante, ele aprende o descritor de rota. Nesse caso, o switch agora sabe que o anel 0xFFFF via bridge 0x1 está localizado na porta 3.
4. Como o pacote é um pacote explorador, o switch encaminha o quadro para todas as portas sob o mesmo TrCRF. Se o explorador precisar ir para portas em diferentes TrCRFs, ele entregará o quadro ao TrBRF, que fará sua funcionalidade de bridge. Se houver portas no mesmo TrCRF, ele encaminhará o quadro de saída sem modificação.

5. A estação no anel 0xFFE deve pegar o explorador e responder a ele. Suponha que o cliente responda com um quadro direcionado. Este quadro direcionado tem a seguinte aparência:

```
0000 0C11 1111 8000 00C1 2345 08E0 FFF1 3001 FFE0
```

08E0 é o campo de controle de roteamento e FFF1 3001 FFE0 é ring 0xFFFF, bridge 0x1, ring 0x300, bridge 0x1, ring 0xFFE.

6. Finalmente, o switch aprende que o anel 0xFFE está localizado na porta 4 e mantém o descritor de rota.

A partir de agora, o switch sabe sobre esses anéis. Se você observar as tabelas, verá que o switch aprendeu sobre o número da bridge e o número do anel. Quaisquer outros anéis após o anel 0xFFFF e o anel 0xFFE não são necessários, porque eles precisam passar pelo anel 0xFFFF ou pelo anel 0xFFE para acessar o switch.

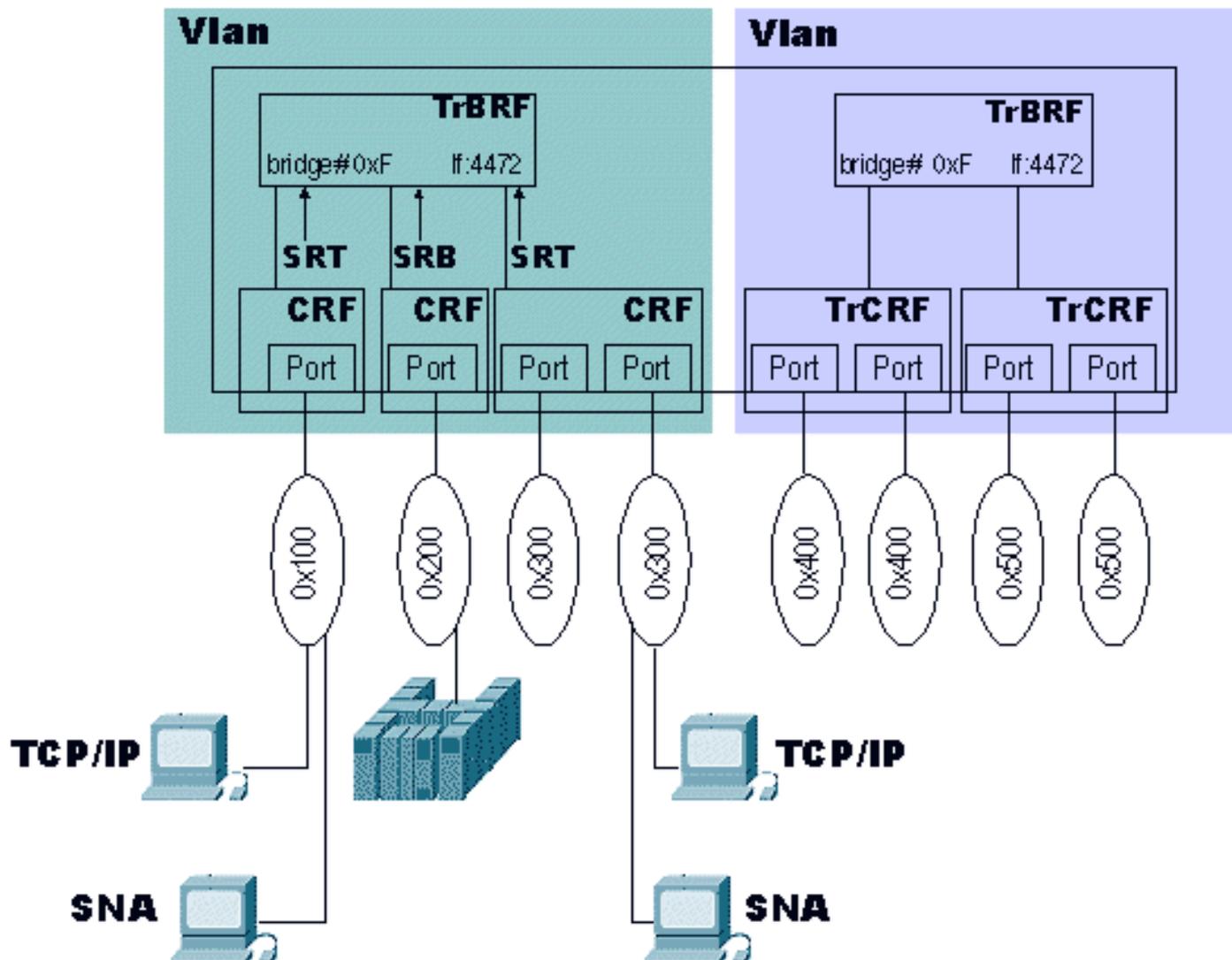
O SRS é um encaminhamento básico de pacotes baseados em RIF sem funcionalidade SRB, como é o caso com o TrCRF.

Observação: para exibir a tabela de informações de roteamento no Catalyst 5000, emita o comando **show rif**.

Source-Route Bridging e Source-Route Transparent

Toda a funcionalidade de bridging de rota de origem está localizada na lógica TrBRF. O TrCRF é aquele que vai comandar o modo de bridging para o TrBRF. Assim, se o TrCRF estiver configurado para o modo SRB para o TrBRF, quando o TrCRF receber um quadro NSR (não roteado na origem), o switch não o encaminhará para a lógica do TrBRF.

Isso pode ser usado se você não quiser que certos tipos de tráfego atinjam ou saiam de um anel específico. Este diagrama mostra um exemplo:



Se os clientes TCP/IP não tivessem a capacidade de enviar pacotes com RIFs, o switch não colocaria esses quadros no mesmo anel com o mainframe (0x200). No entanto, os quadros SNA para o host (que geralmente tem um RIF) chegariam ao mainframe. Essa é uma maneira muito rudimentar de filtrar quadros em uma rede comutada.

Esta é a sequência que o switch segue para encaminhar um quadro de ligação de rota de origem através do TrBRF:

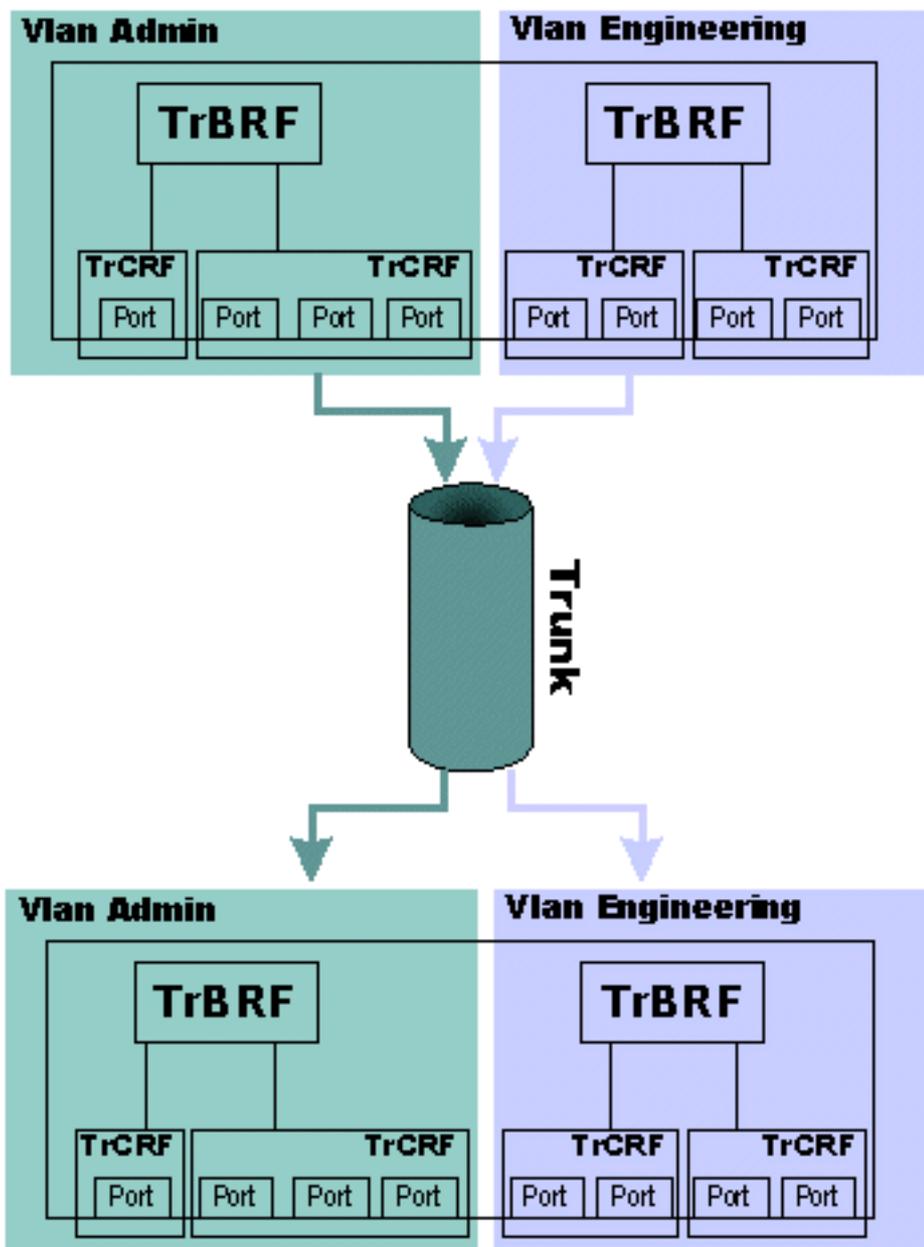
1. A estação SNA no anel 0x300 (porta 4) envia um explorador para acessar o mainframe.
2. Quando o pacote do explorador atinge o switch, ele encaminha o explorador, sem modificação, no mesmo TrCRF; em seguida, ele envia uma cópia ao TrBRF para encaminhar ao restante dos TrCRFs. Nesse caso, como o pacote tem um RIF, ele passa pelo caminho SRB. O switch também precisa aprender a rota.
3. O switch aprenderá o SMAC do quadro, pois ele é mostrado como originário do anel local ao qual o switch está conectado. Isso ocorre porque, em uma combinação de TrCRF de várias portas, o RIF mostra o anel de destino, mas o switch precisa saber qual porta no TrCRF. Portanto, o switch aprende o SMAC dos quadros que estão entrando no nível TrCRF.
4. O pacote vai para todo o resto dos TrCRFs, modificados com suas respectivas combinações de número de anel de bridge.
5. Quando o host responde com o quadro SRB, o switch aprende o SMAC do host para esse TrCRF e o envia para a porta de saída. O tráfego flui para frente e para trás entre os dois.

Observação: para verificar a tabela de endereços MAC no Catalyst 5000, execute o comando

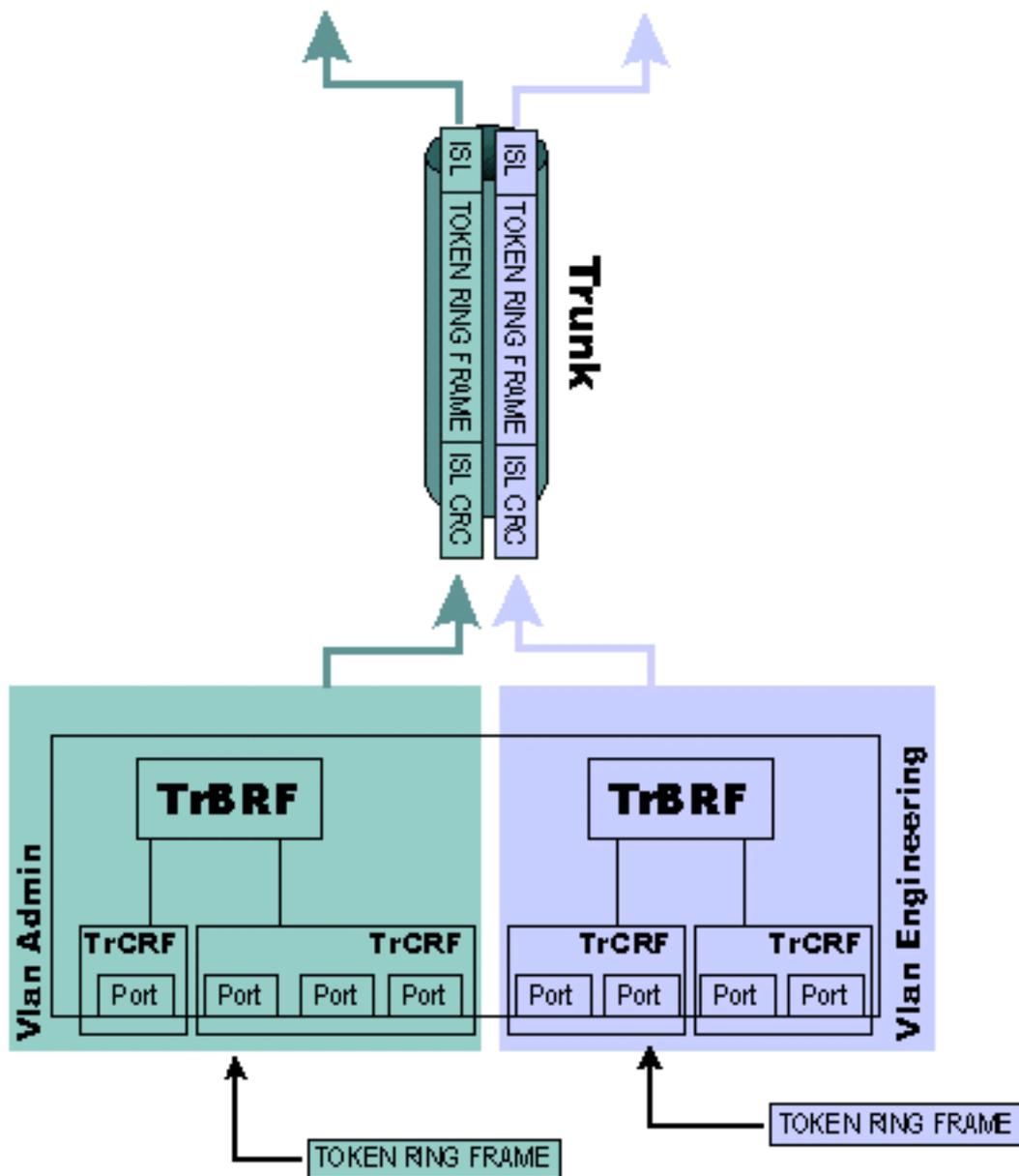
show cam.

Link entre switches

O Inter-Switch Link é um protocolo muito simples. Basicamente, os quadros que atravessam um tronco ISL são encapsulados em um quadro ISL que informa ao outro lado a qual VLAN os quadros pertencem. Por causa disso, as informações da VLAN devem ser compartilhadas manual ou automaticamente entre os switches. Um protocolo conhecido como VLAN Trunking Protocol (VTP) pode lidar com essa tarefa. Para VLANs Token Ring, você deve executar o VTP V2 na rede. Considere este diagrama:



Nesse caso, um único tronco ISL foi criado para transportar, por si só, as VLANs de engenharia e as VLANs de administrador. Nenhum do tráfego em qualquer VLAN se mistura depois de passar pelo tronco. Este diagrama mostra como essa separação é obtida:



Cada quadro dessas VLANs que precisa atravessar o tronco é encapsulado em um quadro ISL e sua VLAN é incluída no quadro. Isso permite que o switch receptor roteie corretamente o quadro para sua VLAN específica. O quadro ISL Token Ring (TRISL) tem alguns campos a mais que um quadro ISL regular. Este diagrama mostra o layout de um quadro TRISL:

40	4	4	48	16	24
DA	TYPE	USER	SA	LEN	AAAA03
24	15	1	16	15	1
HSA	DESTVLAN	BPDU	INDX	SRCVLAN	EXP
16	16	1	1	6	8 to 196600 (1 to 24575 bytes) ENCAP FRAME
DESTRD	SRCRD	T	F	Existe	
ENCAP FRAME (Continued)		8 to 196600 (1 to 24575 bytes) ENCAP FRAME		32	32
				Syn CRC	ISL CRC

Observação: mesmo que TRISL seja executado em interfaces Fast Ethernet, os pacotes contêm um quadro Token Ring padrão e as informações de VLAN associadas a esse quadro, até certo ponto. As VLANs Token Ring permitem até 18 k de tamanhos de quadro, como o ISL. Isso *não* é obtido através da fragmentação do quadro. O quadro inteiro é encapsulado em um quadro ISL em uma peça inteira e enviado através do link. Há um conceito equivocado comum de que o ISL é Ethernet e que seu tamanho máximo de quadro é de 1.500 bytes.

No Catalyst 5000, um protocolo conhecido como Dynamic Trunking Protocol (DTP) tornou-se disponível na versão 4.x. O DTP é o substituto estratégico do DISL (ISL dinâmico) porque incorpora o suporte para negociação de truncamento 802.1q. A função do DISL??? é negociar, somente para ISL, se um link entre dois dispositivos deve ser trunking. O DTP é capaz de negociar o tipo de encapsulamento de entroncamento que será usado entre troncos de VLAN ISL e IEEE 802.1Q. Esse é um recurso interessante, pois alguns dispositivos da Cisco suportam somente ISL ou 802.1Q, enquanto alguns podem executar ambos.

Estes são os cinco estados diferentes para os quais você pode configurar o DTP:

- Auto - No modo Auto (Automático), a porta ouve quadros DTP do switch vizinho. Se o switch vizinho indicar que ele gostaria de ser um tronco - ou um tronco - o modo Automático cria o tronco com o switch vizinho. Isso acontece quando a porta vizinha está definida para o modo Ligado ou Desejável.
- Desejável - O modo Desejável indica ao switch vizinho que ele pode ser um tronco ISL e que gostaria que o switch vizinho também fosse um tronco ISL. A porta se tornará uma porta de tronco se a porta da vizinhança for definida com o modo Ativo, Desejável ou Auto.
- Ligado - O modo Ligado ativa automaticamente o entroncamento ISL em sua porta, independentemente do estado de seu switch vizinho. Ele permanece um tronco ISL, a menos que receba um pacote ISL que desabilite explicitamente o tronco ISL.
- Nonegotiate - O modo Nonegotiate ativa automaticamente o entroncamento ISL em sua porta - independentemente do estado de seu switch vizinho - mas não permite que a porta gere quadros DTP.
- Apagado - No modo Desligado, ISL não é permitido nesta porta independentemente do modo DTP configurado no outro switch.

A família de switches Catalyst 5000 é normalmente usada para fornecer o backbone ISL. O switch Catalyst 3900 pode então ser conectado a esse backbone por meio do módulo de expansão ISL de 100 Mbps duplo. O switch Token Ring do Catalyst 3900 não oferece suporte a nenhum outro

modo além do ISL, portanto, ele está sempre em tronco. Além disso, os módulos ISL do Catalyst 3900 suportam apenas conexões de 100 Mbps e, por padrão, full-duplex.

Tenha muito cuidado ao conectar um Catalyst 3900 e um switch Catalyst 5000 através do link ISL. O principal problema é que o Catalyst 3900 não suporta a negociação de mídia Fast Ethernet. Por esse motivo, se o Catalyst 5000 estiver configurado para o modo Automático, ele assumirá como padrão o modo semiduplex de 100 Mbps. Isso causa problemas como a porta que vai do tronco para o não tronco e a perda de pacotes.

Se quiser conectar a porta ISL do Catalyst 3900 à porta ISL de um Catalyst 5000, você deve configurar manualmente a porta ISL no Catalyst 5000:

1. Emita o comando **set port speed** para definir como 100 Mbps:

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

2. Emita o comando **set port duplex** para definir como full duplex:

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

Se quiser forçar a porta de um switch para o modo de tronco, execute o comando **set trunk** (em uma linha):

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

No comando anterior, vlans é um valor de 1 a 1005 (por exemplo, 2-10 ou 1005) e trunk_type é definido como isl, dot1q, dot10, lane ou negocia.

Quando as portas de tronco estiverem ativas nos switches, você poderá emitir o comando **show trunk** para ver se essas portas de tronco estão ativas.

```
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

Um comando importante a ser usado para observar troncos ISL é o comando **show cdp neighbors detail**. Esse comando também ajuda a entender a topologia da rede.

```
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 dessa saída, você pode ver claramente que um Catalyst 3900 está conectado à porta 10/1. Quando você inspeciona a porta 10/1 na saída do comando anterior **show trunk**, você pode dizer que ela é uma porta trunk.

Árvore de abrangência

O Spanning-Tree em ambientes Token Ring pode se tornar muito complicado, pois é possível executar simultaneamente um total de três diferentes protocolos Spanning-Tree. Por exemplo, um ambiente típico executa o IBM Spanning-Tree no nível TrBRF e executa IEEE (802.1d) ou Cisco no nível TrCRF. Portanto, o Spanning-Tree é um pouco mais complicado de solucionar problemas.

Esta tabela informa o que acontece com base nos diferentes tipos de configurações possíveis:

M o d o d e p o n t e T r C R F	TrCRF	TrBRF
	Executa o Spanning Tree IEEE.	Executa como uma bridge de rota de origem.
S R B	Processa BPDUs (Bridge Protocol Data Units, unidades de dados de protocolo de ponte de abrangência) do IBM a partir de pontes externas.	Executa os protocolos IBM Spanning-Tree para bridges externas.

		Descarta BPDUs transparentes do protocolo Spanning-Tree IEEE do TrCRF.
S RT	Executa o protocolo Cisco Spanning-Tree.	Executa como uma bridge transparente de rota de origem.
	Substitui o endereço do grupo de bridge do campo de endereço de destino por um endereço de grupo específico da Cisco, de modo que as bridges externas não analisem as BPDUs de TrCRF.	Encaminha o tráfego transparente e de rota de origem.
	Gere BPDUs, com o bit RIF definido no campo de endereço de origem no quadro de saída e um RIF de 2 bytes adicionado. Esse formato de quadro garante que o TrCRF permaneça local para o anel lógico e não seja transposto de forma transparente ou roteado de origem para outras LANs. Somente os TrCRFs conectados por loops físicos recebem as BPDUs.	Encaminha o tráfego de rota de origem para todos os outros TrCRFs no TrBRF, estejam eles no modo SRT ou SRB.
	Processar BPDUs de Spanning-Tree IEEE de pontes externas.	

Protocolo de truncamento VLAN

Como, com o ISL, a VLAN determina para onde um pacote deve ir, é importante que cada switch saiba sobre as VLANs na rede. O objetivo do VTP na vida é propagar informações de VLAN através dos switches. O VTP não é executado em roteadores, pois eles devem encerrar a rede da VLAN. Cada switch na rede deve executar o VTP. Caso contrário, o switch normalmente executa apenas uma VLAN (geralmente a VLAN 1) e não executa ISL nesse link, porque não há necessidade. O VTP torna a criação de VLANs uma tarefa muito mais fácil, pois você pode configurar as VLANs em um switch e elas se propagariam pela rede. Claro que isso vem com problemas.

O VTP não é um sistema robusto, como o Enhanced Interior Gateway Routing Protocol (EIGRP) ou o protocolo de roteamento Open Shortest Path First (OSPF). É muito mais simples e funciona com base num conceito muito importante: revisões. No VTP, há três tipos de dispositivos VTP: clientes, servidores e dispositivos transparentes. Os dispositivos VTP do cliente basicamente aceitam informações de VLAN dos dispositivos do servidor e não podem modificar essas informações. Os servidores, no entanto, podem modificar as informações de VTP em qualquer um

dos servidores VTP. Por esse motivo, o VTP tem um sistema de revisão. Qualquer servidor VTP que modifique ou atualize o banco de dados de VLAN alega que é a revisão mais recente. Por esse motivo, deve-se usar muito cuidado, pois o switch com a revisão mais alta irá ganhar?????? e suas informações de VLAN serão válidas. Por exemplo, se você modificar um servidor VTP para dizer que a VLAN 100 do TrBRF fará spanning-tree do IEEE, isso causará problemas em todos os switches, pois poderia fazer com que os switches (como o Catalyst 3900) coloquem as portas no modo de bloqueio, para se protegerem contra loops. Além disso, tenha cuidado ao introduzir novos switches na rede, pois eles podem ter revisões de VTP mais elevadas. No modo transparente, os pacotes VTP recebidos em um tronco são automaticamente propagados, sem alterações, para todos os outros troncos no dispositivo; mas são ignorados no próprio dispositivo.

Ao configurar o VTP com os switches Token Ring, você deve executar o VTP V2. Se você vai ter switches que executam VLANs Ethernet e Token Ring, então você deve atualizar o VTP, mesmo para as VLANs Ethernet. Você *não pode* ter dois domínios VTP diferentes (por exemplo, você não pode ter um para Ethernet e um para Token Ring).

Poda de VTP

Um problema com o entroncamento de VLAN é que as informações de broadcast de uma VLAN se propagam em todos os troncos, porque os switches não sabem quais VLANs existem em um switch remoto. A remoção de VTP foi criada por esse motivo. Ele permite que os switches negociem quais VLANs estão atribuídas às portas na outra extremidade de um tronco e, portanto, removam as VLANs que não estão atribuídas remotamente. A remoção é desativada por padrão nos switches Catalyst 3900 e Catalyst 5000.

Observação: a poda de VTP é suportada no switch Catalyst 3900 na versão 4.1(1).

Cada uma das mensagens de poda VTP contém informações sobre as VLANs em questão e contém um bit que indica se essa VLAN deve ou não ser podada para esse tronco (um 1 indica que ela não deve ser podada). Com a remoção ativada, o tráfego da VLAN não é normalmente enviado através do link de tronco, a menos que o link de tronco receba uma mensagem de junção apropriada com o bit correspondente da VLAN?????. Isso é muito importante porque ele informa que, ao usar a poda de VTP, você deve garantir que as informações e a configuração corretas existam e que todos os switches estejam executando a poda; se um switch não enviar mensagens de junção para outro switch através do tronco, ele poderá ser desligado para uma VLAN ou VLAN específica. Quando a remoção da negociação for concluída, a VLAN terminará em estado de remoção ou de união para esse tronco.

Um recurso muito importante da remoção de VTP permite que você configure uma VLAN para ser elegível ou não. Este recurso informa aos switches que estão executando a poda de VTP para não remover esta VLAN. Quando você habilita a poda de VTP, as VLANs 2 a 1000 estão podando VLANs qualificadas por padrão. Assim, quando você ativa a poda, ela afeta todas as VLANs por padrão. VLAN 1, TrCRF (1003) padrão, TrBRF (1005) padrão e TrCRFs são sempre inelegíveis para remoção; portanto, o tráfego dessas VLANs não pode ser podado.

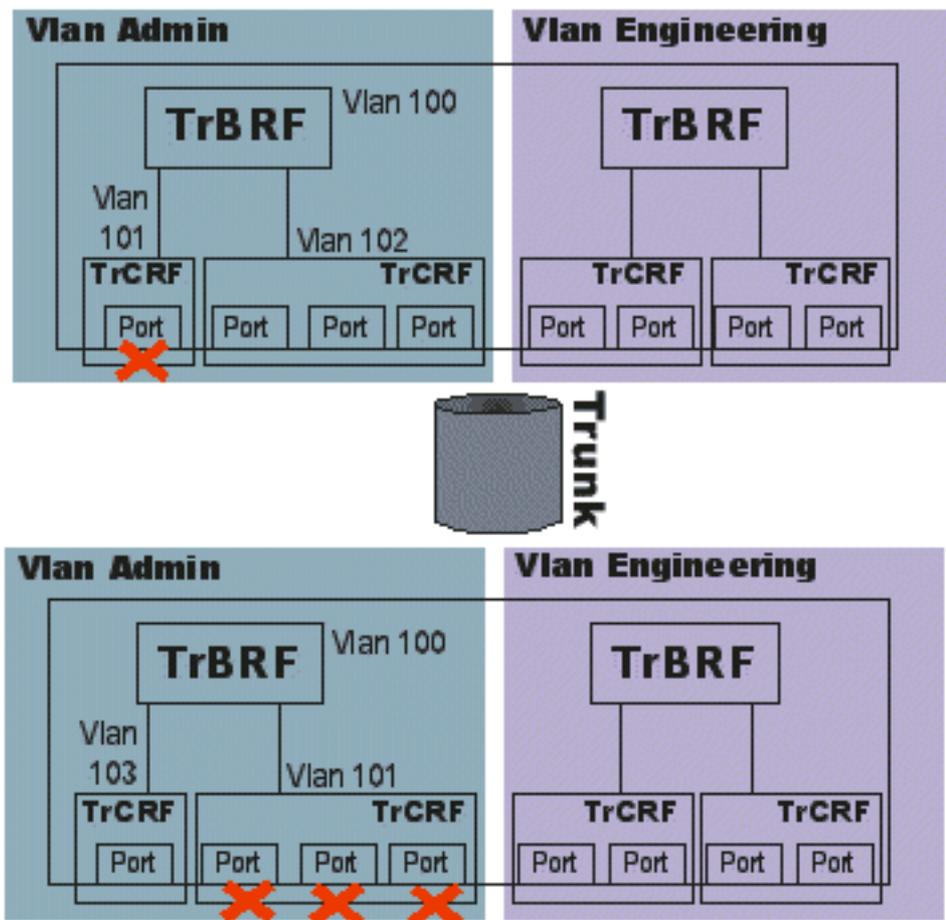
Protocolo de toque duplicado

O Protocolo de Toque Duplicado é projetado para ser executado em switches que executam VLANs de Token Ring. Seu trabalho é garantir a configuração adequada de VLANs Token Ring e criar uma redução de explorador. O DRiP usa o VTP para sincronizar suas informações de banco de dados de VLAN, mas não é necessário que o DRiP funcione (o banco de dados de VLANs

pode ser estabelecido manualmente). Um equívoco é que o DRiP entende os números dos anéis; isso não é verdade. O DRiP depende da exclusividade das VLANs configuradas em uma rede e da configuração do banco de dados da VLAN.

Um dos recursos mais importantes do DRiP é aplicar a distribuição do TrCRF. No mundo Token Ring, é muito perigoso distribuir qualquer VLAN diferente de 1003, devido a problemas de abrangência. Por esse motivo, se um TrCRF diferente da VLAN 1003 for distribuído, todas as portas às quais essa VLAN está associada serão desativadas pelo DRiP.

Este exemplo ilustra este conceito:

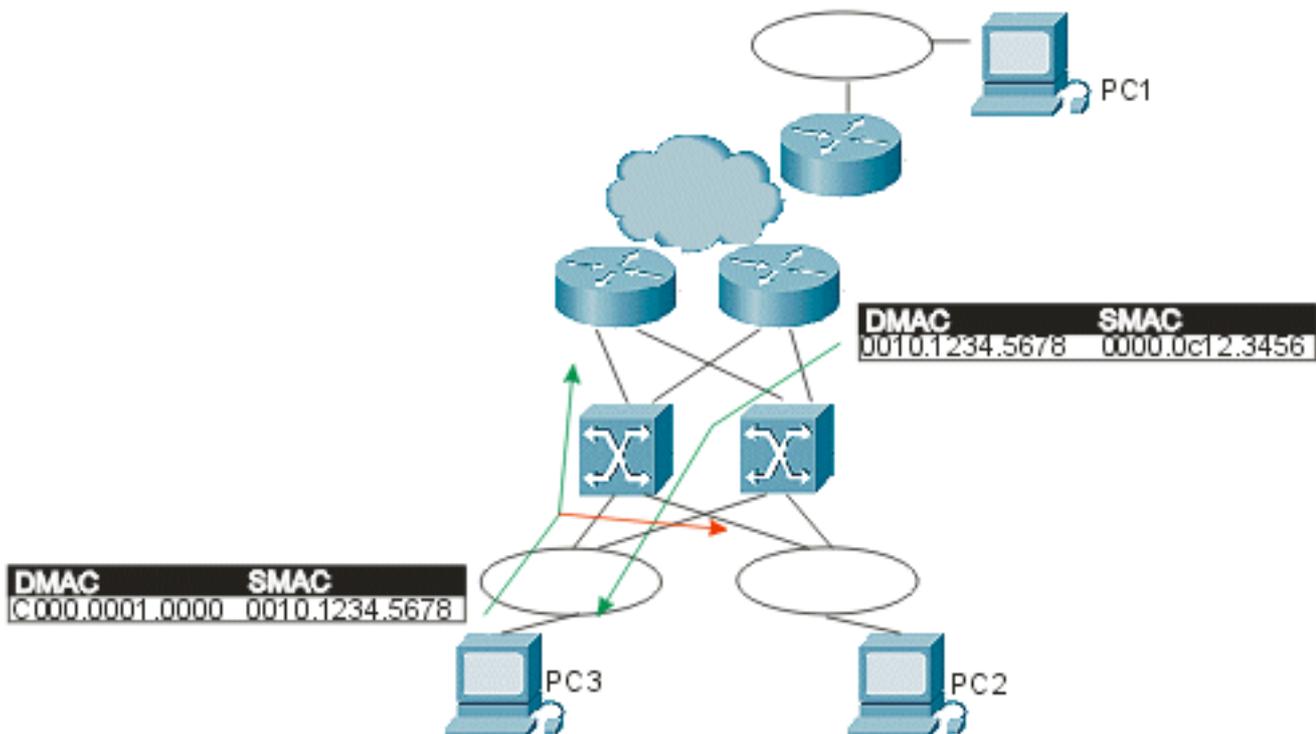


Nesse exemplo, dois switches diferentes têm uma porta atribuída à VLAN 101. O switch, via DRiP, move a spanning-tree da porta para desativar e para de encaminhar tráfego. Isso protege o switch contra uma possível condição de loop.

Se não houver alteração, o DRiP anunciará o status do TrCRF para todas as suas portas de tronco a cada 30 segundos. Qualquer alteração feita por meio da CLI (Command Line Interface, Interface de Linha de Comando) ou SNMP enviaria imediatamente uma atualização para todas as portas. Esses anúncios são quadros ISL tipo 0 e fluxo na VLAN 1 padrão. Como o DRiP apenas anuncia seus efeitos para VLANs, é importante que as informações corretas de VLANs existam nos switches conectados via ISL. Isso é feito via VTP. Se o VTP estiver desabilitado, essa função deverá ser mantida manualmente em todos os switches que compartilham as mesmas VLANs. Os anúncios de DRiP só existem em links ISL. Eles não existem em ATM, Token Ring, Ethernet ou FDDI. Não há árvores de topologia mantidas no DRiP.

VLANs HSRP e Token Ring

Um dos maiores problemas com o HSRP é o uso do endereço multicast na rede. Como ninguém na rede realmente origina pacotes com esse endereço MAC virtual, os switches nunca aprendem esses endereços MAC. Portanto, eles inundam quadros pela rede. Por causa disso, o uso da função **standby use-bia** do HSRP era necessário para enviar pacotes que usavam o endereço MAC gravado da interface ativa do roteador HSRP. O principal problema com esse cenário é que, quando os roteadores HSRP comutam, teriam que enviar um ARP (Protocolo de Resolução de Endereços de broadcast); ARP gratuito) para todas as estações no fio, de modo que as estações aprendam o novo endereço MAC do gateway. Embora esse processo deva funcionar com base em especificações IP, houve alguns problemas conhecidos com ele. Devido a solicitações contínuas do campo, o HSRP foi alterado para que você possa ter o endereço multicast e também possa usar o HSRP sem o **standby use-bia**. Essa alteração foi lançada no Cisco IOS Software Release 11.3(7) e 12.0(3) e posterior.



No diagrama anterior, está ocorrendo comunicação entre PC1 e PC3. O problema é que o tráfego IP do cliente para o roteador padrão nesta imagem usa um endereço de destino multicast. Como ninguém pode obter esse pacote desse endereço, os switches nunca aprendem esse endereço e sempre inundam os pacotes. O DMAC tradicional que depende dos grupos é C000.000X.0000, que nunca pode ser um SMAC em Token Ring. Assim, todos os pacotes destinados de PC3 a PC1 por meio do gateway padrão são agora vistos pelo PC2. Em uma rede com muitas bridges, isso pode se multiplicar muito rapidamente e causar o que parece ser tempestade de broadcast, mas o que é realmente uma grande quantidade de tráfego multicast.

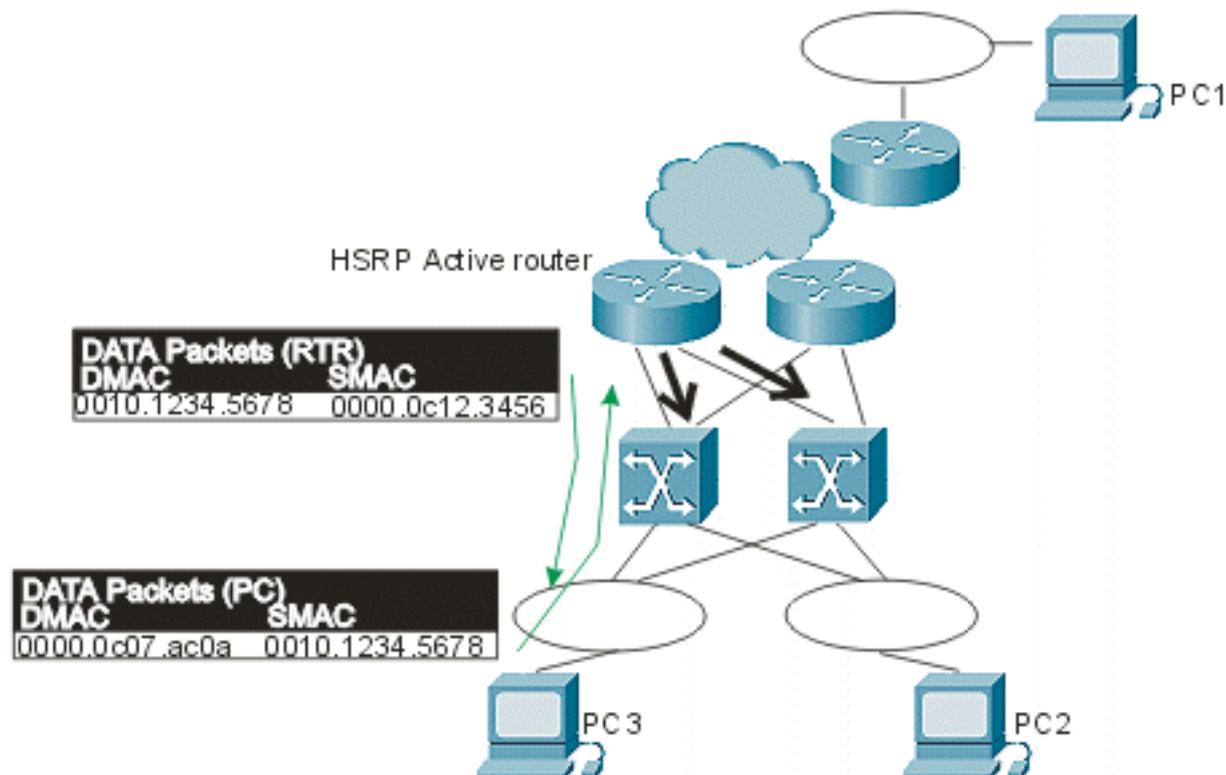
Para superar esse problema, você deve usar um endereço MAC que possa ser usado como um SMAC pelos roteadores nas saudações do HSRP. Isso permite que os switches aprendam esse endereço e, portanto, comutem os pacotes adequadamente. Para fazer isso, configure um novo endereço MAC virtual nos roteadores. Os clientes precisam enviar pacotes para o DMAC desse novo endereço virtual. Este é um exemplo de saída de um 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
```

Nessa saída, um grupo de standby 10 (IP de standby 1.1.1.100) foi criado. O endereço MAC (0000.0c07.ac0a) é o novo endereço MAC virtual e o último byte é o grupo (0xA = 10). Depois de ter essa nova configuração, você terá esse padrão de tráfego, que evita inundações de tráfego:



Agora, como o roteador está fornecendo pacotes com o DMAC do MAC virtual do HSRP, os switches aprendem esse endereço MAC e encaminham apenas os pacotes para o roteador HSRP ativo. Se o roteador HSRP ativo falhar e o standby for ativado, o novo roteador ativo começará a enviar pacotes de hello HSRP com o mesmo SMAC, o que faz com que as tabelas de endereços MAC do switch comutem suas entradas aprendidas para a nova porta do switch e tronco.

Devido ao multianel, é necessário que a operação adicional tenha efeito para garantir que o RIF realmente mude durante a transição (mesmo que seja o mesmo endereço MAC). Multiring é a capacidade do roteador de associar um RIF a um endereço MAC, assim como uma estação final. Os roteadores precisam de multianel em ambientes onde existem bridges SRB, de modo que os pacotes possam atravessá-los para alcançar estações finais.

No mesmo exemplo de antes, você pode ver as etapas adicionais necessárias para que o cliente se conecte ao novo roteador HSRP ativo:

1. O roteador ativo para de funcionar.
2. Quando o roteador em standby detecta a perda de saudações do HSRP, ele inicia o processo para se tornar o roteador HSRP ativo.
3. O roteador envia um ARP gratuito do mesmo SMAC anterior, tanto nas camadas MAC como na camada ARP.
4. O PC agora envia o quadro destinado ao mesmo endereço MAC, mas com o novo RIF.
5. Quando o roteador recebe esse quadro (destinado ao MAC do HSRP), ele envia uma

solicitação ARP diretamente ao cliente, porque *não* tem o endereço MAC desse cliente em sua tabela ARP.

6. Quando a resposta ao pacote ARP é recebida, o roteador pode enviar pacotes ao cliente de destino.

Informações Relacionadas

- [Suporte ao Produto - Switches](#)
- [Suporte de tecnologia de switching de LAN](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)