Concepts de commutation Token Ring

Contenu

Introduction

Pour commencer à comprendre les concepts de la commutation Token Ring, il est très important de comprendre le pontage transparent, le pontage source-route et le protocole Spanning Tree. Les commutateurs Catalyst 3900 et Catalyst 5000 utilisent de nouveaux concepts, comme décrit à l'annexe K de la norme IEEE 802.5. Ces concepts sont les éléments de base des VLAN Token Ring. Ce document explique les différents concepts de pontage et leur fonctionnement :

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

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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

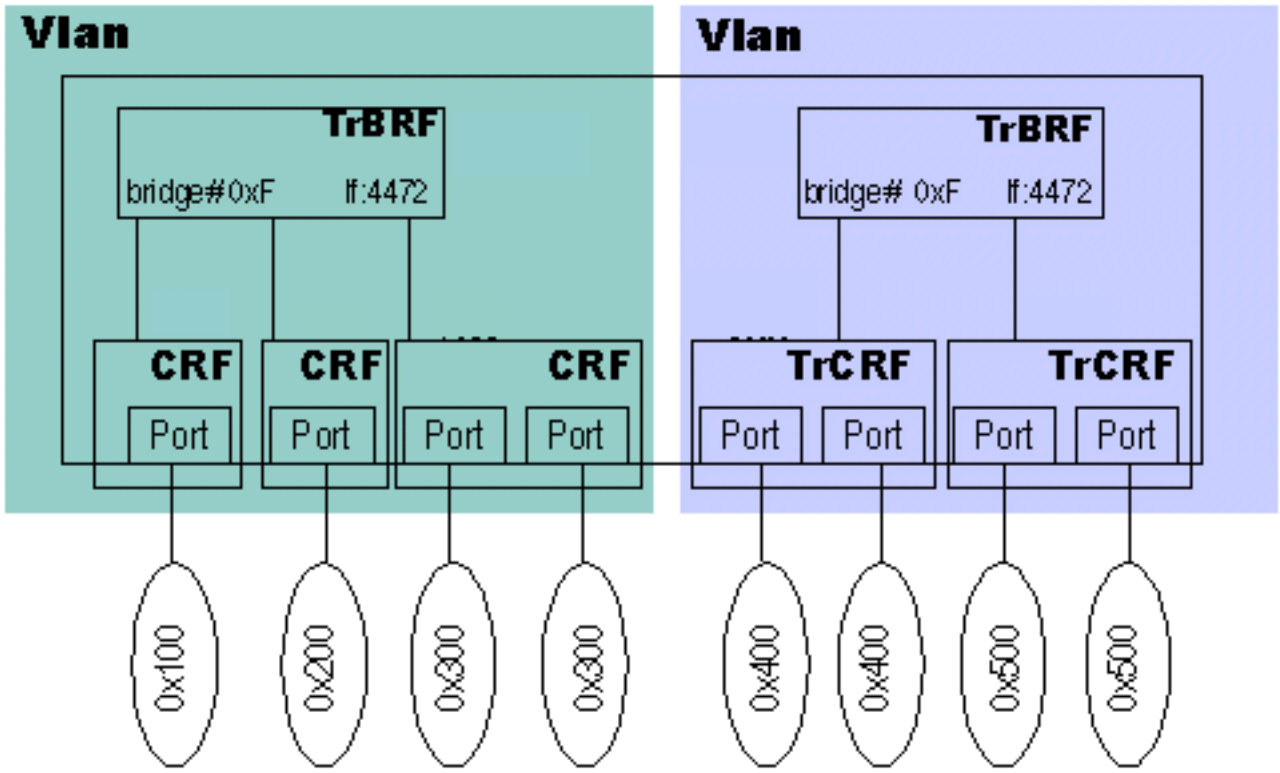
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

TrBRF et TrCRF

La fonction TrBRF (Token Ring Bridge Relay Function) et la fonction TrCRF (Token Ring Concentrator Relay Function) sont les éléments constitutifs de l'architecture du Catalyst 3900 et de la fonctionnalité du Catalyst 5000. TrBRF est simplement la fonction de pont du commutateur, et TrCRF est la fonction de concentrateur du commutateur. Il est important de comprendre que le pontage se produit au niveau de ces deux couches car, dans Token Ring, trois types de pontage différents seront abordés.

La fonctionnalité TrBRF du commutateur contrôle la commutation du trafic ponté de route source, comme le pontage SRB (Source-Route Bridging) et SRT (Source-Route transparent Bridging). Le TrCRF couvre les fonctionnalités de commutation SRS (Source-Route Switching) et de pontage transparent (To). Par exemple, il est possible d'avoir un commutateur Catalyst 3900 qui n'a qu'un TrBRF et un TrCRF et tous les ports du commutateur sont dans le même TrCRF. Cela signifie que le commutateur ne peut faire que SRS et To. Si vous avez défini dix TrCRF différents sous le même TrBRF parent, le trafic des ports connectés au même TrCRF sera transféré via la fonctionnalité TrCRF de SRS ou de TB. Le trafic se dirigeant vers les autres TrCRF du commutateur utiliserait la fonctionnalité TrBRF du commutateur et serait soit ponté par route source, soit ponté de manière transparente par route source. Les différents mécanismes de commutation seront abordés plus loin dans ce document.

Ce diagramme relie le TrBRF et le TrCRF au monde physique :



Vous pouvez voir que chaque TrCRF est connecté à un anneau spécifique. Un TrCRF peut compromettre plusieurs ports, et ces ports compromettraient le même numéro de sonnerie. Le TrBRF connecte les TrCRF ensemble.

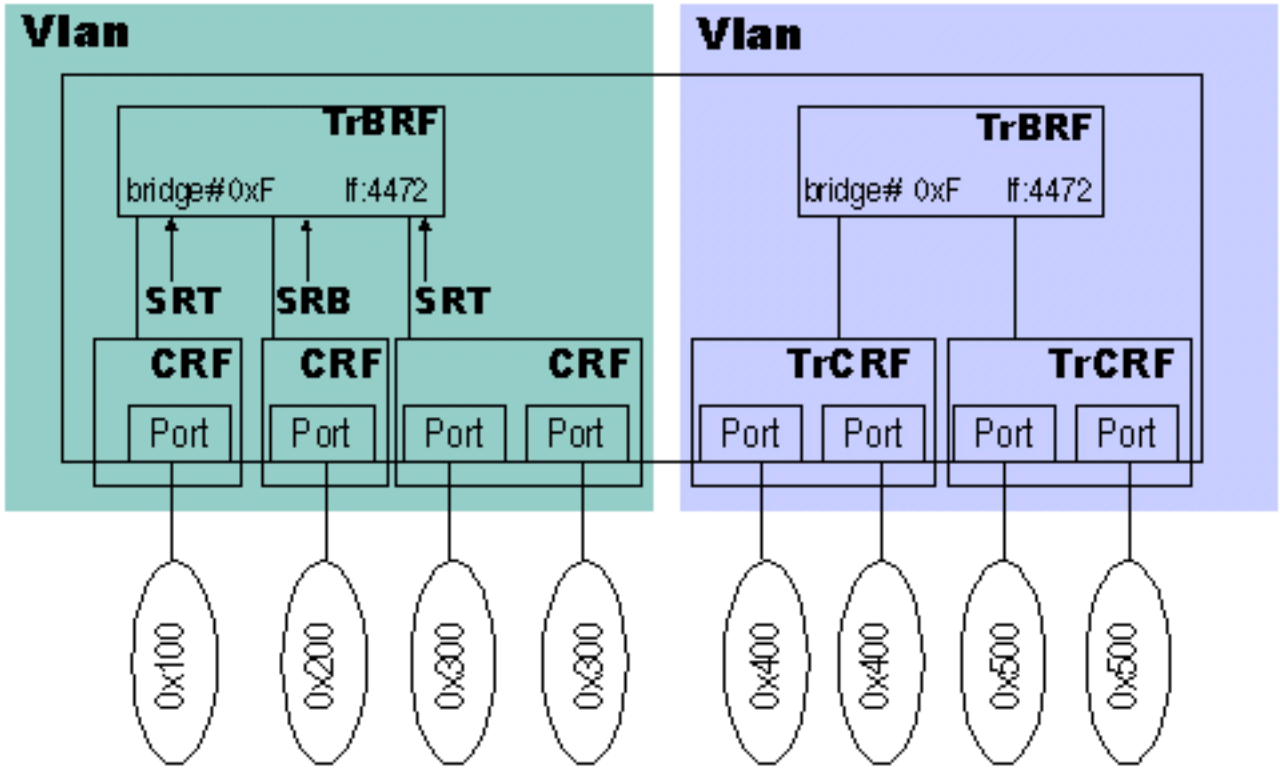
Un TrCRF et un TrBRF en lui-même sont un VLAN différent. Ainsi, dans Token Ring, vous pouvez établir un pont entre les VLAN. Le pontage entre les VLAN Token Ring suit deux règles :

- Le pontage entre deux VLAN TrBRF ne peut être effectué que par un périphérique externe, tel qu'un routeur ou un module de commutation de route (RSM).
- Le pontage entre les VLAN TrCRF ne peut être effectué qu'avec les VLAN TrCRF qui sont des enfants du même VLAN TrBRF parent.

Il est très important de garder cela à l'esprit pour les VLAN Token Ring, car cela rompt le paradigme Ethernet. En résumé, ce qui ressemble à un VLAN Ethernet est la somme d'un TrBRF et de ses enfants TrCRF. Comme vous pouvez établir un pont entre certains VLAN dans Token Ring, vous devez comprendre comment ce pontage se produit.

Remarque : Pour faciliter la compréhension des VLAN Token Ring par rapport aux VLAN Ethernet, n'oubliez pas que la combinaison de TrCRF et TrBRF fait un VLAN en soi.

Dans ce diagramme, vous pouvez voir que le TrCRF décide du mode de pontage entre le TrCRF et le TrBRF.



Les TrCRF individuels ont configuré le type de pontage qu'ils vont faire au TrBRF. Ceci est important car vous pouvez avoir des VLAN TrCRF qui feront le pontage de route source vers d'autres TrCRF mais ne feront pas de trames non routées par source. Dans le schéma précédent, un TrCRF est configuré pour le mode SRB et deux sont en mode SRT. Cela signifie que le trafic SRB peut circuler entre les trois TrCRF, mais SRT ne peut circuler qu'entre les deux qui sont en mode SRT. Cela vous permet de définir de manière granulaire la manière dont le trafic doit circuler entre les TrCRF. Si le mode de pontage était défini sur le TrBRF, il affecterait tous les enfants TrCRF de ce VLAN.

Modes de commutation

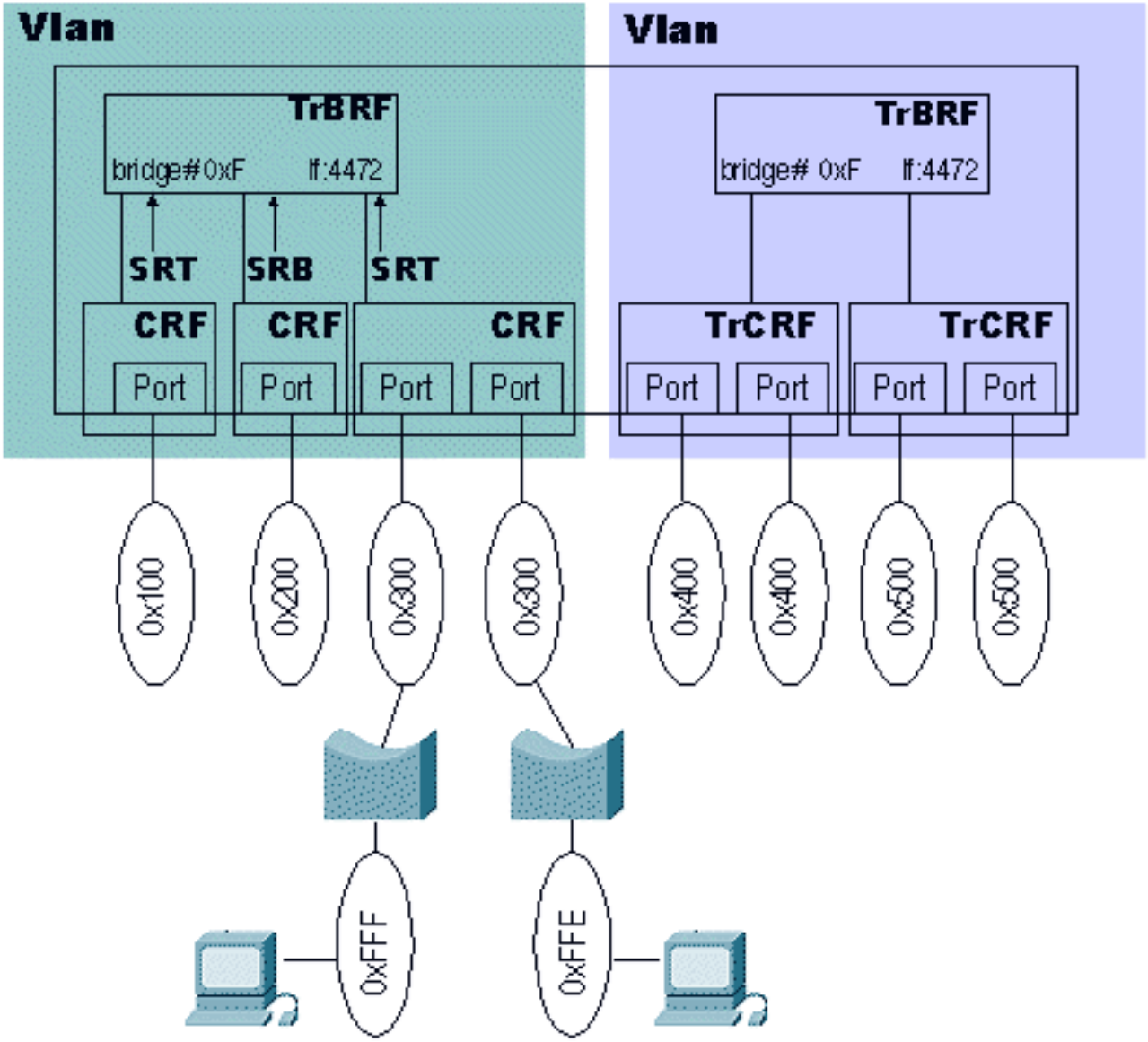
Hors du boîtier, le Catalyst 3900 est configuré avec un TrBRF et un TrCRF. Tous les ports sont affectés au VLAN 1003 TrCRF par défaut. Il en va de même pour la lame Token Ring Catalyst 5000. C'est important parce qu'il donne à la boîte certains ? ? ? plug-and-play ? ? ? . Hors du boîtier, ces commutateurs peuvent effectuer le transfert en fonction de la commutation de route source et du pontage transparent. Les sections suivantes fournissent des détails sur ces technologies.

Pontage transparent

Le pontage transparent est le plus basique de tous les mécanismes de commutation et il est basé sur l’adresse MAC de destination (DMAC) des trames du réseau. Il s’agit du mécanisme de transmission des réseaux Ethernet. Chaque fois qu’un commutateur reçoit une trame, il enregistre l’adresse MAC source (SMAC) de la trame comme étant celle qui appartient à ce port et, dorénavant, transfère le trafic qui est destiné à cet MAC à ce port. Si, dans le processus d’apprentissage, un commutateur ne connaît pas d’adresse MAC, il inonde ce paquet vers tous les ports en état de transmission.

Commutation de routage source

La commutation de route source est un mécanisme de transfert qui est nécessaire lorsqu'un seul TrCRF est affecté aux ports et que le commutateur reçoit des paquets avec des champs RIF (Routing Information Fields). Comme le commutateur ne modifie pas le RIF de la trame (car il ne le transmet pas au TrBRF), le réseau doit être en mesure de prendre des décisions sur le transfert, avec le RIF, sans modification. Considérez ce diagramme de réseau qui montre SRS :



Le trafic passant de l'anneau 0xFFF à l'anneau 0xFFE doit passer par le commutateur. Ce trafic serait un trafic de pont de route source. Voici la séquence de démarrage de la communication entre ces deux clients :

1. Une station envoie un paquet d'exploration à l'anneau sur lequel elle réside. Supposons que le client sur la sonnerie 0xFFF envoie le paquet ; il ressemble à ceci (au format hexadécimal) :
   `0000 00c1 2345 8000 0c11 1111 C270`
   Remarque : ces informations de paquet ne contiennent que des informations DMAC, SMAC et RIF.
2. Une fois que le paquet atteint le pont de route source et transfère la trame au câble, le paquet ressemble à ceci :
   `0000 00C1 2345 8000 0c11 1111 C670 FFF1 3000`
   `C670` est le champ de contrôle de routage et `FFF1 3000` est l'anneau 0xFFF, le pont 0x1, l'anneau 0x300.
3. Maintenant, le paquet touche le commutateur. Comme le commutateur voit le paquet provenant d'un anneau éloigné, il apprend le descripteur de route. Dans ce cas, le commutateur sait maintenant que l'anneau 0xFFF via le pont 0x1 est situé sur le port 3.
4. Comme le paquet est un paquet d'exploration, le commutateur transfère la trame à tous les ports sous le même TrCRF. Si l'explorateur doit accéder à des ports dans des TrCRF

différents, il transmettra la trame au TrBRF, qui fera sa fonctionnalité de pont. S'il y a des ports dans le même TrCRF, il transmettra la trame en sortie sans modification.

5. La station de l'anneau 0xFFE doit obtenir l'explorateur et y répondre. Supposez que le client répond par une trame dirigée. Cette trame dirigée ressemble à ceci :
   `0000 0C11 1111 8000 00C1 2345 08E0 FFF1 3001 FFE0`
   `08E0` est le champ de contrôle de routage et `FFF1 3001 FFE0` est l'anneau 0xFFF, le pont 0x1, l'anneau 0x300, le pont 0x1, l'anneau 0xFFE.
6. Enfin, le commutateur apprend que l'anneau 0xFFE est situé sur le port 4 et conserve le descripteur de route.

Désormais, le commutateur connaît ces anneaux. Si vous regardez les tables, vous verrez que le commutateur a appris le numéro de pont et le numéro de sonnerie. Les autres anneaux après les anneaux 0xFFF et 0xFFE ne sont pas nécessaires, car ils doivent passer par 0xFFF ou 0xFFE pour atteindre le commutateur.

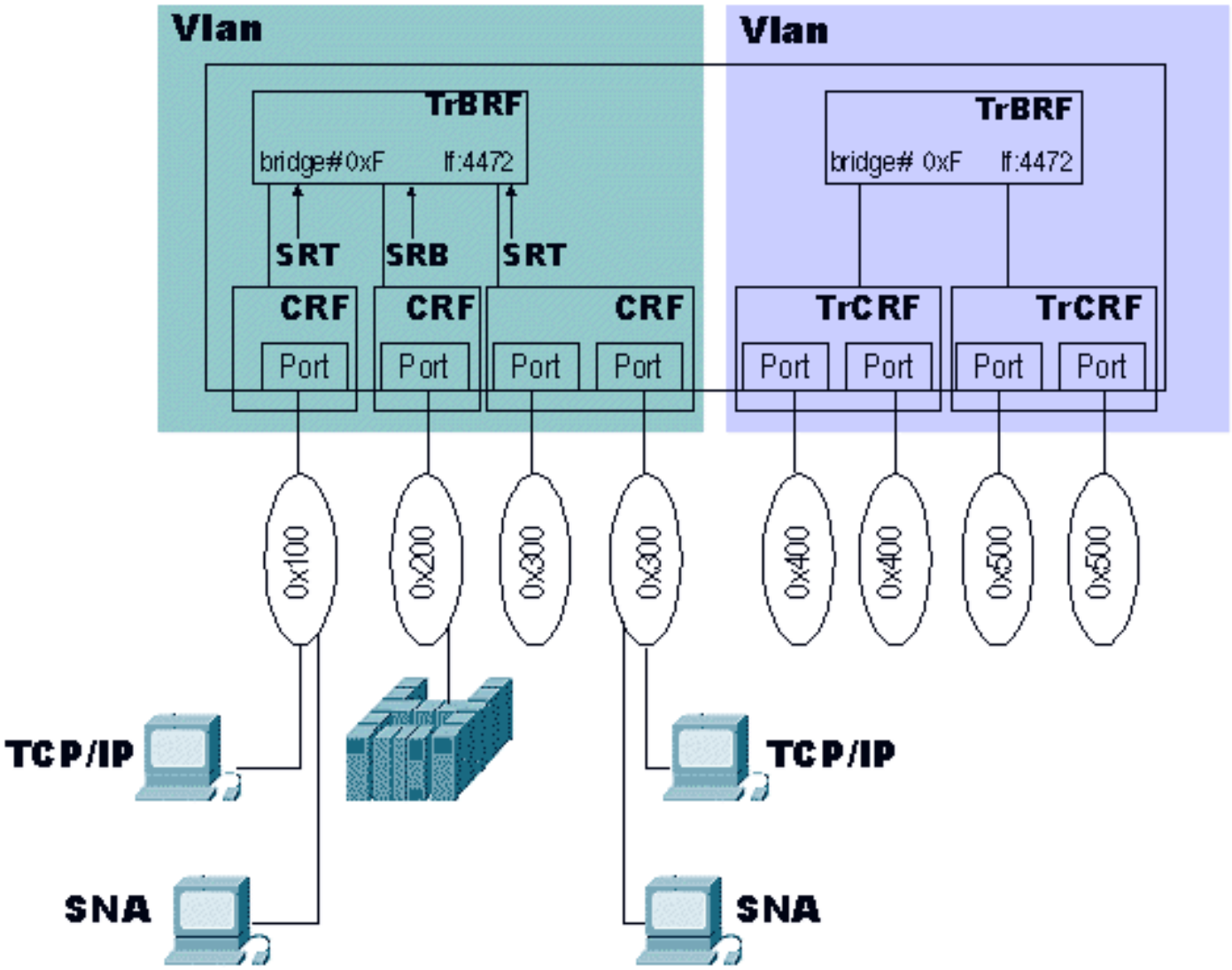
SRS est un transfert de base de paquets basés sur RIF sans fonctionnalité SRB, comme c'est le cas avec TrCRF.

Remarque : pour afficher la table d'informations de routage dans le Catalyst 5000, exécutez la commande **show rif**.

Pontage de route source et transparent de route source

Toutes les fonctionnalités de pontage de route source se trouvent dans la logique TrBRF. Le TrCRF est celui qui va commander le mode de pontage au TrBRF. Ainsi, si le TrCRF est configuré pour le mode SRB vers le TrBRF, alors, lorsque le TrCRF reçoit une trame NSR (non-source-routée), le commutateur ne la transmettra pas à la logique TrBRF.

Cela peut être utilisé si vous ne voulez pas que certains types de trafic atteignent ou quittent un anneau spécifique. Ce schéma présente un exemple :



Si les clients TCP/IP n'avaient pas la capacité d'envoyer des paquets avec des RIF, le commutateur ne placerait pas ces trames dans le même anneau avec le mainframe (0x200). Cependant, les trames SNA vers l'hôte (qui disposent généralement d'un RIF) atteignent le mainframe. Il s'agit d'une façon très rudimentaire de filtrer les trames dans un réseau commuté.

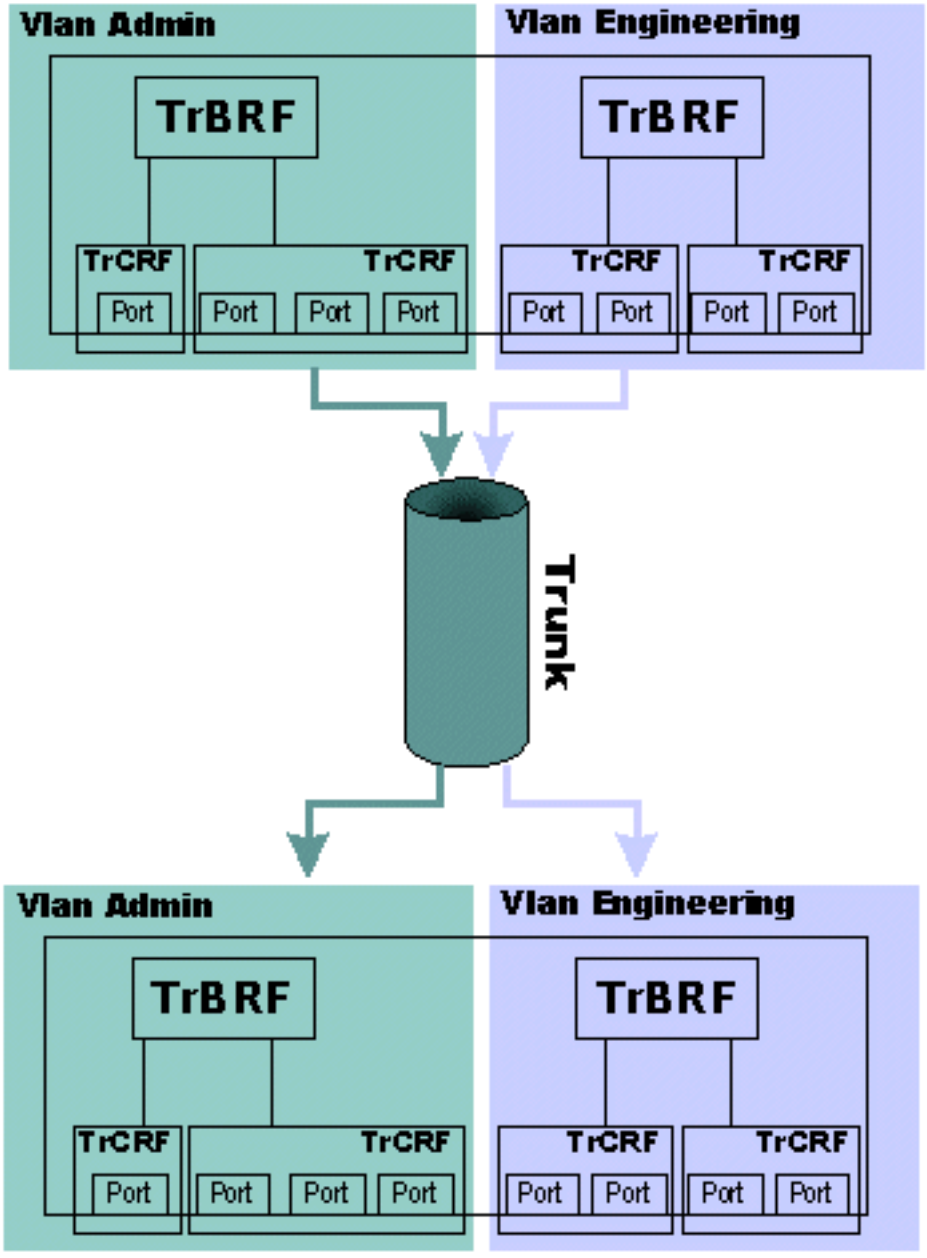
Il s'agit de la séquence que le commutateur suit pour transférer une trame pontée de route source à travers le TrBRF :

1. La station SNA sur l'anneau 0x300 (port 4) envoie un explorateur pour atteindre le mainframe.
2. Lorsque le paquet d'exploration atteint le commutateur, il transfère l'explorateur, sans modification, dans le même TrCRF ; puis il envoie une copie au TrBRF pour la transmettre aux autres TrCRF. Dans ce cas, comme le paquet a un RIF, il passe par le chemin SRB. Le commutateur doit également apprendre la route.
3. Le commutateur va apprendre l'adresse MAC de la trame, car le paquet apparaît comme provenant de l'anneau local auquel le commutateur est connecté. En effet, dans une combinaison TrCRF à plusieurs ports, le RIF indique l'anneau de destination, mais le commutateur doit savoir quel port dans le TrCRF. Par conséquent, le commutateur apprend l'adresse MAC des trames qui entrent au niveau TrCRF.
4. Le paquet est transmis à tous les autres TrCRF, modifiés avec leurs combinaisons respectives de numéros d'anneau de pont.
5. Une fois que l'hôte répond avec la trame SRB, le commutateur apprend l'adresse MAC de

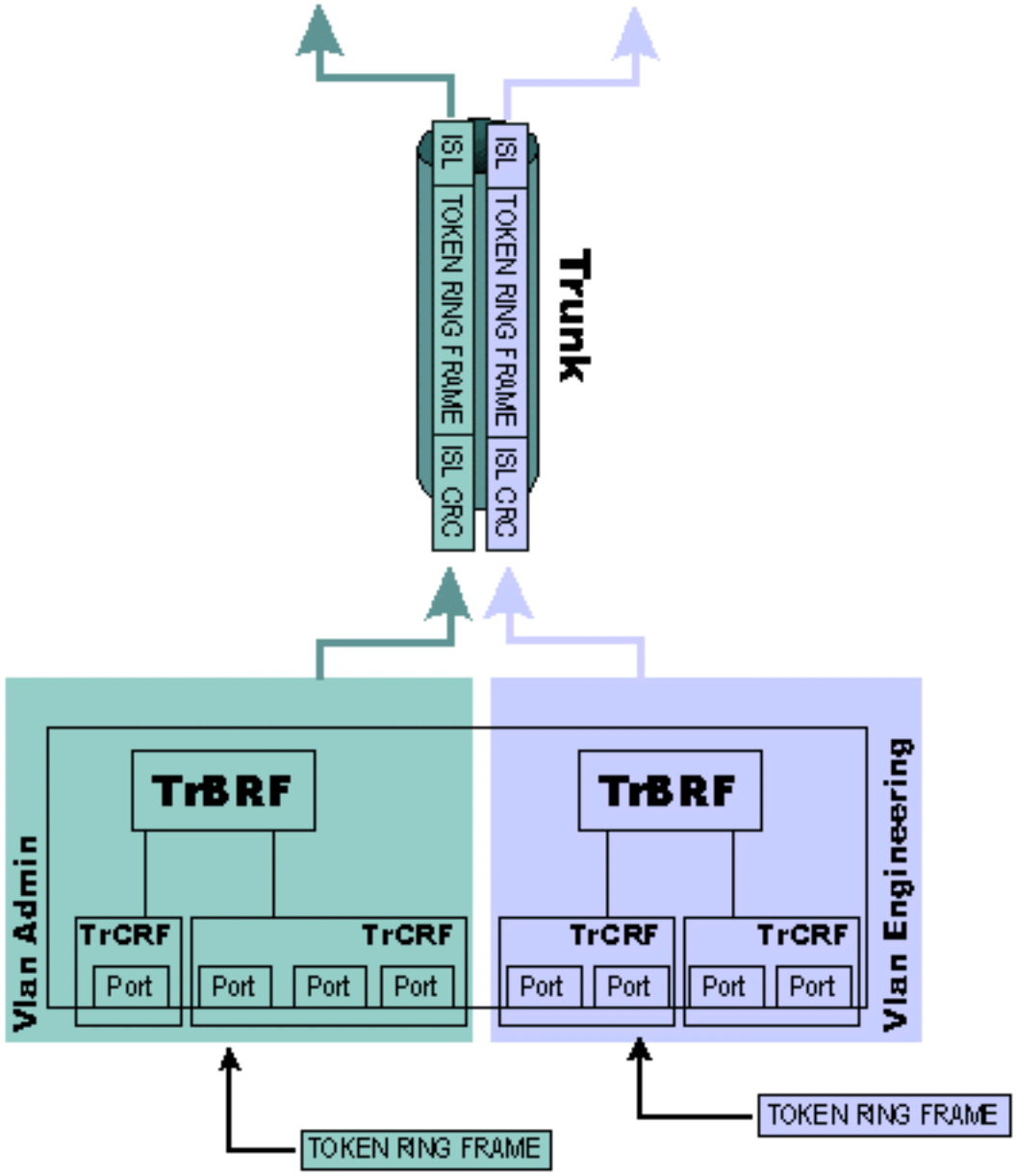
l'hôte pour ce TrCRF et l'envoie au port sortant. Le trafic circule ensuite entre les deux.
Remarque : pour vérifier la table d'adresses MAC sur le Catalyst 5000, exécutez la commande **show cam**.

Liaison entre commutateurs

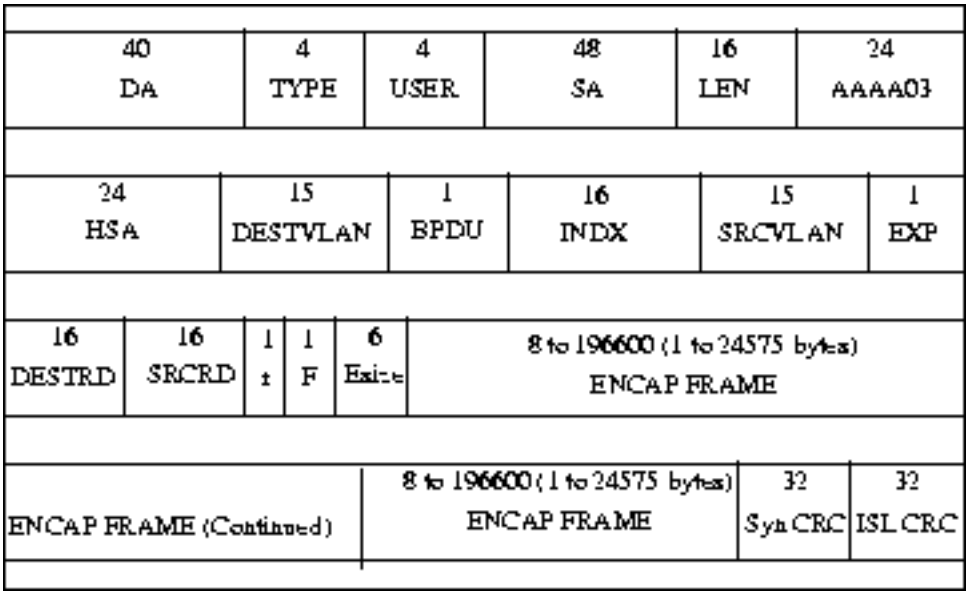
Inter-Switch Link est un protocole très simple. En gros, les trames qui traversent une agrégation ISL sont encapsulées dans une trame ISL qui indique à l'autre côté à quel VLAN appartiennent les trames. De ce fait, les informations VLAN doivent être partagées manuellement ou automatiquement entre les commutateurs. Un protocole appelé VTP (VLAN Trunking Protocol) peut gérer cette tâche. Pour les VLAN Token Ring, vous devez exécuter VTP V2 dans le réseau. Considérez ce diagramme :



Dans ce cas, une seule agrégation ISL a été créée pour transporter, à elle seule, les VLAN d'ingénierie et les VLAN d'administration. Aucun du trafic dans les deux VLAN ne se mélange une fois qu'il passe par l'agrégation. Ce diagramme montre comment cette séparation est réalisée :



Chaque trame de ces VLAN qui doit traverser l'agrégation est encapsulée dans une trame ISL et son VLAN est inclus dans la trame. Cela permet au commutateur récepteur de router correctement la trame vers son VLAN spécifique. La trame TRISL (Token Ring ISL) comporte quelques champs de plus qu'une trame ISL ordinaire. Ce diagramme montre la disposition d'une trame TRISL :



Remarque : Même si TRISL s'exécute sur des interfaces Fast Ethernet, les paquets contiennent une trame Token Ring standard et les informations VLAN associées à cette trame, dans une certaine mesure. Les VLAN Token Ring autorisent jusqu'à 18 000 trames, tout comme ISL. Ceci *n*'est *pas* réalisé par la fragmentation de la trame. L'ensemble de la trame est encapsulé dans une trame ISL en un seul morceau et envoyé sur la liaison. Il est communément admis à tort qu'ISL est Ethernet et que sa taille de trame maximale est de 1 500 octets.

Sur Catalyst 5000, un protocole appelé DTP (Dynamic Trunking Protocol) est devenu disponible dans la version 4.x. Le protocole DTP est le remplacement stratégique de l'ISL dynamique (DISL), car il intègre la prise en charge de la négociation d'agrégation 802.1Q. La fonction de DISL ? ? ? consiste à négocier, pour ISL uniquement, si une liaison entre deux périphériques doit être trunking. DTP est capable de négocier le type d'encapsulation d'agrégation qui sera utilisé entre les agrégations de VLAN ISL et IEEE 802.1Q. Il s'agit d'une fonctionnalité intéressante, car certains périphériques Cisco prennent uniquement en charge ISL ou 802.1Q, alors que d'autres peuvent exécuter les deux.

Voici les cinq états différents pour lesquels vous pouvez configurer DTP :

- Auto : en mode Auto, le port écoute les trames DTP du commutateur voisin. Si le commutateur voisin indique qu'il souhaite être une agrégation (ou qu'il s'agit d'une agrégation), le mode Auto crée l'agrégation avec le commutateur voisin. Cela se produit lorsque le port voisin est défini sur le mode On ou Desirable.
- Souhaitable : le mode Souhaitable indique au commutateur voisin qu'il peut s'agir d'une agrégation ISL et qu'il souhaite que le commutateur voisin soit également une agrégation ISL. Le port devient un port de liaison si le port voisin est défini sur le mode on, desirable ou auto .
- On : le mode On active automatiquement l'agrégation ISL sur son port, quel que soit l'état de son commutateur voisin. Il reste une liaison ISL, à moins qu'il ne reçoive un paquet ISL qui désactive explicitement la liaison ISL.
- Nonegotiate : le mode Nonegotiate active automatiquement l'agrégation ISL sur son port, quel que soit l'état de son commutateur voisin, mais ne permet pas au port de générer des trames DTP.
- Éteint - En mode Éteint, ISL n'est pas autorisé sur ce port, quel que soit le mode DTP configuré sur l'autre commutateur.

La gamme de commutateurs Catalyst 5000 est généralement utilisée pour fournir le réseau fédérateur ISL. Le commutateur Catalyst 3900 peut ensuite être connecté à ce réseau fédérateur

via le module d'extension ISL double 100 Mbits/s. Le commutateur Token Ring Catalyst 3900 ne prend en charge aucun autre mode que ISL, il est donc toujours agrégé. En outre, les modules ISL Catalyst 3900 prennent uniquement en charge les connexions 100 Mbits/s et le mode bidirectionnel simultané par défaut.

Soyez très prudent lorsque vous connectez un commutateur Catalyst 3900 et Catalyst 5000 via la liaison ISL. Le principal problème est que le Catalyst 3900 ne prend pas en charge la négociation de support Fast Ethernet. Pour cette raison, si le Catalyst 5000 est configuré pour le mode Auto, il prend par défaut la valeur 100 Mbits/s en mode semi-duplex. Cela entraîne des problèmes tels que le port passant de trunk à non trunk et la perte de paquets.

Si vous souhaitez connecter le port ISL Catalyst 3900 au port ISL d'un Catalyst 5000, vous devez configurer manuellement le port ISL sur le Catalyst 5000 :

1. Exécutez la commande **set port speed** pour définir à 100 Mbits/s :

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

2. Exécutez la commande **set port duplex** pour définir le mode bidirectionnel simultané :

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

Si vous voulez forcer le port d'un commutateur à passer en mode trunk, émettez la commande **set trunk** (sur une ligne) :

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

Dans la commande précédente, vlans est une valeur comprise entre 1 et 1005 (par exemple, 2-10 ou 1005) et trunk_type est défini sur isl, dot1q, dot10, lane ou negotiation.

Une fois que les ports agrégés sont actifs sur les commutateurs, vous pouvez émettre la commande **show trunk** pour vérifier que ces ports agrégés sont actifs.

```
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
```

Une commande importante à utiliser pour observer les agrégations ISL est la commande **show cdp neighbors detail**. Cette commande vous aide également à comprendre la topologie du réseau.

```
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
```

Àpartir de cette sortie, vous pouvez clairement voir qu'un Catalyst 3900 est connecté au port 10/1. Lorsque vous inspectez le port 10/1 dans la sortie de la précédente commande **show trunk**, vous pouvez dire qu'il s'agit d'un port trunk.

Spanning Tree

Dans les environnements Token Ring, le protocole Spanning Tree peut devenir très compliqué car il est possible d’exécuter simultanément trois protocoles Spanning Tree différents. Par exemple, un environnement type exécute IBM Spanning-Tree au niveau TrBRF et exécute IEEE (802.1d) ou Cisco au niveau TrCRF. Par conséquent, le protocole Spanning Tree est un peu plus compliqué à dépanner.

Ce tableau indique ce qui se passe en fonction des différents types de configurations possibles :

Mode de pontage TrCRF	TrCRF	TrBRF
SRB	Exécute le Spanning Tree IEEE.	Se produit en tant que pont de route source.
	Traite les unités BPDU (Bridge Protocol Data Units) du protocole Spanning Tree IBM à partir de ponts externes.	Exécute les protocoles IBM Spanning Tree sur des ponts

		externes.
		Supprime les BPDU de protocole Spanning Tree IEEE transparentes du TrCRF.
SRT	Exécute le protocole Cisco Spanning Tree.	Il fonctionne comme un pont transparent de route source.
	Remplace l'adresse de groupe de ponts du champ d'adresse de destination par une adresse de groupe spécifique à Cisco, de sorte que les ponts externes n'analysent pas les BPDU TrCRF.	Transfère le trafic transparent et de route source.
	Générez des BPDU, avec le bit RIF défini dans le champ d'adresse source de la trame sortante et un RIF de 2 octets ajouté. Ce format de trame garantit que le TrCRF reste local à l'anneau logique et qu'il n'est pas ponté de manière transparente ni acheminé par la source vers d'autres réseaux locaux. Seuls les TrCRF connectés via des boucles physiques reçoivent les BPDU.	Transfère le trafic de route source à tous les autres TrCRF dans le TrBRF, qu'ils soient en mode SRT ou SRB.
	Traiter les BPDU Spanning Tree IEEE à partir de ponts externes.	

VLAN Trunking Protocol

Puisque, avec ISL, le VLAN détermine où un paquet doit aller, il est important que chaque commutateur connaisse les VLAN du réseau. L'objectif de VTP ? ? ? dans la vie est de propager les informations VLAN sur les commutateurs. Le protocole VTP ne s'exécute pas sur les routeurs, car ils doivent mettre fin au réseau VLAN. Chaque commutateur du réseau doit exécuter le protocole VTP. Si ce n'est pas le cas, le commutateur n'exécute généralement qu'un seul VLAN (généralement VLAN 1) et n'exécute pas ISL sur cette liaison, car il n'y a aucun besoin. Le protocole VTP facilite la création de VLAN, car vous pouvez configurer les VLAN dans un commutateur et les propager sur le réseau. Bien sûr, cela pose problème.

VTP n'est pas un système robuste, comme le protocole EIGRP (Enhanced Interior Gateway

Routing Protocol) ou le protocole de routage OSPF (Open Shortest Path First). Elle est beaucoup plus simple et repose sur un concept très important : révisions. Dans VTP, il existe trois types de périphériques VTP : clients, serveurs et périphériques transparents. Les périphériques VTP clients acceptent simplement les informations VLAN des périphériques serveur et ne peuvent pas modifier ces informations. Les serveurs peuvent cependant modifier les informations VTP sur n'importe quel serveur VTP. Pour cette raison, VTP a un système de révision. Tout serveur VTP qui modifie ou met à jour la base de données VLAN prétend qu'il s'agit de la dernière révision. Pour cette raison, il faut faire preuve d'une extrême prudence, car le commutateur avec la révision la plus élevée gagnera ? ? ? ? ? et ses informations VLAN seront valides. Par exemple, si vous modifiez un serveur VTP pour indiquer que TrBRF VLAN 100 va faire l'arbre recouvrant IEEE, cela causerait des dégâts parmi tous les commutateurs, car cela pourrait faire que les commutateurs (comme Catalyst 3900) mettent les ports en mode de blocage, pour se protéger contre les boucles. En outre, soyez prudent lorsque vous introduisez de nouveaux commutateurs dans le réseau, car ils pourraient avoir des révisions VTP plus élevées. En mode transparent, les paquets VTP reçus sur une agrégation sont automatiquement propagés, sans modification, à toutes les autres agrégations du périphérique ; mais ils sont ignorés sur le périphérique lui-même.

Lorsque vous configurez VTP avec des commutateurs Token Ring, vous devez exécuter VTP V2. Si vous avez des commutateurs qui exécutent à la fois des VLAN Ethernet et Token Ring, vous devez mettre à niveau VTP, même pour les VLAN Ethernet. Vous *ne pouvez pas* avoir deux domaines VTP différents (par exemple, vous ne pouvez pas en avoir un pour Ethernet et un pour Token Ring).

Élagage VTP

Un problème avec l'agrégation de VLAN est que les informations de diffusion d'un VLAN se propagent sur toutes les agrégations, car les commutateurs ne savent pas quels VLAN existent dans un commutateur distant. L'élagage VTP a été créé pour cette raison. Il permet aux commutateurs de négocier les VLAN qui sont attribués aux ports à l'autre extrémité d'une agrégation et, par conséquent, de élaguer les VLAN qui ne sont pas attribués à distance. L'élagage est désactivé par défaut sur les commutateurs Catalyst 3900 et Catalyst 5000.

Remarque : l'élagage VTP est pris en charge sur le commutateur Catalyst 3900 dans la version 4.1(1).

Chacun des messages d'élagage VTP contient des informations sur les VLAN en question et contient un bit qui indique si ce VLAN doit être élagué pour cette agrégation (un `1` indique qu'il ne doit pas être élagué). Lorsque l'élagage est activé, le trafic VLAN n'est normalement pas envoyé sur la liaison agrégée, à moins que la liaison agrégée ne reçoive un message de jointure approprié avec le bit VLAN correspondant activé ? ?. C'est très important car il vous indique que, lorsque vous utilisez l'élagage VTP, vous devez vous assurer que les informations et la configuration correctes existent et que tous les commutateurs exécutent l'élagage ; si un commutateur n'envoie pas de messages de jointure à un autre commutateur sur la liaison, il peut être désactivé pour un ou plusieurs VLAN particuliers. Lorsque la négociation d'élagage est terminée, le VLAN se termine soit en mode élaguage, soit en état joint pour cette agrégation.

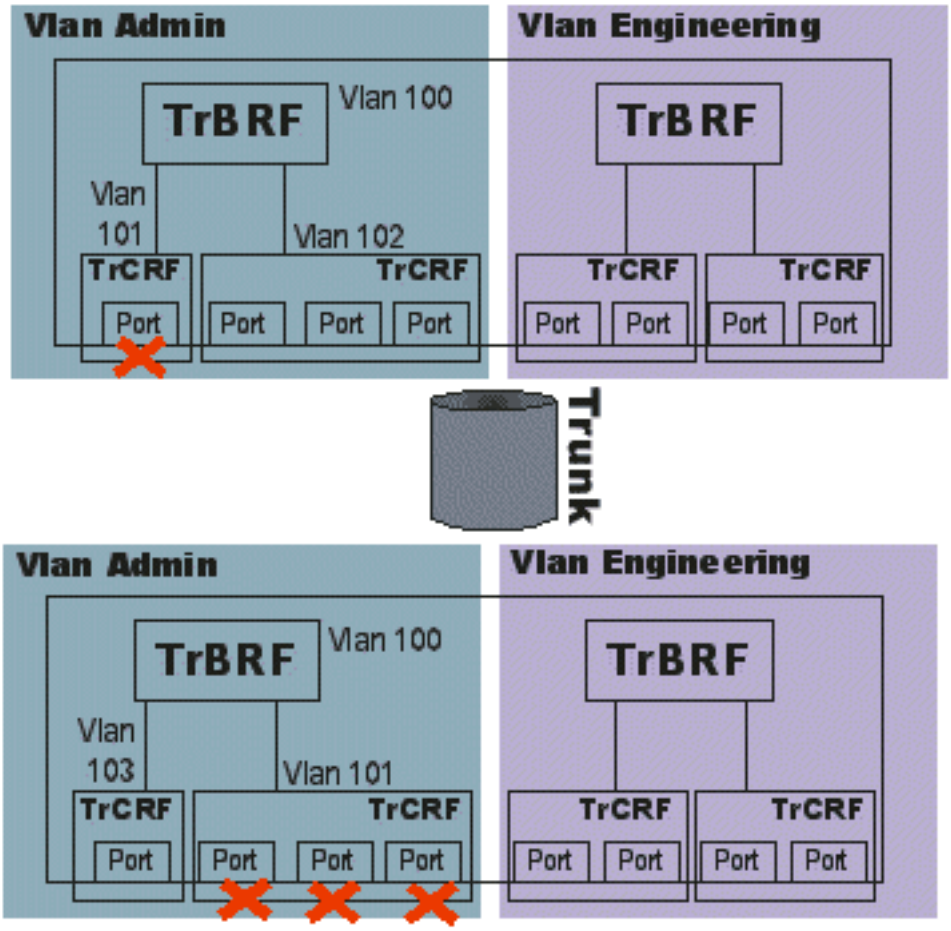
Une fonctionnalité très importante de l'élagage VTP vous permet de configurer un VLAN pour qu'il soit éligible ou non à l'élagage. Cette fonctionnalité indique aux commutateurs qui exécutent l'élagage VTP de ne pas élaguer ce VLAN. Lorsque vous activez l'élagage VTP, les VLAN 2 à 1000 élaguent les VLAN éligibles par défaut. Ainsi, lorsque vous activez l'élagage, il affecte tous les VLAN par défaut. VLAN 1, TrCRF par défaut (1003), TrBRF par défaut (1005) et TrCRF sont toujours non éligibles à l'élagage ; par conséquent, le trafic de ces VLAN ne peut pas être élagué.

Protocole de sonnerie en double

Le protocole Dupliquer Ring est conçu pour s'exécuter sur les commutateurs qui exécutent des VLAN Token Ring. Son travail consiste à assurer la configuration correcte des VLAN Token Ring et à créer une réduction des explorateurs. DRiP utilise VTP pour synchroniser ses informations de base de données VLAN, mais il n'est pas nécessaire pour que DRiP fonctionne (la base de données VLAN peut être établie manuellement). L'une des idées fausses est que DRiP comprend les numéros de sonnerie ; ce n'est pas vrai. Le DRiP repose sur le caractère unique des VLAN configurés dans un réseau et sur cette configuration de base de données VLAN.

L'une des fonctions les plus importantes du DRiP est d'appliquer la distribution TrCRF. Dans le monde Token Ring, il est très dangereux de distribuer tout VLAN autre que 1003, en raison de problèmes de propagation. Pour cette raison, si un TrCRF autre que VLAN 1003 est distribué, tous les ports auxquels ce VLAN est associé sont désactivés par DRiP.

Cet exemple illustre ce concept :



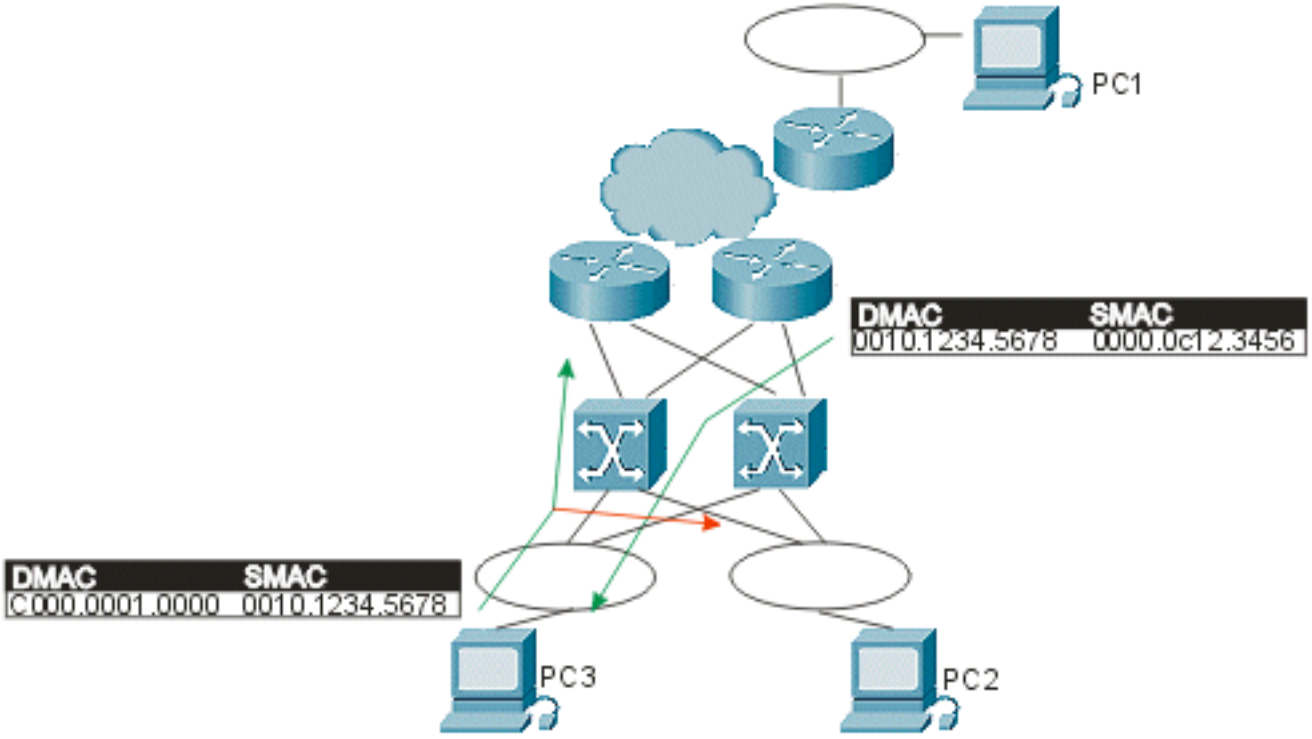
Dans cet exemple, deux commutateurs différents ont un port qui est attribué au VLAN 101. Le commutateur, via DRiP, déplace le spanning-tree du port pour désactiver et arrêter le transfert du trafic. Ceci protège le commutateur contre une éventuelle condition de boucle.

En l'absence de modification, le DRiP annonce l'état TrCRF à tous ses ports agrégés toutes les 30 secondes. Toute modification effectuée via l'interface de ligne de commande (CLI) ou SNMP enverrait immédiatement une mise à jour à tous les ports. Ces annonces sont des trames ISL de type 0 et circulent sur le VLAN 1 par défaut. Comme le DRiP annonce uniquement ses effets pour les VLAN, il est important que les informations de VLAN correctes existent dans les commutateurs connectés via ISL. Ceci est fait via VTP. Si VTP est désactivé, cette fonction doit être gérée

manuellement sur tous les commutateurs qui partagent les mêmes VLAN. Les annonces DRiP n'existent que sur les liaisons ISL. Ils n'existent pas sur ATM, Token Ring, Ethernet ou FDDI. Il n'y a aucune arborescence de topologie conservée dans DRiP.

VLAN HSRP et Token Ring

L'un des plus grands problèmes avec HSRP est l'utilisation de l'adresse de multidiffusion dans le réseau. Étant donné que personne dans le réseau ne crée réellement de paquets avec cette adresse MAC virtuelle, les commutateurs n'apprennent jamais ces adresses MAC. Par conséquent, elles inondent les trames sur l'ensemble du réseau. C'est pourquoi l'utilisation de la fonction **standby use-bia** de HSRP a été requise pour envoyer des paquets qui utilisaient l'adresse MAC brûlée de l'interface de routeur HSRP active. Le principal problème avec ce scénario est que, lorsque les routeurs HSRP basculez, ils doivent envoyer un protocole ARP (Address Resolution Protocol) de diffusion ; ARP gratuit) à toutes les stations du câble, afin que les stations apprennent la nouvelle adresse MAC de la passerelle. Même si ce processus doit fonctionner sur la base des spécifications IP, certains problèmes ont été identifiés. En raison des demandes continues du champ, HSRP a été modifié afin que vous puissiez avoir l'adresse de multidiffusion et également être en mesure d'utiliser HSRP sans **use-bia de secours**. Cette modification a été publiée dans le logiciel Cisco IOS Version 11.3(7) et 12.0(3) et ultérieures.



Dans le schéma précédent, la communication se produit entre PC1 et PC3. Le problème est que le trafic IP du client au routeur par défaut dans cette image utilise une adresse de destination multicast. Comme personne ne peut trouver ce paquet à partir de cette adresse, les commutateurs n'apprennent jamais cette adresse et inondent toujours les paquets. Le DMAC traditionnel qui dépend des groupes est C000.000X.0000, qui ne peut jamais être un SMAC dans Token Ring. Ainsi, tous les paquets destinés de PC3 à PC1 via la passerelle par défaut sont maintenant vus par PC2. Dans un réseau avec beaucoup de ponts, cela peut se multiplier très rapidement et provoquer ce qui pourrait ressembler à des tempêtes de diffusion mais ce qui est en fait une grande quantité de trafic de multidiffusion.

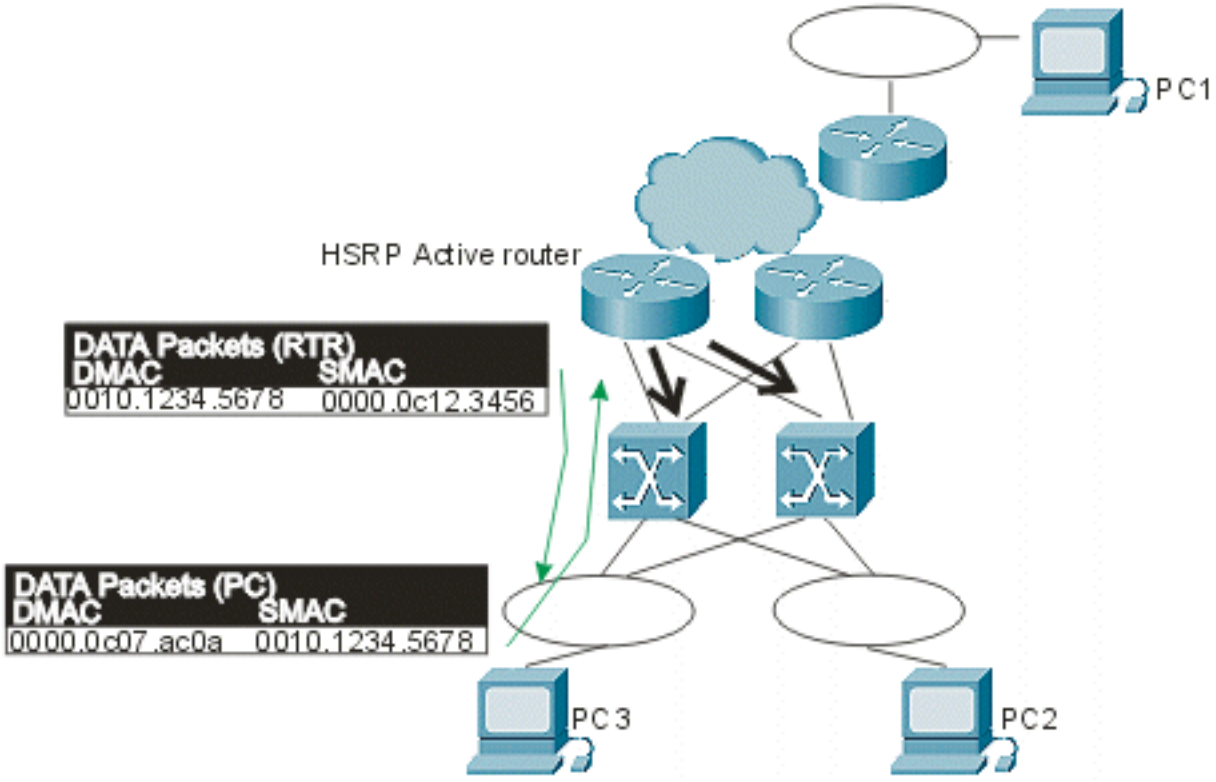
Pour résoudre ce problème, vous devez utiliser une adresse MAC qui peut être utilisée comme adresse MAC par les routeurs dans les HELLO HSRP. Cela permet aux commutateurs

d’apprendre cette adresse et, par conséquent, de commuter les paquets de manière appropriée. Pour ce faire, configurez une nouvelle adresse MAC virtuelle dans les routeurs. Les clients doivent envoyer des paquets au DMAC de cette nouvelle adresse virtuelle. Voici un exemple de sortie d'une commande **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
```

Dans ce résultat, un groupe de secours 10 (IP de secours 1.1.1.100) a été créé. L'adresse MAC (`000.0c07.ac0a`) est la nouvelle adresse MAC virtuelle et le dernier octet est le groupe (0xA = 10). Une fois que vous avez cette nouvelle configuration, vous avez maintenant ce modèle de trafic, qui évite les inondations de trafic :



Maintenant, comme le routeur approvisionne des paquets avec le DMAC de l'adresse MAC virtuelle HSRP, les commutateurs apprennent cette adresse MAC et transmettent uniquement les paquets au routeur HSRP actif. Si le routeur HSRP actif échoue et que la veille devient active, le nouveau routeur actif commence à envoyer des paquets HSRP avec le même SMAC, ce qui fait que les tables d'adresses MAC du commutateur commutent leurs entrées apprises sur le nouveau port de commutateur et la liaison.

En raison de la multiplication des anneaux, des opérations supplémentaires doivent prendre effet pour s’assurer que le RIF change réellement pendant la transition (même s’il s’agit de la même adresse MAC). La multidiffusion est la capacité du routeur à associer un RIF à une adresse MAC, tout comme une station d’extrémité. Les routeurs ont besoin d’une multianneau dans les environnements où des ponts SRB existent, de sorte que les paquets puissent les traverser pour

atteindre les stations d’extrémité.

Dans le même exemple que précédemment, vous pouvez voir les étapes supplémentaires requises pour que le client se connecte au nouveau routeur HSRP actif :

1. Le routeur actif cesse de fonctionner.
2. Une fois que le routeur de secours détecte la perte d'HELLO HSRP, il lance le processus pour devenir le routeur HSRP actif.
3. Le routeur envoie un ARP gratuit à partir du même SMAC que précédemment, dans les deux couches MAC et dans la couche ARP.
4. Le PC envoie maintenant la trame destinée à la même adresse MAC, mais avec le nouveau RIF.
5. Une fois que le routeur reçoit cette trame (destinée à l'adresse MAC HSRP), il envoie une requête ARP directement au client, car il n'a *pas* l'adresse MAC de ce client dans sa table ARP.
6. Une fois que la réponse au paquet ARP est reçue, le routeur peut envoyer des paquets au client de destination.

Informations connexes

- Support pour commutateurs
- Prise en charge de la technologie de commutation LAN
- Support et documentation techniques - Cisco Systems