

Token Ring Switching-Konzepte

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[TrBRF und TrCRF](#)

[Switching-Modi](#)

[Transparentes Bridging](#)

[Source-Route-Switching](#)

[Source-Route-Bridging und transparente Source-Route](#)

[Verbindung zwischen Switches](#)

[Spanning-Tree](#)

[VLAN Trunking Protocol](#)

[VTP-Bereinigung](#)

[Doppeltes Ringprotokoll](#)

[HSRP- und Token-Ring-VLANs](#)

[Zugehörige Informationen](#)

Einführung

Um die Konzepte des Token Ring-Switching zu verstehen, ist es sehr wichtig, dass Sie die Begriffe transparentes Bridging, Source-Route Bridging und Spanning-Tree verstehen. Catalyst 3900 und Catalyst 5000 verwenden neue Konzepte, wie in IEEE 802.5 Annex K beschrieben. Diese Konzepte sind die Bausteine für Token Ring VLANs. In diesem Dokument werden die verschiedenen Bridging-Konzepte und deren Funktionsweise erläutert:

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

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

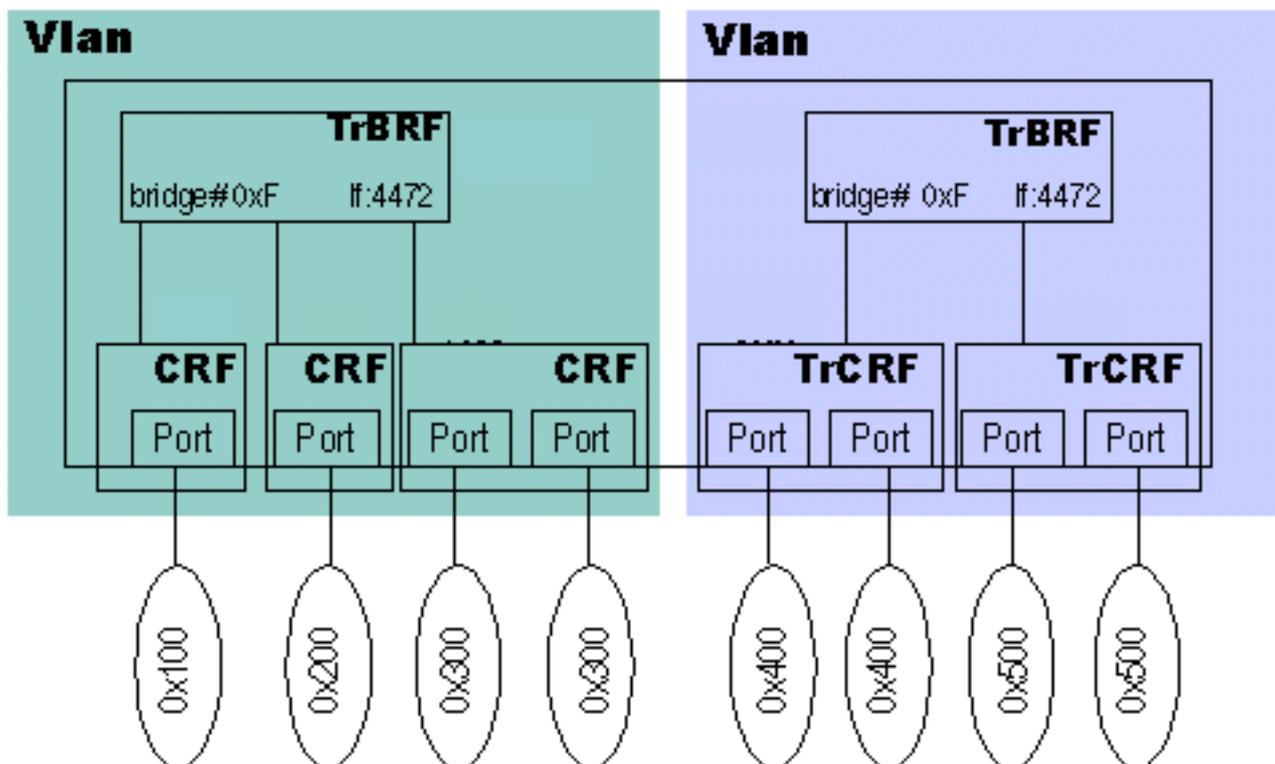
Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

TrBRF und TrCRF

Token Ring Bridge Relay Function (TrBRF) und Token Ring Concentrator Relay Function (TrCRF) sind die Bausteine der Architektur des Catalyst 3900 und der Catalyst 5000-Funktionalität. TrBRF ist einfach die Bridge-Funktion des Switches, und TrCRF ist die Konzentrator-Funktion des Switches. Es ist wichtig zu verstehen, dass Bridging auf beiden Ebenen geschieht, da im Token Ring drei verschiedene Bridging-Typen diskutiert werden.

Die TrBRF-Funktion des Switches steuert das Umschalten von Quell-Route Bridge-Datenverkehr, z. B. Source-Route Bridging (SRB) und Source-Route Transparent Bridging (SRT). Der TrCRF deckt die Funktionalität von Source-Route-Switching (SRS) und transparentem Bridging (TB) ab. So ist es beispielsweise möglich, einen Catalyst 3900-Switch zu verwenden, der nur über einen TrBRF und eine TrCRF verfügt und alle Ports des Switches sich im gleichen TrCRF befinden. Dadurch kann der Switch nur SRS und TB ausführen. Wenn Sie zehn verschiedene TrCRFs unter demselben übergeordneten TrBRF definiert haben, wird der Datenverkehr von Ports, die mit demselben TrCRF verbunden sind, über die TrCRF-Funktionalität von SRS oder TB weitergeleitet. Der Datenverkehr zu den anderen TrCRFs im Switch würde die TrBRF-Funktion des Switches verwenden und entweder als Quell-Route-Bridge oder als Quell-Route-Bridge transparent fungieren. Die verschiedenen Switching-Mechanismen werden später in diesem Dokument behandelt.

In diesem Diagramm werden die TrBRF und die TrCRF mit der physischen Welt verglichen:



Sie sehen, dass jede TrCRF mit einem bestimmten Ring verbunden ist. Eine TrCRF kann mehrere Ports kompromittieren, und diese Ports würden dieselbe Ringnummer gefährden. Der TrBRF verbindet die TrCRFs miteinander.

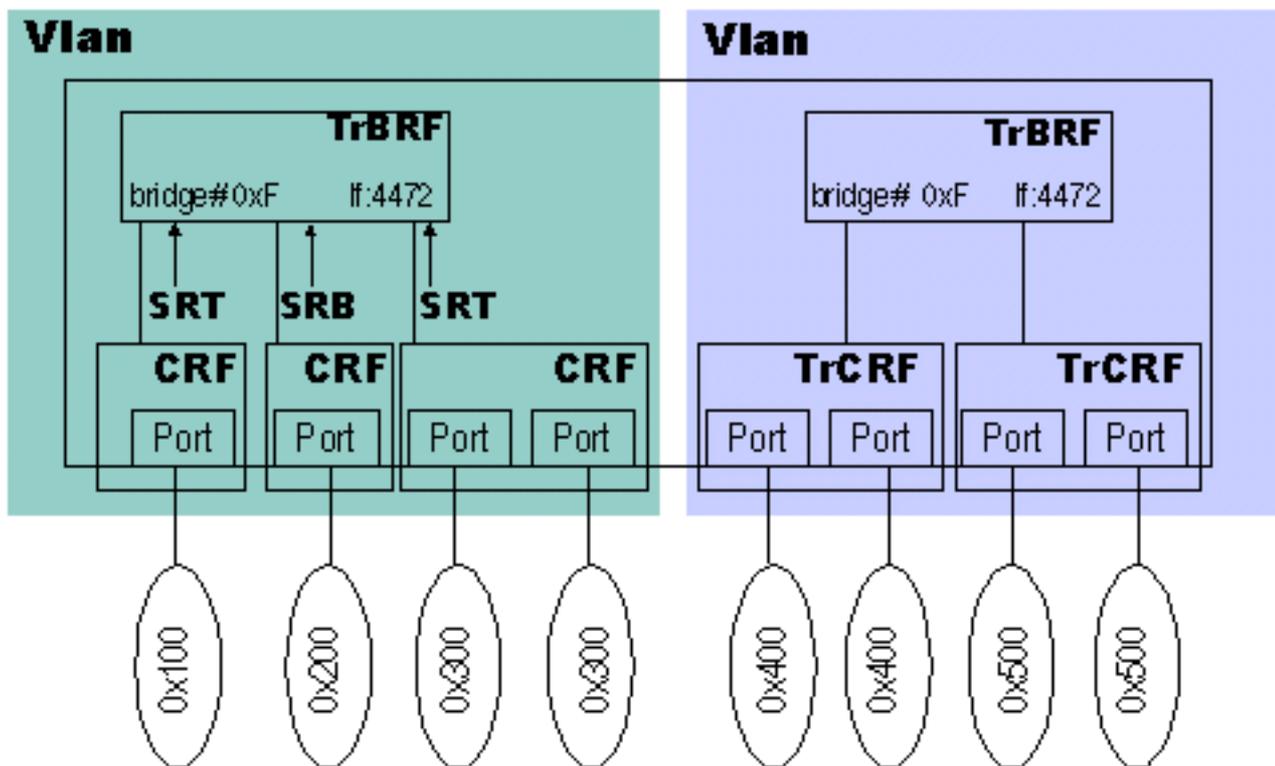
Ein TrCRF und ein TrBRF an sich sind ein anderes VLAN. In Token Ring können Sie also zwischen VLANs wechseln. Beim Bridging zwischen Token-Ring-VLANs werden zwei Regeln befolgt:

- Das Bridging zwischen zwei TrBRF-VLANs kann nur über ein externes Gerät wie einen Router oder ein Route Switch Module (RSM) erfolgen.
- Das Bridging zwischen TrCRF-VLANs kann nur mit TrCRF-VLANs erfolgen, die untergeordnete Elemente desselben übergeordneten TrBRF-VLAN sind.

Dies ist bei Token-Ring-VLANs sehr wichtig, da es das Ethernet-Paradigma durchbricht. Zusammenfassend lässt sich sagen, dass ein Ethernet-VLAN die Summe eines TrBRF und seiner untergeordneten TrCRF ist. Da Sie in Token Ring zwischen bestimmten VLANs eine Brücke schlagen können, müssen Sie wissen, wie diese Bridge erfolgt.

Hinweis: Um das Verständnis von Token Ring-VLANs in Bezug auf Ethernet-VLANs zu vereinfachen, sollten Sie bedenken, dass die Kombination aus TrCRF und TrBRF ein VLAN selbst bildet.

In diesem Diagramm sehen Sie, dass die TrCRF den Bridging-Modus zwischen der TrCRF und der TrBRF bestimmt.



Die einzelnen TrCRFs haben konfiguriert, welche Bridging-Art sie mit dem TrBRF durchführen werden. Dies ist wichtig, da Sie über TrCRF-VLANs verfügen können, die eine Quell-Route-Bridging-Funktion zu anderen TrCRFs ausführen, jedoch keine Frames mit Nicht-Quellrouting ausführen. Im vorherigen Diagramm wird ein TrCRF für den SRB-Modus konfiguriert, zwei befinden sich im SRT-Modus. Dies bedeutet, dass der SRB-Datenverkehr zwischen allen drei TrCRFs fließen kann, SRT jedoch nur zwischen den beiden im SRT-Modus. So können Sie festlegen, wie der Datenverkehr zwischen den TrCRFs fließen soll. Wenn der Bridging-Modus auf dem TrBRF festgelegt wurde, würde dies alle TrCRF-untergeordneten Elemente dieses VLAN betreffen.

Switching-Modi

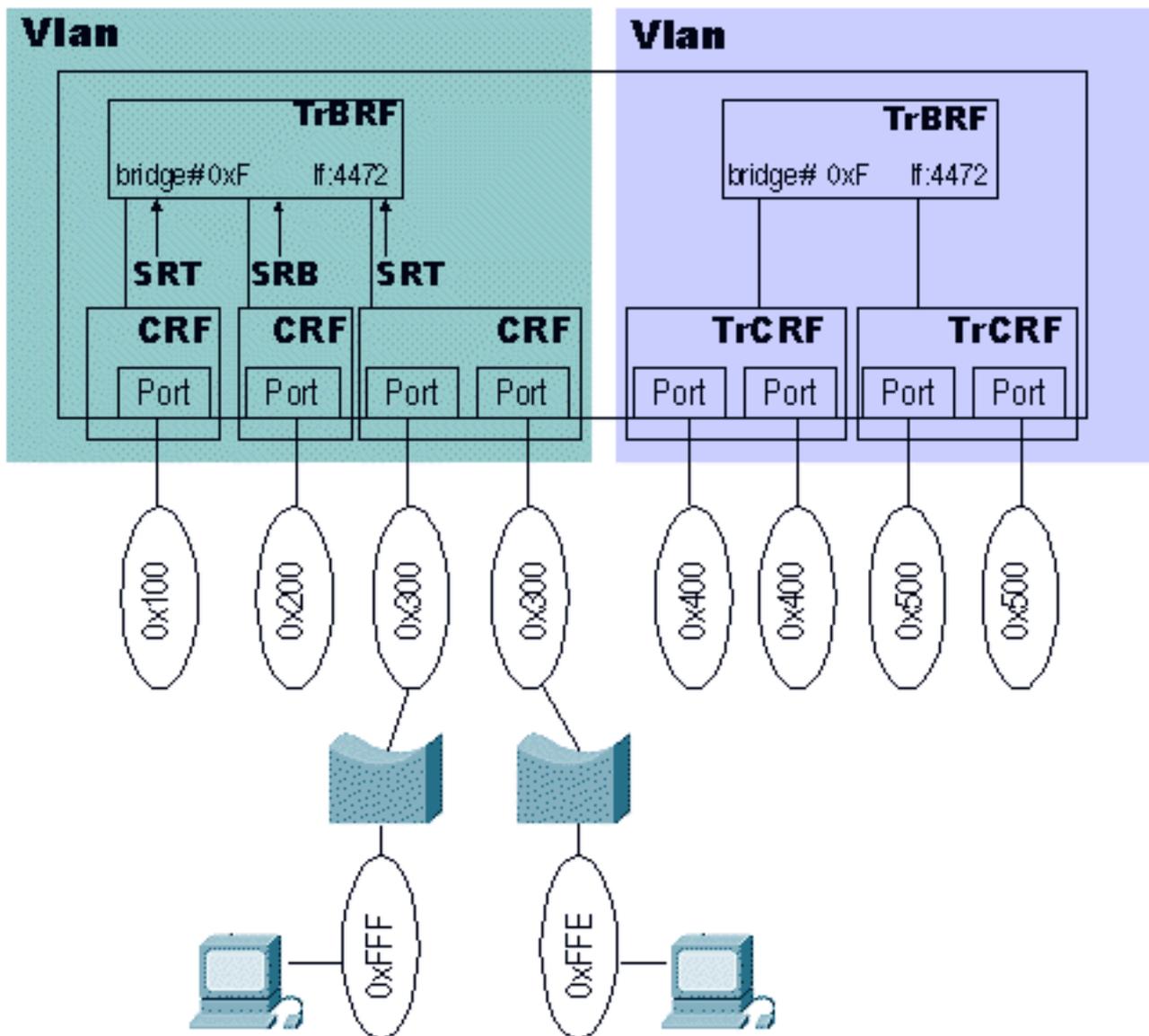
Der Catalyst 3900 ist sofort mit einem TrBRF und einem TrCRF konfiguriert. Alle Ports sind dem Standard-TrCRF-VLAN 1003 zugewiesen. Dasselbe gilt für den Catalyst 5000 Token Ring Blade. Dies ist wichtig, weil es die Box bestimmte ???Plug-and-Play?? Funktionalität. Diese Switches sind sofort einsatzbereit und können Weiterleitung auf Basis von Source-Routing-Switching und transparentem Bridging durchführen. Die nächsten Abschnitte enthalten Details zu diesen Technologien.

Transparentes Bridging

Transparent Bridging ist die grundlegendste aller Switching-Mechanismen und basiert auf der Ziel-MAC-Adresse (DMAC) von Frames im Netzwerk. Dies ist der Weiterleitungsmechanismus von Ethernet-Netzwerken. Jedes Mal, wenn ein Switch einen Frame empfängt, zeichnet er die Quell-MAC-Adresse (SMAC) des Frames als eine Adresse auf, die zu diesem Port gehört, und leitet anschließend Datenverkehr, der für diese MAC-Adresse bestimmt ist, an diesen Port weiter. Wenn ein Switch während des Lernprozesses keine MAC-Adresse kennt, wird dieses Paket an alle Ports im Weiterleitungsstatus übertragen.

Source-Route-Switching

Source-Route-Switching ist ein Weiterleitungsmechanismus, der erforderlich ist, wenn den Ports nur eine TrCRF zugewiesen ist und der Switch Pakete mit Routing Information Fields (RIFs) in diesen empfängt. Da der Switch die RIF des Frames nicht ändert (weil er ihn nicht an den TrBRF übergibt), muss das Netzwerk in der Lage sein, ohne Änderungen Entscheidungen über die Weiterleitung mit dem RIF zu treffen. In diesem Netzwerkdiagramm wird SRS dargestellt:



Der Datenverkehr zwischen Ring 0xFFE und Ring 0xFFF muss den Switch durchlaufen. Dieser Datenverkehr ist Source-Route Bridge-Datenverkehr. Dies ist die Kommunikationsstartsequenz zwischen diesen beiden Clients:

1. Eine Station sendet ein Explorer-Paket an den Ring, auf dem es sich befindet.
Angenommen, der Client im Ring 0xFFF sendet das Paket. es sieht in etwa wie folgt aus (hexadezimal):
0000 00c1 2345 8000 0c11 1111 c270
Hinweis: Diese Paketinformationen enthalten nur DMAC-, SMAC- und RIF-Informationen.
2. Sobald das Paket die Quell-Route-Bridge erreicht und den Frame an die Leitung weiterleitet, sieht das Paket wie folgt aus:
0000 00C1 2345 8000 0c11 1111 C670 FFF1 3000
C670 ist das Routingkontrollfeld und FFF1 3000 Ring 0xFFF, Bridge 0x1, Ring 0x300.
3. Nun trifft das Paket auf den Switch. Da der Switch erkennt, dass das Paket von einem weit entfernten Ring kommt, lernt er den Routendeskriptor. In diesem Fall weiß der Switch jetzt,

dass sich der Ring 0xFFF via Bridge 0x1 auf Port 3 befindet.

4. Da es sich bei dem Paket um ein Explorer-Paket handelt, leitet der Switch den Frame an alle Ports unter derselben TrCRF weiter. Wenn der Explorer zu Ports in verschiedenen TrCRFs wechseln muss, stellt er den Frame an den TrBRF bereit, der seine Bridge-Funktionalität übernimmt. Wenn sich Ports in derselben TrCRF befinden, wird der Frame ohne Änderung an den Ausgang weitergeleitet.
5. Die Station im Ring 0xFFE sollte den Entdecker bekommen und darauf reagieren. Angenommen, der Client antwortet mit einem direkten Frame. Dieser gezielte Rahmen sieht wie folgt aus:
0000 0C11 1111 8000 00C1 2345 08E0 FFF1 3001 FFE0
08E0 ist das Routing-Kontrollfeld und FFF1 3001 FFE0 ist Ring 0xFFF, Bridge 0x1, Ring 0x300, Bridge 0x1, Ring 0xFFE.
6. Schließlich erfährt der Switch, dass sich der Ring 0xFFE auf Port 4 befindet und den Routendeskriptor behält.

Von nun an kennt der Switch diese Ringe. Wenn Sie sich die Tabellen anschauen, sollten Sie sehen, dass der Switch Informationen zur Bridge-Nummer und zur Klingelnummer erhalten hat. Andere Ringe nach 0xFFF und 0xFFE sind nicht erforderlich, da sie entweder durch Ring 0xFFF oder Ring 0xFFE durchlaufen müssen, um den Switch zu erreichen.

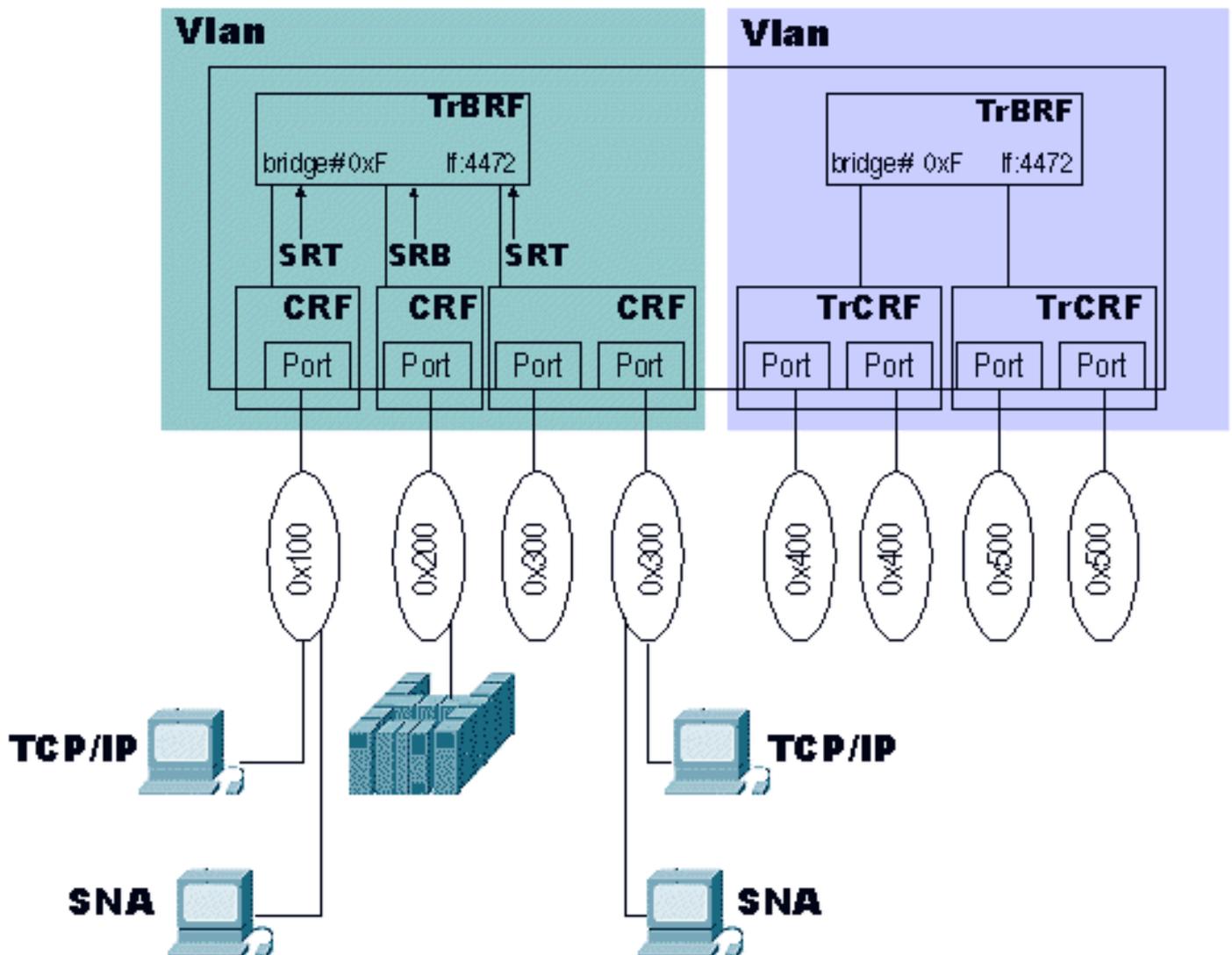
SRS ist eine grundlegende Weiterleitung RIF-basierter Pakete ohne SRB-Funktionalität, wie dies bei der TrCRF der Fall ist.

Hinweis: Geben Sie den Befehl **show rif** ein, um die Routing-Informationstabelle im Catalyst 5000 anzuzeigen.

Source-Route-Bridging und transparente Source-Route

Die gesamte Source-Route-Bridging-Funktionalität befindet sich in der TrBRF-Logik. Der TrCRF steuert den Bridging-Modus zum TrBRF. Wenn die TrCRF für den SRB-Modus zum TrBRF konfiguriert ist, leitet der Switch den NSR-Frame nicht an die TrBRF-Logik weiter, wenn die TrCRF einen NSR-Frame (nicht quellengesteuert) empfängt.

Diese Option kann verwendet werden, wenn bestimmte Arten von Datenverkehr keinen bestimmten Klingelton erreichen oder verlassen sollen. Dieses Diagramm zeigt ein Beispiel:



Wenn die TCP/IP-Clients keine Pakete mit RIFs senden konnten, setzte der Switch diese Frames nicht in denselben Ring wie das Mainframe (0x200). Die SNA-Frames zum Host (die normalerweise über eine RIF verfügen) erreichen jedoch das Mainframe. Dies ist eine sehr rudimentäre Methode zum Filtern von Frames in einem Switch-Netzwerk.

Dies ist die Folge, der der Switch folgt, um einen Quell-Route Bridge-Frame über den TrBRF weiterzuleiten:

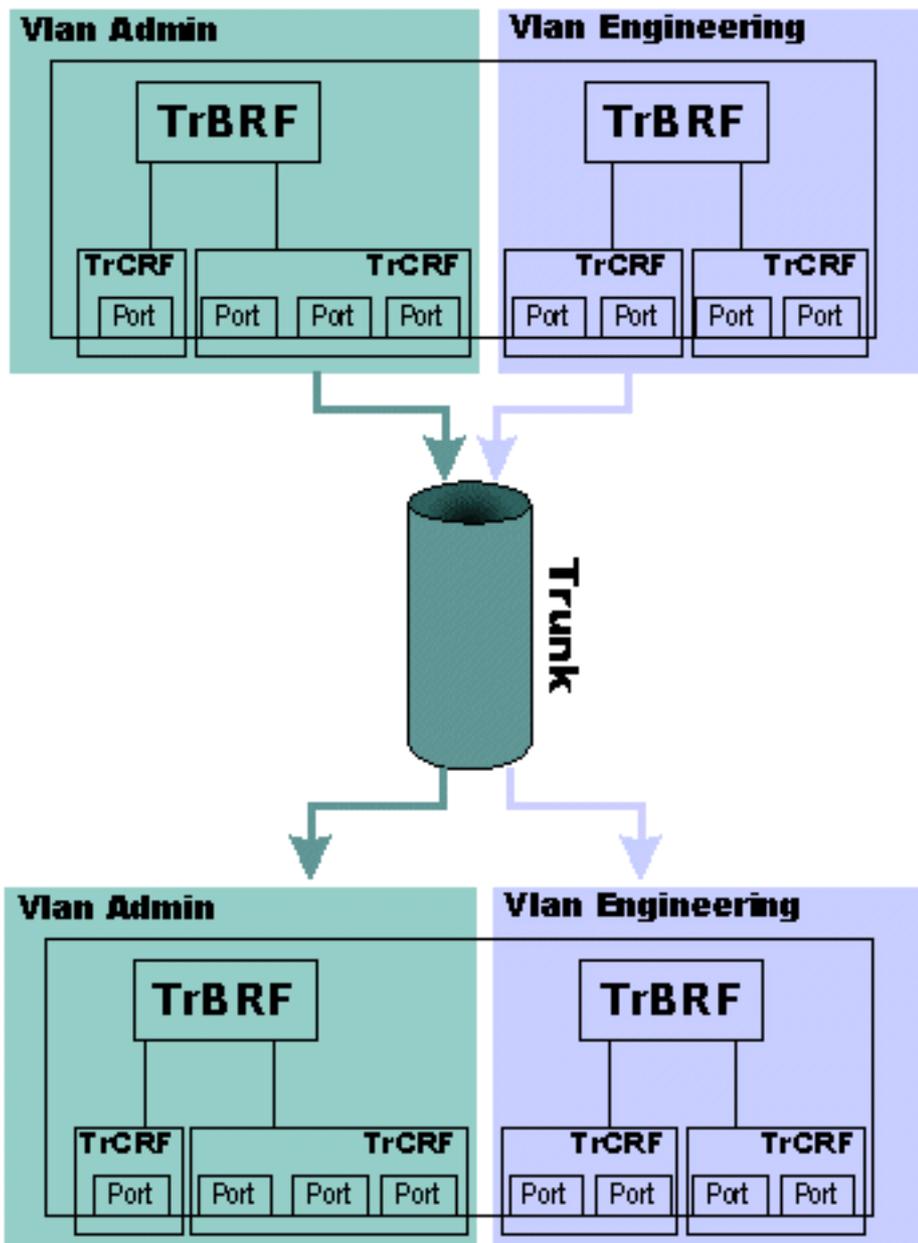
1. Die SNA-Station im Ring 0x300 (Port 4) sendet einen Explorer, um zum Mainframe zu gelangen.
2. Wenn das Explorer-Paket den Switch erreicht, leitet es den Explorer ohne Änderung in derselben TrCRF weiter. dann sendet er eine Kopie an den TrBRF, um sie an die übrigen TrCRFs weiterzuleiten. Da das Paket über eine RIF verfügt, durchläuft es in diesem Fall den SRB-Pfad. Außerdem muss der Switch die Route lernen.
3. Der Switch erkennt die SMAC des Frames, da das Paket als vom lokalen Ring, mit dem der Switch verbunden ist, generiert angezeigt wird. Das liegt daran, dass die RIF in einer Kombination aus mehreren Ports mit TrCRF den Zielring anzeigt, der Switch jedoch wissen muss, welcher Port in der TrCRF vorhanden ist. Aus diesem Grund erfährt der Switch die SMAC der Frames, die auf TrCRF-Ebene eintreffen.
4. Das Paket wird an alle übrigen TrCRFs gesendet, wobei die entsprechenden Kombinationen aus Bridge-Ringnummern geändert werden.
5. Sobald der Host mit dem SRB-Frame antwortet, erfasst der Switch die SMAC des Hosts für

diese TrCRF und sendet sie an den ausgehenden Port. Der Datenverkehr fließt dann zwischen den beiden hin und her.

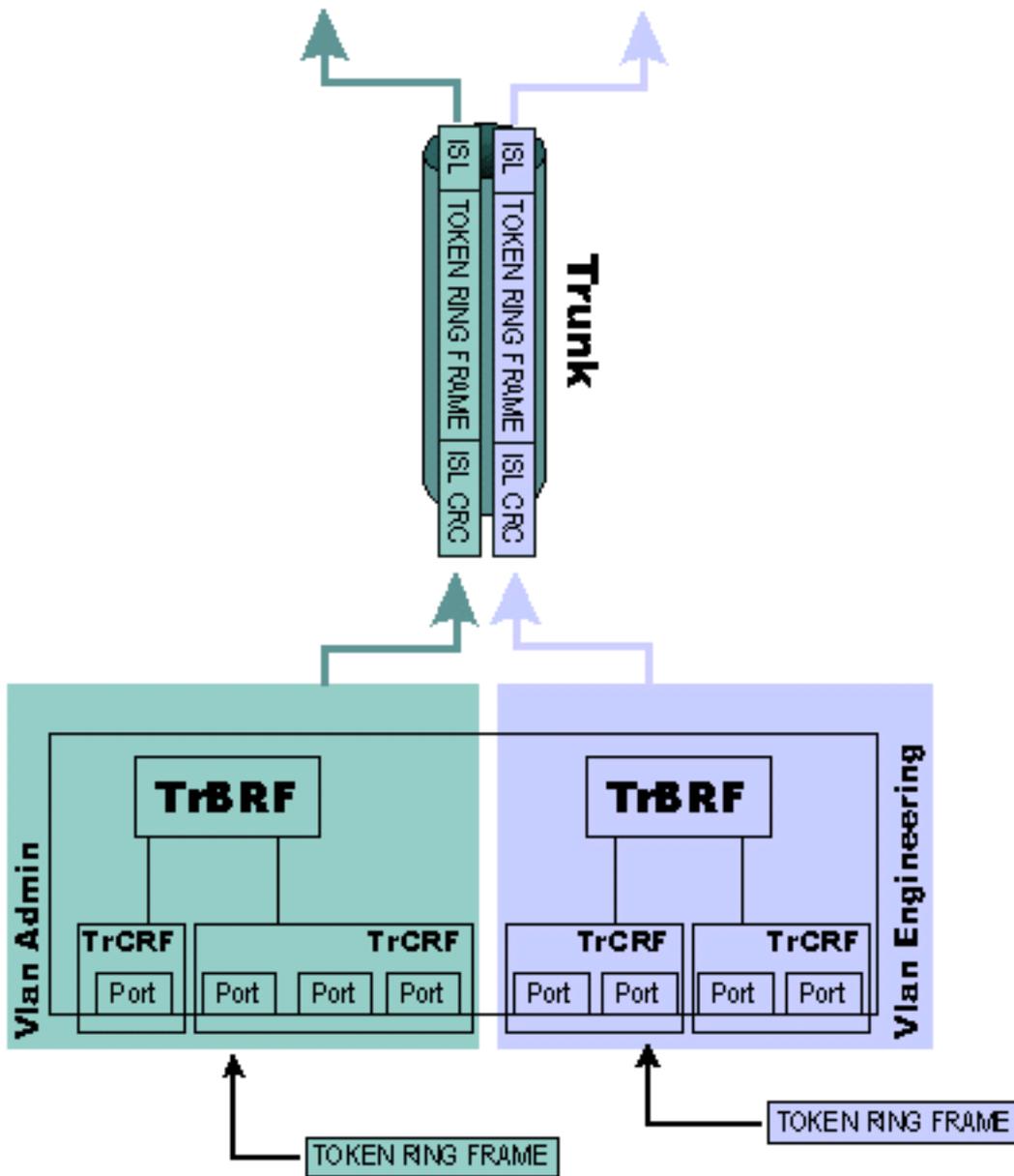
Hinweis: Um die MAC-Adresstabelle auf dem Catalyst 5000 zu überprüfen, führen Sie den Befehl `show cam` aus.

Verbindung zwischen Switches

Inter-Switch Link ist ein sehr einfaches Protokoll. Frames, die über einen ISL-Trunk übertragen werden, werden grundsätzlich in einen ISL-Frame eingekapselt, der der anderen Seite angibt, zu welchem VLAN die Frames gehören. Aus diesem Grund müssen VLAN-Informationen entweder manuell oder automatisch zwischen den Switches freigegeben werden. Ein als VLAN Trunking Protocol (VTP) bezeichnetes Protokoll kann diese Aufgabe bewältigen. Für Token Ring-VLANs muss VTP V2 im Netzwerk ausgeführt werden. Betrachten Sie dieses Diagramm:



In diesem Fall wurde ein einziger ISL-Trunk erstellt, um die Engineering-VLANs und die Admin-VLANs selbst zu übertragen. Kein Datenverkehr in einem VLAN mischt sich, nachdem er den Trunk durchlaufen hat. Dieses Diagramm zeigt, wie diese Trennung erreicht wird:



Jeder Frame der VLANs, die den Trunk durchlaufen müssen, wird in einen ISL-Frame eingekapselt, und das VLAN ist im Frame enthalten. Auf diese Weise kann der empfangende Switch den Frame korrekt in sein spezifisches VLAN weiterleiten. Der TRISL-Frame (Token Ring ISL) verfügt über einige mehr Felder als ein regulärer ISL-Frame. Dieses Diagramm zeigt das Layout eines TRISL-Frames:

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)
DESTRD	SRCRD	T	F	Exist	ENCAP FRAME
ENCAP FRAME (Continued)		8 to 196600 (1 to 24575 bytes)		32	32
		ENCAP FRAME		Syn CRC	ISL CRC

Hinweis: Obwohl TRISL über Fast Ethernet-Schnittstellen ausgeführt wird, enthalten die Pakete einen Token Ring-Standardrahmen und die VLAN-Informationen, die diesem Frame zugeordnet sind, in einem gewissen Umfang. Token Ring-VLANs lassen bis zu 18.000 Frame-Größen zu, ebenso wie ISL. Dies wird *nicht* durch die Fragmentierung des Frames erreicht. Der gesamte Frame wird in einem ISL-Frame in einem ganzen Stück eingekapselt und über die Verbindung gesendet. Es besteht ein allgemeiner Irrtum, dass ISL Ethernet ist und die maximale Frame-Größe 1.500 Byte beträgt.

Auf dem Catalyst 5000 wurde in Version 4.x ein Protokoll namens Dynamic Trunking Protocol (DTP) verfügbar. DTP ist der strategische Ersatz für Dynamic ISL (DISL), da es die Unterstützung von 802.1Q-Trunking-Verhandlungen beinhaltet. DISL?? dient lediglich der Aushandlung, ob eine Verbindung zwischen zwei Geräten als Trunking dienen soll. DTP kann die Art der Trunking-Kapselung aushandeln, die zwischen ISL- und IEEE 802.1Q-VLAN-Trunks verwendet wird. Dies ist eine interessante Funktion, da einige Cisco Geräte nur ISL oder 802.1Q unterstützen, während einige beide Geräte verwenden können.

Es gibt fünf verschiedene Zustände, für die Sie DTP konfigurieren können:

- Auto (Automatisch): Im Auto-Modus überwacht der Port DTP-Frames vom benachbarten Switch. Wenn der benachbarte Switch angibt, dass es sich um einen Trunk handeln soll oder um einen Trunk handelt, erstellt der Auto-Modus den Trunk mit dem benachbarten Switch. Dies geschieht, wenn der benachbarte Port auf On (Ein) oder Desirable (Erwünscht) eingestellt ist.
- Desirable (Erwünscht) - Der Modus Desirable (Erwünscht) gibt dem benachbarten Switch an, dass es sich um einen ISL-Trunk handeln kann und dass der benachbarte Switch auch ein ISL-Trunk sein soll. Der Port wird zu einem Trunk-Port, wenn der benachbarte Port auf den Modus Ein, Erwünscht oder Automatisch eingestellt ist.
- Ein - Der Ein-Modus aktiviert automatisch ISL-Trunking auf seinem Port, unabhängig vom Zustand des benachbarten Switches. Er bleibt ein ISL-Trunk, es sei denn, er empfängt ein ISL-Paket, das den ISL-Trunk explizit deaktiviert.
- Nonegotiate (Nicht verhandeln) - Der Non-egotiate-Modus aktiviert automatisch ISL-Trunking auf seinem Port - unabhängig vom Zustand des benachbarten Switches -, erlaubt dem Port jedoch nicht, DTP-Frames zu generieren.
- Aus - Im Aus-Modus ist ISL für diesen Port nicht zulässig, unabhängig vom DTP-Modus, der auf dem anderen Switch konfiguriert wurde.

Die Catalyst Switches der Serie 5000 werden in der Regel für die Bereitstellung des ISL-Backbones verwendet. Der Catalyst 3900-Switch kann dann über das duale ISL-Erweiterungsmodul mit 100 Mbit/s mit diesem Backbone verbunden werden. Der Catalyst 3900 Token Ring-Switch unterstützt keinen anderen Modus als ISL, daher wird er immer Trunked (Trunking). Darüber hinaus unterstützen die Catalyst 3900 ISL-Module nur Verbindungen mit 100 Mbit/s und die Standardeinstellung für Vollduplex.

Seien Sie vorsichtig, wenn Sie einen Catalyst Switch der Serie 3900 und einen Catalyst Switch der Serie 500 über die ISL-Verbindung verbinden. Das Hauptproblem besteht darin, dass der Catalyst 3900 keine Fast Ethernet-Medienverhandlung unterstützt. Wenn der Catalyst 5000 daher für den Auto-Modus konfiguriert ist, ist die Standardeinstellung 100-Mbit/s-Halbduplex. Dies verursacht Probleme wie den Port, der vom Trunk zum Nicht-Trunk wechselt, und Paketverluste.

Wenn Sie den Catalyst 3900 ISL-Port an den ISL-Port eines Catalyst 5000 anschließen möchten, müssen Sie den ISL-Port auf dem Catalyst 5000 manuell konfigurieren:

1. Geben Sie den Befehl **set port speed (Portgeschwindigkeit festlegen)** auf 100 Mbit/s ein:

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

2. Geben Sie den Befehl **set port duplex** auf full duplex ein:

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

Wenn Sie den Port eines Switches in den Trunk-Modus zwingen möchten, geben Sie den Befehl **set trunk** (auf einer Leitung) ein:

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

Im vorherigen Befehl ist VLANs ein Wert zwischen 1 und 1005 (z. B. 2-10 oder 1005), und trunk_type ist auf isl, dot1q, dot10, lane oder negotiate festgelegt.

Sobald die Trunk-Ports auf den Switches aktiv sind, können Sie den Befehl **show trunk** eingeben, um zu sehen, dass diese Trunk-Ports aktiv sind.

```
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

Ein wichtiger Befehl zur Beobachtung von ISL-Trunks ist der Befehl **show cdp neighbors detail**. Dieser Befehl hilft Ihnen auch, die Netzwerktopologie zu verstehen.

```
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
```

Aus dieser Ausgabe können Sie sehen, dass ein Catalyst 3900 mit Port 10/1 verbunden ist. Wenn Sie Port 10/1 in der Ausgabe des vorherigen Befehls **show trunk** überprüfen, können Sie erkennen, dass es sich um einen Trunk-Port handelt.

Spanning-Tree

Spanning-Tree in Token-Ring-Umgebungen kann sehr kompliziert werden, da man gleichzeitig insgesamt drei verschiedene Spanning-Tree-Protokolle ausführen kann. Beispielsweise wird in einer typischen Umgebung IBM Spanning-Tree auf TrBRF-Ebene ausgeführt und IEEE (802.1d) oder Cisco auf TrCRF-Ebene ausgeführt. Daher ist die Fehlerbehebung für Spanning-Tree etwas komplizierter.

In dieser Tabelle erfahren Sie, was auf der Grundlage der verschiedenen möglichen Konfigurationen geschieht:

TrCRF-Bridging-Modus	TrCRF	TrBRF
SRB	Führt IEEE Spanning Tree aus.	Führt als Quell-Route-Bridge aus.
	Verarbeitet IBM Spanning-Tree Protocol Bridge Protocol Data Units (BPDUs) von externen Bridges.	Führt die IBM Spanning Tree-Protokolle auf externen Bridges aus.
		Legt transparente IEEE Spanning-Tree-Protokoll-BPDUs der TrCRF ab.

SRT	Führt das Cisco Spanning-Tree-Protokoll aus.	Führt als transparente Source-Route-Bridge aus.
	Ersetzt die Bridge-Gruppen-Adresse des Zieladressfelds durch eine Cisco-spezifische Gruppenadresse, sodass externe Bridges keine TrCRF-BPDUs analysieren.	Leitet transparenten und quelloffenen Datenverkehr weiter.
	Generieren Sie BPDUs, wobei das RIF-Bit im Quelladressfeld des ausgehenden Frames festgelegt und ein 2-Byte-RIF hinzugefügt wird. Dieses Frame-Format stellt sicher, dass die TrCRF lokal im logischen Ring bleibt und nicht transparent überbrückt oder an andere LANs weitergeleitet wird. Die BPDUs werden nur an über physische Schleifen verbundene TrCRFs empfangen.	Leiten Sie den Source-Route-Datenverkehr an alle anderen TrCRFs im TrBRF weiter, unabhängig davon, ob sich diese im SRT- oder SRB-Modus befinden.
	Verarbeiten von IEEE Spanning-Tree-BPDUs von externen Bridges.	

VLAN Trunking Protocol

Da das VLAN bei ISL festlegt, wohin ein Paket geleitet werden soll, ist es wichtig, dass jeder Switch über die VLANs im Netzwerk Bescheid weiß. Der Lebenszyklus von VTP? dient der Weitergabe von VLAN-Informationen zwischen Switches. VTP wird nicht in Routern ausgeführt, da sie das VLAN-Netzwerk beenden sollten. Jeder Switch im Netzwerk muss VTP ausführen.

Andernfalls führt der Switch in der Regel nur ein VLAN aus (normalerweise VLAN 1) und führt ISL auf dieser Verbindung nicht aus, da keine Notwendigkeit besteht. VTP vereinfacht die Erstellung von VLANs, da die VLANs in einem Switch konfiguriert und über das Netzwerk verteilt werden können. Das bringt natürlich Probleme mit sich.

VTP ist kein robustes System wie EIGRP (Enhanced Interior Gateway Routing Protocol) oder OSPF (Open Shortest Path First). Es ist viel einfacher und basiert auf einem sehr wichtigen Konzept: Revisionen. In VTP gibt es drei Arten von VTP-Geräten: Clients, Servern und transparenten Geräten. Client-VTP-Geräte akzeptieren im Prinzip nur VLAN-Informationen von Servergeräten und können diese Informationen nicht ändern. Server können jedoch VTP-Informationen auf jedem VTP-Server ändern. Aus diesem Grund verfügt VTP über ein Revisionsystem. Jeder VTP-Server, der die VLAN-Datenbank ändert oder aktualisiert, gibt an, dass es sich um die neueste Version handelt. Aus diesem Grund ist äußerste Vorsicht geboten, da der Switch mit der höchsten Revision den Preis gewinnen wird??? und die VLAN-Informationen sind gültig. Wenn Sie beispielsweise einen VTP-Server so ändern, dass TrBRF VLAN 100 IEEE-Spanning-Tree ausführen wird, würde dies zu Chaos unter allen Switches führen, da dies Switches (wie den Catalyst 3900) dazu führen könnte, Ports in den Blockierungsmodus zu versetzen, um sich vor Schleifen zu schützen. Seien Sie auch vorsichtig, wenn Sie neue Switches in das Netzwerk einführen, da diese möglicherweise höhere VTP-Revisionen aufweisen. Im transparenten Modus werden auf einem Trunk empfangene VTP-Pakete ohne Änderungen automatisch an alle anderen Trunks auf dem Gerät weitergeleitet. Sie werden jedoch auf dem Gerät selbst ignoriert.

Wenn Sie VTP mit Token Ring Switches einrichten, müssen Sie VTP V2 ausführen. Wenn Sie Switches haben, die sowohl Ethernet- als auch Token Ring-VLANs ausführen, müssen Sie VTP aktualisieren, auch für die Ethernet-VLANs. Sie *können nicht* zwei verschiedene VTP-Domänen haben (z. B. keine für Ethernet und eine für Token Ring).

VTP-Bereinigung

Ein Problem beim VLAN-Trunking besteht darin, dass Broadcast-Informationen von einem VLAN über alle Trunks verteilt werden, da die Switches nicht wissen, welche VLANs in einem Remote-Switch vorhanden sind. Aus diesem Grund wurde VTP-Bereinigung erstellt. Es ermöglicht Switches auszuhandeln, welche VLANs Ports am anderen Ende eines Trunks zugewiesen sind, und somit die VLANs zu sperren, die nicht remote zugewiesen sind. Pruning ist auf Catalyst Switches der Serien 3900 und 5000 standardmäßig deaktiviert.

Hinweis: VTP-Bereinigung wird vom Catalyst 3900-Switch in Version 4.1(1) unterstützt.

Jede der VTP-Bereinigungsmeldungen enthält Informationen zu den betreffenden VLANs und enthält ein Bit, das angibt, ob dieses VLAN für diesen Trunk bereinigt werden soll oder nicht (eine 1 bedeutet, dass er nicht bereinigt werden sollte). Bei aktivierter Bereinigung wird normalerweise kein VLAN-Datenverkehr über die Trunk-Verbindung gesendet, es sei denn, der Trunk-Link erhält eine entsprechende Join-Nachricht, wobei das entsprechende Bit des VLAN aktiviert ist. Dies ist sehr wichtig, da es Ihnen sagt, dass Sie beim Verwenden von VTP-Bereinigung sicherstellen müssen, dass die richtigen Informationen und Konfigurationen vorhanden sind und dass alle Switches bereinigt werden. Wenn ein Switch keine Join-Nachrichten an einen anderen Switch über den Trunk sendet, kann er für ein bestimmtes VLAN oder bestimmte VLANs abgeschaltet werden. Wenn die Aushandlung abgeschlossen ist, endet das VLAN entweder im Zustand "Abgeschnitten" oder "Verbunden" für diesen Trunk.

Eine sehr wichtige Funktion der VTP-Bereinigung ermöglicht es Ihnen, ein VLAN so zu

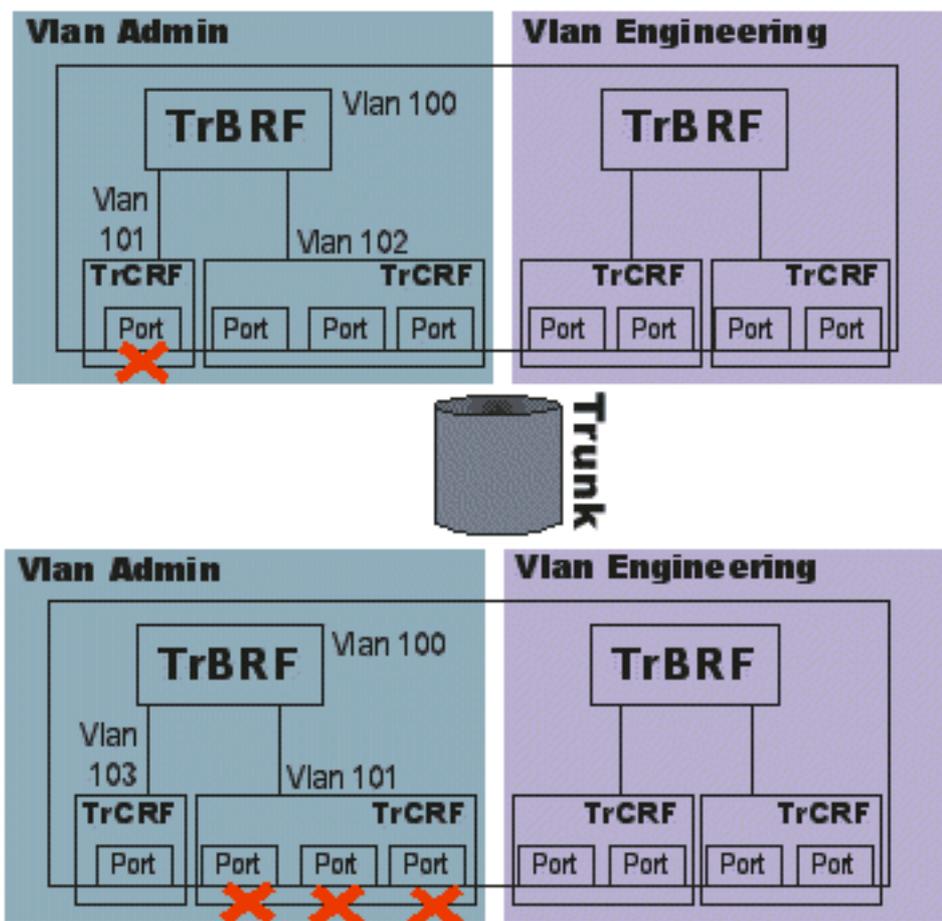
konfigurieren, dass es für die Bereinigung qualifiziert ist oder nicht. Diese Funktion weist die Switches, die VTP bereinigen, an, dieses VLAN nicht zu bereinigen. Wenn Sie die VTP-Bereinigung aktivieren, werden die VLANs 2 bis 1000 standardmäßig mit den zulässigen VLANs verbunden. Wenn Sie also die Bereinigung aktivieren, betrifft dies standardmäßig alle VLANs. VLAN 1, die Standard-TrCRF (1003), die Standard-TrBRF (1005) und die TrCRFs sind immer nicht qualifiziert; Daher kann der Datenverkehr dieser VLANs nicht bereinigt werden.

Doppeltes Ringprotokoll

Das Doppelring-Protokoll wurde für die Ausführung auf Switches entwickelt, auf denen Token Ring-VLANs ausgeführt werden. Die Aufgabe besteht darin, die korrekte Konfiguration der Token Ring-VLANs sicherzustellen und eine Explorerrückmeldung zu erreichen. DRiP verwendet VTP zur Synchronisierung seiner VLAN-Datenbankinformationen, ist jedoch nicht für die DRiP-Funktion erforderlich (die VLAN-Datenbank kann manuell eingerichtet werden). Ein Missverständnis besteht darin, dass DRiP Ringnummern versteht. Das stimmt nicht. DRiP basiert auf der Einzigartigkeit der in einem Netzwerk konfigurierten VLANs und der Konfiguration der VLAN-Datenbank.

Eine der wichtigsten Funktionen von DRiP ist die Durchsetzung der TrCRF-Verteilung. In der Token Ring-Welt ist es aufgrund von Spanning-Problemen sehr gefährlich, jedes VLAN außer 1003 zu verteilen. Aus diesem Grund werden alle Ports, denen dieses VLAN zugeordnet ist, durch DRiP deaktiviert, wenn eine andere TrCRF als VLAN 1003 verteilt wird.

Dieses Beispiel veranschaulicht dieses Konzept:

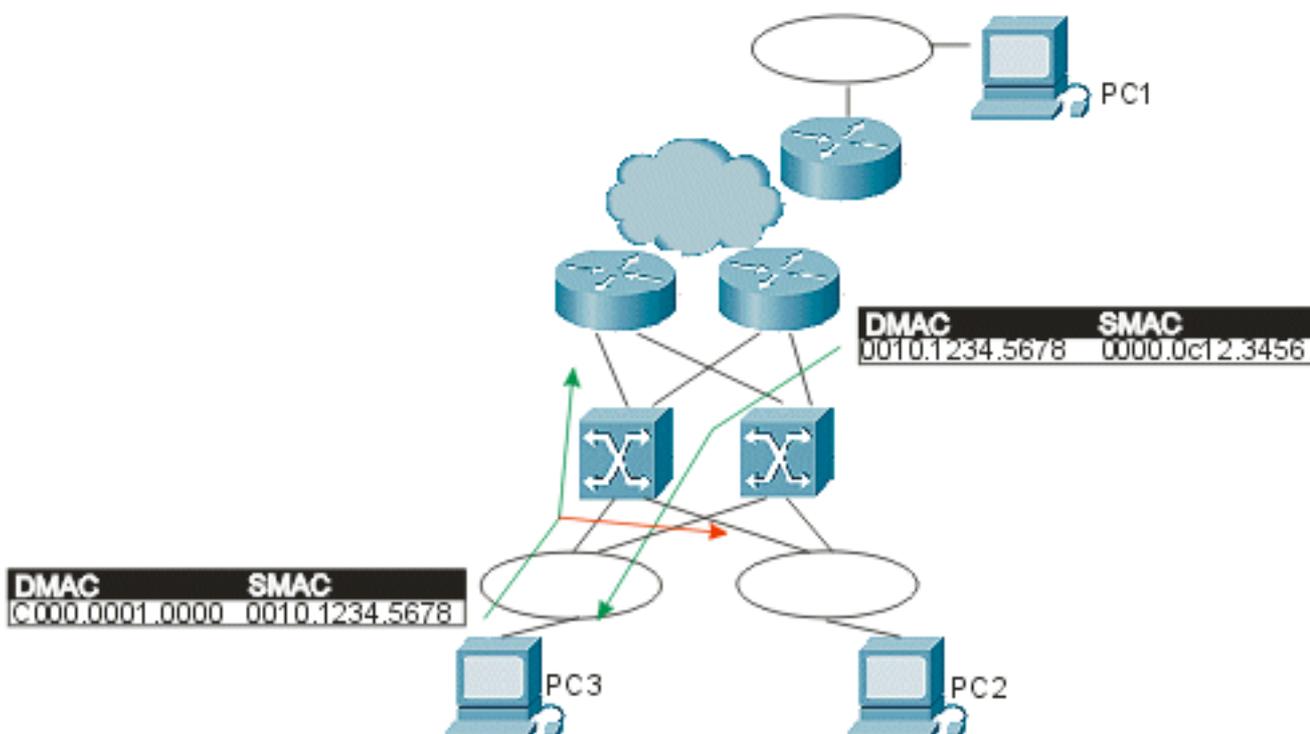


In diesem Beispiel haben zwei verschiedene Switches einen Port, der VLAN 101 zugewiesen ist. Der Switch verschiebt den Port-Spanning-Tree über DRiP, um den Weiterleitungsverkehr zu deaktivieren und zu stoppen. Dies schützt den Switch vor einer möglichen Schleifenbedingung.

Wenn keine Änderung eintritt, informiert DRiP alle 30 Sekunden alle Trunk-Ports über den TrCRF-Status. Jede Änderung über die CLI (Command Line Interface) oder SNMP würde sofort eine Aktualisierung an alle Ports senden. Diese Meldungen sind Typ 0-ISL-Frames und werden im Standard-VLAN 1 ausgeführt. Da DRiP nur die Auswirkungen für VLANs meldet, ist es wichtig, dass die richtigen VLAN-Informationen in den Switches vorhanden sind, die über ISL verbunden sind. Dies erfolgt über VTP. Wenn VTP deaktiviert ist, muss diese Funktion von allen Switches, die dieselben VLANs gemeinsam nutzen, manuell aufrechterhalten werden. DRiP-Werbung existiert nur auf ISL-Links. Sie sind nicht auf ATM, Token Ring, Ethernet oder FDDI verfügbar. Im DRiP werden keine Topologiestrukturen gespeichert.

HSRP- und Token-Ring-VLANs

Eines der größten Probleme bei HSRP ist die Verwendung der Multicast-Adresse im Netzwerk. Da niemand im Netzwerk Pakete mit dieser virtuellen MAC-Adresse tatsächlich bereitstellt, lernen die Switches diese MAC-Adressen nie. Daher überfluten sie Frames im gesamten Netzwerk. Aus diesem Grund musste die **Standby-Use-bia**-Funktion von HSRP Pakete senden, die die gebrannte MAC-Adresse der aktiven HSRP-Router-Schnittstelle verwendeten. Das Hauptproblem bei diesem Szenario besteht darin, dass der Switch der HSRP-Router ein Broadcast Address Resolution Protocol (ARP) senden müsste. frei zugänglichen ARP) an alle Stationen im Kabel, sodass die Stationen die neue MAC-Adresse des Kabelmodems erfassen. Obwohl dieser Prozess auf IP-Spezifikationen basieren sollte, gab es einige bekannte Probleme damit. Aufgrund der fortlaufenden Anfragen aus dem Feld wurde das HSRP so geändert, dass Sie die Multicast-Adresse haben und auch HSRP ohne **Standby-Use-bia** verwenden können. Diese Änderung wurde in der Cisco IOS Software-Version 11.3(7) und 12.0(3) und höher veröffentlicht.



Im vorherigen Diagramm wird die Kommunikation zwischen PC1 und PC3 hergestellt. Das Problem besteht darin, dass der IP-Datenverkehr vom Client zum Standardrouter in diesem Bild eine Multicast-Zieladresse verwendet. Da niemand dieses Paket von dieser Adresse beziehen kann, lernen die Switches diese Adresse nie und überfluten immer die Pakete. Die traditionelle DMAC, die von den Gruppen abhängt, ist C000.000X.000, was niemals ein SMAC im Token Ring sein kann. Alle Pakete, die von PC3 an PC1 über das Standard-Gateway gesendet werden, werden jetzt von PC2 erkannt. In einem Netzwerk mit vielen Brücken kann sich dies sehr schnell

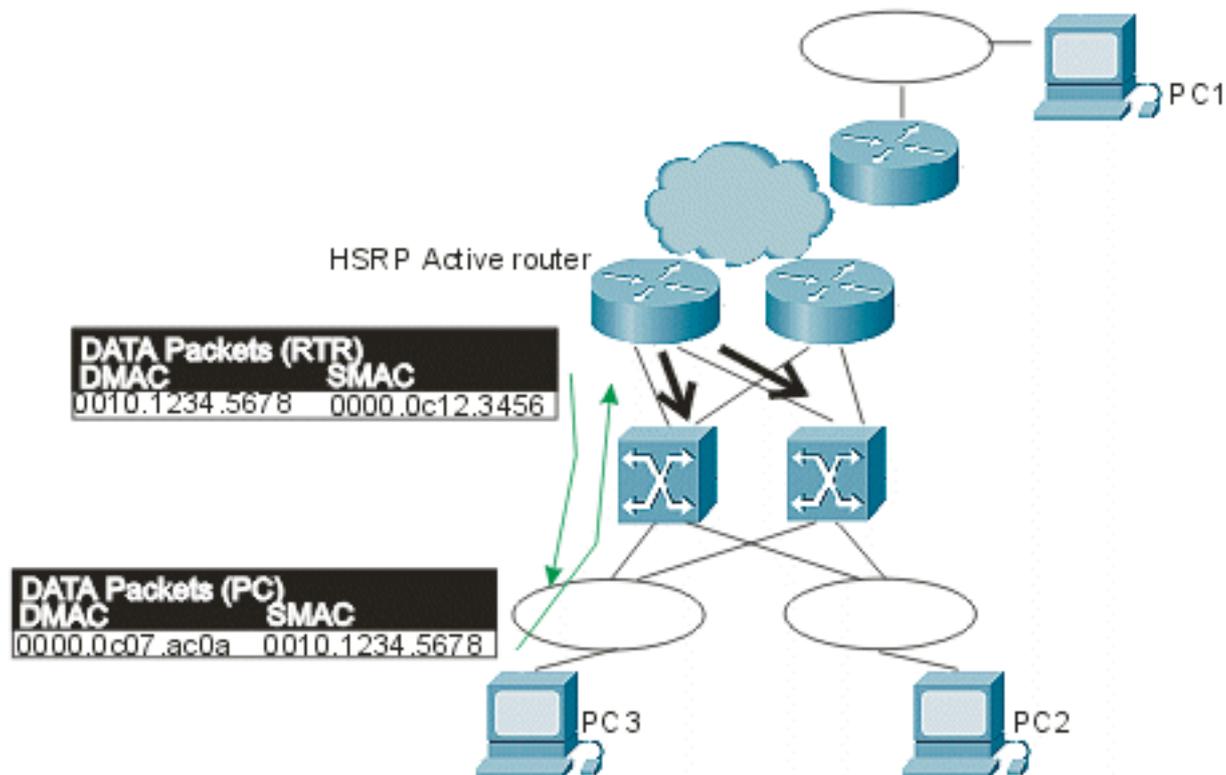
vermehren und so scheinbar Broadcast-Stürme verursachen, aber tatsächlich ist dies ein großer Teil des Multicast-Datenverkehrs.

Um dieses Problem zu beheben, müssen Sie eine MAC-Adresse verwenden, die von den Routern in den HSRP-Hellos als SMAC verwendet werden kann. Auf diese Weise können die Switches diese Adresse ermitteln und die Pakete entsprechend verteilen. Konfigurieren Sie dazu eine neue virtuelle MAC-Adresse in den Routern. Clients müssen Pakete an die DMAC dieser neuen virtuellen Adresse senden. Dies ist die Beispielausgabe eines **show standby**-Befehls:

```
vd1-rsm# show standby
```

```
Vlan500 - Group 10  
Local state is Active, priority 100  
Hellotime 3 holdtime 10  
Next hello sent in 00:00:01.224  
Hot standby IP address is 1.1.1.100 configured  
Active router is local  
Standby router is unknown expired  
Standby virtual mac address is 0000.0c07.ac0a
```

In dieser Ausgabe wurde eine Standby-Gruppe 10 (Standby-IP 1.1.1.100) erstellt. Die MAC-Adresse (0000.0c07.ac0a) ist die neue virtuelle MAC-Adresse, und das letzte Byte ist die Gruppe (0xA = 10). Sobald Sie diese neue Konfiguration haben, erhalten Sie dieses Datenverkehrsmuster, das Überschwemmungen im Datenverkehr verhindert:



Da der Router Pakete mit der DMAC-Adresse der virtuellen HSRP-MAC-Adresse bezieht, erhalten die Switches diese MAC-Adresse und leiten die Pakete nur an den aktiven HSRP-Router weiter. Wenn der aktive HSRP-Router ausfällt und der Standby-Router aktiv ist, beginnt der neue aktive Router, HSRP-Hellos mit demselben SMAC zu senden, was dazu führt, dass die MAC-Adresstabellen des Switches ihre erfassten Einträge auf den neuen Switch-Port und den neuen Trunk umschalten.

Aufgrund des Multiring-Vorgangs muss ein zusätzlicher Vorgang wirksam werden, um

sicherzustellen, dass sich die RIF während der Übergangsphase tatsächlich ändert (obwohl es sich um dieselbe MAC-Adresse handelt). Multiring ist die Fähigkeit des Routers, eine RIF einer MAC-Adresse wie eine Endstation zuzuordnen. Die Router müssen in Umgebungen, in denen SRB-Brücken vorhanden sind, mehrere Verbindungen aufweisen, sodass Pakete diese passieren können, um Endstationen zu erreichen.

Im gleichen Beispiel wie zuvor werden die zusätzlichen Schritte angezeigt, die der Client für die Verbindung mit dem neuen aktiven HSRP-Router benötigt:

1. Der aktive Router funktioniert nicht mehr.
2. Sobald der Standby-Router den Verlust von HSRP-Hellos erkennt, initiiert er den Prozess, um zum aktiven HSRP-Router zu werden.
3. Der Router sendet ein grundloses ARP von demselben SMAC wie zuvor, sowohl in der MAC-Schicht als auch in der ARP-Schicht.
4. Der PC sendet jetzt den Frame an dieselbe MAC-Adresse, jedoch mit der neuen RIF.
5. Sobald der Router diesen Frame empfängt (der für die HSRP-MAC-Adresse bestimmt ist), sendet er direkt eine ARP-Anfrage an den Client, da er *nicht* über die MAC-Adresse dieses Clients in seiner ARP-Tabelle verfügt.
6. Sobald eine Antwort auf das ARP-Paket empfangen wurde, kann der Router Pakete an den Ziel-Client senden.

Zugehörige Informationen

- [Produktsupport für Switches](#)
- [Unterstützung der LAN Switching-Technologie](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)