

權杖環交換概念

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[TrBRF和TrCRF](#)

[交換模式](#)

[透通橋接](#)

[來源路由交換](#)

[來源路由橋接和來源路由透明](#)

[交換器間連結](#)

[生成樹](#)

[VLAN Trunk通訊協定](#)

[VTP修剪](#)

[重複環協定](#)

[HSRP和權杖環VLAN](#)

[相關資訊](#)

簡介

若要開始瞭解權杖環交換的概念，您必須瞭解透通橋接、來源路由橋接和跨距樹狀目錄。Catalyst 3900和Catalyst 5000使用新的概念，如IEEE 802.5 annex K中所述。這些概念是權杖環VLAN的構建基塊。本檔案將說明不同的橋接概念及其運作方式：

- 交換器間連結(ISL)中繼
- 生成樹
- VLAN主幹協定(VTP)
- 重複環通訊協定(DRiP)

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

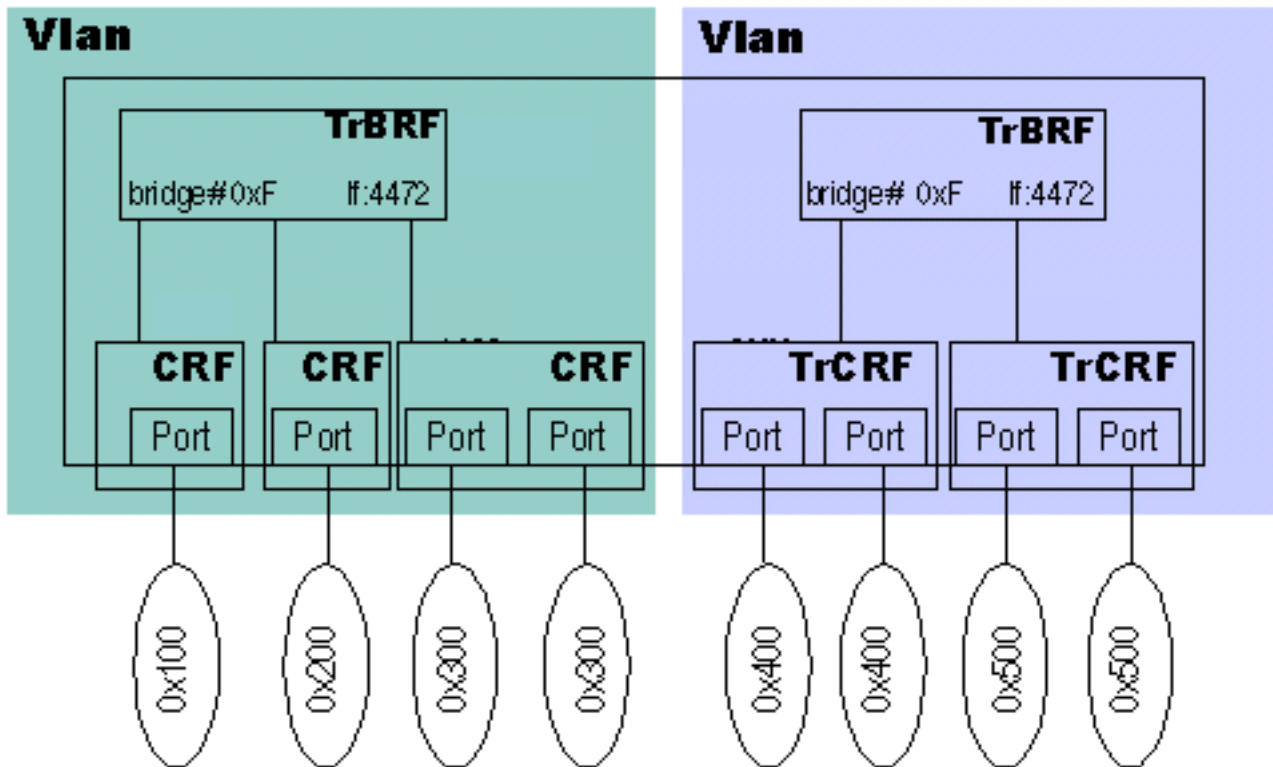
如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

TrBRF和TrCRF

權杖環橋接器中繼功能(TrBRF)和權杖環集中器中繼功能(TrCRF)是Catalyst 3900和Catalyst 5000功能架構的基石。TrBRF只是交換機的橋功能，而TrCRF是交換機的集中器功能。瞭解這兩層都發生橋接非常重要，因為令牌環中會討論三種不同型別的橋接。

交換器的TrBRF功能控制來源路由橋接流量的交換，例如來源路由橋接(SRB)和來源路由透明橋接(SRT)。TrCRF涵蓋源路由交換(SRS)和透明橋接(TB)的功能。例如，Catalyst 3900交換機可能只有一個TrBRF和一個TrCRF，並且交換機的所有埠都在同一個TrCRF中。這會導致交換機只能執行SRS和TB。如果您在同一父TrBRF下定義了十個不同的TrCRF，則來自連線到同一TrCRF的埠的流量將通過SRS或TB的TrCRF功能轉發。流向交換機中其他TrCRF的流量將使用交換機的TrBRF功能，可以是源路由橋接，也可以是源路由透明橋接。不同的交換機制將在本文檔稍後討論。

此圖將TrBRF和TrCRF與物理世界相關聯：



您可以看到每個TrCRF都連線到一個特定的環。TrCRF可以危害多個埠，這些埠會危害同一個環號。TrBRF將TrCRF連線在一起。

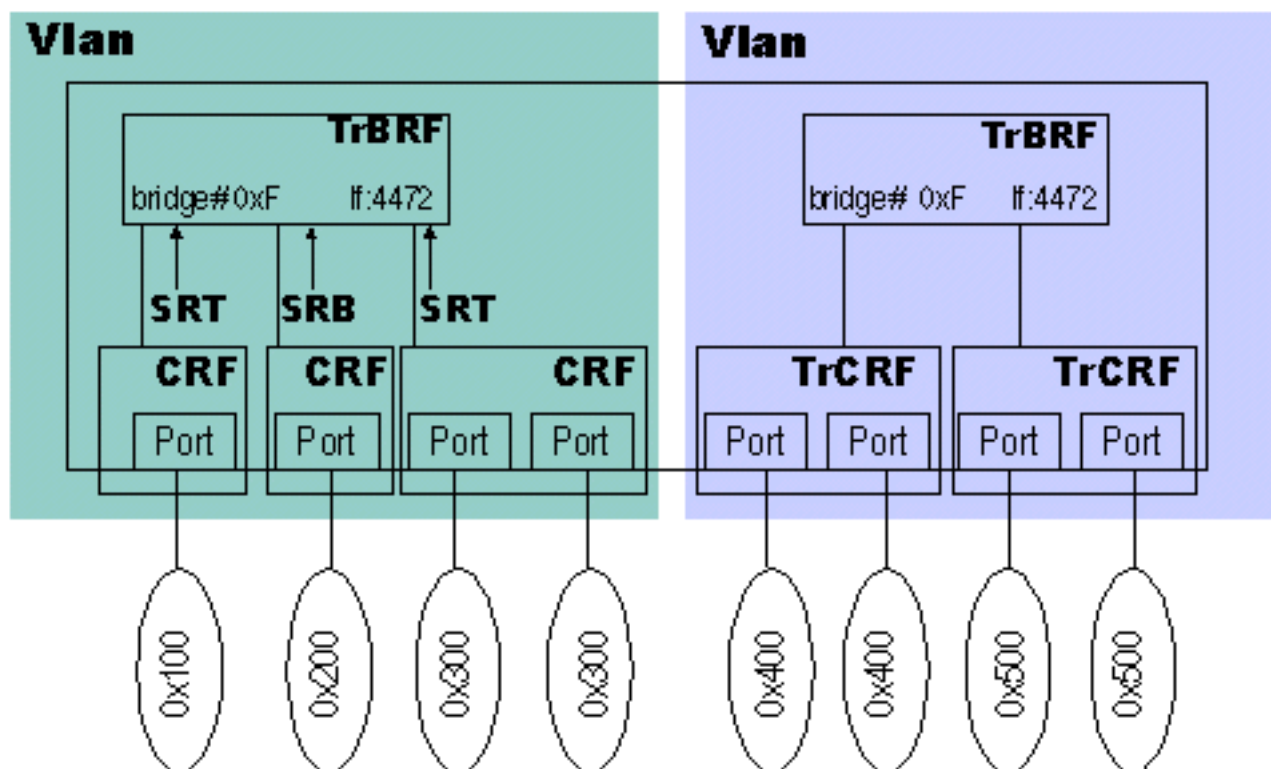
TrCRF和TrBRF本身是不同的VLAN。因此，在權杖環中，您可以在VLAN之間橋接。權杖環VLAN之間的橋接遵循兩個規則：

- 兩個TrBRF VLAN之間的橋接只能由外部裝置完成，例如路由器或路由交換模組(RSM)。
- TrCRF VLAN之間的橋接只能通過屬於同一父TrBRF VLAN子級的TrCRF VLAN來完成。

對於權杖環VLAN，這一點非常重要，因為它打破了乙太網路模式。總之，乙太網VLAN的外觀是一個TrBRF及其子級TrCRF的總和。由於您可以在權杖環中的某些VLAN之間橋接，因此您必須瞭解此橋接的發生方式。

注意：為了便於理解與乙太網VLAN相關的權杖環VLAN，請記住，TrCRF和TrBRF的組合本身就構成了VLAN。

在此圖中，您可以看到TrCRF決定了TrCRF和TrBRF之間的橋接模式。



各個TrCRF已配置它們將對TrBRF執行何種型別的橋接。這一點非常重要，因為您可以有TrCRF VLAN，它們將執行到其他TrCRF的源路由橋接，但不會執行非源路由。在上圖中，一個TrCRF配置為SRB模式，兩個配置為SRT模式。這表示SRB流量可以在所有三個TrCRF之間流動，但SRT只能在兩個處於SRT模式的路由器之間流動。這允許您精細設定流量在TrCRF之間的流向。如果在TrBRF設定了橋接模式，則會影響該VLAN的所有TrCRF子級。

交換模式

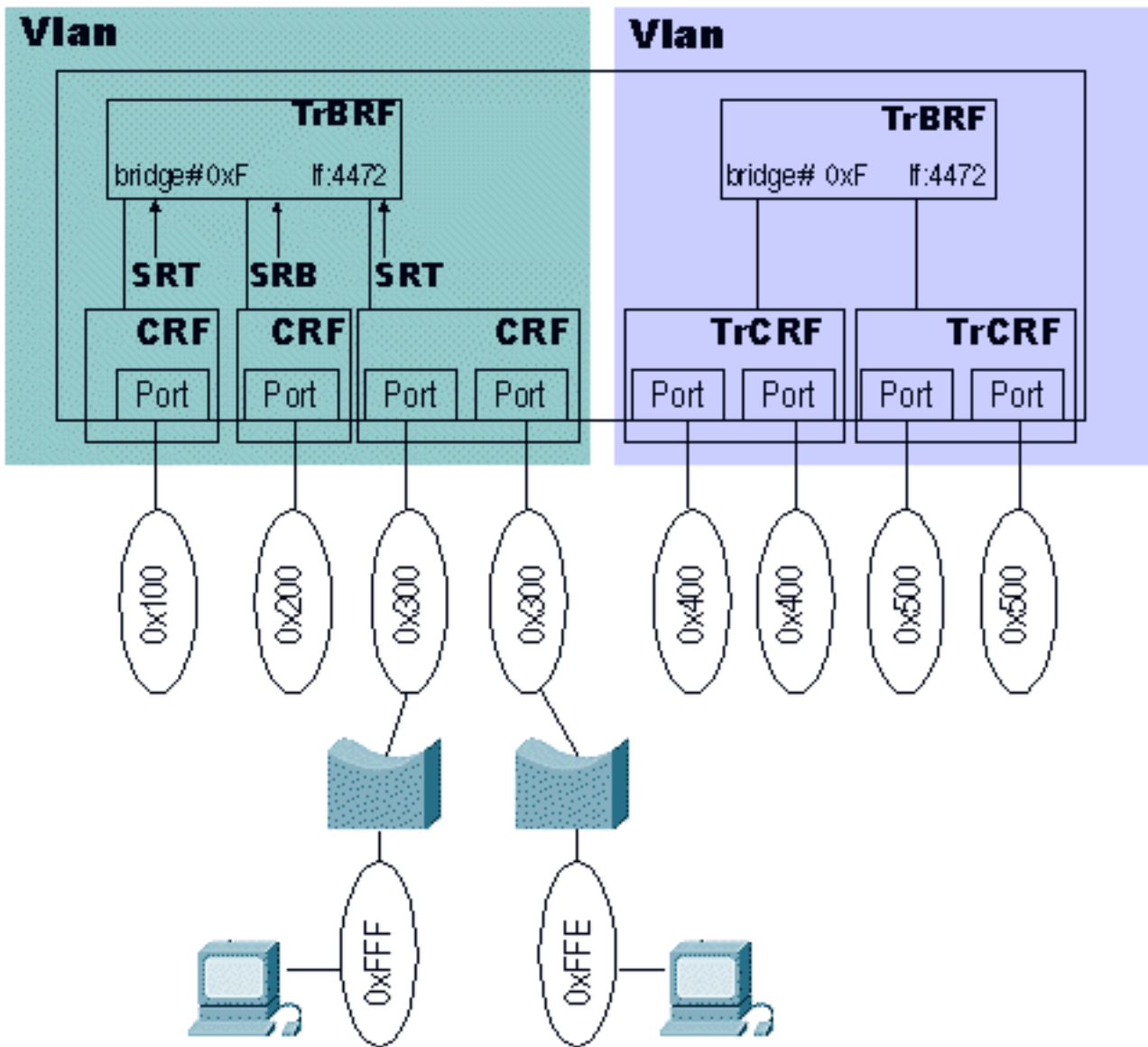
Catalyst 3900開箱即配置了一個TrBRF和一個TrCRF。所有埠都分配到預設的TrCRF VLAN 1003。這同樣適用於Catalyst 5000權杖環刀鋒。這一點很重要，因為它使???盒具有某些「即插即用???功能。這些交換機可開箱即用，根據源路由交換和透明橋接進行轉發。接下來的部分將詳細介紹這些技術。

透明橋接

透明橋接是所有交換機制中最基本的，它基於網路中幀的目標MAC(DMAC)地址。這是乙太網路的轉送機制。交換器每次收到訊框時，都會將訊框的來源MAC(SMAC)位址記錄為屬於該連線埠的位址，且之後會將目的地為該MAC的流量轉送到該連線埠。在學習過程中，如果交換機不知道MAC地址，則會將該資料包泛洪到處於轉發狀態的所有埠。

來源路由交換

當只有一個分配給埠的TrCRF並且交換機接收包含路由資訊欄位(RIF)的資料包時，需要使用源路由交換轉發機制。由於交換機不會修改幀的RIF (因為它不會將其傳遞給TrBRF)，因此網路必須能夠在不修改的情況下使用RIF做出轉發決策。請考慮顯示SRS的網路圖表：



從環0xFFF到環0xFFE的流量需要通過交換機。此流量將是源路由橋接流量。這是這兩個客戶端之間的通訊啟動順序：

1. 一個站將探查器封包傳送到它所在的環。假設環0xFFF上的客戶端傳送資料包；它看起來像這樣（十六進位制）：

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

注意：該資料包資訊僅顯示DMAC、SMAC和RIF資訊。

2. 一旦資料包到達源路由網橋並將幀轉發到線路，資料包將如下所示：

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

C670是路由控制欄位，FFF1 3000是環0xFFF、網橋0x1、環0x300。

3. 現在，封包抵達交換器。由於交換機看到資料包來自遠處的環路，因此它會獲取路由描述符。在這種情況下，交換機現在知道通過網橋0x1的環0xFFF位於埠3上。
4. 由於資料包是explorer資料包，因此交換機將幀轉發到同一TrCRF下的所有埠。如果瀏覽器需要訪問不同TrCRF中的埠，它將將該幀傳送到TrBRF，後者將執行其網橋功能。如果同一個TrCRF中有埠，它將轉發出站幀而無需修改。
5. 0xFFE環中的工作站應獲取瀏覽器並響應。假設客戶端使用定向幀做出響應。此定向幀如下所示：

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

08E0是路由控制欄位，FFF1 3001 FFE0環0xFFF、網橋0x1、環0x300、網橋0x1、環0xFFE。

6. 最後，交換機獲知環0xFFE位於埠4上，並保留路由描述符。

從今以後，交換機就知道這些環了。如果您檢視這些表，您應該會看到交換機已經獲知網橋號和振鈴號。在環0xFFF和環0xFFE之後不需要任何其它環，因為它們必須通過環0xFFF或環0xFFE才能到達交換機。

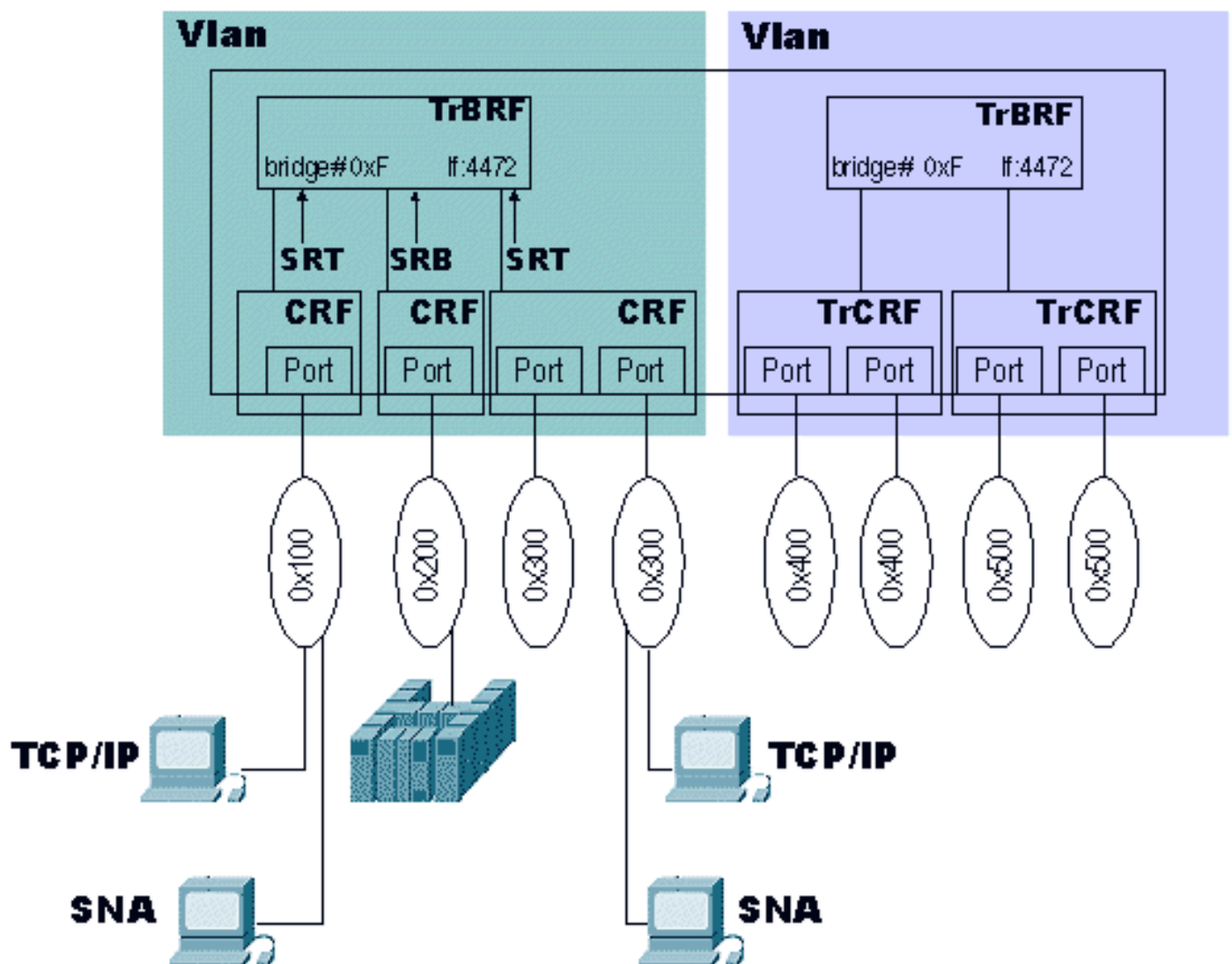
SRS是沒有SRB功能的基於RIF的資料包的基本轉發，TrCRF就是這種情況。

注意：要在Catalyst 5000中檢視路由資訊表，請發出show rif命令。

來源路由橋接和來源路由透明

所有源路由橋接功能都位於TrBRF邏輯中。TrCRF是命令橋接模式到TrBRF的路由器。因此，如果TrCRF配置為SRB模式到TrBRF，那麼，當TrCRF收到NSR（非源路由）幀時，交換機不會將其轉發到TrBRF邏輯。

如果您不希望特定型別的流量命中或離開特定環，則可使用此方法。此圖顯示範例：



如果TCP/IP客戶端無法使用RIF傳送資料包，交換機將不會將這些幀放入與大型機相同的環中(0x200)。但是，到主機SNA幀（通常具有RIF）將到達主機。這是一種非常簡單的在交換網路中過濾幀的方法。

交換器按照以下順序在TrBRF上轉送來源路由橋接訊框：

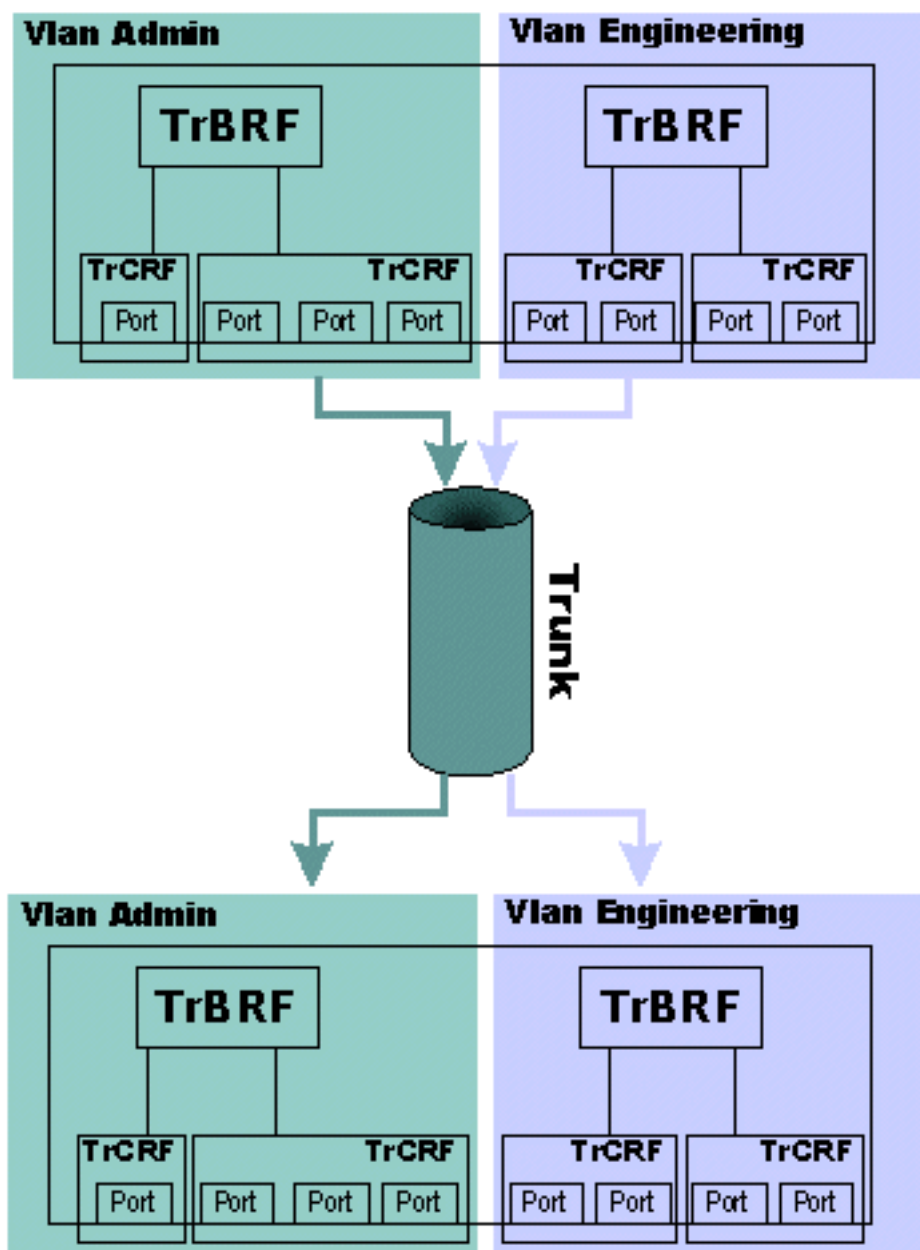
1. 環0x300（埠4）上的SNA工作站會傳送一個資源管理器來訪問大型機。

- 當Explorer資料包到達交換機時，在同一TrCRF中轉發瀏覽器，無需修改；然後向TrBRF傳送一個副本，以轉發到其他TrCRF。在這種情況下，由於封包有一個RIF，因此會通過SRB路徑。交換器也需要學習路由。
- 交換機將獲知幀的SMAC，因為資料包顯示為源自交換機所連線的本地環。這是因為在多埠TrCRF組合中，RIF顯示目標環，但交換機需要知道TrCRF中的哪個埠。因此，交換機獲知在TrCRF級別傳入的幀的SMAC。
- 資料包將傳給所有剩餘的TrCRF，並分別使用各自的網橋環號組合進行修改。
- 一旦主機使用SRB幀做出響應，交換機就會獲知主機的SMAC該TrCRF並將其傳送到出站埠。然後，流量會在兩者之間來回流動。

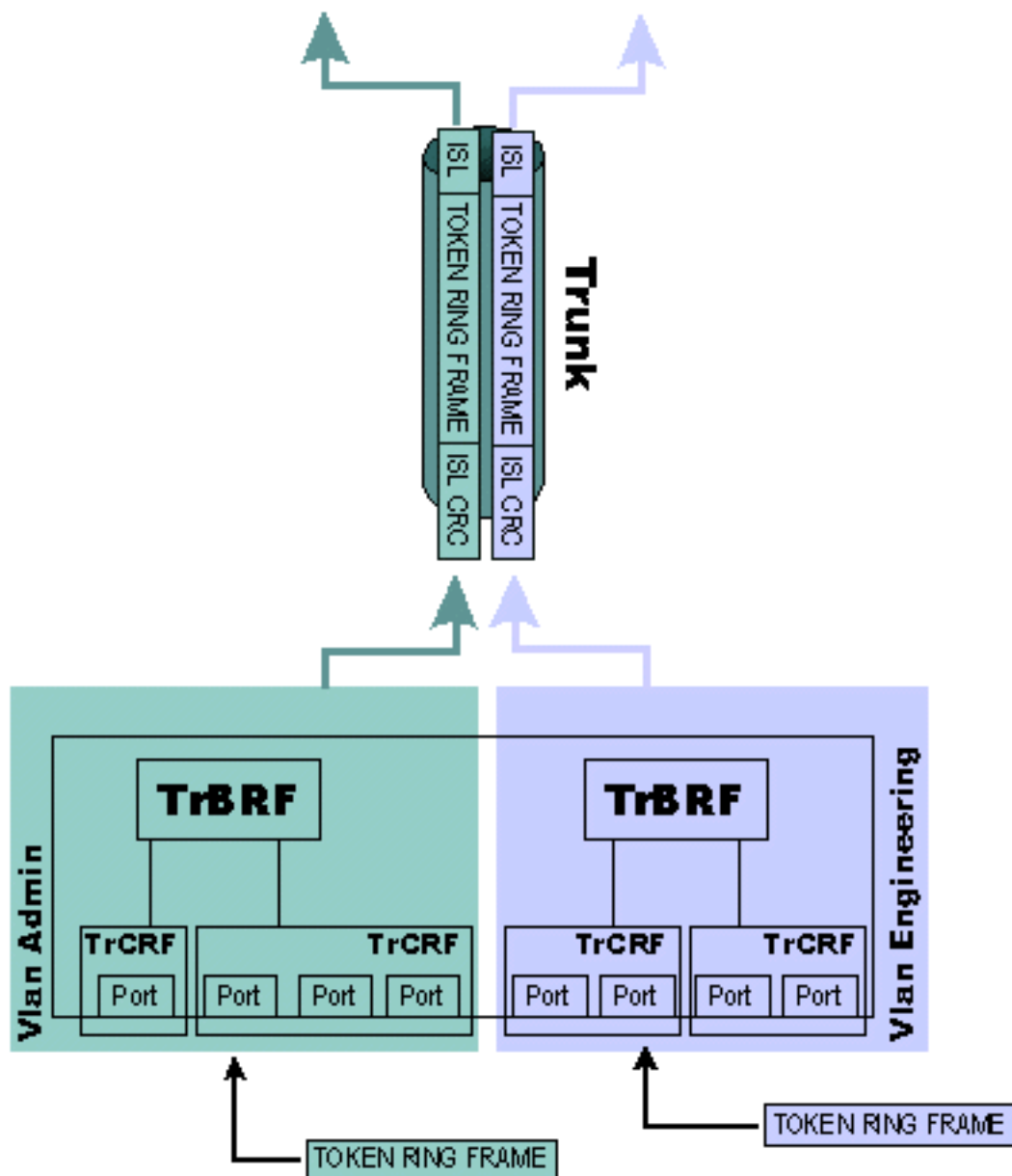
注意：要檢查Catalyst 5000上的MAC地址表，請發出show cam命令。

交換器間連結

交換機間鏈路是一種非常簡單的協定。基本上，通過ISL中繼的幀會封裝在ISL幀中，該幀告知另一端幀屬於哪個VLAN。因此，必須在交換機之間手動或自動共用VLAN資訊。稱為VLAN中繼線協定(VTP)的協定可以處理此任務。對於權杖環VLAN，您必須在網路中運行VTP V2。請考慮以下圖表：



在本例中，建立了一個ISL中繼來單獨承載工程VLAN和管理VLAN。當流量通過TRUNK後，兩個VLAN中的任何流量都不會混合。此圖顯示實現此分離的方式：



來自需要通過中繼的VLAN的每個幀都封裝在ISL幀中，其VLAN也包含在幀中。這樣，接收交換機就可以正確將幀路由到其特定VLAN。權杖環ISL(TRISL)框架比常規ISL框架有更多的欄位。此圖顯示TRISL框架的佈局：

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	Exi-te	
ENCAP FRAME (Continued)		8 to 196600 (1 to 24575 bytes) ENCAP FRAME		32	32
				Syn CRC	ISL CRC

註：即使TRISL在快速乙太網介面上運行，資料包在某種程度上也包含標準令牌環幀以及與該幀關聯的VLAN資訊。令牌環VLAN允許高達18k的幀大小，ISL也是如此。這不是通過分段幀實現的。整個幀將封裝在一段ISL幀中，並通過鏈路傳送。人們普遍錯誤地認為ISL是乙太網，其最大幀大小為1500位元組。

在Catalyst 5000上，4.x版提供了稱為動態中繼協定(DTP)的協定。DTP是動態ISL(DISL)的戰略性替代方案，因為它包含對802.1Q中繼協商的支援。DISL的???能是協商 (僅適用於ISL) 兩個裝置之間的鏈路是否應為中繼。DTP能夠協商ISL和IEEE 802.1Q VLAN中繼之間將使用的中繼封裝型別。這是一項有趣的功能，因為有些思科裝置僅支援ISL或802.1Q，而有些裝置則能夠同時運行這兩種功能。

以下是您可以為其配置DTP的五種不同狀態：

- 自動 — 在自動模式下，埠偵聽來自相鄰交換機的中繼協定(DTP)幀。如果相鄰交換機表示它想成為中繼或中繼，則自動模式會與相鄰交換機建立中繼。當相鄰埠設定為On或Desirable模式時，會發生這種情況。
- Desirable - Desirable模式向相鄰交換機指示它可以是ISL中繼，並希望相鄰交換機也可以是ISL中繼。如果相鄰埠設定為On、Desirable或Auto模式，則該埠會成為中繼埠。
- 開 — 開啟模式自動在其埠上啟用ISL中繼，而不管其相鄰交換機的狀態如何。除非它收到明確禁用ISL中繼的ISL資料包，否則它仍然是ISL中繼。
- 非協商 — 非協商模式自動在其埠上啟用ISL中繼 (無論其相鄰交換機的狀態如何)，但不允許埠生成DTP幀。
- 關閉 — 在關閉模式下，無論在另一個交換機上配置了DTP模式，都不允許在此埠上使用ISL。

Catalyst 5000系列交換機通常用於提供ISL主幹。然後，Catalyst 3900交換器可以通過雙100 Mbps ISL擴充模組連線到此主幹。Catalyst 3900權杖環交換器不支援除ISL以外的任何其他模式，因此一律使用中繼。此外，Catalyst 3900 ISL模組僅支援100 Mbps連線，且預設為全雙工。

透過ISL連結連線Catalyst 3900和Catalyst 5000交換器時，請務必小心。主要問題是Catalyst 3900不支援快速乙太網路媒體交涉。因此，如果Catalyst 5000設定為自動模式，則預設為100 Mbps半雙工。這會導致連線埠從主幹進入非主幹和封包遺失等問題。

如果要將Catalyst 3900 ISL埠連線到Catalyst 5000的ISL埠，則必須手動配置Catalyst 5000上的ISL埠：

1. 發出set port speed命令以設定為100 Mbps:


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

2. 發出set port duplex命令以設定為全雙工：

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

如果要將交換器的連線埠強制進入主幹模式，請發出set trunk指令（在一行上）：

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

在上面的命令中，vlan是1到1005之間的值(例如2-10或1005),trunk_type設定為isl、dot1q、dot10、lane或negotiate。

一旦交換機上的中繼埠處於活動狀態，您就可以發出show trunk命令來檢視這些中繼埠是否處於活動狀態。

```
Pteradactyl-Sup> (enable) show trunk
```

Port	Mode	Encapsulation	Status	Native vlan
5/1	on	isl	trunking	1
10/1	on	isl	trunking	1

```
Port Vlan allowed on trunk
```

5/1	1-1005
10/1	1-1005

```
Port Vlan allowed and active in management domain
```

5/1	
10/1	1

```
Port Vlan in spanning tree forwarding state and not pruned
```

5/1	
10/1	1

用於觀察ISL中繼的一個重要命令是show cdp neighbors detail命令。此命令還有助於您瞭解網路拓撲。

```
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

從該輸出中，您可以清楚地看到Catalyst 3900已連線到連線埠10/1。當在上一個show trunk命令的輸出中檢查連線埠10/1時，可以得知該連線埠為主干連線埠。

生成樹

權杖環環境中的跨距樹狀目錄可能會變得非常複雜，因為一個人可以同時執行全部三個不同的跨距樹狀目錄通訊協定。例如，典型環境在TrBRF級別運行IBM生成樹並在TrCRF級別運行IEEE(802.1d)或Cisco。因此，對生成樹進行故障排除會稍微複雜一些。

下表說明根據不同型別的可能配置會發生的情況：

TrCRF 橋接模式	TrCRF	TrBRF
SRB	運行IEEE生成樹。	作為源路由網橋執行。
	處理來自外部網橋的IBM生成樹協定網橋協定資料單元(BPDU)。	對外部網橋運行IBM生成樹協定。 丟棄TrCRF的透明IEEE生成樹協定BPDU。
SRT	運行思科生成樹協定。	作為源路由透明網橋執行。
	將目標地址欄位的網橋組地址替換為思科特定的組地址，這樣外部網橋就不會分析TrCRF BPDU。	轉發透明流量和源路由流量。
	生成BPDU，在出站幀的源地址欄位中設定RIF位，並新增2位元組RIF。此幀格式可確保TrCRF在邏輯環上保持本地狀態，並且不會透明橋接或源路由到其他LAN。只有通過物理環路連線的TrCRF才能接收BPDU。 處理來自外部網橋的IEEE生成樹BPDU。	將源路由流量轉發到TrBRF中的所有其他TrCRF，無論它們是SRT還是SRB模式。

VLAN Trunk通訊協定

因為使用ISL時，VLAN會決定封包應前往何處，所以每台交換器都必須瞭解網路中的VLAN，這一

點非常重要。VTP生??的目的是在交換機之間傳播VLAN資訊。VTP不會在路由器上運行，因為它們應該終止VLAN網路。網路中的每台交換機都應該運行VTP。如果沒有，則交換器通常只執行一個VLAN（通常是VLAN 1），且不會在該連結上運行ISL，因為不需要這樣做。VTP使建立VLAN的工作變得容易得多，因為您可以在一台交換機中配置VLAN，並且它們將在網路中傳播。當然，這會帶來問題。

VTP不是像增強型內部網關路由協定(EIGRP)或開放最短路徑優先(OSPF)路由協定那樣強大的系統。它要簡單得多，而且基於一個非常重要的概念：修訂版。VTP中有三種型別的VTP裝置：客戶端、伺服器和透明裝置。客戶端VTP裝置基本上只接受來自伺服器裝置的VLAN資訊，無法修改此資訊。但是，伺服器可以在任何VTP伺服器上修改VTP資訊。因此，VTP具有修訂系統。任何修改或更新VLAN資料庫的VTP伺服器都聲稱這是最新版本。因此，必須特別小心，因為具有最高修訂版本的交換機將??win??其VLAN資訊為有效資訊。例如，如果修改一台VTP伺服器，使其表示TrBRF VLAN 100將執行IEEE生成樹，這將在所有交換機之間造成嚴重破壞，因為它可能導致交換機（如Catalyst 3900）將埠置於阻塞模式，以保護自身免受環路的影響。此外，將新交換機引入網路時要小心，因為它們可能具有更高的VTP修訂版。在透明模式下，一個中繼上接收到的VTP資料包會自動傳播到裝置上的所有其它中繼上，而不會發生任何更改；但是，裝置本身卻忽略了它們。

使用權杖環交換器設定VTP時，必須執行VTP V2。如果希望交換器同時執行乙太網路和權杖環VLAN，則必須升級VTP，即使對於乙太網路VLAN也是如此。不能有兩個不同的VTP網域（例如，不能有一個用於乙太網路，另一個用於權杖環）。

VTP修剪

VLAN中繼的一個問題是，來自一個VLAN的廣播資訊會在所有中繼上傳播，因為交換機不知道遠端交換機中存在哪些VLAN。VTP修剪是為此而建立的。它允許交換機協商將哪些VLAN分配給主幹另一端的埠，從而修整未遠端分配的VLAN。Catalyst 3900和Catalyst 5000交換器預設停用修剪。

注意：版本4.1(1)中的Catalyst 3900交換機支援VTP修剪。

每個VTP修剪消息都包含有關所討論VLAN的資訊，並包含一個位，指示是否應為此中繼修剪此VLAN(1指示不應修剪)。啟用修剪後，除非中繼鏈路收到相應的加入消息，並且相應的VLAN位已啟用，否則通常不會通過TRUNK鏈??傳送VLAN流量。這一點非常重要，因為它會告訴您在使用VTP修剪時，必須確儲存在正確的資訊和配置，並且所有交換機都在運行修剪；如果交換器沒有透過主幹將加入訊息傳送至另一台交換器，它可能會針對特定VLAN或VLAN關閉。修剪協商完成後，VLAN將以修剪或加入狀態完成該中繼。

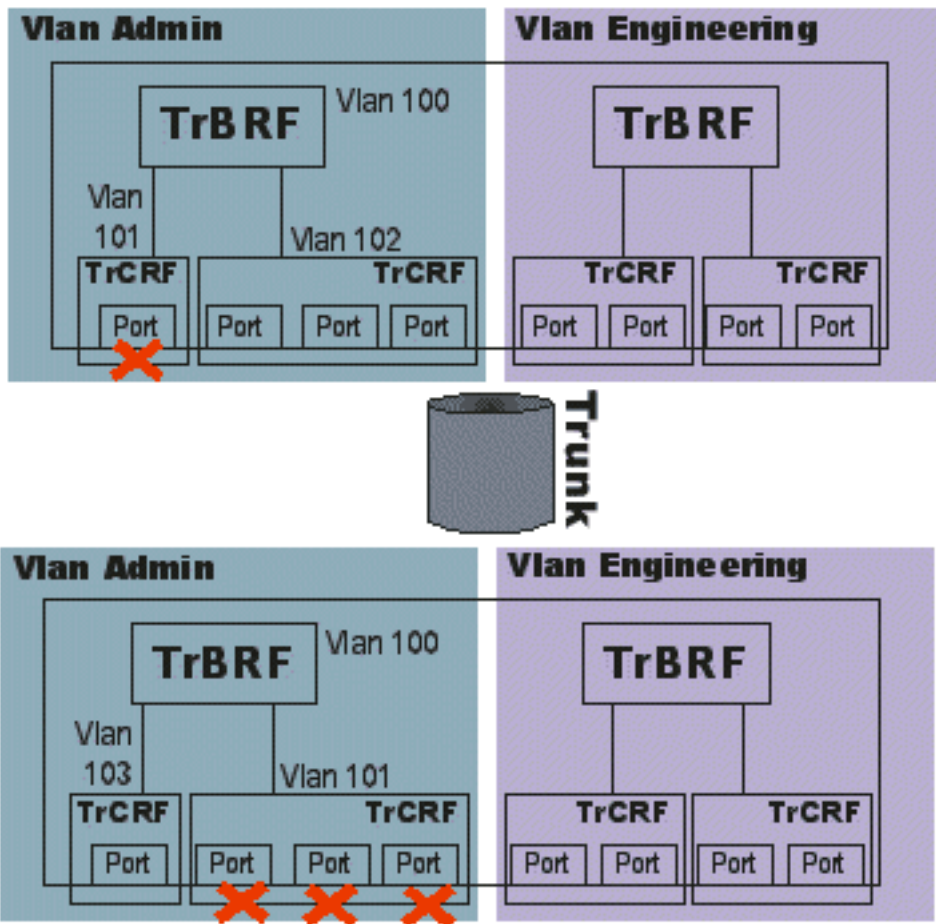
VTP修剪的一個重要功能是配置VLAN是否適合修剪。此功能告知執行VTP修剪的交換機不要修剪此VLAN。啟用VTP修剪時，VLAN 2到1000預設情況下修剪符合條件的VLAN。因此，開啟修剪時，預設情況下會影響所有VLAN。VLAN 1、預設TrCRF(1003)、預設TrBRF(1005)和TrCRF總是剪枝不合格；因此，來自這些VLAN的流量無法修剪。

重複環協定

重複環協定設計為運行權杖環VLAN的交換器上執行。其任務是確保正確配置令牌環VLAN並建立瀏覽器縮減。DRiP使用VTP來同步其VLAN資料庫資訊，但DRiP工作並不需要它（VLAN資料庫可以手動建立）。一個誤解是DRiP理解環號；這不是真的。DRiP取決於網路中配置的VLAN的唯一性和該VLAN資料庫配置。

DRiP的一個重要功能是實施TrCRF分佈。在權杖環中，由於跨距問題，分發除1003以外的任何VLAN都非常危險。因此，如果分發除VLAN 1003之外的TrCRF，則該VLAN關聯的所有埠都會被DRiP禁用。

此範例說明此概念：

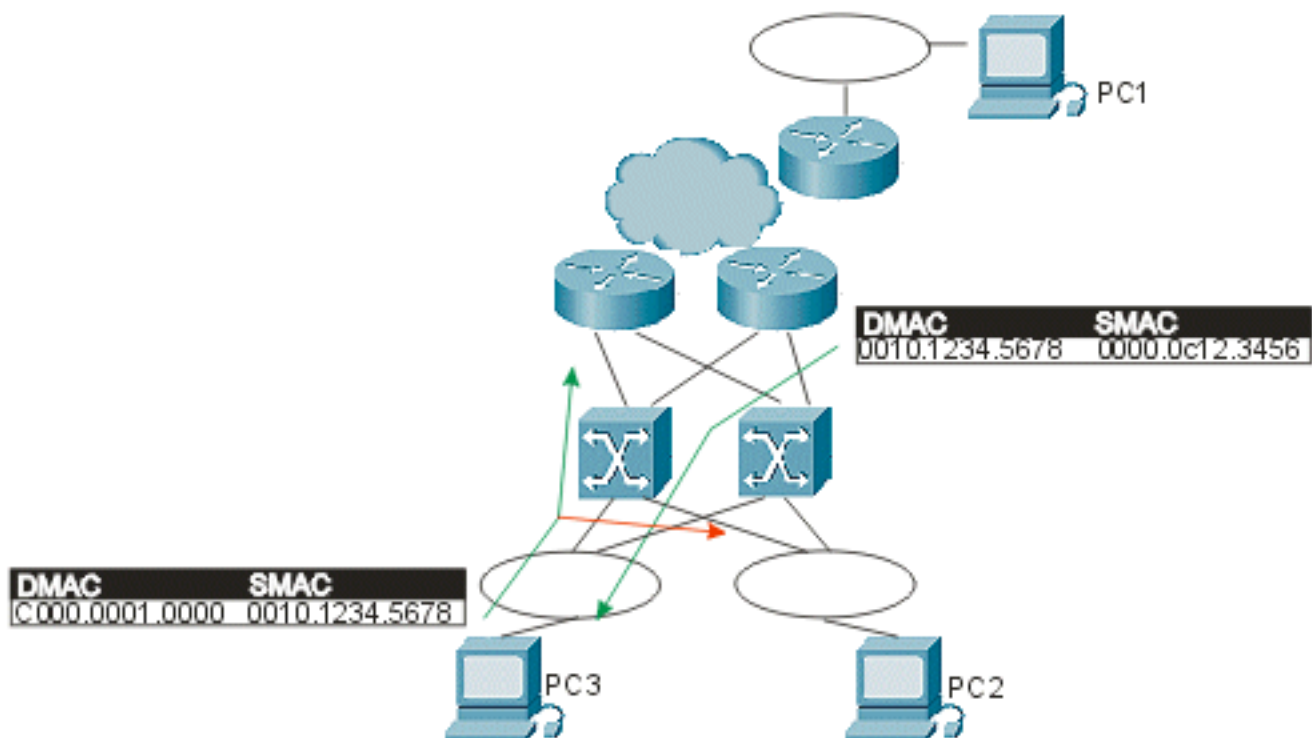


在該示例中，兩台不同的交換機有一個分配給VLAN 101的埠。該交換機通過DRiP將埠生成樹設定為禁用並停止轉發流量。這樣可保護交換器免受可能的回圈情況的影響。

如果沒有變化，DRiP每30秒將向其所有中繼埠通告TrCRF狀態。任何通過CLI（命令列介面）或SNMP進行的更改都會立即向所有埠傳送更新。這些通告是第0類ISL幀，在預設VLAN 1上流動。由於DRiP僅通告其對VLAN的影響，因此通過ISL連線的交換機中存在正確的VLAN資訊非常重要。這是通過VTP完成的。如果禁用VTP，則必須在共用相同VLAN的所有交換機上手動維護此功能。DRiP通告僅存在於ISL鏈路上。ATM、權杖環、乙太網路或FDDI上不存在這些裝置。DRiP中沒有保留任何拓撲樹。

HSRP和權杖環VLAN

HSRP的最大問題之一是在網路中使用組播地址。由於網路中實際上沒有人會使用此虛擬MAC地址來獲取資料包，因此交換機永遠不會獲知這些MAC地址。因此，它們會在整個網路中泛洪幀。因此，需要使用HSRP的standby use-bia功能來傳送使用活動HSRP路由器介面的內嵌MAC地址的資料包。此方案的主要問題是，當HSRP路由器交換時，它們必須傳送廣播地址解析協定(ARP;免費的ARP)，讓線路上的所有站獲知網關的新MAC地址。儘管此過程應基於IP規範運行，但其中存在一些已知問題。由於來自該欄位的持續請求，HSRP已更改，因此您可以擁有組播地址，並且還可以使用HSRP而不使用備用bia。此更改發佈在Cisco IOS軟體版本11.3(7)和12.0(3)及更高版本中。



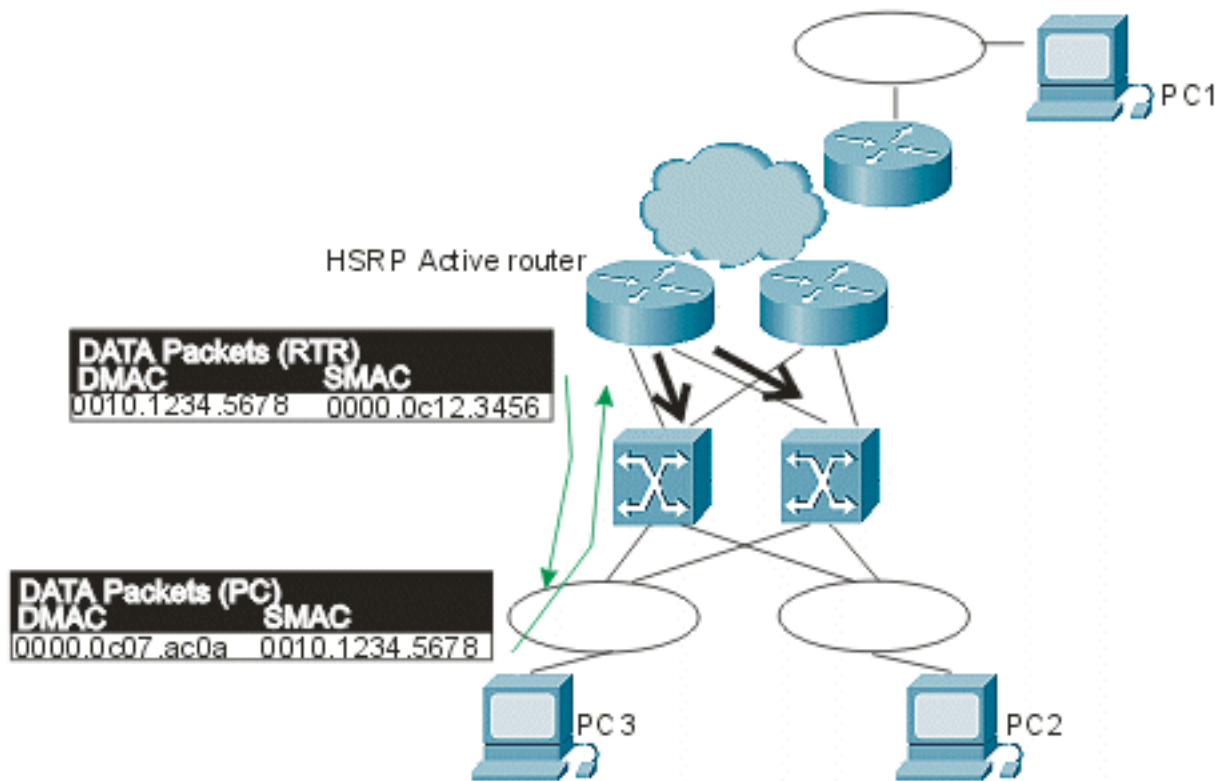
在上圖中，PC1和PC3之間正在進行通訊。問題是此圖中的從客戶端到預設路由器的IP流量使用組播目的地址。由於任何人都不能從該地址獲取此資料包，因此交換機永遠不會獲知此地址，並總是泛洪資料包。依賴組的傳統DMAC是C000.000X.0000，它絕不能是令牌環中的SMAC。因此，所有通過預設網關從PC3發往PC1的資料包現在都被PC2看到。在網橋眾多的網路中，這會非常迅速地激增，造成看似廣播風暴但實際上是大量組播流量的情況。

要解決此問題，您必須使用HSRP hello中的路由器實際可用作SMAC的MAC地址。這樣交換器便可知此位址，因此，會適當地交換封包。為此，請在路由器中配置新的虛擬MAC地址。客戶端需要將資料包傳送到此新虛擬地址的DMAC。以下是show standby命令的輸出示例：

```
vdt1-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
```

在輸出中，已經建立了一個備用組10 (備用IP 1.1.1.100)。MAC地址(000.0c07.ac0a)是新的虛擬MAC地址，最後一個位元組是組(0xA = 10)。一旦您擁有此新配置，您現在就會擁有此流量模式，從而避免流量泛洪：



現在，由於路由器使用HSRP虛擬MAC的DMAC來獲取資料包，因此交換機將獲知此MAC地址，並僅將資料包轉發到活動HSRP路由器。如果主用HSRP路由器發生故障且備用路由器變為主用，則新的主用路由器將開始傳送具有相同SMAC的HSRP hello，這會導致交換機MAC地址表將其獲知的條目切換到新的交換機埠和中繼上。

由於存在多環的情況，需要執行其他操作來確保RIF在轉換期間實際發生更改（即使它是相同的MAC地址）。多環是路由器將RIF與MAC地址關聯的功能，就像終端站一樣。在存在SRB網橋的環境中，路由器需要多環路，以便資料包可以經過這些網橋到達終端站。

在與以前的相同示例中，您可以看到客戶端連線到新的活動HSRP路由器所需的附加步驟：

1. 活動路由器停止工作。
2. 一旦備用路由器檢測到HSRP hello丟失，它將啟動成為活動HSRP路由器的過程。
3. 路由器在MAC層和ARP層都從以前相同的SMAC傳送免費ARP。
4. PC現在將幀傳送到同一個MAC地址，但使用新的RIF。
5. 路由器收到此幀（目的地為HSRP MAC）後，會將ARP請求直接傳送給客戶端，因為它的ARP表中沒有該客戶端的MAC地址。
6. 收到對ARP資料包的響應後，路由器可以將資料包傳送到目的客戶端。

相關資訊

- [交換器產品支援](#)
- [LAN 交換技術支援](#)
- [技術支援與文件 - Cisco Systems](#)