令牌环交换概念

目录

简介

要开始了解令牌环交换的概念，了解透明桥接、源路由桥接和生成树非常重要。Catalyst 3900和Catalyst 5000使用新概念，如IEEE 802.5 annex K中所述。这些概念是令牌环VLAN的构建块。本文档介绍不同的桥接概念及其工作原理：

- 交换机间链路(ISL)中继
- 生成树
- VLAN 中继 协议 (VTP)
- 重复环协议(DRiP)

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

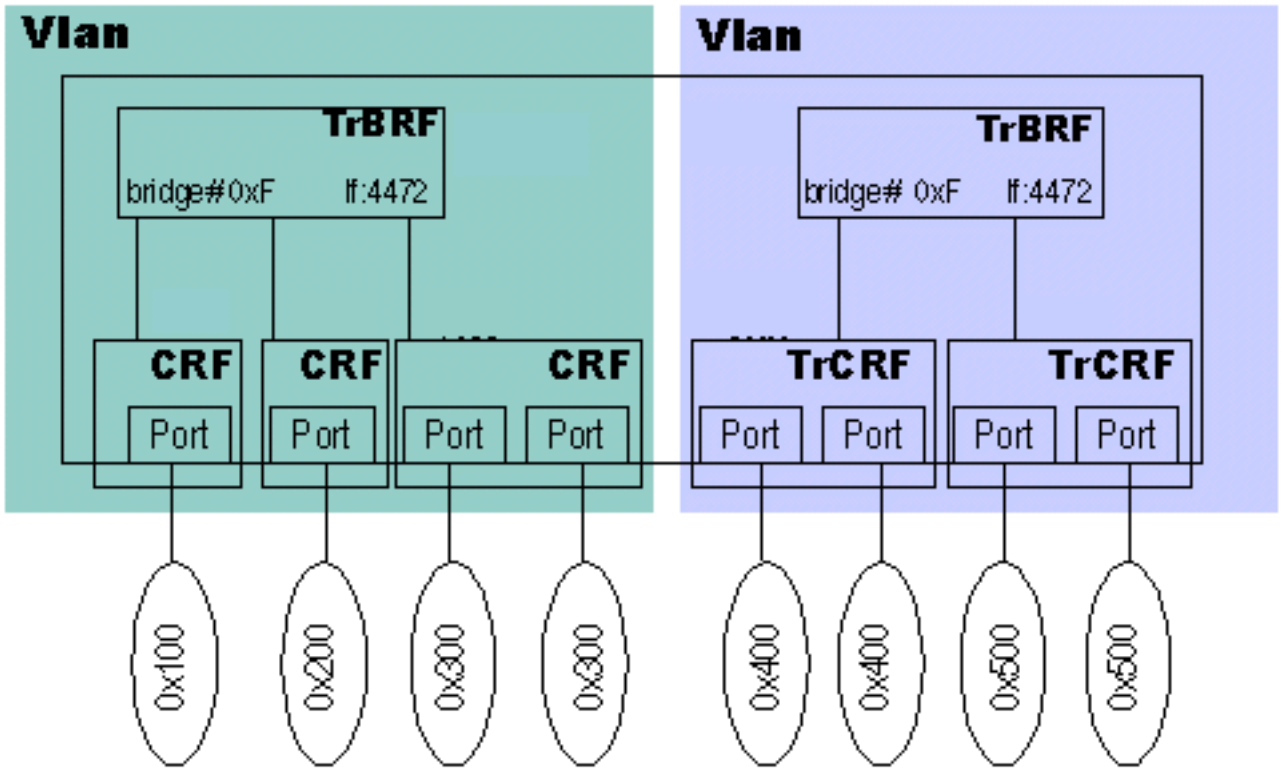
有关文件规则的更多信息请参见“ Cisco技术提示规则”。

TrBRF和TrCRF

令牌环网桥中继功能(TrBRF)和令牌环集中器中继功能(TrCRF)是Catalyst 3900和Catalyst 5000功能架构的构建块。TrBRF是交换机的桥接功能，TrCRF是交换机的集中器功能。了解这两层都发生桥接非常重要，因为在令牌环中，将讨论三种不同类型的桥接。

交换机的TrBRF功能控制源路由桥接流量的交换，例如源路由桥接(SRB)和源路由透明桥接(SRT)。TrCRF涵盖源路由交换(SRS)和透明桥接(TB)的功能。 例如，Catalyst 3900交换机可能只有一个TrBRF和一个TrCRF，并且交换机的所有端口都位于同一TrCRF中。这导致交换机只能执行SRS和TB。如果在同一父TrBRF下定义了十个不同的TrCRF，则来自连接到同一TrCRF的端口的流量将通过SRS或TB的TrCRF功能转发。流向交换机中其他TrCRF的流量将使用交换机的TrBRF功能，并且源路由桥接或源路由透明桥接。本文档稍后将讨论不同的交换机制。

此图将TrBRF和TrCRF与物理世界关联：



您可以看到每个TrCRF都连接到一个特定环。TrCRF可以危害多个端口，并且这些端口会危害相同的环号。TrBRF将TrCRF连接在一起。

TrCRF和TrBRF本身是不同的VLAN。因此，在令牌环中，您可以在VLAN之间桥接。令牌环VLAN之间的桥接遵循两条规则：

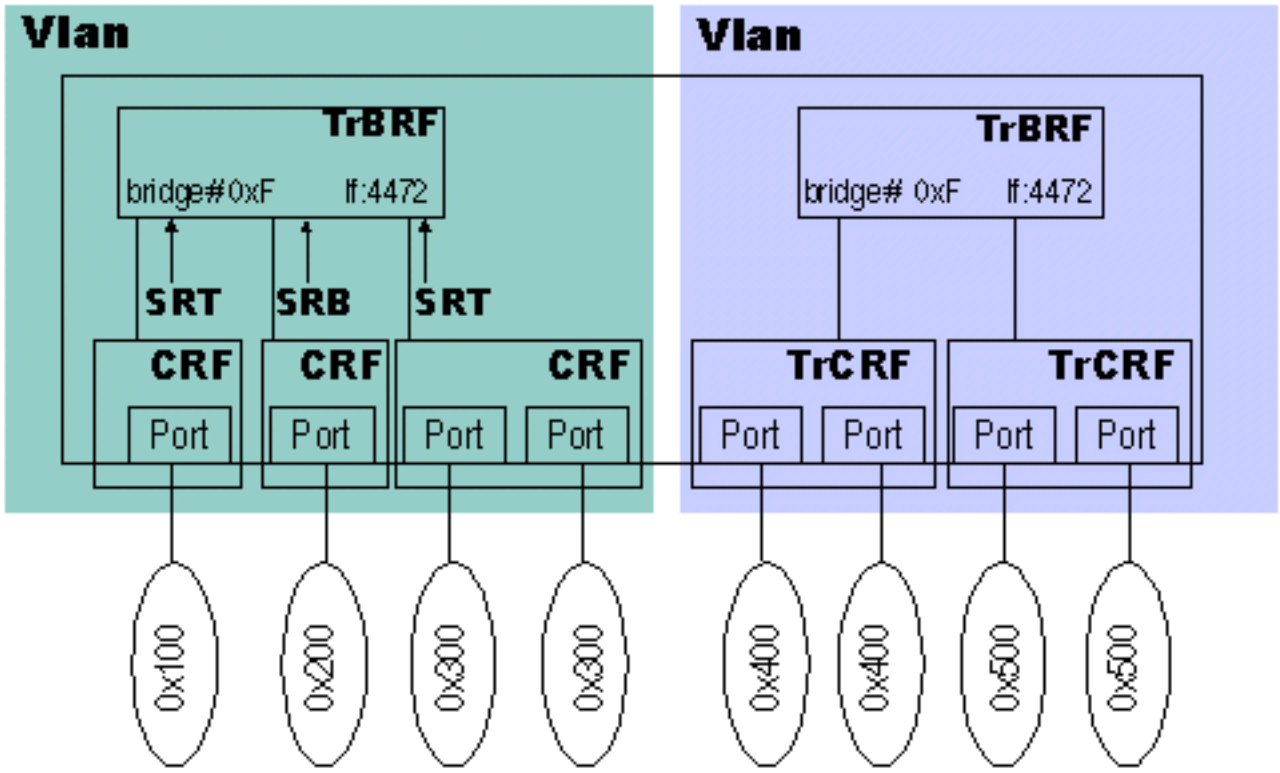
- 两个TrBRF VLAN之间的桥接只能通过外部设备(如路由器或路由交换模块(RSM))完成。
- TrCRF VLAN之间的桥接只能通过TrCRF VLAN完成，这些VLAN是同一父TrBRF VLAN的子VLAN。

对于令牌环VLAN，记住这一点非常重要，因为它打破了以太网模式。总之，以太网VLAN的外观是一个TrBRF及其子TrCRF的总和。由于您可以在令牌环中的某些VLAN之间进行桥接，因此您必须了

解此桥接是如何发生的。

注意：为了更容易理解令牌环VLAN与以太网VLAN的关系，请记住，TrCRF和TrBRF的组合使VLAN本身成为VLAN。

在此图中，您可以看到TrCRF决定TrCRF和TrBRF之间的桥接模式。



各个TrCRF已配置了它们将对TrBRF进行的桥接类型。这一点很重要，因为您可以有TrCRF VLAN，这些VLAN将执行到其他TrCRF的源路由桥接，但不会执行非源路由帧。在上图中，一个TrCRF配置为SRB模式，两个处于SRT模式。这意味着SRB流量可以在所有三个TrCRF之间流动，但SRT只能在处于SRT模式的两个之间流动。这允许您精细地设置流量在TrCRF之间的流动方式。如果在TrBRF上设置桥接模式，则会影响该VLAN的所有TrCRF子级。

交换模式

开箱即用，Catalyst 3900配置了一个TrBRF和一个TrCRF。所有端口都分配给默认TrCRF VLAN 1003。Catalyst 5000令牌环刀片也适用于此。这很重要，因为它为盒子提供特定的即插即用功能。功能。开箱即用后，这些交换机可以基于源路由交换和透明桥接执行转发。接下来的部分提供有关这些技术的详细信息。

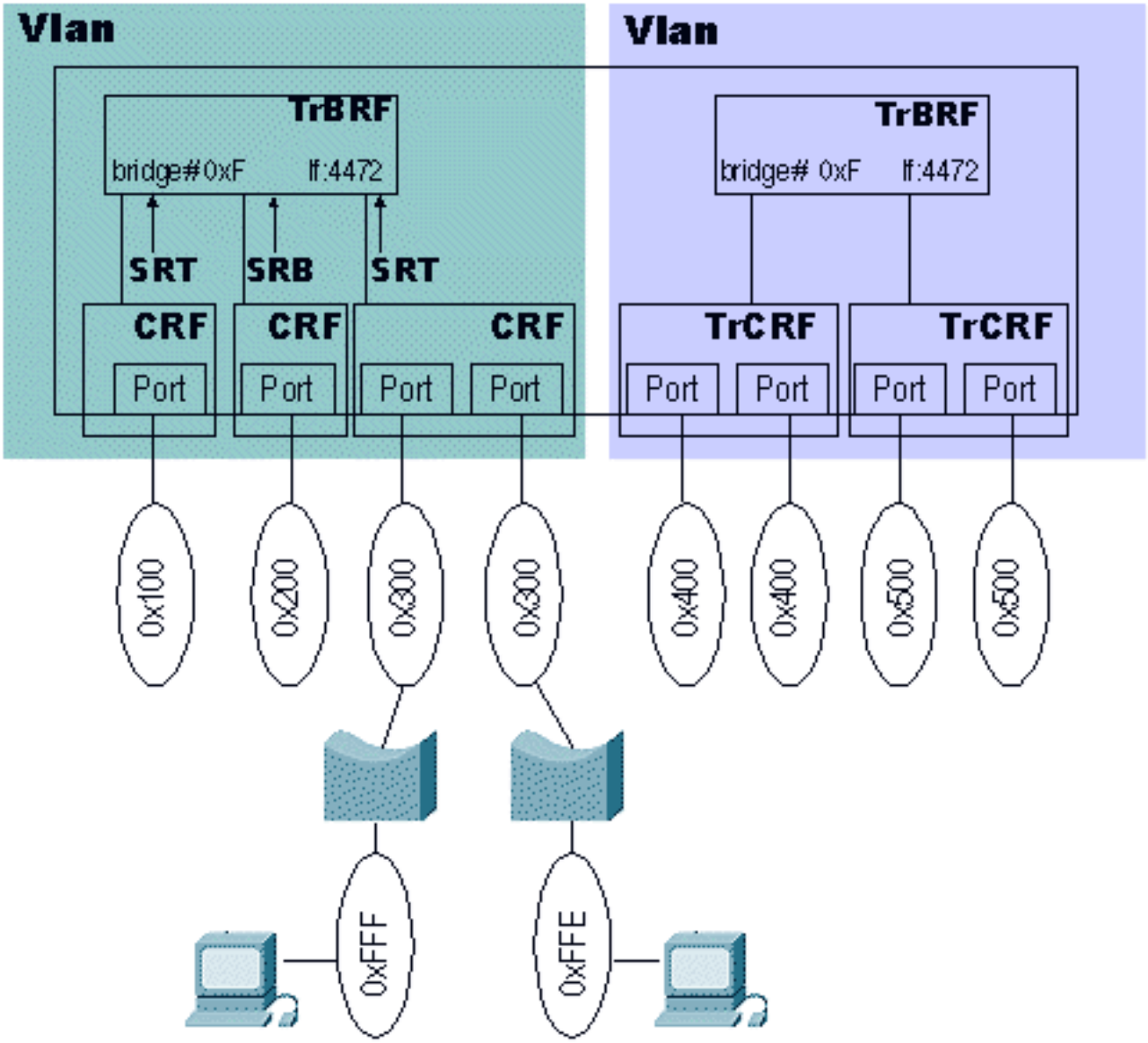
透明桥接

透明桥接是所有交换机制中最基本的，它基于网络中帧的目的MAC(DMAC)地址。这是以太网的转发机制。每当交换机收到帧时，都会将帧的源MAC(SMAC)地址记录为属于该端口的地址，从此将发往该MAC的流量转发到该端口。在学习过程中，如果交换机不知道MAC地址，它会将该数据包泛洪到处于转发状态的所有端口。

源路由交换

源路由交换是一种转发机制，当端口只分配了一个TrCRF，并且交换机接收包含路由信息字段

(RIF)的数据包时，就需要它。由于交换机不会修改帧的RIF（因为它不会将其传递给TrBRF），因此网络必须能够使用RIF做出转发决策，而无需修改。请考虑以下显示SRS的网络图：



从环0xFFF到环0xFFE的流量需要通过交换机。此流量将是源路由网桥流量。以下是这两个客户端之间的通信启动顺序：

1. 一个站点向其所在的环发送探测器数据包。假设环0xFFF上的客户端发送数据包；它看起来类似以下（十六进制）：
   ```
   0000 00c1 2345 8000 0c11 1111 C270
   ```
   注意：该数据包信息仅显示DMAC、SMAC和RIF信息。
2. 一旦数据包到达源路由网桥并将帧转发到线路，数据包将如下所示：
   ```
   0000 00C1 2345 8000 0c11 1111 C670 FFF1 3000
   ```
   C670是路由控制字段,FFF1 3000是环0xFFF、网桥0x1、环0x300。
3. 现在，数据包会到达交换机。由于交换机看到来自远距离环的数据包，因此它会获知路由描述符。在这种情况下，交换机现在知道通过网桥0x1的环0xFFF位于端口3上。
4. 由于数据包是Explorer数据包，交换机将帧转发到同一TrCRF下的所有端口。如果浏览器需要转到不同TrCRF中的端口，它会将帧传送到TrBRF，TrBRF将执行其网桥功能。如果同一TrCRF中有端口，它会将帧转发到出站方向，而不进行修改。
5. 环0xFFE中的站点应该获取浏览器并响应它。假设客户端以定向帧做出响应。此定向帧如下所示：
   ```
   0000 0C11 1111 8000 00C1 2345 08E0 FFF1 3001 FFE0
   ```

08E0是路由控制字FFF1 3001 FFE0是环0xFFF、网桥0x1、环0x300、网桥0x1、环0xFFE。

6. 最后，交换机获知环0xFFE位于端口4上，并保留路由描述符。

从今以后，开关就知道那些戒指了。如果查看表，您应该看到交换机已获知网桥号和环号。在环0xFFF和环0xFFE之后，不需要任何其它环，因为它们必须通过环0xFFF或环0xFFE才能到达交换机。

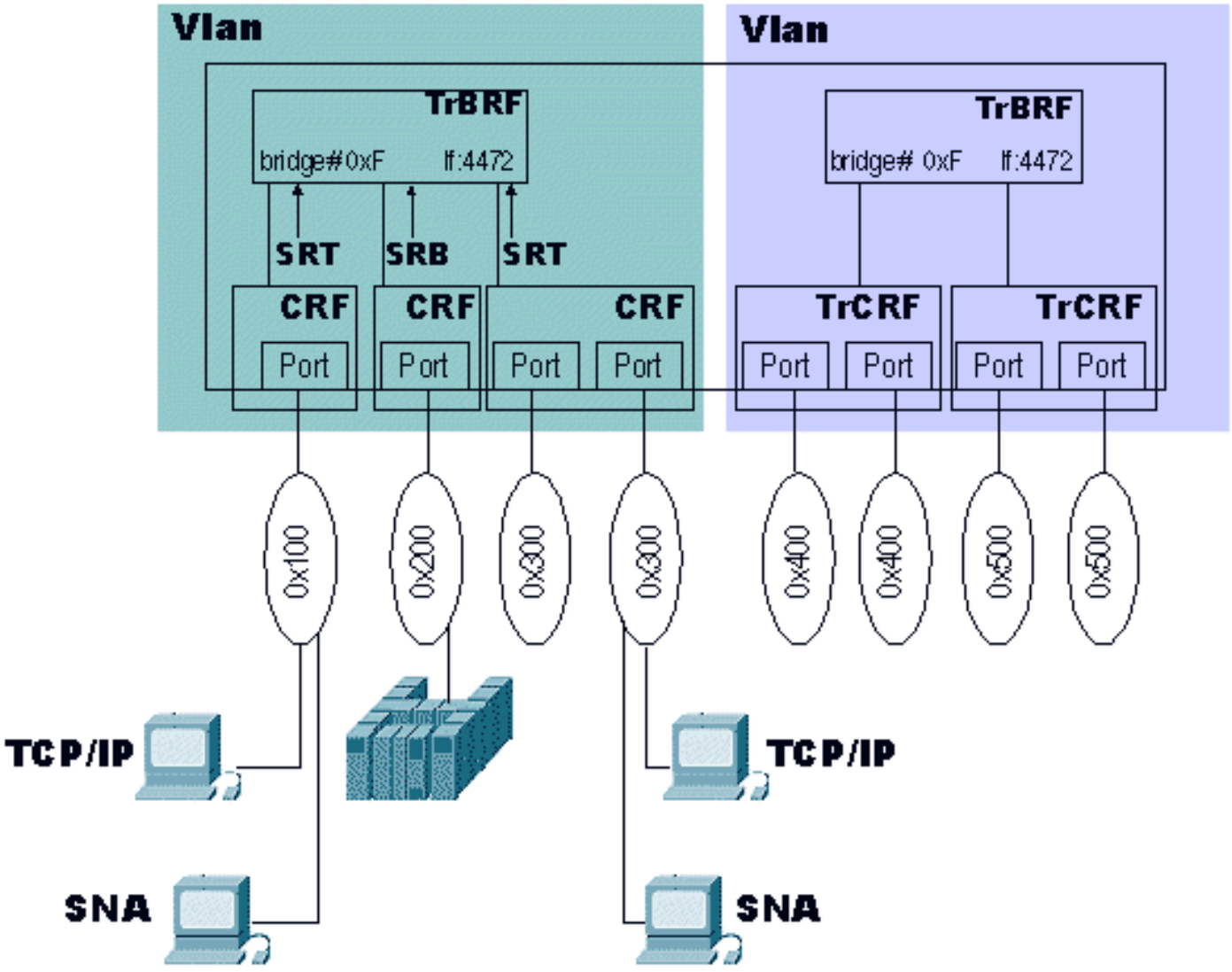
SRS是基于RIF的数据包的基本转发，无SRB功能，TrCRF也是如此。

注意：要查看Catalyst 5000中的路由信息表，请发出**show rif**命令。

源路由桥接和源路由透明

所有源路由桥接功能都位于TrBRF逻辑中。TrCRF是将命令桥接模式到TrBRF的路由器。因此，如果TrCRF配置为SRB模式到TrBRF，则当TrCRF收到NSR（非源路由）帧时，交换机不会将其转发到TrBRF逻辑。

如果您不希望某些类型的流量命中或离开特定环，则可以使用此选项。此图显示了一个示例：



如果TCP/IP客户端无法通过RIF发送数据包，则交换机不会将这些帧与大型机(0x200)置于同一环中。 但是，到主机的SNA帧（通常有RIF）将到达主机。这是一种非常基本的方法来过滤交换网络中的帧。

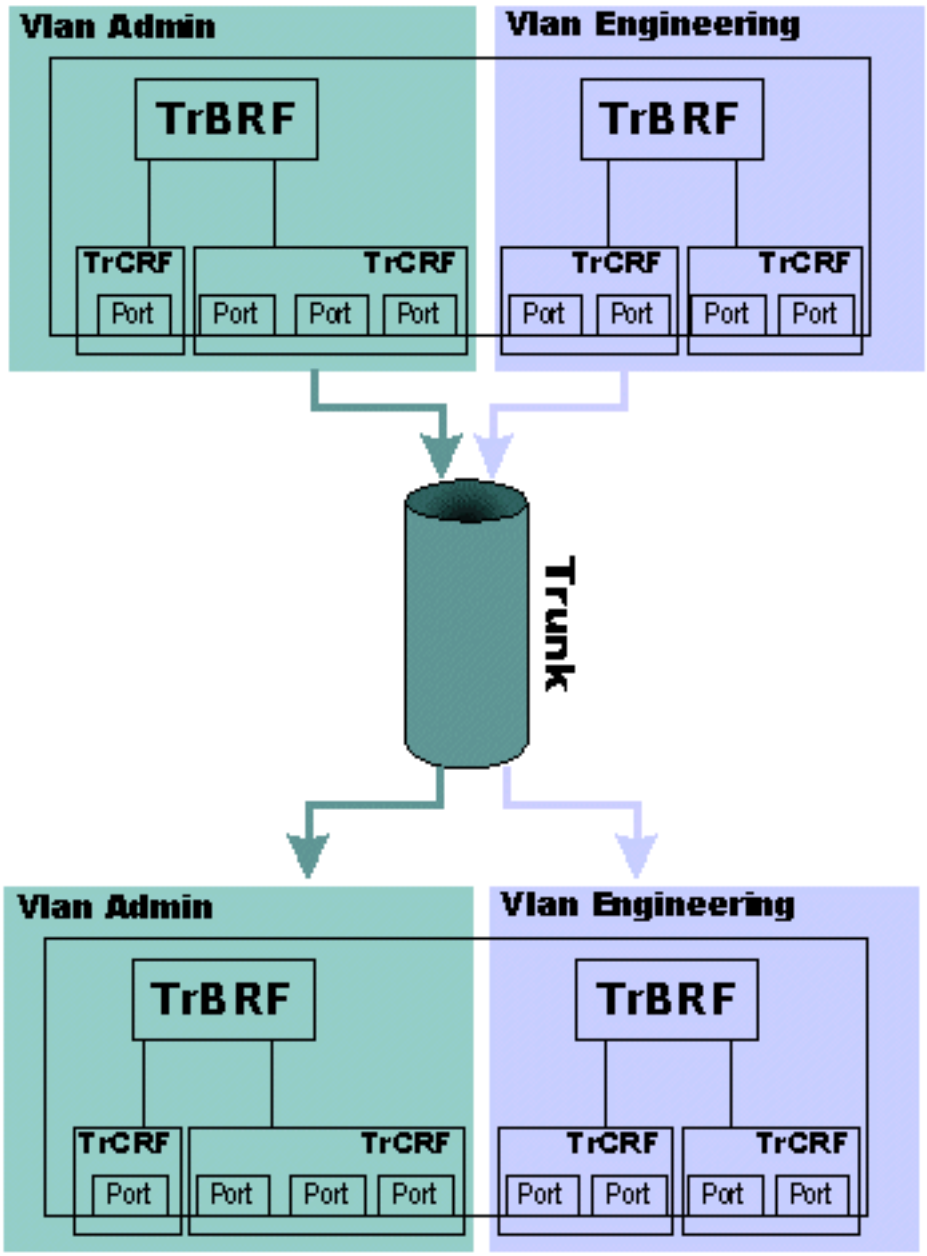
以下是交换机在TrBRF上转发源路由桥接帧时遵循的顺序：

1. 环0x300（端口4）上的SNA站发送一个探测器到达主机。
2. 当探查器数据包到达交换机时，它会在同一TrCRF中转发该探查器，但不进行修改；然后，它会将副本发送到TrBRF，以转发到TrCRF的其余部分。在这种情况下，由于数据包具有RIF，因此它通过SRB路径。交换机还需要学习路由。
3. 交换机将学习帧的SMAC，因为数据包显示为源于交换机所连接的本地环。这是因为，在多端口TrCRF组合中，RIF显示目的环，但交换机需要知道TrCRF中的哪个端口。因此，交换机会获知进入TrCRF级别的帧的SMAC。
4. 数据包将发往其余的所有TrCRF，这些TrCRF使用各自的网桥环号组合进行修改。
5. 一旦主机以SRB帧响应，交换机就会获取该TrCRF的主机SMAC并将其发送到出站端口。然后流量在两者之间来回传输。

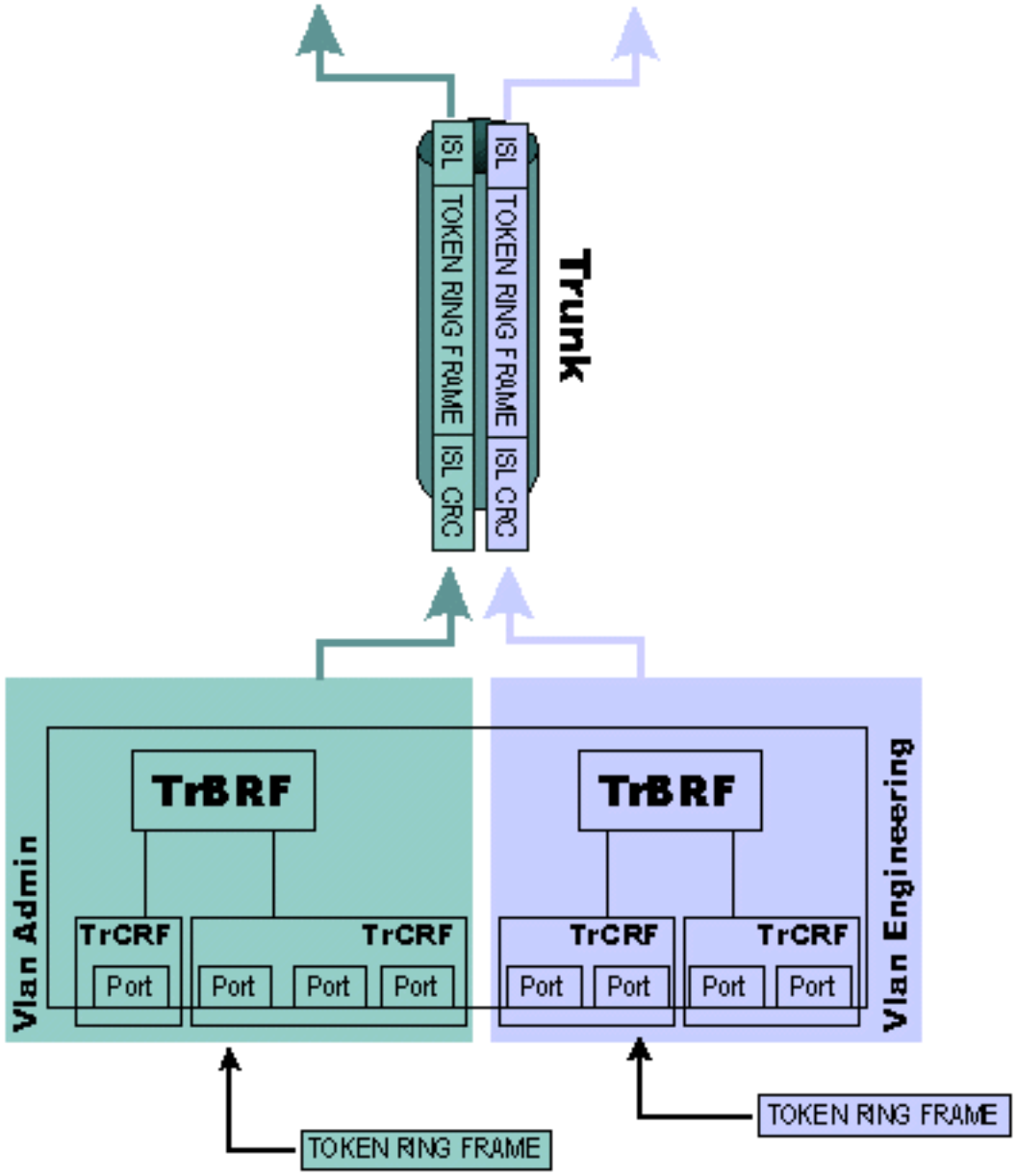
注意：要检查Catalyst 5000上的MAC地址表，请发**出show cam**命令。

交换机间链路

交换机间链路是一种非常简单的协议。基本上，通过ISL中继的帧封装在ISL帧中，该帧告知帧属于哪个VLAN。因此，必须手动或自动在交换机之间共享VLAN信息。称为VLAN中继协议(VTP)的协议可以处理此任务。对于令牌环VLAN，必须在网络中运行VTP V2。请考虑下图：



在这种情况下，创建了单个ISL中继，以自行承载工程VLAN和管理VLAN。任一VLAN中的流量在通过中继后均不混合。此图显示了此分离的实现方式：



这些VLAN中需要通过中继的每个帧都封装在ISL帧中，其VLAN也包含在帧中。这样，接收方交换机就可以将帧正确路由到其特定VLAN。令牌环ISL(TRISL)帧比常规ISL帧有更多字段。下图显示TRISL帧的布局：

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

注意：即使TRISL在快速以太网接口上运行，数据包在一定程度上仍包含标准令牌环帧和与该帧关联的VLAN信息。令牌环VLAN允许的帧大小最多为18k，ISL也允许。这不*是通过*帧的分段来实现的。整个帧封装在整个ISL帧中，并通过链路发送。ISL是以太网，其最大帧大小为1500字节，这是一种常见的误解。

在Catalyst 5000上，4.x版中提供了一种称为动态中继协议(DTP)的协议。DTP是动态ISL(DISL)的战略替代产品，因为它包含对802.1Q中继协商的支持。DISL的功能是仅对ISL进行协商，以确定两台设备之间的链路是否应该进行中继。DTP能够协商ISL和IEEE 802.1Q VLAN中继之间将使用的中继封装类型。这是一个有趣的功能，因为有些Cisco设备只支持ISL或802.1Q，而有些设备则能同时运行这两种功能。

以下是可配置DTP的五种不同状态：

- 自动 — 在自动模式下，端口侦听来自相邻交换机的DTP帧。如果相邻交换机表示它想成为中继（或是中继），则自动模式会与相邻交换机创建中继。当相邻端口设置为“打开”或“期望”模式时，会发生这种情况。
- 期望 — 期望模式向相邻交换机指示它可以是ISL中继，并且它希望相邻交换机也是ISL中继。如果邻接端口设置为 on、desirable 或 auto 模式，那么该端口将变成中继端口。
- 打开 — 打开模式自动在其端口上启用ISL中继，而不管其相邻交换机的状态如何。除非它收到显式禁用ISL中继的ISL数据包，否则它仍是ISL中继。
- Nonegotiate - Nonegotiate模式自动在其端口上启用ISL中继，而不管其相邻交换机的状态如何，但不允许该端口生成DTP帧。
- 关闭 — 在关闭模式下，不允许在此端口上使用ISL，而不管在另一台交换机上配置的DTP模式如何。

Catalyst 5000系列交换机通常用于提供ISL主干。然后，Catalyst 3900交换机可通过双100 Mbps ISL扩展模块连接到此主干。Catalyst 3900令牌环交换机不支持除ISL之外的任何其他模式，因此它始终为中继模式。此外，Catalyst 3900 ISL模块仅支持100 Mbps连接，默认为全双工。

通过ISL链路连接Catalyst 3900和Catalyst 5000交换机时，请非常小心。主要问题是Catalyst 3900不支持快速以太网介质协商。因此，如果Catalyst 5000配置为自动模式，则默认为100 Mbps半双工。这会导致端口从中继转到非中继和丢包等问题。

如果要将Catalyst 3900 ISL端口连接到Catalyst 5000的ISL端口，则必须手动配置Catalyst 5000上的ISL端口：

1. 发出**set port speed**命令，将其设置为100 Mbps:

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

2. 发出**set port duplex**命令以设置为全双工：

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

如果要强制交换机的端口进入中继模式，请发出**set trunk**命令（在一行上）：

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

在上一命令中，vlans是1到1005（例如，2-10或1005）的值，trunk_type设置为isl、dot1q、dot10、lane或negotiate。

一旦交换机上的中继端口处于活动状态，您就可以发出**show trunk**命令来查看这些中继端口是否处于活动状态。

```
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
```

用于观察ISL中继的一个重要命令是**show cdp neighbors detail**命令。此命令还有助于您了解网络拓扑。

```
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
```

从该输出中，您可以清楚地看到Catalyst 3900已连接到端口10/1。当您在上一个**show trunk**命令的输出中检查端口10/1时，您可以判断它是中继端口。

生成树

令牌环环境中的生成树可能非常复杂，因为可以同时运行总共三种不同的生成树协议。例如，典型环境在TrBRF级别运行IBM生成树，在TrCRF级别运行IEEE(802.1d)或Cisco。因此，生成树的故障排除要复杂一些。

此表告诉您根据不同类型的可能配置会发生什么情况：

T	TrCRF	TrBRF

rCRF桥接模式		
SRB	运行IEEE生成树。	用作源路由网桥。
	从外部网桥处理IBM生成树协议网桥协议数据单元(BPDU)。	将IBM生成树协议运行到外部网桥。
		丢弃TrCRF的透明IEEE生成树协议BPDU。
SRT	运行思科生成树协议。	用作源路由透明网桥。
	将目的地址字段的网桥组地址替换为思科特定组地址，以便外部网桥不分析TrCRF BPDU。	转发透明和源路由流量。
	生成BPDU，在出站帧的源地址字段中设置RIF位，并添加2字节RIF。此帧格式可确保TrCRF保持逻辑环的本地性，并且不会透明地桥接或路由到其他LAN的源。只有通过物理环路连接的TrCRF才会接收BPDU。	将源路由流量转发到TrBRF中的所有其他TrCRF，无论它们处于SRT或SRB模式。
	从外部网桥处理IEEE生成树BPDU。	

VLAN 中继协议

由于ISL决定了数据包的去向，因此每台交换机都必须知道网络中的VLAN。VTP的实际用途是跨交换机传播VLAN信息。VTP不在路由器中运行，因为它们应终止VLAN网络。网络中的每台交换机都应运行VTP。否则，交换机通常只运行一个VLAN（通常为VLAN 1），不会在该链路上运行ISL，因为不需要。VTP使VLAN的创建更加容易，因为您可以在一台交换机中配置VLAN，并且VLAN将通过网络传播。当然，这也带来了问题。

VTP不是稳健的系统，如增强型内部网关路由协议(EIGRP)或开放最短路径优先(OSPF)路由协议。它要简单得多，而且运行于一个非常重要的概念：修订。在VTP中，VTP设备有三种类型：客户端、服务器和透明设备。客户端VTP设备基本上只接受来自服务器设备的VLAN信息，无法修改此信息。但是，服务器可以修改任何VTP服务器上的VTP信息。因此，VTP具有修订系统。修改或更新VLAN数据库的任何VTP服务器都声称它是最新的修订版。因此，必须非常谨慎，因为具有最高修订版的交换机将成功$1？????其VLAN信息将是有效信息。例如，如果修改一台VTP服务器，说TrBRF VLAN 100将执行IEEE生成树，这会对所有交换机造成严重破坏，因为它可能导致交换机（如Catalyst 3900）将端口置于阻塞模式，以保护自身免受环路影响。此外，在网络中引入新交换机时要小心，因为它们的VTP修订版可能更高。在透明模式下，一个中继上收到的VTP数据包会自动传播到设备上的所有其他中继，而不会发生更改；但是，设备本身会忽略它们。

当您使用令牌环交换机设置VTP时，必须运行VTP V2。如果要使交换机同时运行以太网和令牌环VLAN，则必须升级VTP，即使对于以太网VLAN也是如此。不*能有*两个不同的VTP域（例如，不能有一个用于以太网，一个用于令牌环）。

VTP 修剪

VLAN中继的一个问题是，来自一个VLAN的广播信息会在所有中继上传播，因为交换机不知道远程交换机中存在哪些VLAN。因此创建了VTP修剪。它允许交换机协商哪些VLAN分配给中继另一端的端口，从而修剪未远程分配的VLAN。默认情况下，在Catalyst 3900和Catalyst 5000交换机上禁用修剪。

注意：版本4.1(1)中的Catalyst 3900交换机支持VTP修剪。

每条VTP修剪消息都包含有关相关VLAN的信息，并包含一个位，指示是否应为此中继修剪此VLAN(1表示不应修剪此VLAN)。 启用修剪功能后，VLAN流量通常不会通过中继链路发送，除非中继链路收到相应的加入消息，且相应的VLAN?？的位已启用。这非常重要，因为它告诉您，当您使用VTP修剪时，必须确保存在正确的信息和配置，并且所有交换机都在运行修剪；如果交换机不通过中继向另一台交换机发送加入消息，则可能会关闭特定VLAN或VLAN。修剪协商完成后，VLAN将以修剪或加入状态完成该中继。

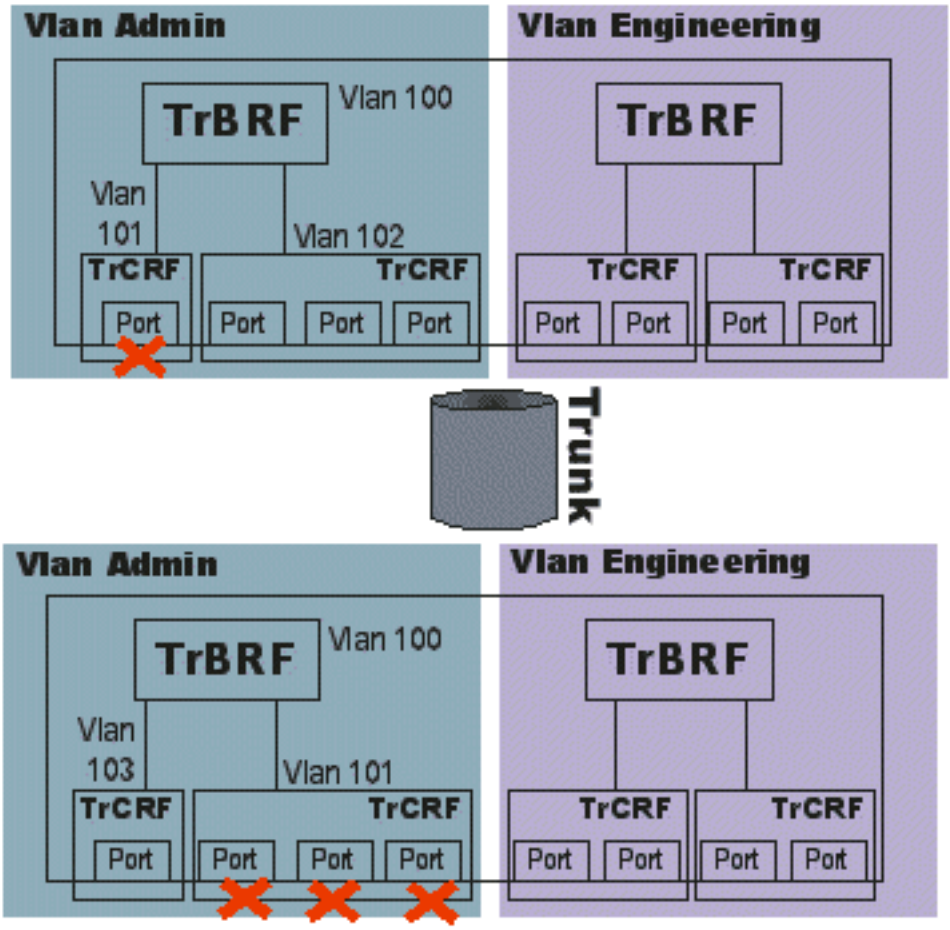
VTP修剪的一个非常重要的功能是允许您将VLAN配置为符合修剪条件或不符合修剪条件。此功能告知运行VTP修剪的交换机不修剪此VLAN。启用VTP修剪时，VLAN 2到1000默认修剪符合条件的VLAN。因此，当您启用修剪时，它会默认影响所有VLAN。VLAN 1、默认TrCRF(1003)、默认TrBRF(1005)和TrCRF始终不符合修剪条件；因此，来自这些VLAN的流量无法修剪。

重复环协议

重复环协议设计为在运行令牌环VLAN的交换机上运行。其工作是确保令牌环VLAN的正确配置并减少资源管理器。DRiP使用VTP来同步其VLAN数据库信息，但DRiP不需要VTP才能工作（VLAN数据库可手动建立）。 一种误解是DRiP能够理解振铃号；这不是真的。DRiP依赖于网络中配置的VLAN的唯一性和VLAN数据库配置。

DRiP最重要的功能之一是实施TrCRF分布。在令牌环世界中，由于生成问题，分发除1003之外的任何VLAN非常危险。因此，如果分配了除VLAN 1003之外的TrCRF，则DRiP会禁用与该VLAN关联的所有端口。

此示例说明此概念：

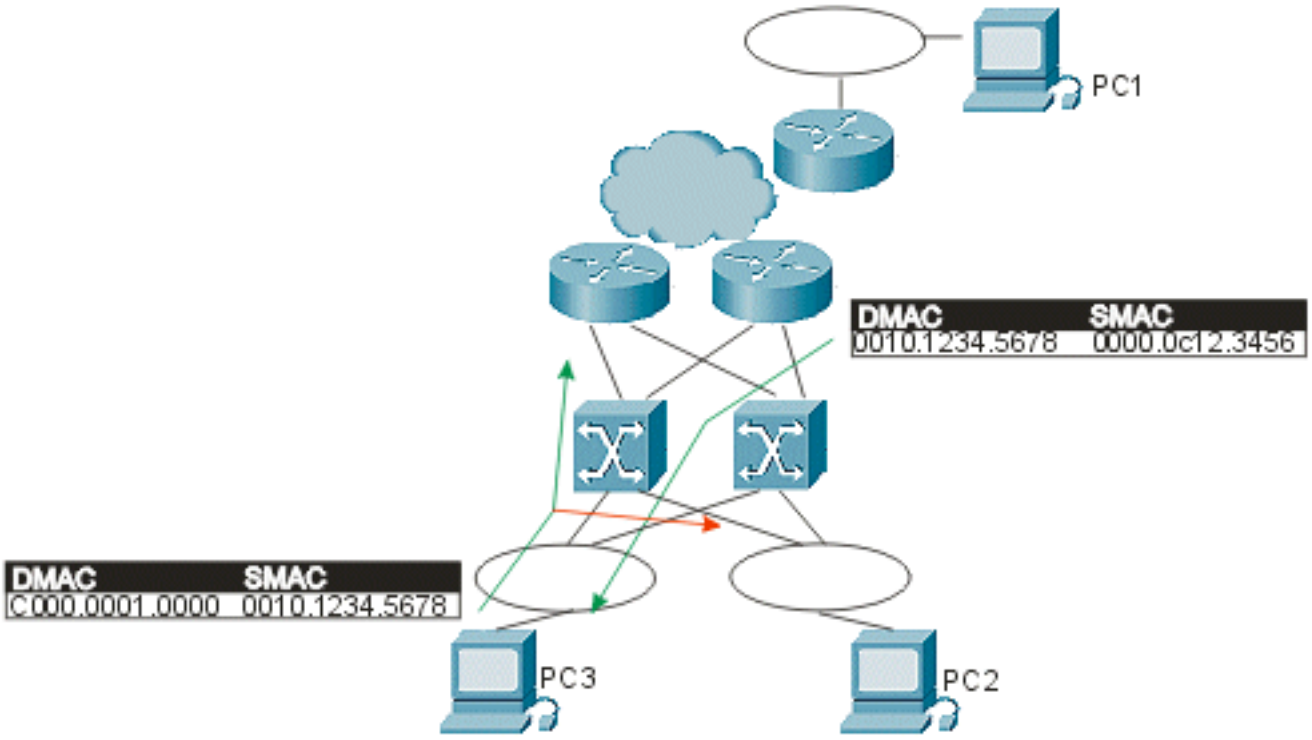


在该示例中，两台不同的交换机具有分配给VLAN 101的端口。交换机通过DRiP将端口生成树移动以禁用和停止转发流量。这样可以防止交换机出现环路。

如果没有变化，DRiP每30秒向其所有中继端口通告TrCRF状态。通过CLI（命令行界面）或SNMP进行的任何更改都会立即向所有端口发送更新。这些通告是0类ISL帧，并在默认VLAN 1上流。由于DRiP只通告其对VLAN的影响，因此通过ISL连接的交换机中必须存在正确的VLAN信息。这通过VTP完成。如果禁用了VTP，则必须在共享相同VLAN的所有交换机上手动维护此功能。DRiP通告仅存在于ISL链路上。它们不存在于ATM、令牌环、以太网或FDDI上。DRiP中没有保留拓扑树。

HSRP和令牌环VLAN

HSRP的最大问题之一是网络中组播地址的使用。由于网络中没有人使用此虚拟MAC地址来实际发送数据包，因此交换机从不学习这些MAC地址。因此，它们会在整个网络中泛洪帧。因此，需要使用HSRP的**standby use-bia**功能来发送使用活动HSRP路由器接口的烧录MAC地址的数据包。此场景的主要问题是，当HSRP路由器交换时，它们必须发送广播地址解析协议(ARP;无故ARP)到线路上的所有站点，以便站点获取网关的新MAC地址。尽管此过程应根据IP规范运行，但是它存在一些已知问题。由于来自该字段的持续请求，HSRP已更改，因此您可以拥有组播地址，也可以使用HSRP而不**使用备用use-bia**。此更改在Cisco IOS软件版本11.3(7)和12.0(3)及更高版本中发布。



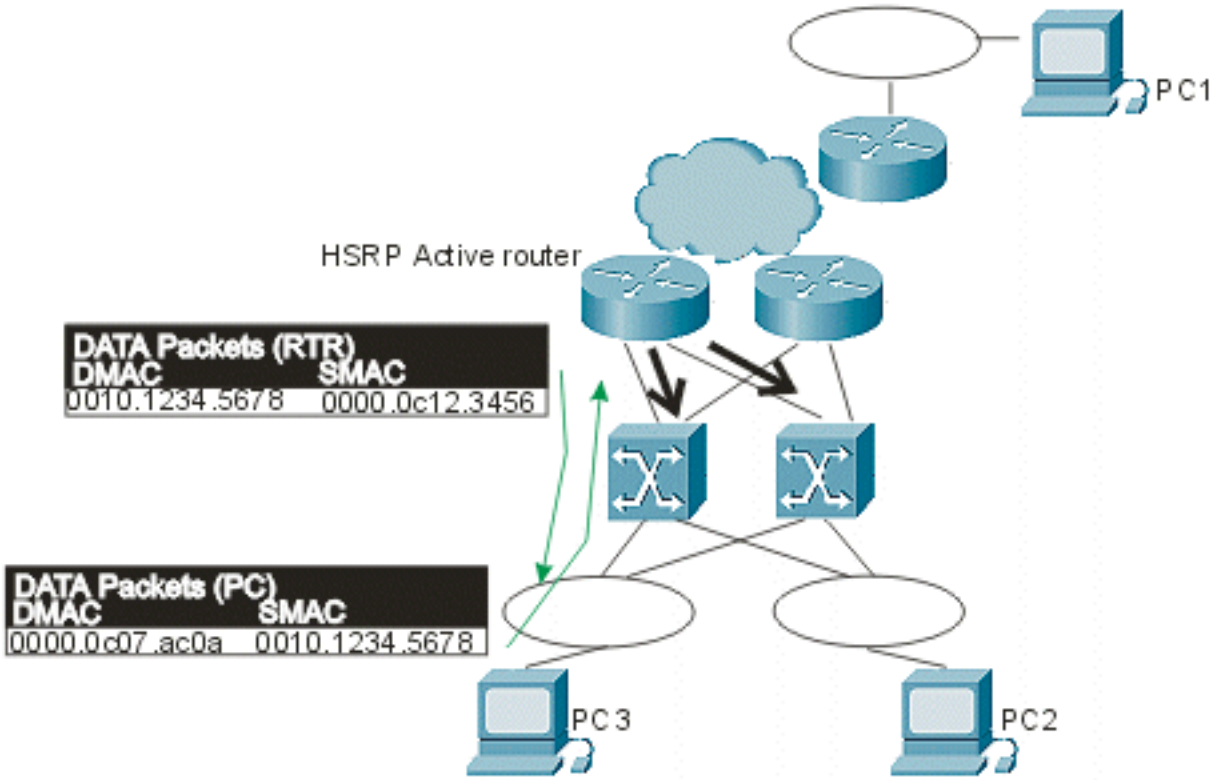
在上图中，PC1和PC3之间正在通信。问题是从客户端到本图中默认路由器的IP流量使用组播目标地址。因为没有人能从该地址获取此数据包，所以交换机永远不会学习此地址，并且始终会泛洪数据包。依赖于组的传统DMAC是C000.000X.0000，在令牌环中，它永远不能是SMAC。因此，PC2现在可以看到从PC3通过默认网关发往PC1的所有数据包。在网桥众多的网络中，这可能会迅速增加，并导致看似广播风暴但实际上是大量组播流量的情况。

要解决此问题，您必须使用MAC地址，该地址实际上可由HSRP Hello中的路由器用作SMAC。这样，交换机就可以获知此地址，从而相应地交换数据包。为此，请在路由器中配置新的虚拟MAC地址。客户端需要将数据包发送到此新虚拟地址的DMAC。以下是show standby命令的**输出**示例：

```
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
```

在该输出中，已创建备用组10（备用IP 1.1.1.100）。MAC地址(`0000.0c07.ac0a`)是新的虚拟MAC地址，最后一个字节是组(0xA = 10)。 一旦您有了此新配置，您现在将拥有此流量模式，可避免流量泛洪：



现在，由于路由器使用HSRP虚拟MAC的DMAC来获取数据包，因此交换机将学习此MAC地址，并仅将数据包转发到活动HSRP路由器。如果主用HSRP路由器发生故障，备用路由器变为主用状态，则新主用路由器将开始发送具有相同SMAC的HSRP问询，这会导致交换机MAC地址表将其学习的条目切换到新交换机端口和中继。

由于多环，需要采取其他操作来确保RIF在过渡期间实际发生更改（即使它是相同的MAC地址）。多环是路由器将RIF与MAC地址关联的功能，就像终端站一样。路由器需要在SRB网桥存在的环境中使用多环，以便数据包可以通过它们到达终端站。

在与以前相同的示例中，您可以看到客户端连接到新的活动HSRP路由器所需的其他步骤：

1. 活动路由器停止工作。
2. 一旦备用路由器检测到HSRP Hello丢失，它将启动进程，使其成为活动HSRP路由器。
3. 路由器从与以前相同的SMAC（在MAC层和ARP层）发送无故ARP。
4. 现在，PC将帧发往同一MAC地址，但是使用新的RIF。
5. 路由器收到此帧（发往HSRP MAC）后，会直接向客户端发送ARP请求，因为它的ARP表中没有该客户端的MAC地址。
6. 收到对ARP数据包的响应后，路由器可以将数据包发送到目的客户端。

相关信息

- 交换机产品支持
- LAN 交换技术支持
- 技术支持和文档 - Cisco Systems