

令牌环交换概念

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[TrBrf和Trcrf](#)

[交换模式](#)

[透明桥接](#)

[源路由交换](#)

[源路由桥接和源路由透明](#)

[交换机间链路](#)

[Spanning-Tree](#)

[VLAN 中继协议](#)

[VTP 修剪](#)

[复制圆环协议](#)

[HSRP和令牌环VLAN](#)

[相关信息](#)

简介

要开始了解令牌环交换的概念，重要的是非常您了解透明桥接、源路由桥接和Spanning-Tree。Catalyst 3900和Catalyst 5000使用新概念，正如IEEE802.5 Annex K所描述。这些概念是令牌环VLAN的构建模块。本文解释不同的桥接概念，并且这些如何工作：

- 交换机间链路(ISL)建立中继
- Spanning-Tree
- VLAN 中继 协议 (VTP)
- 复制圆环协议(DRIP)

本文也解释发生的某些问题，当您运行在令牌环VLAN的热备份路由协议(HSRP)和他们的应急方案。

注意： 关于在本文使用令牌环缩略语的定义，参考[令牌环交换缩略语](#)。

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

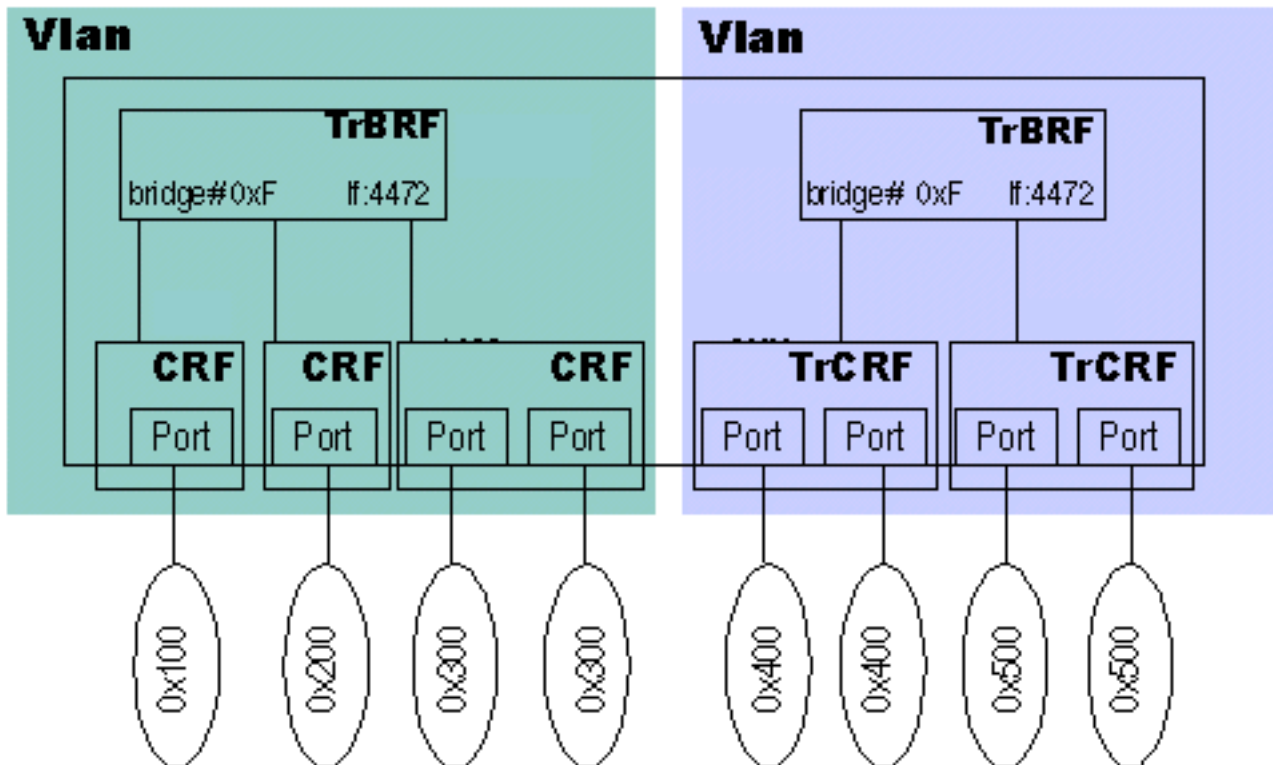
有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

TrBrf和Trcrf

令牌环网桥中转功能(TrBrf)和令牌环集中器中继功能(Trcrf)是Catalyst 3900和Catalyst 5000功能的体系结构的构建模块。TrBrf是交换机的网桥功能，并且Trcrf是交换机的集中器功能。请注意桥接发生在这两块层，因为，在令牌环，三不同种类的桥接讨论。

交换机的TrBrf功能控制源路由桥接数据流交换，类似源路由桥接(SRB)和源路由透明桥接(SRT)。Trcrf报道源路由交换(SRS)和透明桥接(TB)的功能。例如，有Catalyst 3900交换机只有一TrBrf的是可能的，并且一Trcrf和交换机的所有端口在同样Trcrf。这引起交换机只能执行SRS和TB。如果定义十不同的Trcrf在同样parent TrBrf下，则从连接对同样Trcrf的端口的流量通过SRS或TB的Trcrf功能将转发。去在交换机的其他Trcrf的流量将使用交换机的TrBrf功能并且来源路由桥接的或来源路由透明地桥接的。不同的交换机制将是讨论以后在本文。

此图表与物理世界涉及TrBrf和Trcrf：



您能看到每Trcrf连接到一特定环。Trcrf能折衷多个端口，并且这些端口将减弱同一环号。TrBrf一起连接Trcrf。

Trcrf和TrBrf本身是不同的VLAN。因此，在令牌环，您能桥接在VLAN之间。在令牌环VLAN之间的

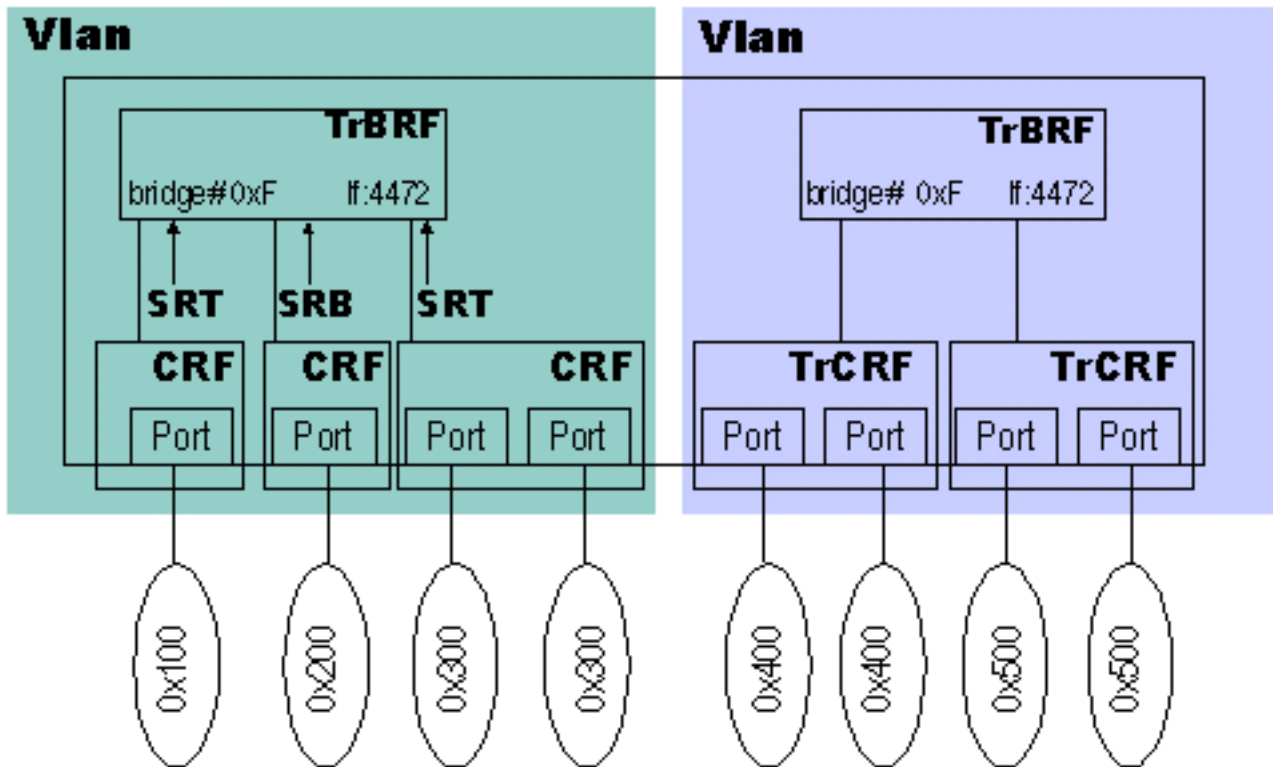
桥接遵从两个规则：

- 桥接在两TrBrf VLAN之间可能由一个外部设备只完成，类似路由器或路由交换模块(RSM)。
- 桥接在Trcrf是同样parent TrBrf VLAN的孩子的VLAN之间可能用Trcrf VLAN只完成。

因为中断以太网示例，这是非常重要为令牌环VLAN记住。要汇总，什么将看起来象以太网VLAN是一TrBrf和其儿童Trcrf的总和。由于您能桥接在令牌环的某些VLAN之间，您必须知道此桥接如何出现。

注意： 要使更加容易关于以太网VLAN了解令牌环VLAN，请记住Trcrf和TrBrf的组合本身做VLAN。

在此图表中，您能看到Trcrf决定在Trcrf和TrBrf之间的桥接模式。



各自的Trcrf配置什么类型的桥接他们进行对TrBrf。这是重要，因为您能有将执行源路由桥接对其他Trcrf的Trcrf VLAN，但是不执行非来源路由的帧。在上一个图表中，一Trcrf为SRB模式配置，并且两在SRT模式。这意味着SRB流量能流在所有三Trcrf之间，但是SRT能只流在SRT模式的两个之间。这允许您对设置的granularly流量如何应该流在Trcrf之间。如果桥接模式设置在TrBrf，将影响该VLAN的所有Trcrf孩子。

交换模式

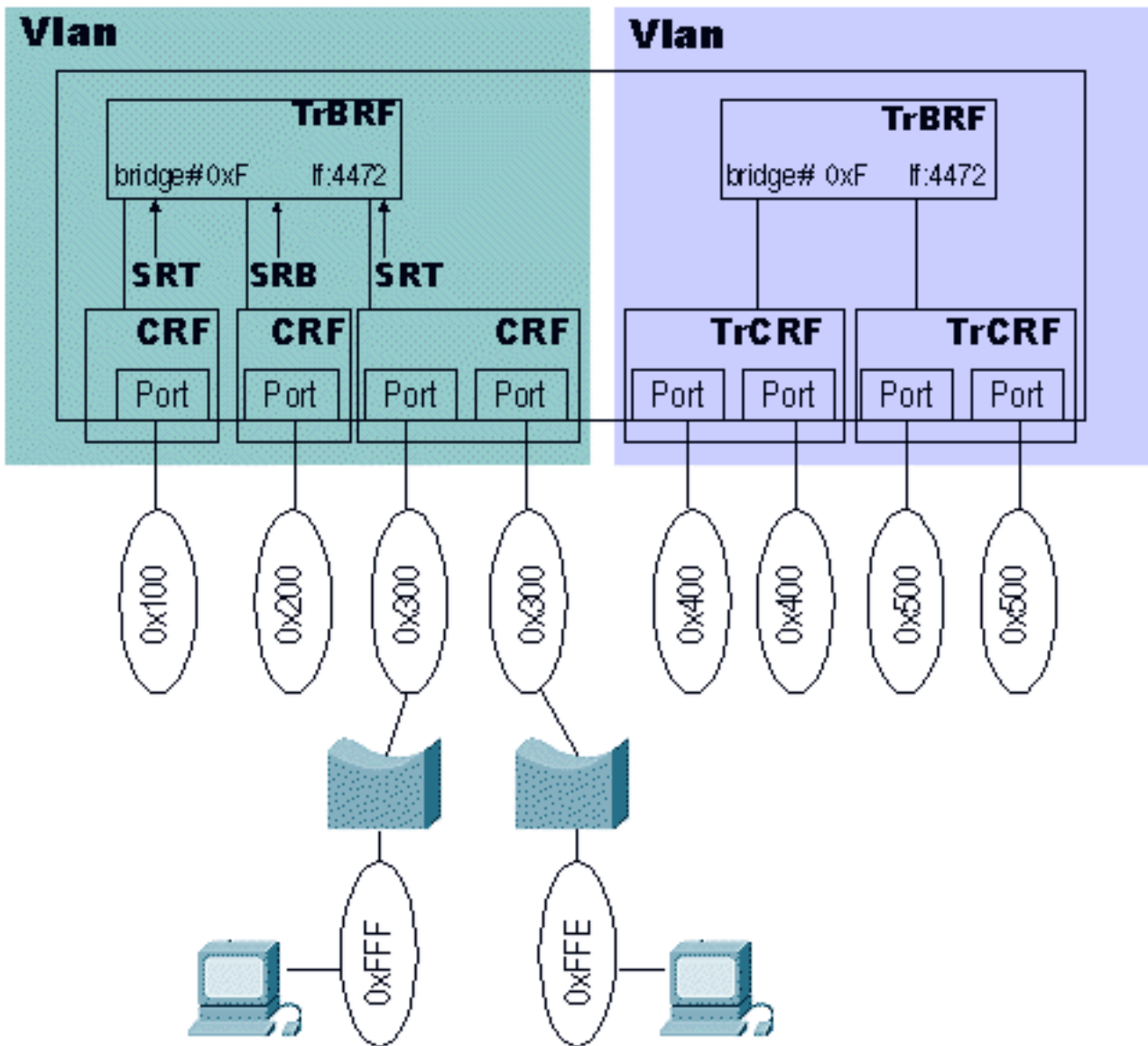
箱外， Catalyst 3900配置与一TrBrf和一Trcrf。所有端口分配到默认Trcrf VLAN1003。同样适用于Catalyst 5000令牌环叶片。因为给确定方框？，这是重要？？即插即用？？功能。箱外，这些交换机能执行根据源路由交换和透明桥接的转发。以下部分提供关于这些技术的细节。

透明桥接

透明桥接是最基本所有交换机制和根据帧目的地MAC (DMAC)地址在网络的。这是以太网转发机制。交换机任何时候接收帧，记录帧的源MAC (SMAC)地址作为属于该端口，并且，从此，转发流量被注定对对该端口的该MAC的一个。如果，在学习进程，交换机不知道关于MAC地址，将充斥该数据包到所有端口在转发状态。

源路由交换

源路由交换是需要的转发机制，当只有一Trcrf分配到端口时，并且交换机收到有路由信息字段的(Rif)数据包他们的。由于交换机不会修改帧的RIF (因为不会通过它对TrBrf)，网络一定能做出在转发的决策，与RIF，不用修改。考虑显示SRS的此网络图：



去从环0xFFF的流量敲响0xFFE需要通过交换机。此流量是源路由网桥数据流。这是在这两个客户端之间的通信启动顺序：

1. 一个站点发送探测包到驻留的环。假设，环的0xFFF客户端发送数据包;它查找如此物(在十六进制)：
0000 00c1 2345 8000 0c11 1111 C270
注意：该数据包信息只显示DMAC、SMAC和RIF信息。
2. 一旦数据包到达源路由网桥并且传送帧对电线，数据包如下所示：
0000 00C1 2345 8000 0c11 1111 C670 FFF1 3000
C670是路由控制字段，并且FFF1 3000是环0xFFF，网桥0x1，环0x300。关于解码Rif的更多信息，参考[配置源路由桥接](#)。
3. 现在，数据包押交换机。由于交换机看到数据包很远来自一敲响，学习路由描述符。在这种情况下，交换机当前知道环0xFFF通过网桥0x1在端口3.查找。
4. 由于数据包是探测包，交换机传送帧对所有端口在同样Trcrf下。如果Explorer需要去端口用不

同的Trcrf，它将提供帧对TrBrf，将执行其网桥功能。如果有同样Trcrf的端口，将传送帧出站，不用修改。

5. 环的0xFFE站点应该获得Explorer和回应到它。假设，客户端回应定向帧。此定向帧如下所示：

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

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

6. 最后，交换机学习环0xFFE在端口4查找并且保持路由描述符。

从此，交换机知道关于那些环。如果查看表，您应该看到交换机了解关于网桥号和环号。任何其他环，在环0xFFF和环0xFFE不是必要的后，因为他们必须穿过环0xFFF或敲响0xFFE到达交换机。

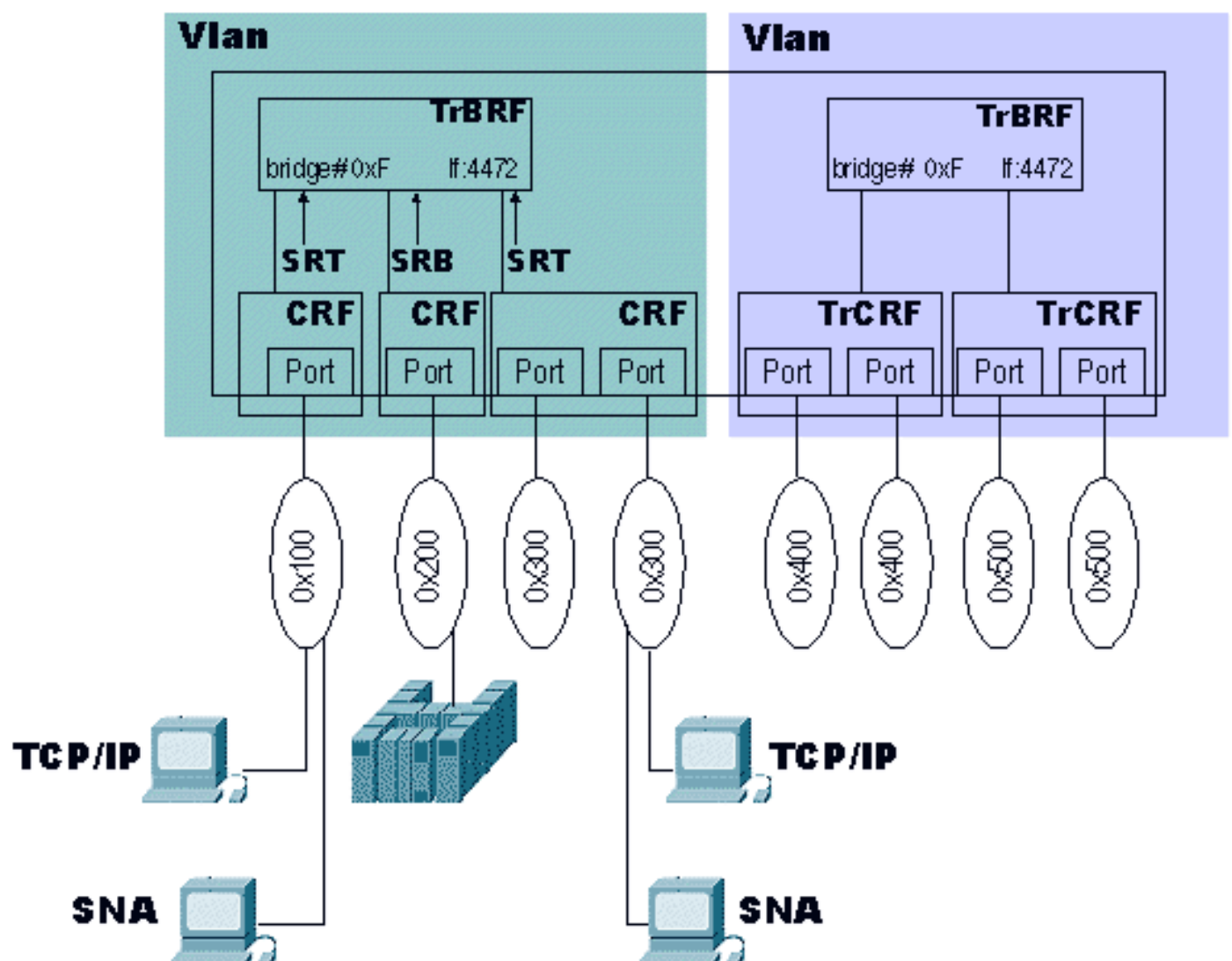
没有SRB功能，SRS是基于RIF的信息包基本转发，对Trcrf通常就是这样。

注意：要查看在Catalyst 3900的路由信息表，参考[每个VLAN的观察路由描述符表](#)在[管理Catalyst 3900](#)。对于Catalyst 5000，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在TrBrf逻辑查找。Trcrf是发出命令桥接模式到TrBrf的那个。因此，如果Trcrf为对TrBrf的SRB模式然后配置，当Trcrf接收NSR (非来源路由的)帧，交换机不会寄它给TrBrf逻辑。

这，如果不希望流量特定类型点击或留下一特定环，可以使用。此图表显示示例：



如果TCP/IP客户端没有能力发送有Rif的数据包，交换机在同一环不会放置那些帧用大型机(0x200)。然而，对(的SNA帧通常有RIF)的主机将到达大型机。这是一个非常基本方式过滤在交换网络的帧。

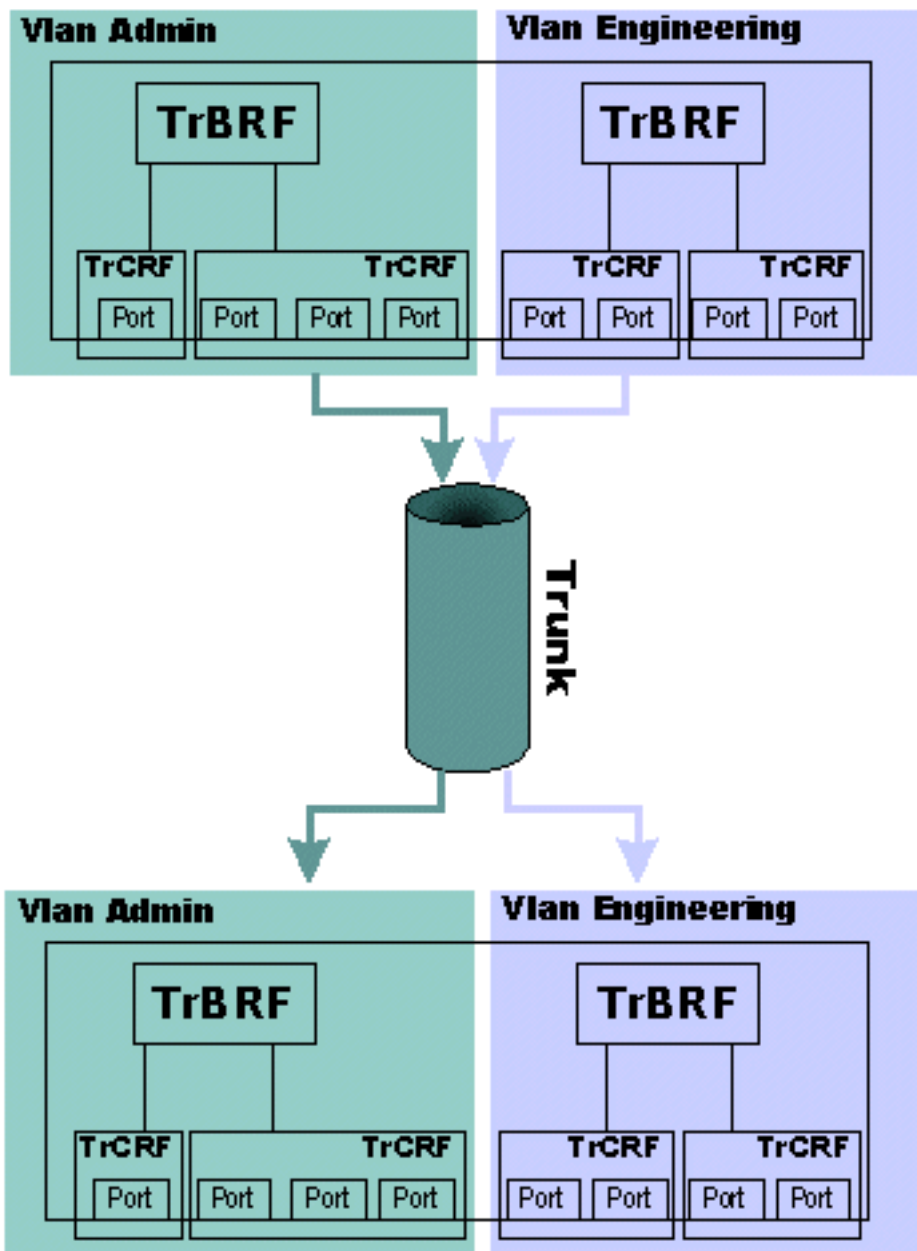
这是交换机跟随传送在TrBrf间的来源路由桥接帧的顺序：

1. 环的0x300 SNA站点(端口4)发送Explorer到达大型机。
2. 当探测包押交换机时，促进Explorer，不用修改，在同样Trcrf;然后它发送复制对TrBrf转发到Trcrf的其余。在这种情况下，因为数据包有RIF，它通过SRB路径。交换机也需要学习路由。
3. 交换机学习帧的SMAC，因为数据包显示如产生在交换机连接的本地环。这是因为，在多个端口Trcrf组合，RIF显示目的地环路，但是交换机需要知道Trcrf的哪个端口。所以，交换机学习进来在Trcrf级别帧的SMAC。
4. 数据包出去对所有Trcrf的其余，修改与他们的各自的网桥环编号组合。
5. 一旦主机回应SRB帧，交换机学习主机的SMAC该Trcrf的并且发送它到出站端口。流量反复然后流在两个之间。

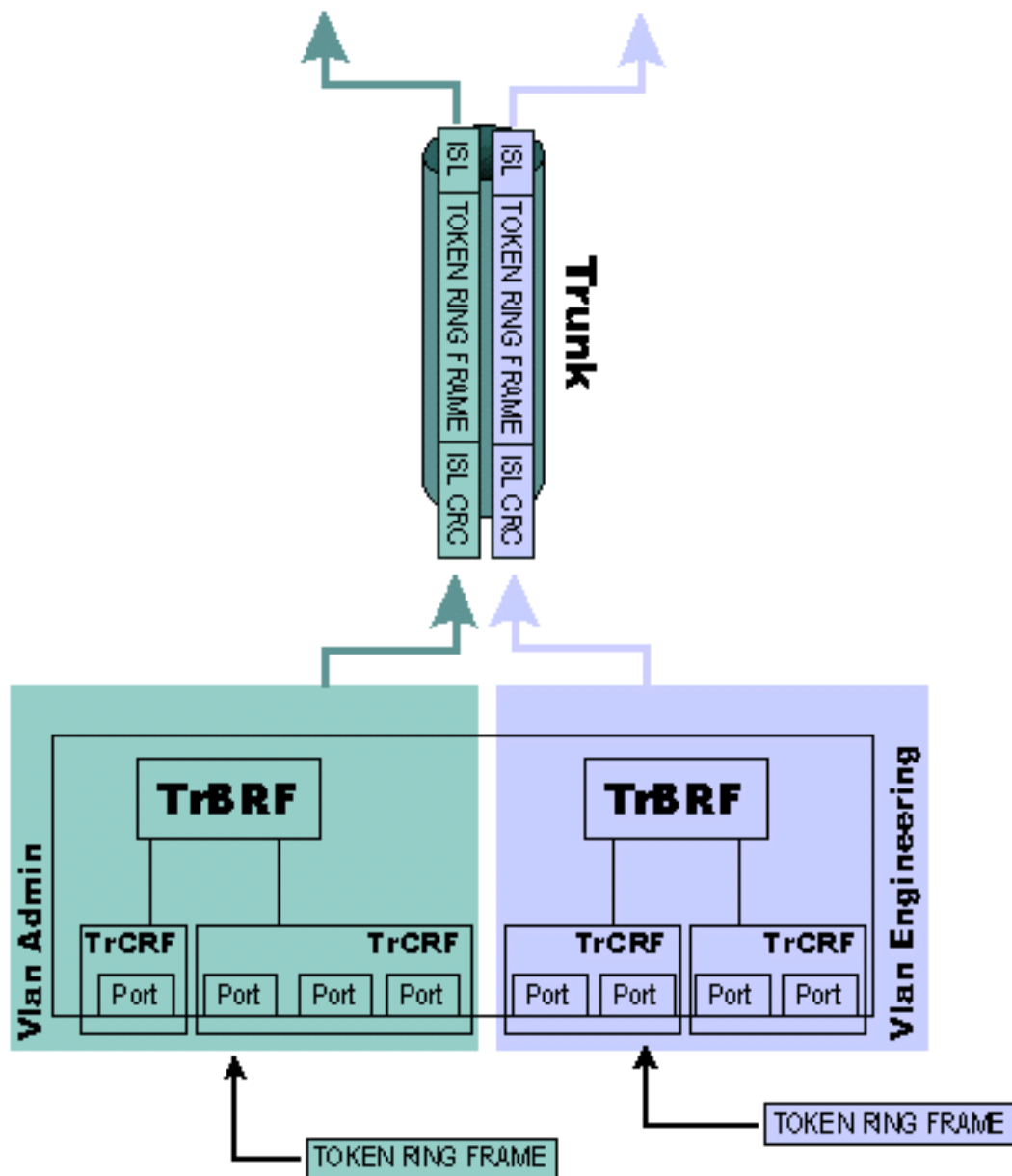
注意：要检查在Catalyst 3900的MAC地址表，参考[查看在管理Catalyst 3900的主地址表](#)。对于Catalyst 5000，请发出[show cam命令](#)。

交换机间链路

交换机间链路是一个非常简单的协议。基本上，在ISL中继线间去的帧在告诉另一侧对的ISL帧被封装哪个VLAN帧属于。因此，必须手动或自动共享VLAN信息在交换机之间。作为VLAN中继协议(VTP)被已知的协议能处理此任务。对于令牌环VLAN，您必须运行在网络的VTP V2。考虑此图表：



在这种情况下，单个ISL中继线创建运载，单独，工程的VLAN和admin VLAN。在通过中继后，流量都在任何一个VLAN不混合。此图表显示此分离达到的方法：



需要在中继间去从那些VLAN的每帧在ISL帧和其VLAN在帧被封装包括。这允许接收的交换机正确地路由帧到其特定VLAN。令牌环ISL (TRISL)帧比一正常ISL帧有更多一些字段。此图表显示 TRISL帧的布局：

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	Exit	
ENCAP FRAME (Continued)			8 to 196600 (1 to 24575 bytes) ENCAP FRAME	32 Syn CRC	32 ISL CRC

注意：即使TRISL运行快速以太网接口，数据包包含用该帧和VLAN信息关联的一个标准的令牌环帧，某种程度上。令牌环VLAN允许至18k帧大小，象ISL。这没有通过帧的分段达到。整个帧在一个全部的片段的一ISL帧被封装并且在链路间发送。有常见的误解ISL是以太网，并且其最大帧大小是1500个字节。

在Catalyst 5000上，作为动态中继协议(DTP)被已知的协议变得可用在版本4.x。因为合并802.1q中继协商的，支持DTP是动态ISL (DISL)的战略替换。DISL ???s功能将仅ISL的协商，两个设备之间的一条链路是否应该建立Trunk。DTP能协商将使用在ISL和IEEE 802.1Q VLAN中继之间的这中继封装。这是有趣的功能，因为一些Cisco设备支持仅ISL或802.1Q，而一些能运行两个。

这些是您能配置DTP的五不同的状态：

- 自动 ??? 在自动模式，端口细听从相邻交换机的DTP帧。如果相邻交换机表明希望是中继 ??? 或者它是中继 ??? 然后自动模式创建中继用相邻交换机。当相邻端口被设置至开或期望的模式时，这发生。
- 理想 ??? 期望的模式表明到相邻交换机是可以是ISL中继线，并且它类似是的相邻交换机也ISL中继线。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。
- 在 ??? 不管其相邻交换机的状态， On模式自动地启用在其端口的ISL中继。它保持ISL中继线，除非收到明确地禁用ISL中继线的ISL数据包。
- Nonegotiate ??? 非协商模式自动地启用在其端口的ISL中继 ??? 不管其相邻交换机的状态 ??? 但是不允许端口产生DTP帧。
- ??? 在Off模式， ISL在此端口没有允许不管在另一交换机配置的DTP模式。

交换机Catalyst 5000系列典型地用于提供ISL骨干网。Catalyst 3900交换机可能然后连接到此骨干网通过双重100 Mbps ISL扩展模块。Catalyst 3900令牌环交换机比ISL不支持其他模式，因此总是建立中继。并且， Catalyst 3900 ISL模块只支持100 Mbps连接并且默认为全双工。

当您通过ISL链路时，连接Catalyst 3900和Catalyst 5000交换机非常小心。主要问题是Catalyst 3900不支持快速以太网媒体协商。为此，如果Catalyst 5000为自动模式配置，它然后默认为100 Mbps半双工。这引起问题类似去从中继的端口到非Trunk和包丢失。

如果要附加Catalyst 3900 ISL端口到Catalyst 5000的ISL端口，您必须手工配置Catalyst 5000的ISL端口：

1. 发出set port speed命令设置为100 Mbps：

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

2. 发出set port duplex命令设置为全双工：

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

如果要迫使交换机的端口到中继模式，请发出set trunk命令(在一条线路)：

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

例如在前面的命令， VLAN是值从1至1005 (2-10或者1005)，并且trunk_type设置为isl， dot1q， dot10， 通道， 或者请协商。

一旦中继端口是活跃的在交换机，您能发出show trunk命令发现这些中继端口是活跃的。

```
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
```

—重要命令使用观察ISL中继线show cdp neighbors detail命令。此命令也帮助您了解网络拓扑。

```
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，您能清楚看见Catalyst 3900连接到端口10/1。当您在输出检查端口10/1上一个show trunk命令中时，您能告诉它是中继端口。

Spanning-Tree

因为一个能同时用总共三个不同的生成树协议，在令牌环环境的Spanning-Tree能获得非常复杂。例如，在TrBrf级别和运行IEEE (802.1d)的一个典型的环境运行在Trcrf级别的IBM生成树或思科。所以，Spanning-Tree是更加复杂的排除故障。

此表告诉您发生了什么基于不同种类的可能的配置：

Trcrf 桥接	Trcrf	TrBrf
-------------	-------	-------

模式		
SRB	运行IEEE生成树。	实行作为源路由网桥。
	进程IBM生成树协议网桥协议数据单元(BPDU)从外部网桥。	用IBM生成树协议到外部网桥。
		下降Trcrf的透明IEEE生成树协议BPDU。
SRT	运行思科生成树协议。	实行作为源路由透明网桥。
	用CISCO专用的组地址替换目的地址字段网桥组地址，因此外部网桥不分析Trcrf BPDU。	转发透明和源路由数据流。
	生成BPDU，在RIF源地址域设置的RIF位被添加的出站帧和2字节的。此帧格式保证Trcrf保持本地对逻辑环和透明地没有桥接或者来源路由对其他LAN。通过物理环路连接的仅Trcrf接收BPDU。	寄源路由数据流给在TrBrf的其他Trcrf，他们是否在SRT或SRB模式。
	进程从外部网桥的IEEE生成树BPDU。	

欲知更多信息，参考在[令牌环VLAN和相关协议的生成树协议](#)。

VLAN 中继协议

由于，与ISL，VLAN确定数据包哪里应该是，重要的是每交换机知道关于在网络的VLAN。VTP？？？s目的在生活中将传播在交换机间的VLAN信息。因为他们应该终止VLAN网络，VTP在路由器不运行。在网络的每交换机应该运行VTP。否则，交换机通常只然后运行一个VLAN(通常VLAN 1)和不会运行在该链路的ISL，因为没有需要。VTP做VLAN的创建一更加容易的任务，因为您可能配置在一交换机的VLAN，并且他们通过网络会传播。当然，那附有问题。

VTP不是一个坚固的系统，类似增强的内部网关路由选择协议(EIGRP)或开放最短路径优先(OSPF)路由协议。它更加简单并且起作用一个非常重要概念：版本。在VTP中，有VTP设备的三种类型：客户端、服务器和透明设备。客户端VTP设备基本上就是接受从服务器设备的VLAN信息，并且不能修改此信息。服务器，然而，能修改关于的VTP信息任何VTP服务器。为此，VTP有一个版本系统。修改或更新VLAN数据库的所有VTP服务器声称它是最新版本。为此，因为有最高的版本的交换机？，必须使用特别警告？？成功？？？并且其VLAN信息将是有效一个。例如，如果修改一个VTP服务器说TrBrf VLAN 100执行IEEE生成树，这将造成在所有的浩劫交换机中，因为在阻塞模式可能引起交换机(类似Catalyst 3900)放置端口，保护自己以防止环路。并且，小心，当您引入新的交换机到网络时，因为他们可能有更高的VTP版本。在透明模式，在一中继接收的VTP数据包自动地被传播，不用更改，到在设备的其他中继;但是，他们在设备忽略。

当您设置VTP用令牌环交换机时，您必须运行VTP V2。如果有运行以太网和令牌环VLAN的交换机，则您必须升级VTP，为以太网VLAN。您不能有两个不同的VTP域(例如，您不能有一以太网的和一个令牌环的)。

欲知更多信息，参考在[令牌环VLAN和相关协议的VLAN中继协议](#)。

VTP 修剪

一问题用VLAN中继是从一个VLAN的广播信息在所有中继间传播，因为交换机不知道哪些VLAN在远程交换机存在。VTP修剪为此创建。它允许交换机协商哪些VLAN分配到端口在中继的另一端，并且，因此，修剪没有远程分配的VLAN。默认情况下修剪在Catalyst 3900及Catalyst 5000交换机禁用。

注意：在版本4.1(1)的Catalyst 3900交换机支持VTP修剪。

其中每一个VTP修剪消息包含指示关于有问题的VLAN的信息并且包含有点是否应该为此中继修剪此VLAN (a 1表明不应该修剪)。当修剪，除非中继链路收到与相应的VLAN的一适当的Join消息？，启用，VLAN流量没有在中继链路间通常发送？？启用的s位。这是非常重要，因为告诉您那，当您使用VTP修剪时，您必须确保，正确信息和配置存在，并且所有交换机运行修剪;如果交换机不传送Join消息到在中继间的另一交换机，可能关闭为特定VLAN或VLAN。当修剪的协商完成，VLAN在prune或加入的状态将完成该中继的。

VTP修剪一个非常重要功能允许您配置VLAN是修剪合格。此功能通知运行VTP修剪不修剪此VLAN的交换机。当您启用VTP修剪时，默认情况下VLAN 2至1000修剪合格VLAN。因此，当您启用修剪时，默认情况下它影响所有VLAN。VLAN1、默认Trcrf (1003)，默认TrBrf (1005)和Trcrf总是修剪不合格的;因此，从这些VLAN的流量不可能被修剪。

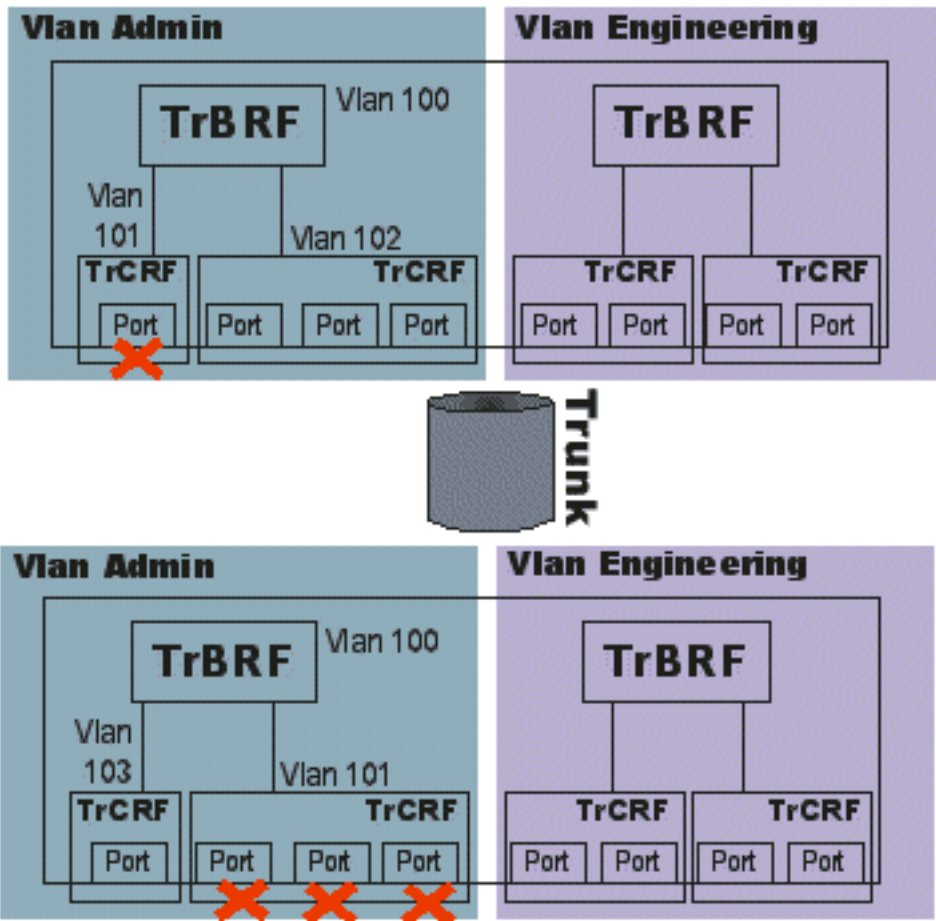
欲知更多信息，参考在[了解令牌环交换的VTP修剪](#)。

复制圆环协议

复制圆环协议在运行令牌环VLAN的交换机设计运行。其工作是保证令牌环的VLAN特有配置和创建搜索减少。DRiP使用VTP同步其VLAN数据库信息，但是没有要求为了DRiP能工作(VLAN数据库可以手工设立)。一种误解是DRiP了解环号;这不是真的。DRiP依靠在网络和该VLAN数据库配置里配置的VLAN的唯一性。

其中一个DRiP最重要的功能是强制执行Trcrf分配。除1003之外，在令牌环世界，分配所有VLAN，由于跨接问题是非常危险的。为此，如果分配除VLAN1003之外的一Trcrf，该VLAN关联的所有端口由DRiP禁用。

此示例说明此概念：



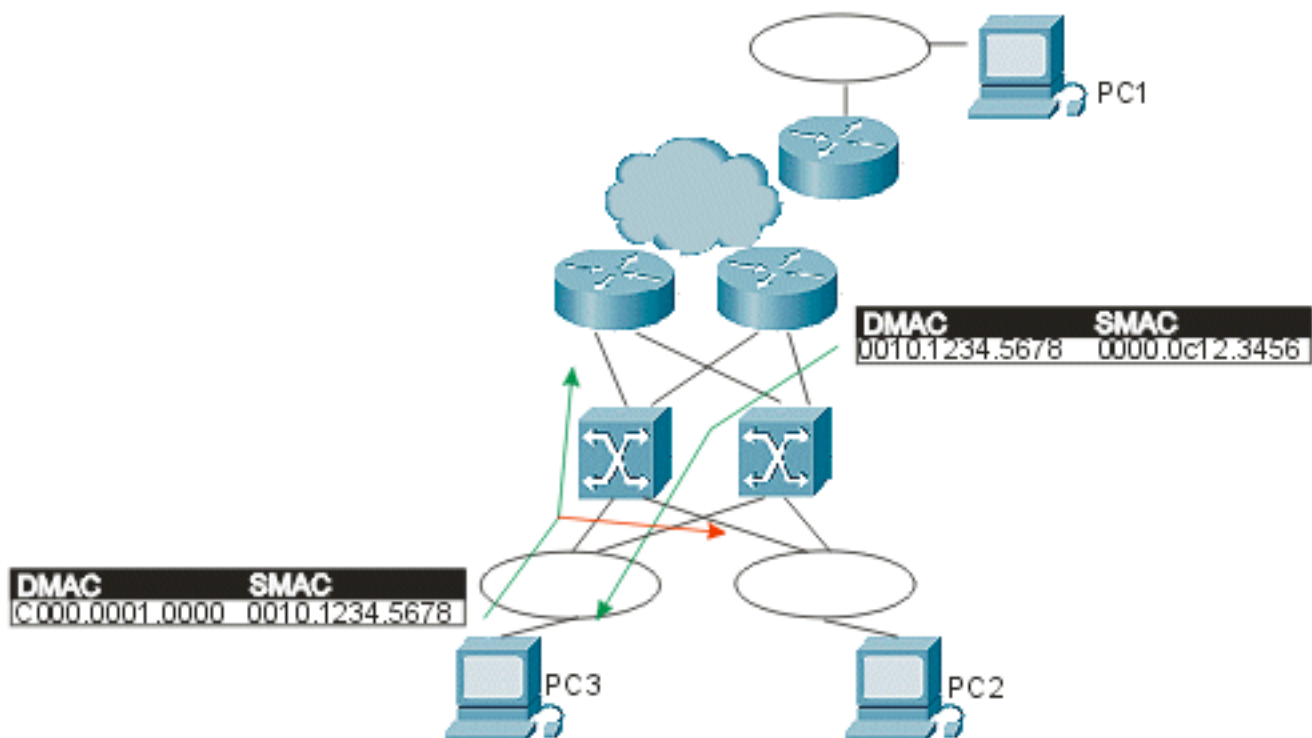
在分配到VLAN 101的该示例中，两不同交换机有端口。交换机，通过DRiP，移动端口生成树禁用并且停止转发流量。这预防交换机可能的环路情况。

如果没有更改，DRiP通告Trcrf状态对所有其中继端口每30秒。其中任一通过CLI (命令行界面)更改完成或SNMP将立即发送更新到所有端口。这些广告是类型0 ISL帧和流在默认VLAN 1。由于DRiP只通告其VLAN的作用，重要的是正确VLAN信息在通过ISL连接的交换机存在。这通过VTP执行。如果VTP禁用，则必须在共享同样VLAN的所有交换机间手工维护此功能。DRiP广告在ISL链路只存在。他们在ATM、令牌环、以太网或者FDDI不存在。没有在DRiP保留的结构树。

欲知更多信息，在[令牌环VLAN和相关协议](#)指南的参考的[复制圆环协议](#)。

HSRP和令牌环VLAN

其中一与HSRP的最大的问题是使用在网络的组播地址。由于没人网络的实际上源包数据包和此虚拟MAC地址一起，交换机从未了解这些MAC地址。所以，他们充斥在网络中的帧。因此，使用HSRP的standby use-bia功能要求发送使用有效HSRP路由器接口的固化MAC地址的数据包。与此方案的主要问题是，当HSRP路由器交换机，他们将必须发送广播地址解析协议(ARP;免费ARP)对电线的所有站点，因此站点了解网关的新的MAC地址。即使此进程应该工作基于IP规格，有与它的一些已知问题。由于从字段的继续请求，HSRP更改，以便您可以有组播地址并且能使用HSRP，不用standby use-bia。此变化实现在[CSCdk55937](#)上并且发布在Cisco IOS软件版本11.3(7)和12.0(3)及以后。



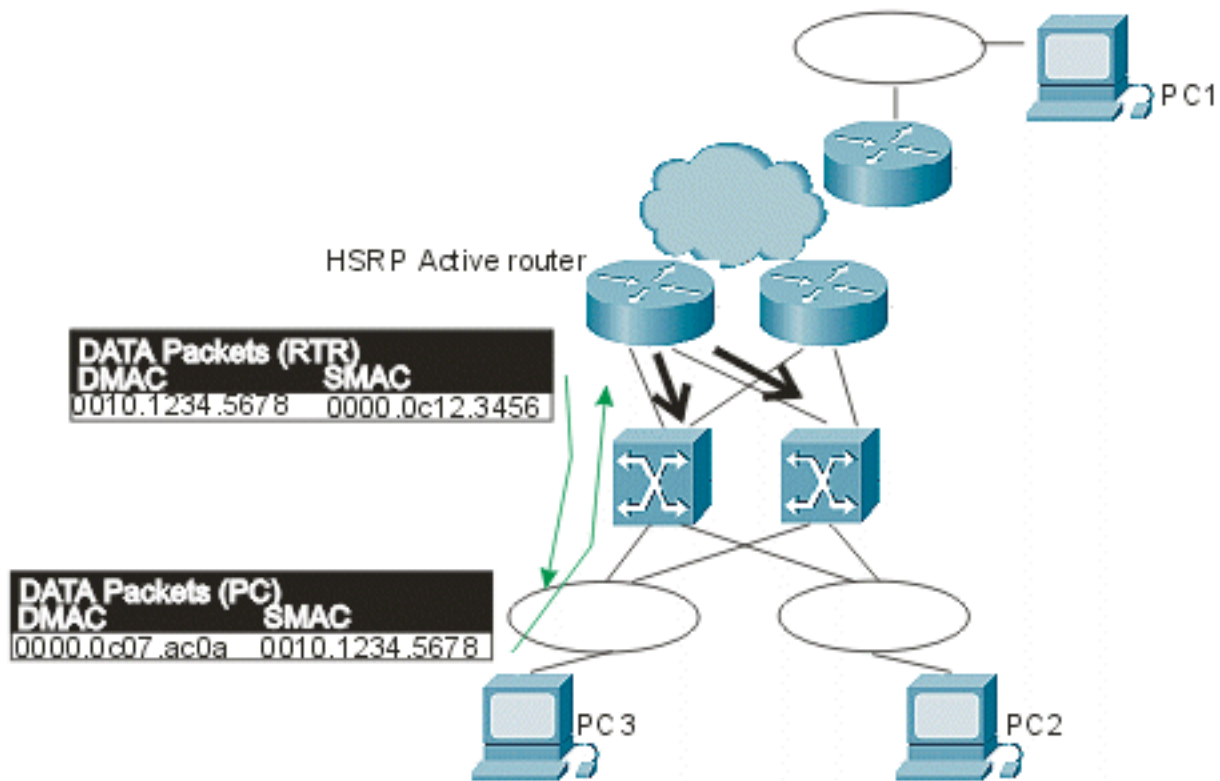
在上一个图表中，通信发生在PC1和PC3之间。问题是从客户端的IP数据流此图片的默认路由器的使用一个组播目的地地址。由于没人能从该地址源信息包此数据包，交换机从未了解此地址和总是充斥数据包。取决于组的传统DMAC是C000.000X.0000，不可以是在令牌环的—SMAC。那么从PC3注定的所有信息包到PC1通过默认网关由PC2当前看到。在网络中用很多网桥，这能非常迅速地倍增和导致什么将似乎类似广播风暴，但是什么实际上是很多组播数据流。

要克服此问题，您必须使用能实际上使用作为SMAC由路由器在HSRP hello的MAC地址。这允许交换机了解此地址，并且，因此，转换数据包适当地。要执行此，请配置在路由器的一个新的虚拟MAC地址。客户端需要发送数据包到此的DMAC新建的虚拟地址。这是从**show standby**命令的示例输出：

```
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，备用组10 (待机IP 1.1.1.100)创建。MAC地址(0000.0c07.ac0a)是新的虚拟MAC地址和最后字节是组(0xA = 10)。一旦有此新建的配置，您当前会有此流量模式，避免数据流洪泛：



现在，因为路由器是有HSRP虚拟MAC的DMAC的源信息包，交换机了解此MAC地址和只转发数据包到有效HSRP路由器。如果有效HSRP路由器出故障，并且待机去激活，新的活动路由器将开始发送与同样SMAC的HSRP hello，造成交换机MAC地址表换成他们的了解到的条目新的交换机端口和建立中继。

由于多环路，另外的操作需要生效保证RIF在转换时实际上更改(即使它是同一MAC地址)。多环路路由器的功能连结RIF与MAC地址，正如终端站。路由器在SRB网桥存在的环境需要多环路，因此数据包能横断他们到达终端站。

在示例中和一样前面，您能看到要求的额外步骤为了客户端能连接到新的有效HSRP路由器：

1. 活动路由器停止工作。
2. 一旦备用路由器检测HSRP hello损耗，开始进程变为有效HSRP路由器。
3. 路由器派出从SMAC的一免费ARP和一样前面，在MAC层和在ARP层。
4. PC当前发送被注定的帧对同一MAC地址，但是与新的RIF。
5. 一旦路由器接收此帧(被注定对HSRP MAC)，直接地发送ARP请求给客户端，因为在其ARP表里没有该客户端MAC地址。
6. 一旦答复到ARP数据包接收，路由器能发送数据包对目的地客户端。

相关信息

- [了解令牌环交换](#)
- [交换机产品支持](#)
- [LAN 交换技术支持](#)
- [技术支持和文档 - Cisco Systems](#)