配置Catalyst交换端口分析器(SPAN):示例

目录

- 简介
- 先决条件
  - 支持 SPAN、RSPAN 和 ERSPAN 的 Catalyst 交换机
  - 要求
  - 使用的组件
- 背景信息
  - SPAN 的简要说明
  - SPAN 术语
  - 源端口的特性
  - 源 VLAN 的特性
  - 目标端口的特性
  - 反射器端口的特性
- Catalyst Express 500/520 中的 SPAN
- Catalyst 2900XL/3500XL交换机上的SPAN
  - 可用功能及限制
  - 配置示例
    - 网络图
    - Catalyst 2900XL/3500XL 配置示例
    - 配置步骤说明
- Catalyst 2948G-L3 和 4908G-L3 中的 SPAN
- Catalyst 8500 中的 SPAN
- 运行 CatOS 的 Catalyst 2900、4500/4000、5500/5000 和 6500/6000 系列交换机中的 SPAN
  - 本地 SPAN
    - PSPAN、VSPAN：监控某些端口或整个 VLAN
    - 使用SPAN监控单个端口
    - 使用 SPAN 监控多个端口
    - 使用SPAN监控VLAN
    - 入口/出口SPAN
    - 在中继上实施 SPAN
    - 对属于中继的 VLAN 的子集进行监控
    - 目标端口上的中继
    - 创建多个同时运行的会话
    - 其他 SPAN 选项
  - 远程 SPAN
    - RSPAN 概述
    - RSPAN 配置示例
    - 在两个交换机 S1 和 S2 之间设置 ISL 中继
    - 创建 RSPAN VLAN
    - 将 S2 的端口 5/2 配置为 RSPAN 目标端口
    - 在 S1 上配置 RSPAN 源端口
    - 检查配置

使用 set rspan 命令可实现的其他配置

功能汇总和限制

Catalyst 2940、2950、2955、2960、2970、3550、3560、3560-E、3750 和 3750-E 系列交换机中的 SPAN

运行 Cisco IOS 系统软件的 Catalyst 4500/4000 和 Catalyst 6500/6000 系列交换机中的 SPAN

配置示例

功能汇总和限制

不同 Catalyst 平台上 SPAN 的性能影响

Catalyst 2900XL/3500XL 系列

体系结构概述

性能影响

Catalyst 4500/4000 系列

体系结构概述

性能影响

Catalyst 5500/5000 和 6500/6000 系列

体系结构概述

性能影响

常见问题与一般问题

SPAN 配置错误导致的连通性问题

SPAN 目标端口打开/关闭

SPAN会话为什么会创建桥接环路

SPAN是否会影响性能？

能否在 EtherChannel 端口上配置 SPAN？

是否可以同时运行多个 SPAN 会话？

错误“% Local Session Limit Has Been Exceeded”

无法删除 VPN 服务模块上的 SPAN 会话，原因是发生错误“% Session [Session No:] Used by Service Module”

为何无法使用 SPAN 捕获损坏的数据包？

Error:% Session 2 used by service module

反射器端口丢弃数据包

始终将 SPAN 会话与 Catalyst 6500 机箱中的 FWSM 一起使用

同一交换机内的 SPAN 和 RSPAN 会话能否具有相同的 ID？

RSPAN 会话能否跨不同的 VTP 域工作？

RSPAN 会话能否跨 WAN 或不同的网络工作？

RSPAN 源会话和目标会话能否存在于同一台 Catalyst 交换机中？

连接到 SPAN 目标端口的网络分析器/安全设备无法访问

相关信息

简介

本文档介绍已实施的交换端口分析器 (SPAN) 的最新功能。

先决条件

支持 SPAN、RSPAN 和 ERSPAN 的 Catalyst 交换机

Catalyst 交换机	SPAN 支持	RSPAN 支持	ERSPAN 支持
Catalyst Express 500/520 系列	Yes	无	无
Catalyst 6500/6000 系列	Yes	Yes	是运行Cisco IOS®软件版本12.2(18)SXE或更高版本的Supervisor 2T（带PFC4）、Supervisor 720（带PFC3B）或PFC3BXL。带有PFC3A的Supervisor 720，硬件版本为3.2或更高版本，运行Cisco IOS®软件版本12.2(18)SXE或更高版本。
Catalyst 5500/5000 系列	Yes	无	无
Catalyst 4900 系列	Yes	Yes	无
Catalyst 4500/4000 系列（包括 4912G）	Yes	Yes	无
Catalyst 3750 城域系列	Yes	Yes	无
Catalyst 3750/3750E/3750X系列	Yes	Yes	无
Catalyst 3560/3560E/3650X系列	Yes	Yes	无
Catalyst 3550 系列	Yes	Yes	无
Catalyst 3500 XL 系列	Yes	无	无
Catalyst 2970 系列	Yes	Yes	无
Catalyst 2960 系列	Yes	Yes	无
Catalyst 2955 系列	Yes	Yes	无
Catalyst 2950 系列	Yes	Yes	无
Catalyst 2940 系列	Yes	无	无
Catalyst 2948G-L3	无	无	无
Catalyst 2948G-L2、2948G-GE-TX、2980G-A	Yes	Yes	无
Catalyst 2900XL 系列	Yes	无	无
Catalyst 1900 系列	Yes	无	无

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息使用CatOS 5.5作为Catalyst 4500/4000、5500/5000和6500/6000系列交换机的参考。在 Catalyst 2900XL/3500XL 系列交换机中，使用的是 Cisco IOS® 软件版本 12.0(5)XU。尽管会根据 SPAN 的变化不断更新本文档，但有关 SPAN 功能的最新发展情况，请参阅交换机平台文档发行版本注释。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

SPAN功能（有时称为端口镜像或端口监控）选择网络流量以供网络分析器分析。网络分析器可以是思科交换机探测设备或其他远程监控(RMON)探测设备。

以前，SPAN 在 Cisco Catalyst 系列交换机中是一项较基本的功能。但是，Catalyst OS (CatOS) 最新版本引入了强大的增强功能并为用户提供了许多新的潜在功能。

本文档不用作 SPAN 功能的备用配置指南，本文档将解答有关 SPAN 的最常见的问题，例如：

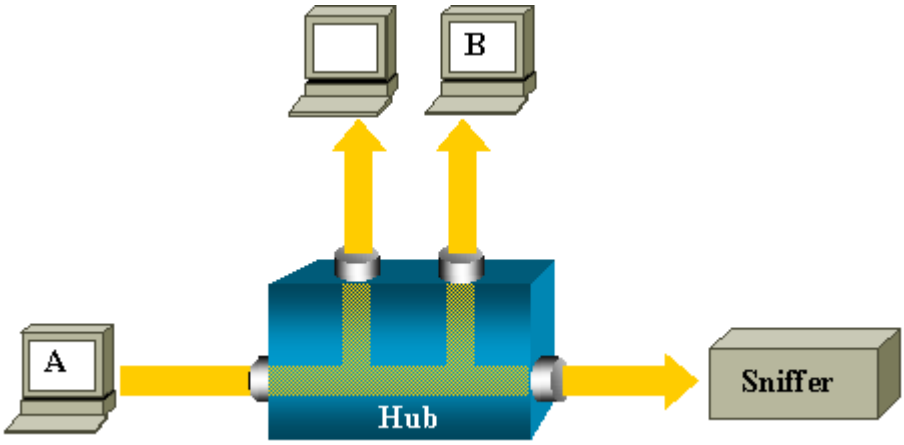
- SPAN 是什么？如何对其进行配置？
- 可用的不同功能有哪些（特别是多个并发SPAN会话）？运行这些功能需要什么软件级别？
- SPAN 是否会影响交换机的性能？

SPAN 的简要说明

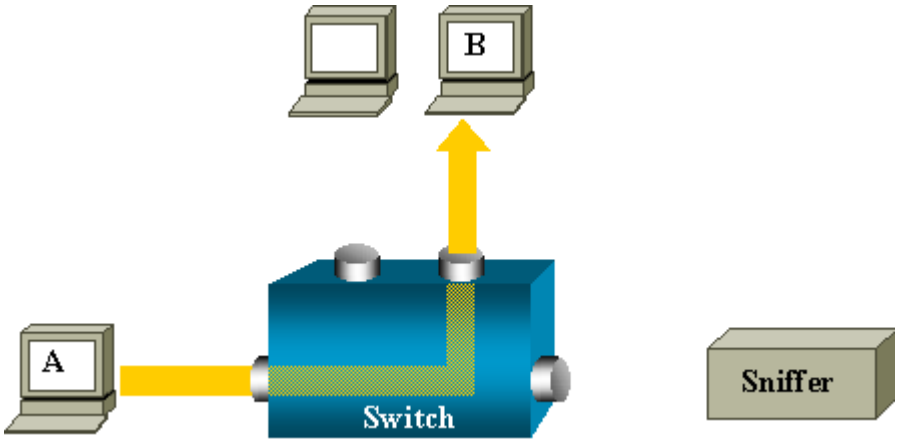
在交换机中引入 SPAN 功能是因为交换机与集线器有本质上的区别。当集线器在某个端口收到一个数据包时，它会在除接收该数据包的端口之外的所有端口上发送该数据包的一个副本。

某交换机启动后，便会开始以它接收的各种数据包的源 MAC 地址为基础构建第二层转发表。此转发表构建完毕后，该交换机便会将发往某个 MAC 地址的流量直接转发到相应的端口。

例如，要捕获由主机A发送到主机B，并且两者都连接到集线器的以太网流量，只需在此集线器上附加一个嗅探器即可。所有其他端口均可获知主机 A 与主机 B 之间的流量：



对于交换机，在获得主机 B 的 MAC 地址之后，会将从 A 到 B 的单播流量仅转发至 B 端口。因此，嗅探器无法获知此流量：



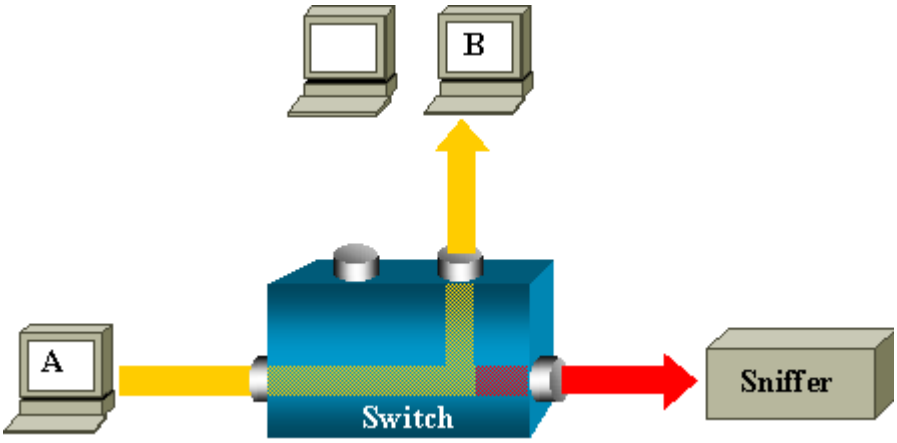
如果采用此配置，嗅探器仅捕获泛洪至所有端口的流量，例如：

- 广播数据流
- 禁用 CGMP 或 Internet 组管理协议 (IGMP) 侦测功能的多播流量
- 未知单播流量

如果交换机的内容可寻址存储器 (CAM) 表中没有目标 MAC，则会发生单播泛洪。

交换机不知在何处发送流量。交换机会将数据包泛洪至目标 VLAN 中的所有端口。

需要使用附加功能将主机 A 发送的单播数据包人工复制到嗅探器端口：

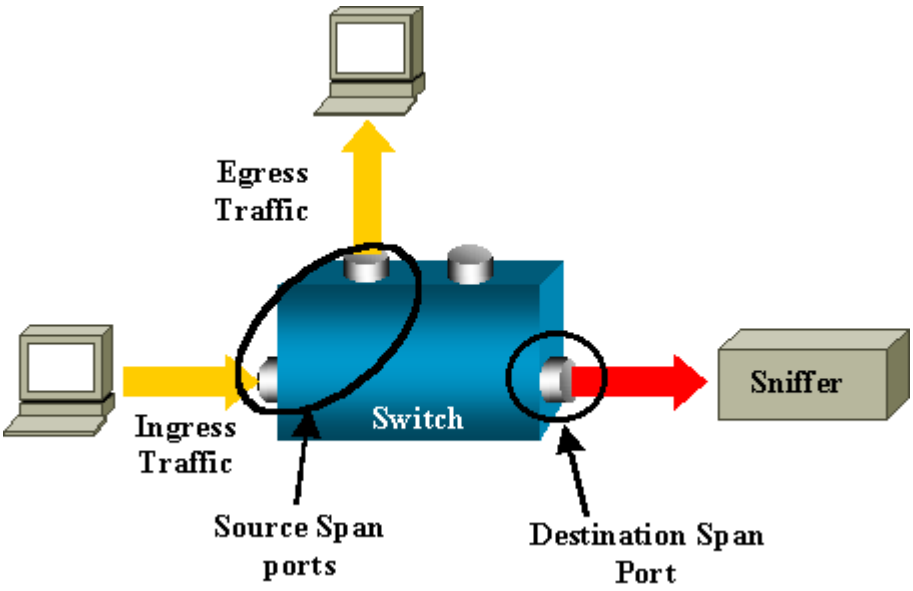


在此图中，嗅探器连接到一个端口，该端口配置为接收主机 A 发送的所有数据包的副本。此端口称为 SPAN 端口。

本文档的其他部分介绍如何精确调整此功能，以便执行更多操作，而不仅仅是监控端口。

SPAN 术语

- 输入流量 — 进入交换机的流量。
- 输出流量 — 从交换机发出的流量。
- 源 (SPAN) 端口 — 使用 SPAN 功能监控的端口。
- 源 (SPAN) VLAN — 使用 SPAN 功能监控其流量的 VLAN。
- 目标 (SPAN) 端口 — 监控源端口的端口，网络分析器通常会连接到此端口。
- 反射器端口 — 将数据包复制到 RSPAN VLAN 的端口。
- 监控端口 — 在 Catalyst 2900XL/3500XL/2950 术语中，监控端口也称为目标 SPAN 端口。



- 本地 SPAN — 当所有受监控的端口与目标端口位于同一交换机中时，SPAN 功能为本地 SPAN 功能。此功能与远程 SPAN (RSPAN) 不同，本列表也包含后者的定义。
- 远程 SPAN (RSPAN) — 与目标端口分属于不同交换机的一些源端口。

RSPAN 是一项高级功能，需要使用特殊的 VLAN 在交换机之间传送由 SPAN 监控的流量。

所有交换机均不支持 RSPAN。请查阅相应的发行版本注释或配置指南，以了解能否在您部署的交换机上使用 RSPAN。

- 基于端口的 SPAN (PSPAN) — 用户指定交换机上的一个或多个源端口以及一个目标端口。
- 基于 VLAN 的 SPAN (VSPAN) — 在特定交换机上，用户可以通过一个命令选择监控属于某个特定 VLAN 的所有端口。
- ESPAN — 指 SPAN 增强版本。在SPAN的演变过程中，此术语曾多次用于命名附加功能，因此，此术语不是很明确，本文档中将其避免。
- 管理源 — 已配置为受监控的源端口或 VLAN 的列表。
- 操作源 — 受到有效监控的端口的列表。此端口列表可能不同于管理源。

例如，某个处于关闭模式的端口可能会出现在管理源中，但不会受到有效监控。

源端口的特性

源端口（也称为受监控的端口）是为进行网络流量分析而监控的交换端口或路由端口。在单个本地 SPAN 会话或 RSPAN 源会话中，可以监控源端口流量，如接收流量 (Rx)、发送流量 (Tx) 或双向流量（接收流量和发送流量）。 交换机支持任意数量的源端口（多达交换机上的最大可用端口数）和任意数量的源 VLAN。

源端口具有以下特性：

- 它可以是任何端口类型，例如EtherChannel、快速以太网、千兆以太网等。
- 可以通过多个 SPAN 会话对其进行监控。
- 它不能是目标端口。
- 可以为每个源端口配置监控方向（输入、输出或双向）。对于 EtherChannel 源，监控方向适用于组中的所有物理端口。
- 源端口可以位于相同的 VLAN 中，也可以位于不同的 VLAN 中。
- 对于 VLAN SPAN 源，源 VLAN 中的所有活动端口都是作为源端口添加的。

VLAN 过滤

当将某中继端口作为源端口进行监控时，默认情况下将监控中继上的所有活动 VLAN。您可以使用VLAN过滤将中继源端口上的SPAN流量监控限制到特定VLAN。

- VLAN 过滤功能仅适用于中继端口或语音 VLAN 端口。
- VLAN 过滤功能仅适用于基于端口的会话，在具有 VLAN 源的会话中不得使用该功能。
- 指定 VLAN 过滤器列表后，只有该列表中的 VLAN 才会在中继端口或语音 VLAN 接入端口受到监控。
- 来自其他端口类型的 SPAN 流量不受 VLAN 过滤影响，这意味着在其他端口上允许所有 VLAN。
- VLAN 过滤仅影响转发至目标 SPAN 端口的流量，并不影响正常流量的交换。
- 不能将一个会话内的源 VLAN 和过滤 VLAN 混合在一起。您可以拥有源 VLAN 或过滤 VLAN，但不能同时拥有二者。

源 VLAN 的特性

VSPAN 用于监控一个或多个 VLAN 中的网络流量。VSPAN 中的 SPAN 或 RSPAN 源接口是 VLAN ID，系统将在所有端口上监控该 VLAN 的流量。

VSPAN 具有以下特性：

- 源 VLAN 中的所有活动端口都是作为源端口添加的，并且可以在出入任一方向或双向进行监控。
- 在某个给定端口上，只有受控 VLAN 中的流量会发送至目标端口。
- 如果某个目标端口属于源 VLAN，则会将其从源列表中排除而不会对其进行监控。
- 如果向源 VLAN 中添加端口或从中移除端口，则会将这些端口在源 VLAN 上接收的流量添加到受监控的源或从受监控的源中移除。
- 不能在具有 VLAN 源的同一会话中使用过滤器 VLAN。
- 只能监控以太网 VLAN。

目标端口的特性

每个本地 SPAN 会话或 RSPAN 目标会话必须有一个目标端口（也称为监控端口），用于从源端口和 VLAN 接收流量副本。

目标端口具有以下特性：

- 目标端口必须位于源端口所在的交换机上（以进行本地 SPAN 会话）。
- 目标端口可以是任何以太网物理端口。
- 一个目标端口一次只能参与一个 SPAN 会话。某一 SPAN 会话中的目标端口不能是另一 SPAN 会话的目标端口。
- 目标端口不能是源端口。
- 目标端口不能是 EtherChannel 组。

  注意：在 Cisco IOS 软件版本 12.2(33)SXH 及更高版本中，PortChannel 接口可以是目标端

口。目标 EtherChannel 不支持端口聚合控制协议 (PAgP) 或链路聚合控制协议 (LACP) 及 EtherChannel 协议；仅支持禁用了所有 EtherChannel 协议支持的 on 模式。

注意：有关详细信息，请参阅本地 SPAN、RSPAN 和 ERSPAN 目标。

- 目标端口可以是分配给某个 EtherChannel 组的物理端口，即使已将该 EtherChannel 组指定为 SPAN 源也是如此。将目标端口配置为 SPAN 目标端口时，会将此目标端口从该组中移除。
- 除非启用识别，否则端口将仅传输 SPAN 会话所需的流量。如果启用了识别，端口还会传输定向到已在目标端口识别的主机的流量。

注意：有关详细信息，请参阅本地 SPAN、RSPAN 和 ERSPAN 目标。

- 可以故意地将目标端口的状态设为打开/关闭。接口显示处于此状态的端口，以表明该端口当前无法用作生产端口。
- 如果为网络安全设备启用了输入流量转发，目标端口将在第二层转发流量。
- 当 SPAN 会话处于活动状态时，目标端口不会参与生成树。
- 如果某端口为目标端口，则该端口不会参与任何第二层协议（STP、VTP、CDP、DTP、PagP）。
- 属于任何 SPAN 会话的源 VLAN 的目标端口将从源列表中排除而不会受到监控。
- 目标端口将接收所有受控源端口发送和接收的流量的副本。如果目标端口使用过度，则可能发生拥塞。这种拥塞会影响一个或多个源端口上转发的流量。

反射器端口的特性

反射器端口是将数据包复制到 RSPAN VLAN 的机制。反射器端口仅转发来自与之关联的 RSPAN 源会话的流量。在禁用 RSPAN 源会话之前，连接到反射器端口的所有设备都将失去连接。

反射器端口具有以下特性：

- 它是设置为进行环回的端口。
- 它不能是 EtherChannel 组，不进行中继，而且不能执行协议过滤。
- 它可以是分配给 EtherChannel 组的物理端口，即使已将该 EtherChannel 组指定为 SPAN 源也是如此。将端口配置为反射器端口时，会将其从组中移除。
- 用作反射器端口的端口不能是 SPAN 源或目标端口，一个端口也不能同时用作多个会话的反射器端口。
- 它对于所有 VLAN 均不可见。
- 反射器端口上环回流量的本地 VLAN 为 RSPAN VLAN。
- 反射器端口将未标记的流量环回到交换机。随后会将这些流量置于 RSPAN VLAN 上，并泛洪至承载 RSPAN VLAN 的所有中继端口。
- 将会在反射器端口上自动禁用生成树。
- 反射器端口将接收所有受监控源端口发送和接收的流量的副本。

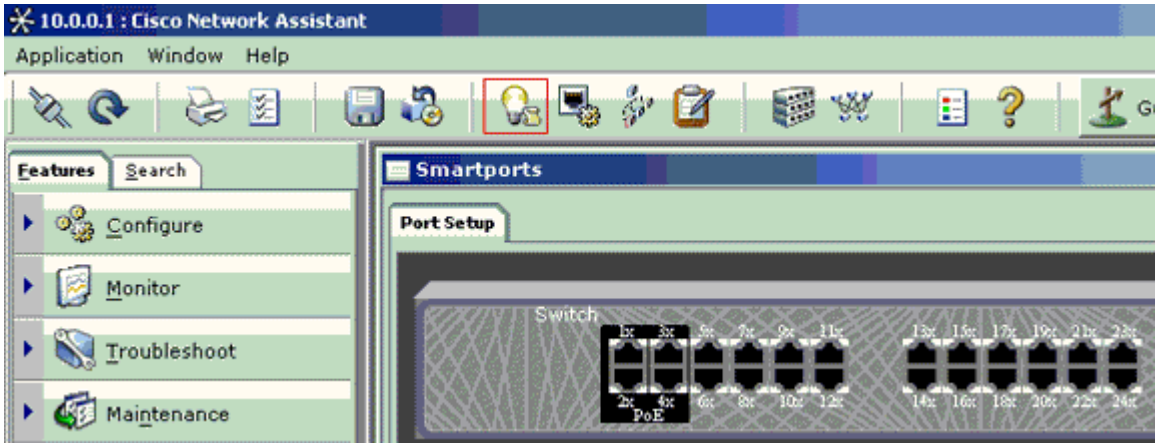
Catalyst Express 500/520 中的 SPAN

Catalyst Express 500 或 Catalyst Express 520 仅支持 SPAN 功能。只能使用 Cisco Network Assistant (CNA) 对 Catalyst Express 500/520 端口进行针对 SPAN 的配置。 完成下列步骤以配置 SPAN：

1. 在 PC 上下载并安装 CNA。

   从软件下载下载CNA（仅限注册客户）。

2. 完成Catalyst Express 500交换机12.2(25)FY入门指南中给出的步骤，以自定义Catalyst Express 500和520的交换机设置。
3. 使用CNA登录交换机并单击Smartport。

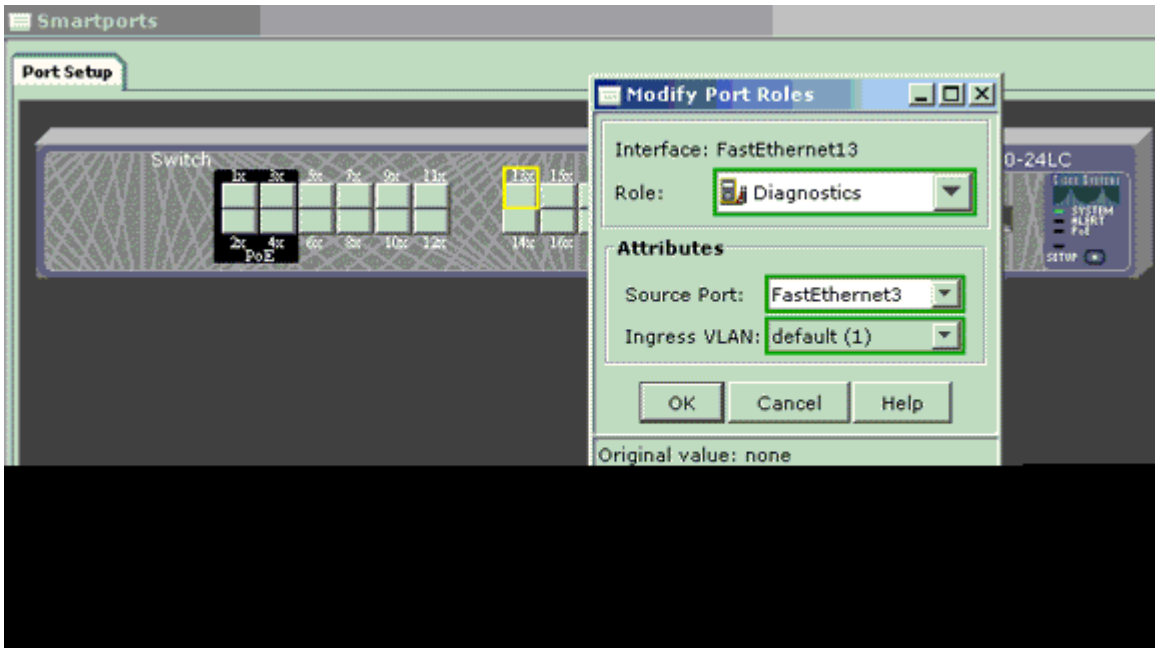


4. 单击您计划连接PC以捕获嗅探器踪迹的任何接口。
5. 单击 Modify。

   此时会显示一个小的弹出框。

6. 为端口选择 Diagnostics 角色。
7. 选择源端口并选择计划监控的 VLAN。

   如果不选择任何内容，端口将仅接收流量。入口 VLAN 允许将 PC 连接到诊断端口，以便向使用该 VLAN 的网络发送数据包。



8. 单击OK关闭弹出框。
9. 单击 OK，然后单击“Apply”应用设置。
10. 设置诊断端口后，可以使用任何Sniffer软件跟踪流量。

Catalyst 2900XL/3500XL交换机上的SPAN

可用功能及限制

Catalyst 2900XL/3500XL 中的端口监控功能并不复杂。因此，此功能相对容易掌握。

您可以根据需要创建任意数量的本地 PSPAN 会话。例如，可以在已选择作为目标 SPAN 端口的配置端口上创建 PSPAN 会话。在这种情况下，请发出port monitor interface命令列出要监控的源端口。在 Catalyst 2900XL/3500XL 术语中，监控端口称为目标 SPAN 端口。

- 主要限制在于，与特定会话相关的所有端口（无论是源端口还是目标端口）必须属于同一 VLAN。
- 如果为 VLAN 接口配置一个 IP 地址，则 port monitor 命令将仅监控发往该 IP 地址的流量。另外，该命令还监控 VLAN 接口接收的广播数据流。但是，该命令不捕获流入实际 VLAN 本身的流量。如果在 port monitor 命令中未指定任何接口，则会监控属于该接口所属的 VLAN 的所有其他端口。

此列表提供了一些限制。有关详细信息，请参阅命令参考指南(Catalyst 2900XL/3500XL)。



注意：只有 ATM 端口无法用作监控端口。然而，可以对 ATM 端口进行监控。此列表中的限制适用于具有端口监控功能的端口。

- 监控端口不能位于 Fast EtherChannel 或千兆 EtherChannel 端口组中。
- 无法启用监控端口的端口安全功能。
- 监控端口不能是多个 VLAN 的端口。
- 监控端口必须是受监控端口所在 VLAN 的成员。对于监控端口和受监控端口，不允许更改 VLAN 成员资格。
- 监控端口不能是动态接入端口或中继端口。但是，静态接入端口可以监控中继端口、多个 VLAN 的端口或动态接入端口中的 VLAN。受监控的 VLAN 是与静态接入端口关联的 VLAN。
- 如果监控端口和受监控端口均为受保护端口，端口监控将不起作用。

请注意，当处于监控状态的端口仍属于它镜像的端口的 VLAN 时，该端口不运行生成树协议 (STP)。例如，如果将端口监控器连接到集线器或网桥并循环到网络的另一个部分，该端口监控器会成为环路的一部分。在这种情况下，可能会陷入灾难性的桥接环路状况，因为 STP 不再为您提供保护。有关如何发生此情况的示例，请参阅本文档的SPAN会话为什么创建桥接环路部分。

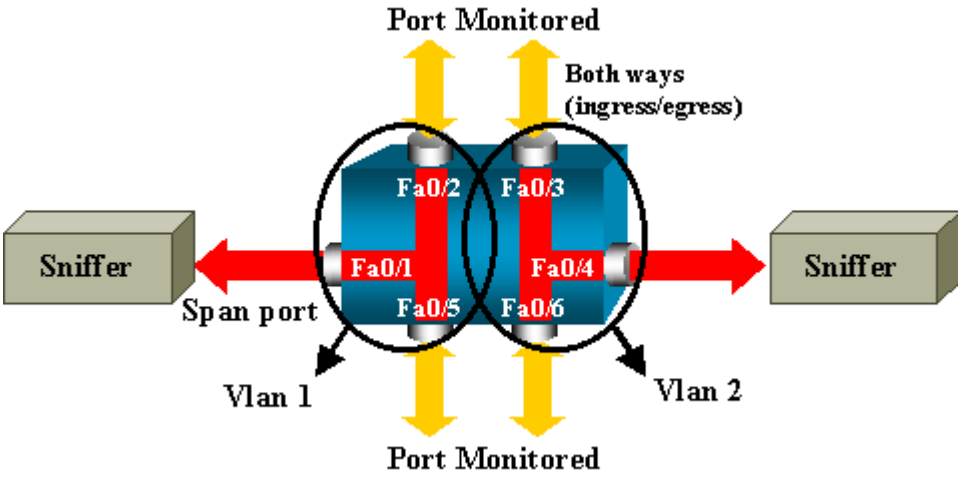
配置示例

本示例创建两个并发 SPAN 会话。

- 快速以太网 0/1 (Fa0/1) 端口监控 Fa0/2 和 Fa0/5 端口发送和接收的流量。端口 Fa0/1 还监控流入管理接口 VLAN 1 及从中流出的流量。
- 端口Fa0/4将对端口Fa0/3以及Fa0/6进行监控。

端口Fa0/3、Fa0/4和Fa0/6均配置在VLAN 2中。其他端口和管理接口配置在默认VLAN 1中。

网络图



Catalyst 2900XL/3500XL 配置示例

2900XL/3500XL SPAN 配置示例

```
!--- Output suppressed.
!
interface FastEthernet0/1
port monitor FastEthernet0/2
 port monitor FastEthernet0/5
 port monitor VLAN1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
!
interface FastEthernet0/4
 port monitor FastEthernet0/3
 port monitor FastEthernet0/6
 switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
 switchport access vlan 2
!
!--- Output suppressed.
!
interface VLAN1
 ip address 10.200.8.136 255.255.252.0
 no ip directed-broadcast
 no ip route-cache
!
!--- Output suppressed.
```

配置步骤说明

要将端口Fa0/1配置为目标端口、源端口Fa0/2和Fa0/5以及管理接口(VLAN 1)，请在配置模式下选择接口Fa0/1:

```
Switch(config)#interface fastethernet 0/1
```

输入要监控的端口的列表：

```
Switch(config-if)#port monitor fastethernet 0/2
Switch(config-if)#port monitor fastethernet 0/5
```

使用此命令，这两个端口接收或发送的每个数据包也会复制到端口Fa0/1。发出port monitor命令的变体以配置管理接口的监控：

```
Switch(config-if)#port monitor vlan 1
```



注意：此命令并不意味着端口Fa0/1监控整个VLAN 1。vlan 1关键字只是指交换机的管理接口。此命令示例说明无法监控另一个 VLAN 中的端口：

```
Switch(config-if)#port monitor fastethernet 0/3
FastEthernet0/1 and FastEthernet0/3 are in different vlan
```

要完成配置，请配置另一个会话。这次，请使用 Fa0/4 作为目标 SPAN 端口：

```
Switch(config-if)#interface fastethernet 0/4
Switch(config-if)#port monitor fastethernet 0/3
Switch(config-if)#port monitor fastethernet 0/6
Switch(config-if)#^Z
```

发出show running命令，或使用show port monitor命令检查配置：

```
Switch#show port monitor
 Monitor Port Port Being Monitored
------------------- ---------------------
```

```
FastEthernet0/1 VLAN1
FastEthernet0/1 FastEthernet0/2
FastEthernet0/1 FastEthernet0/5
FastEthernet0/4 FastEthernet0/3
FastEthernet0/4 FastEthernet0/6
```



注意：Catalyst 2900XL 和 3500XL 不支持仅监控 Rx 方向的 SPAN（Rx SPAN 或入口 SPAN）或仅监控 Tx 方向的 SPAN（Tx SPAN 或出口 SPAN）。 所有 SPAN 端口均设计为捕获 Rx 和 Tx 两个方向的流量。

Catalyst 2948G-L3 和 4908G-L3 中的 SPAN

Catalyst 2948G-L3 和 Catalyst 4908G-L3 是固定配置的交换机路由器或第三层交换机。第三层交换机的 SPAN 功能称为端口侦测。

不过，这些交换机不支持端口侦测。

Catalyst 8500 中的 SPAN

Catalyst 8540 提供一个非常基本的 SPAN 功能，称为端口侦测。有关详细信息，请参阅当前的 Catalyst 8540文档。

端口侦听使您能将业务从一个或者多个源端口透明地镜像至一个目的地端口。

发出snoop命令以设置基于端口的流量镜像或监听。发出此命令的no形式以禁用监听：

```
snoop interface source_port direction snoop_direction

no snoop interface source_port
```

变量 source_port 指受监控的端口。变量 snoop_direction 表示源端口或受监控端口的流量方向：receive、transmit 或 both。

```
8500CSR#configure terminal
8500CSR(config)#interface fastethernet 12/0/15
8500CSR(config-if)#shutdown
8500CSR(config-if)#snoop interface fastethernet 0/0/1 direction both
```

```
8500CSR(config-if)#no shutdown
```

下面的示例显示了 show snoop 命令的输出：

```
8500CSR#show snoop
Snoop Test Port Name: FastEthernet1/0/4 (interface status=SNOOPING)
Snoop option:         (configured=enabled)(actual=enabled)
Snoop direction:      (configured=receive)(actual=receive)
Monitored Port Name:
(configured=FastEthernet1/0/3)(actual=FastEthernet1/0/3)
```



注意：如果运行多服务 ATM 交换机路由器 (MSR) 映像（如 8540m-in-mz），Catalyst 8540 中的以太网端口将不支持此命令。必须改为使用园区交换机路由器 (CSR) 镜像（如 8540c-in-mz）。

运行 CatOS 的 Catalyst 2900、4500/4000、5500/5000 和 6500/6000 系列交换机中的 SPAN

本部分仅适用于下列 Cisco Catalyst 2900 系列交换机：

- Cisco Catalyst 2948G-L2 交换机
- Cisco Catalyst 2948G-GE-TX 交换机
- Cisco Catalyst 2980G-A 交换机

本部分适用于 Cisco Catalyst 4000 系列交换机，其中包括：

- 模块化机箱交换机：
  - Cisco Catalyst 4003 交换机
  - Cisco Catalyst 4006 交换机
- 固定机箱交换机：
  - Cisco Catalyst 4912G 交换机

本地 SPAN

SPAN 功能已逐一添加到 CatOS 中，SPAN 配置由一个 set span 命令组成。目前已有大量可用于该命令的选项：

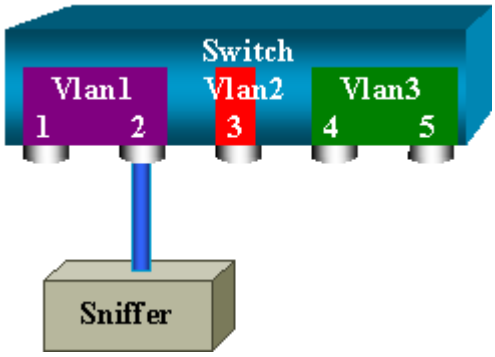
<#root>

```
switch (enable)

set span


Usage: set span disable [dest_mod/dest_port|all]
       set span <src_mod/src_ports...|src_vlans...|sc0>
                <dest_mod/dest_port> [rx|tx|both]
                [inpkts <enable|disable>]
                [learning <enable|disable>]
                [multicast <enable|disable>]
                [filter <vlans...>]
                [create]
```

下面的网络图介绍了使用命令变化形式带来的不同 SPAN 可能性：



此图显示位于 Catalyst 6500/6000 交换机插槽 6 中的某一线路卡的一部分。在这种情况下：

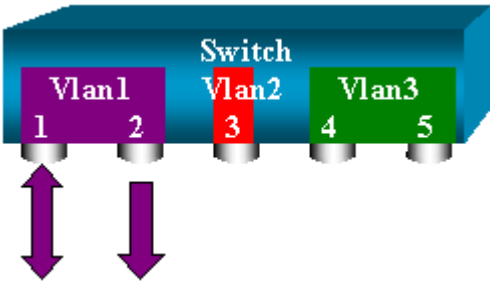
- 端口 6/1 和 6/2 属于 VLAN 1
- 端口 6/3 属于 VLAN 2
- 端口 6/4 和 6/5 属于 VLAN 3

将一个嗅探器连接到端口 6/2，并在几种不同情况下使用该端口作为监控端口。

PSPAN、VSPAN：监控某些端口或整个 VLAN

发出set span命令的最简单形式来监控单个端口。语法为 set span source_port destination_port。

使用SPAN监控单个端口



<#root>

```
switch (enable)

set span 6/1 6/2



Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:04:14 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

使用此配置时，端口6/1接收或发送的每个数据包都会在端口6/2上复制。当您输入配置时，就会显示有关此配置的清晰说明。发出show span命令以接收当前SPAN配置的摘要：

<#root>

```
switch (enable)

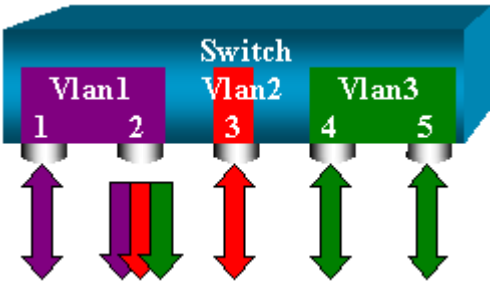
show span



Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active

Total local span sessions: 1
```

使用 SPAN 监控多个端口



使用 set span source_ports destination_port 命令，用户可指定多个源端口。您只需列出要对其实施 SPAN 的所有端口，并用逗号分隔这些端口。命令行解释程序还允许您使用连字符指定端口范围。

本示例说明了这种用以指定多个端口的功能。下面的示例对端口 6/1 以及从 6/3 到 6/5 的三个端口使用 SPAN：

注意：只能有一个目标端口。务必先指定 SPAN 源，然后再指定目标端口。

<#root>

```
switch (enable)

set span 6/1,6/3-5 6/2

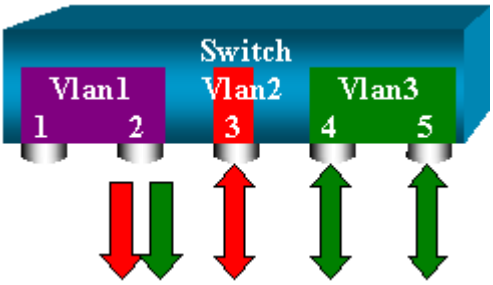


2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
       for destination port 6/2
       Destination : Port 6/2
       Admin Source : Port 6/1,6/3-5
       Oper Source : Port 6/1,6/3-5
       Direction : transmit/receive
       Incoming Packets: disabled
       Learning : enabled
       Multicast : enabled
       Filter : -
       Status : active
       switch (enable) 2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span
       session active for destination port 6/2
```

注意：与Catalyst 2900XL/3500XL交换机不同，Catalyst 4500/4000、5500/5000和6500/6000可以监控属于多个不同VLAN的端口，这些端口的CatOS版本低于5.1。在这里，镜像端口分配给VLAN 1、2和3。

使用SPAN监控VLAN

最后，使用 set span 命令配置端口以监控整个 VLAN 的本地流量。命令是set span source_vlan(s)destination_port。



使用一个或多个 VLAN 的列表作为源，而不是使用端口列表：

<#root>

```
switch (enable)

set span 2,3 6/2
```

```
2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 2-3
Oper Source : Port 6/3-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

采用此配置时，会将进入 VLAN 2（或 VLAN 3）或从中发出的每个数据包复制到端口 6/2。

注意：结果与对属于命令所指定的 VLAN 的所有端口分别实施 SPAN 的结果完全相同。将 Oper Source 字段与 “Admin Source”字段进行比较。基本上说，Admin Source 字段会列出已为 SPAN 会话配置的所有端口，“Oper Source”字段会列出使用 SPAN 的端口。

入口/出口SPAN

在使用 SPAN 监控 VLAN 部分的示例中，进入指定端口及从指定端口发出的流量受到监控。

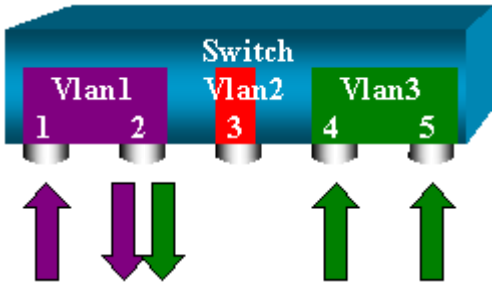
Direction:transmit/receive 字段表明了这一情况。Catalyst 4500/4000、5500/5000 和 6500/6000 系列交换机允许针对某个特定端口仅收集输出（出站）流量或仅收集输入（入站）流量。

在命令末尾添加 rx（接收）或 tx（发送）关键字。默认值为 both（tx 和 rx）。

<#root>

set span source_port destination_port [rx | tx | both]

在本示例中，会话捕获进入 VLAN 1 和 VLAN 3 的所有流量，并将这些流量镜像到端口 6/2：



<#root>

switch (enable)

set span 1,3 6/2 rx

```
2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span session
inactive for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 1,3
Oper Source : Port 1/1,6/1,6/4-5,15/1
Direction : receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

在中继上实施 SPAN

中继是交换机中的特例，因为它们是承载多个 VLAN 的端口。如果选择某中继作为源端口，则会监控该中继上所有 VLAN 的流量。

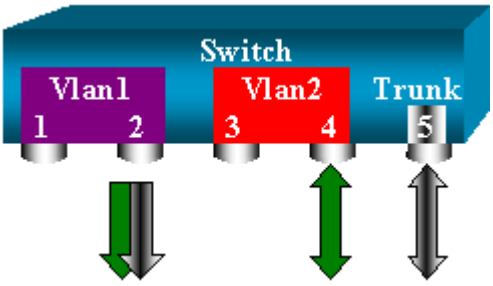
对属于中继的 VLAN 的子集进行监控

在下面的图中，端口 6/5 现在是承载所有 VLAN 的中继。假设您要对端口6/4和6/5的VLAN 2中的流量使用SPAN。只需发出以下命令：

<#root>

```
switch (enable)

set span 6/4-5 6/2
```



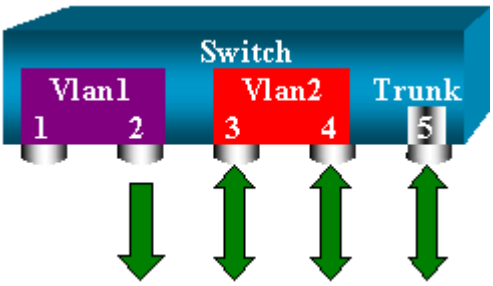
在这种情况下，在 SPAN 端口上接收的流量将是所需流量与中继 6/5 承载的所有 VLAN 的混合流量。

例如，无法在目标端口上区分数据包是来自VLAN 2中的端口6/4还是VLAN 1中的端口6/5。另一种可能是在整个VLAN 2上使用SPAN:

<#root>

```
switch (enable)

set span 2 6/2
```



采用此配置时，至少可以仅监控来自中继的属于 VLAN 2 的流量。问题是，这时也会收到来自端口 6/3 的不需要的流量。

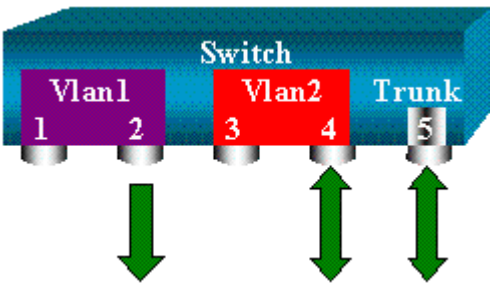
CatOS 包括另一个关键字，可用于从中继中选择某些 VLAN 进行监控：

<#root>

```
switch (enable)

set span 6/4-5 6/2 filter 2


      2000 Sep 06 02:31:51 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
       for destination port 6/2
      Destination : Port 6/2
      Admin Source : Port 6/4-5
      Oper Source : Port 6/4-5
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : 2
      Status : active
```



此命令可以实现目标，因为选择的是所有受监控中继上的 VLAN 2。使用此过滤器选项可指定若干 VLAN。

注意：只有 Catalyst 4500/4000 和 Catalyst 6500/6000 交换机支持此过滤器选项。Catalyst 5500/5000 不支持随 set span 命令提供的过滤器选项。

目标端口上的中继

如果您有属于多个不同VLAN的源端口，或者如果您在中继端口上的多个VLAN上使用SPAN，则您需要确定在目标SPAN端口上收到的数据包属于哪个VLAN。如果在为 SPAN 配置端口之前启用目标端口上的中继，则可以进行上述标识。这样，转发到嗅探器的所有数据包也将带有其各自 VLAN ID 的标记。

注意：您的嗅探器需要识别相应的封装。

<#root>

```
switch (enable)

set span disable 6/2


      This command can disable your span session.
      Do you want to continue (y/n) [n]?y
      Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/4-5
      2000 Sep 06 02:52:22 %SYS-5-SPAN_CFGSTATECHG:local span session
      inactive for destination port 6/2
      switch (enable)

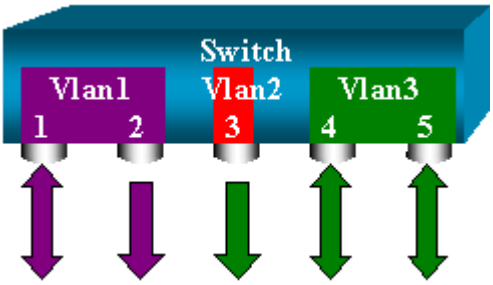
set trunk 6/2 nonegotiate isl



      Port(s) 6/2 trunk mode set to nonegotiate.
      Port(s) 6/2 trunk type set to isl.
      switch (enable) 2000 Sep 06 02:52:33 %DTP-5-TRUNKPORTON:Port 6/2 has become
        isl trunk
      switch (enable) set span 6/4-5 6/2
      Destination : Port 6/2
      Admin Source : Port 6/4-5
      Oper Source : Port 6/4-5
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : -
      Status : active
      2000 Sep 06 02:53:23 %SYS-5-SPAN_CFGSTATECHG:local span session active for
      destination port 6/2
```

创建多个同时运行的会话

到目前为止，只创建了一个 SPAN 会话。每次发出新的 set span 命令时，原有配置都将失效。CatOS 目前具备同时运行多个会话的功能，因此可同时具有不同的目标端口。发出set span source destination create命令以添加其他SPAN会话。在此会话中，端口 6/1 到 6/2 受到监控，同时，VLAN 3 到端口 6/3 也受到监控：



<#root>

```
switch (enable)
```

set span 6/1 6/2

```
2000 Sep 05 08:49:04 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:49:05 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
switch (enable) set span 3 6/3 create
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:55:38 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/3
```

现在，发出show span命令以确定是否同时有两个会话：

<#root>

```
switch (enable)
```

show span

```
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
```

```
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
------------------------------------------------------------------------
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
Total local span sessions: 2
```

创建了其他会话。您需要采取相应方法删除一些会话。命令如下：

<#root>

set span disable {all | destination_port}

由于每个会话只能有一个目标端口，因此目标端口可标识会话。删除所创建的第一个会话，即使用端口 6/2 作为目标端口的会话：

<#root>

```
switch (enable)
```

set span disable 6/2

```
This command can disable your span session.
Do you want to continue (y/n) [n]?y
Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/1
2000 Sep 05 09:04:33 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
```

现在可以检查是否仅剩余一个会话：

<#root>

```
switch (enable)
```

show span

```
      Destination : Port 6/3
      Admin Source : VLAN 3
      Oper Source : Port 6/4-5,15/1
      Direction : transmit/receive
      Incoming Packets: disabled
      Learning : enabled
      Multicast : enabled
      Filter : -
      Status : active

    Total local span sessions: 1
```

发出此命令可在一个步骤中禁用所有当前会话：

<#root>

```
switch (enable)

set span disable all


  This command can disable all span session(s).
      Do you want to continue (y/n) [n]?y
      Disabled all local span sessions
      2000 Sep 05 09:07:07 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
      for destination port 6/3

    switch (enable)

show span


      No span session configured
```

其他 SPAN 选项

set span 命令的语法如下：

<#root>

```
switch (enable)

set span


Usage: set span disable [dest_mod/dest_port|all]
      set span <src_mod/src_ports...|src_vlans...|sc0>
               <dest_mod/dest_port> [rx|tx|both]
```

[inpkts

]

[learning

]

[multicast

]

[filter <vlans...>]
[create]

此部分简要介绍了本文档讨论的选项：

- sc0 — 当需要监控流向管理接口sc0的流量时，可在SPAN配置中指定sc0关键字。此功能在Catalyst 5500/5000和6500/6000交换机上可用，代码版本为CatOS 5.1或更高版本。
- inpkts enable/disable — 此选项极为重要。如本文档所述，配置为 SPAN 目标端口的端口仍属于其原始 VLAN。在目标端口接收的数据包随后进入该 VLAN，就像该端口是正常接入端口一样。您可能需要这种行为。如果您使用PC作为嗅探器，则希望此PC完全连接到VLAN。然而，如果将目标端口连接到在网络中创建环路的其他网络设备，上述连接可能十分危险。目标 SPAN 端口不会运行 STP，而且您可能会陷入危险的桥接环路状况。请参阅本文档的“为什么SPAN会话会创建桥接环路”部分，以了解出现这种情况的原因。此选项的默认设置为禁用，这意味着目标 SPAN 端口将丢弃该端口接收的数据包。这种丢弃可保护端口免受桥接环路的危害。CatOS 4.2 中显示此选项。
- learning enable/disable — 此选项可用于禁用目标端口的识别功能。默认情况下，识别处于启

用状态，目标端口从其接收的传入数据包中获知 MAC 地址。Catalyst 4500/4000 和 5500/5000 上的 CatOS 5.2 以及 Catalyst 6500/6000 上的 CatOS 5.3 中提供此功能。
- multicast enable/disable — 顾名思义，此选项可用于启用或禁用多播数据包的监控。默认为启用。Catalyst 5500/5000 和 6500/6000 上的 CatOS 5.1 及更高版本中提供此功能。
- spanning port 15/1 — 在 Catalyst 6500/6000 上，可以使用端口 15/1（或 16/1）作为 SPAN 源。该端口可以监控转发到 Multilayer Switch Feature Card (MSFC) 的流量。 该端口捕获软件路由至 MSFC 或定向到 MSFC 的流量。

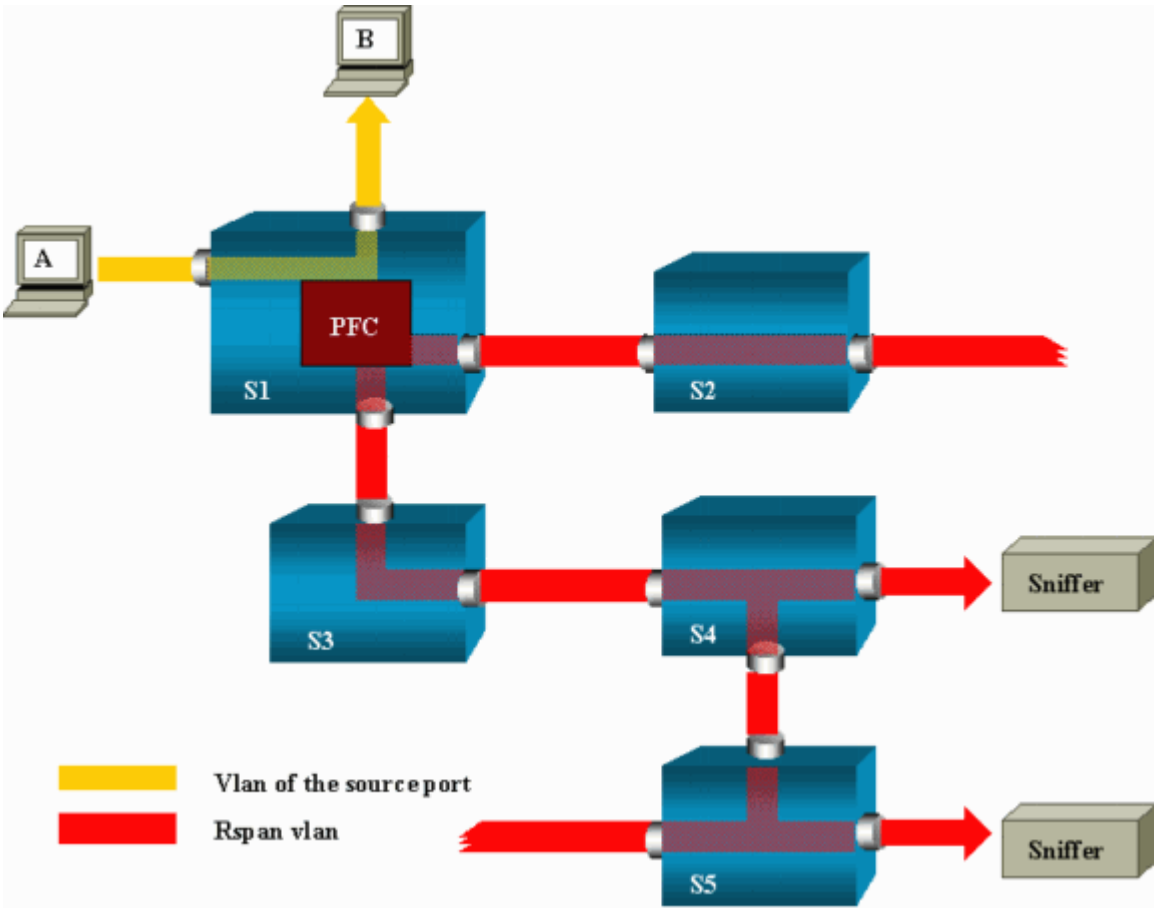
远程 SPAN

RSPAN 概述

使用 RSPAN，可以对遍及交换网络每一个角落的各个源端口进行监控，而不仅仅监控位于具有 SPAN 功能的交换机本地的端口。Catalyst 6500/6000 系列交换机上的 CatOS 5.3 中提供此功能，Catalyst 4500/4000 系列交换机上的 CatOS 6.3 及更高版本也增加了此功能。

该功能的工作方式与常规 SPAN 会话完全相同。由 SPAN 监控的流量并不直接复制到目标端口，而是泛洪至一个专门的 RSPAN VLAN。因此，目标端口可以位于该 RSPAN VLAN 中的任意位置。甚至可以有多个目标端口。

下图显示了 RSPAN 会话的结构：



在本示例中，将 RSPAN 配置为监控主机 A 发送的流量。当 A 生成一个发往 B 的帧时，由 Catalyst 6500/6000 Policy Feature Card (PFC) 的专用集成电路 (ASIC) 将数据包复制到预定义的 RSPAN VLAN。在该处将数据包泛洪至属于该 RSPAN VLAN 的所有其他端口。在此形成的所有交换机间链路均为中继，这是对 RSPAN 的要求。仅有的接入端口是目标端口，用于连接嗅探器（这里连接在 S4 和 S5 上）。

下面是有关此设计的一些说明：

- S1 称为源交换机。数据包只进入配置为 RSPAN 源的交换机中的 RSPAN VLAN。目前，一个交换机只能作为一个 RSPAN 会话的源，这意味着一个源交换机每次只能为一个 RSPAN VLAN 提供数据包。
- S2 和 S3 是中间交换机。它们不是 RSPAN 源，没有目标端口。一个交换机可以作为任意数量 RSPAN 会话的中间交换机。
- S4 和 S5 是目标交换机。它们的部分端口配置为 RSPAN 会话的目标端口。目前，Catalyst 6500/6000 可支持多达 24 个 RSPAN 目标端口，用于一个或多个不同的会话。您可能还注意到，S4 既是目标交换机又是中间交换机。
- 可以看到，RSPAN 数据包泛洪至 RSPAN VLAN。即使未处于指向目标端口的路径中的交换机（如 S2）也会收到发往 RSPAN VLAN 的流量。您会发现，修剪诸如 S1-S2 之类的链路上的此 VLAN 十分有用。
- 为实现泛洪，在RSPAN VLAN上禁用学习。
- 为了防止出现环路，RSPAN VLAN上已运用了STP。因此，RSPAN 无法监控网桥协议数据单元 (BPDU)。

RSPAN 配置示例

本部分的信息说明如何使用非常简单的 RSPAN 设计设置这些不同的元素。S1和S2是两台Catalyst 6500/6000交换机。要监控某些S1端口或来自S2的VLAN，您必须设置一个专用RSPAN VLAN。其余命令的语法与您在典型 SPAN 会话中使用的命令类似。



在两个交换机 S1 和 S2 之间设置 ISL 中继

首先，在每台交换机上放置相同的VLAN中继协议(VTP)域，并将一端配置为期望中继。VTP 协商将执行其余操作。在 S1 上发出以下命令：

<#root>

```
S1> (enable)
```

set vtp domain cisco

```
      VTP domain cisco modified
```

在 S2 上发出以下命令：

<#root>

```
S2> (enable)
```

set vtp domain cisco

```
      VTP domain cisco modified
      S2> (enable)
```

set trunk 5/1 desirable

```
Port(s) 5/1 trunk mode set to desirable.
S2> (enable) 2000 Sep 12 04:32:44 %PAGP-5-PORTFROMSTP:Port 5/1 left bridge
 port 5/1
2000 Sep 12 04:32:47 %DTP-5-TRUNKPORTON:Port 5/1 has become isl trunk
```

创建 RSPAN VLAN

RSPAN 会话需要特定的 RSPAN VLAN。必须创建此 VLAN。不能将现有的 VLAN 转换为 RSPAN VLAN。下面的示例使用 VLAN 100：

<#root>

```
S2> (enable)

set vlan 100 rspan


      Vlan 100 configuration successful
```

在一个配置为 VTP 服务器的交换机上发出此命令。RSPAN VLAN 100 的使用技巧将在整个 VTP 域中自动传播。

将 S2 的端口 5/2 配置为 RSPAN 目标端口

<#root>

```
S2> (enable)

set rspan destination 5/2 100


      Rspan Type : Destination
      Destination : Port 5/2
      Rspan Vlan : 100
      Admin Source : -
      Oper Source : -
      Direction : -
      Incoming Packets: disabled
      Learning : enabled
      Multicast : -
      Filter : -
      Status : active
      2000 Sep 12 04:34:47 %SYS-5-SPAN_CFGSTATECHG:remote span destination session
      active for destination port 5/2
```

在 S1 上配置 RSPAN 源端口

在本示例中，通过端口 6/2 进入 S1 的传入流量将受到监控。发出以下命令：

<#root>

```
S1> (enable)

set rspan source 6/2 100 rx


      Rspan Type : Source
      Destination : -
      Rspan Vlan : 100
      Admin Source : Port 6/2
      Oper Source : Port 6/2
      Direction : receive
      Incoming Packets: -
      Learning : -
      Multicast : enabled
      Filter : -
      Status : active
      S1> (enable) 2000 Sep 12 05:40:37 %SYS-5-SPAN_CFGSTATECHG:remote span
       source session active for remote span vlan 100
```

此时，端口 6/2 上的传入数据包将泛洪至 RSPAN VLAN 100，并通过中继到达在 S1 上配置的目标端口。

检查配置

show rspan 命令可提供交换机上当前 RSPAN 配置的概要信息。同样，一次只能启用一个源 RSPAN 会话。

<#root>

```
S1> (enable)

show rspan


    Rspan Type : Source
    Destination : -
    Rspan Vlan : 100
    Admin Source : Port 6/2
    Oper Source : Port 6/2
    Direction : receive
    Incoming Packets: -
    Learning : -
```

```
Multicast : enabled
Filter : -
Status : active
Total remote span sessions: 1
```

使用 set rspan 命令可实现的其他配置

您可以使用多个命令行配置RSPAN的源和目标。除这一区别外，SPAN 与 RSPAN 的行为其实是相同的。如果有多个目标 SPAN 端口，甚至可以在单个交换机上本地使用 RSPAN。

功能汇总和限制

下表概括了已引入的不同功能，并提供在指定平台上运行这些功能所需的最低 CatOS 版本：

功能	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000
inpkts enable/disable 选项	4.4	4.2	5.1
不同 VLAN 中的多个会话、端口	5.1	5.1	5.1
sc0 选项	—	5.1	5.1
multicast enable/disable 选项	—	5.1	5.1
learning enable/disable 选项	5.2	5.2	5.3
RSPAN	6.3	—	5.3

下表简要概括了目前对可能的 SPAN 会话数量的限制：

功能	Catalyst 4500/4000 系列交换机	Catalyst 5500/5000 系列交换机	Catalyst 6500/6000 系列交换机
Rx 或双向 SPAN 会话	5	1	2
Tx SPAN 会话	5	4	4
微型协议分析器会话	Not Supported	Not Supported	1
Rx、Tx 或双向 RSPAN 源会话	5	Not Supported	1管理引擎720支持两个RSPAN源会话。
RSPAN 目标	5	Not Supported	24
会话总数	5	5	30

有关其他限制和配置指南，请参阅下列文档：

- 配置SPAN和RSPAN(Catalyst 4500/4000)
- 配置SPAN和RSPAN(Catalyst 6500/6000)

Catalyst 2940、2950、2955、2960、2970、3550、3560、3560-

E、3750 和 3750-E 系列交换机中的 SPAN

以下是在 Catalyst 2940、2950、2955、2960、2970、3550、3560、3560-E、3750 和 3750-E 系列交换机上配置 SPAN 功能的指南：

- Catalyst 2950 交换机一次只能启用一个 SPAN 会话，而且只能监控源端口。这些交换机不能监控 VLAN。
- Catalyst 2950 和 3550 交换机可在 Cisco IOS 软件版本 12.1(13)EA1 和更高版本的目标 SPAN 端口上转发流量。
- Catalyst 3550、3560 和 3750 交换机支持一次运行多达两个 SPAN 会话，并且可监控源端口及 VLAN。
- 在配置 RSPAN 会话时，Catalyst 2970、3560 和 3750 交换机不需要配置反射器端口。
- Catalyst 3750 交换机支持使用位于任意交换机堆栈成员上的源端口和目标端口进行会话配置。
- 每个 SPAN 会话只允许有一个目标端口，而且同一端口不能作为多个 SPAN 会话的目标端口。因此，两个 SPAN 会话不能使用同一个目标端口。

Catalyst 2950 和 Catalyst 3550 上的 SPAN 功能配置命令是类似的。但是，Catalyst 2950 不能监控 VLAN。可以配置 SPAN，如下面的示例所示：

<#root>

```
C2950#

configure terminal



C2950(config)#
C2950(config)#monitor session 1 source interface fastethernet 0/2

!--- This configures interface Fast Ethernet 0/2 as source port.

C2950(config)#

monitor

 session 1 destination interface fastethernet 0/3

!--- This configures interface Fast Ethernet 0/3 as destination port.

C2950(config)#

C2950#

show monitor

 session 1
Session 1---------
```

```
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          Fa0/2
Destination Ports: Fa0/3
C2950#
```

还可以将某个端口配置为本地 SPAN 和 RSPAN 的目标端口，用于监控相同的 VLAN 流量。要监控位于两台直连交换机中的特定vlan的流量，请在具有目标端口的交换机上配置这些命令。在本示例中，我们通过 VLAN 5 监控在两个交换机之间传播的流量：

<#root>

```
c3750(config)#

monitor session 1 source vlan < Remote RSPAN VLAN ID >


c3750(config)#

monitor session 1 source vlan 5


c3750(config)#

monitor session 1 destination interface fastethernet 0/3



!--- This configures interface FastEthernet 0/3 as a destination port.
```

在远程交换机上，使用以下配置：

<#root>

```
c3750_remote(config)#

monitor session 1 source vlan 5



!--- Specifies VLAN 5 as the VLAN to be monitored.

c3750_remote(config)#

monitor session 1 destination remote vlan
```

在上一示例中，将一个端口配置为本地 SPAN 和 RSPAN 的目标端口，以监控位于两个交换机中的同一 VLAN 的流量。

注意：与 2900XL 和 3500XL 系列交换机不同，Catalyst 2940、2950、2955、2960、2970、3550、3560、3560-E、3750 和 3750-E 系列交换机支持对源端口流量使用仅 Rx 方向（Rx SPAN 或入口 SPAN）、仅 Tx 方向（Tx SPAN 或出口 SPAN）或双向 SPAN 功能。

注意：对于采用 Cisco IOS 软件版本 12.0(5.2)WC(1) 或任何早于 Cisco IOS 软件版本 12.1(6)EA2 的软件的 Catalyst 2950，不支持该配置中的命令。

注意：采用 Cisco IOS 软件版本 12.1.(9)EA1d 和 Cisco IOS 软件版本 12.1 系列中早期版本的 Catalyst 2950 交换机支持 SPAN。但是，在SPAN目标端口（连接到嗅探设备或PC）上看到的所有数据包都具有IEEE 802.1Q标记，即使SPAN源端口（监控端口）不能是802.1Q中继端口。如果嗅探设备或 PC 网络接口卡 (NIC) 无法识别带有 802.1Q 标记的数据包，该设备可能会丢弃这些数据包或在尝试对这些数据包进行解码时遇到困难。只有 SPAN 源端口为中继端口时，识别 802.1Q 标记帧的功能才具有重要性。在 Cisco IOS 软件版本 12.1(11)EA1 和更高版本中，可以在 SPAN 目标端口启用和禁用数据包标记功能。发出monitor session session_number destination interface interface_id encapsulation dot1q命令以启用目的端口上的数据包封装。如果未指定 encapsulation 关键字，则会发送未标记的数据包，这是 Cisco IOS 软件版本 12.1(11)EA1 和更高版本中的默认设置。

功能	Catalyst 2950/3550
入口 (inpkts) enable/disable 选项	Cisco IOS 软件版本 12.1(12c)EA1
RSPAN	Cisco IOS 软件版本 12.1(12c)EA1

功能	Catalyst 29401、2950、2955、2960、2970、3550、3560、3750
Rx 或双向 SPAN 会话	2
Tx SPAN 会话	2
Rx、Tx 或双向 RSPAN 源会话	2
RSPAN 目标	2
会话总数	2

[1] Catalyst 2940交换机仅支持本地SPAN。此平台不支持 RSPAN。

运行 Cisco IOS 系统软件的 Catalyst 4500/4000 和 Catalyst 6500/6000 系列交换机中的 SPAN

运行 Cisco IOS 系统软件的 Catalyst 4500/4000 和 Catalyst 6500/6000 系列交换机支持 SPAN 功能。这两种交换机平台都使用相同的命令行界面(CLI)和类似于本节介绍的配置的配置。有关相关配置，请参阅下列文档：

- 配置SPAN和RSPAN(Catalyst 6500/6000)
- 配置SPAN和RSPAN(Catalyst 4500/4000)

配置示例

您可以配置SPAN，如下例所示：

```
<#root>

4507R#

configure terminal


Enter configuration commands, one per line. End with CNTL/Z.

4507R(config)#

monitor session 1 source interface fastethernet 4/2



!--- This configures interface Fast Ethernet 4/2 as source port.

4507R(config)#

monitor session 1 destination interface fastethernet 4/3



!--- The configures interface Fast Ethernet 0/3 as destination port.

4507R#

show monitor session 1



Session 1---------
Type : Local Session
Source Ports :
Both : Fa4/2
Destination Ports : Fa4/3

4507R#
```

功能汇总和限制

下表概括了已引入的不同功能，并提供在指定平台上运行这些功能所需的最低 Cisco IOS 软件版本：

功能	Catalyst 4500/4000（Cisco IOS 软件）	Catalyst 6500/6000（Cisco IOS 软件）
入口 (inpkts) enable/disable 选项	Cisco IOS 软件版本 12.1(19)EW	当前不支持[1]
RSPAN	Cisco IOS 软件版本 12.1(20)EW	Cisco IOS 软件版本 12.1(13)E

[1]此功能目前不可用，这些功能的可用性通常在发布之前不会发布。

注意：Cisco Catalyst 6500/6000 系列交换机的 SPAN 功能具有与 PIM 协议相关的限制。将交换机配置为使用 PIM 和 SPAN 后，连接到 SPAN 目标端口的网络分析器/嗅探器即可以监测到不属于 SPAN 源端口/VLAN 流量的 PIM 数据包。产生此问题的原因是交换机的数据包转发体系结构存在限制。SPAN 目标端口不执行任何验证数据包来源的检查。此问题也记录在思科漏洞ID CSCdy57506中（仅限注册客户）。

下表简要概括了目前对可能的 SPAN 和 RSPAN 会话数量的限制：

功能	Catalyst 4500/4000（Cisco IOS 软件）
Rx 或双向 SPAN 会话	2
Tx SPAN 会话	4
Rx、Tx 或双向 RSPAN 源会话	2（Rx、Tx 或双向），对于仅 Tx 最多为 4
RSPAN 目标	2
会话总数	6

有关运行 Cisco IOS 软件的 Catalyst 6500/6000 交换机，请参阅本地 SPAN、RSPAN 和 ERSPAN 会话限制。

在 Catalyst 6500 系列中，请注意出口 SPAN 是在 Supervisor 完成的，这一点很重要。这样，可以将受出口 SPAN 监控的所有流量跨交换结构发送到 Supervisor，然后发送到 SPAN 目标端口，这可能会占用大量系统资源并影响用户流量。入口SPAN可以在入口模块上完成，因此SPAN性能将是所有参与复制引擎的总和。SPAN 功能的性能取决于数据包大小和复制引擎中可用 ASIC 的类型。

使用低于 Cisco IOS 软件版本 12.2(33)SXH 的版本时，端口信道接口 EtherChannel 不能作为 SPAN 目标。使用 Cisco IOS 软件版本 12.2(33)SXH 和更高版本时，EtherChannel 可以作为 SPAN 目标。目标 EtherChannel 不支持端口聚合控制协议 (PAgP) 或链路聚合控制协议 (LACP) 及 EtherChannel 协议；仅支持禁用了所有 EtherChannel 协议支持的 on 模式。

有关其他限制和配置指南，请参阅下列文档：

- 配置 SPAN 和 RSPAN (Catalyst 4500/4000)

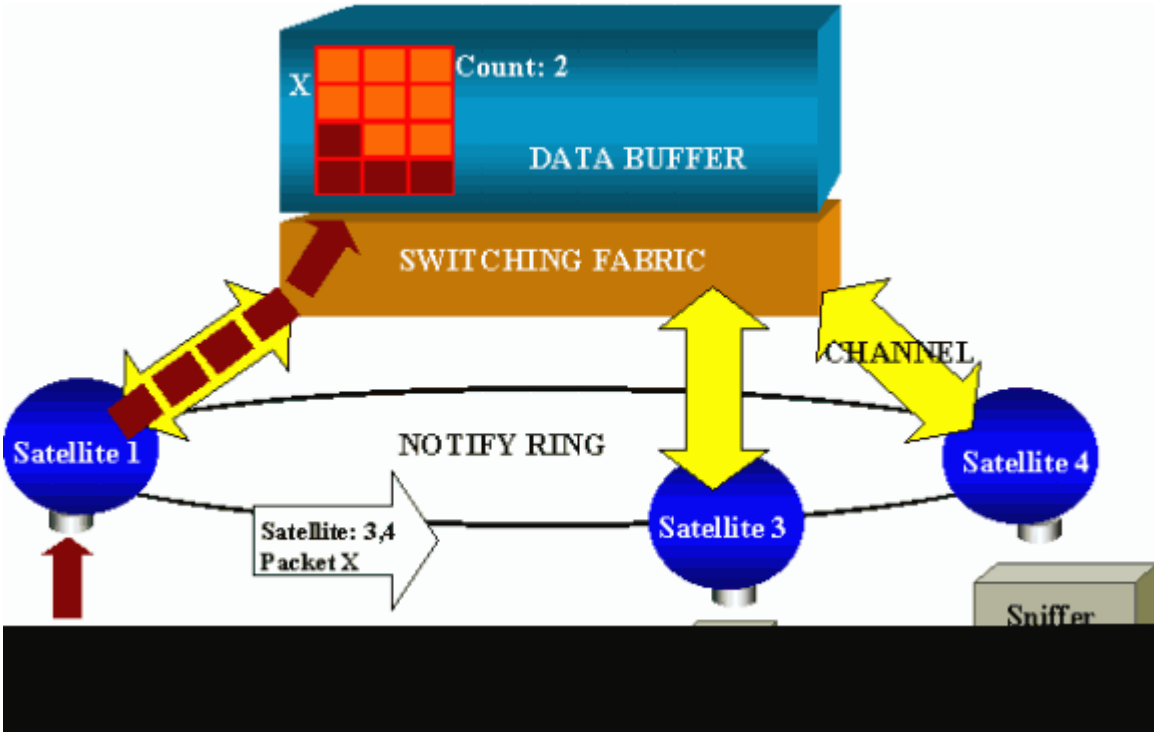
- 配置本地 SPAN、远程 SPAN (RSPAN) 和封装 RSPAN (Catalyst 6500/6000)

不同 Catalyst 平台上 SPAN 的性能影响

Catalyst 2900XL/3500XL 系列

体系结构概述

下面是 2900XL/3500XL 交换机内部体系结构的简单视图：



交换机的各个端口连接到卫星，这些卫星通过放射信道与交换结构进行通信。在顶部，所有卫星通过一个专用于信令流量的高速通知环互相连接。

当卫星从某个端口收到数据包时，会将该数据包拆分为信元并通过一个或多个信道发送到交换结构。随后，数据包将存储在共享内存中。每个卫星均掌握目标端口的信息。在本部分的图表中，卫星 1 获知卫星 3 和 4 将收到数据包 X。卫星 1 通过通知环向其他卫星发送一条消息。这样，卫星 3 和 4 便可以开始通过其放射信道从共享内存中检索信元，并最终得以转发该数据包。由于源卫星了解目标，该卫星还会传输一个表示其他卫星下载此数据包的次数的指数。每次卫星从共享内存中检索该数据包时，该指数将递减。当该指数达到 0 时，便可以释放共享内存。

性能影响

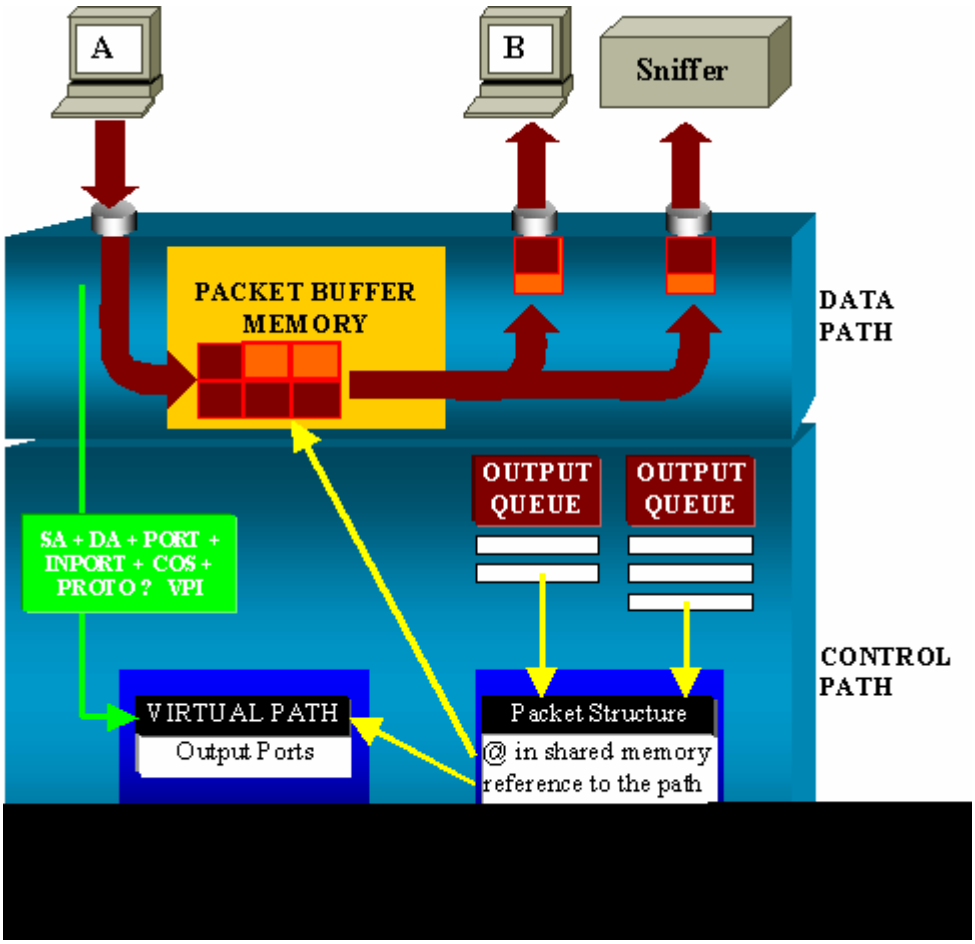
使用SPAN对一些端口进行监控即指额外地将数据包从数据缓冲器复制到一个卫星。对高速交换结构的影响可以忽略不计。

监控端口接收所有受监端口传输和接收的流量的副本。在此体系结构内，发往多个目标的数据包将存储在内存中，直到所有副本转发完毕。如果监控端口在一段时期内持续处于超负荷 50% 的状态，该端口很可能发生拥塞并占据部分共享内存。受监控的一个或多个端口也有可能呈现减速状态。

Catalyst 4500/4000 系列

体系结构概述

Catalyst 4500/4000 基于共享内存交换结构。下图简要概括了数据包通过交换机的路径。事实上，实际的实施过程要复杂得多：



在 Catalyst 4500/4000 上，可以区分数据路径。数据路径与交换机中数据的真实传输路径相对应，您可以将其与做出所有决策的控制路径区分开来。

当数据包进入交换机时，会在数据包缓冲内存（共享内存）中分配缓冲区。

在数据包描述符表 (PDT) 中初始化指向此缓冲区的数据包结构。

将数据复制到共享内存时，由控制路径确定在何处交换数据包。为了进行此确定，将根据以下信息计算散列值：

- 数据包源地址
- 目的地址
- VLAN
- 协议类型
- 输入端口
- 服务等级 (CoS)（IEEE 802.1p 标记或端口默认值）

此值用于在虚拟路径表 (VPT) 中查找路径结构的虚拟路径索引 (VPI)。 VPT 中的此虚拟路径条目包含与该特定数据流相关的若干字段。这些字段包括目标端口。PDT 中的数据包结构现已更新，包含对虚拟路径和计数器的引用。

在本部分的示例中，数据包将发送到两个不同的端口，因此计数器初始化为2。最后，将数据包结构添加到两个目的端口的输出队列。在该队列中，数据从共享内存复制到端口的输出缓冲区，数据包结构计数器递减。当它达到 0 时，共享内存缓冲区将释放。

性能影响

使用 SPAN 功能，必须将数据包发送到两个不同的端口，如体系结构概述部分的示例所述。由于交换结构无阻塞，将数据包发送到两个端口不成问题。

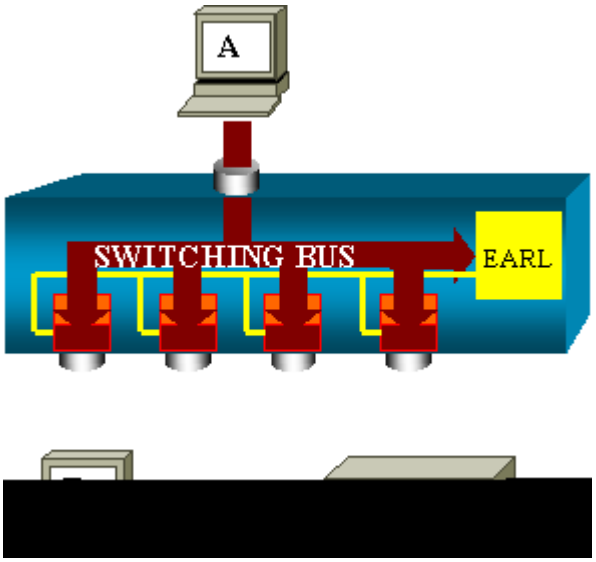
如果目标 SPAN 端口发生拥塞，则会将数据包丢弃在输出队列中，并从共享内存中正确释放。因此对交换机运转没有影响。

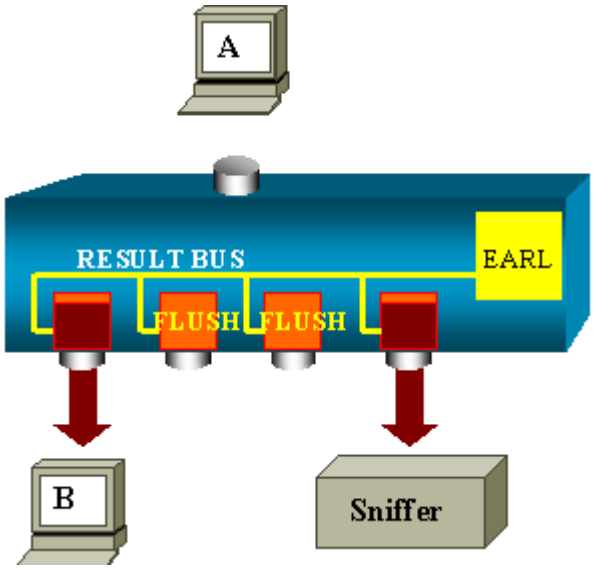
Catalyst 5500/5000 和 6500/6000 系列

体系结构概述

在 Catalyst 5500/5000 和 6500/6000 系列交换机上，在某个端口收到的数据包将通过内部交换总线进行传输。交换机中的每个线路卡开始在内部缓冲区中存储此数据包。

同时，编码地址识别逻辑 (EARL) 收到数据包的报头并计算结果索引。EARL 通过结果总线将结果索引发送到所有线路卡。通过了解此索引，线路卡可以单独决定当线路卡在其缓冲区中接收数据包时是否可以刷新或传输数据包。





性能影响

最终有一个还是多个端口传输数据包对交换机运转没有任何影响。因此，如果考虑此体系结构，SPAN 功能不会对性能产生任何影响。

常见问题与一般问题

SPAN 配置错误导致的连通性问题

由于SPAN配置错误，在早于5.1的CatOS版本中经常出现连接问题。在这些版本中，只能有一个SPAN会话。

即使禁用 SPAN，该会话仍保留在配置中。通过发出 set span enable 命令，用户可重新激活存储的 SPAN 会话。例如，如果用户需要启用 STP，常常会由印刷错误引起此操作。如果使用目标端口转发用户流量，则可能产生严重的连通性问题。

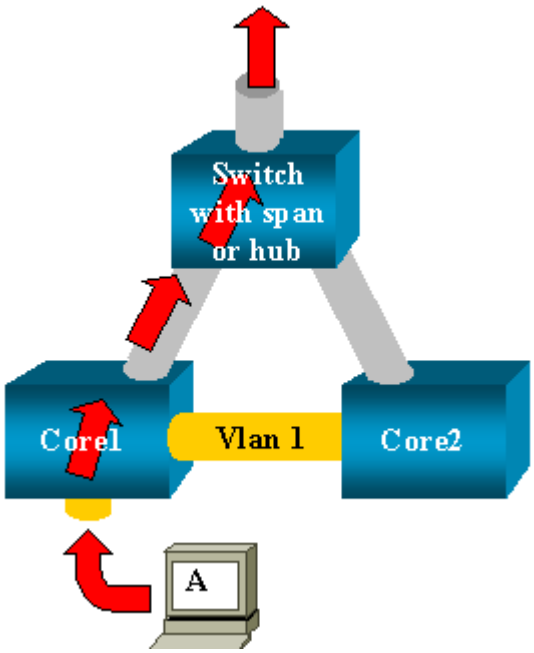
⚠ 警告：当前 CatOS 的实施过程中仍存在此问题。对于选择作为 SPAN 目标的端口，应谨慎操作。

SPAN 目标端口打开/关闭

当端口被纳入监控范围时，端口状态显示为打开/关闭。当您配置 SPAN 会话以监控端口时，目标接口会故意地显示状态“关闭（监控）”。接口显示处于此状态的端口，以表明该端口当前无法用作生产端口。端口显示为打开/关闭监控是正常的。

SPAN会话为什么会创建桥接环路

当管理员尝试伪造 RSPAN 功能时，通常会创建桥接环路。另外，配置错误也可能引发此问题。示例 情景:

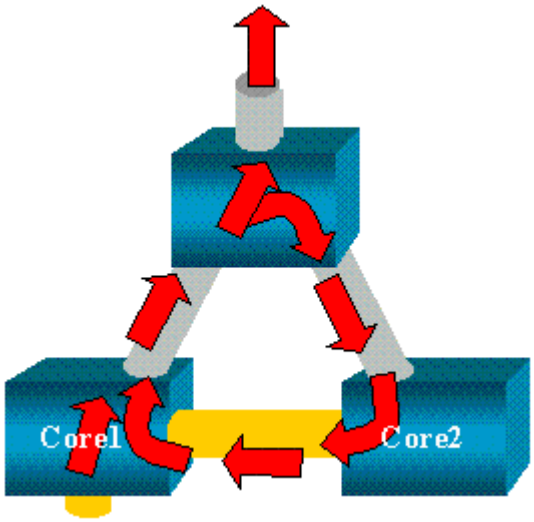


有两台通过中继链接的核心交换机。在这种情况下，每个交换机具有与之连接的若干服务器、客户端或其他网桥。管理员要使用 SPAN 对出现在多个网桥中的 VLAN 1 进行监控。

管理员创建一个 SPAN 会话，用于在每个核心交换机上监控整个 VLAN 1，然后为了合并这两个会话，将目标端口连接到同一个集线器（或使用另一个 SPAN 会话连接到同一交换机）。

管理员实现了目标。核心交换机在 VLAN 1 上收到的每一个数据包将在 SPAN 端口上进行复制并向上转发到集线器。最终由嗅探器捕获流量。

唯一的问题是流量也通过目标SPAN端口重新注入到核心2。流量再次送入核心 2 将在 VLAN 1 中创建桥接环路。请记住，目标 SPAN 端口不会运行 STP，也不能避免形成这样的环路。



注意：由于 CatOS 中引入了 inpkts（输入数据包）选项，因此 SPAN 目标端口将默认丢弃所有传入数据包，从而避免产生这种故障情况。但是，Catalyst 2900XL/3500XL系列交换机上仍然存在潜在问题。

注意：即使有 inpkts 选项防止环路的形成，本部分显示的配置仍有可能在网络中引起一些问题。网络问题可能是由与目标端口上启用的识别功能相关的 MAC 地址识别问题导致的。

SPAN是否会影响性能？

有关对指定 Catalyst 平台性能的影响的信息，请参阅本文档的下列部分：

- Catalyst 2900XL/3500XL 系列
- Catalyst 4500/4000 系列
- Catalyst 5500/5000 和 6500/6000 系列

能否在 EtherChannel 端口上配置 SPAN？

如果链路捆绑中的端口之一为 SPAN 目标端口，则不会形成 EtherChannel。在这种情况下如果尝试配置 SPAN，交换机将提示您：

```
Channel port cannot be a Monitor Destination Port
Failed to configure span feature
```

您可以使用 EtherChannel 链路捆绑中的端口作为 SPAN 源端口。

是否可以同时运行多个 SPAN 会话？

在 Catalyst 2900XL/3500XL 系列交换机上，限制 SPAN 会话数的只有交换机上可用目标端口的数量。

在 Catalyst 2950 系列交换机上，在任何时间只能有一个指定监控端口。如果选择另一个端口作为监控端口，则会禁用原有端口，新选择的端口将成为监控端口。

在采用 CatOS 5.1 和更高版本的 Catalyst 4500/4000、5500/5000 和 6500/6000 交换机上，可以运行若干并发 SPAN 会话。

请参阅本文档的创建多个同时运行的会话和功能概要和限制部分。

错误“% Local Session Limit Has Been Exceeded”

当允许的 SPAN 会话超出 Supervisor 引擎的限制时，将显示以下消息：

```
% Local Session limit has been exceeded
```

Supervisor Engines have a limitation of SPAN sessions.有关详细信息，请参阅配置本地 SPAN、RSPAN 和 ERSPAN 中的本地 SPAN、RSPAN 和 ERSPAN 会话限制部分。

无法删除 VPN 服务模块上的 SPAN 会话，原因是发生错误“% Session [Session No:] Used by Service Module”

出现此问题时，插入虚拟专用网络 (VPN) 模块的机箱中已经插入了交换矩阵模块。

Cisco IOS软件会自动为VPN服务模块创建SPAN会话，以处理组播流量。

发出以下命令可删除软件为VPN服务模块创建的SPAN会话：

<#root>

Switch(config)#

no monitor session session_number service-module

注意：如果删除该会话，VPN 服务模块将丢弃多播流量。

为何无法使用 SPAN 捕获损坏的数据包？

不能使用 SPAN 捕获损坏的数据包，这是交换机通常的运行方式决定的。当数据包通过交换机时，将发生以下事件：

1. 数据包到达入站端口。
2. 数据包至少存储在一个缓冲区中。
3. 最后，数据包在出站端口上重新传输。



如果交换机收到一个损坏的数据包，入站端口通常会丢弃该数据包。因此您在出站端口看不到该数据包。

对于流量的捕获，交换机不是完全透明的。同样，如果在本部分所述情况下在嗅探器中看到损坏的数据包，则可以确定是出口分段在步骤 3 出现了错误。

如果认为损坏的数据包是由某个设备发送的，您可以选择将发送主机和嗅探器设备连接在同一集线器上。集线器不执行任何错误检查。

因此，与交换机不同，集线器不会丢弃数据包。这样，便可以查看数据包。

Error:% Session 2 used by service module

如果安装了防火墙服务模块 (FWSM)（例如，在 CAT6500 中安装并在之后移除），它会自动启用 SPAN 反射器功能。SPAN 反射器功能在交换机中使用一个 SPAN 会话。

如果不再需要此功能，您可以在CAT6500的配置模式下输入no monitor session service module命令，然后立即输入所需的新的SPAN配置。

反射器端口丢弃数据包

反射器端口将接收所有受监控源端口发送和接收的流量的副本。如果反射器端口使用过度，则可能发生拥塞。这可能会影响一个或多个源端口的流量转发。

如果反射器端口的带宽无法满足来自对应源端口的流量，则会丢弃超额数据包。

10/100 端口的反射速率为 100 Mbps。千兆端口的反射速率为 1 Gbps。

始终将 SPAN 会话与 Catalyst 6500 机箱中的 FWSM 一起使用

当您将 Supervisor 引擎 720 与运行 Cisco Native IOS 的机箱中的 FWSM 一起使用时，默认情况下将使用一个 SPAN 会话。如果使用 show monitor 命令检查未使用的会话，则会使用 session 1：

```
<#root>

Cat6K#

show monitor


Session 1
---------
Type : Service Module Session
```

当 Catalyst 6500 机箱中有防火墙刀片时，会自动安装此会话以支持硬件多播复制，因为 FWSM 无法复制多播数据流。

如果来自 FWSM 之后的多播数据流必须在第三层复制到多个线路卡，该自动会话会通过光纤信道将流量复制到 Supervisor。

如果有来自 FWSM 之后的生成多播数据流的多播源，则需要使用 SPAN 反射器。如果将多播源置于外部 VLAN，则不一定需要 SPAN 反射器。SPAN 反射器与通过 FWSM 的桥接 BPDU 不兼容。

您可以使用no monitor session service module命令禁用SPAN反射器。

同一交换机内的 SPAN 和 RSPAN 会话能否具有相同的 ID？

不能，无法对常规 SPAN 会话和 RSPAN 目标会话使用相同的会话 ID。每个SPAN和RSPAN会话必须具有不同的会话ID。

RSPAN 会话能否跨不同的 VTP 域工作？

Yes.RSPAN 会话可以跨越不同的 VTP 域。但需要确保 RSPAN VLAN 存在于这些 VTP 域的数据库中。另外，还要确保会话源到会话目标的路径中不存在第三层设备。

RSPAN 会话能否跨 WAN 或不同的网络工作？

不能。RSPAN 会话不能跨越任何第三层设备，因为 RSPAN 是 LAN（第二层）功能。要监控WAN或其他网络上的流量，请使用封装远程交换机端口分析器(ERSPAN)。 ERSPAN 功能支持不同交换机上的源端口、源 VLAN 和目标端口，从而提供对跨网络的多个交换机的远程监控。

ERSPAN 包括一个 ERSPAN 源会话、可路由的 ERSPAN GRE 封装流量和一个 ERSPAN 目标会话。

您可在不同的交换机上分别配置 ERSPAN 源会话和目标会话。

当前，支持 ERSPAN 功能的系统如下：

- 运行 Cisco IOS 软件版本 12.2(18)SXE 或更高版本的带有 PFC3B 或 PFC3BXL 的 Supervisor 720
- 硬件版本为 3.2 或更高版本并且运行 Cisco IOS 软件版本 12.2(18)SXE 或更高版本的带有 PFC3A 的 Supervisor 720

有关 ERSPAN 的详细信息，请参阅配置本地 SPAN、远程 SPAN (RSPAN) 和封装 RSPAN - Catalyst 6500 系列 Cisco IOS 软件配置指南 (12.2SX)。

RSPAN 源会话和目标会话能否存在于同一台 Catalyst 交换机中？

不能。如果 RSPAN 源会话与 RSPAN 目标会话位于同一交换机上，RSPAN 将无法工作。

如果RSPAN源会话配置了特定RSPAN VLAN，并且该RSPAN VLAN的RSPAN目标会话配置在同一台交换机上，则RSPAN目标会话的目标端口由于硬件限制而无法传输来自RSPAN源会话的捕获数据包。4500 系列和 3750 系列交换机不支持此限制。

此问题记录在思科漏洞ID CSCeg08870中（仅限注册客户）。 示例：

```
monitor session 1 source interface Gi6/44
monitor session 1 destination remote vlan 666
monitor session 2 destination interface Gi6/2
monitor session 2 source remote vlan 666
```

此问题的解决方法是使用常规 SPAN。

连接到 SPAN 目标端口的网络分析器/安全设备无法访问

SPAN 目标端口的基本特性是除 SPAN 会话所需的流量外，不传输任何流量。如果需要通过 SPAN 目标端口到达（IP 可达性）网络分析器/安全设备，则需要启用入口流量转发。

启用入口后，SPAN 目标端口将接受传入数据包（这些数据包可能根据指定封装模式进行标记），并对其进行正常交换。配置 SPAN 目标端口时，您可以指定是否启用入口功能，以及要使用哪个 VLAN 交换未标记的入口数据包。

如果配置了 ISL 封装，则不需要指定入口 VLAN，因为所有 ISL 封装数据包均带有 VLAN 标记。尽管端口进行 STP 转发，但它并不参与 STP，因此配置此功能时请谨慎操作，以免在网络中引入生成树环路。在 SPAN 目标端口上指定入口和中继封装后，该端口便可开始在所有活动 VLAN 中进行转发。不允许将不存在的 VLAN 配置为入口 VLAN。

monitor session session_number destination interface interface [encapsulation {isl | dot1q}]入口 [vlan vlan_IDs]

本示例显示如何使用802.1q封装配置目标端口，以及如何使用本征VLAN 7配置入口数据包。

<#root>

```
Switch(config)#

monitor session 1 destination interface fastethernet 5/48
 encapsulation dot1q ingress vlan 7
```

采用此配置时，会将与会话 1 关联的 SPAN 源发出的流量复制到快速以太网 5/48 接口之外，并采用 802.1q 封装。

接受传入流量并对其进行交换，将未标记的数据包归入 VLAN 7。

相关信息

- 如何在运行Cisco IOS软件的Cisco Catalyst 4500交换机上配置SPAN和RSPAN
- SPAN目标端口显示为“未连接”，且无法与网络的其余部分通信
- 交换机产品支持
- LAN 交换技术支持
- 技术支持和文档

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。