在网络上配置远程交换机端口分析器(RSPAN)设置

目录

目标

本文提供有关如何在交换机上配置RSPAN的说明。

适用设备 |固件版本

- Sx350 | 2.2.5.68(下载最新版)
- SG350X | 2.2.5.68(下载最新版)
- SX550X | 2.2.5.68(下载最新版)

简介

交换机端口分析器(SPAN)（有时称为端口镜像或端口监控）会选择网络流量以供网络分析器分析。网络分析器可以是 Cisco SwitchProbe 设备，也可以是其他远程监控 (RMON) 探测器。

网络设备上使用端口镜像将在单个设备端口、多个设备端口或整个虚拟局域网(VLAN)上看到的网络数据包的副本发送到设备上另一个端口上的网络监控连接。这通常用于需要监控网络流量的网络设备，例如入侵检测系统。连接到监控端口的网络分析器处理用于诊断、调试和性能监控的数据包。

远程交换机端口分析器(RSPAN)是SPAN的扩展。RSPAN通过支持监控网络中的多台交换机并允许在远程交换机上定义分析器端口来扩展SPAN。这意味着您可以集中网络捕获设备。

RSPAN的工作方式是将来自RSPAN会话的源端口的流量镜像到专用于RSPAN会话的VLAN。然后，此VLAN会中继到其他交换机，从而允许RSPAN会话流量通过多台交换机传输。在包含会话的目的端口的交换机上，来自RSPAN会话VLAN的流量仅从目的端口镜像。

RSPAN流量

- 每个RSPAN会话的流量通过用户指定的RSPAN VLAN传输，该VLAN专用于所有参与的交换机中的该RSPAN会话。
- 从启动设备上的源接口发出的流量通过反射器端口复制到RSPAN VLAN。这是必须设置的物理端口。它专门用于构建RSPAN会话。
- 此反射器端口是将数据包复制到RSPAN VLAN的机制。它仅转发来自其所属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。
- 然后，RSPAN流量通过中间设备上的中继端口转发到最终交换机上的目标会话。
- 目的交换机监控RSPAN VLAN并将其复制到目的端口。

RSPAN端口成员规则

- 在所有交换机上 — RSPAN VLAN中的成员仅可标记。
- 启动交换机

- SPAN源接口不能是RSPAN VLAN的成员。

— 反射器端口不能是此VLAN的成员。

— 建议远程VLAN没有任何成员身份。

- 中间交换机

— 建议从所有不用于传递镜像流量的端口中删除RSPAN成员身份。

— 通常，RSPAN远程VLAN包含两个端口。

- 最终交换机

— 对于镜像流量，源端口必须是RSPAN VLAN的成员。

— 建议从所有其他端口（包括目的接口）删除RSPAN成员。

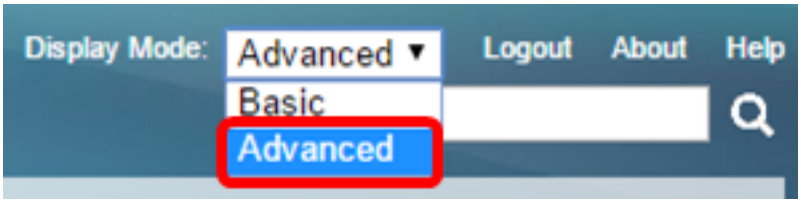
在网络上配置RSPAN

在交换机上配置RSPAN VLAN

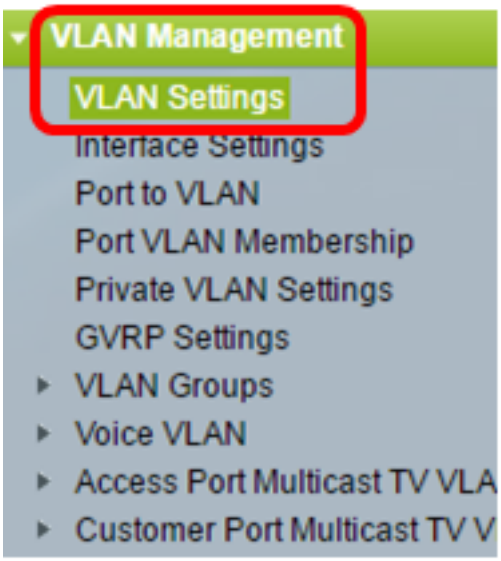
RSPAN VLAN在RSPAN源会话和目标会话之间传输SPAN流量。它具有以下特点：

- RSPAN VLAN中的所有流量始终泛洪。
- RSPAN VLAN上不发生介质访问控制(MAC)地址学习。
- RSPAN VLAN流量仅在中继端口上传输。
- STP可以在RSPAN VLAN中继上运行，但不能在SPAN目标端口上运行。
- 在VLAN配置模式下，必须使用remote-span VLAN配置模式命令在启动交换机和最终交换机上**配置RSPAN VLAN**，或按照以下说明进行配置：

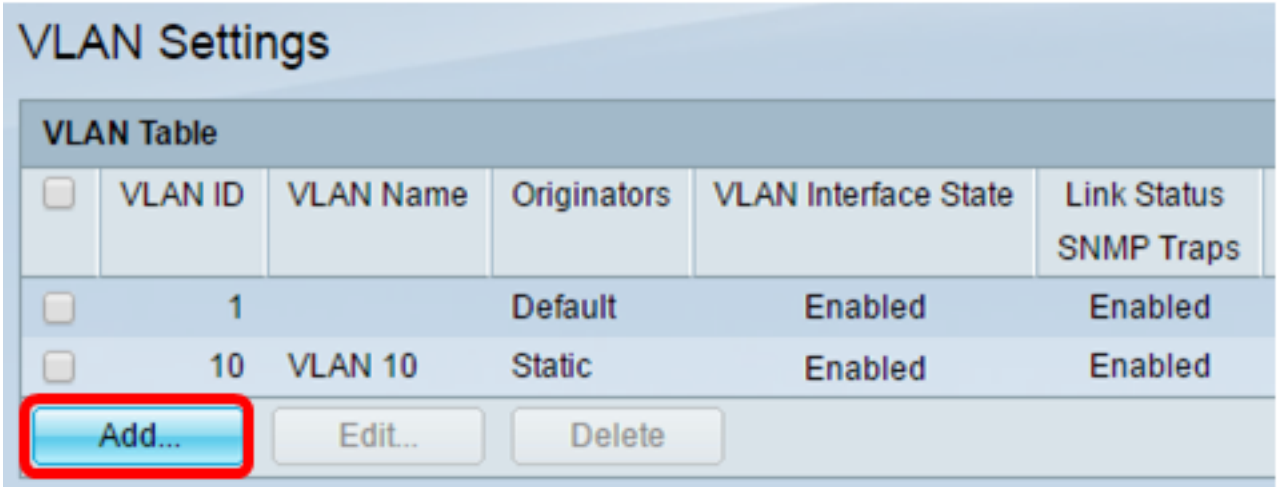
步骤1.登录Start Switch的基于Web的实用程序并在Display Mode下拉列表中选择**Advanced**。



步骤2.选择**VLAN Management > VLAN Settings**。



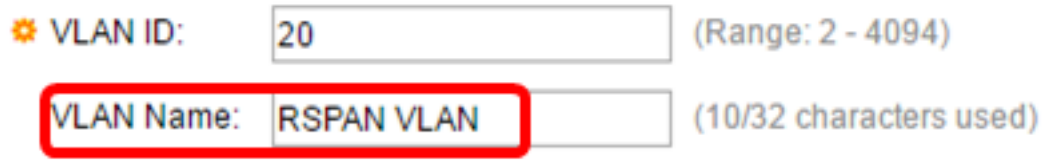
步骤3.单击“添**加**”。



步骤4.在VLAN ID字段中输入*VLAN ID*。

注意：在本例中，VLAN 20用作VLAN ID。

步骤5.（可选）在VLAN Name字段中输入*VLAN*名称。

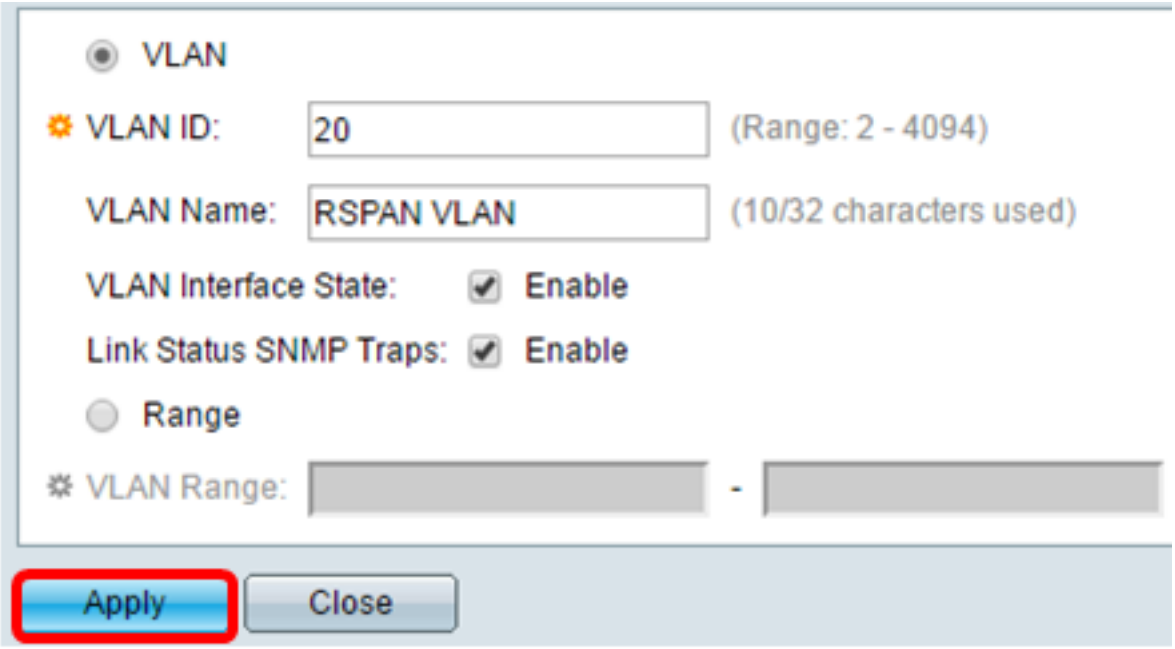


注意：在本例中，RSPAN VLAN用作VLAN名称。

步骤6.（可选）选中VLAN接口状态复选框以启用VLAN。如果VLAN关闭，则VLAN不会从更高级别发送或接收消息。例如，如果关闭配置了IP接口的VLAN，则继续桥接到VLAN，但交换机无法在VLAN上传输和接收IP流量。默认情况下，此功能已启用。

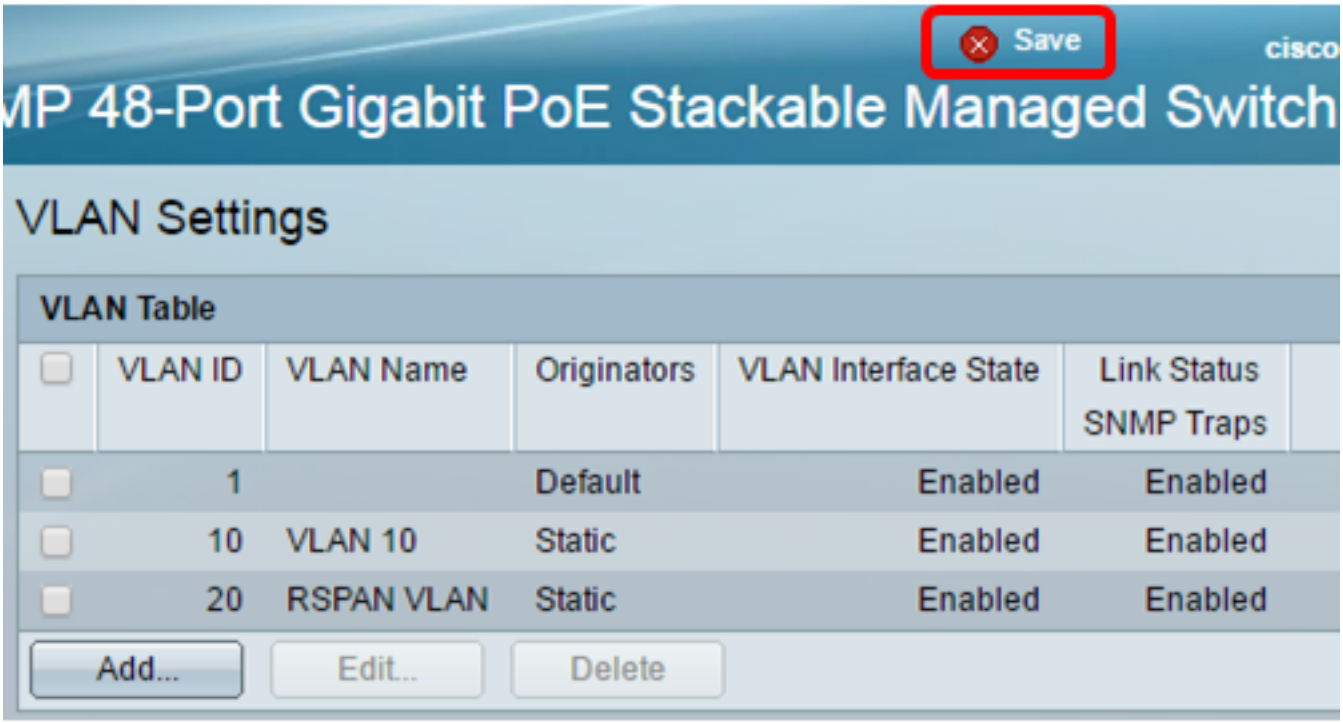
步骤7.（可选）选中Link Status SNMP Traps复选框以启用简单网络管理协议(SNMP)陷阱的链路状态生成。默认情况下，此功能已启用。

步骤8.单击“应用”，然后单击“**关闭**”。



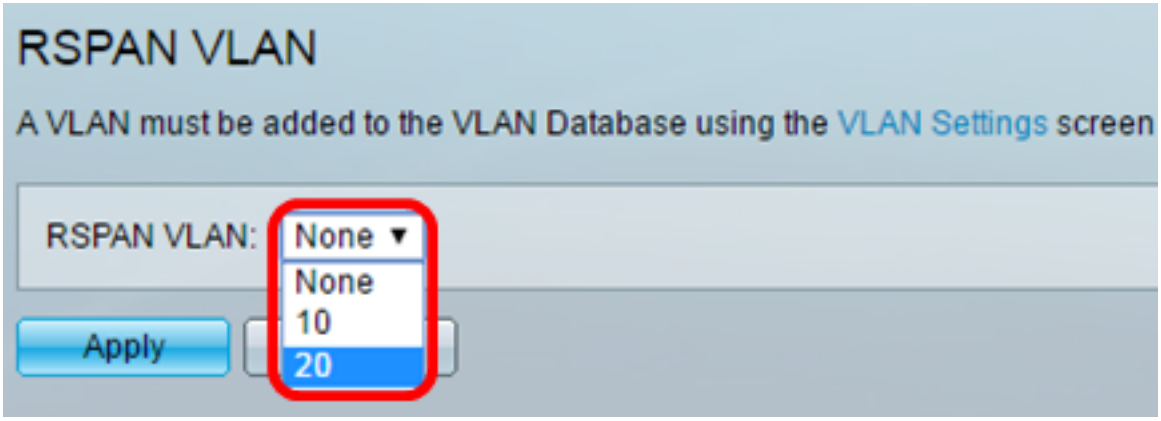
注意：要了解有关在交换机上管理VLAN的详细信息，请单击此处。

步骤9.（可选）单击“保**存**”更新运行配置文件。



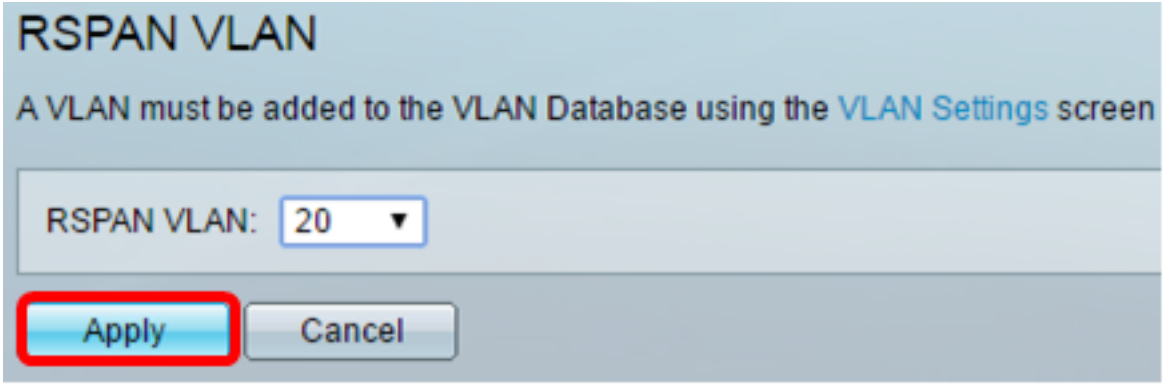
步骤10.选择**Status and Statistics > SPAN & RSPAN > RSPAN VLAN**。

步骤11.从RSPAN VLAN下拉列表中选择VLAN ID。此VLAN应专用于RSPAN。

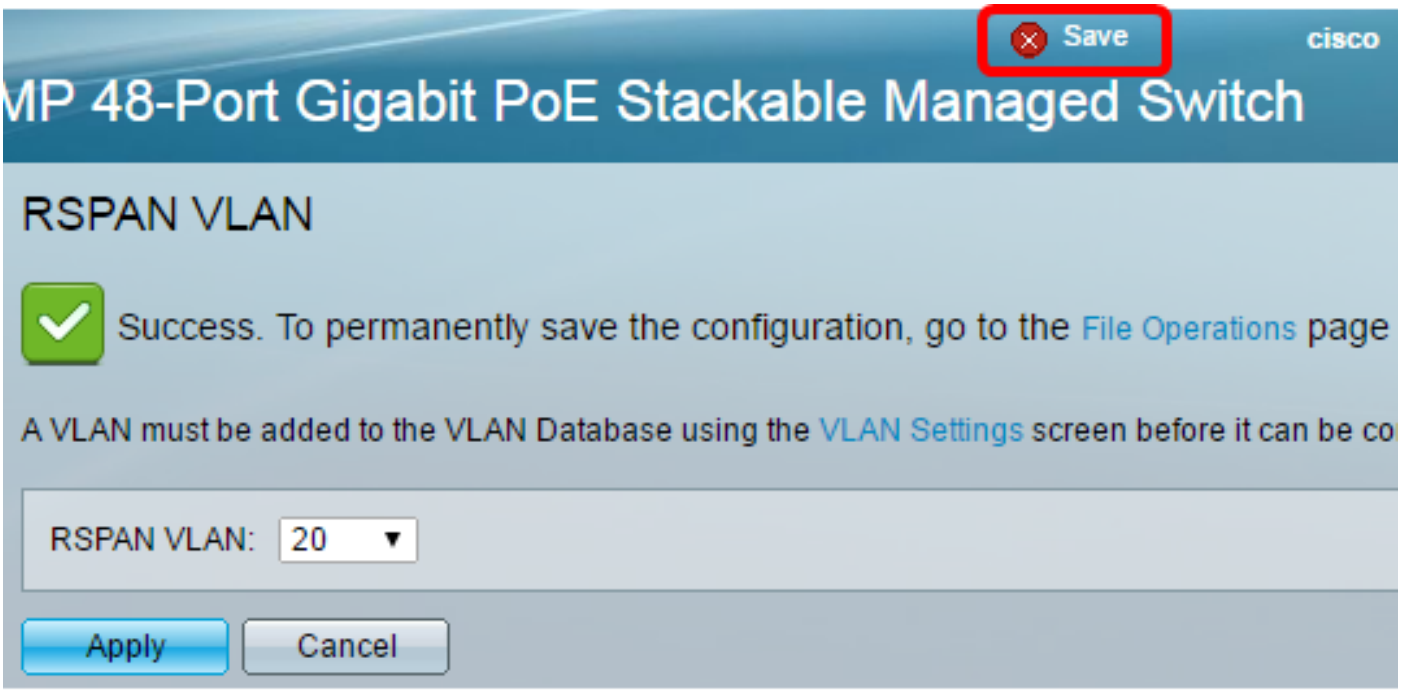


注意：在本示例中，选择VLAN 20。

步骤12.单击“**应用**”。



步骤13.（可选）单击“保**存**”更新运行配置文件。

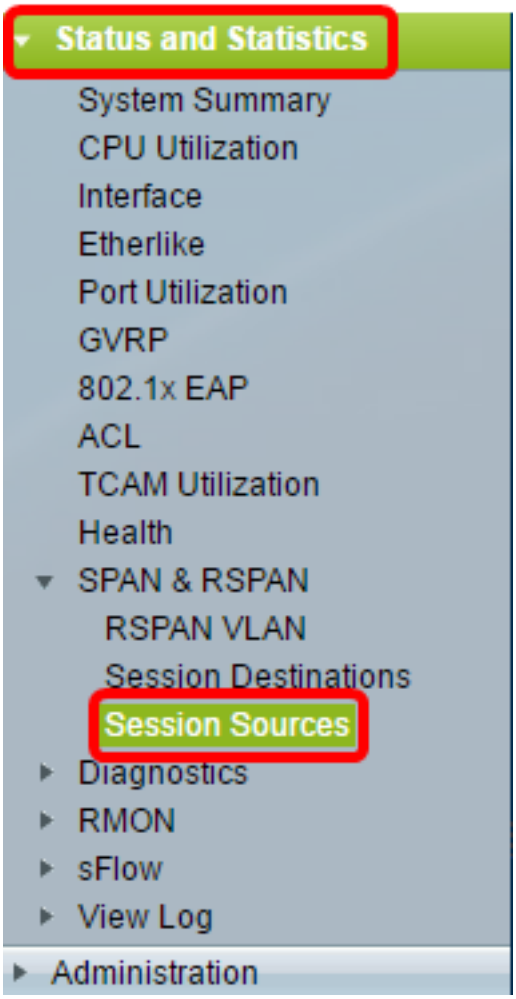


步骤14.在最终交换机中，重复步骤1至13以配置RSPAN VLAN。

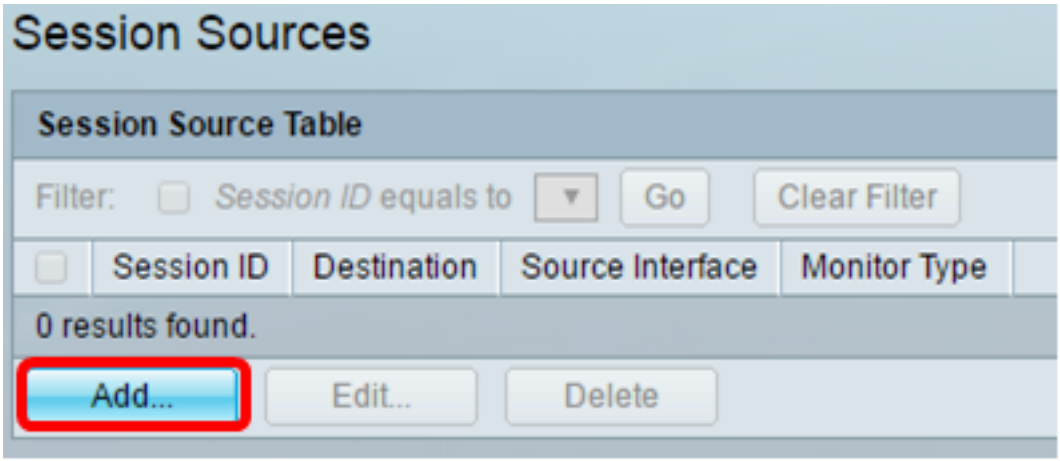
现在，您应该已在开始和最终交换机上配置了专用于RSPAN会话的VLAN。

在启动交换机上配置会话源

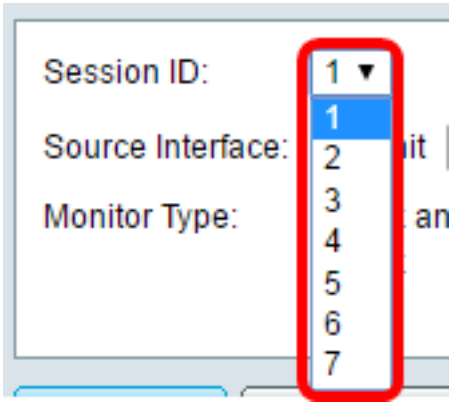
步骤1.选择状**态和统计> SPAN & RSPAN >会话源**。



步骤2.单击“添**加**”。



步骤3.从Session ID下拉列表中选择会话编号。每个RSPAN会话的会话ID必须一致。



注意：在本例中，选择会话1。

步骤4.点击所需源接口类型的单选按钮，然后从下拉列表或列表中选择接口。

重要信息：源接口不能与目标端口相同。

选项有：

- 设备和端口 — 您可以从设备下拉列表中选择所需的选项，并从端口下拉列表中选择要设置为源端口的端口。
- VLAN — 您可以从VLAN下拉列表中选择要监控的所需VLAN。VLAN帮助一组主机通信，就像它们位于同一物理网络一样，无论它们位于何处。如果选择此选项，则无法编辑。
- 远程VLAN — 这将显示已定义的RSPAN VLAN。如果选择此选项，则无法编辑。

注意：在本例中，选择单元1中的端口GE2。这是要监控的远程接口。

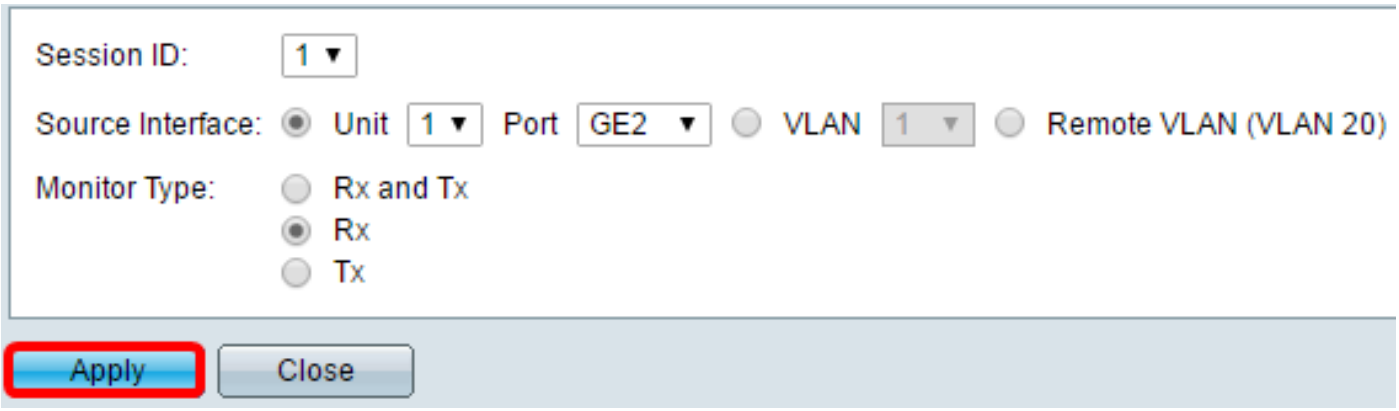
第5步。（可选）如果在第4步中单击了Unit and Port，请点击要监控的流量类型所需的Monitor Type单选按钮。

选项有：

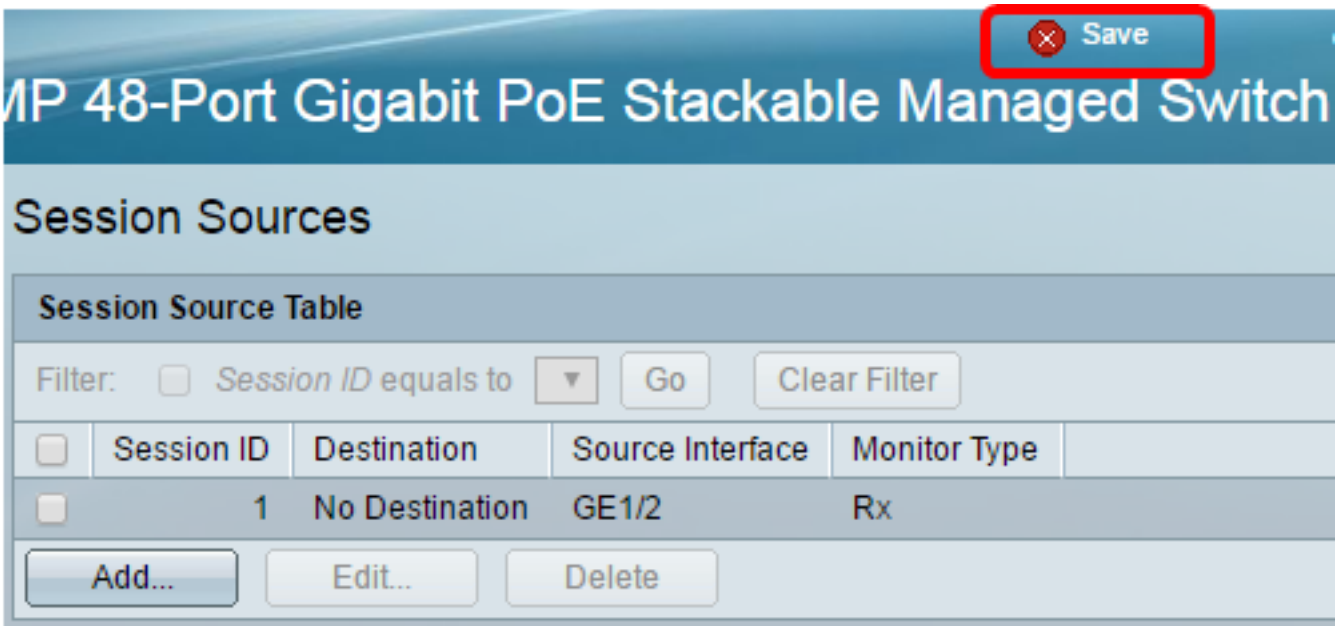
- Rx和Tx — 此选项允许对传入和传出数据包进行端口镜像。默认情况下选择此选项。
- Rx — 此选项允许对传入数据包进行端口镜像。
- Tx — 此选项允许对传出数据包进行端口镜像。

注意：在本例中，选择Rx。

步骤6.单击“应用”，然后单击“**关闭**”。



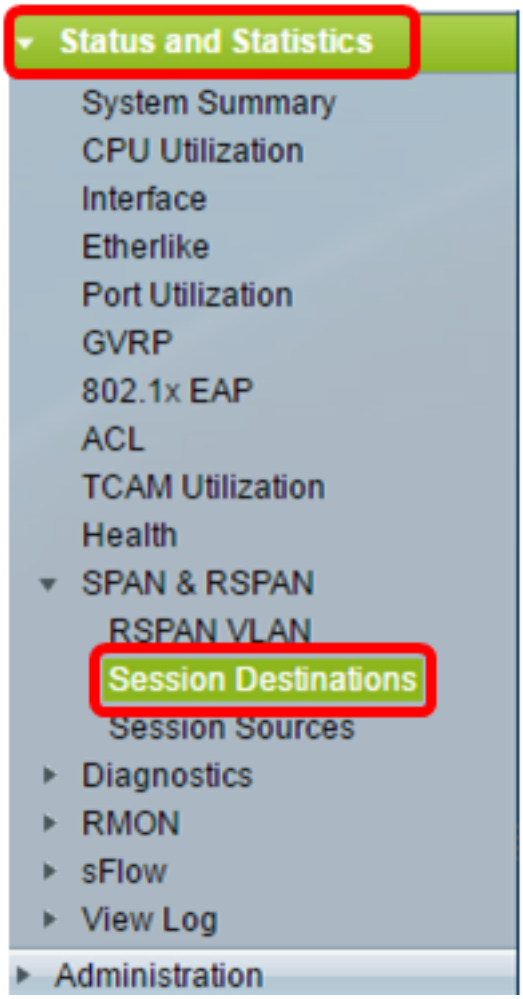
步骤7.（可选）单击“保**存**”更新运行配置文件。



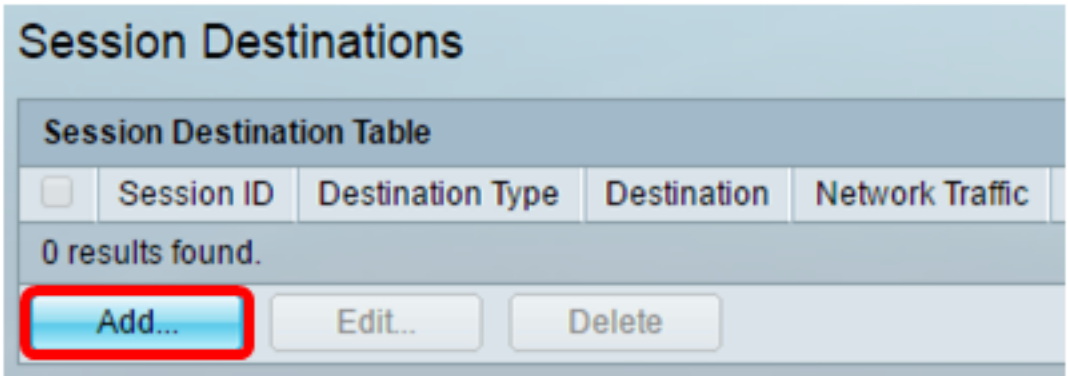
现在，您应该已在启动交换机上配置了会话源。

在启动交换机上配置会话目标

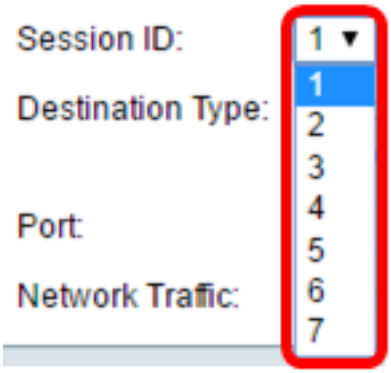
步骤1.选择状**态和统计> SPAN & RSPAN >会话目标**。



步骤2.单击“添**加**”。



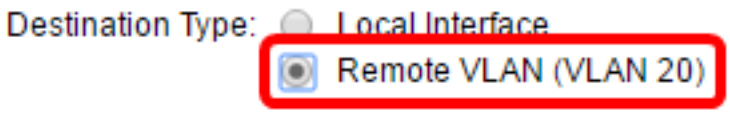
步骤3.从Session ID下拉列表中选择会话编号。它必须与从已配置会话源中选择的ID相同。



注意：在本例中，选择会话1。

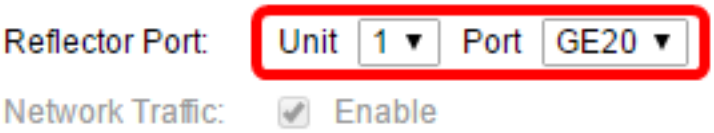
步骤4.从Destination Type区域**单击Remote VLAN**单选按钮。网络分析器（如运行Wireshark的计算机）连接到此端口。

重要信息：目标接口不能与源端口相同。



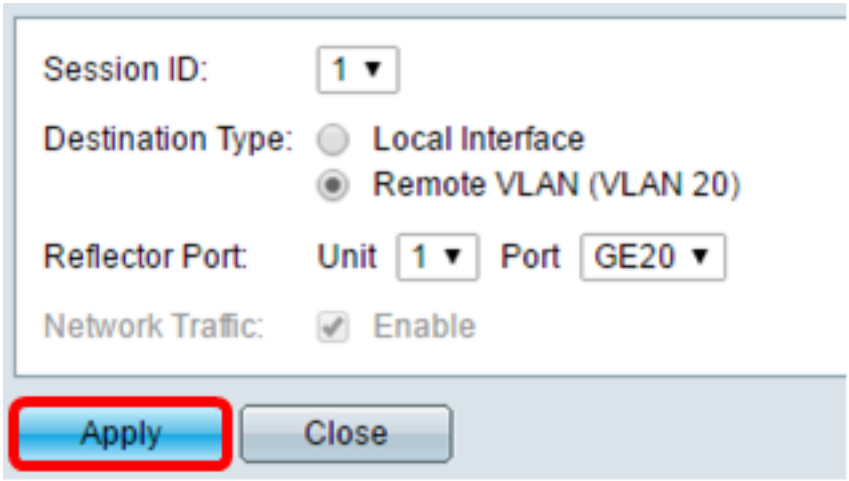
注意：如果选择远程VLAN，则自动启用网络流量。

步骤5.在Reflector Port区域，从Unit下拉列表中选择所需的选项。从Port下拉列表中选择要设置为源端口的端口。

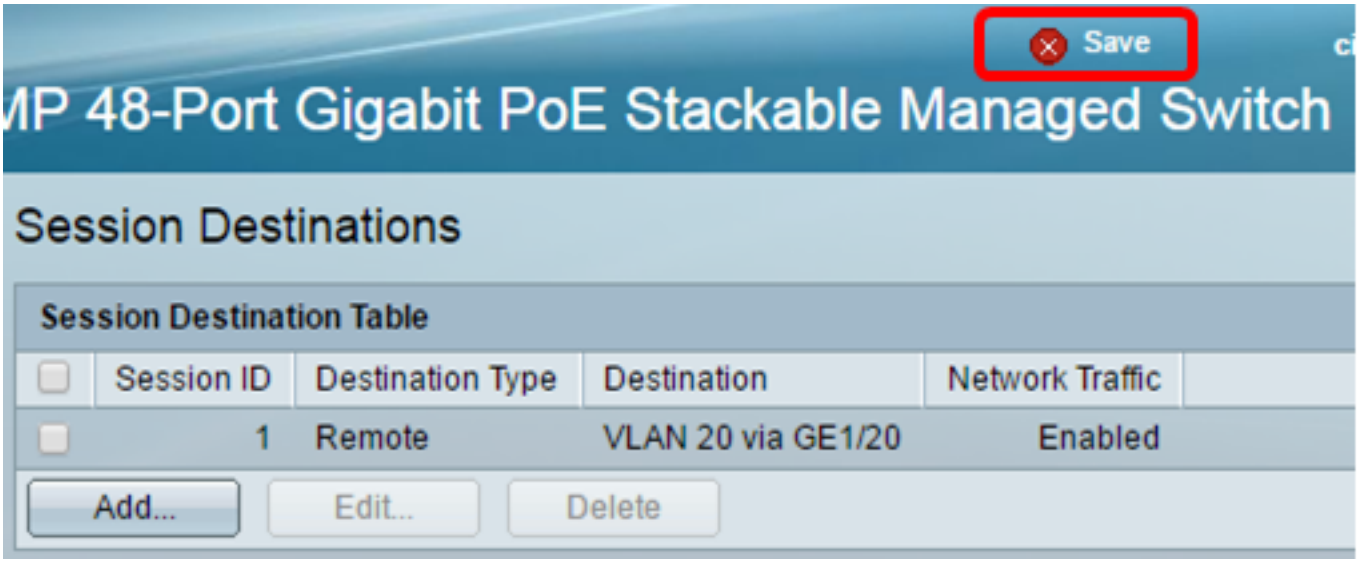


注意：在本示例中，选择单元1中的端口GE20。

步骤6.单击“应用”，然后单击“**关闭**”。



步骤7.（可选）单击“保**存**”更新运行配置文件。



现在，您应该已在启动交换机上配置了会话目标。

中间交换机

还可以有中间交换机将RSPAN源会话和目的会话分隔开。这些交换机不需要能够运行RSPAN，但必须响应RSPAN VLAN的要求。

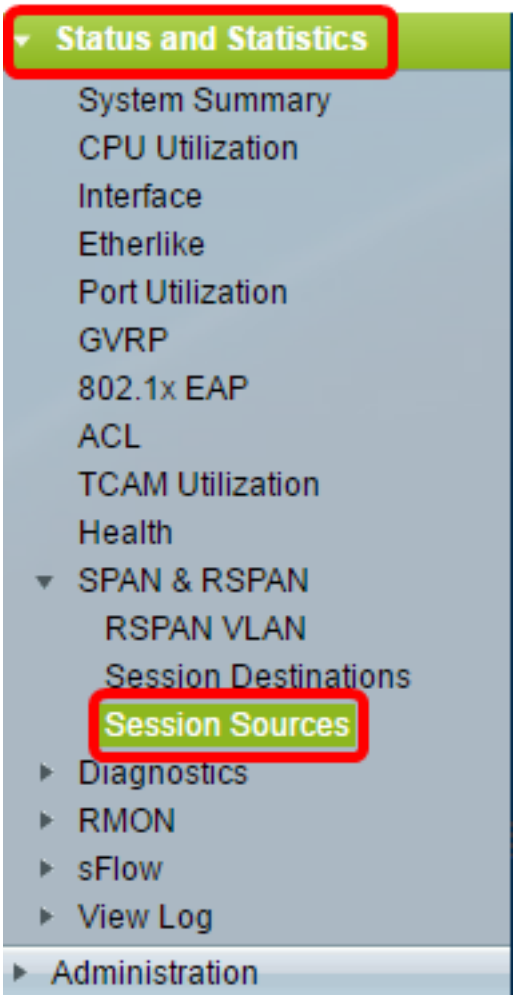
对于VLAN中继协议(VTP)可见的VLAN 1到1005,VLAN ID及其关联的RSPAN特征通过VTP传播。如果在扩展VLAN范围（1006到4094）中分配RSPAN VLAN ID，则必须手动配置所有中间交换机。

要了解如何将接口VLAN分配为中间交换机的中继端口，请单击此处获取说明。

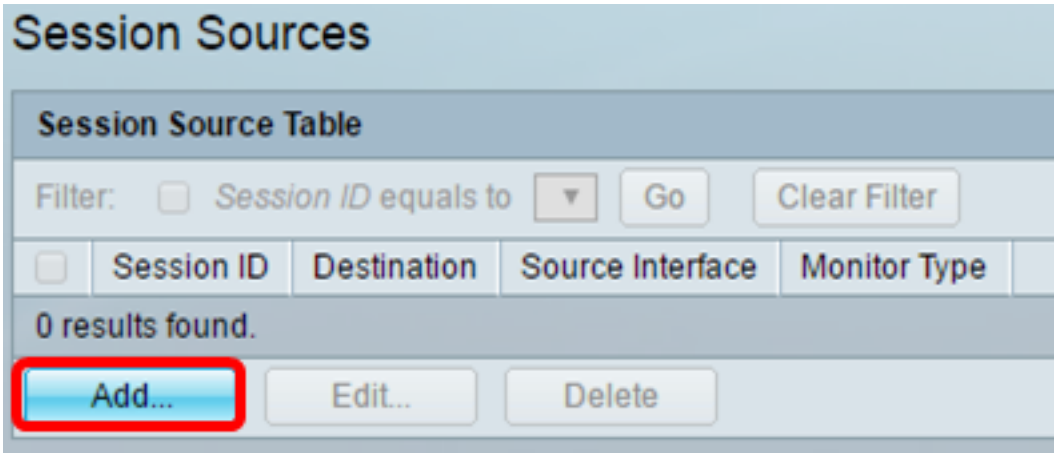
在网络中同时有多个RSPAN VLAN和每个RSPAN VLAN定义网络范围的RSPAN会话是正常的。即，网络中任意位置的多个RSPAN源会话可以为RSPAN会话提供数据包。还可以在整个网络中有多个RSPAN目标会话，监控相同的RSPAN VLAN并向用户呈现流量。RSPAN VLAN ID分隔会话。

在最终交换机上配置会话源

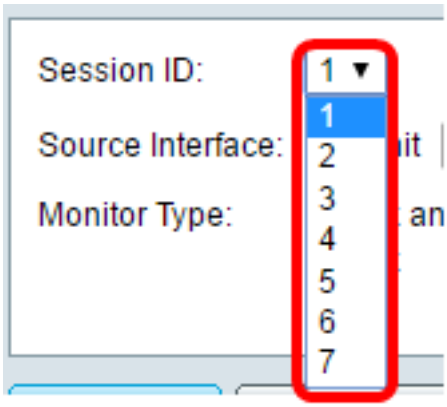
步骤1.选择状**态和统计> SPAN & RSPAN >会话源**。



步骤2.单击“添**加”**。

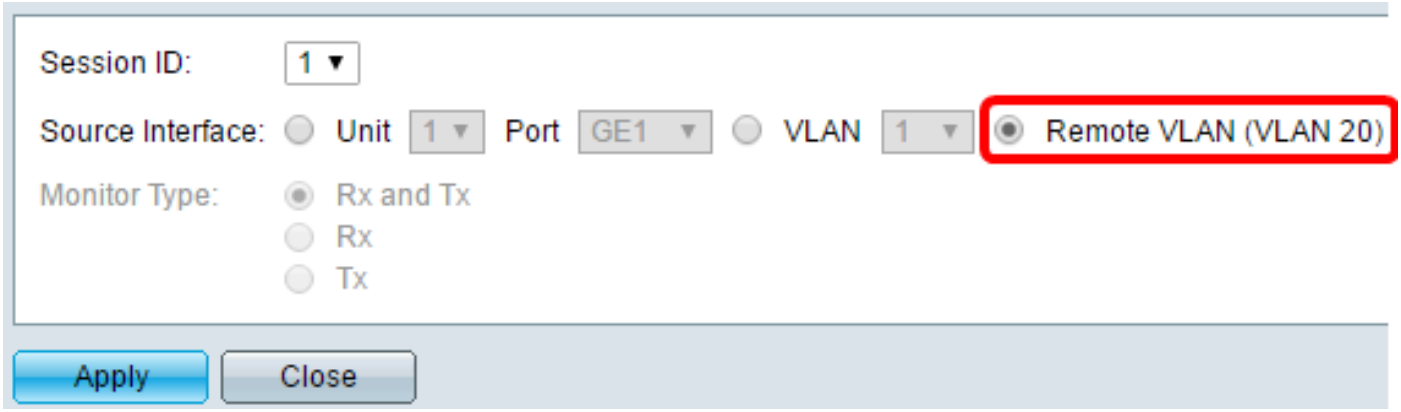


步骤3.（可选）从Session ID下拉列表中选择会话编号。每个会话的会话ID必须一致。



注意：在本例中，选择会话1。

步骤4.从Source Interface区域**单击Remote VLAN**单选按钮。



注意：将自动配置远程VLAN的监控类型。

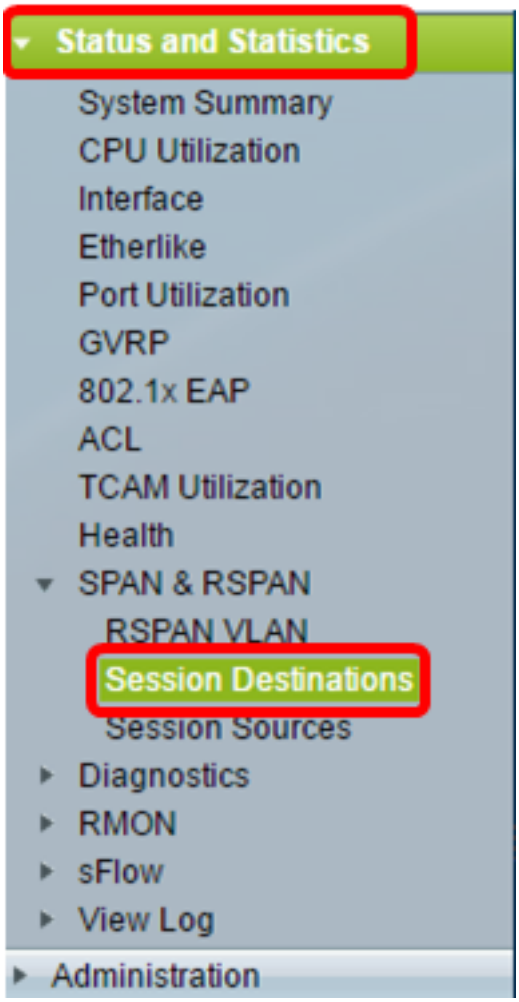
步骤5.单击“应用”，然后单击“**关闭**”。

步骤6.（可选）单击“保**存**”更新运行配置文件。

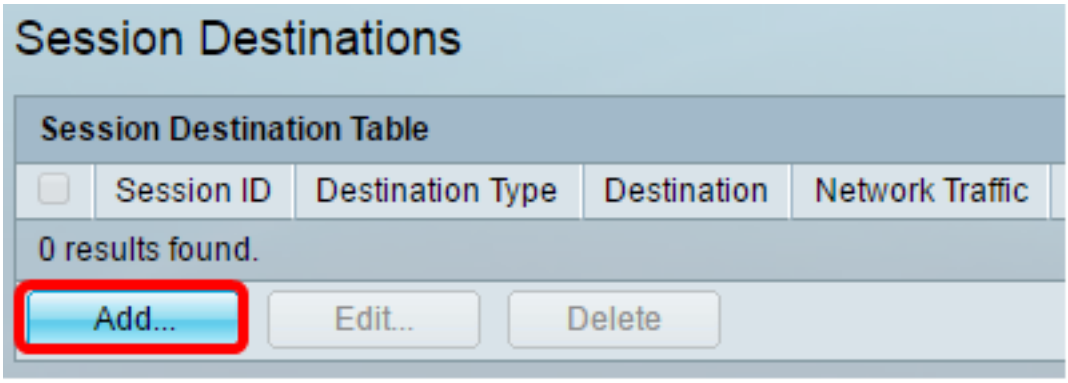
现在，您应该已在最终交换机上配置了会话源。

在最终交换机上配置会话目标

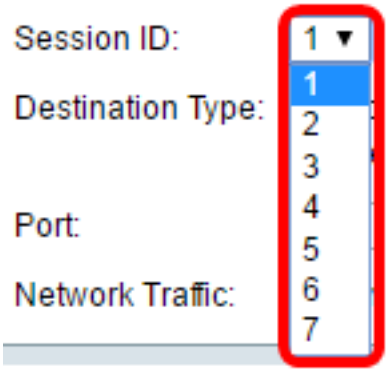
步骤1.选择状**态和统计> SPAN & RSPAN >会话目标。**



步骤2.单击“添**加”。**

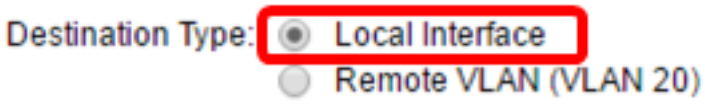


步骤3.从Session ID下拉列表中选择会话编号。它必须与从已配置会话源中选择的ID相同。

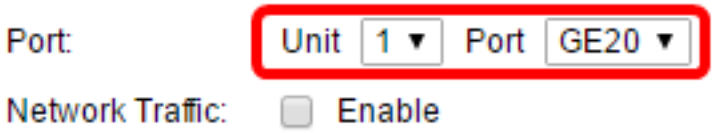


注意：在本例中，选择会话1。

步骤4.从Destination Type区**域单击**Local Interface单选按钮。

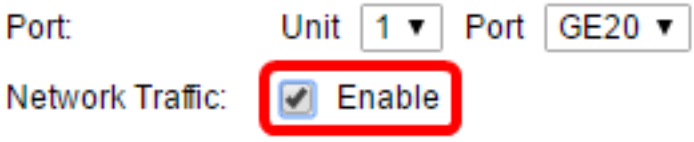


步骤5.在Port区域，从Unit下拉列表中选择所需的选项。从Port下拉列表中选择要设置为源端口的端口。



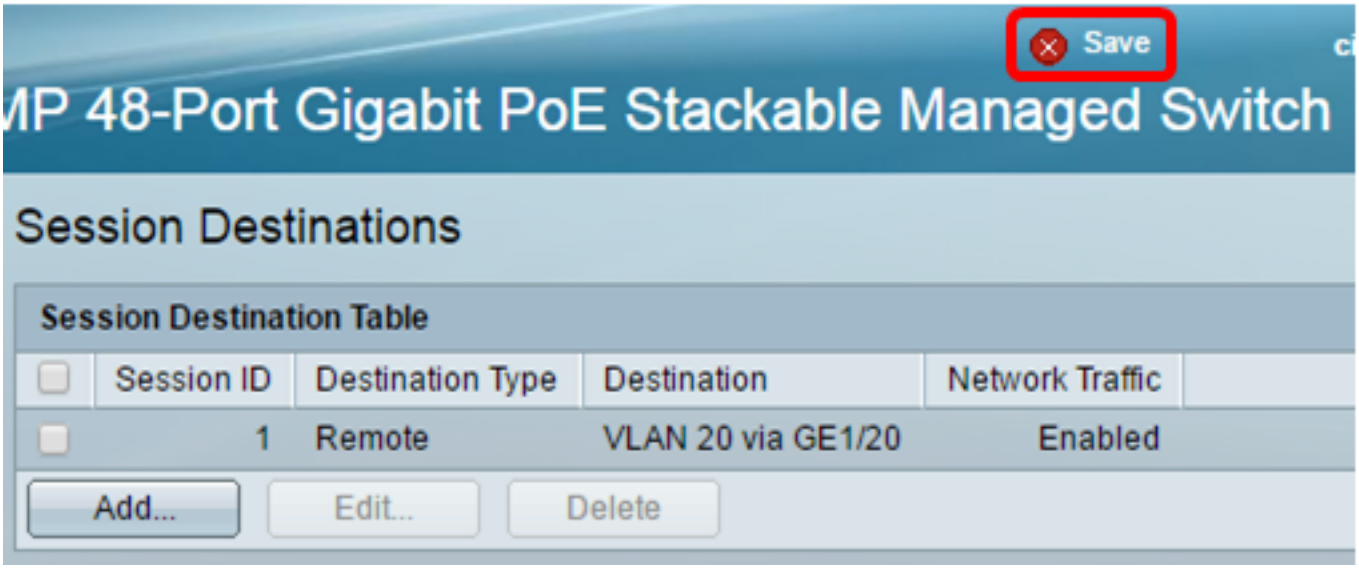
注意：在本示例中，选择单元1中的端口GE20。

步骤6.（可选）选中**Enable** Network Traffic复选框以启用网络流量。



步骤7.单击“应用”，然后单击“**关闭**”。

步骤8.（可选）单击“保**存**”更新运行配置文件。

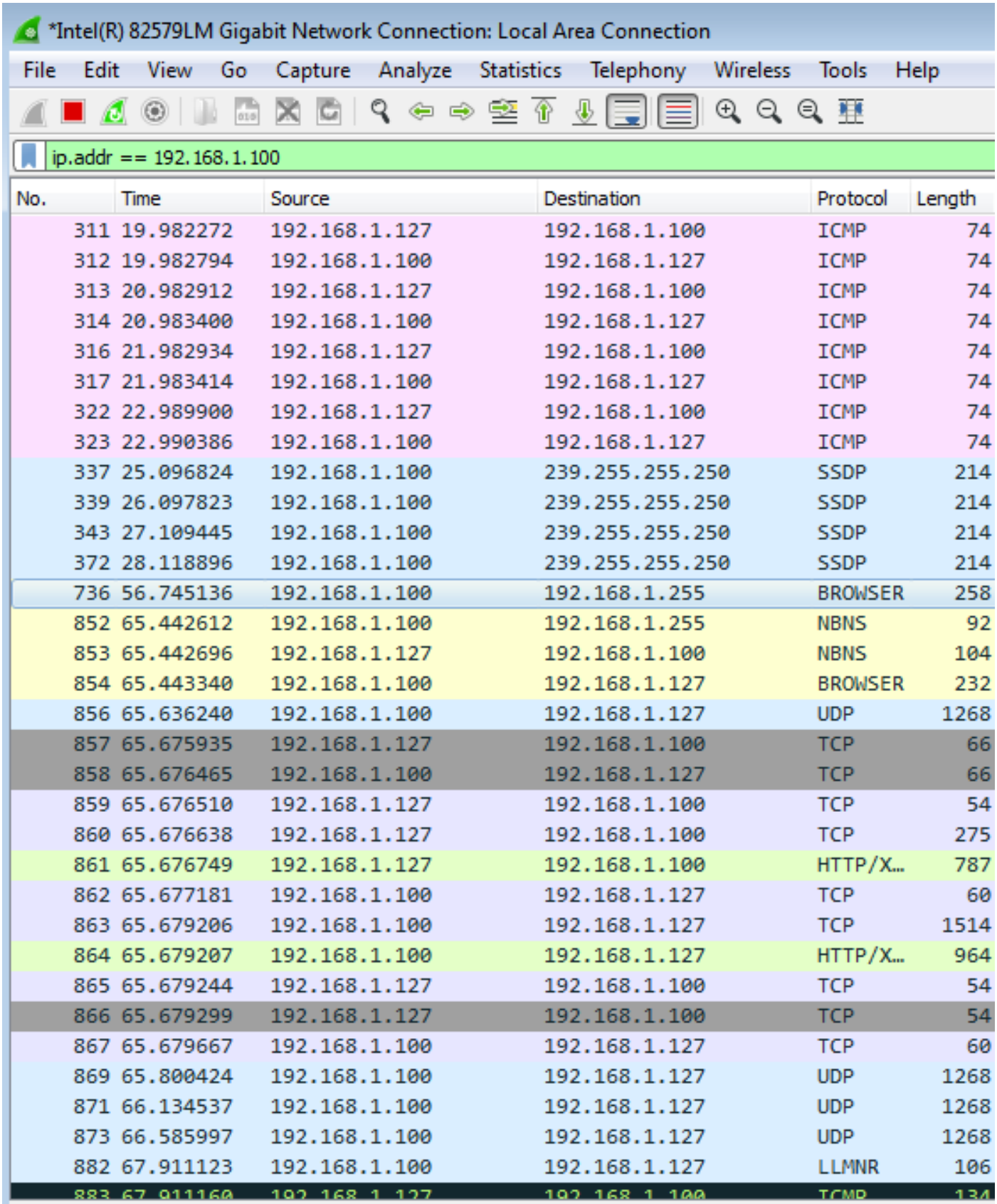


现在，您应该已在最终交换机上配置会话目标。

分析WireShark中捕获的RSPAN VLAN数据包

在此场景中，配置的源接口（单元1中的GE2）中的主机(GE1/2)的IP地址为192.168.1.100。而配置的目标接口（单元1中的GE20）中的主机（通过GE1/20的VLAN 20）的IP地址为地址192.168.1.127。Wireshark正在连接到此端口的主机中运行。

使用过滤器ip.addr == 192.168.1.100,Wireshark显示从远程源接口捕获的数据包。



查看与本文相关的视频……

[单击此处查看思科提供的其他技术讲座]