Configure Remote Switch Port Analyzer (RSPAN) Settings on the Network

Table of Contents

Objective

This article provides instructions on how you can configure RSPAN on your switches.

Applicable Devices | Firmware Version

- Sx350 | 2.2.5.68 (Download latest)
- SG350X | 2.2.5.68 (Download latest)
- Sx550X | 2.2.5.68 (Download latest)

Introduction

Switch Port Analyzer (SPAN), or sometimes called port mirroring or port monitoring, chooses network traffic for analysis by a network analyzer. The network analyzer can be a Cisco SwitchProbe device or other Remote Monitoring (RMON) probe.

Port mirroring is used on a network device to send a copy of network packets seen on a single device port, multiple device ports, or an entire Virtual Local Area Network (VLAN) to a network monitoring connection on another port on the device. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system. A network analyzer connected to the monitoring port processes the data packets for diagnosing, debugging, and performance monitoring.

Remote Switch Port Analyzer (RSPAN) is an extension of SPAN. RSPAN extends SPAN by enabling monitoring of multiple switches across your network and allowing the analyzer port to be defined on a remote switch. This means that you can centralize your network capture devices.

RSPAN works by mirroring the traffic from the source ports of an RSPAN session onto a VLAN that is dedicated for the RSPAN session. This VLAN is then trunked to other switches, allowing the RSPAN session traffic to be transported across multiple switches. On the switch that contains the destination port for the session, traffic from the RSPAN session VLAN is simply mirrored out the destination port.

RSPAN Traffic Flow

- The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches.
- The traffic from the source interfaces on the start device is copied to the RSPAN VLAN through a reflector port. This is a physical port that has to be set. It is used exclusively to build an RSPAN session.
- This reflector port is the mechanism that copies packets to an RSPAN VLAN. It forwards only the traffic from the RSPAN source session with which it is affiliated. Any device connected to a port set as a reflector port loses connectivity until the RSPAN source session is disabled.
- RSPAN traffic is then forwarded over trunk ports on the intermediate devices to the destination session on the final switch.
- The destination switch monitors the RSPAN VLAN and copies it to a destination port.

RSPAN Port Membership Rules

- On all switches — Membership in RSPAN VLAN can be tagged only.
- Start Switch

– SPAN source interfaces cannot be members of RSPAN VLAN.

– Reflector port cannot be a member of this VLAN.

– It is recommended that the remote VLAN does not have any memberships.

- Intermediate Switch

– It is recommended to remove RSPAN membership from all ports not used for passing mirrored traffic.

– Usually, an RSPAN remote VLAN contains two ports.

- Final Switch

– For mirrored traffic, source ports must be members of RSPAN VLAN.

– It is recommended to remove RSPAN membership from all other ports, including the destination interface.

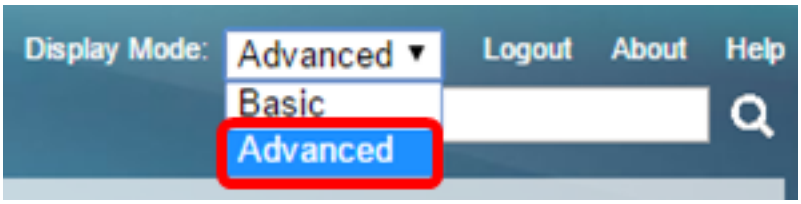
Configure RSPAN on the Network

Configure RSPAN VLAN on the Switch

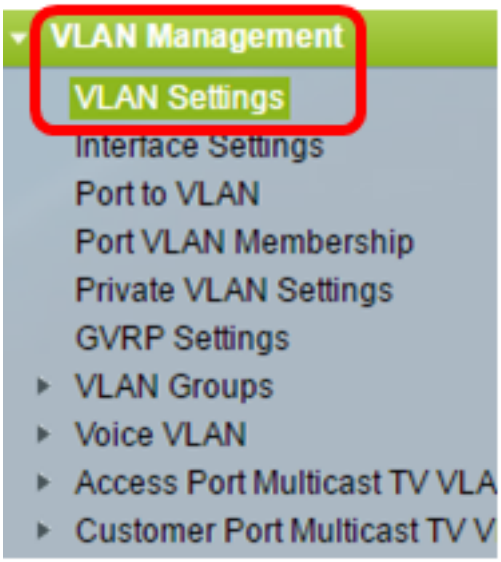
The RSPAN VLAN carries SPAN traffic between RSPAN source and destination sessions. It has these special characteristics:

- All traffic in the RSPAN VLAN is always flooded.
- No Media Access Control (MAC) address learning occurs on the RSPAN VLAN.
- RSPAN VLAN traffic only flows on trunk ports.
- STP can run on RSPAN VLAN trunks but not on SPAN destination ports.
- RSPAN VLANs must be configured on both Start and Final switches in VLAN configuration mode by using the **remote-span** VLAN configuration mode command, or follow the instructions below:

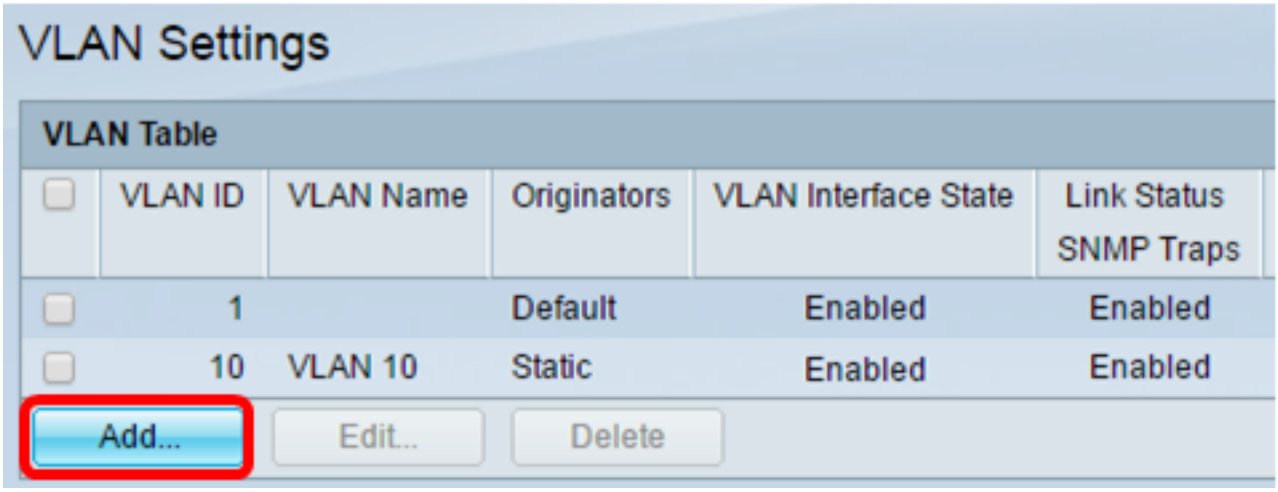
Step 1. Log in to the web-based utility of the Start Switch and choose **Advanced** in the Display Mode drop-down list.



Step 2. Choose **VLAN Management > VLAN Settings**.



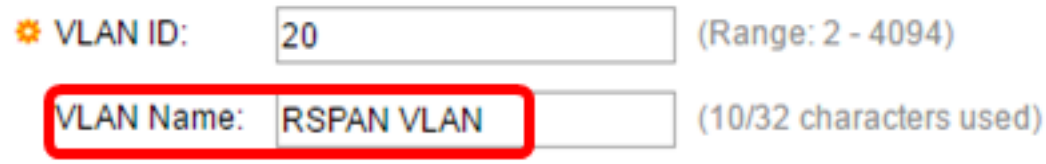
Step 3. Click **Add**.



Step 4. Enter the VLAN ID in the *VLAN ID* field.

Note: In this example, VLAN 20 is used as the VLAN ID.

Step 5. (Optional) Enter the VLAN Name in the *VLAN Name* field.

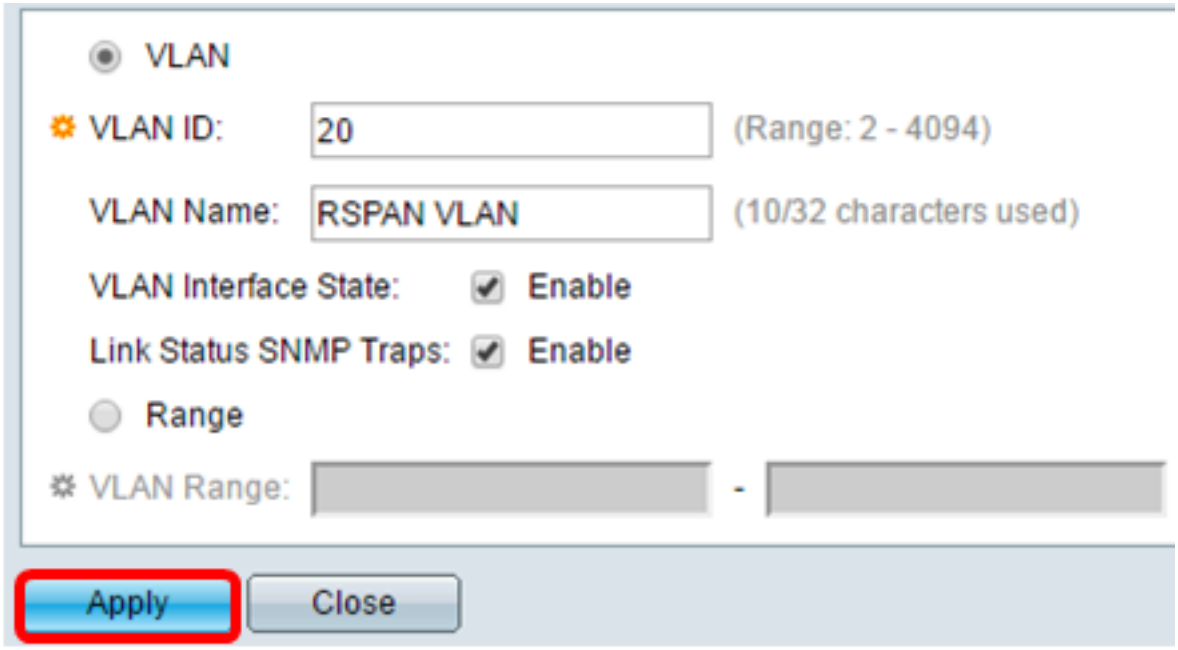


Note: In this example, RSPAN VLAN is used as the VLAN name.

Step 6. (Optional) Check the VLAN Interface State check box to enable the VLAN. If the VLAN is shutdown, the VLAN does not transmit or receive messages from or to higher levels. For example, if you shut down a VLAN, on which an IP interface is configured, bridging into the VLAN continues, but the switch cannot transmit and receive IP traffic on the VLAN. This feature is enabled by default.

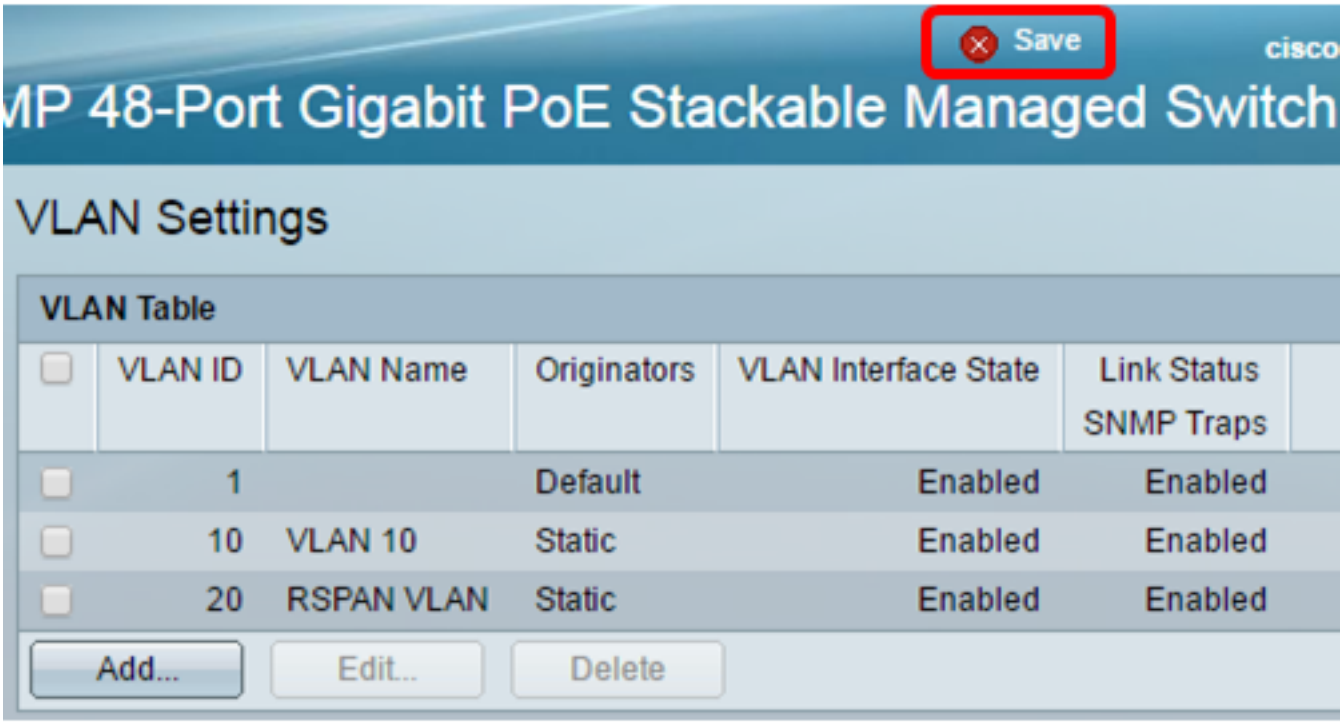
Step 7. (Optional) Check the Link Status SNMP Traps check box to enable link status generation of Simple Network Management Protocol (SNMP) traps. This feature is enabled by default.

Step 8. Click **Apply** then click **Close**.



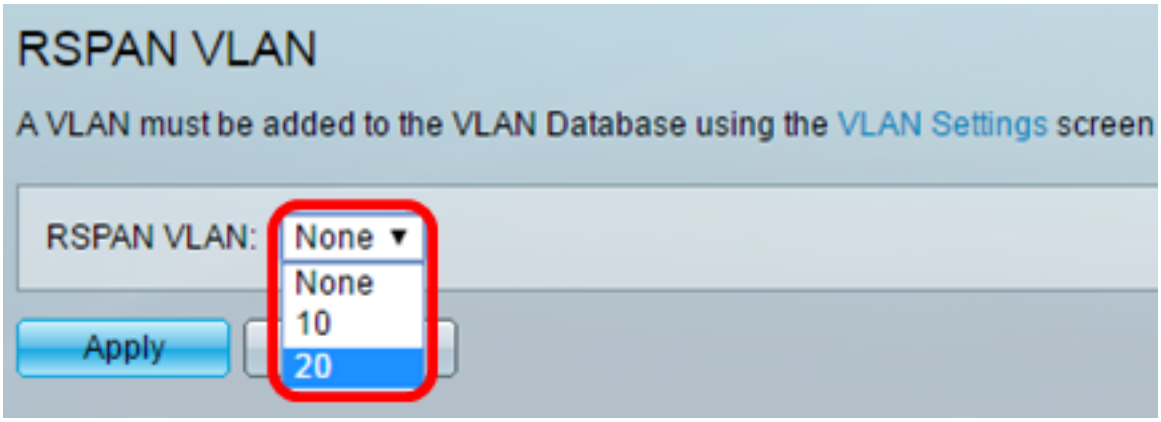
Note: To learn more about managing VLANs on a switch, click here.

Step 9. (Optional) Click **Save** to update the running configuration file.



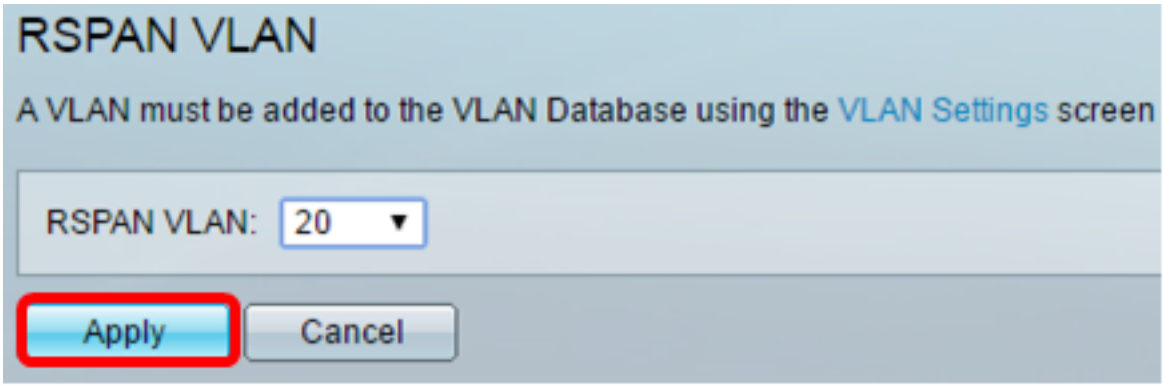
Step 10. Choose **Status and Statistics > SPAN & RSPAN > RSPAN VLAN**.

Step 11. Choose a VLAN ID from the RSPAN VLAN drop-down list. This VLAN should be exclusively used for RSPAN.

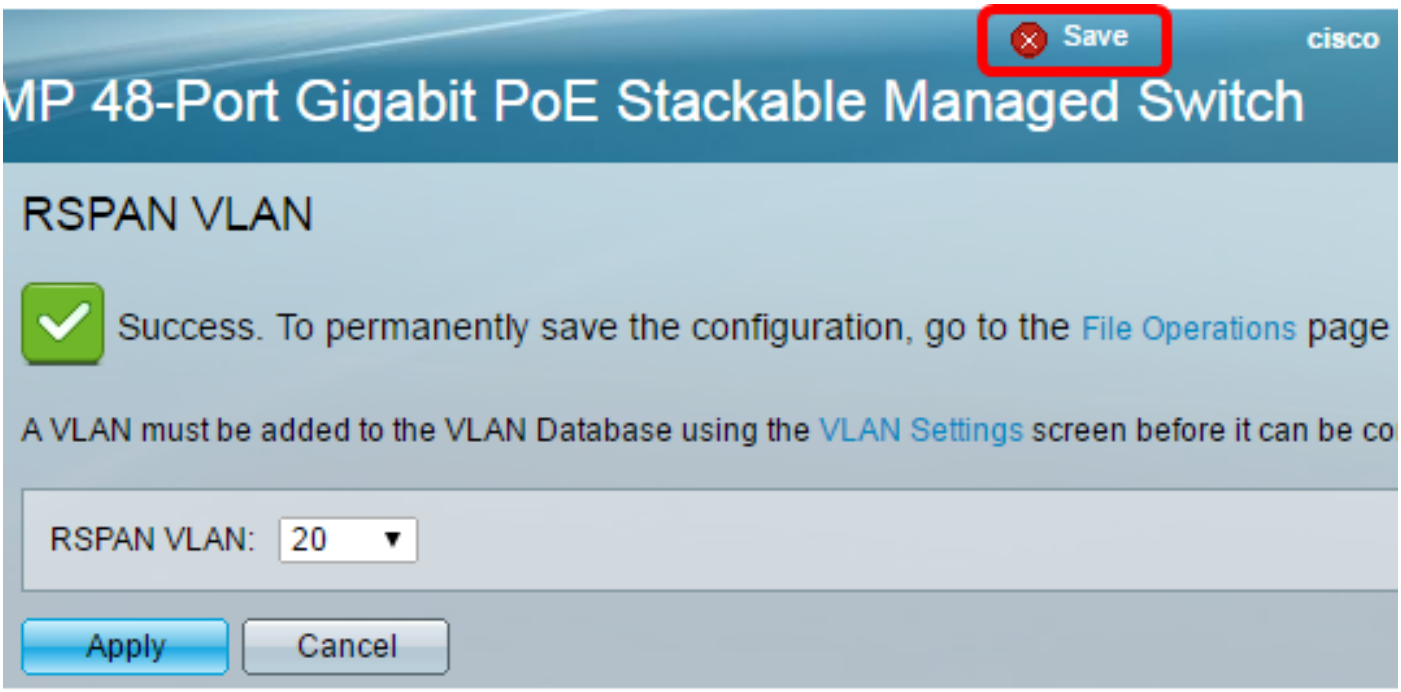


Note: In this example, VLAN 20 is chosen.

Step 12. Click **Apply**.



Step 13. (Optional) Click **Save** to update the running configuration file.

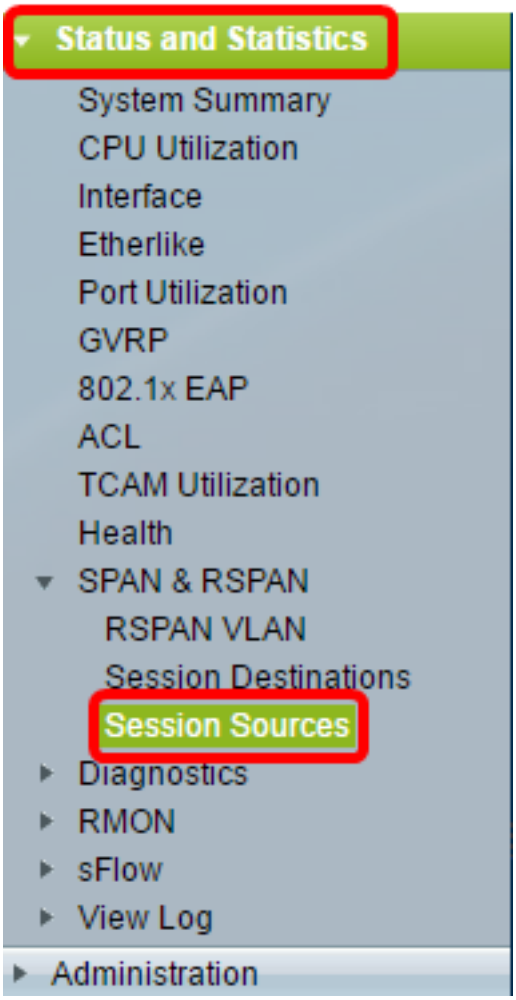


Step 14. In the Final Switch, repeat steps 1 to 13 to configure RSPAN VLAN.

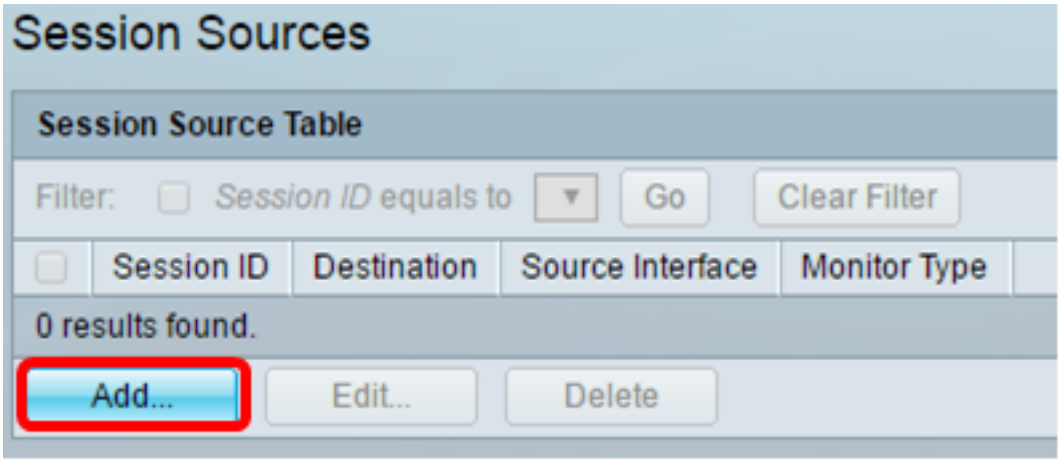
You should now have configured the VLAN that is dedicated to the RSPAN session on both Start and Final Switches.

Configure Session Sources on a Start Switch

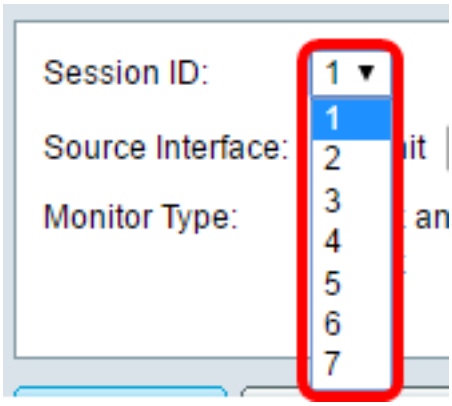
Step 1. Choose **Status and Statistics > SPAN & RSPAN > Session Sources**.



Step 2. Click **Add**.



Step 3. Choose the session number from the Session ID drop-down list. Session ID must be consistent per RSPAN session.



Note: In this example, Session 1 is chosen.

Step 4. Click the radio button for the desired source interface type, and choose the interface from the drop-down list or lists.

Important: The Source Interface cannot be the same as the Destination Port.

The options are:

- Unit and Port — You can choose the desired option from the Unit drop-down list and choose which port to set as the source port from the Port drop-down list.
- VLAN — You can choose the desired VLAN to monitor from the VLAN drop-down list. A VLAN helps a group of hosts to communicate as if they are on the same physical network, regardless of their location. If this option is chosen, it could not be edited.
- Remote VLAN — This will display the defined RSPAN VLAN. If this option is chosen, it could not be edited.

Note: In this example, port GE2 in Unit 1 is chosen. This is the remote interface that would be monitored.

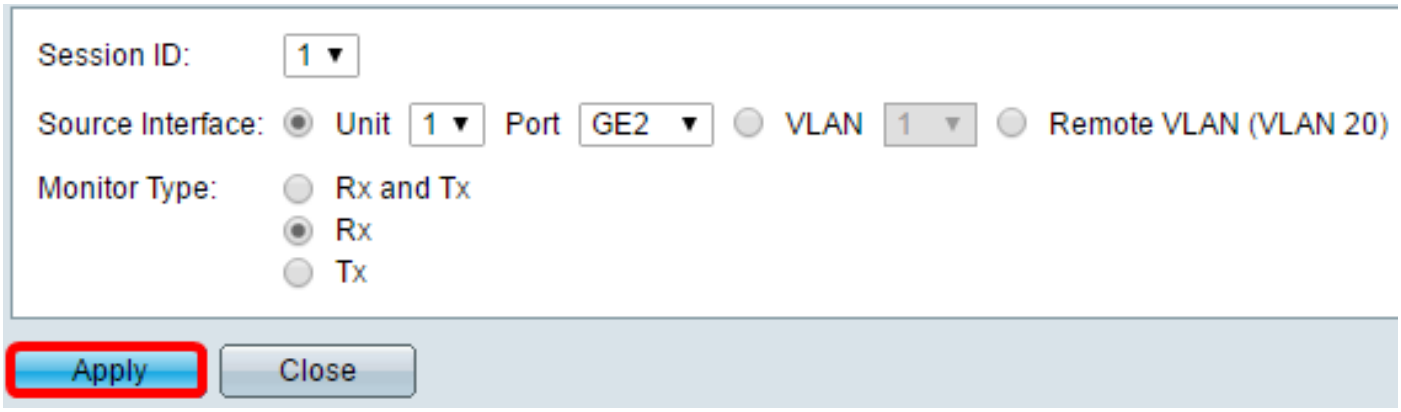
Step 5. (Optional) If Unit and Port are clicked in Step 4, click the desired Monitor Type radio button for the type of traffic to monitor.

The options are:

- Rx and Tx — This option allows port mirroring of incoming and outgoing packets. This option is chosen by default.
- Rx — This option allows port mirroring of incoming packets.
- Tx — This option allows port mirroring of outgoing packets.

Note: In this example, Rx is chosen.

Step 6. Click **Apply** then click **Close**.

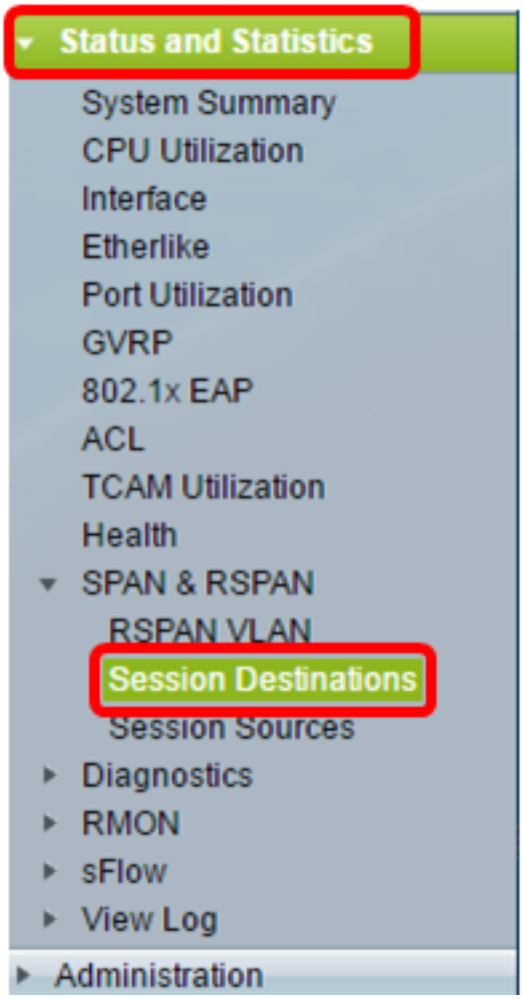


Step 7. (Optional) Click **Save** to update the running configuration file.

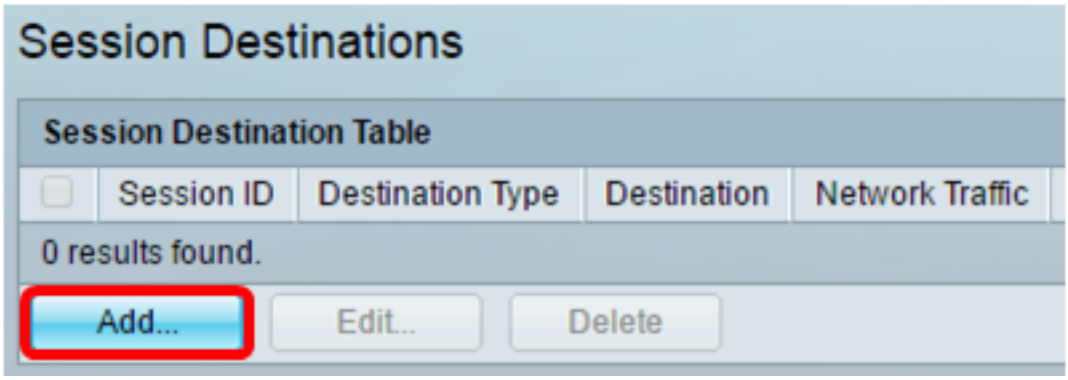
You should now have configured the session source on your Start Switch.

Configure Session Destinations on a Start Switch

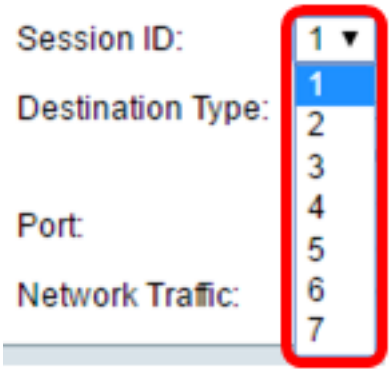
Step 1. Choose **Status and Statistics > SPAN & RSPAN > Session Destinations**.



Step 2. Click **Add**.



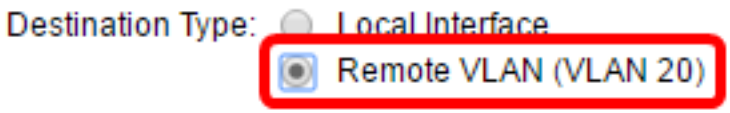
Step 3. Choose the session number from the Session ID drop-down list. It must be the same as the chosen ID from the configured session source.



Note: In this example, Session 1 is chosen.

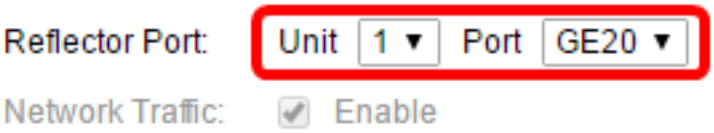
Step 4. Click the **Remote VLAN** radio button from the Destination Type area. A network analyzer, such as a computer running Wireshark, is connected to this port.

Important: The Destination Interface cannot be the same as the Source Port.



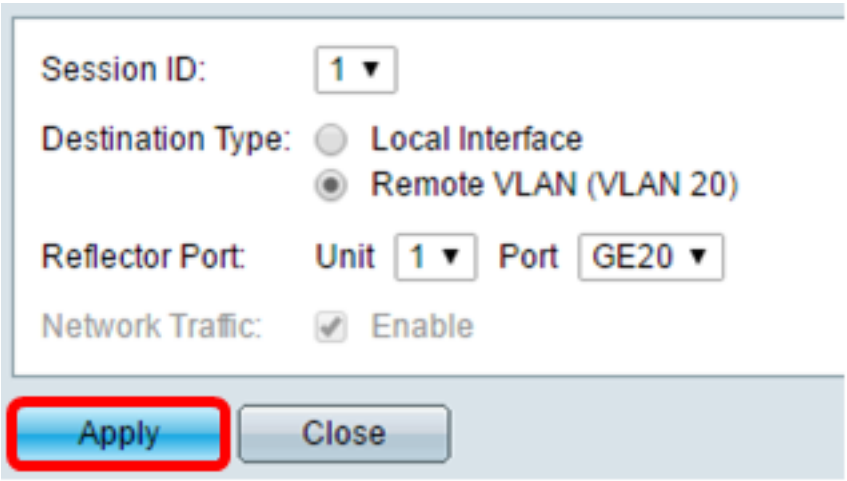
Note: If Remote VLAN is chosen, the Network Traffic is automatically enabled.

Step 5. In the Reflector Port area, choose the desired option from the Unit drop-down list. Choose which port to set as the source port from the Port drop-down list.

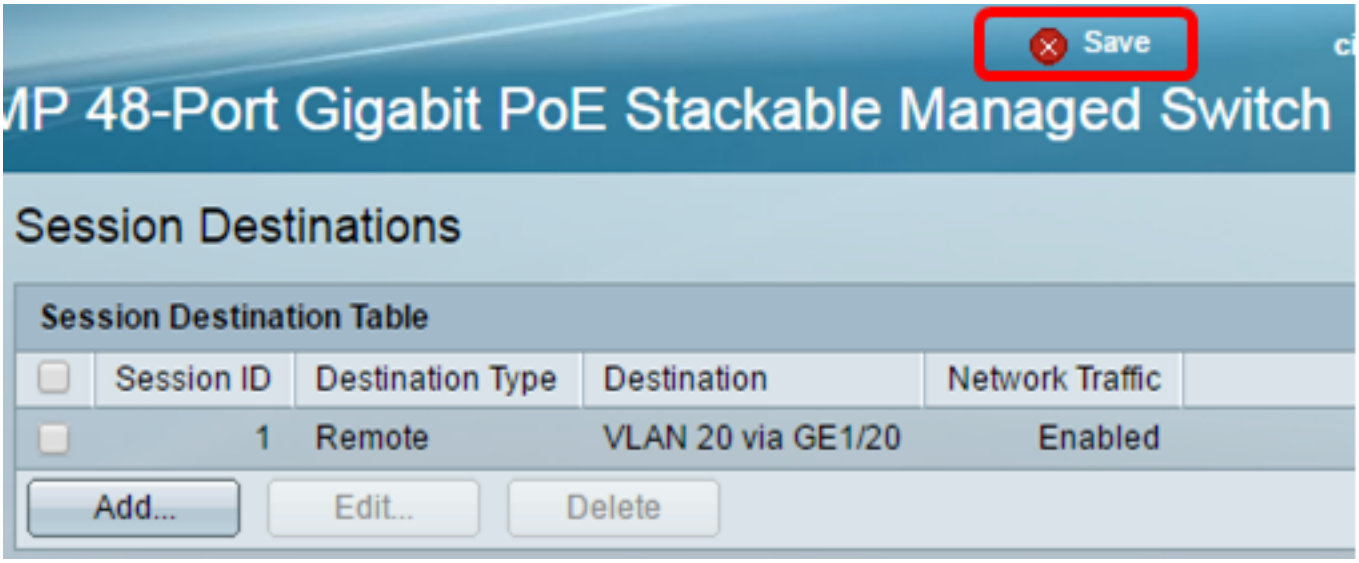


Note: In this example, port GE20 in Unit 1 is chosen.

Step 6. Click **Apply** then click **Close**.



Step 7. (Optional) Click **Save** to update the running configuration file.



You should now have configured the session destinations on your Start Switch.

Intermediate Switches

There can also be intermediate switches separating the RSPAN source and destination sessions. These switches need not be capable of running RSPAN, but they must respond to the requirements of the RSPAN VLAN.

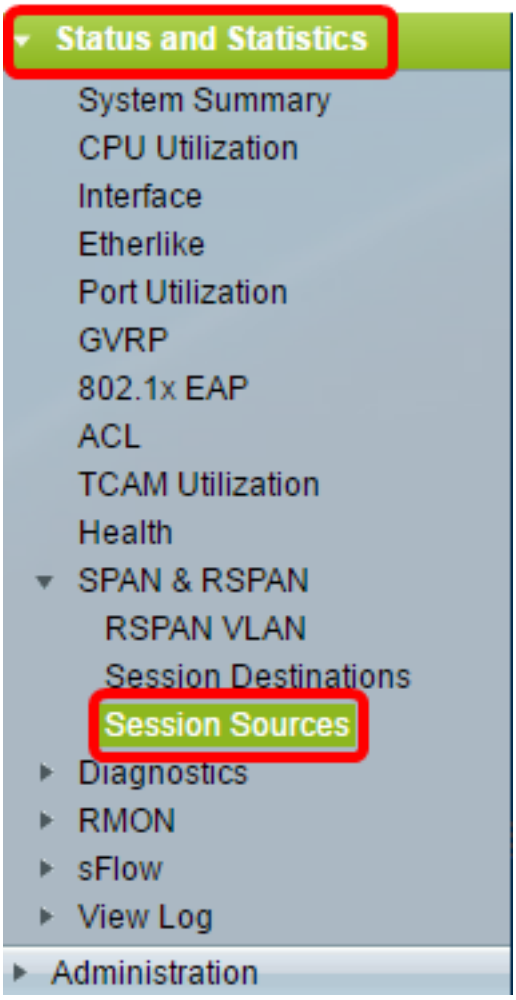
For VLANs 1 to 1005 that are visible to VLAN Trunking Protocol (VTP), the VLAN ID and its associated RSPAN characteristics are propagated by VTP. If you assign an RSPAN VLAN ID in the extended VLAN range (1006 to 4094), you must manually configure all intermediate switches.

To learn how to assign an interface VLAN as a trunk port of an intermediate switch, click here for instructions.

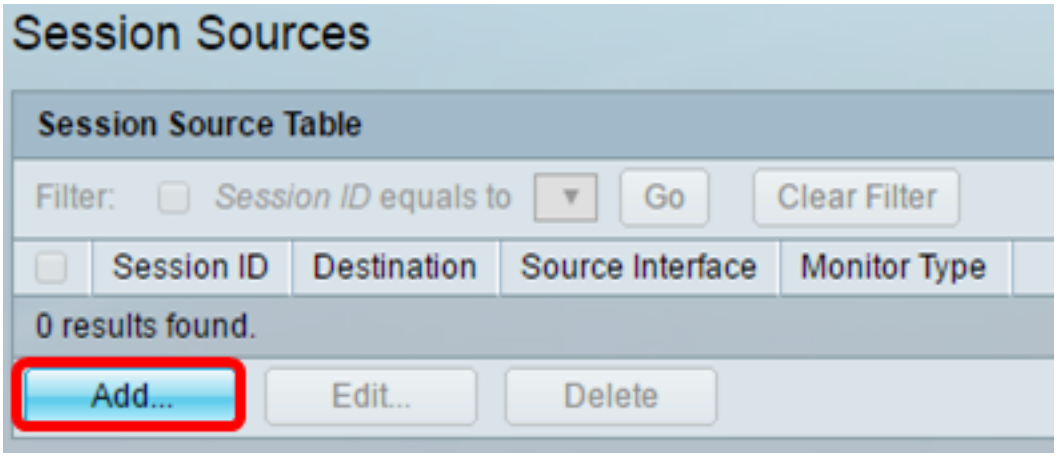
It is normal to have multiple RSPAN VLANs in a network at the same time with each RSPAN VLAN defining a network-wide RSPAN session. That is, multiple RSPAN source sessions anywhere in the network can contribute packets to the RSPAN session. It is also possible to have multiple RSPAN destination sessions throughout the network, monitoring the same RSPAN VLAN and presenting traffic to the user. The RSPAN VLAN ID separates the sessions.

Configure Session Sources on a Final Switch

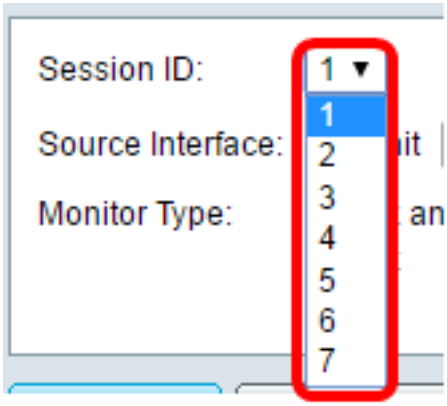
Step 1. Choose **Status and Statistics > SPAN & RSPAN > Session Sources**.



Step 2. Click **Add**.

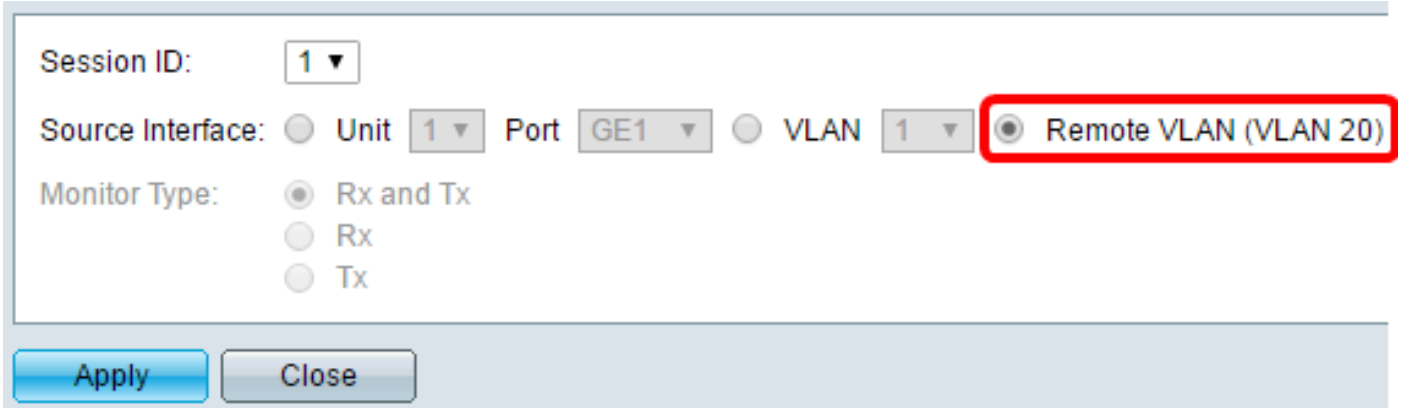


Step 3. (Optional) Choose the session number from the Session ID drop-down list. Session ID must be consistent per session.



Note: In this example, Session 1 is chosen.

Step 4. Click the **Remote VLAN** radio button from the Source Interface area.



Note: The Monitor Type of the Remote VLAN will be automatically configured.

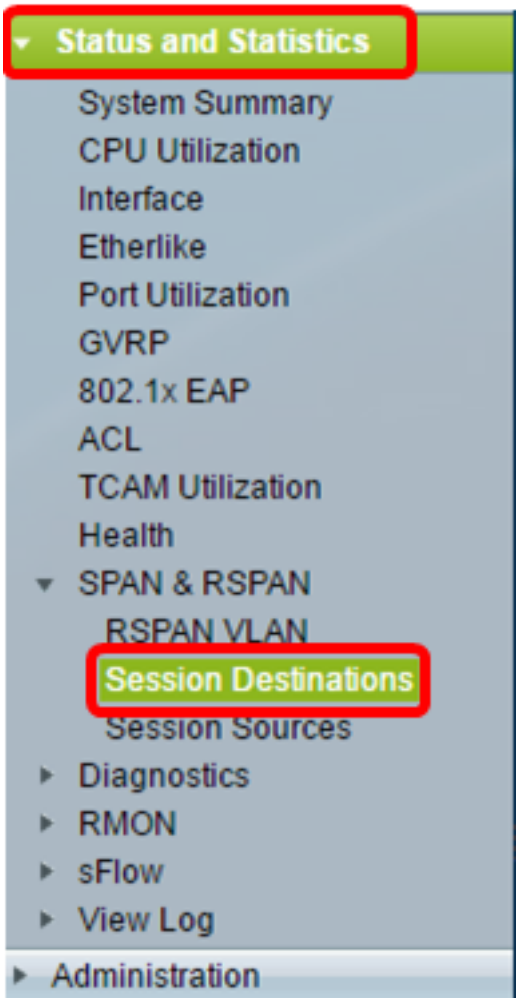
Step 5. Click **Apply** then click **Close**.

Step 6. (Optional) Click **Save** to update the running configuration file.

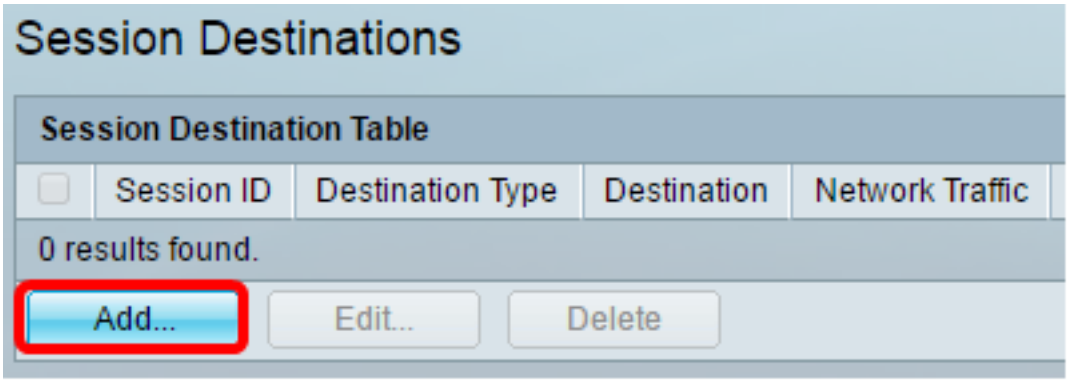
You should now have configured the session sources on your Final Switch.

Configure Session Destinations on a Final Switch

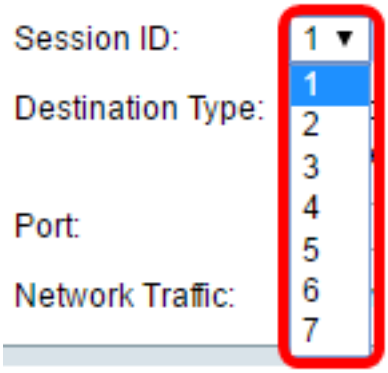
Step 1. Choose **Status and Statistics > SPAN & RSPAN > Session Destinations**.



Step 2. Click **Add**.

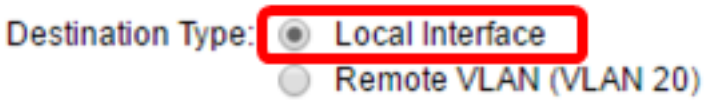


Step 3. Choose the session number from the Session ID drop-down list. It must be the same as the chosen ID from the configured session source.

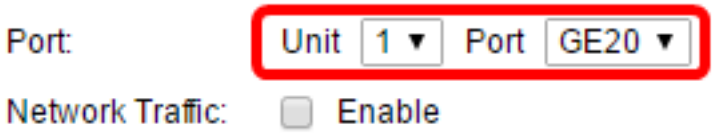


Note: In this example, Session 1 is chosen.

Step 4. Click the **Local Interface** radio button from the Destination Type area.

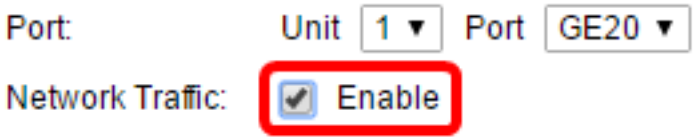


Step 5. In the Port area, choose the desired option from the Unit drop-down list. Choose which port to set as the source port from the Port drop-down list.



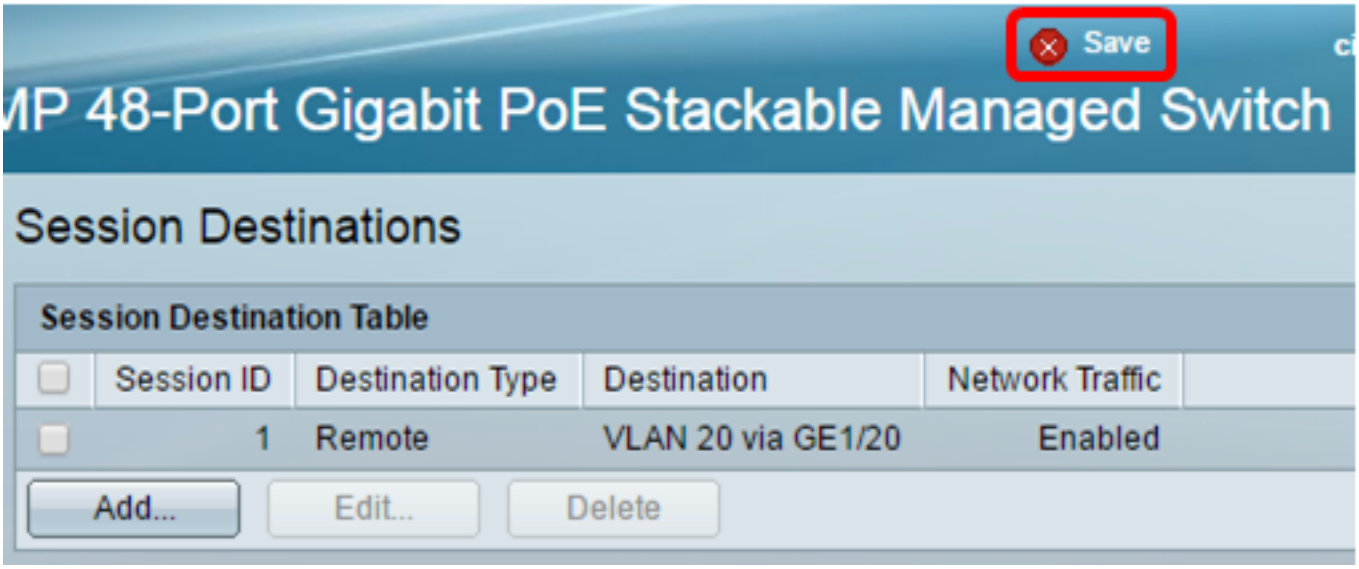
Note: In this example, port GE20 in Unit 1 is chosen.

Step 6. (Optional) Check the **Enable** Network Traffic check box to enable network traffic.



Step 7. Click **Apply** then click **Close**.

Step 8. (Optional) Click **Save** to update the running configuration file.

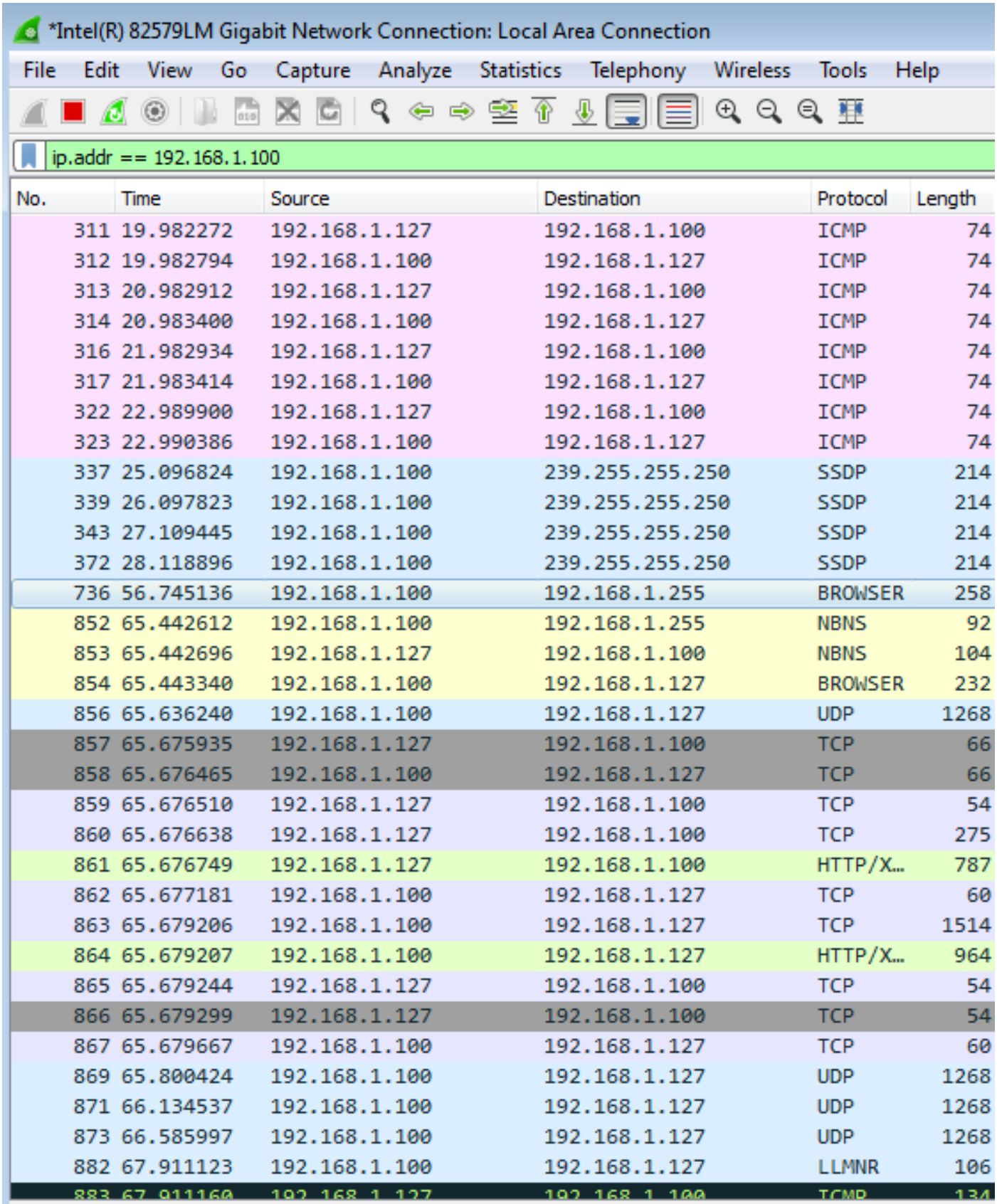


You should now have configured the session destinations on your Final Switch.

Analyze the Captured RSPAN VLAN Packets in WireShark

In this scenario, the host in the configured source interface, GE2 in Unit 1 (GE1/2), has an IP address of 192.168.1.100. While the host in the configured destination interface, GE20 in Unit 1 (VLAN 20 via GE1/20), has an IP address of 192.168.1.127. Wireshark is running in the host that is connected to this port.

Using the filter ip.addr == 192.168.1.100, Wireshark shows the captured packets from the remote source interface.



View a video related to this article...

[Click here to view other Tech Talks from Cisco]