

Configuración de los parámetros del analizador de puertos de switch remoto (RSPAN) en la red

Table Of Contents

- [Objetivo](#)
- [Dispositivos aplicables | Versión del firmware](#)
- [Introducción](#)
- [Configuración de RSPAN VLAN en el Switch](#)
- [Configurar orígenes de sesión en un switch de inicio](#)
- [Configuración de Destinos de Sesión en un Switch de Inicio](#)
- [Switches intermedios](#)
- [Configuración de Orígenes de Sesión en un Switch Final](#)
- [Configuración de Destinos de Sesión en un Switch Final](#)
- [Análisis de los Paquetes VLAN RSPAN Capturados en WireShark](#)

Objetivo

Este artículo proporciona instrucciones sobre cómo configurar RSPAN en sus switches.

Dispositivos aplicables | Versión del firmware

- Sx350 | 2.2.5.68 ([última descarga](#))
- SG350X | 2.2.5.68 ([última descarga](#))
- Sx550X | 2.2.5.68 ([última descarga](#))

Introducción

El analizador de puertos del switch (SPAN), o a veces denominado duplicación de puertos o supervisión de puertos, elige el tráfico de red para su análisis por un analizador de red. El analizador de red puede ser un dispositivo SwitchProbe de Cisco u otra sonda de control remoto (RMON).

La duplicación de puertos se utiliza en un dispositivo de red para enviar una copia de los paquetes de red que se ven en un único puerto de dispositivo, varios puertos de dispositivo o una red de área local virtual (VLAN) completa a una conexión de supervisión de red en otro puerto del dispositivo. Esto se suele utilizar para dispositivos de red que requieren la supervisión del tráfico de red, como un sistema de detección de intrusiones. Un analizador de red conectado al puerto de supervisión procesa los paquetes de datos para el diagnóstico, la depuración y la supervisión del rendimiento.

Remote Switch Port Analyzer (RSPAN) es una extensión de SPAN. RSPAN amplía SPAN al habilitar la supervisión de varios switches en la red y permitir que el puerto del analizador se defina en un switch remoto. Esto significa que puede centralizar sus dispositivos de captura de red.

RSPAN funciona duplicando el tráfico de los puertos de origen de una sesión RSPAN en una VLAN dedicada para la sesión RSPAN. Esta VLAN luego se conecta a otros switches, lo que permite que el tráfico de sesión RSPAN se transporte a través de varios switches. En el switch

que contiene el puerto de destino para la sesión, el tráfico de la VLAN de sesión RSPAN se duplica simplemente fuera del puerto de destino.

Flujo de tráfico RSPAN

- El tráfico para cada sesión RSPAN se transporta a través de una VLAN RSPAN especificada por el usuario y dedicada para esa sesión RSPAN en todos los switches participantes.
- El tráfico de las interfaces de origen en el dispositivo de inicio se copia a la VLAN RSPAN a través de un puerto reflector. Se trata de un puerto físico que debe configurarse. Se utiliza exclusivamente para generar una sesión RSPAN.
- Este puerto reflector es el mecanismo que copia los paquetes a una VLAN RSPAN. Reenvía solamente el tráfico de la sesión de origen RSPAN con la que está afiliado. Cualquier dispositivo conectado a un puerto establecido como puerto reflector pierde la conectividad hasta que se inhabilita la sesión de origen RSPAN.
- El tráfico RSPAN luego se reenvía a través de los puertos troncales en los dispositivos intermedios a la sesión de destino en el switch final.
- El switch de destino monitorea la VLAN RSPAN y la copia en un puerto de destino.

Reglas de pertenencia de puerto RSPAN

- En todos los switches: la pertenencia a RSPAN VLAN se puede etiquetar solamente.
 - Iniciar switch
- Las interfaces de origen SPAN no pueden ser miembros de RSPAN VLAN.
- El puerto reflector no puede ser miembro de esta VLAN.
- Se recomienda que la VLAN remota no tenga ninguna membresía.
 - Switch intermedio
- Se recomienda quitar la pertenencia a RSPAN de todos los puertos no utilizados para pasar tráfico reflejado.
- Normalmente, una VLAN remota RSPAN contiene dos puertos.
 - Switch final
- Para el tráfico duplicado, los puertos de origen deben ser miembros de la VLAN RSPAN.
- Se recomienda quitar la pertenencia a RSPAN de todos los demás puertos, incluida la interfaz de destino.

Configuración de RSPAN en la Red

Configuración de RSPAN VLAN en el Switch

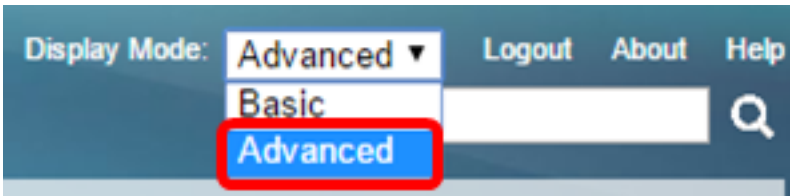
La VLAN RSPAN transporta el tráfico SPAN entre las sesiones de origen y destino de RSPAN. Tiene estas características especiales:

- Todo el tráfico en la VLAN RSPAN siempre se inunda.
- No se produce aprendizaje de direcciones de control de acceso a medios (MAC) en la VLAN

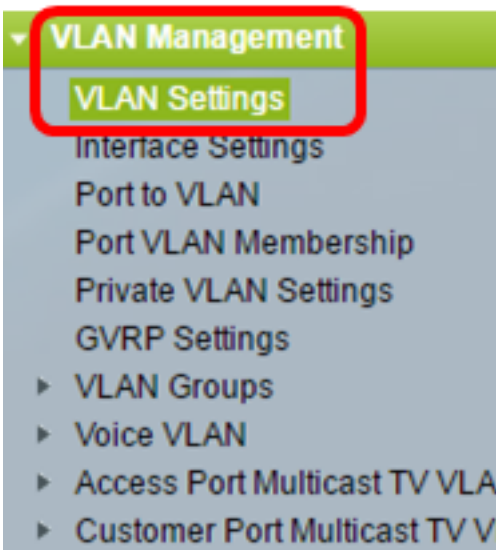
RSPAN.

- El tráfico RSPAN VLAN sólo fluye en los puertos trunk.
- STP puede ejecutarse en los troncales VLAN RSPAN pero no en los puertos de destino SPAN.
- Las VLAN RSPAN se deben configurar en los switches Start y Final en el modo de configuración de VLAN usando el comando **remote-span** VLAN configuration mode, o siga las instrucciones siguientes:

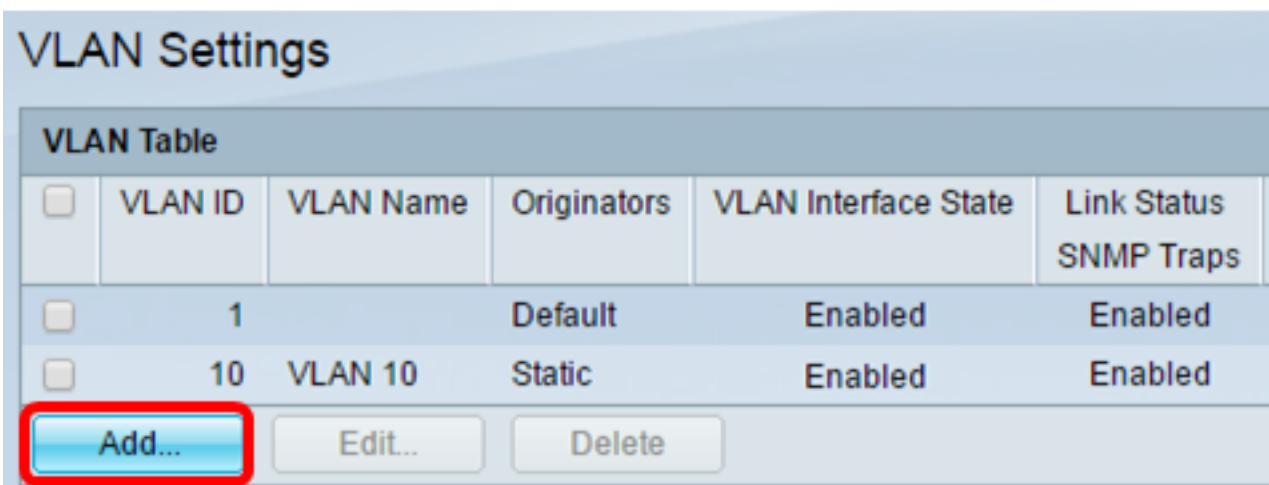
Paso 1. Inicie sesión en la utilidad basada en Web del Start Switch y elija **Advanced** en la lista desplegable Display Mode.



Paso 2. Elija **VLAN Management > VLAN Settings**.



Paso 3. Haga clic en Add (Agregar).



Paso 4. Ingrese el ID de VLAN en el campo *VLAN ID*.

⚙️ VLAN ID: (Range: 2 - 4094)

Nota: En este ejemplo, VLAN 20 se utiliza como ID de VLAN.

Paso 5. (Opcional) Introduzca el nombre de la VLAN en el campo *VLAN Name*.

⚙️ VLAN ID: (Range: 2 - 4094)
VLAN Name: (10/32 characters used)

Nota: En este ejemplo, la VLAN RSPAN se utiliza como nombre de VLAN.

Paso 6. (Opcional) Marque la casilla de verificación VLAN Interface State para habilitar la VLAN. Si se apaga la VLAN, ésta no transmite ni recibe mensajes desde o hacia niveles superiores. Por ejemplo, si cierra una VLAN, en la que se configura una interfaz IP, continúa el puenteo en la VLAN, pero el switch no puede transmitir y recibir tráfico IP en la VLAN. Esta función está activada de forma predeterminada.

Paso 7. (Opcional) Marque la casilla de verificación Link Status SNMP Traps para habilitar la generación de estado de link de las trampas SNMP (del inglés Simple Network Management Protocol, protocolo simple de administración de red). Esta función está activada de forma predeterminada.

Paso 8. Haga clic en **Aplicar** y luego haga clic en **Cerrar**.

VLAN

⚙️ VLAN ID: (Range: 2 - 4094)

VLAN Name: (10/32 characters used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

⚙️ VLAN Range: -

Nota: Para obtener más información sobre la administración de VLAN en un switch, haga clic [aquí](#).

Paso 9. (Opcional) Haga clic en **Guardar** para actualizar el archivo de configuración en ejecución.

MP 48-Port Gigabit PoE Stackable Managed Switch

Save

VLAN Settings

VLAN Table

<input type="checkbox"/>	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
<input type="checkbox"/>	1		Default	Enabled	Enabled
<input type="checkbox"/>	10	VLAN 10	Static	Enabled	Enabled
<input type="checkbox"/>	20	RSPAN VLAN	Static	Enabled	Enabled

Add... Edit... Delete

Paso 10. Elija **Status and Statistics > SPAN & RSPAN > RSPAN VLAN**.

Status and Statistics

- System Summary
- CPU Utilization
- Interface
- Etherlike
- Port Utilization
- GVRP
- 802.1x EAP
- ACL
- TCAM Utilization
- Health
- ▼ SPAN & RSPAN
 - RSPAN VLAN**
 - Session Destinations
 - Session Sources
- ▶ Diagnostics
- ▶ RMON
- ▶ sFlow
- ▶ View Log
- ▶ Administration

Paso 11. Elija un ID de VLAN de la lista desplegable RSPAN VLAN. Esta VLAN se debe utilizar exclusivamente para RSPAN.

RSPAN VLAN

A VLAN must be added to the VLAN Database using the [VLAN Settings](#) screen

RSPAN VLAN: None ▼
None
10
20

Apply

Nota: En este ejemplo, se elige VLAN 20.

Paso 12. Haga clic en Apply (Aplicar).

RSPAN VLAN

A VLAN must be added to the VLAN Database using the [VLAN Settings](#) screen

RSPAN VLAN: 20 ▼

Apply Cancel

Paso 13. (Opcional) Haga clic en **Guardar** para actualizar el archivo de configuración en ejecución.

✖ Save cisco

MP 48-Port Gigabit PoE Stackable Managed Switch

RSPAN VLAN

✓ Success. To permanently save the configuration, go to the [File Operations](#) page

A VLAN must be added to the VLAN Database using the [VLAN Settings](#) screen before it can be co

RSPAN VLAN: 20 ▼

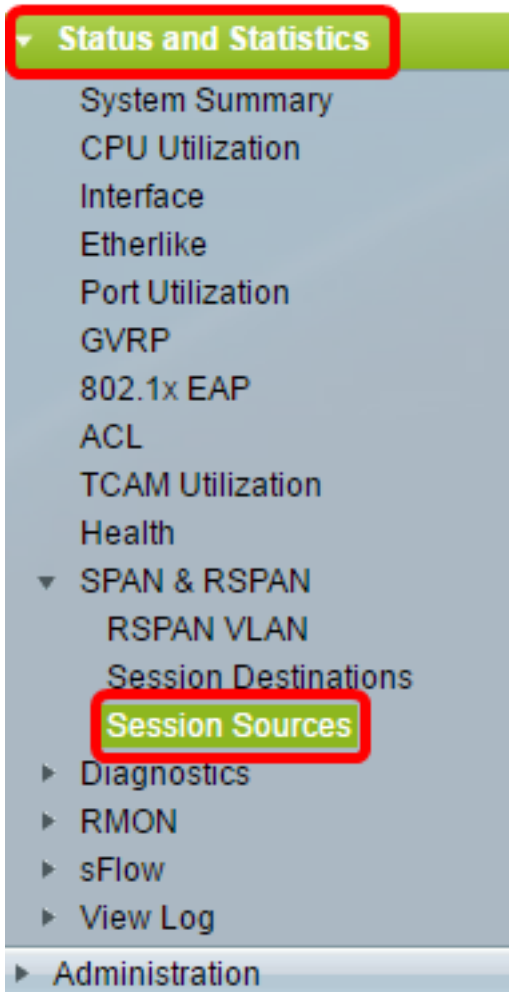
Apply Cancel

Paso 14. En el switch final, repita los pasos 1 a 13 para configurar la VLAN RSPAN.

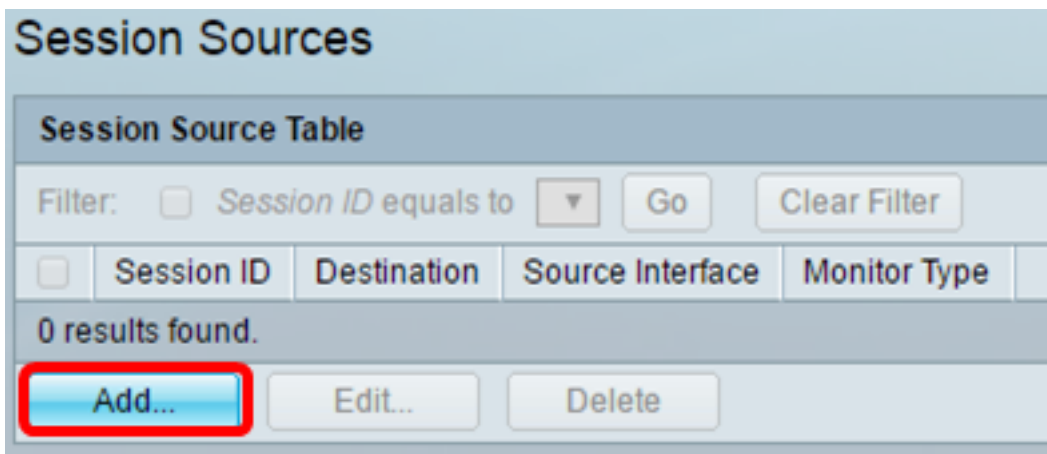
Ahora debería haber configurado la VLAN dedicada a la sesión RSPAN en los switches inicial y final.

Configurar orígenes de sesión en un switch de inicio

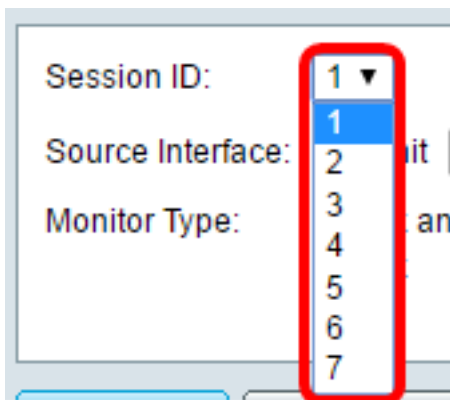
Paso 1. Elija **Status and Statistics > SPAN & RSPAN > Session Sources**.



Paso 2. Haga clic en Add (Agregar).



Paso 3. Elija el número de sesión de la lista desplegable ID de sesión. El ID de sesión debe ser coherente por sesión RSPAN.



Nota: En este ejemplo, se elige la Sesión 1.

Paso 4. Haga clic en el botón de opción del tipo de interfaz de origen deseado y elija la interfaz de la lista desplegable o listas.

Importante: La interfaz de origen no puede ser igual que el puerto de destino.



Las opciones son:

- Unidad y Puerto: puede elegir la opción deseada en la lista desplegable Unidad y elegir qué puerto establecer como puerto de origen en la lista desplegable Puerto.
- VLAN: puede elegir la VLAN que desea supervisar en la lista desplegable VLAN. Una VLAN ayuda a un grupo de hosts a comunicarse como si estuvieran en la misma red física, independientemente de su ubicación. Si se elige esta opción, no se puede editar.
- VLAN remota: esto mostrará la VLAN RSPAN definida. Si se elige esta opción, no se puede editar.

Nota: En este ejemplo, se elige el puerto GE2 en la Unidad 1. Ésta es la interfaz remota que se monitorearía.

Paso 5. (Opcional) Si se hace clic en Unit y Port en el Paso 4, haga clic en el botón de opción Monitor Type (Tipo de monitor) que desee para el tipo de tráfico que desea supervisar.



Las opciones son:

- Rx y Tx: esta opción permite la duplicación de puertos de los paquetes entrantes y salientes. Esta opción se elige de forma predeterminada.
- Rx: esta opción permite la duplicación de puertos de los paquetes entrantes.
- Tx: esta opción permite la duplicación de puertos de los paquetes salientes.

Nota: En este ejemplo, se elige Rx.

Paso 6. Haga clic en **Aplicar** y luego haga clic en **Cerrar**.

Session ID:

Source Interface: Unit Port VLAN Remote VLAN (VLAN 20)

Monitor Type: Rx and Tx
 Rx
 Tx

Paso 7. (Opcional) Haga clic en **Guardar** para actualizar el archivo de configuración en ejecución.

MP 48-Port Gigabit PoE Stackable Managed Switch

Session Sources

Session Source Table

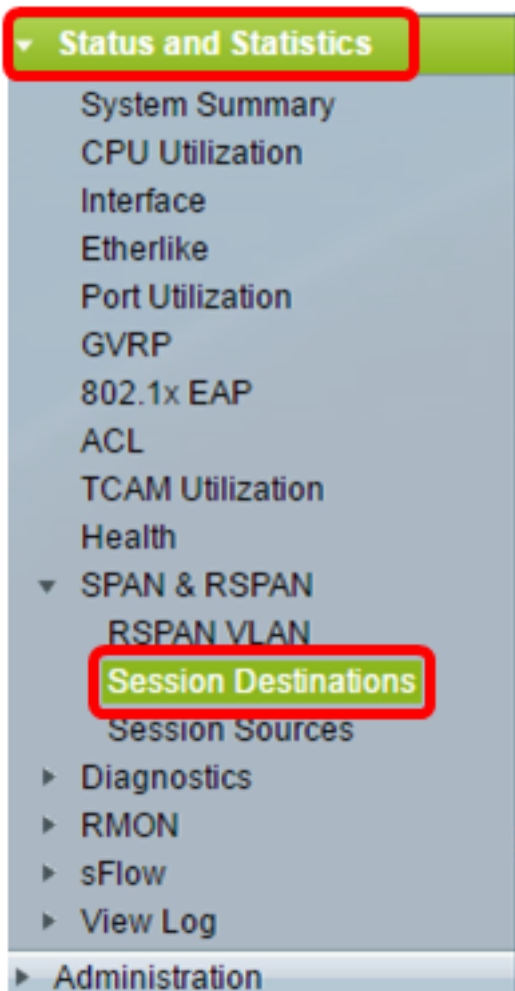
Filter: Session ID equals to

<input type="checkbox"/>	Session ID	Destination	Source Interface	Monitor Type
<input type="checkbox"/>	1	No Destination	GE1/2	Rx

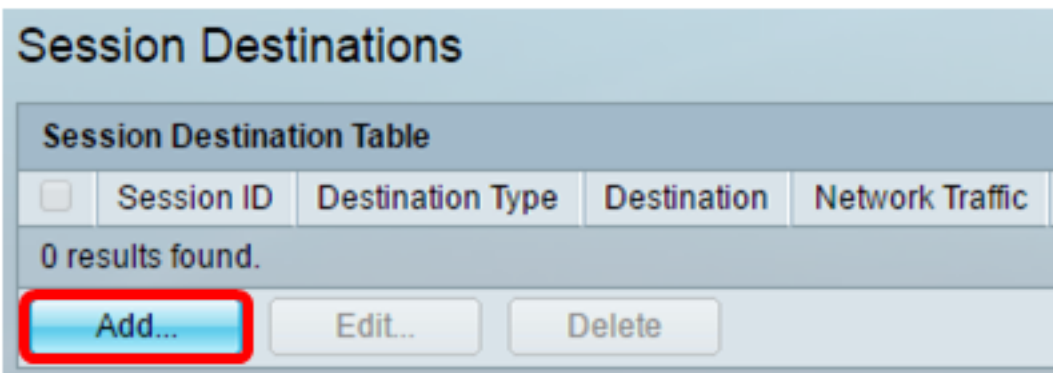
Ahora debería haber configurado el origen de la sesión en el switch de inicio.

Configuración de Destinos de Sesión en un Switch de Inicio

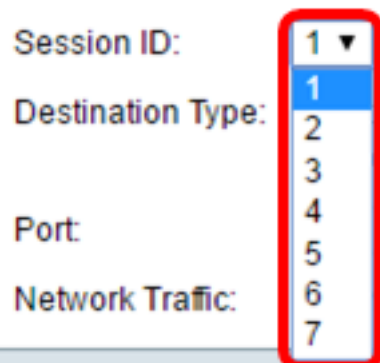
Paso 1. Elija **Status and Statistics > SPAN & RSPAN > Session Destinations**.



Paso 2. Haga clic en Add (Agregar).



Paso 3. Elija el número de sesión de la lista desplegable ID de sesión. Debe ser el mismo que el ID elegido del origen de sesión configurado.



Nota: En este ejemplo, se elige la Sesión 1.

Paso 4. Haga clic en el botón de radio **VLAN remota** del área Tipo de destino. Un analizador de red, como un ordenador que ejecuta Wireshark, está conectado a este puerto.

Importante: La interfaz de destino no puede ser la misma que el puerto de origen.

Destination Type: Local Interface
 Remote VLAN (VLAN 20)

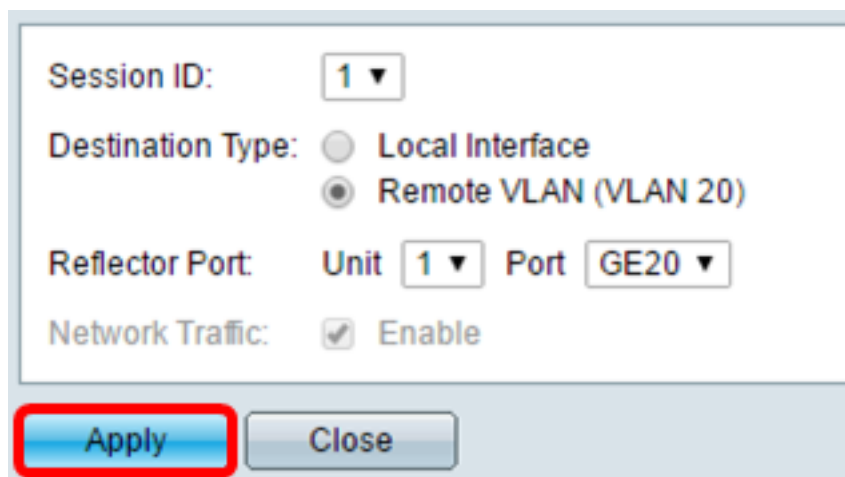
Nota: Si se elige VLAN remota, el tráfico de red se habilita automáticamente.

Paso 5. En el área Puerto reflector, elija la opción deseada en la lista desplegable Unidad. Elija qué puerto establecer como puerto de origen en la lista desplegable Puerto.

Reflector Port: Unit Port
Network Traffic: Enable

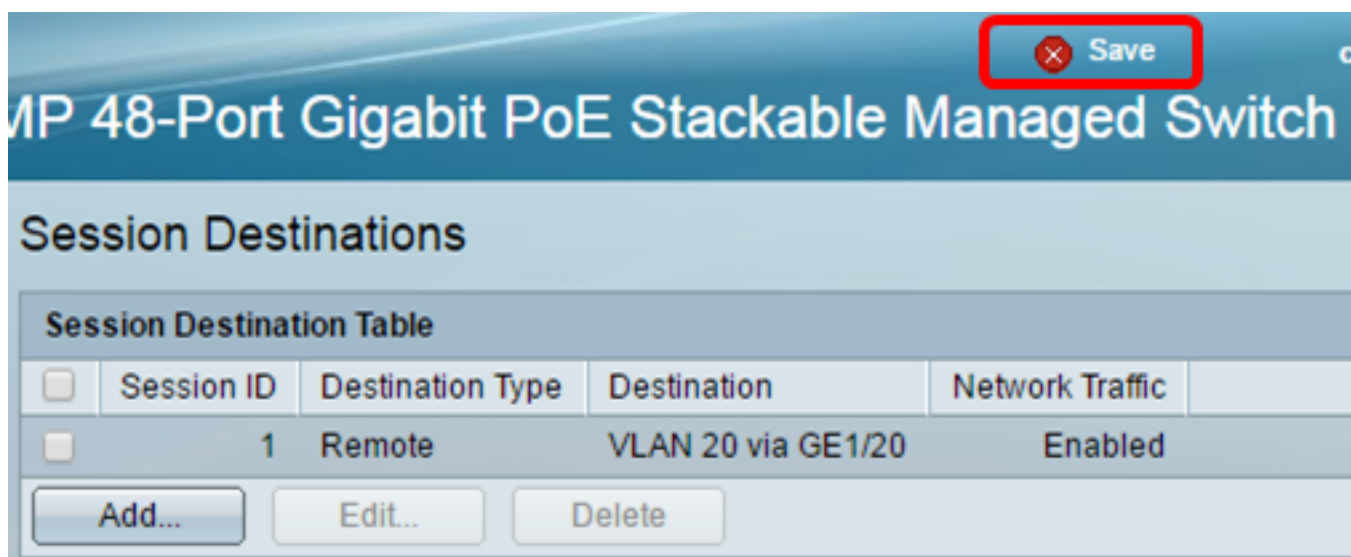
Nota: En este ejemplo, se elige el puerto GE20 en la Unidad 1.

Paso 6. Haga clic en **Aplicar** y luego haga clic en **Cerrar**.



Session ID:
Destination Type: Local Interface
 Remote VLAN (VLAN 20)
Reflector Port: Unit Port
Network Traffic: Enable

Paso 7. (Opcional) Haga clic en **Guardar** para actualizar el archivo de configuración en ejecución.



MP 48-Port Gigabit PoE Stackable Managed Switch

Session Destinations

Session Destination Table				
<input type="checkbox"/>	Session ID	Destination Type	Destination	Network Traffic
<input type="checkbox"/>	1	Remote	VLAN 20 via GE1/20	Enabled

Ahora debería haber configurado los destinos de sesión en el switch de inicio.

Switches intermedios

También puede haber switches intermedios que separan las sesiones de origen y destino de RSPAN. Estos switches no necesitan ser capaces de ejecutar RSPAN, pero deben responder a los requisitos de la VLAN RSPAN.

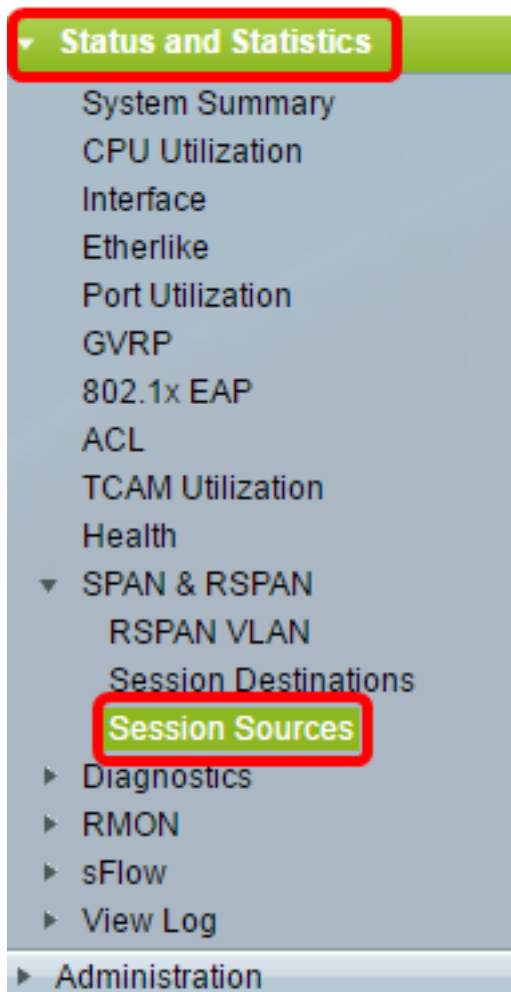
Para las VLAN 1 a 1005 que son visibles para el protocolo de enlace troncal VLAN (VTP), el ID de VLAN y sus características de RSPAN asociadas se propagan por VTP. Si asigna un ID de VLAN RSPAN en el rango de VLAN extendida (1006 a 4094), debe configurar manualmente todos los switches intermedios.

Para aprender a asignar una interfaz VLAN como puerto troncal de un switch intermedio, haga clic [aquí](#) para obtener instrucciones.

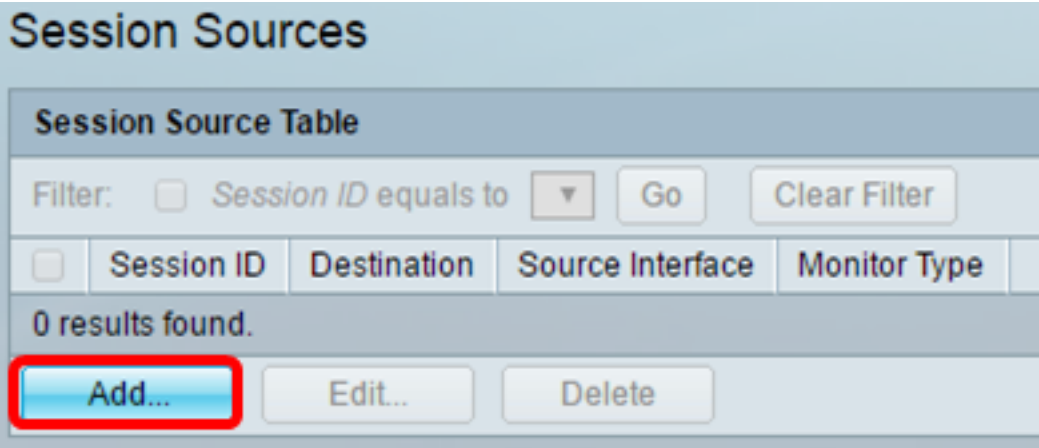
Es normal tener varias VLAN RSPAN en una red al mismo tiempo con cada VLAN RSPAN que define una sesión RSPAN de toda la red. Es decir, varias sesiones de origen RSPAN en cualquier lugar de la red pueden aportar paquetes a la sesión RSPAN. También es posible tener varias sesiones de destino RSPAN en toda la red, monitorear la misma VLAN RSPAN y presentar el tráfico al usuario. El ID de VLAN RSPAN separa las sesiones.

Configuración de Orígenes de Sesión en un Switch Final

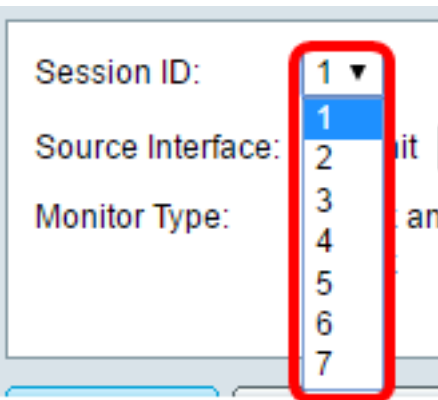
Paso 1. Elija **Status and Statistics > SPAN & RSPAN > Session Sources**.



Paso 2. Haga clic en Add (Agregar).

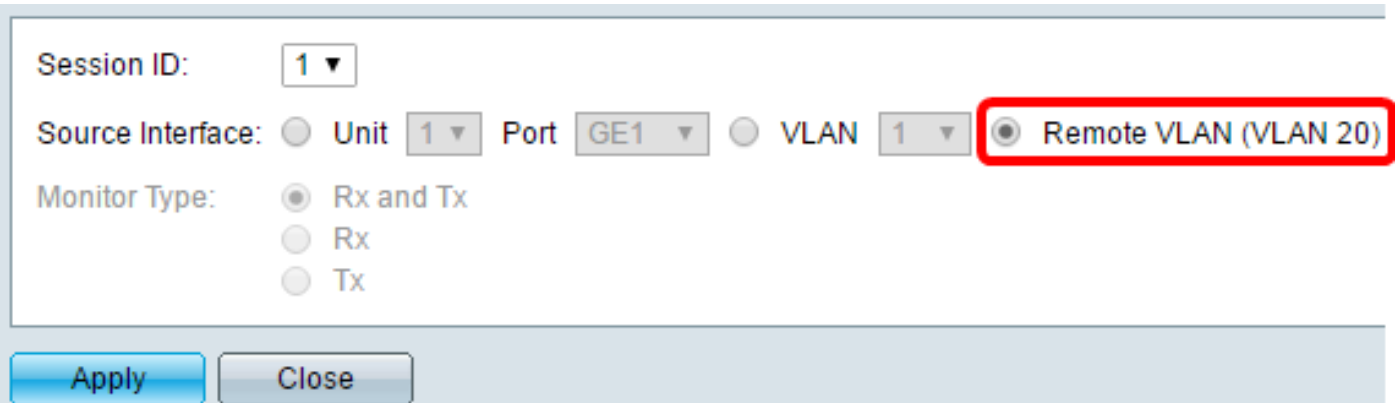


Paso 3. (Opcional) Elija el número de sesión de la lista desplegable ID de sesión. La ID de sesión debe ser coherente por sesión.



Nota: En este ejemplo, se elige la Sesión 1.

Paso 4. Haga clic en el botón de radio **VLAN remota** del área Interfaz de Origen.



Nota: El tipo de monitor de la VLAN remota se configurará automáticamente.

Paso 5. Haga clic en **Aplicar** y luego haga clic en **Cerrar**.

Paso 6. (Opcional) Haga clic en **Guardar** para actualizar el archivo de configuración en ejecución.

MP 48-Port Gigabit PoE Stackable Managed Switch

Session Sources

Session Source Table

Filter: Session ID equals to 1 (GE1/1) Go Clear Filter

<input type="checkbox"/>	Session ID	Destination	Source Interface	Monitor Type
<input type="checkbox"/>	1	VLAN 20		Rx

Add... Edit... Delete

Ahora debería haber configurado los orígenes de sesión en su switch final.

Configuración de Destinos de Sesión en un Switch Final

Paso 1. Elija **Status and Statistics > SPAN & RSPAN > Session Destinations**.

- ▼ Status and Statistics
 - System Summary
 - CPU Utilization
 - Interface
 - Etherlike
 - Port Utilization
 - GVRP
 - 802.1x EAP
 - ACL
 - TCAM Utilization
 - Health
 - ▼ SPAN & RSPAN
 - RSPAN VLAN
 - Session Destinations
 - Session Sources
 - ▶ Diagnostics
 - ▶ RMON
 - ▶ sFlow
 - ▶ View Log
- ▶ Administration

Paso 2. Haga clic en Add (Agregar).

Session Destinations

Session Destination Table				
<input type="checkbox"/>	Session ID	Destination Type	Destination	Network Traffic
0 results found.				
<input type="button" value="Add..."/> <input type="button" value="Edit..."/> <input type="button" value="Delete"/>				

Paso 3. Elija el número de sesión de la lista desplegable ID de sesión. Debe ser el mismo que el ID elegido del origen de sesión configurado.

Session ID:

Destination Type:

Port:

Network Traffic:

Nota: En este ejemplo, se elige la Sesión 1.

Paso 4. Haga clic en el botón de opción **Local Interface** del área Destination Type .

Destination Type: Local Interface Remote VLAN (VLAN 20)

Paso 5. En el área Puerto, elija la opción deseada en la lista desplegable Unidad. Elija qué puerto establecer como puerto de origen en la lista desplegable Puerto.

Port:

Network Traffic: Enable

Nota: En este ejemplo, se elige el puerto GE20 en la Unidad 1.

Paso 6. (Opcional) Marque la casilla de verificación **Enable** Network Traffic para habilitar el tráfico de red.

Port:

Network Traffic: Enable

Paso 7. Haga clic en **Aplicar** y luego haga clic en **Cerrar**.

Paso 8. (Opcional) Haga clic en **Guardar** para actualizar el archivo de configuración en ejecución.



Ahora debería haber configurado los destinos de sesión en su switch final.

Análisis de los Paquetes VLAN RSPAN Capturados en WireShark

En este escenario, el host en la interfaz de origen configurada, GE2 en la Unidad 1 (GE1/2), tiene una dirección IP de 192.168.1.100. Mientras que el host en la interfaz de destino configurada, GE20 en la Unidad 1 (VLAN 20 a través de GE1/20), tiene una dirección IP de 192.168.1.127. Wireshark se está ejecutando en el host que está conectado a este puerto.

Mediante el filtro `ip.addr == 192.168.1.100`, Wireshark muestra los paquetes capturados de la interfaz de origen remota.

*Intel(R) 82579LM Gigabit Network Connection: Local Area Connection

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 192.168.1.100

No.	Time	Source	Destination	Protocol	Length
311	19.982272	192.168.1.127	192.168.1.100	ICMP	74
312	19.982794	192.168.1.100	192.168.1.127	ICMP	74
313	20.982912	192.168.1.127	192.168.1.100	ICMP	74
314	20.983400	192.168.1.100	192.168.1.127	ICMP	74
316	21.982934	192.168.1.127	192.168.1.100	ICMP	74
317	21.983414	192.168.1.100	192.168.1.127	ICMP	74
322	22.989900	192.168.1.127	192.168.1.100	ICMP	74
323	22.990386	192.168.1.100	192.168.1.127	ICMP	74
337	25.096824	192.168.1.100	239.255.255.250	SSDP	214
339	26.097823	192.168.1.100	239.255.255.250	SSDP	214
343	27.109445	192.168.1.100	239.255.255.250	SSDP	214
372	28.118896	192.168.1.100	239.255.255.250	SSDP	214
736	56.745136	192.168.1.100	192.168.1.255	BROWSER	258
852	65.442612	192.168.1.100	192.168.1.255	NBNS	92
853	65.442696	192.168.1.127	192.168.1.100	NBNS	104
854	65.443340	192.168.1.100	192.168.1.127	BROWSER	232
856	65.636240	192.168.1.100	192.168.1.127	UDP	1268
857	65.675935	192.168.1.127	192.168.1.100	TCP	66
858	65.676465	192.168.1.100	192.168.1.127	TCP	66
859	65.676510	192.168.1.127	192.168.1.100	TCP	54
860	65.676638	192.168.1.127	192.168.1.100	TCP	275
861	65.676749	192.168.1.127	192.168.1.100	HTTP/X...	787
862	65.677181	192.168.1.100	192.168.1.127	TCP	60
863	65.679206	192.168.1.100	192.168.1.127	TCP	1514
864	65.679207	192.168.1.100	192.168.1.127	HTTP/X...	964
865	65.679244	192.168.1.127	192.168.1.100	TCP	54
866	65.679299	192.168.1.127	192.168.1.100	TCP	54
867	65.679667	192.168.1.100	192.168.1.127	TCP	60
869	65.800424	192.168.1.100	192.168.1.127	UDP	1268
871	66.134537	192.168.1.100	192.168.1.127	UDP	1268
873	66.585997	192.168.1.100	192.168.1.127	UDP	1268
882	67.911123	192.168.1.100	192.168.1.127	LLMNR	106
883	67.911160	192.168.1.127	192.168.1.100	TCP	134

Ver un vídeo relacionado con este artículo...

[Haga clic aquí para ver otras charlas técnicas de Cisco](#)