

Configurar o RSPAN (Remote Switch Port Analyzer) na rede

Table Of Contents

- [Objetivo](#)
- [Dispositivos aplicáveis | Versão do firmware](#)
- [Introduction](#)
- [Configurar a VLAN RSPAN no Switch](#)
- [Configurar origens de sessão em um switch inicial](#)
- [Configurar destinos de sessão em um switch inicial](#)
- [Switches intermediários](#)
- [Configurar fontes de sessão em um switch final](#)
- [Configurar destinos de sessão em um switch final](#)
- [Analisar os pacotes de VLAN RSPAN capturados no WireShark](#)

Objetivo

Este artigo fornece instruções sobre como configurar o RSPAN em seus switches.

Dispositivos aplicáveis | Versão do firmware

- Sx350 | 2.2.5.68 ([Baixe o mais recente](#))
- SG350X | 2.2.5.68 ([Baixe o mais recente](#))
- Sx550X | 2.2.5.68 ([Baixe o mais recente](#))

Introduction

Switch Port Analyzer (SPAN), ou às vezes chamado de espelhamento de porta ou monitoramento de porta, escolhe o tráfego de rede para análise por um analisador de rede. O analisador de rede pode ser um dispositivo Cisco SwitchProbe ou outra sonda de monitoração remota (RMON).

O espelhamento de portas é usado em um dispositivo de rede para enviar uma cópia dos pacotes de rede vistos em uma única porta de dispositivo, várias portas de dispositivo ou uma VLAN (Virtual Local Area Network, rede local virtual) inteira para uma conexão de monitoramento de rede em outra porta no dispositivo. Isso é comumente usado para dispositivos de rede que exigem monitoramento do tráfego de rede, como um sistema de detecção de intrusão. Um analisador de rede conectado à porta de monitoramento processa os pacotes de dados para diagnóstico, depuração e monitoramento de desempenho.

O Remote Switch Port Analyzer (RSPAN) é uma extensão de SPAN. O RSPAN estende o SPAN permitindo o monitoramento de vários switches na rede e permitindo que a porta do analisador seja definida em um switch remoto. Isso significa que você pode centralizar seus dispositivos de captura de rede.

O RSPAN funciona espelhando o tráfego das portas de origem de uma sessão de RSPAN em uma VLAN dedicada à sessão de RSPAN. Essa VLAN é então entroncada para outros switches, permitindo que o tráfego da sessão de RSPAN seja transportado através de vários switches. No switch que contém a porta de destino para a sessão, o tráfego da VLAN da sessão de RSPAN é

simplesmente espelhado na porta de destino.

Fluxo de tráfego de RSPAN

- O tráfego para cada sessão de RSPAN é transportado sobre uma VLAN de RSPAN especificada pelo usuário dedicada para essa sessão de RSPAN em todos os switches participantes.
- O tráfego das interfaces de origem no dispositivo inicial é copiado para a VLAN de RSPAN através de uma porta refletora. Esta é uma porta física que precisa ser definida. É usado exclusivamente para criar uma sessão de RSPAN.
- Essa porta refletora é o mecanismo que copia pacotes para uma VLAN de RSPAN. Encaminha apenas o tráfego da sessão de origem de RSPAN à qual está afiliado. Os dispositivos conectados a uma porta definida como porta refletora perdem a conectividade até que a sessão de origem de RSPAN seja desabilitada.
- O tráfego de RSPAN é então encaminhado através das portas de tronco nos dispositivos intermediários para a sessão de destino no switch final.
- O switch de destino monitora a VLAN de RSPAN e a copia para uma porta de destino.

Regras de participação de porta RSPAN

- Em todos os switches — A associação na VLAN RSPAN pode ser marcada somente.
 - Iniciar switch
- As interfaces de origem de SPAN não podem ser membros da VLAN de RSPAN.
- A porta refletora não pode ser um membro desta VLAN.
- Recomenda-se que a VLAN remota não tenha associações.
- Switch intermediário
- Recomenda-se remover a associação de RSPAN de todas as portas não usadas para a passagem de tráfego espelhado.
- Geralmente, uma VLAN remota RSPAN contém duas portas.
- Switch final
- Para o tráfego espelhado, as portas de origem devem ser membros da VLAN de RSPAN.
- Recomenda-se remover a associação de RSPAN de todas as outras portas, incluindo a interface de destino.

Configurar RSPAN na rede

Configurar a VLAN RSPAN no Switch

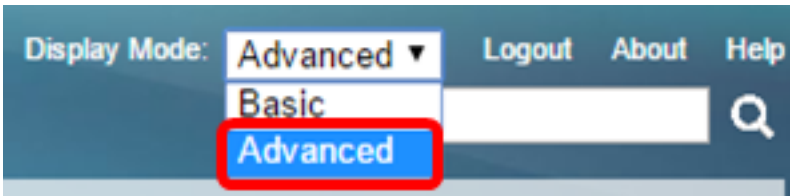
A VLAN de RSPAN transporta tráfego de SPAN entre as sessões de origem e de destino de RSPAN. Tem estas características especiais:

- Todo o tráfego na VLAN de RSPAN é sempre inundado.
- Nenhum endereço de Controle de Acesso ao Meio (MAC - Media Access Control) ocorre na

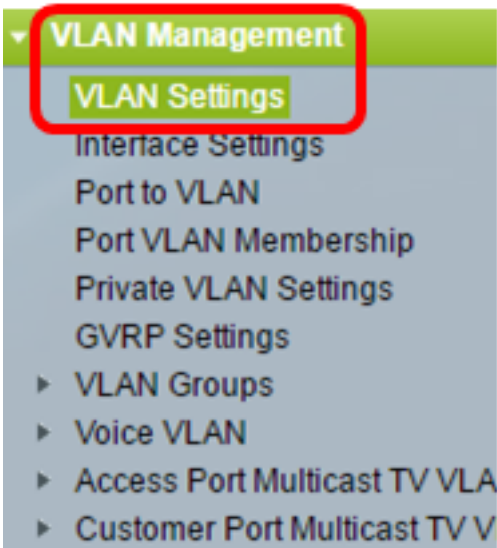
VLAN de RSPAN.

- O tráfego de VLAN de RSPAN flui somente em portas de tronco.
- O STP pode ser executado em troncos de VLAN de RSPAN, mas não em portas de destino de SPAN.
- As VLANs de RSPAN devem ser configuradas nos switches Start e Final no modo de configuração de VLAN usando o comando do modo de configuração de VLAN **remote-span** ou siga as instruções abaixo:

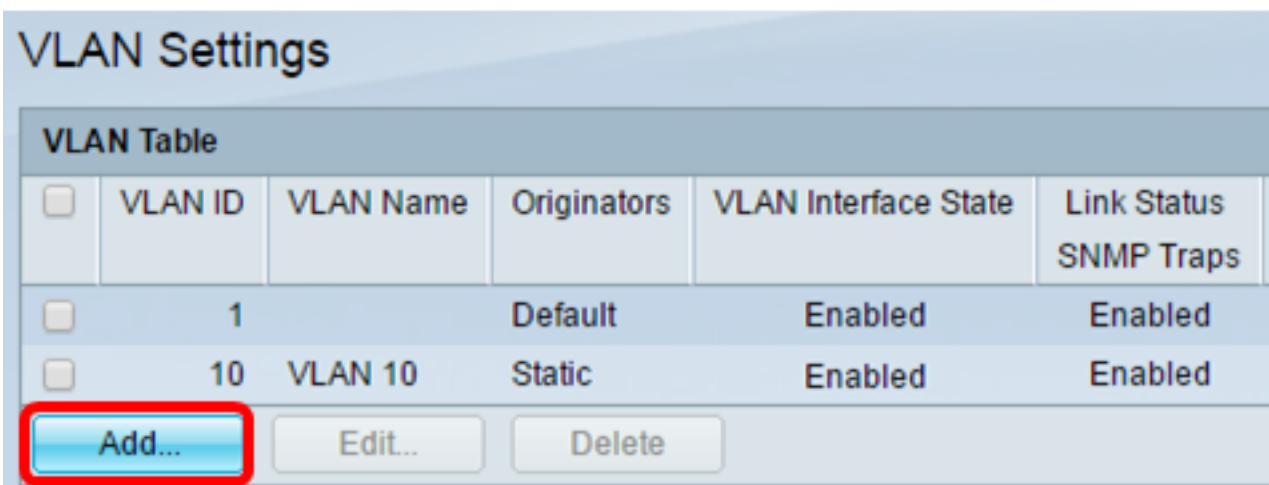
Etapa 1. Efetue login no utilitário baseado na Web do Computador Iniciar e escolha **Avançado** na lista suspensa Modo de vídeo.



Etapa 2. Escolha **VLAN Management > VLAN Settings**.



Etapa 3. Clique em Add.



Etapa 4. Digite o ID da VLAN no campo *VLAN ID*.

 VLAN ID: (Range: 2 - 4094)

Note: Neste exemplo, a VLAN 20 é usada como o ID da VLAN.

Etapa 5. (Opcional) Insira o nome da VLAN no campo *VLAN Name (Nome da VLAN)*.

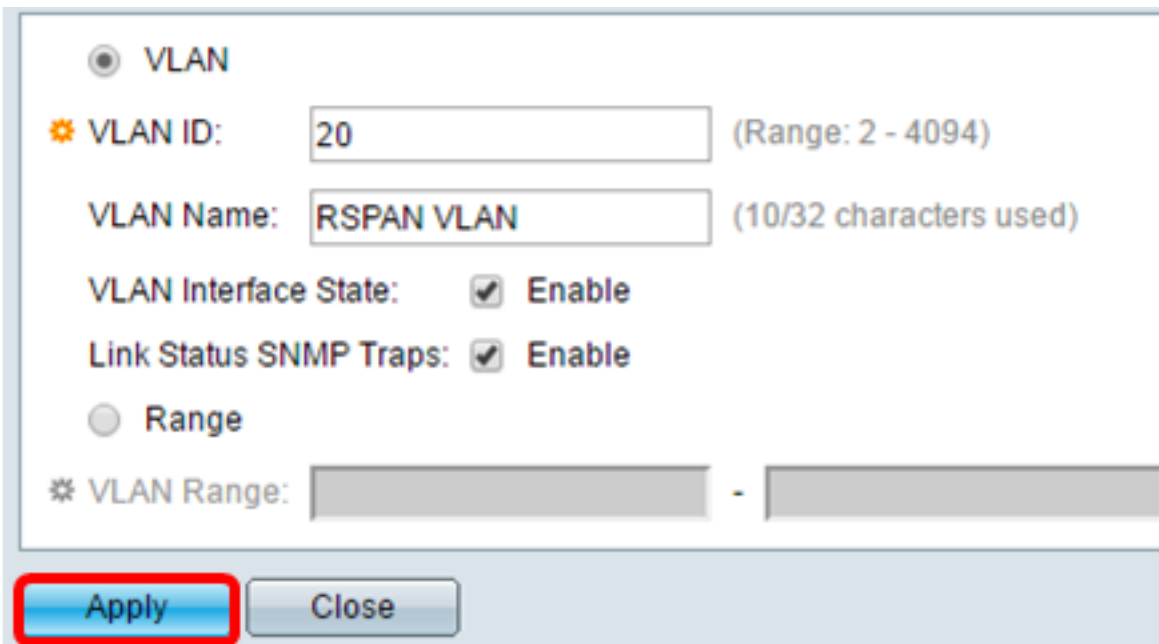
 VLAN ID: (Range: 2 - 4094)
 (10/32 characters used)

Note: Neste exemplo, a VLAN de RSPAN é usada como o nome da VLAN.


Etapa 6. (Opcional) Marque a caixa de seleção VLAN Interface State para ativar a VLAN. Se a VLAN estiver desligada, ela não transmitirá ou receberá mensagens de ou para níveis mais altos. Por exemplo, se você desligar uma VLAN, na qual uma interface IP está configurada, a ligação à VLAN continua, mas o switch não pode transmitir e receber tráfego IP na VLAN. Este recurso é ativado por padrão.

Passo 7. (Opcional) Marque a caixa de seleção Link Status SNMP Traps para habilitar a geração de status de link das interceptações SNMP (Simple Network Management Protocol). Este recurso é ativado por padrão.

Etapa 8. Clique em **Aplicar** e, em seguida, clique em **Fechar**.



VLAN


 VLAN ID: (Range: 2 - 4094)

VLAN Name: (10/32 characters used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

 VLAN Range: -

Note: Para saber mais sobre como gerenciar VLANs em um switch, clique [aqui](#).

Etapa 9. (Opcional) Clique em **Salvar** para atualizar o arquivo de configuração atual.

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	Enabled
<input type="checkbox"/>	10	VLAN 10	Static	Enabled	Enabled	Enabled
<input type="checkbox"/>	20	RSPAN VLAN	Static	Enabled	Enabled	Enabled

Add... Edit... Delete

Etapa 10. Escolha **Status e 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

Etapa 11. Escolha uma ID de VLAN na lista suspensa VLAN de RSPAN. Essa VLAN deve ser usada 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: Neste exemplo, a VLAN 20 é escolhida.

Etapa 12. Clique em Apply.

RSPAN VLAN

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

RSPAN VLAN: 20 ▼

Apply Cancel

Etapa 13. (Opcional) Clique em **Salvar** para atualizar o arquivo de configuração atual.

✖ 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 ▼

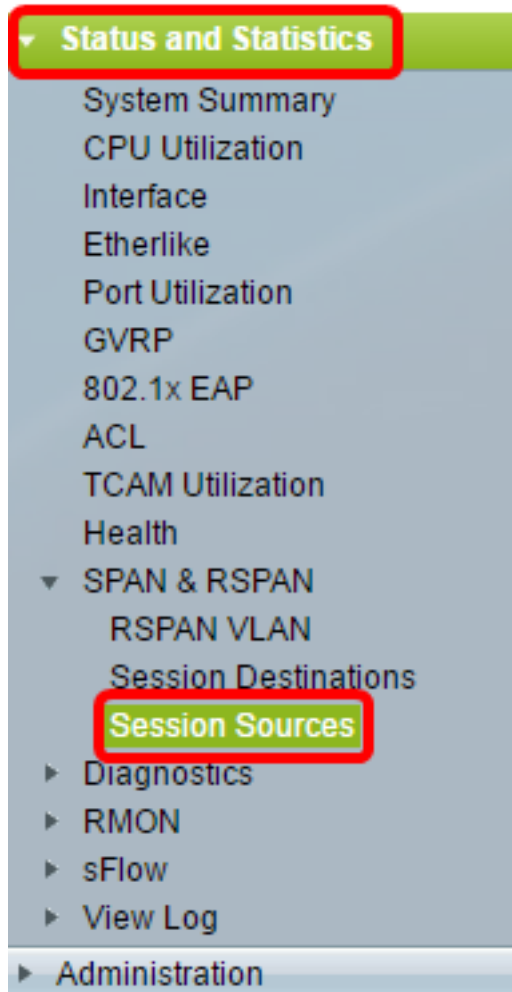
Apply Cancel

Etapa 14. No Switch final, repita as etapas de 1 a 13 para configurar a VLAN de RSPAN.

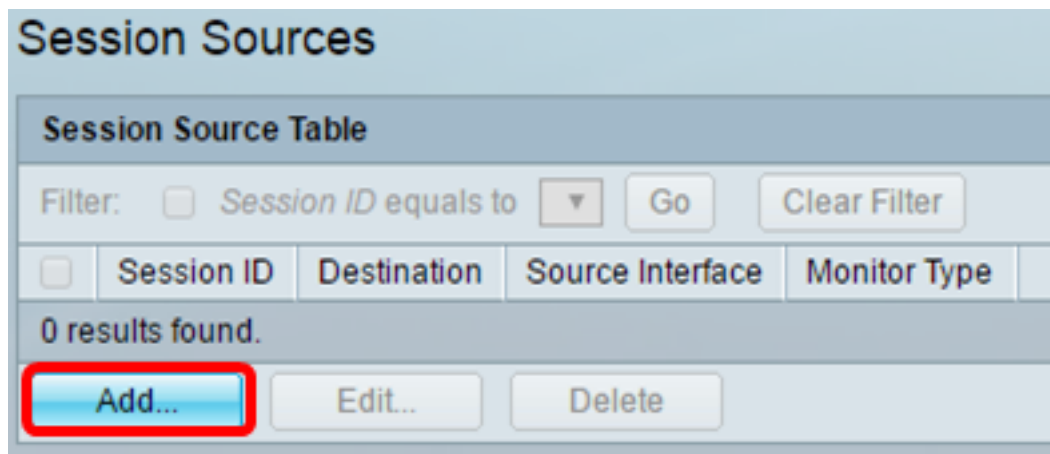
Agora você deve ter configurado a VLAN dedicada à sessão de RSPAN nos Switches Iniciar e Final.

Configurar origens de sessão em um switch inicial

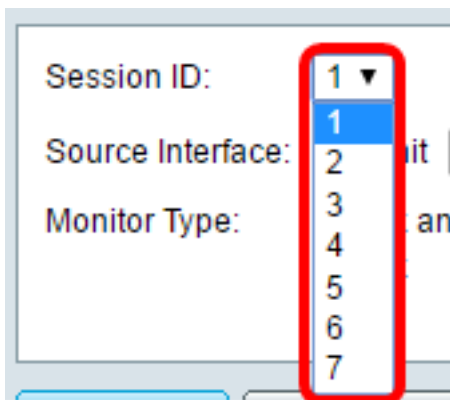
Etapa 1. Escolha **Status e Statistics > SPAN & RSPAN > Session Sources**.



Etapa 2. Clique em Add.



Etapa 3. Escolha o número da sessão na lista suspensa ID da sessão. A ID da sessão deve ser consistente por sessão de RSPAN.



Note: Neste exemplo, a Sessão 1 é escolhida.

Etapa 4. Clique no botão de opção do tipo de interface de origem desejado e escolha a interface na lista suspensa ou nas listas.

Importante: A interface de origem não pode ser a mesma da porta de destino.



As opções são:

- Unidade e porta — Você pode escolher a opção desejada na lista suspensa Unidade e escolher qual porta definir como a porta de origem na lista suspensa Porta.
- VLAN — Você pode escolher a VLAN desejada para monitorar na lista suspensa VLAN. Uma VLAN ajuda um grupo de hosts a se comunicar como se estivessem na mesma rede física, independentemente de sua localização. Se esta opção for escolhida, ela não poderá ser editada.
- VLAN remota — Isso exibirá a VLAN RSPAN definida. Se esta opção for escolhida, ela não poderá ser editada.

Note: Neste exemplo, a porta GE2 na Unidade 1 é escolhida. Essa é a interface remota que seria monitorada.

Etapa 5. (Opcional) Se Unidade e Porta forem clicadas na Etapa 4, clique no botão de opção Tipo de monitor desejado para o tipo de tráfego a ser monitorado.



As opções são:

- Rx e Tx — Essa opção permite o espelhamento de portas de pacotes de entrada e saída. Essa opção é escolhida por padrão.
- Rx — Esta opção permite o espelhamento de portas de pacotes de entrada.
- Tx — Esta opção permite o espelhamento de portas de pacotes de saída.

Note: Neste exemplo, Rx é escolhido.

Etapa 6. Clique em **Aplicar** e, em seguida, clique em **Fechar**.

Session ID:

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

Monitor Type: Rx and Tx
 Rx
 Tx

Passo 7. (Opcional) Clique em **Salvar** para atualizar o arquivo de configuração atual.

MP 48-Port Gigabit PoE Stackable Managed Switch

Session Sources

Session Source Table

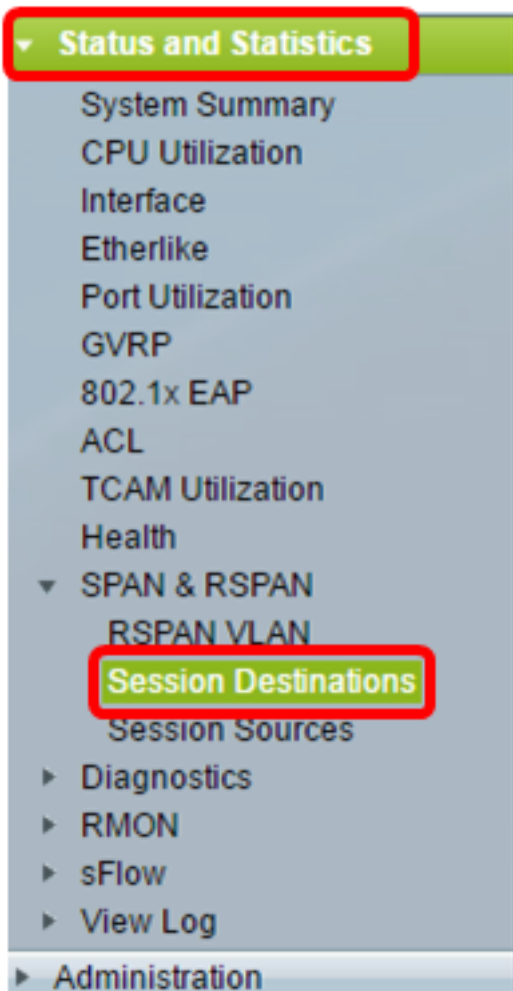
Filter: Session ID equals to

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

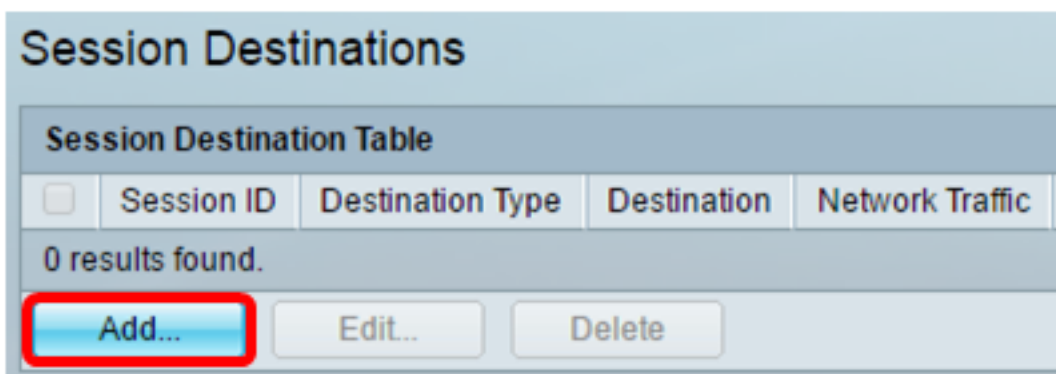
Agora você deve ter configurado a origem da sessão no Switch inicial.

Configurar destinos de sessão em um switch inicial

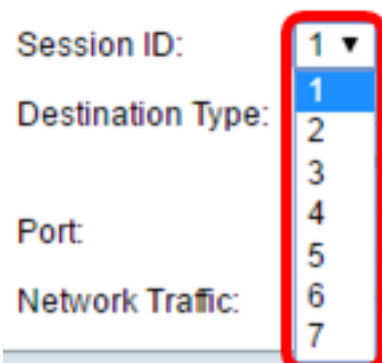
Etapa 1. Escolha **Status e Statistics > SPAN & RSPAN > Session Destinations**.



Etapa 2. Clique em Add.



Etapa 3. Escolha o número da sessão na lista suspensa ID da sessão. Ele deve ser o mesmo que o ID escolhido da origem da sessão configurada.



Note: Neste exemplo, a Sessão 1 é escolhida.

Etapa 4. Clique no botão de opção **VLAN remota** na área Tipo de destino. Um analisador de rede, como um computador que executa o Wireshark, está conectado a esta porta.

Importante: A interface de destino não pode ser a mesma da porta de origem.

Destination Type: Local Interface
 Remote VLAN (VLAN 20)

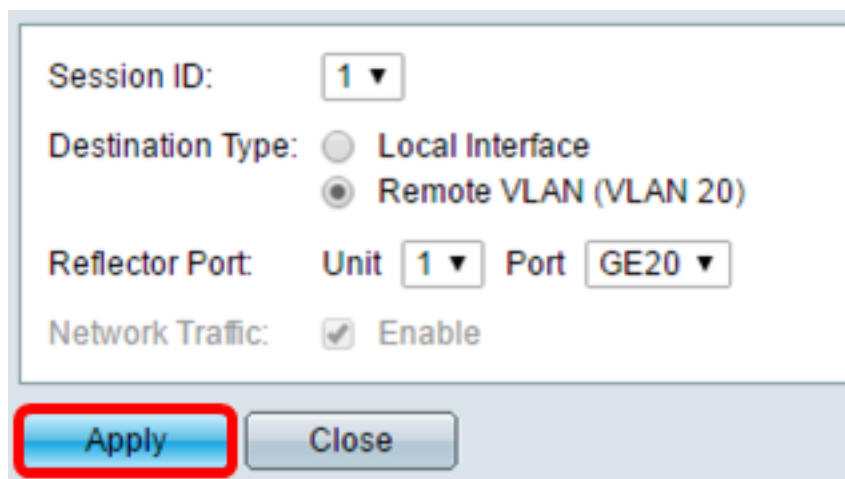
Note: Se a VLAN remota for escolhida, o tráfego de rede será automaticamente ativado.

Etapa 5. Na área Porta do refletor, escolha a opção desejada na lista suspensa Unidade. Escolha qual porta definir como a porta de origem na lista suspensa Porta.

Reflector Port: Unit Port
Network Traffic: Enable

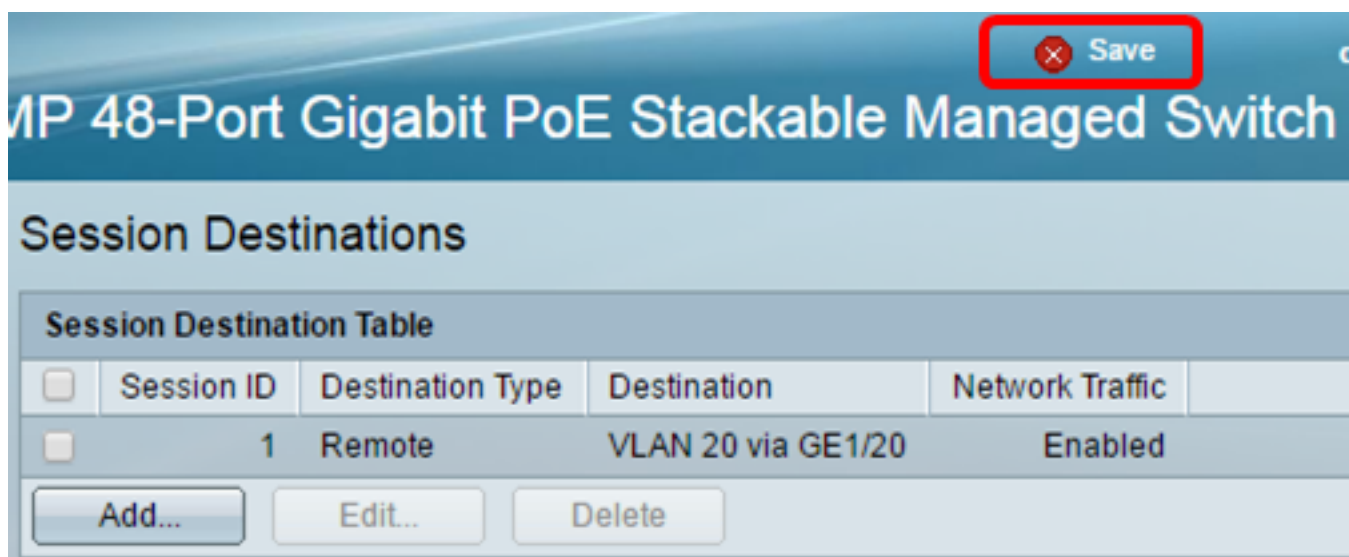
Note: Neste exemplo, a porta GE20 na Unidade 1 é escolhida.

Etapa 6. Clique em **Aplicar** e, em seguida, clique em **Fechar**.



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

Passo 7. (Opcional) Clique em **Salvar** para atualizar o arquivo de configuração atual.



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

Agora você deve ter configurado os destinos da sessão no Switch inicial.

Switches intermediários

Também pode haver switches intermediários separando as sessões de origem e de destino de RSPAN. Esses switches não precisam ser capazes de executar o RSPAN, mas devem responder aos requisitos da VLAN de RSPAN.

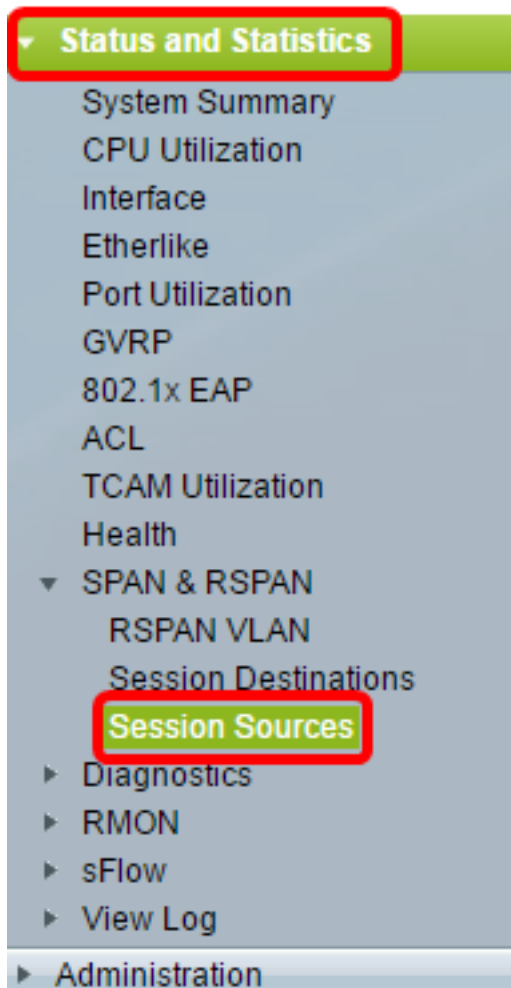
Para as VLANs 1 a 1005 que são visíveis para o VLAN Trunking Protocol (VTP), o ID da VLAN e suas características de RSPAN associadas são propagadas pelo VTP. Se você atribuir um ID de VLAN de RSPAN no intervalo de VLAN estendida (1006 a 4094), deverá configurar manualmente todos os switches intermediários.

Para saber como atribuir uma interface VLAN como porta de tronco de um switch intermediário, clique [aqui](#) para obter instruções.

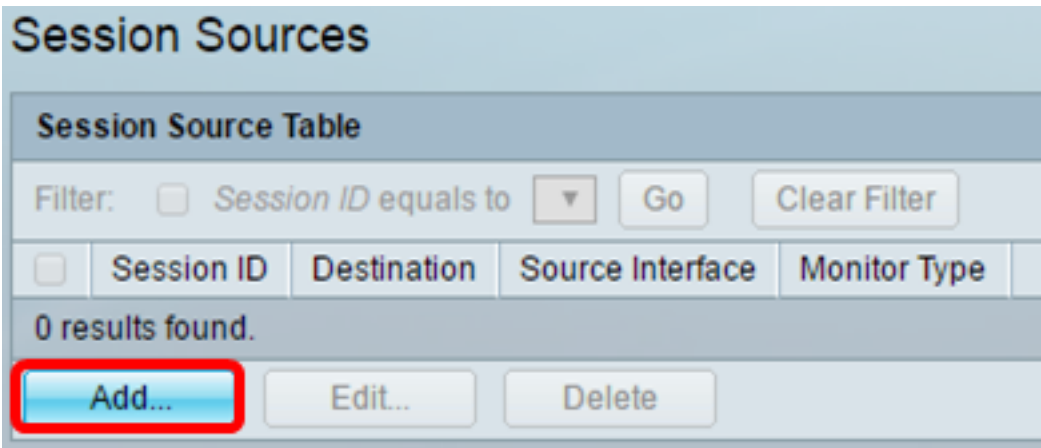
É normal ter várias VLANs de RSPAN em uma rede ao mesmo tempo, com cada VLAN de RSPAN definindo uma sessão de RSPAN em toda a rede. Ou seja, várias sessões de origem de RSPAN em qualquer lugar na rede podem contribuir com pacotes para a sessão de RSPAN. Também é possível ter várias sessões de destino de RSPAN em toda a rede, monitorando a mesma VLAN de RSPAN e apresentando o tráfego ao usuário. O ID da VLAN de RSPAN separa as sessões.

Configurar fontes de sessão em um switch final

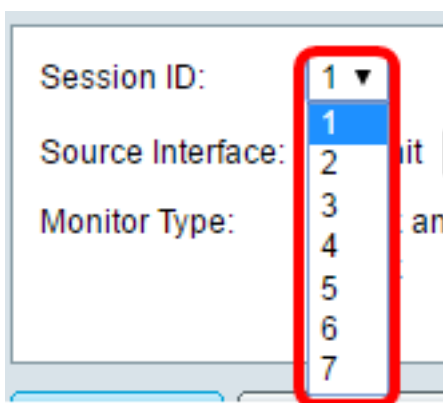
Etapa 1. Escolha **Status e Statistics > SPAN & RSPAN > Session Sources**.



Etapa 2. Clique em Add.

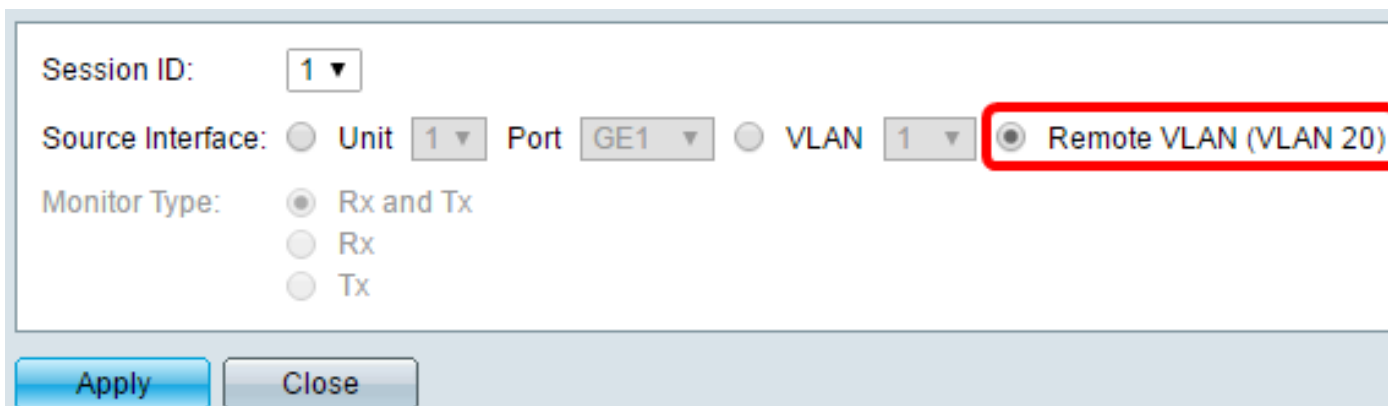


Etapa 3. (Opcional) Escolha o número da sessão na lista suspensa ID da sessão. A ID da sessão deve ser consistente por sessão.



Note: Neste exemplo, a Sessão 1 é escolhida.

Etapa 4. Clique no botão de opção **VLAN remota** na área Interface de origem.



Note: O tipo de monitor da VLAN remota será configurado automaticamente.

Etapa 5. Clique em **Aplicar** e, em seguida, clique em **Fechar**.

Etapa 6. (Opcional) Clique em **Salvar** para atualizar o arquivo de configuração atual.

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

Agora você deve ter configurado as origens da sessão no Switch final.

Configurar destinos de sessão em um switch final

Etapa 1. Escolha **Status e 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

Etapa 2. Clique em Add.

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"/>				

Etapa 3. Escolha o número da sessão na lista suspensa ID da sessão. Ele deve ser o mesmo que o ID escolhido da origem da sessão configurada.

Session ID:

Destination Type:

Port:

Network Traffic:

Note: Neste exemplo, a Sessão 1 é escolhida.

Etapa 4. Clique no botão de opção **Interface local** na área Tipo de destino.

Destination Type: Local Interface Remote VLAN (VLAN 20)

Etapa 5. Na área Porta, escolha a opção desejada na lista suspensa Unidade. Escolha qual porta definir como a porta de origem na lista suspensa Porta.

Port:

Network Traffic: Enable

Note: Neste exemplo, a porta GE20 na Unidade 1 é escolhida.

Etapa 6. (Opcional) Marque a caixa de seleção **Habilitar** Tráfego de Rede para habilitar o tráfego de rede.

Port:

Network Traffic: Enable

Passo 7. Clique em **Aplicar** e, em seguida, clique em **Fechar**.

Etapa 8. (Opcional) Clique em **Salvar** para atualizar o arquivo de configuração atual.



Agora você deve ter configurado os destinos da sessão no Switch final.

Analisar os pacotes de VLAN RSPAN capturados no WireShark

Neste cenário, o host na interface de origem configurada, GE2 na Unidade 1 (GE1/2), tem um endereço IP 192.168.1.100. Enquanto o host na interface de destino configurada, GE20 na Unidade 1 (VLAN 20 via GE1/20), tem um endereço IP 192.168.1.127. O Wireshark está sendo executado no host conectado a esta porta.

Usando o filtro `ip.addr == 192.168.1.100`, o Wireshark mostra os pacotes capturados da interface de origem 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

Exibir um vídeo relacionado a este artigo...

[Clique aqui para ver outras palestras técnicas da Cisco](#)