

Konfigurieren der RSPAN-Einstellungen (Remote Switch Port Analyzer) im Netzwerk

Inhaltsverzeichnis

- [Ziel](#)
- [Anwendbare Geräte | Firmware-Version](#)
- [Einführung](#)
- [Konfigurieren des RSPAN-VLANs auf dem Switch](#)
- [Konfigurieren von Sitzungsquellen auf einem Start-Switch](#)
- [Konfigurieren von Sitzungszielen auf einem Start-Switch](#)
- [Erweiterte Switches](#)
- [Konfigurieren von Sitzungsquellen auf einem abschließenden Switch](#)
- [Konfigurieren von Sitzungszielen auf einem letzten Switch](#)
- [Analyse der erfassten RSPAN-VLAN-Pakete in WireShark](#)

Ziel

Dieser Artikel enthält Anweisungen zur Konfiguration von RSPAN auf Switches.

Anwendbare Geräte | Firmware-Version

- Sx350 | 2.2.5.68 ([aktueller Download](#))
- SG350X | 2.2.5.68 ([aktueller Download](#))
- Sx550X | 2.2.5.68 ([aktueller Download](#))

Einführung

Switch Port Analyzer (SPAN), oder manchmal auch Portspiegelung oder Portüberwachung genannt, wählt Netzwerkverkehr zur Analyse durch einen Netzwerkanalyst aus. Der Netzwerkanalysator kann ein Cisco SwitchProbe-Gerät oder eine andere Remote Monitoring (RMON)-Prüfung sein.

Die Portspiegelung wird auf einem Netzwerkgerät verwendet, um eine Kopie der Netzwerkpakete zu senden, die auf einem einzelnen Geräteport, mehreren Geräteports oder einem gesamten VLAN (Virtual Local Area Network) an eine Netzwerküberwachungsverbindung an einem anderen Port des Geräts angezeigt werden. Dies wird häufig für Netzwerkgeräte verwendet, die eine Überwachung des Netzwerkverkehrs erfordern, z. B. ein Intrusion-Detection-System. Ein mit dem Überwachungsport verbundener Netzwerkanalysator verarbeitet die Datenpakete für Diagnose, Debugging und Leistungsüberwachung.

Remote Switch Port Analyzer (RSPAN) ist eine Erweiterung von SPAN. RSPAN erweitert SPAN, indem es die Überwachung mehrerer Switches im Netzwerk ermöglicht und die Definition des Analyzer-Ports auf einem Remote-Switch ermöglicht. Das bedeutet, dass Sie Ihre Netzwerkerfassungsgeräte zentralisieren können.

RSPAN spiegelt den Datenverkehr von den Quell-Ports einer RSPAN-Sitzung auf ein VLAN, das für die RSPAN-Sitzung dediziert ist. Dieses VLAN wird dann mit anderen Switches verbunden, sodass der Datenverkehr der RSPAN-Sitzung über mehrere Switches übertragen werden kann.

Auf dem Switch, der den Zielport für die Sitzung enthält, wird der Datenverkehr vom RSPAN-Session-VLAN einfach vom Zielport gespiegelt.

RSPAN-Datenverkehrsfluss

- Der Datenverkehr für jede RSPAN-Sitzung wird über ein vom Benutzer angegebenes RSPAN-VLAN übertragen, das für diese RSPAN-Sitzung in allen teilnehmenden Switches dediziert ist.
- Der Datenverkehr von den Quellschnittstellen des Startgeräts wird über einen Reflektorport in das RSPAN-VLAN kopiert. Dies ist ein physischer Port, der eingerichtet werden muss. Es wird ausschließlich zum Erstellen einer RSPAN-Sitzung verwendet.
- Dieser Reflektorport ist der Mechanismus, der Pakete in ein RSPAN-VLAN kopiert. Er leitet nur den Datenverkehr von der RSPAN-Quellsitzung weiter, der er zugeordnet ist. Jedes Gerät, das mit einem als Reflektorport festgelegten Port verbunden ist, verliert die Verbindung, bis die RSPAN-Quellsitzung deaktiviert ist.
- Der RSPAN-Datenverkehr wird dann über Trunk-Ports der zwischengeschalteten Geräte an die Zielsitzung am endgültigen Switch weitergeleitet.
- Der Ziel-Switch überwacht das RSPAN-VLAN und kopiert es in einen Zielport.

Regeln für die RSPAN-Port-Mitgliedschaft

- Auf allen Switches kann die Mitgliedschaft im RSPAN-VLAN nur mit Tags versehen werden.
 - Switch starten
- SPAN-Quellschnittstellen dürfen nicht Mitglieder des RSPAN-VLANs sein.
- Der Reflektorport darf kein Mitglied dieses VLANs sein.
- Es wird empfohlen, dass das Remote-VLAN über keine Mitgliedschaften verfügt.
- Zwischenschalter
- Es wird empfohlen, die RSPAN-Mitgliedschaft von allen Ports zu entfernen, die nicht für die Weiterleitung von gespiegeltem Datenverkehr verwendet werden.
- In der Regel enthält ein Remote-RSPAN-VLAN zwei Ports.
- Endgültiger Switch
- Bei gespiegeltem Datenverkehr müssen Quellports Mitglieder des RSPAN VLANs sein.
- Es wird empfohlen, die RSPAN-Mitgliedschaft von allen anderen Ports, einschließlich der Zielschnittstelle, zu entfernen.

RSPAN im Netzwerk konfigurieren

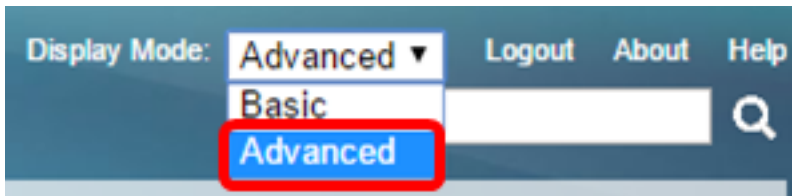
Konfigurieren des RSPAN-VLANs auf dem Switch

Das RSPAN-VLAN überträgt den SPAN-Datenverkehr zwischen Quell- und Zielsitzungen des RSPAN. Es zeichnet sich durch folgende besondere Merkmale aus:

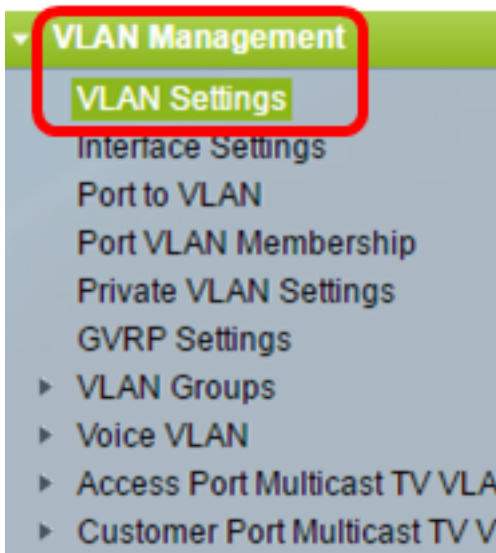
- Der gesamte Datenverkehr im RSPAN-VLAN wird immer geflutet.

- Im RSPAN-VLAN wird keine MAC-Adresserfassung (Media Access Control) durchgeführt.
- Der RSPAN-VLAN-Datenverkehr fließt nur über Trunk-Ports.
- STP kann auf RSPAN-VLAN-Trunks ausgeführt werden, jedoch nicht auf SPAN-Zielports.
- RSPAN-VLANs müssen im VLAN-Konfigurationsmodus auf dem Start- und dem Endswitch mithilfe des Befehls für den **Remote-Span-VLAN-Konfigurationsmodus** konfiguriert werden, oder befolgen Sie die folgenden Anweisungen:

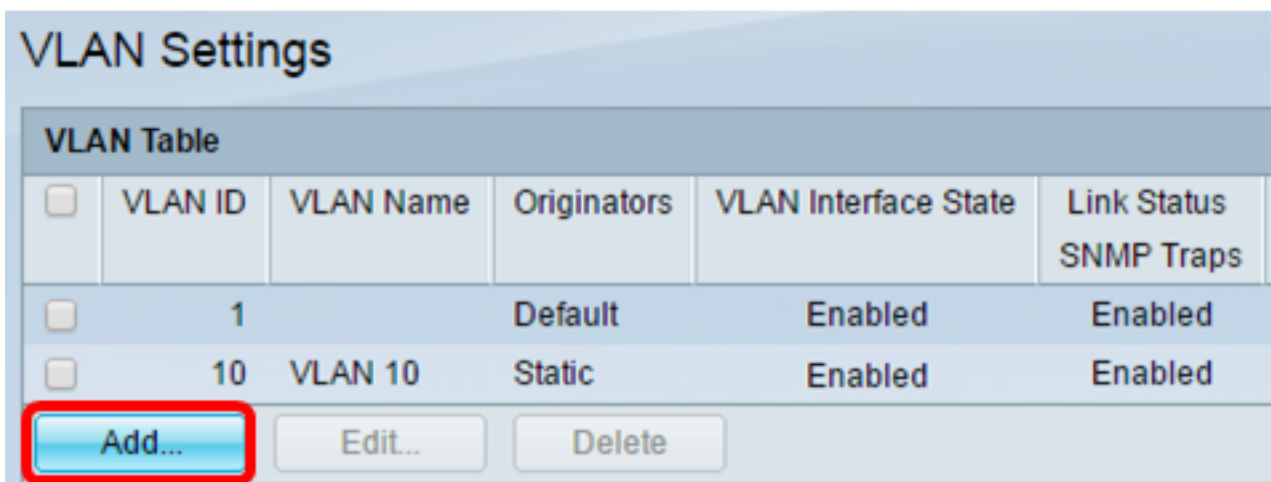
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Start Switches an, und wählen Sie in der Dropdown-Liste Anzeigemodus die Option **Erweitert** aus.



Schritt 2: Wählen Sie **VLAN Management > VLAN Settings** aus.



Schritt 3: Klicken Sie auf **Hinzufügen**.



Schritt 4: Geben Sie die VLAN-ID in das Feld *VLAN-ID* ein.

 VLAN ID: (Range: 2 - 4094)

Hinweis: In diesem Beispiel wird VLAN 20 als VLAN-ID verwendet.

Schritt 5: (Optional) Geben Sie im Feld *VLAN Name* den VLAN-Namen ein.

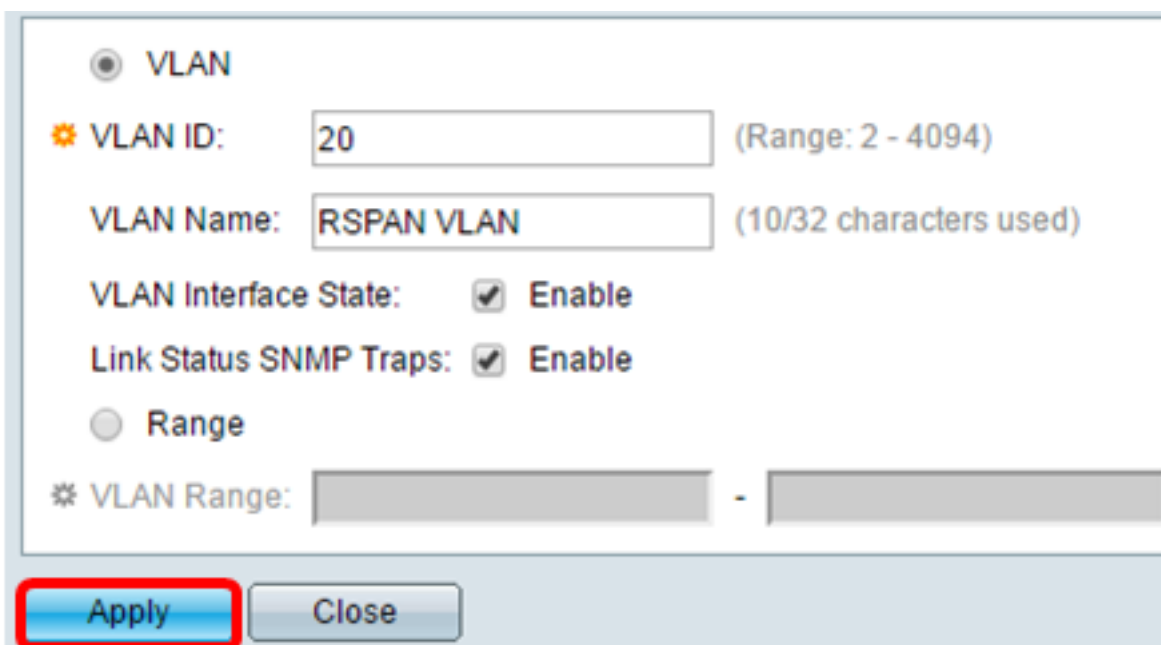
 VLAN ID: (Range: 2 - 4094)
VLAN Name: (10/32 characters used)

Hinweis: In diesem Beispiel wird das RSPAN-VLAN als VLAN-Name verwendet.


Schritt 6: (Optional) Aktivieren Sie das Kontrollkästchen *VLAN Interface State* (VLAN-Schnittstellenstatus), um das VLAN zu aktivieren. Wenn das VLAN heruntergefahren wird, sendet oder empfängt das VLAN keine Nachrichten von oder zu höheren Ebenen. Wenn Sie z. B. ein VLAN, auf dem eine IP-Schnittstelle konfiguriert ist, herunterfahren, wird das Bridging in das VLAN fortgesetzt. Der Switch kann jedoch keinen IP-Datenverkehr im VLAN übertragen und empfangen. Diese Funktion ist standardmäßig aktiviert.

Schritt 7: (Optional) Aktivieren Sie das Kontrollkästchen *Link Status SNMP Traps* (SNMP-Traps für den Verbindungsstatus), um die Generierung von SNMP-Traps (Simple Network Management Protocol) zu aktivieren. Diese Funktion ist standardmäßig aktiviert.

Schritt 8: Klicken Sie auf **Übernehmen** und anschließend auf **Schließen**.



VLAN

 VLAN ID: (Range: 2 - 4094)

VLAN Name: (10/32 characters used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

* VLAN Range: -

Hinweis: Weitere Informationen zur Verwaltung von VLANs auf einem Switch erhalten Sie [hier](#).

Schritt 9: (Optional) Klicken Sie auf **Speichern**, um die aktuelle Konfigurationsdatei zu aktualisieren.

MP 48-Port Gigabit PoE Stackable Managed Switch

Save

VLAN Settings

<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

Schritt 10: Wählen Sie **Status und Statistics > SPAN & RSPAN > RSPAN VLAN** aus.

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

Schritt 11: Wählen Sie in der Dropdown-Liste "RSPAN VLAN" eine VLAN-ID aus. Dieses VLAN sollte ausschließlich für RSPAN verwendet werden.

RSPAN VLAN

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

RSPAN VLAN: None ▼
None
10
20

Apply

Hinweis: In diesem Beispiel wird VLAN 20 ausgewählt.

Schritt 12: Klicken Sie auf **Übernehmen**.

RSPAN VLAN

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

RSPAN VLAN: 20 ▼

Apply Cancel

Schritt 13: (Optional) Klicken Sie auf **Speichern**, um die aktuelle Konfigurationsdatei zu aktualisieren.

✖ 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 ▼

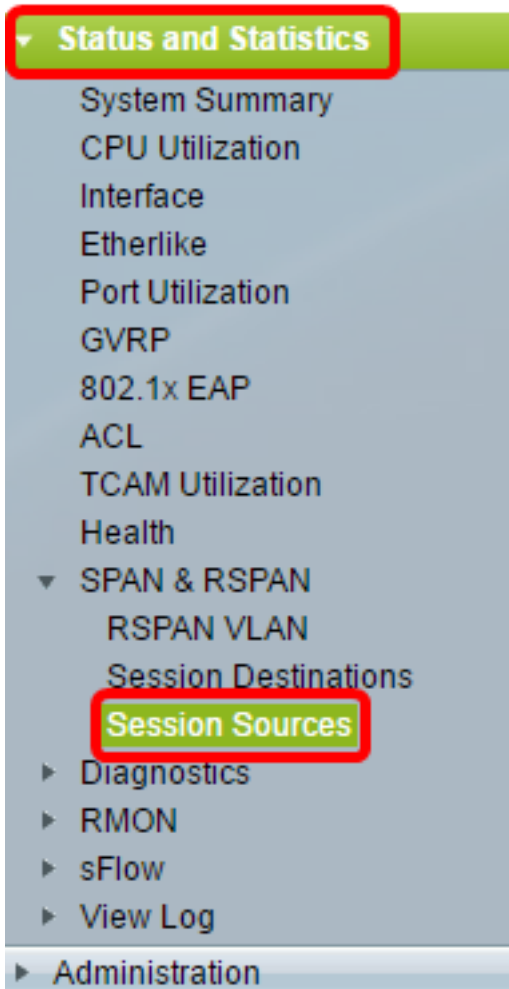
Apply Cancel

Schritt 14: Wiederholen Sie im abschließenden Switch die Schritte 1 bis 13, um das RSPAN-VLAN zu konfigurieren.

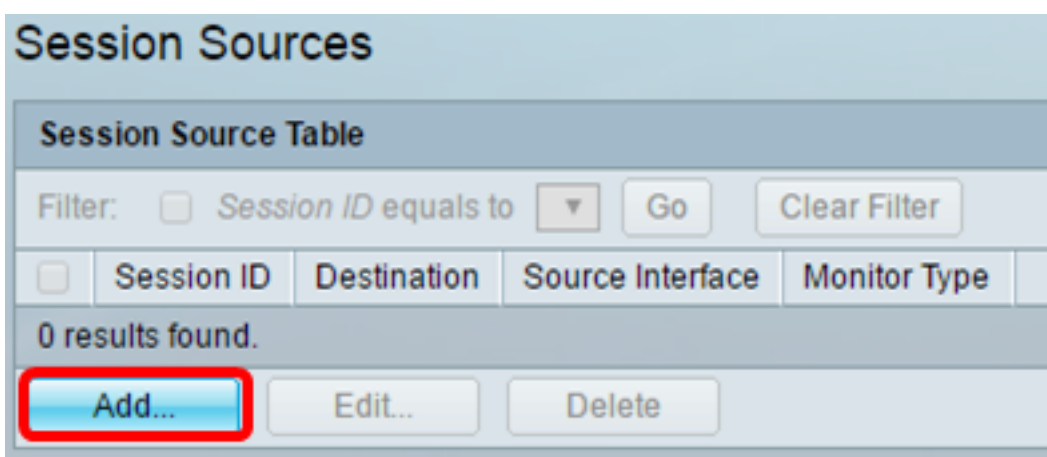
Sie sollten jetzt das VLAN konfiguriert haben, das für die RSPAN-Sitzung auf den Start- und Endswitches reserviert ist.

Konfigurieren von Sitzungsquellen auf einem Start-Switch

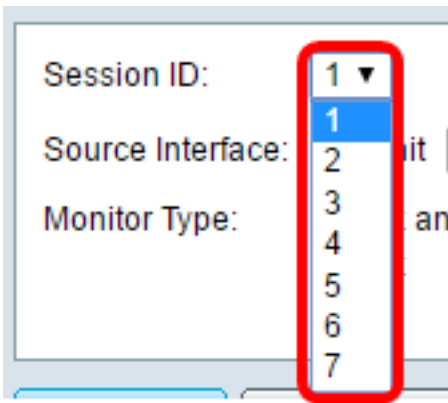
Schritt 1: Wählen Sie **Status und Statistics > SPAN & RSPAN > Session Sources** (Status und Statistiken).



Schritt 2: Klicken Sie auf **Hinzufügen**.



Schritt 3: Wählen Sie in der Dropdown-Liste Session ID (Sitzungs-ID) die Sitzungsnummer aus. Die Sitzungs-ID muss für jede RSPAN-Sitzung konsistent sein.



Hinweis: In diesem Beispiel wird Session 1 ausgewählt.

Schritt 4: Klicken Sie auf das Optionsfeld für den gewünschten Schnittstellentyp, und wählen Sie die Schnittstelle aus der Dropdown-Liste oder den Listen aus.

Wichtig: Die Quellschnittstelle kann nicht mit dem Ziel-Port identisch sein.



Folgende Optionen stehen zur Verfügung:

- Einheit und Port - Sie können die gewünschte Option aus der Dropdown-Liste "Einheit" auswählen und aus der Dropdown-Liste "Port" auswählen, welcher Port als Quellport festgelegt werden soll.
- VLAN: In der VLAN-Dropdown-Liste können Sie das zu überwachende VLAN auswählen. Ein VLAN unterstützt eine Gruppe von Hosts bei der Kommunikation, als befänden sie sich im selben physischen Netzwerk, unabhängig von ihrem Standort. Wenn diese Option ausgewählt ist, konnte sie nicht bearbeitet werden.
- Remote-VLAN - Zeigt das definierte RSPAN-VLAN an. Wenn diese Option ausgewählt ist, konnte sie nicht bearbeitet werden.

Hinweis: In diesem Beispiel wird Port GE2 in Einheit 1 ausgewählt. Dies ist die Remote-Schnittstelle, die überwacht wird.

Schritt 5: (Optional) Wenn in Schritt 4 auf Einheit und Port geklickt wird, klicken Sie auf das Optionsfeld des gewünschten Monitortyps für den zu überwachenden Datenverkehr.



Folgende Optionen stehen zur Verfügung:

- Rx und Tx: Diese Option ermöglicht die Portspiegelung eingehender und ausgehender Pakete. Diese Option wird standardmäßig ausgewählt.
- Rx (Rx): Diese Option ermöglicht die Portspiegelung eingehender Pakete.
- Tx: Diese Option ermöglicht die Portspiegelung ausgehender Pakete.

Hinweis: In diesem Beispiel wird Rx ausgewählt.

Schritt 6: Klicken Sie auf **Übernehmen** und anschließend auf **Schließen**.

Session ID:

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

Monitor Type: Rx and Tx
 Rx
 Tx

Schritt 7: (Optional) Klicken Sie auf **Speichern**, um die aktuelle Konfigurationsdatei zu aktualisieren.

MP 48-Port Gigabit PoE Stackable Managed Switch

Session Sources

Session Source Table

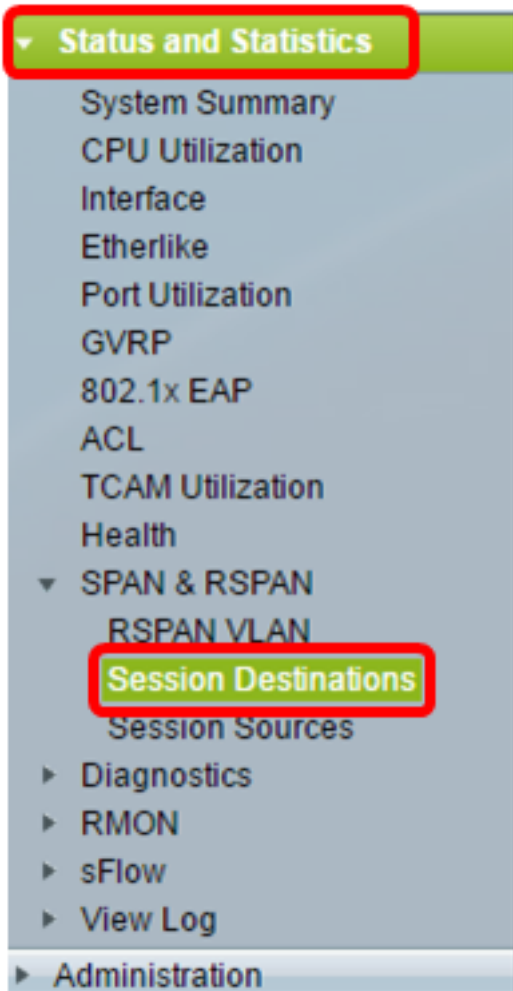
Filter: Session ID equals to

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

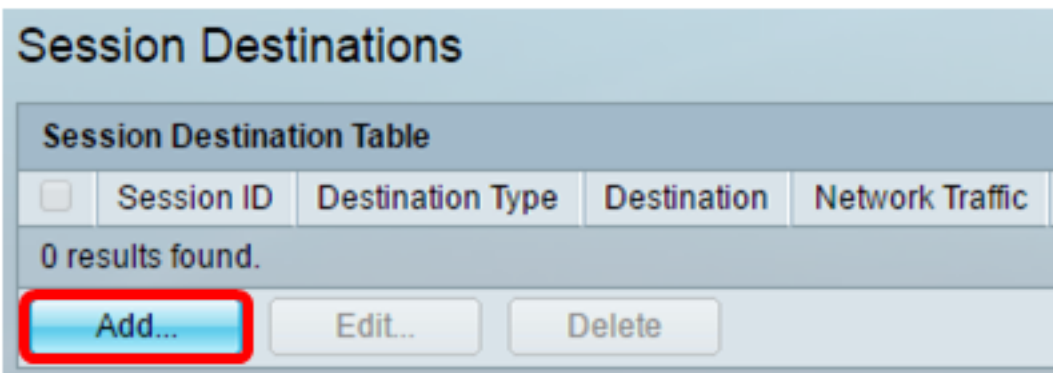
Sie sollten jetzt die Sitzungsquelle auf dem Start Switch konfiguriert haben.

Konfigurieren von Sitzungszielen auf einem Start-Switch

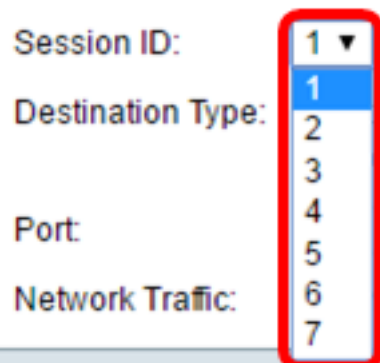
Schritt 1: Wählen Sie **Status und Statistik > SPAN & RSPAN > Session Destinations** aus.



Schritt 2: Klicken Sie auf **Hinzufügen**.



Schritt 3: Wählen Sie in der Dropdown-Liste Session ID (Sitzungs-ID) die Sitzungsnummer aus. Sie muss mit der ausgewählten ID aus der konfigurierten Sitzungsquelle übereinstimmen.



Hinweis: In diesem Beispiel wird Session 1 ausgewählt.

Schritt 4: Klicken Sie im Bereich "Zieltyp" auf das Optionsfeld **Remote VLAN**. Ein Netzwerkanalysator, wie z. B. ein Computer mit Wireshark, ist mit diesem Port verbunden.

Wichtig: Die Zielschnittstelle kann nicht mit dem Quellport identisch sein.

Destination Type: Local Interface
 Remote VLAN (VLAN 20)

Hinweis: Wenn Remote-VLAN ausgewählt wird, wird der Netzwerkverkehr automatisch aktiviert.

Schritt 5: Wählen Sie im Bereich Reflector Port (Reflektorport) die gewünschte Option aus der Dropdown-Liste Unit (Einheit) aus. Wählen Sie aus der Dropdown-Liste Port aus, welcher Port als Quellport festgelegt werden soll.

Reflector Port: Unit Port
Network Traffic: Enable

Hinweis: In diesem Beispiel wird Port GE20 in Einheit 1 ausgewählt.

Schritt 6: Klicken Sie auf **Übernehmen** und anschließend auf **Schließen**.

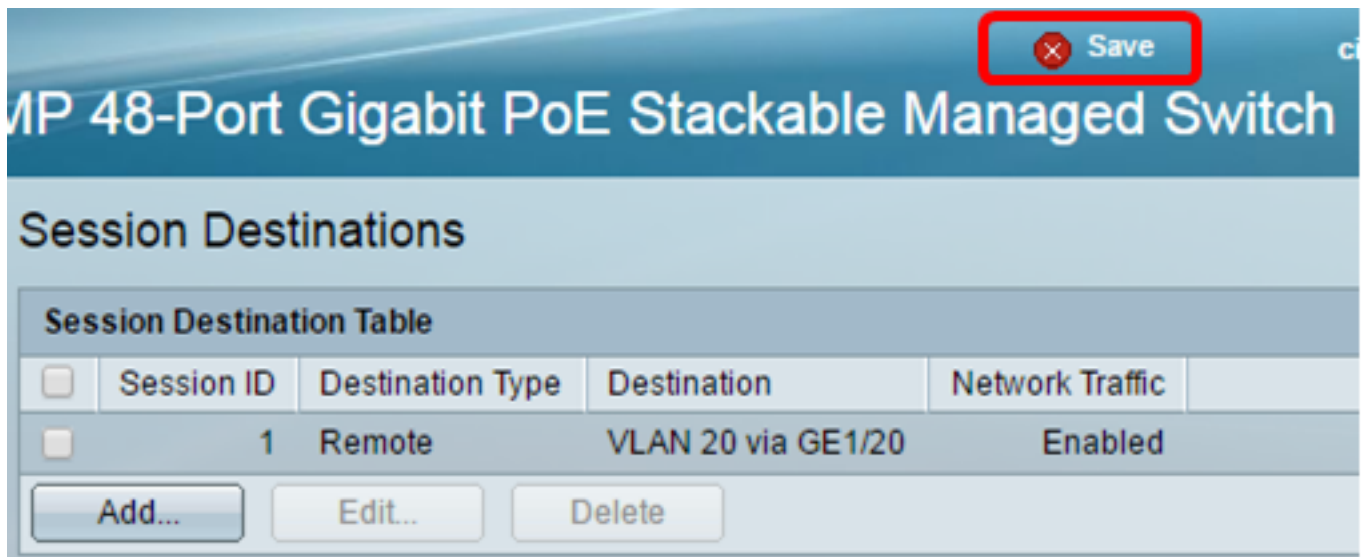
Session ID:

Destination Type: Local Interface
 Remote VLAN (VLAN 20)

Reflector Port: Unit Port

Network Traffic: Enable

Schritt 7: (Optional) Klicken Sie auf **Speichern**, um die aktuelle Konfigurationsdatei zu aktualisieren.



Sie sollten jetzt die Sitzungsziele auf Ihrem Start Switch konfiguriert haben.

Erweiterte Switches

Es können auch zwischengeschaltete Switches vorhanden sein, die die Quell- und Zielsitzungen des RSPAN trennen. Diese Switches müssen nicht für den Betrieb von RSPAN geeignet sein, sondern den Anforderungen des RSPAN-VLAN entsprechen.

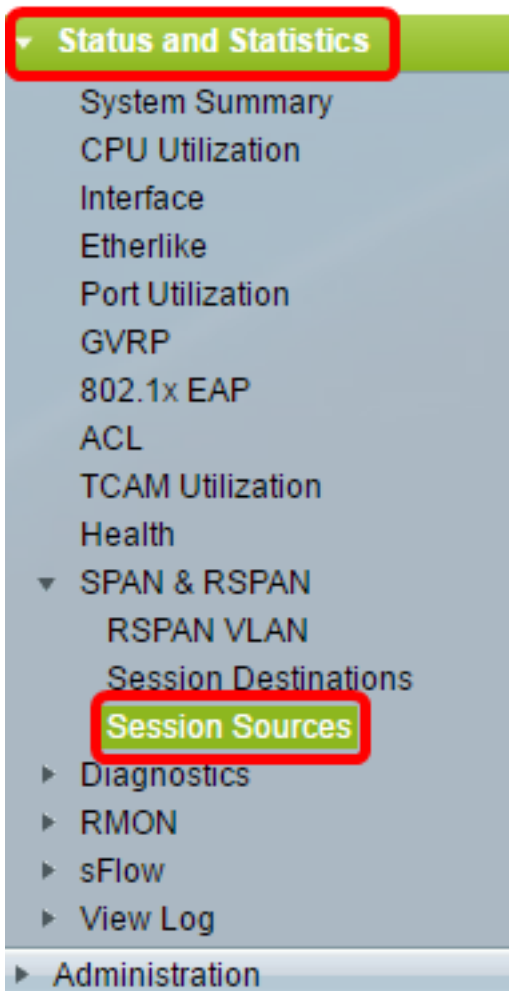
Für VLANs 1 bis 1005, die für VLAN Trunking Protocol (VTP) sichtbar sind, werden die VLAN-ID und die zugehörigen RSPAN-Merkmale vom VTP propagiert. Wenn Sie eine RSPAN-VLAN-ID im erweiterten VLAN-Bereich (1006 bis 4094) zuweisen, müssen Sie alle Zwischen-Switches manuell konfigurieren.

Um zu erfahren, wie Sie ein Schnittstellen-VLAN als Trunk-Port eines zwischengeschalteten Switches zuweisen, klicken Sie [hier](#), um Anweisungen zu erhalten.

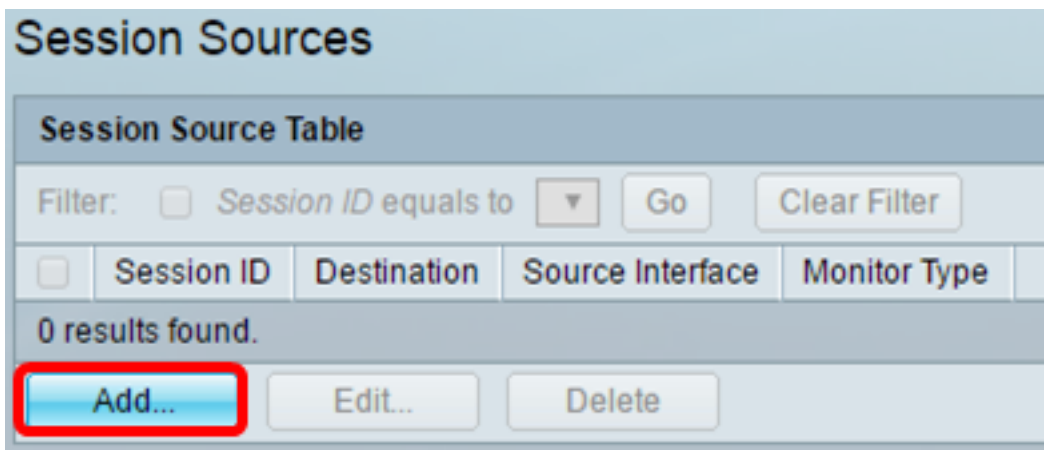
Es ist normal, dass in einem Netzwerk mehrere RSPAN-VLANs gleichzeitig vorhanden sind, während jedes RSPAN-VLAN eine netzwerkweite RSPAN-Sitzung definiert. Das heißt, mehrere RSPAN-Quellsitzungen im gesamten Netzwerk können Pakete zur RSPAN-Sitzung beitragen. Es ist auch möglich, im gesamten Netzwerk mehrere RSPAN-Zielsitzungen einzurichten, um dasselbe RSPAN-VLAN zu überwachen und Datenverkehr an den Benutzer zu übertragen. Die RSPAN-VLAN-ID trennt die Sitzungen.

Konfigurieren von Sitzungsquellen auf einem abschließenden Switch

Schritt 1: Wählen Sie **Status und Statistics > SPAN & RSPAN > Session Sources (Status und Statistiken)**.



Schritt 2: Klicken Sie auf **Hinzufügen**.



Schritt 3: (Optional) Wählen Sie in der Dropdown-Liste Session ID (Sitzungs-ID) die Sitzungsnummer aus. Die Sitzungs-ID muss für jede Sitzung konsistent sein.

Session ID: 1 ▾
 Source Interface: 1
 Monitor Type: 2
 3
 4
 5
 6
 7

Hinweis: In diesem Beispiel wird Session 1 ausgewählt.

Schritt 4: Klicken Sie im Bereich "Quellschnittstelle" auf das Optionsfeld **Remote VLAN**.

Session ID: 1 ▾
 Source Interface: Unit 1 ▾ Port GE1 ▾ VLAN 1 ▾ Remote VLAN (VLAN 20)
 Monitor Type: Rx and Tx
 Rx
 Tx

Apply Close

Hinweis: Der Monitortyp des Remote-VLAN wird automatisch konfiguriert.

Schritt 5: Klicken Sie auf **Übernehmen** und anschließend auf **Schließen**.

Schritt 6: (Optional) Klicken Sie auf **Speichern**, um die aktuelle Konfigurationsdatei zu aktualisieren.

Save

MP 48-Port Gigabit PoE Stackable Managed Switch

Session Sources

Session Source Table

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

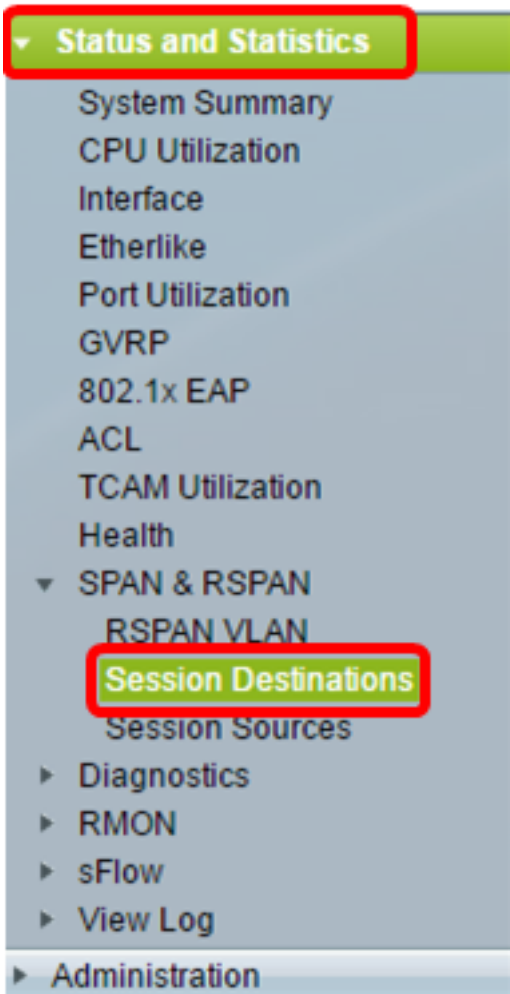
<input type="checkbox"/>	Session ID	Destination	Source Interface	Monitor Type
<input type="checkbox"/>	1	VLAN 20		Rx

Add... Edit... Delete

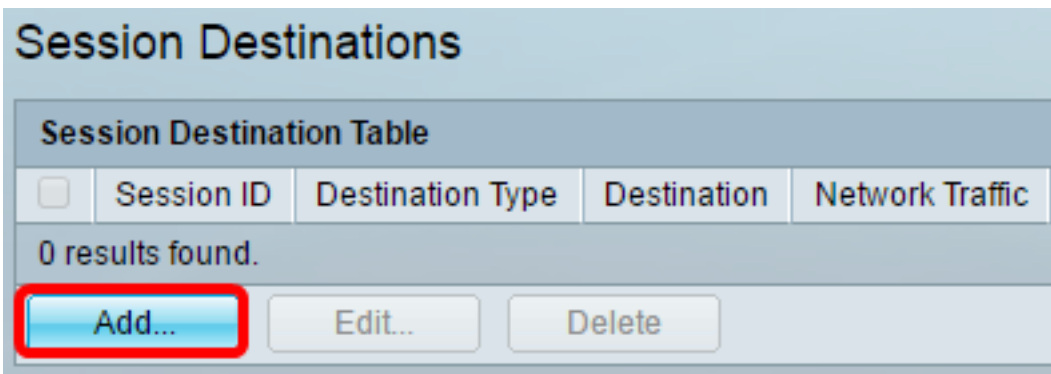
Sie sollten jetzt die Sitzungsquellen auf dem abschließenden Switch konfiguriert haben.

Konfigurieren von Sitzungszielen auf einem letzten Switch

Schritt 1: Wählen Sie **Status und Statistik > SPAN & RSPAN > Session Destinations** aus.



Schritt 2: Klicken Sie auf **Hinzufügen**.



Schritt 3: Wählen Sie in der Dropdown-Liste Session ID (Sitzungs-ID) die Sitzungsnummer aus. Sie muss mit der ausgewählten ID aus der konfigurierten Sitzungsquelle übereinstimmen.

Session ID: 1 ▾
Destination Type: 1
2
3
4
Port: 5
6
Network Traffic: 7

Hinweis: In diesem Beispiel wird Session 1 ausgewählt.

Schritt 4: Klicken Sie im Bereich Zieltyp auf das Optionsfeld **Lokale Schnittstelle**.

Destination Type: Local Interface
 Remote VLAN (VLAN 20)

Schritt 5: Wählen Sie im Bereich Port die gewünschte Option aus der Dropdown-Liste Unit (Einheit) aus. Wählen Sie aus der Dropdown-Liste Port aus, welcher Port als Quellport festgelegt werden soll.

Port: Unit 1 ▾ Port GE20 ▾
Network Traffic: Enable

Hinweis: In diesem Beispiel wird Port GE20 in Einheit 1 ausgewählt.

Schritt 6: (Optional) Aktivieren Sie das Kontrollkästchen Netzwerkverkehr **aktivieren**, um Netzwerkverkehr zu aktivieren.

Port: Unit 1 ▾ Port GE20 ▾
Network Traffic: Enable

Schritt 7: Klicken Sie auf **Übernehmen** und anschließend auf **Schließen**.

Schritt 8: (Optional) Klicken Sie auf **Speichern**, um die aktuelle Konfigurationsdatei zu aktualisieren.



Sie sollten jetzt die Sitzungsziele auf Ihrem letzten Switch konfiguriert haben.

Analyse der erfassten RSPAN-VLAN-Pakete in WireShark

In diesem Szenario hat der Host in der konfigurierten Quellschnittstelle GE2 in Einheit 1 (GE1/2) die IP-Adresse 192.168.1.100. Während der Host in der konfigurierten Zielschnittstelle, GE20 in Einheit 1 (VLAN 20 über GE1/20), die IP-Adresse 192.168.1.127 hat. Wireshark wird auf dem Host ausgeführt, der mit diesem Port verbunden ist.

Mit dem Filter `ip.addr == 192.168.1.100` zeigt Wireshark die erfassten Pakete von der Remote-Quellschnittstelle an.

*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

Sehen Sie sich ein Video zu diesem Artikel an..

[Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.](#)