

Instellingen Remote Switch Port Analyzer (RSPAN) op het netwerk configureren

Inhoud

- [Doel](#)
- [Toepasselijke apparaten | Versie firmware](#)
- [Inleiding](#)
- [RSPAN VLAN op de switch configureren](#)
- [Sessiebronnen op een Start-switch configureren](#)
- [Sessiebestemmingen instellen op een Start-switch](#)
- [Intermediate-switches](#)
- [Sessiebronnen op een eindswitch configureren](#)
- [Sessiebestemmingen op een eindswitch configureren](#)
- [De opgenomen RSPAN VLAN-pakketten in WireShark analyseren](#)

Doel

Dit artikel bevat instructies over de manier waarop u RSPAN op uw switches kunt configureren.

Toepasselijke apparaten | Versie firmware

- SX350 | 2.2.5.68 ([laatste download](#))
- SG350X-software | 2.2.5.68 ([laatste download](#))
- SX550X | 2.2.5.68 ([laatste download](#))

Inleiding

Switch Port Analyzer (SPAN), of soms port mirroring of port monitoring, kiest netwerkverkeer voor analyse door een netwerkanalyzer. De netwerkanalyzer kan een Cisco SwitchProbe-apparaat of een andere RMON-test (Remote Monitoring) zijn.

Port mirroring wordt op een netwerkkapparaat gebruikt om een kopie van netwerkpakketten te verzenden die gezien worden op één apparaatpoort, meerdere apparaatpoorten of een compleet Virtual Local Area Network (VLAN), naar een netwerkbewakingsverbinding op een andere poort op het apparaat. Dit wordt algemeen gebruikt voor netwerkkapparatuur die bewaking van het netwerkverkeer vereist, zoals een inbraakdetectiesysteem. Een netwerkanalyzer die op de controlepoort is aangesloten verwerkt de gegevenspakketten voor het diagnosticeren, het zuiveren, en de prestatiecontrole.

Remote Switch Port Analyzer (RSPAN) is een uitbreiding van SPAN. RSPAN breidt SPAN uit door controle van meerdere switches over uw netwerk mogelijk te maken en de analisatiepoort op een afstandsschakelaar te definiëren. Dit betekent dat u uw netwerkopnamestation kunt centraliseren.

RSPAN werkt door het verkeer van de bronpoorten van een RSPAN-sessie naar een VLAN te spiegelen dat gewijd is aan de RSPAN-sessie. Dit VLAN wordt dan getrunked naar andere switches, zodat het RSPAN sessieverkeer over meerdere switches kan worden getransporteerd. Op de switch die de doelpoort voor de sessie bevat, wordt het verkeer van de RSPAN-sessie VLAN simpelweg uitgevat in de doelpoort.

RSPAN-verkeersstroom

- Het verkeer voor elke RSPAN-sessie wordt overgedragen via een door de gebruiker opgegeven RSPAN VLAN dat geormerkt wordt voor die RSPAN-sessie in alle deelnemende switches.
- Het verkeer van de broninterfaces op het beginapparaat wordt gekopieerd naar RSPAN VLAN door een reflectorpoort. Dit is een fysieke poort die moet worden ingesteld. Het wordt uitsluitend gebruikt om een RSPAN-sessie op te bouwen.
- Deze reflectorpoort is het mechanisme dat pakketten aan een RSPAN VLAN kopieert. Het zendt alleen het verkeer door van de RSPAN-bronsessie waarmee het verbonden is. Elk apparaat dat is aangesloten op een poort dat is ingesteld als reflectorpoort verliest connectiviteit tot de RSPAN bronsessie is uitgeschakeld.
- RSPAN-verkeer wordt vervolgens via boomstampoorten op de tussenliggende apparaten doorgestuurd naar de doelsessie op de eindschakelaar.
- De doelschakelaar controleert RSPAN VLAN en kopieert het naar een doelpoort.

RSPAN-regels voor poortleden

- Op alle switches - Membership in RSPAN VLAN kan alleen worden getagd.
 - Start switch
- SPAN-broninterfaces kunnen geen leden zijn van RSPAN VLAN.
- De reflectiepoort kan geen lid van dit VLAN zijn.
- Aanbevolen wordt dat het VLAN op afstand geen lidmaatschap heeft.
- Intermediaire switch
- Het wordt aanbevolen het RSPAN-lidmaatschap te schrappen van alle havens die niet voor het doorgeven van gespiegeld verkeer worden gebruikt.
- Gewoonlijk bevat een RSPAN-venster op afstand twee poorten.
- Eindswitch
- Voor gespiegeld verkeer moeten bronpoorten leden van RSPAN VLAN zijn.
- Het wordt aanbevolen het RSPAN-lidmaatschap uit alle andere havens, inclusief de doelinterface, te verwijderen.

RSPAN op het netwerk configureren

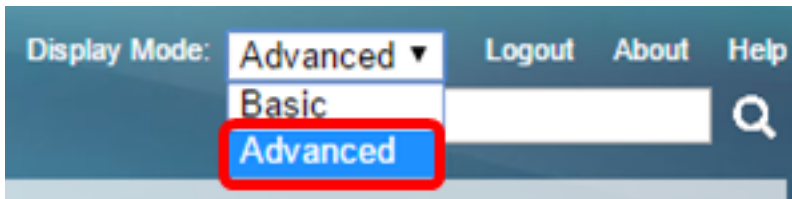
RSPAN VLAN op de switch configureren

RSPAN VLAN vervoert SPAN-verkeer tussen RSPAN-bron- en doelsessies. Het heeft deze bijzondere kenmerken:

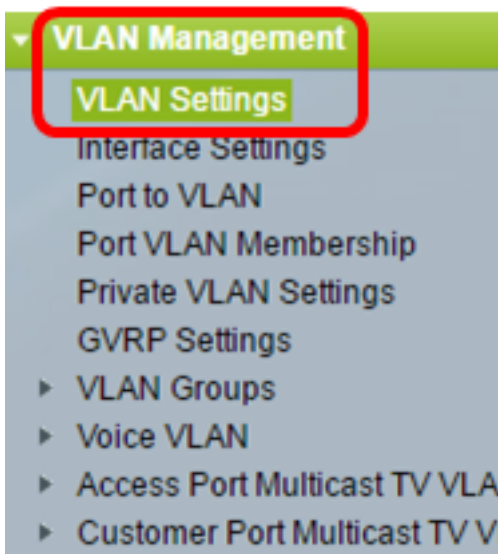
- Al het verkeer in RSPAN VLAN wordt altijd overstromd.
- Er is geen MAC-adresstudie (Media Access Control) op RSPAN VLAN.
- RSPAN VLAN-verkeer stroomt alleen op boompoorten.
- STP kan op RSPAN VLAN-trunks worden uitgevoerd maar niet op SPAN-doelpoorten.

- RSPAN VLAN's moeten op zowel Start- als Eindswitches in VLAN-configuratiemodus worden geconfigureerd door de opdracht VLAN-configuratiemodus op afstand te gebruiken, of de onderstaande instructies te volgen:

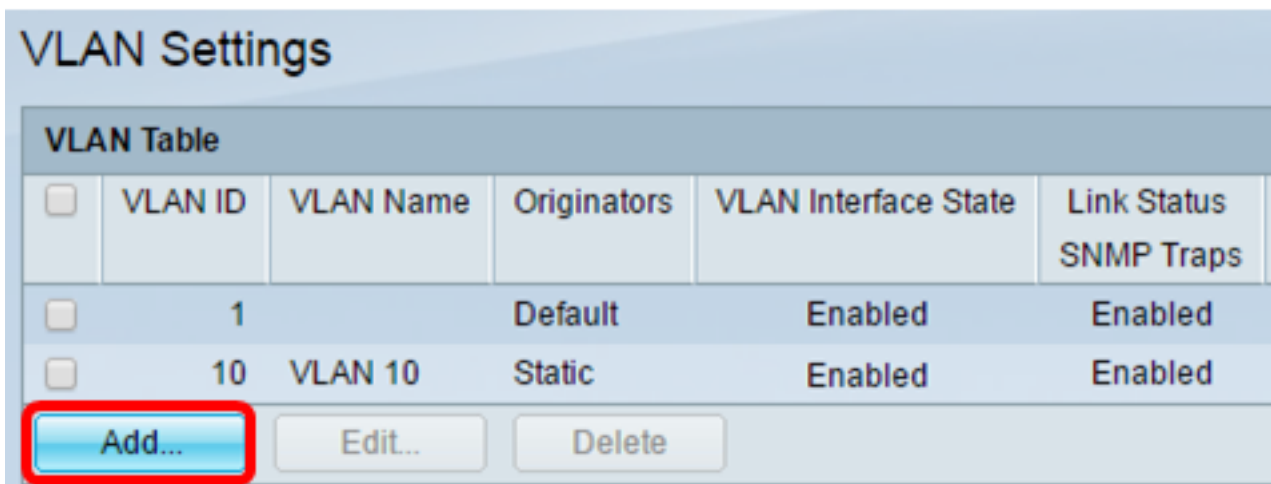
Stap 1. Meld u aan bij het op web gebaseerde hulpprogramma van de Start-switch en kies **Geavanceerd** in de vervolgkeuzelijst Weergavemodus.



Stap 2. Kies **VLAN-beheer > VLAN-instellingen**.



Stap 3. Klik op **Add**.



Stap 4. Voer de VLAN-id in het veld *VLAN-id* in.



Opmerking: In dit voorbeeld wordt VLAN 20 gebruikt als VLAN-id.

Stap 5. (Optioneel) Voer de VLAN-naam in het veld *VLAN-naam* in.

⚙️ VLAN ID: (Range: 2 - 4094)

VLAN Name: (10/32 characters used)

Opmerking: In dit voorbeeld wordt RSPAN VLAN gebruikt als de naam van VLAN.

Stap 6. (Optioneel) Controleer het aankruisvakje VLAN-interfacestatus om het VLAN in te schakelen. Als het VLAN is shutdown, brengt VLAN geen berichten van of aan hogere niveaus over of ontvangt. Als u bijvoorbeeld een VLAN sluit, waarop een IP-interface is geconfigureerd, wordt het overbruggen in het VLAN voortgezet, maar de switch kan IP-verkeer op het VLAN niet verzenden en ontvangen. Deze optie is standaard ingeschakeld.

Stap 7. (Optioneel) Controleer het aanvinkvakje Link Status SNMP Traps om de generatie van de verbindingstatus van Eenvoudig Network Management Protocol (SNMP)-traps mogelijk te maken. Deze optie is standaard ingeschakeld.

Stap 8. Klik op **Toepassen** en vervolgens op **Sluiten**.

VLAN

⚙️ VLAN ID: (Range: 2 - 4094)

VLAN Name: (10/32 characters used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

* VLAN Range: -

Apply Close

Opmerking: Om meer te weten te komen over het beheer van VLAN's op een switch, klik [hier](#).

Stap 9. (Optioneel) Klik op **Opslaan** om het actieve configuratiebestand bij te werken.

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

Stap 10. Kies **Status en statistieken > 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

Stap 1. Kies een VLAN-id in de vervolgkeuzelijst RSPAN VLAN. Dit VLAN dient uitsluitend voor RSPAN te worden gebruikt.

RSPAN VLAN

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

RSPAN VLAN: None ▼
None
10
20

Apply

Opmerking:In dit voorbeeld wordt VLAN 20 geselecteerd.

Stap 12. Klik op **Toepassen**.

RSPAN VLAN

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

RSPAN VLAN: 20 ▼

Apply Cancel

Stap 13. (Optioneel) Klik op **Save** om het actieve configuratiebestand te wijzigen.

✖ 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 ▼

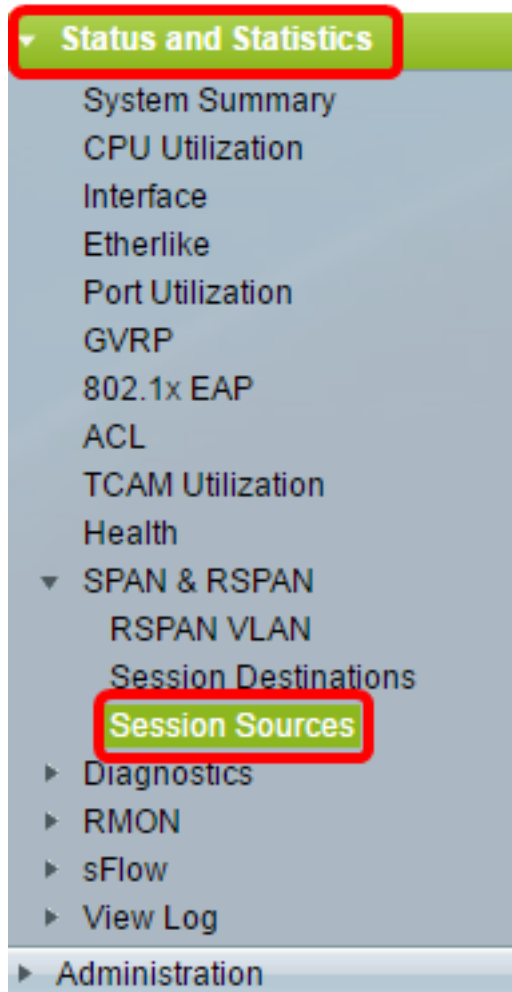
Apply Cancel

Stap 14. In de eindswitch herhaalt u stappen 1 tot 13 om RSPAN VLAN te configureren.

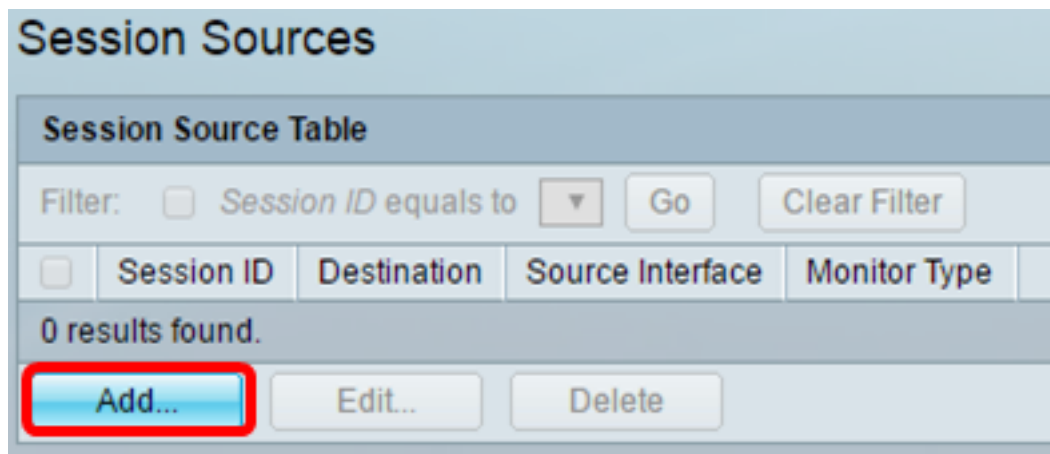
U dient nu het VLAN te hebben geconfigureerd dat wordt toegewijd aan de RSPAN-sessie in zowel Start- als eindswitches.

Sessiebronnen op een Start-switch configureren

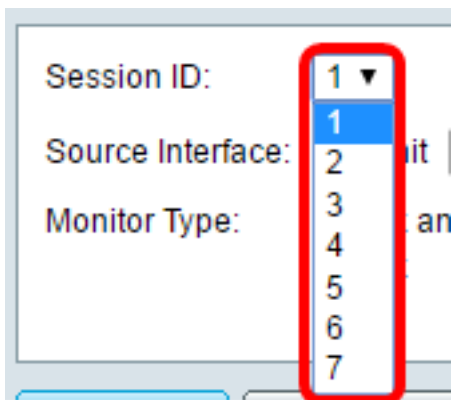
Stap 1. Kies **Status en statistieken** > **SPAN & RSPAN** > **Sessiebronnen**.



Stap 2. Klik op **Add**.



Stap 3. Kies het sessienummer in de vervolgleuzelijst Session-ID. Session-ID moet per RSPAN-sessie consistent zijn.



Opmerking: In dit voorbeeld wordt Session 1 gekozen.

Stap 4. Klik op de radioknop voor het gewenste broninterfacetype, en kies de interface in de vervolgkeuzelijst of de lijsten.

Belangrijk: De Bron Interface kan niet hetzelfde zijn als de Destination Port.



De opties zijn:

- Eenheid en poort - U kunt de gewenste optie uit de vervolgkeuzelijst Eenheid kiezen en kiezen welke poort u als bronpoort wilt instellen in de vervolgkeuzelijst Port.
- VLAN — U kunt het gewenste VLAN kiezen om te controleren van de vervolgkeuzelijst VLAN. Een VLAN helpt een groep hosts te communiceren alsof ze op hetzelfde fysieke netwerk zijn, ongeacht hun locatie. Als u deze optie selecteert, kan deze niet worden bewerkt.
- AfstandsVLAN — Dit zal het gedefinieerde RSPAN VLAN weergeven. Als u deze optie selecteert, kan deze niet worden bewerkt.

Opmerking: In dit voorbeeld wordt poort GE2 in Eenheid 1 geselecteerd. Dit is de interface op afstand die zou worden bewaakt.

Stap 5. (Optioneel) Als op de unit en de poort in Stap 4 is gedrukt, klikt u op de gewenste radioknop voor monitor-type.



De opties zijn:

- RX en TX — Deze optie maakt poortbewaking van inkomende en uitgaande pakketten mogelijk. Deze optie wordt standaard geselecteerd.
- RX - Met deze optie is het mogelijk dat poorten worden gespiegeld van inkomende pakketten.
- TX — Deze optie maakt poortbewaking van uitgaande pakketten mogelijk.

Opmerking: In dit voorbeeld wordt RX gekozen.

Stap 6. Klik op **Toepassen** en vervolgens op **Sluiten**.

Session ID:

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

Monitor Type: Rx and Tx
 Rx
 Tx

Stap 7. (Optioneel) Klik op **Opslaan** om het actieve configuratiebestand bij te werken.

MP 48-Port Gigabit PoE Stackable Managed Switch

Session Sources

Session Source Table

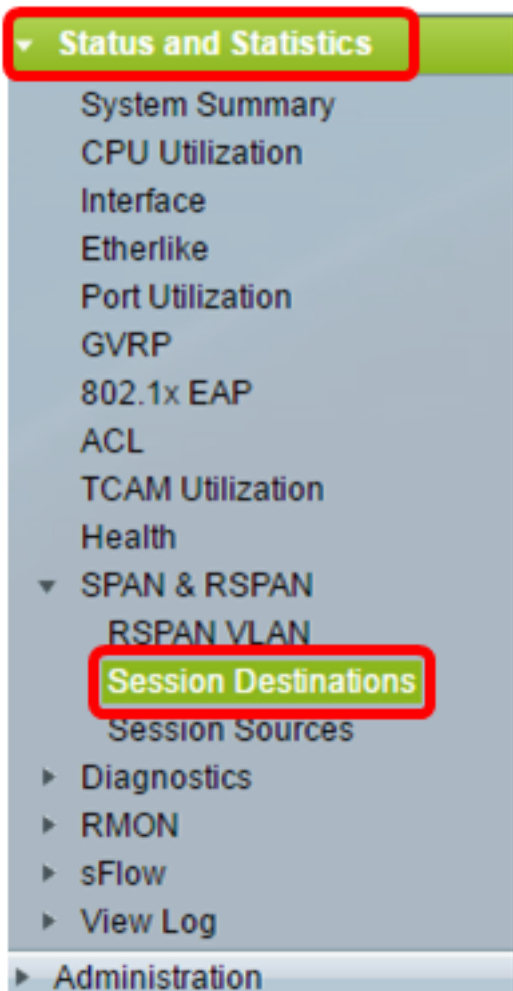
Filter: *Session ID equals to*

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

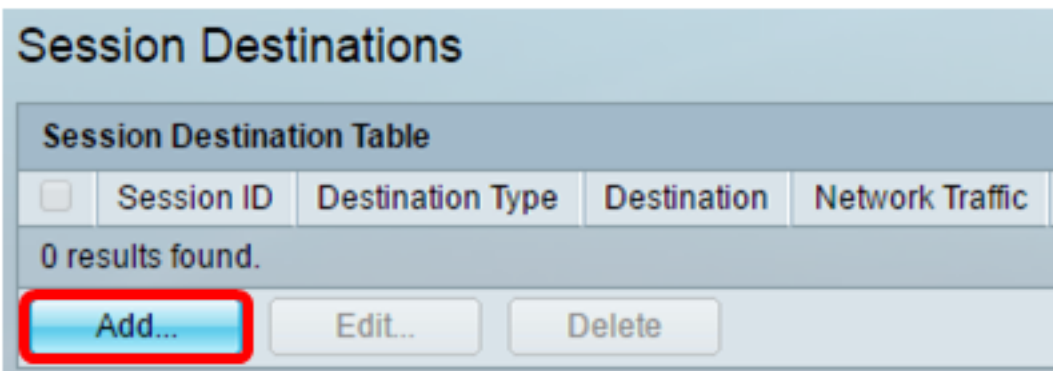
U dient nu de sessiebron op uw Start-switch te hebben geconfigureerd.

Sessiebestemmingen instellen op een Start-switch

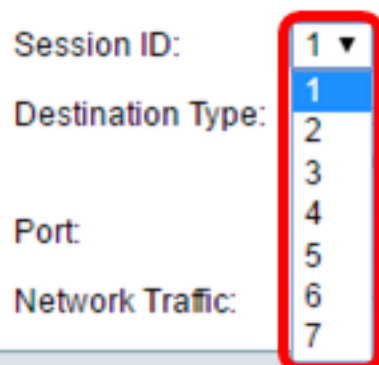
Stap 1. Kies **Status en statistieken > SPAN & RSPAN > Sessiebestemmingen**.



Stap 2. Klik op Add.



Stap 3. Kies het sessienummer in de vervolgkeuzelijst Session-ID. Dit moet hetzelfde zijn als de geselecteerde ID uit de geconfigureerde sessiebron.



Opmerking: In dit voorbeeld wordt Session 1 gekozen.

Stap 4. Klik op de radioknop **Remote VLAN** in het gebied Doeltype. Een netwerkanalyzer, zoals een computer die Wireless-shark uitvoert, is op deze poort aangesloten.

Belangrijk: De Doelinterface kan niet hetzelfde zijn als de Bron Port.

Destination Type: Local Interface
 Remote VLAN (VLAN 20)

Opmerking: Als Remote VLAN is geselecteerd, wordt het netwerkverkeer automatisch ingeschakeld.

Stap 5. Kies in het gebied met de reflectiepoort de gewenste optie uit de vervolgkeuzelijst Eenheid. Kies welke poort u als bronpoort wilt instellen in de vervolgkeuzelijst Port.

Reflector Port: Unit Port
Network Traffic: Enable

Opmerking: In dit voorbeeld wordt poort GE20 in Eenheid 1 gekozen.

Stap 6. Klik op **Toepassen** en vervolgens op **Sluiten**.

Session ID:

Destination Type: Local Interface
 Remote VLAN (VLAN 20)

Reflector Port: Unit Port

Network Traffic: Enable

Stap 7. (Optioneel) Klik op **Opslaan** om het actieve configuratiebestand bij te werken.

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

U hebt nu de sessiebestemmingen in de Start-switch ingesteld.

Intermediate-switches

Er kunnen ook intermediaire switches zijn die de RSPAN-bron- en doelsessies scheiden. Deze switches hoeven RSPAN niet te kunnen gebruiken, maar ze moeten wel voldoen aan de eisen van RSPAN VLAN.

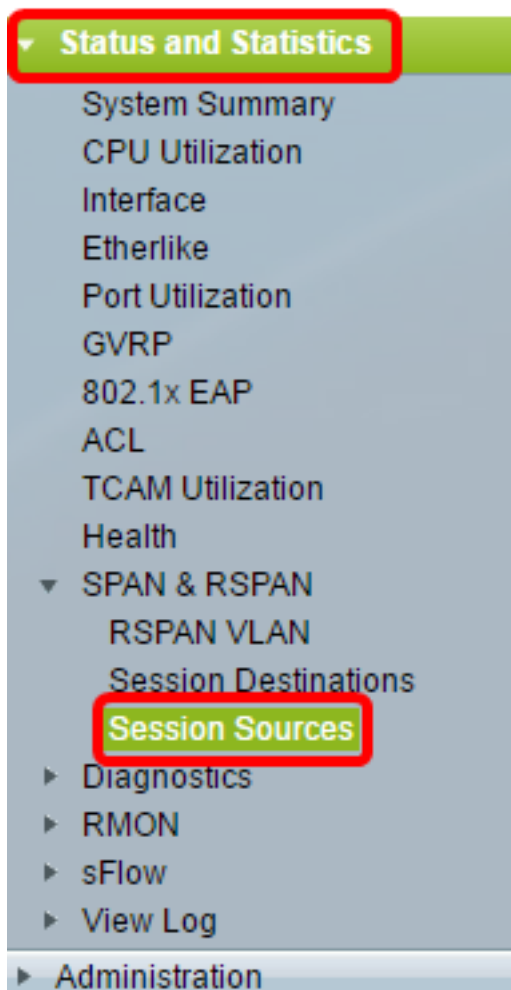
Voor VLAN's 1 tot 1005 die zichtbaar zijn voor VLAN Trunking Protocol (VTP), worden de VLAN-ID en de bijbehorende RSPAN-kenmerken door VTP verspreid. Als u een RSPAN VLAN ID in het uitgebreide VLAN-bereik (1006 tot 4094) toewijst, moet u alle intermediaire switches handmatig configureren.

Om te leren hoe u een interface VLAN als een boomstampoort van een tussenliggende switch kunt toewijzen, klik [hier](#) voor instructies.

Het is normaal om meerdere RSPAN VLAN's in een netwerk tegelijkertijd te hebben met elk RSPAN VLAN dat een netwerk brede RSPAN-sessie definieert. Dat wil zeggen dat meerdere RSPAN-bronsessies overal in het netwerk kunnen bijdragen aan pakketten naar de RSPAN-sessie. Het is ook mogelijk om meerdere RSPAN doelsessies door het netwerk te hebben, hetzelfde RSPAN VLAN te controleren en verkeer aan de gebruiker voor te stellen. De RSPAN VLAN-id scheidt de sessies.

Sessiebronnen op een eindswitch configureren

Stap 1. Kies **Status en statistieken > SPAN & RSPAN > Sessiebronnen**.



Stap 2. Klik op **Add**.

The screenshot shows the 'Session Sources' configuration page. At the top, there is a 'Session Source Table' section with a filter: 'Session ID equals to' and a 'Go' button. Below the filter, there is a table with columns: 'Session ID', 'Destination', 'Source Interface', and 'Monitor Type'. The table currently shows '0 results found.' At the bottom of the table, there are three buttons: 'Add...', 'Edit...', and 'Delete'. The 'Add...' button is highlighted with a red box.

Stap 3. (Optioneel) Kies het sessienummer in de vervolgkeuzelijst Session-ID. Session-ID moet per sessie consistent zijn.

The screenshot shows a dropdown menu for 'Session ID'. The menu is open, showing a list of numbers from 1 to 7. The number 1 is selected and highlighted with a blue background. A red box is drawn around the entire dropdown menu.

Opmerking: In dit voorbeeld wordt Session 1 gekozen.

Stap 4. Klik de radioknop **Remote VLAN** van het Bron-interfacegebied aan.

The screenshot shows the configuration form for a session source. It includes fields for 'Session ID' (set to 1), 'Source Interface' (with radio buttons for 'Unit', 'Port', and 'VLAN'), and 'Monitor Type' (with radio buttons for 'Rx and Tx', 'Rx', and 'Tx'). The 'Remote VLAN (VLAN 20)' radio button is selected and highlighted with a red box. At the bottom, there are 'Apply' and 'Close' buttons.

Opmerking: Het Monitor type van het VLAN op afstand wordt automatisch ingesteld.

Stap 5. Klik op **Toepassen** en vervolgens op **Sluiten**.

Stap 6. (Optioneel) Klik op **Save** om het actieve configuratiebestand te wijzigen.

The screenshot shows the configuration page for a Cisco switch. At the top right, there is a 'Save' button with a red 'X' icon. The page title is 'MP 48-Port Gigabit PoE Stackable Managed Switch'. Below the title is the section 'Session Sources'. Underneath, there is a 'Session Source Table' with a filter section. The filter is set to 'Session ID equals to 1 (GE1/1)'. Below the filter is a table with columns: Session ID, Destination, Source Interface, and Monitor Type. The table contains one entry: Session ID 1, Destination VLAN 20, Source Interface, and Monitor Type Rx. At the bottom of the table are buttons for 'Add...', 'Edit...', and 'Delete'.

Session ID	Destination	Source Interface	Monitor Type
1	VLAN 20		Rx

U hebt nu de sessiebronnen op uw eindswitch ingesteld.

Sessiebestemmingen op een eindswitch configureren

Stap 1. Kies **Status en statistieken > SPAN & RSPAN > Sessiebestemmingen**.

The screenshot shows the navigation menu of the Cisco switch. The 'Status and Statistics' menu item is highlighted with a red box. Underneath it, the 'SPAN & RSPAN' menu item is expanded, and 'Session Destinations' is highlighted with a red box. Other menu items include System Summary, CPU Utilization, Interface, Etherlike, Port Utilization, GVRP, 802.1x EAP, ACL, TCAM Utilization, Health, RSPAN VLAN, Session Sources, Diagnostics, RMON, sFlow, View Log, and Administration.

Stap 2. Klik op **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"/>				

Stap 3. Kies het sessienummer in de vervolgkeuzelijst Session-ID. Dit moet hetzelfde zijn als de geselecteerde ID uit de geconfigureerde sessiebron.

Session ID:

Destination Type:

Port:

Network Traffic:

Opmerking: In dit voorbeeld wordt Session 1 gekozen.

Stap 4. Klik het radioknop **Local Interface** van het gebied van het type bestemming aan.

Destination Type: Local Interface

Remote VLAN (VLAN 20)

Stap 5. Kies in het poortgebied de gewenste optie in de vervolgkeuzelijst Eenheid. Kies welke poort u als bronpoort wilt instellen in de vervolgkeuzelijst Port.

Port:

Network Traffic: Enable

Opmerking: In dit voorbeeld wordt poort GE20 in Eenheid 1 gekozen.

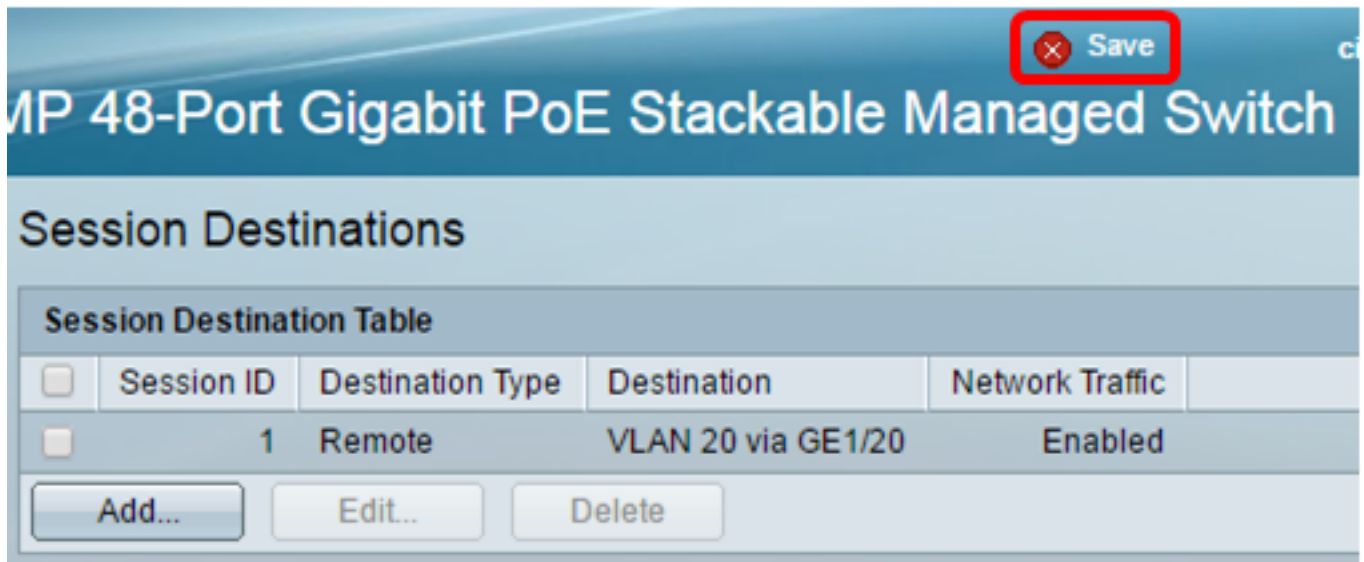
Stap 6. (Optioneel) Controleer het aankruisvakje Network Traffic Shaping **inschakelen** om netwerkverkeer in te schakelen.

Port:

Network Traffic: Enable

Stap 7. Klik op **Toepassen** en vervolgens op **Sluiten**.

Stap 8. (Optioneel) Klik op **Opslaan** om het actieve configuratiebestand bij te werken.



U had nu de sessiebestemmingen op uw eindswitch moeten configureren.

De opgenomen RSPAN VLAN-pakketten in WireShark analyseren

In dit scenario heeft de host in de geconfigureerde broninterface, GE2 in eenheid 1 (GE1/2), een IP-adres van 192.168.1.100. Terwijl de host in de geconfigureerde doelinterface, heeft GE20 in eenheid 1 (VLAN 20 via GE1/20) een IP-adres van 192.168.1.27. Wireshark wordt uitgevoerd in de host die met deze poort is verbonden.

Met het filter `ip.addr = 192.168.1.100` toont Wireshark de opgenomen pakketten van de interface van de afstandsbron.

*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

Bekijk een video gerelateerd aan dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)