

Configurazione delle impostazioni di Remote Switch Port Analyzer (RSPAN) sulla rete

Sommario

- [Obiettivo](#)
- [Dispositivi interessati | Versione firmware](#)
- [Introduzione](#)
- [Configurazione della VLAN RSPAN sullo switch](#)
- [Configurazione delle origini sessione su uno switch di avvio](#)
- [Configurazione delle destinazioni di sessione su uno switch di avvio](#)
- [Switch intermedi](#)
- [Configurazione delle origini della sessione su uno switch finale](#)
- [Configurazione delle destinazioni di sessione su uno switch finale](#)
- [Analisi dei pacchetti VLAN RSPAN acquisiti in WireShark](#)

Obiettivo

In questo documento viene spiegato come configurare RSPAN sugli switch.

Dispositivi interessati | Versione firmware

- Sx350 | 2.2.5.68 ([scarica la versione più recente](#))
- SG350X | 2.2.5.68 ([scarica la versione più recente](#))
- Sx550X | 2.2.5.68 ([scarica la versione più recente](#))

Introduzione

Lo SPAN (Switch Port Analyzer), o talvolta denominato mirroring o monitoraggio delle porte, sceglie il traffico di rete per l'analisi da parte di un analizzatore di rete. L'analizzatore di rete può essere un dispositivo Cisco SwitchProbe o un'altra sonda RMON (monitoraggio da remoto).

Il mirroring delle porte viene utilizzato su un dispositivo di rete per inviare una copia dei pacchetti di rete rilevati su una singola porta del dispositivo, su più porte del dispositivo o su un'intera VLAN (Virtual Local Area Network) a una connessione di monitoraggio di rete su un'altra porta del dispositivo. Generalmente viene utilizzato per le appliance di rete che richiedono il monitoraggio del traffico di rete, ad esempio un sistema di rilevamento delle intrusioni. Un analizzatore di rete connesso alla porta di monitoraggio elabora i pacchetti di dati per la diagnosi, il debug e il monitoraggio delle prestazioni.

RSPAN (Remote Switch Port Analyzer) è un'estensione di SPAN. RSPAN estende lo SPAN consentendo il monitoraggio di più switch in rete e la definizione della porta dell'analizzatore su uno switch remoto. Ciò significa che è possibile centralizzare i dispositivi di acquisizione di rete.

RSPAN esegue il mirroring del traffico dalle porte di origine di una sessione RSPAN su una VLAN dedicata alla sessione RSPAN. Questa VLAN viene quindi trunkata su altri switch, consentendo il trasporto del traffico della sessione RSPAN su più switch. Sullo switch che contiene la porta di destinazione per la sessione, il traffico proveniente dalla VLAN della sessione RSPAN viene semplicemente sottoposto a mirroring sulla porta di destinazione.

Flusso del traffico RSPAN

- Il traffico di ciascuna sessione RSPAN viene trasferito su una VLAN RSPAN specificata dall'utente e dedicata a tale sessione RSPAN in tutti gli switch partecipanti.
- Il traffico proveniente dalle interfacce di origine sul dispositivo di avvio viene copiato sulla VLAN RSPAN tramite una porta riflettore. Questa è una porta fisica da impostare. Viene utilizzato esclusivamente per creare una sessione RSPAN.
- Questa porta del riflettore è il meccanismo che copia i pacchetti su una VLAN RSPAN. Inoltre solo il traffico proveniente dalla sessione di origine RSPAN a cui è affiliato. Qualsiasi dispositivo collegato a una porta impostata come porta di riflessione perde la connettività finché la sessione di origine RSPAN non viene disabilitata.
- Il traffico RSPAN viene quindi inoltrato tramite le porte trunk sui dispositivi intermedi alla sessione di destinazione sullo switch finale.
- Lo switch di destinazione monitora la VLAN RSPAN e la copia sulla porta di destinazione.

Regole di appartenenza della porta RSPAN

- Su tutti gli switch: l'appartenenza alla VLAN RSPAN può essere contrassegnata solo.
 - Interruttore di avvio
- Le interfacce di origine SPAN non possono essere membri di VLAN RSPAN.
- La porta del riflettore non può essere un membro di questa VLAN.
- Si consiglia di non associare la VLAN remota ad alcuna rete.
 - Intermediate Switch
- Si consiglia di rimuovere l'appartenenza RSPAN da tutte le porte non utilizzate per il passaggio del traffico con mirroring.
- In genere, una VLAN remota RSPAN contiene due porte.
 - Switch finale
- Per il traffico con mirroring, le porte di origine devono essere membri di VLAN RSPAN.
- Si consiglia di rimuovere l'appartenenza RSPAN da tutte le altre porte, inclusa l'interfaccia di destinazione.

Configurare RSPAN sulla rete

Configurazione della VLAN RSPAN sullo switch

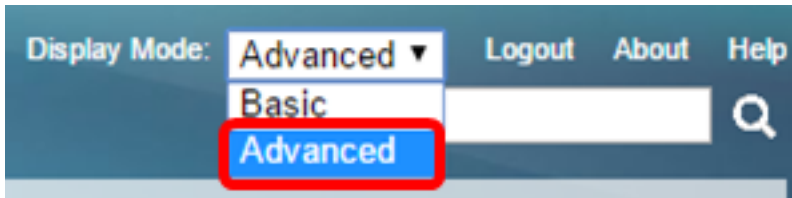
La VLAN RSPAN trasmette il traffico SPAN tra le sessioni di origine e di destinazione RSPAN. Presenta le seguenti caratteristiche speciali:

- Tutto il traffico sulla VLAN RSPAN è sempre inondato.
- Sulla VLAN RSPAN non viene eseguito l'apprendimento dell'indirizzo MAC (Media Access Control).
- Il traffico VLAN RSPAN viene trasmesso solo sulle porte trunk.
- Il protocollo STP può essere eseguito sui trunk della VLAN RSPAN, ma non sulle porte di

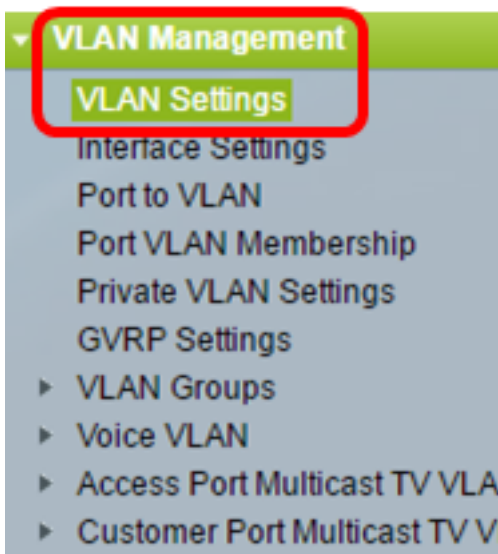
destinazione SPAN.

- Le VLAN RSPAN devono essere configurate su entrambi gli switch Start e Final in modalità di configurazione VLAN usando il comando **remote-span** VLAN configuration mode o seguire le istruzioni riportate di seguito:

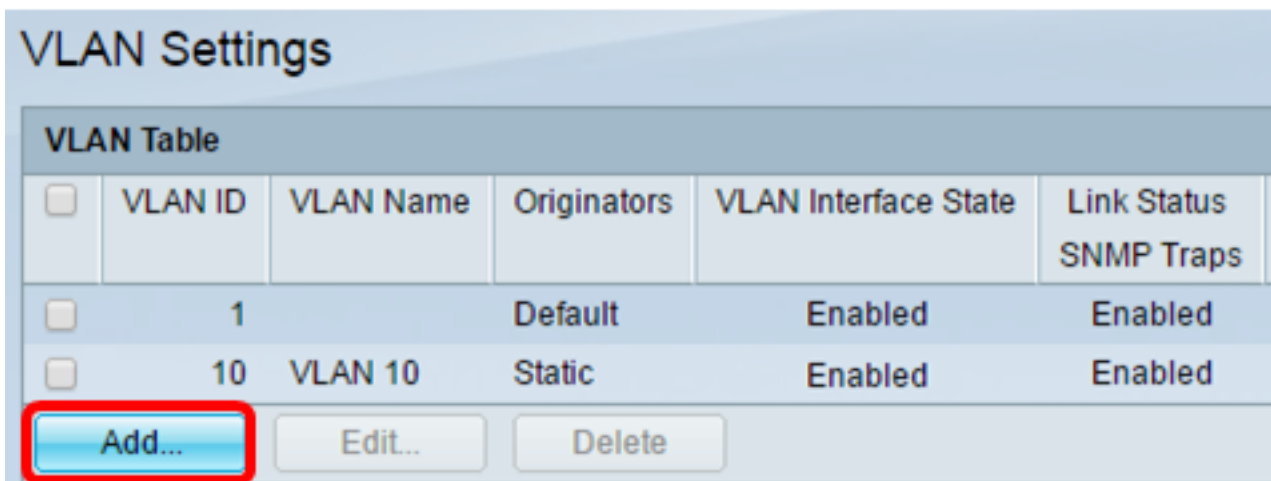
Passaggio 1. Accedere all'utility basata sul Web dello switch di avvio e scegliere **Avanzate** dall'elenco a discesa Display Mode (Modalità di visualizzazione).



Passaggio 2. Selezionare **Gestione VLAN > Impostazioni VLAN**.



Passaggio 3. Fare clic su **Add**.



Passaggio 4. Immettere l'ID VLAN nel campo *VLAN ID*.



Nota: nell'esempio, l'ID VLAN è VLAN 20.

Passaggio 5. (Facoltativo) Immettere il nome della VLAN nel campo *Nome VLAN*.

VLAN ID: (Range: 2 - 4094)

VLAN Name: (10/32 characters used)

Nota: Nell'esempio, il nome della VLAN è RSPAN VLAN.

Passaggio 6. (Facoltativo) Selezionare la casella di controllo Stato interfaccia VLAN per abilitare la VLAN. Se la VLAN è spenta, non trasmette o riceve messaggi da o verso livelli superiori. Ad esempio, se si arresta una VLAN su cui è configurata un'interfaccia IP, il bridging nella VLAN continua, ma lo switch non può trasmettere e ricevere il traffico IP sulla VLAN. Questa funzione è attivata per impostazione predefinita.

Passaggio 7. (Facoltativo) Selezionare la casella di controllo Trap SNMP stato collegamento per abilitare la generazione dello stato del collegamento di trap SNMP (Simple Network Management Protocol). Questa funzione è attivata per impostazione predefinita.

Passaggio 8. Fare clic su **Apply (Applica)**, quindi su **Close** (Chiudi).

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: per ulteriori informazioni sulla gestione delle VLAN su uno switch, fare clic [qui](#).

Passaggio 9. (Facoltativo) Fare clic su **Salva** per aggiornare il file di configurazione in esecuzione.

MP 48-Port Gigabit PoE Stackable Managed Switch

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

Passaggio 10. Scegliere **Stato e statistiche > SPAN & RSPAN > VLAN RSPAN**.

- 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

Passaggio 11. Selezionare un ID VLAN dall'elenco a discesa VLAN RSPAN. Questa VLAN deve essere utilizzata esclusivamente per RSPAN.

RSPAN VLAN

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

RSPAN VLAN: None ▼
None
10
20

Apply Cancel

Nota: nell'esempio riportato di seguito, viene scelta la VLAN 20.

Passaggio 12. Fare clic su **Applica**.

RSPAN VLAN

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

RSPAN VLAN: 20 ▼

Apply Cancel

Passaggio 13. (Facoltativo) Fare clic su **Save** per aggiornare il file della configurazione in esecuzione.

✕ 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 ▼

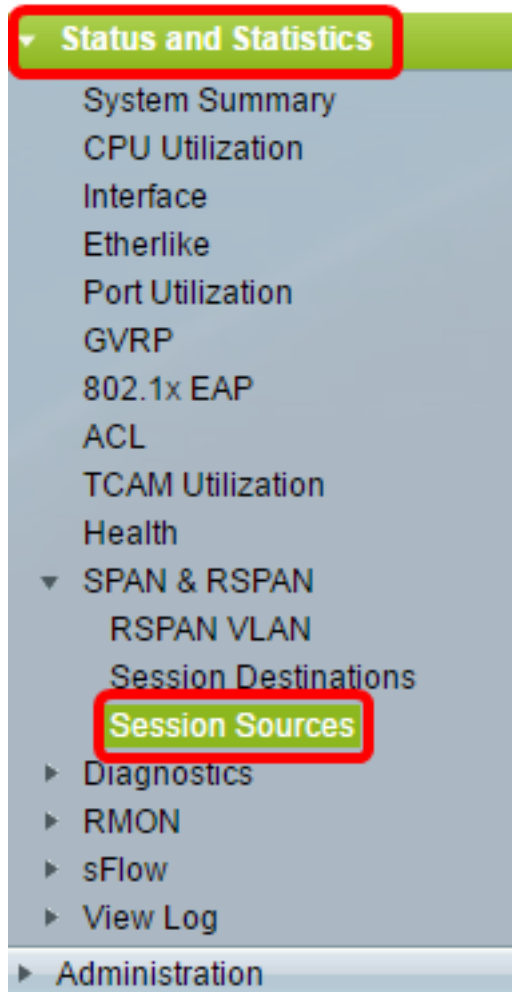
Apply Cancel

Passaggio 14. Nello switch finale, ripetere i passaggi da 1 a 13 per configurare la VLAN RSPAN.

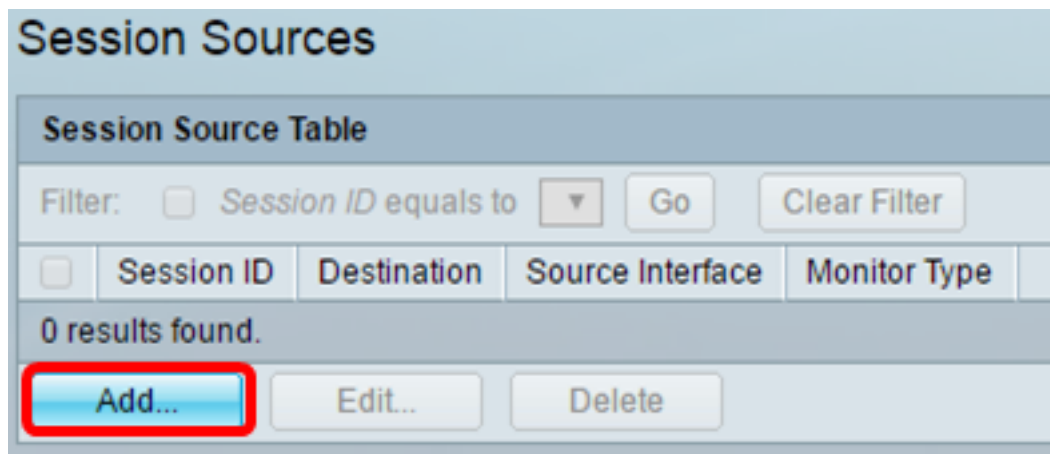
A questo punto, la VLAN dedicata alla sessione RSPAN è configurata sia sullo switch di avvio che su quello finale.

Configurazione delle origini sessione su uno switch di avvio

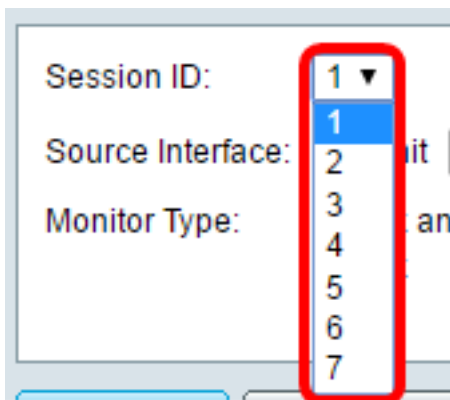
Passaggio 1. Scegliere **Stato e statistiche > SPAN & RSPAN > Origini sessione.**



Passaggio 2. Fare clic su **Add.**



Passaggio 3. Scegliere il numero di sessione dall'elenco a discesa ID sessione. L'ID sessione deve essere coerente per ogni sessione RSPAN.



Nota: Nell'esempio viene scelta Sessione 1.

Passaggio 4. Fare clic sul pulsante di opzione relativo al tipo di interfaccia di origine desiderato e scegliere l'interfaccia dall'elenco o dagli elenchi a discesa.

Importante: L'interfaccia di origine non può essere uguale alla porta di destinazione.



Le opzioni sono:

- Unità e porta: è possibile scegliere l'opzione desiderata dall'elenco a discesa Unità e scegliere quale porta impostare come porta di origine dall'elenco a discesa Porta.
- VLAN: è possibile scegliere la VLAN da monitorare dall'elenco a discesa VLAN. Una VLAN aiuta un gruppo di host a comunicare come se si trovassero sulla stessa rete fisica, indipendentemente dalla loro posizione. Se questa opzione è selezionata, non è possibile modificarla.
- VLAN remota: visualizza la VLAN RSPAN definita. Se questa opzione è selezionata, non è possibile modificarla.

Nota: Nell'esempio, viene scelta la porta GE2 nell'unità 1. Questa è l'interfaccia remota da monitorare.

Passaggio 5. (Facoltativo) Se al passaggio 4 si fa clic su Unità e Porta, fare clic sul pulsante di opzione Tipo di monitor desiderato per il tipo di traffico da monitorare.



Le opzioni sono:

- Rx e Tx: questa opzione consente il mirroring delle porte dei pacchetti in entrata e in uscita. Questa opzione è selezionata per default.
- Rx: questa opzione consente il mirroring delle porte dei pacchetti in ingresso.
- Tx: questa opzione consente il mirroring delle porte dei pacchetti in uscita.

Nota: Nell'esempio, viene scelto Rx.

Passaggio 6. Fare clic su **Apply (Applica)**, quindi su **Close (Chiudi)**.

Session ID:

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

Monitor Type: Rx and Tx
 Rx
 Tx

Passaggio 7. (Facoltativo) Fare clic su **Save** per aggiornare il file di configurazione in esecuzione.

MP 48-Port Gigabit PoE Stackable Managed Switch

Session Sources

Session Source Table

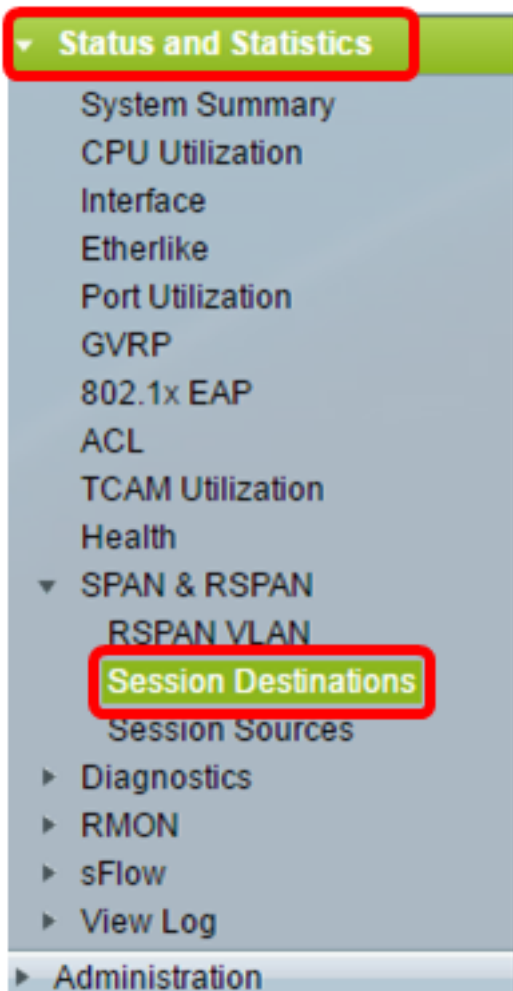
Filter: *Session ID equals to*

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

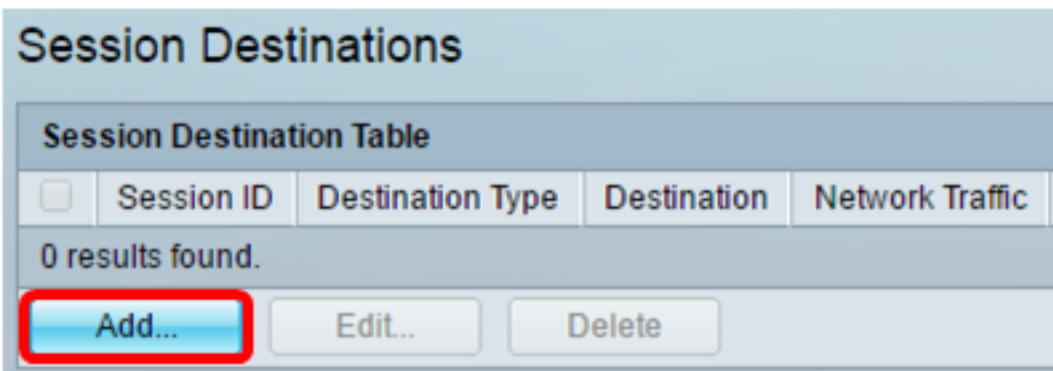
A questo punto, l'origine della sessione è configurata sullo switch di avvio.

Configurazione delle destinazioni di sessione su uno switch di avvio

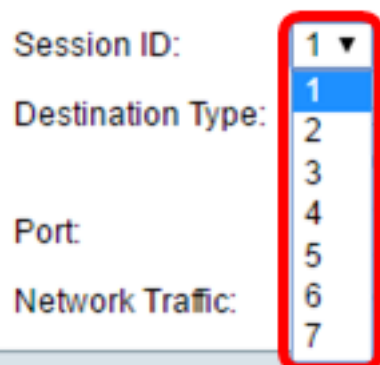
Passaggio 1. Scegliere **Stato e statistiche > SPAN e RSPAN > Destinazioni sessione**.



Passaggio 2. Fare clic su **Add**.



Passaggio 3. Scegliere il numero di sessione dall'elenco a discesa ID sessione. Deve corrispondere all'ID scelto dall'origine della sessione configurata.



Nota: Nell'esempio viene scelta Sessione 1.

Passaggio 4. Fare clic sul pulsante di scelta **VLAN remota** nell'area Tipo di destinazione. A questa porta è connesso un analizzatore di rete, ad esempio un computer che esegue Wireshark.

Importante: L'interfaccia di destinazione non può essere uguale alla porta di origine.

Destination Type: Local Interface
 Remote VLAN (VLAN 20)

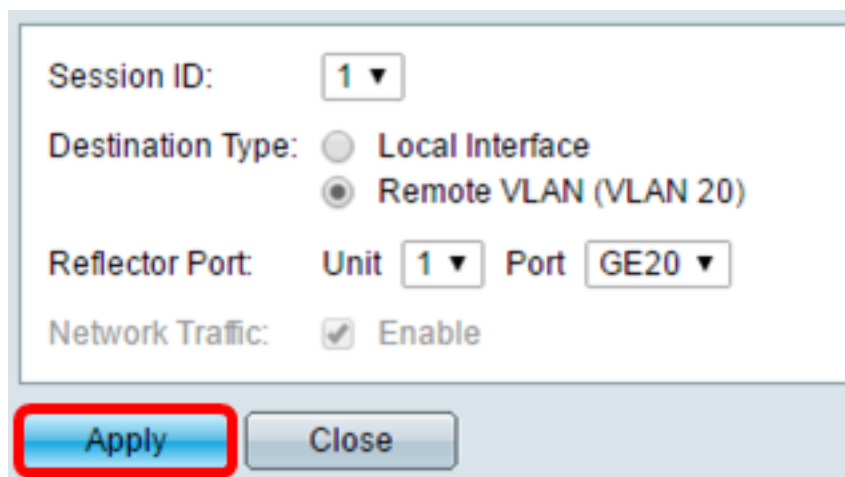
Nota: Se si sceglie VLAN remota, il traffico di rete viene abilitato automaticamente.

Passaggio 5. Nell'area Porta riflettore, scegliere l'opzione desiderata dall'elenco a discesa Unità. Selezionare la porta da impostare come porta di origine dall'elenco a discesa Porta.

Reflector Port: Unit Port
Network Traffic: Enable

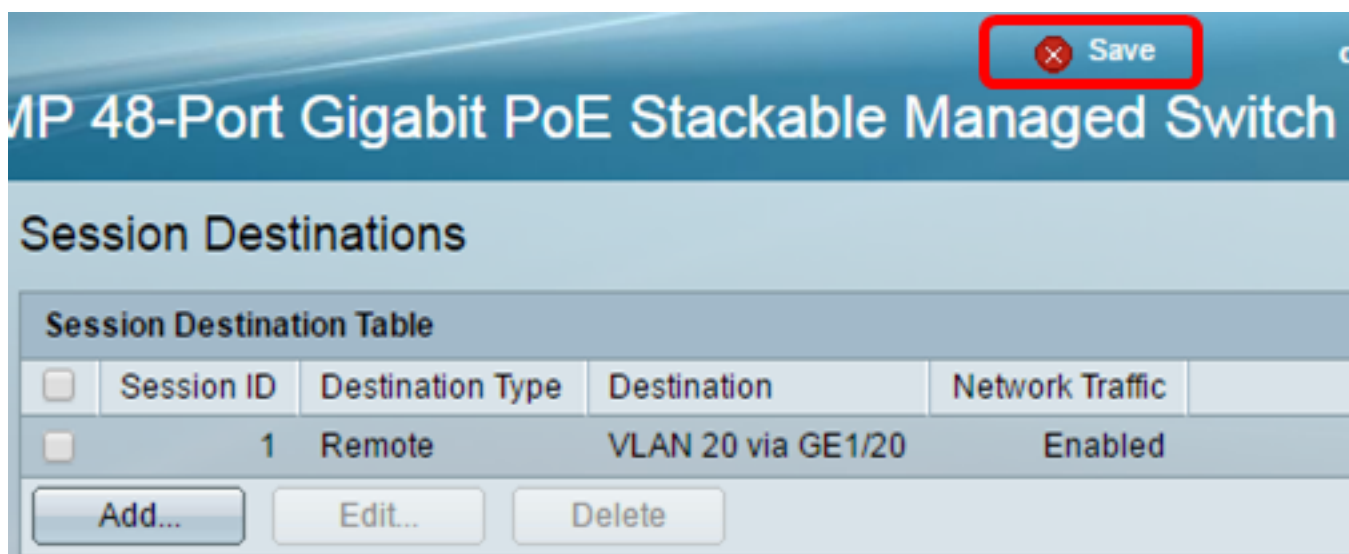
Nota: Nell'esempio, viene scelta la porta GE20 nell'unità 1.

Passaggio 6. Fare clic su **Apply (Applica)**, quindi su **Close (Chiudi)**.



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

Passaggio 7. (Facoltativo) Fare clic su **Save** per aggiornare il file di configurazione in esecuzione.



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

A questo punto, le destinazioni della sessione sono configurate sullo switch di avvio.

Switch intermedi

Possono inoltre esistere switch intermedi che separano le sessioni di origine e di destinazione RSPAN. Non è necessario che questi switch siano in grado di eseguire RSPAN, ma devono rispondere ai requisiti della VLAN RSPAN.

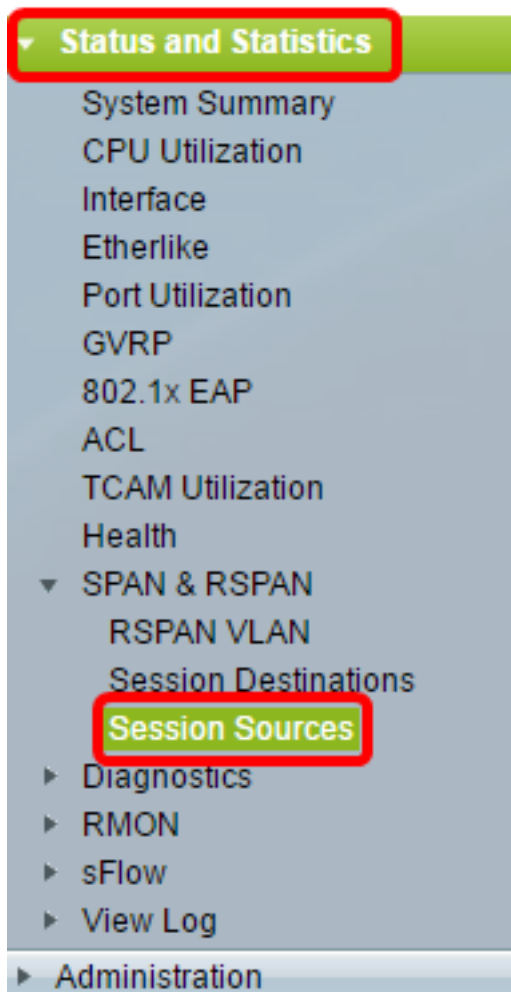
Per le VLAN da 1 a 1005 visibili al VLAN Trunking Protocol (VTP), l'ID VLAN e le relative caratteristiche RSPAN associate vengono propagate dal VTP. Se si assegna un ID VLAN RSPAN nell'intervallo di VLAN esteso (da 1006 a 4094), è necessario configurare manualmente tutti gli switch intermedi.

per informazioni su come assegnare un'interfaccia VLAN come porta trunk di uno switch intermedio, fare clic [qui](#) per istruzioni.

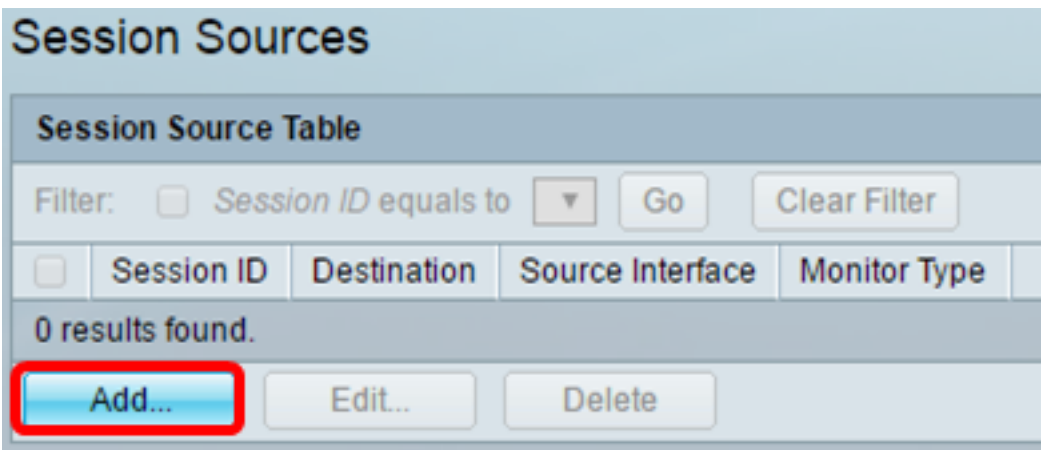
È normale avere più VLAN RSPAN in una rete contemporaneamente quando ciascuna VLAN RSPAN definisce una sessione RSPAN a livello di rete. Vale a dire, più sessioni RSPAN di origine in qualsiasi punto della rete possono contribuire ai pacchetti della sessione RSPAN. È inoltre possibile avere più sessioni di destinazione RSPAN in tutta la rete, monitorando la stessa VLAN RSPAN e presentando il traffico all'utente. L'ID VLAN RSPAN separa le sessioni.

Configurazione delle origini della sessione su uno switch finale

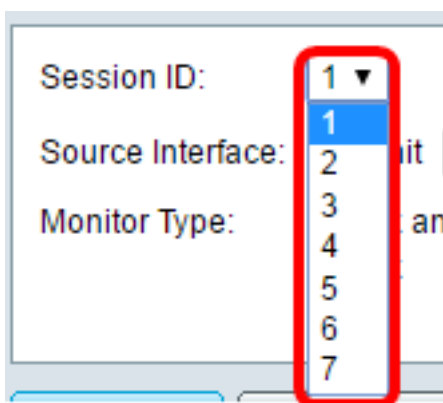
Passaggio 1. Scegliere **Stato e statistiche > SPAN & RSPAN > Origini sessione**.



Passaggio 2. Fare clic su **Add**.

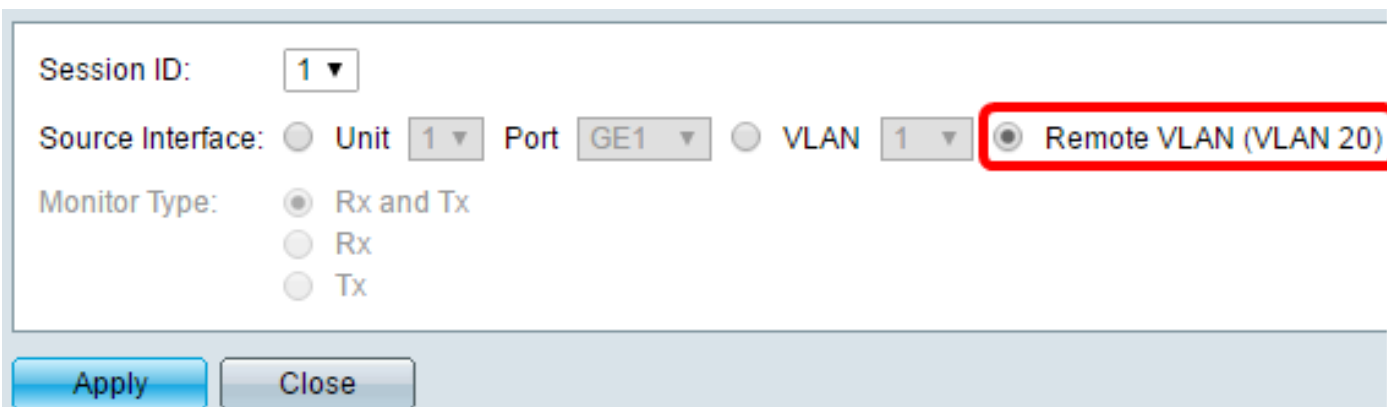


Passaggio 3. (Facoltativo) Scegliere il numero della sessione dall'elenco a discesa ID sessione. L'ID sessione deve essere coerente per sessione.



Nota: Nell'esempio viene scelta Sessione 1.

Passaggio 4. Fare clic sul pulsante di opzione **VLAN remota** nell'area Source Interface (Interfaccia di origine).



Nota: Il tipo di monitoraggio della VLAN remota verrà configurato automaticamente.

Passaggio 5. Fare clic su **Apply (Applica)**, quindi su **Close** (Chiudi).

Passaggio 6. (Facoltativo) Fare clic su **Save** per aggiornare il file di configurazione in esecuzione.

The screenshot shows the configuration page for a Cisco switch. At the top right, there is a 'Save' button with a red 'X' icon, highlighted by a red box. 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)' with 'Go' and 'Clear Filter' buttons. The table has columns for 'Session ID', 'Destination', 'Source Interface', and 'Monitor Type'. One entry is visible: Session ID 1, Destination VLAN 20, Source Interface, and Monitor Type Rx. Below the table are 'Add...', 'Edit...', and 'Delete' buttons.

A questo punto, le origini della sessione sono configurate sullo switch finale.

Configurazione delle destinazioni di sessione su uno switch finale

Passaggio 1. Scegliere **Stato e statistiche** > **SPAN e RSPAN** > **Destinazioni sessione**.

The screenshot shows a configuration menu with a green header 'Status and Statistics' highlighted by a red box. The menu items are: System Summary, CPU Utilization, Interface, Etherlike, Port Utilization, GVRP, 802.1x EAP, ACL, TCAM Utilization, Health, SPAN & RSPAN, RSPAN VLAN, Session Destinations (highlighted by a red box), Session Sources, Diagnostics, RMON, sFlow, View Log, and Administration.

Passaggio 2. Fare clic su **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"/>				

Passaggio 3. Scegliere il numero di sessione dall'elenco a discesa ID sessione. Deve corrispondere all'ID scelto dall'origine della sessione configurata.

Session ID:

Destination Type:

Port:

Network Traffic:

Nota: Nell'esempio viene scelta Sessione 1.

Passaggio 4. Fare clic sul pulsante di opzione **Interfaccia locale** nell'area Tipo di destinazione.

Destination Type: Local Interface

Remote VLAN (VLAN 20)

Passaggio 5. Nell'area Porta, scegliere l'opzione desiderata dall'elenco a discesa Unità. Selezionare la porta da impostare come porta di origine dall'elenco a discesa Porta.

Port:

Network Traffic: Enable

Nota: Nell'esempio, viene scelta la porta GE20 nell'unità 1.

Passaggio 6. (Facoltativo) Selezionare la casella di controllo **Abilita** traffico di rete per abilitare il traffico di rete.

Port:

Network Traffic: Enable

Passaggio 7. Fare clic su **Apply (Applica)**, quindi su **Close** (Chiudi).

Passaggio 8. (Facoltativo) Fare clic su **Save** per aggiornare il file di configurazione in esecuzione.



A questo punto, le destinazioni della sessione sono configurate sullo switch finale.

Analisi dei pacchetti VLAN RSPAN acquisiti in WireShark

In questo scenario, l'host nell'interfaccia di origine configurata, GE2 nell'unità 1 (GE1/2), ha un indirizzo IP di 192.168.1.100. Mentre l'host nell'interfaccia di destinazione configurata, GE20 nell'unità 1 (VLAN 20 tramite GE1/20), ha un indirizzo IP di 192.168.1.127. Wireshark è in esecuzione sull'host connesso a questa porta.

Utilizzando il filtro `ip.addr == 192.168.1.100`, Wireshark mostra i pacchetti acquisiti dall'interfaccia di origine 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

Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco](#)