

Configuration des paramètres RSPAN (Remote Switch Port Analyzer) sur le réseau

Table des matières

- [Objectif](#)
- [Périphériques pertinents | Version du micrologiciel](#)
- [Introduction](#)
- [Configuration du VLAN RSPAN sur le commutateur](#)
- [Configuration des sources de session sur un commutateur de démarrage](#)
- [Configurer les destinations de session sur un commutateur de démarrage](#)
- [Commutateurs intermédiaires](#)
- [Configuration des sources de session sur un commutateur final](#)
- [Configurer les destinations de session sur un commutateur final](#)
- [Analyser les paquets VLAN RSPAN capturés dans WireShark](#)

Objectif

Cet article explique comment configurer RSPAN sur vos commutateurs.

Périphériques pertinents | Version du micrologiciel

- Sx350 | 2.2.5.68 ([Télécharger la dernière version](#))
- SG350X | 2.2.5.68 ([Télécharger la dernière version](#))
- Sx550X | 2.2.5.68 ([Télécharger la dernière version](#))

Introduction

SPAN (Switch Port Analyzer), parfois appelé mise en miroir des ports ou surveillance des ports, choisit le trafic réseau pour analyse par un analyseur de réseau. L'analyseur réseau peut être un périphérique Cisco SwitchProbe ou toute autre sonde de surveillance à distance (RMON).

La mise en miroir des ports est utilisée sur un périphérique réseau pour envoyer une copie des paquets réseau vus sur un port de périphérique unique, plusieurs ports de périphérique ou un VLAN entier à une connexion de surveillance réseau sur un autre port du périphérique. Il est généralement utilisé pour les appliances réseau qui nécessitent une surveillance du trafic réseau, par exemple un système de détection des intrusions. Un analyseur réseau connecté au port de surveillance traite les paquets de données pour le diagnostic, le débogage et la surveillance des performances.

RSPAN (Remote Switch Port Analyzer) est une extension de SPAN. RSPAN étend la fonctionnalité SPAN en activant la surveillance de plusieurs commutateurs sur votre réseau et en permettant la définition du port de l'analyseur sur un commutateur distant. Cela signifie que vous pouvez centraliser vos périphériques de capture réseau.

RSPAN fonctionne en miroir du trafic provenant des ports sources d'une session RSPAN sur un VLAN dédié à la session RSPAN. Ce VLAN est ensuite agrégé à d'autres commutateurs, ce qui permet au trafic de session RSPAN d'être transporté sur plusieurs commutateurs. Sur le commutateur qui contient le port de destination de la session, le trafic provenant du VLAN de

session RSPAN est simplement mis en miroir sur le port de destination.

Flux de trafic RSPAN

- Le trafic de chaque session RSPAN est transmis sur un VLAN RSPAN spécifié par l'utilisateur et dédié à cette session RSPAN dans tous les commutateurs participants.
- Le trafic provenant des interfaces source du périphérique de démarrage est copié sur le VLAN RSPAN via un port de réflecteur. Il s'agit d'un port physique qui doit être défini. Il est utilisé exclusivement pour créer une session RSPAN.
- Ce port de réflecteur est le mécanisme qui copie les paquets vers un VLAN RSPAN. Il transfère uniquement le trafic de la session source RSPAN à laquelle il est affilié. Tout périphérique connecté à un port défini comme port de réflecteur perd la connectivité jusqu'à ce que la session source RSPAN soit désactivée.
- Le trafic RSPAN est ensuite transféré sur les ports agrégés des périphériques intermédiaires vers la session de destination sur le commutateur final.
- Le commutateur de destination surveille le VLAN RSPAN et le copie sur un port de destination.

Règles d'appartenance au port RSPAN

- Sur tous les commutateurs : l'appartenance au VLAN RSPAN peut être étiquetée uniquement.
 - Commutateur de démarrage
- Les interfaces source SPAN ne peuvent pas être membres du VLAN RSPAN.
- Le port de réflecteur ne peut pas être membre de ce VLAN.
- Il est recommandé que le VLAN distant n'ait aucune appartenance.
- Commutateur intermédiaire
- Il est recommandé de supprimer l'appartenance RSPAN de tous les ports non utilisés pour le passage du trafic en miroir.
- Généralement, un VLAN distant RSPAN contient deux ports.
- Commutateur final
- Pour le trafic en miroir, les ports source doivent être membres du VLAN RSPAN.
- Il est recommandé de supprimer l'appartenance RSPAN de tous les autres ports, y compris l'interface de destination.

Configuration de RSPAN sur le réseau

Configuration du VLAN RSPAN sur le commutateur

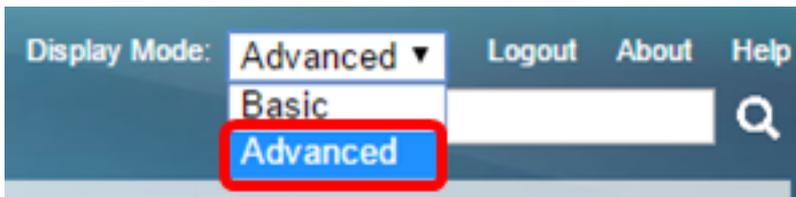
Le VLAN RSPAN transporte le trafic SPAN entre les sessions source et de destination RSPAN. Il présente les caractéristiques suivantes :

- Tout le trafic dans le VLAN RSPAN est toujours diffusé.
- Aucun apprentissage d'adresse MAC (Media Access Control) n'est effectué sur le VLAN

RSPAN.

- Le trafic VLAN RSPAN circule uniquement sur les ports agrégés.
- STP peut s'exécuter sur des agrégations VLAN RSPAN mais pas sur des ports de destination SPAN.
- Les VLAN RSPAN doivent être configurés sur les commutateurs Start et Final en mode de configuration VLAN à l'aide de la commande **remote-span** VLAN configuration mode, ou suivez les instructions ci-dessous :

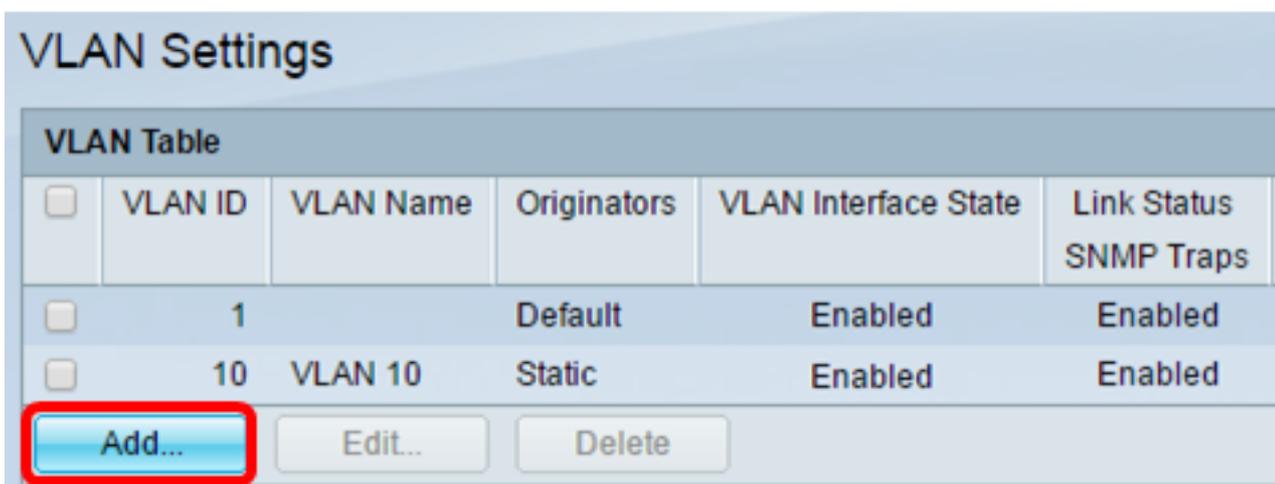
Étape 1. Connectez-vous à l'utilitaire Web du commutateur de démarrage et sélectionnez **Avancé** dans la liste déroulante Mode d'affichage.



Étape 2. Choisissez **VLAN Management > VLAN Settings**.



Étape 3. Cliquez sur **Add**.



Étape 4. Entrez l'ID de VLAN dans le champ *ID de VLAN*.

 VLAN ID: (Range: 2 - 4094)

Note: Dans cet exemple, VLAN 20 est utilisé comme ID de VLAN.

Étape 5. (Facultatif) Saisissez le nom du VLAN dans le champ *VLAN Name*.

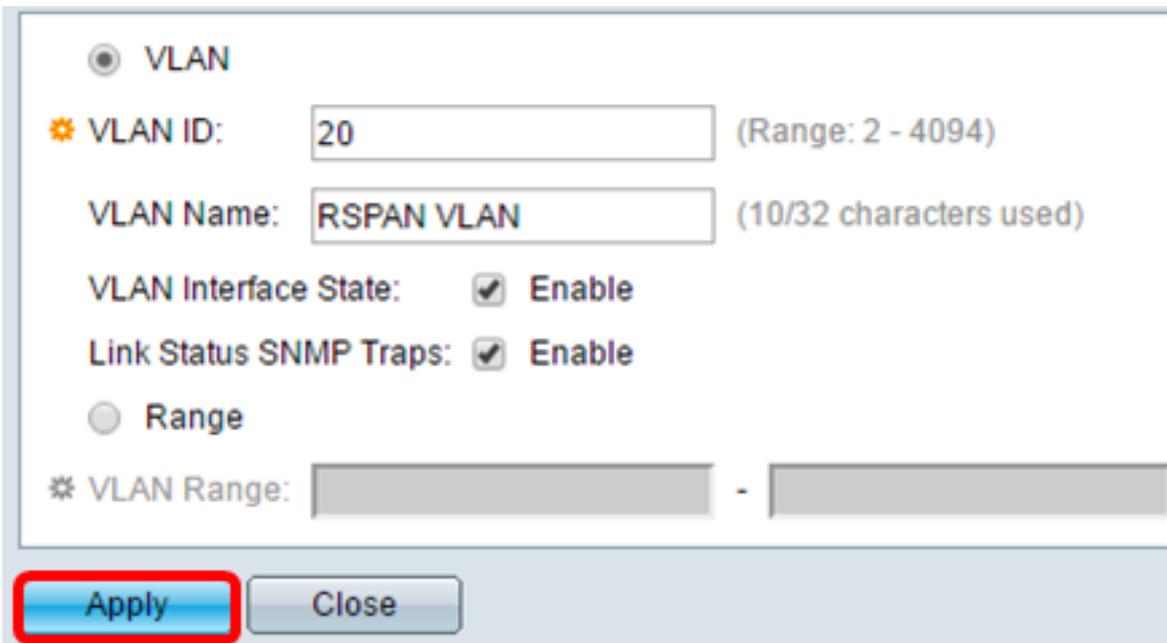
 VLAN ID: (Range: 2 - 4094)
VLAN Name: (10/32 characters used)

Note: Dans cet exemple, le VLAN RSPAN est utilisé comme nom de VLAN.

Étape 6. (Facultatif) Cochez la case VLAN Interface State pour activer le VLAN. Si le VLAN est arrêté, il ne transmet ou ne reçoit pas de messages de ou vers des niveaux supérieurs. Par exemple, si vous arrêtez un VLAN sur lequel une interface IP est configurée, le pontage dans le VLAN continue, mais le commutateur ne peut pas transmettre et recevoir le trafic IP sur le VLAN. Cette fonction est activée par défaut.

Étape 7. (Facultatif) Cochez la case Link Status SNMP Traps pour activer la génération d'état de liaison des dérouterements SNMP (Simple Network Management Protocol). Cette fonction est activée par défaut.

Étape 8. Cliquez sur **Appliquer**, puis sur **Fermer**.



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: Pour en savoir plus sur la gestion des VLAN sur un commutateur, cliquez [ici](#).

Étape 9. (Facultatif) Cliquez sur **Enregistrer** pour mettre à jour le fichier de configuration en cours.

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

Étape 10. Choisissez **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

Étape 11. Sélectionnez un ID de VLAN dans la liste déroulante RSPAN VLAN. Ce VLAN doit être utilisé exclusivement pour RSPAN.

RSPAN VLAN

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

RSPAN VLAN: None ▼
None
10
20

Apply

Remarque : dans cet exemple, VLAN 20 est sélectionné.

Étape 12. Cliquez sur Apply.

RSPAN VLAN

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

RSPAN VLAN: 20 ▼

Apply Cancel

Étape 13. (Facultatif) Cliquez sur **Enregistrer** pour mettre à jour le fichier de configuration en cours.

✖ 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 ▼

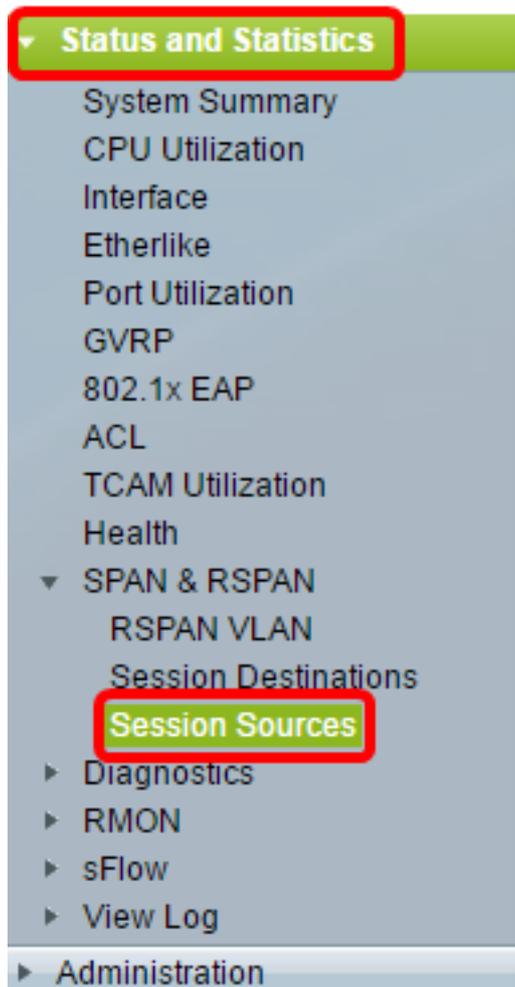
Apply Cancel

Étape 14. Dans le commutateur final, répétez les étapes 1 à 13 pour configurer le VLAN RSPAN.

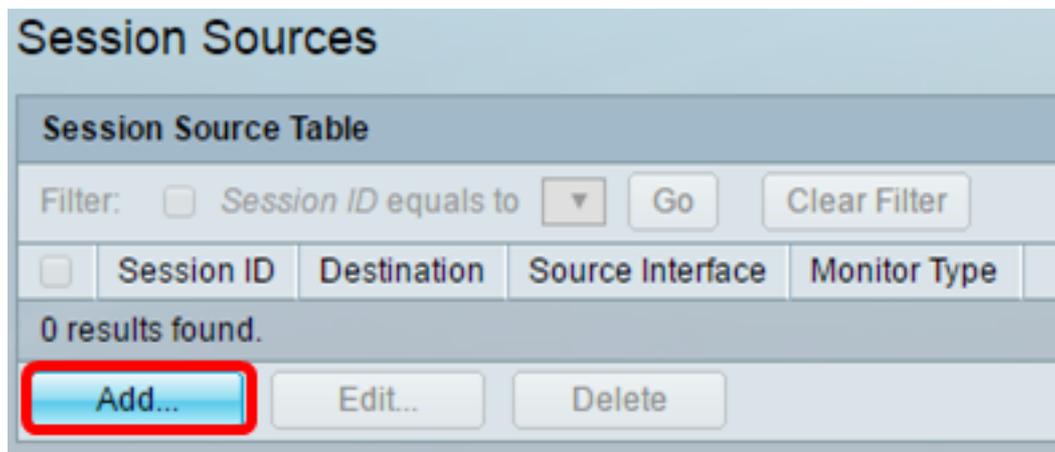
Vous devez maintenant avoir configuré le VLAN dédié à la session RSPAN sur les commutateurs de début et de fin.

Configuration des sources de session sur un commutateur de démarrage

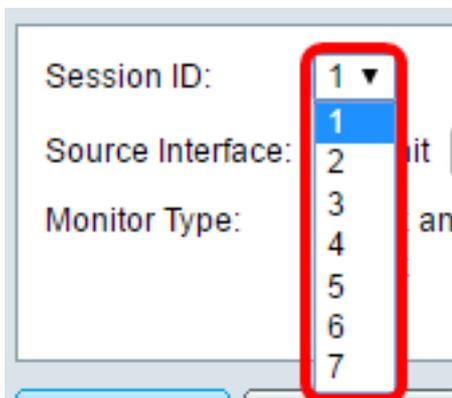
Étape 1. Choisissez **Status and Statistics** > **SPAN & RSPAN** > **Session Sources**.



Étape 2. Cliquez sur **Add**.



Étape 3. Sélectionnez le numéro de session dans la liste déroulante ID de session. L'ID de session doit être cohérent par session RSPAN.



Note: Dans cet exemple, la session 1 est choisie.

Étape 4. Cliquez sur la case d'option correspondant au type d'interface source souhaité, puis sélectionnez l'interface dans la ou les listes déroulantes.

Important : L'interface source ne peut pas être identique au port de destination.



Les options sont les suivantes :

- Unit and Port : vous pouvez choisir l'option souhaitée dans la liste déroulante Unit et choisir le port à définir comme port source dans la liste déroulante Port.
- VLAN : vous pouvez choisir le VLAN à surveiller dans la liste déroulante VLAN. Un VLAN aide un groupe d'hôtes à communiquer comme s'ils se trouvaient sur le même réseau physique, quel que soit leur emplacement. Si cette option est sélectionnée, elle n'a pas pu être modifiée.
- Remote VLAN : affiche le VLAN RSPAN défini. Si cette option est sélectionnée, elle n'a pas pu être modifiée.

Note: Dans cet exemple, le port GE2 de l'unité 1 est choisi. Il s'agit de l'interface distante qui serait surveillée.

Étape 5. (Facultatif) Si vous cliquez sur Unité et port à l'étape 4, cliquez sur la case d'option Type de moniteur correspondant au type de trafic à surveiller.



Les options sont les suivantes :

- Rx and Tx : cette option permet la mise en miroir des ports des paquets entrants et sortants. Cette option est choisie par défaut.
- Rx : cette option permet la mise en miroir des ports des paquets entrants.
- Tx : cette option permet la mise en miroir des ports des paquets sortants.

Note: Dans cet exemple, Rx est sélectionné.

Étape 6. Cliquez sur **Appliquer**, puis sur **Fermer**.

Session ID:

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

Monitor Type: Rx and Tx
 Rx
 Tx

Étape 7. (Facultatif) Cliquez sur **Enregistrer** pour mettre à jour le fichier de configuration en cours.

MP 48-Port Gigabit PoE Stackable Managed Switch

Session Sources

Session Source Table

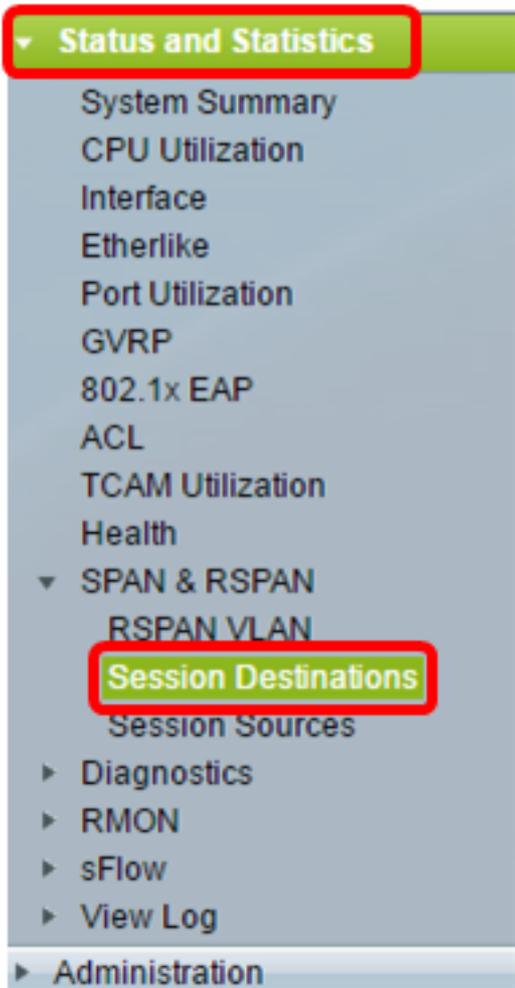
Filter: *Session ID equals to*

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

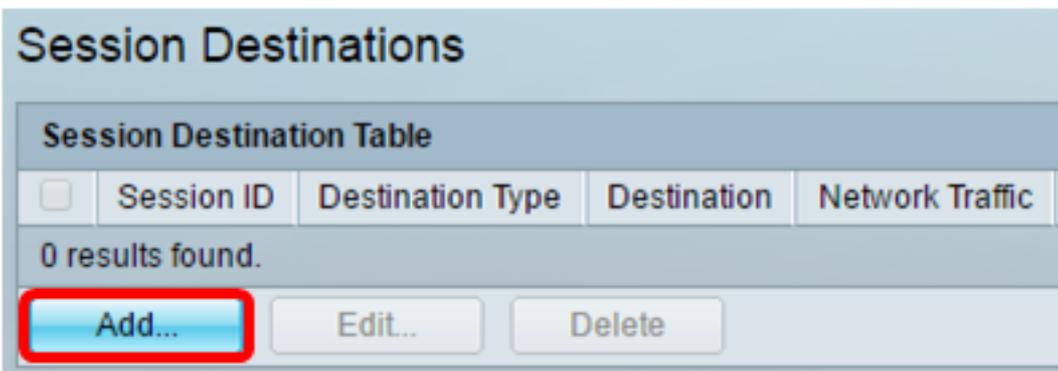
Vous devez maintenant avoir configuré la source de session sur votre commutateur de démarrage.

Configurer les destinations de session sur un commutateur de démarrage

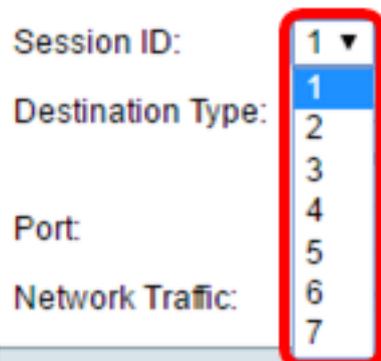
Étape 1. Choisissez **Status and Statistics > SPAN & RSPAN > Session Destinations**.



Étape 2. Cliquez sur **Add**.



Étape 3. Sélectionnez le numéro de session dans la liste déroulante ID de session. Il doit être identique à l'ID choisi dans la source de session configurée.



Note: Dans cet exemple, la session 1 est choisie.

Étape 4. Cliquez sur la case d'option **Remote VLAN** de la zone Destination Type. Un analyseur réseau, tel qu'un ordinateur exécutant Wireshark, est connecté à ce port.

Important : L'interface de destination ne peut pas être identique au port source.

Destination Type: Local Interface
 Remote VLAN (VLAN 20)

Note: Si le VLAN distant est sélectionné, le trafic réseau est automatiquement activé.

Étape 5. Dans la zone Port du réflecteur, sélectionnez l'option souhaitée dans la liste déroulante Unité. Sélectionnez le port à définir comme port source dans la liste déroulante Port.

Reflector Port: Unit Port
Network Traffic: Enable

Note: Dans cet exemple, le port GE20 de l'unité 1 est choisi.

Étape 6. Cliquez sur **Appliquer**, puis sur **Fermer**.

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

Étape 7. (Facultatif) Cliquez sur **Enregistrer** pour mettre à jour le fichier de configuration en cours.

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

Vous devez maintenant avoir configuré les destinations de session sur votre commutateur de

démarrage.

Commutateurs intermédiaires

Il peut également exister des commutateurs intermédiaires séparant les sessions source et de destination RSPAN. Ces commutateurs n'ont pas besoin de pouvoir exécuter RSPAN, mais ils doivent répondre aux exigences du VLAN RSPAN.

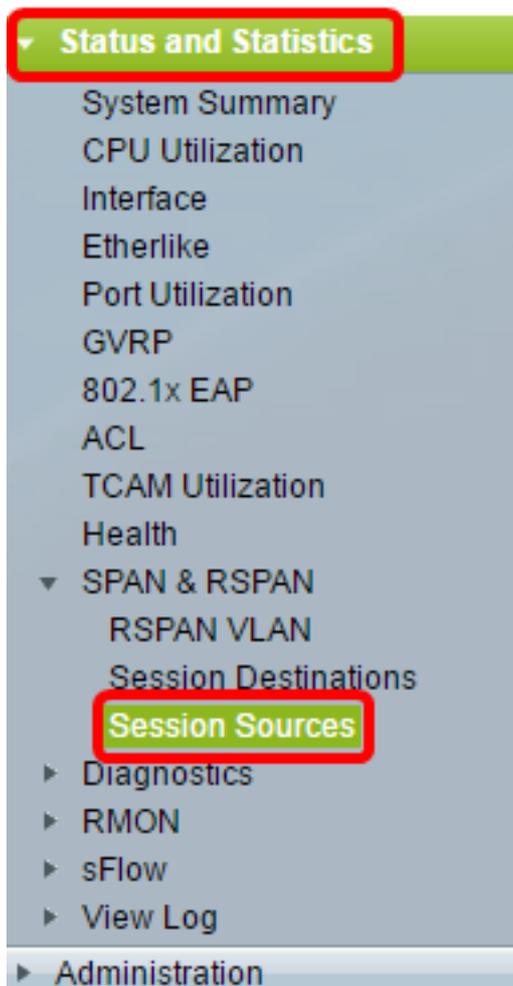
Pour les VLAN 1 à 1005 visibles par le protocole VTP (VLAN Trunking Protocol), l'ID de VLAN et ses caractéristiques RSPAN associées sont propagés par VTP. Si vous affectez un ID de VLAN RSPAN dans la plage de VLAN étendue (1006 à 4094), vous devez configurer manuellement tous les commutateurs intermédiaires.

Pour savoir comment attribuer un VLAN d'interface en tant que port agrégé d'un commutateur intermédiaire, cliquez [ici](#) pour obtenir des instructions.

Il est normal d'avoir plusieurs VLAN RSPAN dans un réseau en même temps avec chaque VLAN RSPAN définissant une session RSPAN à l'échelle du réseau. Autrement dit, plusieurs sessions source RSPAN n'importe où sur le réseau peuvent fournir des paquets à la session RSPAN. Il est également possible d'avoir plusieurs sessions de destination RSPAN sur l'ensemble du réseau, de surveiller le même VLAN RSPAN et de présenter le trafic à l'utilisateur. L'ID VLAN RSPAN sépare les sessions.

Configuration des sources de session sur un commutateur final

Étape 1. Choisissez **Status and Statistics > SPAN & RSPAN > Session Sources**.



Étape 2. Cliquez sur **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 [dropdown] [Go] [Clear Filter]. Below the filter, there is a table with columns: Session ID, Destination, Source Interface, and Monitor Type. The table shows '0 results found.' At the bottom of the table, there are three buttons: 'Add...' (highlighted with a red box), 'Edit...', and 'Delete'.

Étape 3. (Facultatif) Choisissez le numéro de session dans la liste déroulante ID de session. L'ID de session doit être cohérent par session.

The screenshot shows a dropdown menu for 'Session ID'. The number '1' is selected and highlighted with a red box. The dropdown menu also shows options 2, 3, 4, 5, 6, and 7.

Note: Dans cet exemple, la session 1 est choisie.

Étape 4. Cliquez sur la case d'option **Remote VLAN** de la zone Source Interface.

The screenshot shows the 'Source Interface' configuration section. It includes a 'Session ID' dropdown set to '1'. Below it, there are three radio button options: 'Unit [1] Port [GE1]', 'VLAN [1]', and 'Remote VLAN (VLAN 20)' (highlighted with a red box). Below these, there are three radio button options for 'Monitor Type': 'Rx and Tx' (selected), 'Rx', and 'Tx'. At the bottom, there are 'Apply' and 'Close' buttons.

Note: Le type de moniteur du VLAN distant sera automatiquement configuré.

Étape 5. Cliquez sur **Appliquer**, puis sur **Fermer**.

Étape 6. (Facultatif) Cliquez sur **Enregistrer** pour mettre à jour le fichier de configuration en cours.

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

Vous devez maintenant avoir configuré les sources de session sur votre commutateur final.

Configurer les destinations de session sur un commutateur final

Étape 1. Choisissez **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

Étape 2. Cliquez sur **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"/>				

Étape 3. Sélectionnez le numéro de session dans la liste déroulante ID de session. Il doit être identique à l'ID choisi dans la source de session configurée.

Session ID:

Destination Type:

Port:

Network Traffic:

Note: Dans cet exemple, la session 1 est choisie.

Étape 4. Cliquez sur la case d'option **Interface locale** de la zone Type de destination.

Destination Type: Local Interface Remote VLAN (VLAN 20)

Étape 5. Dans la zone Port, sélectionnez l'option souhaitée dans la liste déroulante Unité. Sélectionnez le port à définir comme port source dans la liste déroulante Port.

Port:

Network Traffic: Enable

Note: Dans cet exemple, le port GE20 de l'unité 1 est choisi.

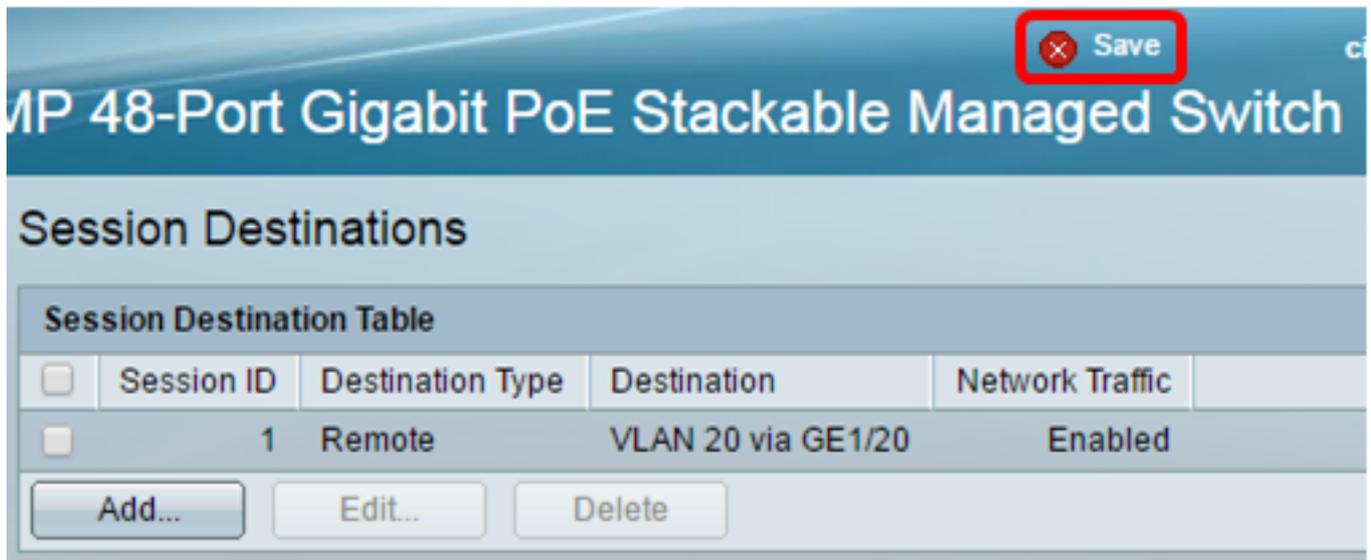
Étape 6. (Facultatif) Cochez la case **Activer le trafic réseau** pour activer le trafic réseau.

Port:

Network Traffic: Enable

Étape 7. Cliquez sur **Appliquer**, puis sur **Fermer**.

Étape 8. (Facultatif) Cliquez sur **Enregistrer** pour mettre à jour le fichier de configuration en cours.



Vous devez maintenant avoir configuré les destinations de session sur votre commutateur final.

Analyser les paquets VLAN RSPAN capturés dans WireShark

Dans ce scénario, l'hôte de l'interface source configurée, GE2 dans l'unité 1 (GE1/2), a l'adresse IP 192.168.1.100. Alors que l'hôte de l'interface de destination configurée, GE20 dans l'unité 1 (VLAN 20 via GE1/20), a une adresse IP de 192.168.1.127. Wireshark s'exécute sur l'hôte connecté à ce port.

En utilisant le filtre `ip.addr == 192.168.1.100`, Wireshark affiche les paquets capturés à partir de l'interface source distante.

*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

Afficher une vidéo relative à cet article...

[Cliquez ici pour afficher d'autres présentations techniques de Cisco](#)