ネットワークでのリモートスイッチポートアナライザ(RSPAN)の設定

目次

- 目的
- 該当するデバイス |ファームウェアのバージョン
- 概要
- スイッチでのRSPAN VLANの設定
- 開始スイッチでのセッションソースの設定
- 開始スイッチでのセッション宛先の設定
- 中間スイッチ
- 最終スイッチでのセッションソースの設定
- 最終スイッチでのセッション宛先の設定
- WireSharkでキャプチャされたRSPAN VLANパケットを分析する

目的

この記事では、スイッチでRSPANを設定する方法について説明します。

該当するデバイス |ファームウェアのバージョン

- Sx350 | 2.2.5.68 (最新のダウンロード)
- SG350X | 2.2.5.68 (最新のダウンロード)
- Sx550X | 2.2.5.68 (最新のダウンロード)

概要

スイッチポートアナライザ(SPAN)、またはポートミラーリングまたはポートモニタリングとも呼ばれる場合、ネットワークアナライザによる分析のためにネットワークトラフィックを選択します。ネットワーク アナライザは、Cisco SwitchProbe デバイスのこともあれば、その他の Remote Monitoring（RMON; リモート モニタリング）プローブのこともあります。

ネットワークデバイス上でポートミラーリングを使用して、1つのデバイスポート、複数のデバイスポート、またはVirtual Local Area Network(VLAN)全体で確認されたネットワークパケットのコピーを、デバイス上の別のポートのネットワークモニタリング接続に送信します。これは、侵入検知システムなどのネットワークトラフィックの監視を必要とするネットワークアプライアンスでよく使用されます。モニタリングポートに接続されたネットワークアナライザは、データパケットを処理して診断、デバッグ、およびパフォーマンスモニタリングを行います。

リモートスイッチポートアナライザ(RSPAN)は、SPANの拡張機能です。RSPANは、ネットワーク全体で複数のスイッチのモニタリングを有効にし、アナライザポートをリモートスイッチで定義できるようにすることで、SPANを拡張します。つまり、ネットワークキャプチャデバイスを一元化できます。

RSPANは、RSPANセッションの送信元ポートからのトラフィックを、RSPANセッション専用のVLANにミラーリングすることで動作します。その後、このVLANは他のスイッチにトランキングされ、RSPANセッショントラフィックを複数のスイッチ間で転送できるようになります。セッションの宛先ポートを含むスイッチでは、RSPANセッションVLANからのトラフィックが宛先ポー

トにミラーリングされます。

RSPANトラフィックフロー

- 各 RSPAN セッションのトラフィックは、すべての参加スイッチの当該 RSPAN セッション専用であるユーザ指定の RSPAN VLAN で伝送されます。
- 開始デバイスの送信元インターフェイスからのトラフィックは、リフレクタポートを介してRSPAN VLANにコピーされます。これは、設定する必要がある物理ポートです。RSPANセッションの構築にのみ使用されます。
- このリフレクタポートは、パケットをRSPAN VLANにコピーするメカニズムです。RSPANは、所属するRSPANソースセッションからのトラフィックのみを転送します。RSPAN ソース セッションがディセーブルになるまで、リフレクタ ポートとして設定されているポートに接続されているどのデバイスでも接続が失われます。
- その後、RSPANトラフィックは、中間デバイスのトランクポートを介して最終スイッチの宛先セッションに転送されます。
- 宛先スイッチはRSPAN VLANをモニタし、宛先ポートにコピーします。

RSPANポートメンバーシップ規則

- すべてのスイッチで：RSPAN VLANのメンバーシップはタグ付けのみ可能です。
- スイッチの開始

- SPAN送信元インターフェイスをRSPAN VLANのメンバにすることはできません。

– リフレクタポートをこのVLANのメンバにすることはできません。

– リモートVLANにメンバーシップがないことをお勧めします。

- 中間スイッチ

– ミラーリングされたトラフィックの通過に使用されないすべてのポートからRSPANメンバーシップを削除することを推奨します。

– 通常、RSPANリモートVLANには2つのポートがあります。

- 最終スイッチ

– ミラートラフィックの場合、送信元ポートはRSPAN VLANのメンバである必要があります。

– 宛先インターフェイスを含む他のすべてのポートからRSPANメンバーシップを削除することを推奨します。

ネットワークでのRSPANの設定

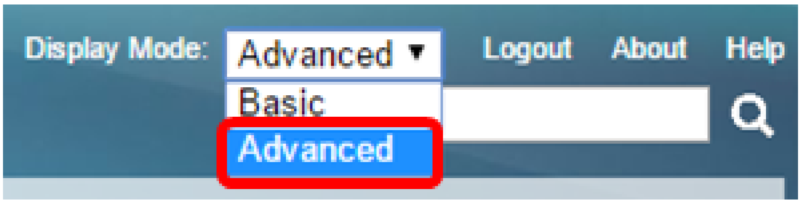
スイッチでのRSPAN VLANの設定

RSPAN VLANは、RSPAN送信元セッションと宛先セッションの間でSPANトラフィックを伝送します。これには次の特性があります。

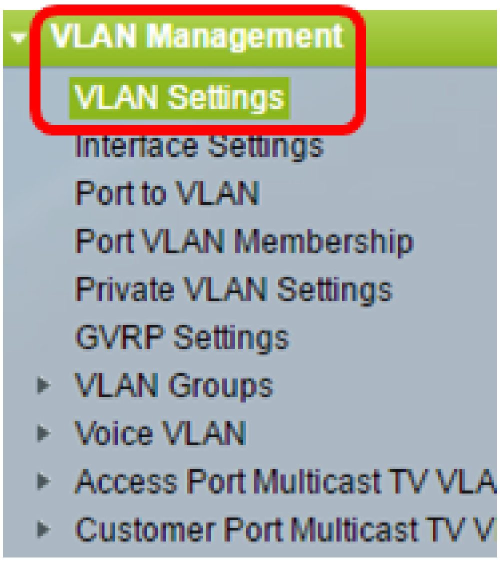
- RSPAN VLAN内のすべてのトラフィックは常にフラッディングされます。
- RSPAN VLANでは、メディアアクセスコントロール(MAC)アドレスの学習は行われません。
- RSPAN VLANトラフィックは、トランクポートでのみ流れます。

- STPはRSPAN VLANトランクでは実行できますが、SPAN宛先ポートでは実行できません。
- RSPAN VLANは、VLANコンフィギュレーションモードで**remote-span VLANコンフィギュレーションモードコマンドを使用して、開始スイッチと最終スイッチの両方で設定する必要があ**り、次の手順に従います。

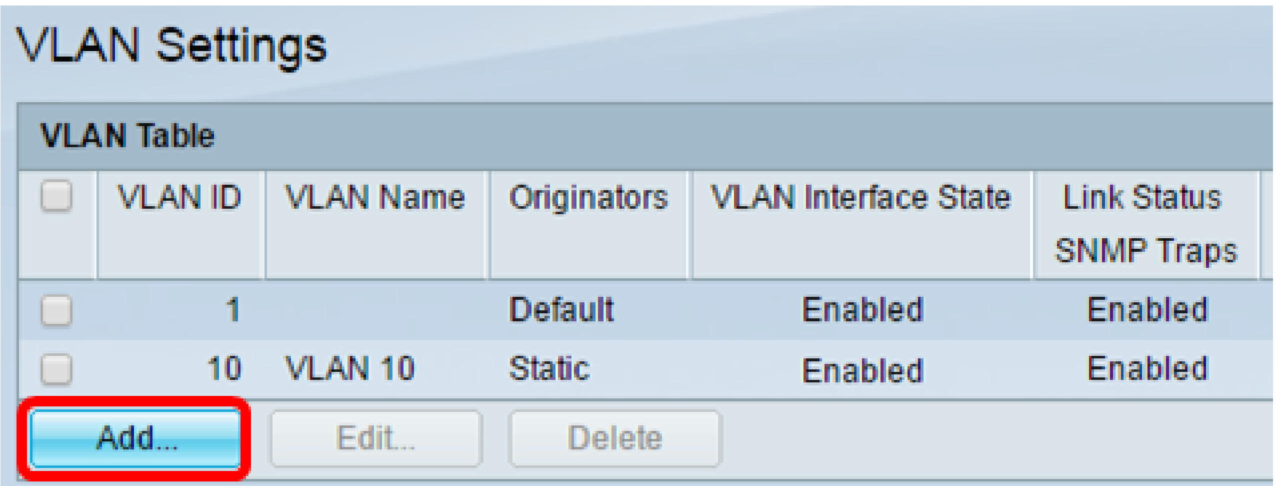
ステップ1：スタートスイッチのWebベースのユーティリティにログインし、[Display Mode]ドロップダウンリストで[**Advanced**]を選択します。



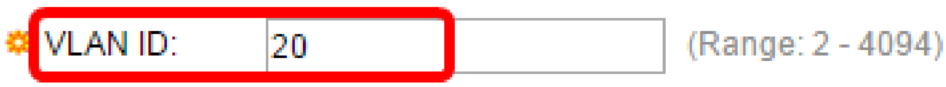
ステップ2:[**VLAN Management] > [VLAN Settings]を選択します。**



ステップ3:[Add]をクリッ**クします。**

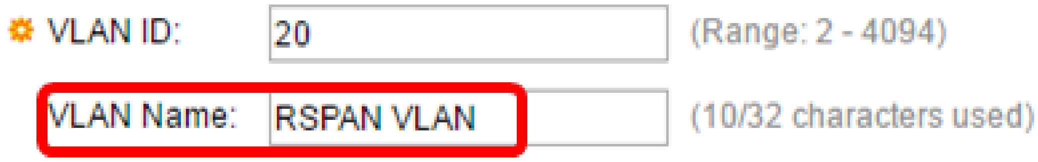


ステップ4:[VLAN ID]フィールドにVLAN IDを入力します。



注：この例では、VLAN IDとしてVLAN 20が使用されています。

ステップ5:（オプション）[VLAN Name]フィールドにVLAN名を入力します。

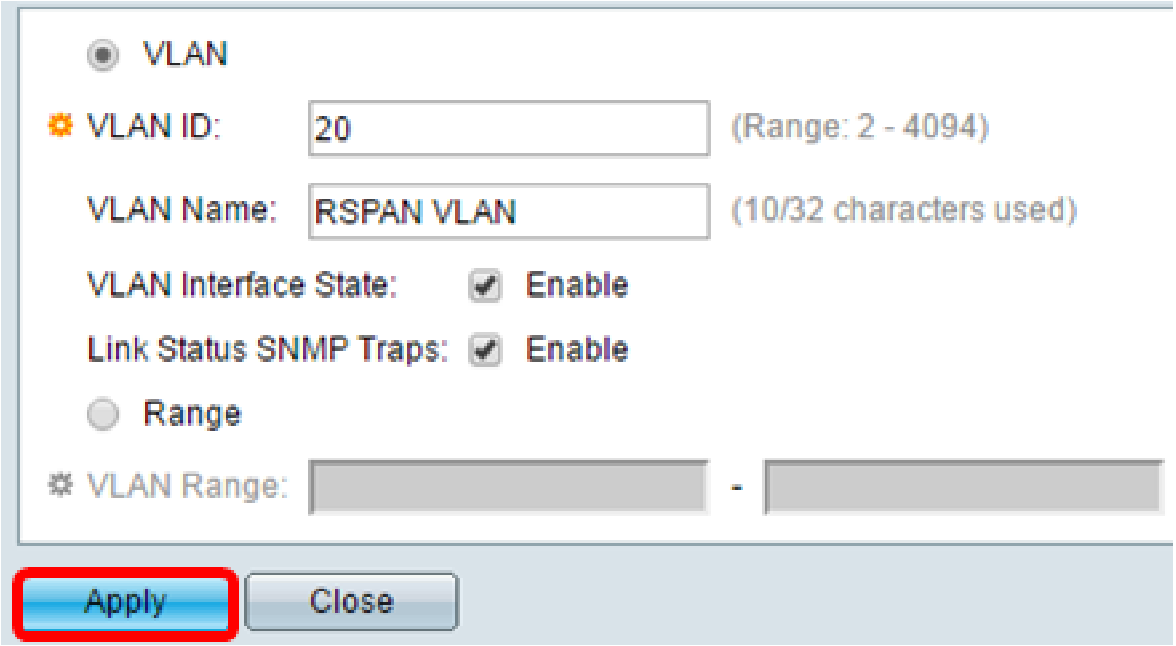


注：この例では、VLAN名としてRSPAN VLANが使用されています。

ステップ6:（オプション）[VLAN Interface State]チェックボックスをオンにして、VLANを有効にします。VLANがシャットダウンされている場合、VLANはメッセージを送受信しません。たとえば、IPインターフェイスが設定されているVLANをシャットダウンすると、VLANへのブリッジングは続行されますが、スイッチはVLAN上でIPトラフィックを送受信できません。この機能はデフォルトで有効になっています。

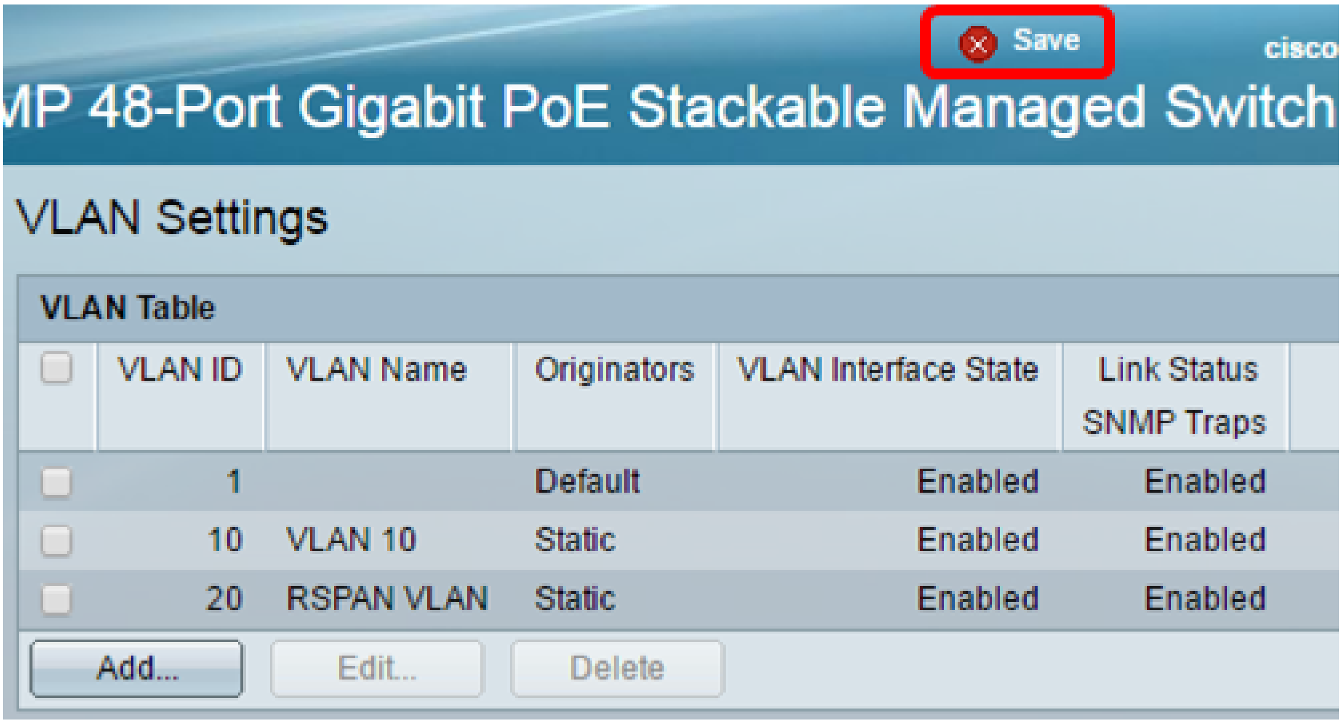
ステップ7:（オプション）[Link Status SNMP Traps]チェックボックスをオンにして、簡易ネットワーク管理プロトコル(SNMP)トラップのリンクステータス生成を有効にします。この機能はデフォルトで有効になっています。

ステップ8:[Apply]をクリックし、**[Close]をクリックします**。

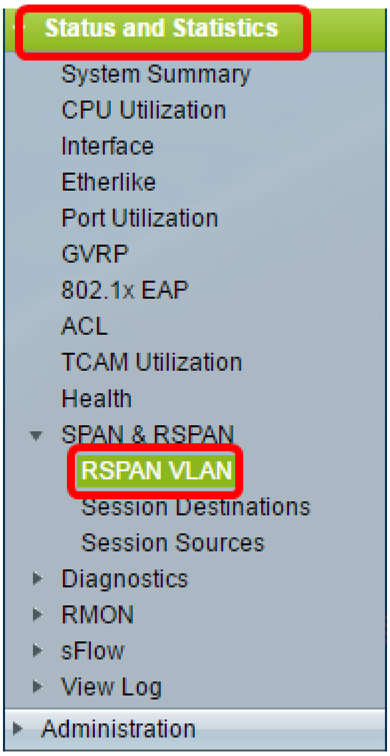


注：スイッチでのVLANの管理の詳細については、ここをクリックして[ください](#)。

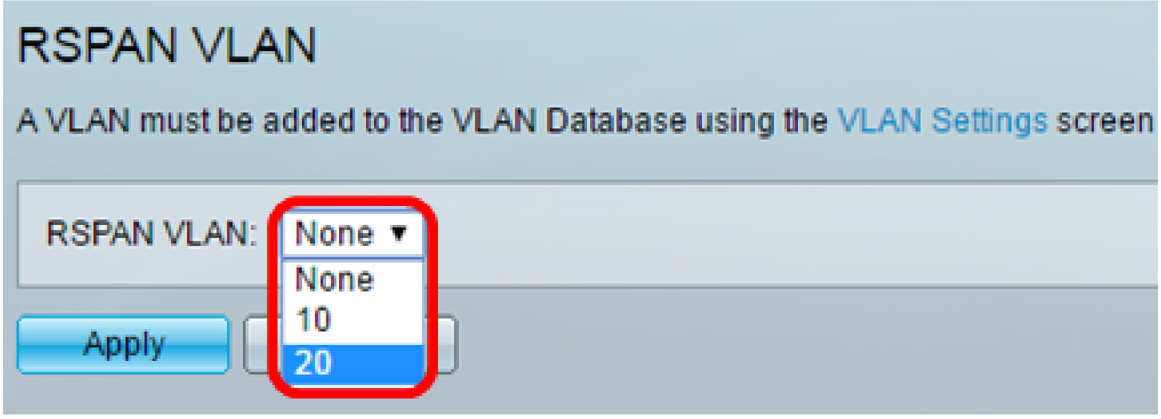
ステップ9:（オプション）**[Save]**をクリック**して実行**構成ファイルを更新します。



ステップ10:[Status and **Statistics] > [SPAN & RSPAN] > [RSPAN VLAN]を選択します。**

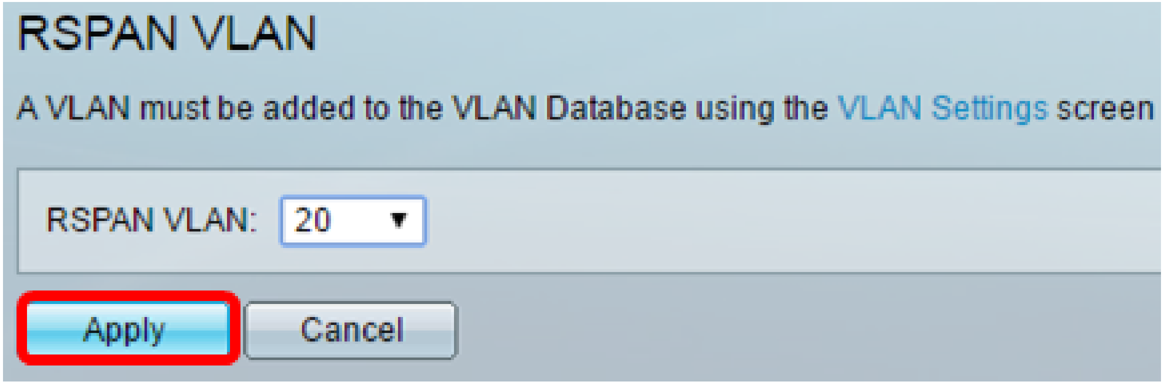


ステップ11:[RSPAN VLAN]ドロップダウンリストからVLAN IDを選択します。このVLANは、RSPAN専用に使用する必要があります。

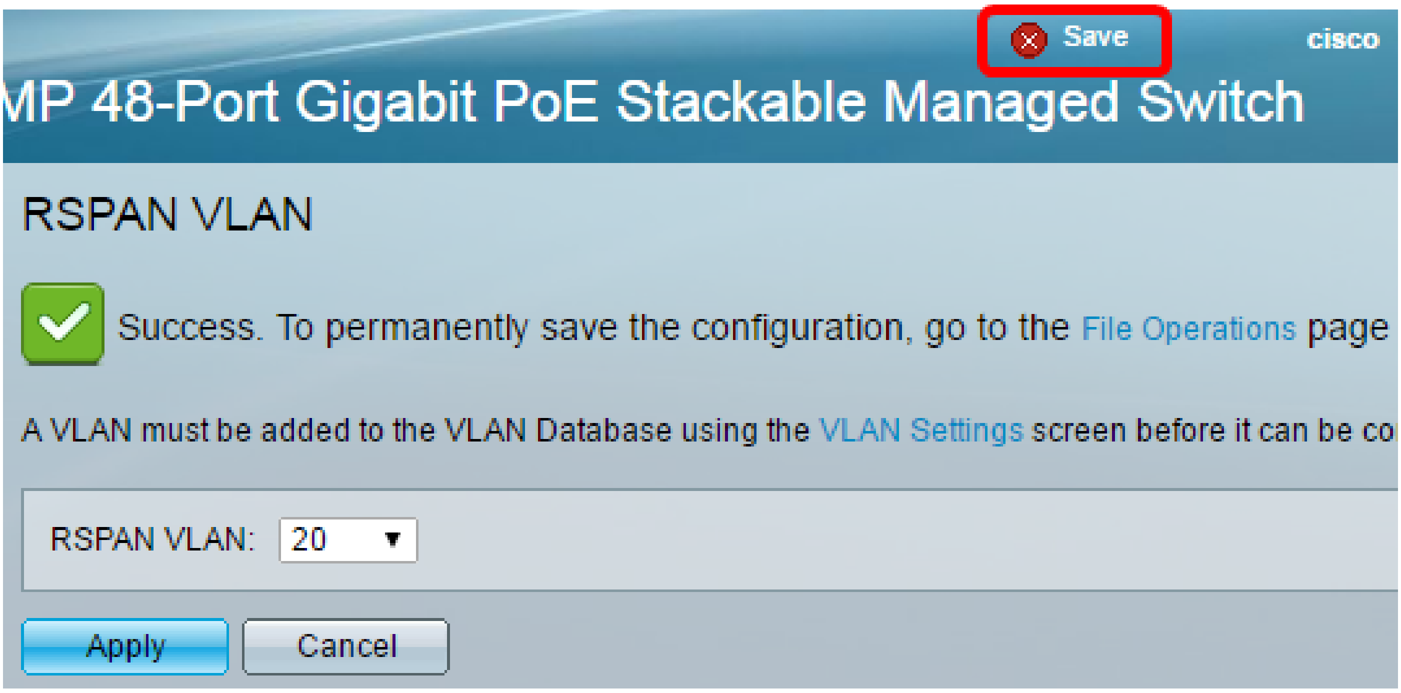


注：この例では、VLAN 20が選択されています。

ステップ12:[Apply]をクリックします。



ステップ13:（オプション）[Save]をクリックし、実行コンフィギュレーションファイルを更新します。

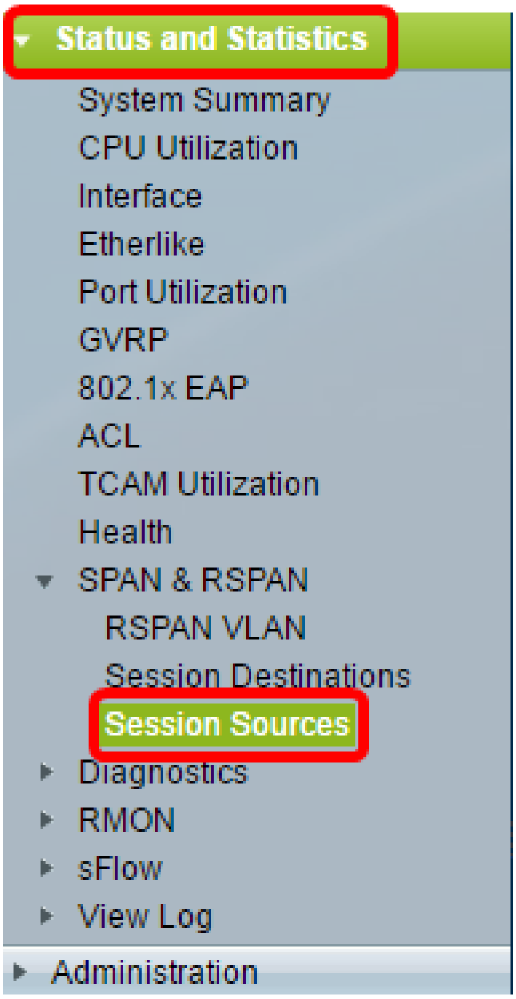


ステップ14：最終スイッチで、ステップ1 ～ 13を繰り返してRSPAN VLANを設定します。

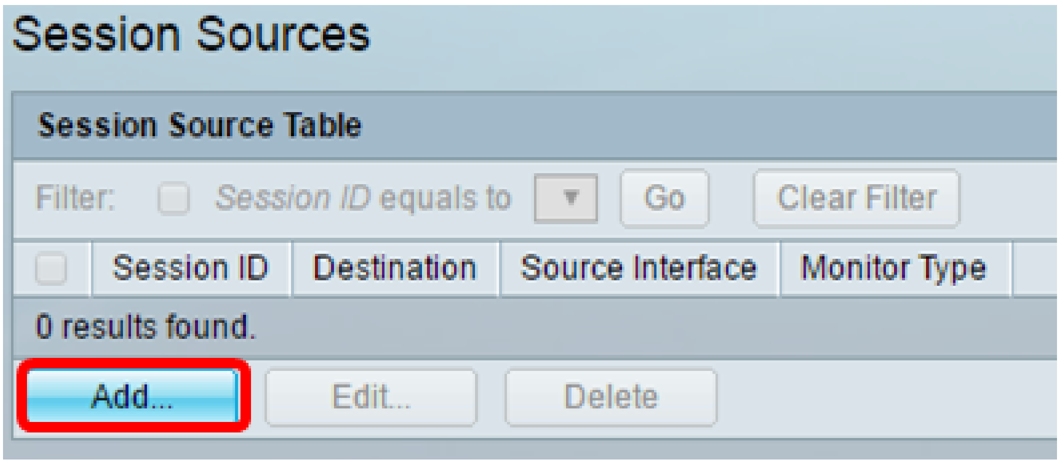
これで、開始スイッチと最終スイッチの両方で、RSPANセッション専用のVLANを設定できました。

開始スイッチでのセッションソースの設定

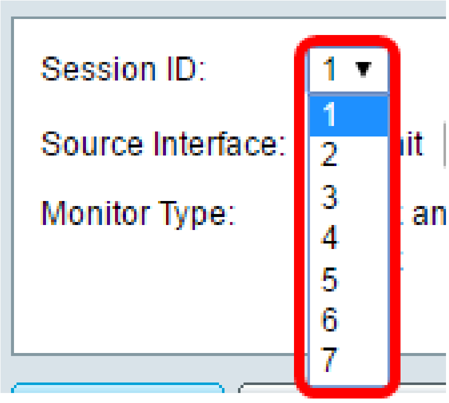
ステップ1:[Status and Statistics] > [SPAN & RSPAN] > [Session Sources]を選択します。



ステップ2:[Add]をクリックします。



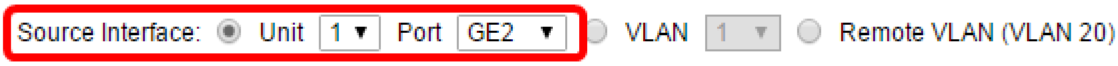
ステップ3:[Session ID]ドロップダウンリストからセッション番号を選択します。セッションIDは、RSPANセッションごとに一貫している必要があります。



注：この例では、Session 1が選択されています。

ステップ4：目的の送信元インターフェイスタイプのオプションボタンをクリックし、ドロップダウンリストからインターフェイスを選択します（複数可）。

重要：送信元インターフェイスを宛先ポートと同じにすることはできません。



次のオプションがあります。

- [Unit and Port]:[Unit]ドロップダウンリストから必要なオプションを選択し、[Port]ドロップダウンリストから送信元ポートとして設定するポートを選択できます。
- VLAN：モニタするVLANを[VLAN]ドロップダウンリストから選択できます。VLANは、ホストのグループが、場所に関係なく、同じ物理ネットワーク上にあるかのように通信するのに役立ちます。このオプションを選択すると、編集できませんでした。
- リモートVLAN：定義されたRSPAN VLANが表示されます。このオプションを選択すると、編集できませんでした。

注：この例では、ユニット1のポートGE2が選択されています。これは、モニタされるリモートインターフェイスです。

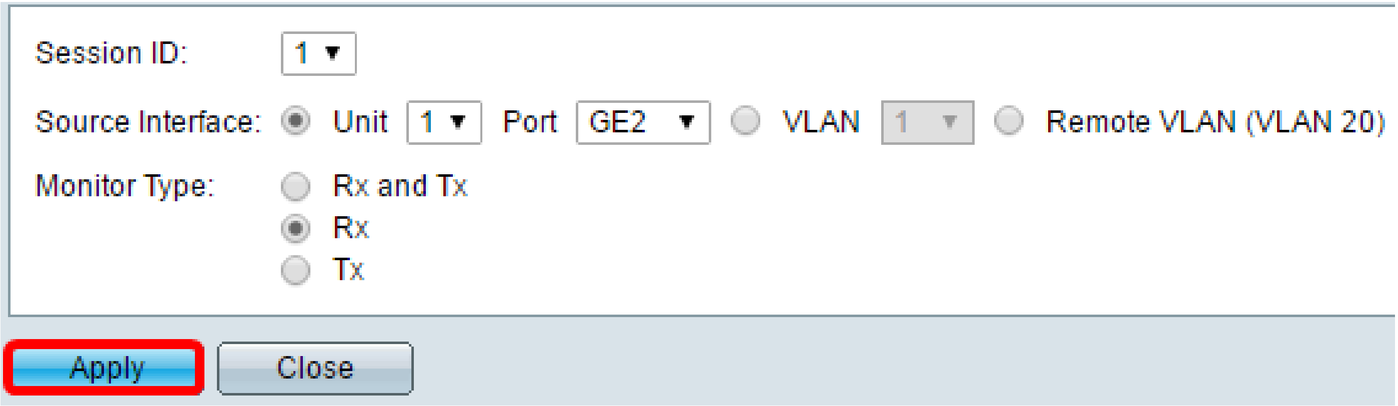
ステップ5:（オプション）ステップ4で[Unit and Port]をクリックした場合は、モニタするトラフィックのタイプに応じて、目的の[Monitor Type]オプションボタンをクリックします。

次のオプションがあります。

- RxおよびTx：このオプションは、着信パケットと発信パケットのポートミラーリングを許可します。このオプションはデフォルトで選択されています。
- Rx：着信パケットのポートミラーリングを許可します。
- Tx：このオプションは、発信パケットのポートミラーリングを許可します。

注：この例では、Rxが選択されています。

ステップ6:[Apply]をクリックし、**[Close]をクリックします。**

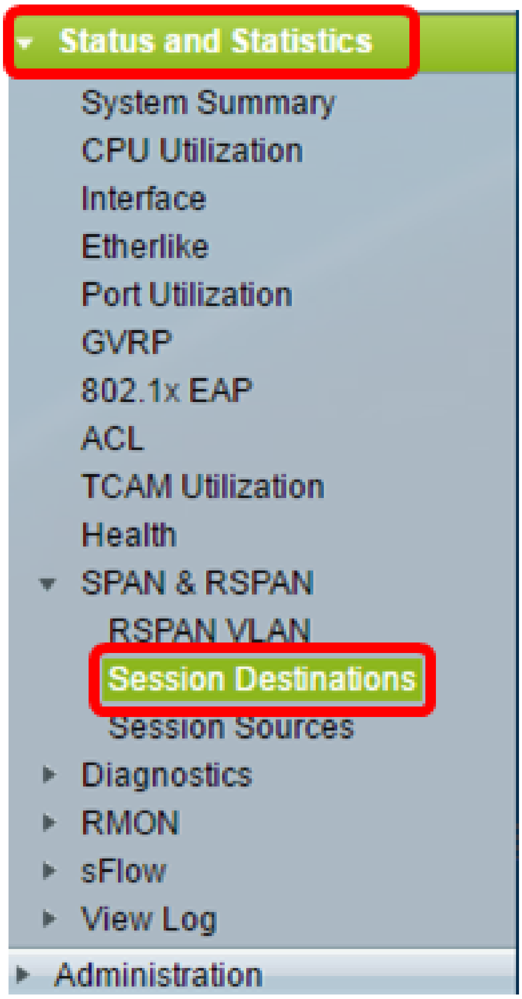


ステップ7:（オプション）**[Save]**をクリックして**実行**構成ファイルを更新します。

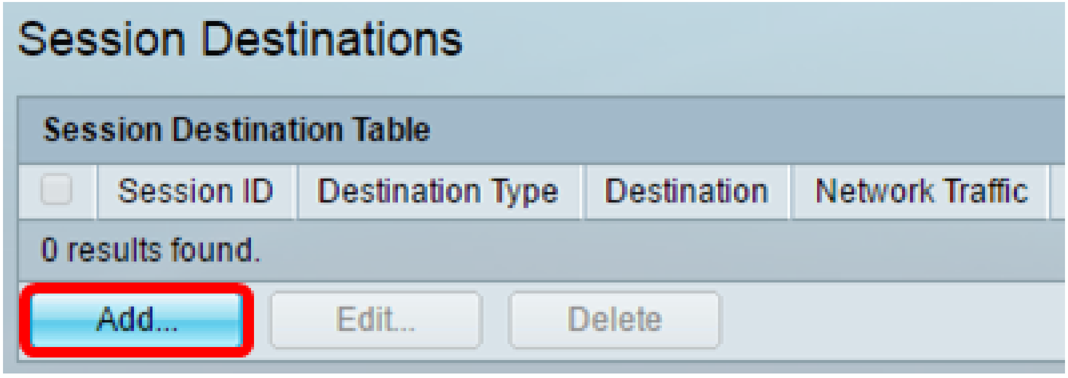
これで、Start Switchでセッションソースを設定できました。

開始スイッチでのセッション宛先の設定

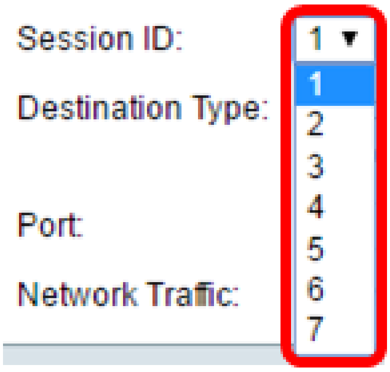
ステップ1:[Status and **Statistics] > [SPAN & RSPAN] > [Session Destinations]を選択します。**



ステップ2:[Add]をクリックします。



ステップ3:[Session ID]ドロップダウンリストからセッション番号を選択します。これは、設定されたセッションソースから選択されたIDと同じである必要があります。



注：この例では、Session 1が選択されています。

ステップ4:[Destination Type]領域から[**Remote VLAN**]オプションボタンをクリックします。Wiresharkを実行しているコンピュータなどのネットワークアナライザがこのポートに接続されています。

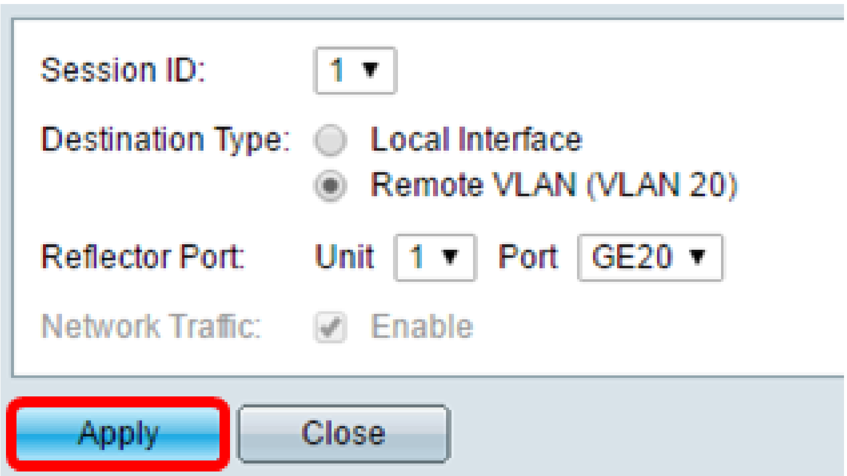
重要：宛先インターフェイスを送信元ポートと同じにすることはできません。

注：[リモートVLAN]を選択すると、ネットワークトラフィックが自動的に有効になります。

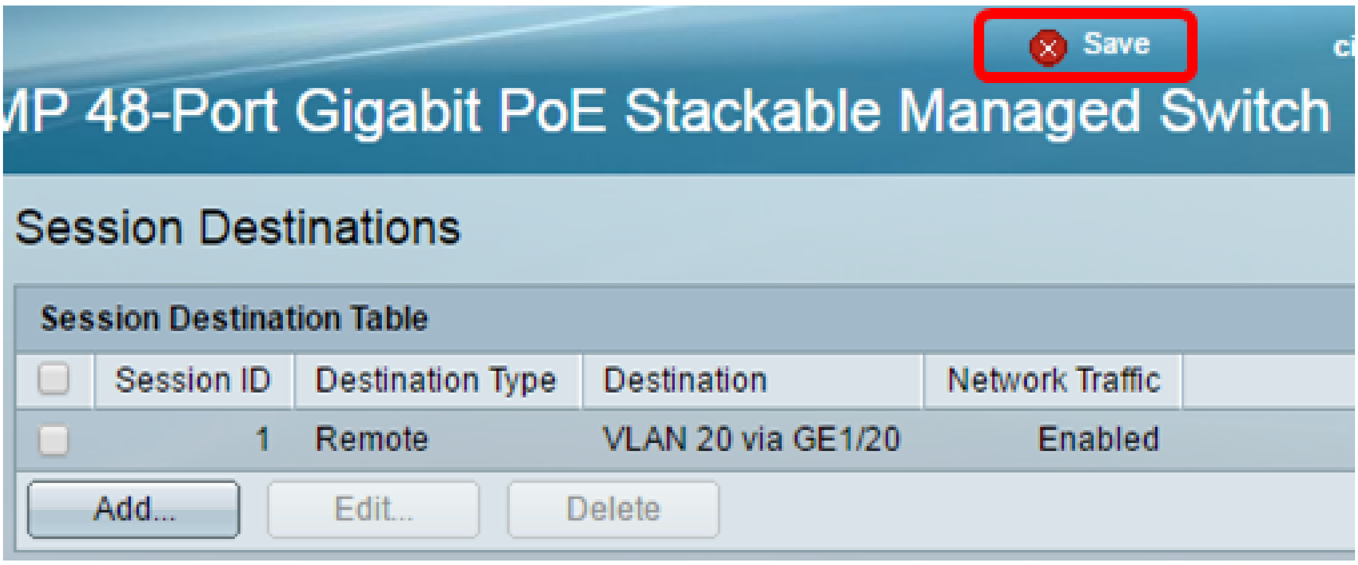
ステップ5:[Reflector Port]領域で、[Unit]ドロップダウンリストから必要なオプションを選択します。[Port]ドロップダウンリストから、送信元ポートとして設定するポートを選択します。

注：この例では、ユニット1のポートGE20が選択されています。

ステップ6:[Apply]をクリックし、[**Close**]をク**リックします**。



ステップ7:（オプション）[**Save**]をクリックし**て実行**構成ファイルを更新します。



これで、Start Switchでセッションの宛先を設定できました。

中間スイッチ

RSPANの送信元セッションと宛先セッションを分離する中間スイッチも存在できます。これらのスイッチはRSPANを実行できる必要はありませんが、RSPAN VLANの要件に対応する必要があります。

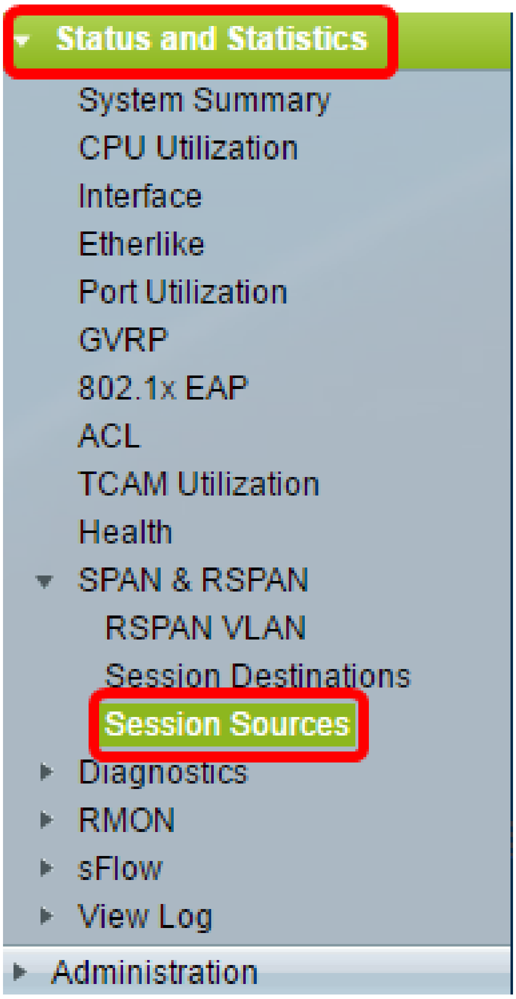
VLAN 1 ～ 1005がVLAN Trunking Protocol(VTP)で認識されている場合、VLAN IDとそれに関連するRSPAN特性はVTPによって伝搬されます。拡張VLAN範囲(1006 ～ 4094)でRSPAN VLAN IDを割り当てる場合は、すべての中間スイッチを手動で設定する必要があります。

インターフェイスVLANを中間スイッチのトランクポートとして割り当てる方法については、ここをクリックしてください。

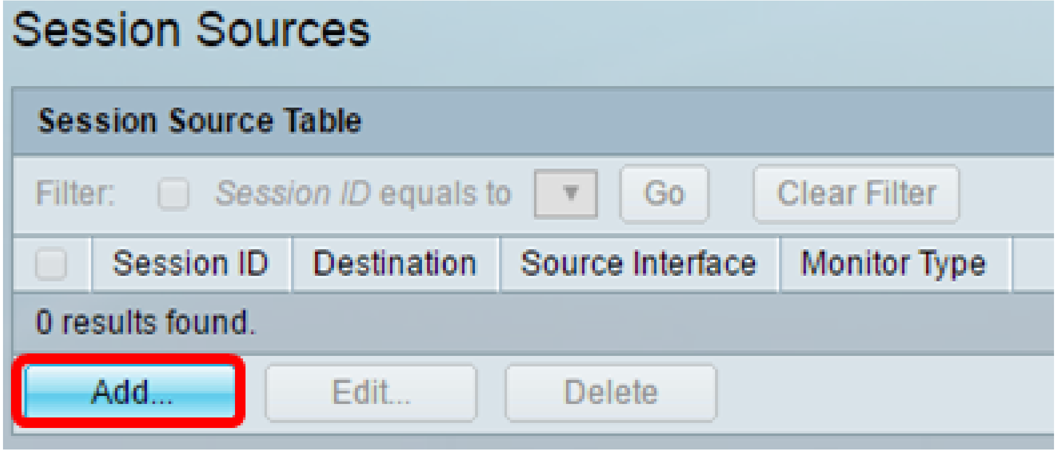
ネットワーク全体のRSPANセッションを定義する各RSPAN VLANと同時に、複数のRSPAN VLANをネットワークに持つことは正常です。つまり、ネットワーク内の任意の場所で複数のRSPAN送信元セッションがパケットをRSPANセッションに送信できます。また、ネットワーク全体で複数のRSPAN宛先セッションを持ち、同じRSPAN VLANを監視し、ユーザにトラフィックを提示することもできます。RSPAN VLAN IDはセッションを分離します。

最終スイッチでのセッションソースの設定

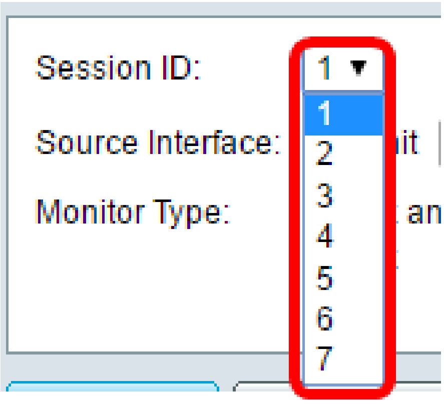
ステップ1:[Status and **Statistics] > [SPAN & RSPAN] > [Session Sources]を選択します。**



ステップ2:[Add]をクリッ**クします。**

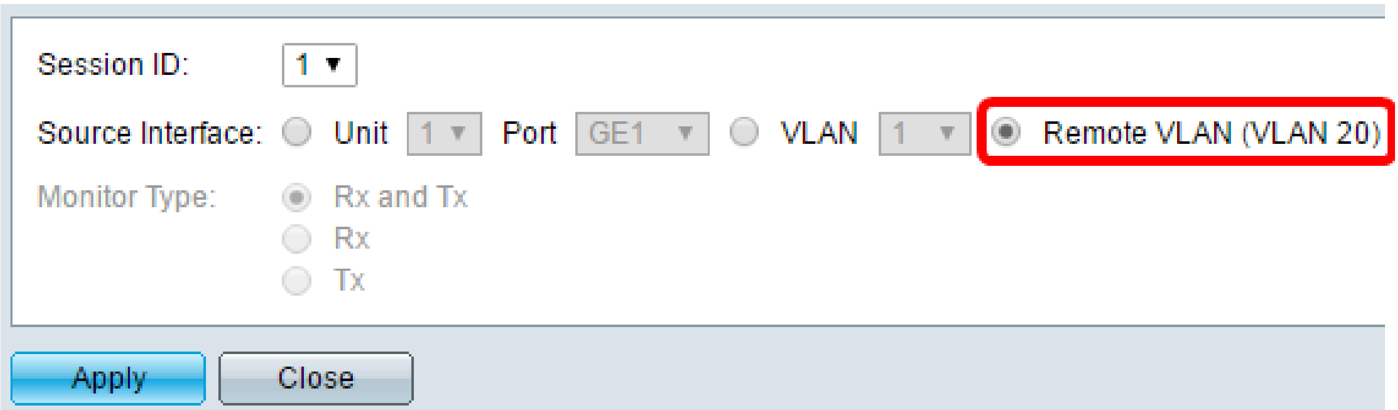


ステップ3:（オプション）[Session ID]ドロップダウンリストからセッション番号を選択します。セッションIDは、セッションごとに一貫している必要があります。



注：この例では、Session 1が選択されています。

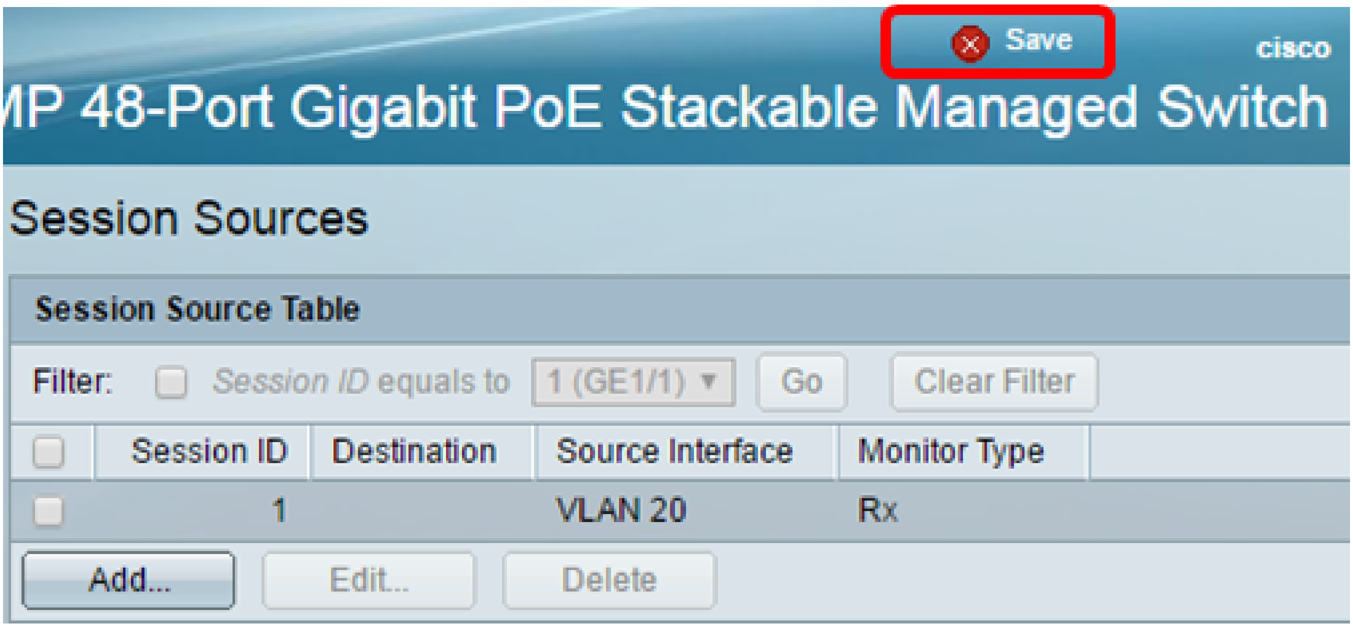
ステップ4:[Source Interface]領域から**[Remote VLAN]**オプションボタンをクリックします。



注：リモートVLANのモニタタイプが自動的に設定されます。

ステップ5:[Apply]をクリックし、**[Close]**をクリック**します。**

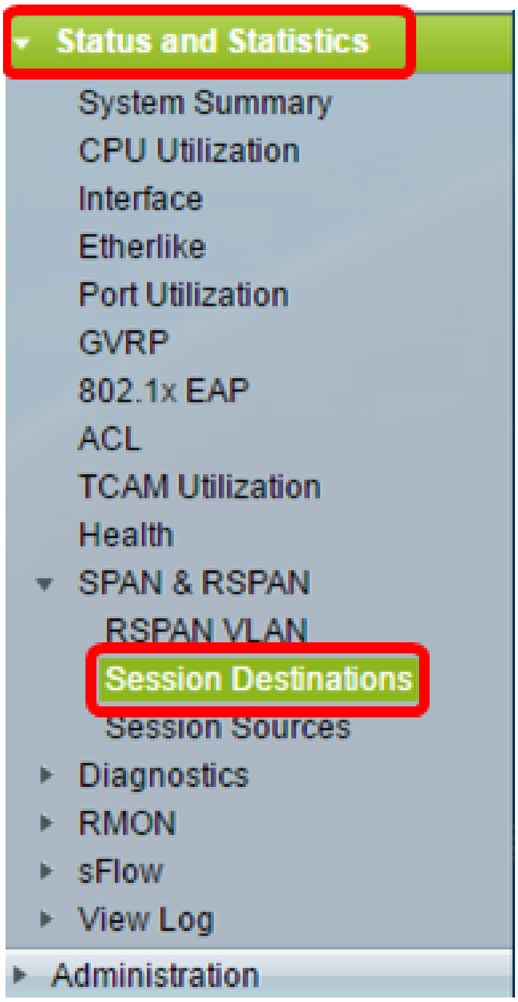
ステップ6:（オプション）**[Save]**をクリックし**て実行**構成ファイルを更新します。



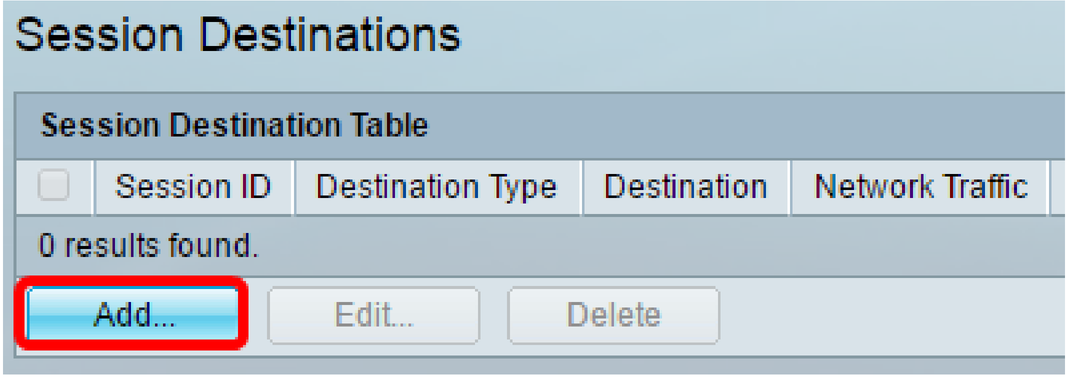
これで、最終スイッチのセッションソースが設定されているはずです。

最終スイッチでのセッション宛先の設定

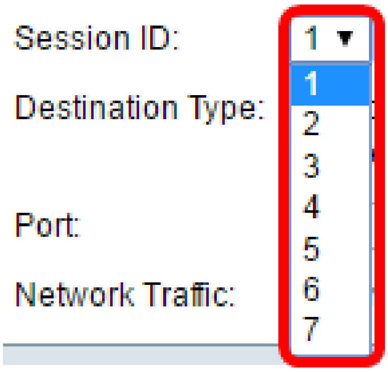
ステップ1:[Status and **Statistics] > [SPAN & RSPAN] > [Session Destinations]を選択します。**



ステップ2:[Add]をクリ**ックします。**



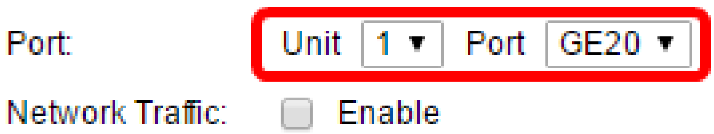
ステップ3:[Session ID]ドロップダウンリストからセッション番号を選択します。これは、設定されたセッションソースから選択されたIDと同じである必要があります。



注：この例では、Session 1が選択されています。

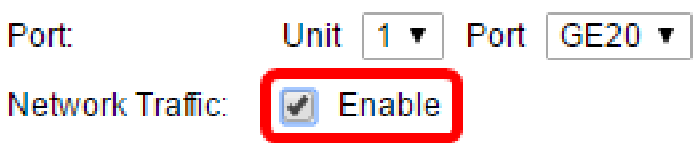
ステップ4:[Destination Type]領域から[**Local Interface**]オプションボタンをクリックします。

ステップ5:[Port（ポート）]領域で、[Unit（ユニット）]ドロップダウンリストから必要なオプションを選択します。[Port]ドロップダウンリストから、送信元ポートとして設定するポートを選択します。



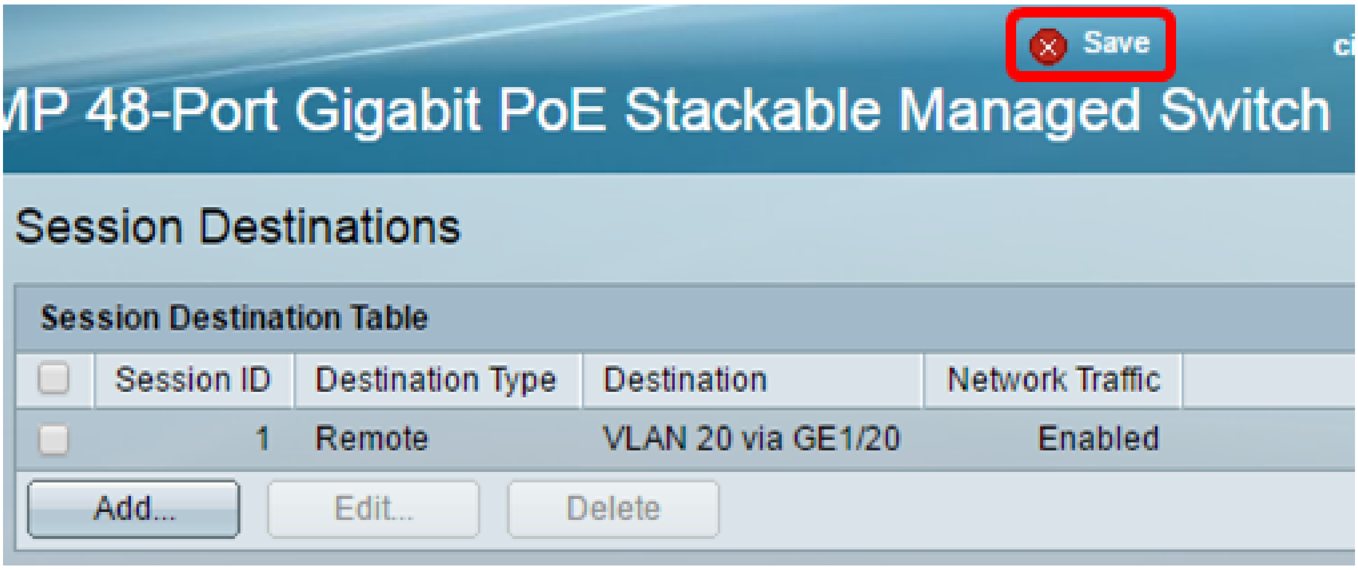
注：この例では、ユニット1のポートGE20が選択されています。

ステップ6:（オプション）ネットワークトラフィックを有効にするには、[**ネットワークトラフィックを有効**にする]チェックボックスをオンにします。



ステップ7:[Apply]をクリックし、[**Close**]をクリ**ックします**。

ステップ8:（オプション）[**Save**]をクリックし**て実行**構成ファイルを更新します。

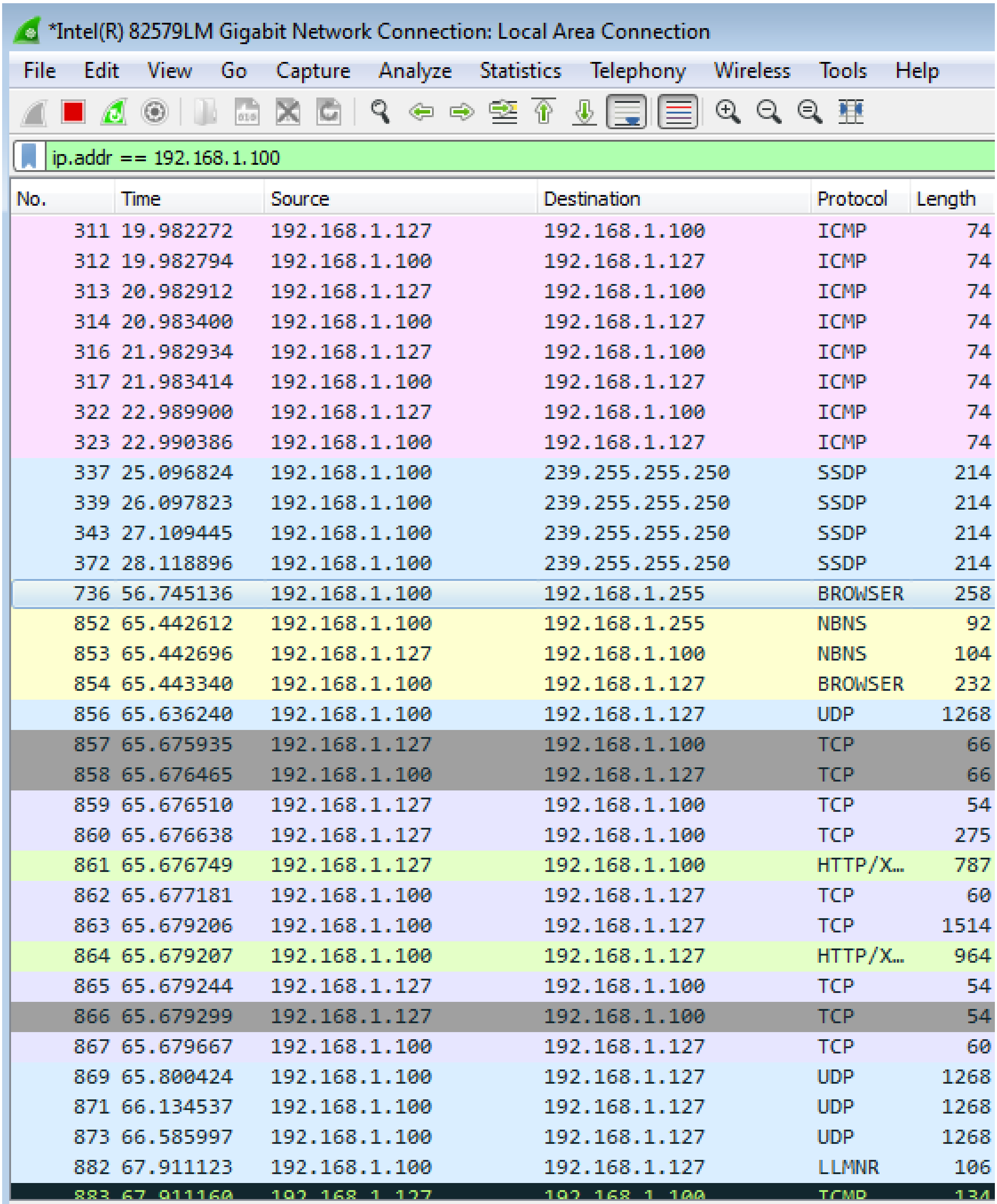


これで、最終スイッチでセッションの宛先を設定できました。

WireSharkでキャプチャされたRSPAN VLANパケットを分析する

このシナリオでは、ユニット1(GE1/2)の送信元インターフェイスのホストGE2(GE1/2)のIPアドレスは192.168.1.100で、ユニット1（GE1/20を介したVLAN 20）のホストのIPアドレスは192.168.1.127ですポート。

フィルタip.addr == 192.168.1.100を使用して、Wiresharkはリモートソースインターフェイスからキャプチャされたパケットを表示します。



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	ICMP	134

この記事に関連するビデオを表示...

シスコのその他のテクニカルトークを表示するには、ここをクリックしてください