



SPAN および RSPAN の設定

この章では、Catalyst 3750 スイッチに Switched Port Analyzer (SPAN; スイッチド ポート アナライザ) および Remote SPAN (RSPAN) を設定する方法について説明します。特に明記しないかぎり、スイッチという用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。



(注)

この章で使用されるコマンドの構文および使用方法の詳細については、このリリースのコマンドリファレンスを参照してください。

この章で説明する内容は、次のとおりです。

- [SPAN および RSPAN の概要 \(p.28-2\)](#)
- [SPAN および RSPAN の設定 \(p.28-11\)](#)
- [SPAN および RSPAN ステータスの表示 \(p.28-25\)](#)

SPAN および RSPAN の概要

ポートまたは VLAN (仮想 LAN) を通過するネットワーク トラフィックを分析するには、SPAN または RSPAN を使用して、そのスイッチの別のポート、またはネットワーク アナライザなどのモニタリング デバイスやセキュリティ デバイスに接続されている別のスイッチ上のポートにトラフィックのコピーを送信します。SPAN は送信元ポートまたは送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー (ミラーリング) して、分析します。SPAN は送信元ポートまたは VLAN 上のネットワーク トラフィックのスイッチングに影響を与えません。宛先ポートを SPAN 専用にする必要があります。SPAN または RSPAN セッションに必要なトラフィック以外のトラフィックを、宛先ポートが受信または転送することはありません。

SPAN を使用してモニタできるのは、送信元ポートを出入りするトラフィックまたは送信元 VLAN に入出力するトラフィックだけです。送信元 VLAN にルーティングされるトラフィックはモニタできません。たとえば、着信トラフィックをモニタしている場合、別の VLAN から送信元 VLAN にルーティングされているトラフィックはモニタできません。ただし、送信元 VLAN で受信し、別の VLAN にルーティングされるトラフィックは、モニタできます。

SPAN または RSPAN 宛先ポートを使用すると、ネットワーク セキュリティ デバイスからトラフィックを送信できます。たとえば、Cisco Intrusion Detection System (IDS; 侵入検知システム) センサ装置を宛先ポートに接続した場合、IDS デバイスは TCP リセット パケットを送信して疑わしい攻撃者の TCP セッションを停止できます。

ここでは、次の概要について説明します。

- [ローカル SPAN \(p.28-2\)](#)
- [RSPAN \(p.28-4\)](#)
- [SPAN および RSPAN の概念と用語 \(p.28-4\)](#)
- [SPAN および RSPAN の他の機能との相互作用 \(p.28-9\)](#)
- [SPAN/RSPAN およびスイッチ スタック \(p.28-10\)](#)

ローカル SPAN

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じスイッチまたはスイッチ スタック内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートあるいは 1 つまたは複数の VLAN から宛先ポートに送信されるトラフィックをコピーして、分析します。たとえば、[図 28-1](#) では、ポート 5 (送信元ポート) 上のすべてのトラフィックがポート 10 (宛先ポート) にミラーリングされています。ポート 10 のネットワーク アナライザは、ポート 5 に物理的に接続しなくても、ポート 5 からすべてのネットワーク トラフィックを受信します。

図 28-1 単一スイッチでのローカル SPAN の設定例

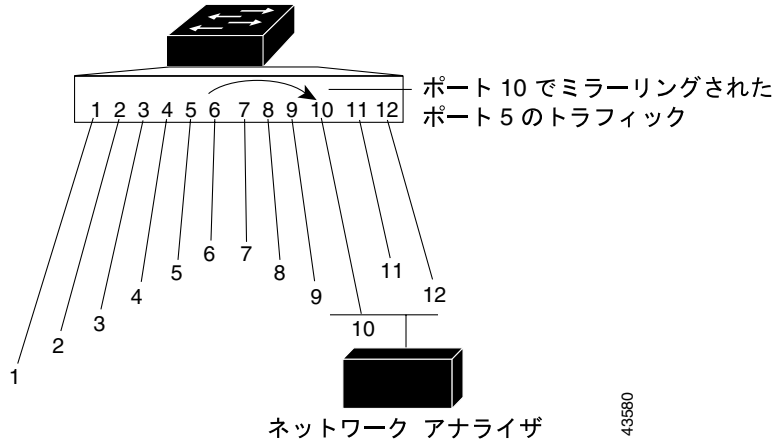
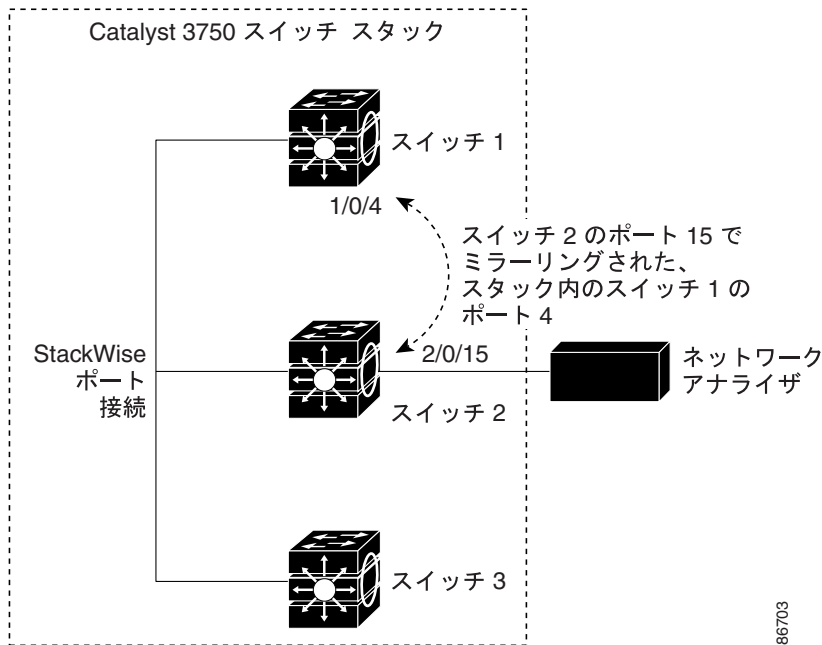


図 28-2 に、送信元ポートおよび宛先ポートが異なるスタック メンバー上にある場合の、スイッチ スタックのローカル SPAN の例を示します。

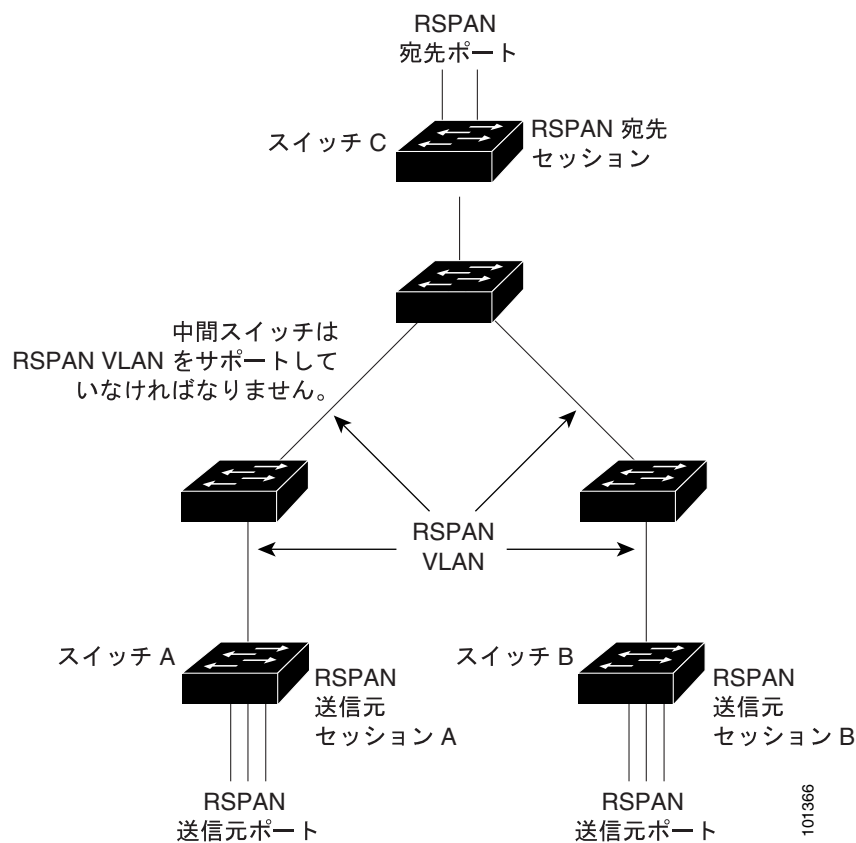
図 28-2 スイッチ スタックでのローカル SPAN の設定例



RSPAN

RSPAN は異なるスイッチ（または異なるスイッチ スタック）上の送信元ポート、送信元 VLAN、および宛先ポートをサポートし、ネットワーク上の複数のスイッチのリモート モニタリングを可能にします。図 28-3 に、スイッチ A およびスイッチ B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、ユーザが指定した RSPAN VLAN 上で搬送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランクポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。各 RSPAN 送信元スイッチでは、RSPAN 送信元としてポートまたは VLAN のいずれかを設定する必要があります。宛先は常に物理ポートになります（図のスイッチ C）。

図 28-3 RSPAN の設定例



SPAN および RSPAN の概念と用語

ここでは、SPAN および RSPAN の設定に関連する概念と用語について説明します。

SPAN セッション

SPAN セッション（ローカルまたはリモート）を使用すると、1 つまたは複数のポート、あるいは 1 つまたは複数の VLAN 上でトラフィックをモニタし、モニタしたトラフィックを 1 つまたは複数の宛先ポートに送信できます。

ローカル SPAN セッションは、宛先ポートと送信元ポートまたは送信元 VLAN (すべて単一のネットワーク デバイス上にある) の対応付けです。ローカル SPAN には、送信元セッションおよび宛先セッションが個別に設定されません。ローカル SPAN セッションはユーザが指定した入力および出力のパケット セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は 1 つまたは複数の RSPAN 送信元セッション、1 つの RSPAN VLAN、および 1 つまたは複数の RSPAN 宛先セッションで構成されます。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを設定するには、送信元ポートまたは送信元 VLAN のセットを RSPAN VLAN と関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN と関連付けます。宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

RSPAN 送信元セッションは、パケット ストリームの転送先を除き、ローカル SPAN セッションに非常に似ています。RSPAN 送信元セッションでは、SPAN パケットに RSPAN VLAN ID ラベルが再設定され、通常のトランク ポートを介して宛先スイッチに転送されます。

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットから VLAN タギングを除去し、宛先ポートに送ります。RSPAN 宛先セッションの目的は、(レイヤ 2 制御パケットを除く) すべての RSPAN VLAN パケットをユーザにコピーして、分析することです。

同じ RSPAN VLAN 内で、複数の送信元セッションと複数の宛先セッションをアクティブにできます。RSPAN 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を配置することもできます。これらのスイッチには RSPAN の実行機能は不要ですが、RSPAN VLAN の要件を満たす必要があります (「RSPAN VLAN」 [p.28-9] を参照)。

SPAN セッションでのトラフィックのモニタには、次のような制限があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- スイッチは 2 つまでのソース セッション (ローカル SPAN と RSPAN のソース セッション) をサポートします。同じスイッチ スタック内でローカル SPAN と RSPAN のソース セッションの両方を実行できます。スイッチ スタックは合計 66 個の送信元および RSPAN 宛先セッションをサポートします。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのスイッチ スタックに設定できる宛先ポートは最大で 64 個です。
- 個別のまたは重複する SPAN 送信元ポートと VLAN の集合を使用して、2 つの独立した SPAN または RSPAN 送信元セッションを設定できます。スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- SPAN セッションは、スイッチの正常な動作を妨げません。ただし、SPAN の宛先がオーバーサブスクライブ型ポートである場合 (たとえば 100 Mbps ポートをモニタする 10 Mbps ポートなど) パケットが廃棄されるか、または消失する可能性があります。
- RSPAN がイネーブルの場合、モニタ中の各パケットは 2 回伝送されます。1 回は標準トラフィックとして、もう 1 回はモニタされたパケットとしてです。したがって、多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- デイセーブルのポート上でも SPAN セッションを設定できます。宛先ポートと、1 つまたは複数の送信元ポートまたは VLAN をイネーブルにしないかぎり、SPAN セッションはアクティブになりません。
- スイッチの単一セッション内では、ローカル SPAN と RSPAN を併用できません。つまり、RSPAN 送信元セッションにローカル宛先ポートを設定したり、RSPAN 宛先セッションにローカル送信元ポートを設定したり、同じスイッチ スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行することはできません。

モニタ対象トラフィック

SPAN セッションは、次のトラフィック タイプをモニタできます。

- 受信 (RX) SPAN 受信 (または入力) SPAN の目的は、スイッチが変更または処理を行う前に送信元インターフェイスまたは VLAN が受信したすべてのパケットをできるかぎり多くモニタすることです。送信元が受信した各パケットのコピーがその SPAN セッションの宛先ポートに送信されます。

Differentiated Services Code Point (DSCP) の変更など、ルーティングまたは Quality of Service (QoS; サービス品質) が原因で変更されるパケットは、変更前にコピーされます。

受信処理中にパケットを廃棄する可能性のある機能は、入力 SPAN には無効です。宛先ポートは、実際の着信パケットが廃棄された場合でも、パケットのコピーを受信します。これらの機能には、標準および拡張 IP 入力 Access Control List (ACL; アクセス制御リスト)、入力 QoS ポリシング、VLAN ACL、出力 QoS ポリシングなどがあります。
- 送信 (TX) SPAN 送信 (または出力) SPAN の目的は、スイッチによる変更または処理がすべて実行されたあとに、送信元インターフェイスから送信されたすべてのパケットをできるかぎり多くモニタすることです。送信元から送信された各パケットのコピーは、その SPAN セッションに対応する宛先ポートに送信されます。コピーは、パケットの変更後送信されます。

ルーティングが原因で変更されたパケット (Time to Live[TTL]、MAC[メディア アクセス制御]アドレス、QoS 値の変更など) は、宛先ポートで (変更されて) コピーされます。

送信処理中にパケットを廃棄する可能性のある機能は、SPAN 用のコピーにも影響を与えます。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングなどがあります。
- 双方向 1つの SPAN セッションで、単一のポートまたは VLAN の送信パケットと受信パケットを両方モニタできます。これはデフォルト設定です。

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。通常、SPAN は Cisco Discovery Protocol (CDP)、VLAN Trunk Protocol (VTP; VLAN トランク プロトコル)、Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル)、Spanning-Tree Protocol (STP; スパニングツリー プロトコル)、Port Aggregation Protocol (PAgP; ポート集約プロトコル) などの Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) パケットおよびレイヤ 2 プロトコルをモニタしません。ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次のように変更されます。

- 送信元ポートの場合と同じカプセル化設定 (タグなし、ISL [スイッチ間リンク] または IEEE 802.1Q) を使用して、パケットが宛先ポートに送信されます。
- BPDU やレイヤ 2 プロトコル パケットを含むすべてのタイプのパケットがモニタされます。

したがって、カプセル化レプリケーションがイネーブル化されたローカル SPAN セッションでは、タグなし、ISL、IEEE 802.1Q タグ付きパケットが宛先ポートに混在する場合があります。

スイッチが輻輳すると、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットが廃棄されることがあります。一般に、これらの特性は相互に依存しません。次に例を示します。

- パケットは通常どおり転送されますが、SPAN 宛先ポートのオーバーサブスクライブが原因でモニタされないことがあります。
- 入力パケットが標準転送されないにもかかわらず、SPAN 宛先ポートに着信することがあります。
- スイッチ輻輳が原因で廃棄された出力パケットは、出力 SPAN から廃棄されます。

SPAN の設定によっては、同じ送信元パケットの複数のコピーが SPAN 宛先ポートに送信される場合があります。たとえば、ポート A では RX モニタ用に、ポート B では TX モニタ用に、双方向 (RX と TX) SPAN セッションが設定されているとします。パケットがポート A を介してスイッチに着信し、ポート B にスイッチングされると、着信パケットと発信パケットの両方が宛先ポートに送信されます。このため、(レイヤ 3 書き換えが行われない場合には、) 両方のパケットは同じものになります (レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります)。

送信元ポート

送信元ポート（モニタ対象ポートともいいます）は、ネットワークトラフィック分析のためにモニタするスイッチドポートまたはルーテッドポートです。1つのローカルSPANセッションまたはRSPAN送信元セッションでは、送信元ポートまたはVLANのトラフィックを単一方向または双方向でモニタできます。スイッチは、任意の数の送信元ポート（スイッチで利用可能なポートの最大数まで）と任意の数の送信元VLAN（サポートされているVLANの最大数まで）をサポートします。ただし、スイッチが送信元ポートまたはVLANでサポートするセッション数は最大2つ（ローカルまたはRSPAN）であるため、単一のセッションにポートおよびVLANを混在させることはできません。

送信元ポートには、次の特性があります。

- 複数のSPANセッションでモニタできます。
- 各送信元ポートに、モニタする方向（入力、出力、両方）を設定できます。
- すべてのポートタイプ（EtherChannel、ファストイーサネット、ギガビットイーサネットなど）が可能です。
- EtherChannel送信元の場合はEtherChannel全体で、または物理ポートがポートチャンネルに含まれている場合は物理ポート上で個別に、トラフィックをモニタできます。
- アクセスポート、トランクポート、ルーテッドポート、または音声VLANポートに指定できます。
- 宛先ポートに指定することはできません。
- 送信元ポートは同じVLAN内にあっても異なるVLANにあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニタできます。

送信元VLAN

VLAN-based SPAN（VSPAN）では、1つまたは複数のVLANのネットワークトラフィックをモニタできます。VSPAN内のSPANまたはRSPAN送信元インターフェイスはVLANIDで指定され、トラフィックはそのVLANのすべてのポートでモニタされます。

VSPANには次の特性があります。

- 送信元VLAN内のすべてのアクティブポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。
- 指定されたポートでは、モニタ対象のVLAN上のトラフィックのみが宛先ポートに送信されます。
- 宛先ポートが送信元VLANに所属する場合は、送信元リストから除外され、モニタされません。
- ポートが送信元VLANに追加または削除されると、これらのポートで受信された送信元VLANのトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN送信元と同じセッション内のフィルタVLANを使用することはできません。
- モニタできるのは、イーサネットVLANだけです。

VLANフィルタリング

トランクポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべてのVLANがモニタされます。VLANフィルタリングを使用すれば、トランク送信元ポートでのSPANトラフィックのモニタを特定のVLANに制限できます。

- VLANフィルタリングが適用されるのは、トランクポートまたは音声VLANポートのみです。
- VLANフィルタリングはポートベースセッションにのみ適用され、VLAN送信元によるセッションでは使用できません。

- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセスポートではリスト内の VLAN のみがモニタされます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響しません。

宛先ポート

各ローカル SPAN セッションまたは RSPAN 宛先セッションには、送信元ポートまたは VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザ（通常はネットワーク アナライザ）に送信する宛先ポート（*モニタ側ポート*ともいいます）が必要です。

宛先ポートには、次の特性があります。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じスイッチ スタックに存在している必要があります。RSPAN セッションの場合、宛先ポートは RSPAN 宛先セッションを含むスイッチ上にあります。RSPAN 送信元セッションのみを実行するスイッチまたはスイッチ スタックには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。SPAN 宛先ポートの設定を削除すると、ポートは以前の設定に戻ります。ポートが SPAN 宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。
- EtherChannel グループに含まれていたポートが宛先ポートとして設定されている場合、そのポートはグループから削除されます。削除されたポートがルーテッド ポートであった場合、このポートはルーテッド ポートではなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにすることはできません。
- 送信元ポートに指定することはできません。
- EtherChannel グループまたは VLAN にはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。このポートでは、SPAN セッションに必要なトラフィック以外の転送は行われません。宛先ポートでは着信トラフィックの学習または転送は行われません。
- 入力トラフィックの転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- スイッチ スタックの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートでは、VLAN タギングおよびカプセル化に関する動作が異なります。

- ローカル SPAN では、宛先ポートに **encapsulation replicate** キーワードが指定されている場合、各パケットに元のカプセル化が使用されます（タグなし、ISL、または IEEE 802.1Q）。これらのキーワードが指定されていない場合、パケットはタグなしフォーマットになります。したがって、**encapsulation replicate** がイネーブル化されたローカル SPAN セッションの出力に、タグなし、ISL、または IEEE 802.1Q タグ付きパケットが混在する場合があります。
- RSPAN の場合、元の VLAN ID は RSPAN VLAN ID で上書きされるため、失われます。したがって、宛先ポート上のすべてのパケットはタグなしになります。

RSPAN VLAN

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

- 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 MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。
- RSPAN VLAN は、**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、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN はプライベート VLAN プライマリまたはセカンダリ VLAN にはできません。

VTP に認識される VLAN 1 ~ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。拡張 VLAN 範囲 (1006 ~ 4094) 内の 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。

通常は、ネットワークに複数の RSPAN VLAN を配置し、同時にそれぞれの RSPAN VLAN でネットワーク全体の RSPAN セッションを定義します。つまり、ネットワーク内の任意の場所にある複数の RSPAN 送信元セッションから RSPAN セッションにパケットを送信できます。また、ネットワーク全体に対して複数の RSPAN 宛先セッションを設定し、同じ RSPAN VLAN をモニタしたり、ユーザにトラフィックを送信することもできます。セッションは RSPAN VLAN ID によって区別されます。

SPAN および RSPAN の他の機能との相互作用

SPAN は次の機能と相互作用します。

- ルーティング SPAN はルーティングされたトラフィックをモニタしません。VSPAN がモニタするのはスイッチに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックはモニタしません。たとえば、VLAN が受信モニタされ、スイッチが別の VLAN からモニタ対象 VLAN にトラフィックをルーティングする場合、そのトラフィックはモニタされず、SPAN 宛先ポートで受信されません。
- STP 宛先ポートの SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。送信元ポートでは、SPAN は STP ステータスに影響を与えません。STP は、RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- CDP SPAN 宛先ポートは、SPAN セッションがアクティブな間は CDP に参加しません。SPAN セッションがディセーブルになると、ポートは再び CDP に参加します。
- VTP VTP を使用して、スイッチ間で RSPAN VLAN をブルーニングできます。
- VLAN およびトランキング 送信元ポート、または宛先ポートの VLAN メンバーシップまたはトランクの設定値は、いつでも変更できます。ただし、宛先ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、SPAN 宛先設定を削除しないかぎり有効になりません。送信元ポートの VLAN メンバーシップまたはトランク設定の変更はただちに有効になり、個々の SPAN セッションは、それに応じて自動的に調整されます。
- EtherChannel EtherChannel グループを送信元ポートに設定できますが、SPAN 宛先ポートには設定できません。グループを SPAN 送信元として設定すると、グループ全体がモニタ対象となります。

モニタ対象 EtherChannel グループに物理ポートを追加すると、新しいポートが SPAN 送信元ポート リストに追加されます。モニタ対象 EtherChannel グループからポートを削除すると、SPAN 送信元ポート リストから自動的に削除されます。

EtherChannel グループに属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。ただし、EtherChannel グループに属する物理ポートを SPAN 宛先ポートに設定した場合は、EtherChannel グループから削除されます。SPAN セッションからポートが削除されると、EtherChannel グループに復帰します。EtherChannel グループから削除されたポートはグループのメンバーに残りますが、非アクティブまたはサスペンド状態になります。

EtherChannel グループに属する物理ポートが宛先ポートであり、かつ、EtherChannel グループが送信元である場合、ポートは EtherChannel グループおよびモニタ対象ポートのリストから削除されます。

- マルチキャストトラフィックをモニタできます。出力側および入力側ポートモニタの場合は、未編集パケットが 1 つだけ SPAN 宛先ポートに送信されます。マルチキャストパケットが送信される回数は反映されません。
- プライベート VLAN ポートは SPAN 宛先ポートにはできません。
- セキュアポートは SPAN 宛先ポートにはできません。

SPAN セッションでは、宛先ポートで入力転送がイネーブルの場合、出力をモニタしているポートでポートセキュリティをイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているどのポートでもポートセキュリティをイネーブルにしないでください。

- IEEE 802.1x ポートは SPAN 送信元ポートにできません。SPAN 宛先ポートで IEEE 802.1x をイネーブルにできますが、SPAN 宛先として削除するまでは IEEE 802.1x はディセーブルに設定されます。

SPAN セッションでは、宛先ポートで入力転送がイネーブルの場合、出力をモニタしているポートで IEEE 802.1x をイネーブルにしないでください。RSPAN 送信元セッションでは、出力をモニタしているどのポートでも IEEE 802.1x をイネーブルにしないでください。

SPAN/RSPAN およびスイッチ スタック

スイッチ スタックは 1 つの論理スイッチとして扱われるため、ローカル SPAN 送信元ポートおよび宛先ポートをスタック内の異なるスイッチに設定できます。したがって、スタックにスイッチを追加または削除すると、ローカル SPAN セッションや、RSPAN 送信元または宛先セッションに影響が及ぶことがあります。スタックからスイッチを削除すると、アクティブセッションが非アクティブになることがあります。スタックにスイッチを追加すると、非アクティブセッションがアクティブになることがあります。

スイッチ スタックの詳細については、[第 5 章「スイッチ スタックの管理」](#)を参照してください。

SPAN および RSPAN の設定

ここでは、次の設定について説明します。

- [SPAN および RSPAN のデフォルト設定 \(p.28-11\)](#)
- [ローカル SPAN の設定 \(p.28-11\)](#)
- [RSPAN の設定 \(p.28-18\)](#)

SPAN および RSPAN のデフォルト設定

表 28-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 28-1 SPAN および RSPAN のデフォルト設定

| 機能 | デフォルト設定 |
|-----------------------------|---|
| SPAN のステート (SPAN および RSPAN) | ディセーブル |
| モニタする送信元ポートのトラフィック | 受信トラフィックと送信トラフィックの両方 (both) |
| カプセル化タイプ (宛先ポート) | ネイティブ形式 (タグなしパケット) |
| 入力転送 (宛先ポート) | ディセーブル |
| VLAN フィルタリング | 送信元ポートとして使用されるトランク インターフェイス上で、すべての VLAN がモニタされます。 |
| RSPAN VLAN | 設定なし |

ローカル SPAN の設定

ここでは、次の設定について説明します。

- [SPAN 設定時の注意事項 \(p.28-11\)](#)
- [ローカル SPAN セッションの作成 \(p.28-12\)](#)
- [ローカル SPAN セッションの作成および入力トラフィックの設定 \(p.28-15\)](#)
- [フィルタリングする VLAN の指定 \(p.28-17\)](#)

SPAN 設定時の注意事項

SPAN を設定する場合は、次の注意事項に従ってください。



- 各スイッチ スタックにつき、最大 2 つの送信元セッションおよび 64 の RSPAN 宛先セッションを設定できます。送信元セッションは、ローカル SPAN セッションか RSPAN 送信元セッションのどちらかになります。
- 10 ギガビット イーサネット モジュール ポートが SPAN または RSPAN 宛先ポートとして設定されている場合、リンク速度が低下します。
- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、または一定範囲のポートまたは VLAN のトラフィックをモニタできます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートは送信元ポートにできません。また、送信元ポートは宛先ポートにできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- スイッチ ポートを SPAN 宛先ポートに設定すると、通常のスイッチ ポートではなくなります。SPAN 宛先ポートを通過するのは、モニタ対象のトラフィックだけです。
- SPAN コンフィギュレーション コマンドを入力しても、設定済みの SPAN パラメータは削除されません。設定された SPAN パラメータを削除するには、`no monitor session {session_number | all | local | remote}` グローバル コンフィギュレーション コマンドを入力する必要があります。



- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットには元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）が付加されます。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。RSPAN 宛先ポートの場合、発信パケットはタグなしです。
- ディセーブルに設定されているポートを送信元または宛先ポートにすることはできませんが、SPAN 機能は、宛先ポートおよび 1 つまたは複数の送信元ポートまたは送信元 VLAN がイネーブルになるまでは起動しません。
- filter vlan** キーワードを使用すると、特定の VLAN に対して SPAN トラフィックを制限できます。モニタ対象がトランクポートの場合、このキーワードで指定された VLAN 上のトラフィックのみがモニタされます。デフォルトでは、トランクポートのすべての VLAN がモニタされます。
- 1 つの SPAN セッション内で送信元 VLAN を混在させたり、VLAN をフィルタリングすることはできません。
- Catalyst 3750-24PS、3750-48PS、3750-24TS、3750-48TS、3750G-12S、3750G-24T、3750G-24TS、および 3750G-16TD スイッチには、SPAN に関連するハードウェアの制限があります。ルーティングされたユニキャストトラフィックの出力 SPAN コピーが、ローカルおよびリモート SPAN セッションの両方で間違った宛先 MAC アドレスを示す場合があります。この制限は、ブリッジングされるパケットには適用されません。ローカル SPAN に対する回避策は、レプリケーション オプションを使用することです。
- Catalyst 3750-24PS、3750-48PS、3750-24TS、3750-48TS、3750G-12S、3750G-24T、3750G-24TS、および 3750G-16TD スイッチには、出力 SPAN ルーテッドパケット（ユニキャストおよびマルチキャストの両方）が間違った送信元 MAC アドレスを示します。宛先ポートでネイティブ形式でカプセル化したローカル SPAN パケットの場合、パケットは VLAN 1 の MAC アドレスを示します。カプセル化レプリケーション オプションを使用している場合、ローカル SPAN ではこの問題が発生しません。この制限は、ブリッジングされるパケットには適用されません。回避策は、**monitor session** グローバル コンフィギュレーション コマンドで **encapsulate replicate** キーワードを使用することです。

ローカル SPAN セッションの作成

SPAN セッションを作成し、送信元（モニタ対象）ポートまたは VLAN、および宛先（モニタ側）ポートを指定するには、イネーブル EXEC モードで次の手順を実行します。

| | コマンド | 説明 |
|--------|---|---|
| ステップ 1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | <code>no monitor session {session_number all local remote}</code> | セッションの既存の SPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての SPAN セッションを削除するには all を、すべてのローカルセッションを削除するには local を、すべてのリモート SPAN セッションを削除するには remote を指定します。 |

| コマンド | 説明 |
|---|--|
| ステップ 3 <code>monitor session session_number source</code> <code>{interface interface-id vlan vlan-id} [, -]</code> <code>[both rx tx]</code> | <p>SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。</p> <p><code>session_number</code> の範囲は、1 ~ 66 です。</p> <p><code>interface-id</code> には、モニタする送信元ポートまたは送信元 VLAN を指定します。</p> <ul style="list-style-type: none"> 送信元 <code>interface-id</code> には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャンネル論理インターフェイス（<code>port-channel port-channel-number</code>）があります。有効なポート チャンネル番号は 1 ~ 48 です。 <code>vlan-id</code> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です（RSPAN VLAN は除く）。 <p> (注) 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。</p> <p>(任意) <code>[, -]</code> 一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</p> <p>(任意) モニタするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、SPAN は送受信両方のトラフィックをモニタします。</p> <ul style="list-style-type: none"> <code>both</code> 送受信両方のトラフィックをモニタします。これはデフォルト設定です。 <code>rx</code> 受信トラフィックをモニタします。 <code>tx</code> 送信トラフィックをモニタします。 <p> (注) <code>monitor session session_number source</code> コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p> |

| | コマンド | 説明 |
|--------|--|---|
| ステップ 4 | monitor session <i>session_number</i> destination { interface <i>interface-id</i> [, -] [encapsulation replicate]} | <p>SPAN セッションおよび宛先ポート (モニタ側ポート) を指定します。</p> <p><i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。</p> <p> (注) ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。</p> <p><i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。</p> <p>(任意)[, -] 一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</p> <p>(任意) 宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するように指定するには、encapsulation replicate を入力します。このように選択しない場合、デフォルトでは、パケットがネイティブ形式 (タグなし) で送信されます。</p> <p> (注) monitor session <i>session_number</i> destination コマンドを複数回使用すると、複数の宛先ポートを設定できます。</p> |
| ステップ 5 | end | イネーブル EXEC モードに戻ります。 |
| ステップ 6 | show monitor [session <i>session_number</i>] show running-config | 設定を確認します。 |
| ステップ 7 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

SPAN セッションを削除する場合は、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、**no monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} グローバル コンフィギュレーション コマンドまたは **no monitor session** *session_number* **destination** **interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの **no** 形式では、**encapsulation** オプションは無視されます。

次に、SPAN セッション 1 を設定し、送信元ポートから宛先ポートへのトラフィックをモニタする例を示します。最初に、セッション 1 の既存の SPAN 設定を削除し、双方向トラフィックをスイッチ 1 の送信元ギガビット イーサネット ポート 1 から宛先ギガビット イーサネット ポート 2 へミラーリングして、カプセル化方式を維持します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
Switch(config)# end
```

次に、SPAN セッション 1 の SPAN 送信元である、ポート 1 を削除する例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1
Switch(config)# end
```

次に、双方向モニタ用に設定された、ポート 1 での受信トラフィック モニタをディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

ポート 1 での受信トラフィックのモニタはディセーブルになりますが、このポートから送信されるトラフィックは引き続きモニタされます。

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ~ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックをスイッチ 1 の宛先ギガビットイーサネット ポート 2 に送信する例を示します。VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするように、コンフィギュレーションが変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

ローカル SPAN セッションの作成および入力トラフィックの設定

SPAN セッションを作成して送信元ポート、送信元 VLAN、および宛先ポートを指定し、ネットワーク セキュリティ デバイス (Cisco IDS センサ装置など) 用の宛先ポート上の入力トラフィックをイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。

入力トラフィックに関連しないキーワードの詳細については、「[ローカル SPAN セッションの作成](#)」(p.28-12) を参照してください。

| | コマンド | 説明 |
|--------|---|--|
| ステップ 1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | <code>no monitor session {session_number all local remote}</code> | セッションの既存の SPAN 設定を削除します。 |
| ステップ 3 | <code>monitor session session_number source {interface interface-id vlan vlan-id} [, -] [both rx tx]</code> | SPAN セッションおよび送信元ポート (モニタ対象ポート) を指定します。 |

| | コマンド | 説明 |
|--------|--|--|
| ステップ 4 | <pre>monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [encapsulation replicate] [ingress {dot1q vlan <i>vlan-id</i> isl untagged vlan <i>vlan-id</i> vlan <i>vlan-id</i>}}</pre> | <p>SPAN セッション、宛先ポート、パケット カプセル化、入力側 VLAN、およびカプセル化を指定します。</p> <p><i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。</p> <p><i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。</p> <p>(任意)[, -] 一連のまたは一定範囲のインターフェイスを指定します。カンマまたはハイフンの前後にはスペースを入力しません。</p> <p>(任意) 宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するように指定するには、encapsulation replicate を入力します。このように選択しない場合、デフォルトでは、パケットがネイティブ形式（タグなし）で送信されます。</p> <p>宛先ポートで入力トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、ingress に次のキーワードを指定して入力します。</p> <ul style="list-style-type: none"> dot1q vlan <i>vlan-id</i> IEEE 802.1Q カプセル化を使用し、デフォルト VLAN として指定された VLAN を設定して、入力パケットを受け入れます。 isl ISL カプセル化を使用して、入力パケットを転送します。 untagged vlan <i>vlan-id</i> または vlan <i>vlan-id</i> タグなしカプセル化タイプを使用し、デフォルト VLAN として指定された VLAN を設定して、入力パケットを受け入れます。 |
| ステップ 5 | <code>end</code> | イネーブル EXEC モードに戻ります。 |
| ステップ 6 | <pre>show monitor [session <i>session_number</i>] show running-config</pre> | 設定を確認します。 |
| ステップ 7 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

SPAN セッションを削除する場合は、`no monitor session session_number` グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから送信元ポート、宛先ポート、または VLAN を削除する場合は、`no monitor session session_number source {interface interface-id | vlan vlan-id}` グローバル コンフィギュレーション コマンドまたは `no monitor session session_number destination interface interface-id` グローバル コンフィギュレーション コマンドを使用します。宛先インターフェイスの場合、このコマンドの `no` 形式では、`encapsulation` および `ingress` オプションは無視されます。

次に、SPAN セッション 2 の既存の設定を削除し、ギガビットイーサネット送信元ポート 1 で受信されたトラフィックをモニタするように SPAN セッション 2 を設定し、このトラフィックを送信元ポートと同じ出力カプセル化タイプを使用して宛先ギガビットイーサネットポート 2 に送信し、IEEE 802.1Q カプセル化およびデフォルト入力 VLAN として VLAN 6 を使用する入力転送をイネーブルにする例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2
encapsulation replicate ingress dot1q vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、イネーブル EXEC モードで次の手順を実行します。

| | コマンド | 説明 |
|--------|--|--|
| ステップ 1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | <code>no monitor session {<i>session_number</i> all local remote}</code> | セッションの既存の SPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての SPAN セッションを削除するには <code>all</code> を、すべてのローカルセッションを削除するには <code>local</code> を、すべてのリモート SPAN セッションを削除するには <code>remote</code> を指定します。 |
| ステップ 3 | <code>monitor session <i>session_number</i> source interface <i>interface-id</i></code> | 送信元ポート (モニタ対象ポート) および SPAN セッションの特性を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>interface-id</i> には、モニタする送信元ポートを指定します。指定されたインターフェイスが、トランク ポートとして設定されている必要があります。 |
| ステップ 4 | <code>monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [, -]</code> | SPAN 送信元トラフィックを特定の VLAN に制限します。 <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 <i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。 (任意) カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して一定範囲の VLAN を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 |
| ステップ 5 | <code>monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [encapsulation replicate]}</code> | SPAN セッションおよび宛先ポート (モニタ側ポート) を指定します。 <i>session_number</i> には、ステップ 3 で入力したセッション番号を指定します。 <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。 (任意) [, -] 一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 (任意) 宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するように指定するには、 <code>encapsulation replicate</code> を入力します。このように選択しない場合、デフォルトでは、パケットがネイティブ形式 (タグなし) で送信されます。 |
| ステップ 6 | <code>end</code> | イネーブル EXEC モードに戻ります。 |
| ステップ 7 | <code>show monitor [session <i>session_number</i>]</code> <code>show running-config</code> | 設定を確認します。 |
| ステップ 8 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

トランク ポート上のすべての VLAN をモニタするには、`no monitor session session_number filter` グローバル コンフィギュレーション コマンドを使用します。

次に、SPAN セッション 2 の既存の設定を削除し、ギガビット イーサネット トランク ポート 2 での受信トラフィックをモニタするように SPAN セッション 2 を設定し、VLAN 1 ~ 5 および VLAN 9 のトラフィックのみを宛先ギガビット イーサネット ポート 1 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1
Switch(config)# end
```

RSPAN の設定

ここでは、次の設定について説明します。

- [RSPAN 設定時の注意事項 \(p.28-18\)](#)
- [RSPAN VLAN としての VLAN の設定 \(p.28-19\)](#)
- [RSPAN 送信元セッションの作成 \(p.28-20\)](#)
- [RSPAN 宛先セッションの作成 \(p.28-21\)](#)
- [RSPAN 宛先セッションの作成および入力トラフィックの設定 \(p.28-22\)](#)
- [フィルタリングする VLAN の指定 \(p.28-24\)](#)

RSPAN 設定時の注意事項

RSPAN の設定時は、次の注意事項に従ってください。

- RSPAN には、「[SPAN 設定時の注意事項](#)」(p.28-11) のすべての項目が当てはまります。
- RSPAN VLAN には特殊なプロパティがあるので、RSPAN VLAN として使用する VLAN をネットワーク上にいくつか確保しておき、これらの VLAN にはアクセス ポートを割り当てないでください。
- RSPAN トラフィックに出力 ACL を適用して、特定の packets を選択してフィルタリングまたはモニタできます。これらの ACL は、RSPAN 送信元スイッチ内の RSPAN VLAN 上で指定します。
- RSPAN の設定では、送信元ポートと宛先ポートをネットワーク内の複数のスイッチに分散できます。
- RSPAN は BPDU パケット モニタリングその他のレイヤ 2 スイッチ プロトコルをサポートしません。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生するのを防ぐため、参加しているすべてのスイッチで VLAN リモート SPAN 機能がサポートされていることを確認してください。
- RSPAN VLAN 上のアクセス ポート (音声 VLAN ポートを含む) は、非アクティブ状態になります。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として組み込まれます。また、RSPAN VLAN を SPAN セッションの送信元にすることもできます。ただし、スイッチはセッション間にわたるトラフィックをモニタしないため、スイッチの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパンニングがサポートされません。
- 任意の VLAN を RSPAN VLAN として設定するには、次の条件を満たす必要があります。
 - すべてのスイッチで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
 - 参加するすべてのスイッチが RSPAN をサポートしている。
- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定してください。

- VTP および VTP プルーニングがイネーブルの場合、RSPAN トラフィックはトランクでプルーニングされ、ネットワーク上で VLAN ID が 1005 以下の RSPAN トラフィックの無用なフラグディングを防止できます。
- Catalyst 3750-24PS、3750-48PS、3750-24TS、3750-48TS、3750G-12S、3750G-24T、3750G-24TS、および 3750G-16TD スイッチには、RSPAN に関連するハードウェアの制限があります。
 - ルーティングされたユニキャストトラフィックの出力 SPAN コピーが、ローカルおよびリモート SPAN セッションの両方で間違った宛先 MAC アドレスを示す場合があります。この制限は、ブリッジングされるパケットには適用されません。ローカル SPAN に対する回避策は、レプリケーション オプションを使用することです。リモート SPAN セッションの場合、回避策はありません。
 - 出力 SPAN ルーテッドパケット（ユニキャストおよびマルチキャスト）が間違った送信元 MAC アドレスを示します。リモート SPAN パケットの場合、送信元 MAC アドレスは出力 VLAN の MAC アドレスでなければならないにもかかわらず、パケットは RSPAN VLAN の MAC アドレスを示します。これには回避策はありません。
 - トラフィックのアクセス量が非常に多くなる間、2 つの RSPAN 送信元セッションが設定される場合、一方の RSPAN セッションにあるパケットの VLAN ID でもう一方の RSPAN の VLAN ID が上書きされる可能性があります。これが発生した場合、一方の RSPAN VLAN 向けのパケットがもう一方の RSPAN VLAN に間違っって送信されてしまいます。この問題は RSPAN 宛先セッションには影響しません。回避策は、RSPAN 送信元セッションを 1 つのみ設定することです。

RSPAN VLAN としての VLAN の設定

最初に、RSPAN セッション用の RSPAN VLAN に設定する VLAN を新規に作成します。RSPAN に参加するすべてのスイッチに RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲（1005 以下）であり、VTP がネットワーク内でイネーブルである場合は、1 つのスイッチに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のスイッチに伝播するように設定できます。拡張範囲 VLAN（1005 を超える ID）の場合、送信元と宛先の両方のスイッチ、およびすべての中間スイッチに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックのフローを効率化するか、または RSPAN トラフィックを伝達する必要のないすべてのトランクから、RSPAN VLAN を手動で削除してください。

RSPAN VLAN を作成するには、イネーブル EXEC モードで次の手順を実行します。

| | コマンド | 説明 |
|--------|---|---|
| ステップ 1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | <code>vlan vlan-id</code> | VLAN ID を入力して VLAN を作成するか、または既存の VLAN の VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 2 ~ 1001、および 1006 ~ 4094 です。 RSPAN VLAN を VLAN 1 (デフォルト VLAN) または VLAN ID 1002 ~ 1005 (トークンリングや FDDI VLAN 専用) にすることはできません。 |
| ステップ 3 | <code>remote-span</code> | VLAN を RSPAN VLAN として設定します。 |
| ステップ 4 | <code>end</code> | イネーブル EXEC モードに戻ります。 |
| ステップ 5 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

VLAN から RSPAN の特性を削除して、標準 VLAN に変換するには、`no remote-span` VLAN コンフィギュレーション コマンドを使用します。

次に、RSPAN VLAN 901 を作成する例を示します。

```
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを開始し、モニタ対象の送信元および宛先 RSPAN VLAN を指定するには、イネーブル EXEC モードで次の手順を実行します。

| | コマンド | 説明 |
|--------|---|---|
| ステップ 1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | <code>no monitor session {session_number all local remote}</code> | セッションの既存の RSPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての RSPAN セッションを削除するには <code>all</code> を、すべてのローカルセッションを削除するには <code>local</code> を、すべてのリモート SPAN セッションを削除するには <code>remote</code> を指定します。 |
| ステップ 3 | <code>monitor session session_number source {interface interface-id vlan vlan-id} [, -] [both rx tx]</code> | RSPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 RSPAN セッションの送信ポートまたは送信元 VLAN を入力します。 <ul style="list-style-type: none"> <i>interface-id</i> には、モニタする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポートチャネル論理インターフェイス（<code>port-channel port-channel-number</code>）があります。有効なポートチャネル番号は 1 ~ 48 です。 <i>vlan-id</i> には、モニタする送信元 VLAN を指定します。指定できる範囲は 1 ~ 4094 です（RSPAN VLAN は除く）。 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内で送信元ポートと送信元 VLAN を併用することはできません。 (任意) [, -] 一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 (任意) モニタするトラフィックの方向を指定します。トラフィックの方向を指定しない場合、送信元インターフェイスは、送受信両方のトラフィックを送信します。 <ul style="list-style-type: none"> <code>both</code> 送受信両方のトラフィックを送信します。 <code>rx</code> 受信トラフィックをモニタします。 <code>tx</code> 送信トラフィックをモニタします。 |
| ステップ 4 | <code>monitor session session_number destination remote vlan vlan-id</code> | RSPAN セッションおよび宛先 RSPAN VLAN を指定します。 <i>session_number</i> には、ステップ 3 で定義した番号を入力します。 <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。 |

| | コマンド | 説明 |
|--------|--|---------------------------------|
| ステップ 5 | end | イネーブル EXEC モードに戻ります。 |
| ステップ 6 | show monitor [session session_number] show running-config | 設定を確認します。 |
| ステップ 7 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

SPAN セッションを削除する場合は、**no monitor session session_number** グローバル コンフィギュレーション コマンドを使用します。

SPAN セッションから送信元ポートまたは VLAN を削除するには、**no monitor session session_number source {interface interface-id | vlan vlan-id}** グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、**no monitor session session_number destination remote vlan vlan-id** コマンドを使用します。

次に、セッション 1 の既存の RSPAN 設定を削除し、複数の送信元インターフェイスをモニタするように RSPAN セッション 1 を設定し、さらに宛先を RSPAN VLAN 901 に設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 1 source interface port-channel 2
Switch(config)# monitor session 1 destination remote vlan 901
Switch(config)# end
```

RSPAN 宛先セッションの作成

RSPAN 宛先セッションは別のスイッチまたはスイッチ スタック（送信元セッションが設定されていないスイッチまたはスイッチ スタック）に設定します。

スイッチ上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、イネーブル EXEC モードで次の手順を実行します。

| | コマンド | 説明 |
|--------|--|--|
| ステップ 1 | configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | vlan vlan-id | 送信元スイッチで作成された RSPAN VLAN の VLAN ID を入力し、VLAN コンフィギュレーション モードを開始します。 両方のスイッチが VTP に参加し、RSPAN VLAN ID が 2 ~ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 2 ~ 4 は不要です。 |
| ステップ 3 | remote-span | VLAN を RSPAN VLAN として識別します。 |
| ステップ 4 | exit | グローバル コンフィギュレーション モードに戻ります。 |
| ステップ 5 | no monitor session {session_number all local remote} | セッションの既存の RSPAN 設定を削除します。 session_number の範囲は、1 ~ 66 です。 すべての RSPAN セッションを削除するには all を、すべてのローカルセッションを削除するには local を、すべてのリモート SPAN セッションを削除するには remote を指定します。 |
| ステップ 6 | monitor session session_number source remote vlan vlan-id | RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 session_number の範囲は、1 ~ 66 です。 vlan-id には、モニタする送信元 RSPAN VLAN を指定します。 |

■ SPAN および RSPAN の設定

| | コマンド | 説明 |
|---------|--|---|
| ステップ 7 | <code>monitor session <i>session_number</i> destination interface <i>interface-id</i></code> | RSPAN セッションおよび宛先インターフェイスを指定します。 <i>session_number</i> には、ステップ 6 で定義した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 <i>interface-id</i> には、宛先インターフェイスを指定します。宛先インターフェイスには物理インターフェイスを指定する必要があります。 <code>encapsulation replicate</code> はコマンドラインのヘルプ スtring に表示されていますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしとして表示されます。 |
| ステップ 8 | <code>end</code> | イネーブル EXEC モードに戻ります。 |
| ステップ 9 | <code>show monitor [session <i>session_number</i>] show running-config</code> | 設定を確認します。 |
| ステップ 10 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

SPAN セッションを削除する場合は、`no monitor session session_number` グローバル コンフィギュレーション コマンドを使用します。SPAN セッションから宛先ポートを削除するには、`no monitor session session_number destination interface interface-id` グローバル コンフィギュレーション コマンドを使用します。セッションから RSPAN VLAN を削除するには、`no monitor session session_number source remote vlan vlan-id` コマンドを使用します。

次に、送信元リモート VLAN として VLAN 901、宛先インターフェイスとしてポート 1 を設定する例を示します。

```
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1
Switch(config)# end
```

RSPAN 宛先セッションの作成および入力トラフィックの設定

RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定し、ネットワーク セキュリティ デバイス (Cisco IDS センサ装置など) 用の宛先ポート上の入力トラフィックをイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。

入力トラフィックに関連しないキーワードの詳細については、「[RSPAN 宛先セッションの作成](#)」(p.28-21) を参照してください。この手順では、RSPAN VLAN がすでに設定してあると想定しています。

| | コマンド | 説明 |
|--------|--|--|
| ステップ 1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | <code>no monitor session {<i>session_number</i> all local remote}</code> | セッションの既存の SPAN 設定を削除します。 |
| ステップ 3 | <code>monitor session <i>session_number</i> source remote vlan <i>vlan-id</i></code> | RSPAN セッションおよび送信元 RSPAN VLAN を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。 |

| | コマンド | 説明 |
|--------|--|---|
| ステップ 4 | monitor session <i>session_number</i> destination { interface <i>interface-id</i> [, -] [ingress { dot1q vlan <i>vlan-id</i> isl untagged vlan <i>vlan-id</i> vlan <i>vlan-id</i> }]} | SPAN セッション、宛先ポート、パケット カプセル化、入力側 VLAN、およびカプセル化を指定します。 <i>session_number</i> には、ステップ 4 で定義した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 <i>interface-id</i> には、宛先インターフェイスを指定します。宛先インターフェイスには物理インターフェイスを指定する必要があります。 encapsulation replicate はコマンドラインのヘルプ スtring に表示されていますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしとして表示されます。 (任意)[, -] 一連のまたは一定範囲のインターフェイスを指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 宛先ポートで入力トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、 ingress と追加のキーワードを入力します。 <ul style="list-style-type: none"> • dot1q vlan <i>vlan-id</i> IEEE 802.1Q カプセル化を使用し、デフォルト VLAN として指定された VLAN を設定して、入力パケットを転送します。 • isl ISL カプセル化を使用して、入力パケットを転送します。 • untagged vlan <i>vlan-id</i> または vlan <i>vlan-id</i> タグなしカプセル化タイプを使用し、デフォルト VLAN として指定された VLAN を設定して、入力パケットを転送します。 |
| ステップ 5 | end | イネーブル EXEC モードに戻ります。 |
| ステップ 6 | show monitor [session <i>session_number</i>] show running-config | 設定を確認します。 |
| ステップ 7 | copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

RSPAN セッションを削除する場合は、**no monitor session** *session_number* グローバル コンフィギュレーション コマンドを使用します。RSPAN セッションから宛先ポートを削除するには、**no monitor session** *session_number* **destination interface** *interface-id* グローバル コンフィギュレーション コマンドを使用します。このコマンドの **no** 形式では、**ingress** オプションは無視されます。

次に、VLAN 901 を RSPAN セッション 2 の送信元リモート VLAN として設定し、ギガビットイーサネット送信元ポート 2 を宛先インターフェイスとして設定し、VLAN 6 がデフォルト入力 VLAN として設定されたインターフェイス上で入力トラフィックの転送をイネーブルにする例を示します。

```
Switch(config)# monitor session 2 source remote vlan 901
Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
vlan 6
Switch(config)# end
```

フィルタリングする VLAN の指定

RSPAN 送信元トラフィックを特定の VLAN に制限するように RSPAN 送信元セッションを設定するには、イネーブル EXEC モードで次の手順を実行します。

| | コマンド | 説明 |
|--------|--|---|
| ステップ 1 | <code>configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 2 | <code>no monitor session {session_number all local remote}</code> | セッションの既存の SPAN 設定を削除します。 <i>session_number</i> の範囲は、1 ~ 66 です。 すべての SPAN セッションを削除するには all を、すべてのローカルセッションを削除するには local を、すべてのリモート SPAN セッションを削除するには remote を指定します。 |
| ステップ 3 | <code>monitor session session_number source interface interface-id</code> | 送信元ポート (モニタ対象ポート) および SPAN セッションの特性を指定します。 <i>session_number</i> の範囲は、1 ~ 66 です。 <i>interface-id</i> には、モニタする送信元ポートを指定します。指定されたインターフェイスが、トランク ポートとして設定されている必要があります。 |
| ステップ 4 | <code>monitor session session_number filter vlan vlan-id [, -]</code> | SPAN 送信元トラフィックを特定の VLAN に制限します。 <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 <i>vlan-id</i> に指定できる範囲は、1 ~ 4094 です。 (任意) カンマ (,) を使用して一連の VLAN を指定するか、ハイフン (-) を使用して一定範囲の VLAN を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 |
| ステップ 5 | <code>monitor session session_number destination remote vlan vlan-id</code> | RSPAN セッションおよび宛先リモート VLAN (RSPAN VLAN) を指定します。 <i>session_number</i> には、ステップ 3 で指定したセッション番号を入力します。 <i>vlan-id</i> には、モニタ対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。 |
| ステップ 6 | <code>end</code> | イネーブル EXEC モードに戻ります。 |
| ステップ 7 | <code>show monitor [session session_number]</code> <code>show running-config</code> | 設定を確認します。 |
| ステップ 8 | <code>copy running-config startup-config</code> | (任意) コンフィギュレーション ファイルに設定を保存します。 |

トランク ポート上のすべての VLAN をモニタするには、`no monitor session session_number filter vlan` グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 での受信トラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ~ 5 および 9 のトラフィックのみを宛先 RSPAN VLAN 902 に送信する例を示します。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

SPAN および RSPAN ステータスの表示

現在の SPAN または RSPAN 設定を表示するには、`show monitor` ユーザ EXEC コマンドを使用します。`show running-config` イネーブル EXEC コマンドを使用すれば、設定された SPAN セッションまたは RSPAN セッションを表示することもできます。

