



SPAN および RSPAN の設定

- [SPAN および RSPAN の前提条件](#) (1 ページ)
- [SPAN および RSPAN の制約事項](#) (1 ページ)
- [SPAN および RSPAN について](#) (4 ページ)
- [SPAN および RSPAN の設定方法](#) (16 ページ)
- [SPAN および RSPAN 動作のモニタリング](#) (42 ページ)
- [SPAN および RSPAN の設定例](#) (42 ページ)
- [SPAN および RSPAN の機能の履歴と情報](#) (45 ページ)

SPAN および RSPAN の前提条件

SPAN

- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランク ポートをモニターしている場合、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ーされます。デフォルトでは、トランクポート上のすべての VLAN がモニターされます。

RSPAN

- 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することを推奨します。

SPAN および RSPAN の制約事項

SPAN

SPAN の制約事項は次のとおりです。

- 各デバイスで 66 のセッションを設定できます。最大 8 つの送信元セッションを設定できます。残りのセッションは、RSPAN 宛先セッションとして設定できます。送信元セッショ

ンは、ローカル SPAN セッションまたは RSPAN 送信元セッションのどちらかになります。

- 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、一定範囲のポートまたは VLAN のトラフィックを監視できます。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。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 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。
- デバイスポートを SPAN 宛先ポートとして設定すると、通常のデバイスポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象トラフィックのみになります。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている 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は元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）を伝送します。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。
- 無効のポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも1つの送信元ポートまたは送信元 VLAN が有効になってからです。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。

SPAN セッションのトラフィック監視には次の制約事項があります。

- 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。
- Wireshark は、出力スパンがアクティブな場合は出力パケットをキャプチャしません。
- 同じデバイスまたはデバイススタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。デバイスまたはデバイススタックは、合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを2つ個別に設定できます。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。
- 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つのデバイススタックあたりに設定できる宛先ポートは最大で 64 個です。

- SPAN セッションがデバイスの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをトラフィック監視するなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN が有効の場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。多数のポートまたは VLAN を監視すると、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。
- ディゼーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- デバイスは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
 - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
 - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
 - 同じデバイスまたはデバイススタック上で、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できません。
- デバイスで DHCP スヌーピングが有効になっている場合、SPAN セッションは Dynamic Host Configuration Protocol (DHCP) 入力パケットのみをキャプチャします。

RSPAN

RSPAN の制約事項は次のとおりです。

- RSPAN は、BPDU パケットモニタリングまたは他のレイヤ 2 デバイス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 に発生しないようにするために、参加しているすべてのデバイスで VLAN RSPAN 機能がサポートされていることを確認してください。
- 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含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、デバイスはスパンされたトラフィックを監視しないため、デバイスの 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。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがプルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラグディングが防止されます。
- RSPAN VLAN をネイティブ VLAN として設定しないことをお勧めします。

SPAN および RSPAN について

SPAN および RSPAN

ポートまたは VLAN を通過するネットワーク トラフィックを解析するには、SPAN または RSPAN を使用して、その device 上、またはネットワーク アナライザやその他のモニター デバイス、あるいはセキュリティ デバイスに接続されている別の device 上のポートにトラフィックのコピーを送信します。SPAN は送信元ポート上または送信元 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、解析します。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は影響しません。宛先ポートは 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、宛先ポートがトラフィックを受信したり転送したりすることはありません。

SPAN を使用してモニターできるのは、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 に出入り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たトラフィックはモニターできません。たとえば、着信トラフィックをモニターしている場合、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ーできません。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、モニターできます。

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注入する場合、SPAN または RSPAN 宛先ポートを使用できます。たとえば、Cisco 侵入検知システム (IDS) センサー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 セッションを停止させることができます。

ローカル SPAN

ローカル SPAN は 1 つの device 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 device または device 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からのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。

図 1: 単一デバイスでのローカル SPAN の設定例

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 に物理的には接続されていま

せんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。

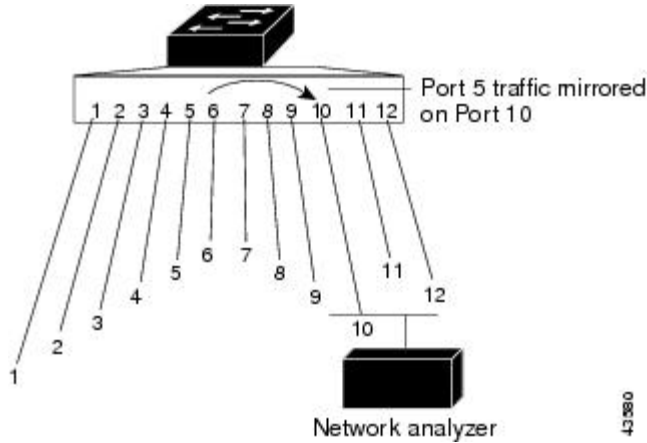
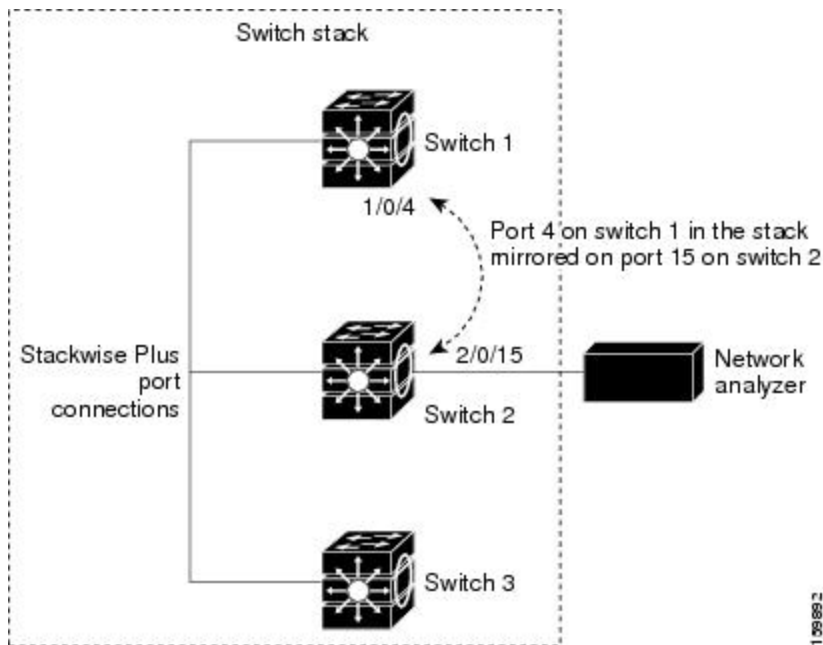


図 2: デバイス スタックでのローカル SPAN の設定例

これは、device スタック内のローカル SPAN の例です。送信元ポートと宛先ポートは異なるスタック メンバにあります。



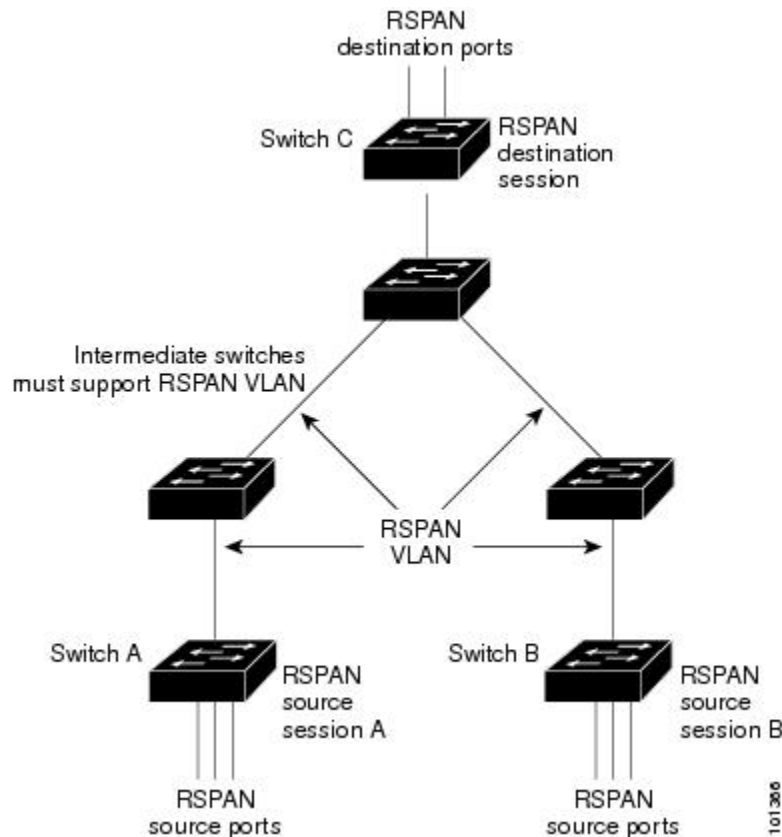
リモート SPAN

RSPAN は、異なる devices (または異なる device 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ているため、ネットワーク上で複数の devices をリモート監視できます。

図 3: RSPAN の設定例

下の図に デバイス A と デバイス 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、ユーザーが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、

参加しているすべての devices の 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 を監視する宛先セッションに転送されます。各 RSPAN 送信元 device には、ポートまたは VLAN のいずれかが RSPAN 送信元として必要です。図中のデバイス C のように、宛先は常に物理ポートになります。



SPAN と RSPAN の概念および用語

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上、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ーし、そのモニター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）を結び付けたものです。ローカル SPAN には、個別の送信元および宛先のセッションはありません。ローカル SPAN セッションはユーザーが指定した入力および出力の packets 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 は少なくとも1つの RSPAN 送信元セッション、1つの RSPAN VLAN、および少なくとも1つの RSPAN 宛先セッションで構成されています。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、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。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 に関連付けます。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が転送される点を除き、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 device 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を取得し、VLAN のタグングを除去し、宛先ポートに送ります。セッションは、(レイヤ2制御パケットを除く)すべての RSPAN VLAN パケットのコピーを分析のためにユーザーに提供します。

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

- ポートまたは VLAN を送信元にはできますが、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。
- 同じ device または device スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。device または device スタックは、合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。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。
- 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 device スタックあたりに設定できる宛先ポートは最大で 64 個です。
- SPAN セッションが device の通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをトラフィック監視するなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN が有効の場合、監視中の各パケットは 2 回送信されます (1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして)。したがって、多数のポートまたは VLAN をモニターすると、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。
- ディゼーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- device は、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
 - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
 - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
 - 同じ device または device 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 タイプを監視できます。

- 受信 (Rx) SPAN : 受信 (または入力) SPAN は、device 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だけ多くモニターリングします。送信元が受信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。

Diffserv コードポイント (DSCP) の変更など、ルーティングや Quality of Service (QoS) が原因で変更されたパケットは、変更される前にコピーされます。

受信処理中にパケットをドロップする可能性のある機能は、入力 SPAN には影響を与えません。宛先ポートは、実際の着信パケットがドロップされた場合でも、パケットのコピーを受信します。パケットをドロップする可能性のある機能は、標準および拡張 IP 入力アクセスコントロールリスト (ACL)、入力 QoS ポリシング、VLAN ACL、および出力 QoS ポリシングです。

- 送信 (Tx) SPAN : 送信 (または出力) SPAN は、device 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限り多くモニターリングします。送信元が送信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。コピーはパケットの変更後に用意されます。

ルーティングが原因で変更されたパケット (存続可能時間 (TTL)、MAC 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ドロップする可能性のある機能は、SPAN 用の複製コピーにも影響します。これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

- 両方 : SPAN セッションで、受信パケットと送信パケットの両方について、ポートまたは VLAN をモニターすることもできます。これはデフォルトです。

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。ただし、宛先ポートを設定する際に **encapsulation replicate** キーワードを入力すると、次の変更が発生します。

- 送信元ポートと同じカプセル化設定 (タグなし、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ーされます。

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

デバイスの輻輳により、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ドロップされることがあります。一般に、これらの特性は互いに無関係です。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。
- deviceの輻輳が原因でドロップされた出力パケットは、出力 SPAN からドロップされません。

SPAN の設定によっては、同一送信元のパケットのコピーが複数、SPAN 宛先ポートに送信されます。たとえば、ポート A での RX モニター用とポート B での TX モニター用に双方向 (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 から device に入ってポート B にスイッチされると、着信パケットも発信パケットも宛先ポートに送信されます。このため、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 (別名モニター側ポート) は、ネットワークトラフィック分析のために監視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ーできます。

デバイスは、任意の数の送信元ポート (デバイス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) をサポートしています。

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。

送信元ポートの特性は、次のとおりです。

- 複数の SPAN セッションでモニターできます。
- モニターする方向 (入力、出力、または両方) を指定して、各送信元ポートを設定できます。
- すべてのポートタイプ (EtherChannel、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ーできます。
- 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。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN 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ーすることが可能です。

送信元 VLAN

VLAN ベースの 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ーできます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスが VLAN ID となり、トラフィックはその VLAN のすべてのポートでモニターされます。

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ーできます。
- 指定されたポートでは、モニター対象の 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、モニターされません。
- 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、モニター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。
- モニターできるのは、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ーする場合、デフォルトでは、トランク上でアクティブなすべての VLAN がモニターされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニター対象を特定の 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該当 VLAN のみがモニターされます。
- 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を与えません。

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、送信元ポートおよび VLAN からのトラフィックのコピーを受信し、SPAN パケットをユーザー（通常はネットワークアナライザ）に送信する宛先ポート（別名モニター側ポート）が必要です。

宛先ポートの特性は、次のとおりです。

- 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deviceまたはdevice スタックに存在している必要があります。RSPAN セッションの場合は、RSPAN 宛先セッションを含むdevice上にあります。RSPAN 送信元セッションのみを実行するdeviceまたはdevice 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。
- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、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。
- 送信元ポートにすることはできません。
- 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。ポートは SPAN セッションに必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック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、モニターされません。
- deviceまたはdevice 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 宛先ポートは、VLAN タギングおよびカプセル化で次のように動作が異なります。

- 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** がイネーブルになっているローカル 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ことがあります。
- RSPAN の場合は、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 の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 を、プライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VLAN トランッキング プロトコル (VTP) に対して可視である 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 devices 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、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 送信元セッションで、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したりできます。セッションは RSPAN VLAN ID によって区別されます。

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッドトラフィックを監視しません。VSPAN が監視するのは device 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監視しません。たとえば、VLAN が受信モニタされ、device が別の VLAN から監視対象 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監視されず、SPAN 宛先ポートで受信されません。
- STP：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 セッションが無効になると、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 セッションがアクティブな間、SPAN 宛先ポートは 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 を使用すると、devices 間で RSPAN VLAN のプルーニングが可能です。

- 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 トランクの設定値を、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が有効になるのは、SPAN 宛先設定を削除してからです。送信元ポートの 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、ただちに有効になり、対応する SPAN セッションが変更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として設定することができます。グループが SPAN 送信元として設定されている場合、グループ全体が監視されます。

監視対象の EtherChannel グループに物理ポートを追加すると、SPAN 送信元ポートリストに新しいポートが追加されます。監視対象の EtherChannel グループからポートを削除すると、送信元ポートリストからそのポートが自動的に削除されます。

EtherChannel グループに所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監視されます。ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。EtherChannel グループから削除されたポートは、グループメンバのままですが、inactive または suspended ステートになります。

EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートは EtherChannel グループおよび監視対象ポート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監視できます。出力ポートおよび入力ポートの監視では、未編集の packets 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 packets の送信回数は反映されません。
- プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。
- セキュア ポートを SPAN 宛先ポートにすることはできません。

SPAN セッションでは、入力転送が宛先ポートで有効の場合、出力を監視しているポートでポートセキュリティを有効にしないでください。RSPAN 送信元セッションでは、出力を監視しているポートでポートセキュリティを有効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す。SPAN 宛先ポート上で IEEE 802.1x を有効にできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x は無効に設定されます。

SPAN セッションでは、入力転送が宛先ポートで有効の場合、出力を監視しているポートで IEEE 802.1x を有効にしないでください。RSPAN 送信元セッションでは、出力を監視しているポートで IEEE 802.1x を有効にしないでください。

SPAN と RSPAN とデバイス スタック

devices のスタックは 1 つの論理 device を表すため、ローカル SPAN の送信元ポートおよび宛先ポートは、スタック内の異なる devices である場合があります。したがって、スタック内の

devicesの追加または削除は、RSPANの送信元セッションまたは宛先セッションだけではなく、ローカル SPAN セッションにも影響を及ぼします。deviceがスタックから削除されると、アクティブセッションが非アクティブになります。また、deviceがスタックに追加されると、非アクティブセッションがアクティブになります。

フローベースの SPAN

送信元ポートで監視されるトラフィックにアクセスコントロールリスト（ACL）を適用するフローベース SPAN（FSPAN）またはフローベース RSPAN（FRSPAN）を使用して、SPAN または RSPAN で監視するネットワークトラフィックのタイプを制御できます。FSPAN ACL は、IPv4、IPv6、および監視される非 IP トラフィックをフィルタリングするように設定できます。

インターフェイスを通して ACL を SPAN セッションに適用します。ACL は SPAN セッション内のすべてのインターフェイスで監視されるすべてのトラフィックに適用されます。この ACL によって許可されるパケットは、SPAN 宛先ポートにコピーされます。ほかのパケットは SPAN 宛先ポートにコピーされません。

元のトラフィックは継続して転送され、接続している任意のポート、VLAN、およびルータ ACL が適用されます。FSPAN ACL は転送の決定に影響を与えることはありません。同様に、ポート、VLAN、およびルータ ACL は、トラフィックのモニタリングに影響を与えません。セキュリティ入力 ACL がパケットを拒否したために転送されない場合でも、FSPAN ACL が許可すると、パケットは SPAN 宛先ポートにコピーされます。しかし、セキュリティ出力 ACL がパケットを拒否したために転送されない場合、パケットは SPAN 宛先ポートにコピーされません。ただし、セキュリティ出力 ACL がパケットの送信を許可した場合だけ、パケットは、FSPAN ACL が許可した場合 SPAN 宛先ポートにコピーされます。これは RSPAN セッションについてもあてはまります。

SPAN セッションには、次の 3 つのタイプの FSPAN ACL を接続できます。

- IPv4 FSPAN ACL : IPv4 パケットだけをフィルタリングします。
- IPv6 FSPAN ACL : IPv6 パケットだけをフィルタリングします。
- MAC FSPAN ACL : IP パケットだけをフィルタリングします。

スタックに設定された VLAN ベースの FSPAN セッションが 1 つまたは複数のデバイス上のハードウェアメモリに収まらない場合、セッションはこれらのデバイス上でアンロードされたものとして処理され、デバイスでの FSPAN ACL およびソーシングのためのトラフィックは、SPAN 宛先ポートにコピーされません。FSPAN ACL は継続して正しく適用され、トラフィックは FSPAN ACL がハードウェアメモリに収まるデバイスの SPAN 宛先ポートにコピーされます。

空の FSPAN ACL が接続されると、一部のハードウェア機能により、その ACL の SPAN 宛先ポートにすべてのトラフィックがコピーされます。十分なハードウェアリソースが使用できない場合、空の FSPAN ACL もアンロードされる可能性があります。

SPAN および RSPAN のデフォルト設定

表 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 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は、すべての VLAN がモニタリングされます。
RSPAN VLAN	未設定

設定時の注意事項

SPAN 設定時の注意事項

- 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** 形式を使用すると、**encapsulation** オプションは無視されます。
- トランクポート上のすべての VLAN をモニターするには、**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。

RSPAN 設定時の注意事項

- すべての SPAN 設定時の注意事項が RSPAN に適用されます。
- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定の packets を選択的にフィルタリングまたはモニターできます。RSPAN 送信元 devices 内の RSPAN VLAN 上で、これらの ACL を指定します。

- RSPAN を設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数の devices に分散させることができます。
- RSPAN VLAN 上のアクセスポート（音声 VLAN ポートを含む）は、非アクティブステートになります。
- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
 - すべての devices で、RSPAN セッションに同じ RSPAN VLAN が使用されている。
 - 参加しているすべての devices で RSPAN がサポートされている。

SPAN および FRSPAN 設定時の注意事項

- 少なくとも 1 つの FSPAN ACL が接続されている場合、FSPAN はイネーブルになります。
- SPAN セッションに空ではない FSPAN ACL を少なくとも 1 つ接続し、ほかの 1 つまたは複数の FSPAN ACL を接続しなかった場合（たとえば、空ではない IPv4 ACL を接続し、IPv6 と MAC ACL を接続しなかった場合）、FSPAN は、接続されていない ACL によってフィルタリングされたと思われるトラフィックをブロックします。したがって、このトラフィックは監視されません。

SPAN および RSPAN の設定方法

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（監視対象）ポートまたは VLAN、および宛先（監視側）ポートを指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** { **interface** *interface-id* | **vlan** *vlan-id* } [, | -] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination** { **interface** *interface-id* [, | -] [**encapsulation** {**replicate** | **dot1q**}] }
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： Device# 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 3	no monitor session {session_number all local remote} 例： Device (config)# no monitor session all	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> session_number の範囲は、1 ～ 66 です。 all : すべての SPAN セッションを削除します。 local : すべてのローカルセッションを削除します。 remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session session_number source { interface interface-id vlan vlan-id } [, -] [both rx tx] 例： Device (config)# monitor session 1 source interface gigabitethernet1/0/1	SPAN セッションおよび送信元ポート（モニター対象ポート）を指定します。 <ul style="list-style-type: none"> session_number の範囲は、1 ～ 66 です。 interface-id には、モニタリング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（port-channel port-channel-number）があります。有効なポートチャネル番号は 1 ～ 48 です。 vlan-id には、監視する送信元 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は送信元ポートと送信元VLANを併用できません。</p>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) <code>[, -]</code>には、一連のインターフェイスまたはインターフェイスの範囲を指定します。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) both rx tx : 監視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かった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 <ul style="list-style-type: none"> • both : 受信トラフィックと送信トラフィックの両方を監視します。 • rx : 受信トラフィックをモニターします。 • tx : 送信トラフィックをモニターします。 <p>(注) monitor session <i>session_number</i>source 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>
ステップ 5	monitor session <i>session_number</i> destination { interface <i>interface-id</i> [, -] [encapsulation { replicate dot1q }] } 例 : <pre>Device(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate</pre>	SPANセッションおよび宛先ポート（モニター側ポート）を指定します。設定変更が有効になると、ポートのLEDがオレンジ色に変わります。LEDはSPAN宛先の設定を削除した後にのみ、元の状態（緑色）に戻ります。 (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。 <ul style="list-style-type: none"> • <i>session_number</i>には、ステップ4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) <code>[, -]</code>には、一連のインターフェイスまたはインターフェイスの範囲を指定します。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。

	コマンドまたはアクション	目的
		<p>(任意) encapsulation replicate には、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ことを指定します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。</p> <p>(任意) encapsulation dot1q は宛先インターフェイスが IEEE 802.1Q カプセル化の送信元インターフェイスの着信パケットを受け入れるように指定します。</p> <p>(注) monitor session session_number destination 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>
ステップ 6	end 例 : Device(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : Device# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例 : Device# 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。

ローカル SPAN セッションの作成および着信トラフィックの設定

SPAN セッションを作成し、さらに送信元ポートまたは VLAN および宛先ポートを指定した後、宛先ポートでネットワークセキュリティデバイス (Cisco IDS センサー装置等) 用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** { **interface** *interface-id* / **vlan** *vlan-id* } [, | -] [**both** | **rx** | **tx**]

5. **monitor session** *session_number* **destination** { **interface** *interface-id* [, | -] [**encapsulation** **replicate**[**ingress** { **dot1q** **vlan** *vlan-id* | **untagged** **vlan** *vlan-id* | **vlan** *vlan-id*]}]}
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： デバイス# 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 3	no monitor session { <i>session_number</i> all local remote } 例： デバイス (config)# no monitor session all	セッションに対する既存の SPAN 設定を削除します。 • <i>session_number</i> の範囲は、1 ~ 4 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session <i>session_number</i> source { interface <i>interface-id</i> vlan <i>vlan-id</i> } [, -] [both rx tx] 例： デバイス (config)# monitor session 2 source gigabitethernet0/1 rx	SPANセッションおよび送信元ポート（監視対象ポート）を指定します。
ステップ 5	monitor session <i>session_number</i> destination { interface <i>interface-id</i> [, -] [encapsulation replicate [ingress { dot1q vlan <i>vlan-id</i> 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、および入力VLANとカプセル化を指定します。 • <i>session_number</i> には、ステップ4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

	コマンドまたはアクション	目的
		<p>必要があります。EtherChannel や VLAN は指定できません。</p> <ul style="list-style-type: none"> • (任意) <code>[, -]</code> : 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマまたはハイフンの前後にスペースを1つずつ入力します。 • (任意) encapsulation replicate : 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ことを指定します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。 • ingress : 宛先ポートでの着信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します。 <ul style="list-style-type: none"> • dot1q vlan vlan-id : デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受け入れます。 • untagged vlan vlan-id または vlan vlan-id : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受け入れます。
ステップ 6	end 例 : デバイス (config) # end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : デバイス # show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例 : デバイス # 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。

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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source interface** *interface-id*
5. **monitor session** *session_number* **filter vlan** *vlan-id* [, | -]
6. **monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**]}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： デバイス# 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 3	no monitor session { <i>session_number</i> all local remote } 例： デバイス(config)# no monitor session all	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session <i>session_number</i> source interface <i>interface-id</i> 例：	送信元ポート（モニター対象ポート）と SPAN セッションの特性を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。

	コマンドまたはアクション	目的
	<pre>デバイス(config)# monitor session 2 source interface gigabitethernet1/0/2 rx</pre>	<ul style="list-style-type: none"> • <i>interface-id</i> には、モニタリングする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランクポートとして設定しておく必要があります。
ステップ 5	<p>monitor session <i>session_number</i> filter vlan <i>vlan-id</i> [, -]</p> <p>例 :</p> <pre>デバイス(config)# monitor session 2 filter vlan 1 - 5 , 9</pre>	<p>SPAN 送信元トラフィックを特定の VLAN に制限します。</p> <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 4 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 VLAN 範囲を指定します。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 6	<p>monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [encapsulation replicate]}</p> <p>例 :</p> <pre>デバイス(config)# monitor session 2 destination interface gigabitethernet1/0/1</pre>	<p>SPAN セッションおよび宛先ポート (モニター側ポート) を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 4 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) [, -] には、一連のインターフェイスまたはインターフェイスの範囲を指定します。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) encapsulation replicate には、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ことを指定します。選択しない場合のデフォルトは、ネイティブ形式 (タグなし) でのパケットの送信です。
ステップ 7	<p>end</p> <p>例 :</p> <pre>デバイス(config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>

	コマンドまたはアクション	目的
ステップ 8	show running-config 例： デバイス# <code>show running-config</code>	入力を確認します。
ステップ 9	copy running-config startup-config 例： デバイス# <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。

RSPAN VLAN としての VLAN の設定

新しい VLAN を作成し、RSPAN セッション用の RSPAN VLAN になるように設定するには、次の手順を実行します。

手順の概要

1. `enable`
2. `configure terminal`
3. `vlan vlan-id`
4. `remote-span`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> <code>enable</code>	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： デバイス# <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 3	vlan <i>vlan-id</i> 例：	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

	コマンドまたはアクション	目的
	デバイス (config) # vlan 100	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 または 1006 ~ 4094 です。 RSPAN VLAN を VLAN 1 (デフォルト VLAN) または VLAN ID 1002 ~ 1005 (トークンリングおよび FDDI VLAN 専用) にすることはできません。
ステップ 4	remote-span 例 : デバイス (config-vlan) # remote-span	VLAN を RSPAN VLAN として設定します。
ステップ 5	end 例 : デバイス (config-vlan) # end	特権 EXEC モードに戻ります。
ステップ 6	show running-config 例 : デバイス # show running-config	入力を確認します。
ステップ 7	copy running-config startup-config 例 : デバイス # 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。

次のタスク

RSPAN に参加するすべての devices に RSPAN VLAN を作成する必要があります。RSPAN VLAN ID が標準範囲 (1005 未満) 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 device に RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他の devices 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 devices、および中間 devices 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 トラフィックが効率的に流れるようにするか、または RSPAN トラフィックの伝送が不要なすべてのトランクから、RSPAN VLAN を手動で削除します。

VLAN からリモート SPAN 特性を削除して、標準 VLAN に戻すように変換するには、**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。

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

セッション 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。

RSPAN 送信元セッションの作成

RSPAN 送信元セッションを作成および開始し、モニター対象の送信元および宛先 RSPAN VLAN を指定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session {session_number | all | local | remote}**
4. **monitor session session_number source {interface interface-id | vlan vlan-id} [, | -] [both | rx | tx]**
5. **monitor session session_number destination remote vlan vlan-id**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： デバイス# 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 3	no monitor session {session_number all local remote} 例： デバイス(config)# no monitor session 1	セッションに対する既存の SPAN 設定を削除します。 • <i>session_number</i> の範囲は、1 ~ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。

	コマンドまたはアクション	目的
ステップ 4	<p>monitor session <i>session_number</i> source {interface <i>interface-id</i> vlan <i>vlan-id</i>} [, -] [both rx tx]</p> <p>例 :</p> <pre>デバイス(config)# monitor session 1 source interface gigabitethernet1/0/1 tx</pre>	<p>RSPAN セッションおよび送信元ポート（モニター対象ポート）を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • RSPAN セッションの送信元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、モニタリング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 (port-channel <i>port-channel-number</i>) があります。有効なポートチャンネル番号は1 ~ 48 です。 • <i>vlan-id</i> には、モニターする送信元 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>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> <ul style="list-style-type: none"> • (任意) [, -] : 一連のインターフェイスまたはインターフェイスの範囲を指定します。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) both rx tx : 監視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かった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 <ul style="list-style-type: none"> • both : 受信トラフィックと送信トラフィックの両方を監視します。 • rx : 受信トラフィックをモニターします。 • tx : 送信トラフィックをモニターします。
ステップ 5	<p>monitor session <i>session_number</i> destination remote vlan <i>vlan-id</i></p> <p>例 :</p>	<p>RSPAN セッション、宛先 RSPAN VLAN、および宛先ポートグループを指定します。</p>

フィルタリングする VLAN の指定

	コマンドまたはアクション	目的
	<pre>デバイス(config)# monitor session 1 destination remote vlan 100</pre>	<ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 4 で指定した番号を入力します。 • <i>vlan-id</i> には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 6	<p>end</p> <p>例：</p> <pre>デバイス(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	<p>show running-config</p> <p>例：</p> <pre>デバイス# show running-config</pre>	入力を確認します。
ステップ 8	<p>copy running-config startup-config</p> <p>例：</p> <pre>デバイス# copy running-config startup-config</pre>	(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。

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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session {*session_number* | all | local | remote}**
4. **monitor session *session_number* source interface *interface-id***
5. **monitor session *session_number* filter vlan *vlan-id* [, | -]**
6. **monitor session *session_number* destination remote vlan *vlan-id***
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： デバイス# 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 3	no monitor session {session_number all local remote} 例： デバイス(config)# no monitor session 2	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> session_number の範囲は、1 ～ 66 です。 all : すべての SPAN セッションを削除します。 local : すべてのローカルセッションを削除します。 remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session session_number source interface interface-id 例： デバイス(config)# monitor session 2 source interface gigabitethernet1/0/2 rx	送信元ポート（モニター対象ポート）と SPAN セッションの特性を指定します。 <ul style="list-style-type: none"> session_number の範囲は、1 ～ 66 です。 interface-id には、モニタリングする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランクポートとして設定しておく必要があります。
ステップ 5	monitor session session_number filter vlan vlan-id [, -] 例： デバイス(config)# monitor session 2 filter vlan 1 - 5 , 9	SPAN 送信元トラフィックを特定の VLAN に制限します。 <ul style="list-style-type: none"> session_number には、ステップ 4 で指定したセッション番号を入力します。 vlan-id 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 VLAN 範囲を指定します。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。

	コマンドまたはアクション	目的
ステップ 6	monitor session session_number destination remote vlan vlan-id 例： デバイス(config)# monitor session 2 destination remote vlan 902	RSPAN セッションおよび宛先リモート VLAN (RSPAN VLAN) を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 4 で指定したセッション番号を入力します。 • <i>vlan-id</i> には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 7	end 例： デバイス(config)# end	特権 EXEC モードに戻ります。
ステップ 8	show running-config 例： デバイス# show running-config	入力を確認します。
ステップ 9	copy running-config startup-config 例： デバイス# 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 宛先セッションの作成

RSPAN 宛先セッションは、別のdeviceまたはdevice スタック（送信元セッションが設定されていないdeviceまたはdevice スタック）に設定します。

このdevice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、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **vlan vlan-id**
4. **remote-span**
5. **exit**
6. **no monitor session {session_number | all | local | remote}**
7. **monitor session session_number source remote vlan vlan-id**

8. **monitor session** *session_number* **destination interface** *interface-id*
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： デバイス# 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 3	vlan <i>vlan-id</i> 例： デバイス(config)# vlan 901	送信元deviceで作成された RSPAN VLAN の VLAN ID を指定し、VLAN コンフィギュレーション モードを開始します。 両方のdevices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 3 ～ 5 は不要です。
ステップ 4	remote-span 例： デバイス(config-vlan)# remote-span	VLAN を RSPAN VLAN として識別します。
ステップ 5	exit 例： デバイス(config-vlan)# 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 6	no monitor session { <i>session_number</i> all local remote } 例： デバイス(config)# no monitor session 1	セッションに対する既存の SPAN 設定を削除します。 • <i>session_number</i> の範囲は、1 ～ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • remote : すべてのリモート SPAN セッションを削除します。
ステップ 7	monitor session session_number source remote vlan vlan-id 例 : デバイス (config) # monitor session 1 source remote vlan 901	RSPAN セッションと送信元 RSPAN VLAN を指定します。 <ul style="list-style-type: none"> • session_number の範囲は、1 ~ 66 です。 • vlan-id には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 8	monitor session session_number destination interface interface-id 例 : デバイス (config) # monitor session 1 destination interface gigabitethernet2/0/1	RSPAN セッションと宛先インターフェイスを指定します。 <ul style="list-style-type: none"> • session_number には、ステップ 7 で指定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。 <ul style="list-style-type: none"> • interface-id 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は物理インターフェイスでなければなりません。 • encapsulation replicate はコマンドラインのヘルプストリングに表示されますが、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になります。
ステップ 9	end 例 : デバイス (config) # end	特権 EXEC モードに戻ります。
ステップ 10	show running-config 例 : デバイス # show running-config	入力を確認します。
ステップ 11	copy running-config startup-config 例 :	(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。

	コマンドまたはアクション	目的
	デバイス# <code>copy running-config startup-config</code>	

RSPAN 宛先セッションの作成および着信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、宛先ポートでネットワーク セキュリティ デバイス（Cisco IDS センサー装置等）用に着信トラフィックをイネーブルにするには、次の手順を実行します。

手順の概要

1. `enable`
2. `configure terminal`
3. `no monitor session {session_number | all | local | remote}`
4. `monitor session session_number source remote vlan vlan-id`
5. `monitor session session_number destination {interface interface-id [, | -] [ingress { dot1q vlan vlan-id | untagged vlan vlan-id | vlan vlan-id}]}`
6. `end`
7. `show running-config`
8. `copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>enable</code> 例： デバイス> <code>enable</code>	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<code>configure terminal</code> 例： デバイス# <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 3	<code>no monitor session {session_number all local remote}</code> 例： デバイス(config)# <code>no monitor session 2</code>	セッションに対する既存の SPAN 設定を削除します。 • <code>session_number</code> の範囲は、1 ～ 66 です。 • <code>all</code> : すべての SPAN セッションを削除します。 • <code>local</code> : すべてのローカルセッションを削除します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session <i>session_number</i> source remote vlan <i>vlan-id</i> 例 : デバイス (config) # monitor session 2 source remote vlan 901	RSPAN セッションと送信元 RSPAN VLAN を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> の範囲は、1 ~ 66 です。 • <i>vlan-id</i> には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 5	monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [ingress { dot1q vlan <i>vlan-id</i> untagged vlan <i>vlan-id</i> vlan <i>vlan-id</i> }]} 例 : デバイス (config) # monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6	SPAN セッション、宛先ポート、パケットカプセル化、および着信 VLAN とカプセル化を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 5 で指定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は物理インターフェイスでなければなりません。 • encapsulation replicate はコマンドラインのヘルプストリングに表示されますが、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になります。 • (任意) [, -] には、一連のインターフェイスまたはインターフェイスの範囲を指定します。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。 • 宛先ポートでの着信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 を追加のキーワードと一緒に入力します。 <ul style="list-style-type: none"> • dot1q vlan <i>vlan-id</i> : デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを転送します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • untagged vlan vlan-id または vlan vlan-id : デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ 6	end 例 : デバイス(config)# end	特権 EXEC モードに戻ります。
ステップ 7	show running-config 例 : デバイス# show running-config	入力を確認します。
ステップ 8	copy running-config startup-config 例 : デバイス# 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。

FSPAN セッションの設定

SPAN セッションを作成し、送信元 (監視対象) ポートまたは VLAN、および宛先 (モニター) ポートを指定し、セッションに FSPAN を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** { **interface** *interface-id* | **vlan** *vlan-id* } [,|-] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination** { **interface** *interface-id* [,|-] [**encapsulation replicate**] }
6. **monitor session** *session_number* **filter** { **ip** | **ipv6** | **mac** } **access-group** { *access-list-number* | *name* }
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： デバイス# 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 3	no monitor session {session_number all local remote} 例： デバイス (config)# no monitor session 2	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> <i>session_number</i> の範囲は、1 ～ 66 です。 all : すべての SPAN セッションを削除します。 local : すべてのローカルセッションを削除します。 remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session session_number source { interface interface-id vlan vlan-id } [, -] [both rx tx] 例： デバイス (config)# monitor session 2 source interface gigabitethernet1/0/1	SPAN セッションおよび送信元ポート（モニター対象ポート）を指定します。 <ul style="list-style-type: none"> <i>session_number</i> の範囲は、1 ～ 66 です。 <i>interface-id</i> には、モニタリング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（port-channel port-channel-number）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、監視する送信元 VLAN を指定します。指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （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は送信元ポートと送信元VLANを併用できません。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) <code>[, -]</code>: 一連のインターフェイスまたはインターフェイスの範囲を指定します。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) <code>[both rx tx]</code>: モニタリング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かった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニターします。 <ul style="list-style-type: none"> • both: 送信トラフィックと受信トラフィックの両方を監視します。これはデフォルトです。 • rx: 受信トラフィックをモニターします。 • tx: 送信トラフィックをモニターします。 <p>(注) monitor session <i>session_number</i>source 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>
<p>ステップ 5</p>	<p>monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [encapsulation replicate]}</p> <p>例:</p> <pre> デバイス(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate </pre>	<p>SPANセッションおよび宛先ポート（モニター側ポート）を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ4で入力したセッション番号を指定します。 • destination では、次のパラメータを指定します。 <ul style="list-style-type: none"> • <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) <code>[, -]</code> には、一連のインターフェイスまたはインターフェイスの範囲を指定します。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) encapsulation replicate には、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ことを指定します。選択しない場合のデフォルトは、

	コマンドまたはアクション	目的
		<p>ネイティブ形式 (タグなし) でのパケットの送信です。</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>monitor session <i>session_number</i> destination 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>
ステップ 6	<p>monitor session <i>session_number</i> filter {ip ipv6 mac} access-group {<i>access-list-number</i> <i>name</i>}</p> <p>例 :</p> <pre>デバイス(config)# monitor session 2 filter ipv6 access-group 4</pre>	<p>SPAN セッション、フィルタリングするパケットのタイプ、および FSPAN セッションで使用する ACL を指定します。</p> <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 4 で入力したセッション番号を指定します。 • <i>access-list-number</i> には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • <i>name</i> には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 7	<p>end</p> <p>例 :</p> <pre>デバイス(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 8	<p>show running-config</p> <p>例 :</p> <pre>デバイス# show running-config</pre>	入力を確認します。
ステップ 9	<p>copy running-config startup-config</p> <p>例 :</p> <pre>デバイス# copy running-config startup-config</pre>	(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。

FRSPAN セッションの設定

RSPAN 送信元セッションを開始し、監視対象の送信元および宛先 RSPAN VLAN を指定し、セッションに FRSPAN を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session_number* | **all** | **local** | **remote**}
4. **monitor session** *session_number* **source** { **interface** *interface-id* | **vlan** *vlan-id* } [, | -] [**both** | **rx** | **tx**]
5. **monitor session** *session_number* **destination remote** **vlan** *vlan-id*
6. **vlan** *vlan-id*
7. **remote-span**
8. **exit**
9. **monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*}
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： デバイス# 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 3	no monitor session { <i>session_number</i> all local remote }	セッションに対する既存の SPAN 設定を削除します。 • <i>session_number</i> の範囲は、1 ～ 66 です。 • all : すべての SPAN セッションを削除します。 • local : すべてのローカルセッションを削除します。 • remote : すべてのリモート SPAN セッションを削除します。
ステップ 4	monitor session <i>session_number</i> source { interface <i>interface-id</i> vlan <i>vlan-id</i> } [, -] [both rx tx] 例：	SPAN セッションおよび送信元ポート（モニター対象ポート）を指定します。 • <i>session_number</i> の範囲は、1 ～ 66 です。

	コマンドまたはアクション	目的
	デバイス (config) # monitor session 2 source interface gigabitethernet1/0/1	<ul style="list-style-type: none"> • <i>interface-id</i> には、モニタリング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 (port-channel port-channel-number) 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、監視する送信元 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は送信元ポートと送信元 VLAN を併用できません。</p> <ul style="list-style-type: none"> • (任意) [<i>, -</i>] : 一連のインターフェイスまたはインターフェイスの範囲を指定します。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) [both rx tx] : モニタリング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かった場合、SPANは送信トラフィックと受信トラフィックの両方をモニターします。 • both : 送信トラフィックと受信トラフィックの両方をモニターします。これはデフォルトです。 • rx : 受信トラフィックをモニターします。 • tx : 送信トラフィックをモニターします。 <p>(注) monitor session session_numbersource 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>
ステップ 5	monitor session session_number destination remote vlan vlan-id 例 :	RSPAN セッションと宛先 RSPAN VLAN を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 4 で指定した番号を入力します。

	コマンドまたはアクション	目的
	デバイス (config) # monitor session 2 destination remote vlan 5	<ul style="list-style-type: none"> • <i>vlan-id</i> には、モニタリングする宛先 RSPAN VLAN を指定します。
ステップ 6	vlan <i>vlan-id</i> 例 : デバイス (config) # vlan 10	VLAN コンフィギュレーションモードを開始します。 <i>vlan-id</i> には、モニタリングする送信元 RSPAN VLAN を指定します。
ステップ 7	remote-span 例 : デバイス (config-vlan) # remote-span	ステップ 5 で指定した VLAN が RSPAN VLAN の一部であることを指定します。
ステップ 8	exit 例 : デバイス (config-vlan) # 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 9	monitor session <i>session_number</i> filter {ip ipv6 mac} access-group {<i>access-list-number</i> <i>name</i>} 例 : デバイス (config) # monitor session 2 filter ip access-group 7	RSPAN セッション、フィルタリングするパケットのタイプ、および FRSPAN セッションで使用する ACL を指定します。 <ul style="list-style-type: none"> • <i>session_number</i> には、ステップ 4 で入力したセッション番号を指定します。 • <i>access-list-number</i> には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • <i>name</i> には、トラフィックのフィルタリングに使用する ACL の名前を指定します。
ステップ 10	end 例 : デバイス (config) # end	特権 EXEC モードに戻ります。
ステップ 11	show running-config 例 : デバイス # show running-config	入力を確認します。
ステップ 12	copy running-config startup-config 例 :	(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。

	コマンドまたはアクション	目的
	デバイス# <code>copy running-config startup-config</code>	

SPAN および RSPAN 動作のモニタリング

次の表で、SPAN および RSPAN 動作の設定と結果を表示して動作をモニタするために使用するコマンドについて説明します。

表 2: SPAN および RSPAN 動作のモニタリング

コマンド	目的
<code>show monitor</code>	現在の SPAN、RSPAN、示します。

SPAN および RSPAN の設定例

例：ローカル SPAN の設定

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポート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、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 にミラーリングします。

```

デバイス> enable
デバイス# configure terminal
デバイス(config)# no monitor session 1
デバイス(config)# monitor session 1 source interface gigabitethernet1/0/1
デバイス(config)# monitor session 1 destination interface gigabitethernet1/0/2
encapsulation replicate
デバイス(config)# end

```

次に、SPAN セッション 1 の SPAN 送信元としてのポート 1 を削除する例を示します。

```

デバイス> enable
デバイス# configure terminal
デバイス(config)# no monitor session 1 source interface gigabitethernet1/0/1
デバイス(config)# end

```

次に、双方向モニタが設定されていたポート 1 で、受信トラフィックのモニタをディセーブルにする例を示します。

```

デバイス> enable

```

```
デバイス# configure terminal
デバイス(config)# no monitor session 1 source interface gigabitethernet1/0/1 rx
```

ポート1で受信する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宛先ポートGigabitEthernet2に送信する例を示します。さらに、この設定は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変更されます。

```
デバイス> enable
デバイス# configure terminal
デバイス(config)# no monitor session 2
デバイス(config)# monitor session 2 source vlan 1 - 3 rx
デバイス(config)# monitor session 2 destination interface gigabitethernet1/0/2
デバイス(config)# monitor session 2 source vlan 10
デバイス(config)# end
```

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ソース送信元ポート1上で受信される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、そのトラフィックを送信元ポートと同じ出力カプセル化方式の宛先ギガビットイーサネットポート2に送信し、デフォルト入力VLANとしてVLAN 6を使用した入力転送をイネーブルにする例を示します。

```
デバイス> enable
デバイス# configure terminal
デバイス(config)# no monitor session 2
デバイス(config)# monitor session 2 source gigabitethernet0/1 rx
デバイス(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress vlan 6
デバイス(config)# end
```

次に、SPANセッション2の既存の設定を削除し、トランクポートGigabitEthernet2で受信されたトラフィックをモニターするようにSPANセッション2を設定し、VLAN 1～5および9に対してのみトラフィックを宛先ポートGigabitEthernet1に送信する例を示します。

```
デバイス> enable
デバイス# configure terminal
デバイス(config)# no monitor session 2
デバイス(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
デバイス(config)# monitor session 2 filter vlan 1 - 5 , 9
デバイス(config)# monitor session 2 destination interface gigabitethernet1/0/1
デバイス(config)# end
```

例 : RSPAN VLAN の作成

この例は、RSPAN VLAN 901 の作成方法を示しています。

```
デバイス> enable
```

```

デバイス# configure terminal
デバイス(config)# vlan 901
デバイス(config-vlan)# remote span
デバイス(config-vlan)# end

```

次に、セッション 1 に対応する既存の 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。

```

デバイス> enable
デバイス# configure terminal
デバイス(config)# no monitor session 1
デバイス(config)# monitor session 1 source interface gigabitethernet1/0/1 tx
デバイス(config)# monitor session 1 source interface gigabitethernet1/0/2 rx
デバイス(config)# monitor session 1 source interface port-channel 2
デバイス(config)# monitor session 1 destination remote vlan 901
デバイス(config)# end

```

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 で受信される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 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

```

デバイス> enable
デバイス# configure terminal
デバイス(config)# no monitor session 2
デバイス(config)# monitor session 2 source interface gigabitethernet1/0/2 rx
デバイス(config)# monitor session 2 filter vlan 1 - 5 , 9
デバイス(config)# monitor session 2 destination remote vlan 902
デバイス(config)# end

```

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。

```

デバイス> enable
デバイス# configure terminal
デバイス(config)# monitor session 1 source remote vlan 901
デバイス(config)# monitor session 1 destination interface gigabitethernet2/0/1
デバイス(config)# end

```

次に、RSPAN セッション 2 で送信元リモート VLAN として VLAN 901 を設定し、送信元ポート GigabitEthernet2 を宛先インターフェイスとして設定し、VLAN 6 をデフォルトの受信 VLAN として着信トラフィックの転送をイネーブルにする例を示します。

```

デバイス> enable
デバイス# configure terminal
デバイス(config)# monitor session 2 source remote vlan 901
デバイス(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress
vlan 6
デバイス(config)# end

```

SPAN および RSPAN の機能の履歴と情報

リリース	変更内容
Cisco IOS XE Everest 16.5.1a	<p>スイッチポートアナライザ (SPAN) : スニファアアナライザまたはRMONプローブを使用してポートまたはVLANのデバイスのトラフィックを監視できます。</p> <p>この機能が導入されました。</p>
Cisco IOS XE Everest 16.5.1a	<p>フローベースのスイッチポートアナライザ (SPAN) : 指定されたフィルタを使用してエンドホスト間の必要なデータのみをキャプチャする手段を提供します。フィルタは、IPv4、IPv6 または IPv4 と IPv6、あるいは指定された送信元と宛先アドレス間の IP トラフィック (MAC) 以外を制限するアクセスリストの観点から定義されます。</p> <p>この機能が導入されました。</p>
Cisco IOS XE Everest 16.5.1a	<p>スイッチポートアナライザ (SPAN) - 分散型出力</p> <p>SPAN : ラインカードにすでに分散された入力 SPAN とともにラインカードに出力 SPAN 機能を分散させます。出力 SPAN 機能をラインカードに分散させることで、システムのパフォーマンスが向上します。</p> <p>この機能が導入されました。</p>

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。