CHAPTER 27

SPAN および RSPAN の設定

この章では、Cisco ME 3400E イーサネット 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。

（注） この章で使用す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。

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 を使用して監視できるのは、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るトラフィックは監視できません。たとえば、着信トラフィックを監視している場合、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監視できません。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監視できます。

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 セッションを停止させることができます。

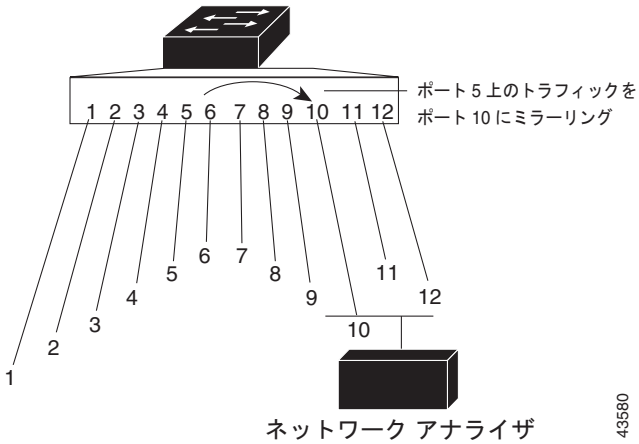
ここでは、次の概要について説明します。

- 「SPAN および RSPAN の他の機能との相互作用」（P.27-8）

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 27-1 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。

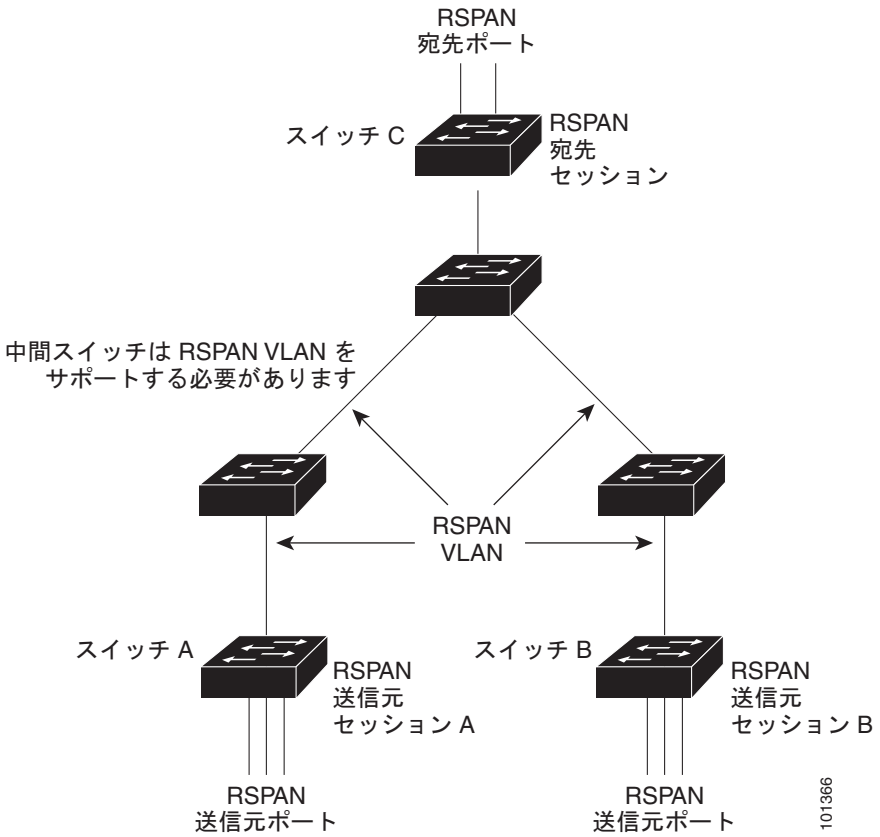
図 27-1　　単一スイッチでのローカル SPAN の設定例



Remote SPAN

RSPAN を使用すると、異なるスイッチ上で送信元ポート、送信元 VLAN、宛先ポートがサポートされるため、ネットワーク内で複数のスイッチの Remote Monitoring（RMON）がイネーブルになります。図 27-2 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 上で伝送されます。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 を監視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（スイッチ C を参照）。

図 27-2　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監視し、監視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.27-8）を参照）。

SPAN セッションでのトラフィックの監視には、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、最大 2 つの送信元セッション（ローカル SPAN および RSPAN 送信元セッション）をサポートします。同じスイッチで、ローカル SPAN 送信元セッション および RSPAN 送信元セッションの両方を実行できます。スイッチは合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 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、設定できる宛先ポートは最大で 64 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。スイッチでメトロ IP アクセス イメージが稼動している場合は、スイッチド ポートおよびルーテッド ポートの両方を SPAN 送信元および SPAN 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 ポートを監視する 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、監視中の各パケットは 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 回は監視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。

監視対象トラフィック

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 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監視することです。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 QoS（Quality of Service）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 コントロール 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監視することです。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監視できます。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; シスコ検出プロトコル）、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 プロトコルを監視しません。ただし、宛先ポートを設定するときにキーワード **encapsulation replicate** を入力すると、次のように変更されます。

- 送信ポートの場合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監視されます。

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、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監視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 からも廃棄されます。

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 監視用に、ポート B では TX 監視用に、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、両方のパケットは同じものになります（レイヤ 3 書き換えが行われない場合には、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 *監視対象ポート*）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監視できます。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 セッションで監視できます。
- 各送信元ポートに、監視する方向（入力、出力、両方）を設定できます。
- すべてのタイプのポート（EtherChannel、ファスト イーサネット、ギガビット イーサネット、User Network Interface（UNI; ユーザ ネットワーク インターフェイス）、Network Node Interface（NNI; ネットワーク ノード インターフェイス）、Enhanced Network Interface（ENI; 拡張ネットワーク インターフェイス）を送信元ポートに設定できます
- 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、トラフィックを監視できます。
- 送信元ポートを、ルーテッド ポート、アクセス ポート、またはトランク ポートにすることができます。
- 宛先ポートに指定できません。
- 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監視できます。

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 トラフィックを監視できます。VSPAN 内の SPAN または RSPAN 送信元インターフェイスは VLAN ID で指定され、トラフィックはその VLAN のすべてのポートで監視されます。

VLAN 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監視できます。
- 指定されたポートでは、監視対象の VLAN 上のトラフィックだけ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、監視されません。
- 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、監視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 は使用できません。
- 監視できるのは、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監視する場合、デフォルトでは、トランク上でアクティブなすべての VLAN が監視されます。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 トラフィックの監視を特定の VLAN に制限できます。

- VLAN フィルタリングは、トランク ポートにだけ適用されます。
- VLAN フィルタリングはポートベース セッションにだけ適用され、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、リスト内のこれらの VLAN だけがトランク ポートで監視されます。
- 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だけ作用し、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（別名*監視側ポート*）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になければなりません。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 送信元セッションだけを実行するスイッチには、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。スイッチでメトロ IP アクセス イメージが稼動していて、ポートがルーテッド ポートであった場合、そ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 ポートにはできません。
- 送信元ポートには指定できません。
- 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送信は行われません。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、監視されません。
- スイッチ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、宛先ポートにキーワード **encapsulation replicate** 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、または IEEE 802.1Q）。**encapsulation dot1q** が指定されている場合、パケットは IEEE 802.1Q カプセル化により表示されます。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、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 ポート上だけです。
- 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。
  - VLAN を UNI-ENI 独立 VLAN（デフォルト）から RSPAN VLAN に変更するには、**rspan-vlan** VLAN コンフィギュレーション モード コマンドを入力します。
  - UNI-ENI コミュニティ VLAN を RSPAN VLAN に変更するには、**no uni-vlan** VLAN コンフィギュレーション モード コマンドを入力してまずコミュニティ VLAN を削除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。

（注）　NNI はデフォルトで STP をサポートし、ENI の STP をイネーブルにできます。UNI では、STP はサポートされていません。

- RSPAN VLAN は、プライベート VLAN のプライマリまたはセカンダリ VLAN にできません。

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 を監視したり、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：メトロ IP アクセス イメージを稼動しているスイッチでは、SPAN はルーテッド トラフィックを監視リングしません。RSPAN が監視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監視しません。たとえば、VLAN が受信監視され、スイッチが別の 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：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。ただし、STP は、NNI または ENI 上でだけサポートされ、UNI は STP に参加しません。
- 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。NNI ではデフォルトで CDP をイネーブルにし、ENI で CDP をイネーブルにできます。UNI は CDP に参加しません。

- 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、グループ全体が監視対象となります。

  監視対象 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。監視対象 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*ステートになります。

  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 グループおよび監視対象ポートのリストから削除されます。
- マルチキャスト トラフィックを監視できます。送信側および受信側ポートのモニタリングの場合は、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 宛先ポートにはなれません。
- セキュア ポートは SPAN 宛先ポートにできません。

  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、出力を監視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、出力を監視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す。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、宛先ポートで受信転送がイネーブルの場合、送信を監視しているポートで 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、送信を監視しているどのポートでも IEEE802.1X をイネーブルにしないでください。

SPAN および RSPAN の設定

SPAN および RSPAN のデフォルト設定

表 27-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 27-1　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。
監視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は、すべての VLAN が監視されます。
RSPAN VLAN	設定なし。デフォルトの VLAN タイプは、UNI-ENI 独立 VLAN です。

ローカル SPAN の設定

SPAN 設定時の注意事項

- スイッチごとに、2 つのローカル SPAN セッションまたは RSPAN 送信元セッションの合計を設定できます。スイッチでは、合計で 66 の SPAN セッション（ローカル RSPAN 送信元および RSPAN 宛先）を設定できます。
- 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、監視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、キーワード **encapsulation replicate** またはキーワード **encapsulation dot1q** 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、または IEEE 802.1Q）が付加されます。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は、送信元または宛先ポートにはできますが、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。

- キーワード **filter vlan** 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。監視対象がトランク ポートの場合、このキーワードで指定された VLAN 上のトラフィックだけが監視されます。デフォルトでは、トランク ポートのすべての VLAN が監視されます。
- 1 つの SPAN セッション内で送信元 VLAN を混在させたり、VLAN をフィルタリングできません。

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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。 *session_number* 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 RSPAN セッションを削除するには **remote** を指定します。

	コマンド	目的
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	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。 *session_number* の範囲は、1 ～ 66 です。 *interface-id* には、監視する送信元ポートまたは送信元 VLAN を指定します。 • 送信元 *interface-id* には、監視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）。 **（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 の併用はできません。 （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）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い場合、SPAN は送受信両方のトラフィックを監視します。 • **both**：送受信両方のトラフィックを監視します。これはデフォルト設定です。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。 **（注）** **monitor session** *session_number* **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。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation**{**dot1q** | **replicate**}]	SPAN セッションおよび宛先ポート（監視側ポート）を指定します。 *session_number* 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。 **（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。 *interface-id* 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）IEEE 802.1Q カプセル化の場合は **encapsulation dot1q** を、または **encapsulation replicate** を入力して、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。 **（注）** **monitor session** *session_number* **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。
ステップ 5	**end**	特権 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、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、キーワード **encapsulation replicate** 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監視する例を示します。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 gigabitethernet0/1
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
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 gigabitethernet0/1
Switch(config)# end
```

次に、双方向監視用に設定された、ポート 1 での受信トラフィック監視をディセーブルにする例を示します。

```
Switch(config)# no monitor session 1 source interface gigabitethernet0/1 rx
```

ポート 1 での受信トラフィックの監視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監視されます。

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監視するように SPAN セッション 2 を設定し、監視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。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監視するように変更されます。

```
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2
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、特権 EXEC モードで次の手順を実行します。

（注）　入力トラフィックに関連性の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.27-11）を参照してください。

	コマンド	目的
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	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	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。

	コマンド	目的
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {[**dot1q** | **untagged] vlan** *vlan-id*}]	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。 *session_number* 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。 *interface-id* 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。カンマまたはハイフンの前後にはスペースを入力します。 （任意）IEEE 802.1Q カプセル化の場合は **encapsulation dot1q** を、または **encapsulation replicate** を入力して、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。 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。 • **dot1q** *:* 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、着信パケットを転送します。 • **untagged** *:* 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、着信パケットを転送します。 • **vlan** *vlan-id* : デフォルト VLAN です。**dot1q** または **untagged** のいずれも指定しない場合、デフォルトでタグなしパケットが転送されます。
ステップ 5	**end**	特権 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、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、送信元ギガビット イーサネット ポート 1 に送信されたトラフィックを監視するように 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 を使用する着信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 gigabitethernet0/1 rx
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。 *session_number* 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 RSPAN セッションを削除するには **remote** を指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id*	送信元ポート（監視対象ポート）および SPAN セッションの特性を指定します。 *session_number* の範囲は、1 ～ 66 です。 *interface-id* には、監視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	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	SPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number* 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。 *vlan-id* では、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	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}]}	SPAN セッションおよび宛先ポート（監視側ポート）を指定します。 *session_number* 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。 *interface-id* 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）**encapsulation dot1q** または **encapsulation replicate** を入力して、IEEE 802.1Q カプセル化また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よう指定します。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 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 8	**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。

トランク ポート上のすべての VLAN を監視するには、**no monitor session** *session_number* **filter** 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監視するように SPAN セッション 2 を設定し、VLAN 1 ～ 5 および VLAN 9 のトラフィックだけを宛先ギガビット 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 gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination interface gigabitethernet0/1
Switch(config)# end
```

RSPAN の設定

RSPAN 設定時の注意事項

- RSPAN には、「SPAN 設定時の注意事項」（P.27-10）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、特定のパケットを選択してフィルタリングまたは監視できます。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させることができます。
- 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 ポートにだけ設定されており、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 ポートは、非アクティブ ステートになります。
- 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監視しないため、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 で、MAC アドレス ラーニング がイネーブルである。

- 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することを推奨します。

RSPAN VLAN としての VLAN の設定

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。送信元スイッチと宛先スイッチ、およびすべての中間スイッチで RSPAN VLAN を設定する必要があります。

RSPAN トラフィックのフローを効率化するために、RSPAN トラフィックを送信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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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*	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。 **（注）** RSPAN VLAN は、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）にできません。 UNI-ENI コミュニティ VLAN の VLAN ID を入力する場合、**no uni-vlan** VLAN コンフィギュレーション コマンドを入力してコミュニティ VLAN のタイプを削除する必要があります。
ステップ 3	**remote-span**	VLAN を RSPAN VLAN として設定します。
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**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。

VLAN から SPAN の特性を削除して、UNI-ENI 独立 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、監視対象の送信元および宛先 RSPAN VLAN を指定するには、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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	**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 RSPAN セッションを削除するには **remote** を指定します。
ステップ 3	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**]	RSPAN 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。 *session_number* 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。 • *interface-id* には、監視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）。 **（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 の併用はできません。 （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）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。 • **both**：送受信両方のトラフィックを監視します。 • **rx**：受信トラフィックを監視します。 • **tx**：送信トラフィックを監視します。
ステップ 4	**monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先 RSPAN VLAN を指定します。 *session_number* には、ステップ 3 で定義した番号を入力します。 *vlan-id* には、監視する送信元 RSPAN VLAN を指定します。
ステップ 5	**end**	特権 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監視するように 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 gigabitethernet0/1 tx
Switch(config)# monitor session 1 source interface gigabitethernet0/2 rx
Switch(config)# monitor session 1 source interface port-channel 12
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（送信元セッションが設定されていないスイッチ）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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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。 **（注）** VLAN が UNI-ENI コミュニティ VLAN として設定される場合、**no uni-vlan** VLAN コンフィギュレーション コマンドを入力してコミュニティ VLAN のタイプを削除する必要があります。
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 RSPAN 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、監視する送信元 RSPAN VLAN を指定します。

	コマンド	目的
ステップ 7	**monitor session** *session_number* **destination interface** *interface-id*	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。 *session_number* には、ステップ 6 で定義した番号を入力します。 （注）　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。 *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には物理インターフェイスを指定する必要があります。 （注）　**encapsulation replicate** はコマンドラインのヘルプ ストリング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になります。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 10	**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 gigabitethernet0/1
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、特権 EXEC モードで次の手順を実行します。

（注）　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.27-20）を参照してください。この手順では、RSPAN VLAN が設定してあると想定しています。

	コマンド	目的
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	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。

	コマンド	目的
ステップ 3	**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、監視する送信元 RSPAN VLAN を指定します。
ステップ 4	**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**ingress** {**dot1q vlan** *vlan-id* | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]}	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。 *session_number* には、ステップ 4 で定義した番号を入力します。 （注）　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。 *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には物理インターフェイスを指定する必要があります。 （注）　**encapsulation replicate** はコマンドラインのヘルプ ストリング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になります。 （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** に次のキーワードを指定して入力します。 • **dot1q vlan** *vlan-id*：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、着信パケットを転送します。 • **untagged vlan** *vlan-id* または **vlan** *vlan-id*：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、着信パケットを転送します。
ステップ 5	**end**	特権 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。

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 に設定し、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 gigabitethernet0/2 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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
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	**no monitor session** {*session_number* | **all** | **local** | **remote**}	セッションの既存の SPAN 設定を削除します。 *session_number* 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 RSPAN セッションを削除するには **remote** を指定します。
ステップ 3	**monitor session** *session_number* **source interface** *interface-id*	送信元ポート（監視対象ポート）および SPAN セッションの特性を指定します。 *session_number* の範囲は、1 ～ 66 です。 *interface-id* には、監視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	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**]	SPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number* 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。 *vlan-id* では、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	**monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 *session_number* 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。 *vlan-id* には、監視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	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show monitor** [**session** *session_number*] **show running-config**	設定を確認します。
ステップ 8	**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。

トランク ポート上のすべての VLAN を監視するには、**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監視するように RSPAN セッション 2 を設定し、VLAN 2 ～ 5 および VLAN 9 のトラフィックだけを宛先 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 gigabitethernet0/2 rx
Switch(config)# monitor session 2 filter vlan 2 - 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** 特権 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。