



SPAN および RSPAN の設定

この章では、Catalyst 2950 または Catalyst 2955 スイッチで 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、このリリースに対応するコマンドリファレンスを参照してください。

この章の内容は、次のとおりです。

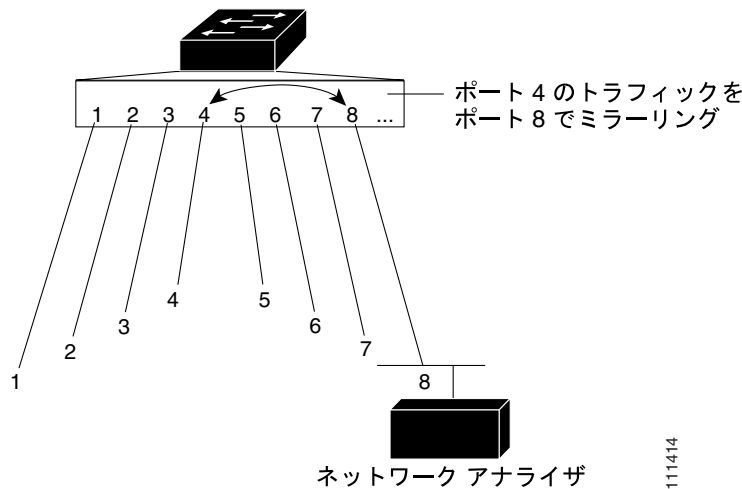
- [SPAN および RSPAN の概要 \(p.24-2\)](#)
- [SPAN の設定 \(p.24-8\)](#)
- [RSPAN の設定 \(p.24-13\)](#)
- [SPAN および RSPAN のステータス表示 \(p.24-18\)](#)

SPAN および RSPAN の概要

SwitchProbe 装置、他の Remote Monitoring (RMON) プローブまたはセキュリティ装置に接続されたスイッチの別のポートに、SPAN を使用してトラフィックのコピーを送信することによって、ポートを通過するネットワーク トラフィックを解析できます。SPAN は 1 つまたは複数の送信元ポートで受信、送信、または送受信されたトラフィックを宛先ポートにミラーリングして解析します。

たとえば、[図 24-1](#) の場合、ポート 4 (送信元ポート) のすべてのトラフィックがポート 8 (宛先ポート) にミラーリングされます。ポート 8 のネットワーク アナライザは、ポート 4 に物理的には接続されていませんが、ポート 4 からのあらゆるネットワーク トラフィックを受信します。

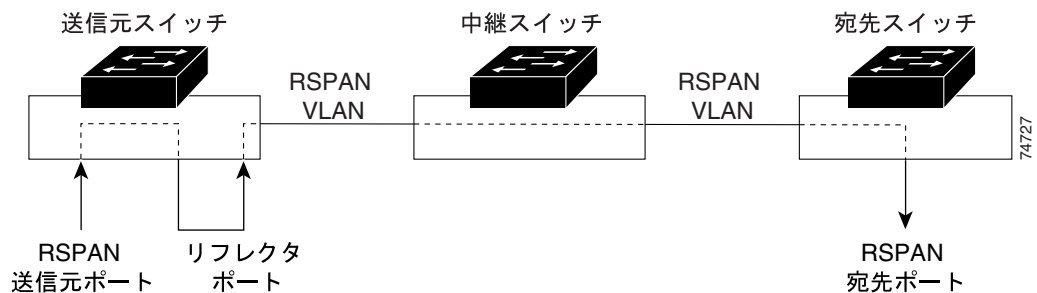
図 24-1 SPAN の設定例



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だけです。

RSPAN はネットワーク上の複数のスイッチをリモート モニタできるようにすることによって、SPAN を拡張します。各 RSPAN セッションのトラフィックは、ユーザが指定したその RSPAN セッション専用の RSPAN VLAN を使用して、関係するすべてのスイッチに伝送されます。SPAN トラフィックは送信元からリフレクタ ポートを通じて RSPAN VLAN にコピーされ、さらに RSPAN VLAN を伝送するトランク ポートで、RSPAN VLAN をモニタする RSPAN 宛先セッションに転送されます。[図 24-2](#) を参照してください。

図 24-2 RSPAN の設定例



SPAN および RSPAN は、送信元ポートでのネットワーク トラフィックのスイッチングには影響を与えません。送信元インターフェイスで送受信されたパケットのコピーが宛先インターフェイスに送信されます。SPAN または RSPAN セッションに必要なトラフィック以外、リフレクタ ポートおよび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 宛先ポートを使用して、ネットワーク セキュリティ装置から送信されたトラフィックを転送できます。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 装置は TCP Reset パケットを送信して、疑わしい攻撃者からの TCP セッションを停止できます。



(注)

RSPAN 宛先ポートを使用して、ネットワーク セキュリティ装置から送信されたトラフィックを転送できません。スイッチは RSPAN 宛先ポートでは、入力転送をサポートしません。

SPAN および RSPAN の概念および用語

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

SPAN セッション

ローカル SPAN セッションは宛先ポートと送信元ポートの対応付けです。一連のポート、またはポート範囲で着信または発信トラフィックをモニタできます。

RSPAN セッションは、ネットワーク全体の送信元ポートと RSPAN VLAN の対応付けです。宛先送信元は RSPAN VLAN です。

SPAN セッションがスイッチ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 のポートをモニタするなど、オーバーサブスクライブの SPAN 宛先は、パケットの廃棄または消失を招きます。

ディセーブルのポートに 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 1 つ以上の送信元ポート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。**show monitor session session_number** イネーブル EXEC コマンドを使用すると、SPAN セッションの稼働ステータスが表示されます。

SPAN セッションはシステムの起動後、宛先ポートが動作可能になるまでは非アクティブです。

トラフィック タイプ

SPAN セッションには、次のトラフィック タイプがあります。

- RX (受信) SPAN — 受信 (または入力) SPAN の役割は、送信元インターフェイスが受信したパケットをできるだけすべて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 セッションに対応する宛先ポートに送られます。SPAN セッションで一連の入力ポートまたは入力ポート範囲をモニタできます。

宛先ポートでは、タグgingがイネーブルの場合、パケットには IEEE 802.1Q ヘッダーが含まれます。タグgingが指定されていない場合、パケットはネイティブ フォーマットになります。

Differentiated Services Code Point (DSCP) の変更など、Quality of Service (QoS; サービス品質) が原因で変更されたパケットは、RX SPAN 用に変更してコピーされます。

- TX (送信) SPAN — 送信 (または出力) SPAN の役割は、スイッチによる変更および処理がすべて完了したあとで、送信元インターフェイスから送信されたパケットをできるだけすべてモニタすることです。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。このコピーは、パケットが変更されたあとで送信されます。SPAN セッションでは出力ポートの範囲をモニタできます。

QoS により変更されたパケットには、SPAN 送信元と異なる DSCP (IP パケット) または Class of Service (CoS; サービス クラス) (非 IP パケット) が設定されていることがあります。

パケットが送信処理時に廃棄される原因となる機能には、SPAN 用に複製されたコピーにも影響を与えるものもあります。これらの機能には、マルチキャスト パケット上の IP 標準および IP 拡張出力 Access Control List (ACL; アクセス制御リスト) などが含まれます。出力 ACL の場合、SPAN 送信元がパケットを廃棄すると、SPAN 宛先もパケットを廃棄します。送信元ポートがオーバーサブスクライブ状態の場合、宛先ポートは別の廃棄動作を行います。

- 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、一連のポートまたはポート範囲をモニタできます。

送信元ポート

送信元ポート (別名、*モニタ対象ポート*) は、ネットワークトラフィックを解析するためにモニタするスイッチドポートです。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、RX、TX、または双方向 (both) の送信元ポートトラフィックをモニタできます。スイッチは任意の数の送信元ポートをサポートします (スイッチで使用できるポートの最大数が限度)。

送信元ポートの特性は、次のとおりです。

- あらゆるポートタイプが可能です (EtherChannel、ファストイーサネット、ギガビットイーサネットなど)。
- 宛先ポートにすることはできません。
- モニタする方向 (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。EtherChannel を送信元とする場合、モニタする方向はグループ内のすべての物理ポートに適用されます。
- 送信元ポートは同じ VLAN 上にあっても異なる VLAN 上にあってもかまいません。

トランクポートを送信元ポートとして設定できます。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。

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、送信元ポートからトラフィックのコピーを受け取る宛先ポート (別名、*モニタ側ポート*) が必要です。

宛先ポートの特性は、次のとおりです。

- 送信元ポートと同じスイッチになければなりません (ローカル SPAN セッションの場合)。
- 任意のイーサネット物理ポートにできます。
- 送信元ポートまたはリフレクタポートにはできません。
- EtherChannel グループまたは VLAN にはできません。
- EtherChannel グループが SPAN 送信元として指定されている場合でも、EtherChannel グループに割り当てられた物理ポートにできます。SPAN 宛先ポートとして設定されている間、そのポートはグループから除外されます。
- 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。
- 入力トラフィックの転送がネットワークセキュリティ装置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。
- SPAN セッションがアクティブな間、スパニングツリーには加わりません。

- これが宛先ポートの場合、Cisco Discovery Protocol (CDP)、VLAN Trunking Protocol (VTP)、Dynamic Trunking Protocol (DTP)、Spanning-Tree Protocol (STP)、Port Aggregation Protocol (PAgP)、Link Aggregation Control Protocol (LACP) などのレイヤ 2 プロトコルに参加しません。
- 宛先ポートでのアドレス学習は行われません。
- 宛先ポートは、モニタされるすべての送信元ポートに対する送受信トラフィックのコピーを受信します。宛先ポートがオーバーサブスクライブ状態の場合、輻輳が起きる可能性があります。その結果、1 つまたは複数の送信元ポートでトラフィック転送に影響を与える可能性があります。

リフレクタ ポート

リフレクタ ポートは、パケットを RSPAN VLAN にコピーするメカニズムです。リフレクタ ポートは、関係している RSPAN 送信元セッションからのトラフィックだけを転送します。リフレクタ ポートとして設定されたポートに接続しているすべての装置は、RSPAN 送信元セッションがディセーブルになるまで接続が切断されます。

リフレクタ ポートの特性は、次のとおりです。

- ループバックに設定されたポートです。
- EtherChannel グループにすることはできません。トランキングしません。また、プロトコル フィルタリングを実行できません。
- EtherChannel グループが SPAN 送信元として指定されている場合でも、EtherChannel グループに割り当てられた物理ポートにできます。リフレクタ ポートとして設定されている間、そのポートはグループから除外されます。
- リフレクタ ポートとして使用しているポートは、SPAN 送信元または宛先ポートにできません。また、同時に複数のセッションのリフレクタ ポートにすることはできません。
- どの VLAN でも認識されません。
- リフレクタ ポートのループバック トラフィックに対応するネイティブ VLAN は、RSPAN VLAN です。
- リフレクタ ポートは、タグなしトラフィックをスイッチにループバックします。そのトラフィックはさらに RSPAN VLAN に送られ、RSPAN VLAN を伝送するあらゆるトランク ポートにフラッディングされます。
- リフレクタ ポートではスパニングツリーが自動的にディセーブルになります。
- リフレクタ ポートは、モニタされるすべての送信元ポートに対する送受信トラフィックのコピーを受信します。リフレクタ ポートがオーバーサブスクライブ状態の場合、輻輳が起きる可能性があります。その結果、1 つまたは複数の送信元ポートでトラフィック転送に影響を与える可能性があります。

リフレクタ ポートの帯域幅が対応する送信元ポートからのトラフィック ボリュームに対して十分でない場合、余ったパケットは廃棄されます。10/100 ポートは 100 Mbps でリフレクトします。ギガビット ポートは 1 Gbps でリフレクトします。

SPAN トラフィック

すべてのネットワーク トラフィックを監視するためにローカル SPAN を使用できます。マルチキャストおよび 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、CDP、VTP、DTP、STP、PAgP、LACP パケットなどが監視できます。RSPAN を使用してレイヤ 2 プロトコルをモニタすることはできません。詳細については、「[RSPAN 設定時の注意事項](#)」(p.24-13) を参照してください。

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、双方向 (RX および TX の両方) SPAN セッションが、a1 RX モニタおよび a2 RX/TX モニタを送信元、d1 を宛先ポートとして設定されているとします。パケットが a1 からスイッチに入って a2 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 d1 に送信されます。

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。

- STP — SPAN または RSPAN セッションがアクティブな間、宛先ポートまたはリフレクタ 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、宛先ポートまたはリフレクタ 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、スイッチ間で 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、宛先ポート、またはリフレクタ 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、宛先ポートまたはリフレクタ 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 または RSPAN セッションをディセーブルにしてからです。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、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はできますが、SPAN 宛先ポートとして設定することはできません。グループが SPAN 送信元として設定されている場合、グループ全体がモニタされます。

モニタ対象の EtherChannel グループに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。モニタ対象の 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。ポートが EtherChannel グループの唯一のポートだった場合は、EtherChannel グループが SPAN から削除されます。

EtherChannel グループに含まれる物理ポートを SPAN 送信元ポート、宛先ポート、またはリフレクタ ポート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、グループメンバーのままですが、*down* または *standalone* 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、宛先ポートまたはリフレクタ 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 グループおよびモニタ対象ポートリストから削除されます。

- QoS — 入力モニタの場合、SPAN 宛先ポートに送信されるパケットと、SPAN 送信元ポートで実際に受信されるパケットが異なる場合があります。これは、入力 QoS 分類およびポリシングの実行後にパケットが転送されるためです。パケットの DSCP は受信されたパケットと異なることがあります。
- マルチキャスト トラフィックをモニタできます。出力ポートおよび入力ポートのモニタでは、未編集のパケットが 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の送信回数は反映されません。
- ポートセキュリティ — 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 および RSPAN セッション限度

スイッチでローカル SPAN セッションを 1 つ、または複数の RSPAN セッションを設定する（さらに NVRAM [不揮発性 RAM] に保管する）ことができます。アクティブセッションの数および組み合わせには、次の制限があります。

- SPAN または RSPAN 送信元 (RX、TX、両方) — アクティブセッション限度は 1 です (SPAN と RSPAN を同じ送信元スイッチに同時に設定することはできません)。
- RSPAN 送信元セッションには、そのセッションに対応付けられた RSPAN VLAN を使用するセッションごとに、1 つずつ宛先が必要です。
- 各 RSPAN 宛先セッションには、サポートする RSPAN VLAN ごとに、1 つまたは複数の宛先インターフェイスが必要です。
- RSPAN 宛先セッション限度は 2 です。または、ローカル SPAN または送信元 RSPAN セッションを同一スイッチで設定する場合、限度は 1 です。

SPAN および RSPAN のデフォルト設定

表 24-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 24-1 SPAN および RSPAN のデフォルト設定

機能	デフォルト値
SPAN ステート	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 (カプセル化タイプのヘッダーなし)
入力転送 (宛先ポート)	ディセーブル

SPAN の設定

ここでは、スイッチ上で SPAN を設定する手順について説明します。内容は次のとおりです。

- [SPAN 設定時の注意事項 \(p.24-8\)](#)
- [SPAN セッションの作成およびモニタ対象ポートの指定 \(p.24-8\)](#)
- [SPAN セッションの作成と入力トラフィックのイネーブル化 \(p.24-10\)](#)
- [SPAN セッションからのポートの削除 \(p.24-12\)](#)

SPAN 設定時の注意事項

SPAN を設定するときには、次の注意事項に従ってください。

- SPAN セッションは、「[SPAN および RSPAN セッション限度](#)」(p.24-7) で説明した限度内で、RSPAN セッションと共存できます。
- 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。
- SPAN セッションごとに設定可能な宛先ポートは 1 つだけです。同じ宛先ポートを使用して 2 つの SPAN セッションを行うことはできません。
- EtherChannel ポートは、SPAN 送信元ポートにすることはできますが、SPAN 宛先ポートにはできません。
- SPAN 送信元ポートの場合、単一ポート、あるいは一連またはある範囲のポートの送信トラフィックおよび受信トラフィックをモニタできます。
- スイッチ ポートを SPAN 宛先ポートとして設定すると、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トラフィックがモニタされるだけです。
- ディセーブル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 1 つ以上の送信元ポートがイネーブルになってからです。
- SPAN 宛先ポートは VLAN スパニングツリーに参加しません。SPAN はモニタ対象トラフィックに BPDU を組み込むので、SPAN セッションの SPAN 宛先ポートで受信されたスパニングツリー BPDU は、SPAN 送信元ポートからのコピーです。
- SPAN がイネーブルの場合、設定を変更すると、次のような結果になります。
 - － 宛先ポートの VLAN 設定を変更した場合、その変更が有効になるのは、SPAN がディセーブルになってからです。
 - － すべての送信元ポートまたは宛先ポートをディセーブルにすると、送信元ポートと宛先ポートの両方がイネーブルになるまで、SPAN 機能は停止します。

SPAN セッションの作成およびモニタ対象ポートの指定

SPAN セッションを作成し、送信元（モニタ対象）ポートおよび宛先（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	目的
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>	セッションに対応する既存の SPAN 設定を消去します。 <i>session_number</i> には 1 を指定します。 すべての SPAN セッションを削除する場合は all を指定します。すべてのローカル セッションを削除する場合は、 local を指定します。すべての RSPAN セッションを削除する場合は、 remote を指定します。
ステップ 3	<code>monitor session <i>session_number</i> source interface <i>interface-id</i> [, -] [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。 <i>session_number</i> には 1 を指定します。 <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 <i>port-channel-number</i>) です。 (任意) [, -] — 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後にスペースを 1 つずつ入力します。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 — 送信トラフィックと受信トラフィックの両方をモニタします。 • rx — 受信トラフィックをモニタします。 • tx — 送信トラフィックをモニタします。
ステップ 4	<code>monitor session <i>session_number</i> destination interface <i>interface-id</i> [encapsulation {dot1q}]</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 1 を指定します。 <i>interface-id</i> には、宛先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が含まれます。 (任意) 発信パケットのカプセル化ヘッダーを指定します。指定しなかった場合、パケットはネイティブ形式で送信されます。 <ul style="list-style-type: none"> • dot1q — IEEE 802.1Q のカプセル化を使用します。
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	<code>show monitor [session <i>session_number</i>]</code>	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 セッションとしてセッション 1 を設定し、宛先ポートへの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 設定を消去し、双方向トラフィックを送信元ポート 1 から宛先ポート 8 へミラーリングします。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastethernet0/1
Switch(config)# monitor session 1 destination interface fastethernet0/8
encapsulation dot1q
Switch(config)# end
```

SPAN セッションの作成と入力トラフィックのイネーブル化

SPAN セッションを作成し、送信元および宛先ポートを指定し、ネットワーク セキュリティ装置 (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。

	コマンド	目的
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>	セッションに対応する既存の SPAN 設定を消去します。 <i>session_number</i> には 1 を指定します。 すべての SPAN セッションを削除する場合は all を指定します。すべてのローカル セッションを削除する場合は、 local を指定します。すべてのリモート RSPAN セッションを削除する場合は、 remote を指定します。
ステップ 3	<code>monitor session session_number source interface interface-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。 <i>session_number</i> には 1 を指定します。 <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) です。 (任意) [, -] — 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後にスペースを 1 つずつ入力します。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 — 送信トラフィックと受信トラフィックの両方をモニタします。 rx — 受信トラフィックをモニタします。 tx — 送信トラフィックをモニタします。

	コマンド	目的
ステップ 4	monitor session <i>session_number</i> destination interface <i>interface-id</i> [encapsulation {dot1q}] [ingress vlan <i>vlan id]</i>	SPAN セッション、宛先ポート（モニタ側ポート）、パケットカプセル化、および入力側 VLAN を指定します。 <i>session_number</i> には 1 を指定します。 <i>interface-id</i> には、宛先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が含まれます。 (任意) 発信パケットのカプセル化ヘッダーを指定します。指定しなかった場合、パケットはネイティブ形式で送信されます。 <ul style="list-style-type: none"> • dot1q — IEEE 802.1Q のカプセル化を使用します。 (任意) ingress vlan <i>vlan id</i> を入力して、入力転送をイネーブルにし、デフォルト VLAN を指定します。
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>]	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。

次の例では、IEEE 802.1Q カプセル化をサポートしないセキュリティ装置を使用して、VLAN 5 の入力トラフィック用の宛先ポートを設定する方法を示します。

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 ingress vlan 5
```

次の例では、IEEE 802.1Q カプセル化をサポートするセキュリティ装置を使用して、VLAN 5 の入力トラフィック用の宛先ポートを設定する方法を示します。

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 encapsulation dot1q ingress vlan 5
```

次の例では、宛先ポートで入力トラフィック転送をディセーブルにする方法を示します。

```
Switch(config)# monitor session 1 destination interface fastethernet0/5 encapsulation dot1q
```

SPAN セッションからのポートの削除

セッションの SPAN 送信元としてのポートを削除するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
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 source interface interface-id [, -] [both rx tx]</code>	<p>削除する送信元ポート（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。</p> <p><code>session</code> には 1 を指定します。</p> <p><code>interface-id</code> には、モニタを中止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>) です。</p> <p>(任意) <code>[, -]</code> を使用して、一連のインターフェイスまたはインターフェイス範囲を指定します。このオプションが有効なのは、受信トラフィックだけをモニタする場合です。カンマの前後にスペースを 1 つずつ入力します。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) モニタを中止するトラフィックの方向 (<code>both</code>、<code>rx</code>、<code>tx</code>) 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は、送受信の両方がディセーブルになります。</p>
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show monitor [session session_number]</code>	設定を確認します。
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。

SPAN セッションから送信元ポートまたは宛先ポートを削除する場合は、`no monitor session session_number source interface interface-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。カプセル化タイプをデフォルト（ネイティブ）に戻す場合は、`encapsulation` キーワードを指定しないで `monitor session session_number destination interface interface-id` を使用します。

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

```
Switch(config)# no monitor session 1 source interface fastethernet0/1
Switch(config)# end
```

双方向モニタが設定されていたポートで、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。

```
Switch(config)# no monitor session 1 source interface fastethernet0/1 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のモニタは継続されます。

RSPAN の設定

ここでは、スイッチ上で RSPAN を設定する手順について説明します。内容は次のとおりです。

- RSPAN 設定時の注意事項 (p.24-13)
- RSPAN VLAN としての VLAN の設定 (p.24-14)
- RSPAN 送信元セッションの作成 (p.24-14)
- RSPAN 宛先セッションの作成 (p.24-16)
- RSPAN セッションからのポートの削除 (p.24-17)

RSPAN 設定時の注意事項

ここで説明する RSPAN 機能を使用するには、スイッチに Enhanced Software Image (EI; 拡張ソフトウェア イメージ) をインストールしておく必要があります。RSPAN を設定するときには、次の注意事項に従ってください。

- 「SPAN 設定時の注意事項」(p.24-8) の全項目は RSPAN にも当てはまります。
- RSPAN VLAN には特殊な特性があるので、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 ポート割り当てをしない必要があります。
- RSPAN セッションは、「SPAN および RSPAN セッション限度」(p.24-7) で説明した限度内で、SPAN セッションと共存できます。
- 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スイッチに分散させることができます。
- RSPAN リフレクタ ポートとして指定されている間、RSPAN 送信元ポートまたは RSPAN 宛先ポートとしては動作できません。
- スイッチ ポートをリフレクタ ポートとして設定すると、通常のスイッチ ポートではなくなります。リフレクタ ポートを通過するのは、ループバック トラフィックだけです。
- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 スイッチ プロトコルをサポートしません。
- Catalyst 2950 または Catalyst 2955 スイッチだけで構成されるネットワークでは、送信元スイッチごとに固有の RSPAN VLAN セッションを使用する必要があります。複数の送信元スイッチで同じ RSPAN VLAN を使用する場合は、スイッチは送信元スイッチとしてだけ動作し、モニタ対象のすべてのトラフィックが確実に宛先スイッチに届くようにします。
- 次の条件を満たすかぎり、任意の VLAN を RSPAN VLAN として設定できます。
 - RSPAN VLAN をネイティブ VLAN として設定することはできません。
 - 拡張範囲 RSPAN VLAN は、VTP を使用する他のスイッチに伝播されません。
 - RSPAN VLAN にアクセス ポートを設定することはできません。
 - 参加するすべてのスイッチで RSPAN をサポートしていなければなりません。



(注) RSPAN VLAN を VLAN 1 (デフォルト VLAN) または 1002 ~ 1005 の VLAN ID (トークンリングおよび FDDI VLAN に予約済み) にすることはできません。


- RSPAN VLAN を作成してから、RSPAN 送信元または宛先セッションを設定する必要があります。
- 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 未満の 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 としての VLAN の設定

まず、RSPAN セッションの RSPAN VLAN とする新しい VLAN を作成します。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 未満) で、VTP がネットワークでイネーブルになっている場合、1 つのスイッチに RSPAN VLAN を作成し、VTP ドメイン内の他のスイッチに伝播できます。拡張範囲 VLAN (1005 より大きい) については、送信元および宛先スイッチの両方と中距離スイッチに 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。

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	目的
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 <i>vlan-id</i></code>	VLAN を作成する VLAN ID を入力するか、または既存 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。有効範囲は 2 ~ 1001 および 1006 ~ 4094 です。  (注) RSPAN VLAN を VLAN 1 (デフォルト VLAN) または 1002 ~ 1005 の VLAN ID (トークンリングおよび FDDI VLAN に予約済み) にすることはできません。
ステップ 3	<code>remote-span</code>	RSPAN VLAN としての VLAN の設定
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 からリモート SPAN 特性を削除して標準 VLAN に戻すには、`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、監視する送信元および宛先 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	目的
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>	セッションに対応する既存の RSPAN 設定を消去します。 <i>session_number</i> には、この RSPAN セッションを特定するセッション番号を指定します。 すべての RSPAN セッションを削除する場合は all を指定します。すべてのローカル セッションを削除する場合は、 local を指定します。すべての RSPAN セッションを削除する場合は、 remote を指定します。

	コマンド	目的
ステップ 3	monitor session <i>session_number</i> source interface <i>interface-id</i> [, -] [both rx tx]	<p>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。</p> <p><i>session_number</i> には、この RSPAN セッションを特定するセッション番号を指定します。</p> <p><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 <i>port-channel-number</i>) です。</p> <p>(任意) [, -] — 一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後にスペースを1つずつ入力します。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。</p> <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モニタします。 • rx — 受信トラフィックをモニタします。 • tx — 送信トラフィックをモニタします。
ステップ 4	monitor session <i>session_number</i> destination remote vlan <i>vlan-id</i> reflector-port interface	<p>RSPAN セッション、宛先リモート VLAN、およびリフレクタポートを指定します。</p> <p><i>session_number</i> には、この RSPAN セッションを特定するセッション番号を入力します。</p> <p><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 (RSPAN VLAN 作成の詳細については、「イーサネット VLAN の作成または変更」 [p.16-9] を参照)。</p> <p><i>interface</i> には、RSPAN トラフィックを RSPAN VLAN にフラッディングするインターフェイスを指定します。</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 [<i>session session_number</i>]	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。

次に、セッション 1 に対応する既存の RSPAN 設定を消去し、複数の送信元インターフェイスをモニタする RSPAN セッション 1 を設定し、さらに宛先 RSPAN VLAN およびリフレクタポートを設定する例を示します。

```
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastethernet0/10 tx
Switch(config)# monitor session 1 source interface fastethernet0/2 rx
Switch(config)# monitor session 1 source interface fastethernet0/3 rx
Switch(config)# monitor session 1 source interface port-channel 102 rx
Switch(config)# monitor session 1 destination remote vlan 901 reflector-port
fastethernet0/1
Switch(config)# end
```

RSPAN 宛先セッションの作成

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	目的
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>monitor session session_number source remote vlan vlan-id</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> には、この RSPAN セッションを特定するセッション番号を指定します。 <i>vlan-id</i> には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 3	<code>monitor session session_number destination interface interface-id [encapsulation {dot1q}]</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、この RSPAN セッションを特定するセッション番号を指定します。 <i>interface-id</i> には、宛先インターフェイスを指定します。 (任意) 発信パケットのカプセル化ヘッダーを指定します。指定しなかった場合、パケットはネイティブ形式で送信されます。 • dot1q — IEEE 802.1Q のカプセル化を使用します。
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>show monitor [session session_number]</code>	設定を確認します。
ステップ 6	<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。

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 5 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 fastethernet0/5
Switch(config)# end
```

RSPAN セッションからのポートの削除

セッションの RSPAN 送信元としてのポートを削除するには、イネーブル EXEC モードで次の手順を実行します。

	コマンド	目的
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> source interface <i>interface-id</i> [, -] [<i>both</i> <i>rx</i> <i>tx</i>]</code>	<p>削除する RSPAN 送信元ポート (モニタ対象ポート) の特性を指定します。</p> <p><i>session_number</i> には、この RSPAN セッションを特定するセッション番号を指定します。</p> <p><i>interface-id</i> には、モニタを中止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 <i>port-channel-number</i>) です。</p> <p>(任意) [, -] を使用して、一連のインターフェイスまたはインターフェイス範囲を指定します。カンマの前後にスペースを1つずつ入力します。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) モニタを中止するトラフィックの方向 (both、rx、tx) 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は、送受信の両方がディセーブルになります。</p>
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show monitor [<i>session session_number</i>]</code>	設定を確認します。
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。

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

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1
Switch(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。

```
Switch(config)# no monitor session 1 source interface fastEthernet0/1 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のモニタは継続されます。

SPAN および RSPAN のステータス表示

現在の SPAN または RSPAN 設定のステータスを表示するには、**show monitor** イネーブル EXEC コマンドを使用します。

SPAN 送信元セッション 1 に対する **show monitor** イネーブル EXEC コマンドの出力例を示します。

```
Switch# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
  RX Only           : None
  TX Only           : None
  Both              : Fa0/4
Source VLANs        :
  RX Only           : None
  TX Only           : None
  Both              : None
Source RSPAN VLAN   : None
Destination Ports   : Fa0/5
Encapsulation: DOT1Q
  Ingress: Enabled, default VLAN = 5
Reflector Port      : None
Filter VLANs        : None
Dest RSPAN VLAN     : None
```