CHAPTER 43

SPAN および RSPAN の設定

この章では、Catalyst 4500 シリーズ スイッチ上で スイッチド ポート アナライザ（SPAN）とリモート SPAN（RSPAN）を設定する方法について説明します。SPAN は、SwitchProbe デバイスまたはその他の Remote Monitoring（RMON）プローブなどのネットワーク アナライザによる解析用に、ネットワーク トラフィックを選択します。

この章の内容は、次のとおりです。

（注） この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6350/index.html

SPAN と RSPAN の概要

ここでは、次の内容について説明します。

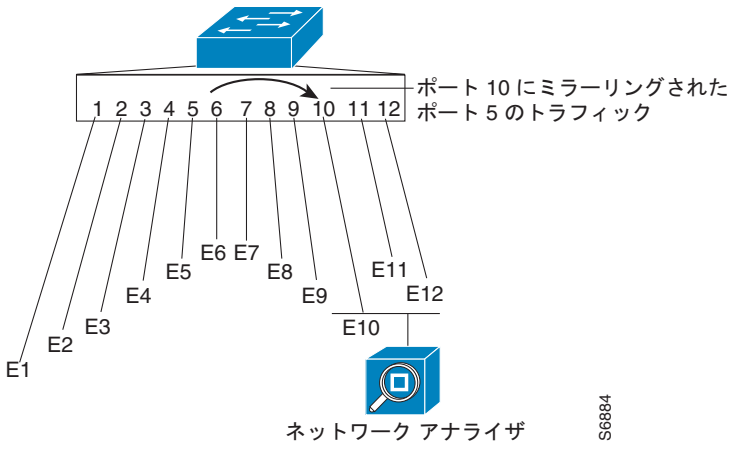
SPAN は、任意の VLAN 上の 1 つまたは複数の送信元インターフェイスからのトラフィック、または 1 つまたは複数の VLAN から宛先インターフェイスへのトラフィックを解析するためにミラーリングします。図 43-1 では、イーサネット インターフェイス 5（送信元インターフェイス）上のすべてのト

ラフィックが、イーサネット インターフェイス 10 にミラーリングされます。イーサネット インターフェイス 10 のネットワーク アナライザは、イーサネット インターフェイス 5 に物理的に接続していなくても、このインターフェイスからのすべてのネットワーク トラフィックを受信できます。

SPAN を設定する場合、送信元インターフェイスと宛先インターフェイスは同一スイッチ上に存在している必要があります。

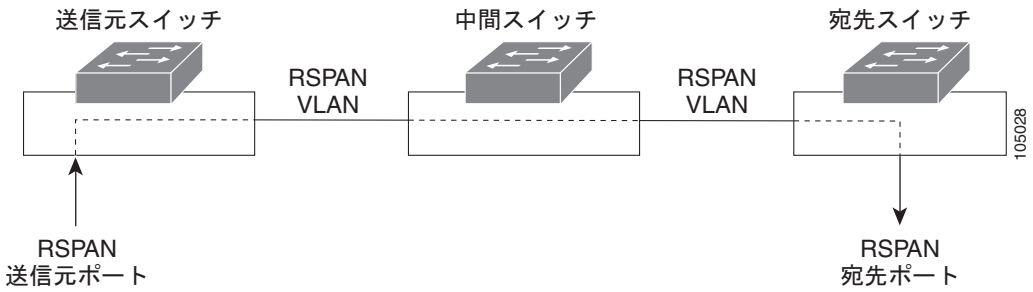
SPAN は、送信元インターフェイス上のネットワーク トラフィックのスイッチングに影響を与えません。送信元インターフェイスが送受信したパケットのコピーは宛先インターフェイスに送信されます。

図 43-1　SPAN の設定例



RSPAN は、ネットワーク内の複数のスイッチのリモート モニタリングをイネーブル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 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。送信元からの SPAN トラフィックは、RSPAN VLAN にコピーされてから、トランク ポートを介して転送されます。トランク ポートは、RSPAN VLAN をモニタリングする RSPAN 宛先セッションに RSPAN VLAN を伝送します（図 43-2 を参照）。

図 43-2　RSPAN の設定例



SPAN と RSPAN は、送信元ポートまたは送信元 VLAN 上でのネットワーク トラフィックのスイッチングに影響しません。送信元によって送受信されたパケットのコピーは、宛先に送信されます。デフォルトでは、SPAN または RSPAN セッションによって必要とされるトラフィックを除いて、宛先ポートはトラフィックの送受信を行いません。

SPAN または RSPAN 宛先ポートを使用して、ネットワーク セキュリティ デバイス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。

SPAN と RSPAN の概念および用語

ここでは、SPAN と RSPAN の設定に関連する概念と用語について説明します。ここでは、次の内容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、宛先ポートを送信元ポートに対応付けます。一連のまたは一定範囲のポートおよび送信元 VLAN の着信または発信トラフィックをモニタリングできます。RSPAN セッションは、送信元ポートと送信元 VLAN をネットワーク上の RSPAN VLAN に対応付けます。宛先の送信元は RSPAN VLAN です。

モニタ対象のネットワーク トラフィックの送信元を指定するパラメータを使用して、SPAN セッションを設定します。

個別のまたは重複する一連の SPAN 送信元を使用して、複数の SPAN または RSPAN セッションを設定できます。スイッチド ポートおよびルーテッド ポートはいずれも、SPAN 送信元または宛先ポートとして設定できます。

RSPAN 送信元セッションは、SPAN 送信元ポートまたは VLAN を宛先 RSPAN VLAN に対応付けます。RSPAN 宛先セッションは、RSPAN VLAN を宛先ポートに対応付けます。

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（たとえば 100 Mbps ポートをモニタリングする 10 Mbps ポート）では、パケットがドロップされるか、失われる可能性があります。

ディセ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。

SPAN セッションは、システムの起動後に、宛先ポートが動作可能になるまでアクティブになりません。

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。

- 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限り多くモニタリングすることです。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。1 つの SPAN セッションで、一連のまたは一定範囲の入力ポートまたは VLAN をモニタリングできます。

  タグ付きパケット（ISL（スイッチ間リンク）または IEEE 802.1Q）では、タギングは入力ポートで削除されます。宛先ポートでは、タギングがイネーブルの場合、パケットは ISL または 802.1Q ヘッダー付きで表示されます。タギングが指定されていない場合、パケットはネイティブ形式で表示されます。

ルーティングが原因で変更されたパケットは、Rx SPAN 用に変更されることなくコピーされます。つまり、元のパケットがコピーされます。Quality of Service（QoS）が原因で変更されたパケット（たとえば、変更済み DiffServ コード ポイント（DSCP））は、Rx SPAN 用に変更されてコピーされます。

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、SPAN では無効です。実際の着信パケットがドロップされた場合でも、宛先ポートは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 入力アクセス コントロール リスト（ACL）、ユニキャストおよび入力側 QoS ポリシング用の標準および拡張 IP 出力 ACL、VLAN マップ、入力側 QoS ポリシング、Policy-Based Routing（PBR; ポリシーベース ルーティング）などがあります。パケットのドロップを引き起こすスイッチ輻輳も、SPAN には影響しません。

- 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限り多くモニタリングすることです。パケットが変更されたあと、送信元から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信されます。1 つの SPAN セッションで一定範囲の出力ポートをモニタできます。

  ルーティングにより変更されたパケット（存続可能時間（TTL）または MAC アドレスによる変更など）は、宛先ポートでも変更されます。QoS が原因で変更されたパケットは、SPAN 送信元とは異なる DSCP（IP パケット）または CoS（IP 以外のパケット）を設定されることがあります。

  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 用の重複されたコピーにも影響を与えることがあります。このような機能には、VLAN マップ、マルチキャスト パケットに対応する標準および拡張 IP 出力 ACL、出力側 QoS ポリシングがあります。出力 ACL の場合は、SPAN 送信元がパケットをドロップすると、SPAN の宛先もパケットをドロップします。出力側 QoS ポリシングの場合は、SPAN 送信元がパケットをドロップしても、SPAN 宛先はパケットをドロップするとは限りません。送信元ポートがオーバーサブスクライブ型である場合、宛先ポートは別の廃棄動作を行います。

- 双方向：1 つの SPAN セッションで、一連の単一ポートまたは一定範囲のポートの受信パケットと送信パケットを両方モニタリングできます。

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。単一のローカル SPAN セッションまたは RSPAN 送信元セッションで、受信（Rx）、送信（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リングできます。スイッチは、任意の数の送信元ポート（スイッチで使用可能なポートの最大数まで）および任意の数の送信元 VLAN をサポートしています。

送信元ポートの特性は、次のとおりです。

- すべてのポート タイプ（EtherChannel、ファスト イーサネット、ギガビット イーサネットなど）が可能です。
- 複数の SPAN セッションでモニタできます。
- 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 の送信元に設定する場合、モニタリング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 にあっても異なる VLAN にあってもかまいません。
- VLAN の SPAN 送信元では、ソース VLAN のすべてのアクティブ ポートが送信元ポートとして含まれます。

トランク ポートを、送信元ポートとして設定できます。デフォルトでは、トランク上でアクティブなすべての VLAN がモニタされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニタ対象を特定の VLAN に制限できます。選択された VLAN のスイッチド トラフィックだけが宛先ポートに送信されます。この機能は、宛先 SPAN ポートに転送されたトラフィックだけに影響し、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。この機能は、VLAN 送信元によるセッションでは許可されません。

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する宛先ポート（別名モニタリング ポート）を設定する必要があります。

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上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指定できます。
- 同時に 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）。
- 送信元ポートに指定することはできません。
- EtherChannel グループに指定することはできません。
- 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指定できます。ポートは、SPAN 宛先ポートとして設定されている間は、グループから削除されます。
- ラーニングがイネーブルに設定されていない限り、ポートは SPAN セッションが必要とするものを除いて、トラフィックの転送を行いません。ラーニングがイネーブルに設定されている場合、ポートは、宛先ポート上で学習されたホストに向けられたトラフィックも伝送します。
- 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。
- SPAN セッションがアクティブな間は、スパニングツリーに参加しません。
- 宛先ポートである場合は、どのレイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）にも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- 宛先ポートは、すべてのモニタ対象送信元ポートの、送受信された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 スクライブ型である場合、輻輳を起こす可能性があり、宛先ポートでパケット ドロップが発生することがあります。この輻輳は送信元ポート トラフィックの転送には影響しません。

VSPAN

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できます。

VSPAN セッションでは、次の注意事項に従ってください。

- RSPAN VLAN 上のトラフィックは、VSPAN セッションではモニタされません。
- モニタ対象の 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、モニタされません。

- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN のトラフィックは、モニタ中の送信元に追加または削除されます。
- VLAN プルーニングと VLAN 許可リストは、SPAN モニタでは無効です。
- VSPAN がモニタリングするのはスイッチに入るトラフィックに限られ、VLAN 間でルーティングされるトラフィックはモニタリングしません。たとえば、VLAN が受信でモニタされ、マルチレイヤ スイッチが別の VLAN からのトラフィックをモニタ対象の VLAN にルーティングする場合、そのトラフィックはモニタ対象とはならず、SPAN 宛先ポート上で受信されません。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニタできるのは、イーサネット VLAN だけです。

SPAN トラフィック

ローカル SPAN を使用すると、マルチキャスト パケットおよびブリッジ プロトコル データ ユニット（BPDU）パケットをはじめ、Cisco Discovery Protocol（CDP）、VLAN Trunk Protocol（VTP）、ダイナミック トランキング プロトコル（DTP）、スパニングツリー プロトコル（STP）、ポート集約プロトコル（PAgP）の各パケットを含む、すべてのネットワーク トラフィックを監視できます。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.43-18）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、送信元 a1 受信モニタおよび a2 受信 / 送信モニタから宛先ポート d1 まで、双方向（受信と送信の両方）SPAN セッションが設定されているとします。パケットが a1 からスイッチに入り、a2 へスイッチングされると、着信パケットおよび発信パケットの両方が宛先ポート d1 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、付加されたレイヤ 3 情報のため異なるパケットになります）。

SPAN と RSPAN のセッション限度

入力送信元を含む同時 SPAN セッションを最大 8 つ設定できます。また、出力送信元を含む同時セッションを最大 8 つ設定できます。双方向送信元は、入力と出力の両方として数えます。RSPAN 宛先セッションは、入力側送信元を含むセッションとして数えます。

SPAN および RSPAN のデフォルト設定

表 43-1 に、SPAN および RSPAN のデフォルト設定を示します。

表 43-1　SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
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**）
フィルタ	すべての VLAN、すべてのパケット タイプ、すべてのアドレス タイプ
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 ヘッダーなし）
入力転送（宛先ポート）	ディセーブル
ホスト学習（宛先ポート）	ディセーブル

SPAN の設定

ここでは、SPAN を設定する方法について説明します。

（注）　SPAN コンフィギュレーション コマンドを入力しても、すでに設定された SPAN パラメータはクリアされません。設定済みの SPAN パラメータを消去するには、**no monitor session** コマンドを使用する必要があります。

SPAN 設定時の注意事項および制約事項

SPAN を設定する際、次の注意事項および制約事項に従ってください。

- ネットワーク アナライザを使用して、インターフェイスをモニタリングする必要があります。
- SPAN セッションでは、送信元 VLAN とフィルタ VLAN を混在させることはできません。送信元 VLAN またはフィルタ VLAN を使用することはできますが、両方を同時には使用できません。
- EtherChannel インターフェイスを、SPAN 送信元インターフェイスにできますが、SPAN 宛先インターフェイスにできません。
- 送信元インターフェイスを指定し、トラフィック タイプ（Tx、Rx、または both）を指定しなかった場合、デフォルトで「both」が使用されます。
- 複数の SPAN 送信元インターフェイスを指定する場合、各インターフェイスはそれぞれ異なる VLAN に属していてもかまいません。
- **no monitor session** *number* コマンドを他のパラメータを指定せずに入力して、SPAN のセッション*番号*をクリアする必要があります。
- **no monitor** コマンドを実行すると、すべての SPAN セッションがクリアされます。
- SPAN 宛先は、スパニングツリー インスタンスに参加しません。SPAN はモニタ対象トラフィックに BPDU を含みます。したがって、SPAN 宛先上で検出される BPDU は、SPAN 送信元からのものです。
- SPAN 宛先ポートは 1 セッションにつき 1 つに制限されています。

SPAN 送信元の設定

SPAN セッションの送信元を設定するには、次の作業を行います。

コマンド	目的
Switch(config)# [**no**] **monitor session** {*session_number*} {**source** {**interface** <*interface_list*> | {**vlan** *vlan_IDs* | **cpu** [**queue** *queue_ids*] } [**rx** | **tx** | **both**]	SPAN セッション番号（1 ～ 6）、送信元インターフェイス（FastEthernet または GigabitEthernet）、VLAN（1 ～ 4094）、CPU から送受信されたトラフィックがセッションの宛先にコピーされるかどうか、および監視するトラフィックの方向を指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface-list* 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。 *vlan_IDs* には、送信元 VLAN を指定します。 *queue_ids* には、関連するキューを指定します。 （任意）**[,** | **-]** には、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。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを 1 つ入れます。 （任意）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い場合、送信元インターフェイスは、送信（tx）と受信（rx）の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけをモニタリングします。 • **rx**：受信トラフィックをモニタリングします。 • **tx**：送信トラフィックをモニタリングします。 • **both**：送受信両方のトラフィック（双方向）をモニタリングします。 キューは、番号または名前のどちらかによって識別されます。キュー名には、便宜上、複数の番号付けキューを組み入れることができます。 デフォルトの設定に戻すには、**no** キーワードを使用します。

次に、SPAN セッション 1 で、送信元ファスト イーサネット インターフェイス 5/1 からの双方向トラフィックをモニタリングするように設定する例を示します。

```
Switch(config)# monitor session 1 source interface fastethernet 5/1
```

次に、SPAN セッション内で送信元を異なる方向に設定する例を示します。

```
Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)#
```

SPAN 宛先の設定

SPAN セッションの宛先を設定するには、次の作業を行います。

コマンド	目的
Switch(config)# [**no**] **monitor session** <*session_number*> **destination interface** <interface> [**encapsulation {isl** | **dot1q**}] [**ingress** [**vlan** *vlan_IDs*] [**learning**}]	SPAN セッション番号（1 ～ 6）および宛先インターフェイスまたは VLAN を指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface* には、宛先インターフェイスを指定します。 *vlan_IDs* には、宛先 VLAN を指定します。 デフォルトの設定に戻すには、**no** キーワードを使用します。

（注）　SPAN 宛先ポートは 1 セッションにつき 1 つに制限されています。

次に、SPAN セッション 1 の宛先として、ファスト イーサネット インターフェイス 5/48 を設定する例を示します。

```
Switch(config)# monitor session 1 destination interface fastethernet 5/48
```

トランク インターフェイス上の送信元 VLAN のモニタリング

SPAN 送信元がトランク インターフェイスである場合、特定の VLAN をモニタリングするには、次の作業を行います。

コマンド	目的
`Switch(config)# [no] monitor session {session_number} filter {vlan vlan_IDs [, | - ]} | {packet-type {good | bad}} | {address-type {unicast | multicast | broadcast} [rx | tx | both]}`	SPAN 送信元がトランク インターフェイスである場合に、特定の VLAN をモニタリングします。filter キーワードで、指定された VLAN 上のトラフィックにモニタリングを限定します。これは通常、トランク インターフェイスをモニタリングする場合に使用します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *vlan_IDs* には、VLAN を指定します。 指定された VLAN のすべてのポートを介したモニタが設定されます。 デフォルトの設定に戻すには、**no** キーワードを使用します。

次に、SPAN 送信元がトランク インターフェイスである場合に、VLAN 1 ～ 5 および 9 をモニタリングする例を示します。

```
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
```

設定例

この章で説明したコマンドを使用して SPAN セッションを完全に設定する例、および設定を解除する例を示します。送信元インターフェイス FastEthernet 4/10 からの双方向トラフィックを監視すると想定します。このインターフェイスは、VLAN 1 ～ 4094 を伝送するトランク インターフェイスとして設定されています。また、そのトランクの VLAN 57 上のトラフィックだけを監視対象とします。宛先インターフェイスとして FastEthernet 4/15 を使用し、次のコマンドを入力します。

```
Switch(config)# monitor session 1 source interface fastethernet 4/10
Switch(config)# monitor session 1 filter vlan 57
Switch(config)# monitor session 1 destination interface fastethernet 4/15
```

これで、VLAN 57 上のファスト イーサネット インターフェイス 4/10 からのトラフィックが、ファスト イーサネット インターフェイス 4/15 でモニタされます。SPAN セッションをディセーブルにする場合は、次のコマンドを入力します。

```
Switch(config)# no monitor session 1
```

SPAN の設定の確認

次に、SPAN セッション 2 の設定を確認する例を示します。

```
Switch# show monitor session 2
Session 2
---------
Source Ports:
```

```
    RX Only:        Fa5/12
    TX Only:        None
    Both:           None
Source VLANs:
    RX Only:        None
    TX Only:        None
    Both:           None
Destination Ports: Fa5/45
Filter VLANs:      1-5,9
Switch#
```

CPU ポートのスニッフィング

SPAN セッションを設定する場合は、CPU（または CPU キューのサブセット）を SPAN 送信元として指定できます。キューは、番号または名前のどちらかで指定されます。このような送信元が指定されると、指定された 1 つのキューを介して CPU に送信されるトラフィックはミラーリングされ、セッションの SPAN 宛先ポートから送信されます。このトラフィックには、（ソフトウェア転送による）CPU で送受信される制御パケットと通常のデータ パケットの両方が含まれます。

CPU 送信元を通常のポート送信元または VLAN 送信元と組み合わせることができます。

CPU 送信元のスニッフィングを設定するには、次の作業を行います。

コマンド	目的
`Switch(config)# [no] monitor session {session_number} {source {interface interface_list | {vlan vlan_IDs | cpu [queue queue_ids] } [rx | tx | both]`	CPU に送受信されたトラフィックを CPU がセッションの宛先にコピーするように指定します。queue 識別子は、指定された CPU キューで受信されたスニッフィングだけのトラフィックを任意で許可します。 *session_number* には、この SPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface-list* 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。 *vlan_IDs* には、送信元 VLAN を指定します。 *queue_ids* には、関連するキューを指定します。 （任意）**[,|-]** には、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。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを 1 つ入れます。 （任意）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い場合、送信元インターフェイスは、送信（tx）と受信（rx）の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけをモニタリングします。 • **rx**：受信トラフィックをモニタリングします。 • **tx**：送信トラフィックをモニタリングします。 • **both**：送受信両方のトラフィック（双方向）をモニタリングします。 キューは、番号または名前のどちらかによって識別されます。キュー名には、便宜上、複数の番号付けキューを組み入れることができます。 デフォルトの設定に戻すには、**no** キーワードを使用します。

次に、CPU によって受信されたすべてのパケットをスニッフィングする CPU 送信元を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source cpu rx
```

次に、Supervisor Engine 2+ から V 10-GE で、SPAN 送信元として CPU のキュー名およびキュー番号の範囲を使用する例を示します。

```
Switch(config)# monitor session 2 source cpu queue control-packet rx
Switch(config)# monitor session 3 source cpu queue 21 -23 rx
```

次の例では、Supervisor Engine 6-E の SPAN 送信元として CPU のキュー名とキュー番号範囲を使用する方法を示します。

```
Switch(config)# monitor session 2 source cpu queue control-packet rx
Switch(config)# monitor session 3 source cpu queue 10 rx
```

（注）　Supervisor Engine 6-E の場合、*control-packet* がキュー 10 にマッピングされます。

カプセル化の設定

SPAN 宛先ポートを設定する場合、ポートで使用するカプセル化タイプを明示的に指定できます。ポートに送信されるパケットは、指定されたモードに基づいてタグ付けされます （また、入力パケット オプションがイネーブルにされている場合、カプセル化モードは、タグ付けされたパケットが処理される方法を制御します）。Catalyst 4500 シリーズ スイッチのスーパーバイザ エンジンでは、ISL カプセル化、802.1Q カプセル化、およびタグなしパケットがサポートされています。

（注）　Superviso Engine 6-E は、802.1q カプセル化*だけ*をサポートします。

「複製」カプセル化タイプはサポートされていません（このタイプでは、元のパケットに適用されたカプセル化を使用してパケットが宛先ポートから送信されます）。カプセル化モードが指定されていない場合、ポートのデフォルトはタグなしです。カプセル化設定の動作については、下記のコマンドの表を参照してください。

入力パケット

入力がイネーブルにされている場合、SPAN 宛先ポートは（指定されたカプセル化モードによってタグ付けされている可能性のある）着信パケットを受け入れ、通常どおりスイッチングします。SPAN 宛先ポートを設定する場合、入力機能がイネーブルにされているか否か、およびタグなし入力パケットをスイッチングするのに使用する VLAN について指定できます （すべての ISL カプセル化パケットに VLAN タグが付加されている場合は、入力 VLAN を指定する必要がありません）。ポートは STP フォワーディング ステートですが、STP には参加しないため、スパニングツリー ループがネットワークに生じないように、この機能を設定する場合は注意してください。入力およびトランク カプセル化の両方が SPAN 宛先ポート上で指定されている場合、すべてのアクティブ VLAN でポートが転送を行います。存在しない VLAN を入力 VLAN として設定することはできません。

デフォルトでは、ホスト学習は入力がイネーブルに設定された SPAN 宛先ポート上でディセーブルに設定されています。また、このポートは VLAN のフラッディング セットから削除されるので、通常のトラフィックは宛先ポートからスイッチングされません。ただし、学習がイネーブルに設定されている場合は、宛先ポート上で学習されたホストのトラフィックが宛先ポートからスイッチングされます。SPAN 宛先ポートに接続されているホストは、ブロードキャスト ARP 要求を受信しないため、応答しません。また、SPAN 宛先ポート上にスタティック ホスト エントリ（スタティック ARP エントリおよび MAC アドレス テーブルのスタティック エントリを含む）を設定することもできます。

（注）　設定は、SPAN セッションに送信元が設定されていない場合は機能しません。このセッションは、SPAN 宛先ポートだけでは、半分しか設定されていないことになります。

入力パケットとカプセル化を設定するには、次の作業を行います。

コマンド	目的
`Switch(config)# [no] monitor session <session_number> destination interface <interface> [encapsulation {isl | dot1q}] [ingress [vlan vlan_IDs] [learning]]`	入力パケットの設定と宛先ポートのカプセル化タイプを指定します。 （注）　**isl** キーワードは、Supervisor Engine 6-E ではサポート*されません*。 *session_number* には、この SPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface* には、宛先インターフェイスを指定します。 *vlan_IDs* には、宛先 VLAN を指定します。 デフォルトの設定に戻すには、**no** キーワードを使用します。

次に、ネイティブ VLAN 7 を使用して、宛先ポートに 802.1Q カプセル化と入力パケットを設定する例を示します。

```
Switch(config)# monitor session 1 destination interface fastethernet 5/48
encapsulation dot1q ingress vlan 7
```

この設定では、セッション 1 に対応付けられた SPAN 送信元からのトラフィックは、802.1Q カプセル化を使用して、ファスト イーサネット インターフェイス 5/48 からコピーされます。着信トラフィックは、タグなしパケットが VLAN 7 に分類されてから、受け入れられてスイッチングされます。

アクセス リスト フィルタリング

SPAN セッションを設定する場合、アクセス リスト フィルタリングを適用できます。アクセス リスト フィルタリングは、出力方向または入力方向でスニッフィングされた SPAN 宛先ポートを通過するすべてのパケットに適用されます。アクセス リスト フィルタは、ローカル SPAN セッションでだけ許可されます。SPAN の宛先が RSPAN VLAN である場合、アクセス リスト フィルタは拒否されます。

（注）　アクセス リスト フィルタリングは、Cisco IOS Release 12.2(20)EW 以降で使用できます。

アクセス コントロール リスト（ACL）設定時の注意事項

SPAN セッション上で ACL を設定できます。ACL/SPAN セッションでは、次の注意事項に従ってください。

- ACL が SPAN セッションに関連付けられている場合、ACL に関連付けられるルールは、SPAN 宛先インターフェイスに存在するすべてのパケットに対して適用されます。それまで SPAN 宛先インターフェイスに関連付けられていた他の VACL または RACL に関連するルールは、適用されません。
- SPAN セッションに関連付けできる ACL は 1 つだけです。
- SPAN 宛先インターフェイスに存在するパケットに ACL が適用されていない場合、それまで宛先インターフェイスまたは SPAN 宛先インターフェイスが所属する VLAN に適用されていた PACL、VACL、または RACL に関係なく、すべてのトラフィックが許可されます。
- ACL が SPAN セッションから削除されると、すべてのトラフィックが再び許可されます。
- SPAN セッションから SPAN 設定が削除されると、SPAN 宛先インターフェイスに関連付けられたすべてのルールが、再び適用されます。
- SPAN 宛先ポートが、トランクポートとして設定され、所属する VLAN に関連付けられた ACL が設定されている場合、トラフィックは VACL の対象となりません。
- ACL 設定は通常、RSPAN VLAN、および RSPAN VLAN を伝送するトランク ポートに適用されます。この設定により、ユーザは RSPAN VLAN 上の VACL を適用できるようになります。ユーザが、宛先ポートを RSPAN VLAN として、SPAN セッション上で ACL の設定を試みる場合、この設定は拒否されます。
- CAM（連想メモリ）が過負荷状態で、パケットが検索のために CPU に引き渡される場合、SPAN セッションに関連付けられた出力ポートの ACL はいずれも、適用されません。
- ACL が作成される前に、名前つき IP ACL が SPAN セッション上で設定される場合、この設定は受け入れられ、ソフトウェアは ACE なしで空の ACL を作成します （空の ACL は、すべてのパケットを許可します）。その後、ACL にルールを追加できます。
- SPAN セッションに関連付けられた ACL は、出力宛先インターフェイス上で適用されます。
- SPAN ポートに存在するトラフィックでは、ポリシングが許可されません。
- SPAN セッションでは、IP ACL だけがサポートされます。

アクセス リスト フィルタリングの設定

アクセス リスト フィルタリングを設定するには、次の作業を行います。

コマンド	目的
`Switch(config)# [no] monitor session {session_number} filter {ip access-group [name | id] }{vlan vlan_IDs [, | - ] } | {packet-type {good | bad}} | {address-type {unicast | multicast | broadcast} [rx | tx | both]}`	アクセス リストに基づいて、フィルタ スニッフィングを指定します。 *session_number* には、この SPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 アクセス リストには、名前または数値の ID のいずれかを指定できます。 *name* には、IP アクセス リスト名を指定します。 *id* には、標準の <1 ～ 199> または拡張の <1300 ～ 2699> の IP アクセス リストを指定します。

（注）　IP アクセス リストは、「Configuring Network Security with ACL」の章に説明されているように、コンフィギュレーション モードで作成する必要があります。

次に、SPAN セッション上で IP アクセス グループ 10 を設定し、アクセス リストが設定されたことを確認する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source interface fa6/1 both
Switch(config)# monitor session 1 destination interface fa6/2
Switch(config)# monitor session 1 filter vlan 1
Switch(config)# monitor session 1 filter ip access-group 10
Switch(config)# exit
Switch# show monitor

Session 1
---------
Type              : Local Session
Source Ports      :
    Both          : Fa6/1
Destination Ports : Fa6/2
    Encapsulation : Native
          Ingress : Disabled
        Learning  : Disabled
Filter VLANs      : 1
IP Access-group   : 10
```

パケット タイプ フィルタリング

SPAN セッションを設定する場合、VLAN フィルタに類似したパケット フィルタ パラメータを指定できます。パケット フィルタを指定した場合、パケット フィルタはスニッフィングされるパケットのタイプを表示します。パケット フィルタが指定されていない場合、すべてのタイプのパケットがスニッフィングされます。別のタイプのパケット フィルタが入力および出力トラフィックに指定される場合もあります。

パケット フィルタリングは、パケットベース（good、error）またはアドレスベース（unicast/multicast/broadcast）の 2 つのカテゴリに分類されます。パケットベースのフィルタは、入力方向だけに適用できます。パケットは、宛先アドレスに基づいたハードウェアによって、ブロードキャスト、マルチキャスト、またはユニキャストに分類されます。

（注）　両方のタイプのフィルタが設定されると、両方のフィルタを通過するパケットだけがスパニングされます。たとえば、「error」と「multicast」の両方を設定すると、エラーのあるマルチキャスト パケットだけがスパニングされます。

パケット タイプ フィルタリングを設定するには、次の作業を行います。

コマンド	目的
Switch(config)# [**no**] **monitor session** {*session_number*} **filter** {**vlan** *vlan_IDs* [, | -] } | {**packet-type** {**good** | **bad**}} | {**address-type** {**unicast** | **multicast** | **broadcast**} **[rx** | **tx** | **both**]}	指定された方向による指定されたパケット タイプのフィルタ スニッフィングを指定します。 *session_number* には、この SPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *vlan_IDs* には、VLAN を指定します。 rx と tx タイプの両方のフィルタ設定をすると同時に、複数のタイプのフィルタを設定できます（たとえば、**good** と **unicast** を設定して、エラーがないユニキャスト フレームだけをスニッフィングします）。VLAN フィルタでは、タイプまたはフィルタが指定されていない場合、すべてのパケット タイプがスニッフィングされます。 デフォルトの設定に戻すには、**no** キーワードを使用します。

次に、入力方向のユニキャスト パケットだけを受け入れるようにセッションを設定する例を示します。

```
Switch(config)# monitor session 1 filter address-type unicast rx
```

設定例

次に、SPAN 拡張機能の一部を使用した SPAN の設定例を示します。

次の例では、インターフェイス Gi1/1 上に着信するユニキャスト トラフィックをスニッフィングするようにセッションを設定します。トラフィックは、ISL カプセル化を使用して、インターフェイス Gi1/2 からミラーリングされます。入力トラフィックが許可されます。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source interface gi1/1 rx
Switch(config)# monitor session 1 destination interface gi1/2 encapsulation isl ingress
Switch(config)# monitor session 1 filter address-type unicast rx
Switch(config)# exit
Switch# show monitor

Session 1
---------
Type              : Local Session
Source Ports      :
    RX Only       : Gi1/1
Destination Ports : Gi1/2
    Encapsulation : ISL
          Ingress : Enabled
         Learning : Disabled
Filter Addr Type  :
    RX Only       : Unicast
```

RSPAN の設定

（注）　この機能は、Supervisor Engine 6-E ではサポートされていません。

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。具体的な設定情報は次のとおりです。

RSPAN 設定時の注意事項

RSPAN を設定するときには、次の注意事項に従ってください。

（注）　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一部確保します。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。

（注）　RSPAN トラフィックに出力アクセス コントロール リスト（ACL）を適用して、特定のパケットを選択的にフィルタリングまたはモニタリングできます。RSPAN 送信元スイッチ内の RSPAN VLAN 上で、これらの ACL を指定します。

- RSPAN セッションは、「SPAN と RSPAN のセッション限度」（P.43-6）に記載された限度内であれば、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 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。
- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生するのを防ぐため、参加しているすべてのスイッチで RSPAN VLAN 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 ポートは自動的にディセーブルになります。
- 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します。
- 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ッディングが防止されます。

- RSPAN トラフィックは RSPAN VLAN のネットワーク上で伝送されるため、ミラーリングされたパケットの元の VLAN アソシエーションは失われます。したがって、RSPAN では、IDS デバイスからユーザが指定した単一 VLAN へのトラフィック転送だけをサポートしています。

RSPAN セッションの作成

最初に、RSPAN に参加させる予定のスイッチのいずれにおいても、RSPAN セッション用として存在していない RSPAN VLAN を作成します。ネットワークで VTP がイネーブルになっている場合、1 つのスイッチで RSPAN VLAN を作成して、VTP がその RSPAN VLAN を、VLAN ID が 1005 未満の、VTP ドメイン内の他のスイッチに伝播させることができます。

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

RSPAN 送信元セッションを開始し、送信元（モニタ対象）ポートおよび宛先 RSPAN VLAN を指定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# no monitor session {session_number | all | local | remote}`	セッションの既存の RSPAN 設定をクリアします。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 すべての RSPAN セッションを削除するには **all** を、すべてのローカル セッションを削除するには **local** を、すべてのリモート SPAN セッションを削除するには **remote** を指定します。
ステップ 3	`Switch(config)# vlan {remote_vlan_ID}`	リモート VLAN ID を指定します。 この VLAN ID がユーザ トラフィックで使用されていないことを確認してください。
ステップ 4	`Switch(config-vlan)# remote-span`	VLAN ID をリモート VLAN ID に変換します。
ステップ 5	`Switch(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。

	コマンド	目的
ステップ 6	`Switch(config)# [no] monitor session {session_number} {source {interface <interface_list> | {vlan vlan_IDs | cpu [queue queue_ids]}} [rx | tx | both]`	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。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface-list* 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。 *vlan-IDs* には、1 つまたは複数のモニタ対象送信元 VLAN を指定します。有効な VLAN の範囲は、1 ～ 4094 です。 *queue_ids* には、一連の CPU キュー識別番号（1 ～ 32）または名前指定のキューのどちらかを指定します。 （任意）**[,** | **-]** には、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。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを 1 つ入れます。 （任意）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い場合、送信元インターフェイスは、送信（tx）と受信（rx）の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけをモニタリングします。 • **rx**：受信トラフィックをモニタリングします。 • **tx**：送信トラフィックをモニタリングします。 • **both**：送受信両方のトラフィック（双方向）をモニタリングします。
ステップ 7	`Switch(config)# monitor session session_number destination remote vlan vlan-ID`	RSPAN セッションと宛先リモート VLAN を指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *vlan-ID* には、モニタ対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。
ステップ 8	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 9	`Switch# show monitor [session session_number]`	入力を確認します。
ステップ 10	`Switch# 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 の既存の RSPAN 設定をクリアし、複数の送信元インターフェイスをモニタリングする RSPAN セッション 1 を設定し、宛先 RSPAN VLAN を設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no monitor session 1
Switch(config)# monitor session 1 source interface fastEthernet3/10 tx
Switch(config)# monitor session 1 source interface fastEthernet3/2 rx
Switch(config)# monitor session 1 source interface fastEthernet3/3 rx
Switch(config)# monitor session 1 source interface port-channel 102 rx
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、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# monitor session` *session_number* `source remote vlan` *vlan-ID*	RSPAN セッションと送信元 RSPAN VLAN を指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *vlan-IDs* 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 3	`Switch(config)# [no] monitor session` <*session_number*> `destination interface` <*interface*> `[encapsulation {isl | dot1q}] [ingress [vlan` *vlan_IDs*`] [learning]]`	RSPAN セッションと宛先インターフェイスを指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface* には、宛先インターフェイスを指定します。 *vlan_IDs* には、必要に応じて、入力 VLAN を指定します。 （任意）**[,** | **-]** には、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。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを 1 つ入れます。 （任意）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、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。追加の送信元ポートは、受信（**rx**）トラフィックだけをモニタリングします。 • **isl**：ISL カプセル化を使用します。 • **dot1q**：802.1Q カプセル化を使用します。
ステップ 4	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Switch# show monitor [session` *session_number*`]`	入力を確認します。
ステップ 6	`Switch# 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、VLAN 901 を送信元リモート VLAN に、ポート 5 を宛先インターフェイスに設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitEthernet1/2
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イネーブル化

RSPAN 宛先セッションを作成して、送信元 RSPAN VLAN を指定し、ネットワーク セキュリティ デバイス（Cisco IDS センサー装置など）用に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、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# monitor session {session_number} source vlan vlan_IDs`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *vlan_IDs* には、1 つまたは複数のモニタ対象送信元 VLAN を指定します。有効な VLAN の範囲は、1 ～ 4094 です。
ステップ 3	`Switch(config)# [monitor session session_number destination interface interface-id [encapsulation {dot1q [ingress vlan vlan id] | ISL [ingress]} | ingress vlan vlan id] [learning]]`	RSPAN セッション、宛先ポート、パケット カプセル化、および入力側 VLAN を指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface-id* には、宛先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などです。 （任意）RSPAN 宛先ポート上で送信されるパケットのカプセル化を指定します。カプセル化タイプが指定されていない場合、すべての送信パケットはネイティブ形式（タグなし）で送信されます。 • タグなしのネイティブ VLAN パケットと、他のすべての **dot1q** タグ付き VLAN **tx** パケットを送信する場合は、**encapsulation dot1q** と入力します。 • ISL を使用してカプセル化されたすべての **tx** パケットを送信する場合は、**encapsulation isl** を入力します。 （任意）RSPAN 宛先ポート上で入力トラフィックの転送をイネーブルにするか否かを指定します。 • ネイティブ（タグなし）および **dot1q** カプセル化の場合、**ingress vlan** *vlan id* を指定し、*vlan id* をネイティブ VLAN として入力転送をイネーブルにします。また、*vlan id* は、送信パケット用のネイティブ VLAN としても使用されます。 • ISL カプセル化を使用する場合、**ingress** を指定して入力転送をイネーブルにします。 • 入力がイネーブルの場合、**learning** を指定して学習をイネーブルにします。
ステップ 4	`Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	`Switch# show monitor [session session_number]`	入力を確認します。
ステップ 6	`Switch# 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、送信元リモート VLAN として VLAN 901 を設定し、802.1Q カプセル化をサポートするセキュリティ デバイスを使用して VLAN 5 上の入力トラフィック用の宛先ポートを設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# monitor session 1 source remote vlan 901
Switch(config)# monitor session 1 destination interface gigabitEthernet1/2 ingress vlan 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、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# **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	Switch(config)# [**no**] **monitor session** {*session_number*} {**source** {**interface** *interface_list* | {**vlan** *vlan_IDs* | **cpu** [**queue** *queue_ids*]} [**rx** | **tx** | **both**]	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。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface-list* には、モニタリング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。 *vlan_IDs* には、1 つまたは複数のモニタ対象送信元 VLAN を指定します。有効な VLAN の範囲は、1 ～ 4094 です。 *queue_ids* には、一連の CPU キュー識別番号（1 ～ 32）または名前指定のキューのどちらかを指定します。 （任意）**[,** | **-]** には、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。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを 1 つ入れます。 （任意）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い場合、送信元インターフェイスは、送信（tx）と受信（rx）の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけをモニタリングします。 • **rx**：受信トラフィックをモニタリングします。 • **tx**：送信トラフィックをモニタリングします。 • **both**：送受信両方のトラフィック（双方向）をモニタリングします。
ステップ 3	Switch(config)# **end**	特権 EXEC モードに戻ります。
ステップ 4	Switch# **show monitor** [**session** *session_number*]	入力を確認します。
ステップ 5	Switch# **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、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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no monitor session 1 source interface gigabitEthernet1/1
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 gigabitEthernet1/1 rx
```

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

モニタリングする VLAN の指定

VLAN のモニタは、ポートのモニタリングと類似しています。モニタリングする VLAN を指定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# no monitor session {`*session_number* `| all | local | remote}`	セッションの既存の SPAN 設定をすべてクリアします。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。

	コマンド	目的
ステップ 3	Switch(config)# [**no**] **monitor session** {*session_number*} {**source** {**interface** *interface_list* | {**vlan** *vlan_IDs* | **cpu** [**queue** *queue_ids*]} [**rx** | **tx** | **both**]	RSPAN セッションおよび送信元 VLAN（モニタ対象ポート）を指定します。モニタリングできるのは、VLAN 上の受信（**rx**）トラフィックだけです *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface-list* には、モニタリング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。 *vlan-IDs* の範囲は 1 ～ 4094 です。先行 0 は入力しないでください。 *queue_ids* には、送信元キューを指定します。 （任意）**[,** | **-]** には、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。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを 1 つ入れます。 （任意）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い場合、送信元インターフェイスは、送信（tx）と受信（rx）の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけをモニタリングします。 • **rx**：受信トラフィックをモニタリングします。 • **tx**：送信トラフィックをモニタリングします。 • **both**：送受信両方のトラフィック（双方向）をモニタリングします。
ステップ 4	Switch(config)# **monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションと宛先リモート VLAN を指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *vlan-id* には、モニタ対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。
ステップ 5	Switch(config)# **end**	特権 EXEC モードに戻ります。
ステップ 6	Switch# **show monitor** [**session** *session_number*]	入力を確認します。
ステップ 7	Switch# **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 セッションから 1 つまたは複数の送信元 VLAN を削除するには、**no monitor session** *session_number* **source vlan** *vlan-id* **rx** 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 の既存の設定をすべてクリアし、VLAN 1 ～ 3 に所属するすべてのポート上で受信トラフィックをモニタリングする RSPAN セッション 2 を設定し、宛先リモート VLAN 902 に送信する例を示します。この設定は次に、VLAN 10 に所属するすべてのポートで受信トラフィックをモニタリングするように変更されています。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source vlan 1 - 3 rx
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# monitor session 2 source vlan 10 rx
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 に制限するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Switch# 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	`Switch(config)# no monitor session {session_number | all | local | remote}`	セッションの既存の SPAN 設定をすべてクリアします。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 すべての SPAN セッションを削除する場合は **all**、すべてのローカル セッションを削除する場合は **local**、すべてのリモート SPAN セッションを削除する場合は **remote** をそれぞれ指定します。
ステップ 3	`Switch(config)# [no] monitor session {session_number} {source {interface interface_list | {vlan vlan_IDs | cpu [queue queue_ids]} [rx | tx | both]`	送信元ポート（モニタ対象ポート）と RSPAN セッションの特性を指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *interface-list* 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。 *vlan-IDs* の範囲は 1 ～ 4094 です。先行 0 は入力しないでください。 *queue_ids* には、送信元キューを指定します。 （任意）**[,** | **-]** には、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。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを 1 つ入れます。 （任意）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い場合、送信元インターフェイスは、送信（tx）と受信（rx）の両方のトラフィックを送信します。追加の送信元ポートは、受信トラフィックだけをモニタリングします。 • **rx**：受信トラフィックをモニタリングします。 • **tx**：送信トラフィックをモニタリングします。 • **both**：送受信両方のトラフィック（双方向）をモニタリングします。
ステップ 4	`Switch(config)# monitor session session_number filter vlan vlan-id [, | -]`	RSPAN 送信元トラフィックを特定の VLAN に制限します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *vlan-id* の範囲は 1 ～ 4094 です。先行 0 は入力しないでください。 （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。カンマのあとにはスペースを入れます。ハイフンの前後にはスペースを 1 つ入れます。

	コマンド	目的
ステップ 5	Switch(config)# **monitor session** *session_number* **destination remote vlan** *vlan-id*	RSPAN セッションと宛先リモート VLAN を指定します。 *session_number* には、この RSPAN セッションで識別されるセッション番号を指定します（1 ～ 6）。 *vlan-id* には、モニタ対象トラフィックを宛先ポートに伝送する RSPAN VLAN を指定します。
ステップ 6	Switch(config)# **end**	特権 EXEC モードに戻ります。
ステップ 7	Switch# **show monitor** [**session** *session_number*]	入力を確認します。
ステップ 8	Switch# **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 をモニタするには、**no monitor session** *session_number* **filter vlan** グローバル コンフィギュレーション コマンドを使用します。

次に、RSPAN セッション 2 の既存の設定をすべてクリアし、トランク ポート 4 上での受信したトラフィックをモニタリングする RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 のトラフィックだけを、宛先リモート VLAN 902 に送信する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no monitor session 2
Switch(config)# monitor session 2 source interface gigabitethernet1/1 rx
Switch(config)# monitor session 2 filter vlan 1 - 5 , 9
Switch(config)# monitor session 2 destination remote vlan 902
Switch(config)# end
```

SPAN および RSPAN 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** 特権 EXEC コマンドを使用します。

次に、SPAN 送信元セッション 1 の **show monitor** コマンドの出力例を示します。

```
Switch# show monitor session 1
Session 1
---------
Type: Local Source Session
Source Ports:
    RX Only:  Fa3/13
    TX Only:       None
    Both:          None

Source VLANs:
    RX Only:       None
    TX Only:       None
    Both:          None
Source RSPAN VLAN: None
Destination Ports: None
    Encapsulation: DOT1Q
    Ingress:Enabled, default VLAN=5
Filter VLANs:      None
Dest RSPAN VLAN: None
Ingress : Enabled, default VLAN=2
Learning : Disabled
```