SPAN および RSPAN の設定

- 機能情報の確認，1 ページ
- SPAN および RSPAN の前提条件，2 ページ
- SPAN および RSPAN の制約事項，2 ページ
- SPAN および RSPAN について，5 ページ
- SPAN および RSPAN の設定方法，19 ページ
- SPAN および RSPAN 動作のモニタリング，44 ページ
- SPAN および RSPAN の設定例，45 ページ
- その他の関連資料，47 ページ
- SPAN および RSPAN の機能の履歴と情報，49 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

SPAN および RSPAN の前提条件

SPAN

- SPAN トラフィックを特定の VLAN に制限するには、**filter vlan** キーワードを使用します。トランク ポートをモニタしている場合、このキーワードで指定された VLAN 上のトラフィックのみがモニタされます。 デフォルトでは、トランク ポート上のすべての VLAN がモニタされます。

RSPAN

- RSPAN VLAN を設定してから、RSPAN 送信元または宛先セッションを設定することを推奨します。

SPAN および RSPAN の制約事項

SPAN

- 各switchでは、最大で 8 つの送信元セッションおよび 58 の RSPAN 宛先セッションを設定できます。 送信元セッションは、ローカル SPAN セッションまたは RSPAN 送信元セッションのどちらかになります。
- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックをモニタできます。 1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- switch ポートを SPAN 宛先ポートとして設定すると、通常のswitch ポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象トラフィックのみになります。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。 設定されている SPAN パラメータを削除するには、**no monitor session** {*session_number* | **all** | **local** | **remote**} グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなしまたは IEEE 802.1Q）を伝送します。 このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。

- 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、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN がイネーブルになってからです。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。
- スタックは、LAN Base イメージを実行しているスイッチのみでサポートされています。

SPAN セッションのトラフィック モニタリングには次の制約事項があります。

- ポートまたはVLANを送信元にできますが、同じセッション内に送信元ポートと送信元VLANを混在させることはできません。
- switchは、最大 2 つのローカル SPAN または RSPAN 送信元セッションをサポートします。
  - 同じswitchまたはswitch スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。 switchまたはswitch スタックは合計 66 の送信元および RSPAN 宛先セッションをサポートします。
  - 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。 スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つの switch スタックあたりに設定できる宛先ポートは最大で 66 個です。
- SPANセッションがswitch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、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。 多数のポートまたは VLAN をモニタすると、大量のネットワーク トラフィックが生成されることがあります。
- デ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。
- switchは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じswitchまたはswitch スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

RSPAN

- RSPAN は、BPDU パケット モニタリングまたは他のレイヤ 2 switch プロトコルをサポートしません。

- RSPAN VLAN はトランク ポートにのみ設定されており、アクセス ポートには設定されていません。 不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのswitchesで VLAN RSPAN 機能がサポートされていることを確認してください。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。 また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。 ただし、switchはスパンされたトラフィックをモニタしないため、switch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。
- VTP および VTP プルーニングをイネーブルにすると、トランク内で RSPAN トラフィックがプルーニングされ、1005 以下の VLAN ID に関して、ネットワークで不必要な RSPAN トラフィックのフラッディングが防止されます。
- RSPAN を使用するには、スイッチが LAN Base イメージを実行している必要があります。

フローベースの SPAN（FSPAN）およびフローベースの RSPAN（FRSPAN）

- 複数の SPAN または RSPAN セッションに ACL をアタッチできます。 ただし、ACL のサイズは FSPAN に割り当てられたメモリ TCAM のサイズを超過することはできません。
- FSPAN ACL が接続されていない場合、FSPAN はディセーブルで、すべてのトラフィックが SPAN 宛先ポートにコピーされます。
- SPAN セッションに空の FSPAN ACL を接続すると、パケットはフィルタリングされず、すべてのトラフィックが監視されます。
- FSPAN ACL は、ポート単位 VLAN 単位のセッションに適用できません。 ポート単位 VLAN 単位のセッションは、最初にポートベースのセッションを設定し、次にセッションに特定の VLAN を設定することにより設定できます。 次に例を示します。

```
Switch(config)# monitor session session_number source interface interface-id
Switch(config)# monitor session session_number filter vlan vlan-id
Switch(config)# monitor session session_number filter ip access-group {access-list-number | name}
```

（注） **filter vlan** および **filter ip access-group** の両方のコマンドを同時に設定できません。 一方を設定すると、他方が拒否されます。

- EtherChannel は FSPAN セッションでサポートされていません。
- TCP フラグまたは **log** キーワードが付いている FSPAN ACL はサポートされていません。
- switchで拡張 IP サービス フィーチャ セットを稼働中に IPv6 FSPAN ACL を設定し、のちに異なるフィーチャ セットを稼働した場合、switchのリブート後、switchでの IPv6 FSPAN ACL 設定が失われる可能性があります。

- IPv6 FSPAN ACL は、IPv6 対応の SDM テンプレートでだけサポートされています。 IPv6 対応の SDM テンプレートを稼働中に IPv6 FSPAN ACL を設定し、のちに非 IPv6 SDM テンプレートを設定してswitchをリブートすると、IPv6 FSPAN ACL 設定が失われます。

SPAN および RSPAN について

SPAN および RSPAN

ポートまたはVLANを通過するネットワーク トラフィックを解析するには、SPANまたはRSPANを使用して、そのswitch上、またはネットワーク アナライザやその他のモニタ デバイス、あるいはセキュリティ デバイスに接続されている別のswitch上のポートにトラフィックのコピーを送信します。 SPAN は送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックを宛先ポートにコピー（ミラーリング）して、解析します。 SPAN は送信元ポートまたはVLAN 上のネットワーク トラフィックのスイッチングには影響しません。 宛先ポートはSPAN専用にする必要があります。 SPAN または RSPAN セッションに必要なトラフィック以外、宛先ポートがトラフィックを受信したり転送したりすることはありません。

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

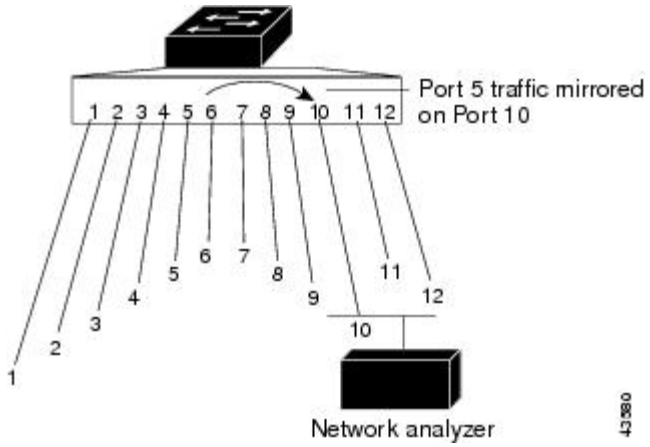
ネットワーク セキュリティ デバイスからトラフィックを注入する場合、SPAN または RSPAN 宛先ポートを使用できます。 たとえば、Cisco侵入検知システム（IDS）センサー装置を宛先ポートに接続した場合、IDSデバイスはTCPリセットパケットを送信して、疑わしい攻撃者のTCPセッションを停止させることができます。

ローカル SPAN

ローカル SPAN は 1 つのswitch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switchまたはswitch スタック内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。

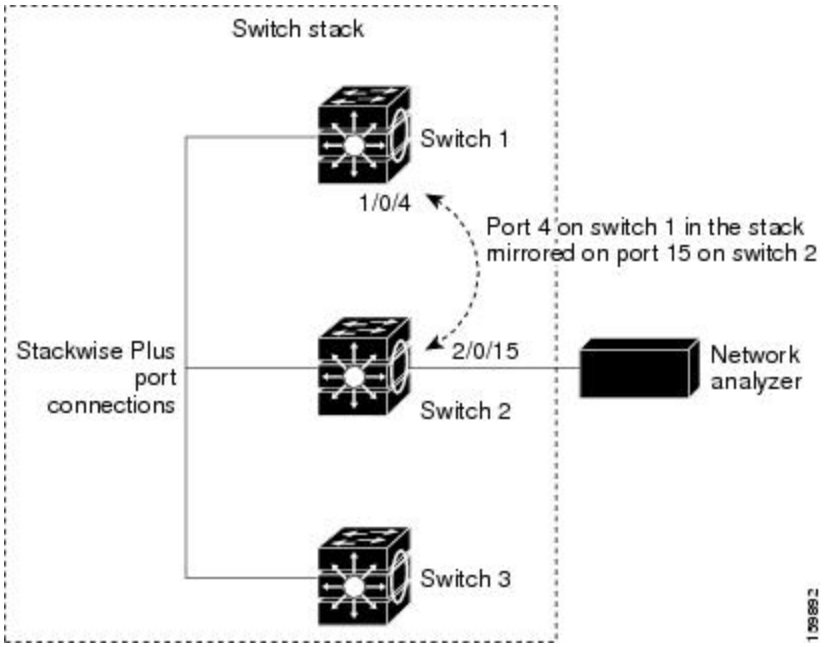
ポート 5（送信元ポート）上のすべてのトラフィックがポート 10（宛先ポート）にミラーリングされます。 ポート 10 のネットワーク アナライザは、ポート 5 に物理的には接続されていませんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。

図 *1*：単一デバイスでのローカル *SPAN* の設定例



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

図 *2*：デバイス スタックでのローカル *SPAN* の設定例



関連トピック

ローカル SPAN セッションの作成, （19 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定, （22 ページ）

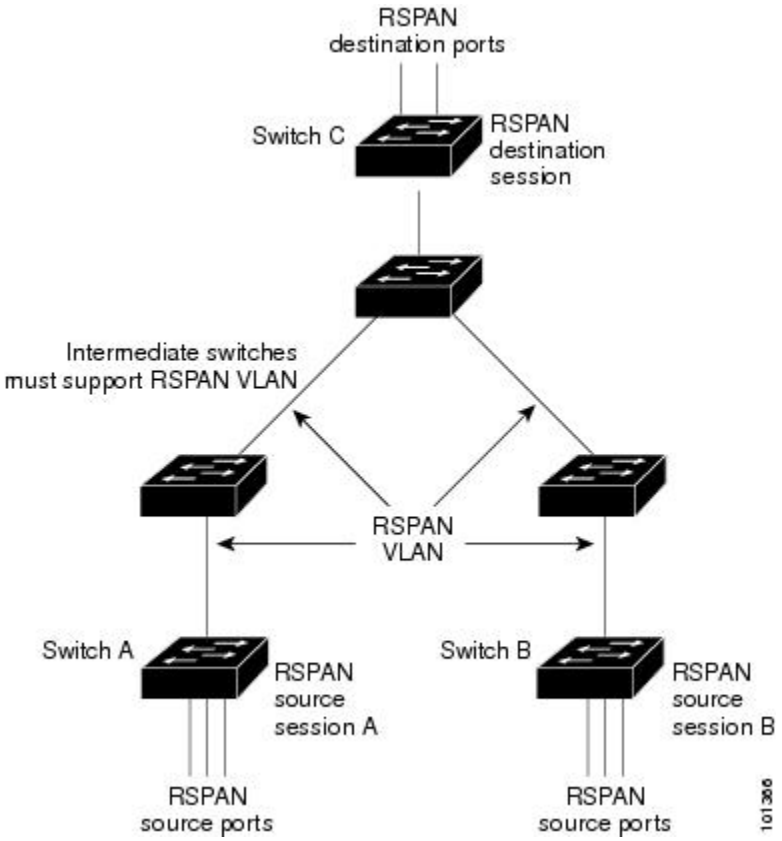
例：ローカル SPAN の設定, （45 ページ）

リモート SPAN

RSPAN は、異なるswitches（または異なるswitch スタック）上の送信元ポート、送信元 VLAN、および宛先ポートをサポートしているので、ネットワーク上で複数のswitchesをリモートモニタリングできます。

次の図に、Switch A およびSwitch B の送信ポートを示します。 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switchesで RSPAN セッション専用です。 送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランク ポートを介して、RSPAN VLAN をモニタする宛先セッションに転送されます。 各 RSPAN 送信元switchには、ポートまたは VLAN のいずれかが RSPAN 送信元として必要です。 図中のSwitch C のように、宛先は常に物理ポートになります。

図 *3*：*RSPAN* の設定例



関連トピック

RSPAN 送信元セッションの作成, （29 ページ）
RSPAN 宛先セッションの作成, （33 ページ）

RSPAN 宛先セッションの作成および着信トラフィックの設定, （36 ページ）
例：RSPAN VLAN の作成, （46 ページ）

SPAN と RSPAN の概念および用語

• SPAN セッション
• 監視対象トラフィック
• 送信元ポート
• 送信元 VLAN
• VLAN フィルタリング
• 宛先ポート
• RSPAN VLAN

SPAN セッション

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

ローカルSPANセッションは、宛先ポートと送信元ポートまたは送信元VLAN（すべて単一のネットワーク デバイス上にある）を結び付けたものです。 ローカル SPAN には、個別の送信元および宛先のセッションはありません。 ローカル SPAN セッションはユーザ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 は少なくとも 1 つの RSPAN 送信元セッション、1 つの RSPAN VLAN、および少なくとも 1 つの RSPAN 宛先セッションで構成されています。 RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。 デバイスに RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。 このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。 別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN VLAN に関連付けます。 宛先セッションは RSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

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

RSPAN 宛先セッションは RSPAN VLAN 上で受信されたすべてのパケットを取得し、VLAN のタギングを除去し、宛先ポートに送ります。 セッションは、（レイヤ 2 制御パケットを除く）すべての RSPAN VLAN パケットのコピーを分析のためにユーザに提供します。

複数のソースおよび宛先ポートを持つ単一 RSPAN セッションを同じセッションに使用できますが、ソースが同じリモート VLAN であるソース セッションの複数使用は許可されていません。

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

- 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。
- switchは、最大 2 つのローカル SPAN または RSPAN 送信元セッションをサポートします。
  - 同じswitchまたはswitch スタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。 switchまたはswitch スタックは合計 64 の送信元および RSPAN 宛先セッションをサポートします。
  - 別個のまたは重複する SPAN 送信元ポートと VLAN のセットによって、SPAN または RSPAN 送信元セッションを 2 つ個別に設定できます。 スイッチド ポートおよびルーテッド ポートはいずれも SPAN 送信元および宛先として設定できます。
- 1 つの SPAN セッションに複数の宛先ポートを設定できますが、1 つのswitch スタックあたりに設定できる宛先ポートは最大で 64 個です。
- SPANセッションがswitch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、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN がイネーブルの場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。 したがって、多数のポートまたは VLAN をモニタすると、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。
- switchは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じswitchまたはswitch スタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

関連トピック

ローカル SPAN セッションの作成, （19 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定, （22 ページ）
例：ローカル SPAN の設定, （45 ページ）

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 タイプをモニタできます。

- 受信（Rx）SPAN：受信（または入力）SPAN は、switchが変更または処理を行う前に、送信元インターフェイスまたはVLANが受信したすべてのパケットをできるだけ多くモニタリン

グします。 送信元が受信した各パケットのコピーがその SPAN セッションに対応する宛先ポートに送られます。

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

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

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

  ルーティングが原因で変更されたパケット（存続可能時間（TTL）、MAC アドレス、QoS 値の変更など）は、宛先ポートで（変更されて）コピーされます。

  送信処理中にパケットをドロップする可能性のある機能は、SPAN 用の複製コピーにも影響します。 これらの機能には、標準および拡張 IP 出力 ACL、出力 QoS ポリシングがあります。

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

ローカル SPAN セッション ポートのデフォルト設定では、すべてのタグなしパケットが送信されます。 通常、SPAN は Cisco Discovery Protocol（CDP）、VLAN トランキング プロトコル（VTP）、Dynamic Trunking Protocol（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）などのブリッジ プロトコル データ ユニット（BPDU）パケットおよびレイヤ 2 プロトコルをモニタしません。 ただし、宛先ポートを設定するときに **encapsulation replicate** キーワードを入力すると、次の変更が発生します。

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

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

Switchの輻輳により、入力送信元ポート、出力送信元ポート、または SPAN 宛先ポートでパケットがドロップされることがあります。一般に、これらの特性は互いに無関係です。 次に例を示します。

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

- switchの輻輳が原因でドロップされた出力パケットは、出力SPANからもドロップされます。

SPANの設定によっては、同一送信元のパケットのコピーが複数、SPAN宛先ポートに送信されます。 たとえば、ポート A での RX モニタ、ポート B での TX モニタ用に、双方向（RX と TX）SPAN セッションが設定されているとします。 パケットがポート A からswitchに入ってポート B にスイッチされると、着信パケットも発信パケットも宛先ポートに送信されます。 このため、両方のパケットは同じものになります。レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります。

送信元ポート

送信元ポート（別名監視対象ポート）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モニタできます。 switchは、任意の数の送信元ポート（switchで利用可能なポートの最大数まで）と任意の数の送信元 VLAN（サポートされている VLAN の最大数まで）をサポートしています。 ただし、switchが送信元ポートまたは VLAN でサポートするセッション数には上限（2 つ）（ローカルまたは RSPAN）があります。 単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

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

送信元 VLAN

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

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブ ポートは送信元ポートとして含まれ、単一方向または双方向でモニタできます。

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

VLAN フィルタリング

トランク ポートを送信元ポートとしてモニタする場合、デフォルトでは、トランク上でアクティブなすべてのVLANがモニタされます。 VLANフィルタリングを使用して、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。

- VLAN フィルタリングが適用されるのは、トランク ポートまたは音声 VLAN ポートのみです。
- VLANフィルタリングはポートベースセッションにのみ適用され、VLAN送信元によるセッションでは使用できません。
- VLAN フィルタ リストが指定されている場合、トランク ポートまたは音声 VLAN アクセス ポートではリスト内の該当 VLAN のみがモニタされます。
- 他のポート タイプから着信する SPAN トラフィックは、VLAN フィルタリングの影響を受けません。つまり、すべての VLAN を他のポートで使用できます。
- VLAN フィルタリング機能は、宛先 SPAN ポートに転送されたトラフィックにのみ作用し、通常のトラフィックのスイッチングには影響を与えません。

宛先ポート

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

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じswitchまたはswitch スタックに存在している必要があります。 RSPAN セッションの場合は、RSPAN 宛先セッションを含むswitch上にあります。 RSPAN 送信元セッションのみを実行するswitchまたはswitch スタックには、宛先ポートはありません。
- ポートを SPAN 宛先ポートとして設定すると、元のポート設定が上書きされます。 SPAN 宛先設定を削除すると、ポートは以前の設定に戻ります。 ポートがSPAN宛先ポートとして機能している間にポートの設定が変更されると、SPAN 宛先設定が削除されるまで、変更は有効になりません。

（注） SPAN の宛先ポートに QoS が設定されている場合、QoS はただちに有効になります。

- ポートが EtherChannel グループに含まれていた場合、そのポートが宛先ポートとして設定されている間、グループから削除されます。 削除されたポートがルーテッド ポートであった場合、このポートはルーテッド ポートでなくなります。
- 任意のイーサネット物理ポートにできます。
- セキュア ポートにすることはできません。
- 送信元ポートにすることはできません。
- EtherChannel グループにすることができます。
- VLAN にすることはできません。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。 ポートは SPAN セッションに必要なトラフィック以外は送信しません。 宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニタされません。
- switchまたはswitch スタックの宛先ポートの最大数は 64 です。

ローカル SPAN および RSPAN 宛先ポートは、VLAN タギングおよびカプセル化で次のように動作が異なります。

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

RSPAN VLAN

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

- RSPAN VLAN 内のすべてのトラフィックは、常にフラッディングされます。
- RSPAN VLAN では MAC アドレスは学習されません。
- RSPAN VLAN トラフィックが流れるのは、トランク ポート上のみです。
- RSPAN VLAN は、**remote-span** VLAN コンフィギュレーション モード コマンドを使用して、VLAN コンフィギュレーション モードで設定する必要があります。
- STP は RSPAN VLAN トランク上で実行できますが、SPAN 宛先ポート上では実行できません。
- RSPAN VLAN を、プライベート VLAN のプライマリまたはセカンダリ VLAN にはできません。

VLAN トランキング プロトコル（VTP）に対して可視である VLAN 1 ～ 1005 の場合、VLAN ID および対応する RSPAN 特性は VTP によって伝播されます。 拡張 VLAN 範囲（1006 ～ 4094）内の RSPAN VLAN ID を割り当てる場合は、すべての中間switchesを手動で設定する必要があります。

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

関連トピック

RSPAN 送信元セッションの作成, （29 ページ）
RSPAN 宛先セッションの作成, （33 ページ）
RSPAN 宛先セッションの作成および着信トラフィックの設定, （36 ページ）
例：RSPAN VLAN の作成, （46 ページ）

SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッド トラフィックを監視しません。 VSPAN が監視するのは switchに出入りするトラフィックに限られ、VLAN 間でルーティングされるトラフィックは監視しません。 たとえば、VLAN が受信モニタされ、switchが別の VLAN から監視対象 VLAN にトラフィックをルーティングする場合、そのトラフィックは監視されず、SPAN 宛先ポートで受信されません。

- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。 SPAN または RSPAN セッションがディセーブルになると、宛先ポートは STP に参加できます。 送信元ポートでは、SPAN は STP ステータスに影響を与えません。 STP は RSPAN VLAN を伝送するトランク ポート上でアクティブにできます。
- CDP：SPAN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、switches間で RSPAN VLAN のプルーニングが可能です。
- VLANおよびトランキング：送信元ポート、または宛先ポートのVLANメンバーシップまたはトランクの設定値を、いつでも変更できます。 ただし、宛先ポートのVLANメンバーシップまたはトランクの設定値に対する変更が有効になるのは、SPAN 宛先設定を削除してからです。 送信元ポートの VLAN メンバーシップまたはトランクの設定値に対する変更は、ただちに有効になり、対応する SPAN セッションが変更に応じて自動的に調整されます。
- EtherChannel：EtherChannelグループを送信元ポートとして設定することはできますが、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 グループに物理ポートを追加すると、SPAN 送信元ポート リストに新しいポートが追加されます。 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。

  EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。 この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータはモニタされます。 ただし、EtherChannel グループに含まれる物理ポートを SPAN 宛先として設定した場合、その物理ポートはグループから削除されます。 SPAN セッションからそのポートが削除されると、EtherChannel グループに再加入します。 EtherChannel グループから削除されたポートは、グループ メンバのままですが、inactive または suspended ステートになります。

  EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートはEtherChannel グループおよびモニタ対象ポート リストから削除されます。
- マルチキャスト トラフィックをモニタできます。 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。
- プライベート VLAN ポートは、SPAN 宛先ポートには設定できません。
- セキュア ポートを SPAN 宛先ポートにすることはできません。

  SPAN セッションでは、入力転送が宛先ポートでイネーブルの場合、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。 RSPAN 送信元セッションでは、出力をモニタしているポートでポート セキュリティをイネーブルにしないでください。
- IEEE 802.1x ポートは SPAN 送信元ポートにできます。 SPAN 宛先ポート上で IEEE 802.1x をイネーブルにできますが、SPAN宛先としてこのポートを削除するまで、IEEE 802.1x はディセーブルに設定されます。

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

SPAN と RSPAN とデバイス スタック

switchesのスタックは1つの論理switchを表すため、ローカルSPANの送信元ポートおよび宛先ポートは、スタック内の異なるswitchesである場合があります。 したがって、スタック内でのswitchesの追加または削除は、RSPANの送信元セッションまたは宛先セッションだけではなく、ローカルSPAN セッションにも影響を及ぼします。 switchがスタックから削除されると、アクティブ セッションが非アクティブになります。また、switchがスタックに追加されると、非アクティブ セッションがアクティブになります。

フローベースの SPAN

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

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

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

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

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

セキュリティ ACL は、switch上の FSPAN ACL よりも高いプライオリティをもっています。 FSPAN ACL が適用され、その後ハードウェア メモリに収まらないセキュリティ ACL を追加する場合、適用された FSPAN ACL は、セキュリティ ACL のスペースを確保するためにメモリから削除されます。 この処理（アンローディングと呼ばれる）は、システム メッセージにより通知されます。メモリ内に常駐するスペースが確保できたら、switch上のハードウェア メモリに FSPAN ACL が

追加されます。この処理（リローディングと呼ばれる）は、システムメッセージにより通知されます。IPv4、IPv6、および MAC FSPAN ACL は、別個にアンロードまたはリロードできます。

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

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

IPv4 および MAC FSPAN ACL は、すべてのフィーチャ セットでサポートされています。IPv6 FSPAN ACL は、拡張 IP Services フィーチャ セットでだけサポートされています。

関連トピック

FSPAN セッションの設定, （38 ページ）
FRSPAN セッションの設定, （41 ページ）

SPAN および RSPAN のデフォルト設定

表 *1*：*SPAN* および *RSPAN* のデフォルト設定

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

設定時の注意事項

SPAN 設定時の注意事項

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

関連トピック

ローカル SPAN セッションの作成, （19 ページ）
ローカル SPAN セッションの作成および着信トラフィックの設定, （22 ページ）
例：ローカル SPAN の設定, （45 ページ）

RSPAN 設定時の注意事項

- すべての SPAN 設定時の注意事項が RSPAN に適用されます。
- RSPAN VLAN には特性があるので、RSPAN VLAN として使用するためにネットワーク上の VLAN をいくつか確保し、それらの VLAN にはアクセス ポートを割り当てないでおく必要があります。
- RSPAN トラフィックに出力 ACL を適用して、特定のパケットを選択的にフィルタリングまたはモニタできます。 RSPAN 送信元switches内の RSPAN VLAN 上で、これらの ACL を指定します。
- RSPANを設定する場合は、送信元ポートおよび宛先ポートをネットワーク内の複数のswitchesに分散させることができます。
- RSPAN VLAN 上のアクセス ポート（音声 VLAN ポートを含む）は、非アクティブ ステートになります。
- 次の条件を満たす限り、任意の VLAN を RSPAN VLAN として設定できます。
  - すべてのswitchesで、RSPAN セッションに同じ RSPAN VLAN が使用されている。
  - 参加しているすべてのswitchesで RSPAN がサポートされている。

関連トピック

RSPAN 送信元セッションの作成, （29 ページ）
RSPAN 宛先セッションの作成, （33 ページ）

RSPAN 宛先セッションの作成および着信トラフィックの設定, （36 ページ）
例：RSPAN VLAN の作成, （46 ページ）

FSPAN および FRSPAN 設定時の注意事項

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

関連トピック

FSPAN セッションの設定, （38 ページ）
FRSPAN セッションの設定, （41 ページ）

SPAN および RSPAN の設定方法

ローカル SPAN セッションの作成

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session all`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Switch(config)# monitor session 1 source interface gigabitethernet1/0/1`	SPANセッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタする送信元ポートを指定します。 有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**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、モニタする送信元 VLAN を指定します。 指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたはVLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （任意）[**,** | **-**] は、一連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）**both** | **rx** | **tx**：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

	コマンドまたはアクション	目的
		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。 ◦ **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。 （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。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]} 例： `Switch(config)# monitor session 1 destination interface gigabitethernet1/0/2 encapsulation replicate`	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。 （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。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *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）[**,** | **-**] は、一連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 replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。 選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 （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 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `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。

関連トピック

ローカル SPAN, （5 ページ）
SPAN セッション, （8 ページ）
SPAN 設定時の注意事項, （18 ページ）

ローカル SPAN セッションの作成および着信トラフィックの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session all`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Switch(config)# monitor session 2 source gigabitethernet1/0/1 rx`	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。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate ingress dot1q vlan 6`	SPAN セッション、宛先ポート、パケットカプセル化、および入力 VLAN とカプセル化を指定します。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *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。カンマまたはハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製するこ

	コマンドまたはアクション	目的
		とを指定します。 選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。 • **ingress** は、宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。 ◦ **dot1q vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを受信します。 ◦ **isl**：ISL カプセル化を使用して入力パケットを転送します。 ◦ **untagged vlan** *vlan-id* または **vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受信します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `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。

関連トピック

ローカル SPAN, （5 ページ）
SPAN セッション, （8 ページ）
SPAN 設定時の注意事項, （18 ページ）
例：ローカル SPAN の設定, （45 ページ）

フィルタリングする VLAN の指定

SPAN 送信元トラフィックを特定の VLAN に制限するには、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session all`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source interface** *interface-id* 例： `Switch(config)# monitor session 2`	送信元ポート（モニタ対象ポート）と 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。

	コマンドまたはアクション	目的
	source interface gigabitethernet1/0/2 rx	• *interface-id* には、モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] 例： `Switch(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* に指定できる範囲は 1 ～ 4094 です。 •（任意）カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。
ステップ 6	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**encapsulation replicate**]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/1`	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。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • *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）[**,** | **-**] 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。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 •（任意）**encapsulation replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。 選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `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 VLAN としての VLAN の設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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。

	コマンドまたはアクション	目的
ステップ 3	**vlan** *vlan-id* 例： `Switch(config)# vlan 100`	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 または 1006 ～ 4094 です。 RSPAN VLAN を VLAN 1（デフォルト VLAN）または VLAN ID 1002 ～ 1005（トークンリングおよび FDDI VLAN 専用）にすることはできません。
ステップ 4	**remote-span** 例： `Switch(config-vlan)# remote-span`	VLAN を RSPAN VLAN として設定します。
ステップ 5	**end** 例： `Switch(config-vlan)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `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。

次の作業

RSPAN に参加するすべてのswitchesに RSPAN VLAN を作成する必要があります。 RSPAN VLAN ID が標準範囲（1005 未満）であり、VTP がネットワーク内でイネーブルである場合は、1 つの switchに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のswitchesに伝播するように設定できます。 拡張範囲 VLAN（1005 を超える ID）の場合、送信元と宛先の両方のswitches、および中間switchesに RSPAN VLAN を設定する必要があります。

VTP プルーニングを使用して、RSPAN トラフィックが効率的に流れるようにするか、または RSPAN トラフィックの伝送が不要なすべてのトランクから、RSPAN VLAN を手動で削除します。

VLAN からリモート SPAN 特性を削除して、標準 VLAN に戻すように変換するには、**no remote-span** VLAN コンフィギュレーション コマンドを使用します。

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

RSPAN 送信元セッションの作成

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

手順の概要

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

手順の詳細

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

	コマンドまたはアクション	目的
ステップ 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Switch(config)# monitor session 1 source interface gigabitethernet1/0/1 tx`	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* の範囲は、1 ～ 66 です。 • RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。 ◦ *interface-id* には、モニタリングする送信元ポートを指定します。 有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。 有効なポートチャネル番号は 1 ～ 48 です。 ◦ *vlan-id* には、モニタする送信元 VLAN を指定します。 指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたはVLAN）を含めることができます。ただし、1つのセッション内で送信元ポートと送信元VLANを併用することはできません。 • （任意）**[,|-]**：一連の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。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意）**both** | **rx** | **tx**：モニタ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。 ◦ **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 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例： `Switch(config)# monitor session 1 destination remote vlan 100`	RSPAN セッション、宛先 RSPAN VLAN、および宛先ポート グループを指定します。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `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。

関連トピック

リモート SPAN, （7 ページ）
RSPAN VLAN, （14 ページ）
RSPAN 設定時の注意事項, （18 ページ）

フィルタリングする VLAN の指定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモートSPANセッションを削除します。
ステップ 4	**monitor session** *session_number* **source interface** *interface-id* 例： `Switch(config)# monitor session 2 source interface gigabitethernet1/0/2 rx`	送信元ポート（モニタ対象ポート）と 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、モニタする送信元ポートを指定します。指定したインターフェイスは、あらかじめトランク ポートとして設定しておく必要があります。
ステップ 5	**monitor session** *session_number* **filter vlan** *vlan-id* [**,** | **-**] 例： `Switch(config)# monitor session 2 filter vlan 1 - 5 , 9`	SPAN 送信元トラフィックを特定の VLAN に制限します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* に指定できる範囲は 1 ～ 4094 です。 • （任意）**,** | **-**：カンマ（**,**）を使用して一連の VLAN を指定するか、ハイフン（**-**）を使用して VLAN 範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。

	コマンドまたはアクション	目的
ステップ 6	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例： `Switch(config)# monitor session 2 destination remote vlan 902`	RSPAN セッションおよび宛先リモート VLAN（RSPAN VLAN）を指定します。 • *session_number* には、ステップ 4 で指定したセッション番号を入力します。 • *vlan-id* には、宛先ポートにモニタ対象トラフィックを伝送する RSPAN VLAN を指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `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 宛先セッションの作成

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

このswitch上で RSPAN VLAN を定義し、RSPAN 宛先セッションを作成し、送信元 RSPAN VLAN および宛先ポートを指定するには、次の手順を実行します。

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 3	**vlan** *vlan-id* 例： `Switch(config)# vlan 901`	送信元switchで作成された RSPAN VLAN の VLAN ID を指定し、VLAN コンフィギュレーション モードを開始します。 両方のswitchesが VTP に参加し、RSPAN VLAN ID が 2 ～ 1005 である場合は、VTP ネットワークを介して RSPAN VLAN ID が伝播されるため、ステップ 3 ～ 5 は不要です。
ステップ 4	**remote-span** 例： `Switch(config-vlan)# remote-span`	VLAN を RSPAN VLAN として識別します。
ステップ 5	**exit** 例： `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。

	コマンドまたはアクション	目的
ステップ 6	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 1`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 7	**monitor session** *session_number* **source remote vlan** *vlan-id* 例： `Switch(config)# monitor session 1 source remote vlan 901`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 8	**monitor session** *session_number* **destination interface** *interface-id* 例： `Switch(config)# monitor session 1 destination interface gigabitethernet2/0/1`	RSPAN セッションと宛先インターフェイスを指定します。 • *session_number* には、ステップ 7 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • *interface-id* には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。 • **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。 元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。
ステップ 9	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 10	**show running-config** 例： `Switch# show running-config`	入力を確認します。

	コマンドまたはアクション	目的
ステップ 11	**copy running-config startup-config** 例： `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。

関連トピック

リモート SPAN, （7 ページ）
RSPAN VLAN, （14 ページ）
RSPAN 設定時の注意事項, （18 ページ）

RSPAN 宛先セッションの作成および着信トラフィックの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source remote vlan** *vlan-id* 例： `Switch(config)# monitor session 2 source remote vlan 901`	RSPAN セッションと送信元 RSPAN VLAN を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* [**,** | **-**] [**ingress** {**dot1q vlan** *vlan-id* | **isl** | **untagged vlan** *vlan-id* | **vlan** *vlan-id*}]} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 ingress vlan 6`	SPAN セッション、宛先ポート、パケット カプセル化、および着信 VLAN とカプセル化を指定します。 • *session_number* には、ステップ 5 で指定した番号を入力します。 RSPAN 宛先セッションでは、送信元 RSPAN VLAN および宛先ポートに同じセッション番号を使用する必要があります。 • *interface-id* には、宛先インターフェイスを指定します。 宛先インターフェイスは物理インターフェイスでなければなりません。 • **encapsulation replicate** はコマンドラインのヘルプ ストリングに表示されますが、RSPAN ではサポートされていません。元の VLAN ID は RSPAN VLAN ID によって上書きされ、宛先ポート上のすべてのパケットはタグなしになります。 • （任意）[**,** | **-**] 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。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定するには、**ingress** を追加のキーワードと一緒に入力します。

	コマンドまたはアクション	目的
		◦ **dot1q vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、IEEE 802.1Q でカプセル化された着信パケットを転送します。 ◦ **isl**：ISL カプセル化を使用して入力パケットを転送します。 ◦ **untagged vlan** *vlan-id* または **vlan** *vlan-id*：デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを転送します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `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。

関連トピック

リモート SPAN, （7 ページ）
RSPAN VLAN, （14 ページ）
RSPAN 設定時の注意事項, （18 ページ）
例：RSPAN VLAN の作成, （46 ページ）

FSPAN セッションの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Switch(config)# monitor session 2 source interface gigabitethernet1/0/1`	SPAN セッションおよび送信元ポート（モニタ対象ポート）を指定します。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。有効なインターフェイスには、物理インターフェイスおよびポート チャネル論理インターフェイス（**port-channel** *port-channel-number*）があります。 有効なポートチャネル番号は 1 ～ 48 です。

	コマンドまたはアクション	目的
		• *vlan-id* には、モニタする送信元 VLAN を指定します。 指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1 つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたは VLAN）を含めることができます。ただし、1 つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （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。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意） **[both**	**rx**	**tx]**：モニタリングするトラフィックの方向を指定します。 トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 ◦ **both**：送信トラフィックと受信トラフィックの両方をモニタします。 これはデフォルトです。 ◦ **rx**：受信トラフィックをモニタします。 ◦ **tx**：送信トラフィックをモニタします。 （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。
ステップ 5	**monitor session** *session_number* **destination** {**interface** *interface-id* **[,** | **-] [encapsulation replicate]**} 例： `Switch(config)# monitor session 2 destination interface gigabitethernet1/0/2 encapsulation replicate`	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。 • *session_number* には、ステップ 4 で入力したセッション番号を指定します。 • **destination** に対して、次のパラメータを指定します。 ◦ *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）**[,**|**-]** は、一連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 replicate** は、宛先インターフェイスが送信元インターフェイスのカプセル化方式を複製することを指定します。 選択しない場合のデフォルトは、ネイティブ形式（タグなし）でのパケットの送信です。

	コマンドまたはアクション	目的
		（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。 **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 6	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} 例： `Switch(config)# monitor session 2 filter ipv6 access-group 4`	SPAN セッション、フィルタリングするパケットのタイプ、および FSPAN セッションで使用する ACL を指定します。 • *session_number* には、 手順 4： • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • *name* には、トラフィックのフィルタリングに使用したい ACL の名前を指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `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。

関連トピック

フローベースの SPAN, （16 ページ）
FSPAN および FRSPAN 設定時の注意事項, （19 ページ）

FRSPAN セッションの設定

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

手順の概要

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

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Switch> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `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 3	**no monitor session** {*session_number* | **all** | **local** | **remote**} 例： `Switch(config)# no monitor session 2`	セッションに対する既存の SPAN 設定を削除します。 • *session_number* の範囲は、1 ～ 66 です。 • **all**：すべての SPAN セッションを削除します。 • **local**：すべてのローカル セッションを削除します。 • **remote**：すべてのリモート SPAN セッションを削除します。
ステップ 4	**monitor session** *session_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} [**,** | **-**] [**both** | **rx** | **tx**] 例： `Switch(config)# monitor session`	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。 • *session_number* の範囲は、1 ～ 66 です。 • *interface-id* には、モニタリングする送信元ポートを指定します。 有効なインターフェイスには、物理インターフェイスお

	コマンドまたはアクション	目的
	2 source interface gigabitethernet1/0/1	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、モニタする送信元 VLAN を指定します。 指定できる範囲は 1 ～ 4094 です（RSPAN VLAN は除く）。 （注） 1つのセッションに、一連のコマンドで定義された複数の送信元（ポートまたはVLAN）を含めることができます。ただし、1つのセッション内では送信元ポートと送信元 VLAN を併用できません。 • （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。 カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。 • （任意） [**both**	**rx**	**tx**]：モニタリングするトラフィックの方向を指定します。 トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニタします。 • **both**：送信トラフィックと受信トラフィックの両方をモニタします。 これはデフォルトです。 • **rx**：受信トラフィックをモニタします。 • **tx**：送信トラフィックをモニタします。 （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。
ステップ 5	**monitor session** *session_number* **destination remote vlan** *vlan-id* 例： `Switch(config)# monitor session 2 destination remote vlan 5`	RSPAN セッションと宛先 RSPAN VLAN を指定します。 • *session_number* には、ステップ 4 で指定した番号を入力します。 • *vlan-id* には、モニタする宛先 RSPAN VLAN を指定します。
ステップ 6	**vlan** *vlan-id* 例： `Switch(config)# vlan 10`	VLAN コンフィギュレーション モードを開始します。 *vlan-id* には、モニタする送信元 RSPAN VLAN を指定します。
ステップ 7	**remote-span** 例： `Switch(config-vlan)# remote-span`	ステップ 5 で指定した VLAN が RSPAN VLAN の一部であることを指定します。

	コマンドまたはアクション	目的
ステップ 8	**exit** 例： `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。
ステップ 9	**monitor session** *session_number* **filter** {**ip** | **ipv6** | **mac**} **access-group** {*access-list-number* | *name*} 例： `Switch(config)# monitor session 2 filter ip access-group 7`	RSPANセッション、フィルタリングするパケットのタイプ、および FRSPAN セッションで使用する ACL を指定します。 • *session_number* には、 手順 4： • *access-list-number* には、トラフィックのフィルタリングに使用したい ACL 番号を指定します。 • *name* には、トラフィックのフィルタリングに使用したいACLの名前を指定します。
ステップ 10	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show running-config** 例： `Switch# show running-config`	入力を確認します。
ステップ 12	**copy running-config startup-config** 例： `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。

関連トピック

フローベースの SPAN, （16 ページ）
FSPAN および FRSPAN 設定時の注意事項, （19 ページ）

SPAN および RSPAN 動作のモニタリング

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

表 *2* : *SPAN* および *RSPAN* 動作のモニタリング

コマンド	目的
show monitor	現在の SPAN、RSPAN、FSPAN、または FRSPAN 設定を表示します。

SPAN および RSPAN の設定例

例：ローカル SPAN の設定

次に、SPAN セッション 1 を設定し、宛先ポートへ向けた送信元ポートのトラフィックをモニタする例を示します。 最初に、セッション 1 の既存の SPAN 設定を削除し、カプセル化方式を維持しながら、双方向トラフィックを送信元ポート GigabitEthernet 1 から宛先ポート GigabitEthernet 2 にミラーリングします。

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

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

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

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

次に、SPAN セッション 2 内の既存の設定を削除し、VLAN 1 ～ 3 に属するすべてのポートで受信トラフィックをモニタするように SPAN セッション 2 を設定し、モニタされたトラフィックを宛先ポート GigabitEthernet 2 に送信する例を示します。 さらに、この設定は VLAN 10 に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

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

```
Switch(config)# monitor session 2 source vlan 10
Switch(config)# end
```

次に、SPAN セッション 2 の既存の設定を削除し、送信元ポート GigabitEthernet 1 上で受信されるトラフィックをモニタするように SPAN セッション 2 を設定し、送信元ポートと同じ出力カプセル化方式を使用してそれを宛先ポート GigabitEthernet 2 に送信し、VLAN 6 をデフォルトの入力 VLAN として IEEE 802.1Q カプセル化を使用する入力転送をイネーブルにする例を示します。

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

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

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

関連トピック

ローカル SPAN セッションの作成および着信トラフィックの設定, （22 ページ）
ローカル SPAN, （5 ページ）
SPAN セッション, （8 ページ）
SPAN 設定時の注意事項, （18 ページ）

例：RSPAN VLAN の作成

この例は、RSPAN VLAN 901 の作成方法を示しています。

```
Switch> enable
Switch# configure terminal
Switch(config)# vlan 901
Switch(config-vlan)# remote span
Switch(config-vlan)# end
```

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

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

次に、RSPAN セッション 2 の既存の設定を削除し、トランク ポート 2 で受信されるトラフィックをモニタするように RSPAN セッション 2 を設定し、VLAN 1 ～ 5 および 9 に対してのみトラフィックを宛先 RSPAN VLAN 902 に送信する例を示します。

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

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

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

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

関連トピック

RSPAN 宛先セッションの作成および着信トラフィックの設定, （36 ページ）
リモート SPAN, （7 ページ）
RSPAN VLAN, （14 ページ）
RSPAN 設定時の注意事項, （18 ページ）

その他の関連資料

関連資料

関連項目	マニュアル タイトル
system コマンド	*Network Management Command Reference, Cisco IOS XE Release 3E*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

標準および RFC

標準/RFC	タイトル
なし	-

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

SPAN および RSPAN の機能の履歴と情報

リリース	変更内容
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	スイッチ ポート アナライザ（SPAN）：スニファやアナライザまたは RMON プローブを使用してポートまたは VLAN のswitchのトラフィックを監視できます。 この機能が導入されました。
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	フローベースのスイッチ ポート アナライザ（SPAN）：指定されたフィルタを使用してエンド ホスト間の必要なデータのみをキャプチャする手段を提供します。 フィルタは、IPv4、IPv6 または IPv4 と IPv6、あるいは指定された送信元と宛先アドレス間の IP トラフィック（MAC）以外を制限するアクセス リストの観点から定義されます。 この機能が導入されました。
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	EtherChannel での SPAN 宛先ポートのサポート：EtherChannel で SPAN 宛先ポートを設定できるようにします。 この機能が導入されました。
Cisco IOS XE 3.2SECisco IOS XE 3.2SE	スイッチ ポート アナライザ（SPAN）-分散型出力 SPAN：ラインカードにすでに分散された入力 SPAN とともにラインカードに出力 SPAN 機能を分散させます。 出力 SPAN 機能をラインカードに分散させることで、システムのパフォーマンスが向上します。 この機能が導入されました。

ネットワーク管理コンフィギュレーション ガイド、Cisco IOS XE Release 3.6E（Catalyst 3850 スイッチ）