



## SPAN および RSPAN の設定

- [SPAN および RSPAN の前提条件](#) (1 ページ)
- [SPAN および RSPAN の制約事項](#) (1 ページ)
- [SPAN および RSPAN について](#) (4 ページ)
- [SPAN および RSPAN の設定](#) (16 ページ)
- [SPAN および RSPAN の設定方法](#) (17 ページ)
- [SPAN および RSPAN 動作のモニタリング](#) (43 ページ)
- [SPAN および RSPAN の設定例](#) (43 ページ)

## SPAN および RSPAN の前提条件

### SPAN

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

### RSPAN

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

## SPAN および RSPAN の制約事項

### SPAN

SPAN の制約事項は次のとおりです。

- 各デバイスで 66 のセッションを設定できます。最大 2 つの送信元セッションを設定できます。残りのセッションは、RSPAN 宛先セッションとして設定できます。送信元セッショ

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

- SPAN 送信元の場合は、セッションごとに、単一のポートまたは VLAN、一連のポートまたは VLAN、一定範囲のポートまたは VLAN のトラフィックを監視できます。1 つの SPAN セッションに、送信元ポートおよび送信元 VLAN を混在させることはできません。
- 宛先ポートを送信元ポートにすることはできません。同様に、送信元ポートを宛先ポートにすることもできません。
- 送信元ポートは、1 つのモニターセッションでのみ使用できます。
- 同じ宛先ポートで 2 つの SPAN セッションを設定することはできません。
- デバイスポートを SPAN 宛先ポートとして設定すると、通常のデバイスポートではなくなります。SPAN 宛先ポートを通過するのは、監視対象トラフィックのみになります。
- SPAN コンフィギュレーション コマンドを入力しても、前に設定した SPAN パラメータは削除されません。設定されている SPAN パラメータを削除するには、**no monitor session {session\_number | all | local | remote}** グローバル コンフィギュレーション コマンドを入力する必要があります。
- ローカル SPAN では、**encapsulation replicate** キーワードが指定されている場合、SPAN 宛先ポートを経由する発信パケットは元のカプセル化ヘッダー（タグなし、ISL、または IEEE 802.1Q）を伝送します。このキーワードが指定されていない場合、パケットはネイティブ形式で送信されます。
- 無効のポートを送信元ポートまたは宛先ポートとして設定することはできますが、SPAN 機能が開始されるのは、宛先ポートと少なくとも 1 つの送信元ポートまたは送信元 VLAN が有効になってからです。
- 単一の SPAN セッションに、送信元 VLAN とフィルタ VLAN を混在させることはできません。

SPAN セッションのトラフィック監視には次の制約事項があります。

- ポートまたは VLAN を送信元にできますが、同じセッション内に送信元ポートと送信元 VLAN を混在させることはできません。
- Wireshark は、出力スパンがアクティブな場合は出力パケットをキャプチャしません。
- 同じデバイスまたはデバイススタック内で、ローカル SPAN と RSPAN の送信元セッションの両方を実行できます。デバイスまたはデバイススタックは、合計 66 の送信元および RSPAN 宛先セッションをサポートします。
- 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。
- SPAN セッションがデバイスの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをトラフィック監視するなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。

- SPAN または RSPAN が有効の場合、監視中の各パケットは 2 回送信されます（1 回は標準トラフィックとして、もう 1 回は監視されたパケットとして）。多数のポートまたは VLAN を監視すると、大量のネットワークトラフィックが生成されることがあります。
- ディゼーブルのポート上に SPAN セッションを設定することはできますが、そのセッション用に宛先ポートと少なくとも 1 つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- デバイスは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じデバイスまたはデバイススタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。
- デバイスで DHCP スヌーピングが有効になっている場合、SPAN セッションは Dynamic Host Configuration Protocol (DHCP) 入力パケットのみをキャプチャします。

## RSPAN

RSPAN の制約事項は次のとおりです。

- IE31xx、IE3x00、および ESS3300 プラットフォームは、ハードウェアの制限により、1 つの RSPAN セッションのみをサポートします。
- 処理チップのハードウェア制限により、制御パケットとデータトラフィックを区別できません。したがって、ミラーリングを有効にすると、制御パケットを含むすべてのパケットがミラーリングされます。



**注意** RSPAN 機能は、実稼働ネットワークに影響を与える可能性があるため、慎重に使用してください。

- RSPAN VLAN はトランクポートにのみ設定されており、アクセスポートには設定されていません。不要なトラフィックが RSPAN VLAN に発生しないようにするために、参加しているすべてのデバイスで VLAN RSPAN 機能がサポートされていることを確認してください。
- RSPAN VLAN を設定できるトランクインターフェイスは 1 つだけです。複数のトランクインターフェイスでリモート VLAN を設定しようとする、次のようなエラーが表示されます。

```
Switch(config-if)#do sh vlan id 2508
```

VLAN Name	Status	Ports
2508 VLAN2508	active	Gil1/1, Gil1/2

```

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----
2508 enet 102508 1500 - - - - - 0 0

Remote SPAN VLAN
-----
Enabled

Primary Secondary Type Ports
-----

Switch(config-if)#exit
Switch(config)#mon sess 1 destination remote vlan 2508
% Platform cannot support remote-span mirroring on VLAN with more than one member
ports.

```



(注) 4 バイトの RSPAN VLAN ID の追加によって発生する RSPAN の受信インターフェイスでのエラーを防ぐために、MTU サイズをモニター対象最大パケットサイズよりも 4 バイト大きい値に設定することが推奨されます。

- プラットフォームは、複数のメンバーポートを含むポートチャネルに関連付けられた VLAN での RSPAN ミラーリングをサポートしません。
- 送信元トランク ポートにアクティブな RSPAN VLAN が設定されている場合、RSPAN VLAN はポートベース RSPAN セッションの送信元として含まれます。また、RSPAN VLAN を SPAN セッションの送信元に設定することもできます。ただし、デバイスはスパンされたトラフィックを監視しないため、デバイスの RSPAN 送信元セッションの宛先として識別された RSPAN VLAN では、パケットの出力スパ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 VLAN をネイティブ VLAN として設定しないことをお勧めします。
- SPAN と RSPAN は同時に動作できます。
- ERSPAN は、IOx の CV に対して内部的にのみ機能します。独立した機能としてはサポートされていません。
- IOx で CV が有効になっている場合、SPAN および RSPAN はサポートされません。
- IOx の CV の有効化後に SPAN/RSPAN が設定された場合、またはその逆の場合は、最新の設定が適用されます。

## SPAN および RSPAN について

ここでは、SPAN および RSPAN について説明します。

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

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

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

### ローカル SPAN

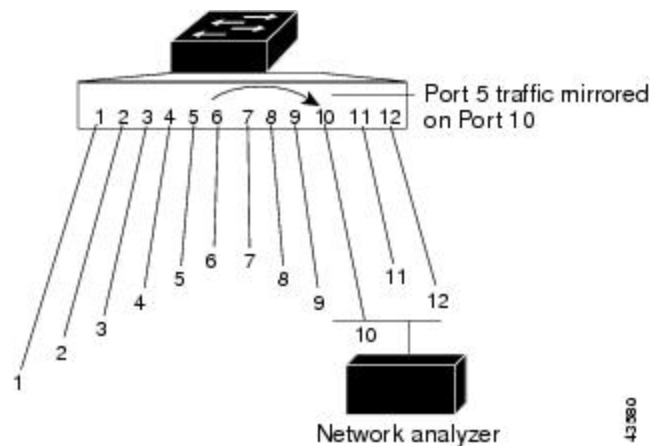
ローカル SPAN は 1 つのデバイス内の SPAN セッション全体をサポートします。すべての送信元ポートまたは送信元 VLAN、および宛先ポートは、同じデバイスまたはデバイススタック内にあります。ローカル SPAN は、任意の VLAN 上の 1 つまたは複数の送信元ポートからのトラフィック、あるいは 1 つまたは複数の VLAN からのトラフィックを解析するために宛先ポートへコピーします。

ローカル SPAN は 1 つのスイッチ内の SPAN セッション全体をサポートします。すべての送信元ポートおよび宛先ポートは、同じスイッチ内にあります。ローカル SPAN は、1 つ以上の送信元ポートからのトラフィックを、解析のため宛先ポートにコピーします。

#### 図 1: 単一デバイスでのローカル SPAN の設定例

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

せんが、ポート 5 からのすべてのネットワーク トラフィックを受信します。



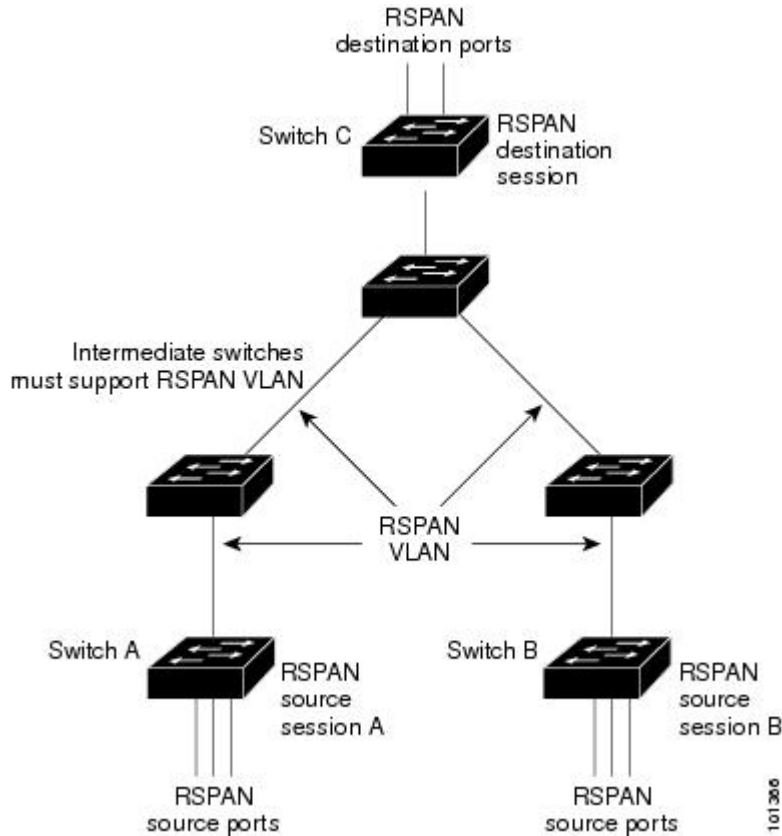
## リモート SPAN

RSPAN は、異なるデバイス（または異なるデバイススタック）上の送信元ポート、送信元 VLAN、および宛先ポートをサポートしているため、ネットワーク上で複数のデバイスをリモート監視できます。

図 2: RSPAN の設定例

下の図にデバイス A とデバイス B の送信元ポートを示します。各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN 上で伝送されます。この RSPAN VLAN は、参加しているすべてのデバイスの RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランクポートを介して、RSPAN VLAN を監視する宛先セッションに転送されます。各 RSPAN 送信元デバイスには、ポートまたは VLAN のいずれかが RSPAN 送信元として必要です。図中のデバ

イス C のように、宛先は常に物理ポートになります。



## SPAN と RSPAN の概念および用語

### SPAN セッション

SPAN セッション（ローカルまたはリモート）を使用すると、1つのポート上、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ーが指定した入力および出力の packets セットを収集し、SPAN データ ストリームを形成して、宛先ポートに転送します。

RSPAN は少なくとも1つの RSPAN 送信元セッション、1つの RSPAN VLAN、および少なくとも1つの RSPAN 宛先セッションで構成されています。RSPAN 送信元セッションと RSPAN 宛先セッションは、異なるネットワーク デバイス上に別々に設定します。デバイスに RSPAN 送信元セッションを設定するには、一連の送信元ポートまたは送信元 VLAN を RSPAN VLAN に関連付けます。このセッションの出力は、RSPAN VLAN に送信される SPAN パケットのストリームです。別のデバイスに RSPAN 宛先セッションを設定するには、宛先ポートを RSPAN

VLANに関連付けます。宛先セッションはRSPAN VLAN トラフィックをすべて収集し、RSPAN 宛先ポートに送信します。

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

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

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

- ポートまたは VLAN を送信元にはできませんが、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。
- SPAN セッションがデバイスの通常の動作を妨げることはありません。ただし、10 Mbps のポートで 100 Mbps のポートをトラフィック監視するなど、オーバーサブスクライブの SPAN 宛先は、パケットのドロップまたは消失を招くことがあります。
- SPAN または RSPAN が有効の場合、監視中の各パケットは2回送信されます（1回は標準トラフィックとして、もう1回は監視されたパケットとして）。したがって、多数のポートまたは VLAN をモニターすると、大量のネットワークトラフィックが生成されることがあります。
- ディ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せんが、そのセッション用に宛先ポートと少なくとも1つの送信元ポートまたは VLAN をイネーブルにしない限り、SPAN セッションはアクティブになりません。
- デバイスは、単一セッション内でのローカル SPAN と RSPAN の併用をサポートしません。
  - RSPAN 送信元セッションにローカル宛先ポートを設定できません。
  - RSPAN 宛先セッションにローカル送信元ポートを設定できません。
  - 同じデバイスまたはデバイススタック上で、同じ RSPAN VLAN を使用する RSPAN 宛先セッションおよび RSPAN 送信元セッションを実行できません。

## モニタ対象トラフィック

SPAN セッションは、次のトラフィックタイプを監視できます。

- 受信 (Rx) SPAN : 受信 (または入力) SPAN は、デバイス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、デバイス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。

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

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

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

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 モニター用とポート B での TX モニター用に双方向 (RX と TX) SPAN セッションが設定されているとします。パケットがポート A からデバイスに入ってポート B にスイッチされると、着信パケットも発信パケットも宛先ポートに送信されます。このため、両方のパケットは同じものになります。レイヤ 3 書き換えが行われた場合には、パケット変更のため異なるパケットになります。

## 送信元ポート

送信元ポート (別名モニター側ポート) は、ネットワークトラフィック分析のために監視するスイッチドポートまたはルーテッドポートです。

1 つのローカル SPAN セッションまたは RSPAN 送信元セッションでは、送信元ポートまたは VLAN のトラフィックを単一方向または双方向でモニターできます。

デバイスは、任意の数の送信元ポート（デバイスで利用可能なポートの最大数まで）と任意の数の送信元 VLAN（サポートされている VLAN の最大数まで）をサポートしています。

単一のセッションにポートおよび VLAN を混在させることはできません。

送信元ポートの特性は、次のとおりです。

- 送信元ポートは、1 つのモニターセッションでのみ使用できます。
- モニターする方向（入力、出力、または両方）を指定して、各送信元ポートを設定できます。
- すべてのポートタイプ（EtherChannel、ギガビットイーサネットなど）が可能です。
- EtherChannel 送信元の場合は、EtherChannel 全体で、または物理ポートがポート チャネルに含まれている場合は物理ポート上で個別に、トラフィックをモニターできます。
- アクセスポート、トランクポート、ルーテッドポート、または音声 VLAN ポートに指定できます。
- 宛先ポートにすることはできません。
- 送信元ポートは同じ VLAN にあっても異なる VLAN にあってもかまいません。
- 単一セッション内で複数の送信元ポートをモニターすることが可能です。

## 送信元 VLAN

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

VSPAN には次の特性があります。

- 送信元 VLAN 内のすべてのアクティブポートは送信元ポートとして含まれ、単一方向または双方向でモニターできます。
- 指定されたポートでは、モニター対象の VLAN 上のトラフィックのみが宛先ポートに送信されます。
- 宛先ポートが送信元 VLAN に所属する場合は、送信元リストから除外され、モニターされません。
- ポートが送信元 VLAN に追加または削除されると、これらのポートで受信された送信元 VLAN のトラフィックは、モニター中の送信元に追加または削除されます。
- VLAN 送信元と同じセッション内のフィルタ VLAN を使用することはできません。
- モニターできるのは、イーサネット VLAN だけです。

## VLAN フィルタリング

トランクポートを送信元ポートとしてモニターする場合、デフォルトでは、トランク上でアクティブなすべての VLAN がモニターされます。VLAN フィルタリングを使用して、トランク送信元ポートでの SPAN トラフィックのモニター対象を特定の VLAN に制限できます。

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

## 宛先ポート

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

宛先ポートの特性は、次のとおりです。

- ローカル SPAN セッションの場合、宛先ポートは送信元ポートと同じデバイスまたはデバイス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デバイス上にあります。RSPAN 送信元セッションのみを実行するデバイスまたはデバイススタックには、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。
- 一度に 1 つの SPAN セッションにしか参加できません（ある SPAN セッションの宛先ポートは、別の SPAN セッションの宛先ポートになることはできません）。
- アクティブな場合、着信トラフィックはディセーブルになります。ポートは SPAN セッションに必要なトラフィック以外は送信しません。宛先ポートでは着信トラフィックを学習したり、転送したりしません。
- 入力トラフィック転送がネットワーク セキュリティ デバイスでイネーブルの場合、宛先ポートはレイヤ 2 でトラフィックを転送します。
- レイヤ 2 プロトコル（STP、VTP、CDP、DTP、PAgP）のいずれにも参加しません。
- 任意の SPAN セッションの送信元 VLAN に所属する宛先ポートは、送信元リストから除外され、モニターされません。
- デバイスまたはデバイス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、これらの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** が有効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、元の VLAN ID を保持したまま RSPAN VLAN ID がパケットに挿入されます。

## RSPAN VLAN

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

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

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

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

## SPAN および RSPAN と他の機能の相互作用

SPAN は次の機能と相互に作用します。

- ルーティング：SPAN はルーテッドトラフィックを監視しません。VSPAN は、受信または送信されるトラフィックのみをモニターし、VLAN 間でルーティングされるトラフィックはモニターされません。たとえば、VLAN が受信モニターされ、別の VLAN からモニタリング対象 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モニターされず、SPAN 宛先ポートで受信されません。
- STP：SPAN または RSPAN セッションがアクティブな間、宛先ポートは STP に参加しません。SPAN または RSPAN セッションが無効になると、宛先ポートは STP に参加できません。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、間で RSPAN VLAN のプルーニングが可能です。
- VLAN およびトランッキング：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できます。SPAN 宛先ポートとしては設定できません。グループが SPAN 送信元として設定されている場合、グループ全体が監視されます。

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

EtherChannel グループに所属する物理ポートを SPAN 送信元ポートとして設定し、引き続き EtherChannel の一部とすることができます。この場合、この物理ポートは EtherChannel に参加しているため、そのポートからのデータは監視されます。ただし、EtherChannel グループ

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、グループメンバーのままですが、inactive または suspended ステートになります。

EtherChannel グループに含まれる物理ポートが宛先ポートであり、その EtherChannel グループが送信元の場合、ポートは EtherChannel グループおよび監視対象ポートリストから削除されます。

- マルチキャストトラフィックを監視できます。出力ポートおよび入力ポートの監視では、未編集の packets が 1 つだけ SPAN 宛先ポートに送信されます。マルチキャスト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有効の場合、出力を監視しているポートでポートセキュリティを有効にしないでください。RSPAN 送信元セッションでは、出力を監視しているポートでポートセキュリティを有効にしないでください。

- IEEE 802.1x ポートは SPAN 送信元ポートにできます。SPAN 宛先ポート上で IEEE 802.1x を有効にできますが、SPAN 宛先としてこのポートを削除するまで、IEEE 802.1x は無効に設定されます。

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

## SPAN と RSPAN とデバイス スタック

※ のスタックが 1 つの論理を表すため、ローカル SPAN の送信元ポートと宛先ポートはスタック内で異なるに存在することがあります。したがって、のスタック内で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。アクティブなセッションは、がスタックから削除された場合に非アクティブになる可能性があり、非アクティブなセッションは、がスタックに追加された場合にアクティブになる可能性があります。

## フローベースの SPAN

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

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

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

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

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

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

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

## SPAN および RSPAN のデフォルト設定

表 1: SPAN および RSPAN のデフォルト設定

機能	デフォルト設定
SPAN のステート (SPAN および RSPAN)	ディセーブル
モニタする送信元ポート トラフィック	受信トラフィックと送信トラフィック ( <b>both</b> ) の両方。
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

# SPAN および RSPAN の設定

## SPAN 設定時の注意事項

- 送信元ポートまたは宛先ポート または VLAN を SPAN セッションから削除するには、**no monitor session session\_number source interface interface-id {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、**encapsulation** オプションは、コマンドの x 形式で無視されます。
- トランクポート上のすべての VLAN をモニターするには、**no monitor session session\_number filter** グローバル コンフィギュレーション コマンドを使用します。

## RSPAN 設定時の注意事項

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

## 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。

## SPAN および RSPAN の設定方法

ここでは、SPAN および RSPAN の設定方法について説明します。

### ローカル SPAN セッションの作成

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

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session\_number* | **all** | **local** | **remote**}
4. **monitor session** *session\_number* **source** {**interface** *interface-id* } [, | -] [**both** | **rx** | **tx**]
5. **monitor session** *session\_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** *replicate*][**ingress**{*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	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	セッションに対する既存の SPAN 設定を削除します。 • ※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。 • <b>all</b> : すべての SPAN セッションを削除します。
	例： Device(config)# <b>no monitor session all</b>	

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>local</b> : すべてのローカルセッションを削除します。</li> <li>• <b>remote</b> : すべてのリモート SPAN セッションを削除します。</li> </ul>
<b>ステップ 4</b>	<p><b>monitor session <i>session_number</i> source {interface <i>interface-id</i> } [, -] [<b>both</b>   <b>rx</b>   <b>tx</b>]</b></p> <p>例 :</p> <pre>Device(config)# monitor session 1 source interface gigabitethernet1/1</pre>	<p>SPAN セッションおよび送信元ポート（モニター対象ポート）を指定します。</p> <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li>• ※ <i>interface-id</i> には、モニター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（<b>port-channel</b> <i>port-channel-number</i>）があります。有効なポートチャネル番号は 1 ~ 48 です。</li> <li>• （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。</li> <li>• （任意）, -] 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</li> <li>• （オプション） <b>both</b> <b>rx</b> <b>tx</b> : モニターするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 <ul style="list-style-type: none"> <li>• <b>both</b> : 受信トラフィックと送信トラフィックの両方を監視します。</li> <li>• <b>rx</b> : 受信トラフィックを監視します。</li> <li>• <b>tx</b> : 送信トラフィックをモニタします。</li> </ul> </li> </ul> <p>（注） ※ <b>monitor session <i>session_number</i> source</b> コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>

	コマンドまたはアクション	目的
ステップ 5	<p><b>monitor session</b> <i>session_number</i> <b>destination</b> {<b>interface</b> <i>interface-id</i> [, -] [<b>encapsulation replicate</b>][<b>ingress</b> {<i>vlan-id</i>}]}</p> <p>例 :</p> <pre>Device(config)# monitor session 1 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 10</pre>	<p>(注) ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。</p> <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> には、ステップ 4 で入力したセッション番号を指定します。</li> <li>• ※ <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。</li> <li>• (任意) , -] 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</li> <li>• (オプション) <b>encapsulation replicate</b> 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。</li> <li>• <b>ingress</b> 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。 <ul style="list-style-type: none"> <li>• <b>vlan <i>vlan-id</i></b>—デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受け入れます。</li> </ul> </li> </ul> <p>(注) ※ <b>monitor session <i>session_number</i> destination</b> 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。</p>
ステップ 6	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	<p><b>show running-config</b></p> <p>例 :</p> <pre>Device# show running-config</pre>	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 8	<b>copy running-config startup-config</b> 例 : Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## ローカル SPAN セッションの作成および着信トラフィックの設定

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

### 手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session\_number* | **all** | **local** | **remote**}
4. **monitor session** *session\_number* **source** {**interface** *interface-id* } [, | -] [**both** | **rx** | **tx**]
5. **monitor session** *session\_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation replicate**] [**ingress** {**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	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : Device# <b>configure terminal</b>	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	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }           例 : Device(config)# <b>no monitor session all</b>	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li>• <b>all</b> : すべての SPAN セッションを削除します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>local</b> : すべてのローカルセッションを削除します。</li> <li>• <b>remote</b> : すべてのリモート SPAN セッションを削除します。</li> </ul>
ステップ 4	<b>monitor session</b> <i>session_number</i> <b>source</b> { <b>interface</b> <i>interface-id</i> } [, -] [ <b>both</b>   <b>rx</b>   <b>tx</b> ] 例 : <pre>Device(config)# monitor session 2 source gigabitethernet1/1 rx</pre>	SPAN セッションおよび送信元ポート（モニター対象ポート）を指定します。
ステップ 5	<b>monitor session</b> <i>session_number</i> <b>destination</b> { <b>interface</b> <i>interface-id</i> [, -] [ <b>encapsulation replicate</b> ] [ <b>ingress</b> { <b>vlan</b> <i>vlan-id</i> }]} 例 : <pre>Device(config)# monitor session 2 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 10</pre>	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。 <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> には、ステップ 4 で入力したセッション番号を指定します。</li> <li>• ※ <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定する必要があります。EtherChannel や VLAN は指定できません。</li> <li>• (任意) , -] : 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマ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。</li> <li>• (オプション) <b>encapsulation replicate</b> 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。</li> <li>• <b>ingress</b> 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。               <ul style="list-style-type: none"> <li>• <b>vlan</b> <i>vlan-id</i>—デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受け入れます。</li> </ul> </li> </ul>
ステップ 6	<b>end</b> 例 :	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
	Device (config) # <b>end</b>	
ステップ 7	<b>show running-config</b> 例： Device# <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## フィルタリングする VLAN の指定

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

### 手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session\_number* | **all** | **local** | **remote**}
4. **monitor session** *session\_number* **source** {**interface** *interface-id* } [, | -] [**both** | **rx** | **tx**]
5. **monitor session** *session\_number* **filter** **vlan** *vlan-id* [, | -]
6. **monitor session** *session\_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** **replicate**][**ingress** {**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	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> } 例 : <pre>Device(config)# no monitor session all</pre>	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> <li>※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li><b>all</b> : すべての SPAN セッションを削除します。</li> <li><b>local</b> : すべてのローカルセッションを削除します。</li> <li><b>remote</b> : すべてのリモート SPAN セッションを削除します。</li> </ul>
ステップ 4	<b>monitor session</b> <i>session_number</i> <b>source</b> { <b>interface</b> <i>interface-id</i> } [,   -] [ <b>both</b>   <b>rx</b>   <b>tx</b> ] 例 : <pre>Device(config)# monitor session 2 source interface gigabitethernet1/2 rx</pre>	送信元ポート（モニター対象ポート）と SPAN セッションの特性を指定します。 <ul style="list-style-type: none"> <li>※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li>※ <i>interface-id</i> には、モニター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。</li> </ul>
ステップ 5	<b>monitor session</b> <i>session_number</i> <b>filter vlan</b> <i>vlan-id</i> [,   -] 例 : <pre>Device(config)# monitor session 2 filter vlan 1 - 5 , 9</pre>	SPAN 送信元トラフィックを特定の VLAN に制限します。 <ul style="list-style-type: none"> <li>※ <i>session_number</i> には、ステップ 4 で指定したセッション番号を入力します。</li> <li>※ <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。</li> <li>（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 の範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</li> </ul>
ステップ 6	<b>monitor session</b> <i>session_number</i> <b>destination</b> { <b>interface</b> <i>interface-id</i> } [,   -] [ <b>encapsulation replicate</b> ][ <b>ingress</b> { <i>vlan</i> <i>vlan-id</i> } ] 例 : <pre>Device(config)# monitor session 2 destination interface gigabitethernet1/1 ingress vlan 6</pre>	SPAN セッションおよび宛先ポート（モニター側ポート）を指定します。 <ul style="list-style-type: none"> <li>※ <i>session_number</i> には、ステップ 4 で入力したセッション番号を指定します。</li> <li>※ <i>interface-id</i> には、宛先ポートを指定します。宛先インターフェイスには物理ポートを指定す</li> </ul>

	コマンドまたはアクション	目的
		<p>る必要があります。EtherChannel や VLAN は指定できません。</p> <ul style="list-style-type: none"> <li>• (任意) ,[-] 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。</li> <li>• (オプション) <b>encapsulation replicate</b> 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。</li> <li>• <b>ingress</b> 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。 <ul style="list-style-type: none"> <li>• <b>vlan vlan-id</b>—デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受け入れます。</li> </ul> </li> </ul>
ステップ 7	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show running-config</b> 例： Device# <b>show running-config</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(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	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>vlan <i>vlan-id</i></b> 例： Device(config)# <b>vlan 100</b>	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	<b>remote-span</b> 例： Device(config-vlan)# <b>remote-span</b>	VLAN を RSPAN VLAN として設定します。
ステップ 5	<b>end</b> 例： Device(config-vlan)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例： Device# <b>show running-config</b>	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 7	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

### 次のタスク

RSPAN に参加するすべてのデバイスに 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 つのデバイスに RSPAN VLAN を作成し、VTP がこの RSPAN VLAN を VTP ドメイン内の他のデバイス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デバイス、および中間デバイスに 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、モニター対象の送信元および宛先 RSPAN VLAN を指定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session {session\_number | all | local | remote}**
4. **monitor session session\_number source {interface interface-id } [, | -] [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	<b>enable</b> 例： <pre>Device&gt; enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： <pre>Device# configure terminal</pre>	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	<b>no monitor session {<i>session_number</i>   all   local   remote}</b> 例： <pre>Device(config)# no monitor session 1</pre>	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> <li>※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li><b>all</b> : すべての SPAN セッションを削除します。</li> <li><b>local</b> : すべてのローカルセッションを削除します。</li> <li><b>remote</b> : すべてのリモート SPAN セッションを削除します。</li> </ul>
ステップ 4	<b>monitor session <i>session_number</i> source {interface <i>interface-id</i> } [,   -] [both   rx   tx]</b> 例： <pre>Device(config)# monitor session 1 source interface gigabitethernet1/1 tx</pre>	RSPAN セッションおよび送信元ポート（モニター対象ポート）を指定します。 <ul style="list-style-type: none"> <li>※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li>RSPAN セッションの送信元ポートまたは送信元 VLAN を入力します。               <ul style="list-style-type: none"> <li>※ <i>interface-id</i> には、モニター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 (<b>port-channel <i>port-channel-number</i></b>) があります。有効なポートチャネル番号は 1 ~ 48 です。</li> </ul> </li> <li>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。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• (任意) ,[-] : 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。</li> <li>• (オプション) <b>both rx tx</b> : モニターするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 <ul style="list-style-type: none"> <li>• <b>both</b> : 受信トラフィックと送信トラフィックの両方を監視します。</li> <li>• <b>rx</b> : 受信トラフィックを監視します。</li> <li>• <b>tx</b> : 送信トラフィックをモニタします。</li> </ul> </li> </ul>
ステップ 5	<b>monitor session session_number destination remote vlan vlan-id</b> 例 : <pre>Device(config)# monitor session 1 destination remote vlan 100</pre>	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。 <ul style="list-style-type: none"> <li>• ※ <i>session_number</i>には、ステップ 4 で定義した番号を入力します。</li> <li>• ※ <i>vlan-id</i>には、モニターする送信元 RSPAN VLAN を指定します。</li> </ul>
ステップ 6	<b>end</b> 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config</b> 例 : <pre>Device# show running-config</pre>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例 : <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

## フィルタリングする VLAN の指定

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

### 手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session\_number* | **all** | **local** | **remote**}
4. **monitor session** *session\_number* **source** {**interface** *interface-id* } [, | -] [**both** | **rx** | **tx**]
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	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	セッションに対する既存の SPAN 設定を削除します。  • ※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。  • <b>all</b> : すべての SPAN セッションを削除します。  • <b>local</b> : すべてのローカルセッションを削除します。  • <b>remote</b> : 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	<b>monitor session</b> <i>session_number</i> <b>source</b> { <b>interface</b> <i>interface-id</i> } [,   -] [ <b>both</b>   <b>rx</b>   <b>tx</b> ] 例：	送信元ポート（モニター対象ポート）と SPAN セッションの特性を指定します。

	コマンドまたはアクション	目的
	<pre>Device(config)# monitor session 2 source interface gigabitethernet1/2 rx</pre>	<ul style="list-style-type: none"> <li>• ※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li>• ※ <i>interface-id</i> には、モニター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。</li> <li>• (任意) <i>, -</i> : 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。</li> <li>• (オプション) <b>both rx tx</b> : モニターするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、送信元インターフェイスは送信トラフィックと受信トラフィックの両方を送信します。 <ul style="list-style-type: none"> <li>• <b>both</b> : 受信トラフィックと送信トラフィックの両方を監視します。</li> <li>• <b>rx</b> : 受信トラフィックを監視します。</li> <li>• <b>tx</b> : 送信トラフィックをモニタします。</li> </ul> </li> </ul>
ステップ 5	<pre>monitor session session_number filter vlan vlan-id [, -]</pre> <p>例 :</p> <pre>Device(config)# monitor session 2 filter vlan 1 - 5 , 9</pre>	<p>SPAN 送信元トラフィックを特定の VLAN に制限します。</p> <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> には、ステップ 4 で指定したセッション番号を入力します。</li> <li>• ※ <i>vlan-id</i> に指定できる範囲は 1 ~ 4094 です。</li> <li>• (オプション) <i>, -</i> 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 の範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。</li> </ul>
ステップ 6	<pre>monitor session session_number destination remote vlan vlan-id</pre> <p>例 :</p> <pre>Device(config)# monitor session 2 destination remote vlan 902</pre>	<p>RSPAN セッションおよび宛先リモート VLAN (RSPAN VLAN) を指定します。</p> <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> には、ステップ 4 で指定したセッション番号を入力します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>※<i>vlan-id</i>には、宛先ポートにモニタリング対象トラフィックを伝送する RSPAN VLAN を指定します。</li> </ul>
ステップ 7	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show running-config</b> 例： Device# <b>show running-config</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(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、別のデバイスまたはデバイススタック（送信元セッションが設定されていないデバイスまたはデバイススタック）に設定します。

このデバイス上で 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* [, | -] [encapsulation replicate][ingress {vlan *vlan-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	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>vlan vlan-id</b> 例： Device(config)# <b>vlan 901</b>	送信元デバイスで作成された 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。  両方のデバイスが 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	<b>remote-span</b> 例： Device(config-vlan)# <b>remote-span</b>	VLAN を RSPAN VLAN として識別します。
ステップ 5	<b>exit</b> 例： Device(config-vlan)# <b>exit</b>	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	<b>no monitor session {session_number   all   local   remote}</b> 例： Device(config)# <b>no monitor session 1</b>	セッションに対する既存の SPAN 設定を削除します。 • ※ <i>session_number</i> に指定できる範囲は 1～66 です。 • <b>all</b> : すべての SPAN セッションを削除します。 • <b>local</b> : すべてのローカルセッションを削除します。 • <b>remote</b> : 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 7	<p><b>monitor session</b> <i>session_number</i> <b>source remote vlan</b> <i>vlan-id</i></p> <p>例 :</p> <pre>Device(config)# monitor session 1 source remote vlan 901</pre>	<p>RSPAN セッションと送信元 RSPAN VLAN を指定します。</p> <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li>• ※ <i>vlan-id</i> には、モニターする送信元 RSPAN VLAN を指定します。</li> </ul>
ステップ 8	<p><b>monitor session</b> <i>session_number</i> <b>destination</b> {<b>interface</b> <i>interface-id</i> [, -] [<b>encapsulation replicate</b>][<b>ingress</b> {<b>vlan</b> <i>vlan-id</i>}]}</p> <p>例 :</p> <pre>Device(config)# monitor session 1 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 10</pre>	<p>RSPAN セッションと宛先インターフェイスを指定します。</p> <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> には、ステップ 7 で定義した番号を入力します。</li> </ul> <p>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。</p> <ul style="list-style-type: none"> <li>• ※ <i>interface-id</i> には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。</li> <li>• (任意) , -] 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。</li> <li>• (オプション) <b>encapsulation replicate</b> 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。</li> <li>• <b>ingress</b> 宛先ポートでの着信トラフィックの転送をイネーブルにして、カプセル化タイプを指定します。 <ul style="list-style-type: none"> <li>• <b>vlan</b> <i>vlan-id</i>—デフォルトの VLAN として指定した VLAN で、タグなしのカプセル化タイプで着信パケットを受け入れます。</li> </ul> </li> <li>• ※ <b>monitor session</b> <i>session_number</i> <b>destination</b> 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。</li> </ul>

	コマンドまたはアクション	目的
ステップ 9	<b>end</b> 例：  Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 10	<b>show running-config</b> 例：  Device# <b>show running-config</b>	入力を確認します。
ステップ 11	<b>copy running-config startup-config</b> 例：  Device# <b>copy running-config startup-config</b>	(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* [,|-] [**encapsulation replicate**] [**ingress** {**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	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例 : <pre>Device# configure terminal</pre>	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	<b>no monitor session {<i>session_number</i>   all   local   remote}</b> 例 : <pre>Device(config)# no monitor session 2</pre>	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li>• <b>all</b> : すべての SPAN セッションを削除します。</li> <li>• <b>local</b> : すべてのローカルセッションを削除します。</li> <li>• <b>remote</b> : すべてのリモート SPAN セッションを削除します。</li> </ul>
ステップ 4	<b>monitor session <i>session_number</i> source remote vlan <i>vlan-id</i></b> 例 : <pre>Device(config)# monitor session 2 source remote vlan 901</pre>	RSPAN セッションと送信元 RSPAN VLAN を指定します。 <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li>• ※ <i>vlan-id</i> には、モニターする送信元 RSPAN VLAN を指定します。</li> </ul>
ステップ 5	<b>monitor session <i>session_number</i> destination {interface <i>interface-id</i> [, -] [encapsulation replicate] [ingress {vlan <i>vlan-id</i>}]}</b> 例 : <pre>Device(config)# monitor session 2 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 10</pre>	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。 <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> には、ステップ 5 で定義した番号を入力します。</li> <li>• 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。</li> <li>• ※ <i>interface-id</i> には、宛先インターフェイスを指定します。宛先インターフェイスは物理インターフェイスでなければなりません。</li> <li>• コマンドラインのヘルプ文字列には表示されませんが、<b>encapsulation replicate</b> は RSPAN ではサポートされません。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。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• (任意) , -] 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。</li> <li>• Enter <b>ingress</b> を追加のキーワードと一緒に入力することで、宛先ポートでの着信トラフィックの転送を有効にして、カプセル化タイプを指定できます。 <ul style="list-style-type: none"> <li>• <b>vlan vlan-id</b>—デフォルトの VLAN として指定した VLAN で、タグなしのカプセル化タイプで着信パケットを転送します。</li> </ul> </li> </ul>
ステップ 6	<b>end</b> 例： Device(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config</b> 例： Device# <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例： Device# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## FSPAN セッションの設定

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

### 手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session\_number* | **all** | **local** | **remote**}
4. **monitor session** *session\_number* **source** {**interface** *interface-id* } [,|-] [**both** | **rx** | **tx**]
5. **monitor session** *session\_number* **destination** {**interface** *interface-id* [,|-] [**encapsulation** **replicate**] [**ingress** {**vlan** *vlan-id*}]}

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	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> } 例： Device(config)# <b>no monitor session 2</b>	セッションに対する既存の SPAN 設定を削除します。 <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> に指定できる範囲は 1 ～ 66 です。</li> <li>• <b>all</b> : すべての SPAN セッションを削除します。</li> <li>• <b>local</b> : すべてのローカルセッションを削除します。</li> <li>• <b>remote</b> : すべてのリモート SPAN セッションを削除します。</li> </ul>
ステップ 4	<b>monitor session</b> <i>session_number</i> <b>source</b> { <b>interface</b> <i>interface-id</i> } [, -] [ <b>both</b>   <b>rx</b>   <b>tx</b> ] 例： Device(config)# <b>monitor session 2 source interface gigabitethernet1/1</b>	SPAN セッションおよび送信元ポート（モニター対象ポート）を指定します。 <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> に指定できる範囲は 1 ～ 66 です。</li> <li>• ※ <i>interface-id</i> には、モニター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（<b>port-channel</b> <i>port-channel-number</i>）があります。有効なポートチャネル番号は 1 ～ 48 です。</li> <li>• （任意）[, -] : 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを 1 つずつ入力します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• (オプション) <b>[both   rx   tx]</b> : モニターするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPAN は送信トラフィックと受信トラフィックの両方をモニターします。 <ul style="list-style-type: none"> <li>• <b>both</b> : 送信トラフィックと受信トラフィックの両方を監視します。これはデフォルトです。</li> <li>• <b>rx</b> : 受信トラフィックをモニタします。</li> <li>• <b>tx</b> : 送信トラフィックをモニタします。</li> </ul> </li> </ul> <p>(注) ※ <b>monitor session session_number source</b> コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>
ステップ 5	<p><b>monitor session session_number destination {interface interface-id [, -] [encapsulation replicate] [ingress {vlan vlan-id}]}</b></p> <p>例 :</p> <pre>Device(config)# monitor session 2 destination interface gigabitethernet1/2 encapsulation replicate ingress vlan 50</pre>	<p>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。</p> <ul style="list-style-type: none"> <li>• ※ <b>session_number</b> 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。</li> <li>• ※ <b>destination</b> には、次のパラメータを指定します。 <ul style="list-style-type: none"> <li>• ※ <b>interface-id</b> 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。</li> <li>• (任意) <b>,- </b> 一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。</li> <li>• (オプション) <b>encapsulation replicate</b> 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。</li> <li>• <b>ingress</b> 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。</li> </ul> </li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>vlan <i>vlan-id</i></b>—デフォルトの VLAN として指定した VLAN で、タグなしでカプセル化された着信パケットを受け入れます。</li> </ul> <p>(注) ローカル SPAN の場合は、送信元および宛先インターフェイスに同じセッション番号を使用する必要があります。</p> <p>※ <b>monitor session <i>session_number</i> destination</b> 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。</p>
ステップ 6	<b>monitor session <i>session_number</i> filter {ip   ipv6   mac} access-group {<i>access-list-number</i>   <i>name</i>}</b> 例 : <pre>Device(config)# monitor session 2 filter ipv6 access-group 4</pre>	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。 <ul style="list-style-type: none"> <li>• ※ <i>session_number</i> には、ステップ 4 で入力したセッション番号を指定します。</li> <li>• ※ <i>access-list-number</i> には、トラフィックのフィルタリングに使用する ACL 番号を指定します。</li> <li>• ※ <i>name</i> には、トラフィックのフィルタリングに使用する ACL の名前を指定します。</li> </ul>
ステップ 7	<b>end</b> 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 8	<b>show running-config</b> 例 : <pre>Device# show running-config</pre>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例 : <pre>Device# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

## FRSPAN セッションの設定

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

### 手順の概要

1. **enable**
2. **configure terminal**
3. **no monitor session** {*session\_number* | **all** | **local** | **remote**}
4. **monitor session** *session\_number* **source** {**interface** *interface-id* } [, | -] [**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	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <b>configure terminal</b>	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	<b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }	セッションに対する既存の SPAN 設定を削除します。
	例： Device(config)# <b>no monitor session 2</b>	<ul style="list-style-type: none"> <li>• ※ <i>session_number</i> に指定できる範囲は 1 ~ 66 です。</li> <li>• <b>all</b> : すべての SPAN セッションを削除します。</li> <li>• <b>local</b> : すべてのローカルセッションを削除します。</li> <li>• <b>remote</b> : すべてのリモート SPAN セッションを削除します。</li> </ul>



	コマンドまたはアクション	目的
ステップ 4	<p><b>monitor session</b> <i>session_number</i> <b>source</b> {<b>interface</b> <i>interface-id</i> } [, -] [<b>both</b>   <b>rx</b>   <b>tx</b>]</p> <p>例 :</p> <pre>Device(config)# monitor session 2 source interface gigabitethernet1/1</pre>	<p>SPANセッションおよび送信元ポート（モニター対象ポート）を指定します。</p> <ul style="list-style-type: none"> <li>• ※ <i>session_number</i>に指定できる範囲は1～66です。</li> <li>• ※ <i>interface-id</i>には、モニター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（<b>port-channel</b> <i>port-channel-number</i>）があります。有効なポートチャネル番号は1～48です。</li> <li>• ※ <i>vlan-id</i>には、モニターする送信元 VLAN を指定します。指定できる範囲は1～4094です（RSPAN VLAN は除く）。 <ul style="list-style-type: none"> <li>（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。</li> </ul> </li> <li>• （任意）, -]：一連のインターフェイスまたはインターフェイスの範囲を指定します。カンマの前後およびハイフンの前後にスペースを1つずつ入力します。</li> <li>• （オプション） [<b>both</b>   <b>rx</b>   <b>tx</b>]：モニターするトラフィックの方向を指定します。トラフィックの方向を指定しなかった場合、SPANは送信トラフィックと受信トラフィックの両方をモニターします。</li> <li>• <b>both</b>：送信トラフィックと受信トラフィックの両方を監視します。これはデフォルトです。</li> <li>• <b>rx</b>：受信トラフィックをモニタします。</li> <li>• <b>tx</b>：送信トラフィックをモニタします。</li> </ul> <p>（注） ※ <b>monitor session</b> <i>session_number</i> <b>source</b> コマンドを複数回使用すると、複数の送信元ポートを設定できます。</p>

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

## SPAN および RSPAN 動作のモニタリング

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

表 2: SPAN および RSPAN 動作のモニタリング

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

## SPAN および RSPAN の設定例

次のセクションに SPAN および RSPAN の設定例を示します

### 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。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1
Device(config)# monitor session 1 source interface gigabitethernet1/1
Device(config)# monitor session 1 destination interface gigabitethernet1/2
Device(config)# encapsulation replicate ingress vlan 7
Device(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。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 1 source interface gigabitethernet1/1
Device(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。

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

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

次に、SPANセッション2内の既存の設定を削除し、VLAN 1～3に属するすべてのポートで受信トラフィックをモニタするようにSPANセッション2を設定し、モニタされたトラフィックを宛先ポートGigabitEthernet2に送信する例を示します。さらに、この設定はVLAN 10に属するすべてのポートですべてのトラフィックをモニタするよう変更されます。

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source vlan 1 - 3 rx

Device(config)# monitor session 2 destination interface gigabitethernet1/2
Device(config)# monitor session 2 source vlan 10
Device(config)# end
```

次に、SPANセッション2の既存の設定を削除し、ギガビットイーサネットソース送信元ポート1上で受信されるトラフィックをモニタするようにSPANセッション2を設定し、そのトラフィックを送信元ポートと同じ出力カプセル化方式の宛先ギガビットイーサネットポート2に送信し、デフォルト入力VLANとしてVLAN 6を使用した入力転送をイネーブルにする例を示します。

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

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

```
Device> enable
Device# configure terminal
Device(config)# no monitor session 2
Device(config)# monitor session 2 source interface gigabitethernet1/2 rx
Device(config)# monitor session 2 filter vlan 1 - 5 , 9
Device(config)# monitor session 2 destination interface gigabitethernet1/1 ingress vlan
  10
Device(config)# end
```

## 例 : RSPAN VLAN の作成

この例は、RSPAN VLAN 901 の作成方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# vlan 901
Device(config-vlan)# remote span
Device(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。

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

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

```
Device> enable
Device# configure terminal
Device(config)# monitor session 1 source remote vlan 901
Device(config)# monitor session 1 destination interface gigabitethernet2/1 ingress vlan 10
Device(config)# end
```

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

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

例：RSPAN VLAN の作成

## 翻訳について

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