

# Catalyst スイッチド ポート アナライザ ( SPAN ) の設定例

## 目次

[概要](#)

[前提条件](#)

[SPAN、RSPAN および ERSPAN をサポートする Catalyst スイッチ](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[SPAN の簡単な説明](#)

[SPAN の用語](#)

[送信元ポートの特性](#)

[ソース VLAN の特性](#)

[宛先ポートの特性](#)

[リフレクタ ポートの特性](#)

[Catalyst Express 500/520 での SPAN](#)

[Catalyst 2900XL/3500XL スイッチでの SPAN](#)

[利用可能な機能と制約事項](#)

[設定例](#)

[ネットワーク図](#)

[Catalyst 2900XL/3500XL での設定例](#)

[設定手順の説明](#)

[Catalyst 2948G-L3 および 4908G-L3 での SPAN](#)

[Catalyst 8500 での SPAN](#)

[CatOS が稼働する Catalyst 2900、4500/4000、5500/5000、および 6500/6000 シリーズ スイッチでの SPAN](#)

[ローカル SPAN](#)

[PSPAN、VSPAN：一部のポートまたは VLAN 全体のモニタ](#)

[SPAN による単一ポートのモニタ](#)

[SPAN による複数ポートのモニタ](#)

[SPAN による VLAN のモニタ](#)

[入力/出力 SPAN](#)

[トランクでの SPAN の実装](#)

[トランクに属する VLAN のサブセット モニタリング](#)

[宛先ポートでのトランキング](#)

[複数同時セッションの作成](#)

[その他の SPAN オプション](#)

[リモート SPAN](#)

[RSPAN の概要](#)

[RSPAN の設定例](#)

[2つのスイッチ S1 および S2 間での ISL トランクの設定](#)

[RSPAN VLAN の作成](#)

[S2 のポート 5/2 を RSPAN の宛先ポートとして設定](#)

[S1 の RSPAN 送信元ポートの設定](#)

[設定の確認](#)

[set rspan コマンドで可能な他の設定](#)

[機能の概要と制限事項](#)

[Catalyst 2940、2950、2955、2960、2970、3550、3560、3560-E、3750 および 3750-E シリーズスイッチでの SPAN](#)

[Cisco IOS システム ソフトウェアが稼働する Catalyst 4500/4000 および Catalyst 6500/6000 シリーズスイッチでの SPAN](#)

[設定例](#)

[機能の概要と制限事項](#)

[異なる Catalyst プラットフォームでの SPAN のパフォーマンスへの影響](#)

[Catalyst 2900XL/3500XL シリーズ](#)

[アーキテクチャ概要](#)

[パフォーマンスへの影響](#)

[Catalyst 4500/4000 シリーズ](#)

[アーキテクチャ概要](#)

[パフォーマンスへの影響](#)

[Catalyst 5500/5000 および 6500/6000 シリーズ](#)

[アーキテクチャ概要](#)

[パフォーマンスへの影響](#)

[よくある質問と一般的な問題](#)

[SPAN の誤設定による接続の問題](#)

[SPAN 宛先ポートが「Up/Down」になります。](#)

[SPAN セッションでブリッジンググループが生成されるのはなぜですか。](#)

[SPAN はパフォーマンスに影響するでしょうか。](#)

[EtherChannel ポートで SPAN の設定はできますか。](#)

[同時に複数の SPAN セッションを実行できますか。](#)

[エラー：% Local Session Limit Has Been Exceeded](#)

[「% Session \[Session No:\] Used by Service Module」エラーにより、VPN サービス モジュールで SPAN セッションを削除できません。](#)

[SPAN で破損したパケットをキャプチャできないのはなぜですか。](#)

[エラー：%% Session 2 used by service module](#)

[リフレクタ ポートでパケットが廃棄されます。](#)

[SPAN セッションは常に、Catalyst 6500 シャーシの FWSM で使用されます。](#)

[SPAN と RSPAN セッションは同じスイッチ内で同じ ID を使用できますか。](#)

[RSPAN セッションは異なる VTP ドメインにわたって機能できますか。](#)

[RSPAN セッションは WAN または異なるネットワークにわたって機能できますか。](#)

[RSPAN ソース セッションおよび宛先セッションは同じ Catalyst スイッチに存在できますか。](#)

[SPAN 宛先ポートに接続されているネットワーク アナライザやセキュリティ デバイスに到達できません。](#)

[関連情報](#)

## 概要

このドキュメントでは、実装済みの Switched Port Analyzer (SPAN; スイッチドポートアナライザ) の最新の機能について説明します。SPAN 機能は、ポートミラーリングあるいはポートモニタリングとも呼ばれ、ネットワークアナライザによる分析のためのネットワークトラフィックを選択します。ネットワークアナライザは、Cisco SwitchProbe デバイスのこともあれば、その他の Remote Monitoring (RMON; リモートモニタリング) プロブのこともあります。以前は、SPAN は Cisco Catalyst シリーズ スイッチの比較的基本的な機能でした。しかし、Catalyst OS (CatOS) の最新のリリースでは、ユーザが利用可能な大幅な拡張と多くの新しい可能性を提供しています。このドキュメントは、SPAN 機能のための代替的な設計ガイドとして意図されたものではありません。この文書は、次のような SPAN についての最も一般的な疑問に答えるものです。

- SPAN とは何か、また、どのように設定するか。
- 使用できる諸機能 (特に複数の同時 SPAN セッション) は何か、また、それを実行するためにどのようなソフトウェアレベルが必要か。
- SPAN は、スイッチのパフォーマンスに影響を与えるか。

## 前提条件

### SPAN、RSPAN および ERSPAN をサポートする Catalyst スイッチ

Catalyst スイッチ	SPAN サポート	RSPAN サポート	ERSPAN サポート
Catalyst Express 500/520 シリーズ	○	なし	なし
Catalyst 6500/6000 シリーズ	○	○	可能 Cisco IOS ソフトウェア リリース 12.2(18)SXE 以降が稼働する、PFC4 を搭載した Supervisor 2T、PFC3B または PFC3BXL を搭載した Supervisor 720。ハードウェア バージョン 3.2 以降を使用し、また Cisco IOS ソフトウェア リリース 12.2(18)SXE 以降が稼働する PFC3A を搭載する Supervisor 720。
Catalyst 5500/5000 シリーズ	○	なし	なし
Catalyst 4900 シリーズ	○	○	なし
Catalyst 4500/4000 シリーズ (4912G を含む)	○	○	なし

Catalyst 3750 Metro シリーズ	○	○	なし
Catalyst 3750/3750E/3750X シリーズ	○	○	なし
Catalyst 3560/3560E/3650X シリーズ	○	○	なし
Catalyst 3550 シリーズ	○	○	なし
Catalyst 3500 XL シリーズ	○	なし	なし
Catalyst 2970 シリーズ	○	○	なし
Catalyst 2960 シリーズ	○	○	なし
Catalyst 2955 シリーズ	○	○	なし
Catalyst 2950 シリーズ	○	○	なし
Catalyst 2940 シリーズ	○	なし	なし
Catalyst 2948G-L3	なし	なし	なし
Catalyst 2948G-L2、2948G-GE-TX、2980G-A	○	○	なし
Catalyst 2900XL シリーズ	○	なし	なし
Catalyst 1900 シリーズ	○	なし	なし

## 要件

このドキュメントに関する固有の要件はありません。

## 使用するコンポーネント

このドキュメントの情報では、Catalyst 4500/4000、5500/5000、および 6500/6000 シリーズ スイッチの基準となる OS として CatOS 5.5 が使用されています。Catalyst 2900XL/3500XL シリーズ スイッチでは、Cisco IOS<sup>®</sup> ソフトウェア リリース 12.0(5)XU が使用されています。このドキュメントは SPAN の変更を反映するために更新されていますが、SPAN 機能の最新の開発情報については、使用しているスイッチ プラットフォーム ドキュメントのリリース ノートを参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始して

います。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## 表記法

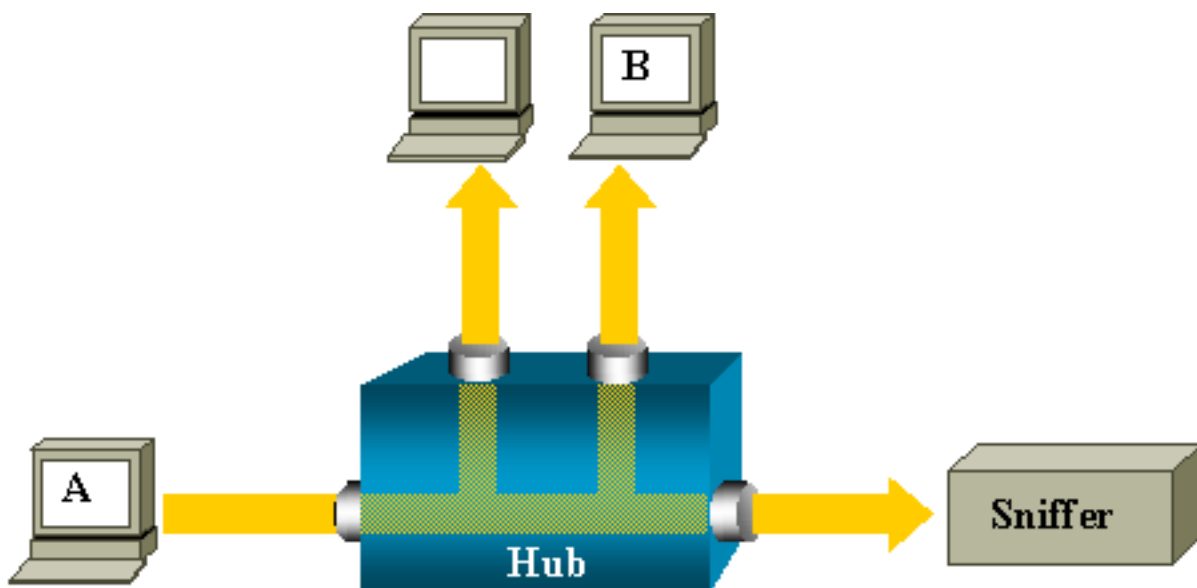
ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

## 背景説明

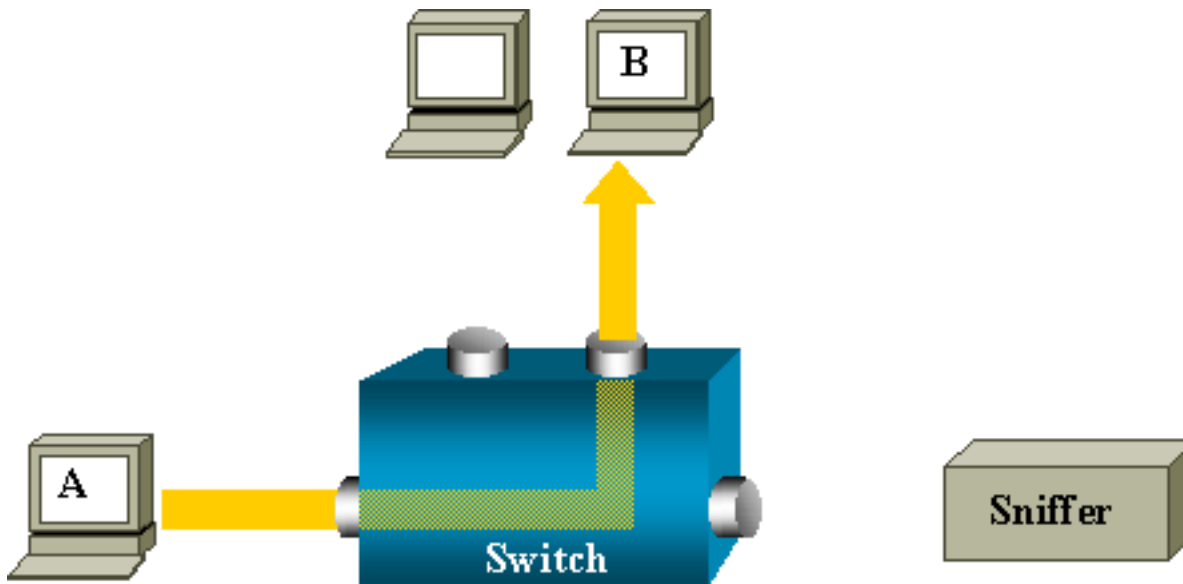
### SPAN の簡単な説明

SPAN とは何で、なぜ必要か。SPAN 機能は、スイッチがハブに関して持つ基本的な相違を補うために、スイッチに導入されました。ハブが 1 つのポートでパケットを受信すると、そのハブはパケットを受信したポート以外のすべてのポートにそのパケットのコピーを送信します。スイッチが起動すると、スイッチで受信されるさまざまなパケットのソース MAC アドレスに基づいて、レイヤ 2 フォワーディング テーブルの構築を開始します。このフォワーディング テーブルが作成された後、スイッチは MAC アドレス宛のトラフィックを該当ポートに直接に転送します。

たとえば、ホスト A からホスト B に送られたイーサネットトラフィックをキャプチャする場合、双方がハブに接続されているならば、このハブにスニファを接続するだけで済みます。他のすべてのポートで、ホスト A と B の間のトラフィックが見えます。



スイッチでホスト B の MAC アドレスが学習されると、ホスト A から B へのユニキャストトラフィックは B のポートだけに転送されます。そのため、スニファからはトラフィックが見えなくなります。

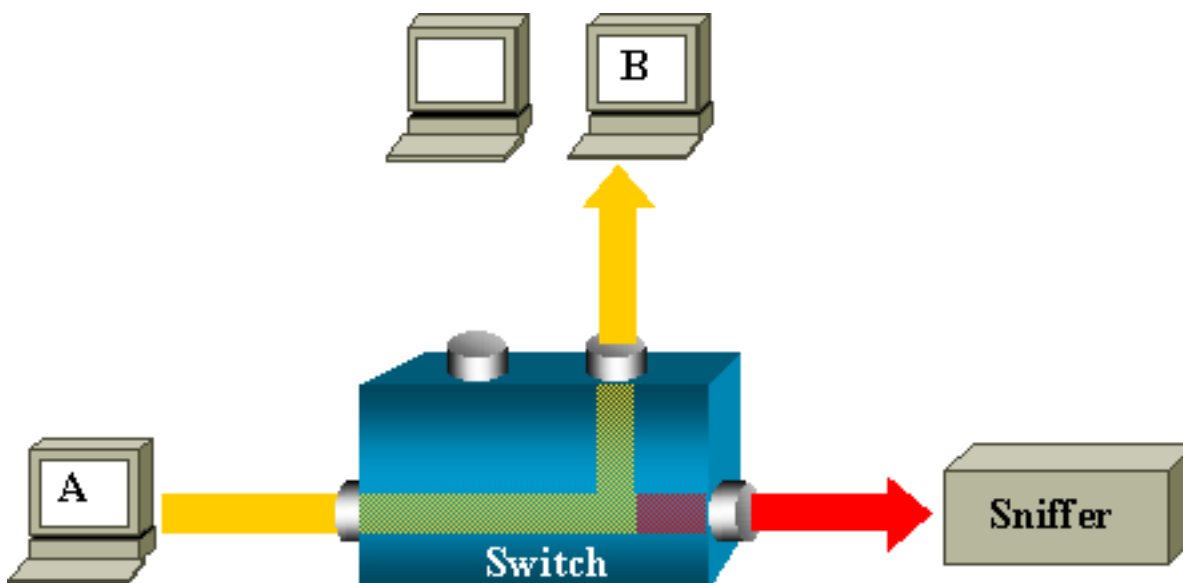


この設定では、スニファでは、次のようなすべてのポートにフラッドするトラフィックをキャプチャするだけです。

- ブロードキャスト トラフィック
- CGMP または Internet Group Management Protocol ( IGMP; インターネット グループ管理プロトコル ) のスヌーピングがディセーブルにされた状態でのマルチキャスト トラフィック
- 不明なユニキャスト トラフィック

ユニキャスト フラッディングが発生するのは、スイッチの Content-Addressable Memory ( CAM; 連想メモリ ) テーブルに宛先 MAC がない場合です。スイッチでは、トラフィックをどこに送信するのかがわかりません。スイッチは、宛先 VLAN のすべてのポートにパケットをフラッディングします。

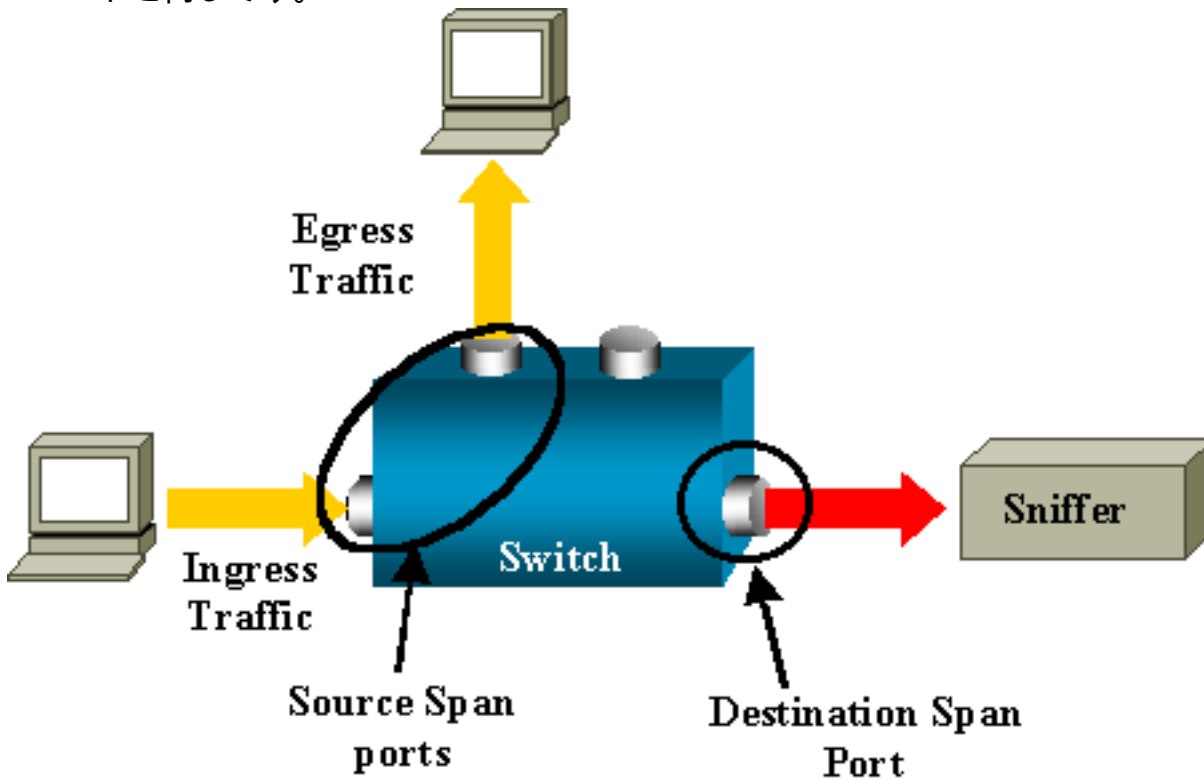
ホスト A によりスニファ ポートに送られるユニキャスト パケットを人工的にコピーする、追加機能が必要です。



この図では、ホスト A により送信されるすべてのパケットのコピーを受信するように設定されたポートに、スニファが接続されます。このポートを SPAN ポートと呼びます。このドキュメントの他のセクションでは、機能の範囲を単にポートのモニタに留まらせないようにするために、この機能を厳密に調整する方法について説明しています。

## SPAN の用語

- 入力トラフィック：スイッチに入るトラフィックです。
- 出力トラフィック：スイッチから出るトラフィックです。
- **送信元 (SPAN) ポート**：SPAN 機能を使用してモニタされるポートです。
- **ソース (SPAN) VLAN**：SPAN 機能を使用してトラフィックがモニタされる VLAN です。
- **宛先 (SPAN) ポート**：送信元ポートをモニタするポートで、通常、そのポートにネットワークアナライザが接続されます。
- **リフレクタポート**：RSPAN VLAN にパケットをコピーするポートです。
- **モニタポート**：モニタポートは、Catalyst 2900XL/3500XL/2950 の用語では、宛先 SPAN ポートと同じです。



- **ローカル SPAN**：モニタ対象ポートのすべてが、宛先ポートと同じスイッチ上にある場合、SPAN 機能はローカルです。この機能は、このリストでも定義されている Remote SPAN (RSPAN; リモート SPAN) と対比されます。
- **リモート SPAN (RSPAN)**：いくつかの送信元ポートは、宛先ポートと同じスイッチにはありません。RSPAN は、スイッチ間で SPAN によりモニタされるトラフィックを搬送するために、特別の VLAN を必要とする拡張機能です。RSPAN はすべてのスイッチでサポートされているわけではありません。導入しようとしているスイッチで RSPAN を使用できるか、該当するリリースノートまたはコンフィギュレーションガイドをチェックしてください。
- **ポートベース SPAN (PSPAN)**：ユーザが、スイッチ上で1つまたは複数の送信元ポートと1つの宛先ポートを指定します。
- **VLAN ベース SPAN (VSPAN)**：特定のスイッチで、ある特定の VLAN に属するすべてのポートをモニタするように、1つのコマンドで選択できます。
- **ESpan**：拡張 SPAN バージョンを意味します。この用語は、SPAN の発展期に追加機能を示すのに何度も使用されています。そのため、この用語は必ずしも明確ではありません。このドキュメントでは、この用語の使用を避けています。
- **管理ソース**：モニタ対象に設定された、送信元ポートまたは VLAN のリストです。
- **運用ソース**：実際にモニタされているポートのリストです。このポートのリストは、管理ソ

ースとは異なる場合があります。たとえば、シャットダウン モードにあるポートは、管理ソースには表示されますが、実際にはモニタされてはいません。

## 送信元ポートの特性

モニタ対象ポートとも呼ばれる送信元ポートは、ネットワークトラフィック分析のためにモニタするルーテッドポートまたはスイッチドポートです。単一のローカル SPAN セッションまたは RSPAN ソース セッションでは、受信 (Rx)、送信 (Tx)、または双方向 (両方) の送信元ポートトラフィックをモニタできます。スイッチは、任意の数の送信元ポート (スイッチで利用可能なポートの最大数まで)、および任意の数のソース VLAN をサポートします。

送信元ポートには次の特性があります。

- EtherChannel、ファストイーサネット、ギガビットイーサネットなどの、いずれかのポートタイプである可能性があります。
- 複数の SPAN セッションでモニタリングできます。
- 宛先ポートにはできません。
- 各送信元ポートは、モニタする方向 (入力、出力、またはその両方) で設定できます。EtherChannel ソースについては、モニタされる方向は、グループのすべての物理ポートに適用されます。
- 送信元ポートは、同じ VLAN にある場合もあれば、異なる VLAN にある場合もあります。
- VLAN SPAN ソースに関しては、ソース VLAN 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ます。

## 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、トランクでアクティブなすべての VLAN はデフォルトでモニタされます。特定の VLAN に対して、トランク送信元ポートで SPAN トラフィックのモニタリングを制限するために、VLAN フィルタリングを使用できます。

- VLAN フィルタリングを適用するのは、トランクポートか音声 VLAN ポートだけです。
- VLAN フィルタリングは、ポートベースのセッションにだけ適用し、VLAN ソースを使用するセッションでは許可されません。
- VLAN フィルタリストが指定される場合、リスト内の VLAN だけがトランクポートまたは音声 VLAN アクセスポートでモニタされます。
- 他のポートタイプから来ている 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。それは、他のポートではすべての VLAN が許可されていることを意味します。
- VLAN フィルタリングが影響するのは、宛先 SPAN ポートに転送されるトラフィックだけで、通常のトラフィックのスイッチングには影響しません。
- 1つのセッション内に、ソース VLAN とフィルタ VLAN を混在させることはできません。ソース VLAN を置くか、あるいはフィルタ VLAN を置くことはできますが、同時に両方を置くことはできません。

## ソース VLAN の特性

VSPAN は、1つ以上の VLAN のネットワークトラフィックのモニタリングです。VSPAN 内の SPAN または RSPAN ソース インターフェイスは VLAN ID であり、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。

- ソース VLAN 内のすべてのアクティブ ポートは送信元ポートに含まれ、片方向または両方向でモニタできます。
- 任意のポートで、モニタ対象の VLAN のトラフィックだけが宛先ポートに送られます。
- 宛先ポートがソース VLAN に属する場合は、ソース リストから除外され、モニタされません。
- ソース VLAN でポートが追加または削除される場合、それらのポートで受信されるソース VLAN のトラフィックは、モニタ対象のソースに追加されるか、モニタ対象のソースから削除されます。
- VLAN ソースと同じセッションでフィルタ VLAN を使用できません。
- モニタできるのは、イーサネット VLAN だけです。

## 宛先ポートの特性

各ローカル SPAN セッションまたは RSPAN 宛先セッションは、送信元ポートと VLAN からトラフィックのコピーを受け取る宛先ポート ( モニタリング ポートとも呼ばれる ) を持つ必要があります。

宛先ポートには次の特性があります。

- 宛先ポートは送信元ポートと同じスイッチにある必要があります ( ローカル SPAN セッションの場合 ) 。
- 任意のイーサネット物理ポートを宛先ポートにできます。
- 宛先ポートが参加できるのは、一度に 1 つの SPAN セッションだけです。1 つの SPAN セッションの宛先ポートを、2 番目の SPAN セッションの宛先ポートにはできません。
- 宛先ポートは、送信元ポートにはできません。
- 宛先ポートは、EtherChannel グループにはできません。注: Cisco IOS ソフトウェア リリース 12.2(33)SXH 以降では、PortChannel インターフェイスを宛先ポートにできます。宛先 EtherChannel では、Port Aggregation Control Protocol ( PAgP ) または Link Aggregation Control Protocol ( LACP ) EtherChannel プロトコルをサポートしません。すべての EtherChannel プロトコルのサポートをディセーブルにしている場合に、オン モードだけがサポートされます。注: 詳細については、「[ローカル SPAN、RSPAN、および ERSPAN の宛先](#)」を参照してください。
- EtherChannel グループが SPAN ソースとして指定されている場合でも、EtherChannel グループに割り当てられている物理ポートを宛先ポートにすることは可能です。そのポートは SPAN 宛先ポートとして設定されている間、グループからは削除されます。
- ポートは、学習機能がイネーブルになっていない場合、SPAN セッションに必要なトラフィック以外のトラフィックを送信しません。学習機能がイネーブルになっている場合、ポートは宛先ポートで学習されたホストに対するトラフィックも送信します。注: 詳細については、「[ローカル SPAN、RSPAN、および ERSPAN の宛先](#)」を参照してください。
- 設計では、宛先ポートの状態は「Up/Down」となっています。インターフェイスは、現在、ポートが実稼働ポートとして使用できないことを明確にするために、この状態でポートを表示します。
- ネットワーク セキュリティ デバイスで入カトラフィックの転送がイネーブルになっている場合、宛先ポートではレイヤ 2 でトラフィックを転送します。
- 宛先ポートは、SPAN セッションがアクティブな間は、スパンニング ツリーに参加しません。
- それは、宛先ポートになっている場合、レイヤ 2 プロトコル ( STP、VTP、CDP、DTP、

PagP ) の何れにも参加しません。

- いずれかの SPAN セッションのソース VLAN に属する宛先ポートは、ソース リストから除外され、モニタされません。
- 宛先ポートは、モニタ対象になっているすべての送信元ポートの送受信トラフィックのコピーを受け取ります。宛先ポートがオーバーサブスクライブされている場合、輻輳状態になる可能性があります。この輻輳により、1 つ以上の送信元ポートのトラフィックの転送が影響を受ける可能性があります。

## リフレクタ ポートの特性

リフレクタ ポートは、RSPAN VLAN にパケットをコピーするためのメカニズムです。リフレクタ ポートは、提携する RSPAN ソース セッションからのトラフィックだけを転送します。RSPAN ソース セッションがディセーブルになるまで、リフレクタ ポートとして設定されているポートに接続されているどのデバイスでも接続が失われます。

リフレクタ ポートには次の特性があります。

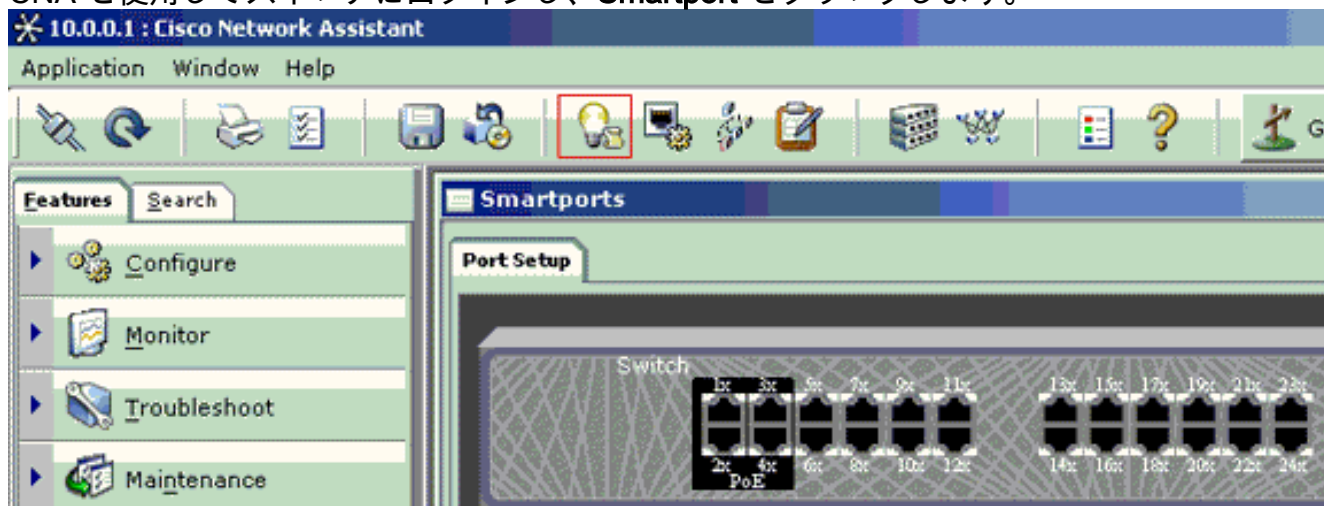
- ループバックに設定されたポートです。
- EtherChannel グループにはなれず、トランキングはできず、プロトコル フィルタリングもできません。
- EtherChannel グループが SPAN ソースとして指定されている場合でも、EtherChannel グループに割り当てられている物理ポートをリフレクタ ポートにすることは可能です。リフレクタ ポートとして設定されている間、そのポートはグループから削除されます。
- リフレクタ ポートとして使用されるポートは、SPAN ソースまたは宛先ポートのいずれにもできず、さらに、ポートを一度に複数のセッションに対応するリフレクタ ポートにすることもできません。
- リフレクタ ポートは、すべての VLAN に対して非表示になります。
- リフレクタ ポート上のループバックトラフィックのネイティブ VLAN は、RSPAN VLAN です。
- リフレクタ ポートでは、タグなしのトラフィックはスイッチにループバックされます。そのトラフィックは RSPAN VLAN に置かれ、RSPAN VLAN を運ぶあらゆるトランク ポートにフラッディングされます。
- リフレクタ ポートでは、スパニング ツリーは自動的にディセーブルにされます。
- リフレクタ ポートは、モニタ対象のすべての送信元ポートでの送受信トラフィックのコピーを受け取ります。

## Catalyst Express 500/520 での SPAN

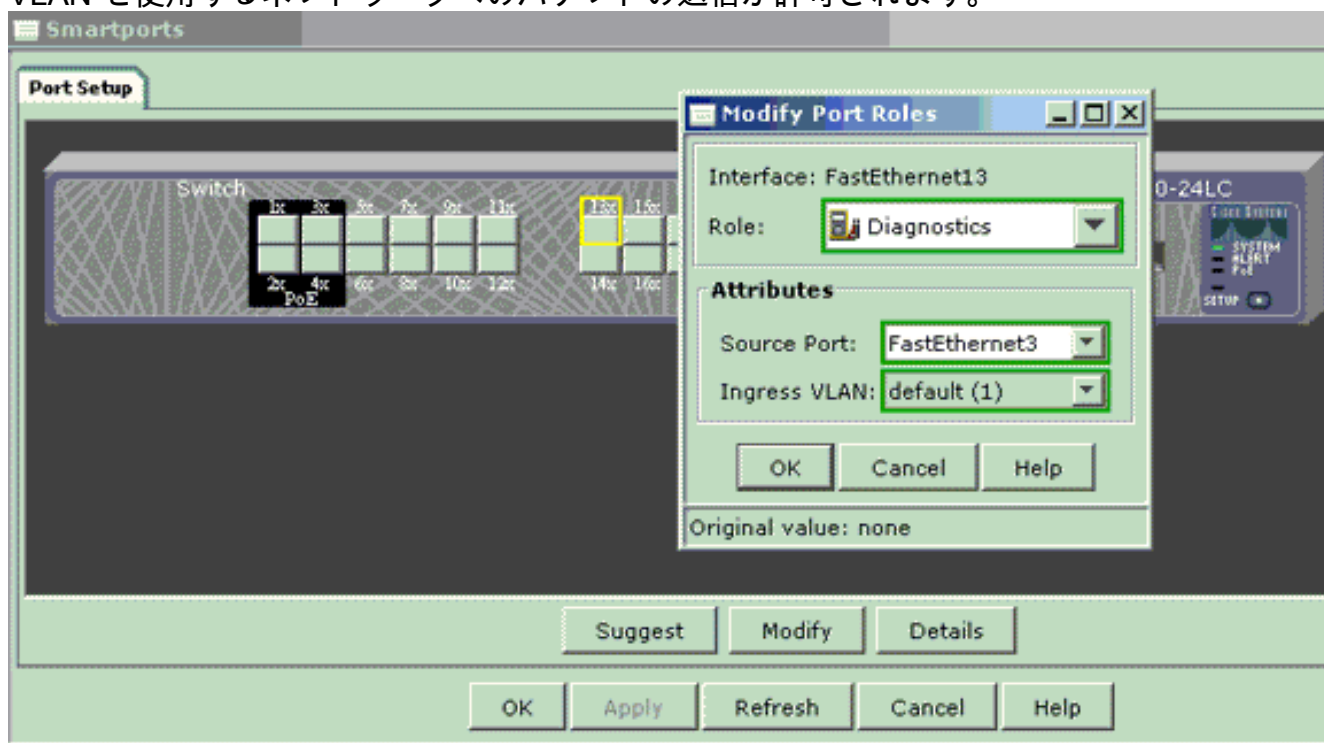
Catalyst Express 500 または Catalyst Express 520 では、SPAN 機能だけがサポートされます。Catalyst Express 500/520 のポートは、Cisco Network Assistant ( CNA ) を使用してのみ、SPAN に設定できます。SPAN を設定するには、次の手順を実行します。

1. PC に CNA をダウンロードしてインストールします。CNA は、「[ソフトウェアダウンロード](#)」( 登録ユーザ専用 ) ページからダウンロードできます。
2. Catalyst Express 500 のスイッチの設定をカスタマイズするには、「[Catalyst Express 500 スイッチ 12.2\(25\)FY の入門ガイド](#)」で説明されている手順を実行します。Catalyst Express 520 についての詳細は、「[Catalyst Express 520 スイッチの入門ガイド](#)」を参照してください。

3. CNA を使用してスイッチにログインし、Smartport をクリックします。



4. スニファトレースをキャプチャするには、PC に接続するインターフェイスをクリックします。
5. **Modify** をクリックします。小さいポップアップボックスが表示されます。
6. ポートで [Diagnostics] ロールを選択します。
7. 送信元ポートを選択し、モニタする VLAN を選択します。どれも選択しない場合、ポートはトラフィックだけを受信します。入力 VLAN では、診断ポートに接続された PC に、その VLAN を使用するネットワークへのパケットの送信が許可されます。



8. OK をクリックして、ポップアップボックスを閉じます。
9. OK をクリックし、次に **Apply** をクリックして設定します。
10. 診断ポートを設定すると、トラフィックをトレースするために任意のスニファソフトウェアを使用できます。

## Catalyst 2900XL/3500XL スイッチでの SPAN

### 利用可能な機能と制約事項

Catalyst 2900XL/3500XL でのポート モニタリング機能は、さほど広範囲なものではありません。そのため、この機能は比較的理解しやすいものです。

必要に応じてローカル PSPAN セッションを作成できます。たとえば、宛先 SPAN ポートとして選択した構成ポートで PSPAN セッションを作成できます。この場合は、[port monitor interface コマンド](#)を発行して、モニタする送信元ポートをリストします。モニタ ポートとは、Catalyst 2900XL/3500XL の用語では、宛先 SPAN ポートを指します。

- 主な制限として、特定のセッションに関連するすべてのポートが (送信元または宛先を問わず) 同じ VLAN に属している必要があります。
- IP アドレスで VLAN インターフェイスを設定する場合、port monitor コマンドは、その IP アドレスを宛先とするトラフィックだけをモニタします。このコマンドは、VLAN インターフェイスで受信されるブロードキャストトラフィックもモニタします。しかし、実際の VLAN に流入するトラフィックをキャプチャするわけではありません。port monitor コマンドでインターフェイスを指定しない場合、同じ VLAN に属するすべてのポートがインターフェイスとしてモニタされます。

次のリストは、いくつかの制約事項を示しています。詳細は、コマンドリファレンスガイド (Catalyst 2900XL/3500XL) を参照してください。

注: ATM ポートは、唯一モニタ ポートにできないポートです。しかし、ATM ポートをモニタすることは可能です。次のリストの制約事項は、ポート モニタ機能を備えるポートに適用されます。

- モニタ ポートは、ファスト イーサチャネルまたはギガビット イーサチャネル ポート グループには入れません。
- ポート セキュリティについては、モニタ ポートを有効にできません。
- モニタ ポートは、マルチ VLAN ポートにはできません。
- モニタ ポートは、モニタ対象のポートと同じ VLAN のメンバである必要があります。VLAN メンバシップの変更は、モニタ ポートおよびモニタ対象のポートでは許可されません。
- モニタ ポートは、ダイナミック アクセス ポートまたはトランク ポートにはできません。しかし、スタティック アクセス ポートでは、トランク上の VLAN、マルチ VLAN、またはダイナミック アクセス ポートをモニタできます。モニタ対象の VLAN は、スタティック アクセス ポートに関連するものです。
- モニタ ポートとモニタ対象のポートの双方がプロテクト ポートである場合は、ポート モニタは動作しません。

モニタ状態にあるポートでは、Spanning Tree Protocol (STP; スパニング ツリー プロトコル) は実行されませんが、ポートがミラーリングしているポートの VLAN に属していることには注意してください。たとえば、ハブやブリッジに接続してネットワークの他の部分へのループを形成している場合、ポート モニタがループの一部になっている可能性があります。この場合、STP による保護は受けていないので、破滅的なブリッジング ループ状態に陥る危険があります。この状態がどのように発生する可能性があるかの例については、このドキュメントの「[SPAN セッションでブリッジング ループが生成されるのはなぜですか。](#)」セクションを参照してください。

## 設定例

次の例では、2 つの同時 SPAN セッションが作成されます。

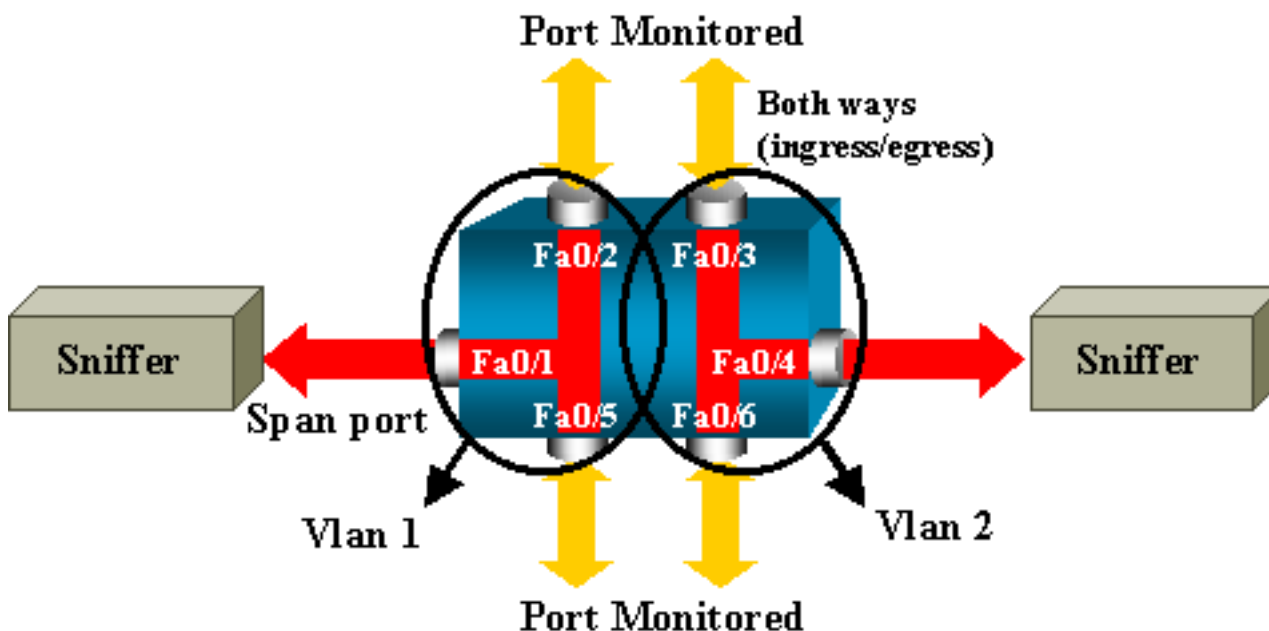
- ポート Fast Ethernet 0/1 (Fa0/1) では、ポート Fa0/2 および Fa0/5 により送受信されるト

ラフィックをモニタしています。ポート Fa0/1 は、管理インターフェイス VLAN 1 で送受信されるトラフィックもモニタします。

- ポート Fa0/4 では、ポート Fa0/3 および Fa0/6 をモニタします。

ポート Fa0/3、Fa0/4、および Fa0/6 は、すべて VLAN 2 に設定されています。他のポートおよび管理インターフェイスは、デフォルトの VLAN 1 に設定されています。

## ネットワーク図



## Catalyst 2900XL/3500XL での設定例

### 2900XL/3500XL SPAN 設定例

```
!--- Output suppressed.
interface FastEthernet0/1
port monitor FastEthernet0/2
port monitor FastEthernet0/5
port monitor VLAN1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
!
interface FastEthernet0/4
port monitor FastEthernet0/3
port monitor FastEthernet0/6
switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
switchport access vlan 2
!
!--- Output suppressed.
!
interface VLAN1
ip address 10.200.8.136 255.255.252.0
```

```
no ip directed-broadcast
no ip route-cache
!
!--- Output suppressed.
```

## 設定手順の説明

ポート Fa0/1 を宛先ポートとして、また送信元ポート Fa0/2、Fa0/5 および管理インターフェイス (VLAN 1) を設定するには、次のようにコンフィギュレーション モードでインターフェイス Fa0/1 を選択してください。

```
Switch(config)#interface fastethernet 0/1
```

モニタされるポートのリストを入力する。

```
Switch(config-if)#port monitor fastethernet 0/2
Switch(config-if)#port monitor fastethernet 0/5
```

このコマンドにより、これら 2 つのポートで送受信されるすべてのパケットは、ポート Fa0/1 にもコピーされます。port monitor コマンドのバリエーションを次のように発行して、管理インターフェイスのモニタリングを設定します。

```
Switch(config-if)#port monitor vlan 1
```

**注:** このコマンドは、ポート Fa0/1 が VLAN 1 全体をモニタすることを意味しません。vlan 1 というキーワードは、単にスイッチの管理インターフェイスを指しているだけです。

次のコマンドの例は、異なる VLAN にあるポートのモニタはできないことを示しています。

```
Switch(config-if)#port monitor fastethernet 0/3
FastEthernet0/1 and FastEthernet0/3 are in different vlan
```

設定を終了するには、他のセッションを設定します。今回は、Fa0/4 を宛先 SPAN ポートとして使用します。

```
Switch(config-if)#interface fastethernet 0/4
Switch(config-if)#port monitor fastethernet 0/3
Switch(config-if)#port monitor fastethernet 0/6
Switch(config-if)#^Z
```

設定を確認するには、show running コマンドを発行するか、または、show port monitor コマンドを使用します。

```
Switch#show port monitor
Monitor Port Port Being Monitored
```

```
-----
FastEthernet0/1 VLAN1
FastEthernet0/1 FastEthernet0/2
FastEthernet0/1 FastEthernet0/5
FastEthernet0/4 FastEthernet0/3
FastEthernet0/4 FastEthernet0/6
```

**注:** Catalyst 2900XL および 3500XL では、Rx 方向のみの SPAN ( Rx SPAN または入力 SPAN ) または Tx 方向のみの SPAN ( Tx SPAN または出力 SPAN ) はサポートされていません。すべての SPAN ポートは、Rx および Tx トラフィックの両方をキャプチャする設計になっています。

# Catalyst 2948G-L3 および 4908G-L3 での SPAN

Catalyst 2948G-L3 および Catalyst 4908G-L3 は、固定構成のスイッチ ルータ、またはレイヤ 3 スイッチです。レイヤ 3 スイッチの SPAN 機能は、ポート スヌーピングと呼ばれます。しかし、これらのスイッチでは、ポート スヌーピングはサポートされていません。『Cisco IOS ソフトウェア リリース 12.0(10)W5(18g) に関する Catalyst 2948G-L3 および Catalyst 4908G-L3 リリース ノート』ドキュメントの「[サポートされていない機能](#)」セクションを参照してください。

## Catalyst 8500 での SPAN

Catalyst 8540 では、非常に基本的な SPAN 機能が、ポート スヌーピングの名前で利用可能です。追加情報については、現行の Catalyst 8540 のドキュメントを参照してください。

ポート スヌーピングを使用すれば、1 つ以上の送信元ポートから宛先ポートへのトラフィックを透過的にミラーリングできます。

ポートベーストラフィックのミラーリング、またはスヌーピングを設定するには、`snoop` コマンドを発行します。スヌーピングをディセーブルにするには、このコマンドの `no` 形式を発行します。

```
snoop interface source_port direction snoop_direction
```

```
no snoop interface source_port
```

変数 `source_port` はモニタ対象のポートを指します。変数 `snoop_direction` は、送信元ポートまたはモニタ対象のポートでのトラフィックの方向です。receive、transmit、または both。

```
8500CSR#configure terminal
8500CSR(config)#interface fastethernet 12/0/15
8500CSR(config-if)#shutdown
8500CSR(config-if)#snoop interface fastethernet 0/0/1 direction both
8500CSR(config-if)#no shutdown
```

次の例は、`show snoop` コマンドの出力結果を示しています。

```
8500CSR#show snoop
Snoop Test Port Name: FastEthernet1/0/4 (interface status=SNOOPING)
Snoop option: (configured=enabled)(actual=enabled)
Snoop direction: (configured=receive)(actual=receive)
Monitored Port Name:
(configured=FastEthernet1/0/3)(actual=FastEthernet1/0/3)
```

注: 8540m-in-mz のような Multiservice ATM Switch Router (MSR; マルチサービス ATM スイッチ ルータ) のイメージを実行している場合、このコマンドは、Catalyst 8540 のイーサネットポートではサポートされません。代わりに、8540c-in-mz のような campus switch router (CSR; キャンパス スイッチ ルータ) イメージを使用する必要があります。

## CatOS が稼働する Catalyst 2900、4500/4000、5500/5000、および 6500/6000 シリーズ スイッチでの SPAN

このセクションは、次の Cisco Catalyst 2900 シリーズ スイッチのみに適用されます。

- Cisco Catalyst 2948G-L2 スイッチ
- Cisco Catalyst 2948G-GE-TX スイッチ
- Cisco Catalyst 2980G-A スイッチ

このセクションは、次を含む Cisco Catalyst 4000 シリーズ スイッチに適用されます。

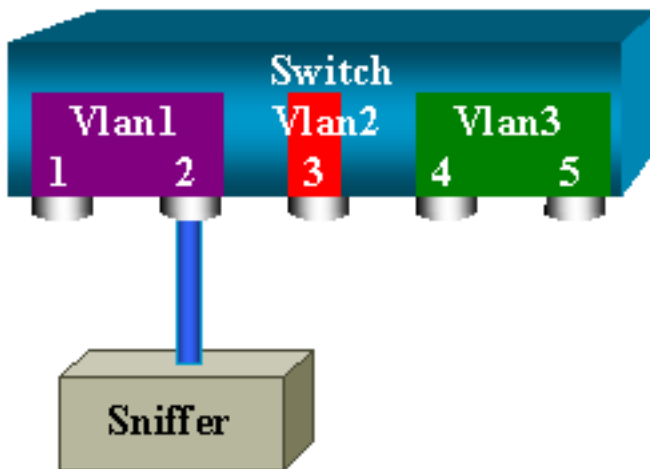
- モジュラ シャーシ スイッチ : Cisco Catalyst 4003 スイッチ Cisco Catalyst 4006 スイッチ
- 固定シャーシ スイッチ : Cisco Catalyst 4912G スイッチ

## ローカル SPAN

CatOS には SPAN 機能が 1 つずつ追加されて来ましたが、SPAN の設定に必要なコマンドは `set span` だけです。コマンドには、広範囲のオプションが利用可能になりました。

```
switch (enable) set span
Usage: set span disable [dest_mod/dest_port|all]
set span <src_mod/src_ports...|src_vlans...|sc0>
<dest_mod/dest_port> [rx|tx|both]
[inpkts <enable|disable>]
[learning <enable|disable>]
[multicast <enable|disable>]
[filter <vlans...>]
[create]
```

次のネットワーク ダイアグラムは、バリエーションの使用によるさまざまな SPAN の可能性を示しています。



このダイアグラムは、Catalyst 6500/6000 スイッチのスロット 6 にある 1 枚のラインカードの部分を表しています。このシナリオでは次のようになっています。

- ポート 6/1 と 6/2 は VLAN 1 に属しています。
- ポート 6/3 は VLAN 2 に属しています。
- ポート 6/4 と 6/5 は VLAN 3 に属しています。

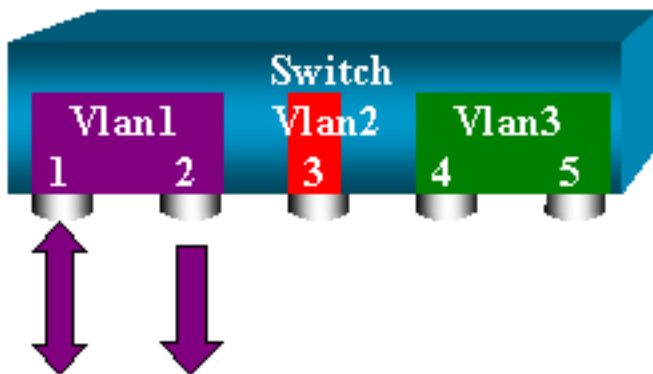
ポート 6/2 にスニファを接続し、複数の異なるケースでモニタ ポートとして使用します。

## PSPAN、VSPAN: 一部のポートまたは VLAN 全体のモニタ

単一ポートのモニタには、`set span` コマンドの最も単純な形式を使用します。構文は、`set span source_port destination_port` です。



## SPAN による単一ポートのモニタ



```
switch (enable) set span 6/1 6/2
```

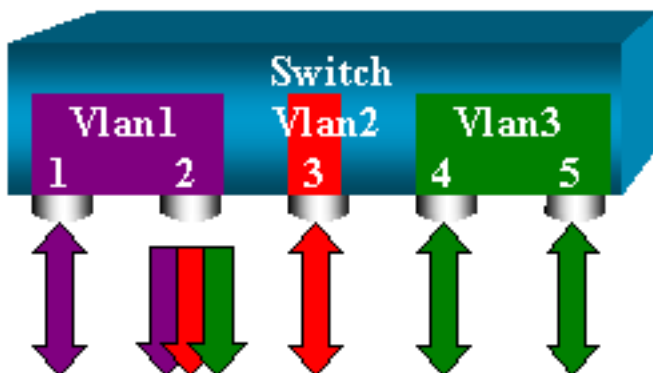
```
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:04:14 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

この設定では、ポート 6/1 で送受信されるすべてのパケットが、ポート 6/2 にコピーされます。設定を入力する際に、この明確な説明が表示されます。現在の SPAN 設定の要約を入手するには、**show span** コマンドを発行します。

```
switch (enable) show span
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
```

```
Total local span sessions: 1
```

## SPAN による複数ポートのモニタ



**set span source\_ports destination\_port** コマンドでは、ユーザは複数の送信元ポートの指定が可能

です。SPAN を実装するすべてのポートを単にリストして、ポートをコンマで区切ります。コマンドライン インタープリタでは、ハイフンを使用して、ポートの範囲を指定することも可能です。次の例は、複数のポートを指定するこの機能を説明したものです。例では、ポート 6/1 および、6/3 から 6/5 までの 3 つのポート範囲で SPAN を使用しています。

注: 宛先ポートは 1 つだけの場合もあります。宛先ポートは常に、SPAN ソースの後に指定してください。

```
switch (enable) set span 6/1,6/3-5 6/2
```

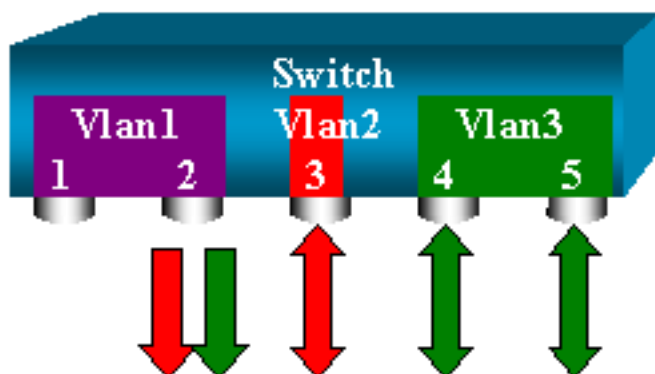
```
2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1,6/3-5
Oper Source : Port 6/1,6/3-5
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

注: Catalyst 2900XL/3500XL スイッチとは異なり、Catalyst 4500/4000、5500/5000、および 6500/6000 では、5.1 よりも前の CatOS バージョンで、複数の異なる VLAN に属するポートのモニタが可能です。ここでは、ミラーポートは VLAN 1、2、および 3 に割り当てられています。

## SPAN による VLAN のモニタ

最終的には、**set span** コマンドで、VLAN 全体のローカルトラフィックをモニタするポートを設定できます。コマンドは、**set span source\_vlan(s) destination\_port** です。

ポートのリストの代わりに、1 つ以上の VLAN のリストをソースとして使用します。



```
switch (enable) set span 2,3 6/2
```

```
2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 2-3
Oper Source : Port 6/3-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
```

```
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

この設定では、VLAN 2 または 3 に出入りするすべてのパケットは、ポート 6/2 にコピーされま  
す。

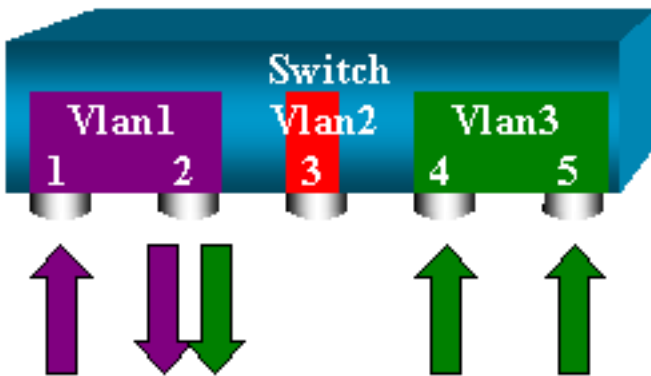
注: これは、このコマンドで指定された VLAN に属するすべてのポートで、個別に SPAN を  
実装したのとまったく同じ結果になります。Oper Source フィールドと Admin Source フィ  
ールドを比較します。Admin Source フィールドには基本的に、SPAN セッション用に設定  
したすべてのポートがリストされ、Oper Source フィールドには SPAN を使用するポート  
がリストされます。

## 入力/出力 SPAN

「[SPAN による VLAN のモニタ](#)」セクションの例では、指定したポートに出入りするトラフィッ  
クがモニタされていました。Direction: transmit/receive フィールドが、これを示しています。  
Catalyst 4500/4000、5500/5000、および 6500/6000 シリーズ スイッチでは、特定のポートで、  
出力 (アウトバウンド) あるいは入力 (インバウンド) トラフィックの一方だけ収集することも  
可能です。コマンドの最後に rx (受信) または tx (送信) キーワードを追加してください。デ  
フォルト値は both (tx および rx) です。

```
set span source_port destination_port [rx | tx | both]
```

この例では、セッションは VLAN 1 および 3 のすべての着信トラフィックをキャプチャし、ポ  
ート 6/2 へトラフィックをミラーリングします。



```
switch (enable) set span 1,3 6/2 rx
2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span session
inactive for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 1,3
Oper Source : Port 1/1,6/1,6/4-5,15/1
Direction : receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

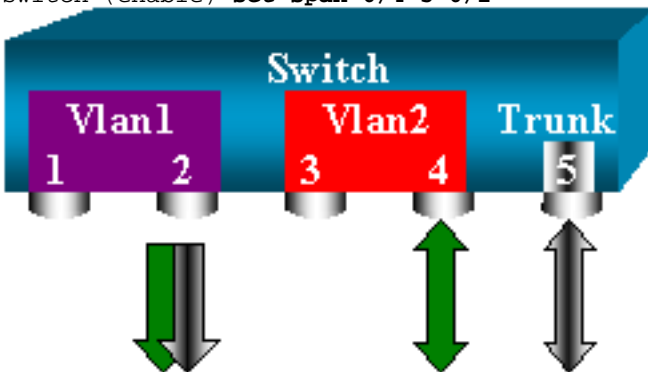
## トランクでの SPAN の実装

トランクは、複数の VLAN を搬送するポートなので、スイッチでの特例になります。トランクが送信元ポートとして選択されると、このトランクのすべての VLAN のトラフィックがモニタされます。

### トランクに属する VLAN のサブセット モニタリング

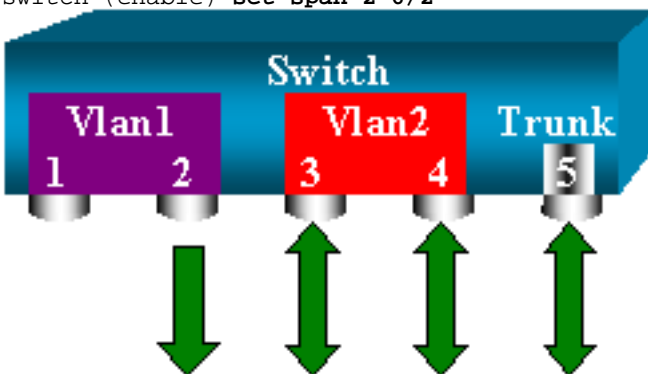
次のダイアグラムでは、ポート 6/5 は、すべての VLAN を搬送するトランクになっています。ポート 6/4 および 6/5 について VLAN 2 のトラフィックに対して SPAN を使用する状況を考えます。次のコマンドを発行します。

```
switch (enable) set span 6/4-5 6/2
```



この場合、SPAN ポートで受信するトラフィックには、必要なトラフィックとトランク 6/5 で搬送されるすべての VLAN が混在しています。たとえば、パケットが VLAN 2 のポート 6/4 が VLAN 1 のポート 6/5 から来るかどうか、宛先ポートで区別する方法はありません。ほかの目的で VLAN 2 の SPAN を使用します。

```
switch (enable) set span 2 6/2
```

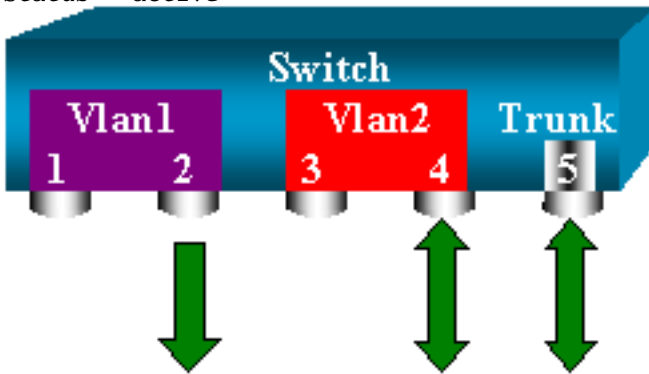


この設定では、最低限、VLAN 2 に属するトラフィックだけをトランクからモニタします。問題は、望んでいないポート 6/3 からのトラフィックも受信してしまうことです。CatOS には、トランクからモニタする VLAN を選択することを可能にする、次のようなキーワードが備わっています。

```
switch (enable) set span 6/4-5 6/2 filter 2
```

```
2000 Sep 06 02:31:51 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/4-5
Oper Source : Port 6/4-5
Direction : transmit/receive
```

Incoming Packets: disabled  
Learning : enabled  
Multicast : enabled  
Filter : 2  
Status : active



このコマンドでは、モニタ対象のすべてのトランクから VLAN 2 だけを選択するため、目的が達成できます。この filter オプションで複数の VLAN を指定できます。

注: この filter オプションがサポートされているのは、Catalyst 4500/4000 および Catalyst 6500/6000 スイッチだけです。Catalyst 5500/5000 では、**set span** コマンドで使用できる filter オプションはサポートされていません。

## 宛先ポートでのトランキング

複数の異なる VLAN に属する送信元ポートがある場合、またはトランクポートで複数の VLAN に SPAN を使用している場合、宛先 SPAN ポートで受信しているパケットが、どの VLAN に属するのか識別する必要がある可能性があります。この識別は、ポートを SPAN に設定する前に、宛先ポートでトランキングをイネーブルにすると可能です。この方法で、スニファに転送されるすべてのパケットは、その対応する VLAN ID でタグ付けされます。

注: スニファは、対応しているカプセル化を認識する必要があります。

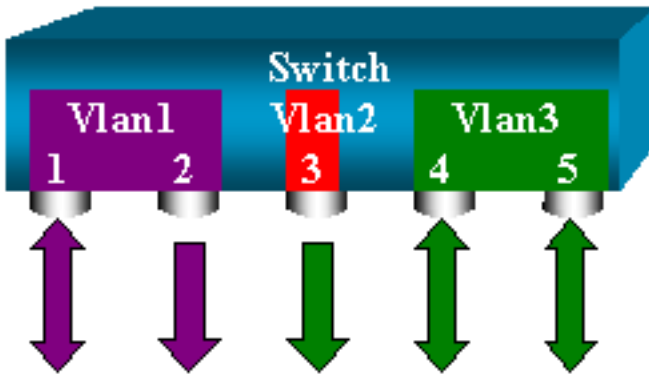
```
switch (enable) set span disable 6/2
This command will disable your span session.
Do you want to continue (y/n) [n]?y
Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/4-5
2000 Sep 06 02:52:22 %SYS-5-SPAN_CFGSTATECHG:local span session
inactive for destination port 6/2
switch (enable) set trunk 6/2 nonegotiate isl

Port(s) 6/2 trunk mode set to nonegotiate.
Port(s) 6/2 trunk type set to isl.
switch (enable) 2000 Sep 06 02:52:33 %DTP-5-TRUNKPORTON:Port 6/2 has become
isl trunk
switch (enable) set span 6/4-5 6/2
Destination : Port 6/2
Admin Source : Port 6/4-5
Oper Source : Port 6/4-5
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
```

```
2000 Sep 06 02:53:23 %SYS-5-SPAN_CFGSTATECHG:local span session active for
destination port 6/2
```

## 複数同時セッションの作成

ここまでで、単一の SPAN セッションが作成されています。新規の **set span** コマンドを入力するたびに、それ以前の設定は無効になります。CatOS には、複数セッションを同時に実行する機能が備わりました。つまり、異なる宛先ポートを同時に持つことができます。SPAN セッションを追加するには、**set span source destination create** コマンドを発行します。次のセッションでは、ポート 6/1 から 6/2、そして同時に VLAN 3 からポート 6/3 をモニタします。



```
switch (enable) set span 6/1 6/2
2000 Sep 05 08:49:04 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:49:05 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
switch (enable) set span 3 6/3 create
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:55:38 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/3
```

次のように **show span** コマンドを発行して、同時に 2 つのセッションがあるか判別します。

```
switch (enable) show span
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
```

Status : active

-----  
Destination : Port 6/3  
Admin Source : VLAN 3  
Oper Source : Port 6/4-5,15/1  
Direction : transmit/receive  
Incoming Packets: disabled  
Learning : enabled  
Multicast : enabled  
Filter : -  
Status : active

Total local span sessions: 2

追加のセッションが作成されました。セッションを削除する方法も必要です。コマンドは次のとおりです。

```
set span disable {all | destination_port}
```

宛先ポートはセッションごとに1つだけ存在するため、宛先ポートでセッションが識別されます。ポート 6/2 を宛先として使用する、作成された最初のセッションを削除します。

```
switch (enable) set span disable 6/2
```

This command will disable your span session.

Do you want to continue (y/n) [n]?y

Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/1

2000 Sep 05 09:04:33 %SYS-5-SPAN\_CFGSTATECHG:local span session inactive

for destination port 6/2

1つのセッションだけが残っていることを確認できます。

```
switch (enable) show span
```

Destination : Port 6/3

Admin Source : VLAN 3

Oper Source : Port 6/4-5,15/1

Direction : transmit/receive

Incoming Packets: disabled

Learning : enabled

Multicast : enabled

Filter : -

Status : active

Total local span sessions: 1

1つのステップで現在のすべてのセッションをディセーブルにするには、次のコマンドを発行します。

```
switch (enable) set span disable all
```

This command will disable all span session(s).

Do you want to continue (y/n) [n]?y

Disabled all local span sessions

2000 Sep 05 09:07:07 %SYS-5-SPAN\_CFGSTATECHG:local span session inactive

for destination port 6/3

```
switch (enable) show span
```

No span session configured

## その他の SPAN オプション

set span コマンドの構文は次のとおりです。

```
switch (enable) set span
```

Usage: set span disable [dest\_mod/dest\_port|all]

set span <src\_mod/src\_ports...|src\_vlans...|sc0>

```
<dest_mod/dest_port> [rx|tx|both]
[inpkts <enable|disable>]
[learning <enable|disable>]
[multicast <enable|disable>]
[filter <vlans...>]
[create]
```

このセクションでは、このドキュメントで説明するオプションについて簡潔に紹介します。

- **sc0** : **sc0** キーワードは、管理インターフェイス sc0 へのトラフィックをモニタする必要がある場合に、SPAN 設定で指定します。この機能は、Catalyst 5500/5000 および 6500/6000 スイッチで、コードバージョン CatOS 5.1 以降で利用可能です。
- **inpkts enable/disable** : このオプションは、特に重要です。このドキュメントで述べたように、SPAN の宛先として設定したポートは、依然として元の VLAN に属しています。宛先ポートで受信したパケットは、その後、ポートが通常のアクセスポートであるかのように、VLAN に入ります。この動作は、必要な場合があります。スニファとして PC を使用する場合、この PC が VLAN に全面的に接続されていることが必要である可能性があります。それでも、この接続は、ネットワークにループを形成するような他のネットワーク機器に宛先ポートを接続している場合には危険があります。送信先 SPAN ポートは STP を実行せず、危険なブリッジングループの状況に陥ることがあります。この状態がどのように発生する可能性があるかの例については、このドキュメントの「[SPAN セッションでブリッジングループが生成されるのはなぜですか。](#)」セクションを参照してください。このオプションのデフォルト設定はディセーブルで、これは、宛先 SPAN ポートが受信したパケットを廃棄することを意味しています。この廃棄により、ポートをブリッジングループから保護します。このオプションは、CatOS 4.2 で登場します。
- **learning enable/disable** : このオプションで、宛先ポートでの学習機能をディセーブルにできます。デフォルトでは、学習機能はイネーブルであり、宛先ポートでは、ポートで受信する着信パケットから MAC アドレスを学習します。この機能は、Catalyst 4500/4000 および 5500/5000 では CatOS 5.2、Catalyst 6500/6000 では CatOS 5.3 で登場します。
- **multicast enable/disable** : その名前が示すように、このオプションでは、マルチキャストパケットのモニタリングをイネーブルまたはディセーブルにできます。デフォルトはイネーブルです。この機能は、Catalyst 5500/5000 および 6500/6000 で、CatOS 5.1 以降で利用可能です。
- **spanning port 15/1** : Catalyst 6500/6000 では、ポート 15/1 (または 16/1) を SPAN ソース (送信元) として使用できます。ポートでは、Multilayer Switch Feature Card (MSFC; マルチレイヤスイッチフィーチャカード) に転送されるトラフィックをモニタできます。ポートでは、MSFC にソフトウェアルーティングされるトラフィックやダイレクトされるトラフィックをキャプチャします。

## リモート SPAN

### RSPAN の概要

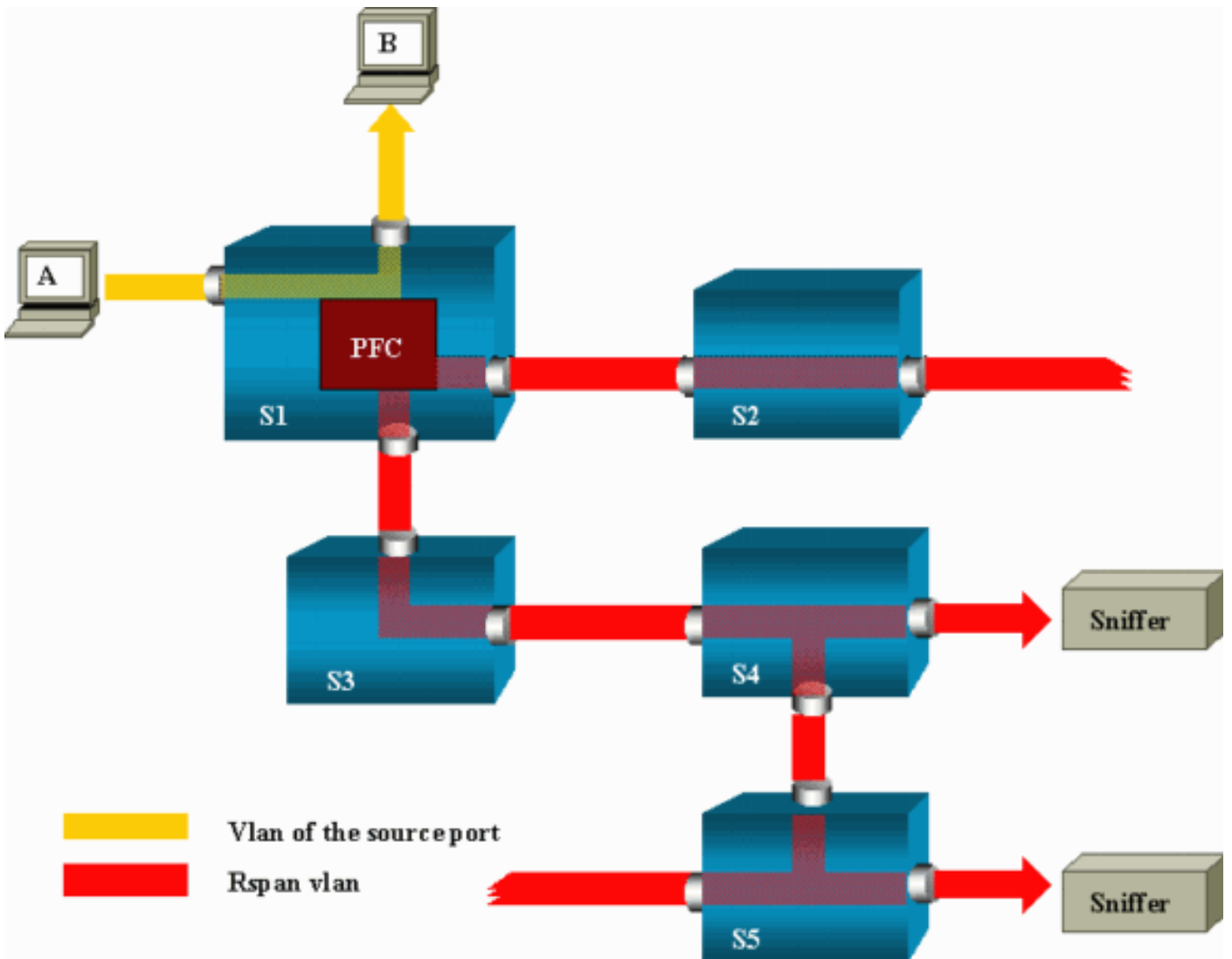
RSPAN は、SPAN を設定したスイッチでのローカルな範囲だけではなく、スイッチドネットワーク全体に渡る送信元ポートのモニタも可能にします。この機能は、Catalyst 6500/6000 シリーズスイッチでは CatOS 5.3 で登場し、Catalyst 4500/4000 シリーズスイッチでは CatOS 6.3. 以降で追加されています。

機能的には、通常の SPAN とまったく同様に動作します。SPAN にモニタされているトラフィックは、宛先ポートには直接コピーされませんが、特別の RSPAN VLAN にフラグディングされま



す。宛先ポートは、この RSPAN VLAN のどの場所にも配置できます 複数の宛先ポートを設定することもできます。

このダイアグラムは RSPAN セッションの構造を示しています。



この例では、ホスト A から送信されるトラフィックをモニタするために RSPAN を設定します。ホスト A がホスト B に宛てたフレームを生成すると、パケットは Catalyst 6500/6000 Policy Feature Card ( PFC; ポリシー フィーチャ カード ) の Application-Specific Integrated Circuit ( ASIC; 特定用途向け集積回路 ) により、事前定義した RSPAN VLAN にコピーされます。そこから、パケットは RSPAN VLAN に属する他のすべてのポートにフラッディングされます。ここで表されるスイッチ間のリンクは、すべてトランクで、これは、RSPAN の要件です。唯一のアクセスポートは宛先ポートで、ここにスニファが接続されます (ここでは、S4 および S5)。

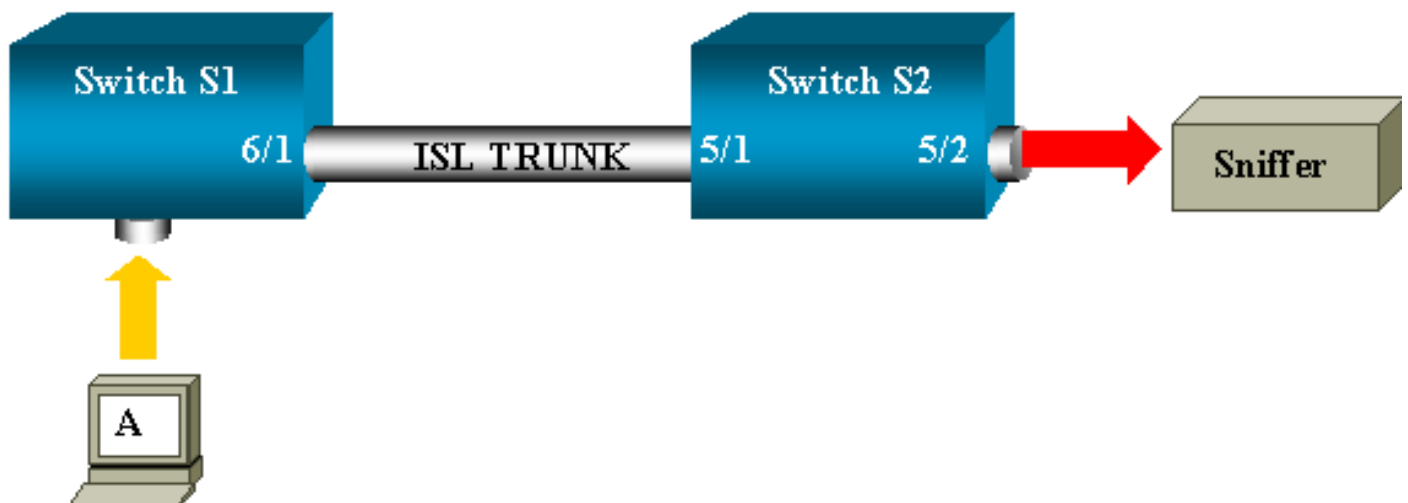
次は、この設計についての備考です。

- S1 はソーススイッチと呼ばれます。パケットは、RSPAN のソースとして設定されたスイッチの RSPAN VLAN だけに入ります。現行では、スイッチは、1つの RSPAN セッションだけのソースになります。つまり、ソーススイッチは、一度に1つの RSPAN VLAN にだけ供給できることを意味します。
- S2 および S3 は、中継スイッチです。これらは RSPAN のソースではなく、宛先ポートはありません。1つのスイッチが、多数の RSPAN セッションの中継スイッチになることができます。

- S4 と S5 は宛先スイッチです。ポートのいくつかは、RSPAN セッションの送信先になるように設定されます。現行では、Catalyst 6500/6000 は、1 つまたは複数の異なるセッションに最大 24 の RSPAN の宛先ポートを持つことが可能です。S4 は宛先と中継スイッチの両方に指定できます。
- RSPAN パケットが RSPAN VLAN にフラッディングされていることがわかります。S2 のような、宛先ポートへのパスにはないスイッチでも、RSPAN VLAN へのトラフィックを受信しています。この VLAN を S1-S2 などのリンクにプルーニングすることが有効であることがわかります。
- フラッディングを起こさせるには、RSPAN VLAN で学習機能をディセーブルにします。
- ループを防止するために、RSPAN VLAN で STP が維持されています。したがって、RSPAN は Bridge Protocol Data Unit ( BPDU; ブリッジ プロトコル データ ユニット ) をモニタできません。

## RSPAN の設定例

このセクションの情報では、非常に簡単な RSPAN の設計を使用して、この異なる要素の設定を説明しています。S1 および S2 は、2 台の Catalyst 6500/6000 スイッチです。S1 のポート、あるいは S2 からの VLAN をモニタするためには、専用の RSPAN VLAN を設定することが必要です。その他のコマンドには、典型的な SPAN セッションで使用されるものに、類似した構文があります。



## 2 つのスイッチ S1 および S2 間での ISL トランクの設定

始めるには、各スイッチに同じ VLAN Trunk Protocol ( VTP; VLAN トランク プロトコル ) ドメインを置き、一方を要トランキングに設定してください。後は、VTP ネゴシエーションで実行されます。S1 で次のコマンドを発行します。

```
S1> (enable) set vtp domain cisco
VTP domain cisco modified
```

S2 で次のコマンドを発行します。

```
S2> (enable) set vtp domain cisco
VTP domain cisco modified
S2> (enable) set trunk 5/1 desirable
```

```
Port(s) 5/1 trunk mode set to desirable.
S2> (enable) 2000 Sep 12 04:32:44 %PAGP-5-PORTFROMSTP:Port 5/1 left bridge
port 5/1
2000 Sep 12 04:32:47 %DTP-5-TRUNKPORTON:Port 5/1 has become isl trunk
```

## RSPAN VLAN の作成

RSPAN セッションには、特定の RSPAN VLAN が必要です。この VLAN を作成する必要があります。既存の VLAN を RSPAN VLAN に変換することはできません。次の例では VLAN 100 を使用しています。

```
S2> (enable) set vlan 100 rspan
Vlan 100 configuration successful
```

VTP サーバとして設定される 1 つのスイッチで、このコマンドを発行します。RSPAN VLAN 100 についての情報は VTP ドメイン全体に自動的に伝播されます。

## S2 のポート 5/2 を RSPAN の終点ポートとして設定

```
S2> (enable) set rspan destination 5/2 100
Rspan Type : Destination
Destination : Port 5/2
Rspan Vlan : 100
Admin Source : -
Oper Source : -
Direction : -
Incoming Packets: disabled
Learning : enabled
Multicast : -
Filter : -
Status : active
2000 Sep 12 04:34:47 %SYS-5-SPAN_CFGSTATECHG:remote span destination session
active for destination port 5/2
```

## S1 の RSPAN 送信元ポートの設定

この例では、ポート 6/2 経由で S1 に入る着信トラフィックをモニタしています。次のコマンドを発行します。

```
S1> (enable) set rspan source 6/2 100 rx
Rspan Type : Source
Destination : -
Rspan Vlan : 100
Admin Source : Port 6/2
Oper Source : Port 6/2
Direction : receive
Incoming Packets: -
Learning : -
Multicast : enabled
Filter : -
Status : active
S1> (enable) 2000 Sep 12 05:40:37 %SYS-5-SPAN_CFGSTATECHG:remote span
source session active for remote span vlan 100
```

ポート 6/2 のすべての着信パケットは、今度は RSPAN VLAN 100 にフラッディングされており

、トランク経由で S1 に設定された宛先ポートに到達します。

## 設定の確認

`show rspan` コマンドで、スイッチの現在の RSPAN 設定の要約が得られます。ここでも、一時点で 1 つのソース RSPAN セッションだけが存在できます。

```
S1> (enable) show rspan
Rspan Type : Source
Destination : -
Rspan Vlan : 100
Admin Source : Port 6/2
Oper Source : Port 6/2
Direction : receive
Incoming Packets: -
Learning : -
Multicast : enabled
Filter : -
Status : active
Total remote span sessions: 1
```

## set rspan コマンドで可能な他の設定

RSPAN で複数のコマンドラインを使用して、送信元および宛先を設定します。この違いとは別に、SPAN と RSPAN は、実際には同じ動作をします。複数の宛先 SPAN ポートが必要な場合、1 つのスイッチで、RSPAN をローカルに使用することも可能です。

## 機能の概要と制限事項

次の表は、紹介したさまざまな機能を要約し、その機能を指定のプラットフォームで実行するために最低限必要な CatOS のリリースを記載しています。

機能	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000
<code>inpkts enable/disable</code> オプション	4.4	4.2	5.1
異なる VLAN での複数セッション、複数ポート	5.1	5.1	5.1
<code>sc0</code> オプション	-	5.1	5.1
<code>multicast enable/disable</code> オプション	-	5.1	5.1
<code>learning enable/disable</code> オプション	5.2	5.2	5.3
RSPAN	6.3	-	5.3

次の表は、可能な SPAN セッション数に関する、現行の制約事項についての概略を説明しています。

機能	Catalyst 4500/4000レンジのスイッチ	Catalyst 5500/5000レンジのスイッチ	Catalyst 6500/6000レンジのスイッチ
Rx または両SPAN セッション	5	1	2
Tx SPAN セッション	5	4	4
ミニプロトコルアナライザセッション	非サポート	非サポート	1
Rx、Tx、または両RSPAN ソースセッション	5	非サポート	1 Supervisor Engine 720 は 2 つの RSPAN ソース セッションをサポート
RSPAN 宛先	5	非サポート	24
合計セッション	5	5	30

その他の制約事項や設定ガイドラインについては、次のドキュメントを参照してください。

- [SPAN と RSPAN の設定](#) ( Catalyst 4500/4000 )
- [SPAN と RSPAN の設定](#) ( Catalyst 6500/6000 )

## Catalyst 2940、2950、2955、2960、2970、3550、3560、3560-E、3750 および 3750-E シリーズ スイッチでの SPAN

Catalyst 2940、2950、2955、2960、2970、3550、3560、3560-E、3750 および 3750-E シリーズ スイッチでの SPAN 機能の設定についてのガイドラインを次に示します。

- Catalyst 2950 スイッチでは、同時にアクティブにできるのは 1 つの SPAN セッションだけで、モニタできるのは送信元ポートだけです。これらのスイッチでは、VLAN のモニタはできません。
- Catalyst 2950 および 3550 スイッチは、Cisco IOS ソフトウェア リリース 12.1(13)EA1 以降では、宛先 SPAN ポートでのトラフィックの転送ができます。
- Catalyst 3550、3560、および 3750 スイッチは、一度に 2 つの SPAN セッションまでサポートでき、送信元ポートおよび VLAN をモニタできます。
- Catalyst 2970、3560、および 3750 スイッチでは、RSPAN セッションを設定する際に、リフレクタ ポートを設定する必要がありません。
- Catalyst 3750 スイッチでは、スイッチ スタックの任意のメンバにある送信元ポートと宛先ポートを使用したセッション設定がサポートされています。
- 1 つの SPAN セッションあたりに 1 つの宛先ポートだけが割り当てられ、同じポートを複数の SPAN セッションの宛先ポートにはできません。したがって、同じ宛先ポートを使用する

2 つの SPAN セッションを置くことはできません。

SPAN 機能の設定コマンドは Catalyst 2950 および Catalyst 3550 では類似していますが、Catalyst 2950 では VLAN のモニタはできません。SPAN は、次の例に示すように設定できます。

```
C2950#configure terminal
C2950(config)#
C2950(config)#monitor session 1 source interface fastethernet 0/2

!--- This configures interface Fast Ethernet 0/2 as source port.

C2950(config)#monitor session 1 destination interface fastethernet 0/3

!--- This configures interface Fast Ethernet 0/3 as destination port.

C2950(config)#
```

```
C2950#show monitor session 1
Session 1-----
Source Ports:
RX Only: None
TX Only: None
Both: Fa0/2
Destination Ports: Fa0/3
C2950#
```

また、ローカル SPAN および同じ VLAN トラフィックの RSPAN の宛先として、ポートを設定できます。直接接続された 2 つのスイッチにある特定の VLAN のトラフィックをモニタするには、宛先ポートのあるスイッチで次のコマンドを設定します。この例では、2 つのスイッチ全体に展開される VLAN 5 からのトラフィックをモニタしています。

```
c3750(config)#monitor session 1 source vlan < Remote RSPAN VLAN ID >
c3750(config)#monitor session 1 source vlan 5
c3750(config)#monitor session 1 destination interface fastethernet 0/3
```

```
!--- This configures interface FastEthernet 0/3 as a destination port.
```

リモートスイッチでは、次の設定を使用します。

```
c3750_remote(config)#monitor session 1 source vlan 5
```

```
!--- Specifies VLAN 5 as the VLAN to be monitored.
```

```
c3750_remote(config)#monitor session 1 destination remote vlan <Remote vlan id>
```

上の例では、2 つのスイッチにある同じ VLAN のトラフィックをモニタするために、ポートはローカル SPAN および RSPAN の両方の宛先ポートとして設定されていました。

**注:** 2900XL および 3500XL シリーズ スイッチとは異なり、Catalyst 2940、2950、2955、2960、2970、3550、3560、3560-E、3750、および 3750-E シリーズ スイッチでは、Rx 方向のみ ( Rx SPAN または入力 SPAN )、Tx 方向のみ ( Tx SPAN または出力 SPAN )、あるいは両方向で、送信元ポートのトラフィックでの SPAN がサポートされています。

**注:** 設定にあるコマンドは、Catalyst 2950 では、Cisco IOS ソフトウェア リリース 12.0(5.2)WC(1)、および Cisco IOS ソフトウェア リリース 12.1(6)EA2 よりも前のソフトウェアではサポートされていません。Cisco IOS ソフトウェア リリース 12.1(6)EA2 よりも前のソフトウェアを使用している Catalyst 2950 で SPAN を設定するには、『[スイッチの管理](#)』の「[スイッチ ポート アナライザをイネーブルにする](#)」セクションを参照してください。

注: Cisco IOS ソフトウェア リリース 12.1 トレインの Cisco IOS ソフトウェア リリース 12.1.(9)EA1d 以前のリリースを使用する Catalyst 2950 スイッチでは SPAN がサポートされています。しかし、SPAN の宛先ポート (スニファ デバイスまたは PC に接続) で見られるすべてのパケットには、SPAN の送信元ポート (モニタ ポート) が 802.1Q トランクポートでなくても、IEEE 802.1Q タグが付加されています。スニファ デバイスまたは PC の Network Interface Card (NIC; ネットワーク インターフェイス カード) で 802.1Q タグ付きパケットが認識されない場合、そのデバイスではパケットが廃棄されたり、パケットのデコードが困難な場合があります。802.1Q タグ付きフレームを識別する能力が重要なのは、SPAN の送信元ポートがトランクポートである場合だけです。Cisco IOS ソフトウェア リリース 12.1(11)EA1 以降では、SPAN の終点ポートでのパケットのタグ付けを、有効に、あるいは無効にすることが可能です。宛先ポートでパケットのカプセル化を有効にするには、[monitor session session number destination interface interface id encapsulation dot1q コマンド](#)を発行します。encapsulation キーワードを指定しないと、パケットはタグ無しで送信されます。Cisco IOS ソフトウェア リリース 12.1(11)EA1 以降では、これがデフォルトです。

機能	Catalyst 2950/3550
Ingress (inpkts) enable/disable オプション	Cisco IOS ソフトウェア リリース 12.1(12c)EA1
RSPAN	Cisco IOS ソフトウェア リリース 12.1(12c)EA1
機能	Catalyst 2940 <sup>1</sup> 、2950、2955、2960、2970、3550、3560、3750
Rx または両 SPAN セッション	2
Tx SPAN セッション	2
Rx、Tx、または両 RSPAN ソース セッション	2
RSPAN 宛先	2
合計セッション	2

1 Catalyst 2940 スイッチでサポートされているのは、ローカル SPAN だけです。このプラットフォームでは、RSPAN はサポートされていません。

SPAN と RSPAN の設定についての詳細は、次のコンフィギュレーション ガイドを参照してください。

- [SPAN の設定](#) ( Catalyst 2940 )
- [SPAN と RSPAN の設定](#) ( Catalyst 2950 および 2955 )
- [SPAN と RSPAN の設定](#) ( Catalyst 2960 )
- [SPAN と RSPAN の設定](#) ( Catalyst 3550 )
- [SPAN と RSPAN の設定](#) ( Catalyst 3560 )
- [SPAN と RSPAN の設定](#) ( Catalyst 3560-E および 3750-E )

- [SPAN と RSPAN の設定](#) ( Catalyst 3750 )

## Cisco IOS システム ソフトウェアが稼働する Catalyst 4500/4000 および Catalyst 6500/6000 シリーズ スイッチでの SPAN

Cisco IOS システム ソフトウェアが稼働する Catalyst 4500/4000 および Catalyst 6500/6000 シリーズ スイッチでは、SPAN 機能がサポートされています。これらの両方のスイッチ プラットフォームでは、「[Catalyst 2940、2950、2955、2960、2970、3550、3560、3560E、3750 および 3750E シリーズ スイッチでの SPAN](#)」セクションで説明されている設定と同一のコマンドライン インターフェイス ( CLI )、および同様の設定を使用します。関連する設定については、次のドキュメントを参照してください。

- [SPAN と RSPAN の設定](#) ( Catalyst 6500/6000 )
- [SPAN と RSPAN の設定](#) ( Catalyst 4500/4000 )

### 設定例

SPAN は、次の例に示すように設定できます。

```
4507R#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

4507R(config)#monitor session 1 source interface fastethernet 4/2

!--- This configures interface Fast Ethernet 4/2 as source port.

4507R(config)#monitor session 1 destination interface fastethernet 4/3

!--- The configures interface Fast Ethernet 0/3 as destination port.

4507R#show monitor session 1

Session 1-----
Type : Local Session
Source Ports :
Both : Fa4/2
Destination Ports : Fa4/3

4507R#
```

### 機能の概要と制限事項

次の表は、紹介したさまざまな機能を要約し、指定のプラットフォームでその機能を実行するために最低限必要な Cisco IOS ソフトウェアのリリースを記載しています。

機能	Catalyst 4500/4000 ( Cisco IOS ソフトウェア )	Catalyst 6500/6000 ( Cisco IOS ソフトウェア )
Ingress (inpkts) enable/disable オプション	Cisco IOS ソフトウェア リリース 12.1(19)EW	現在非サポート <sup>1</sup>
RSPAN	Cisco IOS ソフト	Cisco IOS ソフト



	ウェア リリース 12.1(20)EW	ウェア リリース 12.1(13)E
--	------------------------	-----------------------

1 この機能は、現在利用できません。これらの機能の Availability は、リリースされるまで一般に公表されません。

注: Cisco Catalyst 6500/6000 シリーズ スイッチの SPAN 機能には、PIM プロトコルに関して制限があります。スイッチが PIM および SPAN の両方に設定される場合、SPAN の宛先ポートに接続されるネットワーク アナライザやスニファでは、SPAN 送信元ポートまたは VLAN トラフィックの一部ではない PIM パケットが検出される場合があります。この問題は、スイッチのパケット転送アーキテクチャの制限が原因で発生します。SPAN の宛先ポートでは、パケットの送信元を確認するためのチェックが行われません。この問題は、Cisco Bug ID [CSCdy57506](#) (登録ユーザ専用) にも記載されています。

次の表は、可能な SPAN および RSPAN セッション数に関する、現行の制約事項についての概略を説明しています。

機能	Catalyst 4500/4000 ( Cisco IOS ソフトウェア )
Rx または両 SPAN セッション	2
Tx SPAN セッション	4
Rx、Tx、または両 RSPAN ソース セッション	2 ( Rx、Tx、または両方 )、および Tx だけの場合は最大 4
RSPAN 宛先	2
合計セッション	6

Cisco IOS ソフトウェアが稼働する Catalyst 6500/6000 スイッチ用の「[ローカル SPAN、RSPAN、および ERSPAN セッションの制限](#)」を参照してください。

Catalyst 6500 シリーズでは、出力 SPAN はスーパーバイザで行われることに注意することが重要です。この場合、出力 SPAN の対象になるすべてのトラフィックがファブリック上でスーパーバイザに送信されてから SPAN 宛先ポートに送信されるのが許可されます。これにより、相当のシステム リソースが使用され、ユーザトラフィックに影響が及ぶ可能性があります。入力 SPAN は入力モジュールで行われるため、SPAN のパフォーマンスはすべての構成しているレプリケーション エンジンの合計になります。SPAN 機能のパフォーマンスは、レプリケーション エンジンで利用可能な ASIC のパケット サイズおよび種類によって異なります。

Cisco IOS ソフトウェア リリース 12.2(33)SXH よりも前のリリースでは、ポートチャネル インターフェイス ( EtherChannel ) は SPAN 宛先として設定できません。Cisco IOS ソフトウェア リリース 12.2(33)SXH 以降では、EtherChannel は SPAN 宛先として設定できます。宛先 EtherChannel では、Port Aggregation Control Protocol ( PAgP ) または Link Aggregation Control Protocol ( LACP ) EtherChannel プロトコルをサポートしません。すべての EtherChannel プロトコルのサポートをディセーブルにしている場合に、オン モードだけがサポートされます。

その他の制約事項や設定ガイドラインについては、次のドキュメントを参照してください。

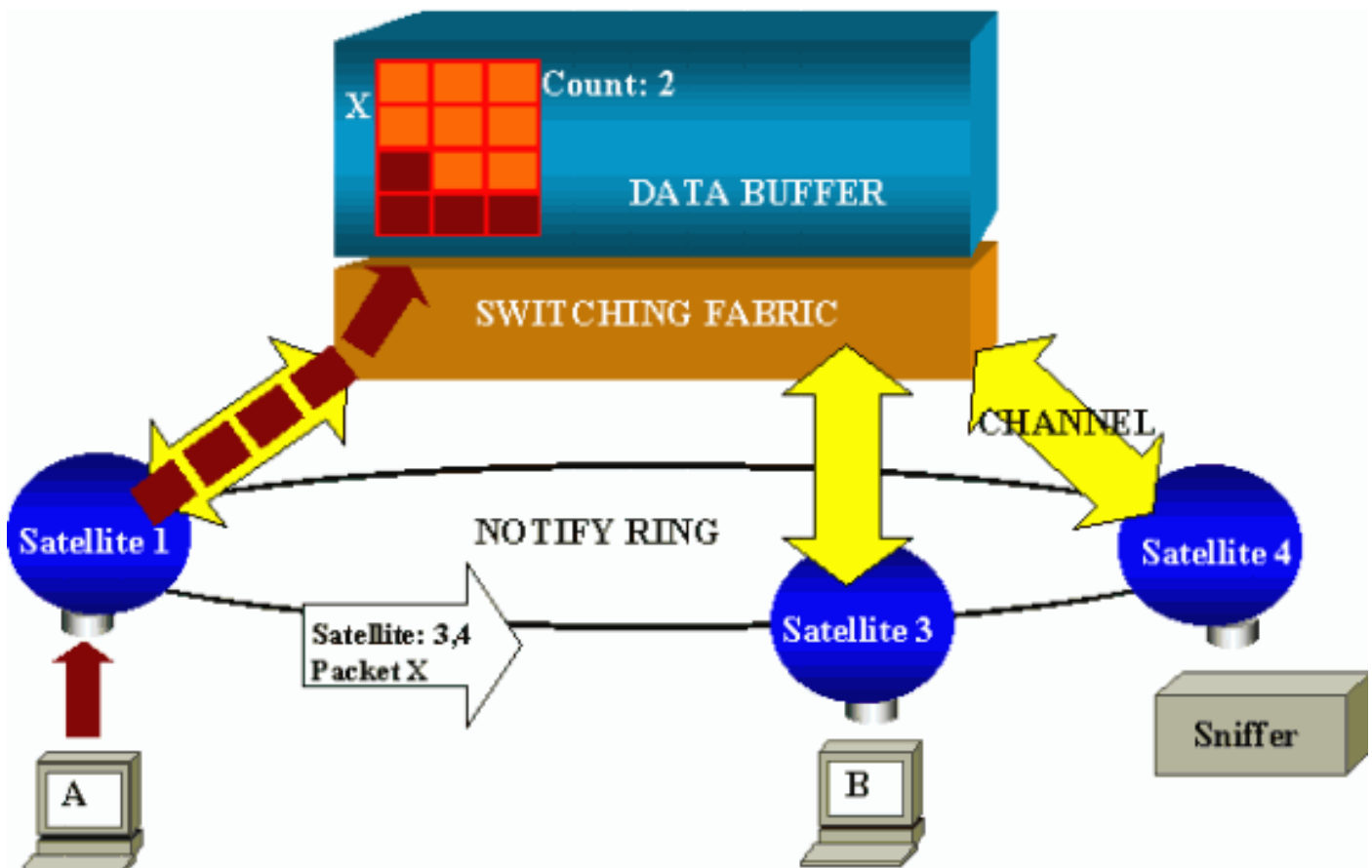
- [SPAN と RSPAN の設定 \( Catalyst 4500/4000 \)](#)
- [ローカル SPAN、リモート SPAN \( RSPAN \)、およびカプセル化 RSPAN の設定 \( Catalyst 6500/6000 \)](#)

## 異なる Catalyst プラットフォームでの SPAN のパフォーマンスへの影響

### Catalyst 2900XL/3500XL シリーズ

#### アーキテクチャ概要

次に 2900XL/3500XL スイッチの内部アーキテクチャの簡略図を示します。



スイッチのポートは、ラジアルチャネル経由でスイッチングファブリックと通信する衛星局に接続されます。上部構造として、すべての衛星局はシグナリングトラフィック専用の高速通知リング経由で相互に接続されます。

衛星局がポートからパケットを受信すると、パケットはセルに分解され、1つまたは複数のチャネル経由でスイッチングファブリックに送られます。そこでパケットは、共有メモリに保管されます。各衛星局は、その宛先ポートを識別しています。このセクションのダイアグラムでは、衛星局1では、パケットXが衛星局3と4で受信されるものであることが認識されています。衛星局1は、通知リング経由で他の衛星局へメッセージを送信します。それから、衛星局3と4は、ラジアルチャネル経由で共有メモリからセルの取得を開始し、最終的にパケットを転送できます。ソース衛星局では宛先が認識されているため、この衛星局からは、その他の衛星局からこのパケットがダウンロードされる回数を指定するインデックスも送信されます。衛星局がパケット

を共有メモリから取得するたびに、このインデックスは減算されていきます。インデックスがゼロに達すると、共有メモリを解放できます。

## パフォーマンスへの影響

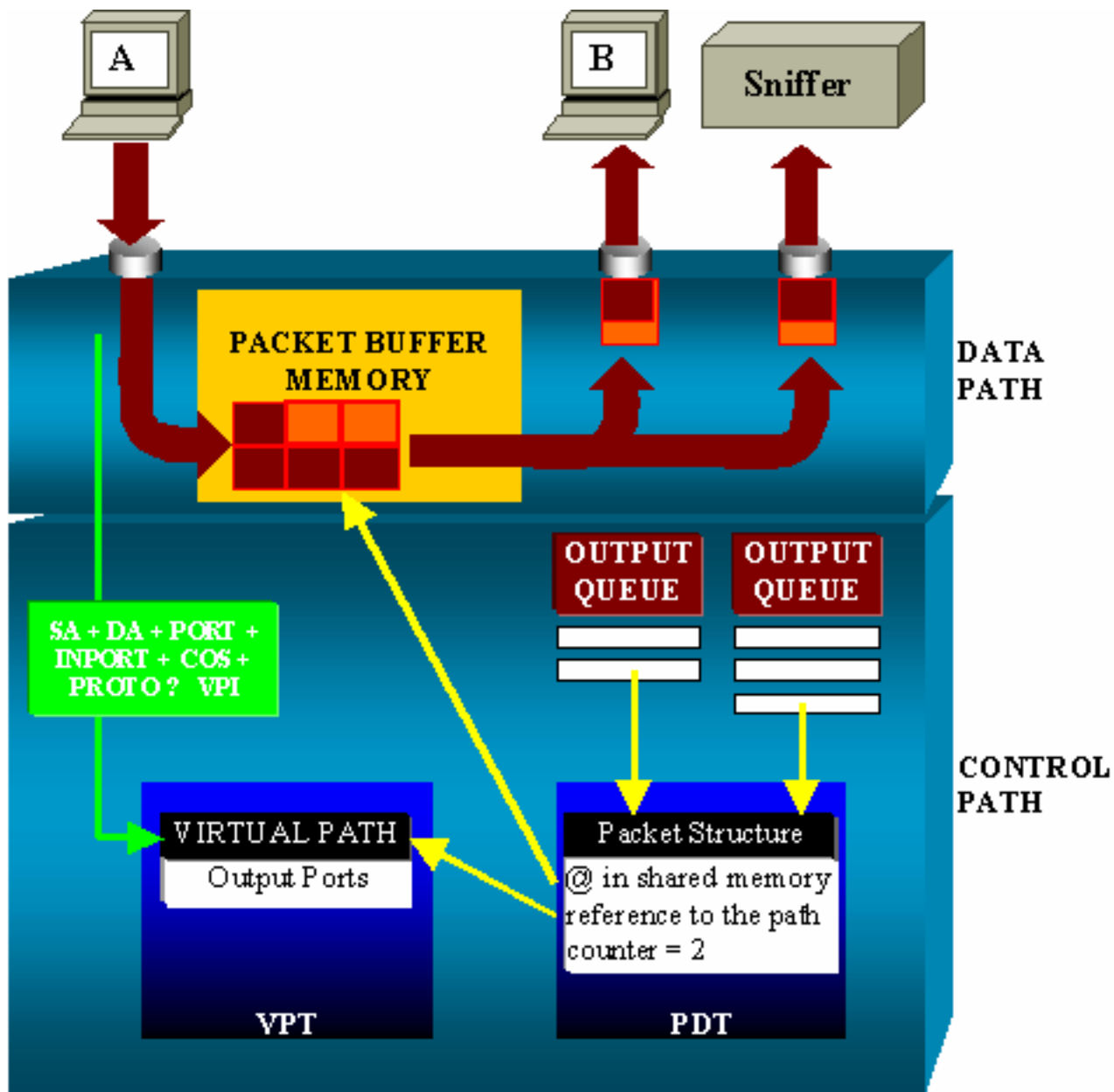
SPAN でポートをモニタするためには、データ バッファから衛星局へのパケットのコピー操作が増加することを意味しています。高速スイッチング ファブリックでの影響は無視できます。

モニタ ポートは、モニタされるすべてのポートの送受信トラフィックのコピーを受け取ります。このアーキテクチャでは、複数の宛先に向けられたパケットは、すべてのコピーが転送されるまで、共有メモリに保管されます。モニタ ポートが、一定の期間 50 % の加入過多の状態が続くと、ポートは輻輳状態になり共有メモリの一部を占有し続ける場合があります。モニタ対象の 1 つまたは複数のポートで、速度の低下が発生する可能性があります。

## Catalyst 4500/4000 シリーズ

### アーキテクチャ概要

Catalyst 4500/4000 は、共有メモリ スwitchング ファブリックを基にしています。次の図は、スイッチを通るパケットのパスの、高レベルの概要を示します。現実の実装は、はるかに複雑です。



Catalyst 4500/4000 では、データパスを区別できます。すべての決定が行われる制御パスから、データパスはスイッチ内で実際のデータ転送に対応します。

パケットがスイッチに入ると、Packet Buffer Memory (共有メモリ) にバッファが割り当てられます。このバッファを指すパケット構造が、Packet Descriptor Table (PDT) で初期化されます。データが共有メモリにコピーされる間、制御パスでは、どこでパケットをスイッチングするかが判断されます。この判断を行うために、次の情報からハッシュ値が計算されます。

- パケットの送信元アドレス
- 宛先アドレス
- VLAN
- プロトコルタイプ
- 入力ポート
- Class of service (CoS; サービスクラス) (IEEE 802.1p タグまたはポートのデフォルトのいずれか)

この値は、Virtual Path Table (VPT) のパス構造の Virtual Path Index (VPI) を見つけるのに使用されます。VPT のこの仮想パスエントリには、この特定のフローに関する複数のフィールドがあります。フィールドには、宛先ポートが含まれています。PDT のパケット構造は、仮想パスとカウンタに関連づけられアップデートされます。このセクションの例では、パケットは2つ

の異なるポートに送信されるので、カウンタは 2 に初期化されています。最後に、このパケット構造が、2 つの宛先ポートの出力キューに追加されます。それから、データは共有メモリからポートの出力バッファにコピーされ、パケット構造カウンタが減算されます。カウンタがゼロに達すると、共有メモリのバッファは解放されます。

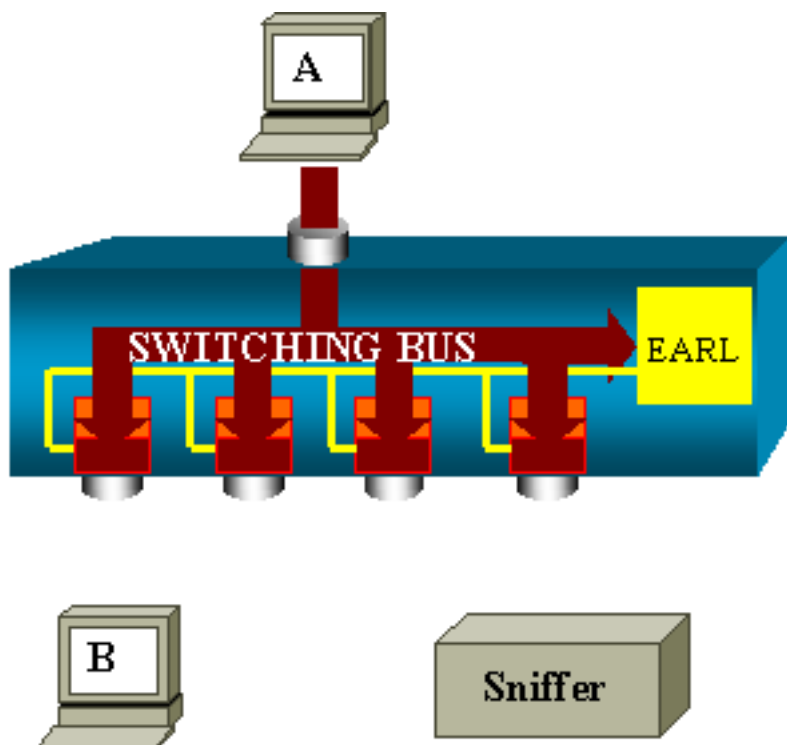
## パフォーマンスへの影響

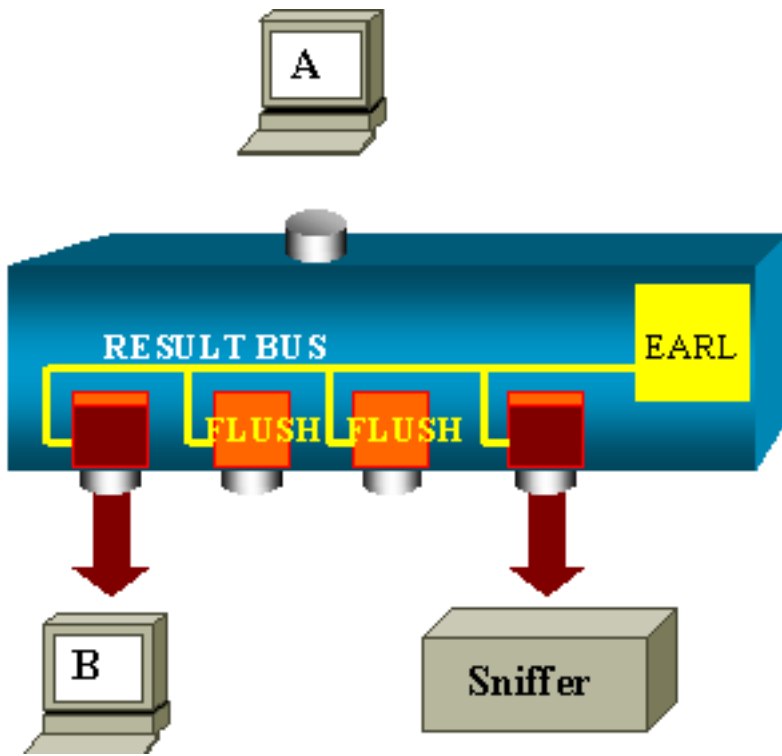
SPAN 機能を使用する場合、「[アーキテクチャ概要](#)」セクションの例のように、パケットは 2 つの異なるポートに送信される必要があります。2 つのポートへのパケットの送信については、スイッチング ファブリックはノンブロッキングのため問題ありません。送信先 SPAN ポートが輻射している場合、パケットは出力キューでドロップし共有メモリから正しくリリースされます。したがって、スイッチ動作への影響もありません。

## Catalyst 5500/5000 および 6500/6000 シリーズ

### アーキテクチャ概要

Catalyst 5500/5000 および 6500/6000 シリーズ スイッチでは、ポートで受信されたパケットは内部スイッチング バスで転送されます。スイッチ内のすべてのラインカードは、このパケットの内部バッファへの格納が開始されます。同時に、Encoded Address Recognition Logic ( EARL ) はパケットのヘッダーを受け取り、結果のインデックスを計算します。EARL は、結果バス経由ですべてのラインカードに結果のインデックスを送信します。このインデックスについての知識により、ラインカードがバッファでパケットを受信して、ラインカードがパケットをフラッシュするか転送するかを個別に判断することが可能になります。





## パフォーマンスへの影響

1つまたは複数のポートが最終的にパケットを送信したかどうかは、スイッチの運用にまったく影響しません。したがって、このアーキテクチャを考慮するとき、SPAN機能がパフォーマンスに影響を与えることはありません。

## よくある質問と一般的な問題

### SPANの誤設定による接続の問題

SPANの誤設定による接続性の問題は、CatOS 5.1よりも前のバージョンで頻繁に発生します。これらのバージョンでは、SPANセッションは1つだけが可能です。SPANをディセーブルにしても、セッションは設定に残ります。set span enable コマンドを発行して、ユーザは保存されたSPANセッションを再度アクティブにします。この処理は、たとえば、ユーザがSTPをイネーブルにする場合など、誤入力によってしばしば発生します。宛先ポートがユーザトラフィックの転送に使用されていると、深刻な接続問題を引き起こす場合があります。

**注意：** この問題は、CatOSの現在の実装でもまだ発生します。SPANの宛先として選択するポートに注意してください。

### SPAN宛先ポートが「Up/Down」になります。

ポートがモニタリング用にスパンされる時、ポートの状態は「Up/Down」のように表示されま

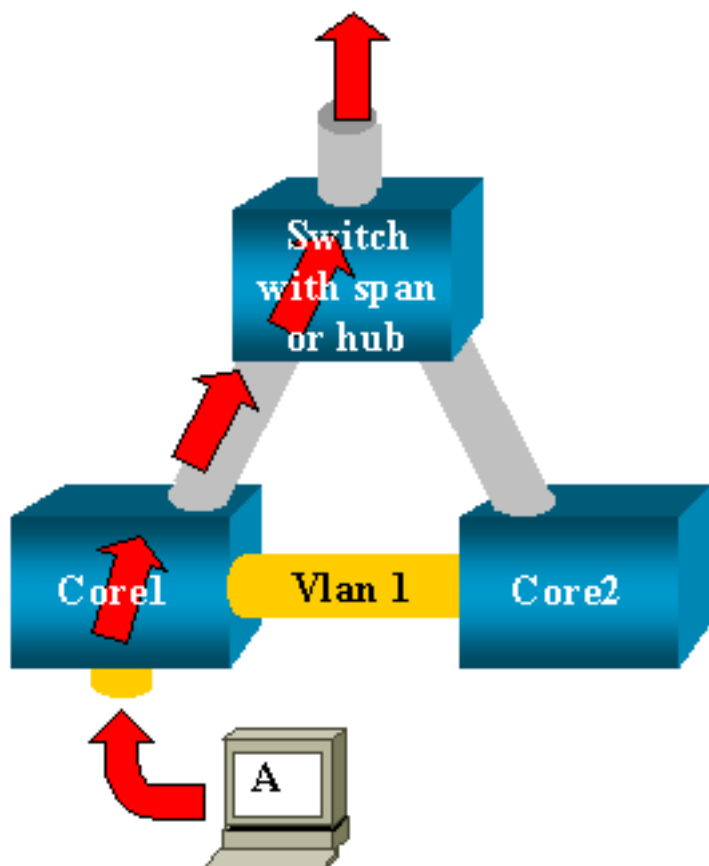
す。

SPAN セッションを設定してポートをモニタする場合は、設計により、宛先インターフェイスは「Down」状態（モニタリング）を示します。インターフェイスは、現在、ポートが実稼働ポートとして使用できないことを明確にするために、この状態でポートを表示します。「Up/Down」状態でモニタリング中のポートは正常です。

## SPAN セッションでブリッジング ループが生成されるのはなぜですか。

ブリッジ ループの作成は、一般的に、管理者が RSPAN 機能の偽装を試みた場合に発生します。問題の原因は、設定エラーによる場合もあります。

次に、例になるシナリオを示します。

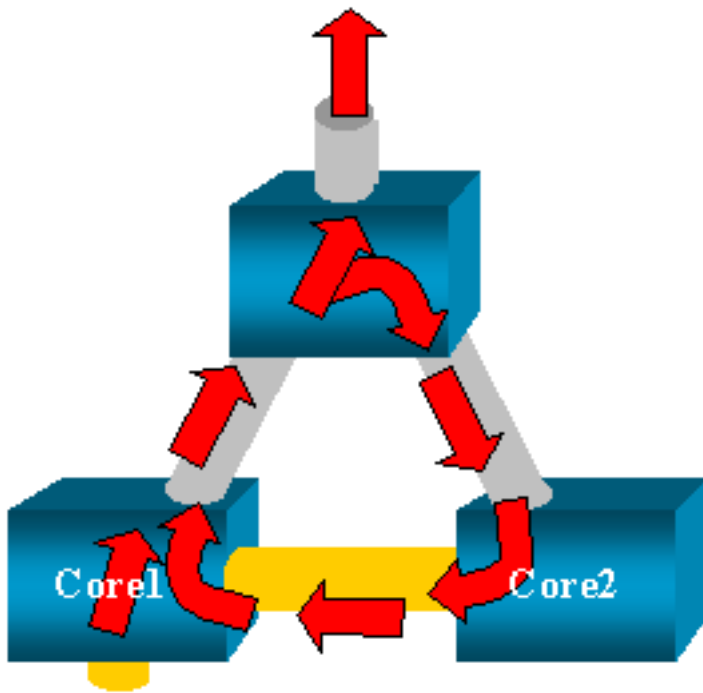


2つのコアスイッチが、トランクによってリンクされています。この場合、各スイッチには、複数のサーバ、クライアント、または他のブリッジが接続されています。管理者が、SPAN を設定した複数のブリッジで現れる VLAN 1 をモニタするとします。管理者は、各コアスイッチで VLAN 1 全体をモニタする SPAN セッションを作成します。そして、これら2つのセッションをマージするため、宛先ポートを同じハブ（または、他の SPAN セッションを使用する同じスイッチ）に接続しています。

管理者は、目的を達成します。コアスイッチが VLAN 1 で受信する各シングル パケットは、SPAN ポートで複製され、上方のハブに転送されます。スニファは最終的にトラフィックをキャプチャします。

唯一の問題は、さらに、トラフィックが宛先 SPAN ポートを通じて、コア 2 に再注入されることです。コア 2 へのトラフィックの再注入により、VLAN 1 でブリッジング ループが作成されます。宛先 SPAN ポートでは STP が実行されておらず、このようなループを防ぐ機能がないことに

留意してください。



注: CatOS での `inpkts` (入力パケット) オプションの導入により、SPAN 宛先ポートではデフォルトですべての着信パケットが廃棄され、この障害のシナリオを防止しています。しかし、Catalyst 2900XL/3500XL シリーズ スイッチでは、この潜在的な問題がまだ残っています。

注: `inpkts` オプションでループが防止されても、このセクションで示されている設定では、ネットワークでいくつかの問題が引き起こされる可能性があります。ネットワークの問題は、宛先ポートでイネーブルにされている学習機能に関連する、MAC アドレス学習機能の問題が原因で発生する場合があります。

## SPAN はパフォーマンスに影響するでしょうか。

指定の Catalyst プラットフォームへのパフォーマンス上の影響については、このドキュメントの次のセクションを参照してください。

- [Catalyst 2900XL/3500XL シリーズ](#)
- [Catalyst 4500/4000 シリーズ](#)
- [Catalyst 5500/5000 および 6500/6000 シリーズ](#)

## EtherChannel ポートで SPAN の設定はできますか。

バンドル内のポートの 1 つが SPAN の終点ポートである場合、EtherChannel は形成されません。この状況で SPAN を設定しようとした場合、スイッチからは次のように通知されます。

```
Channel port cannot be a Monitor Destination Port
Failed to configure span feature
```



EtherChannel バンドルのポートを SPAN 送信元ポートとして使用できます。

## 同時に複数の SPAN セッションを実行できますか。

Catalyst 2900XL/3500XL シリーズ スイッチでは、スイッチで利用可能な宛先ポートの数だけが、SPAN セッションの数に対する制限事項となります。

Catalyst 2950 シリーズ スイッチでは、割り当てられるモニタ ポートは常に 1 つだけです。他のポートをモニタ ポートに選択すると、直前のモニタ ポートはディセーブルされ、新規に選択したポートがモニタ ポートになります。

CatOS 5.1 以降が稼働する Catalyst 4500/4000、5500/5000、および 6500/6000 スイッチでは、同時に複数の SPAN セッションを持てます。このドキュメントの「[複数同時セッションの作成](#)」セクション、および「[機能の概要と制限事項](#)」セクションを参照してください。

## エラー : % Local Session Limit Has Been Exceeded

許可された SPAN セッションがスーパーバイザ エンジンの制限を超過すると、このメッセージが表示されます。

```
% Local Session limit has been exceeded
```

スーパーバイザ エンジンには、SPAN セッションの制限があります。詳細は、『[ローカル SPAN、RSPAN、および ERSPAN の設定](#)』の「[ローカル SPAN、RSPAN、および ERSPAN セッションの制限](#)」セクションを参照してください。

## 「% Session [Session No:] Used by Service Module」エラーにより、VPN サービス モジュールで SPAN セッションを削除できません。

この問題では、スイッチ ファブリック モジュールがすでに挿入されているシャーシに Virtual Private Network (VPN; バーチャル プライベート ネットワーク) モジュールが挿入されます。Cisco IOS ソフトウェアは、マルチキャスト トラフィックを処理するために、VPN サービス モジュールに自動的に SPAN セッションを作成します。

ソフトウェアが VPN サービス モジュールに作成する SPAN セッションを削除するには、次のコマンドを発行してください。

```
Switch(config)#no monitor session session_number service-module
```

注: セッションを削除する場合、VPN サービス モジュールはマルチキャスト トラフィックをドロップします。

## SPAN で破損したパケットをキャプチャできないのはなぜですか。

スイッチが通常動作する方法が原因で、SPAN の破損パケットをキャプチャできません。パケットがスイッチを通過する場合に次のことが発生します。

1. パケットが、入力ポートに到着する。

2. パケットは、少なくとも1つのバッファに保管される。
3. パケットは最終的に出力ポートに再転送される。



スイッチが破損したパケットを受信した場合、入力ポートは通常そのパケットを廃棄します。したがって、パケットは出力ポートには表示されません。トラフィックをキャプチャするという点に関しては、スイッチは完全に透過的ではありません。このセクションのシナリオで、同様にスニファに破損したパケットが表示された場合は、出力セグメントに、ステップ3でエラーが生成されています。

デバイスが破損したパケットを送信していると考えられる場合、送信ホストとスニファ デバイスを同じハブ上に置くことを選択できます。ハブでは、エラーチェックは行われません。したがって、スイッチとは異なり、ハブではパケットはを廃棄されません。この方法で、パケットを表示できます。

## Error: % Session 2 used by service module

Firewall Service Module ( FWSM; ファイアウォール サービス モジュール ) がインストールされた場合、たとえば、インストールして後に削除された場合、CAT6500 では、**SPAN Reflector feature** が自動的にイネーブルになります。SPAN リフレクタ機能は、スイッチで1つのSPAN セッションを使用します。これをもう必要としない場合、CAT 6500 のコンフィギュレーションモードから **no monitor session service module** コマンドを入力できるはずで、それからすぐに必要な新しいSPAN 設定を入力してください。

## リフレクタ ポートでパケットが廃棄されます。

リフレクタ ポートは、モニタ対象のすべての送信元ポートでの送受信トラフィックのコピーを受け取ります。リフレクタ ポートがオーバーサブスクライブされている場合、輻輳する可能性があります。この輻輳により、1つまたは複数の送信元ポートのトラフィックの転送が影響を受ける可能性があります。リフレクタ ポートの帯域幅が対応する送信元ポートからのトラフィック量に対して十分でない場合、超過パケットは廃棄されます。10/100 ポートは、100 Mbps で反映されます。ギガビット ポートは、1 Gbps で反映されます。

## SPAN セッションは常に、Catalyst 6500 シャーシの FWSM で使用されます。

Cisco のネイティブ IOS が稼働しているシャーシで、FWSM を搭載する Supervisor Engine 720 を使用する場合、デフォルトでSPAN セッションが使用されます。show monitor コマンドで使用されていないセッションを調べる場合、**セッション 1** が使用されます。

```
Cat6K#show monitor
```

```
Session 1
```

```
-----
```

```
Type : Service Module Session
```

ファイアウォール ブレードが Catalyst 6500 シャーシにある場合、FWSM はマルチキャスト スト

リームを複製できないため、このセッションはハードウェア マルチキャスト複製のサポートするために自動的にインストールされます。FWSM の背後で供給されるマルチキャスト ストリームがレイヤ 3 で複数のラインカードへ複製する必要がある場合、自動セッションによりファブリック チャンネルを通してスーパーバイザにトラフィックがコピーされます。

FWSM の背後にマルチキャスト ストリームを生成するマルチキャスト ソースがある場合は、SPAN リフレクタが必要です。Outside の VLAN にマルチキャスト ソースを置く場合、SPAN リフレクタは必要ありません。SPAN リフレクタは、FWSM からのブリッジング BPDU と互換性がありません。no monitor session service module コマンドを使用して、SPAN リフレクタを無効にできます。

## SPAN と RSPAN セッションは同じスイッチ内で同じ ID を使用できますか。

いいえ、通常の SPAN セッションと RSPAN 宛先セッションには、同じセッション ID を使用できません。各 SPAN セッションおよび RSPAN セッションは、異なるセッション ID を持つ必要があります。

## RSPAN セッションは異なる VTP ドメインにわたって機能できますか。

はい。RSPAN セッションは、異なる VTP ドメインにわたって機能できます。しかし、RSPAN VLAN がこれらの VTP ドメインのデータベースに存在することを確認してください。また、レイヤ 3 のデバイスが、セッション宛先へのセッション ソースのパスに存在しないことを確認してください。

## RSPAN セッションは WAN または異なるネットワークにわたって機能できますか

。

No.RSPAN セッションは、RSPAN が LAN (レイヤ 2) の機能であるため、レイヤ 3 デバイスを通過できません。WAN または異なるネットワークを介するトラフィックをモニタするには、Encapsulated Remote SwitchPort Analyser (ERSPAN) を使用します。ERSPAN 機能は、送信元ポート、ソース VLAN、および宛先ポートを異なるスイッチでサポートします。この機能により、ネットワーク全体で複数のスイッチのリモート モニタリングが提供されます。

ERSPAN は、ERSPAN ソース セッション、ルーティング可能な ERSPAN GRE カプセル化トラフィックおよび ERSPAN 宛先セッションから構成されています。異なるスイッチで ERSPAN ソース セッションおよび宛先セッションを個別に設定します。

現在、ERSPAN 機能は次でサポートされます。

- Cisco IOS ソフトウェア リリース 12.2(18)SXE 以降が稼働する PFC3B または PFC3BXL を搭載する Supervisor 720。
- ハードウェア バージョン 3.2 以降を使用し、また Cisco IOS ソフトウェア リリース 12.2(18)SXE 以降が稼働する PFC3A を搭載する Supervisor 720。

ERSPAN についての詳細は、『[Catalyst 6500 シリーズ Cisco IOS ソフトウェア コンフィギュレーション ガイド、12.2SX](#)』の「[ローカル SPAN、リモート SPAN \(RSPAN\)、およびカプセル化 RSPAN の設定](#)」を参照してください。

**RSPAN ソース セッションおよび宛先セッションは同じ Catalyst スイッチに存在できませんか。**

No.RSPAN ソース セッションおよび RSPAN 宛先セッションが同じスイッチにある場合、RSPAN は動作しません。

RSPAN ソース セッションが特定の RSPAN VLAN で設定され、その RSPAN VLAN の RSPAN 宛先セッションが同じスイッチで設定されている場合、RSPAN 宛先セッションの宛先ポートでは、ハードウェアの制限により RSPAN ソース セッションからキャプチャされたパケットは送信されません。これは、4500 シリーズおよび 3750 シリーズ スイッチではサポートされていません。この問題は、Cisco Bug ID [CSCeg08870](#) (登録ユーザ専用) に記載されています。

次に例を示します。

```
monitor session 1 source interface Gi6/44
monitor session 1 destination remote vlan 666
monitor session 2 destination interface Gi6/2
monitor session 2 source remote vlan 666
```

この問題の回避策は、通常の SPAN を使用することです。

**SPAN 宛先ポートに接続されているネットワーク アナライザやセキュリティ デバイスに到達できません。**

SPAN 宛先ポートの基本的な特性は、SPAN セッションに必要なトラフィック以外は、どのようなトラフィックも送信しないことです。SPAN 宛先ポートを通してネットワーク アナライザまたはセキュリティ デバイスに到達する (IP 到達可能性) 必要があるならば、入トラフィックの転送をイネーブルにする必要があります。

入力がイネーブルになっている場合、SPAN 宛先ポートでは着信パケットを受け取ります。着信パケットは、指定されたカプセル化モードに応じて潜在的にタグ付けされ、通常はスイッチングされます。SPAN 宛先ポートを設定する際、入力機能がイネーブルにされるかどうかを指定し、タグなしの入力パケットをスイッチングするためにどの VLAN を使用するか指定できます。すべての ISL でカプセル化された VLAN タグを持つパケットのように、ISL カプセル化が設定されていると、入力 VLAN の指定は必要ありません。ポートは STP フォワーディングになっていますが、STP には参加していません。そのため、スパンニングツリー ループがネットワークに導入されないように、この機能を設定する際には注意してください。入力およびトランクのカプセル化の両方が SPAN 宛先ポートで指定されている場合、ポートではすべてのアクティブ VLAN でフォワーディングします。存在しない VLAN を入力 VLAN として設定することは許可されません。

```
monitor session session_number destination interface interface [encapsulation {isl | dot1q}]
ingress [vlan vlan_IDs]
```

次の例では、ネイティブ VLAN 7 を使用して、802.1q カプセル化および入力パケットで宛先ポートを設定する方法を示しています。

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

この設定では、802.1q カプセル化により、セッション 1 に関連付けられた SPAN ソースからのトラフィックが、インターフェイス ファスト イーサネット 5/48 からコピーされます。着信トラフィックは、VLAN 7 に分類されたタグなしのパケットで受け入れられ、スイッチングされます。

。

## 関連情報

- [Cisco IOS ソフトウェアが稼動する Cisco Catalyst 4500 スイッチでの SPAN および RSPAN の設定方法](#)
- [SPAN 宛先ポートが「not connected」（未接続）と表示され、ネットワークの他の部分と通信できない](#)
- [スイッチ製品に関するサポート ページ](#)
- [LAN スイッチングに関するサポート ページ](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)