



## 概要

---

この章の内容は、次のとおりです。

- [レイヤ2イーサネット スイッチングの概要, 1 ページ](#)
- [VLAN, 1 ページ](#)
- [プライベート VLAN, 2 ページ](#)
- [スパンニング ツリー, 2 ページ](#)

## レイヤ2イーサネット スイッチングの概要

このデバイスは、レイヤ2イーサネット セグメント間の同時パラレル接続をサポートします。イーサネットセグメント間のスイッチドコネクションは、パケットが伝送されている間だけ維持されます。次のパケットには、別のセグメント間に新しい接続が確立されます。

また、このデバイスでは、各デバイス（サーバなど）を独自の10、100、1000 Mbps、または10ギガビットのコリジョンドメインに割り当てることによって、広帯域デバイスおよび多数のユーザによって発生する輻輳の問題を解決できます。各LANポートが個別のイーサネット コリジョンドメインに接続されるので、スイッチド環境のサーバは全帯域幅にアクセスできます。

イーサネット ネットワークではコリジョンによって深刻な輻輳が発生するため、全二重通信を使用することが有効な対処法の1つとなります。一般的に、10/100 Mbpsイーサネットは半二重モードで動作するので、各ステーションは送信または受信のどちらかしか実行できません。これらのインターフェイスを全二重モードに設定すると、2つのステーション間で同時に送受信を実行できます。パケットを双方向へ同時に送ることができるので、有効なイーサネット帯域幅は2倍になります。1/10ギガビットイーサネットは、全二重モードだけで動作します。

## VLAN

VLANは、ユーザの物理的な位置に関係なく、機能、プロジェクトチーム、またはアプリケーションなどで論理的に分割されたスイッチドネットワークです。VLANは、物理LANと同じ属

性をすべて備えています。同じ LAN セグメントに物理的に配置されていないエンドステーションもグループ化できます。

どのようなスイッチポートでも VLAN に属することができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN に属する端末だけに転送またはフラッディングされます。各 VLAN は 1 つの論理ネットワークであると見なされます。VLAN に属していないステーション宛てのパケットは、ブリッジまたはルータを経由して転送する必要があります。

デバイスの初回の起動時は、管理ポートを含むすべてのポートがデフォルト VLAN (VLAN1) に割り当てられます。VLAN インターフェイスまたは Switched Virtual Interface (SVI; スイッチ仮想インターフェイス) は、VLAN 間の通信用として作成されるレイヤ 3 インターフェイスです。

このデバイスは、IEEE 802.1Q 規格に基づき、4094 の VLAN をサポートします。これらの VLAN はいくつかの範囲に分かれています。各範囲の使用法は少しずつ異なります。一部の VLAN はデバイスの内部使用のために予約されているため、設定には使用できません。



(注) Cisco Nexus 5000 シリーズ用 NX-OS ソフトウェアでは、スイッチ間リンク (ISL) トランッキングはサポートされていません。

## プライベート VLAN

プライベート VLAN は、レイヤ 2 レベルでのトラフィック分離とセキュリティを提供します。

プライベート VLAN は、同じプライマリ VLAN を使用する、プライマリ VLAN とセカンダリ VLAN の 1 つまたは複数のペアで構成されます。セカンダリ VLAN には、独立 VLAN とコミュニティ VLAN の 2 種類があります。独立 VLAN 内のホストは、プライマリ VLAN 内のホストだけと通信します。コミュニティ VLAN 内のホストは、そのコミュニティ VLAN 内のホスト間およびプライマリ VLAN 内のホストとだけ通信でき、独立 VLAN または他のコミュニティ VLAN 内のホストとは通信できません。

セカンダリ VLAN が独立 VLAN であるかコミュニティ VLAN であるかに関係なく、プライマリ VLAN 内のインターフェイスはすべて、1 つのレイヤ 2 ドメインを構成します。つまり、必要な IP サブネットは 1 つだけです。

## スパニング ツリー

ここでは、スパニングツリープロトコル (STP) の実装について説明します。このマニュアルでは、IEEE 802.1w および IEEE 802.1s を指す用語として、「スパニングツリー」を使用します。このマニュアルで IEEE 802.1D 規格のスパニングツリープロトコルについて記す場合は、802.1D であることを明記します。

## STP の概要

STP は、レイヤ 2 レベルで、ループのないネットワークを実現します。レイヤ 2 LAN ポートは STP フレーム (Bridge Protocol Data Unit (BPDU;ブリッジプロトコルデータユニット)) を一定の時間間隔で送受信します。ネットワークデバイスは、これらのフレームを転送せずに、フレームを使用してループフリーパスを構築します。

802.1D は、オリジナルの STP 規格です。基本的なループフリー STP から、多数の改善を経て拡張されました。Per VLAN Spanning Tree (PVST+) では、各 VLAN に個別にループフリーパスを作成できます。また、機器の高速化に対応して、ループフリーコンバージェンス処理も高速化するために、規格全体が再構築されました。802.1w 規格は、高速コンバージェンスが統合された STP で、Rapid Spanning Tree (RSTP) と呼ばれています。

さらに、802.1s 規格のマルチ スパニング ツリー (MST) では、複数の VLAN を単一のスパニング ツリー インスタンスにマッピングできます。各インスタンスは、独立したスパニング ツリー トポロジで実行されます。

ソフトウェアは、従来の 802.1D システムで相互運用できますが、システムでは Rapid PVST+ および MST が実行されます。特定の VDC に、Rapid PVST+ または MST のどちらかを使用できます。1 つの VDC では両方は使用できません。Rapid PVST+ は、Cisco Nexus 5000 シリーズ用 Cisco NX-OS のデフォルトの STP プロトコルです。



(注) Cisco Nexus 5000 シリーズ用 Cisco NX-OS では、拡張システム ID と MAC アドレス リダクションが使用されます。これらの機能をディセーブルにすることはできません。

また、シスコはスパニング ツリーの動作を拡張するための独自の機能をいくつか作成しました。

## Rapid PVST+

Rapid PVST+ は、ソフトウェアのデフォルトのスパニング ツリー モードで、デフォルト VLAN および新規作成のすべての VLAN 上で、デフォルトでイネーブルになります。

設定された各 VLAN 上で RSTP の単一インスタンスまたはトポロジが実行され、VLAN 上の各 Rapid PVST+ インスタンスに 1 つのルート デバイスが設定されます。Rapid PVST+ の実行中には、VLAN ベースで STP をイネーブルまたはディセーブルにできます。

## MST

このソフトウェアは、MST もサポートしています。MST を使用した複数の独立したスパニング ツリー トポロジにより、データ トラフィック用に複数の転送パスを提供し、ロード バランシングを有効にして、多数の VLAN をサポートするために必要な STP インスタンスの数を削減できます。

MSTにはRSTPが統合されているので、高速コンバージェンスもサポートされます。MSTでは、1つのインスタンス（転送パス）で障害が発生しても他のインスタンス（転送パス）に影響しないため、ネットワークのフォールトトレランスが向上します。



(注) スパニングツリーモードを変更すると、すべてのスパニングツリーインスタンスが前のモードで停止して新規モードで開始されるため、トラフィックが中断されます。

コマンドラインインターフェイスを使用すると、先行標準（標準ではない）のMSTメッセージを指定インターフェイスで強制的に送信できます。

## STP 拡張機能

このソフトウェアは、次に示すシスコ独自の機能をサポートしています。

- **スパニングツリーポートタイプ**：デフォルトのスパニングツリーポートタイプは、標準（normal）です。レイヤ2ホストに接続するインターフェイスをエッジポートとして、また、レイヤ2スイッチまたはブリッジに接続するインターフェイスをネットワークポートとして設定できます。
- **ブリッジ保証**：ポートをネットワークポートとして設定すると、ブリッジ保証によりすべてのポート上にBPDUが送信され、BPDUを受信しないポートはブロッキングステートに移行します。この拡張機能を使用できるのは、Rapid PVST+またはMSTを実行する場合だけです。
- **BPDUガード**：BPDUガードは、BPDUを受信したポートをシャットダウンします。
- **BPDUフィルタ**：BPDUフィルタは、ポート上でのBPDUの送受信を抑制します。
- **ループガード**：ループガードは、非指定ポートがSTPフォワーディングステートに移行するのを阻止し、ネットワーク上でのループの発生を防止します。
- **ルートガード**：ルートガードは、ポートがSTPトポロジのルートにならないように防御します。