



## 概要

---

- [ライセンス要件 \(1 ページ\)](#)
- [サポートされるプラットフォーム \(1 ページ\)](#)
- [レイヤ2イーサネット スイッチングの概要, on page 1](#)
- [VLANs, on page 2](#)
- [スパンニングツリー, on page 2](#)
- [トラフィック ストーム制御, on page 4](#)
- [関連項目, on page 5](#)

## ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、ライセンスの取得および適用の方法については、『[Cisco NX-OS ライセンス ガイド](#)』および『[Cisco NX-OS ライセンス オプション ガイド](#)』を参照してください。

## サポートされるプラットフォーム

Cisco NX-OS リリース 7.0(3)I7(1)以降、「[Nexus スイッチ プラットフォーム サポート マトリクス](#)」を使用して、選択した機能をサポートするさまざまな Cisco Nexus 9000 および 3000 スイッチのリリース元である Cisco NX-OS を知ることができます。

## 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。

デバイスは、高帯域のデバイスおよび多数のユーザに起因する輻輳問題を解決するために、デバイス（サーバなど）ごとに専用のコリジョンドメインを割り当てます。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。

## VLANs

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にすべてのポートがデフォルトのVLAN (VLAN1) に割り当てられます。VLANインターフェイスまたはスイッチ仮想インターフェイス (SVI) 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、4095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。



**Note** Cisco NX-OS では、スイッチ間リンク (ISL) はサポートされません。

## スパニングツリー

ここでは、ソフトウェア上での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 (ブリッジプロトコルデータユニット (BPDU)) 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。現在では、各 VLAN 用の STP に高速コンバージェンスタイムを実装できます。これが、Per VLAN Rapid Spanning Tree (Rapid PVST+) です。

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。Rapid PVST+ は、Cisco Nexus デバイス用のデフォルトの STP プロトコルです。



---

**Note** 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。これらの機能はディセーブルにできません。

---

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。



**Note** 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状態に移行します。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 ガードを使用すると、ポイントツーポイントリンク上の単方向リンク障害によって発生するブリッジングループを防止できます。
- **ルート ガード**：STP ルート ガードを使用すると、ポートがルートポートまたはブロッキングされたポートになることが防止されます。ルート ガードに設定されたポートが上位 BPDU を受信すると、このポートはただちにルートとして一貫性のない（ブロックされた）状態になります。

## トラフィック ストーム制御

トラフィック ストーム制御（トラフィック抑制ともいいます）を使用すると、着信トラフィックのレベルを 1 秒より大きなインターバルでモニタできます。この間、トラフィック レベル（ポートの使用可能合計帯域幅に対するパーセンテージ）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

詳細については、『[Cisco Nexus 9000 シリーズ NX-OS セキュリティ構成ガイド](#)』の「[トラフィック ストーム制御の構成](#)」を参照してください。Cisco NX-OS リリース 10.3(2)F 以降、トラフィック ストーム制御機能はレイヤ 3 でもサポートされます。

## 関連項目

レイヤ 2 スイッチング機能に関連するマニュアルは、次のとおりです。

- 『*Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 9000 Series NX-OS Security Configuration Guide*』
- 『*Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide*』
- 『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』



## 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。