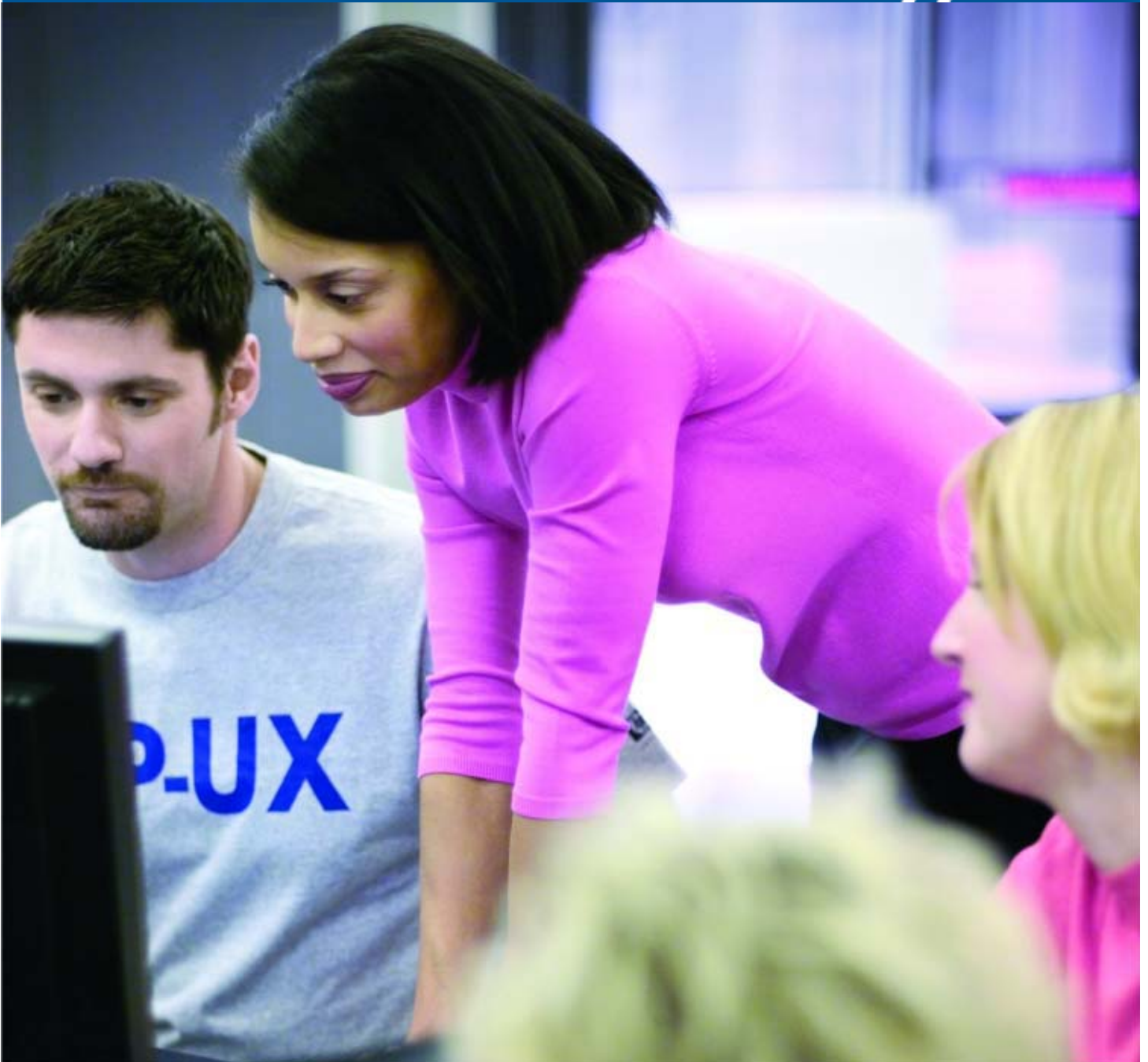


# HP ProCurve Campus LANs

Rev. 9.41





---

# 目次

## モジュール 1: 概要

|  |      |
|--|------|
| はじめに   | 1-2  |
| コースの目的   | 1-4  |
| HP ProCurve について                                       | 1-5  |
| HP ProCurve について: Adaptive Networks                    | 1-6  |
| HP ProCurve について: パーソナライズ                              | 1-7  |
| HP ProCurve について: ProCurve の AdaptiveEDGEArchitecture™ | 1-8  |
| HP ProCurve および Cisco の用語: 一般的な用語                      | 1-9  |
| HP 認定プロフェッショナルプログラム: トレーニングと認定                         | 1-11 |
| 詳細情報へのリンク  | 1-12 |
| 参考資料   | 1-13 |

## モジュール 2: マーケットセグメント

|                                     |     |
|-------------------------------------|-----|
| モジュールの目的                            | 2-2 |
| HP ProCurve の成長                     | 2-3 |
| HP ProCurve の成長: マーケットリーダー          | 2-5 |
| HP ProCurve と標準: 標準への適合を推進          | 2-6 |
| HP ProCurve ネットワーキングの優位性            | 2-7 |
| HP ProCurve ネットワーキングの優位性: 認められたブランド | 2-8 |

## モジュール 3: 製品ラインの概要

|   |      |
|---|------|
| モジュールの目的                                      | 3-2  |
| 統合  | 3-3  |
| 統合: 統合の最初のステップ                                | 3-4  |
| 統合: 統合の 2 番目のステップ                             | 3-5  |
| 統合: 統合の 3 番目のステップ                             | 3-6  |
| スイッチ: ProVision ASIC ベースのスイッチ                 | 3-7  |
| スイッチ: ProCurve Switch 8212zl ハードウェアの概要        | 3-8  |
| スイッチ: 機能グループの違い                               | 3-9  |
| HP ProCurve モビリティ製品: 無線 LAN の発展               | 3-10 |
| HP ProCurve モビリティ製品: 分散インテリジェンス - 最適なアーキテクチャ  | 3-15 |
| HP ProCurve モビリティ製品: マルチサービスモビリティソリューション      | 3-16 |
| HP ProCurve モビリティ製品: センtralコンローラーのラインナップ      | 3-17 |
| HP ProCurve 管理製品: Windows ベースのネットワーク管理ソリューション | 3-18 |

|  |        |
|--|--------|
| HP ProCurve 管理製品: Identity Driven Manager の概要      | 3-19   |
| HP ProCurve 管理製品: Network Immunity Manager の概要     | 3-20   |
| HP ProCurve 管理製品: Mobility Manager の概要             | 3-21   |
| HP ProCurve 管理製品: 包括的な GUI ベースの無線 LAN 管理ツール        | 3-22   |
| HP ProCurve 管理製品: ProCurve Guest Management ソフトウェア | 3-23   |
| HP ProCurve 管理製品                                   | 3-24   |
| HP ProCurve 管理製品: HP ProCurve RP Planner           | 3-25   |
| 製品ラインのまとめ: HP ProCurve 製品                          | 3-26   |
| 確認テスト  | 3-27   |
|  |        |
| モジュール 4: Cisco 製品との比較                              |        |
| モジュールの目的   | 4-2    |
| ポート識別子: 違いの比較                                      | 4-3    |
| ポート識別子: スタックابلスイッチ                                | 4-4    |
| ポート識別子: モジュール式スイッチ                                 | 4-5    |
| 一般的なサービス: サービスの概要                                  | 4-6    |
| ProCurve スイッチがサポートする機能: CDP および IEEE 802.1AB LLDP  | 4-7    |
| VLAN の設定: スイッチ間の接続                                 | 4-8    |
| VLAN の設定: スイッチとコンピューターの間に IP 電話機を接続                | 4-9    |
| 設定シナリオ: スタティックな (リンク) 集約                           | 4-10   |
| 設定シナリオ: LACP を使用したダイナミックな (リンク) 集約                 | 4-11   |
| 設定シナリオ: OSPF 設定の比較                                 | 4-12   |
| 確認テスト  | 4-13   |
|  |        |
| モジュール 5: 使用方法と設定方法                                 |        |
| モジュールの目的   | 5-1-2  |
| モジュール 5-1: スイッチ管理                                  |        |
| ダイレクトシリアル接続  | 5-1-4  |
| スイッチ管理のインターフェイス                                    | 5-1-5  |
| 管理アクセスのセキュリティ確保                                    | 5-1-6  |
| マネージャーレベルとオペレーターレベルの権限の設定                          | 5-1-7  |
| 設定したパスワードの削除                                       | 5-1-8  |
| セキュリティ認証情報: コンフィギュレーションファイルに含まれる                   | 5-1-9  |
| セキュリティ認証情報: コンフィギュレーションファイルの例                      | 5-1-10 |
| 前面パネルのセキュリティ                                       | 5-1-11 |
| 前面パネルのボタンのセキュリティ設定                                 | 5-1-12 |

|  |        |
|--|--------|
| マネージャーレベルとオペレーターレベルの間の移動                       | 5-1-13 |
| CLI のナビゲーション                                   | 5-1-14 |
| CLI のヒントとショートカット                               | 5-1-15 |
| 初期設定での CLI の使用                                 | 5-1-16 |
| Web インターフェイスの使用                                | 5-1-17 |
| リモート管理の有効化の復習                                  | 5-1-18 |
| CDP および IEEE 802.1AB LLDP: ProCurve スイッチでの対応状況 | 5-1-20 |
| 役に立つ show コマンド                                 | 5-1-21 |
| システムログのイベントの表示                                 | 5-1-22 |
| コンフィギュレーションファイルの管理に役立つコマンド                     | 5-1-23 |
| 確認テスト  | 5-1-24 |

## モジュール 5-2: ポートと VLAN

|                              |        |
|------------------------------|--------|
| ポートのタイプ                      | 5-2-2  |
| ポートに関する用語: 違いの比較             | 5-2-3  |
| ポート識別子: スタックブルスイッチ           | 5-2-4  |
| ポート識別子: モジュール式スイッチ           | 5-2-5  |
| ポートの速度とモードの変更                | 5-2-6  |
| ポートステータスの表示                  | 5-2-7  |
| VLAN 設定の比較: スイッチ間            | 5-2-8  |
| VLAN 設定の比較: スイッチ間のノード        | 5-2-9  |
| スイッチとコンピューター間に IP 電話機を接続     | 5-2-10 |
| スイッチ間の VLAN 境界の拡張            | 5-2-11 |
| VLAN 内でのフォワーディング             | 5-2-12 |
| Cisco スイッチでの VLAN の定義        | 5-2-13 |
| VLAN 間のフォワーディング              | 5-2-14 |
| VLAN 間でフォワーディングするためのルートエントリー | 5-2-15 |
| 役に立つ show コマンド               | 5-2-16 |
| 確認テスト                        | 5-2-17 |

## モジュール 5-3: リンクアグリゲーション

|   |       |
|---|-------|
| リンクアグリゲーションの方法                              | 5-3-2 |
| ProCurve スイッチでポートランキングが VLAN ステータスに影響を与える方法 | 5-3-4 |
| フレンドリポート名を使用したトランクステータスの表示                  | 5-3-5 |
| 設定シナリオ: LACP を使用したダイナミックな (リンク) 集約          | 5-3-6 |

|                |       |
|----------------|-------|
| 役に立つ show コマンド | 5-3-7 |
| 確認テスト          | 5-3-8 |

## モジュール 5-4: スパニングツリーの実装

|  |        |
|--|--------|
| STP と RSTP   | 5-4-2  |
| Cisco PVST+ と Rapid PVST+                            | 5-4-3  |
| PVST+と MSTP の比較                                      | 5-4-4  |
| さまざまなスパニングツリー-BPDU                                   | 5-4-5  |
| Cisco-ProCurve のシナリオ 1: Rapid PVST+                  | 5-4-9  |
| Cisco-ProCurve のシナリオ 1: VLAN と PVST                  | 5-4-10 |
| Cisco 機器での Rapid PVST+の設定                            | 5-4-11 |
| Cisco Rapid PVST+: トランクポートで送信される BPDU                | 5-4-12 |
| Cisco-ProCurve のシナリオ 1: ProCurve スイッチの設定             | 5-4-17 |
| Cisco-ProCurve のシナリオ 1: Cisco スイッチの設定                | 5-4-18 |
| Cisco-ProCurve のシナリオ 2: ロードバランシングを行う 場合の Rapid PVST+ | 5-4-20 |
| MSTP の実装   | 5-4-21 |
| MST リージョン  | 5-4-22 |
| MST インスタンス   | 5-4-23 |
| MST リージョンの例  | 5-4-24 |
| 確認テスト  | 5-4-25 |
| MSTP BPDU  | 5-4-27 |
| CST の機能  | 5-4-28 |
| プライオリティの設定: IST と MST インスタンス                         | 5-4-29 |
| MSTP が VLAN 設定を認識しているかどうか?                           | 5-4-30 |
| 冗長パスのあるネットワークでの VLAN の設定                             | 5-4-31 |
| 新しい VLAN の定義   | 5-4-33 |
| MST インスタンスへの VLAN の割り当て                              | 5-4-34 |
| スパニングツリーと LLDP                                       | 5-4-35 |
| MSTP の一般的な設定手順                                       | 5-4-36 |
| Cisco 機器での MSTP の設定                                  | 5-4-37 |
| ProCurve 機器での MSTP の設定                               | 5-4-40 |
| ProCurve でのプライオリティの設定: ProCurve 機器がコアにある場合の例         | 5-4-43 |
| ProCurve 機器でのポートの設定                                  | 5-4-44 |
| ProCurve 機器でのポートの設定: バージョン K.12.04 より前の場合            | 5-4-46 |
| ProCurve がサポートするスパニングツリーのバージョン                       | 5-4-47 |

|                            |        |
|----------------------------|--------|
| MSTP の有効化                  | 5-4-48 |
| ProCurve 機器での MSTP 設定の確認   | 5-4-49 |
| MSTP のトラブルシューティング          | 5-4-51 |
| 役に立つ show コマンド             | 5-4-52 |
| Spanning Tree Hardening    | 5-4-53 |
| Spanning Tree Hardening 機能 | 5-4-54 |
| 確認テスト                      | 5-4-60 |

#### モジュール 5-5: PoE と VoIP 電話機

|                                      |        |
|--------------------------------------|--------|
| PoE デバイス                             | 5-5-2  |
| 管理システム—さまざまな PoE ステータス               | 5-5-3  |
| システム全体の PoE ステータスの管理                 | 5-5-4  |
| ポートレベルの PoE ステータスの表示                 | 5-5-5  |
| すべてのポートの PoE ステータスの表示                | 5-5-6  |
| PoE 設計上の考慮事項                         | 5-5-7  |
| LLDP の動作                             | 5-5-8  |
| LLDP と LLDP-MED の違い                  | 5-5-9  |
| LLDP-MED のコンポーネントモデル                 | 5-5-10 |
| マルチベンダーのサポート: PC と VoIP 電話機による接続の共有  | 5-5-11 |
| 音声の自動設定                              | 5-5-12 |
| VLAN 設定の比較: スイッチとコンピューター間に IP 電話機を接続 | 5-5-13 |
| トラフィックの分類                            | 5-5-14 |
| トラフィックの分類: キューへのマッピング                | 5-5-15 |
| トラフィックのマーキング                         | 5-5-16 |
| QoS プロセスの概要                          | 5-5-17 |
| ProCurve の QoS サポートの概要               | 5-5-18 |
| WAN リンク経由でのプライオリティの保持                | 5-5-19 |
| トラフィックの分類基準                          | 5-5-20 |
| DiffServ Code Point マッピングテーブルの表示     | 5-5-21 |
| 運用上の注意点: DSCP マッピングテーブルの管理           | 5-5-22 |
| QoS 設定の比較                            | 5-5-23 |
| 確認テスト                                | 5-5-24 |

#### モジュール 5-6: DHCP とインテリジェントミラーリング

|                 |       |
|-----------------|-------|
| DHCP スヌーピングの有効化 | 5-6-2 |
| DHCP スヌーピングの設定  | 5-6-3 |

|                                       |        |
|---------------------------------------|--------|
| オプション 82 の設定                          | 5-6-4  |
| 設定例                                   | 5-6-5  |
| レガシートラフィックのミラーリング                     | 5-6-6  |
| インテリジェントミラーリング                        | 5-6-7  |
| インテリジェントミラーリング: セッションのサポート            | 5-6-8  |
| トラフィックの送信方向に基づくフィルタリング                | 5-6-9  |
| ACL を使用したトラフィックのフィルタリング               | 5-6-10 |
| トラフィックのローカルミラーリング: 設定手順の概要            | 5-6-11 |
| トラフィックのローカルミラーリング: ミラーセッションと出力ポート     | 5-6-12 |
| トラフィックのローカルミラーリング: トラフィックの送信元とフィルタリング | 5-6-13 |
| トラフィックのローカルミラーリング: 設定の表示              | 5-6-15 |
| トラフィックのリモートミラーリング: 設定手順の概要            | 5-6-16 |
| 確認テスト                                 | 5-6-17 |
| <br>                                  |        |
| モジュール 5-7: OSPF を使用したルーティング           |        |
| IP ルーティングの有効化                         | 5-7-2  |
| サブネット間のルーティング: 要件                     | 5-7-3  |
| ループバックインターフェイスの使用                     | 5-7-4  |
| ルーティングテーブルの表示                         | 5-7-5  |
| スタティックルートの設定                          | 5-7-6  |
| OSPF の設定                              | 5-7-7  |
| スイッチのコンフィギュレーションファイル: OSPF エントリー      | 5-7-8  |
| OSPF ステータスの確認                         | 5-7-9  |
| OSPF エントリーのあるルーティングテーブル               | 5-7-10 |
| OSPF の設定シナリオ                          | 5-7-11 |
| OSPF 設定の比較                            | 5-7-12 |
| 詳細情報                                  | 5-7-13 |
| 確認テスト                                 | 5-7-14 |



# *HP ProCurve Campus LANs*



## はじめに

この『HP ProCurve Campus LANs』コースは、HP ProCurve 認定試験の受験準備用に開発されました。コースの各モジュールに含まれる確認テストは、コースの理解度の評価に役立ちます。

### コースの内容:

- モジュール1: 概要
- モジュール2: マーケットセグメント
- モジュール3: 製品ラインの概要
- モジュール4: Cisco製品との比較
- モジュール5: 使用方法と設定方法

このコースでは、同じネットワークにあるCisco製品とHP ProCurve製品の類似点と相違点を中心に説明します。このコースの学習には約4時間かかります。

このコースの英語版Webトレーニング『HP ProCurve Campus LANs v9.41』に含まれる資料(Interoperability-ILT-Courseware.zip)には、このトレーニングコース『HP ProCurve Campus LANs v9.41』に対応するStudent GuideおよびLab Guideが含まれています。これはインストラクターが行う形式のトレーニング用のテキストです。受験前にこれらのテキストも学習されることを強くお勧めいたします。

この英語版Webトレーニング『HP ProCurve Campus LANs v9.41』の入手方法については、以下のHP ProCurveサイト(英語)を参照してください。

<http://www.procurve.com/training/training/technical/ase/campus-lans-941.htm>

# モジュール1: 概要



## コースの目的

このコースを修了すると、以下のことができるようになります。

- HP ProCurve Networking製品に関する知識を得る
- Cisco製品とHP ProCurve製品の機能や設定の相違点と類似点を特定する
- 同じネットワーク上で動作するCisco製品とHP ProCurve製品の相互運用について理解する

このコースは、ネットワークエンジニアやHP ProCurveのパートナー、カスタマーを対象としています。HP ProCurve製品とCisco製品を相互運用するネットワークでHP ProCurveスイッチング製品やルーティング製品を設置、設定、管理する方法について学習します。

このコースは、Ciscoのルーターやスイッチに関する知識や経験を前提にしています。

## HP ProCurveについて

### HP ProCurve – Network of Choice

HP ProCurveは、有線ネットワークおよび無線ネットワークにおけるクラス最高のソリューション、製品、サービスを提供します。HP ProCurveのビジョンである Adaptive Networksは、絶えず変化を続けるユーザー、アプリケーション、企業のニーズに適応する、オープンで標準に基づいたネットワークインフラを導入できるようにします。

## HP ProCurveについて: Adaptive Networks

Adaptive Networksとは:

- ユーザーに適応する
- アプリケーションに適応する
- 企業のニーズに適応する



**高度に安全で可用性が高く、柔軟な統合ネットワークインフラ上で実現**

Adaptive Networksを導入することにより、企業は重要度の高いビジネスに集中して、急速に変化するグローバルマーケットで競争力を高め、競争力を保つことができるようになります。

つまり、現在においては、ネットワークインフラは、ビジネスを発展させ、競争に勝つための戦略的資産と言えます。ProCurveのビジョンであるAdaptive Networksは、ユーザー、アプリケーション、企業のニーズに適応します。

## HP ProCurveについて: パーソナライズ

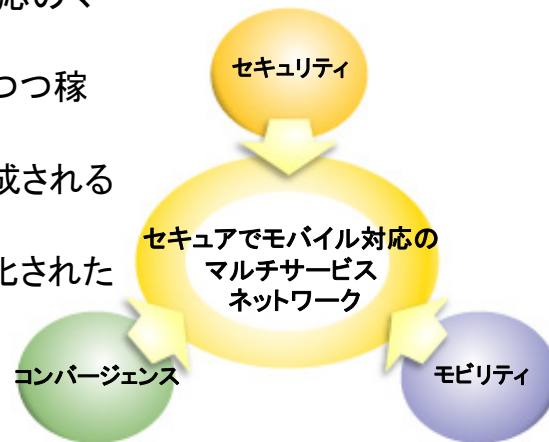


- ネットワークがユーザーのIDとデバイスを認識
- アクセス方法が簡単で、便利な機能を持ち、制御可能
- 承認されたアクセスのみを許可するので、アプリケーションを最適化できる
- 接続する場所に関係なく、一貫した方法でネットワークを使用可能

ProCurveのアダプティブネットワークは、それぞれのユーザーが使用するIDやデバイスを認識するインテリジェントなネットワークです。そのため、ネットワークに接続する場所や、使用するコンピューターや通信デバイスを意識することなく、ネットワークを使用できます。

## HP ProCurveについて: ProCurveのAdaptive EDGE Architecture™

- 統合性が高く、柔軟でシンプルなネットワークインフラにより、セキュアでモバイル対応のマルチサービスネットワークを実現
  - セキュリティ: ネットワークを保護しつつ稼働させる
  - モビリティ: 無線および有線から構成される環境を制御
  - コンバージェンス: シンプルで最適化されたネットワーク



ProCurveが2002年から推進しているAEA - Adaptive EDGE Architecture (AEA)を導入することにより、効果的にネットワークを拡張して、変化を続けるビジネスニーズに適応するリソースに時間や場所を問わずにアクセスできるようになります。このような統合アプローチは、セキュリティやモビリティ、コンバージェンスなどのニーズに対応しています。



## HP ProCurveおよびCiscoの用語: 一般的な用語

|  |  |
|--|--|
| Service-Oriented Network Architecture (SONA) | Ciscoのサービス指向型ネットワークアーキテクチャ (SONA) は、ProCurveの提供するソリューションに最も密接に関連している   |
| Adaptive Network Strategy                    | ProCurveが提供するソリューションの土台となるビジョン   |
| Adaptive Edge Architecture™                  | ProCurveのAdaptive Network Strategyを構成するさまざまなコンポーネントを記述する方法   |
| Networked Infrastructure Layer               | CiscoがSONAのNetworked Infrastructure Layerにおける重要なポイントとする場所: <ul style="list-style-type: none"><li>- キャンパスネットワーク</li><li>- ブランチネットワーク</li><li>- データセンター</li><li>- エンタープライズエッジ</li><li>- WAN/MAN</li><li>- テレワーカー</li></ul> |

このコースでは、CiscoおよびHP ProCurveで一般的に使用される用語や表現について説明します。HP ProCurveでは、Ciscoの現在のアーキテクチャモデルをIINのコンテキスト、つまりCiscoのIntelligent Information Networkの考え方に従って理解しています。Ciscoは、顧客の個々のビジネスニーズに対応する4つの技術上のアーキテクチャを採用しています。その1つであるサービス指向型ネットワークアーキテクチャ (SONA) は、HP ProCurveの提供するソリューションに最も密接に関連しています。HP ProCurveが提供するソリューションは、Adaptive Network Strategyというビジョンに基づいて開発されており、また、このAdaptive Network Strategyを構成するさまざまなコンポーネントを記述する方法をAdaptive Edge Architectureと呼んでいます。Ciscoでは、SONAにおける重要なポイントをNetworked Infrastructure Layerと呼んでいます。

## HP ProCurveおよびCiscoの用語: 一般的な用語

| HP ProCurve<br>Adaptive Network<br>Strategy | Cisco<br>Hierarchical Network<br>Model |
|---|--|
| コア  | バックボーン                                 |
| アグリゲーション<br>またはディストリビューション                  | ディストリビューション                            |
| エッジレイヤー<br>またはアクセスレイヤー                      | アクセスレイヤー                               |

このトレーニングでは、ネットワークアーキテクチャーに関する古くてなじみのあるCiscoの用語である、階層型ネットワークモデルという用語を使用します。これは古いモデルですが、このモデルを使用することで、最も基本的な比較が可能になります。

ProCurveでは、この中間階層を、ディストリビューションではなく、アグリゲーションと表現することがあります。ProCurveでは、以前は、Ciscoでアクセスレイヤーと呼ばれるレイヤーをエッジレイヤーと呼んでいました。最近では、ProCurveでもこれをアクセスレイヤーと呼んでいます。



## HP認定プロフェッショナルプログラム: トレーニングと認定

HP ProCurveトレーニングと認定の詳細:  
<http://www.hp.com/go/procurvetraining>

HP認定プロフェッショナルプログラムの詳細:  
<http://www.hp.com/certification>

HP認定プロフェッショナルプログラムは国際的レベルの認定プログラムです。HPテクノロジーとソリューションの計画、導入、サポート、サービスに必要な技術的、営業的能力と専門性を確実に評価するための認定プログラムで、その有効性は世界的に評価されています。販売や統合に関するHPの認定トレーニングプログラムの詳細については、上記を参照してください。



## 詳細情報へのリンク

HP ProCurve製品およびソリューション: <http://www.procurve.com>

HP ProCurveトレーニングと認定:  
<http://www.hp.com/go/procurvetraining>

HP認定プロフェッショナルプログラム:  
<http://www.hp.com/certification>

ソフトウェアバージョンの対応表:  
<http://www.procurve.com/customcare/support/features-matrix.htm>

以下の資料は、このコースの英語版Webトレーニングに含まれています。  
必要に応じて適宜参照してください。

| 説明   | ファイル  |
|--|---|
| このコースと試験の基本的な情報について説明するデータシート  | HP ProCurve Campus LANs v9 41 Datasheet.pdf |
| 『ProCurve Care Competencies』コース – ProCurveのスイッチング/ルーティング製品を設定、設定、管理するProCurveのパートナーおよびカスタマーのネットワークエンジニア向けのコース                                      | ProCurveCoreCompetencies.zip                |
| コースと演習 – このトレーニングコース『ProCurve Campus LANs』の基となった、『ProCurve and Cisco Network Interoperability Training Version 8.31』コース(インストラクターが行う形式のトレーニング用テキスト) | Interoperability-ILT-Courseware.zip         |

この英語版Webトレーニング『HP ProCurve Campus LANs v9.41』の入手方法については、以下のHP ProCurveサイト(英語)を参照してください。

<http://www.procurve.com/training/training/technical/ase/campus-lans-941.htm>

## 参考資料(続き)

| 説明   | ファイル                         |
|--|------------------------------|
| 『ProCurve Security』コース   | ProCurve Security 731.zip    |
| ProCurve製品の使用および設定に関する基礎コース                                      | AdaptiveEdgeFundamentals.zip |
| 『Building ProCurve Resilient, Adaptive Networks Version 7.42』コース | BPRAN_v7.42_SG_C.pdf         |

## 参考資料(続き)

| 説明   | ダウンロードするファイル                 |
|--|------------------------------|
| MultiService Mobility製品に関するコース                         | MSM_V9.11_SG.pdf             |
| ProVision ASICベースのProCurveスイッチに関する『Technical Overview』 | ProVision-Tech-Overviews.zip |
| このコースで扱うトピックを補足するさまざまな資料やガイド                           | Papers&Guides.zip            |

モジュール1終了





## モジュール2: マーケットセグメント



## モジュールの目的

このモジュールを修了すると、以下のことができるようになります。

- HP ProCurveの成長の過程、標準への準拠、市場での強力な位置付けについて理解する

このモジュールでは、HP ProCurveネットワークの成長の過程、標準への準拠、および市場における強固な位置付けについて説明します。

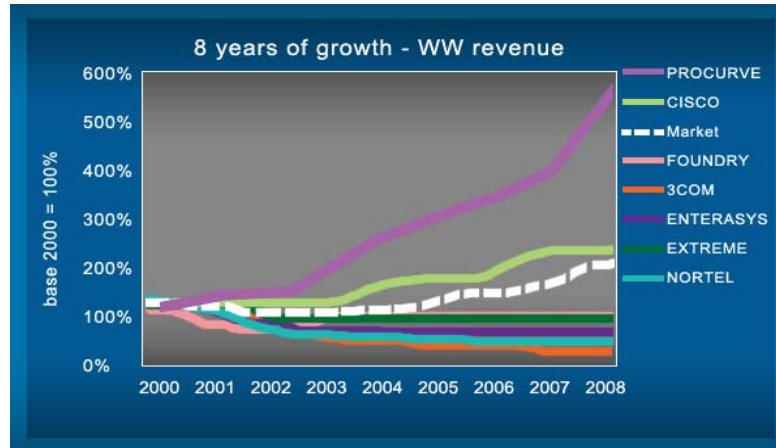
## HP ProCurveの成長

- ProCurveは、市場平均よりもはるかに成長スピードが速い
- ProCurveのビジネス規模は、3年ごとに倍増
  - 前年度に比べて30%の成長。次年度も同様の見込み
- ProCurveは、2003年以来、管理型ポートの出荷\*に関して業界2位

\*出典: IDC、Dell'Oro、2008年

はじめに、ProCurveの成長の概要について説明します。2008年の実績では、ProCurveの成長スピードは市場の平均的な成長よりも速くなっています。ProCurveのビジネス規模は、それ以前の3年間に倍増しており、継続的に投資を行って新たなソリューションの開発を進めることが可能になりました。ProCurveは、業界2位の地位をさらに強化し、成長を続けています。

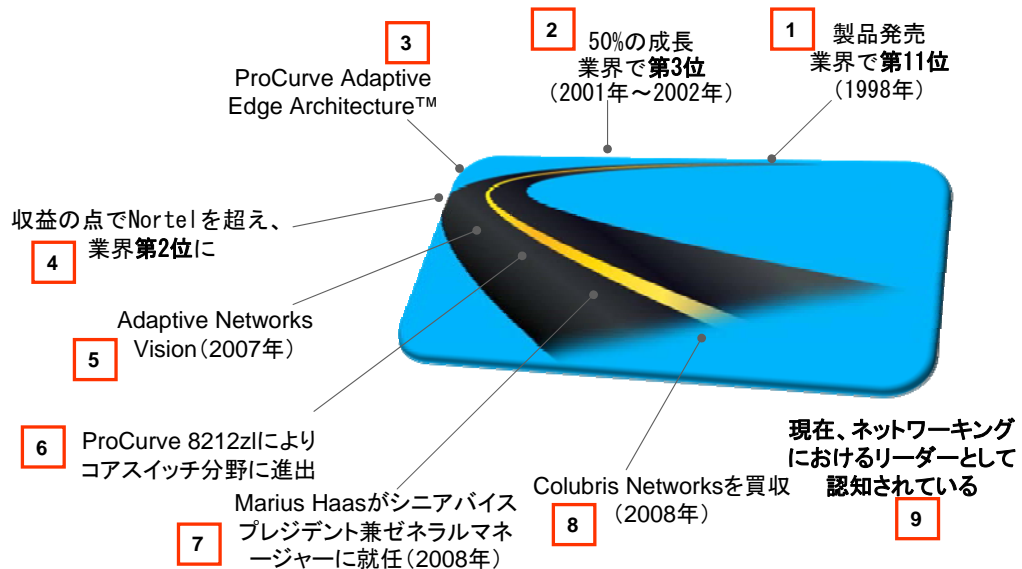
## HP ProCurveの成長



2000年を100%とした場合の世界での収益

このグラフは、Dell'Oro Groupによるデータに基づいて作成したものです。2000年から2008年にかけて、ProCurveがネットワーキング市場や他のネットワークベンダーと比較して、ProCurveが大幅に成長した様子を示しています。

# HP ProCurveの成長: マーケットリーダー



1985年に10Base-Tを開発して以来、HPは、過去25年間にわたってネットワーキングビジネスに取り組んでいます。1990年後半まで、ProCurveはネットワーキング市場において業界第11位でしたが、それ以降、業界におけるProCurveの地位は大幅に向上しました。7年前には、Adaptive Edge Architecture、そして2007年にはAdaptive Networksというビジョンを打ち出し、また、2008年8月にはColubrisを買収することにより、ProCurveは業界第2位にまで成長しました。Colubris Intelligent Mobility Solutionsによって、ProCurveは、無線を統合したアクセス、管理、セキュリティ製品や、802.11n機能を提供できるようになりました。

## HP ProCurveと標準：標準への適合を推進

|                                 |                                    |  |
|---------------------------------|------------------------------------|--|
| 標準策定におけるリーダーシップ                 | <b>IEEE 802.1X</b>                 | 標準を共同開発                                |
|                                 | エンドツーエンドの認証プロトコル                   |  |
|                                 | <b>Trusted Computing Group</b>     | Trusted Network Connect (TNC) 策定における議長 |
|                                 | エンドデバイスの認証/認可                      |  |
|                                 | <b>IETF LWAPP</b>                  | メンバーとして参画                              |
|                                 | Light Weight Access Point Protocol |  |
|                                 | <b>IEEE 802.1AB - LLDP</b>         | 標準を共同開発                                |
| ネットワークの検出とトラブルシューティング           |                                    |  |
| <b>ANSI/TIA-1057 - LLDP-MED</b> | 標準を共同開発                            |  |
| IP電話機の検出と自動設定                   |                                    |  |
| <b>IEEE 802.3ae</b>             | 10G CX4策定における議長                    |  |
| 10Gigabit over Copper           |                                    |  |
| <b>sflow</b>                    | メンバーとして参画                          |  |

ProCurveは、当初から、さまざまな標準策定団体に参加しています。最近の実績の一部をここに示します。ProCurveは、標準が策定されるのを待つのではなく、その策定段階から標準策定団体に加わっています。ProCurveは、多くの領域において標準への準拠や標準の定義を推進しています。ProCurveは、多くの選択肢と柔軟性を提供しており、オープンスタンドードにおけるリーダーシップによって相互運用性を保証し、投資を保護しています。

## HP ProCurveネットワークングの優位性:

ProCurveは、GartnerのLeader Quadrantに位置付けられている



2009年、Campus LANにおけるMagic Quadrant(グローバル)

ProCurveは、GartnerのLeadership Quadrantに位置づけられており、その業績と将来的な発展性が認められています。



HP ProCurve Campus LANs  
マーケットセグメント

## HP ProCurveネットワークの優位性: 認められたブランド

「LANインフラの交換を考えている企業では、HPのProCurve Networking製品を評価リストに加えているはずである」 *Gartner*

「ProCurveのおかげで総運用コストを30%カットできた」 *Hans de Harde, PGGM*



ProCurveのブランド力と勢いはアナリストからも顧客からも認められています。そのマーケットシェアの拡大は、ProCurveが市場に受け入れられる魅力的な製品であることの証明です。ProCurveは、お客様によりよい価値を提供し続けるため、ソリューションの開発を継続的に行い、パフォーマンスの維持と向上に積極的に取り組んでいます。



モジュール2終了



## モジュール3: 製品ラインの概要



## モジュールの目的

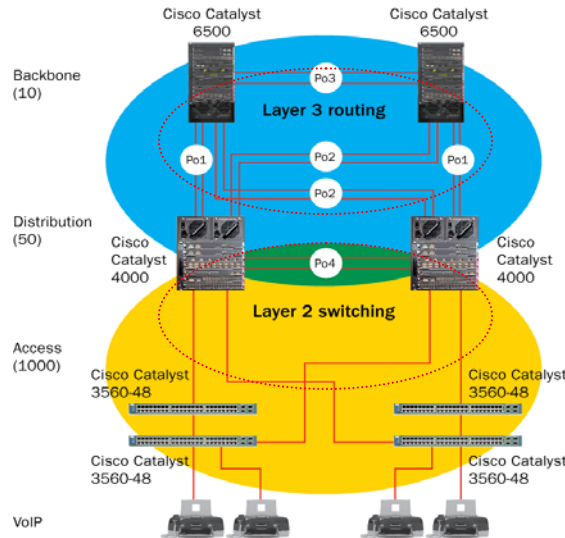
このモジュールを修了すると、以下のことができるようになります。

- ProCurveのスイッチング製品、無線製品にどのようなものがあるかを知る
- ProCurveスイッチの一般的なハードウェア/ソフトウェア機能を理解する

このモジュールでは、ProCurveのスイッチング製品と無線製品のいくつかを紹介し、また、スイッチや無線製品が備える一般的なハードウェア/ソフトウェア機能についても説明します。

# 統合

## シンプルなCiscoネットワークの例

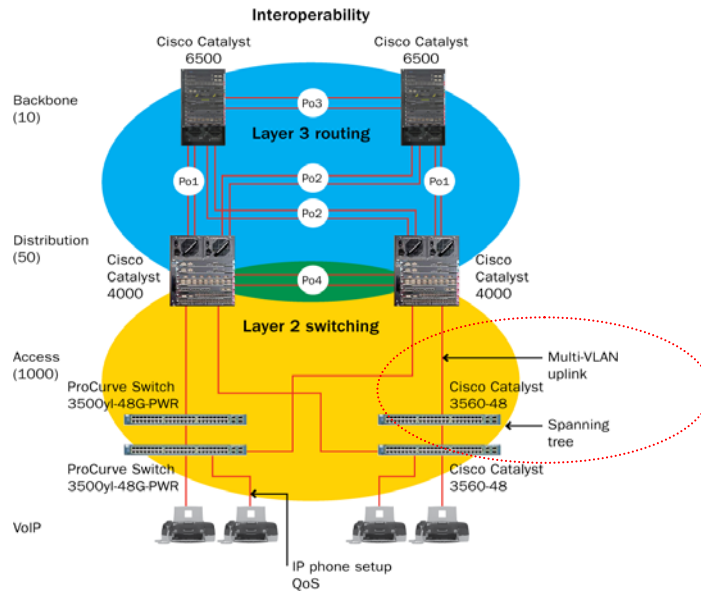


ここに示すのは、Cisco製品によるネットワークの例です。ProCurveとCiscoの相互運用性に関する重要なポイントを説明しやすくするため、ここでは意図的にシンプルなネットワークにしています。ProCurveとCiscoの類似点と相違点について、特にその相互運用性を中心に説明します。

通常、速度が要求されるコアでレイヤー3ルーティングを行うことはありませんが、ここでは相互運用性について説明するためにレイヤー3ルーティングを使用しています。Cisco Catalyst 3500スイッチがアクセスレイヤーに配置されています。これはProCurveでエッジと呼んでいるレイヤーです。ProCurveでは最近、このレイヤーをアクセスレイヤーとも呼んでいます。

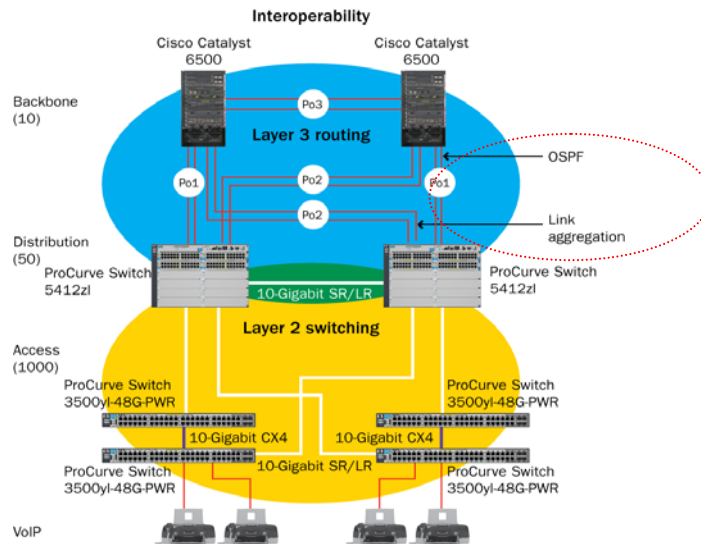
Cisco Catalyst 4000スイッチがディストリビューションレイヤーにあります。これらはいずれもレイヤー2およびレイヤー3スイッチです。コアにあるCisco 6500スイッチは、レイヤー3のみに対応しています。

## 統合: 統合の最初のステップ



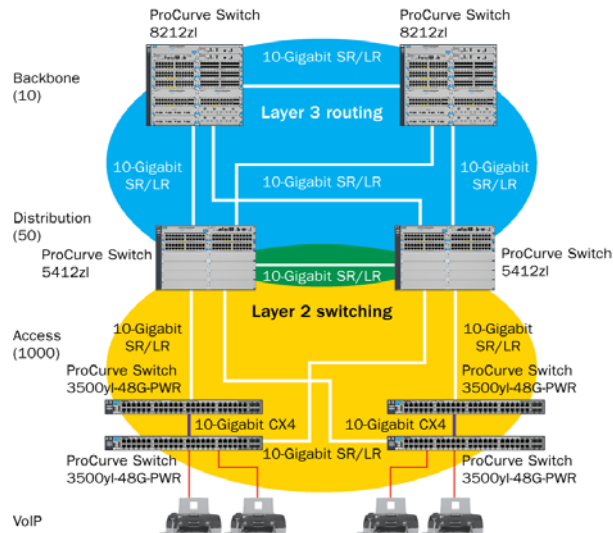
この図は、統合または移行を行う際の最初のステップを示しています。アクセスレイヤーのスイッチがProCurve Edgeスイッチに置き換えられています。アクセスレイヤーのスイッチを置き換えるには、ProCurve Edgeスイッチが、レイヤー2レベルでCisco Catalystディストリビューションスイッチに接続する必要があります。相互運用するレイヤー2には、マルチVLANアップリンクとスパンニングツリーが設定されています。

## 統合: 統合の2番目のステップ



統合の次の段階では、可用性を高めるために、5400zlシリーズのスイッチ、または8206zlスイッチを使用します。ディストリビューションレイヤーでは、リングアグリゲーションを行う場合の相互運用上の要件を考慮し、コアでは、ルーティングプロトコルとしてOSPFを使用して相互運用します。

## 統合: 統合の3番目のステップ



ディストリビューションレイヤーに5400zlシリーズを配置した後、コアに8212zlを導入します。

# スイッチ: ProVision ASICベースのスイッチ

## コア-ディストリビューション- アクセス-データセンター



HP ProCurve Switch 8212zl



HP ProCurve Switch  
5406zl-48G



HP ProCurve Switch  
8206zl



HP ProCurve Switch  
3500yl-24G-PWR



HP ProCurve Switch  
3500yl-48G-PWR



HP ProCurve Switch  
6200yl-24G-mGBIC



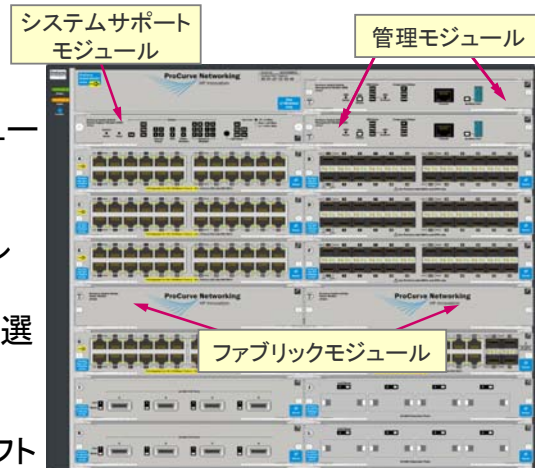
HP ProCurve Switch  
6600ml-24XG

これまでに簡単に説明したように、統合や相互運用はさまざまなレベルで行われ  
ます。ProCurveのProVision ASICベースのスイッチは、このようなシナリオで使われ  
る機会が多い製品です。ASICベースのスイッチは、さまざまな構成が可能です。こ  
の写真の例は、モジュールが実装された状態になっています。さまざまな製品の実  
際の構成については、[www.procurve.com](http://www.procurve.com)を参照してください。



## スイッチ: ProCurve Switch 8212zlハードウェアの概要

- 冗長管理モジュールスロット
- 耐障害性の高いスイッチファブリックモジュールスロット
- 最大12台の"zl"インターフェイスモジュール
- PoE要件に基づいて2つのタイプの電源を選択可能
- 8206zl、5400zl、3500yl、6200ylと同じソフトウェアイメージを使用



8212zl、8206zl、5406zl、5412zl モデルはすべて同じインターフェイスモジュールと電源を使用。

ProCurve Switch 8212zlは、シャーシ型のスイッチで、パフォーマンスや可用性が高く、コアからエッジというアダプティブな統合ネットワークソリューションを実現します。業界初のライフタイム保証付きコアスイッチです。その豊富な機能の例として、冗長管理モジュールスロット、428mppsのスループット、692Gbpsの帯域幅に対応する、耐障害性の高いスイッチファブリックモジュールスロットなどがあります。288Gbpsのポートワイヤースピードを備える最大12個の"zl"インターフェイスモジュール、および最大48個の10Gigabit Ethernetポートを搭載可能です。電源のタイプは2種類あり、PoEの要件に従って選択できます。8212zl は、8206zl、5400zl、3500yl、6200ylと同じソフトウェアイメージを使用しています。

詳細については、このコースの英語版Webトレーニングに含まれる『Technical Overview』を参照してください。

## スイッチ: 機能グループの違い

### Intelligent Edgeスイッチの機能

- IPv4 RIP、スタティックルート
- IGMP
- ACL
- QoS
- 帯域幅の制御
- エッジセキュリティ
- IPv6ホスト\*
- IPv6スタティックルート\*

### Premiumスイッチの機能

Intelligent Edgeの全機能に加え、以下に対応:

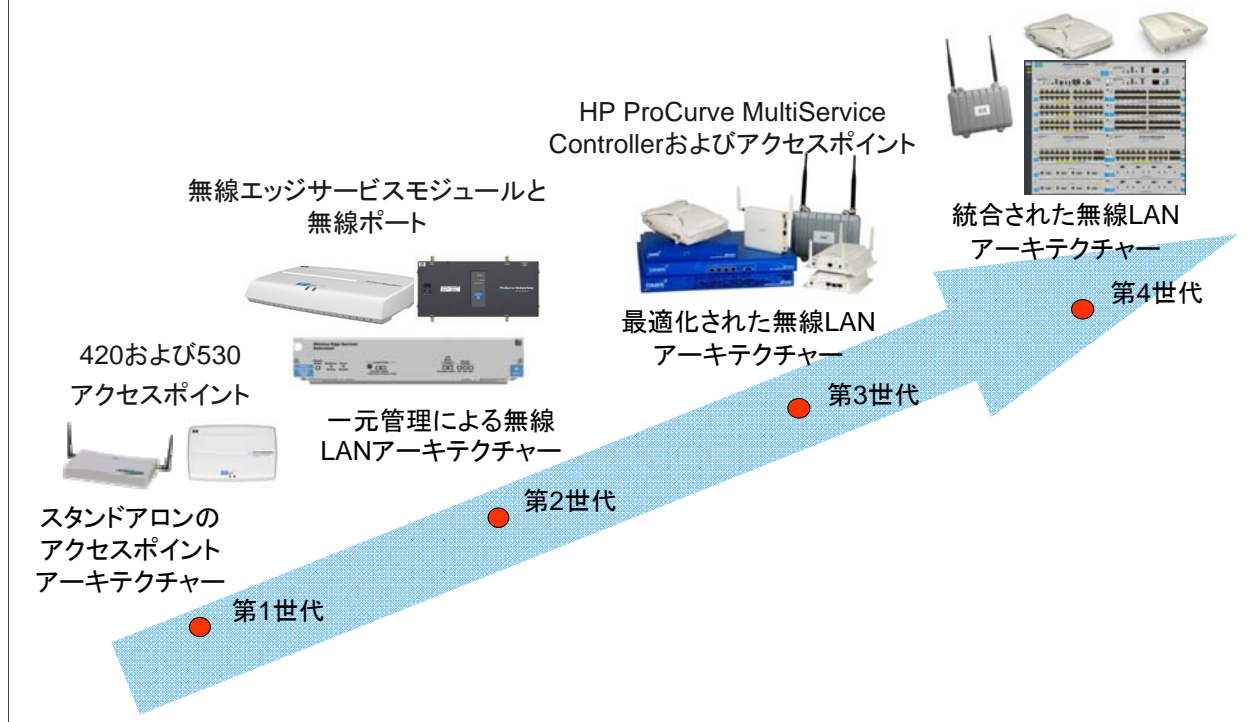
- IPv4 OSPF (ECMP)
- PIM SMおよびPIM DM
- IPv6 OSPF \*
- IPv6 RIP \*
- VRRP
- QinQ VLAN

6200ylシリーズにはライセンスが不要。すべてのプレミアム機能を搭載した状態で出荷

\* IPv6機能には将来的に対応予定

ここには、Intelligent Edgeスイッチの出荷時に搭載されているデフォルトソフトウェア、およびPremiumアップグレードオプションを示しています。これは、基本的な違いの一例です。詳細については、このコースの英語版Webトレーニングに含まれる『Technical Overview』を参照してください。

# HP ProCurveモビリティ製品:無線LANの発展



最近のLANでは、無線接続機能が重視されるようになってきました。ProCurveでは、さまざまな無線LANソリューションの選択肢を用意しています。このような話題はこのトレーニングコースの目的から少しはずれますが、ここで少し説明しておきます。

## HP ProCurveモビリティ製品:無線LANの発展

420および530  
アクセスポイント



スタンドアロンの  
アクセスポイント  
アーキテクチャ

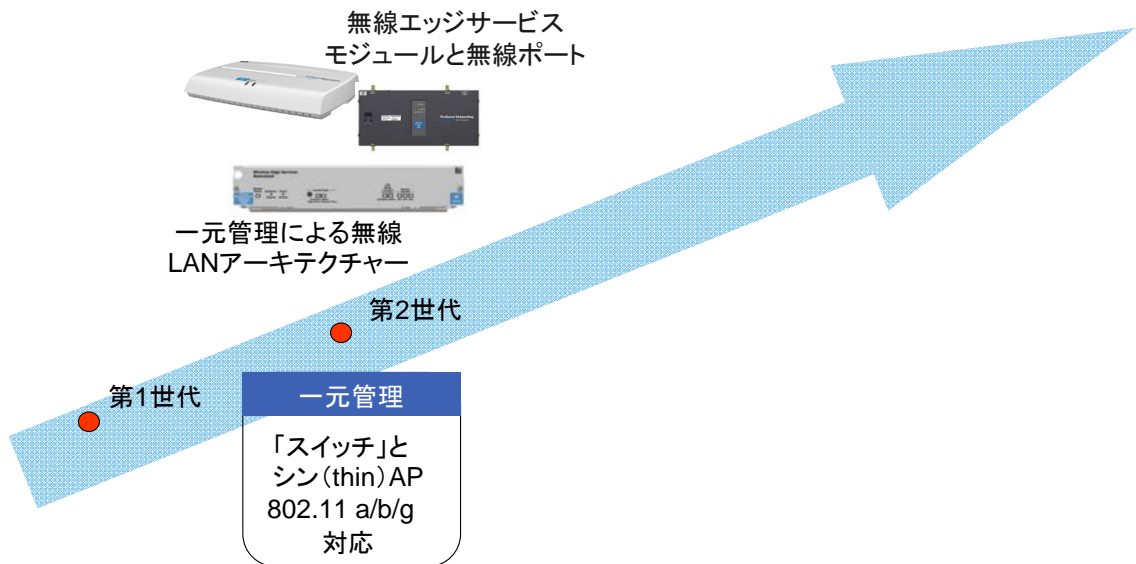
第1世代

オープンスタンダー  
ドに基づく接続性

インテリジェントAP

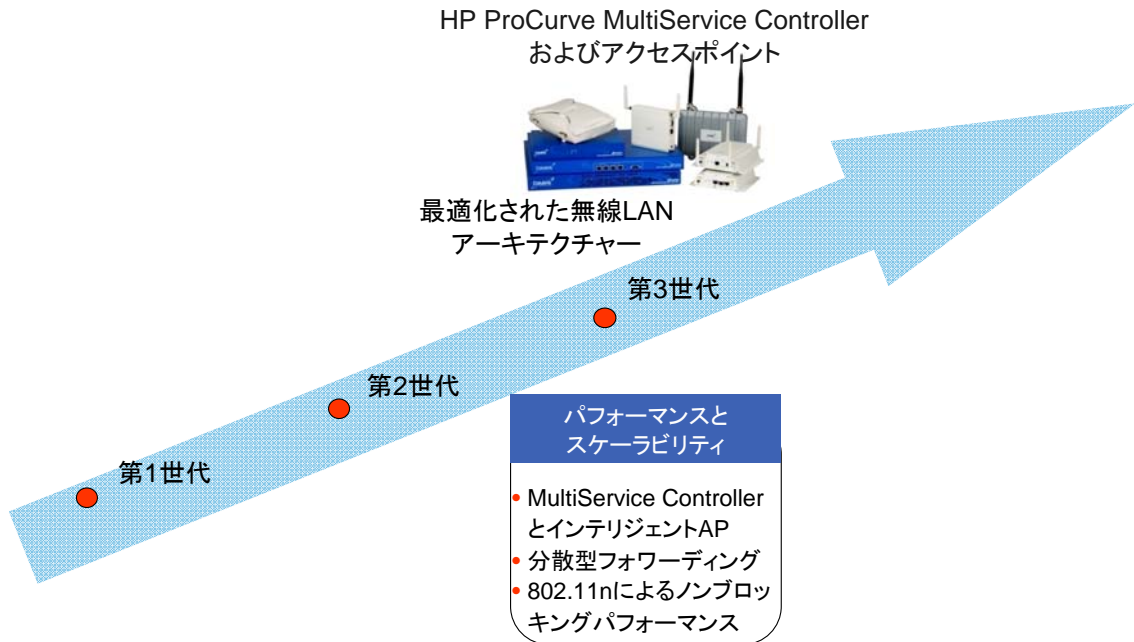
無線アーキテクチャにおける第1世代のアクセスポイントは、インテリジェントまたはファット (fat) アクセスポイントと呼ばれていました。多くの無線LAN製品は、はじめはこのレベルでした。

## HP ProCurveモビリティ製品: 無線LANの発展



第2世代は、IT部門が顧客要件に応じてネットワークに100台以上のAPを配置する必要を満たします。この時期のソリューションでは、一元管理を行っていましたが、このソリューションにはまだ問題がありました。第3世代は、最適化された無線LANアーキテクチャーと呼ばれます。従来型のネットワークと同じように、すべてを一元管理しますが、エッジにインテリジェンスを持たせることで、すべてのデータを中央のポイントに戻して処理する必要がなくなりました。

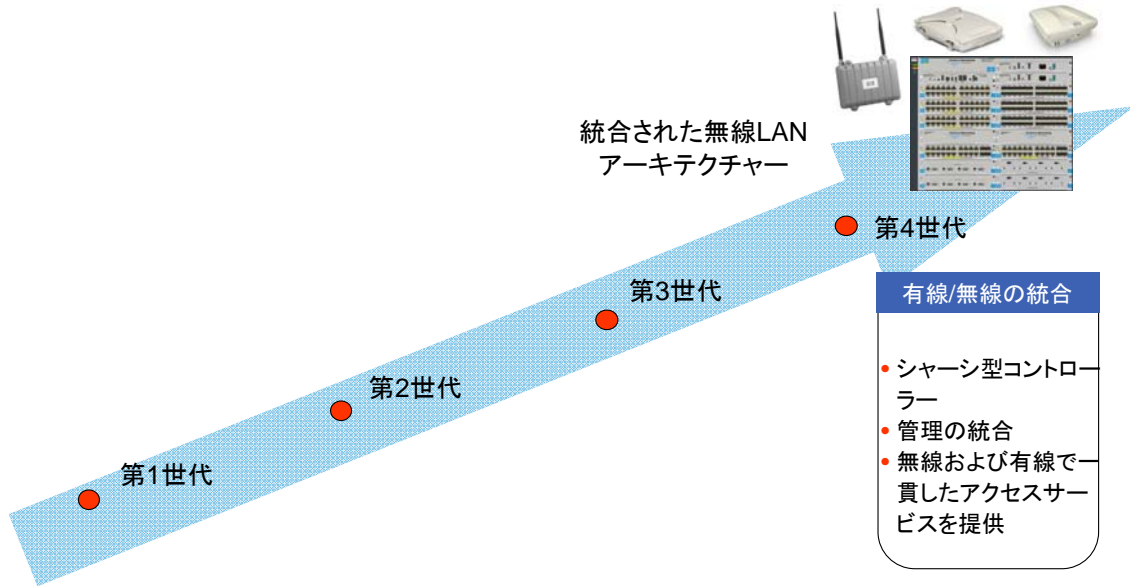
## HP ProCurveモビリティ製品:無線LANの発展



第3世代のモデルでは、エッジでトラフィックを処理するインテリジェントAPが登場しました。無線LANの発展を振り返ると、第3世代に対応するには、ほぼすべての無線ベンダーがそのネットワークを再デザインする必要がありました。

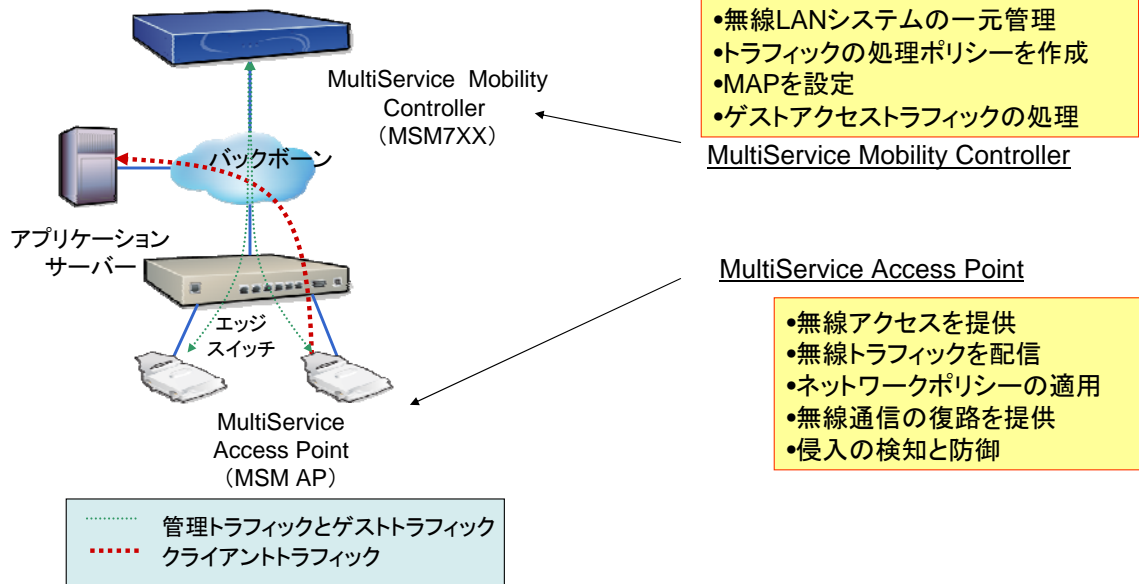
この第3世代では、有線ネットワークは、スイッチングネットワークとは完全に別のオーバーレイとして管理されます。

## HP ProCurveモビリティ製品:無線LANの発展



ProCurveは、統合された無線LANアーキテクチャーを目指しています。IT部門では認証情報を用いて、有線と無線を統合することができます。このようにすると、Ethernetポートへの接続と同様に、無線アクセスでも認証を受けることができます。

# HP ProCurveモビリティ製品: 分散インテリジェンス – 最適なアーキテクチャ



ここで分散インテリジェンスについて少し説明します。この図は、すべてのフローが中央のMultiServiceモビリティコントローラーに戻る構成を示しています。モビリティコントローラーは、無線LANでトラフィックを処理する方法を制御しますが、必ずしもトラフィックの宛先は制御しません。そのため、APを直接設定・管理してネットワークにアクセスすることも可能です。AP (MultiServiceアクセスポイントまたはインテリジェントAP) は、トラフィックの送信先の詳細な制御やネットワークポリシーの適用を行うことができます。この場合、すべてのフローをコントローラーに直接戻すことなく、クライアントトラフィックが必要な宛先に送信されます。



# HP ProCurveモビリティ製品: マルチサービスモビリティソリューション

## エッジデバイス – 無線アクセスポイント

無線接続を提供

- シングル/デュアル/トライ (tri) 無線ユニットモデル
- 屋内、屋外に対応するユニット
- 無線クライアントブリッジ

## コアデバイス – 無線LANのセントラルコントローラー

無線管理と制御に対応

- スタンドアロン型、およびシャーシ型ブレードモジュール

## セキュリティ – 侵入検知/侵入防止

無線セキュリティIDS/IPS

- セキュリティ機器およびRFセンサー

## ソフトウェアとツール

Guest Managementソフトウェア

- 管理用のソフトウェア – PCM / PCM+



ProCurveのモビリティソリューションはさまざまな要素で構成されます。これらの要素は主に4つの領域に分類できます。1つめは、エッジデバイスのアクセスポイントです。2つめは、コントローラーとその機能です。3つめは、セキュリティ、IDS、IPSの技術です。4つめは、すべての設定を行うソフトウェアと管理ツールです。

## HP ProCurveモビリティ製品:セントラルコントローラーの ラインナップ



|                        | MSM710   |   | MSM760   |   | MSM765zl  |
|------------------------|--|---|--|---|---|
| サービスパック                | アクセス<br>(基本)   | モビリティ   | アクセス<br>(基本)   | モビリティ   | モビリティ   |
| サービス                   | <ul style="list-style-type: none"> <li>無線LANの管理と制御</li> <li>Guestアクセス</li> </ul> | <ul style="list-style-type: none"> <li>無線LANの管理と制御</li> <li>Guestアクセス</li> <li>ローミング</li> </ul> | <ul style="list-style-type: none"> <li>無線LANの管理と制御</li> <li>Guestアクセス</li> </ul> | <ul style="list-style-type: none"> <li>無線LANの管理と制御</li> <li>Guestアクセス</li> <li>ローミング</li> </ul> | <ul style="list-style-type: none"> <li>無線LANの管理と制御</li> <li>Guestアクセス</li> <li>ローミング</li> </ul> |
| スケーラビリティ               | 802.11 a/b/g: 10<br>802.11n: 10  |   | 802.11 a/b/g: 40 - 200<br>802.11n: 40 - 200                                      |   | 802.11 a/b/g: 40 - 200<br>802.11n: 40 - 200   |
| 同時接続ユーザー数              | 無制限  |   | 無制限  |   | 無制限   |
| 同時接続guest<br>アクセスユーザー数 | 100  |   | 2000   |   | 2000  |

MultiService Mobilityコントローラーには、単体バージョンとモジュール式バージョンがあります。MSM 700シリーズは、2つの異なる設定で提供されます。MSM710は、802.11nまたはa/b/g対応の、最大10個のAPをサポートします。8200または5400シャーシに装着するMSM 765zl、および単体型のMSM 760は、初期状態では40個のAPライセンスを備えており、40ライセンスずつ、最大200ライセンスまで追加できます。さらに、765zlモジュールでは、1つのシャーシに4個のモジュールを格納できるため、8200zlまたは5400zlプラットフォームで合計800個のAPに対応できます。

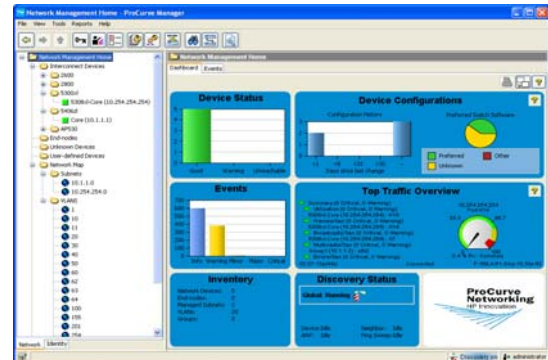
## HP ProCurve管理製品:Windowsベースの ネットワーク管理ソリューション

**一元管理機能**を備えており、  
ネットワークデバイスの設定と  
モニタリングを一箇所から行うことが  
可能

ネットワークを効果的に管理する  
ツール

- デバイスの自動検出とポーリング
- ネットワークとVLANのマッピング
- デバイスの設定と管理を行うツール
- ネットワークトラフィックのモニタリング
- アラートとトラブルシューティング情報

**2つのバージョン:** ProCurve Manager (PCM) および ProCurve Manager Plus (PCM+)



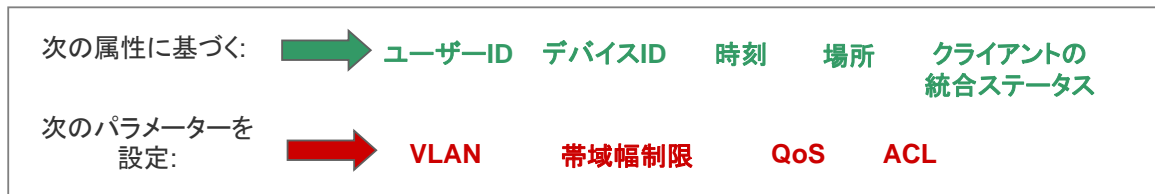
PCMおよびPCM+は、Windowsベースのネットワークソリューションで、Adaptive EDGEネットワークの管理に必要なツールを提供します。PCMおよびPCM+は、一元管理機能を備えており、ネットワークデバイスを一箇所からモニタリングおよび設定することができます。

PCMは、管理可能なすべてのProCurveデバイスに同梱されており、基本的な管理機能を提供します。たとえば、機器やトポロジの自動検出、マッピングやポーリング、デバイスの設定や管理、アラート機能などを備えています。PCM+は、さらに高度なバージョンのアプリケーションで、ライセンスを購入することにより使用できます。たとえば、設定管理、VLAN管理、トラフィックの詳細なモニタリング、グループとポリシーの管理、ソフトウェアの自動アップデートなどの機能があります。

PCMおよびPCM+は、CLIやWebインターフェイスなど、スイッチやデバイスの設定を行うツールの代替とはなりません。PCMやPCM+は、スイッチにリモートでアクセスして、CLIやWebエージェントを起動して個々のスイッチに変更を加える場合に使用できます。

## HP ProCurve管理製品:Identity Driven Managerの概要

- セキュリティ、アクセス、パフォーマンス設定をダイナミックに適用
- ユーザーポリシーグループを簡単に作成して管理し、ネットワークパフォーマンスを最適化したり、ユーザーの生産性や全体的な効率を向上させる
- 管理ポリシーは、ネットワークパラメーターを設定して、必要とするネットワーク機能を提供



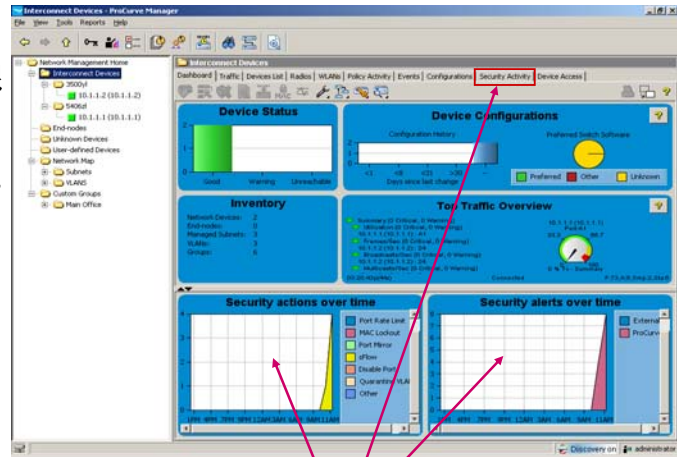
Integrity Driven Manager (IDM) はPCM+に適用するオプションのプラグインです。IDMは、ユーザーID、デバイスID、時刻、場所、クライアントの統合ステータスなど、指定した基準に基づいて、セキュリティ、アクセス、パフォーマンスに関する設定をダイナミックに適用します。また、管理者が設定したアクセスプロファイルに基づいて、ネットワークへの適切なアクセス権を許可します。

IDMは、ProCurveデバイスがその時点でエッジに適用している主要なポリシー定義を有効にします。新しいネットワークリソースを追加することなく、既存のスイッチプラットフォームに搭載することによりネットワークの機能性を高めます。また、RADIUSに準拠しています。

ACLは、ルールを構成する5つの基準のいずれかまたはすべてに基づいて、ユーザーが接続するスイッチにダイナミックに書き込まれます。ACLは、プロトコル、宛先IPアドレス、または宛先TCP/UDPポートへのアクセスを許可または拒否する、ポートまたはアクセスポイントにおいてユーザーに適用されるフィルターです。IPアドレスまたはTCP/UDPアドレスは、個別に指定することも、値の範囲として指定することもできます。

## HP ProCurve管理製品: Network Immunity Manager の概要

- ポートごとの侵入検知、および有線/無線ネットワーク両方のエッジで悪意あるネットワークトラフィックを食い止めることを可能にする、安価で、拡張性のある、使いやすい管理ソリューション
- ポリシーの定義、セキュリティイベントの収集、脅威のモニタリングと緩和の自動化が可能
- 主な機能:
  - 脅威の検出
  - 脅威の緩和
  - 脅威の管理



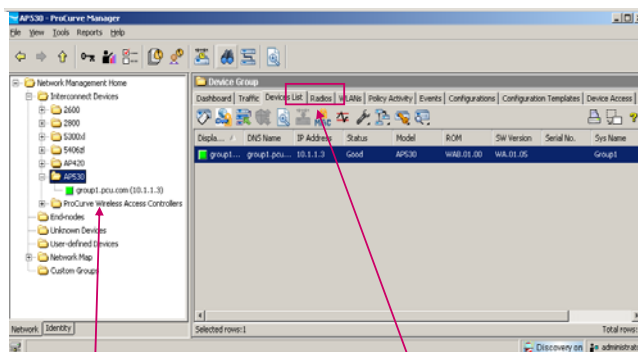
Network Immunity Managerプラグインは、セキュリティ管理と設定を行うためのタブを追加

ProCurve Network Immunity Managerは、PCM+に適用するオプションのプラグインで、ウイルスによる攻撃などネットワーク上の脅威を自動的に検出して処理します。このセキュリティ管理ツールは、ネットワーク上のデバイスをモニタリングして、ネットワーク内部の攻撃を検出し、管理者が検出と対応方法に関するセキュリティポリシーを設定できるようにします。

このツールは、ProVision ASICを搭載したProCurveスイッチに内蔵されているセキュリティ機能とトラフィックモニタリング機能(sFlow、Virus Throttle、リモートミラーリング技術など)を利用し、Network Behavior Anomaly Detection (NBAD)を実行して攻撃を検出します。

## HP ProCurve管理製品: Mobility Managerの概要

- 管理者はアクセスポイントを一元管理可能
  - 機器の設定
  - ソフトウェアのアップデート
  - 無線LANセキュリティの設定
  - 無線ユニットの設定
- 無線ネットワーク管理ツールを提供
  - 不正デバイスの検出
  - モニタリング
  - トラブルシューティング



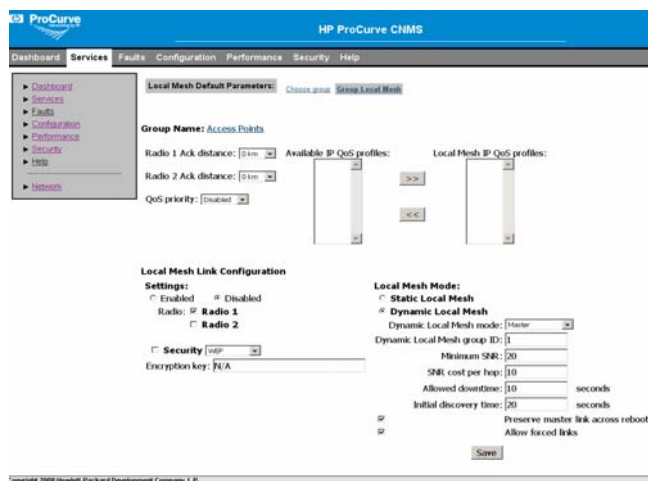
**[Interconnect Devices]**  
フォルダーの下に、APと無線用のサブフォルダーを含むデバイスグループ**ProCurve Wireless Access Controllers**がある

Mobility Managerのプラグインは、APの管理と設定を行うためのタブを追加

ProCurve Mobility ManagerはPCM+に適用するオプションのプラグインです。Mobility ManagerはPCM+のモニタリング機能を拡張して、ProCurve無線アクセスポイント(AP)で使用する設定ツールを追加します。Mobility Managerは、管理対象のProCurve APにあるすべての無線ユニットのモニタリング、信頼された無線ユニットの定義、管理対象APの無線ユニット用の無線LANとSSIDのモニタリングと設定を行う場合に使用できます。

## HP ProCurve管理製品:包括的なGUIベースの 無線LAN管理ツール

- リアルタイムのモニタリング、アラート送信、トラブルシューティング
- レポート作成およびキャパシティ計画用のトレンド分析



HP ProCurve CNMSは、ProCurve MSM製品のすべての設定、パフォーマンスモニタリング、障害管理、トラブルシューティングの機能を一元的に実行できるようにします。

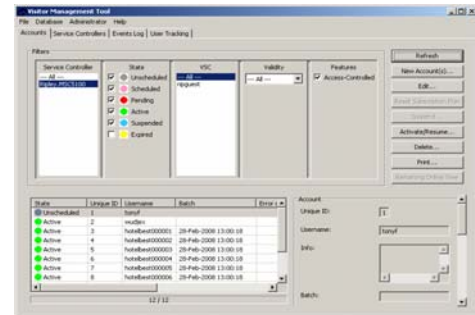
CNMSは、簡単に導入して運用コストを削減できるように設計されています。組み込み型のデータベースを備えており、小規模な無線LANから何万ものクライアントデバイスがある大規模ネットワークにまで簡単に対応できます。

CNMSは、標準のインターネットプロトコルを使用してデバイスと通信するので、ローカルキャンパスネットワークから、何百もの場所にまたがる地理的に分散した大規模ネットワークまで管理可能です。

## HP ProCurve管理製品: ProCurve Guest Management ソフトウェア

### メリット:

- 許可を受けた従業員がguestユーザーアカウントを作成できるようにする
- 技術者以外のスタッフが操作できる設計
- 有効期限が切れると、一時的な認証情報が自己消滅
- 印刷可能なバウチャーを作成する場合に使用可能



HP ProCurve Guest Managementソフトウェアは、受付や管理担当のスタッフが使用することを考慮した直感的なユーザーインターフェイスを備えており、シンプルなウィザードを使用してビジターアカウントを安全に作成したり、ゲストのアクセスバウチャーを作成できるようにします。

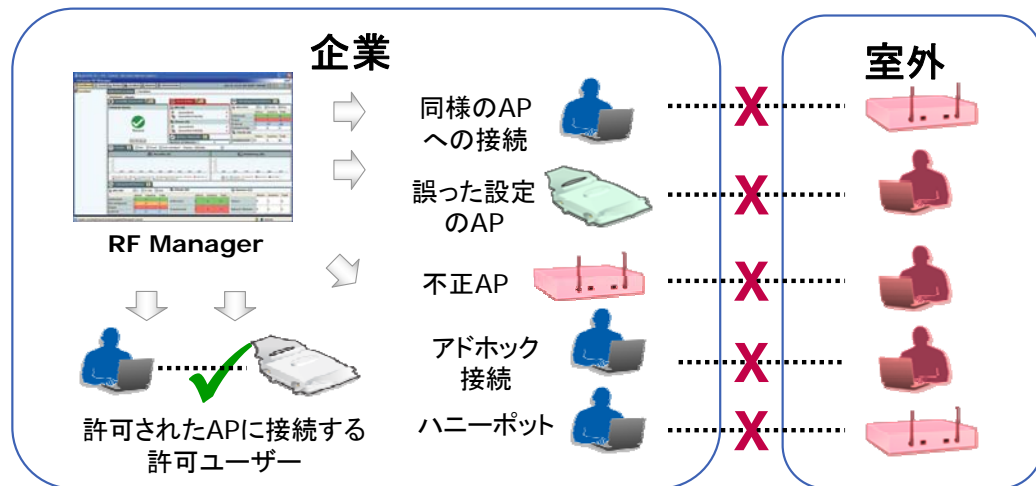
アカウントを作成するには、担当者のワークステーションにProCurve Guest Managementをインストールしてオペレーターアカウントを付与する必要があります。

。



# HP ProCurve管理製品

## RF Managerは、セキュリティ機能を拡張したIDS/IPS



不正アクセスポイント、未許可の接続、ハッカーの攻撃など、未許可のアクセスからネットワークを保護

HP ProCurve RF Managerは、管理対象ネットワークの侵入検知/防止 (IDS/IPS) を実行します。正当なユーザーの通信パフォーマンスを妨げたり低下させることなく、すべての未許可のトラフィックを直ちに自動的にブロックします。RF Managerは、他の問題のスキャンを継続しながら、複数の脅威を同時に防止します。これには、不正AP、設定の誤ったAP、未許可のクライアントによる接続、クライアントの接続間違い、アドホック接続、ハニーポット/Evil Twin攻撃、MACスプーフィングなど、さまざまなタイプの脅威が含まれます。

## HP ProCurve管理製品: HP ProCurve RP Planner



### Windowsプラットフォーム対応の 無線LANプランニングソフトウェア

- 物理的な特徴、建材、機器の特性などを計算に含めた無線LANカバレッジモデル
- 無線LANプランニングにかかる時間と手間を軽減
- APやセンサーのオーバープロビジョニングを削減
- 電波漏洩による脆弱性を評価

ProCurve RF Plannerは、無線LANの設計を簡素化して設計にかかる時間を削減します。物理的な特徴、建材、無線LAN機器の特性などの変数を計算に含めることにより、ネットワーク設計者が正確に無線LANカバレッジを把握できるようにします。RF Plannerは、セキュリティリスクを評価し、機器のリストを生成するので、導入の際に役立ちます。

## 製品ラインのまとめ: HP ProCurve製品

HP ProCurve製品の詳細については、[procurve.com](http://procurve.com)を参照するか、このコースの英語版Webトレーニングに含まれる参考資料を参照してください。

ProCurveは、高い信頼性、実証済みのパフォーマンス、包括的な機能を備える製品で、複雑さを軽減し、IT投資効果を最大化します。

ProCurveスイッチは、受賞歴のあるProVisionテクノロジーによりコアからエッジへの統合ソリューションを可能にし、ネットワークの運用、管理、サポートを効率化します。詳細については、[procurve.com](http://procurve.com)またはこのコースの英語版Webトレーニングに含まれる参考資料を参照してください。



## 確認テスト

## 確認テスト1

3500ylシリーズが使用される場合が多いのは、中規模ビジネスのどのレイヤーですか。

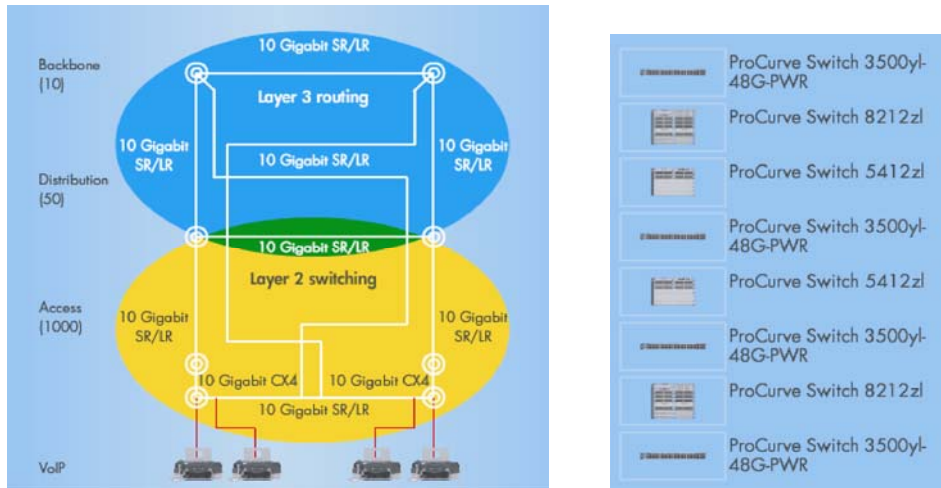
- A. コア
- B. ディストリビューション
- C. トランク
- D. アクセス

## 確認テスト1の解答

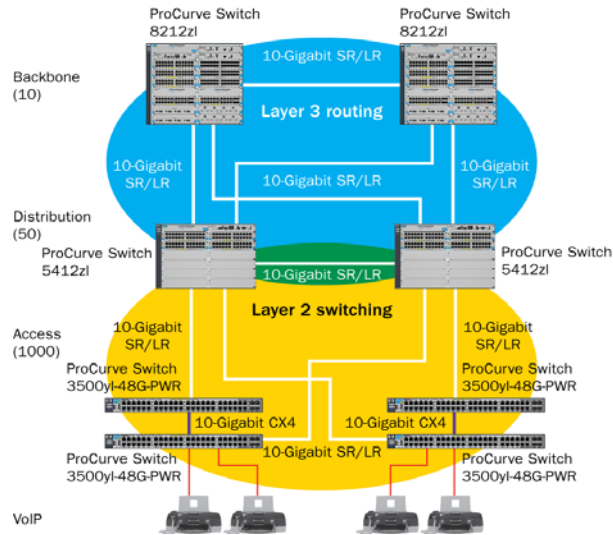
正解: D

## 確認テスト2

右側にあるスイッチを図の正しい位置に配置して、ProCurveのみで構成される適切なネットワークにしてください。



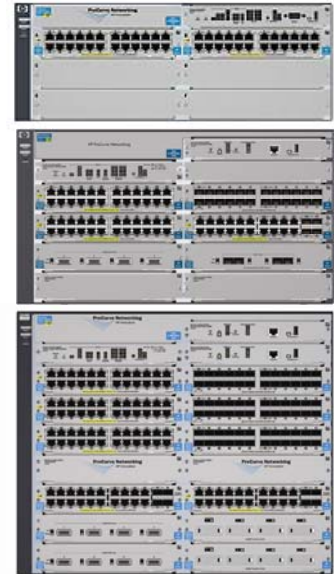
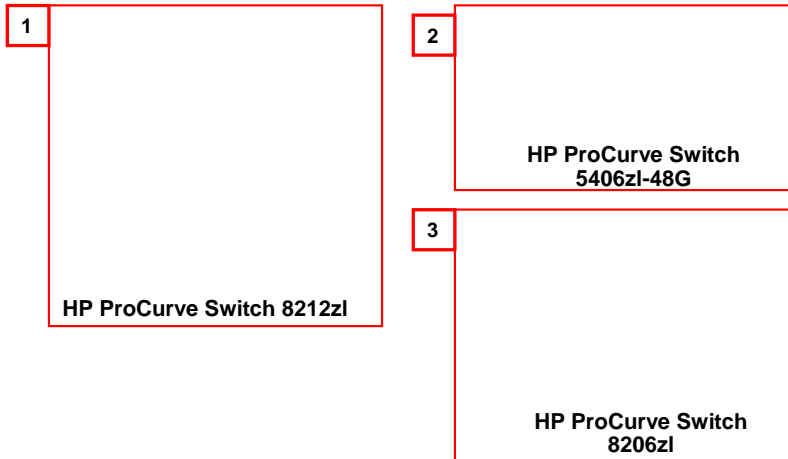
# 確認テスト2の解答





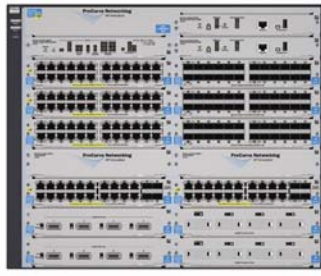
# 確認テスト3

右側のスイッチを左側の正しい位置に配置してください。



## 確認テスト3の解答

1



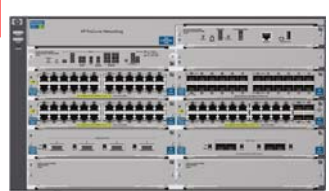
HP ProCurve Switch 8212zl

2



HP ProCurve Switch  
5406zl-48G

3



HP ProCurve Switch  
8206zl

モジュール3終了



## モジュール4: Cisco製品との比較



## モジュールの目的

このモジュールを修了すると、以下のことができるようになります。

- ProCurveとCiscoの用語と使用方法に関する一般的な違いを理解する

このモジュールでは、HP ProCurveとCiscoの用語と使用方法に関する一般的な違いについて説明します。このモジュールは、何度も復習して、両者の違いに関する最も一般的なポイントを確認してください。

## ポート識別子:違いの比較

| スイッチポートの役割                   | ProCurveでの呼び方                                    | Ciscoでの呼び方   |
|------------------------------|--|--|
| 複数のVLANのトラフィックを伝送するスイッチ間のリンク | 複数のVLANに対応するタグ付ポート                               | トランクポート  |
| リンクの統合に使用                    | トランクポート  | ポートチャネルインターフェイス  |
| 複数のVLANに対応するサーバー用に使用         | 複数のVLANに対応するタグ付ポート                               | トランクポート  |
| エンドユーザー用に使用<br>(PC、プリンターなど)  | 1つのVLAN用のタグ無ポート                                  | アクセスポート、VLAN   |
| IP電話機用に使用                    | 音声VLANを伝送するタグ付またはタグ無ポート                          | 補助(音声) VLAN  |
| エンドユーザーとIP電話機用に使用            | エンドユーザー用の1つのVLANに対応するタグ無ポート<br>IP電話機用のタグ付 音声VLAN | 補助(音声) VLANに対応するアクセスポート<br>Multi-VLAN Access Port (MVAP) |

ProCurveとCiscoでは、ポートやVLANの設定機能に関して異なる用語を使用しています。たとえば、Ciscoデバイスのエンドユーザーポートはアクセスポートと呼ばれていますが、ProCurveデバイスでは同様のポートを「タグ無」ポートと呼んでいます。つまりこれは、エンドノードが送信する、802.1Qヘッダーのない標準のEthernetフレームの packets のことを指します。この表には、ProCurveとCiscoで使用する用語のうち重要なものをまとめています。

# ポート識別子: スタックブルスイッチ

## Cisco

```
Switch(config)# interface GigabitEthernet0/1
```

ポート識別子では、相対的なポート番号のほかに、インターフェイスタイプのラベルとスロット番号プレフィックス(0または1)を指定。

例: FastEthernet0/1、GigabitEthernet1/ 1、2

Catalyst 4900



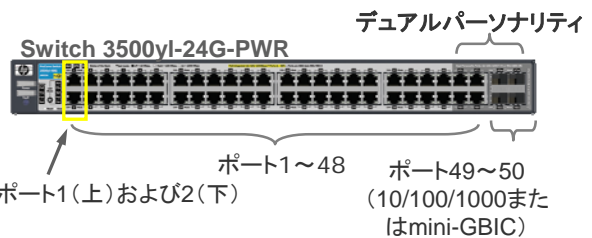
ポート1(上)および2(下)

## ProCurve

```
Switch(config)# interface 1
```

ポート識別子は、相対ポート番号のみを使用して指定。

例: 1、2など



ここでは、現行のほとんどのCiscoスイッチとProCurveスイッチでのポートの指定方法の概要を示します。ProCurveのスタックブルスイッチでは、ポート識別子は単に、1、2、3などの相対ポート番号を使用して表します。CiscoとProCurveそれぞれのCLIでの指定方法の違いを確認してください。

# ポート識別子:モジュール式スイッチ

## Cisco

モジュールは、1、2...のようにラベル付けされる

```
Switch(config)# interface GigabitEthernet2/1
```

ポートはスロット番号プレフィックスと共に番号で指定  
例: GigabitEthernet2/1

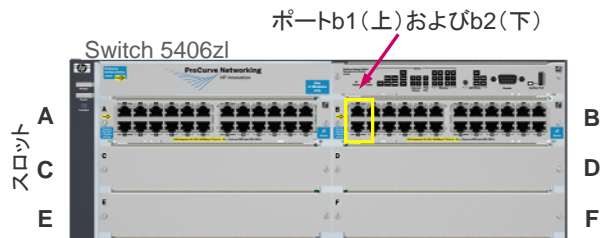


## ProCurve

モジュールは、a、b...のようにラベル付けされる

```
Switch(config)# interface a1
```

ポートはモジュールに対応する文字と共に番号で指定  
例: a1、a4、b1、b24...



Ciscoのモジュール式スイッチでは、ポート識別子はスタックابلスイッチの場合と同じ4つの要素から構成されます。唯一異なるのは、各モジュールに、対応するスロット番号がある点です。ProCurveのモジュール式スイッチでは、ポート識別子は、モジュールまたはスロットを示す、a、b、cのようなアルファベット文字のラベルで構成されます。CLIを使用する場合は、このアルファベットのラベルに、そのモジュールでの相対ポート番号を付けて、a1、a2、a3のように指定します。



## 一般的なサービス: サービスの概要

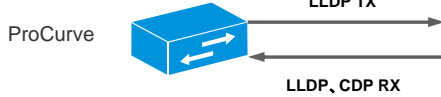
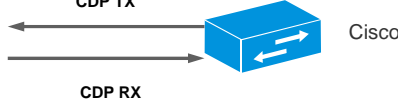


- ProCurveとCiscoのデバイスでは、起動時のサービスの有効化方法が異なる

–ProCurveデバイスでは、TelnetとHTMLサービスがデフォルトで有効

- ProCurveスイッチではデフォルトでポートが「有効(enabled)」
- インターフェイスで"no shut"を実行する必要なし

ProCurveのデバイスとCiscoのデバイスでは、起動時にサービスを有効化する方法が異なります。TelnetやHTMLなどのサービスは、ProCurveデバイスではデフォルトで有効になっており、デバイスまたはVLANにIPアドレスを設定すれば動作状態になります。ProCurveスイッチでは、デフォルトでポートが「有効(enabled)」になっています。また、インターフェイスで"no shut"を実行する必要がありません。ProCurveのEthernetスイッチでは、デフォルトでインターフェイスが「有効(enabled)」になっています。

## ProCurveスイッチがサポートする機能: CDPおよびIEEE 802.1AB LLDP

| ProCurve  | Cisco  |
|---|--|
| <p>デフォルトでは、受信モード (receive mode) のすべてのポートでCDPが有効。CDPパケットの発信には対応していない。<br/>デフォルトでは、すべてのポートでLLDPが有効。</p>                                   | <p>デフォルトでは、すべてのポートでCDPが有効。SNMPサポートなしで12.2(37)SEを実行しているCisco Catalystスイッチシリーズ2950、3760、3750、および12.2(33)SXHを実行しているCisco Catalyst 6500は、LLDPに対応</p> |
|  <p>ProCurve</p>                                       |  <p>Cisco</p>  |
|  <p>エントリーを相互に交換することにより、LLDPとCDP MIBでCiscoスイッチを認識可能</p> |  <p>ProCurveスイッチを認識できない</p>                                   |

最も広くサポートされているネットワーク検出プロトコルに、Link Layer Discovery Protocol (LLDP) と Cisco Discovery Protocol (CDP) があります。Ciscoが開発したCDPは、独自プロトコルで、多くのネットワーク機器ベンダーがこのプロトコルを実装しています。ProCurveデバイスはCDPパケットを発信しませんが、CiscoデバイスなどProCurve以外のデバイスが送信したCDPパケットを読み取ります。

## VLANの設定:スイッチ間の接続

| ProCurve  | Cisco   |
|---|---|
| <pre>vlan 1   untagged a1 vlan 11   tagged a1 vlan 12   tagged a1 vlan 13   tagged a1</pre> | <pre>interface GigabitEthernet 1/20   switchport   switchport trunk encapsulation dot1q   switchport trunk native vlan 1   switchport trunk allowed vlan 11-13   switchport mode trunk   switchport nonegotiate</pre> |

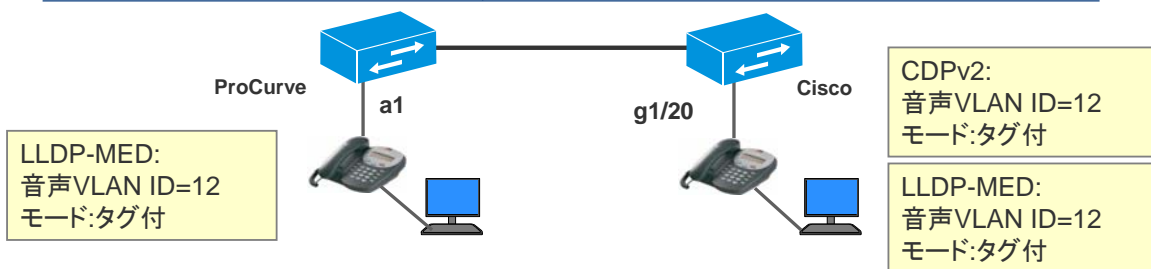


ProCurveデバイスでリンクが複数のVLANを伝送するように設定するには、ポートをその特定のVLANのコンテキスト内で「タグ付」に設定します。

この例では、ポートa1は、VLAN 11、12、13でタグ付けされています。VLAN 1では、ポートをタグ無に指定する必要はありません。これは、すべてのスイッチポートの初期設定でポートがタグ無に設定されているためです。この例では、ProCurveスイッチのポートa1は、タグ付ユーザーVLANのトラフィックと同じ物理リンクでタグ無VLAN 1トラフィックを許可します。Ciscoの設定との比較を図に示しています。

## VLANの設定: スイッチとコンピューターの間にIP電話機を接続

| ProCurve   | Cisco  |
|--|--|
| <pre>vlan 11 untagged a1 vlan 12 voice tagged a1</pre> | <pre>interface GigabitEthernet 1/20 switchport switchport access vlan 11 switchport mode access switchport voice vlan 12</pre> |



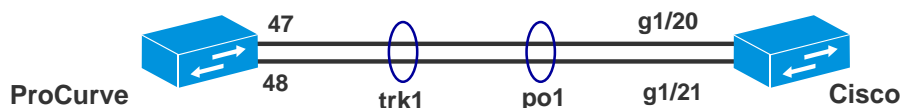
この例では、コンピューターとIP電話機がスイッチポートを共有しています。IP電話機はスイッチポートに接続され、コンピューターはIP電話機に接続されています。

IP電話機は802.1Qをサポートしている場合が多いので、ProCurveスイッチでは、通常、コマンドvlan 11 untagged a1を使用して、ポートをVLAN 11用のタグ無ポートに、また、コマンドvlan 12 tagged a1を使用してVLAN 12用のタグ付に設定します。

VLAN 12については、voiceコマンドを使用して音声VLANも設定します。このコマンドを実行すると、電話機が音声フレームのプライオリティをまだマーキングしていない場合に、VLAN 12のトラフィックのプライオリティを自動的に高くします。

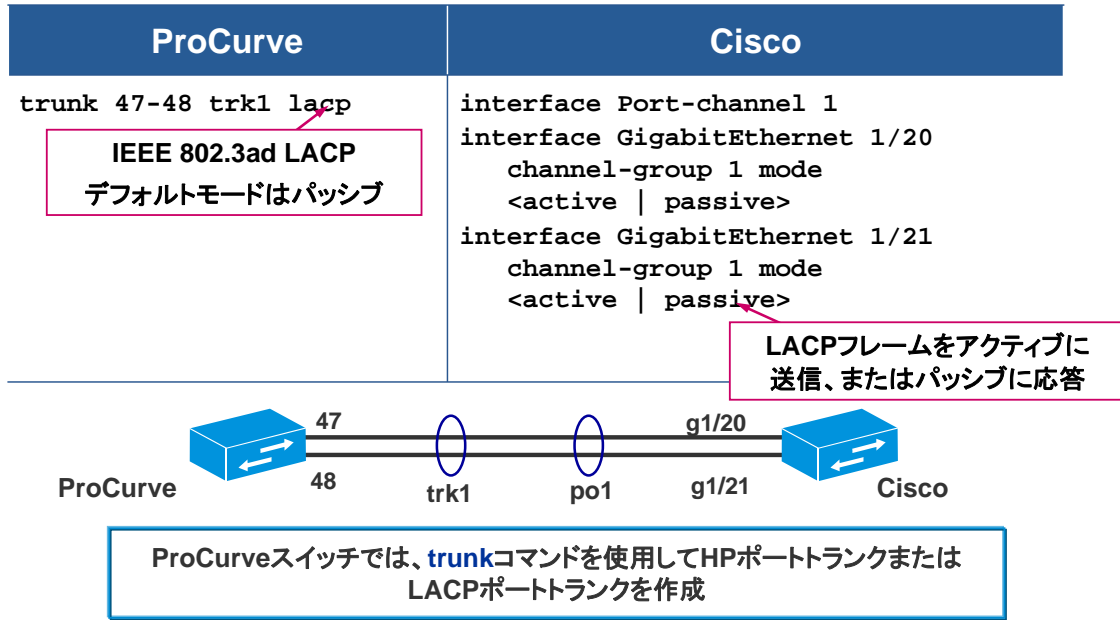
## 設定シナリオ: スタティックな(リンク)集約

| ProCurve   | Cisco  |
|--|--|
| <pre>trunk 47-48 trk1 trunk</pre> <p>このパラメーターは、リンクアグリゲーションの「タイプ」を定義。<br/>“trunk”パラメーターは、HPのポートランキングを示す</p> | <pre>interface Port-channel 1 ← 自動的に作成 interface GigabitEthernet 1/20 channel-group 1 mode on interface GigabitEthernet 1/21 channel-group 1 mode on</pre> |



この図は、ProCurveスイッチとCiscoスイッチの間にスタティックトランクを設定する際に使用できるCLIコマンドを示しています。ProCurveとCiscoの用語の違いを思い出してください。Ciscoの環境では、“trunk”とは、ISLまたは802.1Qタグ付の複数のVLANのフレームを伝送するスイッチ間リンクを意味します。ProCurveでの“trunk”リンクは、HPのポートランクプロトコルまたはLACPのいずれかでリンクアグリゲーションを行うことを意味します。

## 設定シナリオ: LACPを使用したダイナミックな(リンク)集約



ここには、ProCurveスイッチとCiscoスイッチ間のトランクにLACPを設定する方法を示しています。ProCurve側では、trunkコマンドで“trunk”ではなく“lacp”を指定しています。このパラメーターは、トランクの構成にLACPプロトコルを使用することを指定するものです。トランクの他方の側がLACPに対応している場合は、トランクが自動的に構成されます。Cisco側では、“mode”パラメーターを使用して、トランクの各物理インターフェイスをパッシブモードまたはアクティブモードに指定します。アクティブモードの場合は、LACP BPDUがアクティブに送信されますが、パッシブモードでは、最初の受信への応答としてのみLACP BPDUが送信されます。

## 設定シナリオ: OSPF設定の比較

| ProCurve  | Cisco  |
|---|--|
| <pre> router ospf   area backbone interface loopback 1   ip address 10.1.100.1   ip ospf 10.1.100.1 area backbone vlan 1   ip address 10.1.1.1 255.255.255.0   ip ospf 10.1.1.1 area backbone   ip ospf cost 10 vlan 11   ip address 10.1.11.1 255.255.255.0   ip ospf 10.1.11.1 passive   ip ospf 10.1.11.1 area backbone   ip ospf cost 10                     </pre> | <pre> router ospf 1   passive-interface vlan21   network 10.1.1.2 0.0.0.0 area 0   network 10.1.21.2 0.0.0.0 area 0   network 10.1.100.2 0.0.0.0 area 0 interface loopback1   ip address 10.1.100.2 255.255.255.255   ip ospf cost 10 interface vlan1   ip address 10.1.1.2 255.255.255.0   ip ospf cost 10 interface vlan21   ip address 10.2.21.2 255.255.255.0   ip ospf cost 10                     </pre> |

ProCurveでは、グローバルコンフィギュレーションレベルで実行する“router”コマンドでインスタンス番号を指定しません。ProCurveのルーターでは、ospfと指定します。

Ciscoのルーターでは、ospf 1と指定します。

ProCurveデバイスの場合、OSPFに参加しているネットワークは、“VLAN” コンテキスト内に設定されます。

一方Ciscoでは、ルーターコンフィギュレーションレベルで“network” コマンドを使用します。

ProCurveの“vlan 11 IP address” と、Ciscoの“router ospf”、“network IP address”との違いに注目してください。



# 確認テスト



## 確認テスト1

右側にある項目を、中央の列の「ProCurveでの呼び方」に対応させてください。

| スイッチポートの役割                   | ProCurveでの呼び方 | Ciscoでの呼び方   | 対応させる項目                         |
|------------------------------|---------------|--|---------------------------------|
| 複数のVLANのトラフィックを伝送するスイッチ間のリンク |               | トランクポート  | 音声VLANを伝送するタグ付またはタグ無ポート         |
| リンクの統合に使用                    |               | ポートチャネルインターフェイス  | 1つのVLAN用のタグ無ポート                 |
| 複数のVLANに対応するサーバー用に使用         |               | トランクポート  | 複数のVLANに対応するタグ付ポート              |
| エンドユーザー用に使用（PC、プリンターなど）      |               | アクセスポート、VLAN   | 複数のVLANに対応するタグ付ポート              |
| IP電話機用に使用                    |               | 補助（音声）VLAN   | トランクポート                         |
| エンドユーザーとIP電話機用に使用            |               | 補助（音声）VLAN対応アクセスポート（voice）Multi-VLAN Access Port（MVAP） | エンドユーザー用のタグ付IP音声VLANに対応するタグ無ポート |

## 確認テスト1の解答

| スイッチポートの役割                   | ProCurveでの呼び方                   | Ciscoでの呼び方   |
|------------------------------|---------------------------------|--|
| 複数のVLANのトラフィックを伝送するスイッチ間のリンク | 複数のVLANに対応するタグ付ポート              | トランクポート  |
| リンクの統合に使用                    | トランクポート                         | ポートチャンネルインターフェイス   |
| 複数のVLANに対応するサーバー用に使用         | 複数のVLANに対応するタグ付ポート              | トランクポート  |
| エンドユーザー用に使用 (PC、プリンターなど)     | 1つのVLAN用のタグ無ポート                 | アクセスポート、VLAN   |
| IP電話機用に使用                    | 音声VLANを伝送するタグ付またはタグ無ポート         | 補助(音声) VLAN  |
| エンドユーザーとIP電話機用に使用            | エンドユーザー用のタグ付IP音声VLANに対応するタグ無ポート | 補助(音声) VLAN対応アクセスポート(voice)<br>Multi-VLAN Access Port (MVAP) |

## 確認テスト2

**ProCurve**デバイスはCDPをどのように使用しますか。

- A. 送信
- B. 読み取り
- C. 読み取りおよび送信
- D. フォワード

## 確認テスト2の解答

正解: B

## 確認テスト2

ProCurveスイッチにトランクをダイナミックに構成できるようにするコマンドはどれですか。

- A. trunk <port range> <trunk name> lacp
- B. trunk <trunk name> <port range> trunk
- C. trunk <port range> <trunk name> PagP
- D. lag <trunk name> <port range> trunk

## 確認テスト2の解答

正解: A

## 確認テスト3

ProCurveスイッチでOSPFを設定するとき、OSPFに含める「ネットワーク」または「VLAN」はどこで設定しますか。

- A. OSPFルーティング用のグローバルコンテキストで  
“network command”を指定
- B. VLANコンテキストで “ip ospf address area” を指定
- C. router ospf process-idコンテキストで “ip ospf address  
area”を指定

## 確認テスト3の解答

正解: B



モジュール4終了



## モジュール5: 使用方法と設定方法



## モジュールの目的

このモジュールを修了すると、以下のことができるようになります。

- HP ProCurve Campus LANの使用方法と設定方法について理解する。

このモジュールでは、以下のトピックについて説明します。

- スイッチ管理
- ポートとVLAN
- リンクアグリゲーション
- スパニングツリーの実装
- PoEとVoIP電話機
- DHCPとインテリジェントミラーリング
- OSPFを使用したルーティング

このモジュールでは、HP ProCurve Campus LANの使用方法と設定方法について説明します。これは、このコースで最も長いモジュールです。このモジュールを修了すると、ProCurve Campus LANの使用方法と設定方法についてさらに深く理解できるようになります。

# モジュール5-1: 使用方法と設定方法

## スイッチ管理

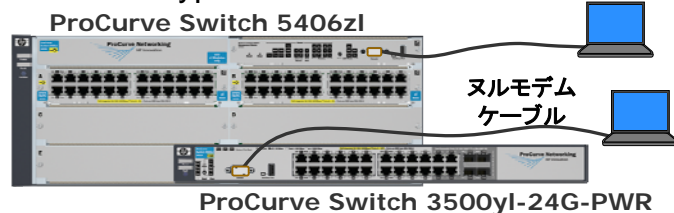


はじめに、「スイッチ管理」について説明します。ここでは、ProCurveスイッチの初期設定手順、およびスイッチの設定とソフトウェアイメージファイルを管理する方法について説明します。スイッチ管理の多くは、Ciscoデバイスの場合と類似しています。

## ダイレクトシリアル接続

初期設定は、多くの場合、直接シリアル接続を使用して実行される

- コンソールポート(DB-9 オス)は、通常、スイッチの前面にある
  - ヌルモデムケーブル(黒)はすべてのスイッチに同梱されている
  - 新しいProCurveスイッチの多くでは、RJ-45「ロール型ケーブル」を使用する
- ターミナルエミュレーションの設定
  - 9600 bps
  - 8データビット、パリティなし、1ストップビット
  - フロー制御なし
- TeraTerm、PuTTY、SecureCRT、HyperTerminalなどを使用可能



CLIは文字ベースのインターフェイスです。スイッチの機能が使用するパラメーターを定義し、これらの機能のステータスを表示できます。CLIは、スイッチにIPアドレスを割り当てた後にTelnet経由で(または追加の設定手順を実行した後にSSH経由で)使用できますが、初期設定では多くの場合、スイッチのコンソールポート経由で直接シリアル接続します。多くのProCurveスイッチでは、スイッチに同梱されているヌルモデムケーブルを使用して、スイッチの前面にあるコンソールポート(DB-9オス)にPCを接続します。

新しいProCurveスイッチの多くでは、RJ-45「ロール型ケーブル」を使用します。

## スイッチ管理のインターフェイス

多くのProCurveスイッチでは、設定とモニタリングで以下のインターフェイスをサポート  
コマンドラインインターフェイス (CLI)

- 直接シリアル接続またはTelnetやSSHセッションを使用してすべての機能の設定とモニタリングを行う
- ユーザー名とパスワードを指定してマネージャーおよびオペレーターレベルでアクセス可能
- RADIUS認証も使用可能

### Webブラウザインターフェイス

- HTTP (<http://<switch-ip-address>>) または SSL (<https://<switch-ip-address>>) アクセス
- RADIUS認証を使用してマネージャーおよびオペレーターレベルでアクセスすることも可能

### メニューインターフェイス ([setup](#) および [menu](#) コマンド)

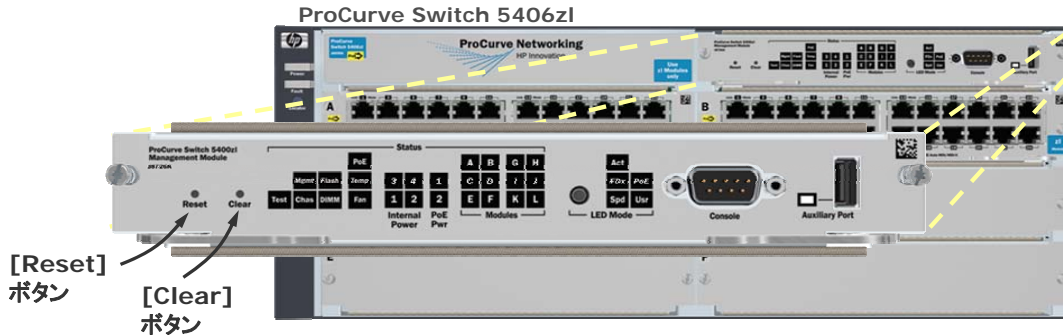
- CLIからアクセス可能

### ProCurve Manager / ProCurve Manager Plus

- グラフィカル アプリケーション インターフェイス

CLIは最も広範な機能を持つ管理ツールです。すべてのスイッチ機能の設定とモニタリングが可能です。[Switch Setup] メニュー (設定コマンド)、[Switch Menu] (メニューコマンド)、およびWebインターフェイスは、CLIで使用できる機能の一部に対応しています。ProCurve Managerを使用することもできますが、これについてはこのトレーニングでは扱いません。

## 管理アクセスのセキュリティ確保



管理アクセスは以下の方法でセキュリティを設定:

- スイッチ本体に物理的なセキュリティを確保する
- ローカルパスワードを割り当てる
  - オペレーターレベル
  - マネージャーレベル
- 前面パネルの [Reset] ボタンと [Clear] ボタンを制御する

HP ProCurveスイッチの前面には、[Reset] ボタンと [Clear] ボタンがあります。ネットワークセキュリティソリューションで最初に行う重要なタスクは、スイッチ自体の物理的セキュリティを確保することです。前面パネルの [Reset] ボタンと [Clear] ボタンの機能を変更して、誰かが許可なくスイッチに物理的にアクセスした場合でも、ボタンを使用できないようにすることができます。

## マネージャーレベルとオペレーターレベルの権限の設定

システムのデフォルトでは、スイッチはパスワードで保護されていない。

- “>” プロンプトは、読み取り専用アクセス、つまりオペレーター権限レベルであることを示す
- “#” プロンプトは、読み取り/書き込みアクセス、つまりマネージャー権限レベルであることを示す

```
5406z1# configure
5406z1(config)# password operator user-name operator plaintext password
5406z1(config)# password manager user-name manager plaintext password
```

マネージャーパスワードを定義してスイッチへの読み取り/書き込みアクセスを保護し、オペレーターパスワードを定義してスイッチへの読み取り専用アクセスを保護。ユーザー名はオプション

```
Username: operator
Password: *****
5406z1> enable
Username: manager
Password: *****
5406z1#
```

- ログインプロンプトで、マネージャーまたはオペレーターのユーザー名/パスワードを指定して、適切なレベルの権限にアクセス
- enableコマンドを使用して、オペレーターレベルからマネージャーレベルに移動することも可能

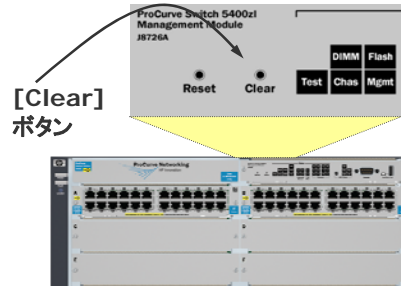
はじめてスイッチに接続すると、CLIプロンプトに、デフォルトのスイッチ名に続いて記号(#や>)が表示されます。デフォルト名は、スイッチのモデルに基づいて決まります。#は読み取り/書き込みモード、つまり「マネージャー」レベルであることを示します。この時点では、パスワードを入力しなくてもスイッチを設定できます。



## 設定したパスワードの削除

### マネージャーパスワードが不明の場合

- [Clear] ボタンを1秒間押すと、マネージャーとオペレーターの名/パスワードが削除される
- この手順では、スイッチに物理的にアクセスできる必要がある



### マネージャーパスワードが既知の場合

- グローバルコンフィギュレーションレベルにアクセスして、[no password](#)コマンドを実行

```
no password <manager | operator | all>
```

```
5406z1(config)# no password manager  
Password protection for manager will be deleted, continue [y/n]? y
```

設定したパスワードを削除する方法は2通りあります。マネージャー権限レベルの現在のパスワードが不明の場合は、上記の [Clear] ボタンを押すとすべてのパスワード保護を削除できます。

また、CLIで“no password”コマンドを実行することによってもパスワードをリセットできます。

## セキュリティ認証情報: コンフィギュレーションファイルに含まれる

**include-credentials** コマンドを実行すると、フラッシュメモリだけでなく、running configurationにもさまざまなセキュリティ設定を追加したり、設定を表示することが可能

- スイッチにアクセスするためのローカルマネージャー/オペレーターのユーザー名とパスワード
- スイッチにアクセスするための802.1Xポートアクセスユーザー名とパスワード
- スイッチにアクセスするためのSSHクライアント公開キー
- RADIUSおよびTACACS+共有シークレット

コンフィギュレーションファイルのバックアップを保存したり、スイッチとの間で転送を行う場合には**注意** が必要

```
5406z1(config)# include-credentials
```

```
**** CAUTION ****
```

```
You have invoked the command 'include-credentials' for the first time. This action will make irreversible changes to the password and ssh public-key storage.
```

```
It will affect *all* stored configurations, which might need to be updated. Those credentials will no longer be readable by older software revisions. It also may break some of your existing user scripts. Continue?[y/n] y
```

```
**** CAUTION ****
```

```
This will insert possibly sensitive information in switch configuration files, and as a part of some CLI commands output. It is strongly recommended that you use sftp rather than tftp for transfer of the configuration over the network, and that you use the web configuration interface only with SSL enabled.
```

```
Proceed?[y/n] y
```

デフォルトでは、スイッチに設定するさまざまなセキュリティ設定は、内部フラッシュに保存され、スイッチのコンフィギュレーションファイルでは確認できません。include-credentialsコマンドを実行すると、スイッチのコンフィギュレーションファイル中のさまざまなセキュリティ設定を保存することができます。

これについての詳細を確認するには、このコースの英語版Webトレーニングに含まれる「student guide」(Interoperability-ILT-Courseware.zip)を参照してください。これは、講師が行う形式のトレーニング用テキストです。

## セキュリティ認証情報: コンフィギュレーションファイルの例

```
5406z1(config)# show running-config
...
RADIUS-server host 10.1.10.10
...
snmpv3 user "snmpadmin"
```

include-credentialsが無効(デフォルト)になっている場合のコンフィギュレーションファイル

```
5406z1(config)# show running-config
...
RADIUS-server host 10.1.10.10 key procurve
...
include-credentials
password operator user-name "operator" sha-1 "64f1ed2b14820bcc04dd88a4ad5517736c07dc32"
password manager user-name "manager" sha-1 "64f1ed2b14820bcc04dd88a4ad5517736c07dc32"
...
ip ssh public-key operator 'ssh-rsa ¥
AAAAAB3NzaClyc2EAAAABJQAAAIB1X9eAtYS5flrcMbKtRrLd+0t8KWV/FNowjgFZj1CX4Rnc¥
zi52wf+4Dy4T27NfyUqKbFipSzNoMbhG1OBqRYH+gtjF00dsYyomKNMPEyDqfX6Iw3887w8A¥
6ZO570807xePPD4EZPxlnv3PoL+1qGGWnt1a3qrxn98ZUY9F3skgbw== "Group1 client"
...
snmpv3 engineid "00:00:00:0b:00:00:00:17:a4:75:c8:00"
snmpv3 user "snmpadmin" auth SHA "d6acf69acd079295cf3c7d25fb87a22d598a786c" priv DES
"d6acf69acd079295cf3c7d25fb87a22d598a786c"
```

include-credentialsが有効になっている場合のコンフィギュレーションファイル

ここでは、include-credentialsコマンドが無効(デフォルト)になっている場合、有効になっている場合、それぞれのコンフィギュレーションファイルの例を示します。

2番目の例は、include-credentialsが有効になっており、共有シークレット、マネージャーレベルとオペレーターレベルに設定したユーザー名およびパスワードのハッシュ値、SSHクライアントの公開キーの値、オペレーターまたはマネージャーに割り当てたアクセスレベルが示されています。スイッチには、SNMPv3エンジン識別子が割り当てられており、SNMPv3ユーザーの認証とプライバシープロトコルの設定、およびそれぞれのパスワードのハッシュ値が表示されています。

ProCurveでは、“do”を実行しなくても、コンフィギュレーションコンテキスト内で“show”コマンドを実行できます。

## 前面パネルのセキュリティ

### スイッチのデフォルトの動作

- パスワードのクリア: [Clear] ボタンを押すと、すべてのローカルパスワードがリセットされる
- 工場出荷時の設定へのリセット: [Clear] および [Reset] ボタンを同時に押すと、スイッチの工場出荷時のデフォルト設定にリセットされる
- 物理的セキュリティを導入しないとセキュリティ上の脅威となる

### 前面パネルのセキュリティ問題

- スイッチを安全な環境に設置しないと、誰でもパスワードをリセットしたり、スイッチへの管理アクセスを実行できてしまう
- スイッチはデフォルト設定にリセットできるため、攻撃者は実装されているセキュリティ機能を回避可能

```
5406z1# show front-panel-security
Clear Password          - Enabled
Reset-on-clear         - Disabled
Factory Reset          - Enabled
Password Recovery      - Enabled
```

← デフォルト設定

HP ProCurveスイッチは、前面パネルの [Clear] ボタンや [Reset] ボタンを無効にすることにより、許可なくパスワードが削除されることを防止する機能を備えています。前面パネルのこれら2つのボタンの機能の一部は、個別に有効/無効にすることが可能です。ボタンを使用して、パスワードのクリア ([Clear] ボタンを使用)、またはスイッチの工場出荷時の設定への復元 ([Reset] ボタンと [Clear] ボタンを同時に使用)を行うことが可能です。

## 前面パネルのボタンのセキュリティ設定

セキュリティ強化のため、[Clear] ボタンおよび [Reset] ボタンの機能は個別に有効/無効にできるようになっている

- [Clear] ボタンを使用してパスワードをクリアできるようにする
- [Clear] ボタンを使ってパスワードをクリアできるようにし、その後システムを強制的にリブートさせる
- [Clear] ボタンと [Reset] ボタンを同時に使って工場出荷時の設定にリセットできるようにする
- ProCurve Customer Careから入手したワンタイム パスワードを使用してパスワードを回復できるようにする

選択した前面パネルのセキュリティ オプションにかかわらず、[Reset] ボタンでスイッチがリブートされる

前面パネルのセキュリティ設定は、コンフィギュレーションファイルではなく、スイッチのフラッシュメモリに保存される。startup configurationを削除しても、前面パネルのセキュリティ設定はデフォルト状態に復元されない。

ほとんどのProCurveスイッチでは、前面パネルのボタンを無効にするCLIコマンドを実行できます。このコマンドを使用して、パスワードのクリア機能と工場出荷時の設定へのリセット機能を個別に無効にすることができます。両方の機能を無効にすることも、一方のみを無効にすることも可能です。工場出荷時の設定へのリセットやパスワードのクリア機能を無効にした後にスイッチの管理パスワードを紛失した場合は、パスワードの回復情報についてHP Customer Careに問い合わせる必要があります。

これについての詳細を確認するには、このコースの英語版Webトレーニングに含まれる「student guide」(Interoperability-ILT-Courseware.zip)を参照してください。これは、講師が行う形式のトレーニング用テキストです。

## マネージャーレベルとオペレーターレベルの間の移動

- **show**: システム情報を表示する
- **ping, link-test**: 接続性をテストする
- **menu, setup**: いずれかのメニューインターフェイスにアクセスする
- **clear**: システムの統計情報カウンタをリセットする
- **erase, write, copy**: イメージとコンフィギュレーションファイルを操作する
- **config**: グローバルコンフィギュレーションレベルに進む
- **exit**: オペレーターレベルに戻る

- **show**: システム情報を表示する
- **ping, link-test**: 接続性をテストする
- **menu**: メニューインターフェイスにアクセスする
- **enable**: マネージャーレベルに進む

オペレーターレベルからマネージャーレベルに移行するには:

```
5406z1> enable
5406z1#
```

マネージャーレベルからオペレーターレベルに戻るには:

```
5406z1# exit
5406z1>
```

マネージャーレベルのプロンプト: Switch#

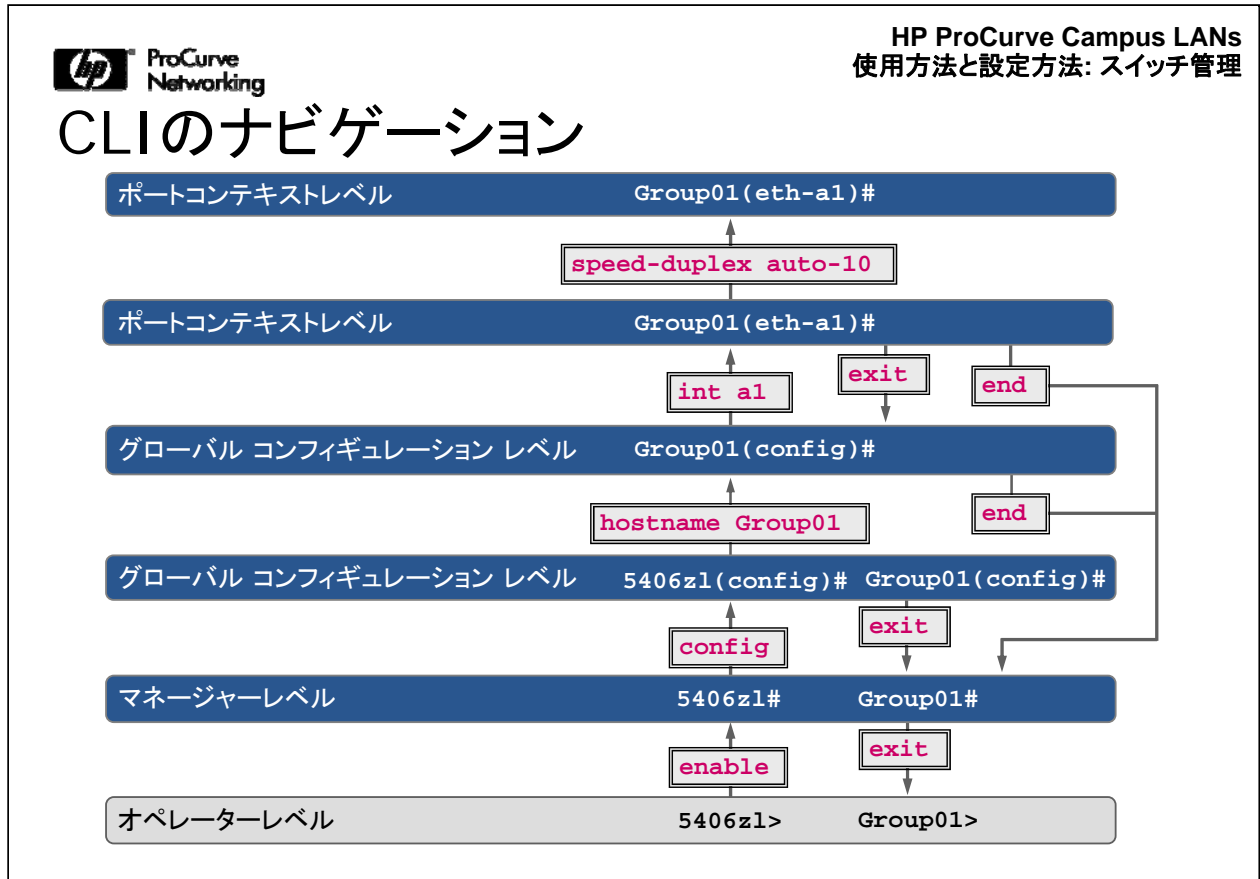
オペレーターレベルのプロンプト: Switch>

ProCurveスイッチには、2つの権限レベル(オペレーターおよびマネージャー)があります。また、2つの主要な設定コンテキスト(グローバルコンフィギュレーションおよびコンテキスト固有コンフィギュレーション)があります。上記の図は、オペレーターレベルとマネージャーレベルの関係を示しています。

オペレーターレベルで使用可能なコマンドは、基本的には、マネージャーレベルで使用可能なコマンドのサブセットです。

適切なパスワードを持つオペレーターユーザーは、enable コマンドを使用して、マネージャーレベルに進むことができます。

# CLIのナビゲーション



CLIでは、ここに示すように、さまざまなレベルで設定やモニタリングを行うことができます。

## CLIのヒントとショートカット

- [?] キーまたは [Tab] キーは、CLIコマンドのコンテキストリストを表示する
- 文字列の入力後に [?] キーまたは [Tab] キーを押すと、指定した文字列で始まるコマンドの一覧が表示される
- コマンドは一意に区別できる限り、最小の文字数に短縮できる
- 最近入力したCLIコマンドは、履歴バッファから呼び出し、編集、および実行できる
- 履歴バッファのコマンドは、実行間に設定可能な間隔で設定可能な回数だけ繰り返すことができる

Ciscoスイッチと同様に、さまざまなショートカットがあり、コマンドを入力したり、CLIをナビゲートする場合に役立ちます。

CLIには、コンテキスト依存ヘルプ、短縮コマンド、タブ補完、コマンド履歴バッファの機能が組み込まれており、コマンド構文の確認や、コマンドの入力に必要なキーストロークを減らすことができます。



## 初期設定でのCLIの使用

```

HP ProCurve Switch 5406ZL# show running-config
...
vlan 1
  untagged a1-a24,b1-b24
  ip address bootp-dhcp
...
HP ProCurve Switch 5406ZL# config
HP ProCurve Switch 5406ZL(config)# hostname Group01
Group01(config)# vlan 1
Group01(vlan-1)# ip address 10.1.1.1/24
Group01(vlan-1)# exit
Group01(config)# ip default-gateway 10.1.1.254
Group01(config)# write memory
Group01(config)# show running-config
...
hostname "Group01"
...
ip default-gateway 10.1.1.2
vlan 1
  untagged a1-a24,b1-b24
  ip address 10.1.1.1 255.255.255.0
  
```

すべてのポートはVLAN 1のタグ無メンバー

デフォルトのIPアドレスソースはBOOTP/DHCP

ProCurveでは、サブネットマスクの指定に CIDR表記を使用できる

ProCurveでは、コンフィギュレーションコンテキストでもrunning configurationを表示できる

ProCurveのCLIは、CiscoデバイスのCLIと類似しています。この画面には、いくつかのProCurveコマンドの実行例を示しています。

"show running-config" – running-configの現在の内容が表示されます。

"config" – コンフィギュレーションコンテキストに移動しています。コンフィギュレーションコンテキストに入ると、さらに入力続けるためのプロンプトが表示されます。

"hostname Group 01" – ホスト名をスイッチに割り当てています。

"vlan1" – VLANコンテキストレベルに入ります。

"ip address 10.1.1.1/24" – IPアドレスとマスクを定義します。

"exit" – VLANコンテキストレベルを終了します。

"ip default-gateway 10.1.1.254" – グローバルコンフィギュレーションレベルでデフォルトゲートウェイを定義します。

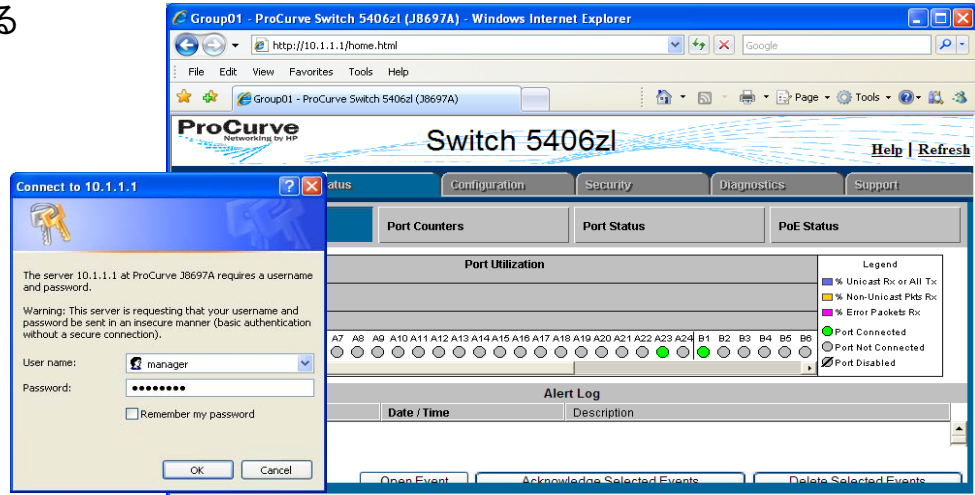
"write memory" – フラッシュに変更を保存します。

"show runing-config" – 変更内容を確認します。

## Webインターフェイスの使用

Webエージェントのアクセスは、コンソールインターフェイスと同じユーザー名/パスワードで保護されている

- SSLアクセスは、ポート443または他の未使用のポートを使用して設定可能
- Webエージェントを使用するには、ブラウザでSun JRE2をサポートしている必要がある



ProCurveのすべての管理型スイッチには、WebブラウザからアクセスできるWebサーバーが含まれています。スイッチのWebサーバーは、Webエージェントと呼ばれることもあります。Webインターフェイスは、スイッチにIPアドレスが割り当てられるとすぐにHTTP経由で使用可能になり、スイッチの設定変更に使用できるようになります。表示がダイナミックに更新されるので、スイッチの動作をモニタリングする際にも役立ちます。

## リモート管理の有効化の復習

右側の項目を、該当する説明に対応させてください。

インバンドデバイスの管理に使用(ヒント:  
ほとんどのProCurveスイッチでは、2つが  
デフォルトで有効)

CLIのマネージャーレベルとオペレーター  
レベルに設定するセキュリティ制御(ヒント  
:一方はデフォルトで設定済み、他方は  
null)

物理的セキュリティを確保するために前面  
パネルで設定できる制御機能

VLAN IPアドレスのパラメーターの割り当  
てに使用

ユーザー名とパスワード

[Clear] と [Reset]

DHCPおよびスタティックアド  
レス設定

Telnet、SSH、HTTP、SSL

ここで、リモート管理の有効化について少し復習します。画面の右側の項目を、左側の正しい説明に対応させてください。

## リモート管理の有効化の復習: 解答

インバンドデバイスの管理に使用(ヒント:  
ほとんどのProCurveスイッチでは、2つが  
デフォルトで有効)

Telnet、SSH、HTTP、SSL

CLIのマネージャーレベルとオペレーター  
レベルに設定するセキュリティ制御(ヒント  
:一方はデフォルトで設定済み、他方は  
null)

ユーザー名とパスワード

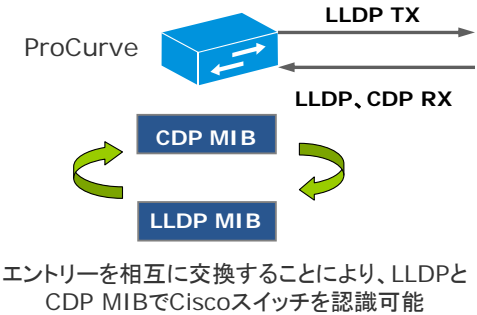
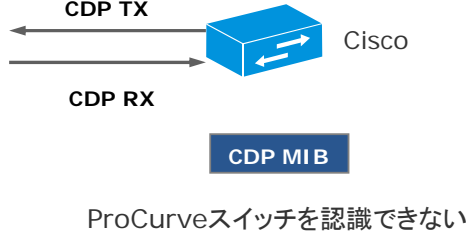
物理的セキュリティを確保するために前面  
パネルで設定できる制御機能

[Clear] と [Reset]

VLAN IPアドレスのパラメーターの割り当  
てに使用

DHCPおよびスタティックアドレ  
ス設定

## CDPおよびIEEE 802.1AB LLDP: ProCurve スイッチでの対応状況

| ProCurve  | Cisco  |
|---|--|
| <p>デフォルトでは、受信モード (receive mode) のすべてのポートでCDPが有効。<br/>CDPパケットの発信には対応していない。</p>   | <p>デフォルトでは、すべてのポートでCDPが有効。</p>   |
| <p>デフォルトでは、すべてのポートでLLDPが有効。</p>   | <p>SNMPサポートなしで12.2(37)SEを実行しているCisco Catalystスイッチシリーズ2950、3760、3750、および12.2(33)SXHを実行しているCisco Catalyst 6500は、LLDPに対応。</p> |
|  <p>エントリーを相互に交換することにより、LLDPと CDP MIBでCiscoスイッチを認識可能</p> |  <p>ProCurveスイッチを認識できない</p>              |

モジュール4「Cisco製品との比較」で説明したように、最も広くサポートされているネットワーク検出プロトコルとして、Link Layer Discovery Protocol (LLDP) と Cisco Discovery Protocol (CDP) があります。Ciscoが独自に開発したCDPは、多くのネットワーク機器ベンダーが実装しています。ProCurveデバイスはCDPパケットを発信しませんが、CiscoデバイスなどProCurve以外のデバイスが送信したCDPパケットを読み取ります。

## 役に立つshowコマンド

| 説明                            | ProCurve  | Cisco  |
|-------------------------------|---|--|
| CDPネイバー情報                     | <code>show cdp neighbor</code>                        | <code>show cdp neighbor</code>                         |
| 詳細なCDPネイバー情報                  | <code>show cdp neighbor detail</code>                 | <code>show cdp neighbor detail</code>                  |
| 詳細なCDPポート固有のネイバー情報            | <code>show cdp neighbor &lt;port-id&gt; detail</code> | <code>show cdp neighbor &lt;port-id&gt; detail</code>  |
| LLDPネイバー情報                    | <code>show lldp info remote</code>                    | <code>show lldp neighbor</code>                        |
| 詳細なLLDPおよびLLDP-MEDネイバー情報      | <code>show lldp info remote all</code>                | <code>show lldp neighbor detail</code>                 |
| 詳細なLLDPおよびLLDP-MEDポート固有ネイバー情報 | <code>show lldp info remote &lt;port-id&gt;</code>    | <code>show lldp neighbor &lt;port-id&gt; detail</code> |

この表には、LLDPまたはCDPプロトコルが検出したネイバー情報を表示する際に、ProCurveスイッチとCiscoスイッチで使用できるCLIコマンドの比較を示しています。

## システムログのイベントの表示

スイッチは、発生したシステムイベントをフラッシュ中のログに保存。ログエントリを表示するには、**show logging**コマンドを実行。

```
Group01(config)# show logging [-a|-r|-m|-p|-w|-i|-d|substring ...]
Keys:  W=Warning  I=Information
       M=Major    D=Debug
-----Event Log listing: Events Since Boot -----
M 01/01/90 00:00:00 sys: `System reboot due to Power Failure
I 01/01/90 00:00:02 lacp: Passive Dynamic LACP enabled on all ports
I 01/01/90 00:00:06 chassis: Slot A inserted
I 01/01/90 00:00:07 dhcpr: DHCP relay agent feature enabled
I 01/01/90 00:00:07 chassis: Slot B inserted
I 01/01/90 00:00:08 chassis: Slot A downloading
...
I 01/01/90 12:57:23 mgr: changing time
I 05/18/09 09:14:01 mgr: new time set
```

“show logging” コマンドを実行すると、スイッチが起動してから記録されていたイベントが表示されます。イベントログの各エントリには、4つの重要度レベル(warning、information、major、またはdebug)のいずれか、およびイベントを登録したソフトウェアモジュールの説明(「Slot B」など)が含まれています。この例では、シヤーシソフトウェアモジュールが、スイッチに搭載された各物理モジュールの認識状況、およびソフトウェアの各モジュールへのダウンロード状況をレポートしています。

syslogサーバーを定義してログレポートを受信することもできます。

## コンフィギュレーションファイルの管理に役立つコマンド

| コマンド   | 説明   |
|--|--|
| <code>copy config &lt;src-file&gt; tftp &lt;ip-address&gt; &lt;dst-file&gt;</code>                 | スイッチからTFTPサーバーにコンフィギュレーションファイルの名前を指定してコピー                        |
| <code>copy &lt;running-config   startup-config&gt; tftp &lt;ip-address&gt; &lt;dst-file&gt;</code> | running configurationまたはstartup configurationをスイッチからTFTPサーバーにコピー |
| <code>copy tftp config &lt;src-file&gt; &lt;ip-address&gt; &lt;dst-file&gt;</code>                 | TFTPサーバーからスイッチにコンフィギュレーションファイルの名前を指定してコピー                        |
| <code>copy tftp startup-config &lt;ip-address&gt; &lt;dst-file&gt;</code>                          | TFTPサーバーからスイッチのstartup configurationにコンフィギュレーションファイルをコピー         |
| <code>copy config &lt;src-file&gt; config &lt;dst-file&gt;</code>                                  | スイッチのフラッシュ上でコンフィギュレーションファイルを別の名前を指定してコピー                         |
| <code>rename config &lt;old-file&gt; &lt;new-file&gt;</code>                                       | スイッチのフラッシュで、コンフィギュレーションファイルの名前を変更                                |
| <code>erase config &lt;filename&gt;</code>   | スイッチのフラッシュで、コンフィギュレーションファイルの名前を指定して削除                            |
| <code>erase startup-config</code>  | startup configurationファイル、ユーザー名/パスワードを削除してリポート                   |
| <code>startup-default [&lt;primary   secondary&gt;] config &lt;filename&gt;</code>                 | デフォルトのコンフィギュレーションファイルをフラッシュの指定の場所で使用するよう設定                       |

設定やシステムソフトウェアを保存したりアップロードする多くのコマンドは、Ciscoのコマンドに類似しています。頻繁に使用するコマンドの一部を上記の表に示しています。

一部のProCurveスイッチは、コンパクトフラッシュに最大3つのコンフィギュレーションファイルを保持する機能を備えています。たとえば、Switch 8200zl、5400zl、3500yl、6200ylシリーズなどがこの機能に対応しています。また、このようなスイッチは、フラッシュに最大2つの異なるソフトウェアイメージを保持することが可能です。ソフトウェアイメージのそれぞれを異なるコンフィギュレーションファイルに関連付けることができます。

これについての詳細を確認するには、このコースの英語版Webトレーニングに含まれる「student guide」(Interoperability-ILT-Courseware.zip)を参照してください。これは、講師が行う形式のトレーニング用テキストです。





## 確認テスト

## 確認テスト1

ProCurve CLIは、以下のどの方法で使用できますか。(当てはまるものをすべて選択)

- A. Telnet
- B. RTelnet
- C. SSH
- D. コンソールポート
- E. USBシリアル

## 確認テスト1の解答

正解: A、C、D

## 確認テスト2

Webブラウザインターフェイスは、次のどの方法で使用できますか。(当てはまるものをすべて選択)

- A. SLIP
- B. SSL
- C. RMON
- D. HTML
- E. SSH

## 確認テスト2の解答

解答: B、D

## 確認テスト3

include-credentialsコマンドにより、フラッシュメモリだけでなく、running configurationにもさまざまなセキュリティ設定を追加したり、設定を表示することが可能になります。これには、どのような認証情報が含まれますか。(当てはまるものをすべて選択)

- A. スイッチにアクセスするためのローカルマネージャー/オペレーターのユーザー名とパスワード
- B. スイッチにアクセスするための802.1Xポートアクセスユーザー名とパスワード
- C. スイッチにアクセスするためのSSHクライアント公開キー
- D. SSL証明書
- E. RADIUSおよびTACACS+共有シークレット

## 確認テスト3の解答

正解: A、B、C、E

## 確認テスト4

IPアドレスは、次のどのコンテキストで設定しますか。(当てはまるものをすべて選択)

- A. グローバルインターフェイス
- B. インターフェイス
- C. VLAN
- D. 物理



## 確認テスト4の解答

正解: C

## 確認テスト5

ProCurveデバイスはCDPをどのように使用しますか。(当てはまるものをすべて選択)

- A. 送信
- B. 読み取り
- C. 読み取りおよび送信
- D. フォワード

## 確認テスト5の解答

正解: B

## モジュール5-1: 使用方法と設定方法

「スイッチ管理」終了



# モジュール5-2: 使用方法と設定方法

## ポートとVLAN



ここでは、CiscoスイッチとProCurveスイッチが相互運用できるようにVLANを設定する手順を説明します。タグ無およびタグ付VLAN(ポート)の考え方、およびProCurveとCiscoでの類似点と相違点について説明します。

## ポートのタイプ

- Ciscoでいう「アクセスポート」は、ProCurveでは「タグ無ポート」と呼ぶ
- Ciscoでいう「トランクポート」は、ProCurveでは「タグ付ポート」と呼ぶ
- Ciscoでいう「ポートチャンネル」は、ProCurveで「トランク」と呼んでいるリンクアグリゲーションに対応する
- ProCurveでいうトランキングとは、複数のポートを統合することを意味する
  - Ciscoでは、複数のVLANを1つのポートで処理することを意味する
- PCなどのエンドユーザーデバイス1つのみを接続している場合は、この接続はタグ無である
  - Ciscoでは、このタイプのポートを「アクセスポート」と呼ぶ

ProCurveとCiscoでは、VLANの設定機能の一部に関して異なる用語を使用しています。たとえば、Ciscoデバイスのエンドユーザーポートはアクセスポートと呼ばれていますが、ProCurveでは同様のポートを「タグ無」ポートと呼んでいます。つまり、この場合、PCが送信するすべてのパケットは、標準のEthernetフレームで802.1Qヘッダーがありません。

おそらく最も大きな用語の違いは、「トランク」という言葉の使い方です。ProCurveでいう「トランキング」とは、リンクアグリゲーションのことを指し、Ciscoでは、複数のVLANを伝送する1つのスイッチポートのことを指します。

## ポートに関する用語: 違いの比較

| スイッチポートの役割                    | ProCurveでの呼び方                                    | Ciscoでの呼び方   |
|-------------------------------|--|--|
| 複数のVLANからのトラフィックを伝送するスイッチ間で使用 | 複数のVLANに対応するタグ付ポート                               | トランクポート  |
| リンクの統合に使用                     | トランクポート  | ポートチャネルインターフェイス  |
| 複数のVLANに対応するサーバー用に使用          | 複数のVLANに対応するタグ付ポート                               | トランクポート  |
| エンドユーザー用に使用 (PC、プリンターなど)      | 1つのVLAN用のタグ無ポート                                  | アクセスポート、VLAN   |
| IP電話機用に使用                     | 音声VLANのタグ付またはタグ無ポート                              | 補助(音声) VLAN  |
| エンドユーザーとIP電話機用に使用             | エンドユーザー用の1つのVLANに対応するタグ無ポート<br>IP電話機用のタグ付 音声VLAN | 補助(音声) VLANに対応するアクセスポート<br>Multi-VLAN Access Port (MVAP) |

モジュール「Cisco製品との比較」で、ProCurveとCiscoでは、ポートやVLANの設定機能の一部に関して異なる用語を使用していることを説明しました。この表は、いくつかの用語の意味とその違いを再確認するためのものです。

## ポート識別子: スタッカブルスイッチ

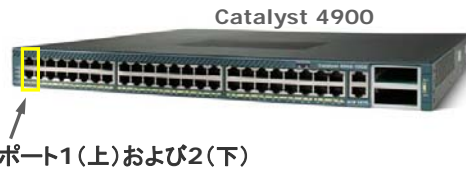
### Cisco

ポート識別子として、相対的なポート番号のほかに、インターフェイスのタイプを示すラベルとスロット番号プレフィックス(0または1)を指定。

例:

FastEthernet0/1、GigabitEthernet1/ 1 ...

```
Switch(config)# interface GigabitEthernet0/1
```



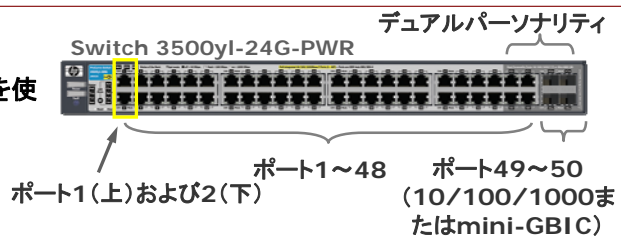
### ProCurve

ポート識別子として、相対ポート番号のみを使用。

例:

1、2...

```
Switch(config)# interface 1
```



復習のため、現行のほとんどのCiscoスイッチとProCurveスイッチでのポートの呼び方の概要をここに示します。これについては、モジュール「Cisco製品との比較」で学習しました。ProCurveのスタッカブルスイッチでは、単に相対ポート番号のみを使用してポート識別子を指定します。ほとんどのCiscoスイッチとProCurveスイッチでは、ポートパラメーターを設定するには、CLIのグローバルコンフィギュレーションコンテキストでinterfaceコマンドを実行します。

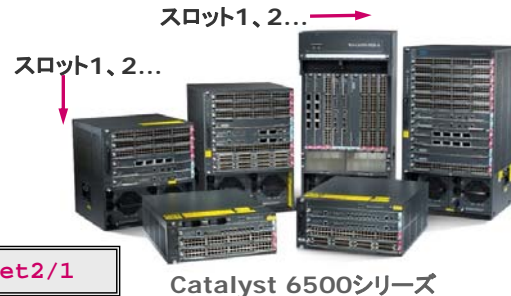


## ポート識別子: モジュール式スイッチ

### Cisco - モジュール式スイッチ

- モジュールは、1、2 ... のようにラベル付けされる
- ポートはスロット番号プレフィックスと共に番号で指定
  - 例: GigabitEthernet2/1

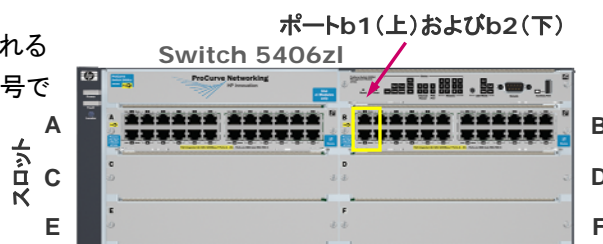
```
Switch(config)# interface GigabitEthernet2/1
```



### ProCurve - モジュール式スイッチ

- モジュールは、a、b ... のようにラベル付けされる
- ポートはモジュールに対応する文字と共に番号で指定
  - 例: a1、a4、b1、b24...

```
Switch(config)# interface a1
```



ここでは、これまでに学習した、その他の主な違いを示します。

Ciscoのモジュール式スイッチでは、ポート識別子はスタックブルスイッチの場合と同じ4つの要素から構成されます。対応するスロット番号が各モジュールにある点が、ProCurveと異なります。

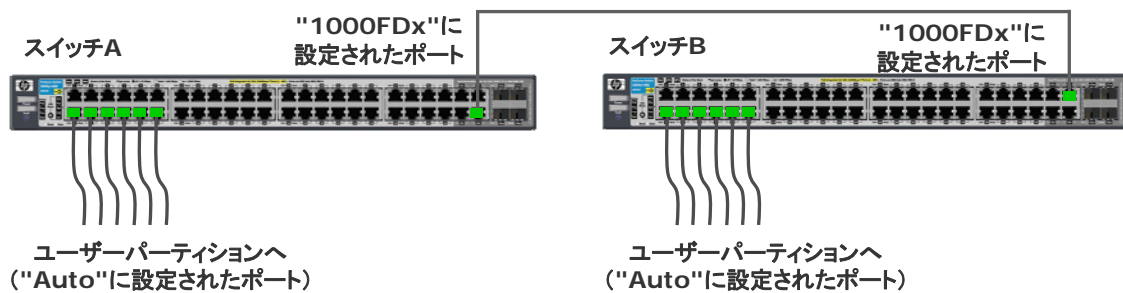
ProCurveのモジュール式スイッチでは、ポート識別子はモジュールまたはスロットを示す、a、b、cのようなアルファベット文字のラベルで構成されます。CLIを使用する場合は、このアルファベットのラベルに、そのモジュールでの相対ポート番号を付けて、a1、a2、a3のように指定します。

## ポートの速度とモードの変更

- 任意のポートの速度とモードを設定可能
- デフォルトは「Auto」

```
Switch_A(config)# int 48  
Switch_A(eth-48)# speed-duplex 1000-full
```

```
Switch_B(config)# int 47  
Switch_B(eth-47)# speed-duplex 1000-full
```



すべてのHP ProCurveスイッチでは、ポートのモードと速度をすべて手動で設定できます。ポートの速度とモードを手動で設定すると、クロスケーブルなしでスイッチ間の接続を可能にする、auto-MDIXが無効になります。スイッチ間リンクの速度やモードを手動で設定する場合は、クロスケーブルを使用する必要があります。

## ポートステータスの表示

ポートステータスはいくつかの方法で表示可能

- CLIコマンド: show interfaces brief
- メニューインターフェイス: [Status and Counters] メニューから [Port Status] を選択
- Webインターフェイス: [Port Status] タブを選択

```
Switch_A(config)# show int brief
Status and Counters - Port Status

```

| Port | Type      | Intrusion |         |        |         | MDI Mode | Flow Ctrl | Bcast Limit |
|------|-----------|-----------|---------|--------|---------|----------|-----------|-------------|
|      |           | Alert     | Enabled | Status | Mode    |          |           |             |
| 1    | 100/1000T | No        | Yes     | Down   | 1000FDx | Auto     | off       | 0           |
| 2    | 100/1000T | No        | Yes     | Down   | 1000FDx | Auto     | off       | 0           |
| ...  |           |           |         |        |         |          |           |             |
| 48   | 100/1000T | No        | Yes     | Up     | 100FDx  | MDI      | off       | 0           |

ポートを有効/無効にする方法: `int [port-list] [enable|disable]`

ProCurveスイッチのポートステータスは、CLI、メニューインターフェイス、またはWebインターフェイスから表示できます。

## VLAN設定の比較: スイッチ間

| ProCurve                      | Cisco  |
|-------------------------------|--|
| vlan 1 ← デフォルト<br>untagged a1 | interface GigabitEthernet 1/20<br>switchport ← アクセススイッチでのデフォルト                 |
| vlan 11<br>tagged a1          | switchport trunk encapsulation dot1q<br>switchport trunk native vlan 1 ← デフォルト |
| vlan 12<br>tagged a1          | switchport trunk allowed vlan 11-13  |
| vlan 13<br>tagged a1          | switchport mode trunk<br>switchport nonegotiate ← Cisco DTPを無効化                |



ProCurveデバイスでは、1つのリンクが複数のVLANを伝送するように設定するには、その特定のVLANのコンテキスト内でポートを「タグ付」に設定します。

この例では、ポートa1は、VLAN 11、12、13にタグ付けされています。VLAN 1については、ポートをタグ無に指定する必要はありません。これは、すべてのスイッチポートの初期設定でこのように設定されているためです。この例の場合、ProCurveスイッチのポートa1では、タグ付ユーザーVLANトラフィックを伝送する物理リンクでタグ無VLAN 1トラフィックも許可されます。

上記には、Ciscoデバイスで同様の設定を行う場合の比較も示しています。

## VLAN設定の比較: スイッチ間のノード

| ProCurve                       | Cisco   |
|--------------------------------|---|
| <pre>vlan 11 untagged a1</pre> | <pre>interface GigabitEthernet 1/20 switchport switchport access vlan 11 switchport mode access</pre> |



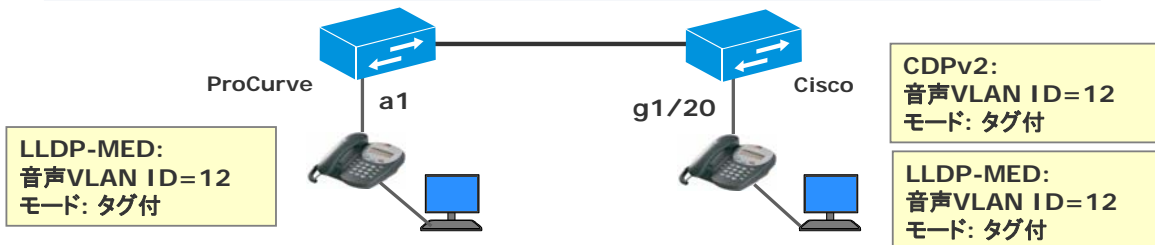
「アクセスポート」の設定は簡単です。この場合、エンドユーザーのPCまたは他のタイプのエッジデバイスに接続しているポートは、1つのVLANに所属します。

ProCurveスイッチでは、通常、このようなポートはVLANのタグ無メンバーに設定します。たとえば、CLIコマンド `vlan 2 untagged a1` を実行すると、上記と同様の設定ができます。

Ciscoスイッチの場合は、`switchport access vlan 2` コマンドを実行します。その後、`switchport mode access` コマンドを実行して、このポートをアクセスポートに設定します。

## スイッチとコンピューター間にIP電話機を接続

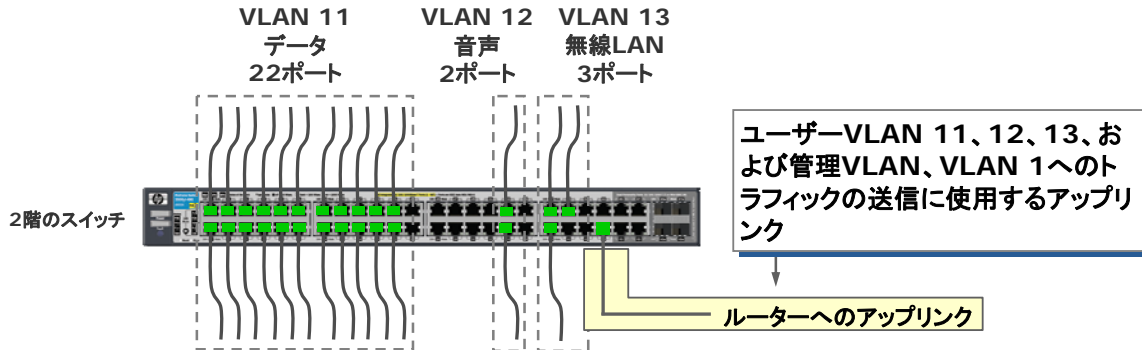
| ProCurve   | Cisco  |
|--|--|
| <pre>vlan 11   untagged a1 vlan 12   voice   tagged a1</pre> | <pre>interface GigabitEthernet 1/20   switchport   switchport access vlan 11   switchport mode access   switchport voice vlan 12</pre> |



この例では、1台のコンピューターと1台のIP電話機がスイッチポートを共有しています。IP電話機はスイッチポートに接続され、コンピューターはIP電話機に接続されています。

多くのIP電話機は802.1Qをサポートしているので、ProCurveスイッチの場合は、コマンドvlan 11 untagged a1を使用してポートをVLAN 11のタグ無ポートに設定し、コマンドvlan 12 tagged a1を使用してポートをVLAN 12のタグ付に設定し、さらにVLAN 12に対してvoiceコマンドを使用して音声VLANも設定します。このコマンドを実行すると、電話機が音声フレームのプライオリティをまだマーキングしていない場合に、VLAN 12のトラフィックのプライオリティが自動的に高く設定されます。

## スイッチ間のVLAN境界の拡張

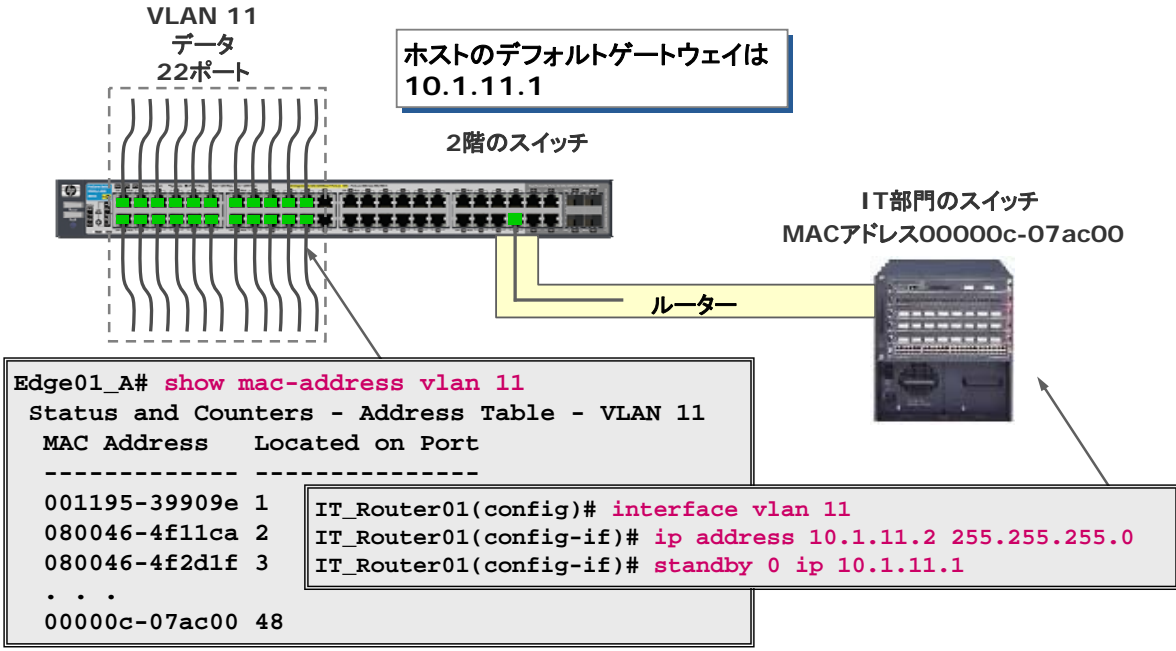


- アップリンクをVLAN 11、12、13のメンバーとして割り当て
- アップリンクをVLAN 1のメンバーにすることで、リモート管理が可能になる
- スイッチがユーザーVLANのトラフィックと管理トラフィックを区別できるように、以下のコマンドを実行してアップリンクポートをタグ付メンバーとして定義する

```
Edge01_A(config)# vlan 11 tagged 48
Edge01_A(config)# vlan 12 tagged 48
Edge01_A(config)# vlan 13 tagged 48
```

ここでは、ある建物での設定を例に説明します。上記は、建物の2階の設定を示しています。アップリンクポートは、VLAN 11、12、13の「タグ付」メンバーとして定義されています。つまりこの場合、このポートで送受信する各VLANの packets に802.1Qタグが付いている必要があります。この例では、VLAN 11 packets を示すタグ、VLAN 12 packets を示すタグ、VLAN 13 packets を示すタグがそれぞれ付加されます。スイッチは、伝送する各VLANに対応する packets に適切なタグを付加します。リモート管理アクセス対応にする場合は、ポートをVLAN 1のタグ無メンバーのままにします。

# VLAN内でのフォワーディング

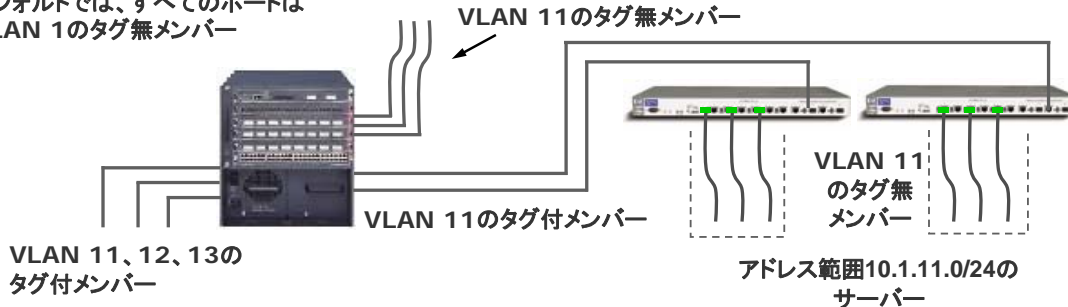


上記は、1階にあるIT部門のCiscoスイッチに接続する、2階にあるProCurveスイッチのアップリンクポートを示しています。IT部門のスイッチには、IPアドレス10.1.11.1/24のVLAN 11用の論理インターフェイスがあり、VLAN 11のすべてのホストのデフォルトゲートウェイとして機能しています。この設定により、VLAN 11ホストは、ACLの設定に従って、他のVLANのネットワークサービスにアクセスできるようになります。



## CiscoスイッチでのVLANの定義

デフォルトでは、すべてのポートは  
VLAN 1のタグ無メンバー



- IT部門のスイッチは、以下のスイッチに直接接続されている
  - 他の3フロアのスイッチ
  - すべての部門にアクセス可能なサーバーに接続しているスイッチ

### スイッチ間のタグ付ポートの設定例

```
IT_Router01(config)# interface GigabitEthernet 1/1
IT_Router01(config-if)# switchport trunk encapsulation dot1q
IT_Router01(config-if)# switchport trunk allowed vlan 1,11-13
```

### スイッチとエンドユーザー間のタグ無ポートの設定例

```
IT_Router01(config)# interface GigabitEthernet 1/20
IT_Router01(config-if)# switchport access vlan 11
IT_Router01(config-if)# switchport mode access
```

IT部門にあるCiscoスイッチは、さまざまなユーザーVLANへのアクセスに対応しています。VLAN間でフォワーディングできるようにするには、いくつかの手順を実行する必要があります。まず、他のフロアにあるスイッチに接続するアップリンクポートを設定します。これには、switchport trunk allowed vlanコマンドを使用して、対応する各VLAN内のポートに「タグ付け」し、このようなアップリンク経由で伝送するVLANを指定します。

## VLAN間のフォワーディング

IT部門のスイッチは、直接接続しているVLAN間でIPトラフィックのフォワーディングを行う。これには、以下の2つの項目を設定

1. 以下のコマンドを使用してIPルーティングを有効にする

```
IT_Router01(config)# ip routing
```

2. IT部門のスイッチの各VLANにIPアドレスを割り当てて、IPフォワーディングを実行できるようにする

- IPアドレスは、該当するVLANのホストの範囲内にある必要がある
- VLAN内のIPホストでは、ルーターのIPインターフェイスがデフォルトゲートウェイとして定義されている必要がある
- デフォルトでは、VLANにIPアドレスが設定されている場合、「ルーター」がそのVLANのルーティングを行う

VLAN 12と13でも同様

```
IT_Router01(config)# interface vlan 11  
IT_Router01(config-if)# ip address 10.1.11.1 255.255.255.0
```

IT部門のスイッチは、複数のVLAN間でトラフィックをフォワーディングする必要があります。この機能を有効にするには、VLANポートのタグ付けに加え、2つの設定手順を実行する必要があります。つまり、IPルーティングを有効にし、各VLANにIPアドレスを割り当てる必要があります。

## VLAN間でフォワーディングするためのルート エントリー

```
IT_Router01# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       ...

Gateway of last resort is not set

 10.0.0.0/24 is subnetted, 4 subnets
C       10.1.11.0 is directly connected, Vlan11
C       10.1.13.0 is directly connected, Vlan13
C       10.1.12.0 is directly connected, Vlan12
C       10.1.1.0 is directly connected, Vlan1
```

IT\_Router01スイッチの  
IPルーティングテーブル

### ホスト間のトラフィックのフォワーディング

IT部門のスイッチは、1つのVLANにあるホストから別のVLANにあるホストにトラフィックを転送する場合に以下を行う

- ARPキャッシュ中の宛先MACアドレスを検索する
- そのエントリが期限切れの場合、スイッチはARP要求を送信してMACアドレスを確認する
- IPパケットに新しいレイヤー2ヘッダーを作成する
- パケットを宛先に転送する

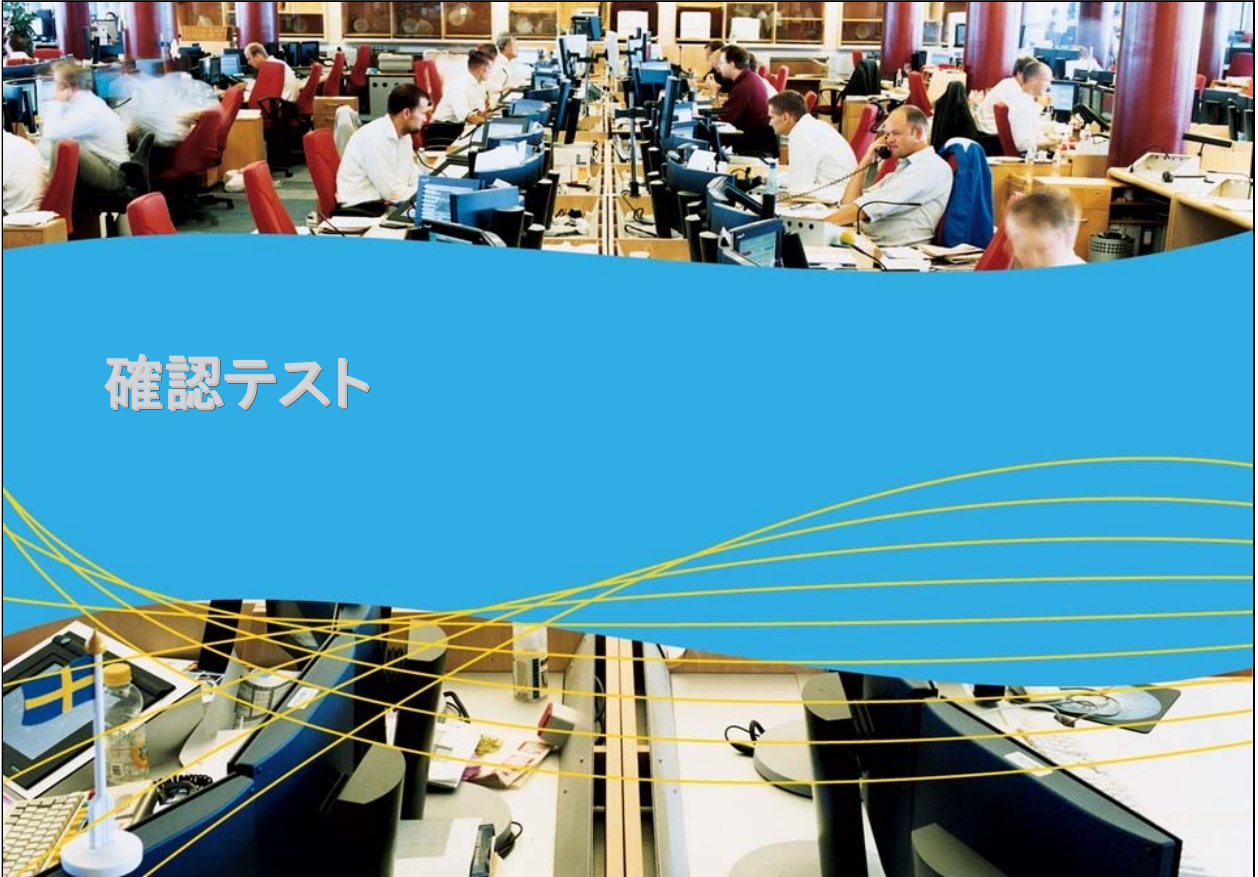
show ip routeコマンドを使用すると、設定済みのすべてのVLANインターフェイスのルーティング情報を調べることができます。

ここに示すように、IT部門のスイッチのIPルーティングテーブルには、スイッチが認識している、直接接続されているネットワークアドレスすべてが入っています。スイッチはこのテーブルを使用して、トラフィックを各宛先ネットワークに転送する際に使用するインターフェイスを決定します。

## 役に立つshowコマンド

| 説明                      | ProCurve   | Cisco   |
|-------------------------|--|---|
| ポートステータスの確認             | <code>show interfaces brief</code>                                     | <code>show interfaces status</code>                                       |
| ポートカウンターと使用率の確認         | <code>show interfaces</code><br><code>&lt;port-list&gt;</code>         | <code>show interfaces</code><br><code>&lt;port-list&gt;</code>            |
| 設定されているVLANの確認          | <code>show vlans</code>  | <code>show vlan brief</code>  |
| ある特定のVLANの詳細の確認         | <code>show vlans &lt;vlan-id&gt;</code>                                | <code>show vlan &lt;vlan-id&gt;</code>                                    |
| ポートが所属しているタグ無VLANの確認    | <code>show vlans ports</code><br><code>&lt;port-list&gt; detail</code> | <code>show interfaces status</code>                                       |
| Ciscoレイヤー2ポートであるかどうかの確認 |  | <code>show interfaces</code><br><code>&lt;port-list&gt; switchport</code> |
| ポートに設定されているVLANの確認      | <code>show vlans ports</code><br><code>&lt;port-list&gt; detail</code> | <code>show interfaces</code><br><code>&lt;port-list&gt; trunk</code>      |
| 複数のVLANがあるポートの確認        | <code>show interfaces brief</code>                                     | <code>show interfaces trunk</code>  |

この表には、VLANや関連する設定情報を表示する際に、ProCurveスイッチとCiscoスイッチで使用できるCLIコマンドを示しています。



## 確認テスト1

右側にあるProCurve の用語を、該当するCisco の用語に対応させてください。

| ProCurve | Cisco  |
|----------|--|
|          | トランクポート  |
|          | ポートチャンネルインターフェイス   |
|          | トランクポート  |
|          | アクセスポート、VLAN   |
|          | 補助(音声) VLAN  |
|          | 補助(音声) VLANに対応するアクセスポート<br>Multi-VLAN Access Port (MVAP) |

### ProCurveの用語:

- 複数のVLANに対応するタグ付ポート
- IP電話機用のタグ付 音声 VLAN
- 複数のVLANに対応するタグ付ポート
- トランクポート
- 1つのVLAN用のタグ無ポート
- エンドユーザー用の1つのVLANにあるタグ無ポート
- Voice VLANのタグ付またはタグ無ポート

## 確認テスト1の解答

| ProCurve                                       | Cisco  |
|--|--|
| 複数のVLANに対応するタグ付ポート                             | トランクポート  |
| トランクポート  | ポートチャネルインターフェイス  |
| 複数のVLANに対応するタグ付ポート                             | トランクポート  |
| 1つのVLAN用のタグ無ポート                                | アクセスポート、VLAN   |
| Voice VLANのタグ付またはタグ無ポート                        | 補助(音声) VLAN  |
| エンドユーザー用の1つのVLANにあるタグ無ポート<br>IP電話機用のタグ付 音声VLAN | 補助(音声) VLANに対応するアクセスポート<br>Multi-VLAN Access Port (MVAP) |

## 確認テスト2

HP ProCurveのモジュール式スイッチでは、以下のどのタイプの文字でスロットにラベル付けしますか。

- A. 番号のみ
- B. アルファベットと番号
- C. アルファベットのみ
- D. 記号



## 確認テスト2の解答

正解: C

## 確認テスト3

HP ProCurveデバイスのコンフィギュレーションコンテキストで "vlan 20" と入力した後、ポートA13をVLAN 20にするには、以下のどのコマンドを実行しますか。

- A.tagged a13
- B.trunked a13
- C.a13 tagged vlan 20
- D.a13 trunked vlan 20

## 確認テスト3の解答

正解: A

## 確認テスト4

ProCurveスイッチのIPアドレスはどこで割り当てますか。

- A. インターフェイスコンテキスト内
- B. ポートコンテキスト内
- C. VLANコンテキスト内
- D. グローバルコンテキスト内

## 確認テスト4の解答

正解: C

## モジュール5-2: 使用方法と設定方法

「ポートとVLAN」終了



# モジュール5-3: 使用方法と設定方法

## リンクアグリゲーション



ここでは、Cisco EtherChannel、HP Port Trunkingなど、リンクアグリゲーションの方法に関する基本的な考え方、およびリンクアグリゲーションに関するIEEE 802.3ad 標準 ( LACP: Link Aggregation Control Protocol) について説明します。

## リンクアグリゲーションの方法

### Cisco EtherChannel

- 同じ速度の最大8個のリンクで「ポートチャネル」グループを作成する場合に使用
- スタティックに定義、またはPAgPを使用してダイナミックに構成可能

### HP Port Trunking

- HP ProCurveでは、リンクアグリゲーションのことを「トランキング」という
- ProCurveでの「トランク」とは、同じリンクにある複数のVLANのことではなく、「リンクアグリゲーション」を意味する
- スタティックに定義した最大8個の同じ速度のリンクに対応

### IEEE 802.3ad LACP

- リンクアグリゲーションに関する標準に基づく方法
- スタティックに定義、またはダイナミックに構成可能

Ciscoスイッチでは、EtherChannelという独自の方法でリンクのグループを統合および設定できます。同様に、ProCurveスイッチでは、HP Port Trunkingという独自の方法を使用してリンクを統合できます。CiscoとProCurveはいずれも、業界標準のIEEE 802.3ad Link Aggregation Control Protocol (LACP)もサポートしています。

このトピックの詳細については、このコースの英語版Webトレーニングに含まれる『ProCurve and Cisco Network Interoperability Training Student Guide』のモジュール4を参照してください。

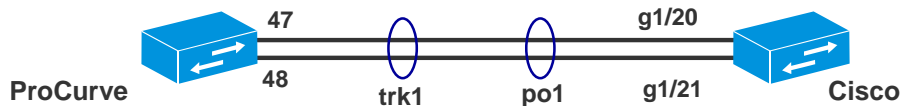


## リンクアグリゲーションの方法

| ProCurve                          | Cisco   |
|-----------------------------------|---|
| <pre>trunk 47-48 trk1 trunk</pre> | <pre>interface Port-channel 1 interface GigabitEthernet 1/20 channel-group 1 mode on interface GigabitEthernet 1/21 channel-group 1 mode on</pre> |

このパラメーターは、リンクアグリゲーションの「タイプ」を定義。“trunk”パラメーターは、HP Port Trunkingを示す。

自動的に作成



この図は、ProCurveスイッチとCiscoスイッチの間にスタティックトランクを設定する際に使用できるCLIコマンドを示しています。ここでProCurveとCiscoの用語の違いを思い出してください。Ciscoの環境では、“trunk”とは、ISLまたは802.1Qタグ付の複数のVLANのフレームを伝送するスイッチ間リンクを意味します。ProCurveの環境では、“trunk”とは、HP Port TrunkingまたはLACPのいずれかを使用してリンクアグリゲーションを行うことを意味します。

## ProCurveスイッチでポートランキングがVLANステータスに影響を与える方法

```
Edge01_A# show run
...
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-48
  ip address 10.1.1.2 255.255.255.0
exit
vlan 11
  name "VLAN11"
  tagged 48 ...
```

トランクの作成前は、ポート48はVLAN 11のタグ付メンバーになっている。

```
Edge01_A(config)# trunk 47,48 trk1 lacp
```

ポート47および49のトランクを作成。

```
Edge01_A# show run
...
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-48,Trk1
  ip address 10.1.1.2 255.255.255.0
exit
vlan 11
  name "VLAN11"
  tagged ...
```

トランクを作成すると、*Trk1*がデフォルトVLANのタグ無メンバーとなる。  
ポート48はもうVLAN 11に割り当てられておらず、ポート47はもうVLAN 11に割り当てられていない。

```
Edge01_A(config)# vlan 11 tagged trk1
```

*Trk1*をVLAN 11のタグ付メンバーとして割り当てる必要がある。

この図では、トランクを定義する前は、スイッチのアップリンクは、VLAN 11のタグ付トラフィックとVLAN 1のタグ無トラフィックを伝送する1つのポート(ポート48)です。

ポート47と48を論理エンティティ"Trk1"(トランクに統合したリンクグループの論理インターフェイス)に割り当てて、2つのポートをトランキングしてアップリンクとして使用するようスイッチを設定すると、このアップリンクを通過するVLAN 11のホストが隔離されます。そのため、VLAN 11のタグ付メンバーであったポート48とVLAN 11との関連付けが解除されます。

## フレンドリポート名を使用したトランクステータスの表示

```
Edge01_A(config)# interface 47 name 'Link-1 to Cisco Switch'  
Edge01_A(config)# interface 48 name 'Link-2 to Cisco Switch'  
Edge01_A(config)# show trunk
```

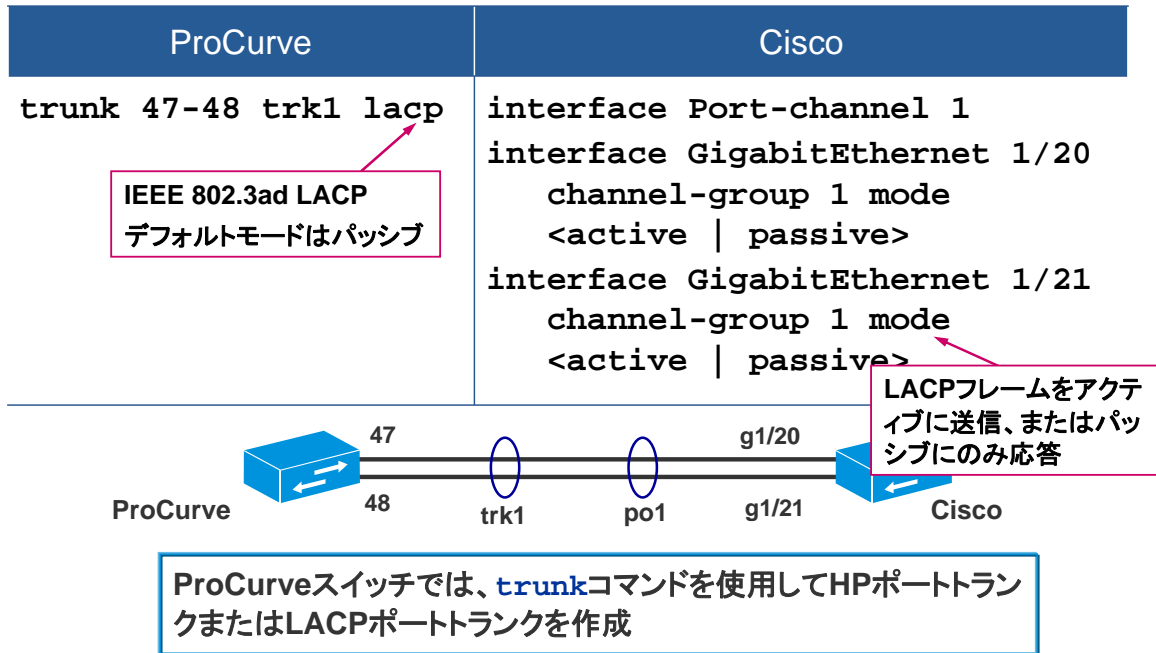
Load Balancing

| Port | Name                   | Type      | Group | Type  |
|------|------------------------|-----------|-------|-------|
| 47   | Link-1 to Cisco Switch | 100/1000T | Trk1  | Trunk |
| 48   | Link-2 to Cisco Switch | 100/1000T | Trk1  | Trunk |

ポートごとにフレンドリポート名を定義してわかりやすくすることが可能

上記は、スタティックに定義したトランクのProCurve側のステータスを示しています。ここでは、管理上の規則に従って、フレンドリポート名を設定しています。

## 設定シナリオ: LACPを使用したダイナミックな(リンク)集約



ここには、ProCurveスイッチとCiscoスイッチ間のリンクにLACPを設定する方法を示しています。ProCurve側では、trunkコマンドで“trunk”ではなく“lacp”を指定しています。これは、LACPプロトコルを使用してリンクを構成することを意味します。リンクの他方の側がLACPに対応している場合は、リンクが自動的に構成されます。

Cisco側では、“mode” パラメーターを使用して、リンクの物理インターフェイスをパッシブモードまたはアクティブモードに指定します。パッシブモードの場合は、LACP BPDUがアクティブに送信されますが、パッシブモードでは、最初の受信への応答としてのみLACP BPDUが送信されます。

## 役に立つshowコマンド

| 説明                               | ProCurve                             | Cisco  |
|----------------------------------|--------------------------------------|--|
| リンクアグリゲーションに所属するポートを確認           | <code>show trunk</code>              | <code>show etherchannel &lt;port-channel&gt; [summary   detail]</code> |
| ポートが所属しているリンクアグリゲーションを確認         | <code>show trunk &lt;port&gt;</code> | <code>show interfaces &lt;port&gt; etherchannel</code>                 |
| 出カトラフィック用に使用するロードバランシングアルゴリズムの確認 |                                      | <code>show etherchannel load-balance</code>                            |
| 特定のLACP情報の表示                     | <code>show lacp</code>               | <code>show lacp</code>   |

この表には、スタティック/ダイナミック リンクアグリゲーションの設定を表示する際に、ProCurveとCiscoスイッチで使用できるCLIコマンドを示しています。



## 確認テスト

## 確認テスト1

ProCurveスイッチにスタティックにトランクを構成するコマンドは以下のどれですか。

- A. lag <port range> <trunk name> trunk
- B. trunk <port range> <trunk name> trunk
- C. lag <trunk name> <port range> trunk
- D. trunk <trunk name> <port range> trunk

## 確認テスト1の解答

正解: B



## 確認テスト2

他のスイッチがアクティブモードの場合に、ProCurveスイッチにダイナミックにトランクを構成できるようにするコマンドは以下のどれですか。

- A. trunk <port range> <trunk name> lacp
- B. trunk <trunk name> <port range> trunk
- C. trunk <port range> <trunk name> PagP
- D. lag <trunk name> <port range> trunk

## 確認テスト2の解答

正解: A

## モジュール5-3: 使用方法と設定方法

「リンクアグリゲーション」終了



# モジュール5-4: 使用方法と設定方法

## スパニングツリーの実装

PVST+とMSTPを使用したスパニングツリーの実装



ここでは、スパニングツリーの実装に関する考慮事項、およびCisco Per VLAN Spanning Tree Plus (PVST+)とIEEE 802.1Q Multiple Spanning Tree Protocol (MSTP)の設定手順について説明します。

Cisco製品のエキスパートであれば、スパニングツリープロトコル(STP)に精通しているはずですが、PVST+とMSTP(8021.Q)を使用したネットワークを適切に統合するには、その相互運用性について理解する必要があります。ここでは、その主要なポイントを中心に説明します。

## STPとRSTP

- IEEE 802.1D-1998 STPおよびIEEE 802.1w RSTPは、VLANの使用の有無に関係なく冗長リンクのループプロテクションを設定可能にする
- すべてのVLANが同じ物理トポロジを使用する必要があるため、リンクを未使用のままにすることが可能

最初のSTP:

IEEE 802.1D-1998

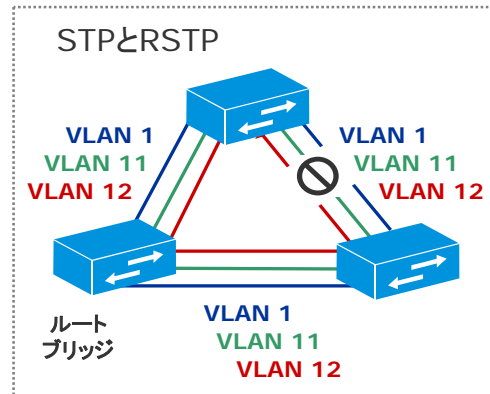
Rapid STP(RSTP):

IEEE 802.1w-2001

リンクコストとブリッジプライオリティ値に関する変更:

IEEE 802.1t-2001

IEEE 802.1D-2004



スパニングツリープロトコル(STP)に関する最初の基準は、IEEE 802.1D-1998仕様に規定されています。STPに関するその後のリビジョンでは、Rapid Spanning Tree Protocol(RSTP)が規定され、IEEE 802.1w-2001仕様として定義されました。RSTPでは、スパニングツリーのコンバージェンス時間を削減するパフォーマンス上の改良が加えられています。IEEE 802.1wは現在、IEEE 802.1D-2004仕様のサブセットになっています。

スパニングツリーの動作について復習するには、このコースの英語版Webトレーニングに含まれる『ProCurve and Cisco Network Interoperability Training guide』のモジュール5を参照してください。

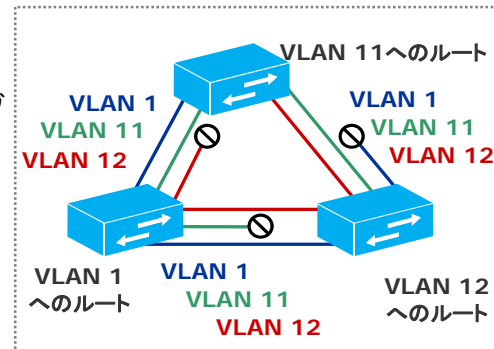
## Cisco PVST+ とRapid PVST+

PVSTは、設定済みの各VLANでスパニングツリーインスタンスをサポート

- VLANとSTPインスタンスのマッピングを1対1で行う(つまり別のプロセスになる)
- 各VLANで、VLAN固有のBPDUを使用
- ISLランキングを使用して、一部のVLANトランクのフォワーディングを許可(その他はブロック)

PVST+は、PVSTと同じ機能を持つが、802.1Qにも対応

Rapid PVST+ではコンバージェンス時間が改善(RSTPの場合と類似)



Ciscoは、独自プロトコルPer VLAN Spanning Tree (PVST)、およびその改良版であるPer VLAN Spanning Tree PlusとRapid PVST+を開発しました。PVST+は、PVSTと同じ機能を備えていますが、Ciscoのスイッチ間リンク (ISL) に加え、802.1Qトランクに対応しています。Rapid PVST+は、そのコンセプトの点でRSTPに類似しており、コンバージェンス時間が改善されています。PVST+という場合、特に違いを明示する必要がある場合以外は、一般的にはこれら3つのプロトコルすべてを指します。

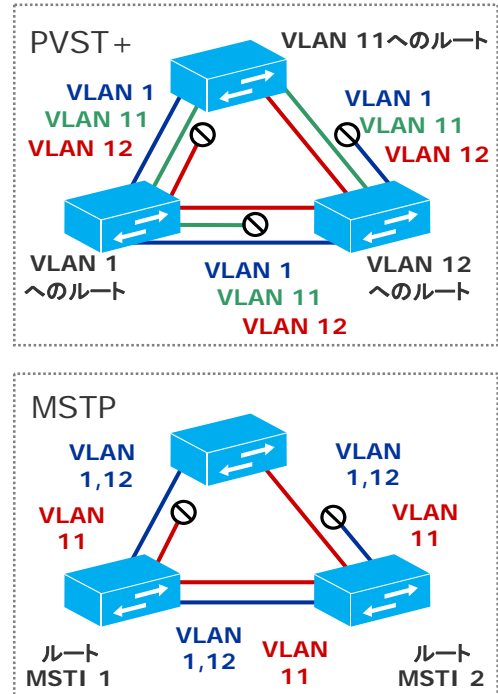
## PVST+とMSTPの比較

IEEE 802.1s MSTPは、標準に準拠した802.1D/w/Qスイッチが、冗長リンクを構成する複数の論理パスを設定できるようにするために開発された。

802.1sは、802.1Qを拡張して、VLANのグループを別のスパニングツリーに割り当てられるようにしたものの。

- インスタンスは、適用可能な複数の論理パスにレイヤー2ネットワーク経路でマッチさせることができる
- 多くの場合、PVST+のようにVLANとインスタンスを1対1マッチングするのではなく、少数のインスタンスのみを必要とする

|                           |                    |
|---------------------------|--------------------|
| VLAN:<br>IEEE 802.1Q-1998 | } IEEE 802.1Q-2003 |
| MSTP:<br>IEEE 802.1s-2002 |                    |



IEEE 802.1s MSTPは、標準に準拠したスイッチが、冗長リンクを構成する複数の論理パスを設定できるようにするために開発されました。IEEE 802.1sは、最終的にはIEEE 802.1Q仕様のサブセットになりました。

MSTPは、802.1Qを拡張して、VLANのグループを別のスパニングツリーに割り当てられるようにしたものです。インスタンスを選択して、適用可能な複数の論理パスにレイヤー2ネットワーク経路でマッチさせることができます。多くの場合、PVST+のようにVLANとインスタンスを1対1マッチングするのではなく、少数のインスタンスのみが必要です。

CiscoとProCurveの相互運用は、IEEE標準に従って行います。Cisco環境では、ネットワークで多くの場合PVST+を使用しています。そのため、まず、PVST+とMSTPの相互運用性について説明します。

## さまざまなスパニングツリーBPDU

| 1                                      | 802.1D<br>STP  | タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00  |  |             |  |        |  |  |        |        |         |  |
|--|----------------|---|--|-------------|--|--------|--|--|--------|--------|---------|--|
| 2                                      | 802.1w<br>RSTP | タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00  |  |             |  |        |  |  |        |        |         |  |
| 3                                      | 802.1s<br>MSTP | <table border="1"> <tr> <td>タグ無<br/>IEEE宛先MAC:<br/>01:80:c2:00:00:00</td> <th colspan="2">RSTPとMSTP共通</th> <th colspan="2">MSTP固有</th> </tr> <tr> <td></td> <td>CSTデータ</td> <td>ISTデータ</td> <td colspan="2">MSTIデータ</td> </tr> </table> | タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00 | RSTPとMSTP共通 |  | MSTP固有 |  |  | CSTデータ | ISTデータ | MSTIデータ |  |
| タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00 | RSTPとMSTP共通    |   | MSTP固有                                 |             |  |        |  |  |        |        |         |  |
|  | CSTデータ         | ISTデータ  | MSTIデータ                                |             |  |        |  |  |        |        |         |  |

PVST+とMSTPの相互運用性を理解するにあたって最も重要なポイントは、おそらく、それぞれで使用するMACアドレスと、MACアドレスが実際に使用される場合について理解することです。

この図は、特定のスパニングツリープロトコルに対応するスイッチ間の通信に使用されるスパニングツリー制御メッセージ(BPDU: Bridge Protocol Data Unit)の概要を示しています。複数のベンダーのスイッチ間で相互運用を行う場合には、宛先MACアドレスなどのBPDU形式が同じになっている必要があります。

最初のBPDUは、IEEE 802.1D-1998スパニングツリーフレームに基づいています。このBPDUはタグ無で、標準のMACアドレスを使用します。同様に、2番目のBPDUはRSTPに対応し、3番目のBPDUはMSTPに対応し、いずれもタグ無で、標準のMACアドレスを使用します。MSTP BPDUは、Common Spanning Tree(CST)インスタンス、およびMSTP固有インスタンスに関する情報も含んでいます。



## さまざまなスパニングツリーBPDU



4番目のBPDUは、Cisco PVST+フレームで使用される形式を示しています。PVST+ BPDUには3種類の形式があります。

1. CiscoのネイティブVLANの場合と同様に、VLANがタグ無であり、かつVLAN 1がトランクで許可されている場合は、ネイティブVLANはタグ無BPDUを許可します。このタグ無BPDU形式は、IEEE標準に準拠する、Cisco以外のすべてのデバイスが認識できるIEEE宛先MACを使用します。

## さまざまなスパニングツリーBPDU

|                      |   |   |                          |
|----------------------|---|---|--------------------------|
| 802.1D<br>STP        | タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00                    |   |                          |
| 802.1w<br>RSTP       | タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00                    |   |                          |
| 802.1s<br>MSTP       | タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00                    | RSTPとMSTP共通<br>CSTデータ                                       | MSTP固有<br>ISTデータ MSTIデータ |
| Ciscoトランク<br>でのPVST+ | 1. ネイティブVLANに対し<br>タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00 | 2. ネイティブVLANに<br>対してタグ無<br>Cisco宛先MAC:<br>01:00:0c:cc:cc:cd |                          |
|                      | CiscoトランクでVLAN 1が許可されている場合のみ                              |   |                          |

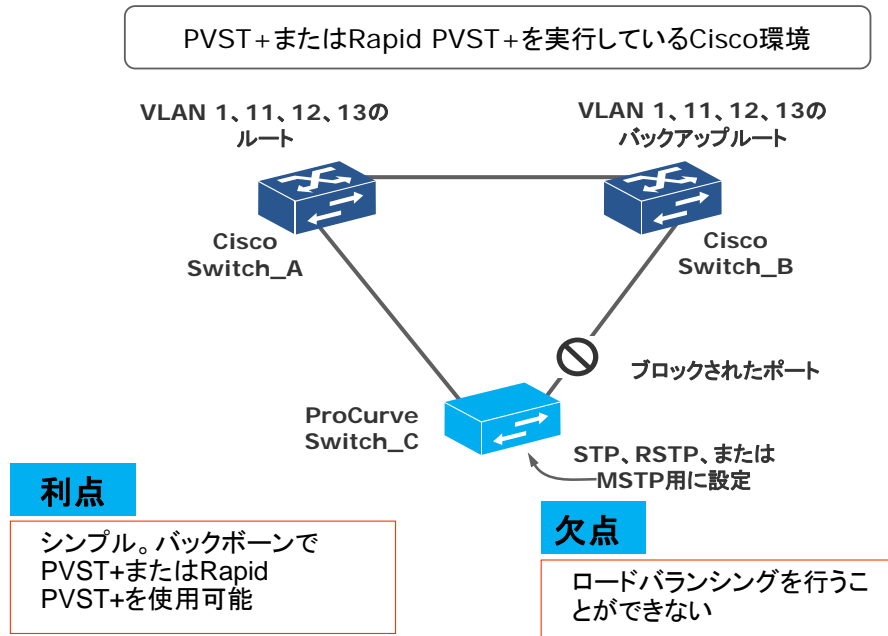
2. VLAN 1が許可されていない場合でも、BPDUはタグ無になりますが、Cisco形式のMACアドレスを使用します。この場合、ProCurveスイッチは、自身を宛先として認識しないので、このBPDUを認識できません。PVST+とIEEE標準のスパニングツリーを相互運用するには、トランクポートでVLAN 1を許可する必要があります。もちろん、ネイティブVLANが必要ですが、VLAN 1を許可する必要があります。

## さまざまなスパニングツリーBPDU

|                      |  |   |   |
|----------------------|--|---|---|
| 802.1D<br>STP        | タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00                     |   |   |
| 802.1w<br>RSTP       | タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00                     |   |   |
| 802.1s<br>MSTP       | タグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00                     | RSTPとMSTP共通<br>CSTデータ                                       | MSTP固有<br>ISTデータ<br>MSTIデータ                                 |
| Ciscoトランク<br>でのPVST+ | 1. ネイティブVLANに<br>対してタグ無<br>IEEE宛先MAC:<br>01:80:c2:00:00:00 | 2. ネイティブVLANに<br>対してタグ無<br>Cisco宛先MAC:<br>01:00:0c:cc:cc:cd | 3. その他のVLANに<br>対してはタグ付<br>Cisco宛先MAC:<br>01:00:0c:cc:cc:cd |
|                      | CiscoトランクでVLAN 1が許可されている場合のみ                               |   |   |

3. タグ付でトランクポートから送信されたPVST+ BPDUは、ProCurve機器が認識できないCisco形式のMACアドレスを使用します。ProCurveスイッチは、同じVLAN IDを持つタグ付ポートでこのようなBPDUを受信した場合、これをフォワーディングします。

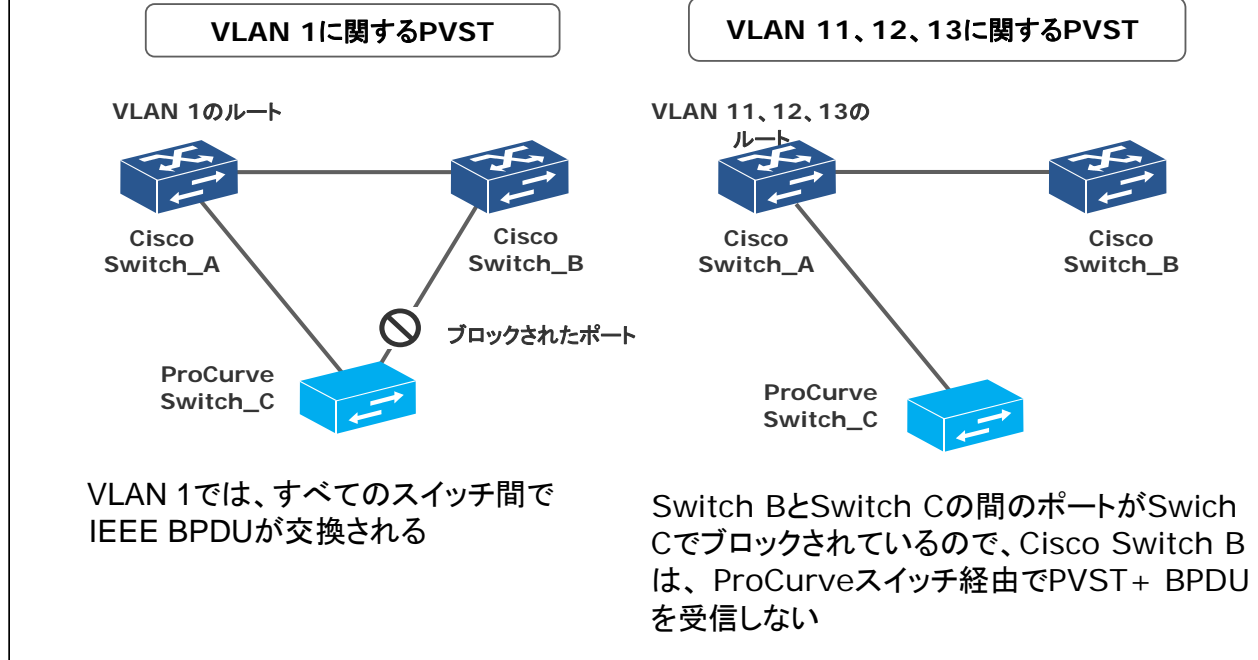
## Cisco-ProCurveのシナリオ1: Rapid PVST+



この図は、Ciscoスイッチ間でPVST+を使用している簡単なネットワークの例です。この例は、ロードバランシングに対応しません。ディストリビューションレイヤーにCiscoスイッチが2台あり、エッジにProCurveスイッチが1台あります。Switch\_Aが、すべてのVLANのルートになっており、Switch\_Bがバックアップルートになっています。

また上記には、この場合の利点と欠点も示しています。

## Cisco-ProCurveのシナリオ1: VLANとPVST



この図は、CiscoスイッチからみたVLANトポロジを示しています。1つはVLAN 1について、もう1つはその他すべてのVLANについて示しています。

VLAN 1では、標準のBPDUが交換されているので、ProCurveスイッチは標準のBPDUを認識し、そのポートの1つをブロック状態に設定しています。この例は、ProCurveがSTP、RSTP、またはMSTPを使用して動作していることを想定しています。どのスパニングツリープロトコルが実行されている場合でも、結果は同じになります。

この他のVLANに関しては、CiscoスイッチはProCurveスイッチからのすべてのBPDUできません。それはProCurveスイッチの右側のポートがブロックされており、ProCurveスイッチは通常の packets と同様にタグ付BPDUを送信しないためです。結果的に、Ciscoスイッチは、Ciscoスイッチ以外の他のネイバーを認識しません。Ciscoスイッチは、Ciscoスイッチ間でやり取りする以外のBPDUを受信しないので、どのリンクもブロックしません。

## Cisco機器でのRapid PVST+の設定

### 1 Rapid PVST+をグローバルに有効化

```
Cisco(config)# spanning-tree mode rapid-pvst
Cisco(config)# spanning-tree extend system-id
Cisco(config)# spanning-tree pathcost method long
```

### 2 ブリッジプライオリティを変更して、VLANごとにSTPルートの選択を調整

```
Cisco(config)# spanning-tree vlan 1,11-13 priority 4096
```

### 3 必要に応じて、VLANごとにインターフェイスコストを変更

```
Cisco(config)# interface gigabitethernet1/1
Cisco(config-if)# spanning-tree vlan 1,11-13 cost 10000
```

### 4 必要に応じて、VLANごとにインターフェイスプライオリティを変更

```
Cisco(config)# interface gigabitethernet1/1
Cisco(config-if)# spanning-tree vlan 1,11-13 port-priority 4
```

ここでは、CiscoスイッチにPVST+を設定する場合の詳細について説明します。

1. 最初のCLIコマンドは、スパニングツリーモードをRapid PVST+に設定して、このプロトコルを各VLANで使用できるようにするものです。  
2番目のCLIコマンドは、システムIDを拡張して、最大4096個のすべてのVLANを使用できるようにします。“spanning-tree pathcost method long” コマンドを実行すると、RSTPとMSTPで使用されているパスコストをスイッチが使用するようになります。
2. 各VLANで使用するプライオリティ値を指定しています。
- 3, 4. これらのコマンドは、インターフェイスコストとポートプライオリティ値の設定方法の例を示しています。

## Cisco Rapid PVST+ : トランクポートで送信されるBPDU

```
interface GigabitEthernet 1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,11-13
switchport mode trunk
```

タグ無VLAN 1のRSTP BPDU

タグ付VLAN 11、12、13の  
PVST+ BPDU

```
interface GigabitEthernet 1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 11-13
switchport mode trunk
```

タグ無VLAN 1およびタグ付VLAN  
11、12、13のPVST+ BPDU

VLAN 1がトランクポートで許可されていないとどうなるか?

VLAN 1がトランクポートで許可されていないと、IEEE BPDUが送信されない

この図は、PVST+をサポートしていないProCurve機器および他のベンダーの機器に影響を与えるBPDUフレーム形式を示しています。

以降の数ページでは、これについて説明します。

## Cisco Rapid PVST+: トランクポートで送信されるBPDU

```
interface GigabitEthernet 1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,11-13
switchport mode trunk
```

タグ無VLAN 1のRSTP BPDU

タグ付VLAN 11、12、13の  
PVST+ BPDU

Ciscoスイッチのトランクポートに関する最初のシナリオでは、ネイティブVLANがVLAN 1、許可されているVLANがVLAN 1、11～13です。VLAN 1では、Ciscoスイッチは、ProCurveスイッチが認識できる標準のRSTP BPDUをタグ無フレームとして送信します。

その他のVLAN 11～13では、Ciscoスイッチは、レイヤー2宛先アドレスとしてCisco MACアドレスを持つタグ付PVST+ BPDUを送信します。ProCurve機器は、このようなフレームを認識できません。



## Cisco Rapid PVST+: トランクポートで送信されるBPDU

```
interface GigabitEthernet 1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,11-13
switchport mode trunk
```

タグ無VLAN 1のRSTP BPDU

タグ付VLAN 11、12、13の  
PVST+ BPDU

```
interface GigabitEthernet 1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 11-13
switchport mode trunk
```

タグ無VLAN 1およびタグ付VLAN 11、  
12、13のPVST+ BPDU

Ciscoスイッチのトランクポートに関する2番目のシナリオでは、VLAN 1が許可されていません。VLAN 1は必ずしもネイティブVLANである必要はありません。CiscoトランクポートでVLAN 1を許可しない場合は、Ciscoスイッチは、タグ付PVST+ BPDUのみを送信し、標準のBPDUは送信しません。これにより、CiscoスイッチとProCurveスイッチの相互運用上の制約が発生することを防ぎます。

## Cisco Rapid PVST+: トランクポートで送信されるBPDU

```
interface GigabitEthernet 1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 1,11-13
switchport mode trunk
```

タグ無VLAN 1のRSTP BPDU



タグ付VLAN 11、12、13の  
PVST+ BPDU



```
interface GigabitEthernet 1/1
switchport trunk encapsulation dot1q
switchport trunk native vlan 1
switchport trunk allowed vlan 11-13
switchport mode trunk
```

タグ無VLAN 1およびタグ付VLAN  
11、12、13のPVST+ BPDU



VLAN 1がトランクポートで許可されていないと、IEEE BPDUが送信されない

標準のBPDUは、任意のVLAN番号のネイティブVLANで送信できることを思い出してください。ネイティブVLANでは、VLAN 1が許可されている限り、BPDUはIEEE標準に従います。ProCurveスイッチの動作に実際に関連する設定は、CiscoのネイティブVLANの設定と、VLAN 1の許可に関する設定です。

## Cisco Rapid PVST+: アクセスポートで送信されるBPDU

```
interface GigabitEthernet 1/20  
switchport access vlan 11  
switchport mode access
```

タグ無VLAN 11のRSTP BPDU



```
interface GigabitEthernet 1/20  
switchport access vlan 11  
switchport mode access  
switchport voice vlan 12
```

タグ無VLAN 11およびタグ付VLAN 12の  
PVST BPDU

ポートが音声VLAN用のタグ付でもある場合は、PVST+ BPDUのみが送信される

Ciscoスイッチのアクセスポートは、音声VLANを処理する設定になっていない限り、IEEE標準のBPDUを送信します。ポートをIP電話機用に設定した場合は、Ciscoは標準のBPDUを送信しなくなります。IP電話機用に設定したポートにはスイッチを接続しないので、通常、これは問題になりません。ベストプラクティスとしては、スイッチ間リンクを設定する場合にはトランクポートを使用します。このようにすれば、確実にIEEE標準のBPDUを送信できます。

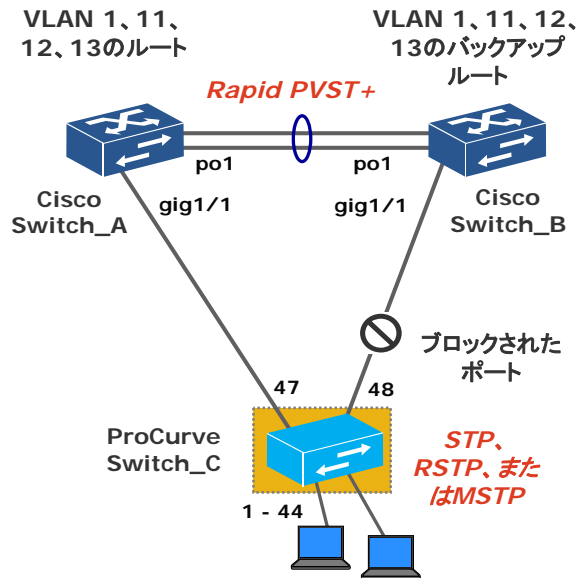
## Cisco-ProCurveのシナリオ1: ProCurveスイッチの設定

- Rapid PVST+用に設定されたCiscoスイッチ
- RSTP用に設定されたProCurveスイッチ

### ProCurve Switch\_Cの設定

```

vlan 1
 name "management"
 untagged 47-48
 ip address 10.1.1.1/24
vlan 11
 tagged 47,48
vlan 12
 tagged 47,48
vlan 13
 tagged 47,48
spanning tree
spanning tree 1-44 admin-edge-port
    
```



ここには、ProCurveスイッチの設定例を示します。Ciscoスイッチに接続しているポートは、VLAN 1でタグ無、およびVLAN 11、12、13でタグ付になっています。ProCurveスイッチではデフォルトでスパニングツリーが有効になっていないので、使用する場合はこれを有効にする必要があります。Ciscoスイッチでは、デフォルトで有効になっています。

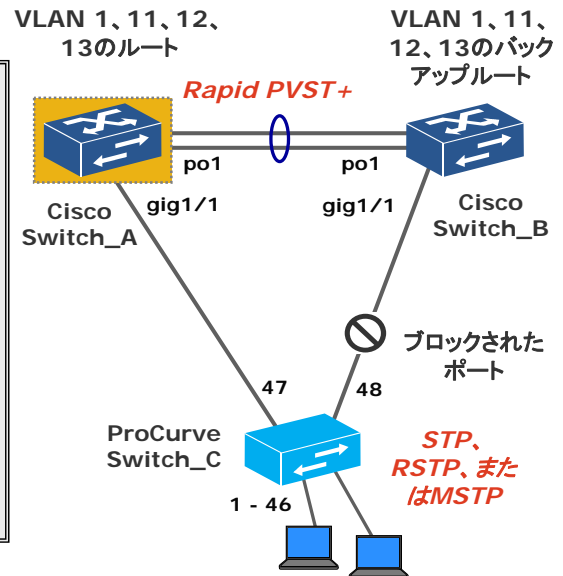
## Cisco-ProCurveのシナリオ1: Ciscoスイッチの設定

### Cisco Switch\_Aの設定

```
spanning tree mode rapid-pvst
spanning tree extend system-id
spanning tree pathcost method long
spanning tree vlan 1-4094 priority 0

interface Port-channel1
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,11-13
switchport mode trunk

interface GigabitEthernet1/1
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,11-13
switchport mode trunk
```



ここには、図の左側にあるCisco Switch\_Aの設定例を示しています。このスイッチは、すべてのVLANのルートに設定されています。

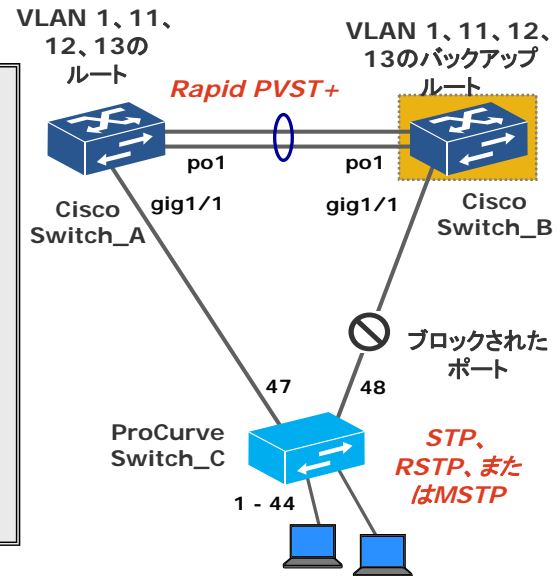
## Cisco-ProCurveのシナリオ1: Ciscoスイッチの設定(続き)

### Cisco Switch\_Bの設定

```
spanning tree mode rapid-pvst
spanning tree extend system-id
spanning tree pathcost method long
spanning tree vlan 1-4094 priority 4096

interface Port-channel1
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,11-13
switchport mode trunk

interface GigabitEthernet1/1
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,11-13
switchport mode trunk
```

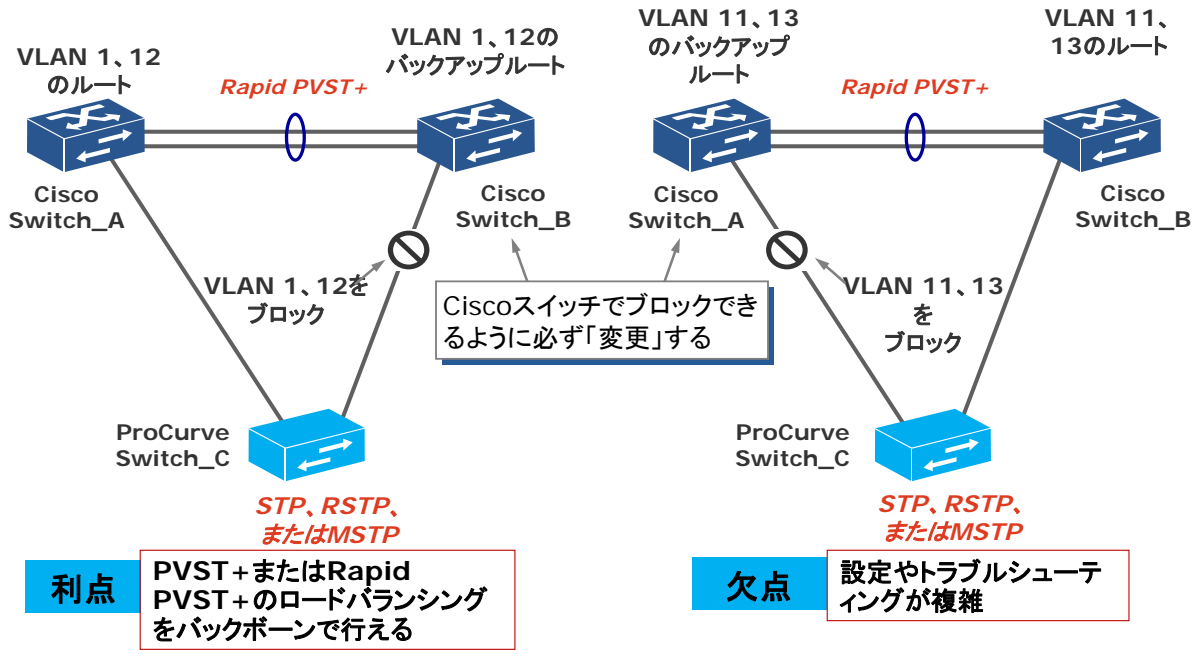


ここには、図の右側にあるCisco Switch\_Bの設定例を示しています。このスイッチは、Switch\_Aよりも高いプライオリティ値が設定されているので、すべてのVLANのバックアップルートに設定されます。

Ciscoスイッチのプライオリティ値は、ProCurveの従来のプライオリティと同様に0～32,768の間で設定できます。ProCurveスイッチでRSTPまたはMSTPを使用する場合、プライオリティ値は0～15の間で順に増加させることができます。ProCurveとCiscoのプライオリティをマッチさせるには、ProCurveのプライオリティ値に4,096を乗算します。たとえば、ProCurveでのプライオリティ1は、Ciscoでは4096になります。

。

## Cisco-ProCurveのシナリオ2: ロードバランシングを行う場合のRapid PVST+



この例は、CiscoスイッチとProCurveスイッチを設定してロードバランシングを行う方法を示しています。この例での最適な実装方法を理解するには、これまでに学んだ原則が役に立ちます。

ProCurveとCiscoの違いは、Ciscoスイッチではプライオリティ値の設定が異なる点のみです。適切にロードバランシングを行うには、ProCurveスイッチではブロックせず、Ciscoスイッチでブロックされるように設定する必要があります。Ciscoスイッチ側でブロックする理由は、Ciscoのバックアップルートが、ProCurveスイッチが使用するパス経由でPVST+ BPDUを受信できるようにするためです。

また、上記には、この例の場合の利点と欠点を示しています。ロードバランシングの詳細については、このコースの英語版Webトレーニングに含まれる『ProCurve and Cisco Network Interoperability Training guide』を参照してください。

## MSTPの実装

### ✓ PVST+の実装

### MSTPの実装

- 概念と動作の復習
- グローバル設定
- MSTPインスタンスへのVLANの割り当て
- CiscoスイッチとProCurveスイッチの設定

### MSTPの相互運用性と互換性

### Spanning Tree Hardening

これまでに、PVST+の実装について説明しました。次に、MSTPの実装について説明します。

CiscoとProCurveの相互運用性は、IEEE標準に従うことによって実現できます。しかし、Cisco環境では、多くの場合、ネットワークでPVST+を使用しています。CiscoとProCurveの両方のデバイスでIEEE標準を使用する場合は、標準ベースのモデルに従うことを推奨します。ただし、設定に関していくつかの点を考慮する必要があります。



## MSTリージョン

複数のスパニングツリーインスタンスを集合的に定義するスイッチのグループは、**MSTリージョン**と呼ばれる

- 各スイッチは1つのリージョンのみに所属できる

設定属性が同じスイッチは、同じMSTPリージョンに所属する

- MST設定名 (32バイト、大文字小文字を区別)
- MST リビジョン番号 (2バイト)
- 対応するVLAN割り当てがあるMSTインスタンス

スイッチは、以下のスイッチからBPDUを受信するとリージョン境界を定義する

- 設定属性が異なるMSTPスイッチ
- STPまたはRSTPスイッチ

### MSTPの設定例

```
設定名 = "PCU"  
リビジョン番号 = 1  
インスタンス1 = VLAN 1、12  
インスタンス2 = VLAN 11、13
```

MSTPは、同じMSTP設定を持つ1つ以上のスイッチで構成されるリージョンという考え方に基づいています。MSTPでは、受信するMST BPDUの内容に基づいてMSTリージョンの境界をダイナミックに判断します。すべてのMSTスイッチは、VLANとスパニングツリーインスタンスを関連付けるテーブルのメッセージダイジェストを作成し、そのダイジェストをBPDUで送信します。BPDUを受信すると、MSTが有効になっているスイッチがダイジェストを抽出して、送信されたダイジェストと自身のダイジェストを比較します。名前とダイジェストが一致した場合は、BPDUを送信したスイッチは、そのBPDUを受信したスイッチと同じリージョンの一部となります。名前とダイジェストが一致しない場合は、これらのスイッチは異なるリージョンに所属することになります。このときの、トランザクションに関与するポートは、リージョン間の境界と見なされます。

## MSTインスタンス

**各MSTインスタンス(MSTI)には1つ以上のVLANが含まれる**

- インスタンスとVLAN間のマッピングは、ある特定のMSTPリージョンにあるスイッチ間で同じになっている必要がある

**1つのMSTPリージョンに、最大16個のMSTIを定義可能**

**Internal Spanning Tree (IST) インスタンスには、他のインスタンスに割り当てられていない1~4094のすべてのVLANが含まれる**

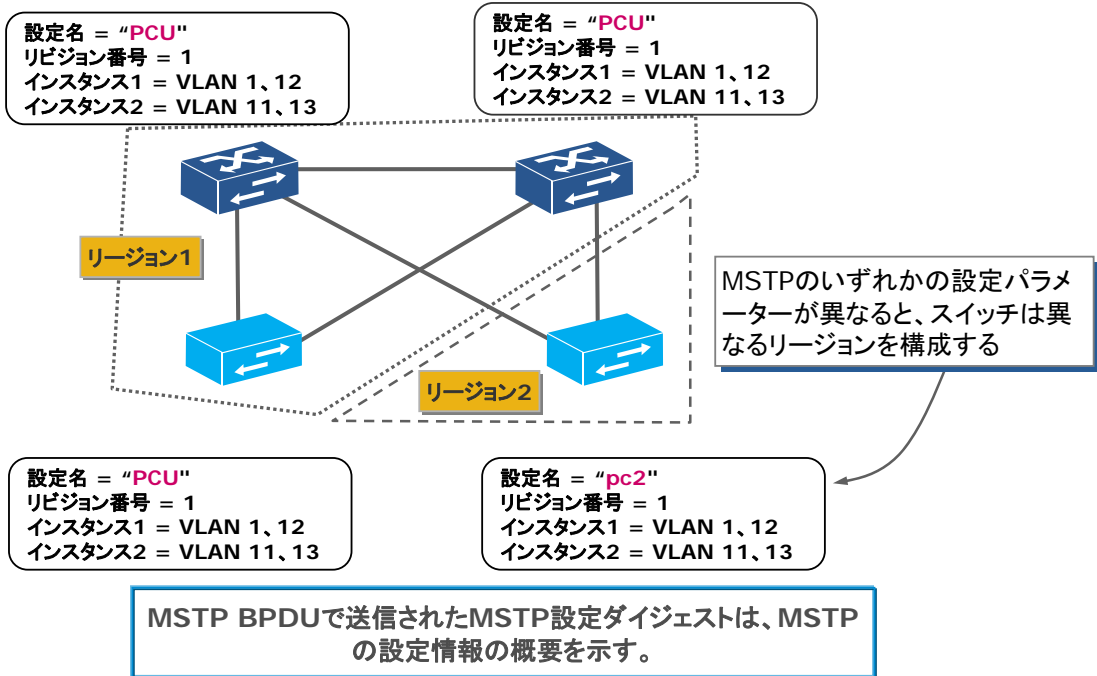
- ISTインスタンスは、「デフォルトの」インスタンスとして機能する

**MSTIから削除されたVLANは、ISTインスタンスに割り当てられる**

MSTP を有効にするとすぐに、スイッチに設定されたすべてのVLANは、MSTPリージョン内に存在するRSTPインスタンスであるIST (Internal Spanning Tree) の一部となります。新しいインスタンスを追加してVLANに関連付けると、そのVLANはISTから削除されます。ただしISTは、明示的にマッピングされているVLANがない場合でも削除されません。

ほとんどの場合、ユーザー定義のVLANは、MSTPリージョン内のすべてのスイッチで同様に設定されたユーザー定義のインスタンスに関連付けられます。デフォルトVLAN (VLAN ID 1) は、常にISTに関連付けられています。これにより重要な利点を得られます。つまり、VLANからインスタンスへのマッピングの設定が間違っても、ISTとVLAN 1の関連付けがあることによって接続性が完全には失われないため、スイッチにアクセスすることができます。

## MSTリージョンの例



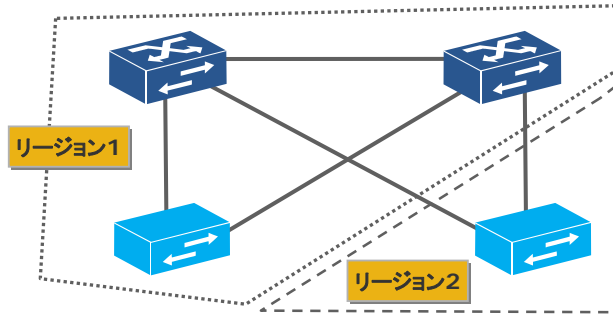
この図は、2つのMSTリージョンがある場合の例を示しています。リージョン1は以前から存在し、MSTリージョンが正しく設定されています。リージョン2は、誤って他のスイッチと異なる設定名を指定したために作成されたものです。MSTの設定名では、大文字小文字が区別されます。

## 確認テスト

以下の設定名には問題があります。正しい設定名は何ですか？

設定名 = "PCU"  
リビジョン番号 = 1  
インスタンス1 = VLAN 1, 12  
インスタンス2 = VLAN 11, 13

設定名 = "PCU"  
リビジョン番号 = 1  
インスタンス1 = VLAN 1, 12  
インスタンス2 = VLAN 11, 13



設定名 = "PCU"  
リビジョン番号 = 1  
インスタンス1 = VLAN 1, 12  
インスタンス2 = VLAN 11, 13

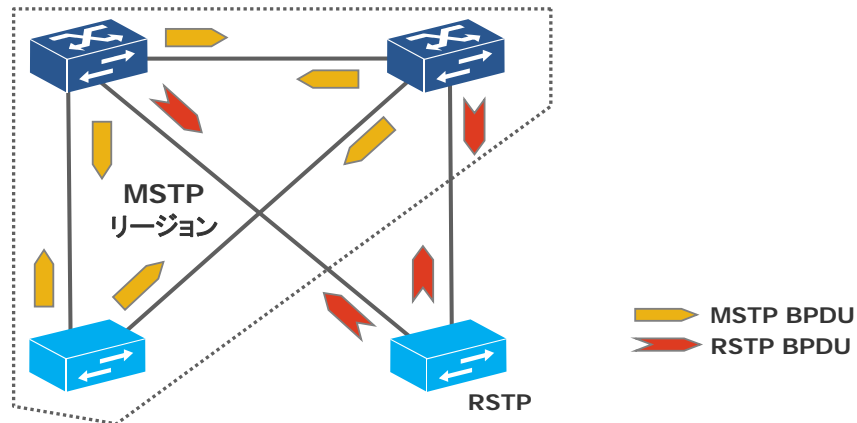
設定名 = "pc2"  
リビジョン番号 = 1  
インスタンス1 = VLAN 1, 12  
インスタンス2 = VLAN 11, 13

## 確認テストの解答

正解: PCU (大文字小文字を区別する)

## MSTP BPDU

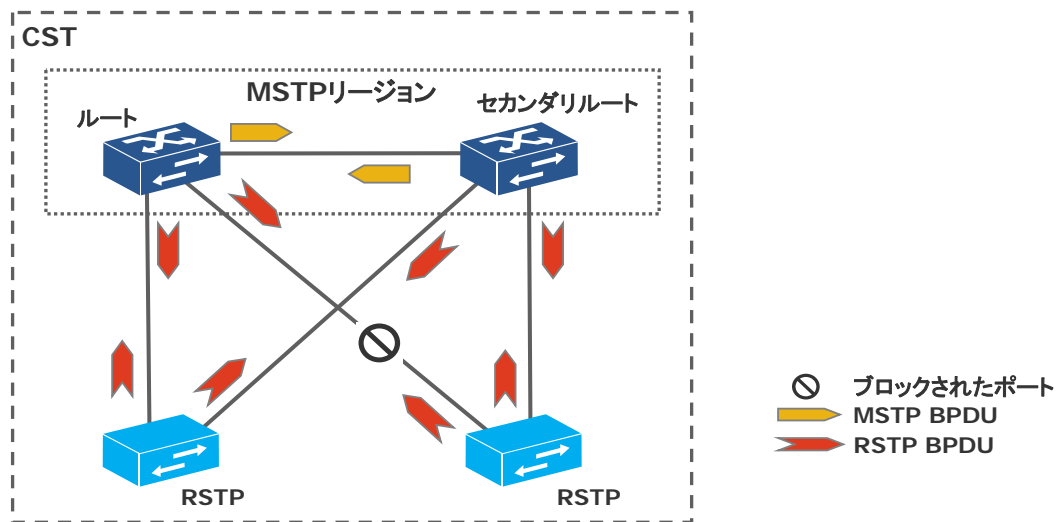
- MSTPリージョンでは、MSTP BPDUが交換される
- MSTPリージョン外では、ISTインスタンスの設定を特定するRSTP/STP BPDUが送受信される



MSTPリージョン内では、そのリージョンのメンバーになっているスイッチ間でMSTP BPDUが交換されます。MSTPリージョン外では、ISTインスタンスの設定を特定するRSTPまたはSTP BPDUが送受信されます。MSTのメンバーとRSTPまたはSTP BPDUを交換するリンクがMST境界です。

## CSTの機能

- CSTは、ブリッジされたLAN内のRSTP/STPスイッチとMSTPリージョン間のスパニングツリーを管理する
- MSTPリージョン外のCSTでは、IST設定が使用される



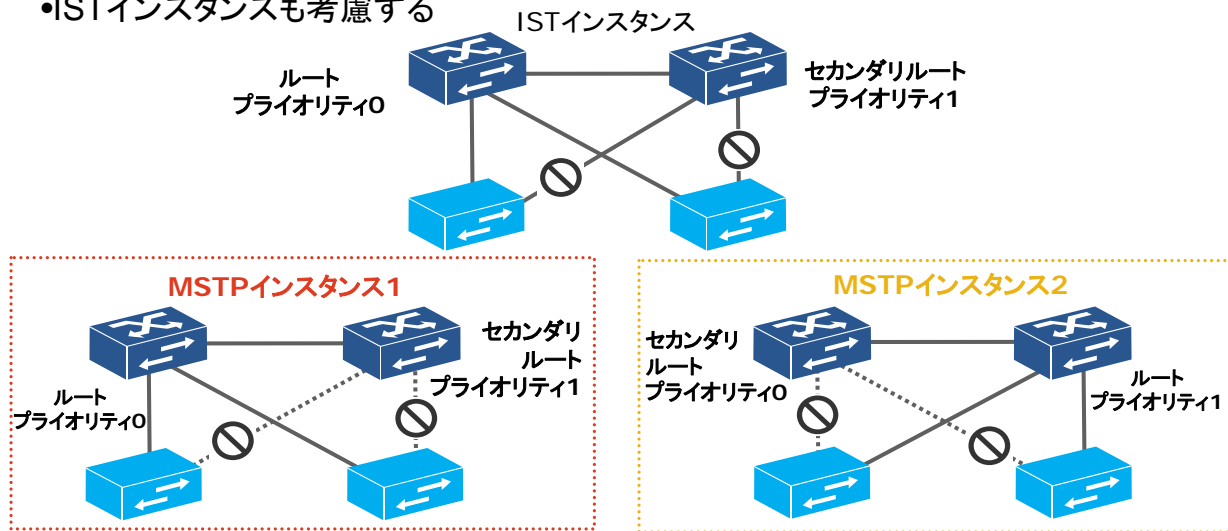
Common Spanning Tree (CST)機能は、MSTP、STP、およびRSTPを相互運用できるようにします。通常、CSTは、STPとRSTPを実行しているスイッチから受信したBPDUを基に、ISTとシングルスパニングツリー (SST)ドメインから構成されます。このようにして、CSTは、すべてのISTインスタンスとすべてのSSTドメイン間にループのないパスを1つ作成します。

この例では、上部の2つのスイッチが1つのMSTPリージョンを構成し、MSTP BPDUを交換しています。下部の2つのスイッチではRSTPが実行されており、上部のスイッチがMSTPを実行していることを認識しません。下部の2つのスイッチは、RSTPを実行している別のスイッチとしてこれらのMSTPスイッチを認識します。

## プライオリティの設定: ISTとMSTインスタンス

ロードバランシングを効果的に行うには、コアスイッチとディストリビューションスイッチ間のMSTインスタンスに割り当てたプライオリティを変更

- ISTインスタンスも考慮する

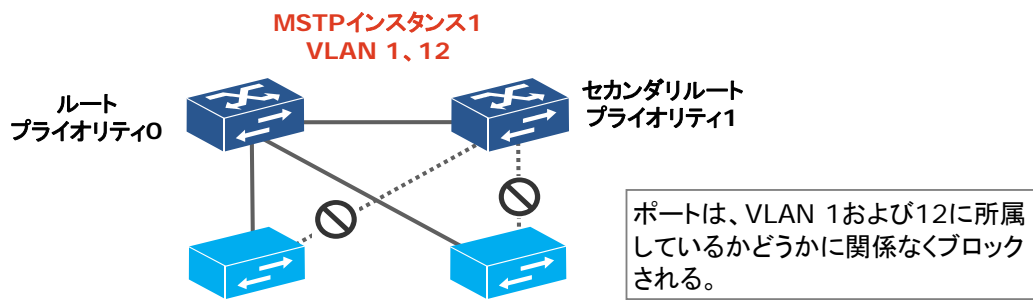


すべてのスイッチがMSTPを実行しているネットワーク環境でMSTPのロードバランシング機能を活用するには、適切な設定が必要です。まず、別のVLANトポロジを構成するための冗長リンクがネットワークに必要です。また、別のMSTインスタンスを設定して、それぞれに別のVLANグループを割り当てる必要があります。このプロセスの一環として、同じMSTリージョン内のコアスイッチまたはディストリビューションスイッチには別々のプライオリティを割り当てます。ISTインスタンスにも同様の方法でプライオリティを設定する必要があります。



## MSTPがVLAN設定を認識しているかどうか?

MSTPは、VLANポートの設定に関係なく各インスタンスにトポロジを作成。ポートは、あるインスタンスのルートポートまたは代替ポートになる。これは、このインスタンスのVLANに所属しているかどうかには関係しない。

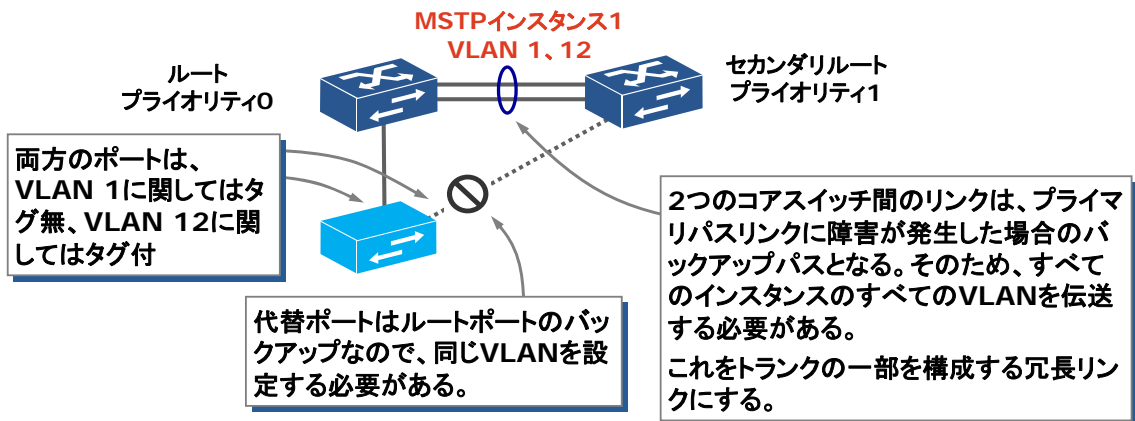


MSTPは、VLANポートの設定に関係なく各インスタンスにトポロジを作成します。ポートは、ある1つのMSTインスタンスのルートポートまたは代替ポートになります。これは、このポートが、このインスタンスのVLANに所属しているかどうかには関係しません。

## 冗長パスのあるネットワークでのVLANの設定

基本ルール:

- バックアップパスにあるリンクでは、バックアップ対象のパスと同じVLANを伝送する必要がある。
- つまり、代替ポートのVLANは、ルートポートと同様に設定する。

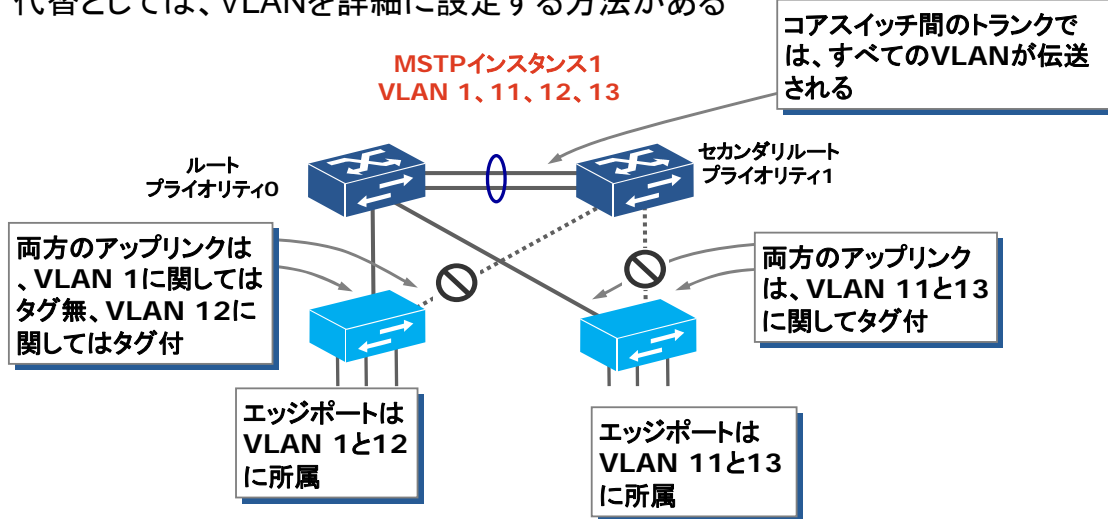


MST環境を適切に設定するには、ブロックされていないポートで特定のVLANを伝送できるようにします。トポロジの変更が発生してバックアップポートがアクティブになった場合の設定も同様に行います。

## 冗長パスのあるネットワークでのVLANの設定(続き)

すべてのリンクですべてのVLANにタグ付けするのが簡単な方法

- ブロードキャストドメインがネットワーク全体に及んでしまう欠点がある
- 代替としては、VLANを詳細に設定する方法がある

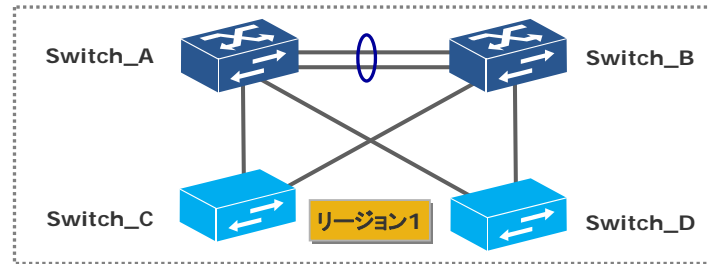


MSTリージョンに影響するさまざまなネットワーク障害に備えて確実にすべてのアクティブ/バックアップリンクを設定するには、すべてのリンクのすべてのVLANにタグ付けします。これは簡単な方法ですが、ブロードキャストドメインがネットワーク全体に及んでしまう欠点もあります。代替として、VLANを詳細に設定する方法がありますが、これにはさまざまなリンク障害を想定する必要があるので時間がかかります。

## 新しいVLANの定義

VLANを定義しただけでは、MSTP設定ダイジェストが変更されず、スイッチは、そのMSTPリージョン内でのみ認識される。

- 特定のMSTPインスタンスに割り当てられていないすべてのVLAN(1~4094)は、未定義のVLANも含め、デフォルトでISTインスタンスにマッピングされる。



VLAN 14を定義する前

MST設定名 = "PCU"  
MSTリージョン番号 = 1  
MSTインスタンス1 = VLAN 1, 12  
MSTインスタンス2 = VLAN 11, 13  
ISTインスタンス = VLAN 2~10, 14~4094

VLAN 14を定義してから変更を行っていない

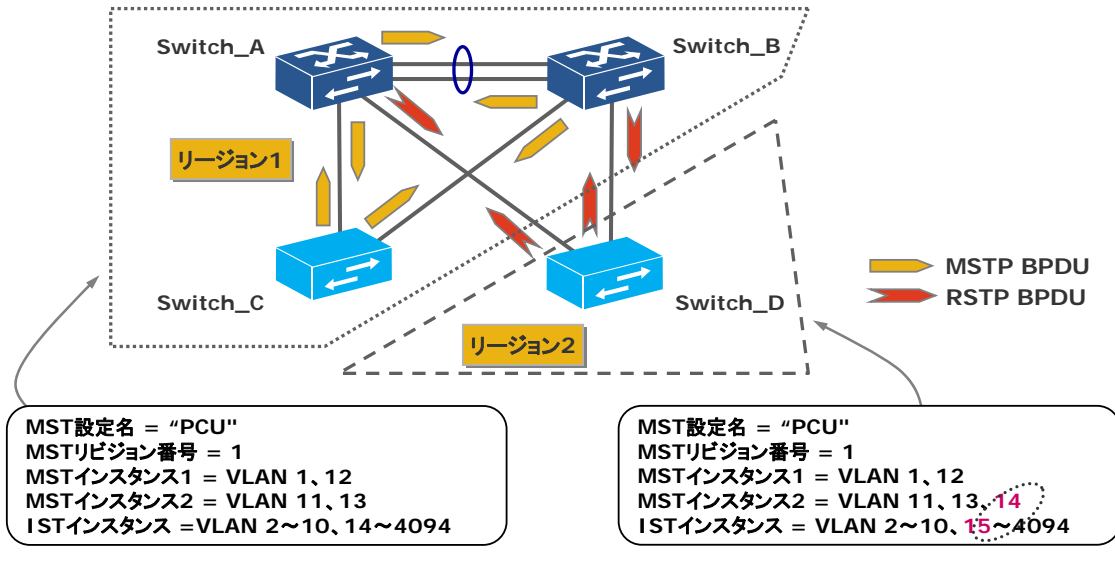
MST設定名 = "PCU"  
MSTリージョン番号 = 1  
MSTインスタンス1 = VLAN 1, 12  
MSTインスタンス2 = VLAN 11, 13  
ISTインスタンス = VLAN 2~10, 14~4094

ここでは、MSTPを実行しているスイッチに新しいVLANを定義する場合を考えます。直接の影響はどのようなものでしょうか。VLANを定義しただけでは、MSTP設定ダイジェストは変更されず、スイッチは、そのMSTPリージョン内でのみ認識されます。これには2つの理由があります。1つは、特定のMSTPインスタンスに割り当てられていないすべてのVLAN(1~4094)が、デフォルトでISTインスタンスにマッピングされることです。これには、スイッチにまだ定義されていないVLANも含まれます。もう1つの理由は、このVLANが特定のVLANインスタンスにまだ割り当てられていないことです。

この図の例では、上記の4つのスイッチそれぞれにVLAN 14が定義されています。showコマンドを実行すると、ISTインスタンスにはVLAN 14がありますが、MSTインスタンスにはVLAN 14が含まれていないことを確認できます。

## MSTインスタンスへのVLANの割り当て

スイッチ上でMSTインスタンスにVLANが割り当てられると、そのスイッチは別のMSTPリージョンになり、トラフィックが短時間中断される

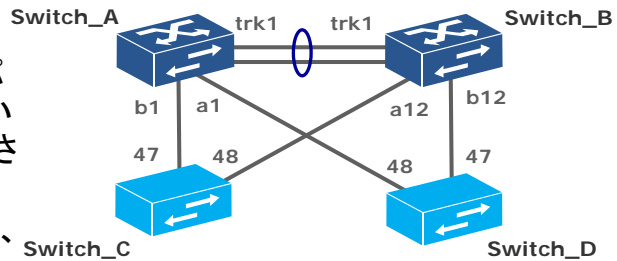


ネットワーク管理者としてこの新しいVLANを実装する場合は、MSTPに関して必要な変更をスイッチに1つずつ設定する必要があります。もちろん、起動用の設定を準備しておくこともできますが、必ずしもすべてのスイッチを一度に起動することはできません。

この図では、Switch\_D上でMSTインスタンス2にVLAN 14が割り当てられていますが、この変更は、他のスイッチにはまだ適用されていません。その結果、Switch\_Dは新しいリージョン(リージョン2)に所属しています。これにより、Switch\_Dは、Switch\_AおよびSwitch\_BとRSTP BPDUを交換するようになります。この状態に移行するには、通常、数秒かかります。

## スパニングツリーとLLDP

- LLDPパケットは、ポートのスパニングツリーがブロックされているかどうかに関係なく、送受信される
- すべてのレイヤー2ネイバーは、LLDPで検出できる



```
Switch_A# show lldp info remote
LocalPort SysName
-----
trk1      Switch_B
a1        Switch_D
a2        Switch_C
```

```
Switch_B# show lldp info remote
LocalPort SysName
-----
trk1      Switch_A
a12       Switch_C
b12       Switch_D
```

```
Switch_C# show lldp info remote
LocalPort SysName
-----
47        Switch_A
48        Switch_B
```

```
Switch_D# show lldp info remote
LocalPort SysName
-----
47        Switch_B
48        Switch_A
```

ここでは、最後に、LLDPがSTP、RSTP、MSTPと連携する方法について説明します。他のすべての「データ」パケットとは異なり、LLDPパケットはブロックされたポートで送受信されます。そのため、スイッチのLLDPテーブルには、他のすべての隣接スイッチが表示されています。隣接スイッチに関する情報のみを持つSTP、RSTP、またはMSTPとは、この点が異なります。

## MSTPの一般的な設定手順

### MSTPを設定する場合に推奨される手順

1. 必要なVLANを作成する
2. MSTPに対してスパニングツリープロトコルを有効にする
3. リージョンパラメーターを定義する
  - 設定名、リビジョン番号、インスタンス
4. プライオリティを設定して、各MSTインスタンスのルートおよびセカンダリルートを定義する
5. アップリンクポートとエッジポートの特性を設定する
6. スパニングツリーを有効にする
7. 冗長ケーブルを接続する

MSTPでは、VLANを異なるインスタンスに割り当てることで、冗長リンクを使用できるようにします。MSTPは、VLANを認識するスパニングツリーを簡単に設定できるようにしますが、帯域幅と冗長リンクを効率的に使用できるようにするには、慎重なプランニングが必要となります。効率的なMSTP設定を行うには、まず基本的な方針として、上記の手順に従います。

## Cisco機器でのMSTPの設定

すべてのCiscoスイッチで以下を実行:

- MSTPを有効にする

```
Cisco(config)# spanning-tree mode mst
```

- 1つのMSTPリージョンを使用する場合の一般的な設定を行う

```
Cisco(config)# spanning-tree mst configuration
Cisco(config-mst)# instance 1 vlan 1,12
Cisco(config-mst)# instance 2 vlan 11,13
Cisco(config-mst)# name PCU-building-1
Cisco(config-mst)# revision 1
```

### IEEE 802.1s-2002標準への準拠方法:

IEEE 802.1s-2002標準に準拠するには、以下に示すバージョン以降のソフトウェアをCiscoスイッチで実行

- Cisco Catalyst 2950、3550、3560、3750: IOS 12.2(25)SEC
- Cisco Catalyst 4000: native IOS 12.2(25)SG
- Cisco Catalyst 6000:native IOS 12.2(18)SXFまたはCatOS 8.3

ここでは、CiscoスイッチにMSTPを設定する方法の詳細について説明します。Ciscoスイッチがネットワークで正常に稼動しており、必要とするすべてのVLANが設定されていることを前提とします。

まずはじめに、スパニングツリーモードをMSTPに設定します。次に、MSTの設定(MSTの設定名、リビジョン番号、およびVLANとMSTインスタンスのマッピング情報)を定義します。



## Cisco機器でのMSTPの設定(続き)

- ブリッジプライオリティを変更して、MSTインスタンスごとにルート選択を調整

```
Cisco(config)# spanning-tree mst <instance-id> priority 4096
```

- 必要に応じて、MSTインスタンスごとにインターフェイスコストを変更

```
Cisco(config)# interface gigabitethernet1/1  
Cisco(config-if)# spanning-tree mst 1 cost 10000
```

- 必要に応じて、MSTインスタンスごとにインターフェイスのプライオリティを変更

```
Cisco(config)# interface gigabitethernet1/1  
Cisco(config-if)# spanning-tree mst 1 port-priority 4
```

先に説明したCisco PVST+の設定方法と同様に、MSTPの場合もコアスイッチまたはディストリビューションスイッチにブリッジプライオリティの設定が必要です。当然、CLIのコマンド構文は異なりますが、最も重要な違いは、PVST+ではVLANインスタンスを個別に設定するのに対し、MSTPではMSTインスタンスごとにブリッジプライオリティを設定する点です。

また、インターフェイスコストとインターフェイスプライオリティをMSTインスタンスごとに設定することも可能です。

## Cisco機器でのMSTPの設定(続き)

エンドユーザーインターフェイスで必要なSTPエッジポート(portfast)を有効にする

- トランクポート以外のポートに対してグローバルに設定

```
Cisco(config)# spanning-tree portfast default
```

- または、インターフェイスごとに設定

```
Cisco(config)# interface gigabitethernet0/2  
Cisco(config-if)# spanning-tree portfast default
```

グローバルコンフィギュレーションレベル、またはインターフェイスごとに、portfast設定を適用して、エンドユーザーのポートをエッジポートに設定します。

## ProCurve機器でのMSTPの設定

すべてのProCurveスイッチで以下を実行:

- VLANおよびタグアップリンクを作成(まだ作成していない場合)

```
Switch(config)# vlan 11 tagged 47,48  
Switch(config)# vlan 12 tagged 47,48  
Switch(config)# vlan 13 tagged 47,48
```

この図は、ProCurveスイッチでMSTPを設定する場合のCLIコマンドを示しています。これらのコマンドは、VLANを定義する基本的なコマンドですが、Ciscoスイッチのみの環境にProCurveを導入する場合の参考のために記しています。ProCurveスイッチで実行する必要があるその他の準備手順に加え、ネットワークで使用するVLANを定義して、そのVLANのアップリンクに対してタグ付けを設定する必要があります。

## ProCurve機器でのMSTPの設定(続き)

すべてのProCurveスイッチで以下を実行:

- VLANおよびタグアップリンクを作成(まだ作成していない場合)

```
Switch(config)# vlan 11 tagged 47,48
Switch(config)# vlan 12 tagged 47,48
Switch(config)# vlan 13 tagged 47,48
```

- 使用するプロトコルとしてMSTPを設定(デフォルトのSTPプロトコルになっていない場合)

```
Switch(config)# spanning-tree protocol-version mstp
Switch(config)# reload
```

- MSTPグローバルコンフィギュレーションパラメーターを定義

```
Switch(config)# spanning-tree config-name "PCU-building-1"
Switch(config)# spanning-tree config-revision 1
```

比較的新しいProCurveスイッチ(Switch 8200zl、5400zl、3500yl、6200ylシリーズなど)では、MSTPがデフォルトのスパニングツリープロトコルになっています。そのため、ここに示すコマンドを実行して、スイッチで稼働させるスパニングツリープロトコルとしてMSTPを設定する必要はありません。

次に、MSTPの設定パラメーターを設定して、Ciscoスイッチでの定義と正確にマッチさせる必要があります。MSTの設定名とリビジョン番号に関する設定を上記に示しています。MST設定名は大文字小文字を区別するので注意してください。

## ProCurve機器でのMSTPの設定(続き)

すべてのProCurveスイッチで以下を実行:

- MSTインスタンスにVLANをマッピング

```
Switch(config)# spanning-tree instance 1 vlan 1,11  
Switch(config)# spanning-tree instance 2 vlan 12-13
```

- MSTPの設定を確認

```
Switch(config)# show spanning-tree mst-config
```

MSTの設定手順には、各MSTインスタンスにVLANを割り当てる設定も含まれます。前述したように、各MSTインスタンスには、複数のVLANを割り当てることはできませんが、1つのVLANには、1つのMSTインスタンスしか割り当てることはできません。

ProCurveスイッチでMSTPの設定を確認するには、`show spanning-tree mst-config`コマンドを実行します。

## ProCurveでのプライオリティの設定: ProCurve機器 がコアにある場合の例

Switch\_AがISTインスタンスのルートである場合

```
Switch(config)# spanning-tree priority 0
```

Switch\_AがMSTI 1のルート、およびMSTI 2のセカンダリルートである場合

```
Switch(config)# spanning-tree instance 1 priority 0  
Switch(config)# spanning-tree instance 2 priority 1
```

---

Switch\_BがISTインスタンスのセカンダリルートである場合

```
Switch(config)# spanning-tree priority 1
```

Switch\_BがMSTI 2のルート、およびMSTI 1のセカンダリルートである場合

```
Switch(config)# spanning-tree instance 1 priority 1  
Switch(config)# spanning-tree instance 2 priority 0
```

上記のCLIコマンドは、コアに配置した2台のProCurveスイッチにMSTPを設定する方法を示しています。コアにある場合は、Ciscoスイッチに関して前述したように、インスタンス間にロードバランシングを設定するには、ISTおよびMSTPプライオリティ値を設定します。

## ProCurve機器でのポートの設定

スイッチ間のアップリンクは、**非エッジかつポイントツーポイント**に設定する必要がある

ここでは、ProCurveスイッチがネットワークのエッジに導入され、Ciscoスイッチがコアにある場合のシナリオに戻ります。この場合、ProCurveスイッチで、アップリンクとエンドノードポートにMSTPを設定する方法を考慮する必要があります。

ProCurveスイッチでは、スイッチ間のアップリンクは、非エッジかつポイントツーポイントに設定する必要があります。その一方、エンドノードに接続するアクセスポートまたはエッジポートは、エッジかつポイントツーポイントに設定する必要があります。

## ProCurve機器でのポートの設定

スイッチ間のアップリンクは、**非エッジ**かつ**ポイントツーポイント**に設定する必要がある。

エンドノードに接続するアクセスポートまたはエッジポートは、**エッジ**かつ**ポイントツーポイント**に設定する必要がある。

ProCurveスイッチ(バージョンK.12.04以降)では、デフォルトですべてのポートがMSTP自動エッジモードで動作。

- 以下を指定するのと同様の設定

```
Switch(config)# spanning-tree <port-list> auto-edge-port
```

- エッジポートの自動定義をサポート — ポートはBPDUの有無を3秒間チェックし、ない場合は、パケットのフォワーディングを開始
- 必要に応じて、以下を実行して、ポートが直ちにフォワーディングモードに移行するように設定可能

```
Switch(config)# spanning-tree <port-list> admin-edge-port
```

バージョンK.12.04以降のソフトウェアを実行しているProCurveスイッチ(Switch 8200zl、5400zl、3500yl、6200ylシリーズ)では、デフォルトですべてのポートがMSTP自動エッジモードで稼働します。これは、spanning-tree <port-list> auto-edge-portコマンドを実行した場合と同じ設定です。

自動エッジポートの設定により、エッジポートが自動検出されます。つまり、ポートはBPDUの有無を3秒間チェックし、BPDUがない場合は、パケットのフォワーディングを開始します。必要に応じて、spanning-tree <port-list> admin-edge-portコマンドを実行すると、ポートが直ちにフォワーディングモードに移行するように設定できます。



## ProCurve機器でのポートの設定: バージョンK.12.04 より前の場合

バージョンK.12.04より前のソフトウェアを実行しているProCurveスイッチでは、デフォルトですべてのポートがMSTPの非エッジモードで動作

- 以下を指定するのと同様の設定

```
Switch(config)# no spanning-tree <port-list> edge-port
```

すべてのエンドユーザーポートもエッジポートに設定する必要がある。これはCiscoでの *portfast* の設定に相当

- 以下のコマンドを実行

```
Switch(config)# spanning-tree <port-list> edge-port
```

このスライドは、K.12.04より前のバージョンのソフトウェアを使用する場合のCLIコマンド構文の違いを示しています (Switch 8200zl、5400zl、3500yl、6200ylシリーズでサポート)。

K.12.04より前のバージョンのソフトウェアを実行しているスイッチでは、デフォルトですべてのトランクポートとエンドユーザーポートがMSTP非エッジモードで動作します。エンドユーザーポートをエッジポートに設定するには、`spanning-tree <port-list> edge-port` コマンドを実行します。

## ProCurveがサポートするスパニングツリーのバージョン

|  | 802.1D-1998 STP  | 802.1D (802.1w) RSTP  | 802.1Q (802.1s) MSTP                             |
|--|--|---|--|
| 1600M<br>2424M<br>4000M<br>8000M                               | Yes<br>(デフォルト)   | No  | No   |
| 2500<br>4100gl   | Yes<br># span protocol-version stp<br>(リポートが必要)  | Yes<br>(デフォルト)  | No   |
| 2600<br>2800<br>3400cl<br>6400cl<br>5300xl                     | Yes<br># span protocol-version stp<br>(リポートが必要)  | Yes<br>(デフォルト)  | Yes<br># span protocol-version mstp<br>(リポートが必要) |
| 2510<br>2810<br>4200vl<br>3500yl<br>6200yl<br>5400zl<br>8200zl | Yes<br># span force-version stp-compatible<br># span legacy-path-cost<br>(デフォルトのポートロールを適用) | Yes<br># span force-version stp-compatible<br>(デフォルトのポートロールを適用) | Yes<br>(デフォルト)                                   |
| デフォルトのSTP<br>ポート<br>ロール  | no mode fast   | edge-port   | no edge-port (旧)<br>auto-edge (新)                |

この表には、さまざまなProCurveスイッチファミリーでのデフォルトのスパニングツリープロトコルのバージョンをまとめています。一番下の行には、それぞれのスパニングツリープロトコルのバージョンに対応するデフォルトのスパニングツリーポートロールを示しています。

一部のスイッチでは、デフォルトのスパニングツリープロトコルを変更したり、下位互換モードで動作させることができます。

ProVision ASICスイッチでは、デフォルトでMSTPが有効です。

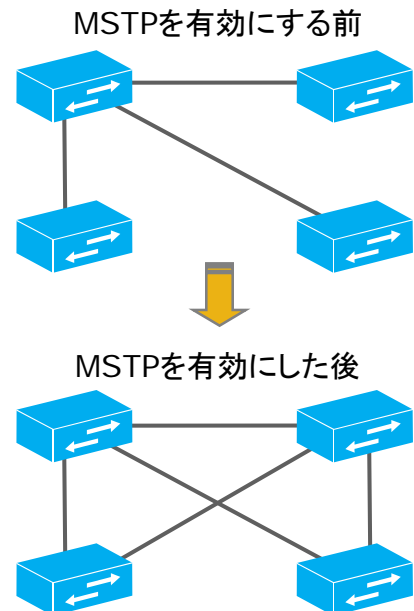
## MSTPの有効化

すべてのスイッチで以下を実行

- スパニングツリーを有効にする

```
Switch(config)# spanning-tree
```

- 冗長ケーブルを接続する
- MSTPステータスを確認してテストする



MSTPを実装する最後の手順では、スパニングツリーを有効にして、冗長ケーブルを接続し、MSTPの設定を確認およびテストします。設定したスパニングツリーを「オンにする」には、ProCurveスイッチでspanning-treeコマンドを実行します。

## ProCurve機器でのMSTP設定の確認

```
Switch# show spanning-tree mst-config
MST Configuration Identifier Information
MST Configuration Name : PCU-building-1
MST Configuration Revision : 1
MST Configuration Digest : 0x2DC307C6A31621DC6311050884E69C4E
IST Mapped VLANs : 1
Instance ID Mapped VLANs
-----
1          1,12
2          11,13
```

ISTインスタンスには、他のMSTPインスタンスに割り当てられていない1～4094のすべてのVLANが含まれる

•これには、定義済みおよび未定義のVLANが含まれるが、コマンド出力には定義済みVLANのみが表示される

ここには、ProCurveスイッチでshow spanning-tree mst-configコマンドを実行した場合の出力例を示しています。

## ProCurve機器でのMSTP設定の確認(続き)

show spanning-tree <port-list> instance <id>コマンドを実行すると、MSTインスタンス内のアップリンクのステータスが表示される。

```
Switch# show spanning-tree 47-48 instance 2
```

### MST Instance Information

```
Instance ID : 2
Mapped VLANs : 11,13
Switch Priority : 32768
Topology Change Count : 4
Time Since Last Change : 13 mins
Regional Root MAC Address : 00097c-2b8100
Regional Root Priority : 0
Regional Root Path Cost : 20000
Regional Root Port : 2
Remaining Hops : 19
```

### 以下を確認

- このスイッチがルートになっているか
- ルートプライオリティの値
- どのポートがルートポートになっているか
- ルートパスコストの値
- どのポートがブロックされているか

| Port | Type      | Cost  | Priority | Role      | State      | Designated Bridge |
|------|-----------|-------|----------|-----------|------------|-------------------|
| 47   | 100/1000T | 20000 | 128      | Alternate | Blocking   | 000af4-967180     |
| 48   | 100/1000T | 20000 | 128      | Root      | Forwarding | 00097c-2b8100     |

show spanning-tree <port-list> instance <id>コマンドを実行すると、ProCurveスイッチのMSTインスタンス内のアップリンクのステータスが表示されます。この例では、ポート47と48が、MSTPを実行している、コアにあるCiscoスイッチへのアップリンクになっています。

## MSTPのトラブルシューティング

スイッチが誤ってインスタンスのルートになっている場合は、このスイッチは別のMSTPリージョンに所属する

- MSTPの設定パラメーターを確認

ルートポートがダウンして通信が遮断された場合、エッジスイッチで代替ポートのVLAN設定を確認

- 代替ポートとルートポートは同じVLANを伝送している必要がある

### MSTPがすぐに統合されない場合にどうするか

MSTPがすぐに統合されない場合は、アップリンクがポイントツーポイントに設定されているかどうかを確認する

基本的なトラブルシューティングとして、スイッチが誤ってインスタンスのルートになっている場合の対応があります。これは、スイッチが別のMSTPリージョンに所属していることを意味します。まず、MSTの設定パラメーター(MSTの設定名、リビジョン番号、およびVLANとMSTインスタンスの割り当て)を確認します。

ルートポートがダウンして通信が遮断された場合は、エッジスイッチで代替ポートのVLAN設定を確認します。代替ポートとルートポートは同じVLANを伝送している必要があります。

MSTPがすぐに統合されない場合は、アップリンクがポイントツーポイントに設定されているかどうかを確認します。

## 役に立つshowコマンド

| 説明                          | ProCurve   | Cisco   |
|-----------------------------|--|---|
| MSTの設定を確認                   | <code>show span mst-config</code>  | <code>show span mst configuration</code><br><code>show span mst configuration digest</code> |
| 別のスイッチが同じMSTリージョンにあるかどうかの確認 | <code>show span instance &lt;port&gt; detail</code><br>MSTリージョンの境界を見つける                            | <code>show span interface [&lt;port&gt; detail]</code><br>バインド状態(PVST、RPVST、RSTP)を見つける      |
| CSTでブロックされているポートの確認         | <code>show span</code>   | <code>show span</code>  |
| ISTインスタンス0でブロックされているポートの確認  | <code>show span instance ist</code>  | <code>show span instance 0</code>   |
| 他のインスタンスでブロックされているポートの確認    | <code>show span instance &lt;id&gt;</code>   | <code>show span instance &lt;id&gt;</code>  |
| 最近行ったトポロジ変更箇所の確認            | <code>show span debug-counters instance 0 port all</code><br>すべてのポートについて「Topology Changes Rx」の値を確認 | <code>show span active detail</code>  |

この表には、ProCurveスイッチとCiscoスイッチでMSTPの設定とステータスを確認する場合に使用できるCLIコマンドの一部を示しています。

## Spanning Tree Hardening

- ✓ PVST+の実装
- ✓ MSTPの実装
- ✓ MSTPの相互運用性と互換性

### Spanning Tree Hardening

- スパニングツリーの問題
- CiscoとProCurveの保護機能

次のセクションでは、スパニングツリーで発生しうる基本的な問題や脆弱性の一部について説明します。その後、CiscoとProCurveがサポートする、スパニングツリーの脆弱性を緩和するための保護機能の概要を説明します。



## Spanning Tree Hardening機能

| ProCurve  | Cisco   |
|---|---|
| オートネゴシエーションを使用するRemote-Fault Notification (RFN) | オートネゴシエーションを使用するRemote-Fault Notification (RFN) |
| Uni-directional Link Detection (UDLD)           | Uni-directional Link Detection (UDLD)           |
| BPDUプロテクション                                     | BPDUガード   |
| ループプロテクション                                      | キープアライブ   |
| ルートガード  | ルートガード  |
| -   | ループガード  |

ProCurve機器とCisco機器は、いくつかのスパニングツリー保護機能を備えていますが、これらは機能的に類似しています。CLIコマンドを使用してスパニングツリーを強固(harden)にする点などが似ています。たとえば、ProCurveでループプロテクションと呼ぶ機能は、Ciscoではキープアライブといいます。また、ProCurveでのBPDUプロテクションは、CiscoではBPDUガードと呼ばれます。

## Spanning Tree Hardening機能

| ProCurve  | Cisco   |
|---|---|
| オートネゴシエーションを使用するRemote-Fault Notification (RFN) | オートネゴシエーションを使用するRemote-Fault Notification (RFN) |
|   |   |
|   |   |
|   |   |
|   |   |
|   |   |

オートネゴシエーションを使用するRemote-Fault Notification (RFN)は、レイヤー1で行われます。オートネゴシエーションは通常、Gigabit Ethernetポートでデフォルトで有効になっているので、RFNの理解に関して混乱が生じています。RFNはオプションで使用しますが、オートネゴシエーションを使用している場合はCiscoスイッチとProCurveスイッチの両方の1000BaseXポートでデフォルトで有効になっています。1000BaseXポートでは必ずオートネゴシエーションを使用する必要があります。

## Spanning Tree Hardening機能

| ProCurve                              | Cisco                                 |
|---------------------------------------|---------------------------------------|
| Uni-directional Link Detection (UDLD) | Uni-directional Link Detection (UDLD) |
|                                       |                                       |
|                                       |                                       |
|                                       |                                       |
|                                       |                                       |

CiscoのUDLDとProCurveのUDLDが相互運用できないのは、同じ宛先MACアドレスを使用していないことが原因です。Ciscoでは、Cisco固有のMACアドレスを使用しています。ProCurveでは、標準のMACアドレスを使用しています。

## Spanning Tree Hardening機能

| ProCurve                              | Cisco                                 |
|---------------------------------------|---------------------------------------|
| Uni-directional Link Detection (UDLD) | Uni-directional Link Detection (UDLD) |

### CiscoのUDLDフレーム:

```

Ethernet II, Src: Cisco_ee:99:82 (00:0c:85:ee:99:82), Dst: PVST+ (01:00:0c:cc:cc:cd)
  Destination: PVST+ (01:00:0c:cc:cc:cd)
    Address: PVST+ (01:00:0c:cc:cc:cd)
    ....1.... = IG bit: Group address (multicast/broadcast)
    ....0.... = LG bit: Globally unique address (factory default)
  Source: Cisco_ee:99:82 (00:0c:85:ee:99:82)
    Address: Cisco_ee:99:82 (00:0c:85:ee:99:82)
    ....0.... = IG bit: Individual address (unicast)
    ....0.... = LG bit: Globally unique address (factory default)
  
```

### ProCurveのUDLDフレーム:

```

Ethernet II, Src: HewlettP_22:f2:40 (00:17:08:22:f2:40), Dst: FoundryN_00:00:00 (00:e0:52:00:00:00)
  Destination: FoundryN_00:00:00 (00:e0:52:00:00:00)
    Address: FoundryN_00:00:00 (00:e0:52:00:00:00)
    ....0.... = IG bit: Individual address (unicast)
    ....0.... = LG bit: Globally unique address (factory default)
  Source: HewlettP_22:f2:40 (00:17:08:22:f2:40)
    Type: Foundry proprietary (0x885a)
  Data (46 bytes)
  
```

上記は、キャプチャーしたフレームの例です。ここでMACアドレスの違いを確認できます。

## Spanning Tree Hardening機能

| ProCurve    | Cisco   |
|-------------|---------|
|             |         |
|             |         |
| BPDUプロテクション | BPDUガード |
|             |         |
|             |         |
|             |         |

この2つの機能に関しては、相互運用性に関する考慮事項はありません。これは、ネットワークのエッジを保護するための設定です。

## Spanning Tree Hardening機能

| ProCurve   | Cisco   |
|------------|---------|
|            |         |
|            |         |
|            |         |
| ループプロテクション | キープアライブ |
| ルートガード     | ルートガード  |
| -          | ループガード  |

ループプロテクションとキープアライブは、特別なMACアドレスを使用してパスが有効であることを確認する同等の機能です。

ProCurveとCiscoは、ルートガードという、別のスパニングツリー保護機能にも対応しています。ルートガード機能は、現在のルートスイッチが、新たなスイッチから高プライオリティ値のBPDUをポートで受信した場合の処理に対応します。



## 確認テスト

## 確認テスト1

802.1sでは、タグ無BPDUをどのMACアドレスに送信しますか。

- A. 01:80:c2:20:00:00
- B. 01:00:0c:ec:cc:cd
- C. 01:80:c2:00:00:00
- D. 01:00:0c:cc:cc:cd



## 確認テスト1の解答

正解: C

## 確認テスト2

Cisco環境で802.1sを使用している際に、Ciscoデバイスがタグ無BPDUを01:80:c2:20:00:00に送信するのは以下どの場合ですか？

- A. PVST+と802.1sを両方ともトランクポートで使用している場合
- B. トランクポートで802.1sのみを使用している場合
- C. トランクポートでVLAN 1が許可されている場合
- D. トランクポートでネイティブが許可されている場合



## 確認テスト2

正解: C

## 確認テスト3

右側にあるProCurve Spanning Tree Hardeningの説明を、該当するCiscoの機能に対応させてください。

| ProCurve | Cisco   |
|----------|---|
|          | オートネゴシエーションを使用するRemote-Fault Notification (RFN) |
|          | Uni-directional Link Detection (UDLD)           |
|          | BPDUガード   |
|          | キープアライブ   |
|          | ルートガード  |

### ProCurve Spanning Tree Hardeningの説明:

- BPDUプロテクション
- Uni-directional Link Detection (UDLD)
- ループプロテクション
- ルートガード
- オートネゴシエーションを使用するRemote-Fault Notification (RFN)

## 確認テスト3の解答

| ProCurve  | Cisco   |
|---|---|
| オートネゴシエーションを使用するRemote-Fault Notification (RFN) | オートネゴシエーションを使用するRemote-Fault Notification (RFN) |
| Uni-directional Link Detection (UDLD)           | Uni-directional Link Detection (UDLD)           |
| BPDUプロテクション                                     | BPDUガード   |
| ループプロテクション                                      | キープアライブ   |
| ルートガード  | ルートガード  |

## モジュール5-4: 使用方法と設定方法

「スパニングツリーの実装」終了



# モジュール5-5: 使用方法と設定方法

## PoEとVoIP電話機



ここでは、PoEの機能とその利点、およびProCurveスイッチとCiscoスイッチにPoEを設定する方法について説明します。また、CiscoスイッチとProCurveスイッチを使ってネットワークにIP電話機を導入する方法についても説明します。Cisco製品のエキスパートであれば、PoEとVoIPの概念について理解していることを前提としています。ここでは、これらの機能の実装に関して、Cisco製品とProCurve製品での相違点と類似点を中心に説明します。

## PoEデバイス

### PD—Powered Device(受電デバイス)

- PSEから電源を供給されるデバイス
- 802.3af準拠のIP電話機
- PoE機能を備える無線AP
- IPカメラ、RFIDスキャナー、タブレットPC



### PSE—Power Sourcing Equipment(給電機器)

- Ethernetケーブル経由でデバイスに直接電力を供給(DC 44~57V)するデバイス



### IEEE 802.3afでは、以下の項目が指定されている

- 受電デバイス用の最大ワット数
- 受電電力をネゴシエーションするメカニズム

### IEEE 802.3atでは、以下の項目が指定されている

- Cat5E以上のケーブルで最大24W
- ProCurve Switch 8200zl、5400z、2910alスイッチはPoE+に対応

PoEの実装には、2つのタイプのデバイスが関与します。1つは「受電デバイス(PD)」と呼ばれ、「給電機器(PSE)」と呼ばれるもう1つのデバイスから電力を受け取ります。

受電デバイスは、データポート経由で電力を受け取るEthernetデバイスです。現在、このようなデバイスには、VoIP電話機、IP対応カメラ、Radio Frequency Identification(RFID)スキャナー、タブレットPCなどがあります。

ProCurve 3500yl、5400zl、8200zlシリーズなど、給電機器であるPoE対応のスイッチは、IEEE 802.3afの仕様(電圧DC47~57V、最大ワット数15.4W)を満たす必要があります。

Ethernetスイッチは、IEEE 802.3af標準に従ってCAT 5 Ethernetケーブル経由でネットワーク信号とともに電力を供給できます。

ProCurve 8200zl、5400zl、2910alシリーズのスイッチはPoE+(802.3at)に対応しており、Cat5Eケーブル経由で24Wの電力を供給できます。



## 管理システムーさまざまなPoEステータス

```

Group01(config)# show power-management ?
[ethernet] PORT-port-list Show the ports' power
brief Show summary of power statu
<cr>

Switch_A(config)# show power-management
Status and Counters - System Power Status

Max Power : 406 Operational Status : On
Power in Use : 15 W +/- 6W Usage Threshold (%) : 80

Switch_A(config)# power threshold ?
<1-99> Enter a number for the 'threshold'
command/parameter.

Switch_A(config)# power threshold 40

Switch_A(config)# show power

Status and Counters - System Power Status

Max Power : 406 Operational Status : On
Power in Use : 15 W +/- 6W Usage Threshold (%) : 40
    
```

使用可能総電力に対する使用電力の割合がここに示す値(%)を超えると、イベントログメッセージとSNMPトラップが生成される。しきい値を下回ると、別のメッセージとトラップが生成される。

モジュール式スイッチでは、モジュールごとにしきい値を設定可能

CLIを使用すると、ProCurveスイッチの電力統計情報を調べたり、PoEの動作に関するログとSNMPトラップを設定することができます。電力ステータスは、インターフェイスごと、またはシステム全体について調べることが可能です。上の図に示すように、システム全体のステータスを調べるコマンドでは、最大ワット数と現在使用中の電力量が表示されます。トラップを設定またはイベントログを記録することにより、消費電力が設定可能なしきい値を上回った場合、または下回った場合に情報を確認できます。

ProCurveのPoE対応スタックブル式/モジュール式スイッチでは、PoEがデフォルトで有効になっています。上記のコマンドを使用すると、デフォルトのプライオリティ設定を変更できます。プライオリティはcritical、high、およびlowに設定できます。デフォルト設定はlowで、スイッチの番号が小さいほうのポートが、番号が大きいポートよりもデフォルトでプライオリティが高くなっています。このプライオリティメカニズムでは、使用可能なワット数を超えた場合に、プライオリティがcriticalの機器が、highやlowの機器よりも先に電力を受け取ります。

## システム全体のPoEステータスの管理

IEEE 802.3af互換のPDに対応するProCurveスイッチは、IEEE 802.3af標準化前のPDもサポート

802.3af標準化前のPDの例:

- Cisco 7902G、7905G、7912G、7940G、7960G VoIP電話機
- Cisco Aironet 350、1100、1200、1230AGアクセスポイント

802.3af標準化前のCiscoのVoIP電話機は、PSEへの接続にストレートケーブルが必要

IEEE 802.3af互換のPDに対応するProCurveスイッチは、IEEE 802.3af標準化前のPDもサポートします。

802.3af標準化前のPDの例を上記に示しています。

802.3af標準化前のCiscoのVoIP電話機は、PSEへの接続にストレートケーブルが必要です。このようなIP電話機は、DC電圧の極性に依存 (IEEE 802.3afとは異なる) し、Ethernetケーブルのデータペア (1、2、3、6) がVoIP電話機とPSE間がクロスケーブルで接続している場合は適切に動作しません。

## ポートレベルのPoEステータスの表示

```
Group01(eth-3)# show power eth 3
Status and Counters - Port Power Status for port 3

Power Enable      :Yes

Priority          : Low                Configured Type   : Other
Detection Status : Delivering         Power Class       : 0

Over Current Cnt : 0                  MPS Absent Cnt   : 0
Power Denied Cnt : 0                  Short Cnt        : 0

Voltage          : 50.6 dV             Current           : 290 mA
Power            : 14674 mW
```

14674 mW = 14.674 W  
他のリストでは15Wに切り上げ

290 mA = 50.6Vで0.290A

特定のポートの電力設定と使用率を表示するには、特定のポート番号を指定して show power-management ethernet コマンドを実行します。上記のスイッチでは、指定のポートに接続されているPDに15Wの電力を供給しています。

## すべてのポートのPoEステータスの表示

```

Group01(config)# show power-management brief
Status and Counters - Port Power Status

```

| Port | Power Enable | Priority   | Configured Type | Detection Status  | Power Class |
|------|--------------|------------|-----------------|-------------------|-------------|
| 1    | Yes          | Low        | Other           | Searching         | 0           |
| 2    | Yes          | Low        | Other           | Searching         | 0           |
| 3    | <b>Yes</b>   | <b>Low</b> | <b>Other</b>    | <b>Delivering</b> | <b>3</b>    |
| 4    | Yes          | Low        | Other           | Searching         | 0           |
| 5    | Yes          | High       | Other           | Searching         | 0           |
| 6    | Yes          | Low        | Other           | Searching         | 0           |
| 7    | Yes          | Low        | Other           | Searching         | 0           |

```

Group01(config)# interface 7
Group01(eth-7)# power ?
critical
high
low
<cr>

```

Searching: 現在、電力検出を実行中  
 Delivering: 給電中  
 Disabled: このポートでPoEがオフになっている  
 Fault: PDデバイスに障害が発生している

Fault状態の後には、2回目の電力検出(Searching)試行が行われる。  
 Searching/Fault状態が2回出現すると、エラーログエントリーとSNMPトラップが生成される。

すべてのポートのPoEステータスの概要を表示するには、show power-management brief コマンドを実行します。このコマンドの出力には、すべてのポートのPoE検出ステータス、およびPoEが有効な各ポートのプライオリティが含まれます。

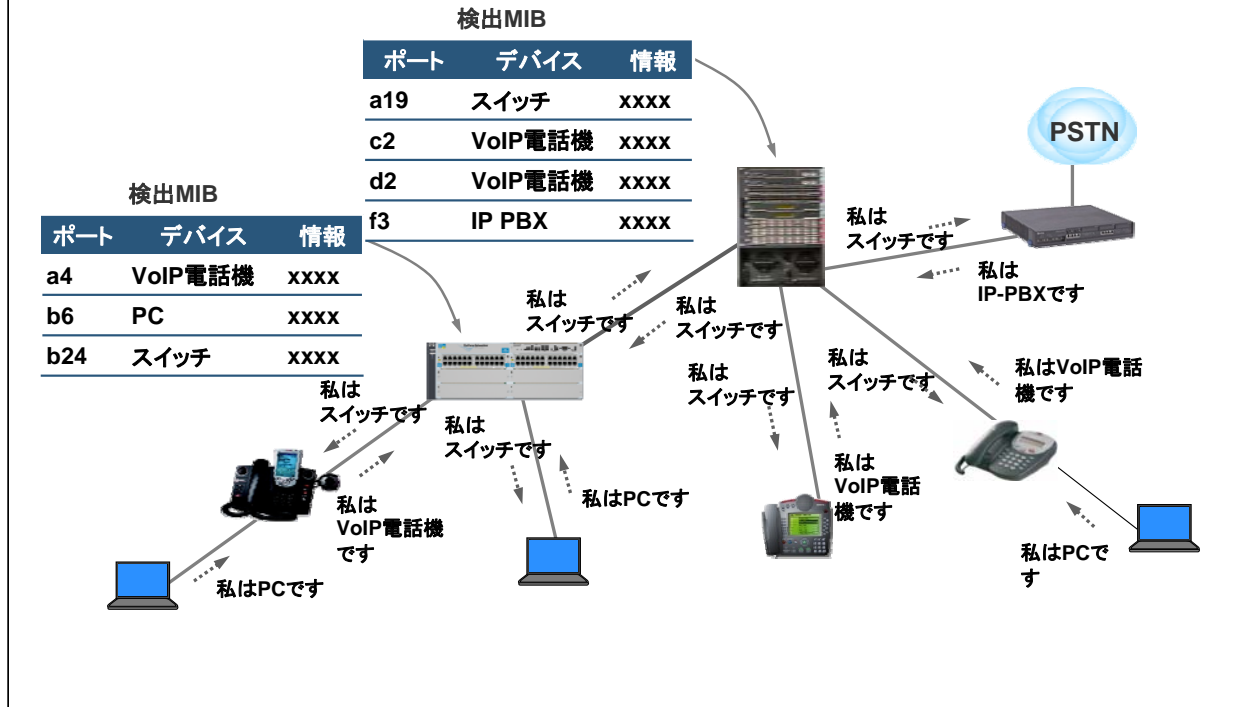
## PoE設計上の考慮事項

- 1 高プライオリティのデバイスをポート番号が小さいポートに接続する
  - たとえば、APをポート1～12、IP電話機をポート13～24、PDA充電器をポート40～44
- 2 PDの受電は変動する可能性がある
  - IP電話機は起動または呼び出し時に10W受電し、アイドル時に6Wに戻る
  - 4Wの差は、PSEのプールに返される
- 3 電力バジレットの計上時に、各PDの最大受電を許容する
  - PoEスイッチへの電力を追加するには、Switch zl Power Shelfまたは620 RPS/EPSを使用
  - PSEからPDへの電力低下として16%を許容する
- 4 標準化前の802.3afのPDもサポート可能。サポートはデフォルトで有効

ProCurveスイッチを使用してPoEソリューションを実装する場合は、以下の点に注意してください。

1. 高プライオリティのデバイスをポート番号が小さいポートに接続します。これは、スイッチのデフォルト設定では、ポート番号が小さい順に電力が割り当てられるためです。この設定が適切でない場合は、プライオリティをカスタマイズすることも可能です。
2. PDに供給される電力は変動する可能性があります。接続されているPDごとに、必要とされる最大電力を見積もってください。
3. 各PDに最大電力を許可します。スイッチの電力バジレットの割り当て時に、接続されているデバイスすべてが必要とする最大総電力を考慮する必要があります。このようにしない場合は、需要が高い期間にスイッチが需要過多になる可能性があります。
4. 標準化前の802.3afのPDもサポート可能です。サポートはデフォルトで有効になっています。

## LLDPの動作



これまでの説明でPoEデバイスへの給電方法については理解できたと思います。ここでは、LLDPがVoIPを機能させる方法について説明します。

ここでは、Link Layer Discovery Protocol (LLDP) の基本的な考え方を復習し、LLDPの拡張版であるMedia Endpoint Discovery (LLDP-MED) について説明します。その後、VoIPの典型的な起動プロセス、およびエッジスイッチをVoIP電話機に対応させる場合の設定方法について簡単に説明します。

Link Layer Discovery Protocol (LLDP) は、標準に基づいて、スイッチ、ルーター、無線アクセスポイントなどのEthernetベースのネットワークデバイスが隣接デバイス（ネイバー）に自分自身をアドバタイズして、隣接デバイスに関する情報を学習できるようにします。これはCDPに類似しています。LLDPは、IEEE 802.1AD標準に準拠しています。

## LLDPとLLDP-MEDの違い

### LLDP

#### ネットワーク管理

- ネットワークの物理トポロジを正確に検出

#### ネットワークのインベントリデータ

- システム名と説明、機能と管理アドレス

#### ネットワークのトラブルシューティング

- IPアドレスの設定誤りや、到達不能なIPアドレスを持つデバイスを検出
- 速度と二重化のミスマッチを検出

### LLDP-MED

#### 相互運用性

- 管理機能はベンダー依存

#### 統合ネットワークポリシーを自動的に導入

- 音声VLAN、レイヤー2/3 QoSポリシー

#### ロケーションサービス

- 緊急コールサービスにより、IP電話機でE911通話が可能

#### 詳細なインベントリ管理

- モデル、製造者、ソフトウェア、ファームウェア、資産情報を収集

#### 高度なPoE

- 詳細な電源管理とバックアップ電力の保存

#### IP電話ネットワークのトラブルシューティング

- 音声に関する不適切なポリシーの検出

LLDP-MEDは、LLDPの機能を拡張したものです。ここでは、その追加された機能について説明します。

その1つは、許可されたVLAN、レイヤー2プライオリティとDiffserveの設定などのLANポリシーの自動検出機能です。この機能により、VoIP電話機などのさまざまなデバイスをプラグ&プレイで簡単に接続できるようになります。

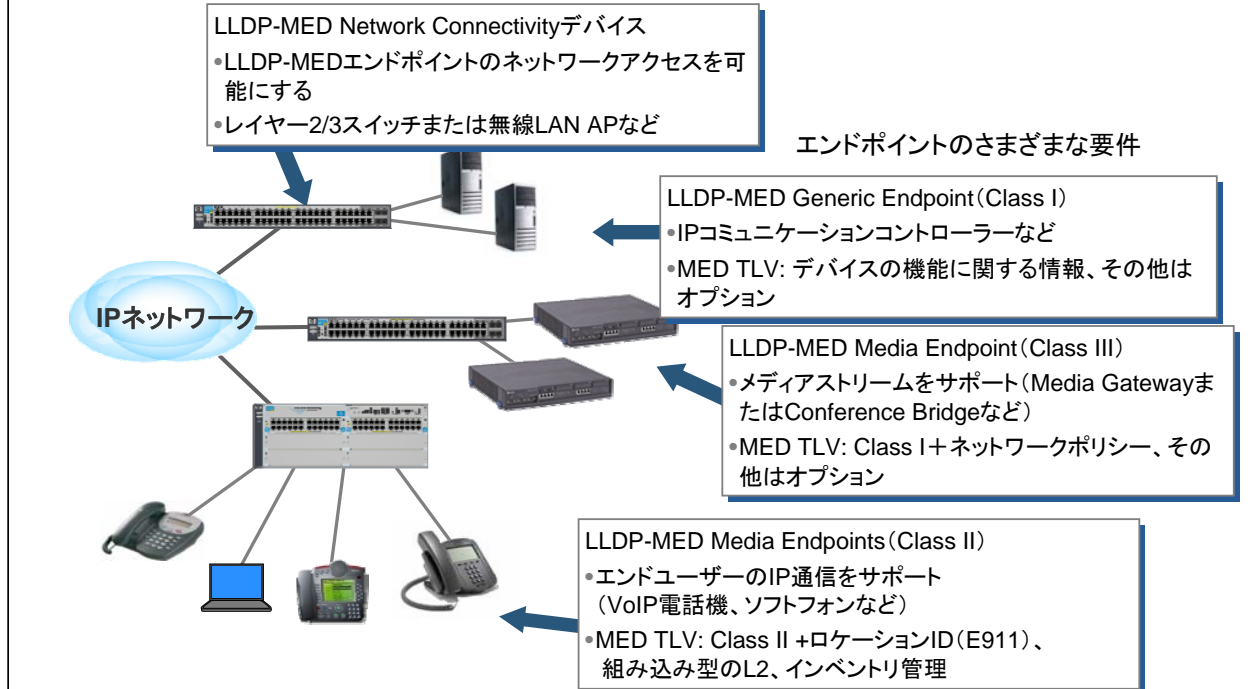
もう1つの機能は、場所を検出できるようにするロケーションデータベースの作成と、VoIP電話機でのEnhanced 911 (E911) サービス(北米のみ対応)の提供です。

また、PoEエンドポイントの電力管理が拡張され、自動化されています。

インベントリ管理は、ネットワーク管理者がネットワークデバイスを追跡して、製造業者、ソフトウェア/ハードウェアのバージョン、シリアル番号や資産番号などのデバイスの特性を特定できるようにする機能です。

VoIP電話機のベンダーの多くは、コスト上の制約や管理が複雑になるなどの理由でSNMPのサポートを予定していなかったため、VoIPではLLDP-MEDをサポートすることが非常に重要です。

## LLDP-MEDのコンポーネントモデル



LLDP-MEDは、プロトコルを使用するさまざまなコンポーネントを定義します。これには、ネットワーク接続デバイス、一般的なエンドポイント、メディアエンドポイントなどがあります。

ネットワーク接続デバイスは、LLDP-MEDエンドポイントがネットワークにアクセスできるようにします。たとえば、レイヤー2または3のスイッチ、無線LAN APなどです。

Generic Endpoint (Class 1)には、IP通信のコントローラーとして機能するデバイスが含まれます。LLDP-MEDに対応している場合、このようなデバイスの機能に関する情報を提供するType Length Value (TLV)を含めます。

Media Endpoint (Class III)は、Media GatewayまたはConference Bridgeなどのメディアストリームをサポートします。LLDP-MEDに対応している場合、LLDP-MEDは、このようなデバイスのネットワークポリシーに関する情報を提供するTLVを含めます。また、Class IIIデバイスは、Class I TLVもサポートします。

Media Endpoint (Class II)は、VoIP電話機やソフトフォンなどエンドユーザーによるIP通信をサポートします。LLDP-MEDに対応している場合、LLDP-MEDは、このようなデバイスに関して、場所の特定機能 (E911サービス)、および組み込み型のレイヤー2インベントリ管理情報を提供するTLVを含めます。Class IIデバイスは、Class II TLVもサポートします。



## マルチベンダーのサポート: PCとVoIP電話機による接続の共有

### VoIP電話機が音声VLANとQoSを自動設定する方法

- LLDP-MED (ProCurveスイッチ) または CDPv2 (Ciscoスイッチ) を使用
- 多くのVoIP電話機は「ベンダー固有」のDHCPプロセスを使用した自動設定をサポート
  - Avaya、Alcatel、Mitel、Siemens、ShoreTelなど
  - データVLANのDHCPサーバーが音声VLAN IDとQoSをアドバタイズ
- 一回の手動設定
  - Ciscoの場合は、Ciscoネットワークに接続する際に、Network Configuration セットアップを使用してadmin VLAN IDを設定

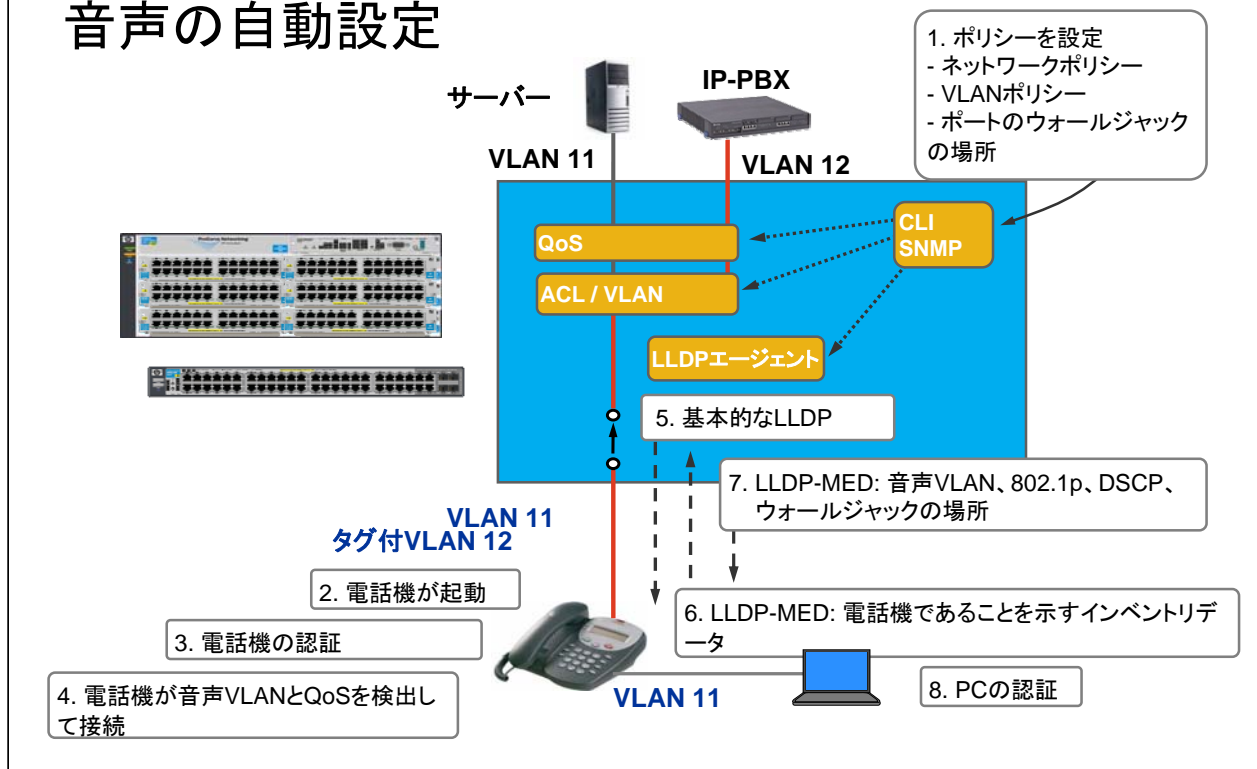


1. LLDP-MEDとCisco CDPv2は、VoIP電話機が、音声VLANとQoSを自動的に設定できるようにします。

2. VoIP電話機の多くは、「ベンダー固有」のDHCPプロセスを使用する自動設定にも対応しています。このようなベンダーには、Avaya、Alcatel、Mitel、Siemens、ShoreTelなどがあります。DHCPは、この他の目的に対応するベンダー固有の拡張機能もサポートしています。VoIPの自動設定プロセスでは、データVLAN上のDHCPサーバーは、音声VLAN IDとQoS、および使用するIPアドレスやデフォルトゲートウェイなど、その他の典型的な属性の割り当てをアドバタイズします。

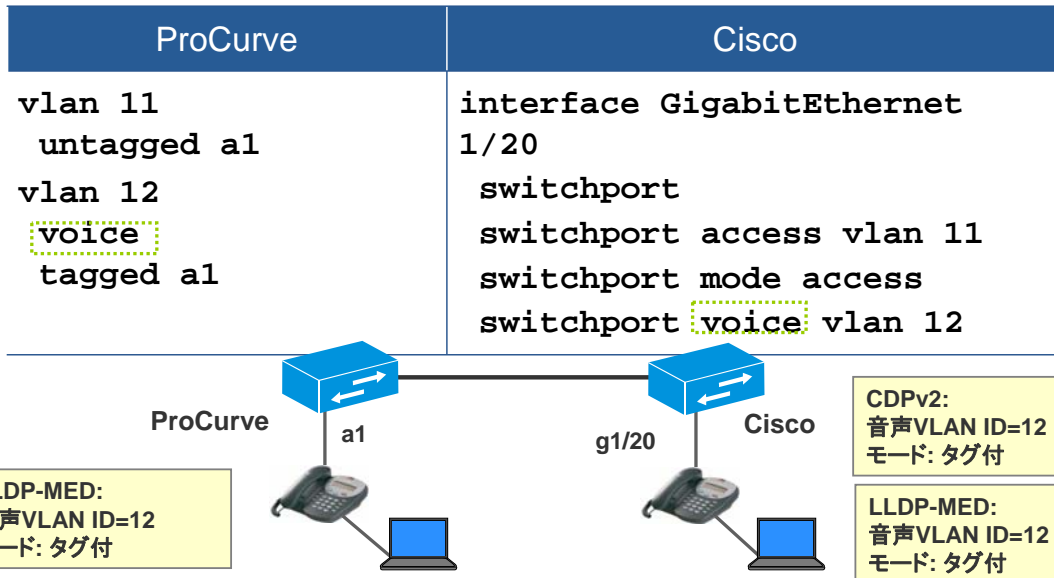
3. 3つめの方法として、VLAN識別子とQoS設定の自動設定を手動で一回行う方法があります。たとえば、Ciscoの場合は、Ciscoネットワークに接続する際に、Network Configurationセットアップを使用して管理用のVLAN IDを設定します。

# 音声の自動設定



この図は、LLDP-MEDを使用してVLAN識別子とQoSに関する自動設定プロセスが動作する様子を示しています。

## VLAN設定の比較: スイッチとコンピューター間に IP電話機を接続

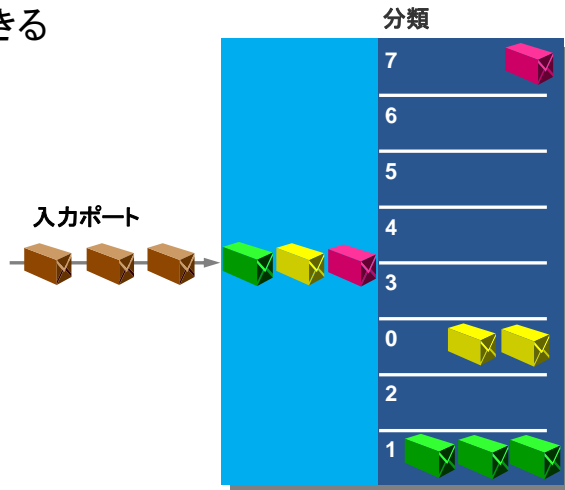


ここでは、ProCurveスイッチとCiscoスイッチのコンフィギュレーションファイルに指定して、VoIP電話機とPCを接続したエッジ(アクセス)ポートを機能させるCLIコマンドの例を示します。

この例では、VLAN 11を使用してPCとの間でデータトラフィックを送受信し、VLAN 12を使用してVoIP電話機との間で音声トラフィックを送受信しています。ProCurveスイッチでは、データVLANのポートはタグ無ですが、音声VLANではタグ付になっています。Ciscoの場合でも同様の設定を行います。

## トラフィックの分類

- トラフィックを分類して、プライオリティを高くするトラフィックを認識
  - これは、VLAN ID、入力ポート、デバイスのIPアドレスなどさまざまな特性に基づいて行う
- さまざまなProCurveスイッチで、トラフィックを最大8個のクラスにマッピングできる



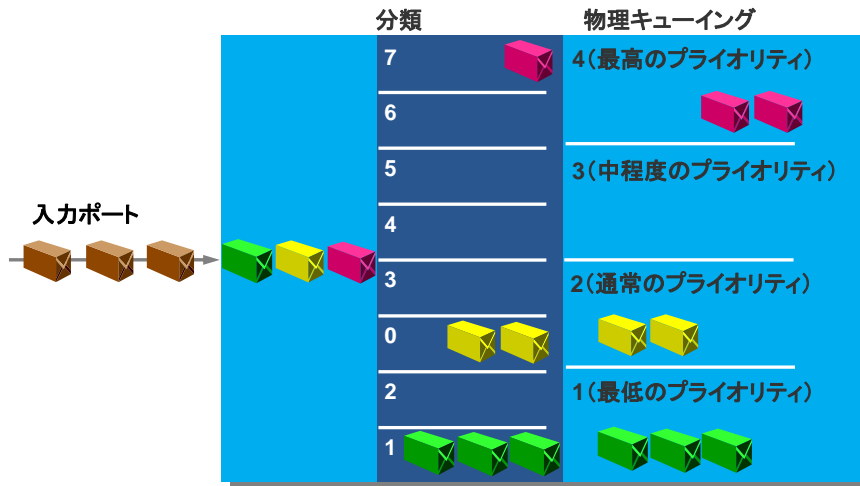
ここでは、特定のトラフィックに対してネットワークサービスを優先させるQuality of Service (QoS)機能の使用方法を学習します。レイヤー2 IEEE 802.1pおよびレイヤー3 Differentiated Servicesのプライオリティ付けの方法、ポートのキューごとの最低保証帯域幅、レート制限によるトラフィックの制御の概要について説明します。

統合アプリケーションに適切なサービスを提供するには、トラフィックのプライオリティを設定するエンドツーエンドの方法をネットワークインフラが備えている必要があります。データ送信で許容可能な遅延のレベルによっては、VoIPまたはネットワークベースのビデオが使用できなくなる可能性があります。

## トラフィックの分類: キューへのマッピング

8個のトラフィッククラスがスイッチのキューにマッピングされる。設定可能なキューの数は、2個、4個、または8個。

各キューには、最少の割合(%)で帯域幅が割り当てられる。高プライオリティのトラフィックには、最大の割合が割り当てられる。



トラフィックを分類する際に、スイッチは、特定のスイッチポートに関連付けられたキューを転送する物理的なハードウェアに、8個のトラフィッククラスまたはプライオリティレベルをマッピングします。上記の例では、このスイッチは各ポートで4個のキューをサポートしており、各キューに2個のトラフィッククラスをマッピングします。

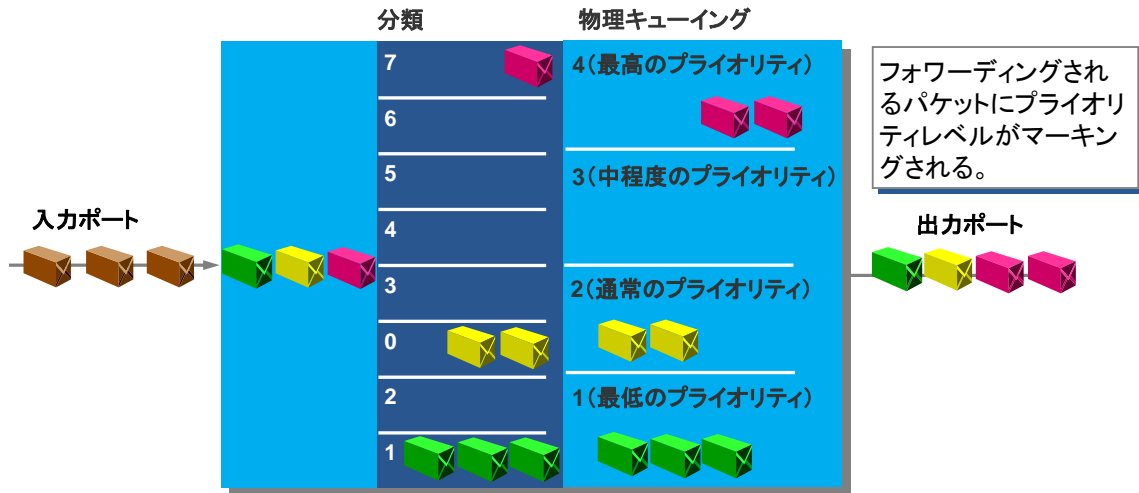
スイッチでサポートするキューの数は、変更可能です。たとえば、Switch 8200zl、5400zl、6200yl、3500ylシリーズでは、各スイッチポートに対して、2個、4個、または8個のハードウェアキューを設定できます。デフォルト設定は、8キューです。

トラフィッククラス0は、最低のプライオリティでなく、通常のプライオリティにマッピングされることに注意してください。未分類のトラフィックは、デフォルトではクラス0に割り当てられるので、通常のプライオリティのフォワーディングが設定されます。トラフィッククラス1と2は、プライオリティが最も低いキューにマッピングされます。

## トラフィックのマーキング

スイッチは、パケットヘッダーでプライオリティレベルを示すことができる。これには、レイヤー2マーキング (IEEE 802.1p) およびレイヤー3マーキング (DiffServ) が含まれる。

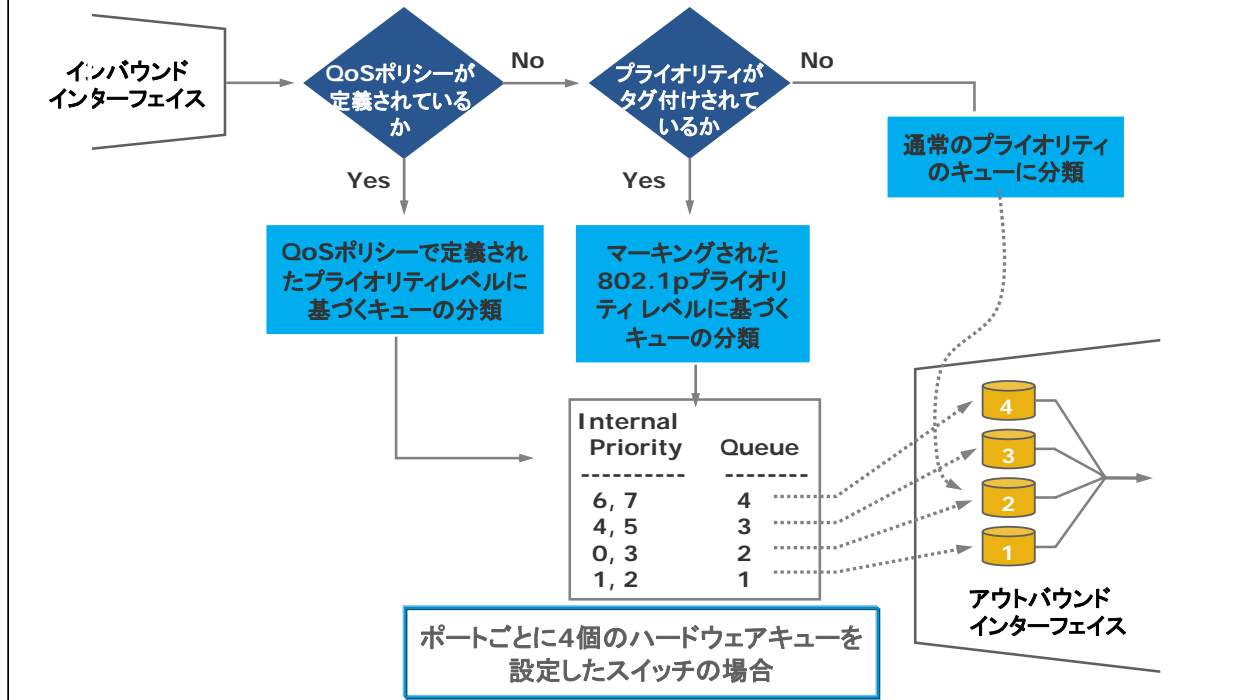
プライオリティレベルは、受信側のスイッチに対してトラフィックを処理する方法を示す。



マーキング手順では、スイッチは、レイヤー2および/またはレイヤー3のヘッダーにプライオリティレベルを設定します。トラフィックをマーキングして、パケットを受信する次のスイッチがこの情報を使用できるようにします。

トラフィックのマーキングは2つの方法で行われます。レイヤー2ではIEEE 802.1p、レイヤー3ではDifferentiated Services (DiffServ) に従って行われます。レイヤー2とレイヤー3の両方のヘッダーの対応するフィールドを設定する場合も、一方のみを設定する場合もあります。これは、スイッチがレイヤー3マーキングを行う設定になっているかどうか、また、トラフィックの伝送に使用するポートの性質によって決まります。レイヤー2では、ポートがタグ付かどうかで決まります。

## QoSプロセスの概要



パケットを受信すると、定義済みQoSポリシーにパケットがマッチするかどうかの判断が行われます。

複数のQoSポリシーが定義されている場合は、優先順位に基づいて判断します。この点については、このモジュールで後ほど詳しく説明します。

QoSポリシーが定義されている場合は、ポリシーに定義されている802.1pプライオリティレベルに基づいてパケットがキューに分類されます。

この例では、スイッチのポートごとに4個のハードウェアキューがあります。

QoSポリシーが定義されていない場合は、受信パケットがタグ付かどうかの判断が行われます。パケットがタグ付の場合は、802.1Qヘッダーの802.1pプライオリティ値を使用して、どのキューに分類するかを決定します。

受信パケットがタグ付でない場合は、検討を要する802.1pプライオリティ値がありません。そのため、パケットは通常のプライオリティキューに分類されます。この例では4個のキューがあるので、通常のプライオリティのキューはキュー2になります。

## ProCurveのQoSサポートの概要

ProCurve ASICベースのスイッチでのQoSサポート

•Switch 8200zl、5400zl、3500y、6200ylシリーズ

| 分類 | レイヤー<br>2<br>802.1p | レイヤー<br>3<br>DSCP | レイヤー3プ<br>ライオリティ | VLAN<br>ID | 入力<br>ポート | TCP/UDP<br>ポート | IPアドレ<br>ス | LANプロ<br>トコル |
|----|---------------------|-------------------|------------------|------------|-----------|----------------|------------|--------------|
|    | ✓                   | ✓                 | ✓                | ✓          | ✓         | ✓              | ✓          | ✓            |

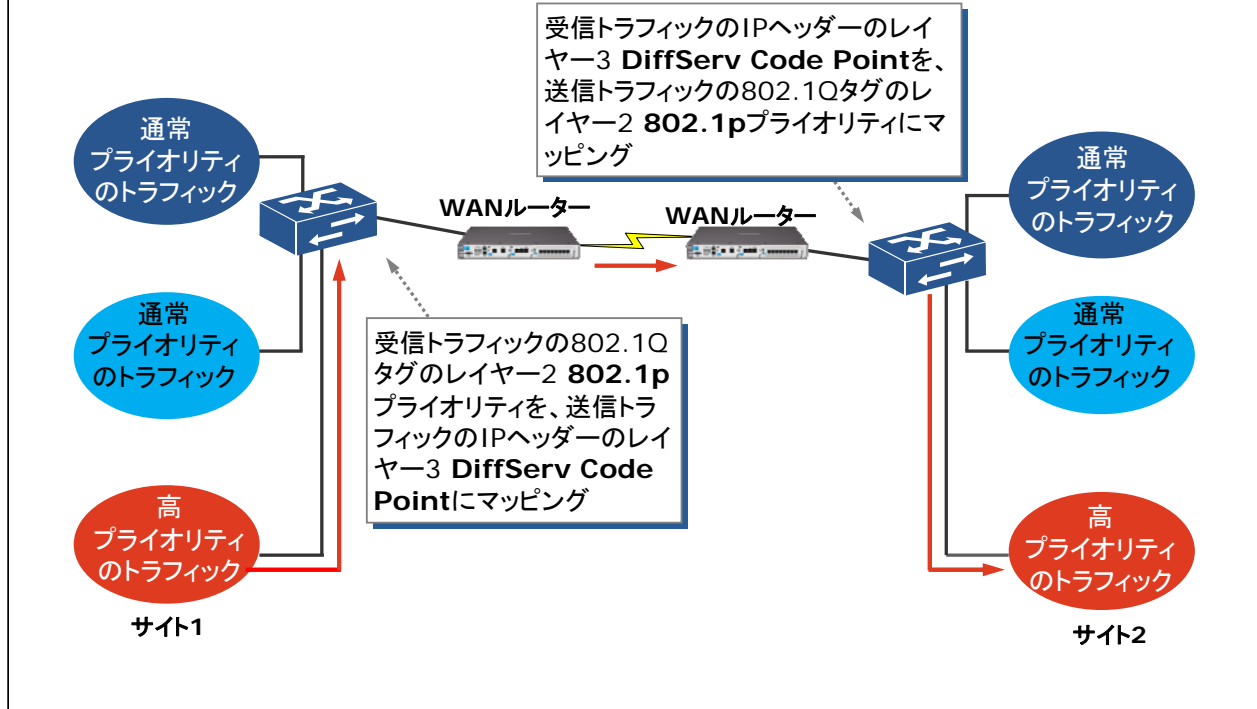
| キューイング | ポートごとのキューの数   | キューイング動作の変更               |
|--------|---------------|---------------------------|
|        | 8(2または4に変更可能) | GMB:出力のみ<br>レート制限:入力および出力 |

| マーキング | レイヤー<br>2 802.1p | レイヤー<br>3 DSCP | レート制限により、1つ<br>のポートで使用できる<br>帯域幅の上限も制御で<br>きる(デフォルトでは無<br>効)。 | 保証最小帯域幅(GMB)の設定に<br>従って、ある特定のポートのアウト<br>バウンドキューそれぞれに最小帯域<br>幅が適用される(デフォルトではキュー<br>の数に基づく)。 |
|-------|------------------|----------------|---|--|
|       | ✓                | ✓              |   |  |

この図は、Switch 8200zl、5400zl、6200yl、3500yl シリーズで使用できるQoS機能の概要(対応する分類基準、キューの設定機能、対応するマーキング基準)を示しています。



## WANリンク経由でのプライオリティの保持



VoIPなど、遅延の影響を受けやすい多くのアプリケーションでは、比較的低速のWANリンク上でトラフィックをルーティングする際に適用するプライオリティ設定が必要となります。ただし、フレームタイプがEthernetから、PPPなどのWANプロトコルのいずれかに変わる際には、802.1Qタグ(および中に含まれる802.1pプライオリティ値)は保持されません。

この問題を解決するには、スイッチがDiffServeをサポートするように設定して、受信トラフィックの802.1pプライオリティ値を送信パケットのIPヘッダーのDSCP値にマッピングできるようにする必要があります。これで、WANルーターには、エッジスイッチとコアスイッチで設定されたプライオリティを適用する際に必要な情報が提供されます。

## トラフィックの分類基準

Switch 8200zl、5400zl、3500yl、6200ylシリーズおよびその他のスイッチファミリーは、7つの基準に基づいてトラフィックを分類可能。

複数のプライオリティポリシーが定義されている場合は、プライオリティが高い方から低い方へと基準が評価される。

1. UDP/TCPポート番号
2. デバイスのIPアドレス
3. IP ToSフィールド(DiffServまたはPrecedenceビット)
4. LANプロトコルタイプ(IP、ARPなど)
5. VLAN ID
6. 入力スイッチポート
7. 受信する802.1pの値(入力ポートがタグ付けされている場合)



デフォルト設定では、受信する802.1p値のみを評価(802.1p値がある場合)。  
その他の基準は無効(未定義)または“no-override”に設定される。

Switch 8200zl、5400zl、3500yl、6200ylシリーズおよびその他のスイッチファミリーは、7つの基準に基づいてトラフィックを分類します。

複数のプライオリティポリシーが定義されている場合は、プライオリティが高い方から低い方へと基準が評価されます。

スイッチに複数のプライオリティ基準が設定されている場合は、スイッチは図のように、プライオリティが高い方から低い方へと基準を評価します。

## DiffServ Code Pointマッピングテーブルの表示

```
Switch# show qos dscp-map
DSCP -> 802.p priority mappings
DSCP policy 802.lp tag Policy name
-----
000000 No-override
000001 No-override
...
001010 1
001011 No-override
001100 1
001101 No-override
001110 2
001111 No-override
010000 No-override
010001 No-override
010010 0
010011 No-override
010100 0
010101 No-override
010110 3
010111 No-override
011000 No-override
011001 No-override
...
```

デフォルトでは、13個のDSCPに802.1pプライオリティレベルが割り当てられている

“No-override”は、802.1pプライオリティレベルが割り当てられていないことを示す

| DSCPポリシー   |       |         |     |               |           |
|------------|-------|---------|-----|---------------|-----------|
| カテゴリー      | 転送クラス | ドロップ優先度 | 10進 | 802.1pプライオリティ | マッピングキュー* |
| AF Class 1 | 001   | 010     | 10  | 1             | 1         |
|            | 001   | 100     | 12  | 1             | 1         |
|            | 001   | 110     | 14  | 2             | 2         |
| AF Class 2 | 010   | 010     | 18  | 0             | 3         |
|            | 010   | 100     | 20  | 0             | 3         |
|            | 010   | 110     | 22  | 3             | 4         |
| AF Class 3 | 011   | 010     | 26  | 4             | 5         |
|            | 011   | 100     | 28  | 4             | 5         |
|            | 011   | 110     | 30  | 5             | 6         |
| AF Class 4 | 100   | 010     | 34  | 6             | 7         |
|            | 100   | 100     | 36  | 6             | 7         |
|            | 100   | 110     | 38  | 7             | 8         |
| EF         | 101   | 110     | 46  | 7             | 8         |

\* 8個のハードウェアキューがある場合

802.1pプライオリティ値に基づいてQoSポリシーを定義することに加え、DiffServ Code Point(DSCP)値に基づいてQoSポリシーを設定することができます。

show qos dscp-mapコマンドを実行すると、DSCPマッピングテーブルを表示できます。ここには、64個のDSCPそれぞれに対応する802.1pプライオリティ値が表示されます。デフォルト設定では、DSCPマッピングテーブルには、IETFの定義に従って割り当てられた802.1pプライオリティ値を持つ13個のコードポイントがあります。51個の他のコードポイントには、“No-override”が設定されます。これは、単にそのコードポイントに802.1pプライオリティ値が設定されていないことを意味します。コードポイントは、6個の2進数で表示されます。

## 運用上の注意点: DSCPマッピングテーブルの管理

DSCPマッピングテーブルは以下の方法で変更可能

- DSCPマッピングテーブルの特定のコードポイントのデフォルトプライオリティ値を変更する
- DSCPマッピングテーブルの未定義("no-override" ステータス)のコードポイントにプライオリティ値を割り当てる

```
Switch(config)# qos dscp-map 001010 priority 7
```

DSCP 001010  
をデフォルトプライ  
オリティ1から7に  
変更

```
Switch(config)# qos dscp-map 000010 priority 1
```

DSCP 000010を  
"No-override"  
からプライオリティ  
1に変更

定義済みの802.1pプライオリティ値が割り当てられているコードポイントを変更したり、現在"No-override"に設定されているコードポイントに対して802.1pプライオリティ値を割り当てることができます。

これ以外の例については、このコースの英語版Webトレーニングに含まれる「student guide」のモジュール7を参照してください。

## QoS設定の比較

|           | ProCurve            | Cisco       |
|-----------|---------------------|-------------|
| 分類        | 主にグローバルに設定される       | ポートごとに設定される |
| マーキング     | 主にグローバルに設定される       | ポートごとに設定される |
| キューの分類    | ポートごとに設定される         | ポートごとに設定される |
| QoSのデフォルト | 有効、802.1pの設定に基づいて動作 | 無効          |

このテーブルは、ProCurveスイッチとCiscoスイッチでの基本的なQoS設定機能の概要を示しています。ProCurveスイッチの場合は、分類基準はグローバル、ポートレベル、VLANレベルで設定できます。Ciscoスイッチの場合は、ポートレベルで設定します。

ProCurveスイッチでは、トラフィックのマーキングは主にグローバルに行われます。たとえば、DiffServを使用するには、グローバルレベルで有効にします。また、DiffServ Code Point値を802.1pプライオリティ値にマッピングする方法を指定するDSCPマッピングテーブルもグローバルレベルで設定します。DiffServ Code Pointまたは802.1pプライオリティ値は、ポートまたはVLANレベルで設定できます。

ProCurveスイッチとCiscoスイッチでは、キューの分類はポートごとに設定します。つまり、プライオリティレベルまたは、各キューに割り当てられているレベルを指定します。

デフォルトでは、ProCurveスイッチは受信パケットの802.1Qタグヘッダーにある802.1pプライオリティ値を読み取って、それを送信パケットに含めます。802.1Qヘッダーは、ポートが1つ以上のVLANのタグ付メンバーになっている場合に付加されません。



## 確認テスト1

IEEE 802.3af互換のPDに対応するProCurveスイッチは、IEEE 802.3af標準化前のPDをサポートできない。

- A. 正解
- B. 不正解



## 確認テスト1の解答

正解: B



## 確認テスト2

802.3af標準化前のCiscoのVoIP電話機は、PSEへの接続にクロスケーブルが必要。

- A. 不正解
- B. 正解

## 確認テスト2の解答

正解: B

## 確認テスト3

ProCurveの802.3af標準化前のPDへの対応状況について正しく述べているものはどれですか。(当てはまるものをすべて選択)

- A. グローバルコンテキストで有効
- B. デフォルトで有効
- C. VLANで有効
- D. インターフェイスで有効
- E. 不可能
- F. クロスケーブルを使用する必要がある

## 確認テスト3の解答

正解: A

## 確認テスト4

LLDP-MEDとCisco CDPv2は、VoIP電話機が、使用する音声 VLANとQoSを自動的に設定できるようにする。

- A. 正解
- B. 不正解

## 確認テスト4の解答

正解: A

## 確認テスト5

右側の項目を、該当するProCurve QoSの説明に対応させてください。

| ProCurve            |
|---------------------|
| 主にグローバルに設定される       |
| 主にグローバルに設定される       |
| ポートごとに設定される         |
| 有効、802.1pの設定に基づいて動作 |

対応させる項目:

- マーキング
- QoSのデフォルト
- キューの分類
- 分類

## 確認テスト5の解答

| 解答        | ProCurve            |
|-----------|---------------------|
| 分類        | 主にグローバルに設定される       |
| マーキング     | 主にグローバルに設定される       |
| キューの分類    | ポートごとに設定される         |
| QoSのデフォルト | 有効、802.1pの設定に基づいて動作 |



## モジュール5-5: 使用方法と設定方法

「PoEとVoIP電話機」終了



## モジュール5-6: 使用方法と設定方法

### DHCPとインテリジェントミラーリング



ここでは、ProCurve DHCPのスヌーピング機能とインテリジェントミラーリング機能について説明します。

DHCPスヌーピングは、Cisco製品での実装に非常に類似しています。Cisco製品のエキスパートであれば、この基本的な機能について理解していることを前提としています。ここでは、その設定の一部についてのみ説明します。

インテリジェントミラーリングは、CiscoのSPANおよびRSPANに類似しています。ここでは、HP ProCurveでの実装の詳細について説明します。

## DHCPスヌーピングの有効化

まずDHCPスヌーピングをグローバルで有効にし、さらに各VLANを保護

```
Group01(config)# dhcp-snooping ?
authorized-server    Configure valid DHCP Servers.
database             Configure lease database transfer options.
option              Configure DHCP snooping operational behavior.
trust                Configure trusted interfaces.
verify              Enable/Disable DHCP packet validation.
vlan                 Enable/Disable snooping on a VLAN.
<cr>
```

```
Group01(config)# dhcp-snooping
Group01(config)# dhcp-snooping vlan 11
Group01(config)# dhcp-snooping vlan 12
```

設定するには、まずDHCPスヌーピングを有効にする

VLANに適用してアクティブにする



DHCPスヌーピングを実装するには、まず最初にスイッチでDHCPスヌーピングをグローバルに有効にします。これにはdhcp-snoopingコマンドを使用します。このコマンドによりDHCPスヌーピングが有効になります（または、コマンドに"no"を付けて実行すると無効になります）。

次の手順として、特定のVLANに対してDHCPスヌーピング機能を有効にします。これには、dhcp-snooping vlanコマンドに、DHCPスヌーピング機能で保護するVLANを指定して実行します。VLAN IDの範囲を指定する場合は、ハイフンを使用します。カンマで列挙して指定することはできません。

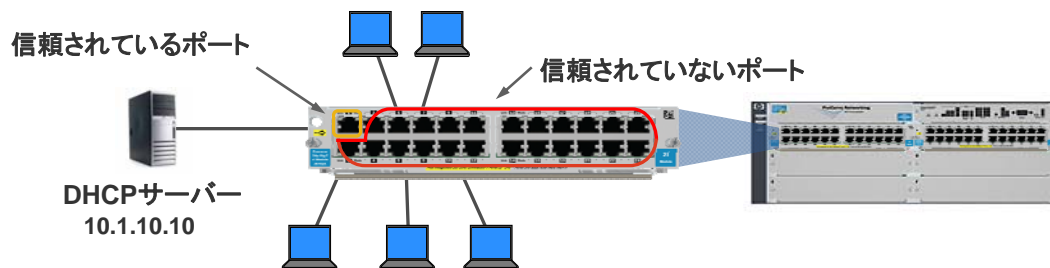
## DHCPスヌーピングの設定

信頼されているポートを定義

```
Group01(config)# dhcp-snooping trust a1
```

オプションで、信頼されているポート経由で到達可能な、認可DHCPサーバーを定義

```
Group01(config)# dhcp-snooping authorized-server 10.1.10.10
```



信頼されているポートを定義するには、dhcp-snooping trustコマンドに、該当するポートを指定して実行します。たとえば、アップリンクポート、および信頼されているポートとしてDHCPサーバーに直接接続しているポートを指定します。信頼されているポートを定義すると、スイッチはそのポートのすべてのDHCPパケットをフィルタリングしません。

信頼されているポートを追加するほか、ネットワーク上に認可DHCPサーバーも定義できます。

## オプション82の設定

オプション82を設定するときに、リレーするDHCP要求の「remote ID」フィールドに挿入する値を指定する

- 同じDHCPサーバーを使用する複数のVLANがスイッチにある場合は、通常 subnet-ip オプションを選択

[no] dhcp-snooping option 82 remote-id [mac | subnet-ip | mgmt-ip]

デフォルト

Group01(config)# dhcp-snooping option 82 remote-id subnet-ip

オプション82が設定されている、信頼されていないエンドポイントからのDHCP要求をスイッチが処理する方法を指定する

[no] dhcp-snooping option 82 untrusted-policy [drop | keep | replace]

デフォルト

Group01(config)# dhcp-snooping option 82 untrusted-policy replace

この設定タスクはオプション

VLANでDHCPスヌーピングを有効にすると、クライアントとDHCPが同じVLANにあるか別のVLANにあるかに関係なく、スイッチは常にオプション82をDHCP要求に挿入します。

オプション82を設定する際には、DHCPヘッダーに挿入する、スイッチのremote-idの値を指定します。クライアントから受信したパケットにオプション82フィールドがない場合は、スイッチは、ユーザー指定の値を挿入します。クライアントがすでにオプション82の値を挿入している場合は、スイッチは、この値をユーザー指定の値に置き換えます。

## 設定例

```
...
vlan 11
  name "VLAN11"
  untagged A9-A12
  ip helper-address 10.1.11.10
  ip address 10.1.11.1 255.255.255.0
  exit
vlan 12
  name "VLAN12"
  untagged A13-A16
  ip helper-address 10.1.11.10
  ip address 10.1.12.1 255.255.255.0
  exit
...
dhcp-snooping
dhcp-snooping authorized-server 10.1.11.10
dhcp-snooping database file "tftp://10.1.11.10/core-bind.db"
dhcp-snooping option 82 untrusted-policy replace remote-id subnet-ip
dhcp-snooping vlan 11 12
...
interface A1
  dhcp-snooping trust
  exit
```

### この例の設定:

- DHCPスヌーピングが有効
- 2つのVLANに適用
- 信頼されているポート
- 認可サーバー
- TFTPサーバーに保存されているバインディングデータベース
- 受信したオプション82の値を置き換え
- IPヘルパーアドレスが設定されている

このスライドは、DHCPスヌーピングが有効になり、設定されているスイッチのコンフィギュレーションファイルの一部を示しています。

スイッチは、VLANの定義に基づいて、VLAN11およびVLAN12からIPアドレス10.1.11.10のDHCPサーバーにDHCP要求をリレーします。このサーバーはVLAN11にあり、信頼されているポートに接続しています。

スイッチは、VLAN 11とVLAN 12でDHCPトラフィックを「スヌーピング」し、攻撃の兆候がないかどうかをチェックします。このチェックの一環として、スイッチは、信頼されていないエンドポイントから送信されたDHCP要求中のオプション82フィールドを探します。オプション82があった場合は、スイッチは、このフィールドの情報を、DHCP要求を受信したVLANに関連付けられている自身のIPアドレスに置き換えます。

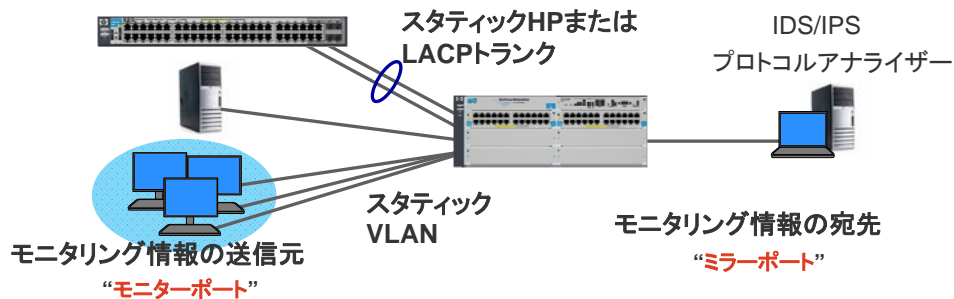
## レガシートラフィックのミラーリング

トラフィックやポートのミラーリング機能は、さまざまなProCurveスイッチおよび他のベンダーのスイッチで使用可能

- 1つのスイッチポートのトラフィックを別のスイッチポートに「コピー」する
- 通常、宛先ポートに接続されているホストは、パケットアナライザーを実行しているPC、またはIDS/IPSデバイス

送信元は通常、1つのポート、ポートのグループ、メッシュポート、スタティックリンク、またはスタティックVLAN

- 宛先は1つのポート

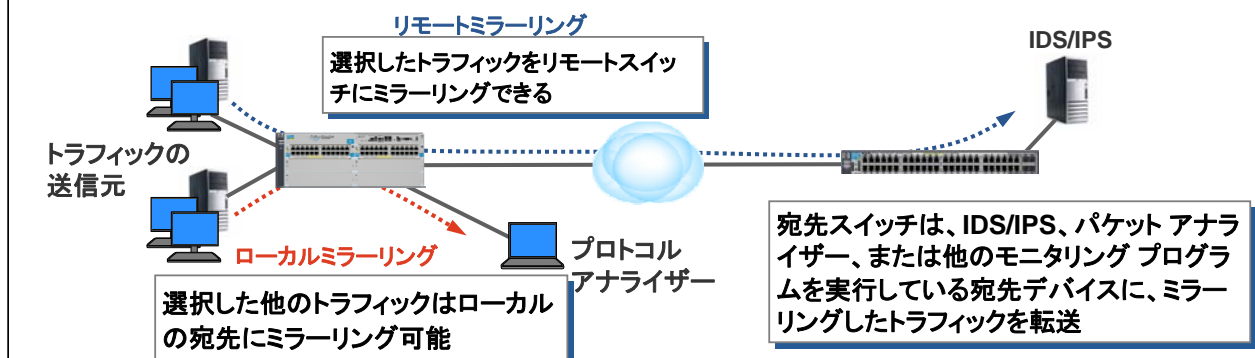


ここでは、トラフィックのローカルミラーリングとリモートミラーリングを行うProCurveのインテリジェントミラーリング機能について説明します。ローカルミラーリングでは、物理ポート、論理ポート、またはVLANからのトラフィックを収集して、そのトラフィックを同じスイッチ上の出力ポートにコピーします。リモートミラーリングでは、同じタイプの送信元からのトラフィックを収集して、リモートスイッチの出力ポートに送信します。送信元から宛先(出力)ポートに送信されたトラフィックは、さまざまな基準でフィルタリングできます。

従来型のトラフィックミラーリング(ポートミラーリングとも呼ばれる)は、トラフィックをモニタリングして、脅威の検出、問題のトラブルシューティング、ネットワーク管理を行う場合に主に使用されています。たとえば、PC上でネットワークプロトコルアナライザーを使用して、ミラーリングしたデータストリームを検証し、障害の発生しているネットワークのトラブルシューティングを行う場合などです。

## インテリジェントミラーリング

- インテリジェントミラーリングでは、トラフィックをローカルに「ミラーリング」および/または複数のリモートスイッチに送信。
- 複数のモニタリングセッションを送信元スイッチで開始可能。
- ミラーリング情報を宛先に送信する前に、送信元トラフィックをフィルタリング可能。
  - ポートまたはVLANに基づく入力および/または出力モニタリング
  - ACLを使用した入力モニタリング
- インテリジェントミラーリングは、各スイッチのポートをモニタリングする必要をなくし、必要なセキュリティ機器の数を削減



インテリジェントミラーリング機能は、トラフィックをモニタリングして、脅威の検出、問題のトラブルシューティング、ネットワーク管理を行うことを可能にします。たとえば、リモートサイトにあるPC上でネットワークプロトコルアナライザーを使用して、ミラーリングしたデータストリームを検証し、障害の発生しているネットワークのトラブルシューティングを行うことができます。

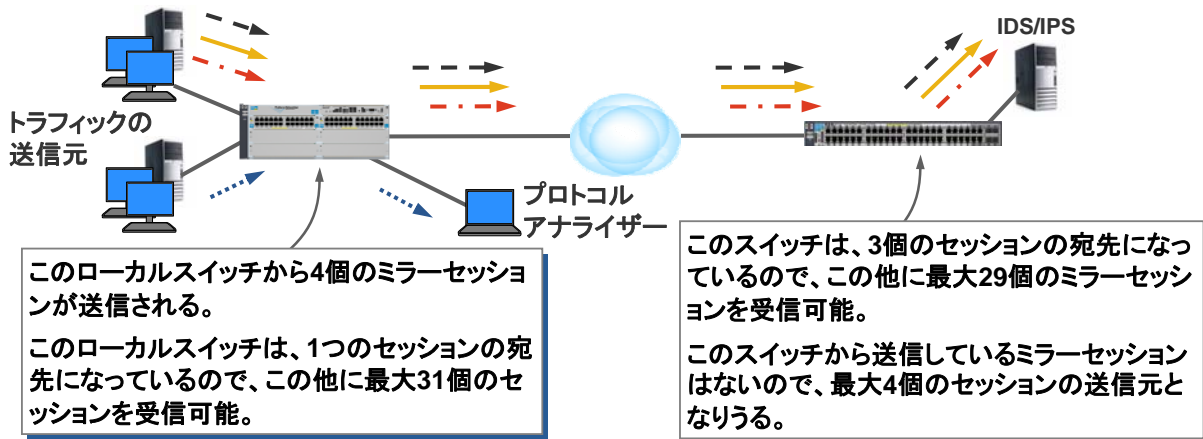


## インテリジェントミラーリング: セッションのサポート

各スイッチは以下になりうる

- 最大4個のミラーセッションの送信元。宛先はローカルスイッチまたは別のスイッチ
- 最大32個のミラーセッションの宛先

複数のミラーセッションを設定して同じ出力ポートを使用するようにするか、または複数の出力ポート間で「ロード バランシング」を行うことが可能

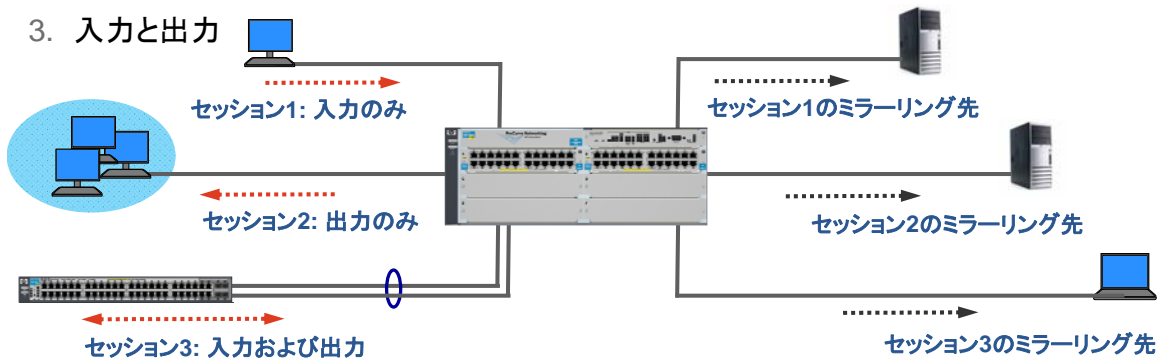


各スイッチは、最大4個のミラーセッションの送信元になることができます。ミラーセッションは、データストリームを管理する送信元/宛先スイッチに従って定義されます。

## トラフィックの送信方向に基づくフィルタリング

モニタリング対象となる送信元のトラフィックは、その送信方向に基づいてフィルタリング可能

1. 入力のみ
2. 出力のみ
3. 入力と出力



モニタリング対象となる送信元は通常、1つのポート、ポートのグループ、メッシュポート、トランク、またはVLAN

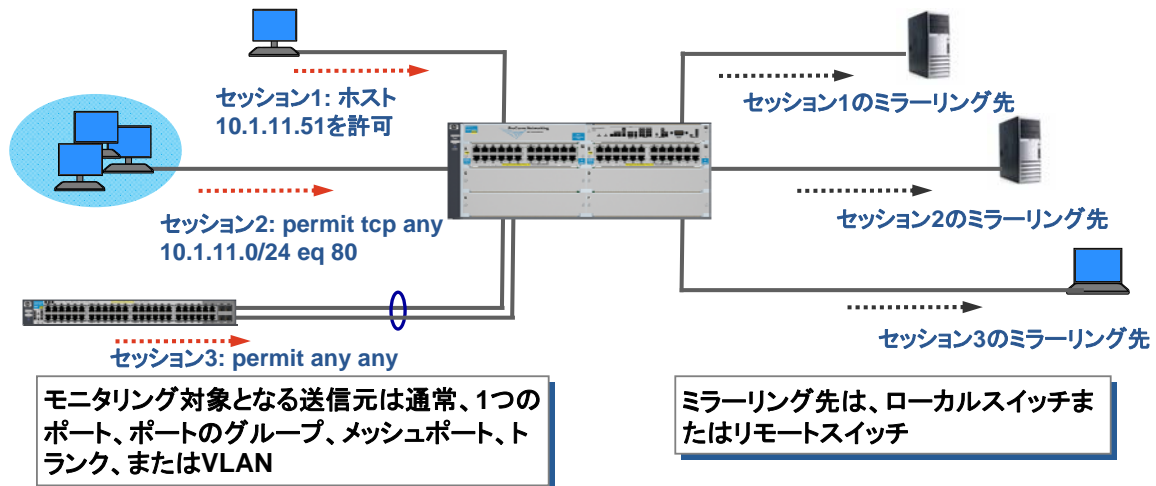
ミラーリング先は、ローカルスイッチまたはリモートスイッチ

インテリジェントミラーリングの主な利点の1つは、送信元で収集したモニタリング対象のトラフィックを「フィルタリング」できることです。対象とするトラフィックを特定する2つのオプションがあります。

## ACLを使用したトラフィックのフィルタリング

モニタリング対象の送信元のトラフィックをフィルタリングする別の方法として、ACLを使用可能

- 入カトラフィックのみを収集可能
- 標準ACLおよび拡張ACLを使用可能
- VLANの場合は、VACL(ブリッジング)またはRACL(ルーティング)を適用可能



モニタリング対象のトラフィックを送信方向に基づいてフィルタリングする代わりに、標準ACLまたは拡張ACLを使用できます。ACLを使用すると、モニタリングするトラフィックを非常に詳細なレベルで指定することができます。標準ACLまたは拡張ACLは、ポートのユーザーアクセスを制御する場合と同様の方法で作成します。唯一の違いは、この場合、ACLはユーザーの権限を制御するのではなく、ミラーリング対象とするユーザートラフィックのサブセットを指定する点です。たとえば、拡張ACLでは、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号、プロトコルなどの基準を指定します。

## トラフィックのローカルミラーリング: 設定手順の概要

1. ローカルスイッチでミラーセッションを設定
  - トラフィックの宛先(出力ポート)
2. ローカルスイッチでモニタリング対象とする送信元を設定
  - モニタリング対象とするトラフィックの送信元
  - オプションでトラフィックをフィルタリング(方向またはACL)

### トラフィックの送信元



どこから送信されたか?

- 1つのポート
- ポートのグループ
- メッシュポート
- スタティックリンク
- スタティックVLAN

Switch\_A

ローカルスイッチ



出力ポート

IDS/IPS  
プロトコルアナライザ



方向またはACLで  
フィルタリング

セッション番号  
-- 1~4

宛先ポート

トラフィックのミラーリングを設定するには、主に2つの手順を実行します。最初の手順では、ローカルまたはリモートにあるモニタリング対象トラフィックの送信先となる宛先スイッチを設定します。別のスイッチがフォワーディングしたミラーリング対象トラフィックを処理できるように宛先スイッチを設定していない場合は、パフォーマンスが低下する可能性があります。これは、宛先スイッチに接続しているデバイス(稼働中のIDS/IPSまたはネットワークプロトコルアナライザ)宛の packets を宛先スイッチが認識できないためです。

2番目の手順では、送信元スイッチを設定します。トラフィックをローカルミラーリングする場合、これは同じスイッチになります。この手順では、ミラーセッション番号およびミラーセッションの宛先を定義します。トラフィックのローカルミラーリングでは、宛先は同じスイッチ上のポートになります。リモートトラフィックミラーリングの場合は、宛先は別のスイッチになります。

## トラフィックのローカルミラーリング: ミラーセッションと出力ポート

手順1: ミラーセッションと出力ポートを指定

```
mirror <1-4> [name <name>] port <port-id>
```

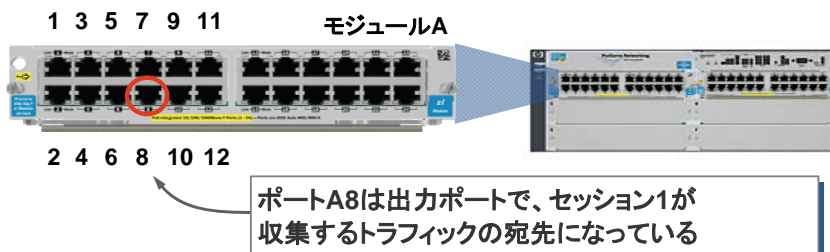
### オプション

<1-4> 1~4の値を使用してミラーセッションを指定

<name> セッションを特定しやすくするための名前

<port-id> ローカルスイッチの出力ポート

```
Switch_A(config)# mirror 1 port a8
```



トラフィックのローカルミラーリングを設定する場合は、まず、グローバルコンフィギュレーションレベルでmirrorコマンドを使用して出力ポートを設定します。コマンドに"no"を付けて実行すると、ミラーセッションおよびそのセッションに以前に割り当てたミラー対象の送信元が削除されます。

この手順は、送信元インターフェイスを定義する前に実行する必要があります。最初に送信元インターフェイスを設定しようとする、指定したセッション番号に対して宛先を指定しないとコマンドが適用されないことを示すメッセージがCLIに表示されます。

## トラフィックのローカルミラーリング: トラフィックの送信元とフィルタリング

手順2: 送信元の「インターフェイス」(「ポート」またはVLAN)、およびフィルタリングのタイプ(トラフィックの方向またはACL)を指定

```
[interface <port-id | trunk-id | mesh> | vlan <vid>] monitor
  all <in | out | both> mirror <1-4> [<1-4> ...]
```

— または —

```
[interface <port-id | trunk-id | mesh> | vlan <vid>] monitor
  ip access-group <acl-id> mirror <1-4> [<1-4> ...]
```

### オプションの説明

|                                    |   |
|------------------------------------|---|
| interface <port-id / trunk / mesh> | ポートID、トランク名、HPメッシュを送信元として指定する場合に使用  |
| vlan <vid>                         | VLANを送信元として指定する場合に使用  |
| all [in   out   both]              | 方向に基づいてトラフィックをフィルタリングする場合に使用:<br>in = スイッチが受信するトラフィック<br>out = スイッチから送信されるトラフィック<br>both = すべてのトラフィック |
| ip access-group <acl-id>           | 標準ACLまたは拡張ACLでトラフィックをフィルタリングする場合に使用   |
| <1-4>                              | 以前に定義したミラーセッション   |

トラフィックのローカルミラーリングを設定する2番目の手順では、monitorコマンドを使用して、トラフィックの送信元およびミラーリング対象のトラフィックを指定します。monitorコマンドにはいくつかの形式があります。

まず、トラフィックの送信元を物理/論理インターフェイス(ポート、トランク、メッシュポート)、またはVLANとして指定します。

前者を指定する場合は、interfaceコマンドプレフィックスを使用します。後者を指定する場合は、VLANコマンドプレフィックスを使用します。

次に、モニタリング対象とするトラフィックを指定する方法を選択します。

これは、スイッチから見たトラフィックの送信方向、または標準/拡張ACLを使用して指定します。ACLを使用する場合は、ACLの基準にマッチする受信トラフィックのサブセットのみがミラーリングされます。

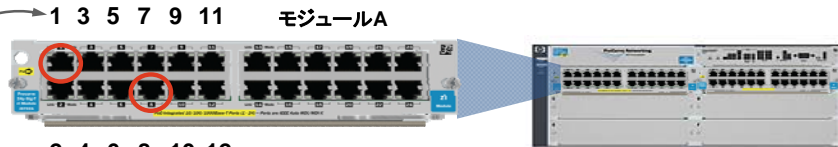
## トラフィックのローカルミラーリング: トラフィックの送信元とフィルタリング (続き)

例:

- 送信元がポートで、方向に基づくフィルタリングを行う場合

```
Switch_A(config)# interface a1 monitor all both mirror 1
```

ポートA1が送信元ポート。  
セッション1が入力/出力トラフィックをモニタリング



ポートA8は出力ポートで、セッション1が収集するトラフィックの宛先になっている

- 送信元がVLANで、定義済みの拡張ACLを使用して入力(暗黙の)トラフィックをフィルタリングする場合

```
Switch_A(config)# vlan 13 monitor ip access-group acl-http mirror 1
```

acl-http = permit tcp any any eq 80

この図は、ローカルミラーリング用にトラフィックの送信元とフィルタリングを設定する場合の2つの例を示しています。

最初の例では、1つの物理ポートがモニタリング対象とする送信元になっており、トラフィックの方向に従ってトラフィックがフィルタリングされます。この例では、入力および出力トラフィックの両方を収集してミラーリングするように指定しています。実際には、ポートA1で送受信するすべてのトラフィックがミラーリングされます。

2番目の例では、1つのVLANがモニタリング対象とする送信元になっており、拡張ACLを使用してトラフィックがフィルタリングされます。ACLを指定しているため、ACLを構成するアクセス制御リストに従って入力トラフィックのみがミラーリングされます。

。

## トラフィックのローカルミラーリング: 設定の表示

```
Switch_A(config)# show monitor
Network Monitoring
  Sessions  Status      Type  Sources  ACL
  -----  -
  1         active     port  1         no
  2         not defined
  3         not defined
  4         not defined
There are no Remote Mirroring endpoints currently assigned.
```

タイプportは、ローカルミラーセッションであることを示す

[Sources] は、ミラーセッションの基準数を示す

```
Switch_A(config)# show monitor 1
Network Monitoring
  Session: 1   Session Name:
  ACL: no ACL relationship exists
  Mirror Destination: A8 (Port)
  Monitoring Sources  Direction
  -----
  Port: A1           Both
```

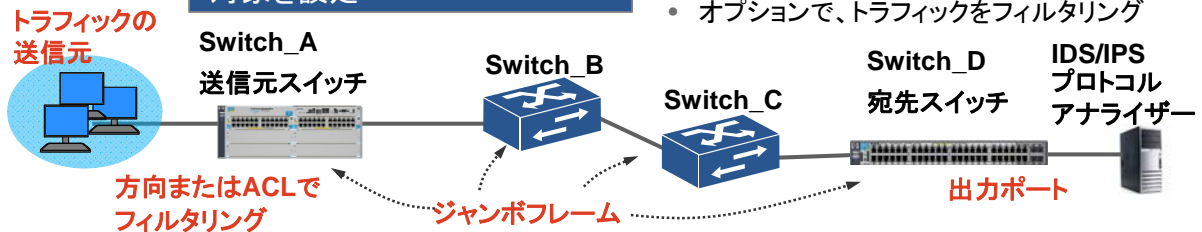
ACLとは異なり、トラフィックの方向に基づいてトラフィックが選択される

show monitorコマンドを使用すると、スイッチのトラフィックミラーリングに関する設定を表示できます。



## トラフィックのリモートミラーリング: 設定手順の概要

1. ジャンボフレームを有効にする
  - 送信元、宛先、および中間スイッチの VLANで行う
2. 宛先スイッチでミラーセッションを設定
  - トラフィックの宛先 (出力ポート)
  - トラフィックが使用するVLANまたはサブネット
3. 送信元スイッチでミラーセッションを設定
  - セッション番号
  - 宛先スイッチへの一致パラメーター
4. 送信元スイッチにモニタリング対象を設定
  - モニタリング対象とするトラフィックの送信元
  - オプションで、トラフィックをフィルタリング



トラフィックのリモートミラーリングの設定は、ローカルトラフィックのミラーリングよりも手順が多く複雑です。トラフィックのリモートミラーリングは、Cisco SPANに類似しています。

トラフィックのリモートミラーリングの設定手順は以下のようになります。

必要に応じてジャンボフレームを有効にする

ローカルミラーセッションを設定する

ミラーリング対象とする送信元を設定する

モニタリング対象とする送信元を設定する



## 確認テスト

## 確認テスト1

ProCurveスイッチのIPヘルパーアドレスはどこで割り当てますか。

- A. インターフェイスコンテキスト内
- B. ポートコンテキスト内
- C. VLANコンテキスト内
- D. グローバルコンテキスト内

## 確認テスト1の解答

正解: C

## 確認テスト2

HP ProCurveのインテリジェントミラーリングについて適切に説明しているのはどれですか。(当てはまるものをすべて選択)

- A. トラフィックをローカルにミラーリングおよび/または複数のリモートスイッチに送信する
- B. 複数のモニタリングセッションを送信元スイッチで開始可能
- C. 送信元トラフィックは、ミラーリング先に送信する前にフィルタリング可能
- D. ポートまたはVLANに基づく入力および/または出力モニタリングを行う
- E. ACLを使用して入力モニタリングを行う

## 確認テスト2の解答

正解: A、B、C、D、E

## 確認テスト3

以下の手順を、トラフィックのリモートミラーリングを設定する場合の適切な順番に並べ替えてください。

- 宛先スイッチでミラーセッションを設定
- 送信元スイッチでモニタリング対象を設定
- ジャンボ フレームを有効にする
- 送信元スイッチでミラーセッションを設定

## 確認テスト3の解答

1. ジャンボ フレームを有効にする
2. 宛先スイッチでミラーセッションを設定
3. 送信元スイッチでミラーセッションを設定
4. 送信元スイッチでモニタリング対象を設定



## モジュール5-6: 使用方法と設定方法

「DHCPとインテリジェントミラーリング」終了



# モジュール5-7: 使用方法と設定方法

## OSPFを使用したルーティング



ここでは、OSPFを使用したルーティングについて説明します。Cisco製品のエキスパートであれば、このプロトコルに習熟しているはずですが、ProCurveとCiscoでは動作にいくつかの違いがあるので、設定例と共に説明します。

## IPルーティングの有効化

デフォルトでは、ProCurveスイッチでは、IPルーティングが無効になっている

有効にする方法:

```
Switch(config)# ip routing
```

ルーティングが有効になっているかどうかを確認する方法:

```
Switch(config)# show ip
Internet (IP) Service
IP Routing :Enabled

Default TTL      : 64
Arp Age         : 20
Domain Suffix   :
DNS server      :

VLAN             | IP Config  IP Address   Subnet Mask   Proxy ARP
-----+-----
DEFAULT_VLAN    | Manual     10.1.1.1     255.255.255.0 No No
```

スイッチでは、IPルーティングを必ず有効にする必要があります。スイッチに直接接続しているルートと1つ以上のスタティックルートを使用する簡単なルーティングを行う場合でも、ネットワークのディストリビューションレイヤーまたはコアレイヤーで複雑なルーティングを行う場合でもこの設定が必要です。

ProCurveスイッチとCiscoスイッチでは、CLIのグローバルコンフィギュレーションレベルで ip routing コマンドを実行すると、IPルーティングを簡単に有効にできます。ProCurveスイッチでは、show ip コマンドを使用してIPルーティングが有効になっているかどうかを確認できます。

## サブネット間のルーティング: 要件

VLANに設定するIPアドレスの例 :

```
Switch(config)# vlan 11 ip address 10.1.11.1/24
Switch(config)# vlan 12 ip address 10.1.12.1/24
```

```
Switch(config)# show run

vlan 11
 name "VLAN11"
 untagged A1-A6
 tagged A24,B24
 ip address 10.1.11.1 255.255.255.0
 exit
vlan 12
 name "VLAN12"
 untagged B1-B6
 tagged A24,B24
 ip address 10.1.12.1 255.255.255.0
 exit
```

さらに、タグ無およびタグ付にするポートを割り当て

```
Switch(config)# show ip
...
VLAN | IP Config | IP Address | Subnet Mask | Proxy ARP
-----+-----
DEFAULT_VLAN | Manual | 10.1.1.1 | 255.255.255.0 | No No
VLAN11 | Manual | 10.1.11.1 | 255.255.255.0 | No No
VLAN12 | Manual | 10.1.12.1 | 255.255.255.0 | No No
```

スイッチが複数のVLAN間でルーティング(フォワーディング)を行う基本的なルーティングでは、各VLANにIPアドレスを割り当てる必要があります。この簡単な例では、2つのVLANをProCurveスイッチに追加しています。また、エンドユーザーデバイスに対応するエッジポートはタグ無になっています。コアにある他のスイッチに接続するアップリンクポートは、この新しい2つのVLANでタグ付けされています。

## ループバックインターフェイスの使用

最大8個のループバックインターフェイスを設定可能

```
Switch(config)# interface loopback 1 ip address 10.1.100.1  
Switch(config)# interface loopback 7 ip address 10.1.100.17
```

ProCurveとCiscoでは、OSPFルーターIDとして使用するループバックの選択方法が異なる

3500yl、5400zl、6200ylシリーズのスイッチでは、最大8個のループバックインターフェイスを設定できます。

ループバックは、OSPFを使用しているときにルーターIDを選択する場合などに使用します。ルーターIDを設定していない場合は、ProCurveスイッチは、IPアドレスを持つ設定済みVLANから1つのアドレスを選択して割り当てるか、またはIPアドレスが設定されているループバックインターフェイスから選択します。ProCurveデバイスによって詳細が異なりますが、ProCurveスイッチの最新モデルのほとんど(特に3500yl、5400zl、6200ylシリーズ)では、ProCurveのルーターIDの選択プロセスで、設定済みループバックインターフェイスの最も小さいIPアドレスが選択されます。これは、設定済みの最も大きいアドレスを選択するCiscoデバイスとは逆になります。DRとBDRの選択に関するOSPFプロセスは標準に従っていますが、ルーターIDのインターフェイス番号の選択方法は、ProCurveとCiscoでは異なります。これはOSPF標準でこのような柔軟性を許容しているためです。

## ルーティングテーブルの表示

設定されているVLANとループバックインターフェイスを示すルーティングテーブル

```
Switch(config)# show ip route
```

IP Route Entries

| Destination    | Gateway | VLAN | Type      | Sub-Type | Metric | Dist. |
|----------------|---------|------|-----------|----------|--------|-------|
| 10.1.100.1/32  | lo1     |      | connected |          | 1      | 0     |
| 10.1.100.17/32 | lo7     |      | connected |          | 1      | 0     |
| 10.1.11.0/24   | VLAN11  | 11   | connected |          | 1      | 0     |
| 10.1.12.0/24   | VLAN12  | 12   | connected |          | 1      | 0     |
| 127.0.0.0/8    | reject  |      | static    |          | 0      | 0     |
| 127.0.0.1/32   | lo0     |      | connected |          | 1      | 0     |

デフォルトループバック(lo0)インターフェイス

直接接続しているルートが、設定済みのIPアドレスに基づいて自動的に生成された

show IP route コマンドは、IPルーティングテーブルで現在アクティブになっているすべてのエントリを表示します。この例では、VLANとループバックインターフェイスから生成された直接接続ルートの一覧が表示されています。

## スタティックルートの設定

```
ip route <dest-ip-address>/<mask-bits> <gateway-ip> [distance <1-255>]
```

— または —

```
ip route <dest-ip-address> <decimal-mask> <gateway-ip> [distance <1-255>]
```

例:

↑ ネットワーク、サブネット、またはホスト固有

↑ ネクストホップルーターまたはローカルインターフェイス

↑ 管理ディスタンス、デフォルト = 1

```
Switch(config)# ip route 10.2.11.0/24 10.1.1.2
```

ネットワークルート

```
Switch(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.3
```

デフォルトルート

```
Switch(config)# show ip route
```

IP Route Entries

| Destination  | Gateway  | VLAN | Type   | Sub-Type | Metric | Dist. |
|--------------|----------|------|--------|----------|--------|-------|
| 0.0.0.0/0    | 10.1.1.3 | 1    | static |          | 1      | 1     |
| 10.2.11.0/24 | 10.1.1.2 | 1    | static |          | 1      | 1     |

ProCurveスイッチにスタティックルートを作成するには、ここに示すip routeコマンドを使用します。ここでは2種類のコマンドを示しています。宛先IPアドレスのマスクは、マスクするビット数(CIDR表記)、またはドット区切りの10進数で指定します。

## OSPFの設定

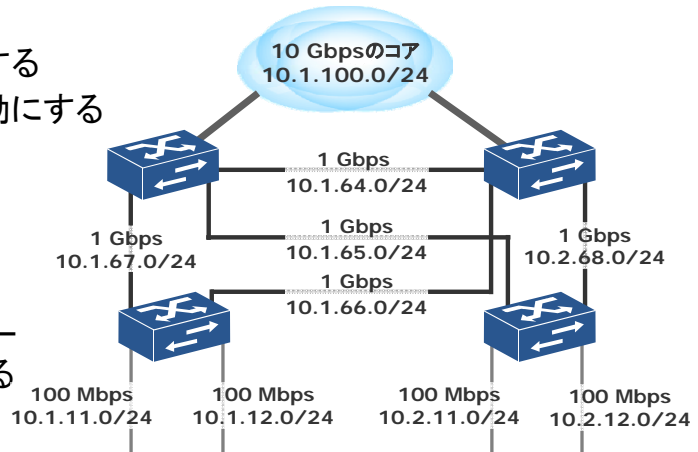
OSPFの設定を行う主な手順:

- OSPFをグローバルに有効にする
- インターフェイスでOSPFを有効にする
- リンクコストを割り当てる
- OSPFステータスを確認する

リンクコスト

- リンク速度に反比例し、ネットワーク全体で一貫している必要がある

| リンク速度    | コスト |
|----------|-----|
| 10 Gbps  | 1   |
| 1 Gbps   | 10  |
| 100 Gbps | 100 |



ProCurveにOSPFを設定する場合の主な手順は4つあります。

1, OSPFをグローバルに有効にする—グローバルコンフィギュレーションレベルから `router ospf` コマンドを使用して設定します。

2, インターフェイスでOSPFを有効にする—`router ospf` コマンドを実行してOSPFをグローバルに有効にすると、グローバルOSPFコンテキストに入ります。そのコンテキストから、`area` コマンドを使用して、自律システム内でルーティングスイッチを1つ以上のOSPFエリアに割り当てます。

ルーティングスイッチは、1つのエリアまたは複数のエリアに所属できます。割り当てた特定のエリアに参加するには、1つ以上のVLANまたはサブネットを設定して、それぞれを該当するエリアに割り当てる必要があります。

3, リンクコストを割り当てる—コストを使用して、インターフェイス経由でパケットを送信する場合に必要なオーバーヘッドを指定します。

4, OSPFステータスを確認する—`show` コマンドにはさまざまなオプションがあり、OSPFの設定や現在の状態を調査できます。



## スイッチのコンフィギュレーションファイル: OSPFエントリー

```

router ospf
  area backbone
  exit

vlan 11
  untagged a1-a20
  tagged a24
  ip address 10.1.11.1 255.255.255.0
  ip ospf 10.1.11.1 passive
  ip ospf 10.1.11.1 area backbone
  ip ospf cost 10
  exit

vlan 64
  tagged a24
  ip address 10.1.64.1 255.255.255.0
  ip ospf 10.1.64.1 area backbone
  ip ospf cost 10
  exit

interface loopback 0
  ip address 10.1.100.1
  ip ospf 10.1.100.1 area backbone
  exit
  
```

OSPFをグローバルに有効化 – プロセスID不要

OSPFを送信させないVLANに対してOSPFをパッシブに設定。この場合、エンドユーザーサブネットなどのネットワークはOSPFアドバタイズメントに含まれる

OSPFリンクコストを設定 (デフォルト = 1)

別のVLANでOSPFを設定

ループバックインターフェイスでOSPFを設定  
最小のループバックIPアドレスをOSPFルーターIDとして使用

上記のCLI出力は、スイッチのコンフィギュレーションファイルの一部を示しています。OSPFに関連する一般的なエントリー部分を強調しています。

router ospfコマンドを実行すると、OSPFがグローバルに有効になります。上記のサブエントリー"area backbone"は、(OSPFコンテキストで) area backboneコマンドを実行してスイッチをOSPFバックボーンに割り当てたことを示しています。ProCurveでは、「プロセスID」を使用しないので注意してください。

各VLANコンテキスト内で、area <ospf-area-id > コマンドを実行すると、自律システム内で、対応するインターフェイスにOSPFを割り当てて、ルーティングスイッチを1つ以上のOSPFエリアに割り当てることができます。エリアIDは、そのエリアに所属するVLANのIPアドレスにマッチさせる値(この例の場合)、または特定のAS内のエリアで使用する番号付けシステムに従った値になります。エリアIDは、整数またはドット区切りの10進数の形式で指定します。たとえば、エリアIDとして256を入力した場合は、スイッチの設定では 0.0.1.0になり、エリアIDとして0または0.0.0.0を入力した場合は、そのルーティングスイッチをバックボーンエリアに自動的に参加させます。

## OSPFステータスの確認

### OSPFが有効になっている場所の確認

```
Switch(config)# show ip ospf interface
```

OSPF Interface Status

| IP Address | Status  | Area ID  | State | Auth-type | Cost | Pri | Passive |
|------------|---------|----------|-------|-----------|------|-----|---------|
| 10.1.11.1  | enabled | backbone | DR    | none      | 1    | 1   | yes     |
| 10.1.64.1  | enabled | backbone | DR    | none      | 1    | 1   | no      |
| 10.1.100.1 | enabled | backbone | LOOP  | none      | 1    | 1   | no      |

### 隣接関係の確認

```
Switch(config)# show ip ospf neighbor
```

OSPF Neighbor Information

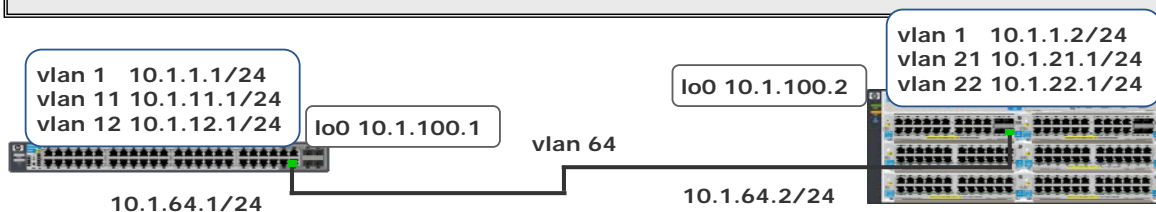
| Router ID  | Pri | IP Address | NbIfState | State | Rxmt Qlen | Events | Helper Status |
|------------|-----|------------|-----------|-------|-----------|--------|---------------|
| 10.1.100.2 | 1   | 10.1.64.2  | DR        | FULL  | 0         | 5      |               |

“FULL”以外になっている場合は、問題が発生していることを示す

このスライドは、show ip ospf コマンドにオプションやサブオプションを指定する場合の例を2つ示しています。

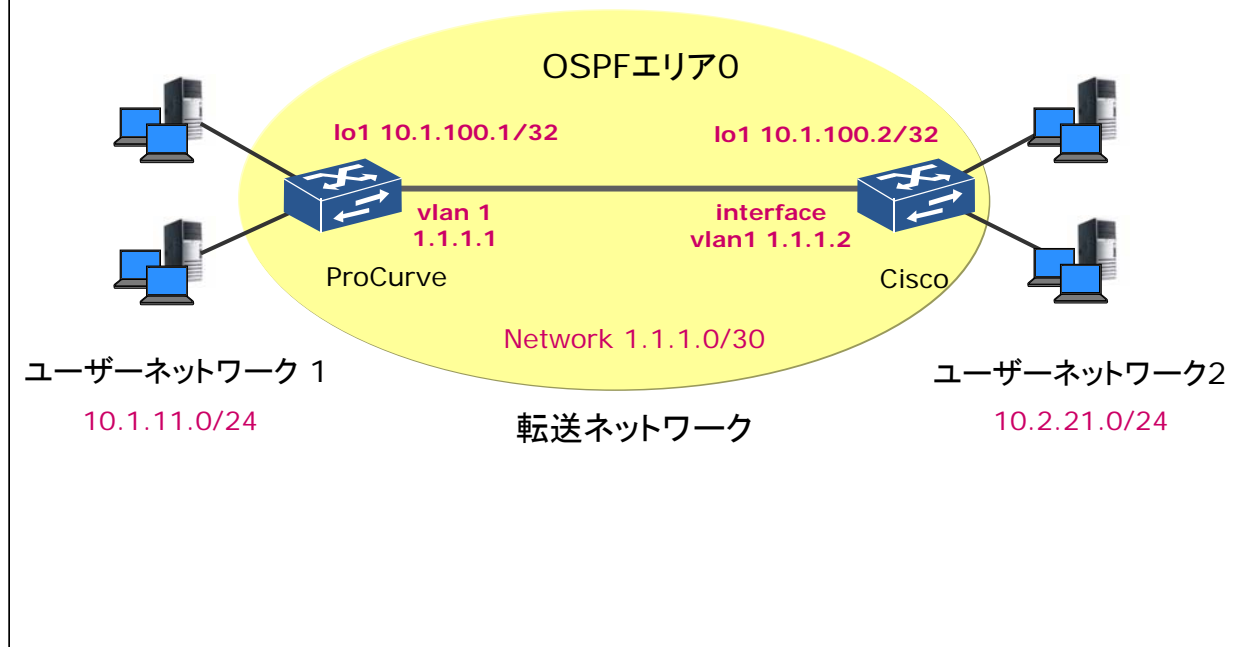
## OSPFエントリーのあるルーティングテーブル

```
Switch(config)# show ip route
IP Route Entries
-----
Destination          Gateway          VLAN Type      Sub-Type  Metric  Dist.
-----
10.1.100.1/32        lo1              connected    1         0
10.1.100.17/32       lo7              connected    1         0
10.1.11.0/24         VLAN11          11          connected    1         0
10.1.12.0/24         VLAN12          12          connected    1         0
127.0.0.0/8          reject          static       0         0
127.0.0.1/32        lo0              connected    1         0
10.1.21.0/24         10.1.64.2       64          ospf         IntraArea 2         110
10.1.22.0/24         10.1.64.2       64          ospf         IntraArea 2         110
10.1.100.2/32        10.1.64.2       64          ospf         IntraArea 2         110
```



この図のshow ip routeコマンドの出力は、OSPFが設定され、最低1つの隣接OSPFルーターと通信を確立しているスイッチのルーティングテーブルにあるOSPFエントリーの例を示しています。

## OSPFの設定シナリオ



ここには、ProCurveスイッチとCiscoスイッチにOSPFを設定して相互運用する場合のシンプルなネットワークを示しています。

## OSPF設定の比較

|   | ProCurve  | Cisco  |
|---|---|--|
| 1 | <pre>router ospf   area backbone interface loopback 1   ip address 10.1.100.1   ip ospf 10.1.100.1 area backbone vlan 1   ip address 10.1.1.1 255.255.255.0   ip ospf 10.1.1.1 area backbone   ip ospf cost 10 vlan 11   ip address 10.1.11.1 255.255.255.0   ip ospf 10.1.11.1 passive   ip ospf 10.1.11.1 area backbone   ip ospf cost 10</pre> | <pre>router ospf 1   passive-interface vlan21   network 10.1.1.2 0.0.0.0 area 0   network 10.1.21.2 0.0.0.0 area 0   network 10.1.100.2 0.0.0.0 area 0 interface loopback1   ip address 10.1.100.2 255.255.255.255   ip ospf cost 10 interface vlan1   ip address 10.1.1.2 255.255.255.0   ip ospf cost 10 interface vlan21   ip address 10.2.21.2 255.255.255.0   ip ospf cost 10</pre> |

1. ProCurveでは、グローバルコンフィギュレーションレベルで実行する“router”コマンドでインスタンス番号を指定しません(上記の1を参照)。

ProCurveでは、router ofpf

Ciscoでは、router ospf 1

2. ProCurveでは、“VLAN” インターフェイス内でネットワークを設定しますが、Ciscoでは、グローバルコンフィギュレーションレベルでnetworkコマンドを使用して設定します(上記の2を参照)。

OSPFの設定方法の詳細については、以下のマニュアルを参照  
<http://cdn.procurve.com/training/Manuals/3500-5400-6200-8200-MRG-Jan08-5-IP-Routing.pdf>

その他の設定例については、上記のリンクが示すファイルを参照してください。



## 確認テスト

## 確認テスト1

ProCurveスイッチで、ルーティングテーブルの情報に基づいてIPパケットをフォワーディングする機能を有効にする場合、以下のどのコマンドを使用しますか。

- A.Switch(config)# ip routing
- B.Switch(config-if)# ip routing
- C.Switch(config-vlan)# ip routing



## 確認テスト1の解答

正解: A

## 確認テスト2

OSPFに含める「ネットワーク」または「VLAN」はどのように設定しますか。

- A.OSPFルーティング用のグローバルコンテキストで“network command”を指定
- B.VLANコンテキストで “ip ospf address area” を指定
- C.router ospf process-idコンテキストでip ospf address area コマンドを実行

## 確認テスト2の解答

正解: B

## 確認テスト3

ProCurveでは、複数のループバックインターフェイスが設定されている場合、その最も小さいIPアドレスをルーターIDとして選択します。

- A. 正解
- B. 不正解

## 確認テスト3の解答

正解: A

## モジュール5-7: 使用方法と設定方法

「OSPFを使用したルーティング」終了

