VLAN（拡張機能）

学習内容

1. VTPの概要と仕組み
2. VTPの基本設定
3. VLAN間ルーティングの基礎
4. サブインターフェースによるルーティング

01

VTPの概要と仕組み

VTP（VLAN Trunking Protocol）とは？

スイッチ間でVLAN情報を自動的に同期し、管理を一元化するシスコ独自のプロトコル

1台のスイッチでVLANを設定すれば、他のスイッチにも**自動的に情報が伝播**

VTPドメイン名が同じスイッチ間でのみ情報が同期される

スイッチ間の接続は**トランクポート**である必要がある

トランクポートを通じて「**VTPアドバタイズメント**」を交換し情報を同期

VTPを構成する3つの動作モード

各スイッチは「サーバ」「クライアント」「トランスペアレント」のいずれかのモードで動作します

サーバモード (デフォルト)	クライアントモード	トランスペアレントモード
VLANの作成・削除・変更が可能。自身の情報を他のスイッチへ通知し、他からの通知で自身も同期する**司令塔**の役割	自身でのVLAN設定は不可。サーバから受信した情報で同期し、その情報を他のスイッチへ転送する**受け身**の役割	VLAN設定は可能だが他へ通知しない。受信した通知も自身には反映せず転送するのみ。**独立してVLANを管理**するモード

設定の鍵：コンフィグレーションリビジョン番号

VLAN情報の新旧を判断するためのバージョン番号。意図しない情報の上書きに注意が必要です

仕組みと役割

サーバモードのスイッチでVLAN設定を変更するたびに**番号が1ずつ増加**

VTPアドバタイズメントで配布され、スイッチは自身の番号と比較

自身より**大きい番号**を受信すると、その情報を最新と判断してVLAN情報を上書き

リスクと対策

【リスク】リビジョン番号が大きいスイッチを後から接続すると、**既存のVLAN情報が全て消える**可能性がある

【対策】新規スイッチは接続前にトランスペアレントモードに変更し、**リビジョン番号を0にリセット**することが推奨される

VTPの補足機能とバージョン

帯域幅の節約に役立つ「プルーニング」と、機能が拡張されたバージョン

VTPプルーニング

トランクリンクを通る**不要なVLANのトラフィックを自動的に抑制**する機能。特定のVLANに属するホストが存在しないスイッチへの無駄な転送を防ぎ、帯域を節約

VTPバージョン

v1が基本、**v2**でトークンリング等に対応。**v3**では拡張VLAN（1006〜4094）もサポート。同一ドメイン内では**バージョンを揃える**必要がある点に注意

02

VTPの基本設定

VTPの基本設定フロー

VTPを利用するには、ドメイン名やモードなどを設定します。ここでは代表的な設定手順を解説します

1. **VTPバージョンの設定**: `vtp version [1|2|3]`
2. **VTPドメイン名の設定**: `vtp domain domain-name` (大文字/小文字を区別)
3. **VTPモードの設定**: `vtp mode [server|client|transparent]`
4. **VTPパスワードの設定 (任意)**: `vtp password password`
5. **VTPプルーニングの有効化 (任意)**: `vtp pruning`

設定内容の確認方法 (show vtp status)

設定後、`show vtp status`コマンドで現在の動作状態を詳細に確認できます

【コマンド出力例】

VTP Version : 2

Configuration Revision : 5

Operating Mode : Server

VTP Domain Name : ABC

VTP Pruning Mode : Enabled

【確認ポイント】

稼働バージョン: 現在動作しているVTPバージョン

リビジョン番号: 最新の更新番号。同期の鍵

動作モード: Server, Client, Transparent のいずれか

ドメイン名: 設定したVTPドメイン名

プルーニング状態: 有効か無効か

03 VLAN間ルーティングの基礎

VLAN間ルーティングの必要性

VLANを作成すると、各VLANは独立したネットワークとなり、デフォルトではVLAN間の通信はできません

VLANはそれぞれが**独立したブロードキャストドメイン**を形成する

L2スイッチだけでは、異なるVLANに属する端末同士は直接通信できない

異なるVLAN間で通信を行うには、IPパケットを中継する**ルーティング機能**が必要

この役割を担うのが、**ルータ**や**L3スイッチ**といったL3機器

解決策：サブインターフェースとは？

1本の物理リンクで複数のVLANのトラフィックを扱うための「Router on a Stick」構成

課題

VLANの数だけルータの物理インターフェースが必要になると、コストもポートも非効率

サブインターフェース

ルータの**1つの物理インターフェースを論理的に分割**し、VLANごとに仮想的なインターフェースとして利用する機能

カプセル化

各サブインターフェースで、どのVLANタグ（**encapsulation dot1q**）を処理するかを指定。これにより、1本のケーブルで複数VLANのトラフィックを正しく識別できる

サブインターフェースによるルーティング設定手順

ルータ側で、VLANごとにサブインターフェースを作成し、IPアドレスとカプセル化タイプを設定します

サブインターフェース作成	カプセル化タイプ指定	IPアドレス設定
`interface FastEthernet0/0.10` のように、物理インターフェースにドットと番号を付けて作成	`encapsulation dot1q 10` のように、どのVLAN IDのトラフィックを扱うか指定	`ip address 192.168.10.254 ...` のように、VLANのデフォルトゲートウェイとなるIPアドレスを設定

設定例の比較：ISL vs IEEE802.1Q

トランキングプロトコルによってルータ側の設定、特にカプセル化の指定方法が異なります

ルータ側設定 (802.1Q)

`interface FastEthernet0/0.10`

`encapsulation dot1q 10`

`ip address 192.168.10.254 ...`

ネイティブVLANの場合:

`encapsulation dot1q 1 native`

スイッチ側設定 (共通)

`interface FastEthernet0/24`

`switchport mode trunk`

`switchport trunk encapsulation dot1q` (機種による)

ルータと接続するポートを**トランクモード**に設定

障害発生時のトラフィック動作

構成のどこに障害が発生するかによって、通信への影響範囲は異なります

正常時の通信

同一VLAN内の通信: L2スイッチ内で完結。ルータは経由しない

異なるVLAN間の通信: 必ずルータのサブインターフェースを経由してルーティングされる

障害時の影響

スイッチ障害: そのスイッチに接続されている全ての端末が通信不能になる

ルータ障害: **VLAN間ルーティングが停止**。ただし、**同一VLAN内の通信は継続可能**