

## VLAN

### 1. ポート VLAN とタグ VLAN

VLAN(ブイラン:Virtual LAN) はスイッチングハブ(データリンク層)の機能であり, VLAN を利用することにより, 物理的なネットワークに制限されること無く, 論理的なネットワークを構築することが可能となる.

VLAN ではスイッチングハブの通信ポート毎に VLAN ID を割り当て, 同じ VLAN ID を持つ通信ポートが同じネットワークとして認識される(この手法をポート VLAN と呼ぶ). 逆に言えば, VLAN ID の違う通信ポートは違うネットワークに属することになるので, それらの通信ポート間の直接的な通信(データリンク層での通信)は不可能になる(間にルータが必要となる).

複数のスイッチングハブを接続して VLAN を形成する場合には, トランクポート(ベンダーにより呼び方が変わる場合もある)と呼ばれる通信ポートを用意し, そのポートを使ってスイッチングハブ同士を接続する(図 5.11). トランクポート上では, スイッチングハブ内の複数の VLAN のフレームが同じケーブル上を流れる. これらのフレームを区別するために, 各フレームにはそれが属する VLAN を示す 4Byte の VLAN ID のタグ(VLAN タグ)が付加される(この手法をタグ VLAN または VLAN タギングと呼ぶ).

4Byte の VLAN タグが付加されたため, トランクポート上のイーサネットフレームサイズの上限は 1522Byte となる(通常は最大 1518Byte). この 4Byte の拡張が行われる際に, 既存のスイッチが誤作動を起こすのではないかと憂慮されたが, 各ベンダー共データサイズに余裕を持たせてスイッチを設計していたため, それ程の混乱は生じることなく拡張が行われた. これらの VLAN タギングの手法は IEEE802.1Q として標準化されている(図 5.13).

タグ VLAN の応用として, スイッチングハブの通信ポートを全てトランクポートにし, 各ノード(PC)の NIC 側で VLAN タグを処理する方法もある. この場合は, 各ノード(PC)の NIC 每にネットワークを設定でき, 同じ NIC を使用していれば, 場所の移動に関係なくどのスイッチングハブのポートに接続しても, 必ず同じネットワークに参加することになる.

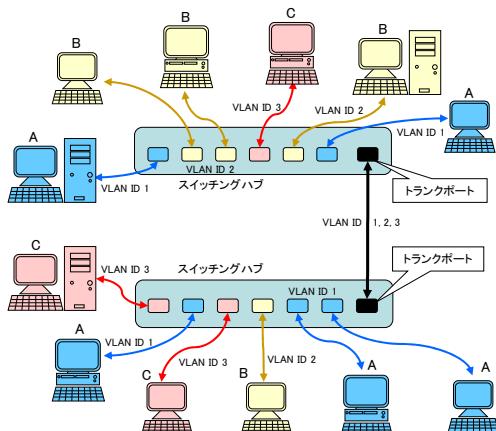


図 5.11 ポート VLAN  
(図中の A,B,C は属するネットワークを表す)

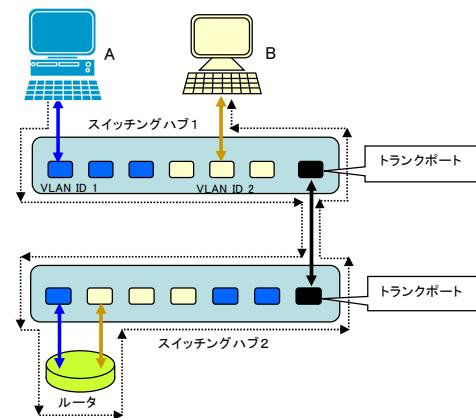


図 5.12 VLAN 環境下でのルーティング  
(A→B の通信)

宛先 Mac ア ドレス(6)	送信元 Mac アドレス(6)	タイプ(2) 0x8100	TCI(2)			タイプ(2)	データ (46~1500)	FCS(4)
			優先度[3]	CFI[1]	VLAN ID [12]			
VLAN タグ								

- ()内の数字は該当フィールドの Byte 長, []は bit 長を表す.
- タイプ: VLAN の場合は 0x8100 となる.
- TCI: Tag Control Information.
- CFI: Canonical Format Indicator. フォーマットを表す. イーサネットの場合は常に 0
- VLAN ID: 0x000 と 0xFFFF は予約されているので, ID として使用できる値は 1~4094.  
通常 1 はデフォルトの VLAN ID としてシステムで使用される場合が多い.

図 5.13 IEEE802.1Q のフレーム構造

## 2. VLAN 環境でのルーティング

VLAN はデータリンク層の機能であるため, 異なった VLAN 間で通信を行う場合にはルータまたは Layer3 のスイッチングハブ (L3 スイッチ, ルータ機能を持ったスイッチングハブ) が必要となる.

例えば, 図 5.12において, ノード A から異なった VLAN 上のノード B へ通信を行う場合, スイッチングハブ 1 にはルータが接続されていないため, ノード A からの通信データはスイッチングハブ 2 に接続されたルータを経由して, 再びスイッチングハブ 1 に戻ってこなければならない(図 5.12 の点線の矢印).

このように VLAN を使用すると非常に柔軟に論理ネットワークを形成することが可能となる一方で, 場合によっては通信効率が悪くなる恐れもある.

## まとめ

- VLAN はスイッチの機能である.
- 物理的なネットワークに制限される事無く, 論理的なネットワークを構築できる.
  - 通常 物理ネットワーク = 論理ネットワーク
  - VLAN 物理ネットワーク ≠ 論理ネットワーク
- ネットワークは VLAN ID により区別される.
- VLAN ID はスイッチのポート毎に割り当てられる. すなわち, ポート毎に所属するネットワークを指定することが出来る.
- ルータが無い場合 (L2 VLAN のみの場合), VLAN 間で通信することはできない.
- VLAN 機能を持つ L3 スイッチを使用すれば, VLAN 間で通信することが可能.
- 一本の線を複数の VLAN で使用可能. VLAN タギング (IEEE802.1Q) を使用する. VLAN タギングではパケットに VLAN ID の書かれたタグを付けることによって, そのパケットがどの VLAN に属するか判別することが出来る. VLAN タギングされたポートをトランクポートまたはタグ付きポート (tagged port) などと呼ぶ.