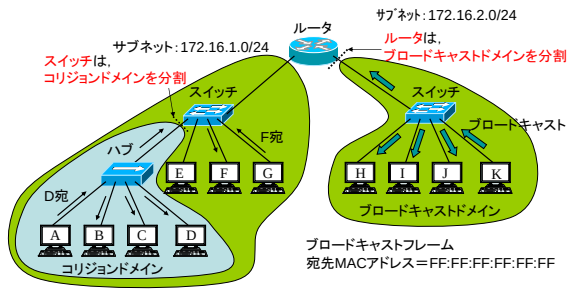
第5回
VLANの機能と使用方法

コリジョンドメインとブロードキャストドメイン
VLANの機能と利点
VLANの設定

ドメイン（領域）の分割



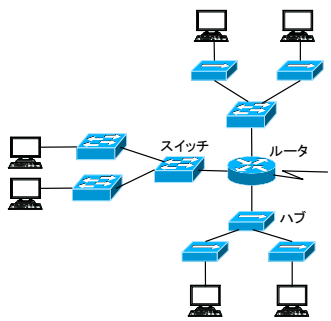
ドメイン（領域）の種類

- コリジョンドメイン：同時に送信したフレームが衝突する範囲
  - コリジョン（衝突），ドメイン（範囲）
- ハブに接続されたホストは同じコリジョンドメインに属する．
  - あるホストが送信したフレームは，全ホストに転送される．
  - そのため，同時に複数のホストがフレームを送信すると衝突が起きる．
- スイッチはコリジョンドメインを分割する．
  - スイッチに接続されたホストは異なるコリジョンドメインに属する．

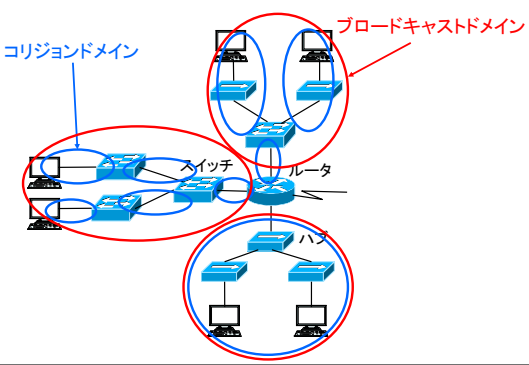
- ブロードキャストドメイン：ブロードキャストフレーム(注)が届く範囲
- スイッチに接続されたホストは同じブロードキャストドメインに属する．
- ルータはブロードキャストドメインを分割する．
  - ルータに接続されたホストは異なるブロードキャストドメインに属する．
  - 通常の運用では，ブロードキャストドメイン＝サブネット

注：宛先MACアドレスがFF:FF:FF:FF:FF:FF（オール1）のフレーム．
同じ情報をネットワーク内の全ホストに届ける（Broadcast：放送）ときに使用する

インターネットワーキングの例



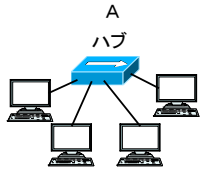
インターネットワーキングの例



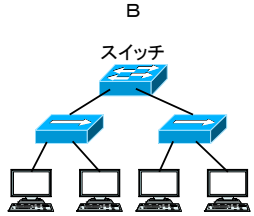
問題：ドメインの識別（1）

次の図で，以下のそれぞれのﾃﾞﾊﾞｲｽが持つｺﾘｼﾞｮﾝﾄﾞﾒｲﾝとﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝの数を挙げなさい．（指定の無いﾃﾞﾊﾞｲｽは全てﾊﾌﾞ）

A

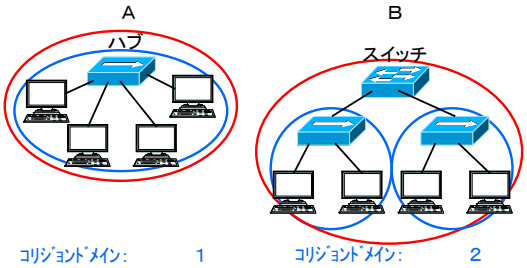


B



問題:ドメインの識別(1)

次の図で，以下のそれぞれのﾃﾞﾊﾞｲｽが持つｺﾘｼﾞｮﾝﾄﾞﾒｲﾝとﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝの数を挙げなさい．(指定の無いﾃﾞﾊﾞｲｽは全てﾊﾌﾞ)

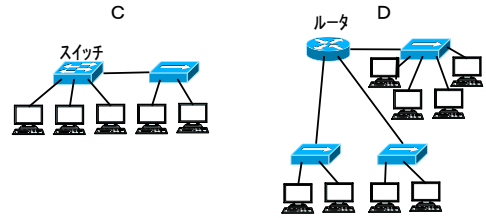


ｺﾘｼﾞｮﾝﾄﾞﾒｲﾝ:　1
ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝ:　1

ｺﾘｼﾞｮﾝﾄﾞﾒｲﾝ:　2
ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝ:　1

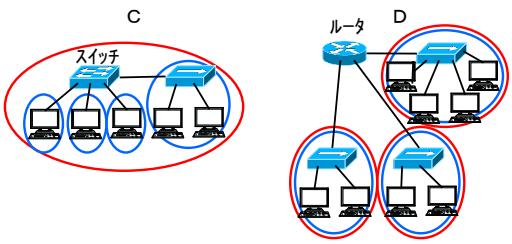
問題:ドメインの識別(2)

次の図で，以下のそれぞれのﾃﾞﾊﾞｲｽが持つｺﾘｼﾞｮﾝﾄﾞﾒｲﾝとﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝの数を挙げなさい．(指定の無いﾃﾞﾊﾞｲｽは全てﾊﾌﾞ)



問題:ドメインの識別(2)

次の図で，以下のそれぞれのﾃﾞﾊﾞｲｽが持つｺﾘｼﾞｮﾝﾄﾞﾒｲﾝとﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝの数を挙げなさい．(指定の無いﾃﾞﾊﾞｲｽは全てﾊﾌﾞ)

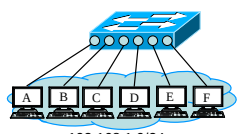


ｺﾘｼﾞｮﾝﾄﾞﾒｲﾝ:　4
ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝ:　1

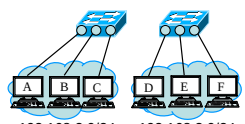
ｺﾘｼﾞｮﾝﾄﾞﾒｲﾝ:　3
ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝ:　3

VLAN

VLANを導入しない場合



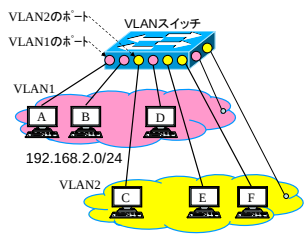
192.168.1.0/24
単一のブロードキャストドメイン



192.168.2.0/24　192.168.3.0/24

ドメインを分けるためには，違うスイッチに収容

VLAN(Virtual LAN)の導入

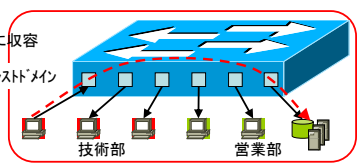


VLAN：仮想的なLANセグメントを作る技術
同じスイッチ内で複数のブロードキャストドメイン
複数のスイッチにまたがったVLANも可能

VLANの必要性(1)

(1)全ﾎｽﾄを1台のｽｲｯﾁに収容

全体で1つのﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝ
(全体で1つのｻﾌﾞﾈｯﾄ)

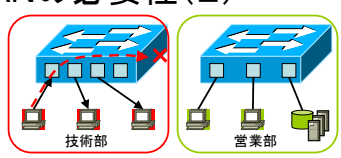


①転送効率
ブロードキャストフレーム(宛先ｱﾄﾞﾚｽ:オール1)(注)が全ホストに届く．
・ﾈｯﾄﾜｰｸ規模が大きいとﾌﾞﾛｰﾄﾞｷｬｽﾄ数が増加する(ﾊﾟﾌｫｰﾏﾝｽの低下)
注:ﾌﾞﾛｰﾄﾞｷｬｽﾄﾌﾚｰﾑは，ARP要求，DHCP要求・DHCP応答などで用いる
②セキュリティ
他部門からのｱｸｾｽ制限ができない
・技術部のPCから営業部のｻｰﾊﾞにｱｸｾｽできてしまう(顧客情報の漏洩など)

VLANの必要性(2)

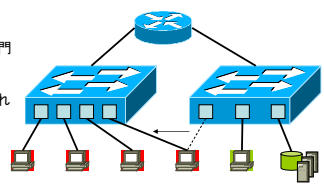
(2－1)複数のｽｲｯﾁを導入
ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝを分割

①転送効率②ｾｷｭﾘﾃｨの
問題は解決
しかし，このままでは，部
門間の通信ができない



(2－2)ｽｲｯﾁ間をﾙｰﾀで接続
ﾙｰﾀのｱｸｾｽ制御機能で他部門
からのｱｸｾｽ制限は可能

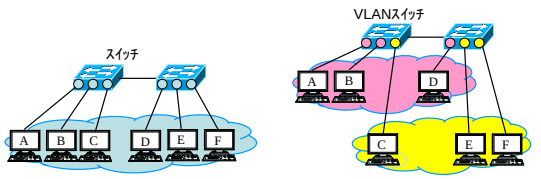
③しかし，部門間の異動があれ
ば，ｹｰﾌﾞﾙの接続替えが必要



VLAN（Virtual LAN）の利点

1つの物理LAN を，複数のVLAN（ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝ）に分割

利点1：ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾗﾌｨｯｸを局在化（より広い帯域幅を提供）
利点2：ルータを使った分割と比べると低コスト
利点3：柔軟なﾈｯﾄﾜｰｸ設計（追加，移動，変更は，VLANﾎﾟｰﾄの設定のみで可能）
利点4：ｾｷｭﾘﾃｨの向上（ユーザを部門などでｸﾞﾙｰﾌﾟ化し，アクセス制限が可能）

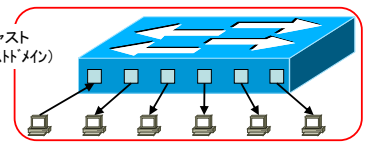


フラットなネットワーク（ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝ1つ）
ｽｲｯﾁ間を接続すると同じﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝになる

複数のVLAN（ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝ）に分割

利点1：ﾌﾞﾛｰﾄﾞｷｬｽﾄのﾄﾗﾌｨｯｸを局所化

全ポートへのブロードキャスト
（全体で1つのﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝ）

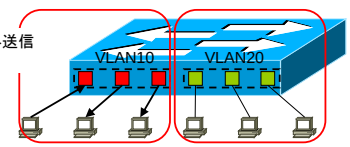


ブロードキャストフレーム

	DA	SA	データ	FCS

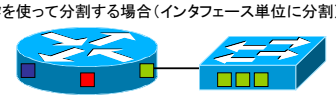
FF:FF:FF:FF:FF:FF

同じVLANのポートにのみ送信
ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝを分割



利点2：低コスト（ﾌﾞﾛｰﾄﾞｷｬｽﾄﾄﾞﾒｲﾝの分割）

ルータを使って分割する場合（インタフェース単位に分割）

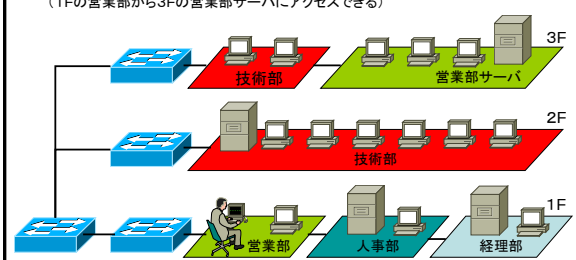


ルータのポート単価はスイッチより高い
設置できるポート数も少ない
（ポート数を増やすには，インタフェースにスイッチを接続）

VLANによる分割の場合

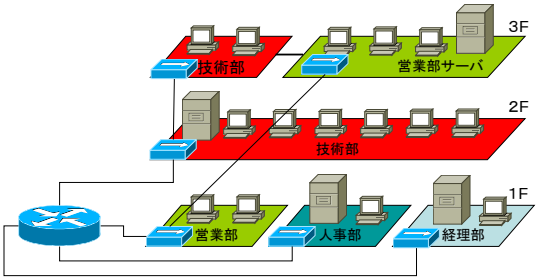
利点3：柔軟なネットワーク設計

VLANはSWの設定のみでブロードキャストドメインを分割できる
SW間にまたがるVLANの設定が可能
・異動や配置変更があっても，物理的な配線の変更が不要
（1Fの営業部から3Fの営業部サーバにアクセスできる）

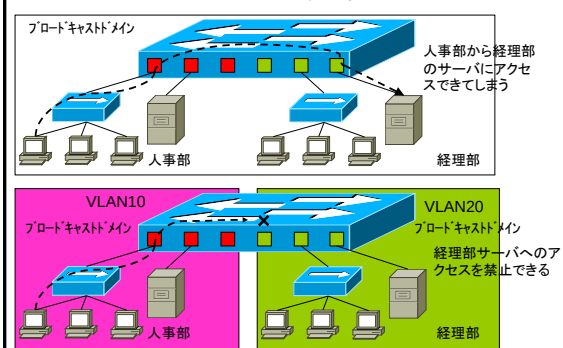


参考：ルータにハブを接続したLAN

ルータのインタフェース毎にブロードキャストドメインの分割は可能
・配置変更の度に，ホスト・サーバとハブへの接続変更，ハブの増設などが必要
・部内は同じコリジョンドメインとなるので，スループットが低下
・これを解決するには，ハブをスイッチに変更要→VLANを導入した方がbetter

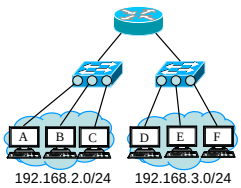


利点4：セキュリティの向上

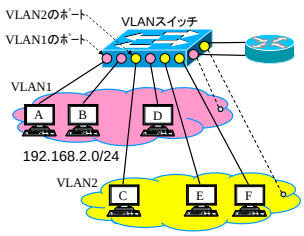


VLAN間の通信

スイッチ間の接続



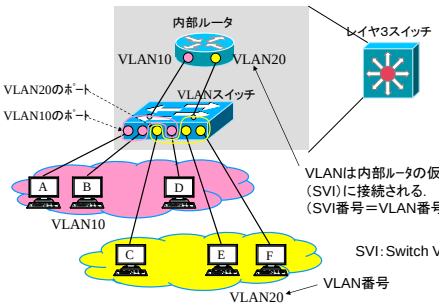
VLAN間の接続



原則的には，VLAN間の接続にはルータが必要
（ルータを別に購入し，接続する必要がある）

レイヤ3スイッチ

レイヤ3スイッチ
・VLANスイッチとルータの機能（内部ﾙｰﾀ機能）を併せ持ったスイッチ



VLANの作成

VLANはVLAN-ID（VLAN番号）で管理される.
初期状態では，管理用VLANであるVLAN1が作成されており，全ポートはVLAN1に割り当てられている.
ポートをVLAN1以外に割り当てる場合には，予めVLANを作成しておく必要がある.

VLANの作成方法（1）
(config)# vlan vlan-id　　VLANを作成し，番号を割り当てる
（VLAN番号を数字で投入）
(config-vlan)# name vlan-name　　VLAN名の設定（部署名などを付ける）.
省略時は，VLAN＋番号が名前
VLANの作成方法（2）　VLANデータベースを利用
vlan database　　VLANﾃﾞｰﾀﾍﾞｰｽﾓｰﾄﾞにする
（vlan)# vlan vlan-id [name vlan-name]
省略可

（1）VLANの作成

- (config)#　vlan 2
- (config-vlan)#　name sales
- (config-vlan)#

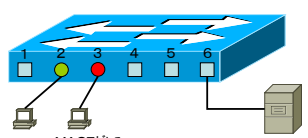
- 2950C #vlan database
- 2950C(vlan) #vlan 2 name Sales VLAN番号と名称
- VLAN 2 added:
- 　　Name: Sales
- 2950C (vlan) #vlan 3 name Marketing
- VLAN 3 added:
- 　　Name : Marketing
- 2950C(vlan) #apply　　applyで適用
- APPLY completed.
- 2950C(vlan) #

ポートに対するVLANの指定

- ポート種別の指定：VLANのリンクには，アクセスリンクとトランクリンクがある.
  - 通常のホストを収容するリンクは，アクセスリンク（access）とする.
  - (config-if)#switchport mode access
- VLANメンバーシップ：各ポートが，どのVLANに帰属するかをポート毎に指定
  - 以下の2モードがある
- スタティックVLAN
  - ポートとVLANが固定的に対応．管理者が手動で行う
  - (config-if)# switchport access vlan vlan-id
- ダイナミックVLAN
  - ポートに接続したホストのMACｱﾄﾞﾚｽを見て動的マッピング
  - VMPSを使用（VLAN Management Policy Server）
  - (config-if)# switchport access vlan dynamic
- メンバーシップの確認
  - # show vlan brief

特定のVLANに帰属させるのはアクセスリンク

ダイナミックVLANのメンバーシップ



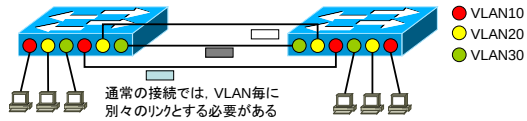
MACｱﾄﾞﾚｽ	VLAN
AAA	20
BBB	20
CCC	30
:	:

(config)# int e0/3
(config-if)# switchport access vlan dynamic

3番ポートにホストが接続
ホストからフレームを受信
VMPSサーバに問い合わせ
登録されているVLAN20を割り当てる

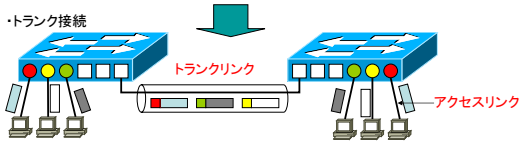
トランクリンクとアクセスリンク

フレームは，同じVLANに属するポートにのみ転送される
・通常の接続（アクセスリンクによる接続）



通常の接続では，VLAN毎に
別々のﾘﾝｸとする必要がある

・トランク接続



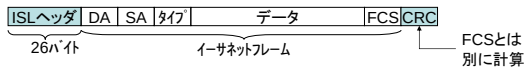
トランクリンク（複数のVLANのデータを転送できる特別なﾘﾝｸ）を設定
フレームにVLANを示すヘッダ情報を付加して転送
注：アクセスリンク（1つのVLANのデータしか転送しない通常のリンク）

トランクプロトコル

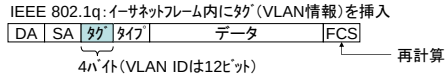
VLAN IDを使用した識別方式
（ﾌﾚｰﾑに設定するﾀｸﾞﾍｯﾀﾞの構成等）

ISL	Cisco独自	Inter-Switch Link	一方のみｻﾎﾟｰﾄの機種がある
IEEE802.1q	標準	他社ﾍﾞﾝﾀﾞ間の接続に使用	
LANE	標準	LAN Emulation　ATMに使用	
802.10	Cisco独自	FDDIに使用	

ISL：ISLヘッダとCRCにより，ｲｰｻﾈｯﾄﾌﾚｰﾑをｶﾌﾟｾﾙ化



IEEE 802.1q：ｲｰｻﾈｯﾄﾌﾚｰﾑ内にﾀｸﾞ（VLAN情報）を挿入

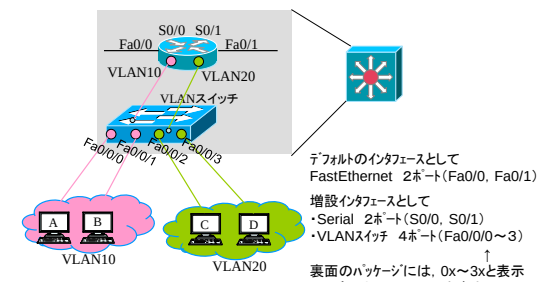


トランクの設定

- インタフェースの指定
  - #config t
  - (config) #int f0/1
- トランクの有効化
  - (config-if) #switchport mode trunk
- プロトコルの指定（ﾄﾗﾝｸﾘﾝｸ両端のﾎﾟｰﾄが同じﾌﾟﾛﾄｺﾙである必要がある）
- IEEE 802.1qの場合
  - (config-if)# switchport trunk encapsulation dot1q
- ISLの場合
  - (config-if)# switchport trunk encapsulation isl
- トランクの確認（メッセージはp.239参照）
  - # show interface trunk

1800ルータの構成

1800ルータは，小規模なレイヤ3スイッチとルータを複合した装置



ﾃﾞﾌｫﾙﾄのｲﾝﾀﾌｪｰｽとして
FastEthernet　2ﾎﾟｰﾄ（Fa0/0，Fa0/1）

増設ｲﾝﾀﾌｪｰｽとして
・Serial　2ﾎﾟｰﾄ（S0/0，S0/1）
・VLANｽｲｯﾁ　4ﾎﾟｰﾄ（Fa0/0/0～3）

裏面のﾊﾟｯｹｰｼﾞには，0x～3xと表示
ｺﾏﾝﾄﾞではFa0/0/0～3とする

前ｽﾗｲﾄﾞの構成におけるVLANの設定

（1）VLANの作成

```
cn-x#vlan database
cn-x(vlan)#vlan 10
cn-x(vlan)#vlan 20
cn-x(vlan)#exit
```

VLANデータベースによるVLANの作成
・作成されたVLANはﾙｰﾀの仮想ﾎﾟｰﾄ（SVI）に接続される．
・SVI番号はVLAN番号（vlan 10，vlan 20）になる

（2）VLANの割り当て：ﾎﾟｰﾄにVLANを割り当てる（VLANﾒﾝﾊﾞｰｼｯﾌﾟの設定）

```
cn-x#conf t
cn-x(config)#int Fa0/0/0
cn-x(config-if)#switchport access vlan 10
cn-x(config-if)#int Fa0/0/1
cn-x(config-if)#switchport access vlan 10
cn-x(config-if)#int Fa0/0/2
cn-x(config-if)#switchport access vlan 20
cn-x(config-if)#int Fa0/0/3
cn-x(config-if)#switchport access vlan 20
```

この例は，2ﾎﾟｰﾄずつを別のVLANとしている．
全ﾎﾟｰﾄを1つのVLANに帰属，各ﾎﾟｰﾄを別の
VLAN帰属など，任意の組み合わせが可能

（3）IPｱﾄﾞﾚｽの設定：ﾙｰﾀの仮想ﾎﾟｰﾄ（SVI）にIPｱﾄﾞﾚｽを設定

```
cn-x(config-if)#int vlan10
cn-x(config-if)#ip address 192.168.10.1 255.255.255.0
cn-x(config-if)#no shutdown
cn-x(config-if)#int vlan20
cn-x(config-if)#ip address 192.168.20.1 255.255.255.0
cn-x(config-if)#no shutdown
```

物理ﾎﾟｰﾄ番号（Fa0/0，S0/0など）と
同じようにvlan10，vlan20と指定する

IPｱﾄﾞﾚｽの削除は no ip address