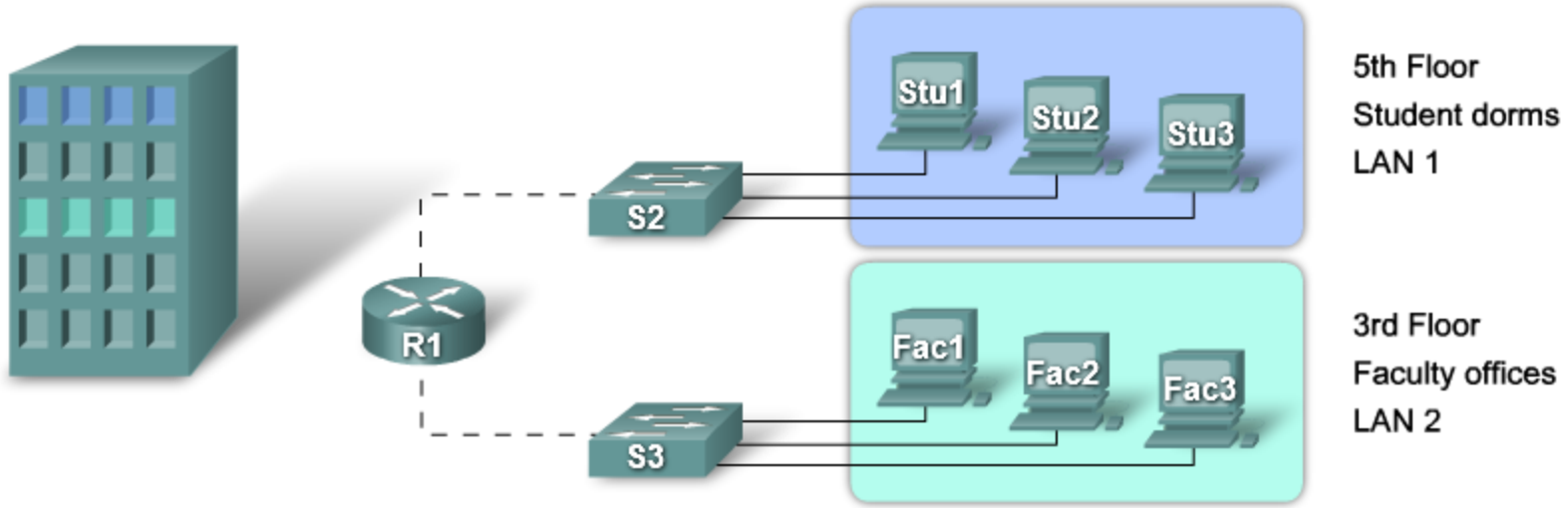
Module 4

Extending Switched Networks with VLANs

VLAN Operation Overview

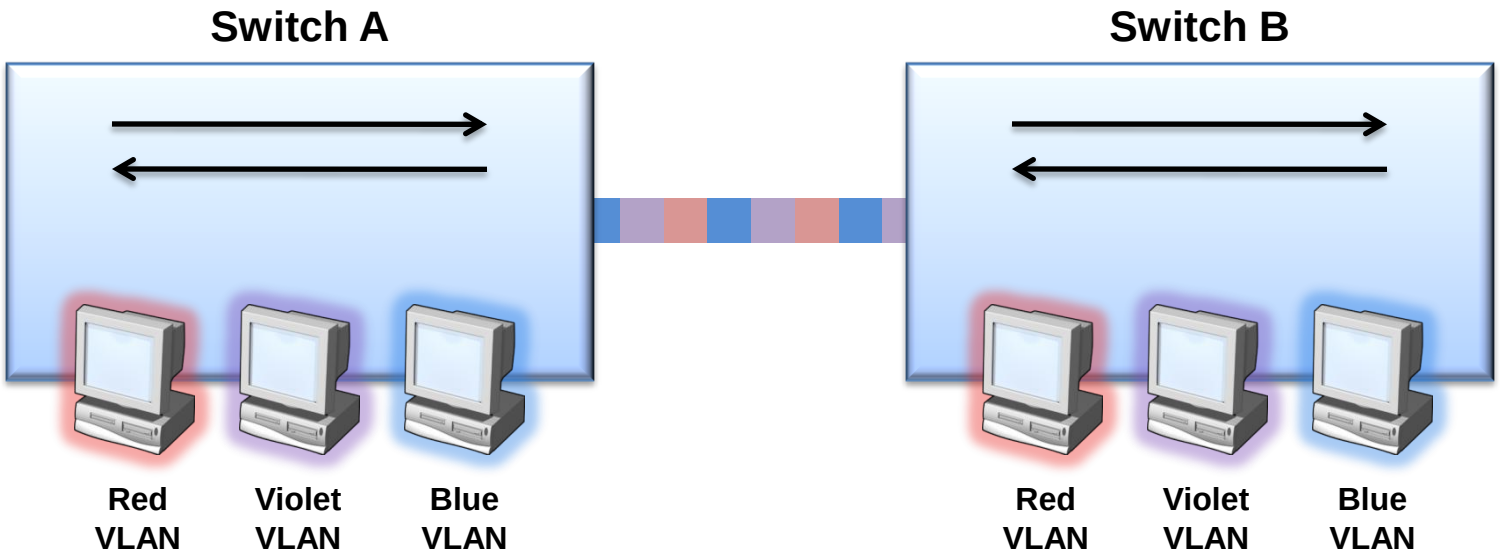
VLAN Overview

A VLAN = A Broadcast Domain = Logical Network(Subnet)



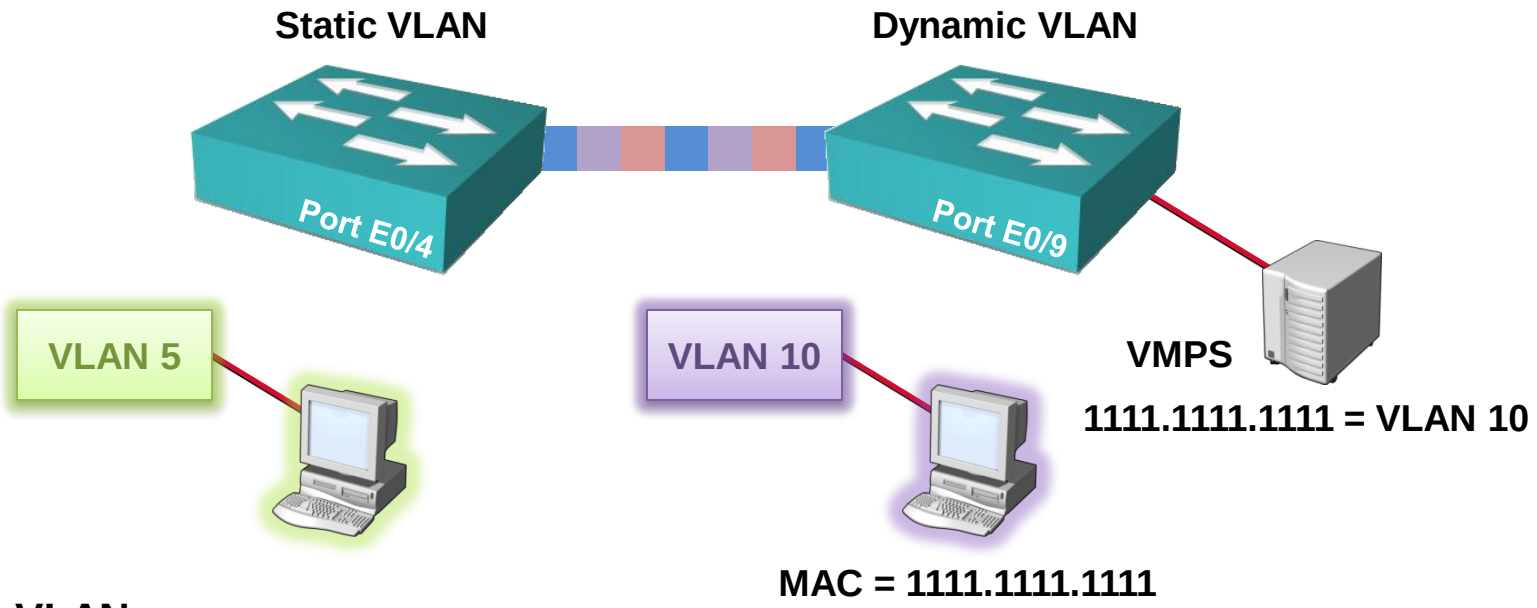
- **Segmentation**
- **Flexibility**
- **Security**

VLAN Operation



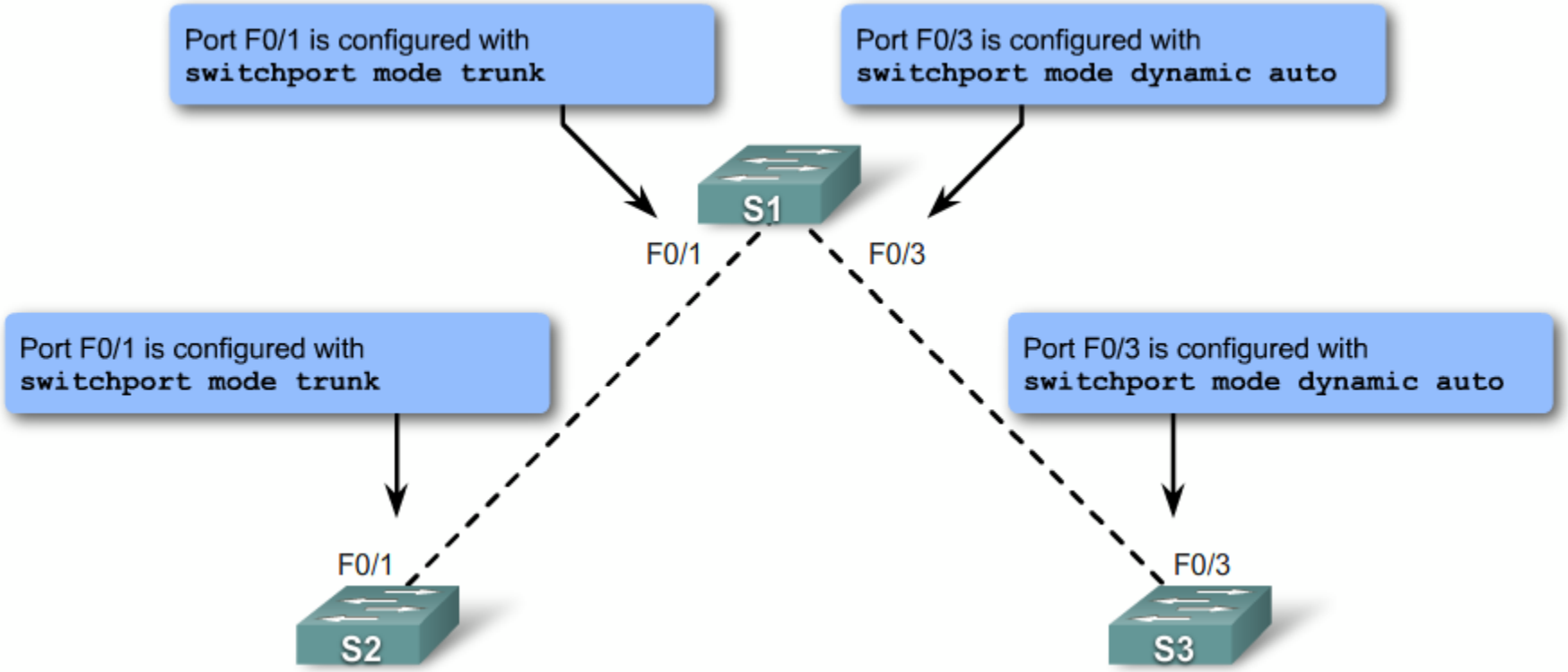
- 각각의 Logical VLAN은 별도의 Physical Bridge와 동일하다
- VLAN을 여러대의 Switch로 확장할 수 있다
- Trunk Link는 Traffic을 여러 VLAN으로 전달한다

VLAN Membership Models



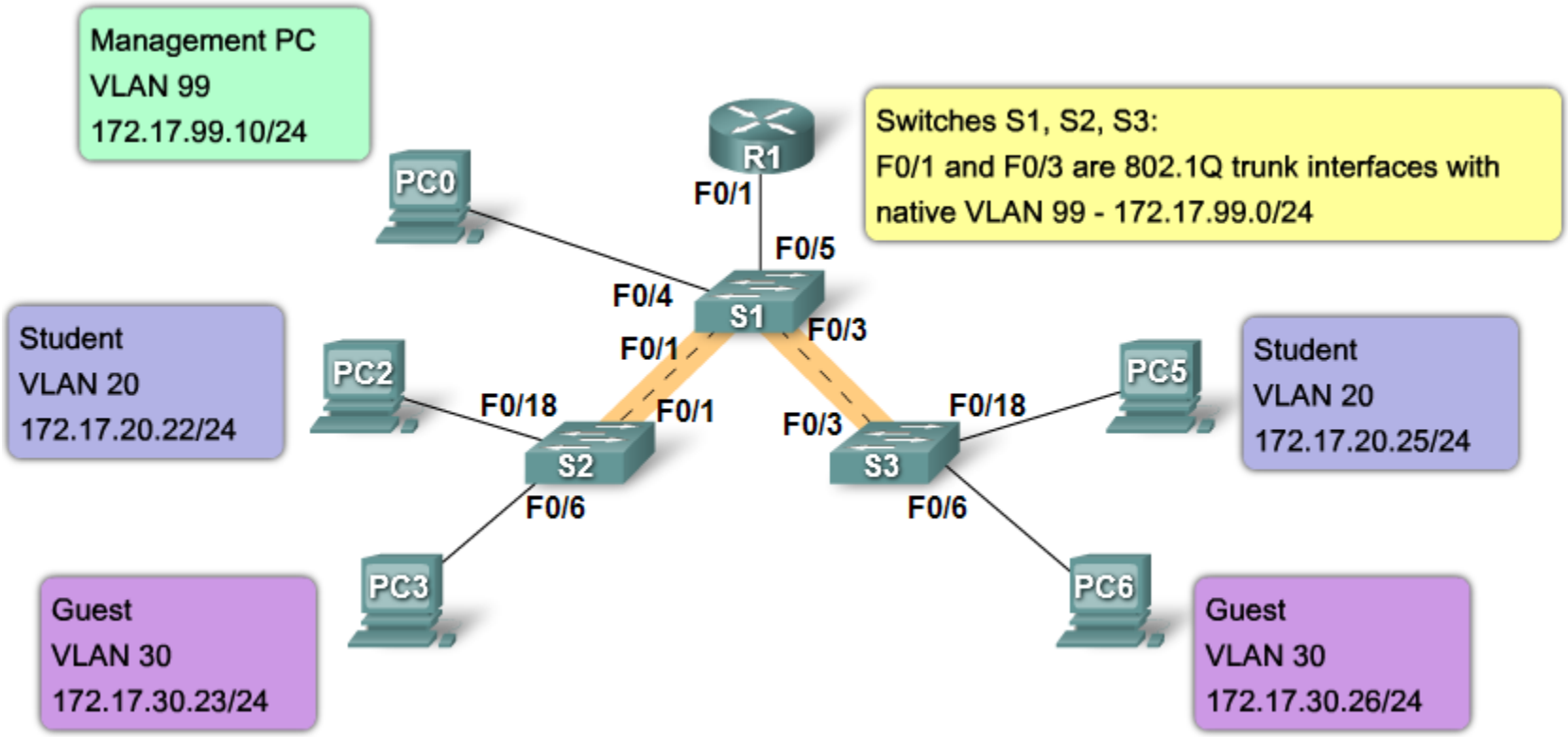
- Static VLAN
  - 관리자가 직접 하나의 포트에 VLAN을 할당하는 VLAN이다
- Dynamic VLAN
  - VMPS(VLAN Membership Policy Server)를 사용하여 포트에 연결된 호스트에 MAC Address를 기반으로 Switch가 VMPS에 질의하여 해당 포트에 VLAN을 결정한다

802.1Q Trunking



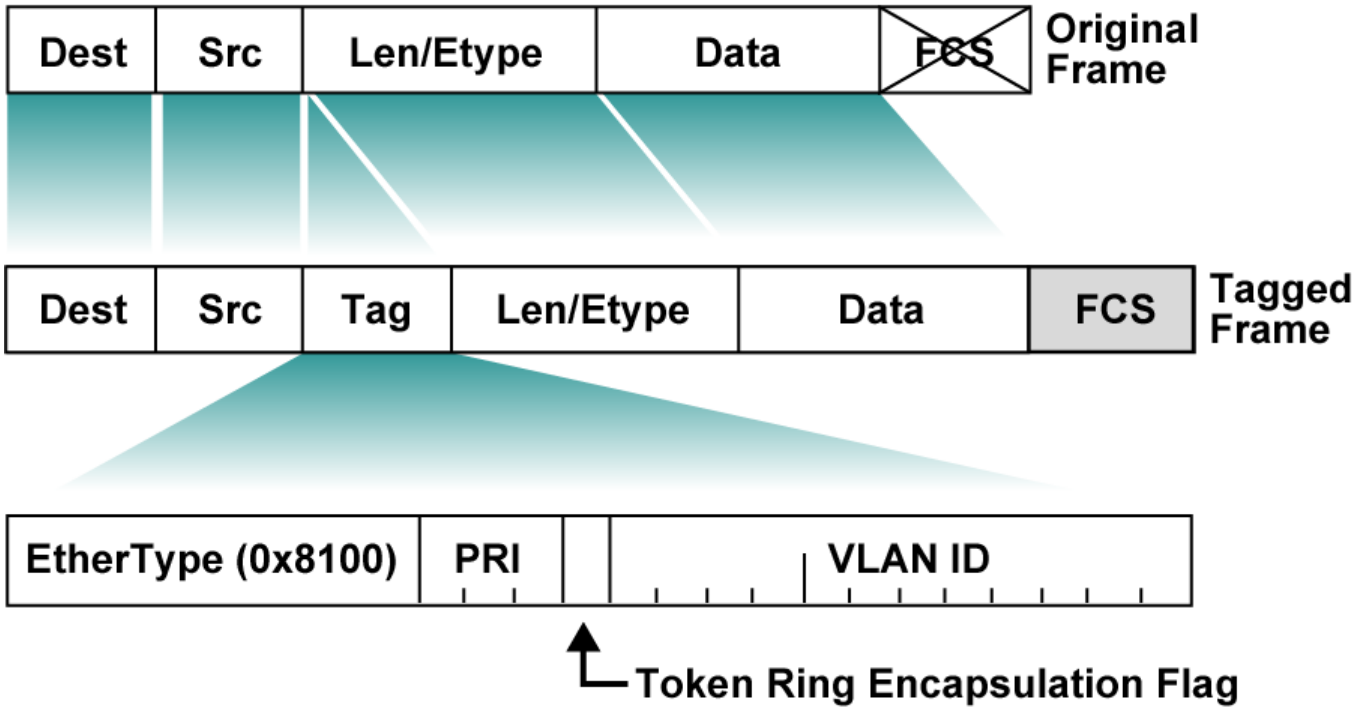
- 여러 스위치, 라우터 서버 사이의 VLAN을 서로 연결한다
- Cisco에서는 FastEthernet과 GigabitEthernet Interface에 대해 IEEE 802.1Q를 지원
- Cisco Switch에서는 802.1Q를 일반적으로 dot1q라고 부른다

Importance of Native VLANs



- **Ethernet이 공유매체이고 대화하지 않더라도 통신은 할 수 있어야 한다. 이러한 이유로 인해 802.1Q를 Native VLAN으로 정의하기도 한다. Native VLAN은 Tag되지 않은 Frame을 전달하는 VLAN을 정의한다**

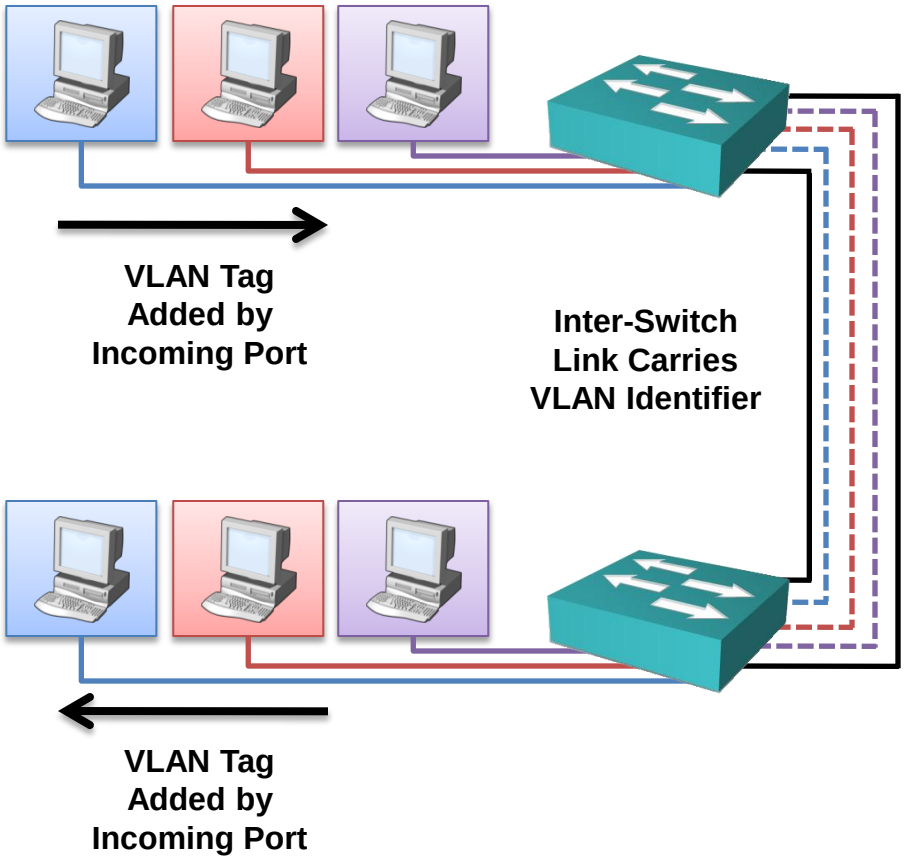
802.1Q Frame



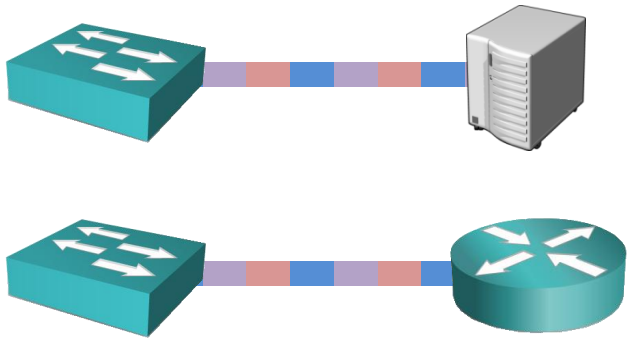
- 802.1Q Frame Tag : 4Byte = 2Byte(TPID) + 2Byte(TCI)
  - TPID(Tag Protocol ID) : 0x8100 (이 값은 802.1Q 호환 장비는 0x8100값을 보고 이 프레임에 태그가 붙어 있으며, 다음 2Byte가 802.1Q 정보용으로 사용된다고 인식한다
  - TCI (Tag control Information) : Priority(3bit) QoS용도, CFI(1bit) 0인 경우 Ethernet 1인 경우 Tokenring을 의미함, CFI의 마지막 12bit는 VLAN ID이다

ISL Tagging

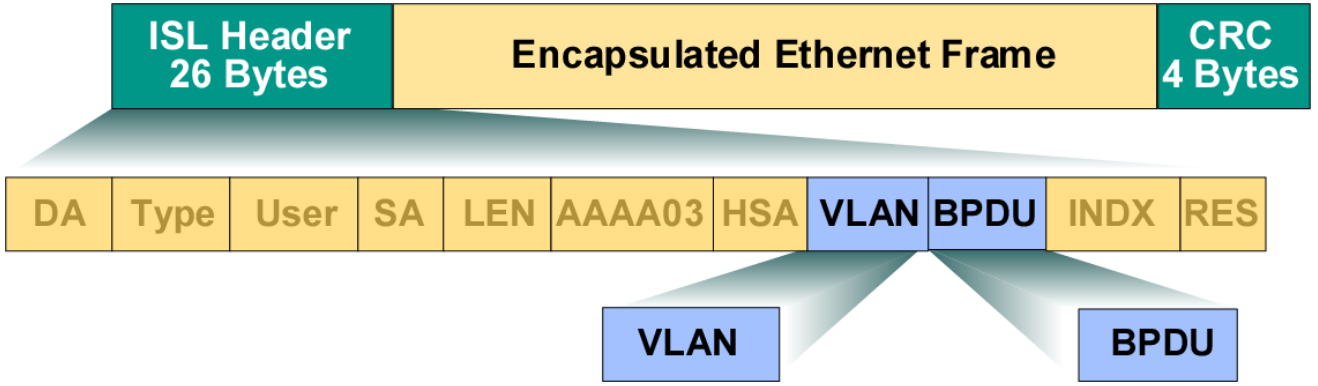
ISL trunks enable VLANs across a backbone



- ASIC (Application-Specific Integrated Circuits)와 함께 수행
- Client는 ISL 헤더를 알지 못함
- Switch사이, Router와 Switch사이, Switch와 ISL NIC가 장착된 Server 사이에서 효과적이다



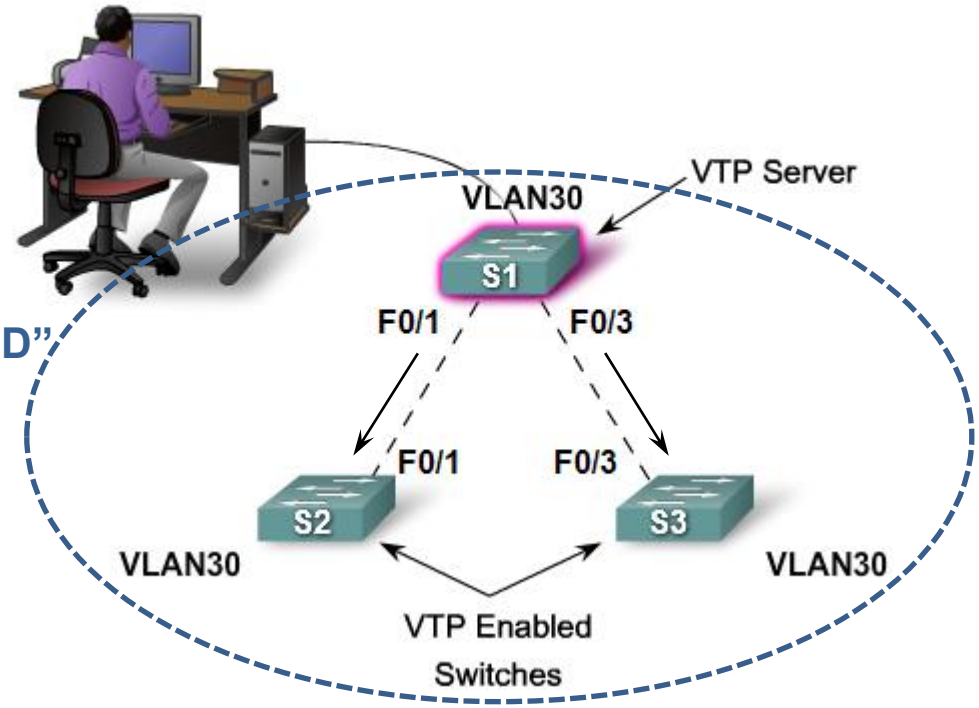
ISL Encapsulation



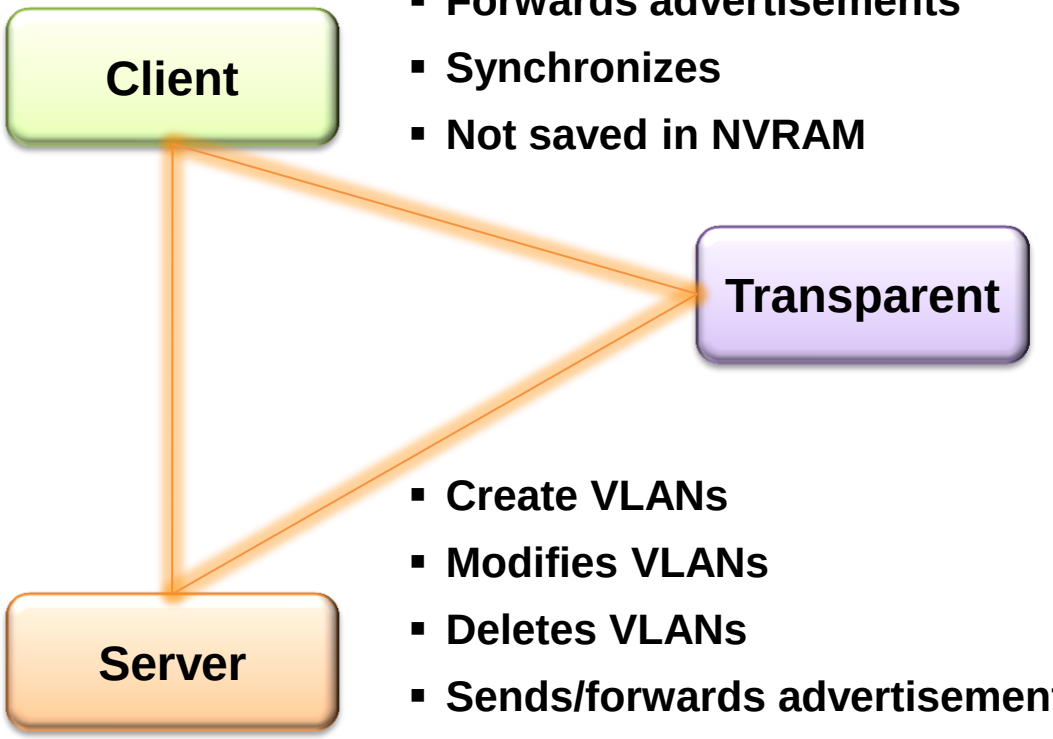
DA	40bit의 Multicast 목적지 주소
Type	Encapsulation Type, (Ehternet 0000, Tokenring 0001, FDDI 0010, ATM 0011)
User	Ethernet 우선 순위 (Low 0, High 3)
SA	송신하는 Catalyst Switch에 48Bit송신지 MAC Address
LEN	Frame에서 DA, Type, User, DA, LEN, CRC를 제외한 길이
AAA03	표준 SNAP 802.2 LLC Header
HAS	SA의 처음 3Byte (제조업체의 ID나 조직의 고유 ID)
VLAN	15Bit의 VLAN ID
BPDU	Frame의 Spanning Tree BPDU 여부를 나타내는 1bit 서술자, CDP도 1로 설정된다
INDEX	송신포트 ID를 나타내는 16bit 서술자 (진단용으로 사용)
RES	Tokenring과 FDDI (Fiber Distributed Data Interface) 프레임 FC(Framd Check) 필드의 부가정보에 사용되는 16bit 예약 필드

VTP Protocol Features

- VTP는 Switch Network 전체에 설정되어 있는 VLAN에 관해 확인한 정보를 분재하고 동기화 하기 위해 사용되는 Protocol이다
- Switch Network에서 일관된 VLAN 설정을 손쉽게 한다
- VTP Server에 의해 생성된 VLAN 정보는 Trunk를 통해 모든 스위치로 분배된다



VTP Modes



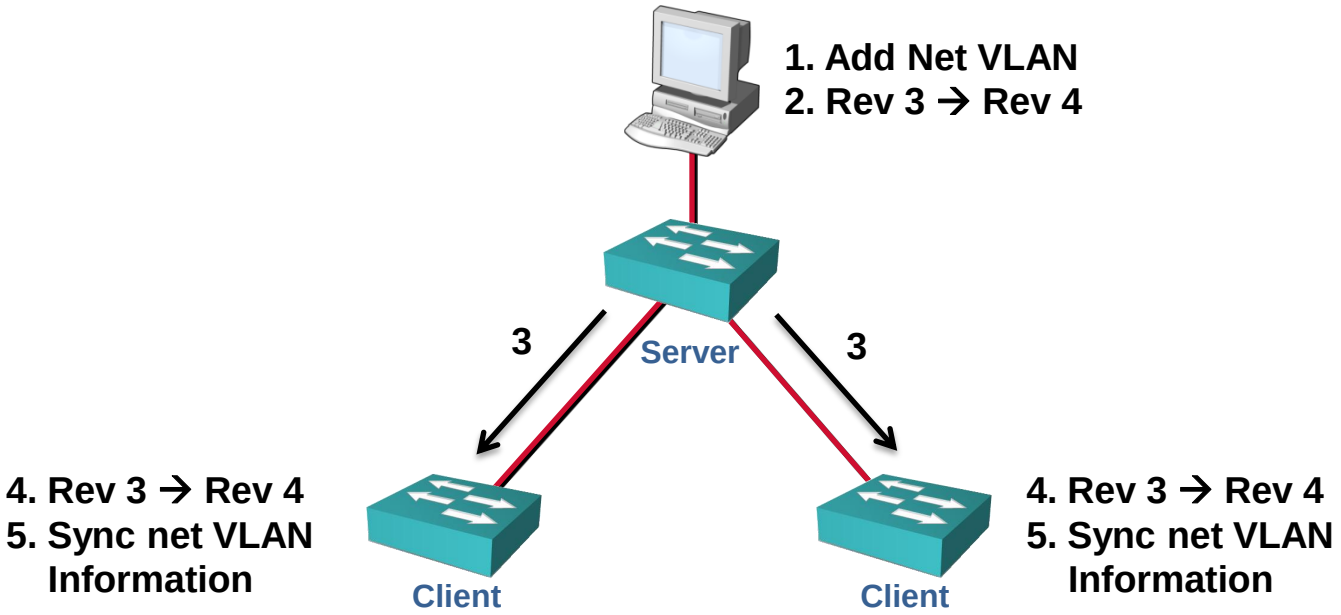
- Forwards advertisements
- Synchronizes
- Not saved in NVRAM

- Creates VLANs
- Modifies VLANs
- Deletes VLANs
- Forward advertisements
- Does not synchronize
- Saved in NVRAM

- Create VLANs
- Modifies VLANs
- Deletes VLANs
- Sends/forwards advertisements
- Synchronized
- Saved in NVRAM

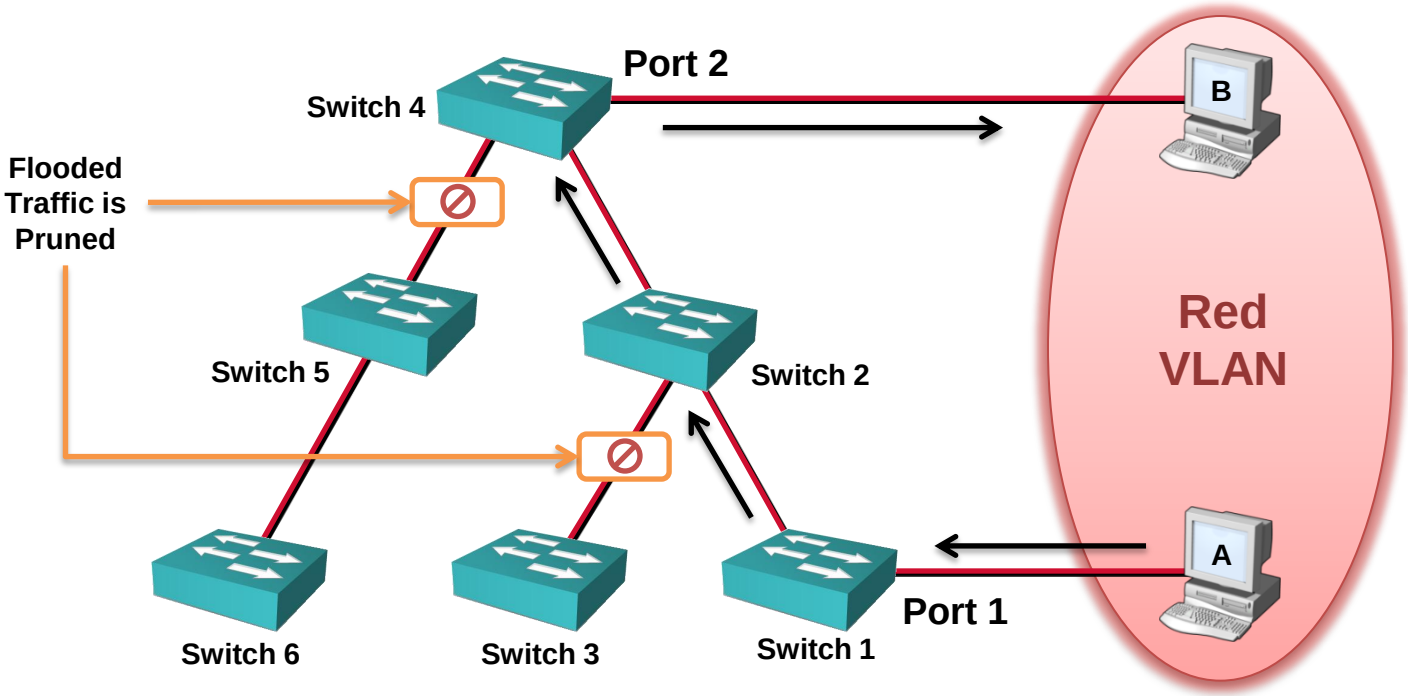
VTP Operation

- VTP 광고는 Multicast Frame으로 전달된다
- VTP Server와 Client는 Revision Number가 큰 값이 더 최근 정보로 간주된다
- VTP 광고는 변경이 없어도 매 5분마다 정기적으로 전달한다

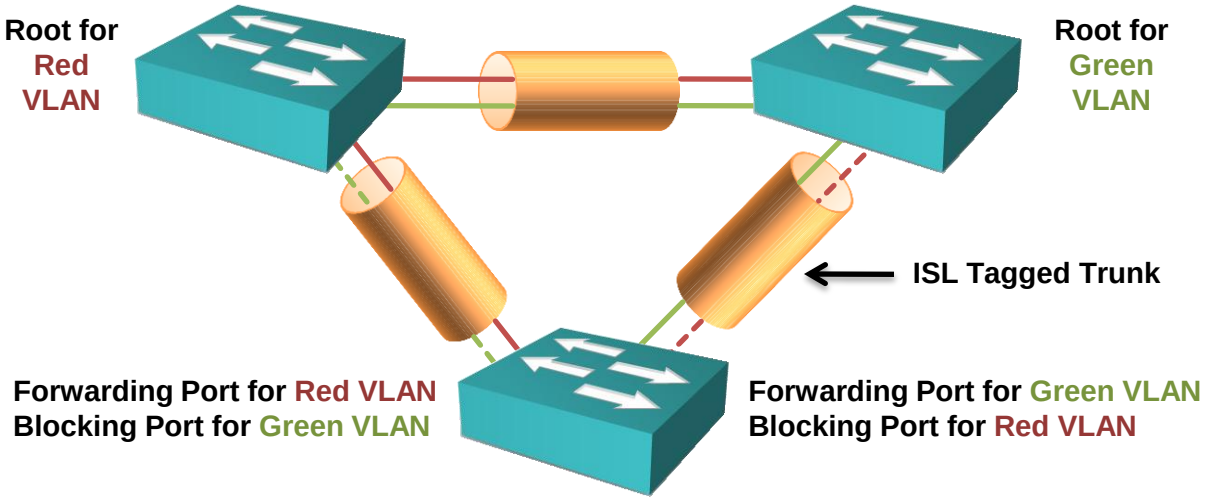


VTP Pruning

- 일부 traffic을 운반할 필요가 없는 Link들을 가로질러 필요 없이 Flooding되는 traffic을 차단하는 기능이다
- Host A와 Host B는 같은 VLAN에 있기 때문에 호스트 A에서 전달한 traffic이 Switch 1 → Switch 2 → Switch 4를 통해서 전달되어야 한다. 그러나 Switch 3, Switch 5, Switch 6은 Red VLAN이 없기 때문에 Traffic이 전달되지 않는다



Per-VLAN Spanning Tree



- VLAN에서 고려해야 할 한가지 사항은 STP(Spanning Tree Protocol)이다
- 802.1Q 표준에서는 네트워크의 모든 VLAN이 한 개의 Spanning-tree를 운영한다
- 802.1Q에서 한 개의 Spanning-tree는 Native VLAN에서 동작하여 비 호환 스위치와도 통신할 수 있다. (이 단일 Interface를 CST(Common Spanning Tree)라고 한다)
- PVST는 시스코에 의해 만들어지며 VLAN마다 Spanning-tree를 운영한다
- PVST는 ISL이나 802.1Q를 사용하여 링크관리 및 STP에 의한 병렬 링크들 간 트래픽 로드 밸런싱을 구현할 수 있다

Configuring VLANs

VTY Configuration Guidelines

- VTP domain name – Default None
- VTP mode(server/client/transparent) – VTP server mode is the default
- VTP pruning – Default Disabled
- VTP password – None
- VTP trap – Default Disabled

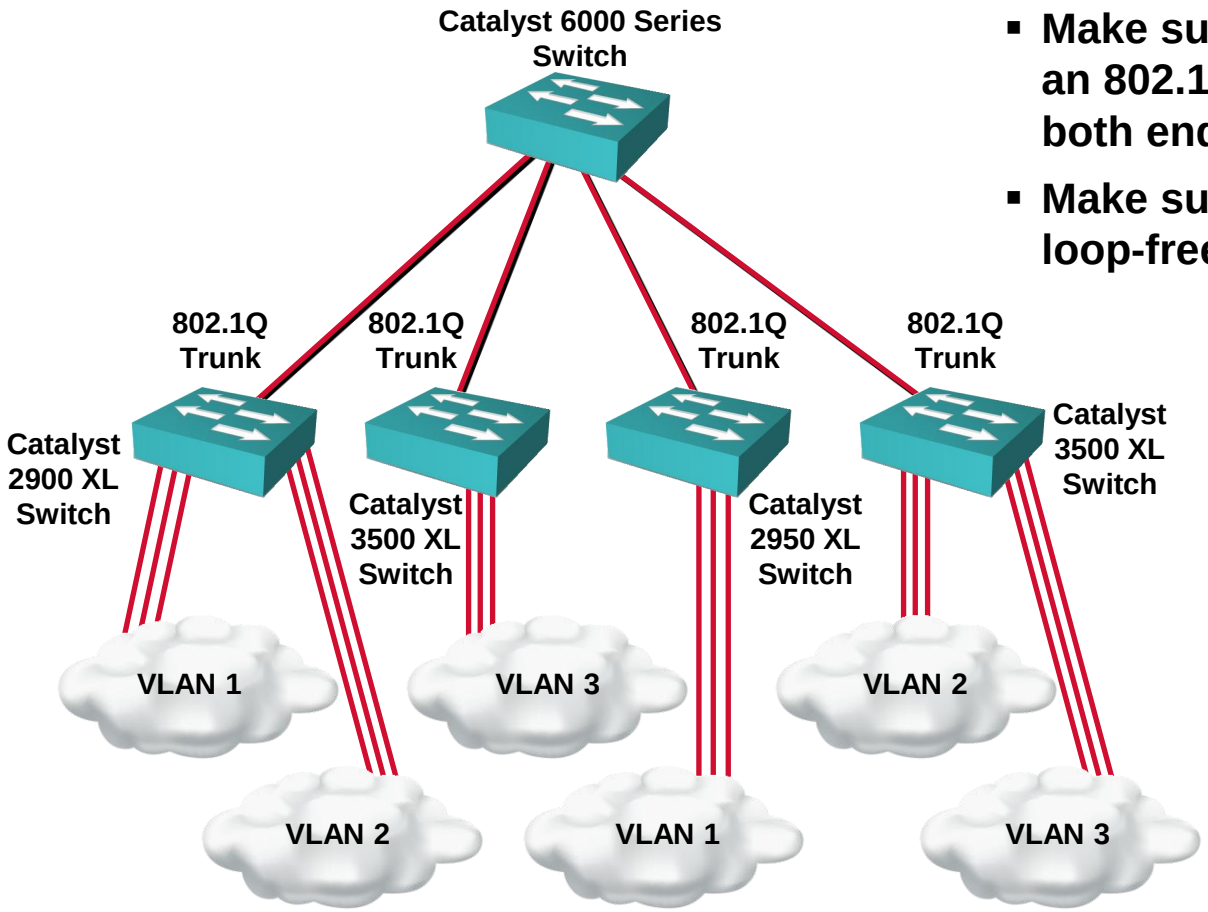
- 주의 : 기존 도메인에 새로운 스위치를 추가할 때 스위치에 대한 설정 개정 번호가 0인지를 확인하여 새로운 스위치가 부정확한 VLAN 정보를 전파하지 못하도록 한다. (새로운 스위치에 VTP 설정 개정 번호를 Reset하여 VTP에 추가한다)

Creating a VTP Domain

- **Catalyst 2950**

```
ASW2950(config)#vtp domain domain-name
ASW2950(config)#vtp password password
ASW2950(config)#vtp pruning
ASW2950(config)#vtp snmp-server enable traps vtp
ASW2950(config)#vtp  mode [ server | client | transparent ]
```

802.1Q Trunking Limitations



- Make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link
- Make sure your network is loop-free before disabling STP

Configuring 802.1Q Trunking

- **Configures the port as a VLAN trunk**

```
ASW2950(config-if)#switchport mode trunk
```

- **Catalyst 3550 등은 trunk encapsulation type을 지정해야 수동 설정이 가능하다**
- **ASW(config-if)#switchport trunk encapsulation {dot1q | isl}을 이용하여 설정하면 된다**

Configuring ISL Trunking

```
ASW3550(config-if)#switchport trunk encapsulation isl
ASW3550(config-if)#switchport mode trunk
```

Adding a VLAN

- **Catalyst 2950**

```
ASW2950(config)# vlan vlan_ID
ASW2950(config-vlan)# name <word>
```

```
ASW2950#vlan database
% Warning: It is recommended to configure VLAN from config
mode,as VLAN database mode is being deprecated. Please consult
user documentation for configuring VTP/VLAN in config mode.

ASW2950(vlan)#vlan 10 name sales
```

Assigning Switch Ports to a VLAN

- **Catalyst 2950**

```
ASW2950(config)# interface fa0/1
ASW2950(config-if)#switchport access vlan <vlan_id>
```

- **fa0/1번 포트부터 10번 포트까지 , fa0/15부터 19번 포트까지 설정을 한번에 구성하기**

```
ASW2950(config)# interface range fa0/1-10, fa0/15-19
ASW2950(config-if-range)#switchport access vlan <vlan_id>
```

Verifying the VTY Configuration for the Catalyst 2950

```
ASW2950#show vtp status
```

```
ASW2950#show vtp status
VTP Version                     : 2   <--- Indicates v2-capable
Configuration Revision          : 4
Maximum VLANs supported locally : 68
Number of existing VLANs        : 6
VTP Operating Mode              : Server
VTP Domain Name                 : switchlab
VTP Pruning Mode                : Enabled
VTP V2 Mode                     : Disabled   <--- Indicates v2 disabled; v1 set
VTP Traps Generation            : Disabled   <--- Catalyst 2950 default
MD5 digest                      : 0x3D 0x02 0xD4 0x3A 0xC4 0x46 0xA1 0x03
Configuration last modified by 10.1.1.40 at 5-4-02 22:25:
```

Verifying a Trunk

- **Catalyst 2950**

```
ASW2950#show interface interface switchport
```

```
wg_sw_2950#show interface fa0/2 switchport
Name: Fa0/2
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
. . .
```

Verifying a VLAN

- **Catalyst 2950**

```
ASW2950#show vlan id [vlan_id]
```

```
ASW11#show vlan id 1

VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                   Fa0/6, Fa0/7, Fa0/8, Fa0/9
                                                   Fa0/10, Fa0/11, Fa0/12, Fa0/13
                                                   Fa0/14, Fa0/15, Fa0/16, Fa0/17
                                                   Fa0/18, Fa0/19, Fa0/20, Fa0/21
                                                   Fa0/22, Fa0/23, Fa0/24, Gi0/1
                                                   Gi0/2

VLAN Type  SAID        MTU  Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -          -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
```

Verifying VLAN Membership on a Catalyst 2950

```
ASW2950#show vlan brief
```

```
ASW2950#show vlan brief
VLAN     Name                         Status             Ports
----     ---------------------------- ---------          -----------------------
1        default                        active           Fa0/4, Fa0/5, Fa0/6, Fa0/7,
                                                         Fa0/8, Fa0/9, Fa0/10, Fa0/11,
                                                         Fa0/12, Fa0/13, Fa0/14, Fa0/15,
                                                         Fa0/16, Fa0/17, Fa0/18, Fa0/19,
                                                         Fa0/20, Fa0/21
5        VLAN5                          active           Fa0/3
9        VLAN9                        active             Fa0/22, Fa0/23
1002     fddi-default                   active
1003     token-ring-default             active
1004     fddinet-default                active
1005     trnet-default                  active
```

```
ASW2950#show interfaces interface switchport
```

Verifying STP for a VLAN

- **Catalyst 2950**

```
ASW2950#show spanning-tree vlan [vlan#]
```

```
ASW11#show spanning-tree vlan 1

VLAN0001
  Spanning tree enabled protocol ieee
  Root ID             Priority             32769
                               Address    0007.5044.4980
                               This bridge is the root
                               Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769  (priority 32768 sys-id-ext 1)
                               Address      0007.5044.4980
                               Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
                               Aging Time 300

Interface            Role  Sts    Cost    Prio.Nbr  Type
---------------      ----  ---   -------  --------  --------------------------
Fa0/23               Desg  FWD    19      128.23    P2p
```

VLAN Configuration LAB