VLAN
(Virtual LAN)

Index

1. VLAN

1. 1 VLAN이란?

- 논리적으로 분할된 스위치 네트워크
- 하나의 Switch에 연결된 모든 장비들은 같은 Broadcast domain안에 있게 된다, 이러한 Broadcast domain을 나누려면 중간에 Router(Layer 3 장비) 를 두어야 한다. 그러나 VLAN을 사용함으로써 한 대의 Switch를 여러 대의 Switch처럼 사용하고, 여러 개의 네트워크 정보를 하나의 포트를 통해 전송할 수 있다. 또한, 하나의 Switch에 연결된 장비들도 Broadcast domain이 서로 다를 수 있게 된다.
- VLAN이 없다면 한 포트에서 수신한 Broadcast Frame을 동일 스위치 뿐만 아니라 다른 Switch로도 Flooding한다. 또한, MAC Address table이 모두 차면 Switch가 모두장비에 대해 Hub처럼 동작하다.

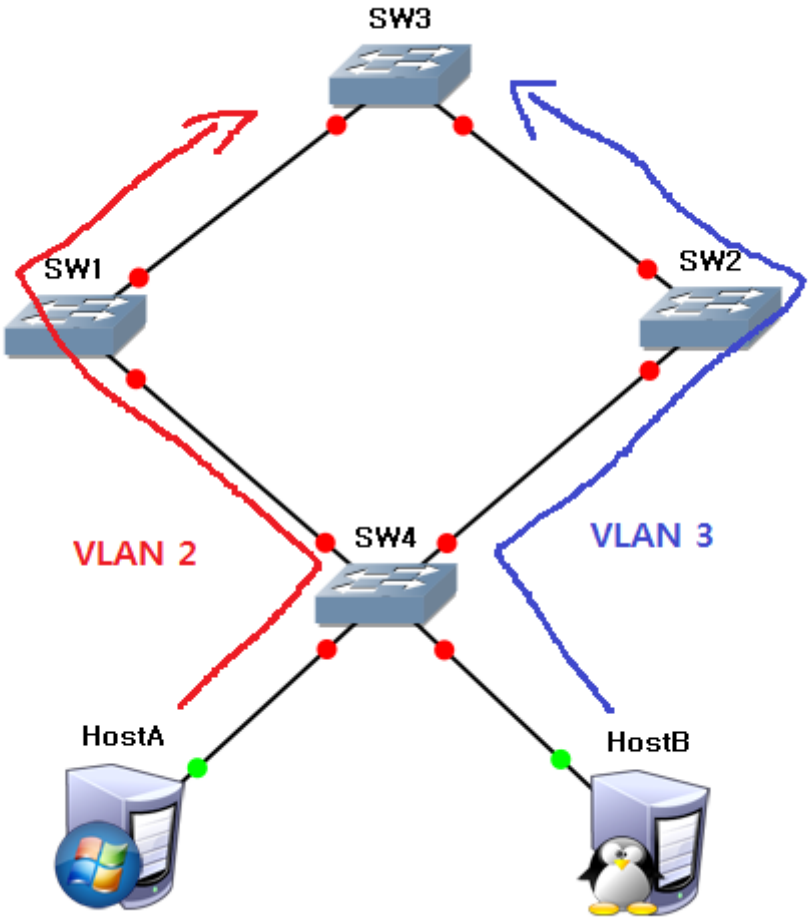
결과적으로 Switch 네트워크의 성능과 보안에 문제가 발생한다.

1. 2 VLAN의 역할

- Broadcast Domain분할
  - ■ 필요하거나 원하는 포트에만 Broadcast Frame이 전송된다.

- 보안성 강화
  - ■ 서로 다른 VLAN에 접속된 장비들은 Layer 3 장비(Router, L3 Switch)를 통해서만 가능하다.

- 부하분산(Load-Balancing)
  - ■ VLAN이 없다면 Layer 2 Load-Balancing이 불가능하다.



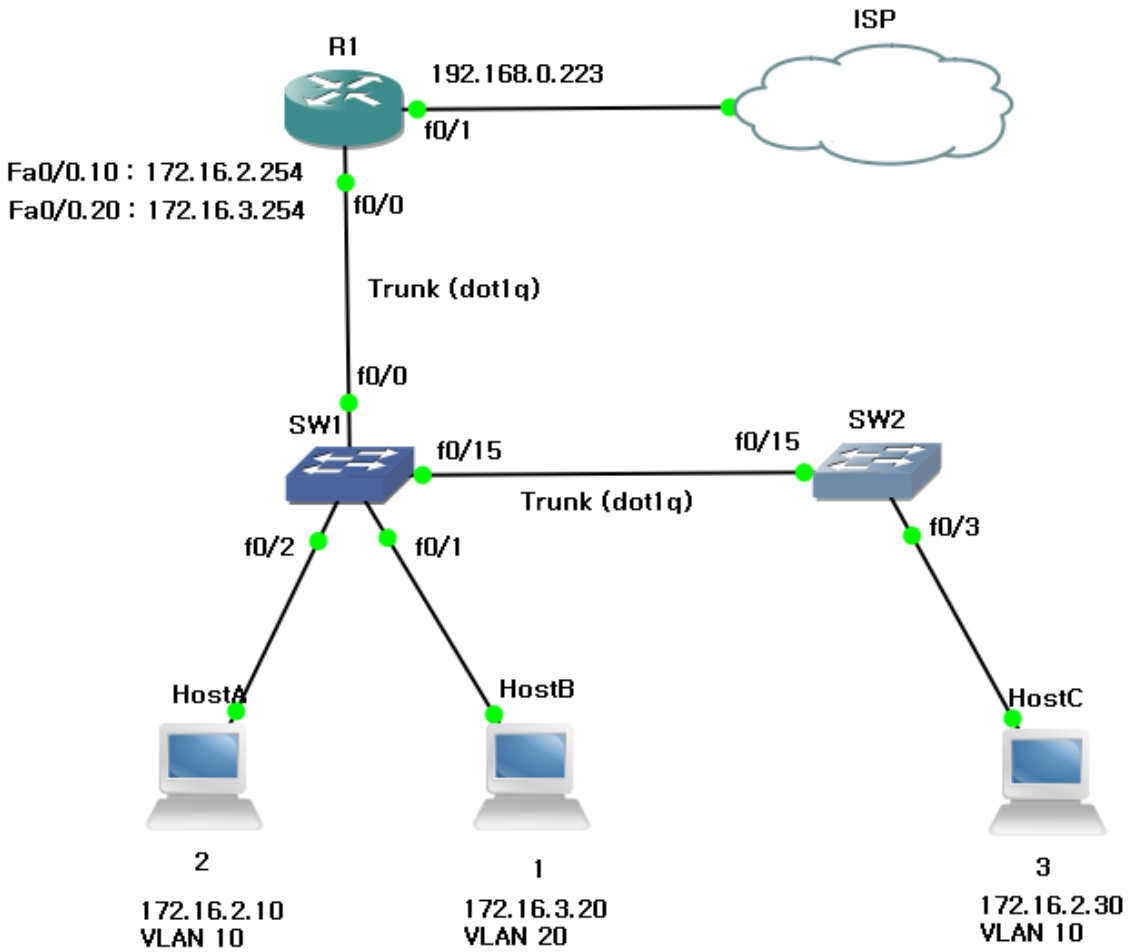
- SW1이나 SW2의 링크에 장애가 발생시 모든 트래픽은 나머지 링크를 통하여 전송된다.

1. 3 VLAN 번호

- VLAN은 번호로 구분한다.
- 사용 가능한 VLAN 번호는 1 – 4094 사이이며, 일반(normal) VLAN은 1 - 1005 사이, 그 중에서 1002 – 1005는 토큰링과 FDDI용으로 사용되며 Ehternet에서 사용할 수 있는 VLAN번호는 1 – 1001까지이다.
- VLAN 번호가 1006 – 4094 인 것을 확장(Extended) VLAN 이라 한다
- 사용 가능한 VLAN의 범위는 Switch모델에 따라 다르게 된다.
- VLAN 별로 서로 다른 STP를 사용하는 것을 PVST(per VLAN Spanning Tree)라고 하며, VLAN당 하나씩의 Spanning Tree가 지원되는 수는 128개 이다.

1. 4 VLAN과 IP Address

- VLAN이 다르면 IP Subnet도 달라야 한다.
- 당연한 얘기지만, 왜 그래야 하는지 한번 생각해 보면 아리송하다.



- Host A와 Host B는 VLAN이 서로 다르게 나뉘어져 있다. 물론 서로 통신도 잘 된다. VLAN으로 나뉘어져 있으니 서로 간의 통신은 R1을 거친 후 통신을 해야 한다. 여기서 Host B의 IP를 '172.16.2.20' 으로 변경한다면?

당연히 Host A와 Host B의 통신은 되지 않는다.

- 그 이유는 “ARP” 때문이다.

Vmware_05:66:ce	Broadcast	ARP	Who has 172.16.3.254? Tell 172.16.3.20
c4:07:11:3c:00:00	Vmware_05:66:ce	ARP	172.16.3.254 is at c4:07:11:3c:00:00

- 먼저, 서로 VLAN이 다를 때 Host B->Host A로의 Ping시의 ARP Packet이다. Router를 통해야 전송이 되므로 ARP로 Layer 3 Interface의 주소를 찾기 시작한다(Packet을 라우터로 전송시키는 것으로 보면된다).

Vmware_05:66:ce	Broadcast	ARP	Who has 172.16.2.10? Tell 172.16.2.20
Vmware_05:66:ce	Broadcast	ARP	Who has 172.16.2.10? Tell 172.16.2.20
Vmware_05:66:ce	Broadcast	ARP	Who has 172.16.2.10? Tell 172.16.2.20

- 이번엔, VLAN이 다르고 IP Subnet이 같을 때 Host B->Host A로의 Ping시의 ARP Packet이다. Router의 Interface가 아닌, 곧 바로 해당 Host로 ARP를 전송한다. Router(Layer 3 장비)는 Broadcast frame을 차단시키므로 Host B의 ARP Request Packet은 Host A로 전달되지 않으므로 서로 통신이 되지 않게 된다.

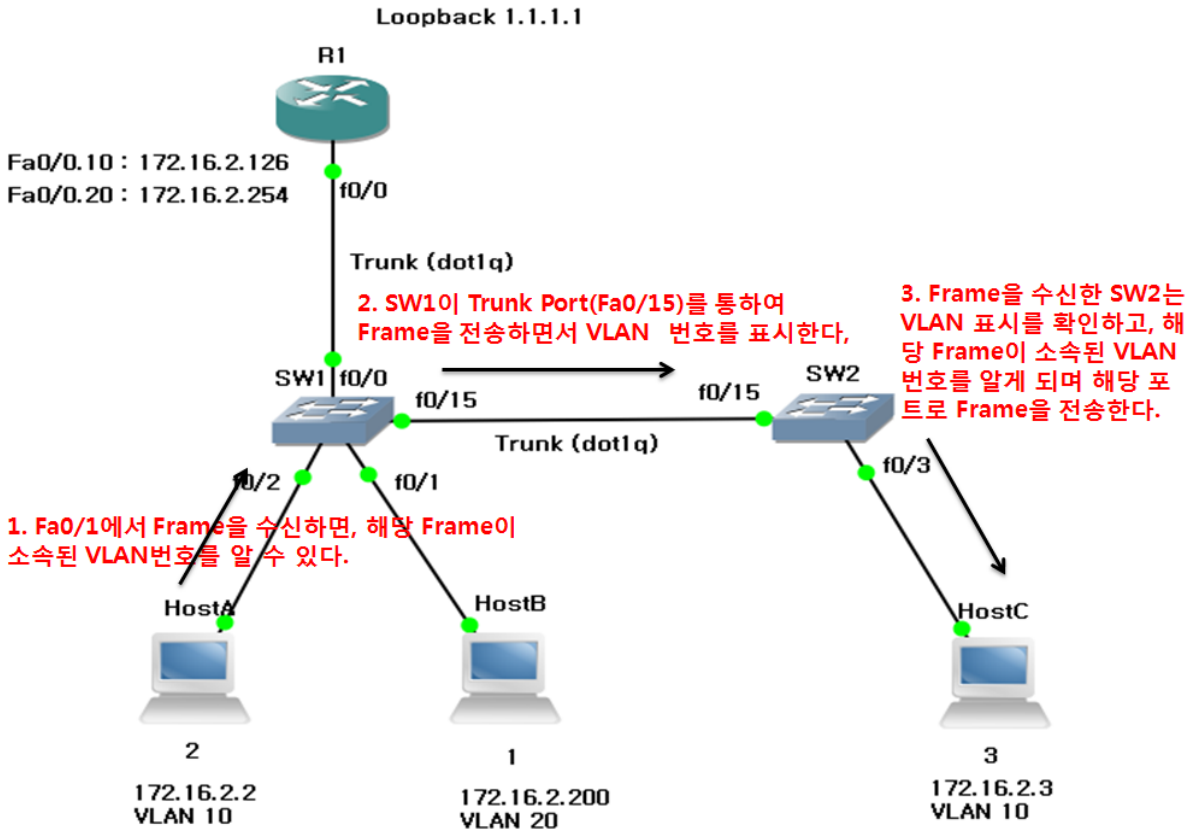
- VLAN의 특성과 ARP를 이해하고 있다면, 어렵지 않게 이해할 수 있다.

1. 5 Trunking

- Trunk, 복수개의 VLAN Frame을 전송할 수 있는 링크
- 특정 포트를 Trunk Port로 동작시키는 것을 Trunking이라 한다.
- 주로 Switch간의 연결 시 사용하며, 만약 VLAN이 하나뿐이라면 Access Port를 사용하는 것이 좋다.

■ Trunking Protocol

- Trunk Port를 통하여 Frame을 전송 할 때는 Frame이 속하는 VLAN 번호를 표시해주어야 한다.
- Trunking Protocol은 Trunk로 연결된 Switch 사이에서만 동작한다.
- Trunking Protocol 을 Trunking Encapsulation 이라고도 한다.



- Trunking Protocol에는 표준 Trunking Protocol인 IEEE 802.1Q와 Cisco에서 개발한 ISL(Inter-Switch Link)이 있다.

■ IEEE 802.1Q

- 원래의 Ethernet Frame의 출발지 주소 다음에 4Byte의 tag를 추가하여 VLAN 번호와 기타 정보를 표시한다.

목적지 주소	출발지 주소	802.1Q Tag	타입/길이	데이터	FCS

EtherType(16 Bits)	Priority (3 Bits)	CFI (1 Bit)	VLAN번호(12 Bits)

- Ether Type : Frame이 802.1Q Frame이라는 것을 표시하며, 값이 항상 0x8100이다. TPID(Tag Protocol Identifier)라고도 한다.
- Priority : Frame의 우선순위를 표시하며, 802.1P 우선순위 필드 또는 CoS(Class of Servier)필드라고도 한다.
- CFI(Canonical Format Identifier) : Tokin Ring에서 사용되는 MAC Address형태를 non-canonical이라고 한다. 따라서 이 bit가 1로 설정되면 Token Ring Frame이 Encapsulation된 것임을 표시한다.
- VLAN 번호(VLAN Identifier): Frame의 VLAN번호를 표시한다.

■ Native VLAN

- 802.1Q Trunk에서만 사용된다. ISL은 Encapsulation되지 않은 Frame을 수신하면 폐기하게 되지만, 802.1Q는 Native VLAN을 이용하여 Enacapsulation되지 않은 Frame도 송,수신 한다.
- Native VLAN과 같은 VLAN에 속하는 Port에서 수신한 Frame을 Trunk로 전송할 때는 Encapsulation하지 않고 보낸다, Trunk를 통하여 Encapsulation되지 않은 Frame을 수신한 Switch는 해당 Frame이 Native VLAN에 소속된 것이라 여기며 해당 Port포트로 전송한다.
- 기본적인 Native VLAN 번호는 1이며, 양측 Trunk Port에서 설정한 Native VLAN 번호가 동일해야 통신이 되며, 그렇지 않을 경우 Spanning-Tree Loop 가 발생할 수 있다.

■ ISL

- Cisco에서 개발한 Encapsulation방식이며, 확장 VLAN은 지원하지 못한다.
- Ethernet Frame은 변경하지 않고 Frame앞에 26Byte의 ISL header를 추가하고, Ethernet FCS 다음에 별도로 4Byte의 ISL FCS를 추가한다.

ISL Header (26 Bytes)	Ethernet Header (14 Bytes)	Data (46–1500 Bytes)	Ethernet FCS (4 Bytes)	ISL FCS (4 Bytes)

- ISL Header
  - DA(40 bit) : ISL Frame임을 표시하며, 0x01-00-0C-00-00 or 0x03-00-0C-00-00의 값을 가진다.
  - Type(4 bit) : Encapsulation된 Frame의 종류를 표시하며 0000은 Ethernet, 0001은 Token Ring, 0010은 FDDI, 0011은 ATM을 나타낸다.
  - User(4 bit) : Ethernet Frame의 우선순위를 표시한다.
  - SA(48 Bit) : 출발지 Switch의 MAC Address를 나타낸다.
  - LEN(16 Bit) : Frame의 길이를 표시한다.
  - SNAP(24 Bit) : Sub Network Access Protocol을 표시하며, 0xAA-AA-03의 값을 가진다.
  - HAS(24 Bit) : 출발지 Switch의 주소 중 상위 3 Byte, Vendor Code또는 OUI(Organizationally Unique Identifier)를 표시한다.
  - VLAN 번호(15 Bit) : VLAN 번호를 표시하며, 할당 bit 중 실제로 10 bit 만 사용한다.
  - BPDU : BPDU, VTP, CDP Frame을 전송할 때 이 필드를 1 로 표시한다.

1. 6 DTP(Dynamic Trunking Protocol)

- Cisco Switch에서 상대 Switch와 Trunk와 관련된 사항을 협상할 때 사용되는 Protocol이다.
- DTP에 의해 결정되는 것은 Trunk Port 전환 여부와 Trunk Port로 동작 시 Encapsulation방식이다.

- Access : Access Port로 동작하며, 상대 Port와는 상관없이 동작한다.
- Trunk : Trunk Port로 동작하며, 상대 Port와는 상관없이 동작한다.

상대 Port를 Trunk Port로 동작시키기 위한 DTP Packet을 전송한다.

- Dynamic desirable : 상대 Port가 Trunk, Desirable, auto인 경우 자신도 Trunk Port로 동작한다.

상대 Port가 Access라면, 자신도 Access로 동작한다.

■ Dynamic auto : 상대 Port가 Trunk, Desirable인 경우 Trunk로 동작하며, Auto나 Access라면 자신도 Access로 동작한다.

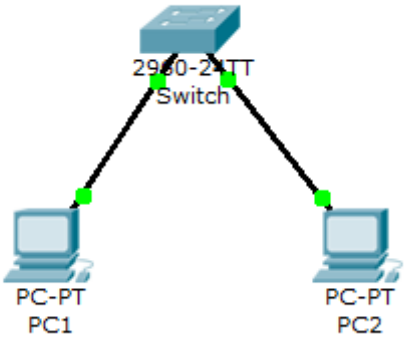
■ Nonegotiage : Switch Port가 Trunk일 때, 상대 Port에게 DTP Packet을 전송하지 않는다.

Dynamic mode에서는 사용할 수 없으며, 상대 측 Port도 반드시 Trunk Port로 설정해야만 Trunk로 동작한다.

	Access	Trunk	Dynamic Desirable	Dynamic Auto
Access	Access	X	Access	Access
Trunk	X	Trunk	Trunk	Trunk
Dynamic Desirable	Access	Trunk	Trunk	Trunk
Dynamic Auto	Access	Trunk	Trunk	Access

1. 7 설정

- Access mode




```
Switch(config)#vlan 10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#exit
Switch(config)#in fa0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#in fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#
```

- VLAN을 생성 후, 해당 포트가 소속될 VLAN번호를 설정한다.

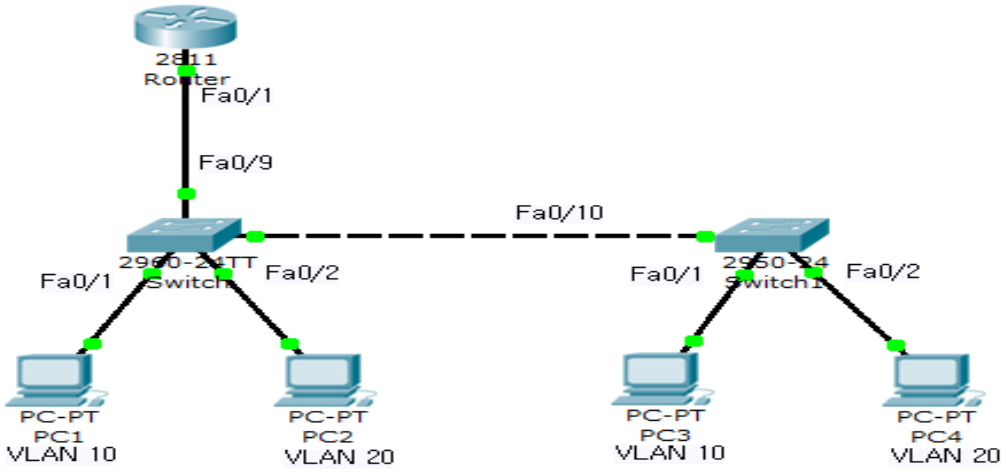
(config-if)#switchport mode access

-> 해당 포트를 access port로 동작

(config-if)#switchport access vlan [vlan number]

-> 포트가 소속될 vlan 번호 설정

- Trunk mode



> Switch 설정

(config)#vlan 10
(config)#vlan 20

: Interface FastEthernet 0/1에서 설정

(config-if)#switchport mode access
(config-if)#switchport access vlan 10

: Interface FastEthernet 0/2에서 설정

(config-if)#switchport mode access
(config-if)#switchport access vlan 20

: Interface FastEthernet 0/9, 0/10에서 설정

(config-if)#switchport trunk encapsulation dot1q

-> trunk encapsulation 을 dot1q(IEEE 802.1Q)로 지정

(config-if)#switchport mode trunk

-> 해당 포트를 trunk mode로 동작

(config-if)#switchport trunk allowed vlan 10,20

-> Trunk를 사용할 수 있는 VLAN 지정

- 기타 VLAN 설정

(config-if)#switchport trunk allowed vlan add 10,20

-> Trunk를 사용할 수 있는 VLAN 추가, Trunk 사용 가능한 VLAN 리스트에 특정 VLAN 추가

(config-if)#switchport trunk allowed vlan all

-> 모든 VLAN이 Trunk를 사용 할 수 있다.

(config-if)#switchport trunk allowed vlan except [VLAN number]

-> 해당 VLAN을 Trunk port에서 제외한다.

(config-if)#switchport trunk allowed vlan none

-> 모든 VLAN이 Trunk port를 사용할 수 없다.

(config-if)#switchport trunk allowed vlan remove [VLAN number]

-> Trunk를 사용 할 수 있는 VLAN중 특정 VLAN을 삭제한다.

> Switch1 설정

VLAN 을 생성하여도 되고, VTP 를 사용하여 Switch 의 VLAN 정보를 받아도 된다(VLAN 10,20 에 대하여)

: Interface FastEthernet 0/1에서 설정

(config-if)#switchport mode access
(config-if)#switchport access vlan 10

: Interface FastEthernet 0/2에서 설정

(config-if)#switchport mode access
(config-if)#switchport access vlan 20

: Interface FastEthernet 0/10에서 설정

(config-if)#switchport trunk encapsulation dot1q
(config-if)#switchport mode trunk
(config-if)#switchport trunk allowed vlan 10,20

> Router 설정

: Interface FastEthernet Fa0/1 에서 설정

(config-if)#no shutdown
(config)#interface fastethernet 0/1.10
(config-if)#encapsulation dot1q 10
(config-if)#ip address 172.16.2.126 255.255.255.128
(config)#interface fastethernet 0/1.20
(config-if)#encapsulation dot1q 20
(config-if)#ip address 182.16.2.254 255.255.255.128

-> 한 개의 인터페이스에서 복수개의 IP 주소를 사용하기 위해 서브 인터페이스 사용, 해당 서브 인터페이스 마다 Trunking Encapsulation 과 VLAN 번호 지정

- Access, Trunk 이외의 DTP mode 설정

(config-if)#switchport mode dynamic auto

-> dynamic auto 방식으로 설정

(config-if)#switchport mode dynamic desirable

-> dynamic desirable 방식으로 설정

- nonegotiate 설정

(config-if)#switchport nonegotiate

-> dynamic 옵션과 동시에 사용할 수 없다.

2. VTP

2. 1 VTP란?

- VLAN Trunking Protocol, 복수개의 Switch들이 VLAN 정보를 교환할 때 사용하는 프로토콜이다.

2. 2 VTP 동작 원리

1. Switch에서 VLAN 설정정보가 변경(VLAN 추가, 삭제, 수정 등)되어, 새로운 VLAN정보를 다른 Switch에게 전송해야 한다.

2. 설정을 변경한 Switch에서 Revision Number를 기존 값 보다 1을 증가시켜 다른 Switch에게 새로운(변경된) VLAN정보와 함께 전송한다.

3. VTP 정보를 수신한 Switch는 자신의 VTP 설정 번호와 수신한 번호를 비교한다.

-> 자신의 VTP Configuration Revision이 수신한 VTP Configuration Revision 보다 낮다면 VLAN 정보를 새로운 정보로 변경한다.

-> 자신의 VTP Configuration Revision이 수신한 것과 같다면 무시한다.

-> 자신의 VTP Configuration Revision이 수신한 것보다 높다면, 자신의 VTP 정보를 역으로 전송한다.

2. 3 VTP 동작

- VTP 정보는 Multicast Frame으로 전달되며, 변경사항이 없어도 매 5분마다 정기적으로 전달하고 변경 시엔 즉시 전달한다.
- VTP Domain Name이 같은 Switch간에만 정보를 교환한다.
- VTP가 동작하기 위한 최소의 조건은 VTP Domain Name이 같고, Trunk Port로 연결되어야 한다.
- 한 개의 Switch에서 VTP Domain Name을 설정하면, Trunk Port로 연결된 Switch들은 자동으로 VTP Domain Name이 설정된다.

- 하지만, Trunk Port로 연결되어 있어도, VTP Domain Name이 설정되어 있지 않다면 동작하지 않는다.

- Switch 간에 VTP Domain Name이 다르면, 상대방이 전송한 VTP 정보를 무시하며 DTP에 의해 동적으로 변한 Trunk Port는 Access Port로 변하게 된다.
- 만약, VTP Domain Name이 다른 Switch을 Trunking하려면 직접 Trunking Encapsulation과 Trunk mode를 지정해야 한다.
- VTP 정보는 Router를 넘어 전송되지 않으며, Switch 사이에 Router가 있다면 VTP Domain은 분리된다.

2. 4 VTP Mode

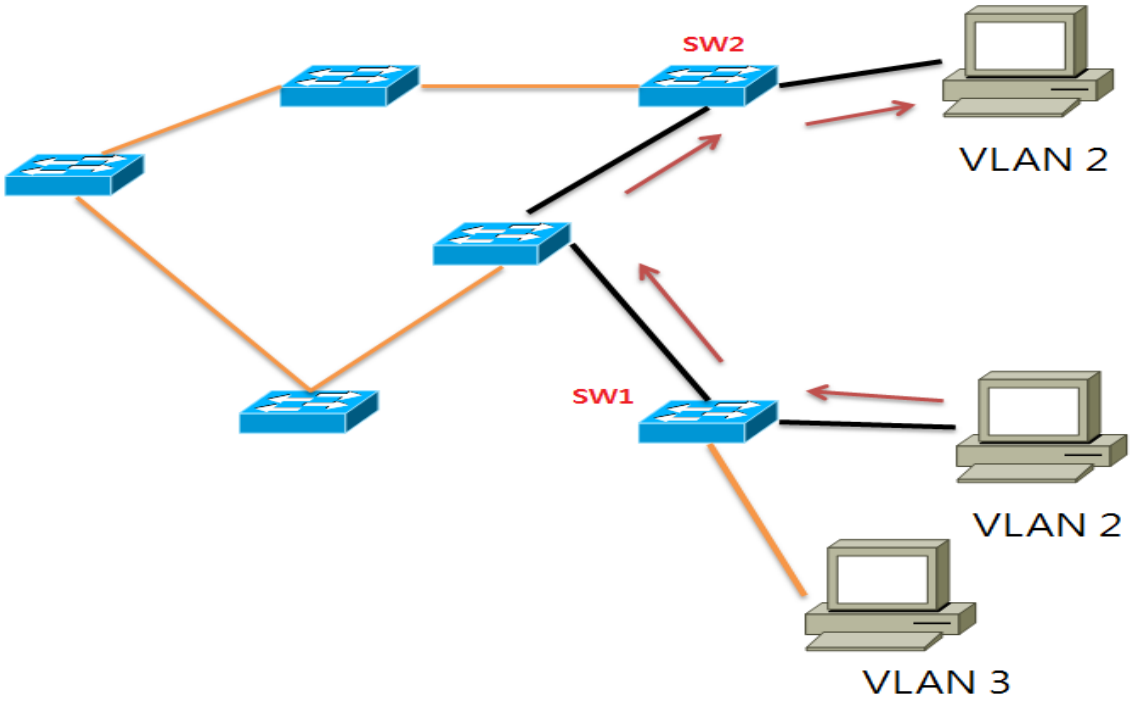
■ Server : VLAN의 생성, 수정, 삭제 등을 할 수 있으며, VLAN정보를 다른 Switch에게 전송한다. 또한, 다른 Switch에게서 받은 정보를 자신의 것과 동기화 시키고 이를 다른 Switch에게 전송(중계)한다. Switch의 기본 VTP mode이며, NVRAM(vlan.dat)에 저장한다.

■ Client : Switch(VTP Server)에게 받은 정보를 자신의 것과 동기화 시키며, 다른 Switch에게 전송(전달 받은 것을 넘겨준다.)한다. VLAN의 생성, 수정, 삭제 등이 불가능하며, NVRAM에 저장하지 않는다.

■ Transparent : 독립된 영역을 만들 때 사용하며, 다른 Switch에게서 받은 VLAN 정보를 자신의 것과 동기화 시키진 않고, 다른 Switch에게 전송(중계)만 해준다. VLAN의 생성, 수정, 삭제 등이 가능하며 NVRAM에 저장한다.

2. 5 VTP Pruning

- 필요 없는 Broadcast Frame은 전송되지 않는다.



- 일부 Traffic(Packet)을, 전송할 필요가 없는 링크를 가로질러 필요 없이 Flooding되는 Traffic을 차단하는 기능이다.
- SW2에는 VLAN 3에 속하는 포트가 없기 때문에 VLAN 3으로 보내는 Broadcast Traffic을 SW2에게 전송할 필요가 없다.

2. 6 설정

- VTP Domain name 설정

: config 모드에서 설정

(config)#vtp domain [Domain name]

: vlan database 에서 설정

(vlan)#vtp domain [Domaine name]

- VTP Mode 설정

: config 모드에서 설정

(config)#vtp mode {server | client | transparent}

: vlan database 에서 설정

(vlan)#vtp {server | client | transparent}

- VTP Password 설정

: config 모드에서 설정

(config)#vtp password [Password]

: vlan database 에서 설정

(vlan)#vtp password [Password]

- VTP Pruning 설정

: config 모드에서 설정

(config)#vtp pruning

: vlan database 에서 설정

(vlan)#vtp pruning

3. Private VLAN

3. 1 사설 VLAN이란?

- Switch당 제한적인 VLAN의 개수를 효과적으로 사용할 수 있게 해준다.
- 같은 Subnet이라도 서로 다른 VLAN을 사용한 것처럼 보여진다.
- Mode에 따라 같은 VLAN번호를 할당하여도 통신이 되지 않는다.

(보안성 증대)

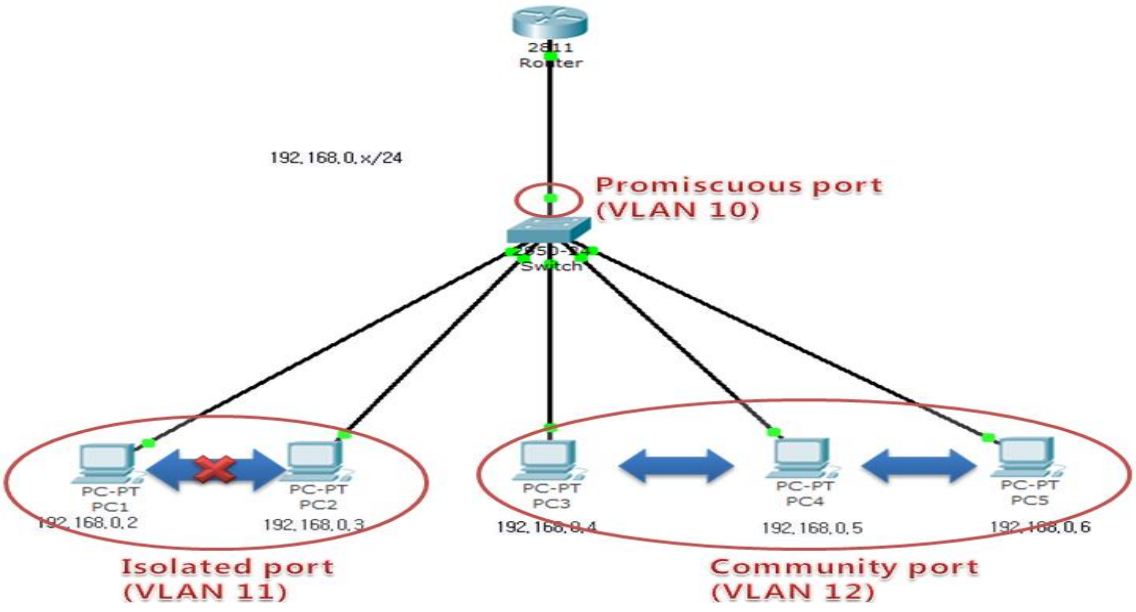
3. 2 Private VLAN의 Port

- Primary VLAN
  - Promiscuous Port : isolated port와 community port에 속한 장비들과 인터넷 등 외부장비와의 연결을 위한 포트이다.

- Secondary VLAN
  - isolated port : isolated port에 소속된 장비들간의 Packet은 Layer 2에서 차단, 이 포트들은 동일한 VLAN에 속하지만 다른 VLAN에 소속된 것처럼 서로 간의 Packet의 Layer 2에서 차단된다.

그러나 동일한 Gateway를 사용하는 것이 일반적이고 Subnet도 동일하다.

  - community port : isolated port와 특성은 비슷하지만, 동일한 VLAN에 소속된 community port간의 통신은 가능하다



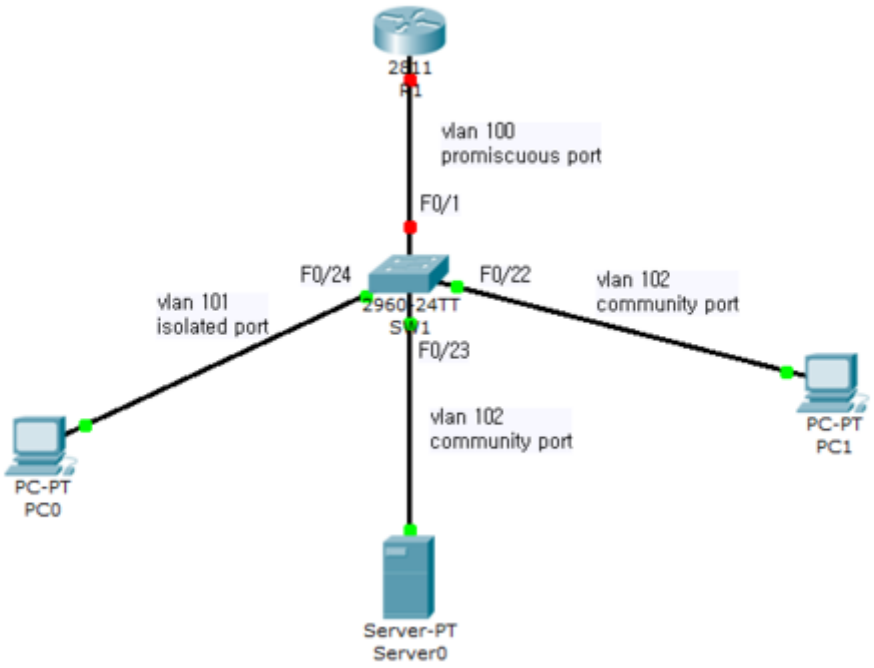
3. 3 Private VLAN 의 특징

- Trunk Port 는 일반 VLAN Traffic 뿐만 아니라, Private VLAN Traffic 도 전달한다.
- 하나의 Primary VLAN 만을 갖는다. 하지만 하나의 Primary VLAN 에 소속되는 포트는 필요에 따라 복수개를 설정할 수 있으며 Private VLAN 내부의 모든 포트들은 Primary VLAN 의 멤버이다.
- 오직 하나의 isolated VLAN 을 갖는다, 그러나 isolated VLAN 에 소속되는 포트는 많다.
- Layer 3 Gateway 는 보통, Promiscuous port 를 통하여 Switch 와 연결된다.
- Primary VLAN 과 Secondary VLAN 을 Trunking 시켜 여러 개의 장비에 걸쳐 설정할 수 있다.
- VTP Version 2 에서는 Private VLAN 을 지원하지 않기 때문에 모든 Switch 에 직접 설정해야 한다.
- Primary VLAN SVI 에 IP Address 를 부여하면, 해당 Subnet 이 전체 Private VLAN 의 서브넷이 된다.

3. 4 Private VLAN 설정 시 주의사항

- VTP Transparent mode 에서 설정해야 한다. Private VLAN 설정 후 VTP mode 변경이 불가능하다.
- VLAN Database 에서는 설정할 수 없다.
- vlan.dat 가 아니라 config 파일에 저장된다.
- VLAN 번호 1, 1002-1005 은 사용할 수 없으며, 확장 VLAN 은 사용할 수 있다.
- Etherchannel port 를 Private VLAN port 로 설정하면 Etherchannel 이 비활성화 된다.
- Promiscuous port 에 portfast 나 BPDU 를 설정하면 안된다.
- Private VLAN 을 설정하면 Sticky ARP 가 자동으로 활성화 된다. Layer 3 Private VLAN Interface 를 통하여 학습된 ARP 는 Sticky ARP 이다.
- Private VLAN 포트들은 SPAN 의 목적지 포트로 설정할 수 없다.

3. 5 설정



> SW1 설정

(config)#vtp mode transparent

-> VTP mode 설정

- VLAN 101 설정(isolated port)

(config-vlan)#name [VLAN name]
(config-vlan)#priavate-vlan isolated

-> isolated port 설정

- VLAN 102 설정(community port)

(config-vlan)#name [VLAN name]
(config-vlan)#private-vlan community

-> community port 설정

- VLAN100 설정(promiscuous port)

(config-vlan)#name [VLAN name]
(config-vlan)#private-vlan primary

-> primary VLAN 설정

(config-vlan)#private-vlan association 101-102

-> primary VLAN 에 소속되는 VLAN 을 지정

: Interface FastEthernet 0/1 에서 설정

(config-if)#switchport mode private-vlan promiscuous

-> promiscuous port 설정

(config-if)#switchport private-vlan mapping 100 101-102

-> primary VLAN 과 secondary VLAN 을 설정(여기선 VLAN 100 이 primary VLAN, 101-102 가 secondary VLAN 이 된다)

: Interface FastEthernet 0/24

(config-if)#switchport mode private-vlan host

-> isolated 나 community port 로 동작할 것이라는 것을 선언

(config-if)#switchport private-vlan association 100 101

-> primary VLAN 에 secondary VLAN 을 소속시킨다(여기선 VLAN 100(primary VLAN)에, VLAN 101(secondary VLAN)을 소속시킨다)

: Interface FastEthernet 0/22, 0/23

(config-if)#switchport mode private-vlan host
(config-if)#switchport private-vlan association 100 102