Switch Network(VLAN)

스위치에서 VALN을 구성하는 이유는 여러 가지가 있지만 다음의 몇 가지 이유로 정리할 수 있다.

1. 기능별 그룹화(논리적 그룹화)
2. 타 네트워크와의 격리(보안성)
3. 네트워크 성능 개선(Broadcast Domain)

1. 주소 관리(MAC-Table)

스위치는 2계층 장비이기 때문에 IP위주가 아닌 MAC위주로 통신을 연결한다. 이러한 MAC주소는 정적 주소와 동적 주소가 있는데. 스위치에서 **#sh mac-address-table** 명령을 사용하면 학습된 주소의 종류를 알 수 있다

```
switch1#sh mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0000.0000.0001    DYNAMIC     Fa0/1
   1    0000.0000.0002    DYNAMIC     Fa0/2
   1    00e0.f938.720e    DYNAMIC     Fa0/14
```

- ***Vlan*** : 스위치는 기본적으로 1개의 vlan을 갖고 있는데, 이 번호는 거의 대부분 1이다.
- ***Mac Address*** : 학습된 Mac주소를 확인할 수 있다. MAC주소는 변경이 가능한데,
  Switch(config-if)#**mac-address** 0000.0001.1111 과 같은 방식으로 입력한다.
- ***Type*** : 주소의 학습 방식을 표시한다. Dynamic, Static의 2가지 방식이 있다. 일반적인 학습 방식은 동적 방식이며, 정적 학습을 원하는 경우는 다음의 명령어를 사용한다.

Switch(config)#**mac-address-table static** 1111.1111.1111 **vlan** 1 **int** fa0/1 학습된 정적 주소는 다음과 같이 표시된다.

```
switch1#sh mac-address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    0000.0000.0001    DYNAMIC     Fa0/1
   1    0000.0000.0002    DYNAMIC     Fa0/2
   1    00e0.f938.720e    DYNAMIC     Fa0/14
   1    1111.1111.1111    STATIC      Fa0/1
```

- ***Port*** : 학습된 포트를 표시한다. 한 개의 포트에 다수의 주소가 학습된 경우는 다른 네트워크 장비가 연결된 Trunk port일 가능성이 높다.

2. VLAN 설정하기

VLAN은 번호로써 구분된다. 스위치가 가질 수 있는 vlan은 1 ~ 4094까지 이며, 기본적으로 갖는 vlan은 다음과 같이 모두 5개 이다.

```
VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
```

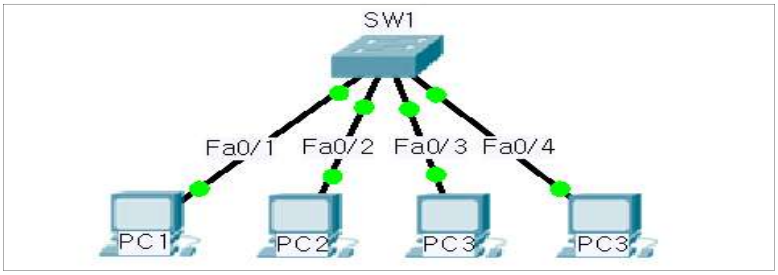
1005 trnet-default active

1~1005 까지는 일반 Vlan이며, 이중에서 1002~1005는 토큰링과 FDDI용으로 사용되고, Ethernet용은 1~1001까지이다.

Vlna번호가 **1006 ~ 4094인 것을 확장(Extended) Vlan**이라고 한다. 사용할 수 있는 Vlan숫자는 스위치마다 다르다.

Vlna을 구성하는 방법은 의외로 간단하다. 먼저 vlan을 구성하고 난 후에 원하는 Interface를 할당하면 된다.

[그림2-1]



1. 위 그림과 같은 환경에서 PC1, PC2는 Vlan 10에 할당하고 PC3, PC4는 Vlan 20에 할당해 보자

```
Switch1(config)#vlan 10                 ==> vlan 10 생성
Switch1(config-vlan)#name VLAN_A        ==> vlan 이름 부여
Switch1(config-vlan)#vlan 20            ==> vlan 20 생성
Switch1(config-vlan)#name VLAN_B        ==> vlan 이름 부여
```

2. 다음으로 특정 인터페이스를 vlan에 할당해 보자

```
Switch(config)#int range fa0/1 , fastEthernet 0/2       ==> fa0/1, fa0/2 선택
Switch(config-if-range)#switchport mode access          ==>일반 스위치 포트로 설정
Switch(config-if-range)#switchport access vlan 10       ==>vlan10에 할당
Switch(config-if-range)#exit
Switch(config)#int range fa0/3 , fastEthernet 0/4       ==>fa0/3, fa0/4 선택
Switch(config-if-range)#switchport mode access          ==>일반 스위치 포트로 설정
Switch(config-if-range)#switchport access vlan 20       ==>vlan20에 할당
```

3. 구성된 vlan정보를 확인 한다.

```
Switch#sh vlan

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Fa0/5, Fa0/6, Fa0/7, Fa0/8
                    ----------omit--------------
10   VLAN_A                            active    Fa0/1, Fa0/2
20   VLAN_B                            active    Fa0/3, Fa0/4
1002 fddi-default                      active
1003 token-ring-default                active
1004 fddinet-default                   active
1005 trnet-default                     active
```

결과를 보면 vlan10, vlan20이 생성되었으며, 생성된 vlan에 인터페이스가 할당된 것을 볼 수 있다.

※이렇게 생성된 vlan은 이제부터 서로 다른 네트워크가 되므로 IP, Subnetmask값을 별도 입력해 줘야 한다.

```
Switch1(config)#int vlan 10
Switch1(config-if)#no shutdown
Switch1(config-if)#ip addr 192.168.0.1 255.255.255.0
```

=>스위치는 물리 인터페이스에 ip를 부여하는 경우보다는 관리(원격제어)를 위한 목적에서 vlan에 할당하는 경우가 많다.

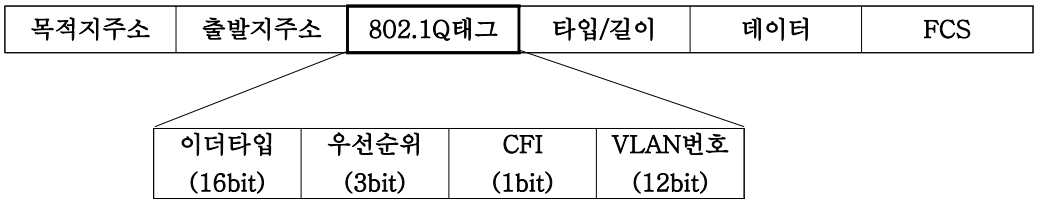
3.Trunking

스위치의 모든 포트는 기본적으로 vlan1에 할당되어 있다는 것은 이미 설명하였다. 단일 스위치만을 이용하는 경우에는 모든 포트의 운영 모드가 access상태가 된다. 이 상태에서는 전송되는 프레임의 Tag에 추가된 내용을 식별하지 않게 되는데, 스위치는 vlan1에 대해서는 Native vlan 이라고 하여 프레임의 끝에 Tag처리를 하지 않은 상태에서 전송을 하게 된다. 그렇기 때문에 스위치의 모든 PC들은 연결된 상태에서 동일한 IP, SubnetMask정보를 갖고 있으면, 통신 가능 상태가 되는 것이다. 스위치<->스위치, 스위치<->라우터 간에 사용되는 인터페이스의 경우 단일의 vlan을 사용하면 문제가 없겠으나, 서로다른 vlan을 사용하는 경우에는 프레임 tag를 식별하도록 포트를 바꿔줘야 한다. 이렇게 서로 다른 vlan간
통신을 지원하기 위하여 스위치의 포트에 지정하는 것이 Trunk port가 되겠다. Trunk Port에서는 서로 다른 vlan정보를 식별하기 위해서 프로토콜을 사용하고 있는데, 시스코의 ISL과 ISO의 IEEE802.1Q가 있다. 최근에는 QOS와 타 스위치와의 호환성을 고려한 802.1Q(dot1q라고 함)가 많이 사용된다.

3-1. 802.1Q 트렁킹

802.1Q 트렁킹은 IEEE802.1Q에서 정의된 표준 트렁킹 프로토콜이다. 이 방식은 원래의 이더넷 프레임의 출발지 주소 다음에 4바이트 길이의 802.1Q Tag를 추가하여 VLAN번호와 기타 정보를 표시한다.

[그림3-1]



- **이더타입** : 현재의 프레임이 802.1Q 프레임이라는 것을 표시하며, 항상 값이 0x8100이다.
- **우선순위** : 프레임의 우선순위를 표시한다. 이것을 802.1P 우선순위필드 또는, CoS(class of service)필드라고도 한다. 0에서 7사이의 값을 가지며, 값이 클수록 우선순위가 높다. 음성이나 동영상 테이터 전송시 사용.
- **CFI(Canonical format identifier)** : 토큰링에서 사용되는 MAC 주소 형태를 non-canonical이라고 한다. 이 비트를 1로 설정하면 토큰링 프레임이 인캡슐레이션된 것임을 표시한다.
- **VLAN번호** : 프레임의 VLAN 번호를 표시한다. 필드의 길이가 12비트이므로, 802.1Q 트렁킹 방식을 사용하면 4096개의 VLAN을 지원한다.

※프로토콜 지정은 다음과 같이 한다.

Switch1(config-if)#switchport trunk encapsulation dot1q

3-2 Native VLAN

Native vlan방식은 802.1q에서만 사용된다. 이것은 스위치에서 frame tag를 처리할 경우 뒤에 tag가 없는 프레임을 갖는 vlan을 의미하는 것으로 기본적으로 스위치가 갖는 native vlan은 vlan 1이다. 네이티브 vlan은 스위치 입장에서 Tag를 처리할 필요가 없기 때문에 부하를 다소나마 줄일 수 있게 된다. 따라서, 다수의 PC가 편성된 Vlan을 Native Vlan으로 구성하는 것이 좋다고 할 수 있다.

※네이티브 vlan 설정은 다음과 같이 한다.

*Switch1(config-if)#switchport trunk native vlan 2 ==>*vlan 2를 네이티브로 구성

3-2 트렁크 허용 VLAN 번호 설정

기본적으로 트렁크는 모든 VLAN이 사용할 수 있다. 그러나, 특정 VLAN만 트렁크를 사용하게 하려면 **switchport trunk allowed vlan** 명령을 사용한다. 명령어 다음에 특정 VLAN 번호를 지정하면 해당 VLAN만 이 트렁크를 사용할 수 있게 된다.

```
Switch1(config)#int fa0/24
Switch1(config-if)#switchport trun allowed vlan 10,20
```

결과를 확인해 보면 다음과 같다

Switch#sh int trun

Port Mode Encapsulation Status Native vlan
Fa0/24 on 802.1q trunking 1
Port Vlans allowed on trunk
Fa0/24 10,20
----------omit----------

위 결과에서 알 수 있듯이 특정 vlan에 소속된 장비로 부터의 트래픽만을 허용한다.

허용된 VALN에 추가적인 허용, 거부, 제외, 제거를 하는 경우는 다음의 명령어를 사용한다.

Switch1(config)#int fa0/24
Switch1(config-if)#switchport trunk allowed vlan add 30-40 ==>vlan 30~40추가
Switch1(config-if)#switchport trunk allowed vlan all ==>모든 vlan허용
Switch1(config-if)#switchport trunk allowed vlan except 100-200 ==>100~200은 제외
Switch1(config-if)#switchport trunk allowed vlan remove 30-40 ==>30~40제거