

제2장 VLAN(Virtual LAN)

VLAN(Virtual LAN):

내부 네트워크 환경에 시스템이 많이 있거나 또는 추가되면 브로드캐스트 플러딩이 비례적으로 증가되므로 대역폭 부족 현상, 전송 장비 부하라는 문제가 발생될 수 있다. 그리고 스위치로 구성된 내부 네트워크는 하나의 브로드캐스트 도메인으로 동작하기 때문에 시스템들 간에 유니캐스트 접근 자체가 가능하므로 보안적인 측면에서도 문제가 발생될 수 있다.

이러한 문제를 해결하기 위해서 스위치에는 VLAN 기능을 지원한다. VLAN 기능을 이용하면 내부 네트워크를 여러 개의 논리적인 네트워크로 분리할 수 있기 때문에 브로드캐스트 플러딩을 최소화하고 서로 다른 VLAN 간에 유니캐스트 접근을 차단시킬 수 있다.

VLAN을 구성한 내부 네트워크는 다음과 같은 장점을 갖게된다.

- ① 논리적인 브로드캐스트 도메인을 분할하여 브로드캐스트 플러딩을 최소화한다.
- ② 서로 다른 VLAN 간에 브로드캐스트가 차단되므로 ARP 학습에 의한 유니캐스트 접근이 불가능하다.
- ③ Spanning-Tree 이중화 환경에서 VLAN 로드 분산이 가능하다.
- ④ 논리적인 브로드캐스트 도메인이기 때문에 위치상 제약이 없으며, 관리가 효율적이다.

```
SW1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, 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, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

- Vlan 1 : 브로드캐스트가 공유되는 포트
- VLAN1 안에 있는 포트들은 같은 네트워크가 된다.

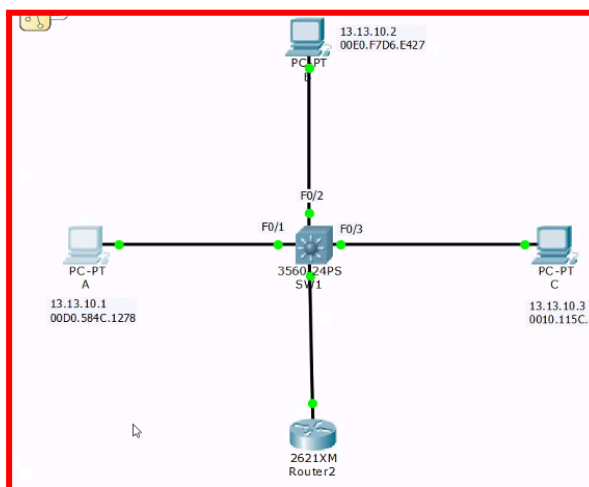


```

FastEthernet0/24      unassigned      YES unset  down      down
GigabitEthernet0/1    unassigned      YES unset  down      down
GigabitEthernet0/2    unassigned      YES unset  down      down
Vlan1                 13.13.10.101    YES manual up         up
SW1#
SW1#show vlan brief
VLAN Name                Status    Ports
----
1    default              active    Fa0/1, Fa0/2, Fa0/3, 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, Fa0/22, Fa0/23, Fa0/24,
                                           Gig0/1, Gig0/2

```

- A, B, C는 같은 VLAN에 있고 등록이 되어 있으므로 통신이 가능하다.
- 따라서 관리자는 스위치에 Telnet 접속을 개인 PC에서 가능하다.
- 관리목적으로 사용이 가능하다.



```

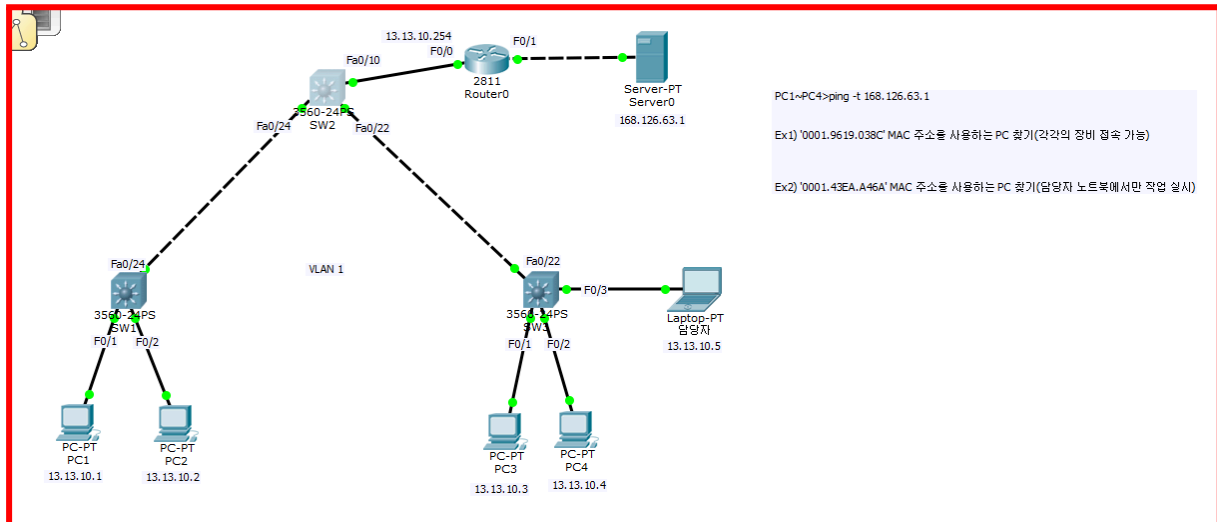
Enter configuration commands, one per line. End with Ctrl-Z.
SW1(config)#
SW1(config)#no ip default-gateway 13.13.10.254
SW1(config)#
SW1(config)#do ping 168.126.63.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 168.126.63.1, timeout is 2 seconds:
....
Success rate is 0 percent (0/5)

SW1(config)#
SW1(config)#ip default-gateway 13.13.10.254
SW1(config)#
SW1(config)#do ping 168.126.63.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 168.126.63.1, timeout is 2 seconds:
!!!!

```

- 스위치에서도 게이트웨이를 지정할 수 있다.
- 나머지는 라우터랑 다 비슷하다.

Ex1) '0001.9619.038C' MAC 주소를 사용하는 PC 찾기(각각의 장비 접속 가능)



```
Router0
Physical Config CLI
IOS Command Line Interface

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state up

R1>en
Password:
R1#
R1#
R1#show arp
Protocol Address Age (min) Hardware Addr Type Interface
Internet 13.13.10.1 3 000B.BE12.90C0 ARPA FastEthernet0/0
Internet 13.13.10.2 3 0001.43EA.A46A ARPA FastEthernet0/0
Internet 13.13.10.3 3 0001.9619.038C ARPA FastEthernet0/0
Internet 13.13.10.4 3 00E0.B049.32C6 ARPA FastEthernet0/0
Internet 13.13.10.254 - 000C.CF94.2401 ARPA FastEthernet0/0
Internet 168.126.63.1 3 000C.CFE0.C069 ARPA FastEthernet0/1
Internet 168.126.63.254 - 000C.CF94.2402 ARPA FastEthernet0/1
R1#
```

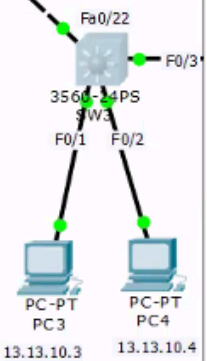
- 위에서부터 아래로 찾아보자

2번 스위치 확인

```
SW2>
SW2>en
Password:
SW2#
SW2#show mac address-table
                Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0001.43ea.a46a    DYNAMIC Fa0/24
1       0001.9619.038c    DYNAMIC Fa0/22
1       000b.be12.90c0    DYNAMIC Fa0/24
1       000c.cf94.2401    DYNAMIC Fa0/10
1       0090.0cb2.8518    DYNAMIC Fa0/24
1       00e0.b049.32c6    DYNAMIC Fa0/22
SW2#
```

- 22번포트에 있다.

3번 스위치 찾자:



```
SW3>en
Password:
SW3#
SW3#show mac ad
SW3#show mac address-table
                Mac Address Table
-----
Vlan    Mac Address      Type    Ports
----    -
1       0001.9619.038c    DYNAMIC Fa0/1
1       000c.cf94.2401    DYNAMIC Fa0/22
1       0030.f223.c516    DYNAMIC Fa0/22
1       00e0.b049.32c6    DYNAMIC Fa0/2
SW3#
```

- 3번 PC를 찾았다.
- 위에서부터 찾으면 금방 찾는다.

담당자 노트북에서만 찾아보자:

```
PC>telnet 13.13.10.254
Trying 13.13.10.254 ...Open

User Access Verification

Password:
R1>enable cisco
^
% Invalid input detected at '^' marker.

R1>enable cisco
^
% Invalid input detected at '^' marker.

R1>enable
Password:
R1#show arp

```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	13.13.10.1	19	000B.BE12.90C0	ARPA	FastEthernet0/0
Internet	13.13.10.2	19	0001.43EA.A46A	ARPA	FastEthernet0/0
Internet	13.13.10.3	19	0001.9619.038C	ARPA	FastEthernet0/0
Internet	13.13.10.4	19	00E0.B049.32C6	ARPA	FastEthernet0/0
Internet	13.13.10.5	0	0001.C7E1.E3D5	ARPA	FastEthernet0/0
Internet	13.13.10.254	-	000C.CF94.2401	ARPA	FastEthernet0/0
Internet	168.126.63.1	19	000C.CFE0.C069	ARPA	FastEthernet0/1
Internet	168.126.63.254	-	000C.CF94.2402	ARPA	FastEthernet0/1

- telnet으로 접속
- 맥 어드레스 찾기

2번스위치 접속:

하지만 VLAN 설정이 되지 않았다.

```
!
interface Vlan1
  no ip address
  shutdown
!
ip classless
!
ip flow-export version 9
!
```

따라서 관리자 노트북에서 접속 불가능

스위치마다 관리자 설정을 해준다:

```
@ SW1
conf t
int vlan 1
ip address 13.13.10.101 255.255.255.0
no shutdown
end
```

```
@ SW2
conf t
int vlan 1
ip address 13.13.10.102 255.255.255.0
no shutdown
end
```

```
@ SW3
conf t
int vlan 1
ip address 13.13.10.103 255.255.255.0
no shutdown
end
```

2번 스위치:

```
Password:
SW2>en
Password:
SW2#show mac
SW2#show mac ad
SW2#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.43ea.a46a    DYNAMIC   Fa0/24
1       0001.9619.038c    DYNAMIC   Fa0/22
1       0001.c7e1.e3d5    DYNAMIC   Fa0/22
1       000b.be12.90c0    DYNAMIC   Fa0/24
1       000c.cf94.2401    DYNAMIC   Fa0/10
1       0090.0cb2.8518    DYNAMIC   Fa0/24
1       00e0.b049.32c6    DYNAMIC   Fa0/22
SW2#
```

- 이제 접속 가능하다

3번 스위치 접속:

```

Passw0rd.
SW3>en
Password:
Password:
SW3#show mac address
SW3#show mac address-table
      Mac Address Table
-----
Vlan    Mac Address      Type      Ports
----    -
1       0001.9619.038c    DYNAMIC   Fa0/1
1       0001.c7e1.e3d5    DYNAMIC   Fa0/3
1       000c.cf94.2401    DYNAMIC   Fa0/22
1       0030.f223.c516    DYNAMIC   Fa0/22
1       00e0.b049.32c6    DYNAMIC   Fa0/2
SW3#
  
```

- 관리자 권한으로 관리자 PC에서 접속 가능하다.

show cdp neighbor

```

User Access Verification

Password:
R1>en
Password:
R1#
R1#show arp
Protocol Address          Age (min)  Hardware Addr  Type   Interface
-----
Internet 13.13.10.1          26         000B.BE12.90C0  ARPA   FastEthernet0/0
Internet 13.13.10.2          26         0001.43EA.A46A  ARPA   FastEthernet0/0
Internet 13.13.10.3          26         0001.9619.038C  ARPA   FastEthernet0/0
Internet 13.13.10.4          26         00E0.B049.32C6  ARPA   FastEthernet0/0
Internet 13.13.10.5          7          0001.C7E1.E3D5  ARPA   FastEthernet0/0
Internet 13.13.10.254        -          000C.CF94.2401  ARPA   FastEthernet0/0
Internet 168.126.63.1        26         000C.CFE0.C069  ARPA   FastEthernet0/1
Internet 168.126.63.254     -          000C.CF94.2402  ARPA   FastEthernet0/1
R1#
R1#show cdp neighbor
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID         Local Intrfce   Holdtme    Capability Platform  Port ID
SW2               Fas 0/0        176        SRP          3560      Fas 0/10
R1#
  
```

- 연결상태, 뭐가 연결되어있는지 알 수 있다.

show cdp neighbor detail

```

R1#show cdp neighbor detail

Device ID: SW2
Entry address(es):
  IP address : 13.13.10.102
Platform: cisco 3560, Capabilities:
Interface: FastEthernet0/0, Port ID (outgoing port): FastEthernet0/10
Holdtime: 173

Version :
Cisco IOS Software, C3560 Software (C3560-ADVIPSERVICESK9-M), Version 12.2(37)SE1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 05-Jul-07 22:22 by pt_team

advertisement version: 2
Duplex: full

R1#
  
```

- 더 자세한 정보가 나온다.
 - 운영체제 정보, 관리자 IP 등 (CISCO 장비인지 아닌지도 알수 있다.)

cdp는 보안문제때문에 지금은 잘 사용하지 않는다.

```
SW3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW3(config)#
SW3(config)#no cdp en
SW3(config)#no cdp
% Incomplete command.
SW3(config)#no cdp run
SW3(config)#
```

- CDP 동작을 다 끈다

LLDP 라는 유사한 동작이 있다. (사용을 잘 안한다)

Ex2) '0001.43EA.A46A' MAC 주소를 사용하는 PC 찾기(담당자 노트북에서만 작업 실시)