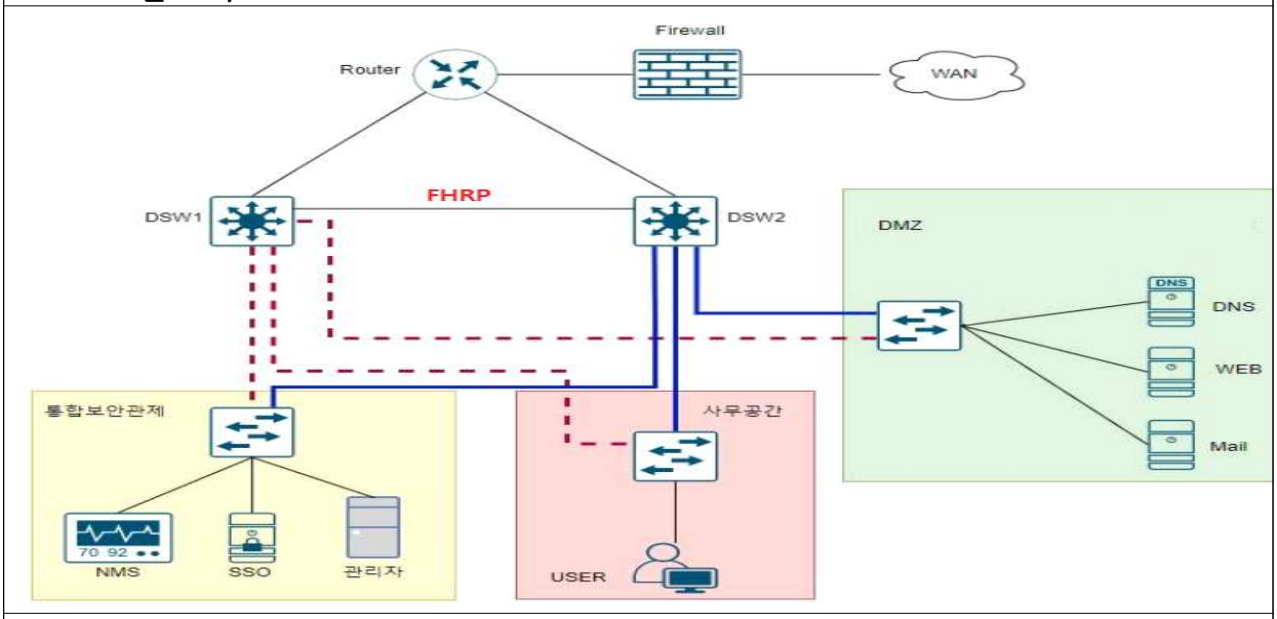
RADIUS 인증 시스템을 이용한 인프라스트럭처 구축

작성자 : **설****, **유****, **강****

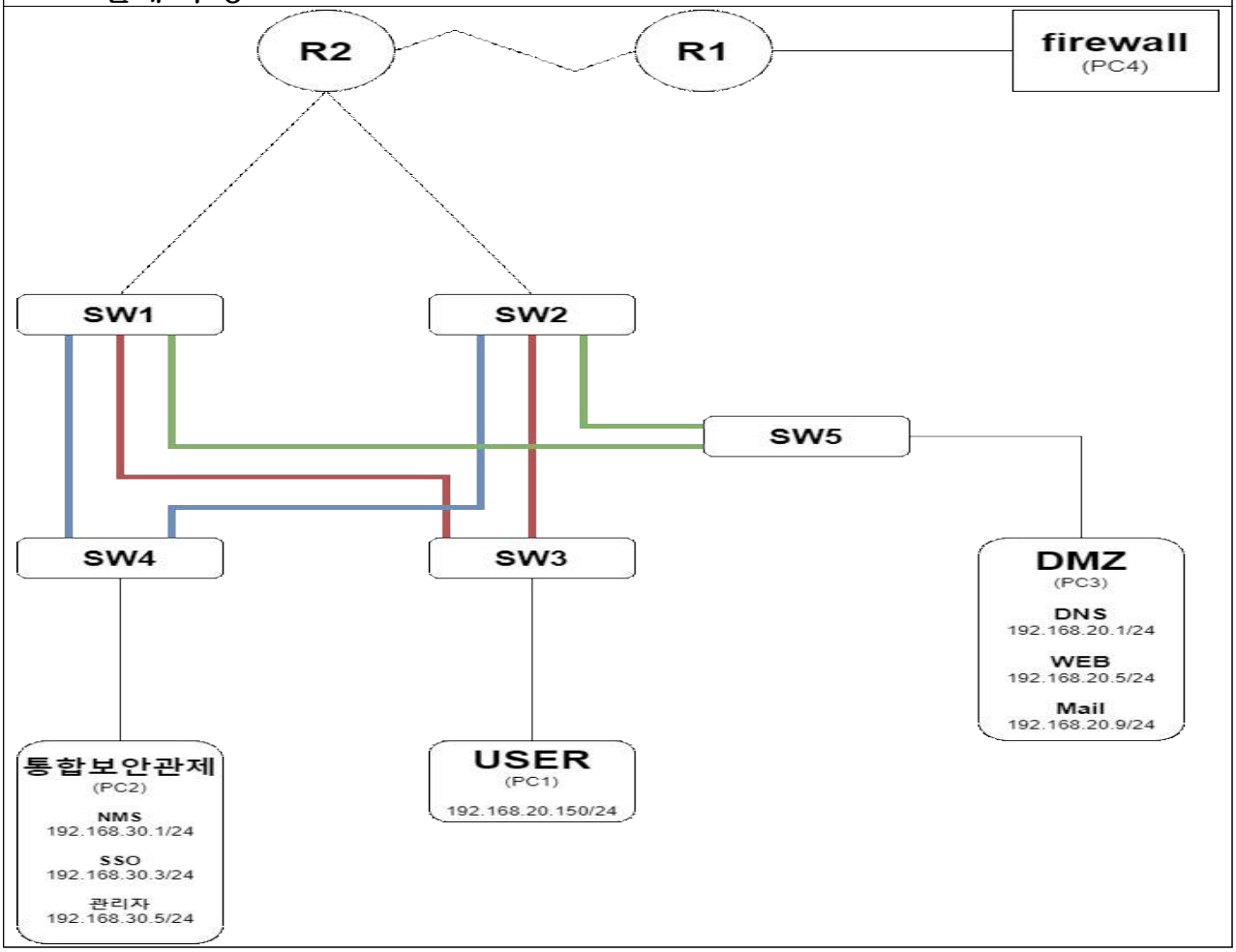
목 차

1. 네트워크 구성도

1-1. 토폴로지



1-2. 실제 구성도



2. 인프라 설계

장비명	OS	네트워크 종류	IP	Gateway	Interface
R1(Router)	**Cisco 2811**	Static	172.16.10.13/30	172.16.10.14/30	F/E 0/0
		OSPF	172.16.10.10/30		S 0/0/0
R2(Router)	**Cisco 2801**	OSPF	172.16.10.9/30	172.16.10.14/30	S 0/1/0
			172.16.10.5/30		F/E 0/1
			172.16.10.1/30		F/E 0/0
SW1(L3_sw)	**Cisco WS -C3550-24**	OSPF	172.16.10.1/30	172.16.10.14/30	F/E 0/5
			192.168.10.252/24	192.168.10.254/24	Vlan 10
			192.168.20.252/24	192.168.20.254/24	Vlan 20
			192.168.30.252/24	192.168.10.254/24	Vlan 30
SW2(L3_sw)	**Cisco WS -C3750G-24Ts**	OSPF	172.16.10.6/30	172.16.10.14/30	G 2/0/6
			192.168.10.253/24	192.168.10.254/24	Vlan 10
			192.168.20.253/24	192.168.20.254/24	Vlan 20
			192.168.30.254/24	192.168.30.254/24	Vlan 30
SW3(L2_sw)	**Cisco WS-C2950-24**	Vlan 10	192.168.10.250/24	192.168.10.254/24	Vlan 10
SW4(L2_sw)	**Cisco WS-C2950-24**	Vlan 30	192.168.30.250/24	192.168.30.254/24	Vlan 30
SW5(L2_sw)	**Cisco WS-C2960G -24TC-L**	Vlan 20	192.168.20.250/24	192.168.20.254/24	Vlan 20
Firewall01	**Centos 7**	IPtables	172.16.10.14/30	10.100.102.1/24	ens 34
			10.100.102.241/24	10.100.102.1/24	ens 33
NMS	**Ubuntu**	Vlan 30	192.168.30.1/24	192.168.30.254	Vlan 30
SSO	**Ubuntu**	Vlan 30	192.168.30.3/24	192.168.30.254	Vlan 30
관리자	**Centos 7 (GUI)**	Vlan 30	192.168.30.5/24	192.168.30.254	Vlan 30
USER	**Win7**	Vlan 10	192.168.10.150/24	192.168.10.254	Vlan 10
DNS	**Centos 7**	Vlan 20	192.168.20.1/24	192.168.20.254	Vlan 20
WEB	**Centos 7**	Vlan 20	192.168.20.5/24	192.168.20.254	Vlan 20
MAIL	**Centos 7**	Vlan 20	192.168.20.9/24	192.168.20.254	Vlan 20

3. 인프라 구축

3-1. R1(Router) 구축 및 설정

▶ IP 설정

- 각각의 Interface에 IP를 설정

```
interface FastEthernet0/0
 ip address 172.16.10.13 255.255.255.252
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 172.16.10.10 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 clock rate 2000000
```

▶ 라우팅 설정

- OSPF 프로토콜을 사용하였고, area는 0으로 설정
- Static 설정 및 OSPF에 default-information originate 설정

```
router ospf 100
 router-id 5.5.5.5
 log-adjacency-changes
 redistribute static subnets
 network 172.16.10.8 0.0.0.3 area 0
 default-information originate
!
ip route 0.0.0.0 0.0.0.0 172.16.10.14
```

▶ NMS 및 SSO 설정

- SSO(radius) 설정
- NMS(librenms) 설정

```
logging trap debugging
logging 192.168.30.1
snmp-server host 192.168.30.1 version 2c r1
!
!
!
!
!
radius-server host 192.168.30.3 auth-port 1812 acct-port 1646 key 1234
```

```
aaa new-model
!
!
aaa authentication login default group radius local
!
!
aaa session-id common
```

▶ NAT, 포트포워딩

- 192.168.10.0 ~ 192.168.30.254까지 NAT설정(ACL설정) 및 포트포워딩 설정

```
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/0 overload
ip nat inside source static tcp 192.168.30.5 22 172.16.10.13 22 extendable
ip nat inside source static tcp 192.168.20.9 25 172.16.10.13 25 extendable
ip nat inside source static tcp 192.168.20.1 53 172.16.10.13 53 extendable
ip nat inside source static udp 192.168.20.1 53 172.16.10.13 53 extendable
ip nat inside source static tcp 192.168.20.5 80 172.16.10.13 80 extendable
ip nat inside source static udp 192.168.30.1 161 172.16.10.13 161 extendable
ip nat inside source static tcp 192.168.20.5 443 172.16.10.13 443 extendable
ip nat inside source static tcp 192.168.30.5 1812 172.16.10.13 1812 extendable
!
ip radius source-interface Serial0/0/0
logging trap debugging
logging 192.168.30.1
access-list 1 permit 192.168.10.0 0.0.0.255
access-list 1 permit 192.168.20.0 0.0.0.255
access-list 1 permit 192.168.30.0 0.0.0.255
```

3-2. R2(Router) 구축 및 설정

▶ IP 설정

- 각각의 Interface에 IP를 설정

```
interface FastEthernet0/0
 ip address 172.16.10.1 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 172.16.10.5 255.255.255.252
 duplex auto
 speed auto
!
interface Serial0/1/0
 ip address 172.16.10.9 255.255.255.252
 no fair-queue
```

▶ 라우팅 설정

- OSPF 프로토콜을 사용하였고, area는 0으로 설정

```
router ospf 100
 router-id 4.4.4.4
 log-adjacency-changes
 network 172.16.10.0 0.0.0.3 area 0
 network 172.16.10.4 0.0.0.3 area 0
 network 172.16.10.8 0.0.0.3 area 0
```

▶ NMS 및 SSO 설정

- SSO(radius) 설정
- NMS(librenms) 설정

```
logging trap debugging
logging 192.168.30.1
snmp-server host 192.168.30.1 version 2c r2
!
!
!
!
!
radius-server host 192.168.30.3 auth-port 1812 acct-port 1646 key 1234
aaa new-model
!
!
aaa authentication login default group radius local
aaa authentication login LPIC group radius local
!
!
aaa session-id common
```

3-3. SW1(L3_sw) 구축 및 설정

▶ IP 설정

- 각각의 Vlan에 IP를 설정
- 다른 스위치와 연결된 포트를 trunk mode 설정

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.10.252 255.255.255.0
 standby 10 ip 192.168.10.254
 standby 10 priority 150
 standby 10 preempt
 standby 10 track FastEthernet0/5 51
!
interface Vlan20
 ip address 192.168.20.252 255.255.255.0
 standby 20 ip 192.168.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 192.168.30.252 255.255.255.0
 standby 30 ip 192.168.30.254
 standby 30 priority 150
 standby 30 preempt
 standby 30 track FastEthernet0/5 51
```

```
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/5
 no switchport
 ip address 172.16.10.2 255.255.255.252
```

▶ 라우팅 설정

- OSPF 프로토콜을 사용하였고, area는 0으로 설정
- L3 Switch이기 때문에 'ip routing' 사용

```
router ospf 100
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface Vlan10
 passive-interface Vlan20
 passive-interface Vlan30
 network 172.16.10.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
```

▶ NMS 및 SSO 설정

- SSO(radius) 설정
- NMS(librenms) 설정

```
logging trap debugging
logging 192.168.30.1
snmp-server host 192.168.30.1 version 2c cloud_sw1
radius-server host 192.168.30.3 auth-port 1812 acct-port 1646 key 1234
aaa new-model
!
!
aaa authentication login default group radius local
!
!
!
aaa session-id common
```

▶ 게이트웨이 이중화

- 이중화 프로토콜 HSRP를 사용
- SW1에는 Vlan 10과 Vlan 30을 Active 설정
- SW1과 SW2의 라우팅을 끊어주기 위해 passive-interface를 설정

```
interface Vlan10
 ip address 192.168.10.252 255.255.255.0
 standby 10 ip 192.168.10.254
 standby 10 priority 150
 standby 10 preempt
 standby 10 track FastEthernet0/5 51
!
interface Vlan20
 ip address 192.168.20.252 255.255.255.0
 standby 20 ip 192.168.20.254
 standby 20 preempt
!
interface Vlan30
 ip address 192.168.30.252 255.255.255.0
 standby 30 ip 192.168.30.254
 standby 30 priority 150
 standby 30 preempt
 standby 30 track FastEthernet0/5 51
router ospf 100
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface Vlan10
 passive-interface Vlan20
 passive-interface Vlan30
```

▶ ACL 설정

- Vlan 20의 Access-list는 120으로 설정
- Vlan 30의 Access-list는 130으로 설정

```
access-list 120 permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.1 eq domain
access-list 120 permit udp 192.168.10.0 0.0.0.255 host 192.168.20.1 eq domain
access-list 120 permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.5 eq www
access-list 120 permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.5 eq 443
access-list 120 permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.9 eq smtp
access-list 120 permit tcp 192.168.10.0 0.0.0.255 host 192.168.20.9 eq pop3
access-list 120 permit udp host 192.168.10.250 host 192.168.20.100 eq tftp
access-list 120 permit tcp host 192.168.10.250 host 192.168.20.100 eq 72
access-list 120 permit icmp 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 120 deny   ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 120 permit udp host 192.168.30.250 host 192.168.20.100 eq tftp
access-list 120 permit tcp host 192.168.30.250 host 192.168.20.100 eq 72
access-list 120 permit udp host 192.168.30.1 192.168.20.0 0.0.0.255 eq snmp
access-list 120 permit udp host 192.168.30.1 192.168.20.0 0.0.0.255 eq syslog
access-list 120 permit tcp host 192.168.30.1 192.168.20.0 0.0.0.255 eq 601
access-list 120 permit udp host 192.168.30.3 192.168.20.0 0.0.0.255 eq 1812
access-list 120 permit tcp host 192.168.30.5 192.168.20.0 0.0.0.255 eq 22
access-list 120 permit tcp 192.168.20.0 0.0.0.255 192.168.20.0 0.0.0.255 eq 22
access-list 120 permit icmp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 120 permit icmp 192.168.20.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 120 deny   ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 120 permit ip any any
interface Vlan20
 ip address 192.168.20.252 255.255.255.0
 ip access-group 120 out
 standby 20 ip 192.168.20.254
 standby 20 preempt
```

```
access-list 130 permit udp host 192.168.10.250 host 192.168.30.1 eq snmp
access-list 130 permit udp host 192.168.10.250 host 192.168.30.1 eq syslog
access-list 130 permit tcp host 192.168.10.250 host 192.168.30.1 eq 601
access-list 130 permit udp host 192.168.10.250 host 192.168.30.3 eq 1812
access-list 130 permit tcp host 192.168.10.250 host 192.168.30.5 eq 22
access-list 130 permit icmp 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 130 deny   ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 130 permit udp host 192.168.20.100 host 192.168.30.250 eq tftp
access-list 130 permit tcp host 192.168.20.100 host 192.168.30.250 eq 72
access-list 130 permit udp 192.168.20.0 0.0.0.255 host 192.168.30.1 eq snmp
access-list 130 permit udp 192.168.20.0 0.0.0.255 host 192.168.30.1 eq syslog
access-list 130 permit tcp 192.168.20.0 0.0.0.255 host 192.168.30.1 eq 601
access-list 130 permit udp host 192.168.20.250 host 192.168.30.3 eq 1812
access-list 130 permit tcp 192.168.20.0 0.0.0.255 host 192.168.30.5 eq 22
access-list 130 permit icmp 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 130 deny   ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 130 permit ip any any
interface Vlan30
 ip address 192.168.30.252 255.255.255.0
 ip access-group 130 out
 standby 30 ip 192.168.30.254
 standby 30 priority 150
 standby 30 preempt
 standby 30 track FastEthernet0/5 51
```

3-4. SW2(L3_sw) 구축 및 설정

▶ IP 설정

- 각각의 Vlan에 IP를 설정
- 다른 스위치와 연결된 포트를 trunk mode 설정

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan10
 ip address 192.168.10.253 255.255.255.0
 standby 10 ip 192.168.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 192.168.20.253 255.255.255.0
 standby 20 ip 192.168.20.254
 standby 20 priority 150
 standby 20 preempt
 standby 20 track GigabitEthernet2/0/5 51
!
interface Vlan30
 ip address 192.168.30.253 255.255.255.0
 standby 30 ip 192.168.30.254
 standby 30 preempt
```

```
interface GigabitEthernet2/0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface GigabitEthernet2/0/5
 no switchport
 no ip address
 shutdown
!
interface GigabitEthernet2/0/6
 no switchport
 ip address 172.16.10.6 255.255.255.252
```

▶ 라우팅 설정

- OSPF 프로토콜을 사용하였고, area는 0으로 설정
- L3 Switch이기 때문에 'ip routing' 사용

```
router ospf 100
 router-id 1.1.1.2
 log-adjacency-changes
 passive-interface Vlan10
 passive-interface Vlan20
 passive-interface Vlan30
 network 172.16.10.4 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
```

▶ NMS 및 SSO 설정

- SSO(radius) 설정
- NMS(librenms) 설정

```
ip http server
ip http secure-server
snmp-server host 192.168.30.1 version 2c cloud_sw2
radius-server host 192.168.30.3 auth-port 1812 acct-port 1646 key 1234
```

```
aaa new-model
!
!
aaa authentication login default group radius local
aaa authentication login LPIC group radius local
!
!
!
aaa session-id common
```

▶ 게이트웨이 이중화

- 이중화 프로토콜 HSRP를 사용
- SW2에는 Vlan 20을 Active 설정
- SW1과 SW2의 라우팅을 끊어주기 위해 passive-interface를 설정

```
interface Vlan10
 ip address 192.168.10.253 255.255.255.0
 standby 10 ip 192.168.10.254
 standby 10 preempt
!
interface Vlan20
 ip address 192.168.20.253 255.255.255.0
 standby 20 ip 192.168.20.254
 standby 20 priority 150
 standby 20 preempt
 standby 20 track GigabitEthernet2/0/5 51
!
interface Vlan30
 ip address 192.168.30.253 255.255.255.0
 standby 30 ip 192.168.30.254
 standby 30 preempt
 passive-interface Vlan10
 passive-interface Vlan20
 passive-interface Vlan30
```

▶ ACL 설정

- Vlan 20의 Access-list는 120으로 설정
- Vlan 30의 Access-list는 130으로 설정
- SW1과 동일하게 설정

3-5. SW3(L2_sw) 구축 및 설정

▶ IP 설정

- telnet과 ssh 접속을 위한 Vlan 10 IP설정
- Default-gateway 설정
- 다른 스위치와 연결된 포트를 trunk mode 설정
- User와 연결된 포트에 access mode를 사용하여 Vlan 10을 연결

```
interface Vlan10
 ip address 192.168.10.250 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.10.254
```

```
interface FastEthernet0/1
 switchport access vlan 10
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
```

▶ NMS 및 SSO 설정

- SSO(radius) 설정
- NMS(librenms) 설정

```
logging trap debugging
logging 192.168.30.1
snmp-server host 192.168.30.1 version 2c cloud_sw3
radius-server host 192.168.30.3 auth-port 1812 acct-port 1813 key 1234
aaa new-model
aaa authentication login default group radius local
```

3-6. SW4(L2_sw) 구축 및 설정

▶ IP 설정

- telnet과 ssh 접속을 위한 Vlan 30 IP설정
- Default-gateway 설정
- 다른 스위치와 연결된 포트를 trunk mode 설정
- User와 연결된 포트에 access mode를 사용하여 Vlan 30을 연결

```
interface Vlan30
 ip address 192.168.30.250 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.30.254
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport mode trunk
!
interface FastEthernet0/3
 switchport mode trunk
```

▶ NMS 및 SSO 설정

- SSO(radius) 설정
- NMS(librenms) 설정

```
logging trap debugging
logging 192.168.30.1
snmp-server host 192.168.30.1 version 2c cloud_sw4
radius-server host 192.168.30.3 auth-port 1812 acct-port 1813 key 1234
```

```
aaa new-model
aaa authentication login default group radius local
```

3-7. SW5(L2_sw) 구축 및 설정

▶ IP 설정

- telnet과 ssh 접속을 위한 Vlan 20 IP설정
- Default-gateway 설정
- 다른 스위치와 연결된 포트를 trunk mode 설정
- User와 연결된 포트에 access mode를 사용하여 Vlan 20을 연결

```
interface Vlan20
 ip address 192.168.20.250 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.20.254
interface GigabitEthernet0/1
 switchport access vlan 20
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface GigabitEthernet0/3
 switchport mode trunk
```

▶ NMS 및 SSO 설정

- SSO(radius) 설정
- NMS(librenms) 설정

```
logging trap debugging
logging 192.168.30.1
snmp-server host 192.168.30.1 version 2c cloud_sw5
radius-server host 192.168.30.3 auth-port 1812 acct-port 1646 key 1234
aaa new-model
aaa authentication login default group radius local
```

4. 테스트
실제 패킷이 열리는지 확인

5. 결론
프로젝트하면서 느낀점