# 패킷트레이서 과제

제작자 : 김민호

## 가. 과제 개요

아래 지시에 따라 Cisco Packet Tracer로 네트워크 시뮬레이션을 구성합니다.

## 나. 소프트웨어 및 운영 체제 준비

- Cisco Packet Tracer 7.2.1 이상
- Window 10 64bit 이상

## 다. 주의사항

- 패킷트레이서의 오류로 인한 프로그램 종료에 대비하기 위해 수시로 저장합니다.
- 라우터의 Host Name을 Display Name으로 구성합니다.
- 대소문자를 구분하여 구성합니다.
- IP 주소가 명시되지 않은 ES는 DHCP로 구성합니다.
- 토폴로지나 문제에서 주어지지 않은 사항에 대해서는 최소한의 설정으로 유효한 값을 선수가 임의로 사용합니다.
- 별도의 지시가 없는 경우 종단 장치의 기본 게이트웨이는 해당 서브넷의 가용 가능한 마지막 주소를 사용합니다. (IPv6의 경우 첫번째 주소를 사용합니다.)
- 문제지에 명시되어 있지 않은 서비스는 토폴로지를 참고하여 구성합니다.

# 라. 과제 내용

## 1. Routing

- DR4-SR1 에 Floating Routing을 구성하여 가용중인 회선 Fa1/0에 문제가 발생할 시 백업 회선 Fa1/1를 통해 통신할 수 있어야 합니다. (AD값은 2와 3을 사용합니다.)
- Static Routing 구간에 DR4와 SR6을 메인 라우팅 테이블 라우터로 구성합니다.
- Default Routing이 필요한 경우 알맞은 곳에 최소한으로 구성합니다.
- RIPv2 사용 시 자동 축약을 사용하지 않습니다.
- OSPF Backbone 영역은 Meraki Server0, PC36 에게 라우팅 테이블을 광고하지 않습니다.
- R10에 IPv5 네트워크를 위한 Unequal cost Load balancing을 구성합니다.
- 사설 네트워크는 광고하지 않습니다.
- 토폴로지의 명시된 라우팅 프로토콜을 사용하여 적절하게 Full Routing을 구성합니다.

## 2. DHCP

- DHCP pool Name은 기본적으로 "DHCP"를 사용하며 VLAN일 경우 해당 VLAN 이름을 사용합니다.
- D-SW3에 PC2와 PC3을 위한 고정 DHCP를 주소를 받아올 수 있도록 구성합니다.
- AP는 Server5 로부터 150-200 사이의 주소를 받을 수 있도록 구성합니다.
- PC35는 ASA5506으로부터 해당 서브넷의 150-180 사이의 IP를 받아오도록 구성합니다.
- VLAN48과 VLAN58 구역은 DHCP 서버로 Server2를 사용합니다.
- 지정되지 않은 DHCP 서버는 자신의 게이트웨이 라우터를 DHCP서버로 지정합니다.

## 3. HSRP

| | Interface | Priority | Virtual IPv4 | Group Number |
|---|---|---|---|---|
| DR4 | Fa0/1 | 150 | .200 | 15 |
| DR5 | Gig0/1 | 100 | | |

- IPv6장비는 DR4를 Gateway로 구성합니다.

| | Interface | Priority | Virtual IPv4 | Group Number |
|---|---|---|---|---|
| ER3 | Fa0/1 | 88 | .200 | 3 |
| ER4 | Fa0/0 | 66 | | |
| ER5 | Fa0/0 | 44 | | |

## 4. VoIP

- 1001 1002 는 INTERNAL을, 2001 2002 2003 는 SR5를, 30001 30002는 ER9를 VOIP 서버로 구성합니다.
- Dial-Peer 설정 시 VoIP 첫번째 주소가 1일 경우 INTERNAL로, 2일 경우 SR5로, 3일 경우 ER9로 전화가 걸리도록 구성합니다.
- PC11은 EasyVPN 연결 시 번호 "1002"를 할당 받을 수 있도록 구성합니다.

## 5. Switch balance

- PC17과 PC23이 통신할 때 SW5를 지나서 통신하게 구성합니다.
- VLAN에 알맞게 스위치를 구성하고 VTP Pruning을 수동으로 구성합니다.

## 6. EtherChannel

- SW1-SW4간에 시스코 전용 프로토콜을 이용하여 SW1를 협상 모드로 구성합니다.
- SW1-SW4에 이더채널 구성 시 Source, Destination MAC Address를 XOR 연산한 결과로 포트가 선출될 수 있도록 구성합니다.
- con1-con3간에 IEEE 802.3ad 프로토콜을 이용하여 con1을 협상 모드로 구성합니다.
- con1-con4간에 프로토콜 없이 이더채널을 구성합니다.

## 7. Frame-Relay

- Cloud0에 LMI VC Identifiers 값 1023을 사용하여 Broadcast를 전달합니다.
- Cloud1에 캡슐화 방식을 IETF를 사용합니다.

## 8. NAT

- 사설 대역에 적절하게 NAT, PAT를 구성합니다.
- EX 스위치에 L2NAT를 구성하여 PC15와 PC16이 서로 통신할 수 있도록 합니다.
- ER12와 6pc간에 통신을 위한 터널을 구성합니다. 이때, Client는 MAC주소를 기반으로 한 IPv6 자동 할당 기법을 사용하여 Server6의 웹사이트에 접속하도록 구성합니다.
  (ER12 Tunnel IP : 2019:826::1)
- NR1에 NAT를 구성하되, ES의 IP가 3번째 Octet이 홀수이고, 4번째 Octet이 짝수일 경우에만 외부와 통신할 수 있도록 구성합니다.
- BR5에 IPv4와 IPv6의 통신을 위한 NAT를 구성합니다. 구성 뒤 IPv4 네트워크에서 119.37.5.4로 접속 시 2097::/96으로 변환되어 Server9에 웹 접속되어야 합니다.

## 9. ASA

- 다음 표를 참고하여 ASA0을 구성합니다. 이때, "no forward" 명령어는 사용하지 않습니다.

| | Et0/0 | Et0/1 | Et0/2 – VLAN20 | Et0/2 – VLAN30 |
|---|---|---|---|---|
| nameif | OUTSIDE | DMZ | INSIDE20 | INSIDE30 |
| Security-Level | 0 | 70 | 100 | 100 |

- ASA0은 Object Name 을 "NAT + (VLAN Number)"로 구성합니다.
- VLAN20은 동적NAT를 INSIDE30은 Static NAT로 구성합니다.
- ASA1은 적절하게 NAT를 구성합니다.

## 10. Gre Over IPsec VPN

- SR3-SR7간의 다음 값을 이용하여 서로 보안된 통신을 하도록 구성합니다.

► Isakmp Policy : 10
► Encryption : aes-256
► Hash : md5
► Transform-set : TS
► PSK : privatekey
► crypto map : gvpn

## 11. Dot1x Authentication

- con3의 Fa0/4에 연결된 PC12는 Dot1x Authentication을 인증을 거치도록 구성합니다.
- AAA서버로 Server4를 지정하고 유저 ID로 "user" Password로 "cisco" 를 사용합니다.

## 12. DNS

- 모든 IPv4 Client들은 DNS 서버로 Server0을 지정합니다.
- Server0은 DNS Cache Server로, Server7을 root서버로, Server9을 2차 서버로 지정합니다.
- cisco.com 도메인 질의 시 Server0 -> Server7 -> Server9으로 순차적 질의를 합니다.
- Server0에는 "com"에 대하여 Server7은 "cisco.com"에 대하여 NS 레코드를 구성합니다.
- Server9에 다음 표를 참고하여 A레코드를 추가합니다.

| FQDN | IP |
|---|---|
| www.cisco.com | 149.21.6.1 |
| iot.cisco.com | 211.16.48.100 |
| service.cisco.com | 175.91.20.100 |

## 13. PPPoE

- 다음 값으로 username : ipv6 , password : skills 유저 local 인증을 구성합니다.
- R3의 DHCPv6 서버로부터 2019:ABCD::1/64 대역의 주소를 할당 받도록 구성합니다.

## 14. Easy VPN

- ER7에 아래 값을 참고하여 PC11을 위한 Easy VPN Server를 구성합니다.

► Isakmp Policy : 5 ► Encryption : 3des

► Hash : sha ► Transform-set : EZ

► Pool name : IP [192.168.2.100-192.168.2.200] ► AAA : ALIST [Radius : 175.91.20.100]

► crypto map : VPN ► Dynamic map : DM

► GroupName, Key 는 "ezskills"로 Username, Password는 "sysop"를 사용합니다.

## 15. Wireless

- AP는 암호화 없이 SSID값을 "AP" 를 사용합니다.
- WR0는 SSID값을 "WR0"으로 지정하고, WPA2 Personal으로 인증하고 Passphrase 값으로 "worldskills123"을 사용합니다.
- WR0의 무선장비들은 ftp service를 사용 못하게 막고, 펌웨어를 업데이트 합니다.

## 16. FTP, SYSLOG, NTP, EMAIL

- PC0과 PC1은 service.cisco.com으로 username : skills, password : cisco123을 사용해 접속할 수 있도록 구성합니다. 이때 skills는 RW의 권한만 가지도록 구성합니다.
- ER2의 SYSLOG를 Server4에 저장할 수 있도록 구성합니다.
- SR5는 NTP Server로 Server5를 지정합니다. 그 외 Static 라우터들은 SR5를 NTP MASTER SERVER로 지정합니다. (password : cisco123)
- PC1, PC24, PC26에 올바르게 E-Mail을 구성하고, E-Mail 서버로 Server0을 사용합니다. Incoming, Outgoing Server로 service.cisco.com을 사용합니다.

## 17. QOS

- SR7에 웹 트래픽 우선순위 조정을 위한 QOS를 구성합니다.
- www.cisco.com는 immediate로 마킹 하고 service.cisco.com는 network로 마킹 합니다.
- class-map으로 "www"와 "service"를 사용하고 policy-map으로는 "PM"을 사용합니다.

## 18. Remote Telnet Login Service

- PC2가 DR1의 Telnet서비스를 사용할 수 있도록 구성합니다.
- 접근 사용자로 username : telnet , password : accessp2 를 사용합니다.
- telnet 접근 후 10초 이내 사용자 인증에 2번 실패할 경우 30초간 telnet 접근을 차단합니다.
- telnet 사용 시 banner로 "Hello welcome to DR1"이 뜨도록 구성합니다.

### 19. Firewall

- PC10을 제외한 나머지 Client들은 Server1로의 웹 서비스 접근을 차단합니다.
- IPS를 사용하여 Router2의 PC36이 핑을 보낼 순 있지만 받을 순 없게 구성합니다.
- SR5에 ZBF를 구성합니다. (Se0/0/1 – OUTSIDE , Se0/0/0 – INSIDE)

  INSIDE -> OUTSIDE 모든 서비스 허용

  OUTIDE -> INSIDE 토폴로지를 구성하며 필요한 서비스만 허용

  Policy-map, Class-map, ACL은 "출발지-목적지" 형식으로 구성합니다. Ex) INSIDE-OUTSIDE
- ZBF 구성 시 필요한 서비스를 제외한 나머지 트래픽은 기본적으로 차단합니다.

## 마. Secret-ZONE configuration

### 1. Cell Tower

- CO-Server에 PAP Authentication을 구성합니다. (Username : cisco , password : cisco123)
- SP1-SP2는 Cell Tower0에 접속하고 Router27은 Cell Tower1에 접속하게 구성합니다.
- Router27에 I-WR0, Laptop3를 위한 wireless service를 구성합니다. 이때, SSID는 "819HGW"를 사용하고 WPA Passphrase는 "connect"를 사용합니다.

### 2. IOT Device

- IoT1, IoT2는 wireless 로 I-WR0에 접속합니다.
- IoT 서버로 Server2를 지정하고, SP1에서 iot.cisco.com으로 접속하여 구성합니다.
- IoT1의 문이 열렸을 경우 Light의 불이 켜지도록 관련 장치들을 구성합니다.

### 3. Bluetooth

- Laptop3에 Bluetooth기능을 활성화 시킨 뒤 Smartphone2-3이 접속할 수 있도록 구성합니다.
- Smartphone2-3은 Laptop3와 Bluetooth tethering으로 연결되도록 구성합니다.

## 4. WLC

- 관리 사이트의 접속할 시 username : admin , password : Cisco123을 사용합니다.
- System Name은 "WLC"로 Profile Name 은 "wireless"를 사용합니다.
- PC13, PC14는 WEP(40bits) 방식으로 "1234567890" key값으로 접속합니다.

## 5. 2811 Wireless

- Smartphone4를 위한 무선 랜을 구성합니다.
- SSID : onlySP , WPA PassPhrase : world19 를 사용합니다.
- Smartphone4의 config 탭은 사용하지 않습니다.

## 6. Meraki Server

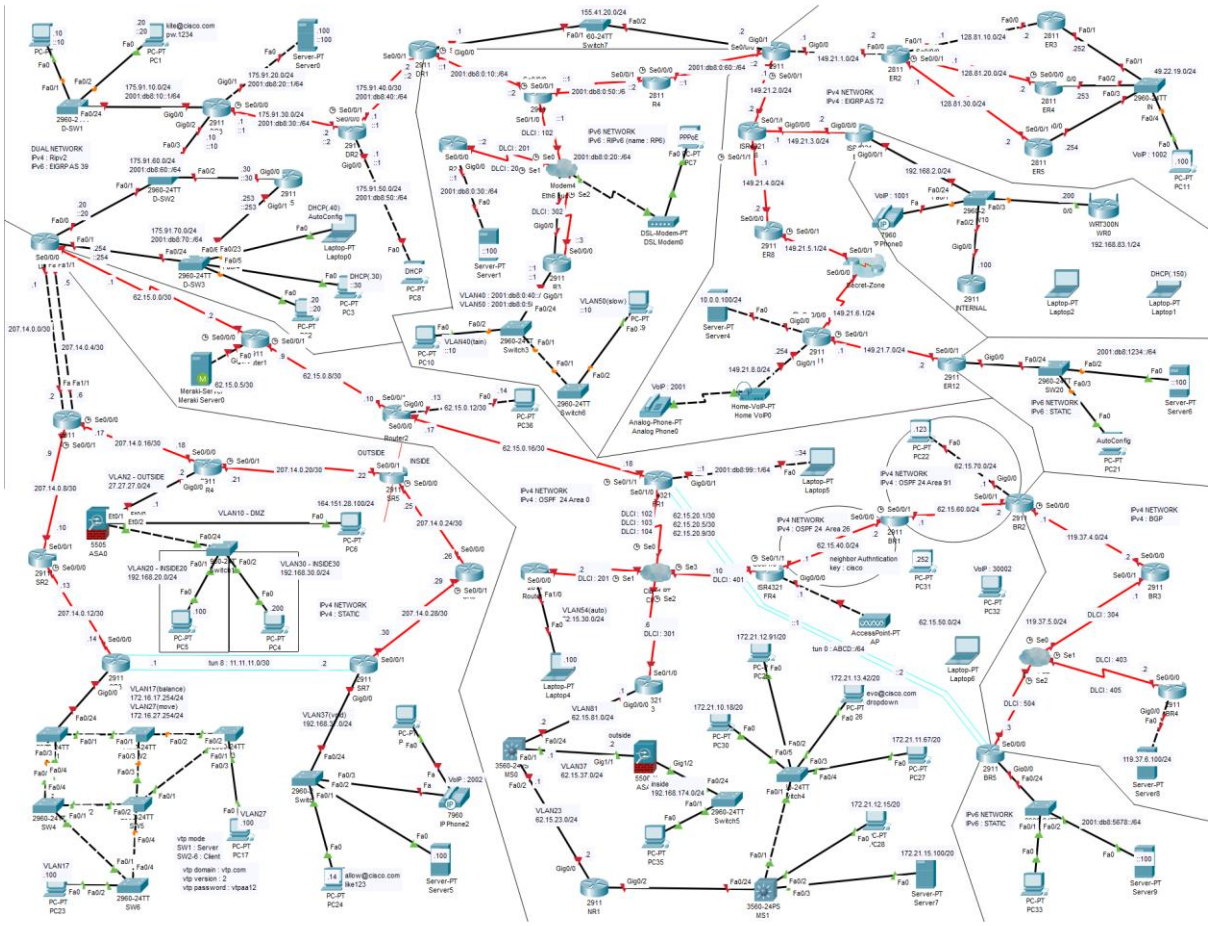
- Tablet과 Printer를 위한 무선 랜을 Security appliance0에 구성합니다.
- SSID : Meraki , WPA2 PassPhrase : public 을 사용하여 구성합니다.

## 7. HomeRouter

- Server3와 PC19, PC20을 Home-WR0에 연결 합니다.
- Server3는 SSID로 "inter"을 사용 하고, WPA2 Enterprise로 Server2에게 인증 받아 Username : service , password : default 를 사용하고 Home-WR0으로부터 DHCP를 받아올 수 있도록 구성합니다.
- PC19는 SSID로 "vlan14"을 사용 하고, WPA2 Personal로 PassPhrase 값으로 "worldskills"를 사용하여 인증합니다. DHCP 서버와 게이트웨이로 ER10을 지정합니다.
- PC20는 SSID로 "PC20"을 사용 하고, 암호화 없이 ER10으로부터 DHCP를 받아오도록 구성합니다.

# 바. Topology

## 1. ALL-NETWORK



## 2. Secret-ZONE