

# 2026년 지방기능경기대회 과제

|       |           |       |                   |             |      |
|-------|-----------|-------|-------------------|-------------|------|
| 직 종 명 | IT네트워크시스템 | 과 제 명 | Secret Challenges | 과제번호        | 제3과제 |
| 경기시간  | 4시간       | 비 번 호 |                   | 심사위원<br>확 인 | (인)  |

## 1. 과제 소개

가. 과제 개요

나. 소프트웨어 요구사항

- 1) Cisco PacketTracer 8.2.2

다. 지급 재료

- 1) [제3과제].pka

라. 주의 사항

- 1) 패킷트레이서의 오류로 인한 프로그램 종료에 대비하기 위하여 파일을 수시로 저장하여야 합니다.
- 2) 토폴로지나 문제에서 주어지지 않은 사항에 대해서는 유효한 값을 선수가 사용할 수 있습니다.
- 3) 시스템 구축 진행 시 암호가 필요할 경우 "Skill39\*\*"을 기본값으로 사용합니다.
- 4) 과제 수행 시 대문자와 소문자를 구분하여 설정합니다.
- 5) 경기 중 어떠한 파일도 참고할 수 없으므로 주의합니다.
- 6) 정해진 USB장치 이외의 저장장치의 반입을 금지합니다.
- 7) 경기 시작 전 휴대폰 등과 같은 스마트기기는 심사위원(또는 관리 위원)에게 보관하도록 합니다.
- 8) 경기 종료 후 임의로 설정을 변경하거나 서비스를 재시작할 수 없으며 재점 시 모든 서비스가 정상적으로 동작되어야 합니다.

## 2. 과제 요구사항

### A. 기본 구성

#### 가. 공통 구성

- 1) 모든 라우터와 스위치의 이름은 토폴로지의 이름을 참고하여 변경합니다.
- 2) 네트워크 토폴로지를 참고하여 각 디바이스에 IP 주소를 할당합니다.

#### 나. 네트워크 설계

- 1) R3의 내부 네트워크는 10.255.255.0/24 주소 대역을 네트워크당 가용한 주소 60개가 할당될 수 있도록 서브네팅하며 첫 번째 네트워크의 가용한 마지막 주소를 GigabitEthernet 0/2 인터페이스에 할당합니다.
- 2) L3SW의 내부 네트워크는 172.16.0.0/24 주소 대역을 네트워크당 가용한 주소 30개 할당될 수 있도록 서브네팅 합니다.
  - a) 첫 번째 네트워크의 가용한 마지막 주소를 L3SW 디바이스의 VLAN990 인터페이스에 할당합니다.
  - b) 첫 번째 네트워크의 가용한 첫 번째 주소를 RT2 디바이스의 GigabitEthernet 0/0 인터페이스에 할당합니다.
  - c) 두 번째 네트워크의 가용한 마지막 주소를 L3SW 디바이스의 VLAN10 인터페이스에 할당합니다.
  - d) 세 번째 네트워크의 가용한 마지막 주소를 L3SW 디바이스의 VLAN20 인터페이스에 할당합니다.
  - e) 네 번째 네트워크의 가용한 마지막 주소를 L3SW 디바이스의 VLAN30 인터페이스에 할당합니다.

## B. L2 네트워킹

### 가. VLAN 및 Trunk

- 1) 아래 표를 참고하여 스위치 디바이스에 VLAN을 추가합니다.

| VLAN ID | VLAN 이름     | 디바이스                    |
|---------|-------------|-------------------------|
| 10      | CLIENT1     | L3SW SW1 SW2 SW3        |
| 20      | CLIENT2     | L3SW SW1 SW2 SW3        |
| 30      | SERVER      | L3SW SW1 SW2 SW3        |
| 990     | CALLMANAGER | L3SW                    |
| 991     | ISP1        | L3SW                    |
| 992     | ISP2        | L3SW                    |
| 101     | ACCESS1     | DS1 DS2 AS1 AS2 AS3 AS4 |
| 102     | ACCESS2     | DS1 DS2 AS1 AS2 AS3 AS4 |
| 103     | ACCESS3     | DS1 DS2 AS1 AS2 AS3 AS4 |
| 104     | ACCESS4     | DS1 DS2 AS1 AS2 AS3 AS4 |
| 999     | CORE        | DS1 DS2 AS1 AS2 AS3 AS4 |

- 2) DS1, DS2 및 AS1~AS4 스위치에 VTP를 구성합니다. DS1 및 DS2 스위치를 VTP 서버로 구성하며 AS1~AS4 스위치를 VTP 클라이언트로 구성합니다.
- 3) VTP 도메인을 SKILL39로 설정하며 VTP 암호를 설정하도록 합니다.
- 4) DS1 및 DS2와 AS1~AS4 스위치 간 연결된 인터페이스를 Trunk 포트 구성합니다.
- 5) DS1, DS2 및 AS1~AS4 스위치의 Trunk 포트에 VLAN101~104 트래픽만 전송되도록 합니다.
- 6) L3SW와 SW1~SW3 스위치 간 연결된 인터페이스를 Trunk 포트 구성합니다.
- 7) L3SW 스위치의 Trunk 포트에 VLAN10/20/30만 트래픽이 전송되도록 합니다.
- 8) 과제 요구사항 및 네트워크 토폴로지를 참고하여 각 스위치 디바이스 인터페이스에 VLAN이 할당되도록 합니다.

### 나. Spanning Tree Protocol

- 1) DS1 디바이스를 VLAN101 및 VLAN102 VLAN에 대한 Root Bridge로 구성합니다. DS1 디바이스에 장애가 발생할 경우 DS2 디바이스가 Root Bridge가 되어야 합니다.
- 2) DS2 디바이스를 VLAN103 및 VLAN104 VLAN에 대한 Root Bridge로 구성합니다. DS2 디바이스에 장애가 발생할 경우 DS1 디바이스가 Root Bridge가 되어야 합니다.
- 3) L3SW 디바이스를 모든 VLAN에 대한 Root Bridge로 구성합니다.
- 4) 빠른 STP 수렴을 위해 STP 프로토콜을 Rapid PVST+로 구성합니다.

## C. L3 네트워킹

### 가. 네트워크 인터페이스 구성

#### 1) 라우터

- a) ISP-Core 라우터에 Loopback 0 인터페이스를 생성하며 8.8.8.8/32 주소를 할당합니다.
- b) RT1 라우터에 Loopback 0 인터페이스를 생성하며 192.168.0.1/32 주소를 할당합니다.
- c) Core1 및 Core2 라우터에 Loopback 0 인터페이스를 생성하며 1.1.1.1/32 주소를 할당합니다.
- d) Core1 라우터에 Loopback 1 인터페이스를 생성하며 1.1.1.5/30 주소를 할당합니다.
- e) Core2 라우터에 Loopback 1 인터페이스를 생성하며 1.1.1.9/30 주소를 할당합니다.
- f) RT1 라우터에 Loopback 1 인터페이스를 생성하며 11.11.11.11/32 주소를 할당합니다.
- g) RT2 라우터에 Loopback 0 인터페이스를 생성하며 22.22.22.22/32 주소를 할당합니다.

#### 2) L3 스위치

- a) DS1 및 DS2 스위치에 포함되는 VLAN의 SVI 인터페이스를 생성합니다.
- b) L3SW 스위치에 포함되는 VLAN의 SVI 인터페이스를 생성합니다.

#### 3) 고가용성

- a) DS1 및 DS2 스위치에 VLAN101~VLAN104에 대한 HSRP를 구성하며 VLAN ID를 HSRP 그룹 번호로 구성합니다.
- b) HSRP 가상 인터페이스에 네트워크 내 가용한 주소 중 마지막 주소를 할당합니다.
- c) VLAN101 및 VLAN102 네트워크에 대해 DS1 디바이스가 우선적인 활성 디바이스이며 해당 디바이스에 장애가 발생할 경우 DS2 디바이스로 대체되어야 합니다.
- d) VLAN103 및 VLAN104 네트워크에 대해 DS2 디바이스가 우선적인 활성 디바이스이며 해당 디바이스에 장애가 발생할 경우 DS1 디바이스로 대체되어야 합니다.

## 나. Routing

#### 1) OSPF

- a) GW, R1, R2 및 R3 디바이스에 OSPF 프로토콜을 활용하여 플라우팅 구성하며 Process ID로 1을 사용합니다.
- b) GW 라우터와 연결되는 인터페이스를 백본 에어리어로 구성합니다.
- c) R3 라우터와 연결되는 인터페이스를 Area 1으로 구성하며 Area 1은 Stub

Area로 구성합니다.

d) GW 라우터는 디폴트 경로를 내부에 전달하도록 합니다.

## 2) EIGRP

a) Core1, Core2, RT1, DS1 및 DS2 디바이스에 EIGRP 프로토콜을 활용하여 폴라우팅 구성하며 AS 65000을 할당합니다.

b) Access 네트워크를 통해 EIGRP 네이버를 수립하지 않도록 구성합니다.

c) HSRP 활성 디바이스가 우선되도록 EIGRP 경로를 조정합니다.

d) BGP 경로를 EIGRP 내부 네트워크에 재분배합니다. 이때 모든 경로를 디폴트 경로로 축약하여 전송합니다.

## 3) Static

a) ISP-Core 라우터에 0.0.0.0/0 네트워크의 Null0 라우팅을 구성합니다.

b) ISP3 라우터에 2.2.2.2/32 네트워크의 정적 라우팅을 구성하며 next-hop으로 GW 디바이스를 지정합니다.

c) GW 라우터에 디폴트 경로의 정적 라우팅을 구성하며 next-hop으로 ISP3 라우터를 지정합니다.

d) ISP4 라우터에 7.7.7.0/29 네트워크의 Floating 라우팅을 구성하며 next-hop으로 L3SW 디바이스를 지정합니다. 이때 GigabitEthernet 0/0 인터페이스를 우선합니다.

e) L3SW 스위치에 디폴트 경로의 Floating 라우팅을 구성하며 next-hop으로 ISP4 라우터를 지정합니다. 이때 VLAN991 인터페이스를 우선합니다.

f) RT1과 RT2는 Loopback주소를 사용하여 정적 라우팅을 구성합니다.

## 4) eBGP

a) 아래 표를 참조하여 각 라우터에 eBGP를 구성합니다.

| 디바이스     | AS    |
|----------|-------|
| ISP-Core | 10000 |
| ISP1     | 1     |
| ISP2     | 2     |
| ISP3     | 3     |
| ISP4     | 4     |
| Core1    | 65001 |
| Core2    | 65002 |

b) 각 라우터는 직접 연결된 디바이스와 BGP 네이버를 수립하도록 합니다.

c) BGP 라우터는 Loopback 인터페이스 및 정적 라우팅 경로를 네이버에게 광고합니다.

## D. 네트워크 서비스

### 가. Network Address Translation

#### 1) Port Address Translation

- a) Core1의 내부 네트워크 디바이스가 1.1.1.4~7 주소로 변환되어 외부 네트워크와 통신할 수 있도록 구성합니다.
- b) Core2의 내부 네트워크 디바이스가 1.1.1.8~11 주소로 변환되어 외부 네트워크와 통신할 수 있도록 구성합니다.
- c) L3SW 디바이스의 내부 네트워크 디바이스가 7.7.7.2~6 주소로 변환되어 외부 네트워크와 통신할 수 있도록 구성합니다.

#### 2) Static NAT

- a) Server0 디바이스가 2.2.2.2 주소로 변환되어 외부 네트워크와 통신할 수 있도록 구성합니다.
- b) Server1 디바이스가 7.7.7.7 주소로 변환되어 외부 네트워크와 통신할 수 있도록 구성합니다.

### 나. DHCP 서비스

#### 1) 아래 표를 참고하여 각 디바이스에 DHCP 서비스를 구성합니다.

| 디바이스 | 대상 네트워크 | 주소 범위            | 기본 게이트웨이        |
|------|---------|------------------|-----------------|
| RT1  | VLAN101 | 192.168.101.0/24 | VLAN101 HSRP    |
|      | VLAN102 | 192.168.102.0/24 | VLAN102 HSRP    |
|      | VLAN103 | 192.168.103.0/24 | VLAN103 HSRP    |
|      | VLAN104 | 192.168.104.0/24 | VLAN104 HSRP    |
| L3SW | VLAN10  | 서브네팡 네트워크        | L3SW VLAN10 SVI |
|      | VLAN20  | 서브네팡 네트워크        | L3SW VLAN20 SVI |

- 2) DHCP 서버는 음성 클라이언트가 Call Manager에 연결할 수 있도록 DHCP option을 부여합니다.
- 3) DS1 및 DS2 스위치에 DHCP relay를 구성하여 RT1 디바이스에 DHCP 패킷을 전달하도록 구성합니다.
- 4) L3SW에서 172.16.0.100으로 DNS서버주소를 할당하도록 구성합니다.
- 5) RT에서 2.2.2.2로 DNS서버주소를 할당하도록 구성합니다.

### 다. VoIP 서비스

#### 1) 아래 표를 참고하여 각 디바이스에 VoIP 서비스를 구성합니다.

| Call Manager | 디바이스 | 번호   |
|--------------|------|------|
| RT1          | PC0  | 1001 |
|              | PC1  | 1002 |
|              | PC2  | 1003 |
|              | PC3  | 1004 |
| RT2          | PC4  | 2001 |
|              | PC5  | 2002 |

- 2) RT1 디바이스는 Loopback 주소를 활용해 VoIP 서비스를 구성합니다.
- 3) 모든 IP Phone이 서로 전화가 가능하도록 Dial-Peer를 구성합니다.

#### 라. Netflow

- 1) ISP4에 gig0/0/0으로 들어오는 IPv4에 대한 모든 트래픽을 모니터링합니다.
- 2) 모니터링한 트래픽을 Server0에서 수집 및 분석하도록 구성합니다.

#### 마. 사용자 추가 및 banner

- 1) 아래의 표를 참고해 ISP-Core에 로컬 사용자를 추가합니다.

| UserName      | Password  | Privilege |
|---------------|-----------|-----------|
| administrator | Skill39** | 15        |

- 2) 로그인을 시도하면 “Warning! Access to authorized users only”를 출력합니다.
- 3) 사용자의 비밀번호는 암호화합니다.

#### 바. SSH

- 1) L3SW에서 SSH 구성하고 사용자인증을 Radius를 통해 인증합니다.
- 2) 로그인 시도횟수를 5회로 설정합니다.
- 3) 사용자는 아래 표를 참고해 추가합니다.
- 4) Radius Port를 1812로 설정합니다.
- 5) Radius Server는 Server1에 구성합니다.
- 6) 로그인 성공시 L3SW에 로그가 출력되어야합니다.

| UserName | Password  |
|----------|-----------|
| L3SW     | Skill39** |

#### 사. DNS 및 HTTP

- 1) Server1 및 Server0에 적절한 dns 및 http를 구성합니다.
- 2) 아래에 표를 참고하여 구성합니다.

| ServerName | Name           | Type     | Detail       |
|------------|----------------|----------|--------------|
| Server0    | webservice.com | A Record | 7.7.7.7      |
|            | www.itnsa.com  | A Record | 2.2.2.2      |
| Server1    | webservice.com | A Record | 172.16.0.100 |

| ServerName | URL                         | Value                  |
|------------|-----------------------------|------------------------|
| Server0    | www.itnsa.com               | Welcome to this Server |
| Server1    | webservice.com/welcome.html | Welcome to this Site!  |

아. Site-to-Site VPN 구성

1) 아래 표를 참고하여 GW와 ISP4에 Server0와 Server10이 통신하기 위한 Gre Over IPsec VPN을 구성합니다.

|               |                         |
|---------------|-------------------------|
| IKE 정책 순서     | 10                      |
| 암호화 방식        | 3des                    |
| 인증방식          | pre-share               |
| Hash          | sha                     |
| DH-Group      | 5                       |
| Transform set | IPsec-TS                |
| Encryption    | (esp-aes. esp-sha-hmac) |
| Crypto map    | IPsec                   |
| acl Name      | VPN_ACL                 |

- 아래 표를 참고해 tunnel interface를 구성합니다.

|      |             |
|------|-------------|
| GW   | 10.0.0.1/30 |
| ISP4 | 10.0.0.2/30 |



### 3. 부록

## 가. 네트워크 토폴로지

