본사 & 지사 네트워크 이중화 프로젝트

HSRP 기반 고가용성 네트워크 및 라우팅 설계

1. 프로젝트 개요

1-1. 목적

본사 네트워크의 VLAN 분리 및 HSRP 이중화 구현, 지사 네트워크 확장을 통한 안정적인 엔터프라이즈 네트워크 구축

1-2. 구현 범위

* 본사 : Product, Groupware, Storage, Building-A, Building-B
* 지사 : Branch
* 이중화 : L3 스위치 HSRP 적용
* 라우팅 : 본사-지사 간 정적 라우팅 연결

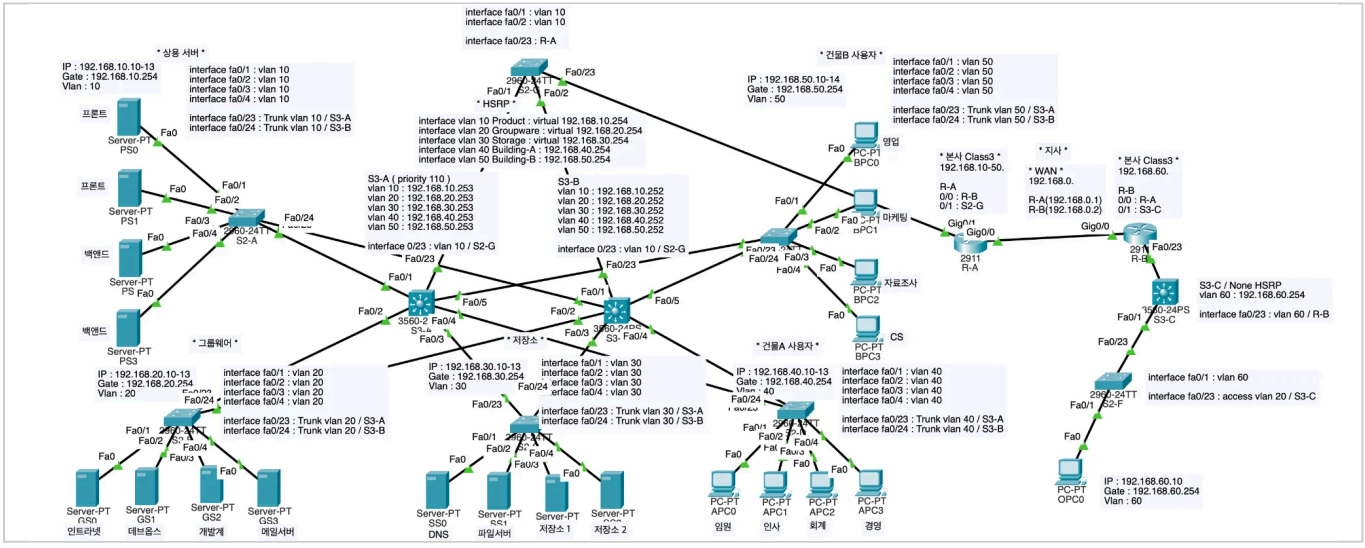
1-3. 핵심 구현 기술

HSRP, VLAN Segmentation, Inter-VLAN Routing, Static Routing, L2/L3 Switch

1-4. 작업 방식

* Step 1 : 본사 VLAN 그룹 정의 및 HSRP 이중화 구성
* Step 2 : 본사-지사 라우팅 확장

2. 최종 네트워크 토폴로지



3. 본사 네트워크 구축

3-1. VLAN 설계

본사 네트워크는 서비스 및 부서별로 5개의 VLAN으로 분리하여 브로드캐스트 도메인을 격리하고 보안성을 확보하였다.

3-2. IP 할당표

구분	VLAN	네트워크	게이트웨이	용도
본사	10	192.168.10.0/24	192.168.10.254	Product
본사	20	192.168.20.0/24	192.168.20.254	Groupware
본사	30	192.168.30.0/24	192.168.30.254	Storage
본사	40	192.168.40.0/24	192.168.40.254	Building-A
본사	50	192.168.50.0/24	192.168.50.254	Building-B
지사	60	192.168.60.0/24	192.168.60.254	Branch
WAN	-	192.168.0.0/24	-	본사-지사 연결

3-3. 장비 구성

* L2 스위치 (2960) : 각 VLAN별 Access 스위치 배치
* L3 스위치 (3560) : 백본 스위치 2대 (S3-A, S3-B)
* 라우터 (2911) : 본사-지사 연결용 (R-A, R-B)

4. HSRP 이중화 구성

4-1. HSRP 설계

L3 스위치 2대(S3-A, S3-B)를 활용하여 Active-Standby 구조의 게이트웨이 이중화를 구현하였다.

장비	역할	Priority	실제 IP	가상 IP
S3-A	Active	110	.253	.254
S3-B	Standby	100	.252	

4. HSRP 이중화 구성

4-2. Failover 테스트 시나리오

Active → 장애발생 → Standby 승격 → 복구 → Active 회수

4-3. 테스트 과정

> **① 정상 상태 확인 (S3-A: Active, S3-B: Standby)**
>
> Product 서버(192.168.10.10)에서 Building-B PC(192.168.50.11)로 ping 테스트 실행

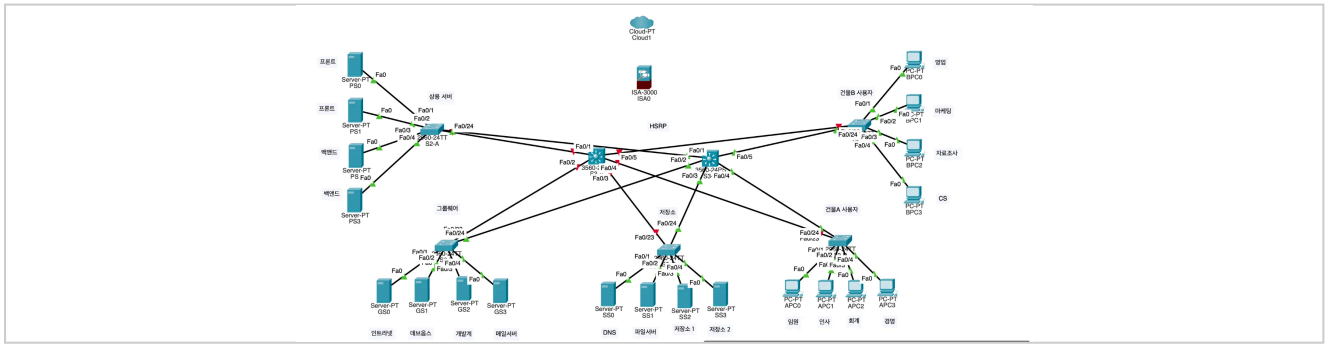
```
C:\>ping -t 192.168.50.11
Reply from 192.168.50.11: bytes=32 time<1ms TTL=127
Reply from 192.168.50.11: bytes=32 time<1ms TTL=127
```

> **② S3-A 장애 발생 (Shutdown)**
>
> Active 장비인 S3-A의 인터페이스를 강제로 shutdown하여 장애 상황 시뮬레이션

```
Switch(config)#interface range fa0/1-5
Switch(config-if-range)#shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
```

> **③ S3-B Standby → Active 전환**
>
> S3-A 장애 감지 후 S3-B가 자동으로 Active 역할 승격

```
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan30 Grp 30 state Standby -> Active
```



[S3-A Shutdown 후 S3-B가 Active로 승격된 상태]

4. HSRP 이중화 구성

④ Ping 일시 중단 후 자동 복구

HSRP 전환 중 약 4~5회 timeout 발생 후 통신 자동 복구

```
Reply from 192.168.50.11: bytes=32 time=14ms TTL=127
Request timed out.
Request timed out.
Reply from 192.168.50.11: bytes=32 time=4ms TTL=127  ← 복구

Ping statistics: Packets: Sent = 109, Received = 104, Lost = 5 (5% loss)
```

⑤ S3-A 복구 (No Shutdown)

관리자가 수동으로 인터페이스를 복구(no shutdown)한 후, Preempt 설정에 의해 Active 역할이 자동 회수됨

```
Switch(config-if-range)#no shutdown
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Standby -> Active
%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Standby -> Active
```

⑥ S3-B Active → Standby 복귀

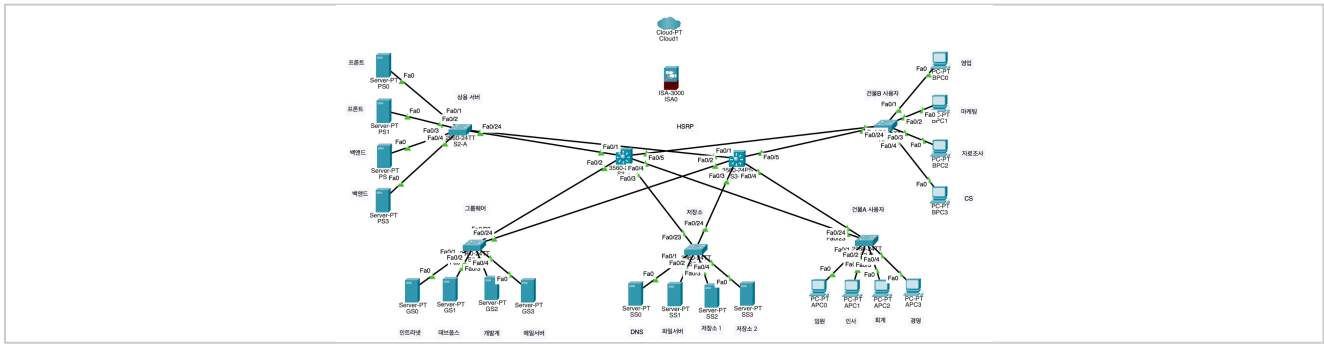
S3-A가 Active 회수 후 S3-B는 다시 Standby 상태로 복귀

```
%HSRP-6-STATECHANGE: Vlan10 Grp 10 state Speak -> Standby
%HSRP-6-STATECHANGE: Vlan20 Grp 20 state Speak -> Standby
```

⑦ 최종 상태 확인

S3-A: Active, S3-B: Standby 상태로 원복되어 정상 통신 확인

```
C:\>ping -t 192.168.50.11
Reply from 192.168.50.11: bytes=32 time<1ms TTL=127
Ping statistics: Packets: Sent = 5, Received = 5, Lost = 0 (0% loss)
```



[S3-A 복구 후 Active 상태로 원복]

5. 지사 네트워크 확장

5-1. 확장 구조

본사 네트워크 구축 완료 후, 라우터(R-A, R-B)를 통해 지사 네트워크를 연결하였다. WAN 구간은 192.168.0.0/24 대역을 사용하며, 정적 라우팅으로 본사-지사 간 통신을 구현하였다.

5-2. 라우팅 설계

장비	인터페이스	IP	연결 대상
R-A	gi0/1	192.168.10.100	본사 (S2-G)
R-A	gi0/0	192.168.0.1	WAN
R-B	gi0/0	192.168.0.2	WAN
R-B	gi0/1	192.168.60.100	지사 (S3-C)

5-3. 정적 라우팅 설정

```
! R-A (본사 라우터)
ip route 192.168.60.0 255.255.255.0 192.168.0.2

! R-B (지사 라우터)
ip route 192.168.10.0 255.255.255.0 192.168.0.1
ip route 192.168.20.0 255.255.255.0 192.168.0.1
ip route 192.168.30.0 255.255.255.0 192.168.0.1
```

6. 최종 검증

6-1. 본사 ↔ 지사 통신 테스트

```
C:\>ping 192.168.60.10
Reply from 192.168.60.10: bytes=32 time=1ms TTL=125
Ping statistics: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
```

7. 추후 기대 효과

7-1. 인터넷 구간 확장

향후 ISP 연동 및 NAT 설정을 통해 외부 인터넷 연결이 가능하며, AWS VPC와의 Site-to-Site VPN 구성을 통해 클라우드 하이브리드 환경으로 확장할 수 있다.

7-2. 보안 정책 (ACL)

VLAN 간 접근 제어를 위한 ACL 적용으로 보안을 강화할 수 있다. Building-A/B 사용자가 Storage 서버에 직접 접근하는 것을 제한하거나, 특정 서비스 포트만 허용하는 정책을 구현할 수 있다.