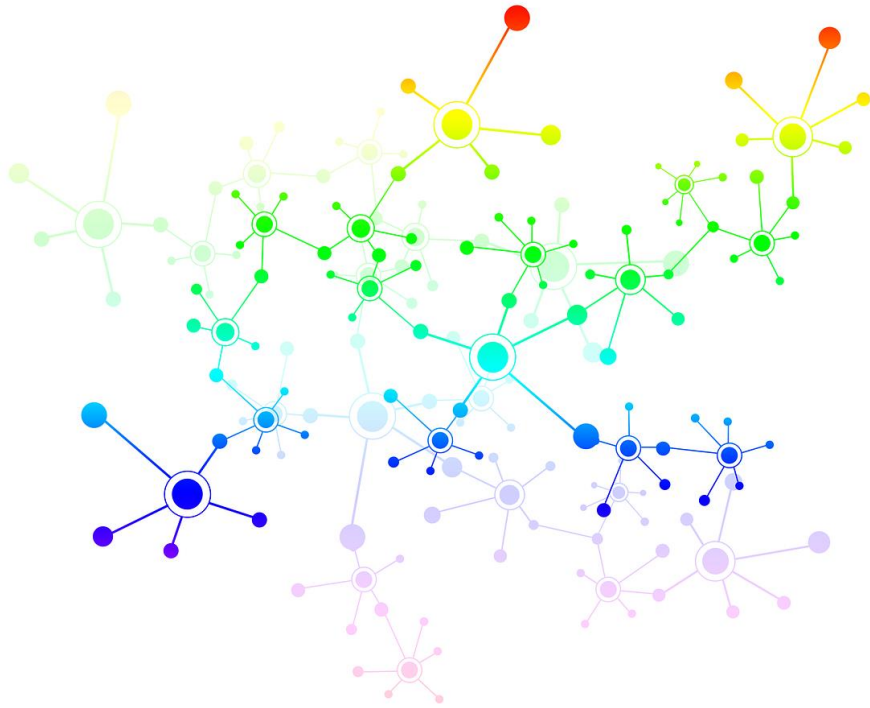


# 3 Tier Network 설계 & NMS 모니터링 구축

---

**김학남**

(8기)클라우드 데브옵스(DevOps) 엔지니어 및 관리자 양성과정



김학남









(8기)클라우드 데브옵스(DevOps) 엔지니어 및 관리자 양성과정

# INDEX

- 01. 프로젝트 기간 및 일정
- 02. 고객사 정보 및 요구사항
- 03. 네트워크 설계 Topology
- 04. 사용 장치 및 기술
- 05. 상세 구축내용
- 06. 네트워크 구축 결과
- 07. 시행 착오
- 08. Q&A

# 프로젝트 기간 및 일정

2023.05.29. ~ 2023.06.05 (8일)

	5/29	5/30	5/31	6/1	6/2	6/3	6/4	6/5
요구 분석								
네트워크 설계								
NMS 서버 설계 및 구축								
네트워크 구축								
원격 접속 설정								
Zabbix 설치 및 연동								
테스트 및 오류 수정								
발표								

## 고객사 정보 및 요구 사항

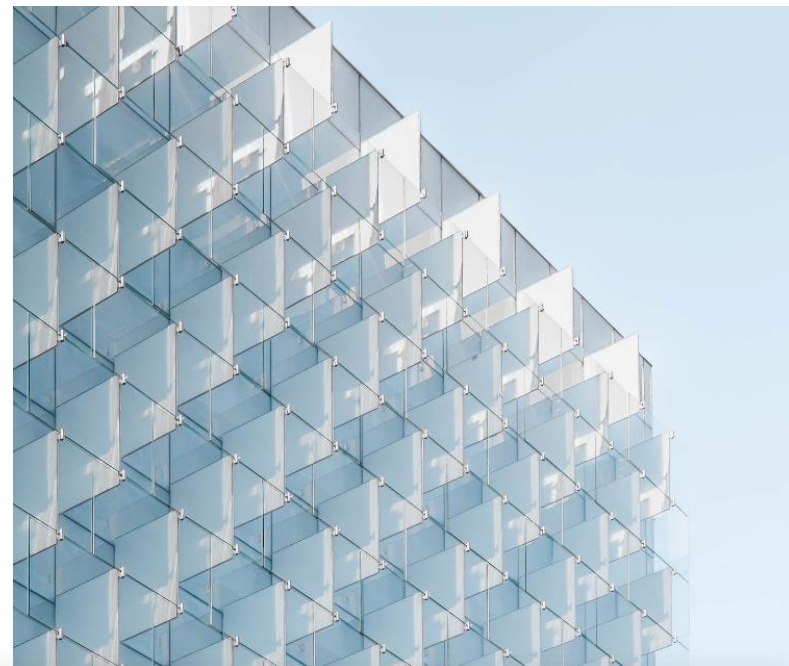
### 배경

고객사는 네트워크 인프라 문제를 겪고 있습니다.

첫째로, 기존 스위치와 라우터가 오랜 사용으로 인해 고장이 나서 이로 인해, 트래픽이 원활하게 전달되지 않고, 네트워크 통신이 불가능한 장비도 있습니다.

둘째로, 현재 고객사의 네트워크 구조는 단일 포인트 장애(SPOF)를 가지고 있습니다. 한 대의 네트워크 장비가 고장이 나면 전체 네트워크가 마비될 수 있는 상황으로 업무 및 서비스 중단으로 이어질 수 있습니다.

셋째로, 현재 사용 중인 전체 네트워크 구조는 계층 간 분리 및 보안 연결이 부족하거나 미흡합니다. 이로 인해 외부 공격자가 취약점을 쉽게 발견할 수 있고 더 나아가 고객 데이터 유출 위험이 있습니다.



### 이지모빌



직원 수: 1500명

주소: 서울특별시 마포구 합정동 789번지

설립일: 2015년 2월 10일

업종: 스마트 모빌리티

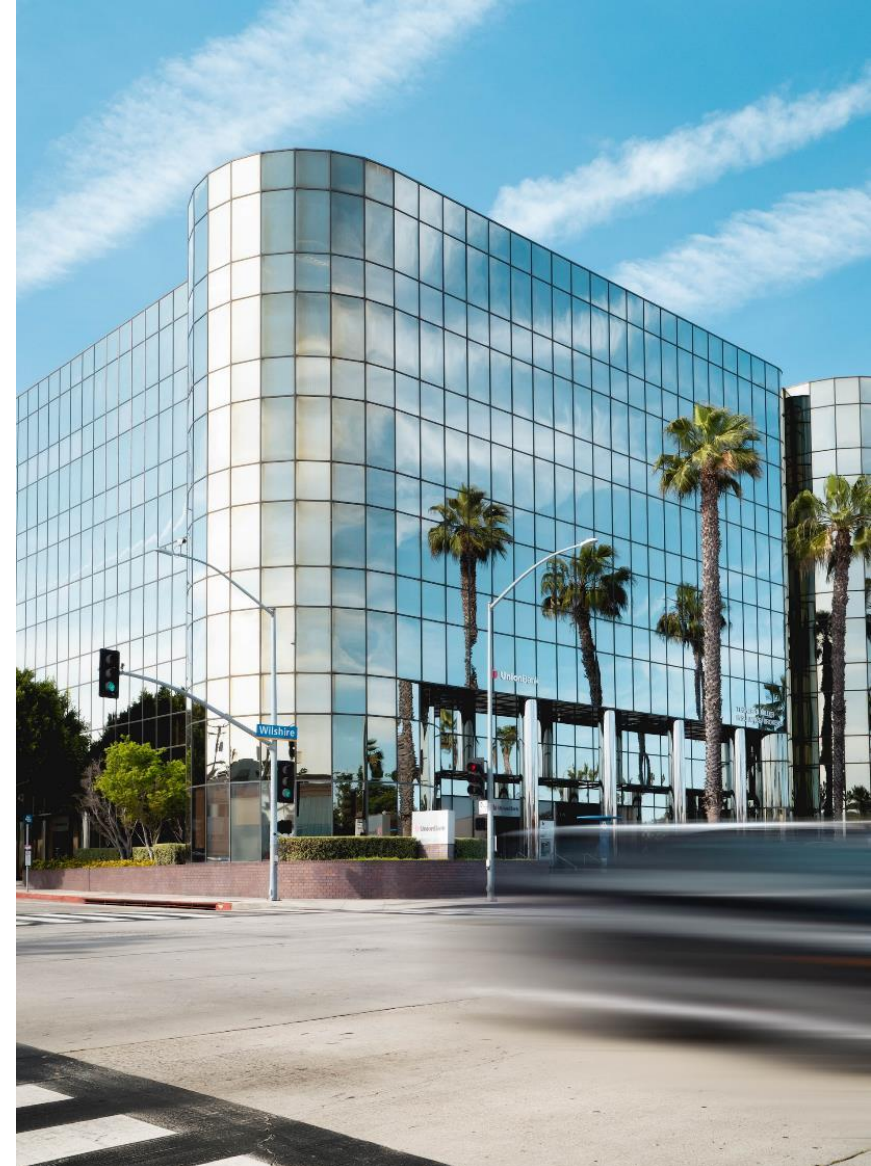
주요 제품: 전기 자전거, 전동 스쿠터, 스마트 시티 솔루션

## 고객사 정보 및 요구 사항

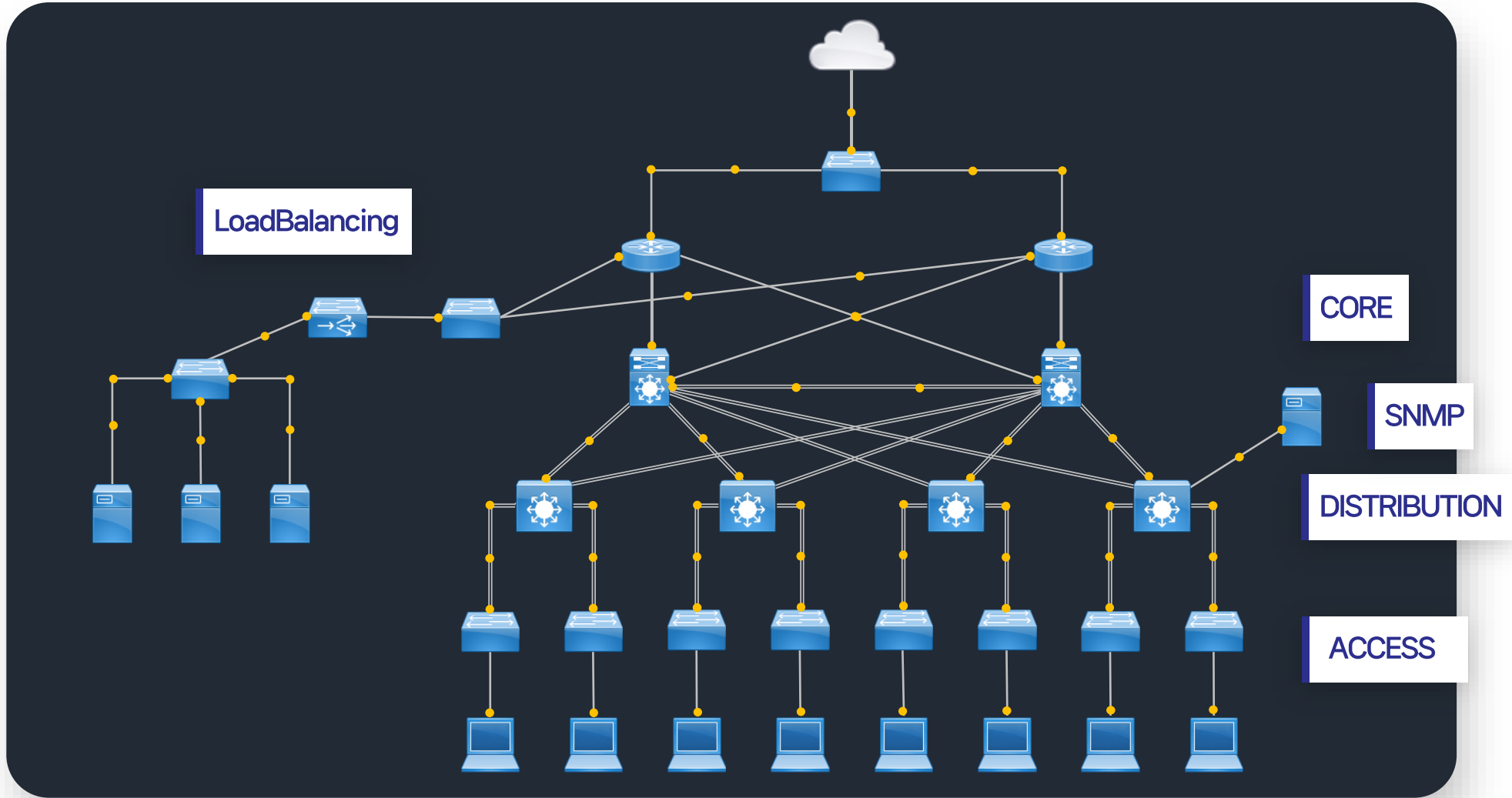


### 고객사 요구 사항

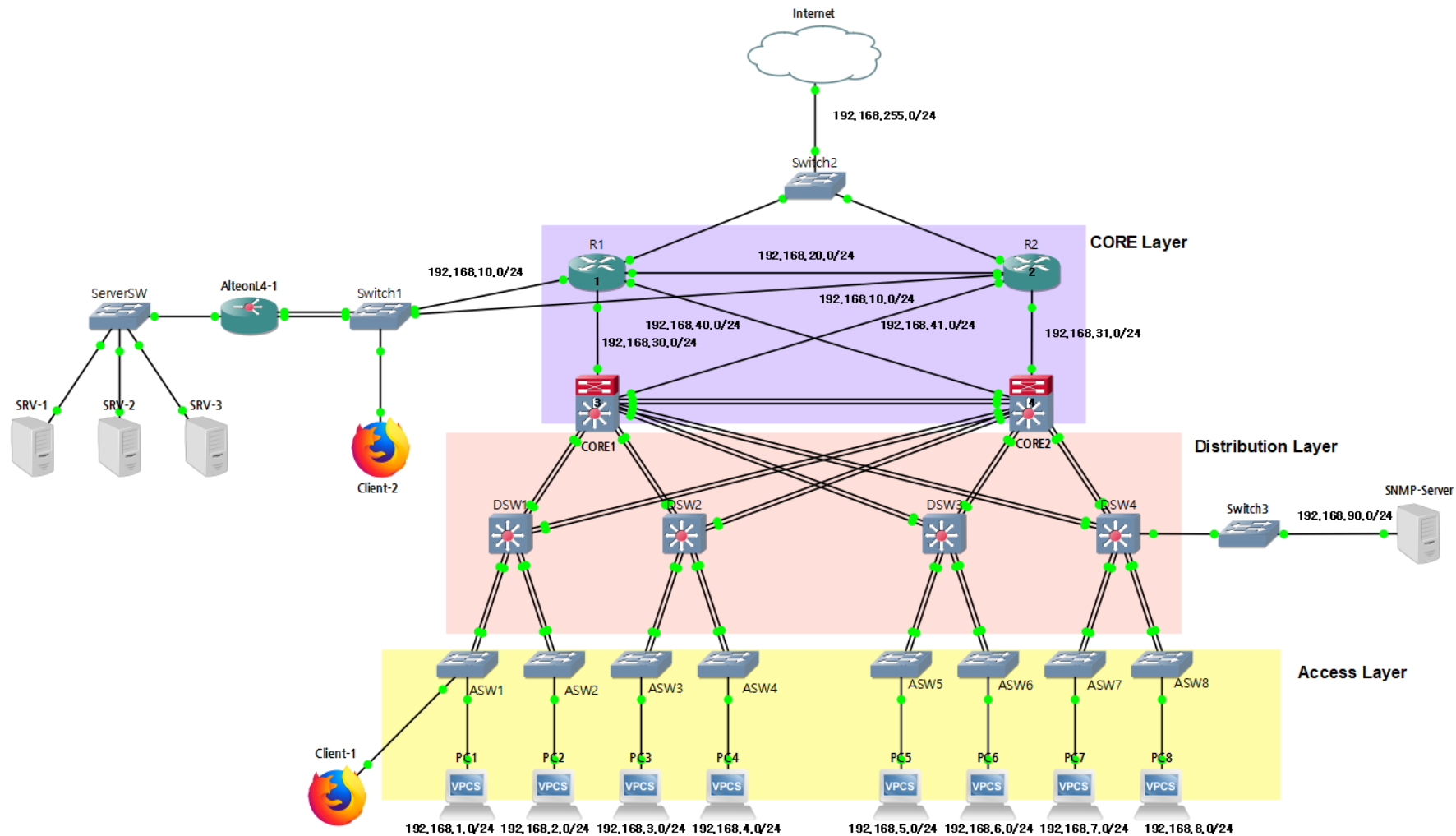
- 장비 간 이중 케이블 구성
- 이중화 구조로 가용성 확보
- 웹 서버 로드밸런싱
- 부서 별로 독립적인 네트워크 구성
- 네트워크 장비 모니터링
- 스위치 부하분산
- 확실한 계층 분리
- 외부 사용자는 내부 접속 차단 (웹서버 제외)



# 네트워크 설계 Topology



# 네트워크 설계 Topology



# 네트워크 설계 Topology

- Switch 간 연결은 traffic 관리 차원에서 이중 케이블로 구성하는 것이 좋다.
- Loop가 발생할 수 있기 때문에 신중히 디자인
- Switch는 반드시 여유분의 포트 확보 (확장성, 장애대비)

## Core Layer

- High-Speed backbone
- 네트워크 핵심
- 대량의 데이터 처리

## Access Layer

- 사용자와 네트워크 연결
- 직접 연결
- VLAN으로 브로드캐스트 영역 분리

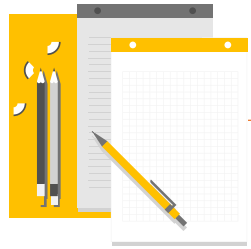
## Router

- 여러 네트워크 간의 연결 관리
- 외부 인터넷과 통신

## Distribution Layer

- Core와 Access 연결 관리
- 확장성
- 경로 선택
- 빠른 네트워크 트래픽 분배





### 독립된 네트워크 분리 및 Route

- VLAN
- VTP
- OSPF

### 이중화 구조 및 부하 분산

- MSTP
- HSRP

### 원격 접속

- Telnet

### 보안, 제한

- NAT
- Port Security
- BPDU Filter
- Root Guard

### Load\_Balancing

- ALTEON-L4

### System Monitoring

- ZABBIX
- MARIA DB
- Nginx & PHP



# 상세 구축 내용

## 05 링크 통합 및 VLAN

```
Number of channel-groups in use: 5
Number of aggregators:          5

Group  Port-channel  Protocol    Ports
-----+-----+-----+-----
10     Po10(SU)        -           Et0/2(P)   Et0/3(P)
11     Po11(SU)        -           Et1/0(P)   Et1/1(P)
12     Po12(SU)        -           Et1/2(P)   Et1/3(P)
13     Po13(SU)        -           Et2/0(P)   Et2/1(P)
14     Po14(SU)        -           Et2/2(P)   Et2/3(P)
```

```
CORE1(config)#do sh vlan brief

VLAN Name                Status    Ports
----+-----+-----+-----
1    default              active    Et3/0, Et3/1, Et3/2, Et3/3
10   VLAN0010              active
20   VLAN0020              active
30   VLAN0030              active
40   VLAN0040              active
50   VLAN0050              active
60   VLAN0060              active
70   VLAN0070              active
80   VLAN0080              active
100  Management            active
1002 fddi-default          act/unsup
1003 trcrf-default        act/unsup
1004 fddinet-default       act/unsup
1005 trbrf-default         act/unsup
```

### 링크통합

스위치는 VLAN을 통한 연결로 인한 모든 트래픽은 링크를 공유하며 통신 → 성능 최적화 및 대역폭 문제  
2개의 Link를 연결하여 두 인터페이스를 하나의 논리적 인터페이스로 묶어서 트래픽을 각 포트에 분산

### 부서 별로 네트워크 분리

각 부서마다 다른 VLAN을 부여하여  
고객사 전체 네트워크에서 Broadcast Domain을 L2 layer에서 분할 → IP 대역을 논리적으로 분할  
보안성과 스위치 성능 향상(Broadcast Domain 크기 감소)

# 상세 구축 내용

## 05 VTP (Cisco)

연결된 스위치끼리 VLAN 정보를 자동으로 주고 받아 동기화 하는 프로토콜 (CISCO 전용)

```
CORE1(config)#do sh vtp status
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : haknam.vm
VTP Pruning Mode         : Enabled
VTP Traps Generation     : Disabled
Device ID                 : aabb.cc80.0d00
Configuration last modified by 192.168.1.251 at 7-10-23 05:16:00
Local updater ID is 192.168.1.251 on interface Vl10 (lowest numbered VLAN interface found)

Feature VLAN:
-----
VTP Operating Mode       : Server
Maximum VLANs supported locally : 1005
Number of existing VLANs : 14
Configuration Revision   : 14
MD5 digest               : 0x79 0x89 0x87 0xAF 0xF8 0x85 0x49 0x45
                        : 0x83 0x41 0x3C 0x63 0xBB 0x42 0x81 0x50
```

```
DSW1(config)#do sh vtp status
VTP Version capable      : 1 to 3
VTP version running      : 2
VTP Domain Name          : haknam.vm
VTP Pruning Mode         : Enabled
VTP Traps Generation     : Disabled
Device ID                 : aabb.cc80.0100
Configuration last modified by 192.168.1.251 at 7-10-23 05:16:00

Feature VLAN:
-----
VTP Operating Mode       : Client
Maximum VLANs supported locally : 1005
Number of existing VLANs : 14
Configuration Revision   : 14
MD5 digest               : 0x79 0x89 0x87 0xAF 0xF8 0x85 0x49 0x45
                        : 0x83 0x41 0x3C 0x63 0xBB 0x42 0x81 0x50
```

### VTP – Server mode

VLAN 정보를 직접 생성, 전송할 수 있다.

### VTP – Client mode

같은 Domain에 password가 설정된 VTP Server로부터  
VLAN 정보를 받아 저장한다.

직접 VLAN 정보를 설정할 수 없다.

# 상세 구축 내용

## 05 Trunk Mode

```
CORE1(config)#do sh int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Pol0	on	802.1q	trunking	1
Pol1	on	802.1q	trunking	1
Pol2	on	802.1q	trunking	1
Pol3	on	802.1q	trunking	1
Pol4	on	802.1q	trunking	1

```
Port Vlan allowed on trunk
```

Pol0	1-4094
Pol1	1-4094
Pol2	1-4094
Pol3	1-4094
Pol4	1-4094

```
Port Vlan allowed and active in management domain
```

Pol0	1,10,20,30,40,50,60,70,80,100
Pol1	1,10,20,30,40,50,60,70,80,100
Pol2	1,10,20,30,40,50,60,70,80,100
Pol3	1,10,20,30,40,50,60,70,80,100
Pol4	1,10,20,30,40,50,60,70,80,100

```
Port Vlan in spanning tree forwarding state and not pruned
```

```
Port Vlan in spanning tree forwarding state and not pruned
```

Pol0	1,10,20,30,40,50,60,70,80,100
Pol1	1,10,20,100
Pol2	1,30,40,100
Pol3	1,100
Pol4	1,100

### Trunk mode

하나의 인터페이스를 Trunk Link로 설정하여 다수의 VLAN을 전송할 수 있다.

→ 고객사 네트워크 내에 부서 간 통신이 가능하다.

# 상세 구축 내용

## 05 Access mode, Portfast, BPDUfilter, Root guard

```
ASW2#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Et0/3, Et1/0, Et1/1, Et1/2 Et1/3, Et2/0, Et2/1, Et2/2 Et2/3, Et3/0, Et3/1, Et3/2 Et3/3
10	VLAN0010	active	
20	VLAN0020	active	Et0/2
30	VLAN0030	active	
40	VLAN0040	active	
50	VLAN0050	active	
60	VLAN0060	active	
70	VLAN0070	active	
80	VLAN0080	active	
100	Management	active	
1002	fddi-default	act/unsup	
1003	trcrf-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trbrf-default	act/unsup	

```
interface Ethernet0/2
switchport access vlan 40
switchport mode access
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security aging time 5
switchport port-security aging type inactivity
switchport port-security
spanning-tree portfast edge
spanning-tree bpdufilter enable
spanning-tree guard root
```

### Access - mode

스위치의 특정 인터페이스에 VLAN이라는 식별 값을 부여하고, 이 값이 동일한 포트끼리만 데이터 전달을 허용한다. Unicast, Multicast, Broadcast 프레임이 동일한 VLAN으로 설정된 포트로만 전달될 수 있다.

### Portfast

Portfast가 설정된 인터페이스는 Listening, Learning 상태를 거치지 않고 "no shutdown"을 하면 즉시 "UP" 상태로 변경  
굳이 STP를 작동할 필요가 없어서 활성화시키는 것이 좋다.

### BPDUfilter

특정 포트로 BPDU를 보내지 않는 기능이다.  
BPDU를 송신하지 않아 스위치 및 포트에 접속된 종단 장치에 불필요한 부하가 걸리는 것을 방지

### Root Guard

특정 포트에 접속된 네트워크에 있는 스위치들은 Root 스위치가 될 수 없도록 하는 기능이다.  
더 낮은 값의 Bridge-ID를 담은 BPDU를 수신하면 해당 포트를 down시켜서 Root 스위치 선출에 참여하지 못하도록 막음

# 상세 구축 내용

## 05 Port Security

```
ASW1(config)#do sh port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
              (Count)      (Count)      (Count)
-----
Et0/2         2          0          0          Restrict
Et0/3         2          1          0          Restrict
Et2/0         2          0          0          Restrict
Et2/1         2          0          0          Restrict
Et2/2         2          0          0          Restrict
Et2/3         2          0          0          Restrict
Et3/0         2          0          0          Restrict
Et3/1         2          0          0          Restrict
Et3/2         2          0          0          Restrict
Et3/3         2          0          0          Restrict
-----
Total Addresses in System (excluding one mac per port)    : 0
Max Addresses limit in System (excluding one mac per port) : 4096
```

### Port - Security

특정 포트에 학습할 수 있는 MAC주소를 제한하거나 허가된  
MAC 주소만 접속 가능하게 설정  
default 설정에는 MAC주소 제한이 없어 MAC Flooding  
Attack, ARP spoofing로부터 위험

### 세부 설정

- 최대 학습 가능한 MAC 주소는 2개로 제한
- restrict : 위반 장비의 통신을 차단하고 Log를 남김
- aging time (Mac address-table 갱신 주기) : 5분
- Inactivity : aging time동안 데이터 트래픽이 없는 경우  
Port-security에 등록된 MAC 주소 삭제

# 상세 구축 내용

## 05 MSTP

```
MST1
Spanning tree enabled protocol mstp
Root ID      Priority    24577
             Address    aabb.cc00.0d00
             This bridge is the root
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority    24577 (priority 24576 sys-id-ext 1)
             Address    aabb.cc00.0d00
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface                Role Sts Cost      Prio.Nbr Type
-----
Po10                     Desg FWD 1000000    128.65 P2p
Po11                     Desg FWD 1000000    128.66 P2p
Po12                     Desg FWD 1000000    128.67 P2p
Po13                     Desg FWD 1000000    128.68 P2p
Po14                     Desg FWD 1000000    128.69 P2p

MST2
Spanning tree enabled protocol mstp
Root ID      Priority    24578
             Address    aabb.cc00.0e00
             Cost        1000000
             Port        65 (Port-channel10)
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID    Priority    28674 (priority 28672 sys-id-ext 2)
             Address    aabb.cc00.0d00
             Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Interface                Role Sts Cost      Prio.Nbr Type
-----
Po10                     Root FWD 1000000    128.65 P2p
Po11                     Desg FWD 1000000    128.66 P2p
Po12                     Desg FWD 1000000    128.67 P2p
Po13                     Desg FWD 1000000    128.68 P2p
Po14                     Desg FWD 1000000    128.69 P2p
```

```
MST1
Spanning tree enabled proto
Root ID      Priority    2457
             Address    aabb
             Cost        1000
             Port        65 (
             Hello Time 2 s

Bridge ID    Priority    3276
             Address    aabb
             Hello Time 2 s

Interface                Role Sts
-----
Po11                     Root FWD
Po15                     Altn BLK
Po21                     Desg FWD
Po22                     Desg FWD
```

### MSTP 설정

VLAN 별로 STP Root 스위치를 다르게 설정하여 CORE  
스위치 부하 분산 및 이중화 → 효율성 및 성능 향상  
여러 VLAN을 하나의 Instance로 묶음

### 스위치 간 Loop 방지

이중화 구성을 했을 때 만약 한 장비에 이상이 발생하여 작동을  
하지 않더라도 네트워크가 끊어지지 않고 계속 동작한다.  
→ 네트워크 Looping 발생  
그래서 스위치에 특정 포트를 차단하여 Loop 구조를 막는다.

# 상세 구축 내용

## 05 Err-disable

```
CORE1(config)#errdisable recovery cause all
CORE1(config)#errdisable recovery interval 300
CORE1(config)#do sh errdisable recovery
ErrDisable Reason      Timer Status
-----
arp-inspection          Enabled
bpdguard                Enabled
channel-misconfig (STP) Enabled
dhcp-rate-limit         Enabled
dtp-flap                Enabled
gbic-invalid            Enabled
inline-power            Enabled
l2ptguard               Enabled
link-flap               Enabled
mac-limit               Enabled
link-monitor-failure    Enabled
loopback                Enabled
oam-remote-failure      Enabled
pagp-flap               Enabled
port-mode-failure       Enabled
pppoe-ia-rate-limit     Enabled
psecure-violation       Enabled
security-violation       Enabled
sfp-config-mismatch     Enabled
storm-control           Enabled
udld                    Enabled
--More--
```

### errdisable

Switch에서 포트에 대한 장애 및 에러 유무를 주기적으로 모니터링하여 에러가 발생하면 자동으로 포트가 Errdisabled 상태로 변경되며 Shutdown 상태가 된다.

### 자동 포트 활성화

Default 설정으로 모든 ErrDisable Reason detect가 활성화되어 있는 상태이다.  
Shutdown 되었을 때 다시 자동으로 포트 활성화를 하는 설정만 추가하였음



# 상세 구축 내용

## 05 Router의 SLA, Track

```
R1(config)#do sh ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending

ID          Type          Destination      Stats      Return      Last
-----
*1          icmp-echo    192.168.255.2    RTT=3      OK          1 second ago

R1(config)#do sh track
Track 10
  IP SLA 1 reachability
  Reachability is Up
    2 changes, last change 01:27:03
  Latest operation return code: OK
  Latest RTT (milliseconds) 3
  Tracked by:
    Static IP Routing 0
R1(config)#
R1(config)#do sh run | sec track
track 10 ip sla 1 reachability
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0 192.168.255.2 track 10
```

### SLA

IP를 이용해 네트워크 성능을 모니터링  
여러 방법 중 ICMP Check를 사용하여 다른 네트워크의  
성능을 확인 → 네트워크 관리 효율성 증대

### Track 적용

장비 내에서 발생하는 이벤트를 추적, 감지하고 그에 대한  
동작을 수행  
여기선 Router에서 외부 인터넷으로의 경로를 추적 및 감지

# 상세 구축 내용

## 05 Core Switch의 SLA, Track

```
CORE1(config)#do sh track
Track 1
  IP SLA 1 reachability
  Reachability is Up
    4 changes, last change 00:52:21
  Latest operation return code: OK
  Latest RTT (milliseconds) 1
  Tracked by:
    Track List 100
Track 2
  IP SLA 2 reachability
  Reachability is Up
    4 changes, last change 00:52:31
  Latest operation return code: OK
  Latest RTT (milliseconds) 1
  Tracked by:
    Track List 100
Track 100
  List boolean or
  Boolean OR is Up
    2 changes, last change 01:27:57
    object 1 Up
    object 2 Up
  Tracked by:
    HSRP Vlan10 10
    HSRP Vlan20 20
    HSRP Vlan30 30
    HSRP Vlan40 40
    HSRP Vlan50 50
    HSRP Vlan60 60
    HSRP Vlan70 70
    HSRP Vlan80 80
    HSRP Vlan100 100
```

```
CORE1(config)#do sh ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
```

ID	Type	Destination	Stats (ms)	Return Code	Last Run
*1	icmp-echo	192.168.30.1	RTT=1	OK	0 seconds ago
*2	icmp-echo	192.168.41.2	RTT=1	OK	0 seconds ago

### SLA 설정

CORE Switch에서 각각 R1, R2로 향하는 경로를 ICMP Check로 감지 및 성능 체크

### Track 적용

두 SLA를 각 Track으로 만든 후 Track list Boolean 설정  
만약 R1과 R2로 packet을 보내지 못하는 장애가 발생하면  
HSRP 프로토콜로 인해 다른 CORE Switch가 게이트웨이 역할 담당

# 상세 구축 내용

## 05 Router HSRP (CISCO)

```
R1(config)#do sh standby
GigabitEthernet0/1 - Group 1
  State is Active
    2 state changes, last state change 01:45:02
  Virtual IP address is 192.168.10.254
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 1 sec, hold time 3 sec
    Next hello sent in 0.208 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.10.2, priority 120 (expires in 2.672 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Gi0/1-1" (default)
```

### 게이트웨이 이중화

만약 한 경로에 문제가 생겼을 때 다른 경로에서 계속  
게이트웨이 역할을 해줄 수 있는 가상 게이트웨이를 설정  
물리적으로 2대 이상의 장비가 있어야 한다.  
→ 높은 네트워크 가용성 제공

### ALTEON Server 대상

Alteon과 연결되어 있는 Server의 게이트웨이를 HSRP로  
가상 게이트웨이 지정 (R1, R2)  
만약 R1 경로에 이상이 발생하면 R2 경로가 작동

# 상세 구축 내용

## 05 Core Switch HSRP

```
CORE1(config)#do sh standby
Vlan10 - Group 10
  State is Active
    2 state changes, last state change 01:37:10
  Virtual IP address is 192.168.1.254
  Active virtual MAC address is 0000.0c07.ac0a (MAC In Use)
  Local virtual MAC address is 0000.0c07.ac0a (v1 default)
  Hello time 1 sec, hold time 3 sec
  Next hello sent in 0.112 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.252, priority 110 (expires in 2.768 sec)
  Priority 120 (configured 120)
  Track object 100 state Up decrement 100
  Group name is "hsrp-Vl10-10" (default)
```

```
Vlan50 - Group 50
  State is Standby
    4 state changes, last state change 01:36:10
  Virtual IP address is 192.168.5.254
  Active virtual MAC address is 0000.0c07.ac32 (MAC Not In Use)
  Local virtual MAC address is 0000.0c07.ac32 (v1 default)
  Hello time 1 sec, hold time 3 sec
  Next hello sent in 0.208 secs
  Preemption enabled
  Active router is 192.168.5.252, priority 120 (expires in 2.816 sec)
  Standby router is local
  Priority 110 (configured 110)
  Track object 100 state Up decrement 100
  Group name is "hsrp-Vl50-50" (default)
```

### 각 부서 PC 게이트웨이

각 부서의 종단 장비 게이트웨이를 CORE1과 CORE2를 묶어 하나의 가상 게이트웨이를 설정

### VLAN으로 구분하여 Active Switch 지정

VLAN 10 – 40, 100은 CORE1이 게이트웨이 역할로 작동  
VLAN 50 – 80은 CORE2가 게이트웨이 역할로 작동

# 상세 구축 내용

## 05 OSPF

```
Gateway of last resort is 192.168.255.2 to network 0.0.0.0

0 E2 192.168.1.0/24 [110/20] via 192.168.40.4, 01:58:40, GigabitEthernet0/4
    [110/20] via 192.168.30.3, 01:58:40, GigabitEthernet0/3
0 E2 192.168.2.0/24 [110/20] via 192.168.40.4, 01:58:40, GigabitEthernet0/4
    [110/20] via 192.168.30.3, 01:58:40, GigabitEthernet0/3
0 E2 192.168.3.0/24 [110/20] via 192.168.40.4, 01:58:40, GigabitEthernet0/4
    [110/20] via 192.168.30.3, 01:58:40, GigabitEthernet0/3
0 E2 192.168.4.0/24 [110/20] via 192.168.40.4, 01:58:40, GigabitEthernet0/4
    [110/20] via 192.168.30.3, 01:58:40, GigabitEthernet0/3
0 E2 192.168.5.0/24 [110/20] via 192.168.40.4, 01:58:40, GigabitEthernet0/4
    [110/20] via 192.168.30.3, 01:58:40, GigabitEthernet0/3
0 E2 192.168.6.0/24 [110/20] via 192.168.40.4, 01:58:40, GigabitEthernet0/4
    [110/20] via 192.168.30.3, 01:58:40, GigabitEthernet0/3
0 E2 192.168.7.0/24 [110/20] via 192.168.40.4, 01:58:40, GigabitEthernet0/4
    [110/20] via 192.168.30.3, 01:58:40, GigabitEthernet0/3
0 E2 192.168.8.0/24 [110/20] via 192.168.40.4, 01:58:40, GigabitEthernet0/4
    [110/20] via 192.168.30.3, 01:58:40, GigabitEthernet0/3
0 192.168.31.0/24 [110/20] via 192.168.20.2, 01:58:29, GigabitEthernet0/2
0 192.168.41.0/24 [110/20] via 192.168.20.2, 01:58:29, GigabitEthernet0/2
192.168.90.0/24 is variably subnetted, 3 subnets, 2 masks
0 IA 192.168.90.0/24
    [110/20] via 192.168.40.4, 01:58:40, GigabitEthernet0/4
    [110/20] via 192.168.30.3, 01:58:40, GigabitEthernet0/3
0 IA 192.168.90.12/32
    [110/11] via 192.168.20.2, 01:58:29, GigabitEthernet0/2
```

### OSPF Routing Protocol

링크 상태를 확인하여 최단 경로를 찾는 알고리즘을 통해  
확인된 최단 경로를 바탕으로 패킷을 전달한다.

SPF 알고리즘을 사용

Area를 통해 OSPF 네트워크를 더 작은 영역으로 나눠  
관리가 가능 → 대규모 네트워크에 적합한 운영 가능

# 상세 구축 내용

## 05 OSPF

```
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.255.10
  It is an area border and autonomous system boundary router
  Redistributing External Routes from,
  Number of areas in this router is 4. 2 normal 0 stub 2 nssa
  Maximum path: 4
  Routing for Networks:
  Routing on Interfaces Configured Explicitly (Area 0):
    GigabitEthernet0/4
    GigabitEthernet0/3
    GigabitEthernet0/2
  Routing on Interfaces Configured Explicitly (Area 1):
    GigabitEthernet0/1
  Routing on Interfaces Configured Explicitly (Area 192.168.255.1):
    Loopback0
  Passive Interface(s):
    GigabitEthernet0/1
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.31.4      110           02:00:34
    192.168.30.3      110           02:00:34
    192.168.255.20    110           01:25:17
  Distance: (default is 110)
```

```
Area 1
  Number of interfaces in this area is 1
  It is a NSSA area
  Perform type-7/type-5 LSA translation
  Area has no authentication
  SPF algorithm last executed 02:02:26.401 ago
  SPF algorithm executed 2 times
  Area ranges are
  Number of LSA 2. Checksum Sum 0x01B7C9
  Number of opaque link LSA 0. Checksum Sum 0x000000
  Number of DCbitless LSA 0
  Number of indication LSA 0
  Number of DoNotAge LSA 0
  Flood list length 0
```

### OSPF area

Router와 CORE Switch 링크에 Area 0 (Backbone area)으로 설정

Loopback IP, ALTEON 연결 중인 링크엔 각각 다른 area 부여 → Backbone area로 인해 서로 다른 area끼리도 통신 가능

### Totally NSSA area 설정

다른 Routing protocol로 동작하는 장치가 추가되는 것을 고려하여 Totally NSSA를 선언한다

→ 만약 추가되면 LSA Type 5가 Type 7으로 변경되어 backbone area를 거치지 않더라도 경로 정보 전달이 가능하다.

그 후 NSSA ABR이 다시 LSA Type 5로 변경 후 area 0으로 광고

# 상세 구축 내용

## 05 NAT (PAT 방식)

```
ip nat inside source list 1 interface GigabitEthernet0/0 overload
ip nat inside source static tcp 192.168.10.150 80 interface GigabitEthernet0/0 80
```

```
R1#show ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
tcp 192.168.255.10:80  192.168.10.150:80  ---              ---
```

### 네트워크 주소 변환

외부에서 내부 네트워크를 알 수 없음 (경로 정보 또한 알 수 없음)

사실 네트워크에 속한 여러 호스트가 하나의 공인 IP 주소를 사용하여 인터넷에 접속

사실 IP를 공인 IP로 변경할 수 있기 때문에 IPv4 부족 현상을 줄여 준다.

그러나 장치에 부하가 많이 걸린다.

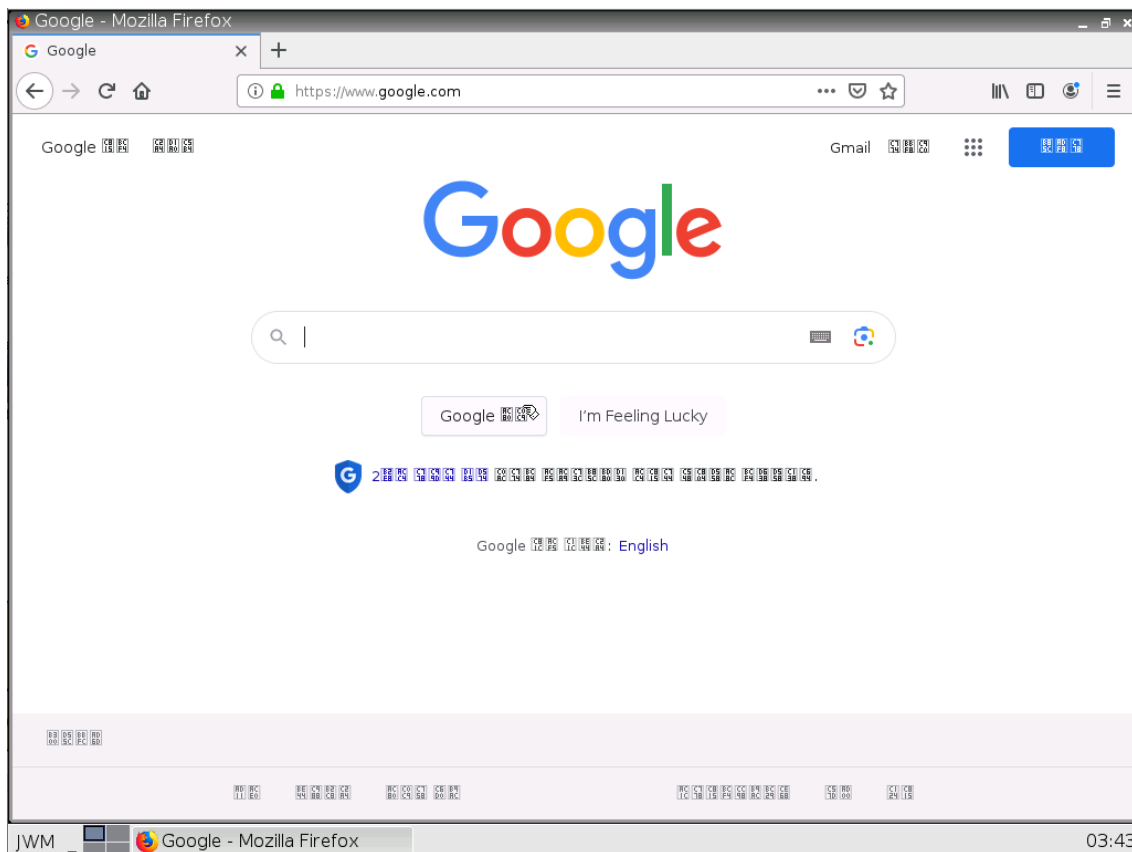
### Port Forwarding

어떠한 IP 주소와 포트 번호의 통신 요청을 특정 다른 IP와 포트 번호로 넘겨준다.

게이트웨이(외부망)의 반대쪽에 위치한 내부 사설 네트워크에 상주하는 호스트에 대한 서비스 생성 가능

# 상세 구축 내용

## 05 외부 인터넷 통신 확인



Client1 에서 접속

외부 인터넷 사용 가능 확인



# 상세 구축 내용

## 05 Telnet 접속 제한

```
R1(config)#do show run | sec access-list
access-list 1 permit any
access-list 2 permit 192.168.90.0 0.0.0.255
R1(config)#
R1(config)#do sh run | sec line
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
line vty 0 4
access-class 2 in
exec-timeout 5 30
logging synchronous
login local
transport input telnet ssh
```

### telnet 접속 IP를 제한

내부 장비를 관리하기 위해 각 장비에 원격으로 접속할 필요가 있다.

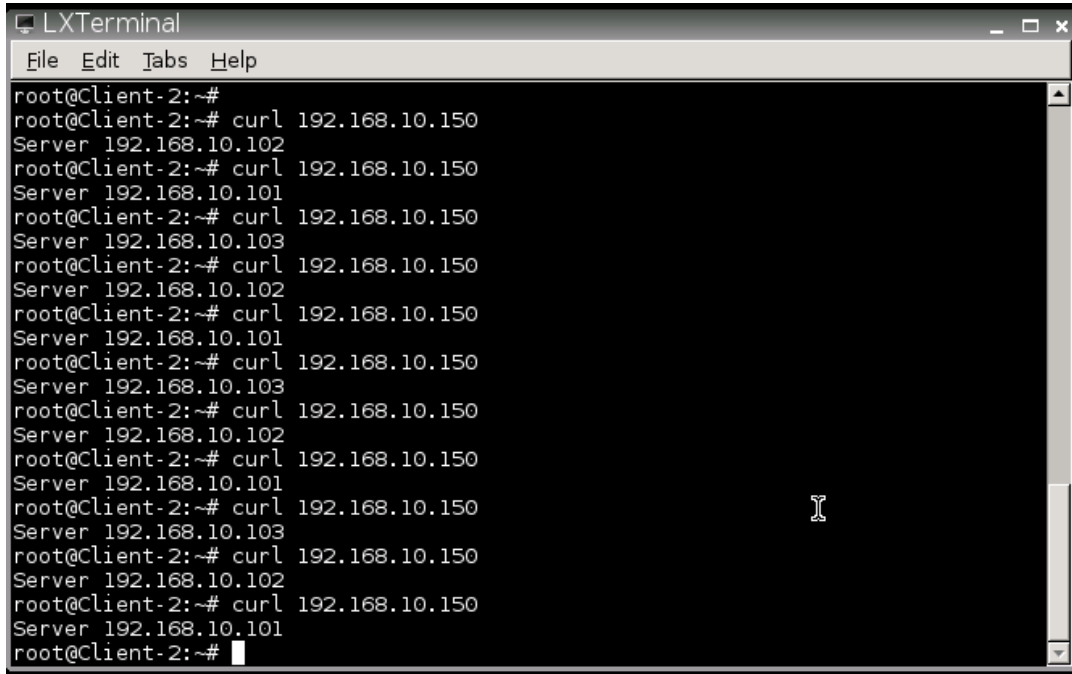
그래서 설정한 관리용 IP 대역으로만 장비에 Telnet 원격 접속을 허용한다.

SSH는 인증을 위한 공개키를 만들어서 사용해야 하지만 Telnet은 인증이 없다

오로지 사설 IP 대역으로 설정한 내부 장비에 원격 접속을 할 것이기 때문에 SSH 대신 Telnet으로 사용

# 상세 구축 내용

## 05 ALTEON



```
LXTerminal
File Edit Tabs Help
root@Client-2:~#
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.102
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.101
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.103
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.102
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.101
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.103
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.102
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.101
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.103
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.102
root@Client-2:~# curl 192.168.10.150
Server 192.168.10.101
root@Client-2:~#
```

### Load Balancer

서버에 가해지는 부하를 분산해주는 장치  
한 대의 서버로 부하가 집중되지 않도록 트래픽을 관리하여  
각각의 서버가 최적의 퍼포먼스를 보일 수 있도록 한다.

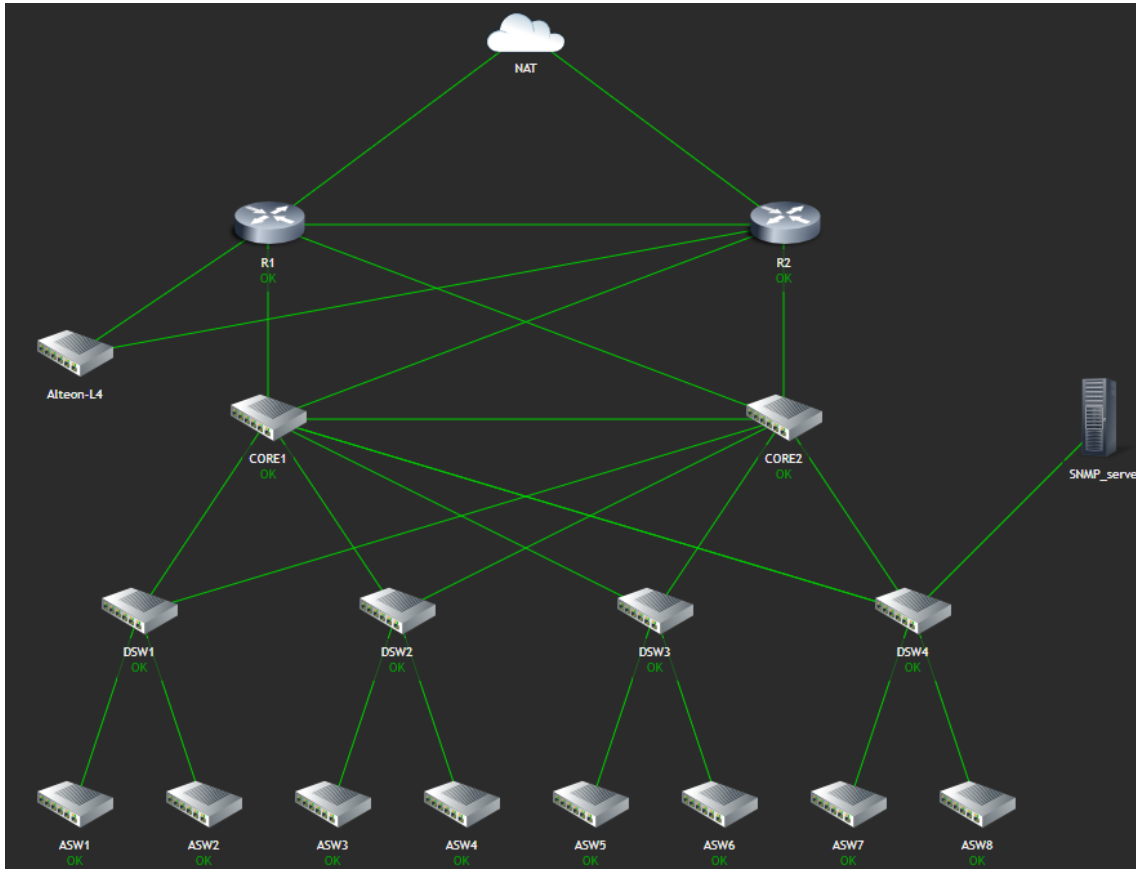
만약 Scale-Out 방식으로 서버를 증설한다면 로드밸런싱이  
반드시 필요

### Round Robin

서버에 들어온 요청을 순서대로 돌아가며 배정하는 방식  
여러 대의 서버가 동일한 스펙을 갖고 있고, 서버와의 연결이  
오래 지속되지 않는 경우에 적합하다.

# 상세 구축 내용

## 05 SNMP 모니터링



### Zabbix

Zabbix는 분산 모니터링 솔루션  
IP 기반 네트워크상의 각 호스트로부터 정기적으로 여러 관리  
정보를 자동으로 수집하거나 실시간으로 상태를 모니터링 및  
설정

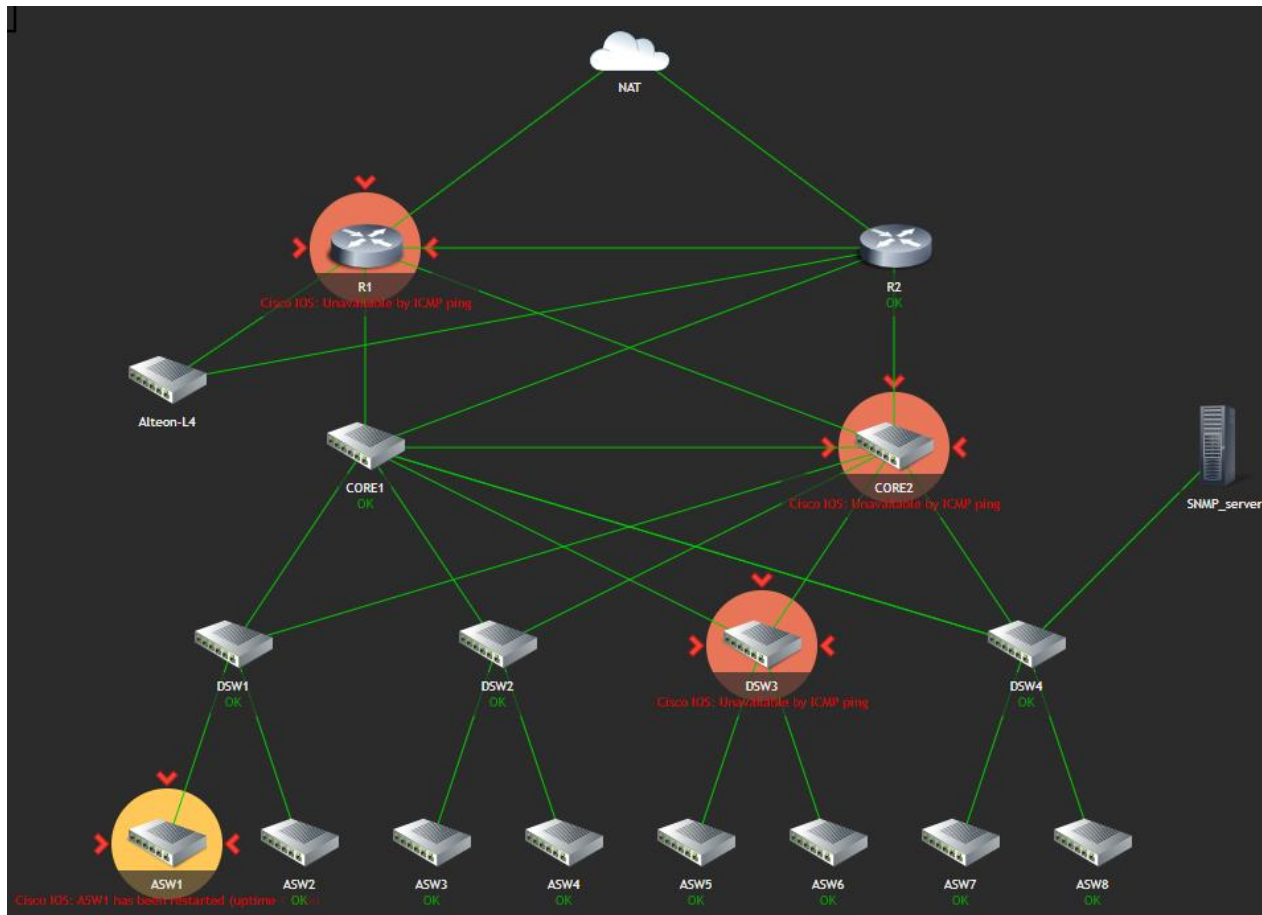
PHP로 구현된 Apache 기반 웹 브라우저 지원

### Zabbix Map 구성

장비의 구성을 한 눈에 보기에 편하다.  
등록된 host 장비를 불러와서 구성

# 상세 구축 내용

## 05 SNMP 모니터링



시스템 장애  
발생 시  
Map 확인

# 상세 구축 내용

05

## SNMP 모니터링

Time	Severity	Recovery time	Status	Info	Host	Problem	Duration	Ack	Actions	Tags
17:47:28	Warning		PROBLEM		DSW3	↓ Cisco IOS: DSW3 has been restarted (uptime < 10m) ?	55s	No		class: network component: system scope: notice ...
17:46:55	Warning		PROBLEM		CORE2	↓ Cisco IOS: CORE2 has been restarted (uptime < 10m) ?	1m 28s	No		class: network component: system scope: notice ...
17:46:51	Warning		PROBLEM		R1	↓ Cisco IOS: R1 has been restarted (uptime < 10m) ?	1m 32s	No		class: network component: system scope: notice ...
17:45:37	Warning	17:45:35	RESOLVED		ASW6	↑ ↓ Cisco IOS: High ICMP ping loss	58s	No		class: network component: health component: network ...
17:45:34	High	17:45:33	RESOLVED		ASW3	↑ Cisco IOS: Unavailable by ICMP ping ?	59s	No		class: network component: health component: network ...
17:44:43	Warning		PROBLEM		ASW3	↓ Cisco IOS: ASW3 has been restarted (uptime < 10m) ?	3m 40s	No		class: network component: system scope: notice ...
17:43:35	High	17:43:35	RESOLVED		ASW6	↑ Cisco IOS: Unavailable by ICMP ping ?	1m	No		class: network component: health component: network ...
17:43:35	High	17:43:35	RESOLVED		ASW5	↑ Cisco IOS: Unavailable by ICMP ping ?	1m	No		class: network component: health component: network ...
17:43:29	High	17:43:29	RESOLVED		DSW3	↑ Cisco IOS: Unavailable by ICMP ping ?	3m	No		class: network component: health component: network ...
17:43:26	High	17:43:25	RESOLVED		CORE2	↑ Cisco IOS: Unavailable by ICMP ping ?	2m 59s	No		class: network component: health component: network ...
17:43:21	High	17:43:21	RESOLVED		R1	↑ Cisco IOS: Unavailable by ICMP ping ?	3m	No		class: network component: health component: network ...
17:43:19	Warning		PROBLEM		ASW1	↓ Cisco IOS: ASW1 has been restarted (uptime < 10m) ?	5m 4s	No		class: network component: system scope: notice ...

Displaying 12 of 12 found

시스템 장애  
발생 시

# 상세 구축 내용

## 05 SNMP 모니터링



ASW4 → DSW2 대량의트래픽 전송

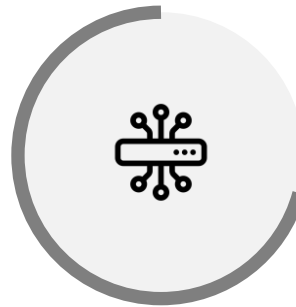
트래픽 급증

## 네트워크 구축 결과



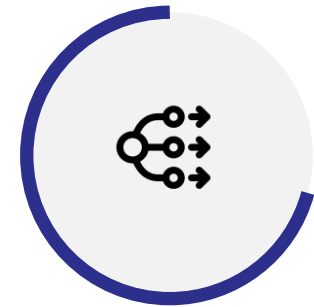
### 3-Tier Network

확장성  
관리 용이성  
성능 향상  
보안 강화



### SNMP Monitoring

장비 정보 자동 수집  
실시간 상태 모니터링



### Load Balancing

여러 서버로 부하 분산  
효율 및 안정성 증가

# 네트워크 구축 결과

## 3 – Tier Network

- 각 계층을 분리하여 확장성 높임
- Access, Distribution Layer는 필요에 따라 장치 추가 가능

### 확장성

- 계층 분리 → 네트워크 관리 간소화
- Access Layer : 개별 사용자, 장치 관리
- Distribution Layer : 네트워크 간 연결과 경로 선택
- Core Layer : 전체 네트워크의 연결 및 데이터 전송

### 관리 용이성

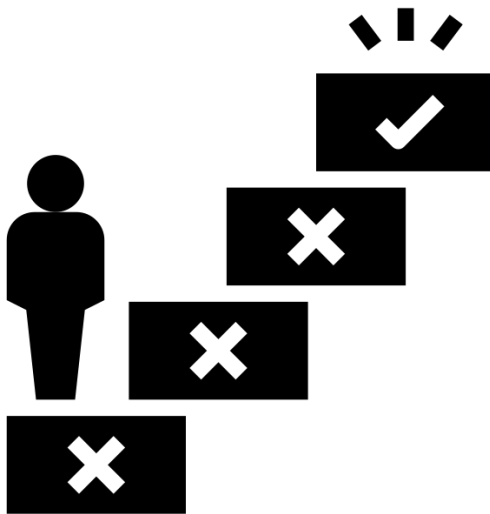
### 성능 향상

- Distribution Layer : Access와 Core 간의 트래픽 조절 → 병목 현상 방지
- Core Layer : 고성능 장비로 구성하여 대량의 데이터를 빠르게 전송

### 보안 강화

- Access Layer : 사용자와 직접적인 연결을 관리
- Distribution Layer : 보안 정책 적용하여 외부 침입을 제어
- Core Layer : 다른 네트워크와의 연결 관리, 방화벽과 같은 보안 장비 이용





SNMP server에서 모든 장비 통신이 되지 않았음

SNMP server와 연결되어 있는 DSW4 포트에  
VLAN access 설정을 하지 않았음

SNMP server에서 Router loopback으로  
통신이 되지 않음

- 원래 Router의 Loopback IP를 OSPF area 0으로  
설정하였음 → Non-backbone area로 수정
- 그리고 SNMP management IP 192.168.254.0  
대역으로 사용 → VMware 가상 서버로 만들었는데  
Host-only 네트워크 대역과 같음 → 충돌
- 그래서 SNMP management 네트워크 대역을  
192.168.90.0으로 수정



# Q & A