K-Digital Training

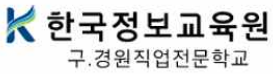
결재	담당	원장

클라우드데브옵스(DevOps) 엔지니어및관리자 양성과정(8기)

NW 프로젝트 완료 보고서

- 3 Tier Network 설계 및 NMS 모니터링 구축 -

2023.06.05



프로젝트 완료 보고서		
프로젝트 주제	3 Tier Network 설계 및 NMS 소프트웨어 모니터링 구축	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.06.05

문서 개정 이력

개정번호	개정일자	시행일자	개정내용	담당자
1.0	2023.06.05.		최초 작성	김학남

교 육 기 관 : 한 국 정 보 교 육 원

팀 장 : 김학남

목차

프로젝트 완료 보고서		
프로젝트 주제	3 Tier Network 설계 및 NMS 소프트웨어 모니터링 구축	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.06.05

Ⅰ. 프로젝트 개요

1. 프로젝트 명

   3 Tier Network 설계 및 NMS 소프트웨이 모니터링 구축

2. 프로젝트 기간

   2023.05.29. ~ 2023.06.05.(총 8일)

3. 프로젝트 배경 및 요구 사항

고객사는 네트워크 인프라 문제를 겪고 있습니다.

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

(2) 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.

(3) 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.

[요구 사항]

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

4. 프로젝트 범위

4.1 프로젝트 대상

◆ 3 Tier Network 구축 기획 및 설계
- 고객사의 요청에 따른 체계적인 구축방법 수립
- 부서별로 분리된 네트워크
- 3 Tier 구조 Network 환경으로 모든 서비스 마비(down)을 방지
- 여러 대의 Web Server가 동시에 동작하여 성능을 높이고 일부 문제가 발생하더라도 빠른 시간 안에 서비스를 복구

◆ Network 구성
- 이중화 구성으로 장애가 발생하더라도 서비스의 연속성 유지
- VTP 설정으로 Switch의 VLAN 정보를 동기화시켜 서버가 클라이언트에게 Update
- Trunk 자동협상 기능으로 여러 VLAN이 한꺼번에 통신 가능
- Port security로 MAC Flooding attack 등의 문제 해결에 용이
- 게이트웨이 이중화 프로토콜 HSRP를 사용하여 장애 대비
- LoadBalancing으로 부하분산 및 Zabbix를 이용한 장비 모니터링 가능

4.2 프로젝트 수행 요건

가. 개발 적용 지침 및 가이드라인

○ 행정기관 클라우드 업무환경 도입 가이드(행정자치부, 2016.11)
○ 민간 부문의 클라우드 도입 실무 가이드라인(방송통신위원회, 2012.12)
○ 클라우드컴퓨팅 주요법령 해설서(과학기술정보통신부, 2017.11)
○ 클라우드 정보보호 안내서(한국인터넷진흥원, 2017.12)
○ 중소기업 보안위협 예방 및 대응가이드(한국인터넷진흥원, 2019.7)
○ 중소기업 정보보호 업무가이드(한국인터넷진흥원, 2019.7)

나. 설계 및 개발 요건

○ 본 프로젝트는 기 운영 중인 한국정보교육원의 인프라 환경과 연관성을 가지고 개발·구축 되어야 하며, 시범운영을 마친 후 서비스를 개시하여야 한다.

○ 시스템은 추가 및 확장이 용이하도록 설계되어야 한다.

○ 안정적인 서비스 운영이 가능하도록 서버는 상시적으로 동작이 가능 하도록 별도의 공간에서 운영되어야 하며 항온·항습 등을 유지할 수 있어야 한다.

○ 훈련생들의 프로젝트를 위한 Instance의 생성·삭제·유지 보수 등이 용이 하도록 GUI가 제공되어야 하며 해당 UI에는 한국정보교육원을 상징할 수 있도록 설계·개발 되어야 한다.

○ 훈련생 실습용 인스턴스는 인터넷 접속이 불가능 하므로 내부에서 도메인을 이용한 대시보드 접속이 가능하도록 한국정보교육원 내의 모든 PC는 2차 DNS는 10.0.0.0/8 로 설정하여야 한다.

○ 시스템의 물리적/논리적 Scale out/up에 대비하여 설계되어야 한다.

○ 라우터의 NAT기능을 통해 내/외부 간 통신은 가능케 하되, 직접적인 연결은 차단한다.

○ 네트워크 및 서버의 물리적/논리적 이중화를 중점적으로 구현

○ VLAN으로 구간이 나뉜 운영 서버 간 통신환경을 고려하여 구현

Ⅱ. 프로젝트 추진 체계

1. 프로젝트 참여인력 총괄표

성 명	소 속	역할	담 당 업 무
김 학 남	한국정보교육원	Project Leader	프로젝트 총괄

2. 참여인력 업무분장

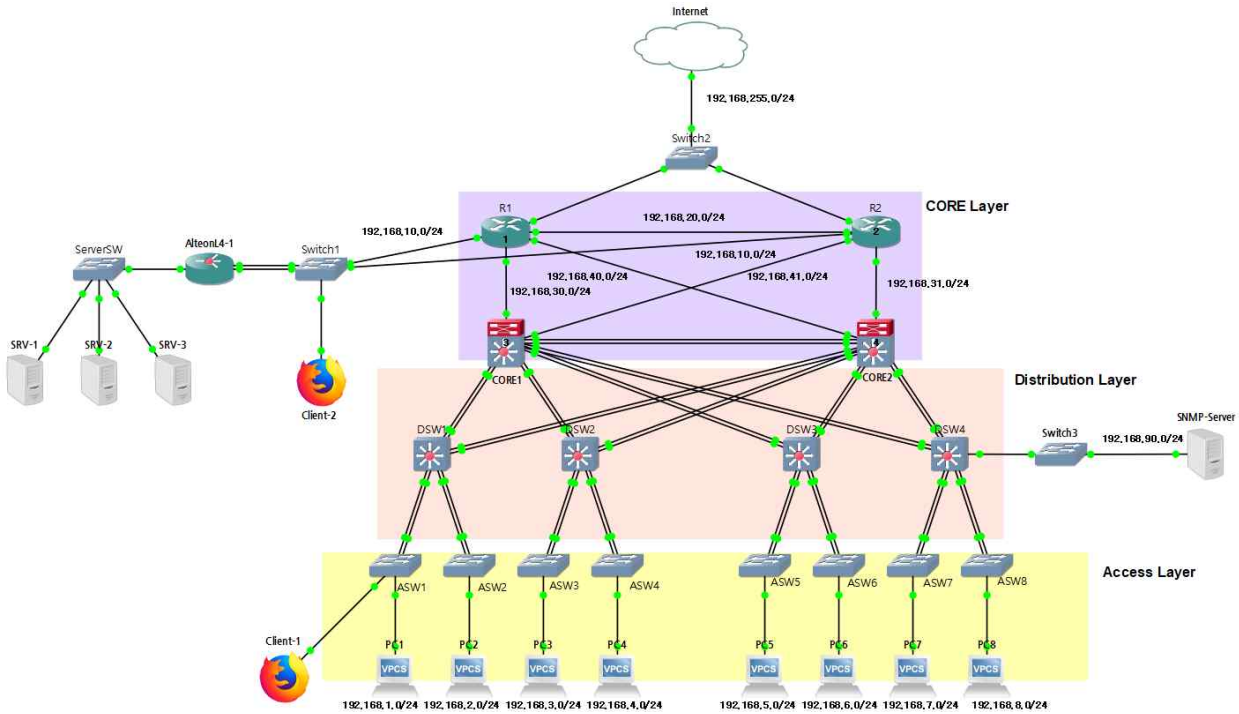
업무명	업무내용
PM	- 프로젝트 수행 관리 및 책임 - 프로젝트 범위, 인원, 일정, 결과 보고 - 프로젝트 진행 상황에 따른 계획 조정 - 기타 서류, 보고서 작성 및 발표
3 Tier 서버/네트워크 설계/구축	- 서버 및 네트워크 Topology 구성 (부서별로 네트워크 분리) - 물리적 서버/네트워크 장비 수 산정 및 배분 - 서버 리소스 설정 및 관리 - OSPF Routing protocol - L2, L3 Switch에 VLAN 구성 - Routing 및 NAT 구축
DB서버 구축	- MariaDB 설치 및 환경 구성 - Zabbix 서버 구축
모니터링 설정	- Zabbix 서버 연동 - Zabbix 모니터링 설정
검토	- 고객사의 요구사항 충족 확인 - 구축에 따른 단계별 산출물 검토

프로젝트 완료 보고서		
프로젝트 주제	3 Tier Network 설계 및 NMS 소프트웨어 모니터링 구축	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.06.05

Ⅲ. 세부 프로젝트 내용

(1) 메인 토폴로지

3 tier Network 전체 토폴로지



- 부서별 VLAN 분리로 독립적인 네트워크 설정 및 이중화 구성으로 장애에도 연속성 유지
- 이중화 구성으로 장애시 다른 통로 통신으로 연속성 유지 및 네트워크 상태 확인 가능
- 세 대의 Web 서버와 Zabbix 모니터링 솔루션으로 최적화 및 장비 장애시 빠른 복구 가능
- NAT를 통해 외부망에서 내부 Web 서버의 서비스 이용 가능

(2) 상세 구축 및 구성내용

가상서버 구성 현황	
Hypervisor OS	VMWARE ESXi 6.7
Server OS	Rocky Linux 8.7
Server Disk	OS(root) : 20GB (운영)DATA(NFS) : 150GB / (DR)DATA(NFS) : 50GB
WEB	Nginx 1.14.1
WAS	Tomcat 10.1.7
DB	MariaDB 10.5
SELINUX	permissive 설정 (NFS사용으로 인한 권한 문제 발생 방지)
VM Name 체계	(운영 구분)_(용도) 조합 예) Prod1_WEB = 운영 1번 서버에 있는 WEB 서버
Hostname 체계	운영구분 : p(운영), r(DR) 서비스코드 : you(통일) 용도 : wb(WEB), ap(WAS), db(DB) OS구분 : l (linux) (운영구분 1자리)+(서비스 코드 3자리)+(용도 2자리)+(OS구분1자리)+(체번 1자리) 조합 예) pyouwbl1 = OS가 리눅스인 운영 웹 1번 서버
예외	NFS와 Zabbix는 구분을 위해 호스트명에 서비스명 그대로 사용

※ IP표기 형식 (내부망 / NAT망)

Link Aggregation

```
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)
```

- VLAN을 통한 연결로 인한 모든 트래픽은 링크를 공유하며 통신. 이로 인해 성능 최적화 및 대역폭 문제 발생
- 2개의 Link를 연결하여 두 인터페이스를 하나의 논리적 인터페이스로 묶어서 트래픽을 각 포트에 분산
- 스위치 사이 Etherchannel 구성으로 1개의 회선이 끊어져도 다른 회선으로 대체할 수 있어 네트워크 장애를 예방

VLAN

```
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
```

- 각 부서마다 다른 VLAN을 부여하여 부서별 독립적인 네트워크 환경 구성
- 고객사 전체 네트워크에서 Broadcast Domain을 분할 (논리적인 IP 대역 분할)
- 부서 할당 VLAN : 10 ~ 80
- VLAN 100은 관리용

Trunk

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

Port        Mode             Encapsulation  Status        Native vlan
Po10        on               802.1q         trunking      1
Po11        on               802.1q         trunking      1
Po12        on               802.1q         trunking      1
Po13        on               802.1q         trunking      1
Po14        on               802.1q         trunking      1

Port        Vlans allowed on trunk
Po10        1-4094
Po11        1-4094
Po12        1-4094
Po13        1-4094
Po14        1-4094

Port        Vlans allowed and active in management domain
Po10        1,10,20,30,40,50,60,70,80,100
Po11        1,10,20,30,40,50,60,70,80,100
Po12        1,10,20,30,40,50,60,70,80,100
Po13        1,10,20,30,40,50,60,70,80,100
Po14        1,10,20,30,40,50,60,70,80,100

Port        Vlans in spanning tree forwarding state and not pruned

Port        Vlans in spanning tree forwarding state and not pruned
Po10        1,10,20,30,40,50,60,70,80,100
Po11        1,10,20,100
Po12        1,30,40,100
Po13        1,100
Po14        1,100
```

- SW(포트) 간 Trunk 설정
- 서로 다른 VLAN 간 통신 가능
- 스위치 간 연결되어 있는 회선 Trunk 설정

VTP

```
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
```

- Cisco 전용
- 연결된 스위치끼리 VLAN 정보를 자동으로 주고 받아 동기화를 하는 프로토콜 (CISCO 전용)
- CORE1, CORE2 SW를 VTP Server mode로 정하여 VLAN 정보를 직접 생성 및 전송
- 나머지 SW는 VTP Client mode로 설정하여 같은 Domain에 PW가 설정된 VTP Server로부터 VLAN 정보를 받아 저장. 직접 VLAN 정보를 저장할 수 없음

VLAN Access mode

```
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
```

- 각 부서와 연결되어 있는 SW에 부여된 VLAN을 Access mode 설정하여 VLAN이 동일한 포트끼리만 데이터 전달을 허용
- Unicast, Multicast, Broadcast 프레임이 동일한 VLAN으로 설정된 포트로만 전달될 수 있음

Portfast, BPDUfilter, Root Guard

```
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 SW에 설정
- Portfast : 해당 인터페이스는 Listening, Learning 상태를 거치지 않고 "no shutdown" 입력 시 "UP" 상태로 변경.
- BPDUfilter : 종단 장치엔 BPDU를 송신할 필요가 없어서 BPDU를 보내지 않는다.
- Root Guard : 더 낮은 값의 Bridge-ID를 담은 BPDU를 수신하면 해당 포트를 Down하여 Root SW 선출에 참여하지 못하도록 막음

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
```

- Access SW에 설정
- 해당 포트에 학습할 수 있는 최대 MAC주소를 2개로 제한 (MAC Flooding Attack, ARP spoofing 방지)
- restrict : 위반 장비의 통신을 차단하고 Log를 남김
- aging time (Mac address-table 갱신 주기) : 5분
- Inactivity : aging time동안 데이터 트래픽이 없는 경우 등록된 MAC주소 삭제

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
```

- 스위치 이중화 구조를 구성했을 때 발생하는 Loop 차단 (장비에 이상이 발생하여 작동을 멈추더라도 네트워크는 끊어지지 않고 계속 동작하기 때문이다)
- 스위치에 특정 포트를 차단하여 Loop 구조를 막음
- VLAN 10~40, 100 : MST1 instance로 묶어서 CORE1 SW를 Root SW로 선정
- VLAN 50~80 : MST2 instance로 묶어서 CORE2 SW를 Root SW로 선정
- 아래 사진은 DSW1의 spanning-tree이다. 만약 CORE1 SW에 작동 이상이 발생하면 CORE2 SW와 연결되어 있는 DSW1의 po15는 Alternative port에서 Root port로 바뀌고 Listening 상태로 변경.

다) VMWARE Network 구성

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
bpduguard                    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--
```

- 스위치에서 포트에 대한 장애 및 에러 유무를 주기적으로 모니터링하여 에러가 발생하면 자동으로 포트가 Errdisabled 상태로 변경되어 Shutdown
- Shutdown 되었을 때 300초 후 자동으로 포트 활성화를 하는 설정을 추가
- 에러 해결이 안될 시 shutdown 유지

Router SLA, Track

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

ID           Type        Destination       Stats       Return      Last
                                           (ms)        Code        Run
---------------------------------------------------------------------
*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 (millisecs) 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. ICMP Check를 사용하여 다른 네트워크의 성능을 확인
- Track : 장비 내에서 발생하는 이벤트를 추적, 감지하고 그에 대한 동작을 수행. 여기선 Router에서 외부 인터넷으로의 경로를 추적 및 감지
- Router에서 외부 인터넷과 연결되는 경로에 IP SLA, Track 설정하여 경로 감지

CORE SW SLA, Track

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

ID           Type        Destination       Stats       Return      Last
                                           (ms)        Code        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
```

```
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 (millisecs) 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 (millisecs) 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
```

- CORE SW에서 각각 R1, R2로 향하는 경로를 ICMP Check로 감지 및 성능 체크
- 두 SLA를 각 Track으로 만든 후 Track list boolean 설정
- 만약 CORE1 SW에서 R1, R2로 packet을 보내지 못하는 장애가 발생하면 HSRP로 인해 다른 CORE SW가 게이트웨이 역할을 담당

Router HSRP (CISCO전용)

```
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 이중화로 만약 한 경로에 문제가 생겼을 때 다른 경로에서 계속 게이트웨이 역할을 해줄 수 있는 가상 게이트웨이 설정
- Alteon LoadBalancer와 연결되어 있는 Web 서버의 게이트웨이를 R1과 R2 대상으로 HSRP를 설정하여 가상 게이트웨이로 지정
- R1을 Active 상태, R2를 Standby 상태로 설정. 만약 R1 경로에 이상이 발생하면 R2가 Active 상태로 변경되어 게이트웨이 역할 수행

CORE SW HSRP (CISCO전용)

```
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 종단 장비 게이트웨이를 CORE1과 CORE2를 묶어 하나의 가상 게이트웨이를 설정
- VLAN 10~40, 100은 CORE1이 게이트웨이 역할을 수행
- VLAN 50~80은 CORE2가 게이트웨이 역할을 수행

OSPF

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

O 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
O 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
O 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
O 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
O 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
O 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
O 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
O 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
O     192.168.31.0/24 [110/20] via 192.168.20.2, 01:58:29, GigabitEthernet0/2
O     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
O 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
O IA     192.168.90.12/32
           [110/11] via 192.168.20.2, 01:58:29, GigabitEthernet0/2
```

- 경로 장애가 발생했을 때 수동으로 경로를 수정하는 Static Routing이 아닌 Dynamic Routing OSPF protocol로 사용
- 링크 상태를 확인하여 최단 경로를 찾는 알고리즘(SPF)을 통해 확인된 최단 경로를 바탕으로 packet을 전달
- Area를 통해 OSPF 네트워크를 더 작은 영역으로 나눠 대규모 네트워크에 적합한 운영 가능

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)
```

- Router와 CORE SW가 연결되어 있는 회선에 Area 0(Backbone area)를 설정
- Loopback IP, 그리고 Alteon LoadBalancer와 연결되어 있는 회선에 각각 다른 area를 부여 (총 3개의 area)
- Backbone area로 인해 서로 다른 area 간 통신 가능

Totally NSSA area

```
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
```

- Router에 다른 Routing protocol로 동작하는 장치가 추가되는 것을 고려하여 Totally NSSA를 선언
- 만약 추가되면 LSA type 5가 type 7으로 변경되어 backbone area를 거치지 않더라도 경로 전보 전달이 가능
- 그 후 NSSA ABR이 다시 LSA type 7를 type 5로 변경 후 area 0으로 광고

NAT (PAT)

```
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  ---                ---
```

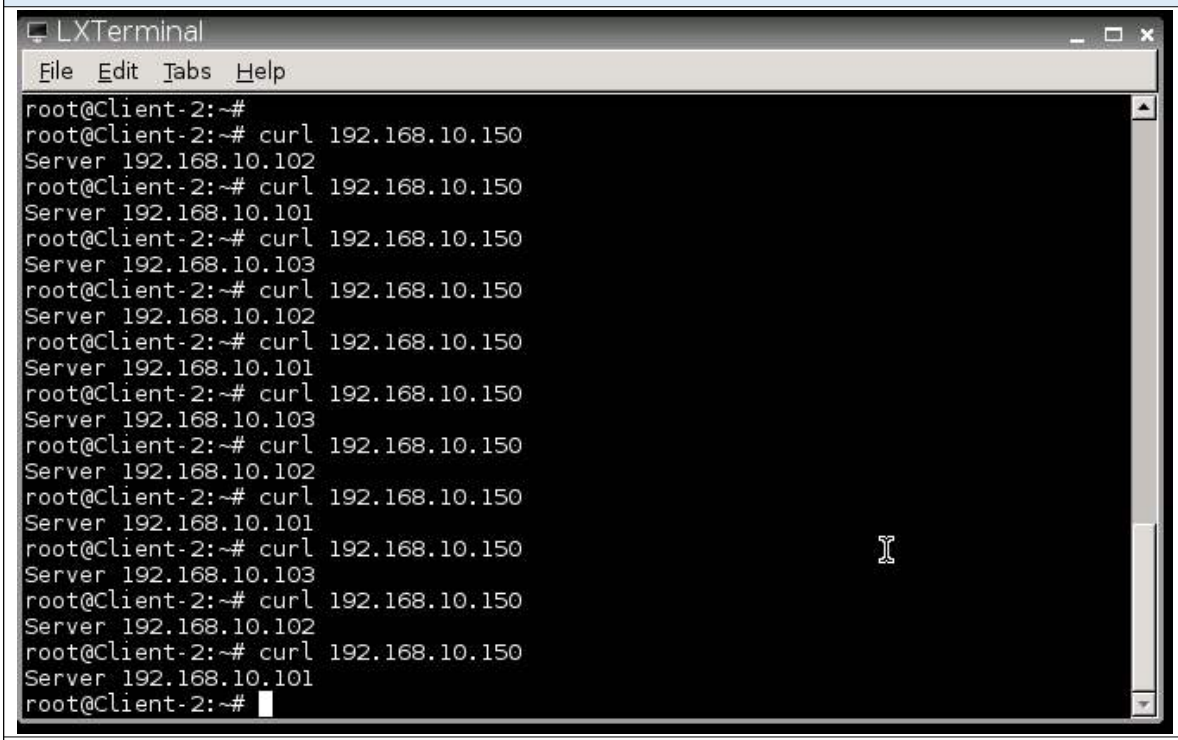
- NAT를 설정하여 외부망에서 내부 네트워크의 경로 정보를 알 수 없음
- 내부 사설 네트워크에 속한 여러 사용자가 하나의 공인 IP주소를 사용하여 외부 인터넷에 접속
- Port Forwarding : 어떠한 IP주소와 포트 번호의 통신 요청을 다른 IP 포트 번호로 넘겨줌
- 외부망에서 내부 사설 네트워크에 상주하는 Web 서버 호스트에 대한 서비스 생성 가능
- 192.168.10.150 주소는 Web 서버 3대의 그룹 대표 IP주소

Telnet

```
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
```

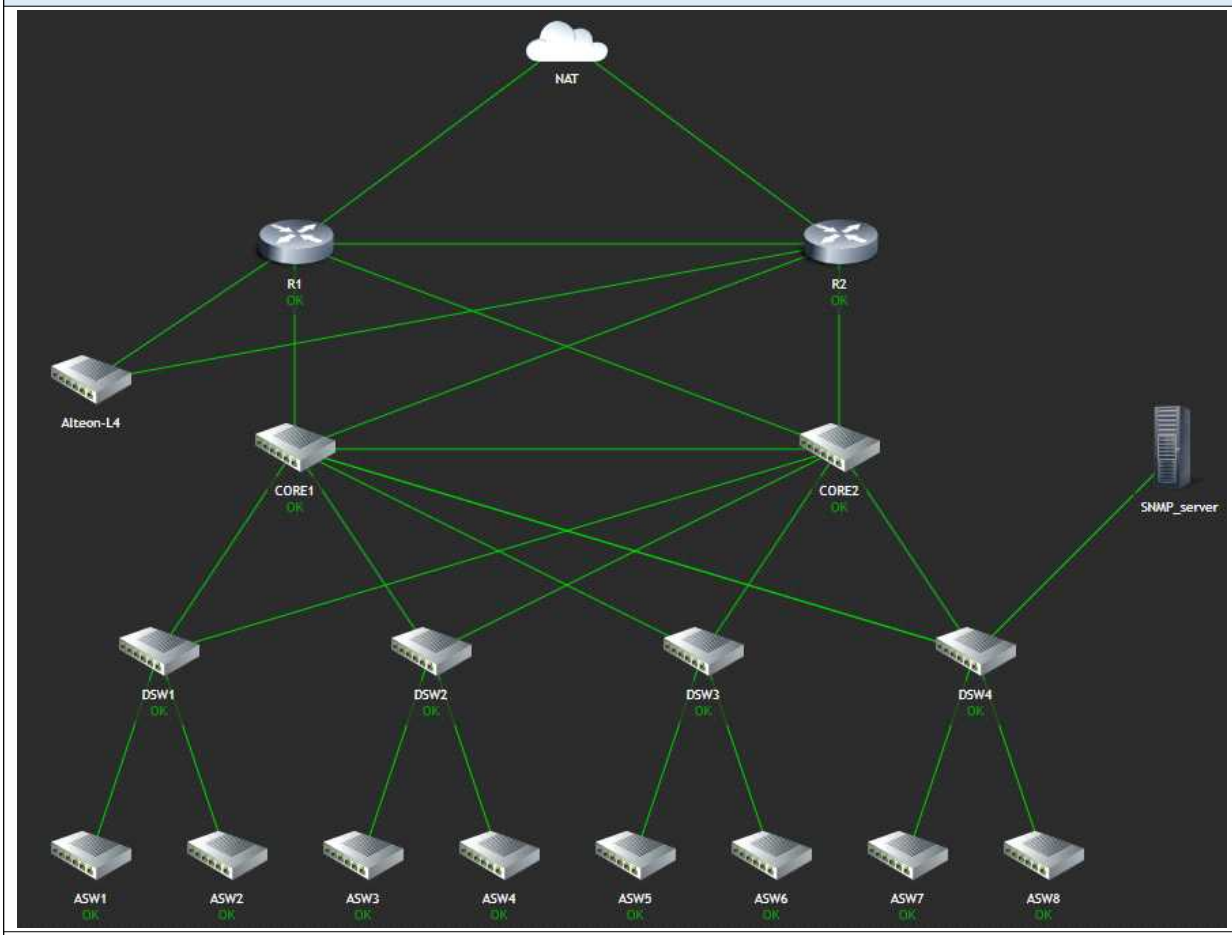
- 내부 장비를 관리하기 위해 각 장비에 원격으로 접속할 필요가 있음
- 설정한 관리용 IP 대역으로만 장비에 원격 접속을 허용
- 다른 내부 IP로는 원격 접속 불가능
- 오로지 내부 사설 IP대역으로 작동하는 내부 장비만 원격 접속하여 관리할 예정이기 때문에 SSH 대신 Telnet 사용

LoadBalancing



- L4 Alteon 장비를 이용해 Web 서버에 부하분산
- 한 대의 서버로 부하가 집중되지 않고 각 세 대의 서버에 트래픽을 분산하여 관리
- 만약 Scale-Out 방식으로 서버를 증설한다면 LoadBalancing 반드시 필요
- Round-Robin 방식을 사용하여 서버에 들어온 요청을 순서대로 들어가며 배정
- Real server group 가상 IP로 통신을 보냈더니 각 서버가 순서대로 응답

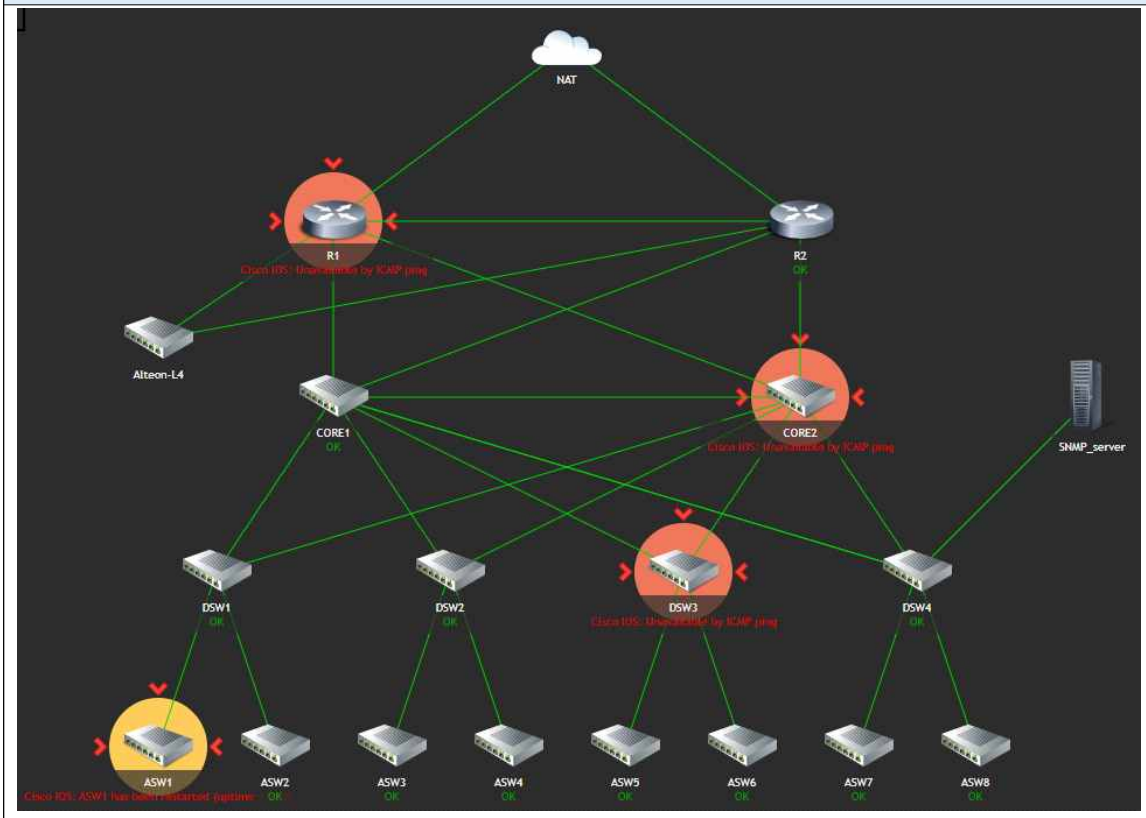
Zabbix(NMS SW)를 이용한 모니터링



- Zabbix는 분산 모니터링 솔루션
- IP 기반으로 네트워크 상의 각 호스트 장비로부터 정기적으로 여러 관리 정보를 자동으로 수집하거나 실시간으로 상태를 모니터링 및 설정
- PHP로 구현된 Apache 기반 웹브라우저 지원
- 위 Zabbix Map를 통해 장비의 전체적인 구성을 가시적으로 쉽게 확인 가능

프로젝트 완료 보고서		
프로젝트 주제	3 Tier Network 설계 및 NMS 소프트웨어 모니터링 구축	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.06.05

Zabbix(NMS SW)를 이용한 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	17:46:35	RESOLVED		ASW6	Cisco IOS: High ICMP ping loss	58s	No		class: network component: health component: network
17:45:34	High	17:46:33	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	17:44:35	RESOLVED		ASW6	Cisco IOS: Unavailable by ICMP ping	1m	No		class: network component: health component: network
17:43:35	High	17:44:35	RESOLVED		ASW5	Cisco IOS: Unavailable by ICMP ping	1m	No		class: network component: health component: network
17:43:29	High	17:46:29	RESOLVED		DSW3	Cisco IOS: Unavailable by ICMP ping	3m	No		class: network component: health component: network
17:43:26	High	17:46:25	RESOLVED		CORE2	Cisco IOS: Unavailable by ICMP ping	2m 59s	No		class: network component: health component: network
17:43:21	High	17:46:21	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

- 장비에 장애가 발생한다면 해당 장비를 신속하고 쉽게 확인 가능
- 장애 발생한 호스트 장비에 관한 message 확인 가능

프로젝트 완료 보고서		
프로젝트 주제	3 Tier Network 설계 및 NMS 소프트웨어 모니터링 구축	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.06.05

Zabbix(NMS SW)를 이용한 모니터링

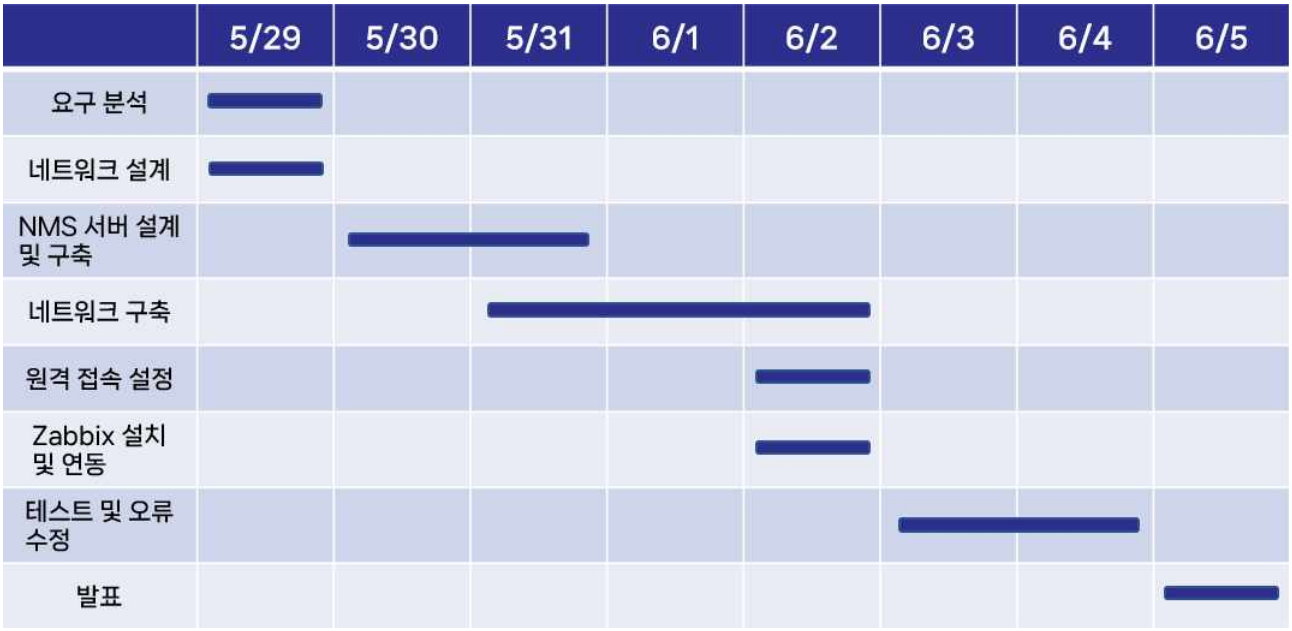
- 호스트 장비 간에 트래픽이 급증했을 경우 그래프 형태로 확인 가능
- ASW4에서 DSW2로 대량의 트래픽을 전송했을 때의 그래프

(3) 설치 및 설정된 운영환경 정보

구분	장비 및 소프트웨어	버전	기타
가상 플랫폼 소프트웨어	VMware WORKSTATION 16 PRO	16.2.1 build-18811642	
OS	Rocky	8.7	
DB	MariaDB	10.5.13-MariaDB	
WEB	Apache	V2.4.6	
	PHP	V7.4.26	
NMS	Zabbix		
하드웨어	Cisco Router Cisco L3/L2 Switch Load Balancer Alteon L4 Switch		

프로젝트 완료 보고서		
프로젝트 주제	3 Tier Network 설계 및 NMS 소프트웨어 모니터링 구축	
단계 : 프로젝트 완료	작성자 : 김학남	작성일 : 2023.06.05

Ⅳ. 프로젝트 일정



V. 유지보수 계획

(1) 유지보수 개요

■ 유지보수 방안 : 구축된 시스템의 유지관리를 위해 본 프로젝트 팀은 단계별 유지관리 계획을 유·무상 유지관리로 구분하고, 본 프로젝트 이후 안정화 단계를 거친 후 활용 및 개선 단계로 나누어 체계적인 관리가 되도록 다음과 같이 유지보수 방안을 수립한다.

(2) 유지보수 지원

2.1 무상 유지 보수 지원 :

- 무상유지보수 기간 : 검수 완료 후 한국정보교육원과 협의하여 정한 기간
- 무상유지보수 내역

지원분야	주요 지원 내용
시스템 안정화 지원	- 검수일로부터 1개월로 시스템 안정화를 위해 개발 및 구축에 참여한 실무 담당자 각 1명이 최소 1개월 이상 기술지원
원격점검 지원	- 원격 지원 시스템을 이용한 원격점검 지원
응급복구 지원	- 무상보수기간 동안 추가요청 사항이나 변경 사항이 발생할 경우 수정 보완 지원 - 시스템 장애가 발생한 경우 신고 후 4시간 이내 복구
유무선 지원	- 전화, Fax, 이메일 서비스 등 신속한 고객 응대를 통해 정확한 장애원인 판단 및 해결방안 제시 - Help Desk 운영

2.2 유상 유지 보수 지원 :

- 무상 보증기간 경과 후 1년 단위로 유지보수 계약을 체결한 경우에 한함
- 유상 유지보수 지원 내역은 무상 유지보수 지원 내역과 동일