NETWORK 사업 계획

SC제일은행의 IDC 내부 망 신축 및 전체 네트워크 망의 보안 강화를 위한 솔루션

COMPANY | JPL NETWORK

Standard Chartered SC제일은행

JPL NETWORK COMPANY
READER IN NETWORK SERVICE

INDEX

01
- ✓ JPL NETWORK 소개
- ✓ 조직도

02
- ✓ 사업 개요
- ✓ IDC 설립의 의의

03
- ✓ 네트워크 구성도
- ✓ 기술요약

04
- ✓ 내부 네트워크
- ✓ 공중망
- ✓ 보안 기술

05
- ✓ IP 할당 내역
- ✓ Configuration

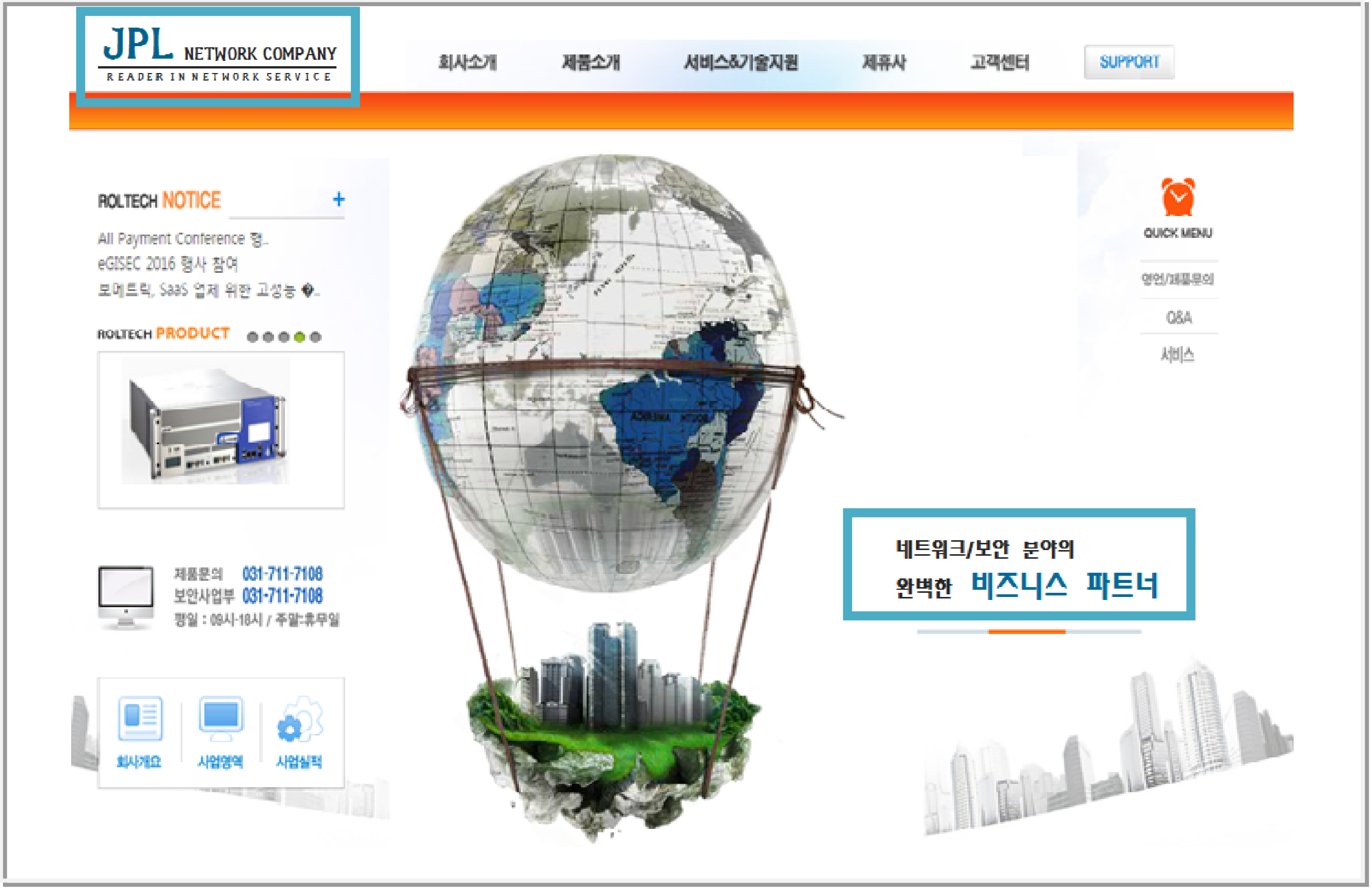
회사소개

01

✓ JPL NETWORK 소개

✓ 조직도

회사소개



All Payment Conference 행..

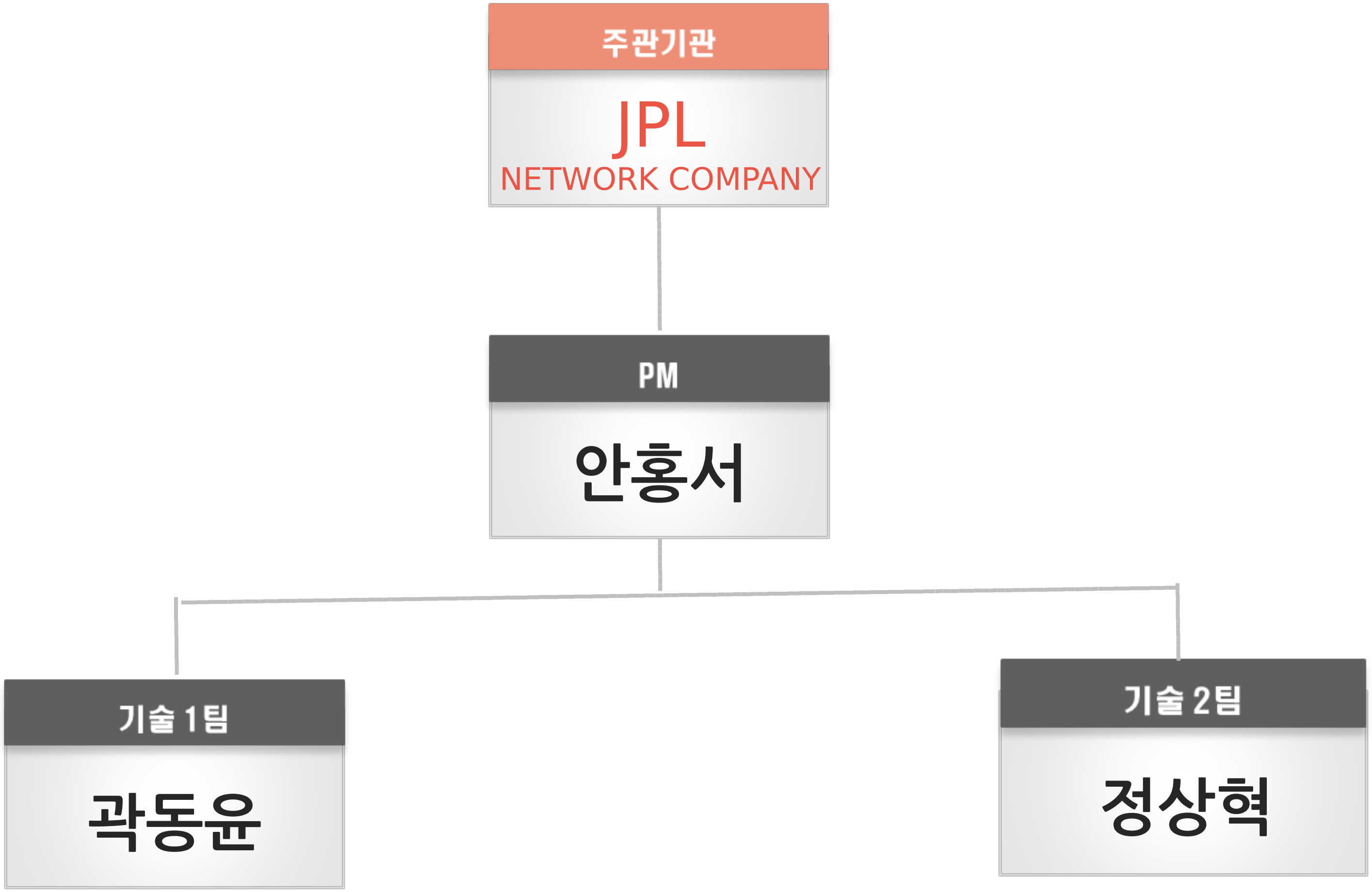
eGISEC 2016 행사 참여

보메트릭, SaaS 결제 위한 고성능 �..

제품문의 031-711-7108
보안사업부 031-711-7108
평일 : 09시-18시 / 주말:휴무일

네트워크/보안 분야의
완벽한 비즈니스 파트너

조직도



주관기관

JPL
NETWORK COMPANY

PM

안홍서

기술 1팀

곽동윤

기술 2팀

정상혁

사업 내용

02

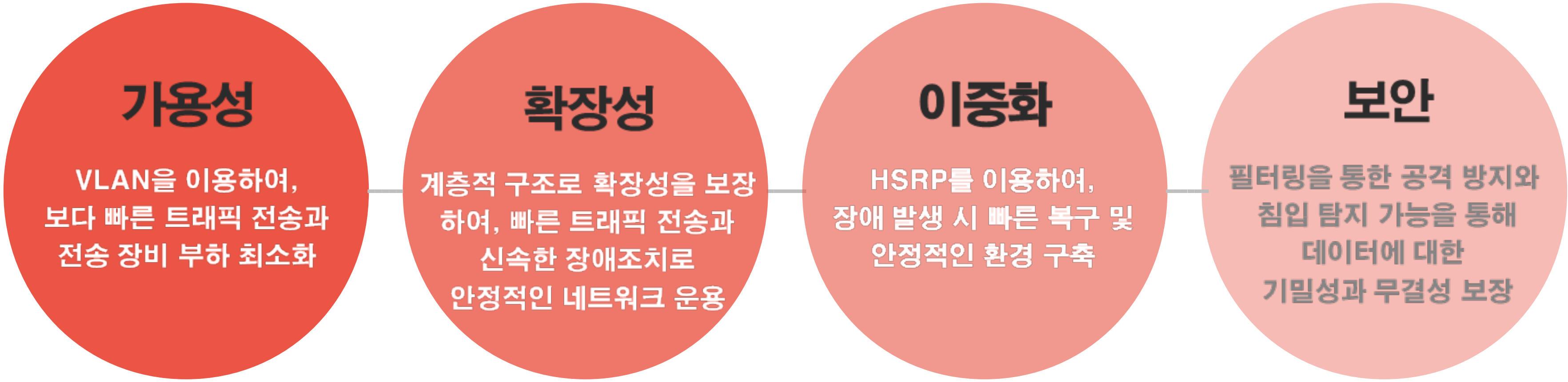
- ✓ 사업 개요
- ✓ IDC 설립의 의의

01 사업 개요

▷ 사 업 명 : SC 은행의 IT 데이터 센터 내부망 신축 및 전체 네트워크 보안 강화

▷ 일 정 : 2016.10.04 ~ 2016.10.11

▷ 목 적



가용성

VLAN을 이용하여, 보다 빠른 트래픽 전송과 전송 장비 부하 최소화

확장성

계층적 구조로 확장성을 보장하여, 빠른 트래픽 전송과 신속한 장애조치로 안정적인 네트워크 운용

이중화

HSRP를 이용하여, 장애 발생 시 빠른 복구 및 안정적인 환경 구축

보안

필터링을 통한 공격 방지와 침입 탐지 가능을 통해 데이터에 대한 기밀성과 무결성 보장

▷ 구축 범위

- **내부 네트워크 망 구축**
  - 이더채널, VTP, RSTP, SVI, Inter-vlan, EIGRP, Portfast, HSRP, Trunk

- **인터넷 망 구축**
  - OSPF
- **본사, 지사, 서버간 망 구축**
  - DMVPN/IPSEC

- **EZVPN**
- **TACACS+**
  - AAA/ACS
- **서버 구축**
  - Syslog, NTP, DHCP

- **방화벽 구축**
  - CBAC / ACL

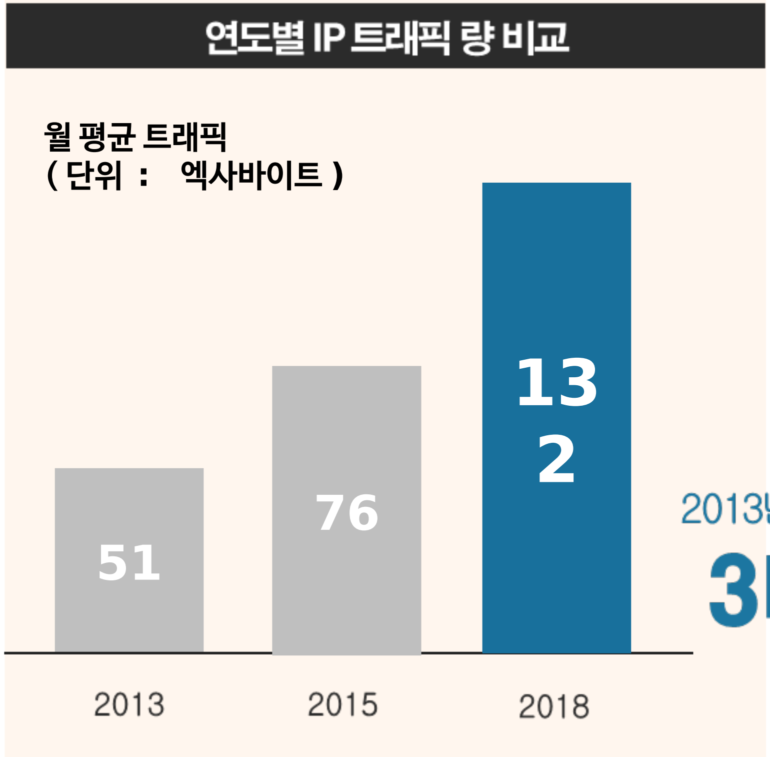
02 IDC 설립의 의의

IDC 의 필요성

개별적으로 관리, 운영하기에는 부담이 큰

서버 장비 및 통신 장비의 운영과 관리를 **집중화**

서비스의 안전성과 효율성 증대



2013년 대비 **3배** 증가 예상

자료출처 : 2013~2018 시스코 비주얼 네트워킹 인덱스 글로벌 전망 및 서비스 도입 보고서

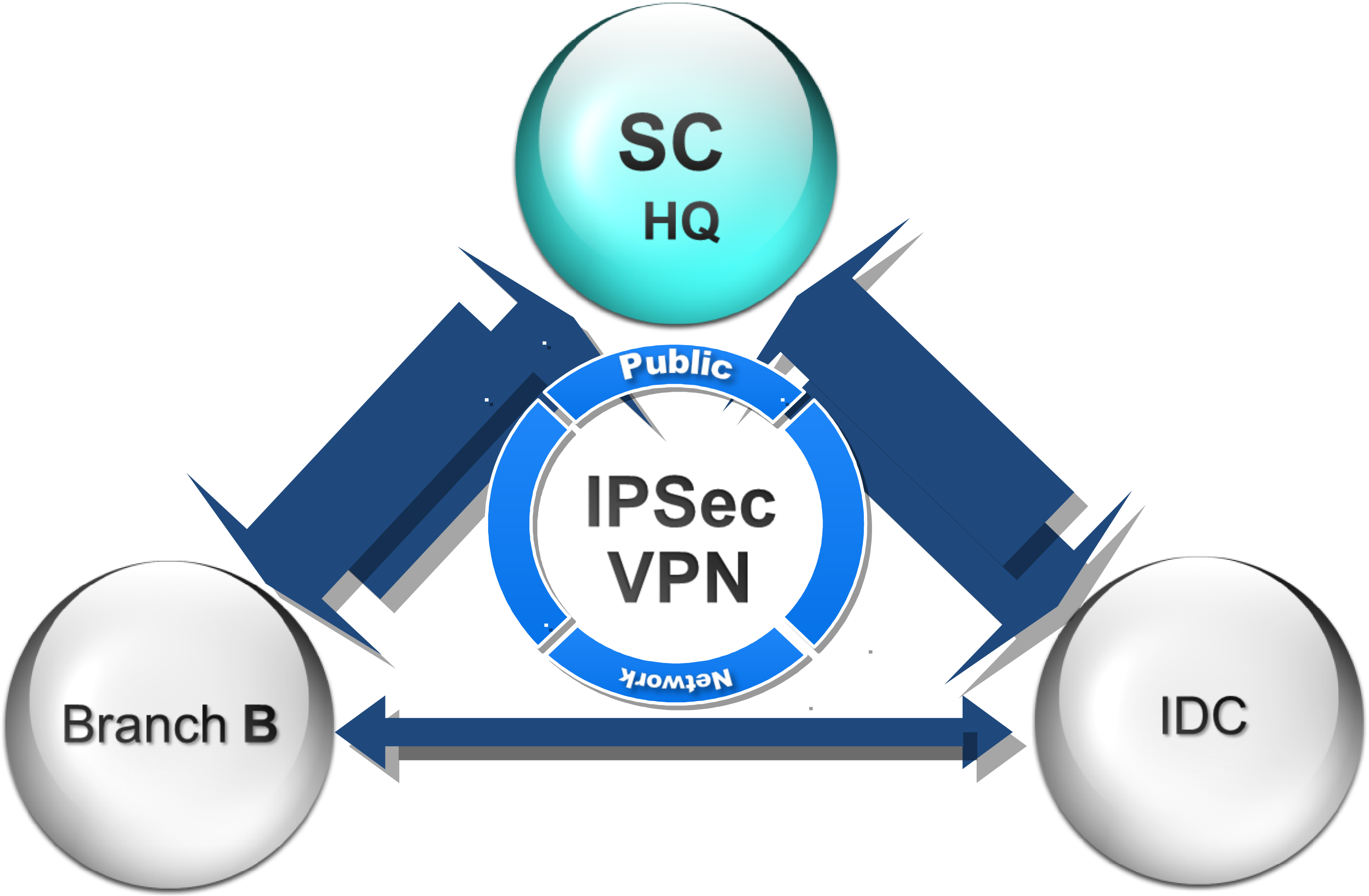
구축 내용

03

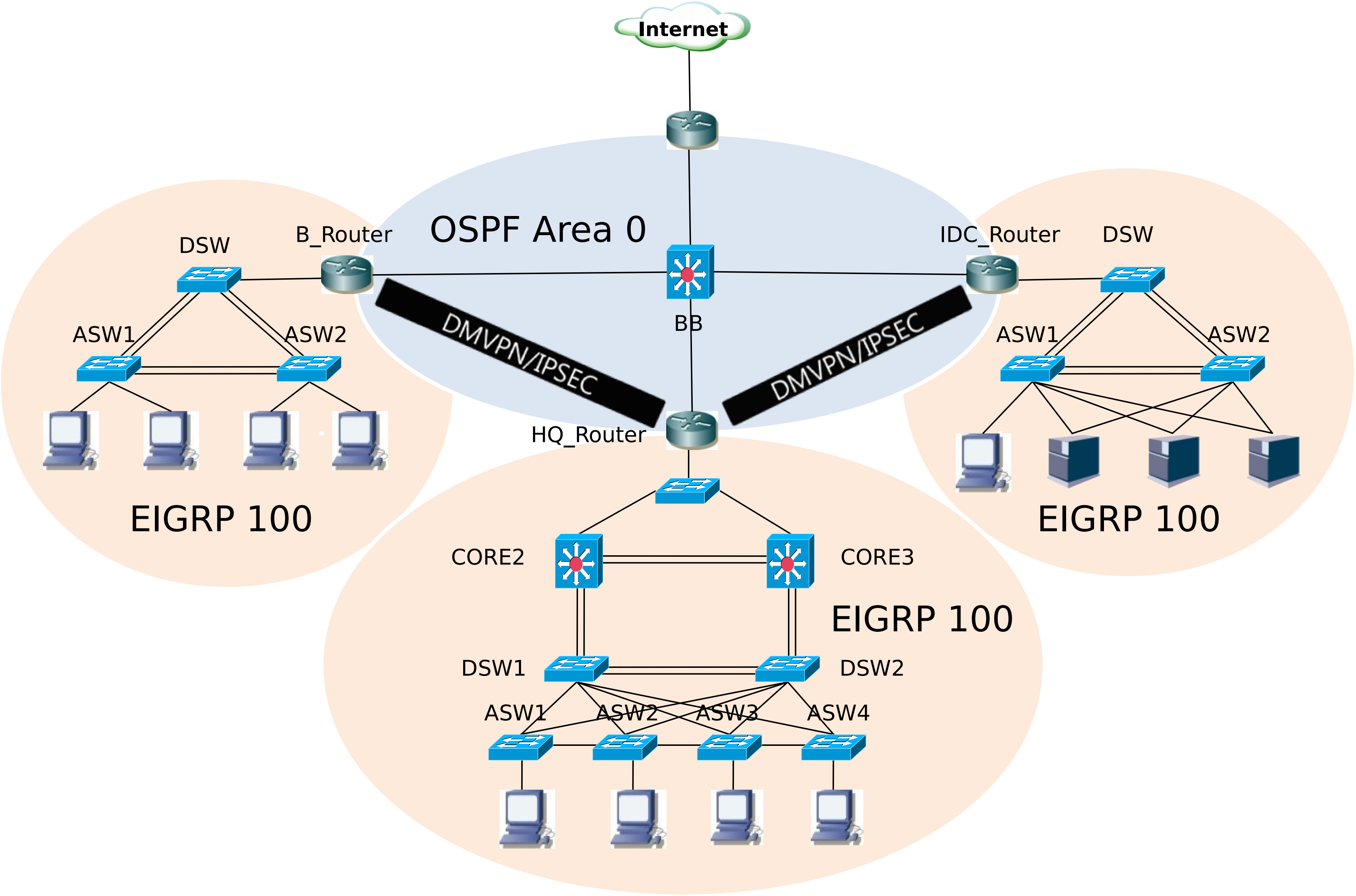
✓ 네트워크 구성도

✓ 기술 요약

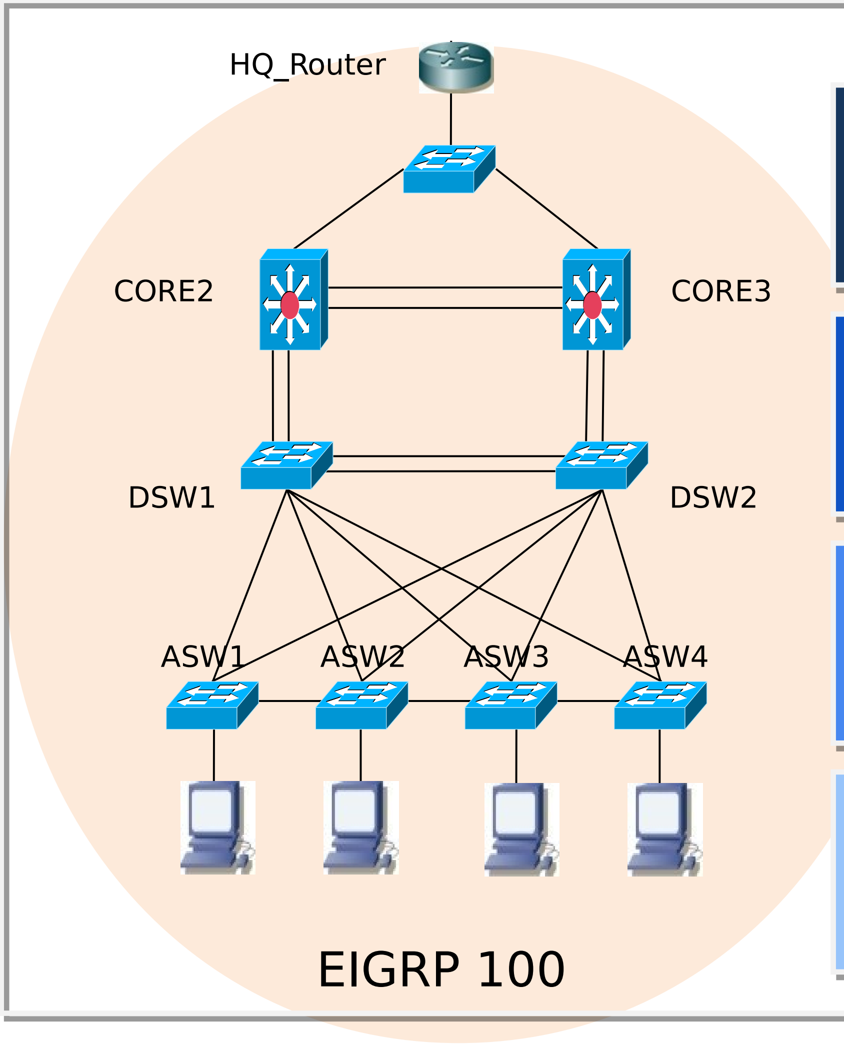
01 네트워크 구성도



01 네트워크 구성도

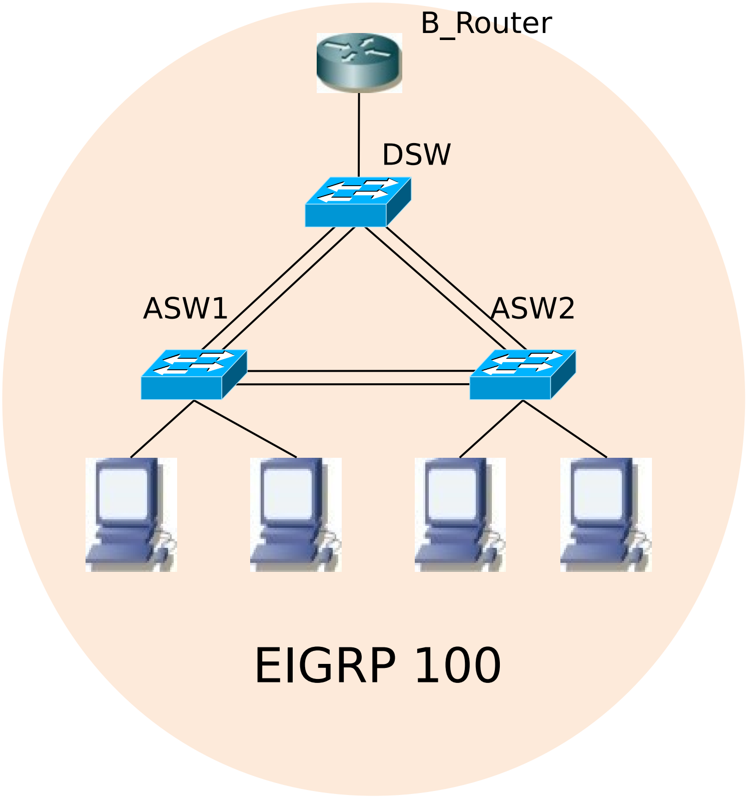

Internet
OSPF Area 0
B_Router
IDC_Router
DSW
DSW
BB
ASW1
ASW2
ASW1
ASW2
DMVPN/IPSEC
DMVPN/IPSEC
HQ_Router
EIGRP 100
EIGRP 100
CORE2
CORE3
EIGRP 100
DSW1
DSW2
ASW1
ASW2
ASW3
ASW4

(1) HQ



장비 구성	CISCO Router 2621xm 1EA CISCO Switch 3560 (L3) 2EA CISCO Switch 3560 (L2) 7EA
내부 구성	Basic config / Trunk / Etherchannel VTP / VLAN / Portfast / RSTP L3 Switch / SVI / HSRP EIGRP / PVST
외부 구성	OSPF DMVPN EZVPN
보안 구성	Syslog AAA/ACS CBAC IPSec

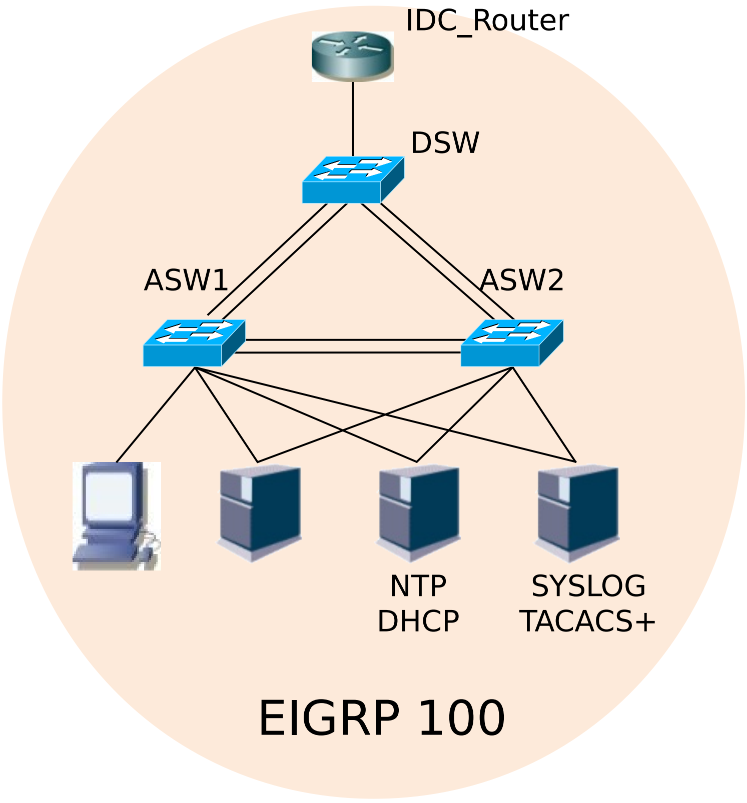
(2) Branch



장비 구성	CISCO Router 2621xm CISCO Switch 3560 (L2)	1EA 3EA
내부 구성	Basic config / Trunk / Etherchannel VTP / VLAN / Portfast / RSTP Inter-VLAN / EIGRP / PVST	
외부 구성	OSPF DMVPN EZVPN	
보안 구성	Syslog AAA/ACS CBAC IPSec	

(3) IDC

Internet Data Center



장비 구성	CISCO Router 2621xm 1EA CISCO Switch 3560 (L2) 3EA
내부 구성	Basic config / Trunk / Etherchannel VTP / VLAN / Portfast / RSTP Inter-VLAN / EIGRP / PVST Syslog / AAA / ACS / NTP / DHCP Server
외부 구성	OSPF DMVPN EZVPN
보안 구성	Syslog AAA/ACS CBAC IPSec

기술 내용

04

✓ 내부 네트워크

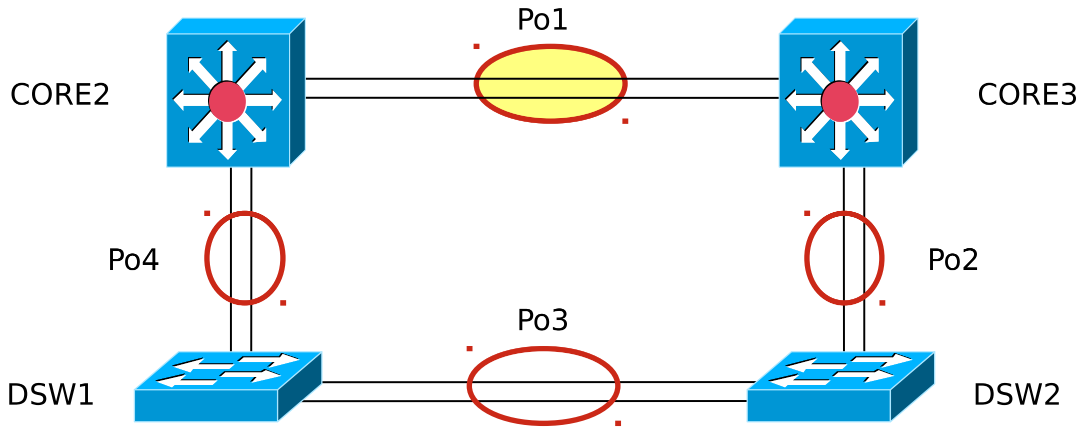
✓ 공중망

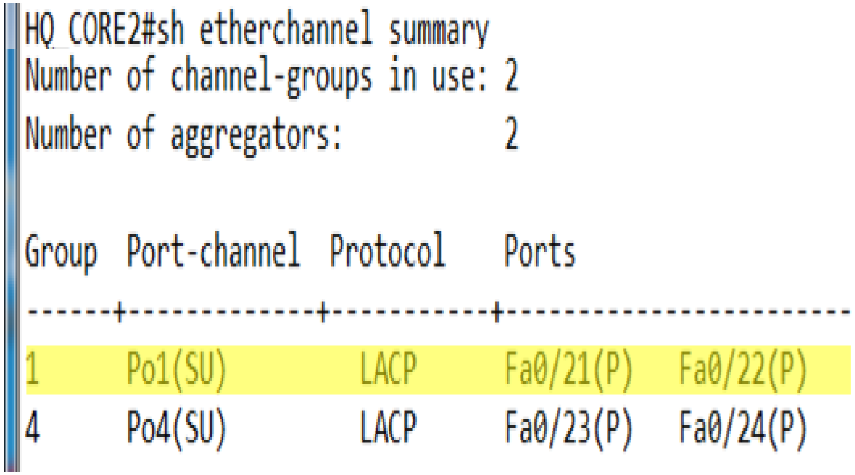
✓ 보안기술

Etherchannel

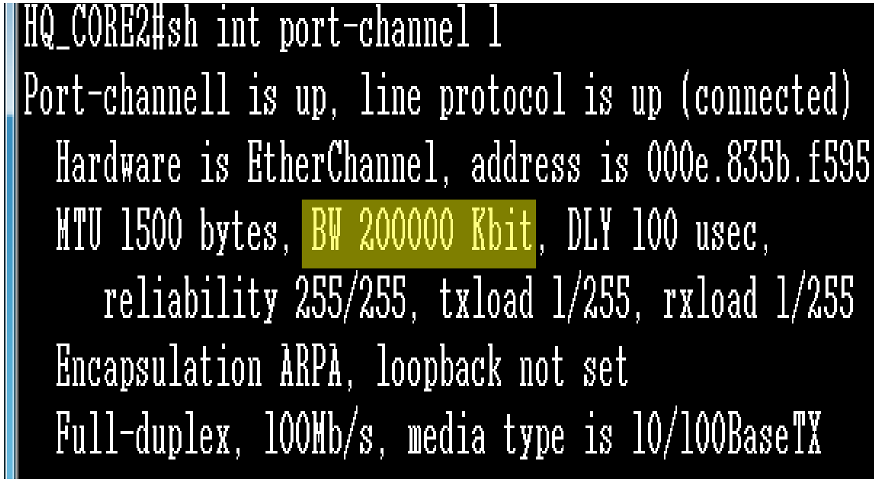
구현 목표

- 스위치간에 연결된 다수의 포트를 논리적인 하나의 포트로 구성
- 대역폭 확장 및 이중화 링크 구현





```
HQ_CORE2#sh etherchannel summary
Number of channel-groups in use: 2
Number of aggregators:           2

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------
1      Po1(SU)         LACP      Fa0/21(P)   Fa0/22(P)
4      Po4(SU)         LACP      Fa0/23(P)   Fa0/24(P)
```



```
HQ_CORE2#sh int port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is 000e.835b.f595
  MTU 1500 bytes, BW 200000 Kbit, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
```

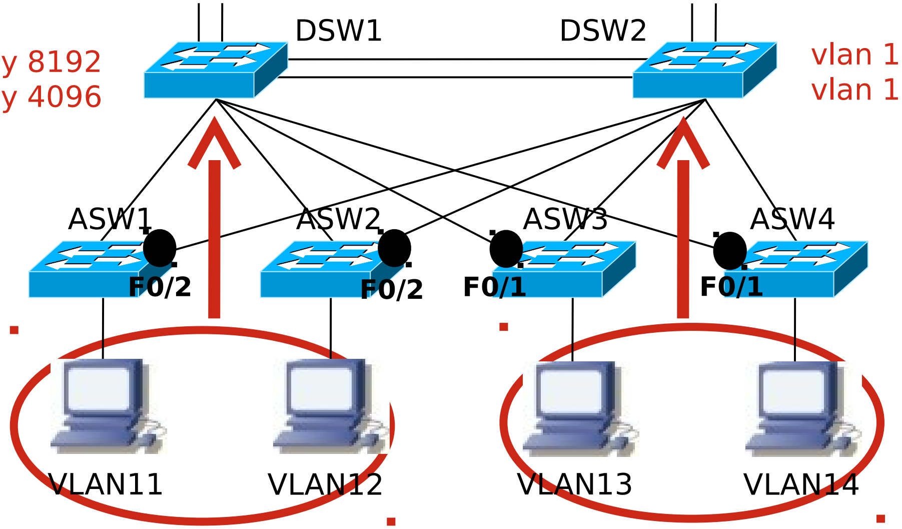
01 내부 네트워크기술 내용

PVST

Per Vlan Spanning Tree

구현 목표

- 각각의 VLAN에 STP를 지원함으로써 VLAN마다 서로 다른 루트 브리지 선출 가능
- VLAN 로드 분산 가능



vlan 11,12 priority 8192
vlan 13,14 priority 4096

vlan 11,12 priority 4096
vlan 13,14 priority 8192

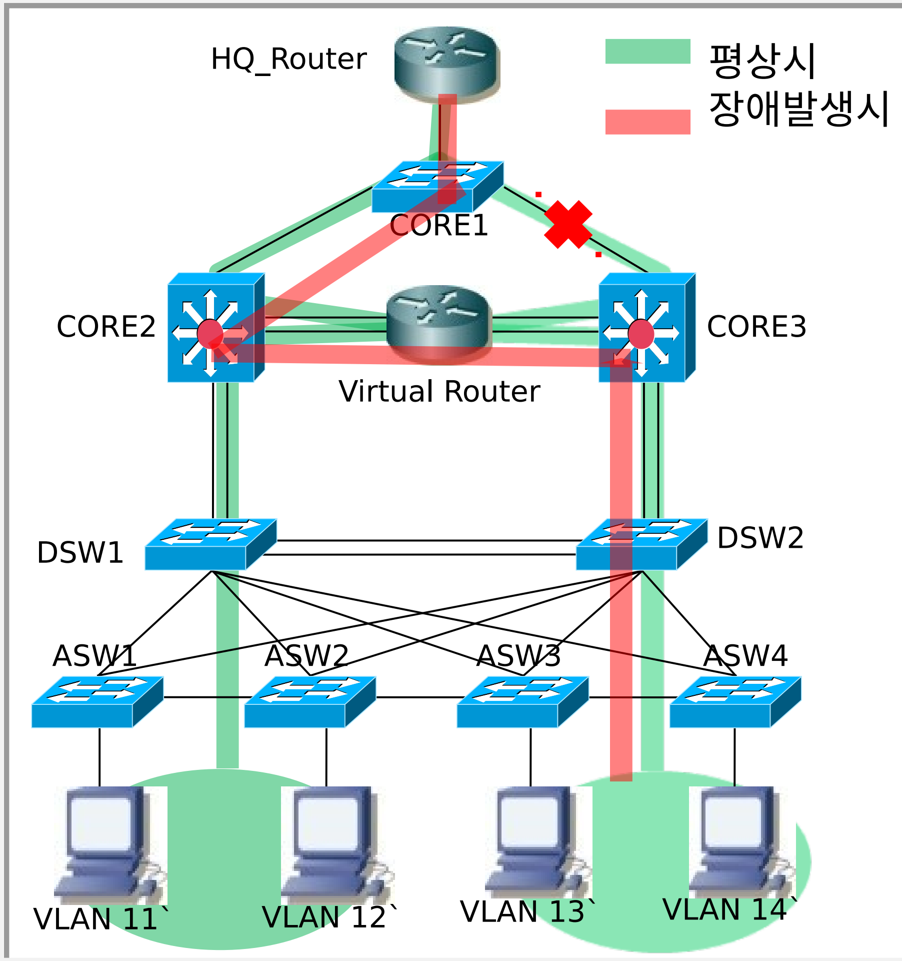
VLAN 11,12	Interface Role Sts Cost Prio.Nbr Type ------------------- ---- --- --------- -------- ------ Fa0/1 Root FWD 19 128.1 P2p Fa0/2 Altn BLK 19 128.2 P2p
VLAN 13,14	Interface Role Sts Cost Prio.Nbr Type ------------------- ---- --- --------- -------- ------ Fa0/1 Altn BLK 19 128.1 P2p Fa0/2 Root FWD 19 128.2 P2p

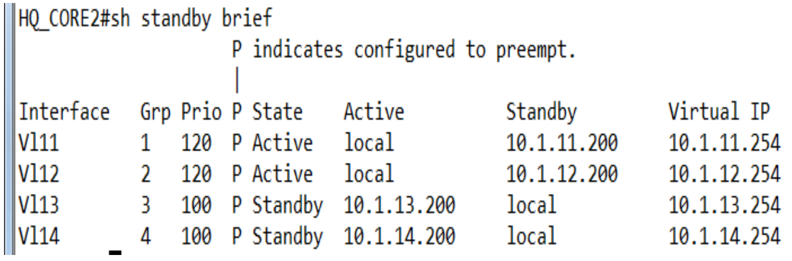
HSRP

Hot Standby Router Protocol

구현 목표

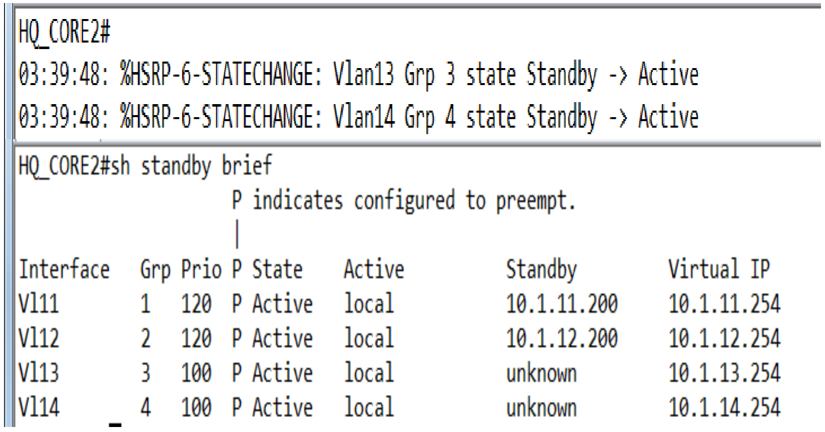
- 논리적인 가상 게이트웨이를 만들어 기존에 사용하고 있는 게이트웨이가 장애가 발생되면 , 대기하고 있는 다른 라우터가 게이트웨이를 수행
- 안정적인 네트워크 환경 구축





```
HQ_CORE2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State   Active          Standby         Virtual IP
Vl11        1   120  P Active  local           10.1.11.200     10.1.11.254
Vl12        2   120  P Active  local           10.1.12.200     10.1.12.254
Vl13        3   100  P Standby 10.1.13.200     local           10.1.13.254
Vl14        4   100  P Standby 10.1.14.200     local           10.1.14.254
```

평상시



```
HQ_CORE2#
03:39:48: %HSRP-6-STATECHANGE: Vlan13 Grp 3 state Standby -> Active
03:39:48: %HSRP-6-STATECHANGE: Vlan14 Grp 4 state Standby -> Active
```

```
HQ_CORE2#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State   Active          Standby         Virtual IP
Vl11        1   120  P Active  local           10.1.11.200     10.1.11.254
Vl12        2   120  P Active  local           10.1.12.200     10.1.12.254
Vl13        3   100  P Active  local           unknown         10.1.13.254
Vl14        4   100  P Active  local           unknown         10.1.14.254
```

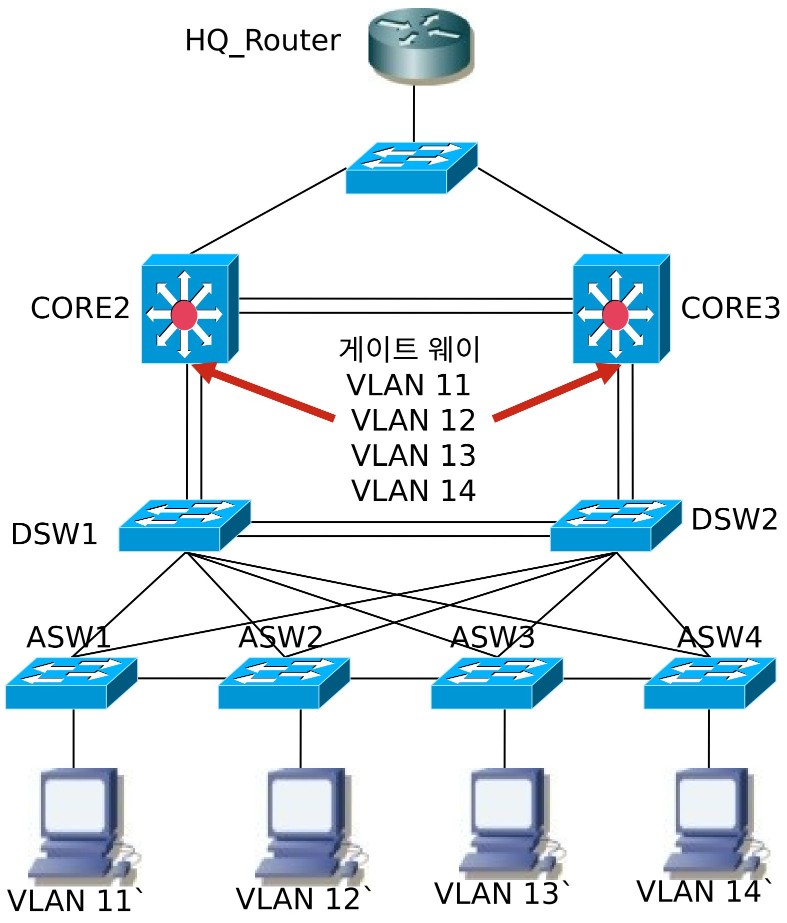
장애 발생시

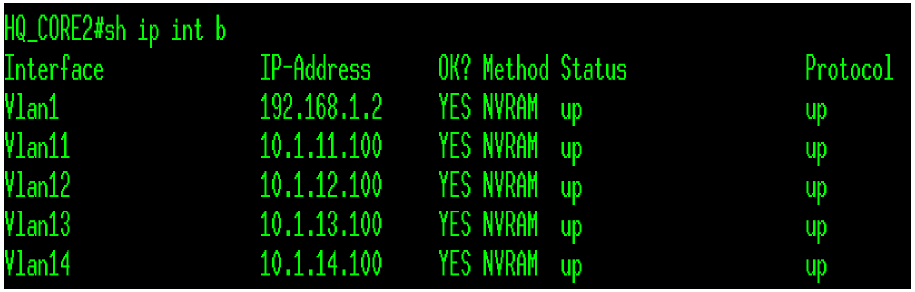
SVI

Switch Virtual Interface

구현 목표

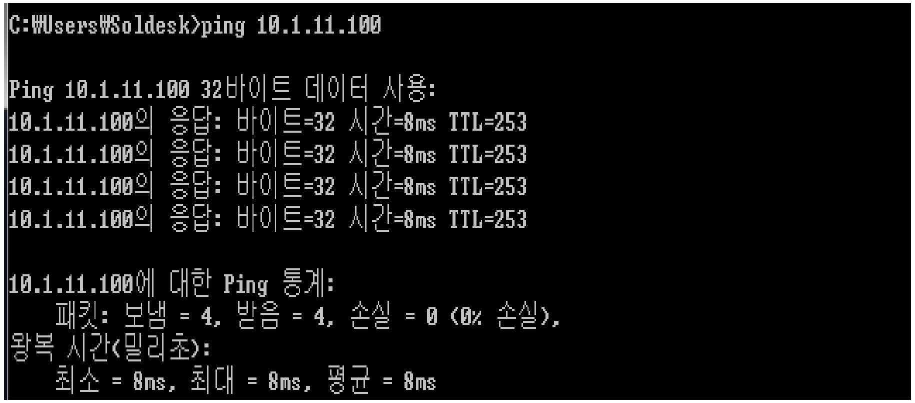
- L3 스위치는 동일한 VLAN 포트간에 스위칭기능을 제공하고 서로다른 VLAN 포트간에는 라우팅 기능을 제공
- VLAN 간의 라우팅을 위해서는 L3 스위치가 효과적





```
HQ_CORE2#sh ip int b
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.2     YES NVRAM  up                    up
Vlan11                 10.1.11.100     YES NVRAM  up                    up
Vlan12                 10.1.12.100     YES NVRAM  up                    up
Vlan13                 10.1.13.100     YES NVRAM  up                    up
Vlan14                 10.1.14.100     YES NVRAM  up                    up
```

L3 스위치 각 VLAN 에 대한 게이트웨이 설정



```
C:₩Users₩Soldesk>ping 10.1.11.100

Ping 10.1.11.100 32바이트 데이터 사용:
10.1.11.100의 응답: 바이트=32 시간=8ms TTL=253
10.1.11.100의 응답: 바이트=32 시간=8ms TTL=253
10.1.11.100의 응답: 바이트=32 시간=8ms TTL=253
10.1.11.100의 응답: 바이트=32 시간=8ms TTL=253

10.1.11.100에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 8ms, 최대 = 8ms, 평균 = 8ms
```

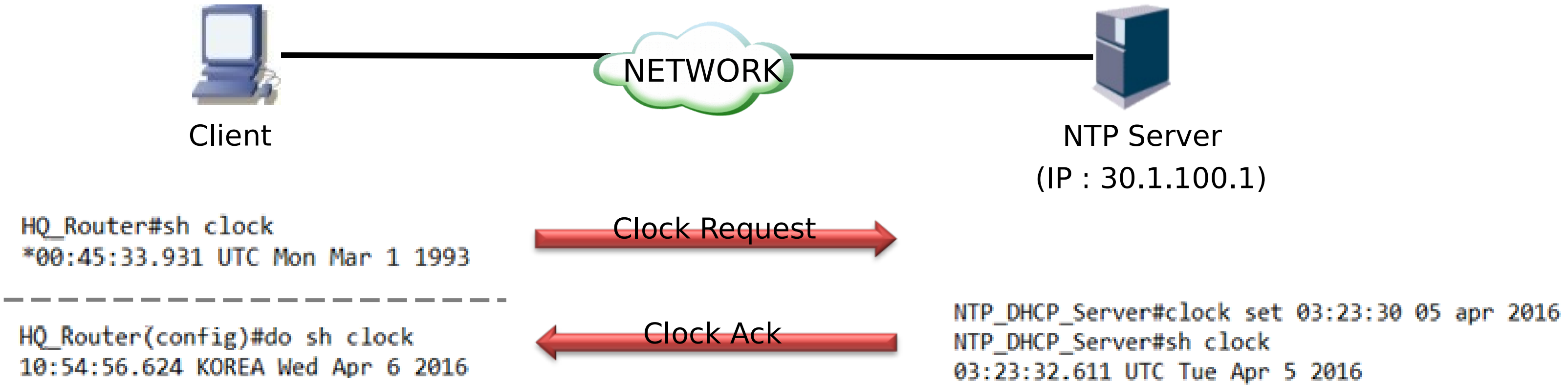
PC(VLAN 11) 에서 게이트웨이 (VLAN11) Ping Test

01 내부 네트워크 기술 내용_Server

NTP
Network Time Protocol

구현 목표

- 지사(IDC)에서 NTP 정보를 받아 동기화
- 네트워크의 시스템 관리 및 로그분석을 원활히 진행할 수 있음

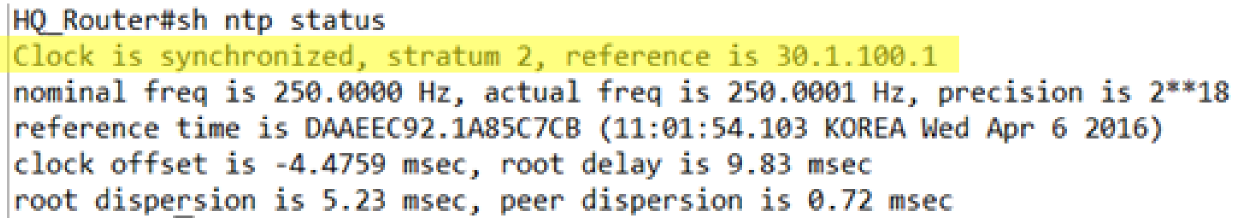


```
HQ_Router#sh clock
*00:45:33.931 UTC Mon Mar 1 1993
```

```
HQ_Router(config)#do sh clock
10:54:56.624 KOREA Wed Apr 6 2016
```

```
NTP_DHCP_Server#clock set 03:23:30 05 apr 2016
NTP_DHCP_Server#sh clock
03:23:32.611 UTC Tue Apr 5 2016
```

NTP 동기화 현황



```
HQ_Router#sh ntp status
Clock is synchronized, stratum 2, reference is 30.1.100.1
nominal freq is 250.0000 Hz, actual freq is 250.0001 Hz, precision is 2**18
reference time is DAAEEC92.1A85C7CB (11:01:54.103 KOREA Wed Apr 6 2016)
clock offset is -4.4759 msec, root delay is 9.83 msec
root dispersion is 5.23 msec, peer dispersion is 0.72 msec
```

01 내부 네트워크 기술 내용_Server

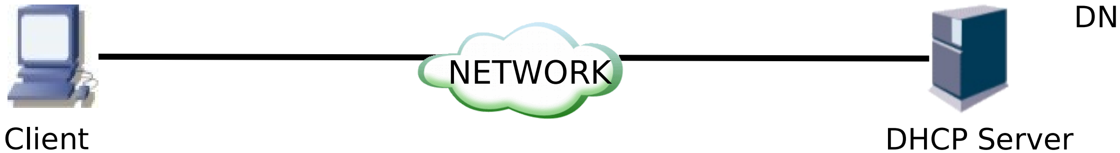
DHCP

Dynamic Host Configuration Protocol

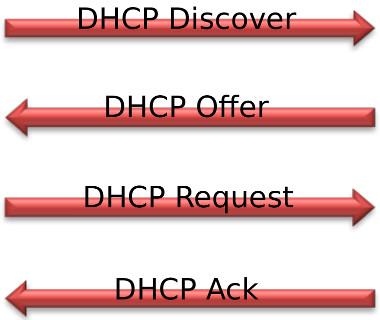
구현 목표

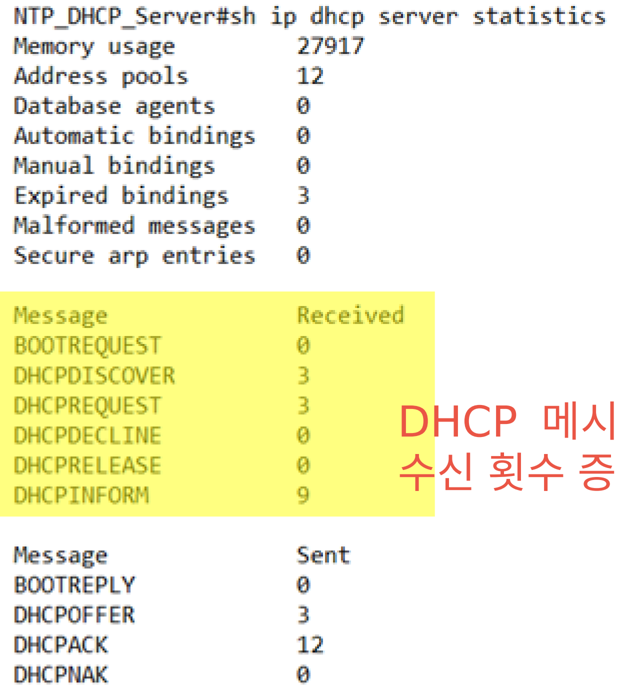
- 서버에서 IP를 관리하고 각각의 호스트에게 고유의 IP 자동 할당
- IP 임대 개념으로, 필요 시 동적으로 네트워크 재구성 가능

DNS 서버 : 168.126.63.1



(IP : 30.1.100.1)





```
NTP_DHCP_Server#sh ip dhcp server statistics
Memory usage            27917
Address pools           12
Database agents         0
Automatic bindings      0
Manual bindings         0
Expired bindings        3
Malformed messages      0
Secure arp entries      0

Message                 Received
BOOTREQUEST             0
DHCPDISCOVER            3
DHCPREQUEST             3
DHCPDECLINE             0
DHCPRELEASE             0
DHCPINFORM              9

Message                 Sent
BOOTREPLY               0
DHCPOFFER               3
DHCPACK                 12
DHCPNAK                 0
```

DHCP 메시지
수신 횟수 증가

01 내부 네트워크 기술 내용_Server

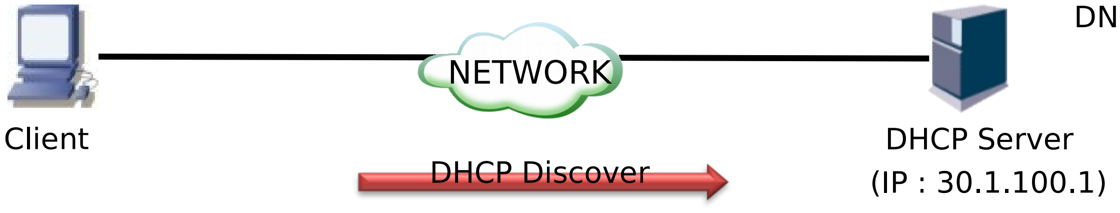
DHCP

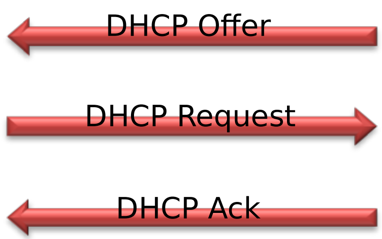
Dynamic Host Configuration Protocol

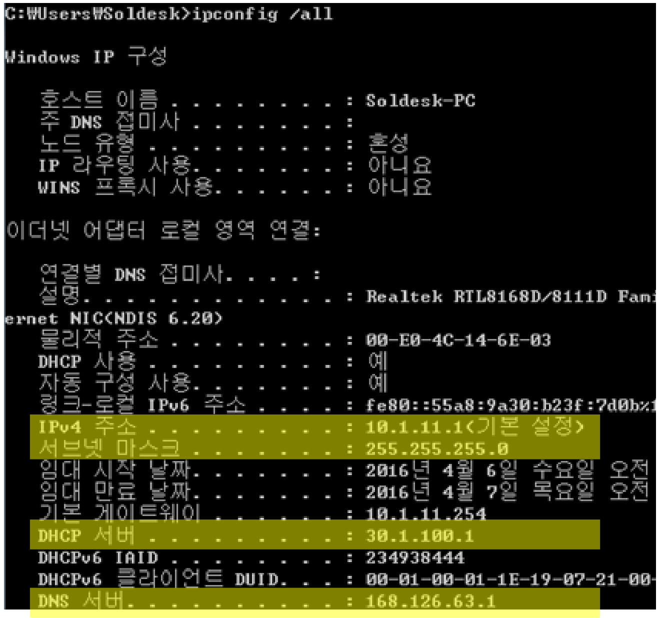
구현 목표

- 서버에서 IP를 관리하고 각각의 호스트에게 고유의 IP 자동 할당
- IP 임대 개념으로, 필요 시 동적으로 네트워크 재구성 가능

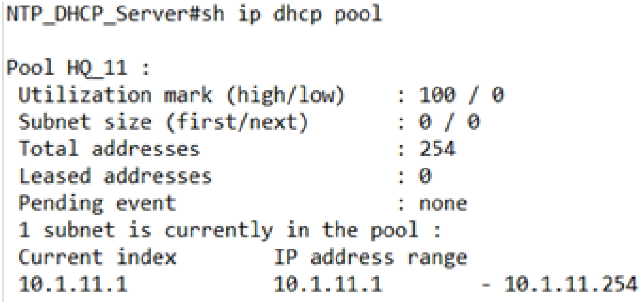
DNS 서버 : 168.126.63.1







```
C:\Users\Soldesk>ipconfig /all

Windows IP 구성

   호스트 이름 . . . . . . . . . : Soldesk-PC
   주 DNS 접미사 . . . . . . . . :
   노드 유형 . . . . . . . . . . : 혼성
   IP 라우팅 사용. . . . . . . . : 아니요
   WINS 프록시 사용. . . . . . . : 아니요

이더넷 어댑터 로컬 영역 연결:

   연결별 DNS 접미사. . . . :
   설명. . . . . . . . . . . . : Realtek RTL8168D/8111D Fami
ernet NIC(NDIS 6.20)
   물리적 주소 . . . . . . . . . : 00-E0-4C-14-6E-03
   DHCP 사용 . . . . . . . . . . : 예
   자동 구성 사용. . . . . . . . : 예
   링크-로컬 IPv6 주소 . . . . . : fe80::55a8:9a30:b23f:7d0b%1
   IPv4 주소 . . . . . . . . . . : 10.1.11.1(기본 설정)
   서브넷 마스크 . . . . . . . . : 255.255.255.0
   임대 시작 날짜. . . . . . . . : 2016년 4월 6일 수요일 오전
   임대 만료 날짜. . . . . . . . : 2016년 4월 7일 목요일 오전
   기본 게이트웨이 . . . . . . . : 10.1.11.254
   DHCP 서버 . . . . . . . . . . : 30.1.100.1
   DHCPv6 IAID . . . . . . . . . : 234938444
   DHCPv6 클라이언트 DUID. . . : 00-01-00-01-1E-19-07-21-00-
   DNS 서버. . . . . . . . . . . : 168.126.63.1
```



```
NTP_DHCP_Server#sh ip dhcp pool

Pool HQ_11 :
 Utilization mark (high/low)    : 100 / 0
 Subnet size (first/next)       : 0 / 0
 Total addresses                : 254
 Leased addresses               : 0
 Pending event                  : none
 1 subnet is currently in the pool :
 Current index        IP address range
 10.1.11.1            10.1.11.1        - 10.1.11.254
```

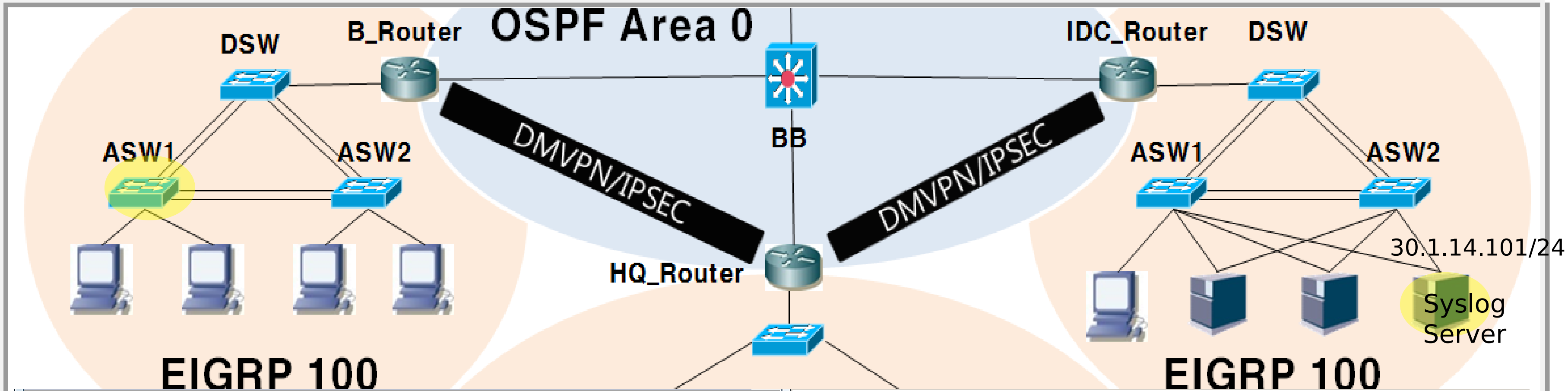
DHCP Pool 에 있는 IP 범위에 따라
IP 가 호스트에게 자동 할당됨

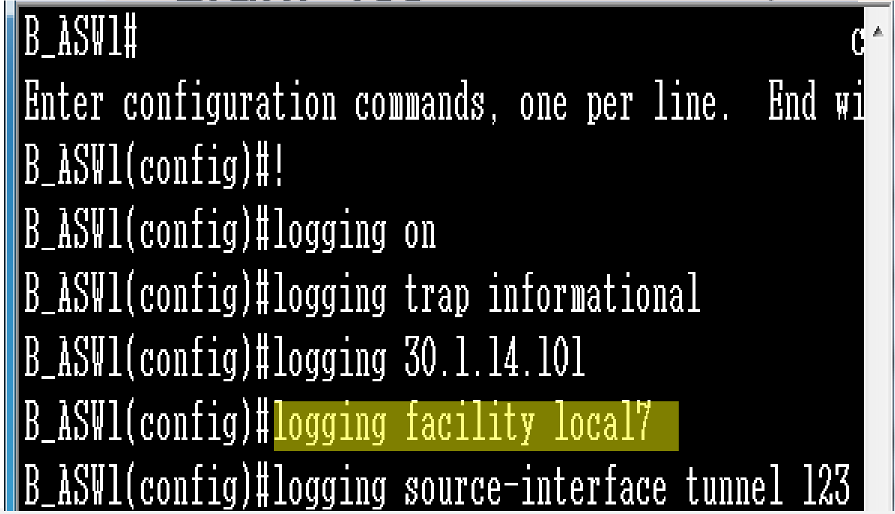
01 내부 네트워크 기술 내용_Server

SYSLOG

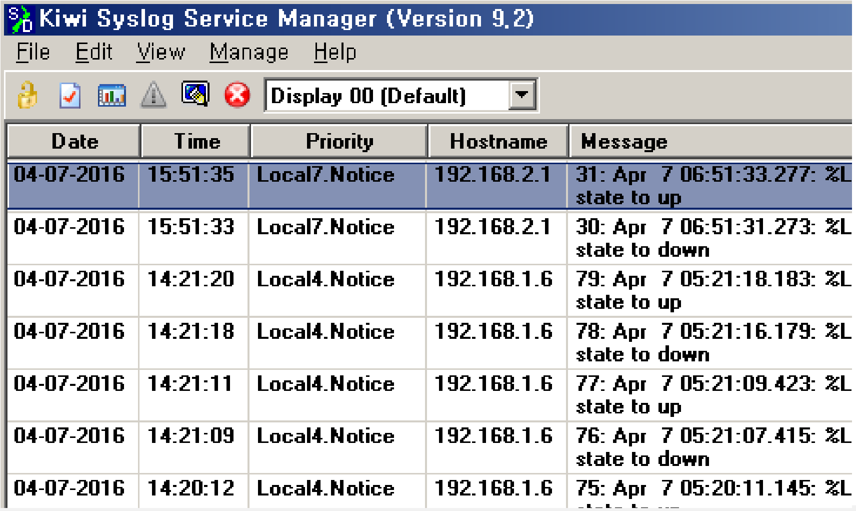
구현 목표

- Syslog 서버 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 장비에서 발생되는 Syslog 체크 및 저장 (EX : 지사B_ASW1)





```
B_ASW1#                                              c
Enter configuration commands, one per line.  End wi
B_ASW1(config)#!
B_ASW1(config)#logging on
B_ASW1(config)#logging trap informational
B_ASW1(config)#logging 30.1.14.101
B_ASW1(config)#logging facility local7
B_ASW1(config)#logging source-interface tunnel 123
```



Kiwi Syslog Service Manager (Version 9.2)

Date	Time	Priority	Hostname	Message
04-07-2016	15:51:35	Local7.Notice	192.168.2.1	31: Apr 7 06:51:33.277: %L state to up
04-07-2016	15:51:33	Local7.Notice	192.168.2.1	30: Apr 7 06:51:31.273: %L state to down
04-07-2016	14:21:20	Local4.Notice	192.168.1.6	79: Apr 7 05:21:18.183: %L state to up
04-07-2016	14:21:18	Local4.Notice	192.168.1.6	78: Apr 7 05:21:16.179: %L state to down
04-07-2016	14:21:11	Local4.Notice	192.168.1.6	77: Apr 7 05:21:09.423: %L state to up
04-07-2016	14:21:09	Local4.Notice	192.168.1.6	76: Apr 7 05:21:07.415: %L state to down
04-07-2016	14:20:12	Local4.Notice	192.168.1.6	75: Apr 7 05:20:11.145: %L

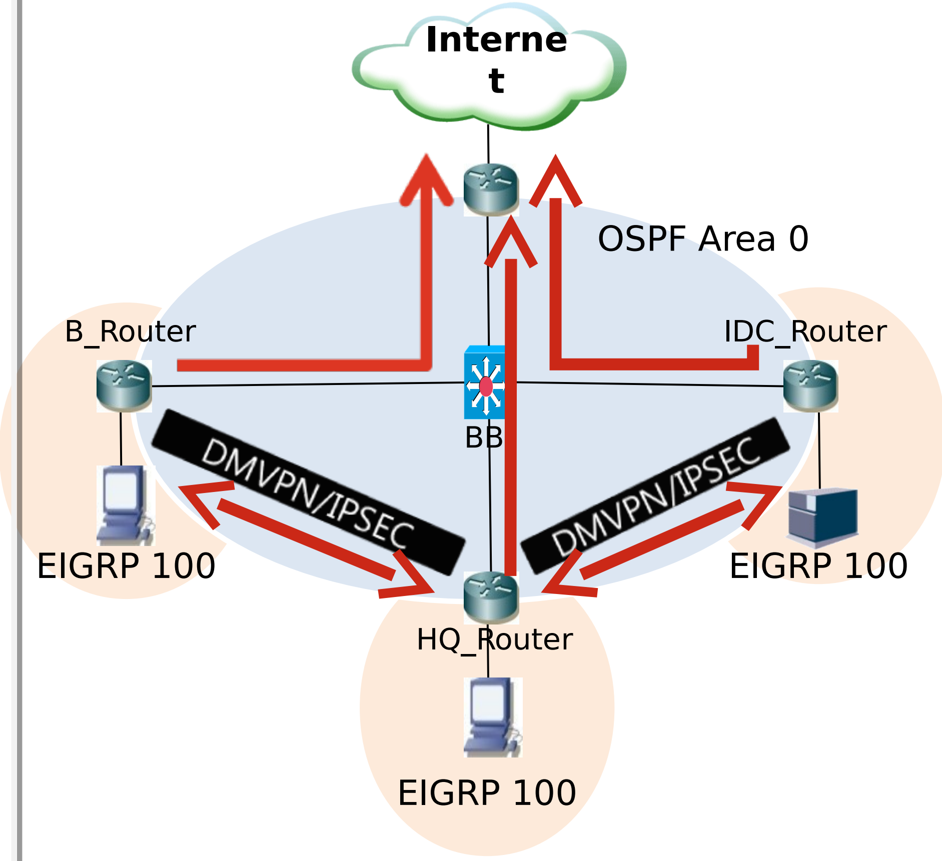
02 공중망기술 내용 (Routing Protocol)

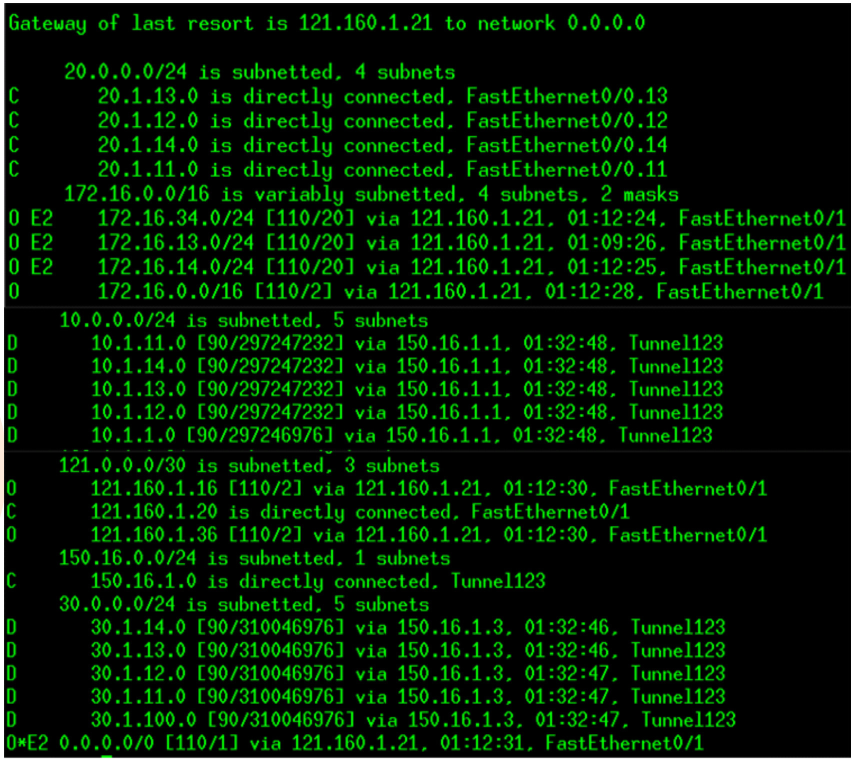
OSPF

Open Shortest Path First

구현 목표

- 인터넷을 사용하기 위해 내부에서 외부로 나가는 트래픽 경로 구성
- 본사와 지사간에 논리적인 연결 (Tunnel) 이 가능





```
Gateway of last resort is 121.160.1.21 to network 0.0.0.0

     20.0.0.0/24 is subnetted, 4 subnets
C       20.1.13.0 is directly connected, FastEthernet0/0.13
C       20.1.12.0 is directly connected, FastEthernet0/0.12
C       20.1.14.0 is directly connected, FastEthernet0/0.14
C       20.1.11.0 is directly connected, FastEthernet0/0.11
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O E2    172.16.34.0/24 [110/20] via 121.160.1.21, 01:12:24, FastEthernet0/1
O E2    172.16.13.0/24 [110/20] via 121.160.1.21, 01:09:26, FastEthernet0/1
O E2    172.16.14.0/24 [110/20] via 121.160.1.21, 01:12:25, FastEthernet0/1
O       172.16.0.0/16 [110/2] via 121.160.1.21, 01:12:28, FastEthernet0/1
     10.0.0.0/24 is subnetted, 5 subnets
D       10.1.11.0 [90/297247232] via 150.16.1.1, 01:32:48, Tunnel123
D       10.1.14.0 [90/297247232] via 150.16.1.1, 01:32:48, Tunnel123
D       10.1.13.0 [90/297247232] via 150.16.1.1, 01:32:48, Tunnel123
D       10.1.12.0 [90/297247232] via 150.16.1.1, 01:32:48, Tunnel123
D       10.1.1.0 [90/297246976] via 150.16.1.1, 01:32:48, Tunnel123
     121.0.0.0/30 is subnetted, 3 subnets
O       121.160.1.16 [110/2] via 121.160.1.21, 01:12:30, FastEthernet0/1
C       121.160.1.20 is directly connected, FastEthernet0/1
O       121.160.1.36 [110/2] via 121.160.1.21, 01:12:30, FastEthernet0/1
     150.16.0.0/24 is subnetted, 1 subnets
C       150.16.1.0 is directly connected, Tunnel123
     30.0.0.0/24 is subnetted, 5 subnets
D       30.1.14.0 [90/310046976] via 150.16.1.3, 01:32:46, Tunnel123
D       30.1.13.0 [90/310046976] via 150.16.1.3, 01:32:46, Tunnel123
D       30.1.12.0 [90/310046976] via 150.16.1.3, 01:32:47, Tunnel123
D       30.1.11.0 [90/310046976] via 150.16.1.3, 01:32:47, Tunnel123
D       30.1.100.0 [90/310046976] via 150.16.1.3, 01:32:47, Tunnel123
O*E2 0.0.0.0/0 [110/1] via 121.160.1.21, 01:12:31, FastEthernet0/1
```

지사에서 확인한 Routing Table

외부로 나가는 경로와 본사와 서버간에 Tunnel123 으로

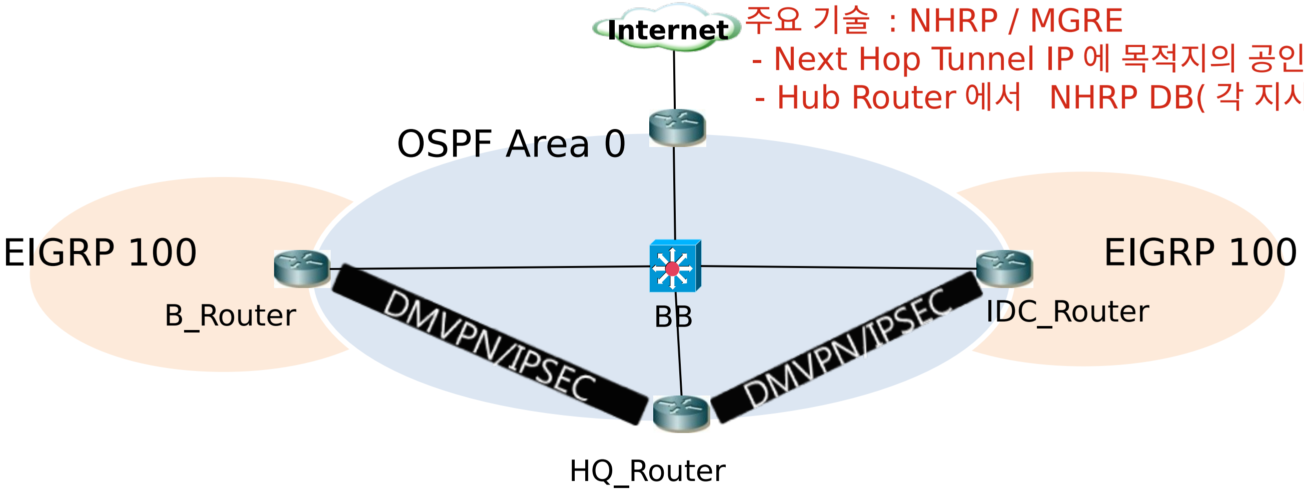
논리적인 연결 확립

DMVPN

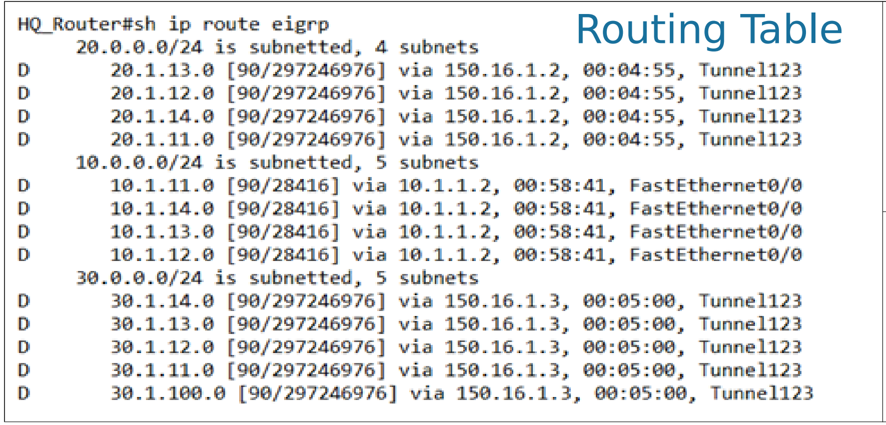
Dynamic Multipoint VPN

구현 목표

- 본사와 여러개의 지사를 연결하는 VPN 환경에서 확장성과 간편성 증대
- 본사와 지사 간의 Permaent IPSec Tunnel을 유지하며, 지사끼리도 통신 가능

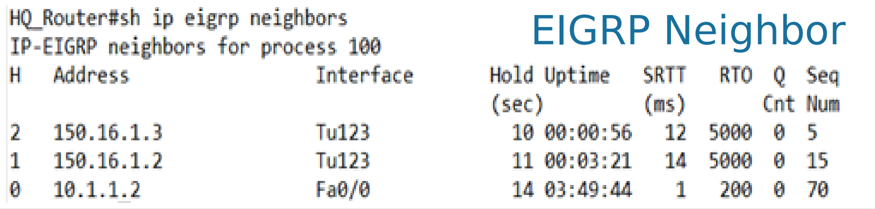


주요 기술 : NHRP / MGRE
- Next Hop Tunnel IP 에 목적지의 공인 IP 를 Mapping
- Hub Router 에서 NHRP DB(각 지사의 IP) 를 관리



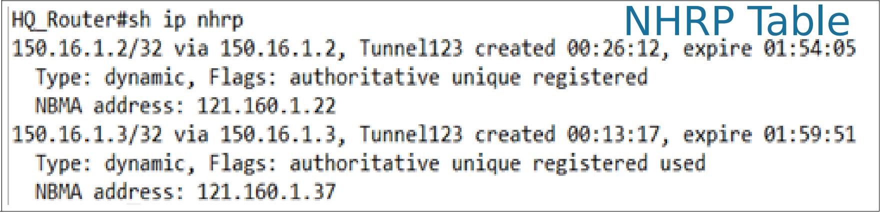
Routing Table

```
HQ_Router#sh ip route eigrp
     20.0.0.0/24 is subnetted, 4 subnets
D       20.1.13.0 [90/297246976] via 150.16.1.2, 00:04:55, Tunnel123
D       20.1.12.0 [90/297246976] via 150.16.1.2, 00:04:55, Tunnel123
D       20.1.14.0 [90/297246976] via 150.16.1.2, 00:04:55, Tunnel123
D       20.1.11.0 [90/297246976] via 150.16.1.2, 00:04:55, Tunnel123
     10.0.0.0/24 is subnetted, 5 subnets
D       10.1.11.0 [90/28416] via 10.1.1.2, 00:58:41, FastEthernet0/0
D       10.1.14.0 [90/28416] via 10.1.1.2, 00:58:41, FastEthernet0/0
D       10.1.13.0 [90/28416] via 10.1.1.2, 00:58:41, FastEthernet0/0
D       10.1.12.0 [90/28416] via 10.1.1.2, 00:58:41, FastEthernet0/0
     30.0.0.0/24 is subnetted, 5 subnets
D       30.1.14.0 [90/297246976] via 150.16.1.3, 00:05:00, Tunnel123
D       30.1.13.0 [90/297246976] via 150.16.1.3, 00:05:00, Tunnel123
D       30.1.12.0 [90/297246976] via 150.16.1.3, 00:05:00, Tunnel123
D       30.1.11.0 [90/297246976] via 150.16.1.3, 00:05:00, Tunnel123
D       30.1.100.0 [90/297246976] via 150.16.1.3, 00:05:00, Tunnel123
```



EIGRP Neighbor

```
HQ_Router#sh ip eigrp neighbors
IP-EIGRP neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q  Seq
                                            (sec)         (ms)       Cnt Num
2   150.16.1.3              Tu123             10 00:00:56   12  5000  0  5
1   150.16.1.2              Tu123             11 00:03:21   14  5000  0  15
0   10.1.1.2                Fa0/0             14 03:49:44    1   200  0  70
```



NHRP Table

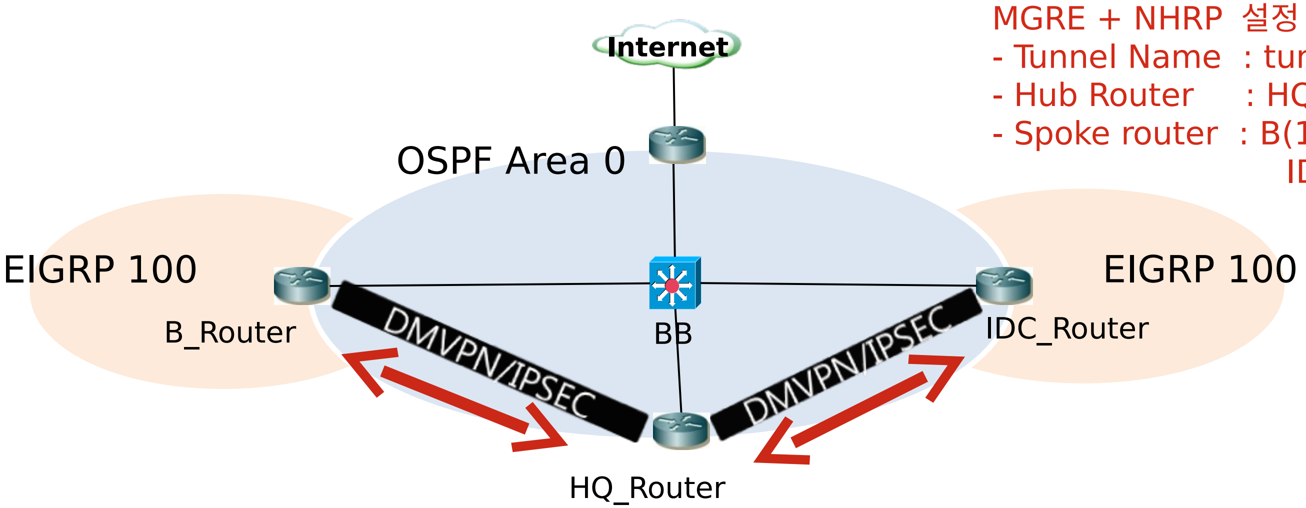
```
HQ_Router#sh ip nhrp
150.16.1.2/32 via 150.16.1.2, Tunnel123 created 00:26:12, expire 01:54:05
  Type: dynamic, Flags: authoritative unique registered
  NBMA address: 121.160.1.22
150.16.1.3/32 via 150.16.1.3, Tunnel123 created 00:13:17, expire 01:59:51
  Type: dynamic, Flags: authoritative unique registered used
  NBMA address: 121.160.1.37
```

DMVPN

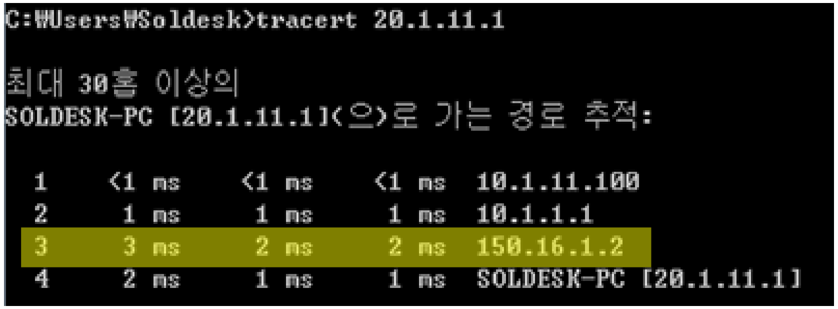
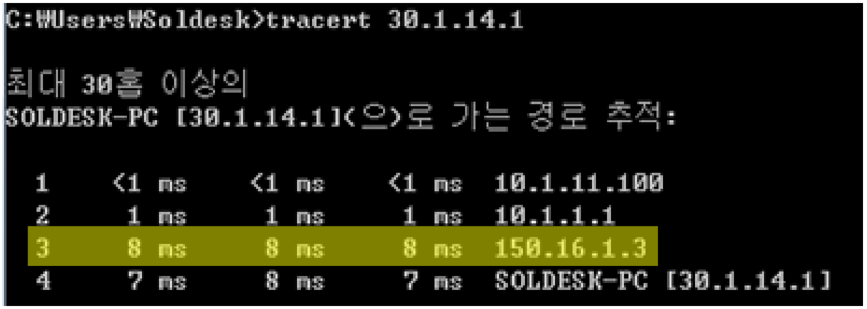
Dynamic Multipoint VPN

구현 목표

- 본사와 여러개의 지사를 연결하는 VPN 환경에서 확장성과 간편성 증대
- 본사와 지사 간의 Permaent IPSec Tunnel을 유지하며, 지사끼리도 통신 가능



MGRE + NHRP 설정
- Tunnel Name : tunnel 123
- Hub Router : HQ(150.16.1.1)
- Spoke router : B(150.16.1.2)
  IDC(150.16.1.3)

본사 PC → 지사 PC	본사 PC → 센터 PC
	

```
C:₩Users₩Soldesk>tracert 20.1.11.1

최대 30홉 이상의
SOLDESK-PC [20.1.11.1](으)로 가는 경로 추적:

  1    <1 ms    <1 ms    <1 ms  10.1.11.100
  2     1 ms     1 ms     1 ms  10.1.1.1
  3     3 ms     2 ms     2 ms  150.16.1.2
  4     2 ms     1 ms     1 ms  SOLDESK-PC [20.1.11.1]
```

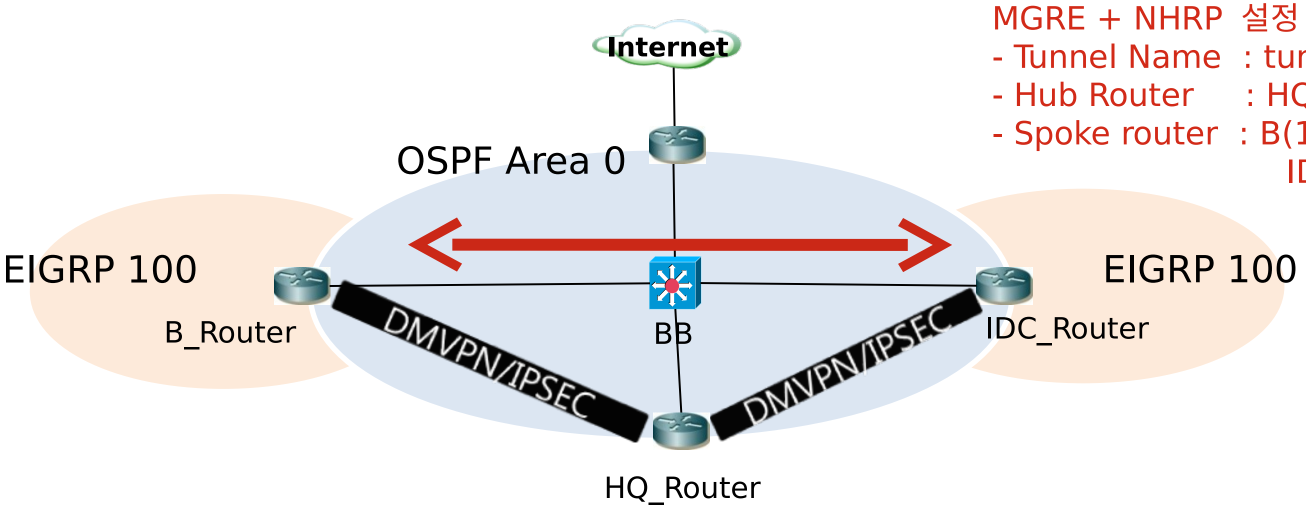
```
C:₩Users₩Soldesk>tracert 30.1.14.1

최대 30홉 이상의
SOLDESK-PC [30.1.14.1](으)로 가는 경로 추적:

  1    <1 ms    <1 ms    <1 ms  10.1.11.100
  2     1 ms     1 ms     1 ms  10.1.1.1
  3     8 ms     8 ms     8 ms  150.16.1.3
  4     7 ms     8 ms     7 ms  SOLDESK-PC [30.1.14.1]
```

DMVPN

Dynamic Multipoint VPN

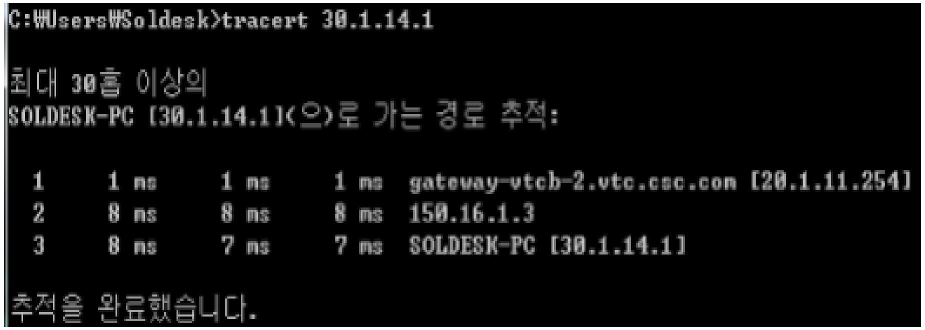
구현 목표

- 본사와 여러개의 지사를 연결하는 VPN 환경에서 확장성과 간편성 증대
- 본사와 지사 간의 Permaent IPSec Tunnel을 유지하며, 지사끼리도 통신 가능



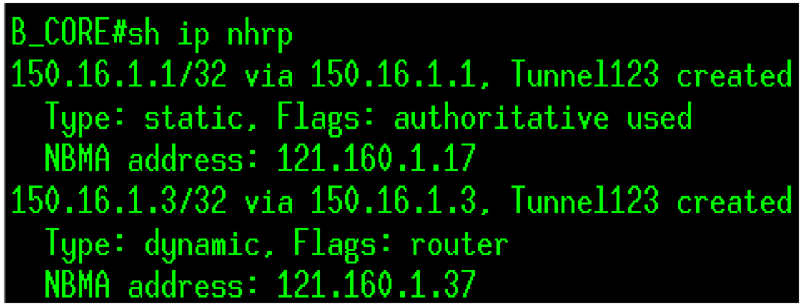
MGRE + NHRP 설정
- Tunnel Name : tunnel 123
- Hub Router : HQ(150.16.1.1)
- Spoke router : B(150.16.1.2)
  IDC(150.16.1.3)

센터 PC → 지사 PC



```
C:₩Users₩Soldesk>tracert 30.1.14.1

최대 30홉 이상의
SOLDESK-PC [30.1.14.1](으)로 가는 경로 추적:

  1     1 ms     1 ms     1 ms  gateway-vtcb-2.vtc.csc.com [20.1.11.254]
  2     8 ms     8 ms     8 ms  150.16.1.3
  3     8 ms     7 ms     7 ms  SOLDESK-PC [30.1.14.1]

추적을 완료했습니다.
```

NHRP Table



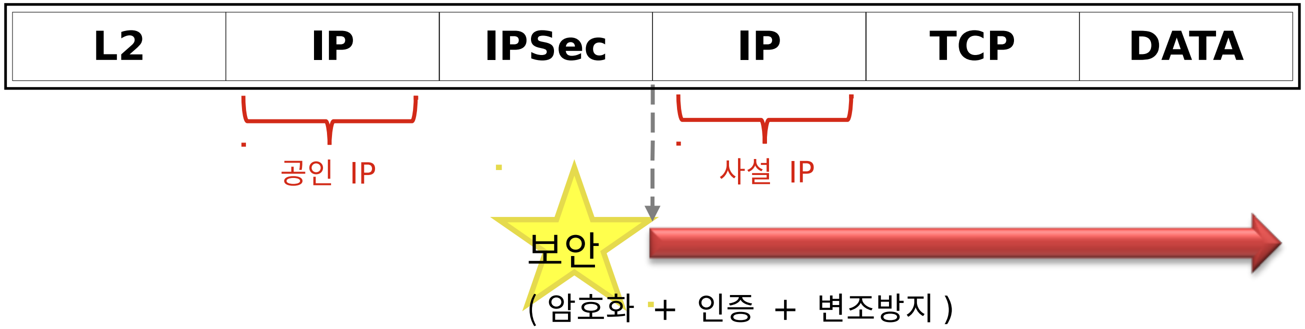
```
B_CORE#sh ip nhrp
150.16.1.1/32 via 150.16.1.1, Tunnel123 created
  Type: static, Flags: authoritative used
  NBMA address: 121.160.1.17
150.16.1.3/32 via 150.16.1.3, Tunnel123 created
  Type: dynamic, Flags: router
  NBMA address: 121.160.1.37
```

03 보안 기술 내용

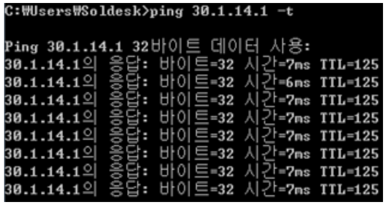
IPSEC
Internet Protocol Security

구현 목표

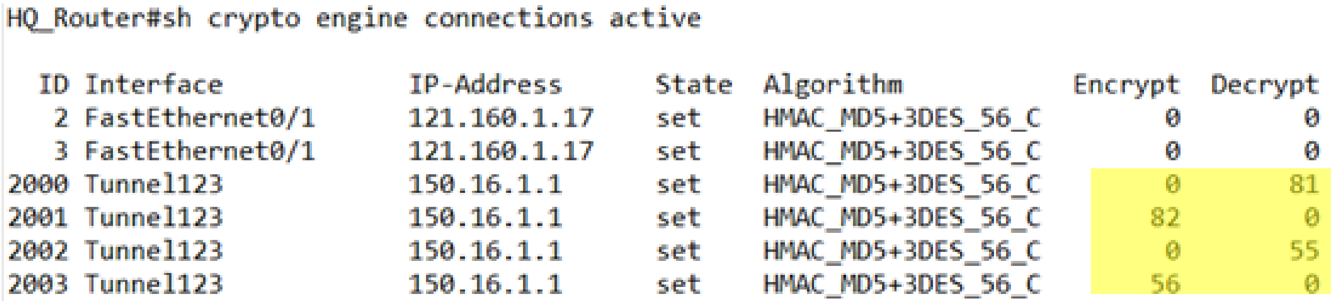
- IP는 자체적인 보안 요소가 없으므로 IPSEC을 통해 패켓단위의 보안 강화
- 공중망에서의 내부 네트워크 사설 IP 보호(Tunnuling Mode 지원)



외부로 Ping 을 보냈을 때

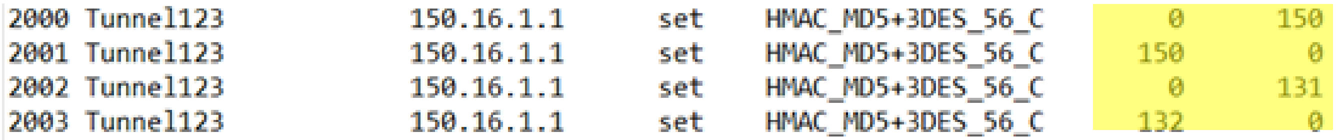


```
C:\Users\Soldesk>ping 30.1.14.1 -t

Ping 30.1.14.1 32바이트 데이터 사용:
30.1.14.1의 응답: 바이트=32 시간=7ms TTL=125
30.1.14.1의 응답: 바이트=32 시간=6ms TTL=125
30.1.14.1의 응답: 바이트=32 시간=7ms TTL=125
30.1.14.1의 응답: 바이트=32 시간=7ms TTL=125
30.1.14.1의 응답: 바이트=32 시간=7ms TTL=125
30.1.14.1의 응답: 바이트=32 시간=7ms TTL=125
30.1.14.1의 응답: 바이트=32 시간=7ms TTL=125
30.1.14.1의 응답: 바이트=32 시간=7ms TTL=125
```



```
HQ_Router#sh crypto engine connections active

  ID Interface            IP-Address      State  Algorithm           Encrypt  Decrypt
   2 FastEthernet0/1      121.160.1.17    set    HMAC_MD5+3DES_56_C        0        0
   3 FastEthernet0/1      121.160.1.17    set    HMAC_MD5+3DES_56_C        0        0
2000 Tunnel123            150.16.1.1      set    HMAC_MD5+3DES_56_C        0       81
2001 Tunnel123            150.16.1.1      set    HMAC_MD5+3DES_56_C       82        0
2002 Tunnel123            150.16.1.1      set    HMAC_MD5+3DES_56_C        0       55
2003 Tunnel123            150.16.1.1      set    HMAC_MD5+3DES_56_C       56        0
```

암호화 / 복호화 통계 수치 상승 확인



```
2000 Tunnel123            150.16.1.1      set    HMAC_MD5+3DES_56_C        0      150
2001 Tunnel123            150.16.1.1      set    HMAC_MD5+3DES_56_C      150        0
2002 Tunnel123            150.16.1.1      set    HMAC_MD5+3DES_56_C        0      131
2003 Tunnel123            150.16.1.1      set    HMAC_MD5+3DES_56_C      132        0
```

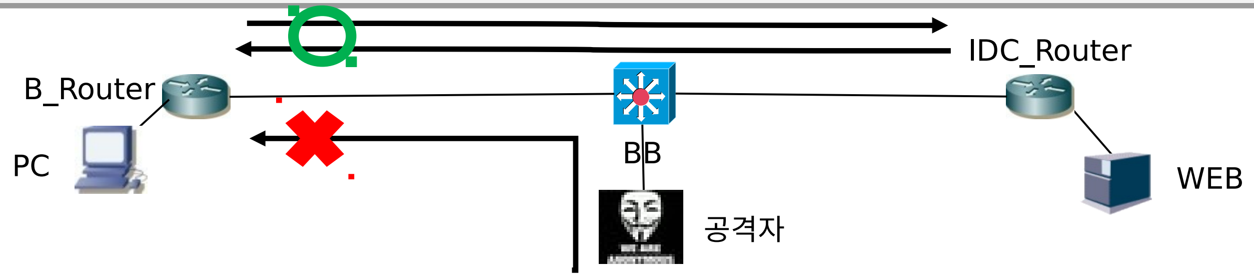
03 보안기술 내용

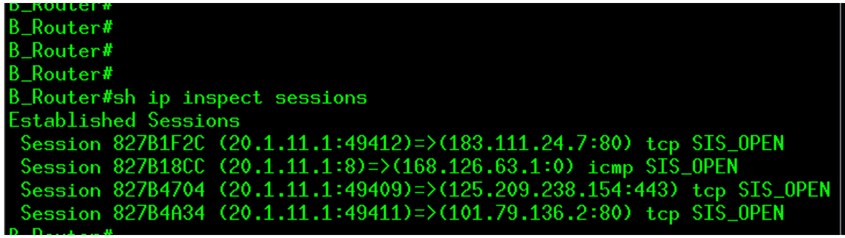
CBAC

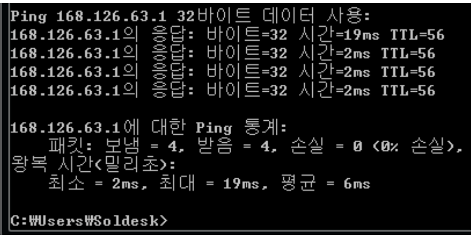
Context-Based Access Control

구 현 목 표

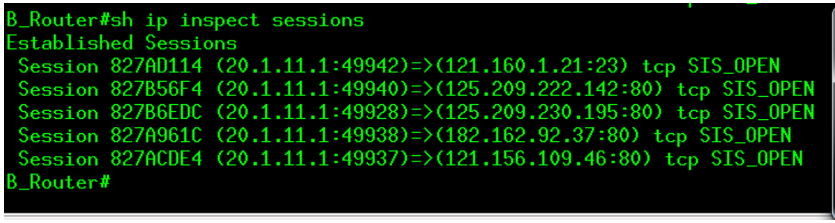
- 내부에서 외부로 나가는 세션을 검사하여 , 그 세션에 대한 응답 패킷을 수신하기 위한 임시 통로를 만들어 TCP, UDP, ICMP 를 허용
- 다양한 필터링을 이용한 DOS 공격 방지와 침입 탐지가 가능 하기 때문에 방화벽 구성으로 가장 뛰어난 보안 솔루션임

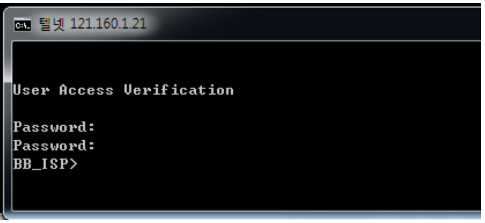



```
B_Router#
B_Router#
B_Router#
B_Router#sh ip inspect sessions
Established Sessions
 Session 827B1F2C (20.1.11.1:49412)=>(183.111.24.7:80) tcp SIS_OPEN
 Session 827B18CC (20.1.11.1:8)=>(168.126.63.1:0) icmp SIS_OPEN
 Session 827B4704 (20.1.11.1:49409)=>(125.209.238.154:443) tcp SIS_OPEN
 Session 827B4A34 (20.1.11.1:49411)=>(101.79.136.2:80) tcp SIS_OPEN
```


```
Ping 168.126.63.1 32바이트 데이터 사용:
168.126.63.1의 응답: 바이트=32 시간=19ms TTL=56
168.126.63.1의 응답: 바이트=32 시간=2ms TTL=56
168.126.63.1의 응답: 바이트=32 시간=2ms TTL=56
168.126.63.1의 응답: 바이트=32 시간=2ms TTL=56

168.126.63.1에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),
왕복 시간(밀리초):
    최소 = 2ms, 최대 = 19ms, 평균 = 6ms

C:\Users\Soldesk>
```

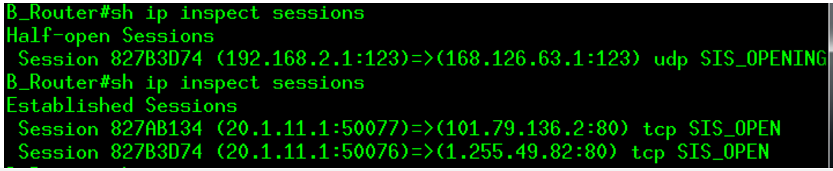
ICMP 에 대한 통로가 열렸는지 확인

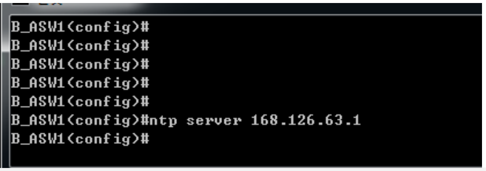

```
B_Router#sh ip inspect sessions
Established Sessions
 Session 827AD114 (20.1.11.1:49942)=>(121.160.1.21:23) tcp SIS_OPEN
 Session 827B56F4 (20.1.11.1:49940)=>(125.209.222.142:80) tcp SIS_OPEN
 Session 827B6EDC (20.1.11.1:49928)=>(125.209.230.195:80) tcp SIS_OPEN
 Session 827A961C (20.1.11.1:49938)=>(182.162.92.37:80) tcp SIS_OPEN
 Session 827ACDE4 (20.1.11.1:49937)=>(121.156.109.46:80) tcp SIS_OPEN
B_Router#
```


텔넷 121.160.1.21

```
User Access Verification

Password:
Password:
BB_ISP>
```

TCP 에 대한 통로가 열렸는지 확인


```
B_Router#sh ip inspect sessions
Half-open Sessions
 Session 827B3D74 (192.168.2.1:123)=>(168.126.63.1:123) udp SIS_OPENING
B_Router#sh ip inspect sessions
Established Sessions
 Session 827AB134 (20.1.11.1:50077)=>(101.79.136.2:80) tcp SIS_OPEN
 Session 827B3D74 (20.1.11.1:50076)=>(1.255.49.82:80) tcp SIS_OPEN
```


```
B_ASW1(config)#
B_ASW1(config)#
B_ASW1(config)#
B_ASW1(config)#
B_ASW1(config)#
B_ASW1(config)#ntp server 168.126.63.1
B_ASW1(config)#
```

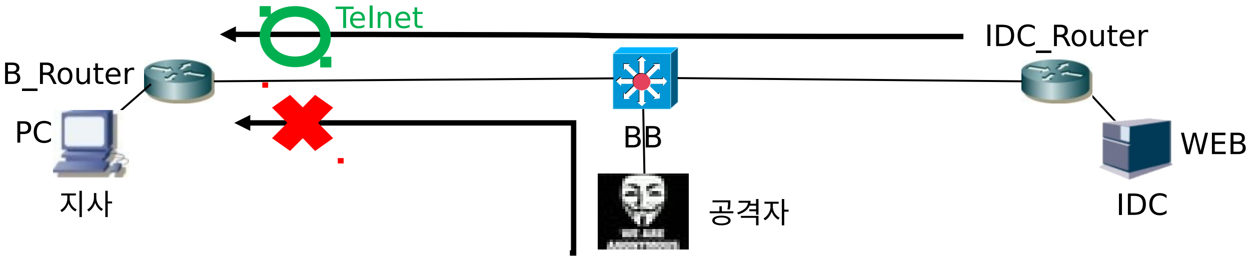
UDP 에 대한 통로가 열렸는지 확인

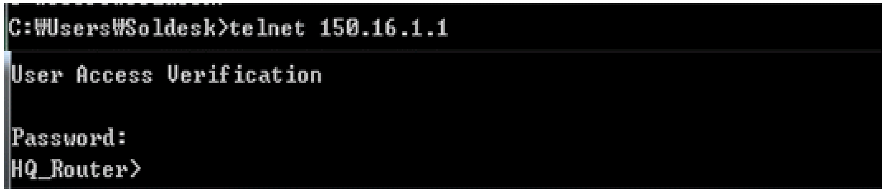
03 보안기술 내용

ACL
Access-List

구현 목표

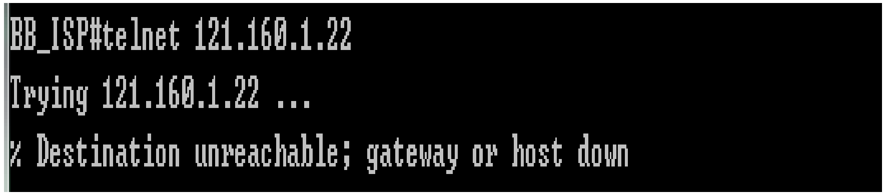
- 본사와 지사간에 Telnet, Ping Test, 라우팅 업데이트 , TACCAS 등 중요한 정보만 허용케 하고 나머지는 모두 차단
- CBAC 을 단독적으로 사용할경우 모든 트래픽이 허용 되므로 ACL 과 같이 사용





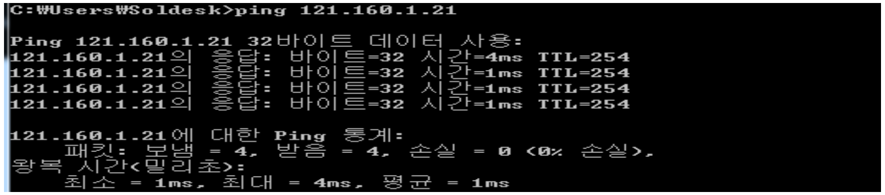
```
C:WUsersWSoldesk>telnet 150.16.1.1

User Access Verification

Password:
HQ_Router>
```

지사 pc(vlan 11) 에서 본사로 Telnet 접속



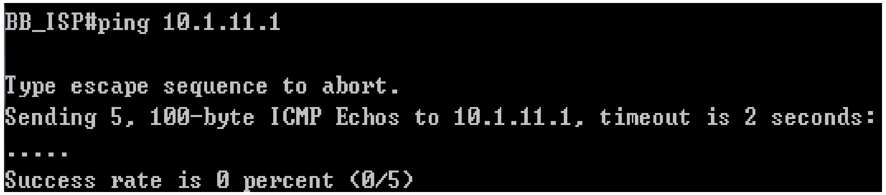
```
BB_ISP#telnet 121.160.1.22
Trying 121.160.1.22 ...
% Destination unreachable; gateway or host down
```

외부에서 본사로 Telnet 접속



```
C:WUsersWSoldesk>ping 121.160.1.21

Ping 121.160.1.21 32바이트 데이터 사용:
121.160.1.21의 응답: 바이트=32 시간=4ms TTL=254
121.160.1.21의 응답: 바이트=32 시간=1ms TTL=254
121.160.1.21의 응답: 바이트=32 시간=1ms TTL=254
121.160.1.21의 응답: 바이트=32 시간=1ms TTL=254

121.160.1.21에 대한 Ping 통계:
    패킷: 보냄 = 4, 받음 = 4, 손실 = 0 <0% 손실>,
왕복 시간<밀리초>:
    최소 = 1ms, 최대 = 4ms, 평균 = 1ms
```

지사 pc(vlan 11) 에서 본사로 Ping Test



```
BB_ISP#ping 10.1.11.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.11.1, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

외부에서 본사로 Ping Test

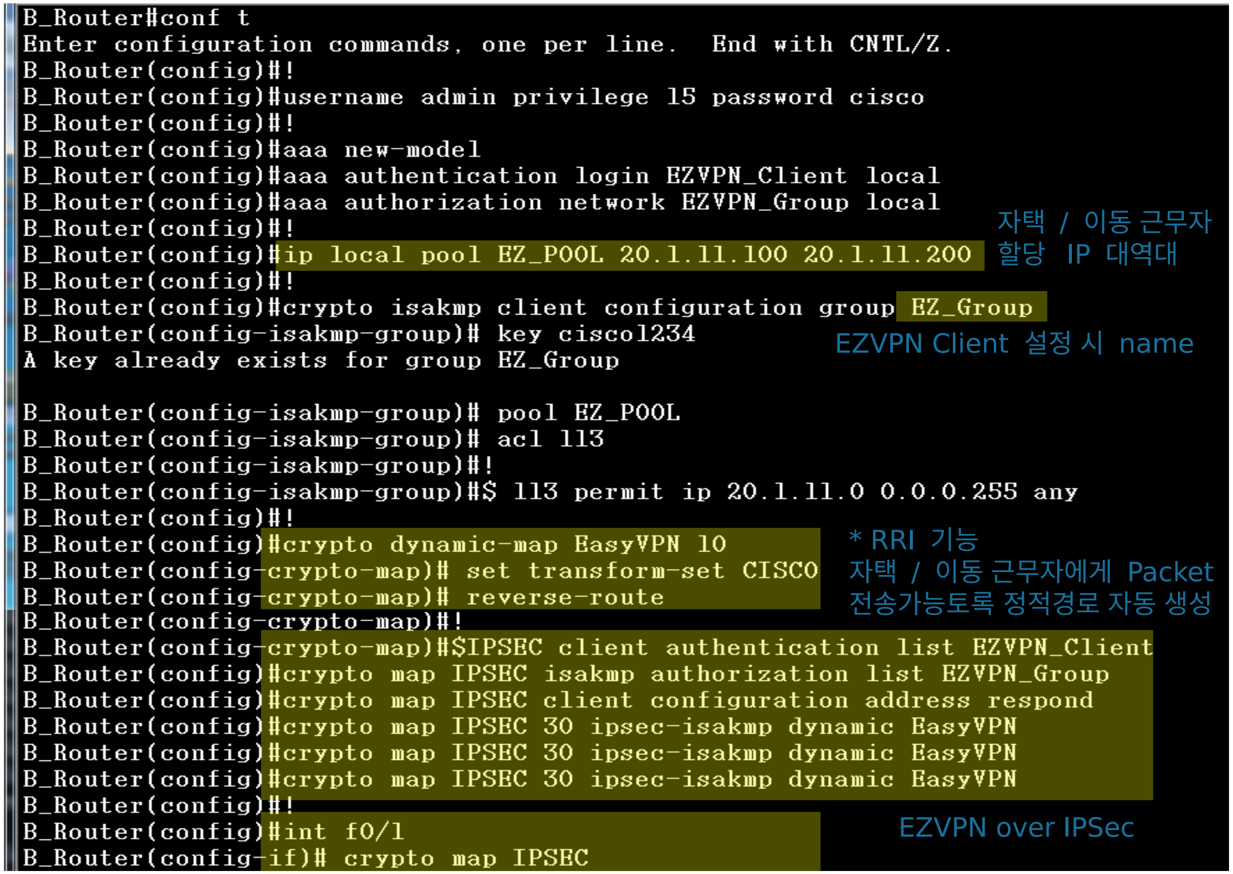
03 보안기술 내용

EZVPN
Easy VPN

구현 목표

- EZVPN 구성 (EX : 지사B)
- 자택근무자 / 이동 근무자들에게 원격으로 IPSec VPN을 손쉽게 사용

지사B_Router EZVPN 설정



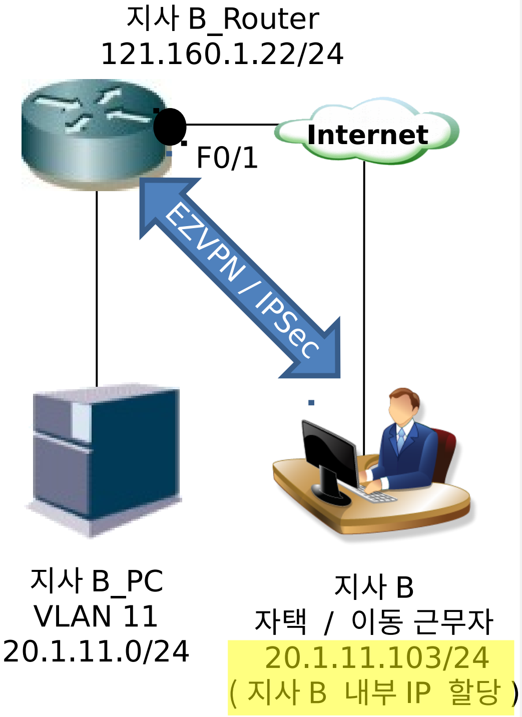
```
B_Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
B_Router(config)#!
B_Router(config)#username admin privilege 15 password cisco
B_Router(config)#!
B_Router(config)#aaa new-model
B_Router(config)#aaa authentication login EZVPN_Client local
B_Router(config)#aaa authorization network EZVPN_Group local
B_Router(config)#!
B_Router(config)#ip local pool EZ_POOL 20.1.11.100 20.1.11.200
B_Router(config)#!
B_Router(config)#crypto isakmp client configuration group EZ_Group
B_Router(config-isakmp-group)# key cisco1234
A key already exists for group EZ_Group

B_Router(config-isakmp-group)# pool EZ_POOL
B_Router(config-isakmp-group)# acl 113
B_Router(config-isakmp-group)#!
B_Router(config-isakmp-group)#$ 113 permit ip 20.1.11.0 0.0.0.255 any
B_Router(config)#!
B_Router(config)#crypto dynamic-map EasyVPN 10
B_Router(config-crypto-map)# set transform-set CISCO
B_Router(config-crypto-map)# reverse-route
B_Router(config-crypto-map)#!
B_Router(config-crypto-map)#$IPSEC client authentication list EZVPN_Client
B_Router(config)#crypto map IPSEC isakmp authorization list EZVPN_Group
B_Router(config)#crypto map IPSEC client configuration address respond
B_Router(config)#crypto map IPSEC 30 ipsec-isakmp dynamic EasyVPN
B_Router(config)#crypto map IPSEC 30 ipsec-isakmp dynamic EasyVPN
B_Router(config)#crypto map IPSEC 30 ipsec-isakmp dynamic EasyVPN
B_Router(config)#!
B_Router(config)#int f0/1
B_Router(config-if)# crypto map IPSEC
```

자택 / 이동 근무자 할당 IP 대역대

EZVPN Client 설정 시 name

* RRI 기능
자택 / 이동 근무자에게 Packet 전송가능토록 정적경로 자동 생성

EZVPN over IPSec



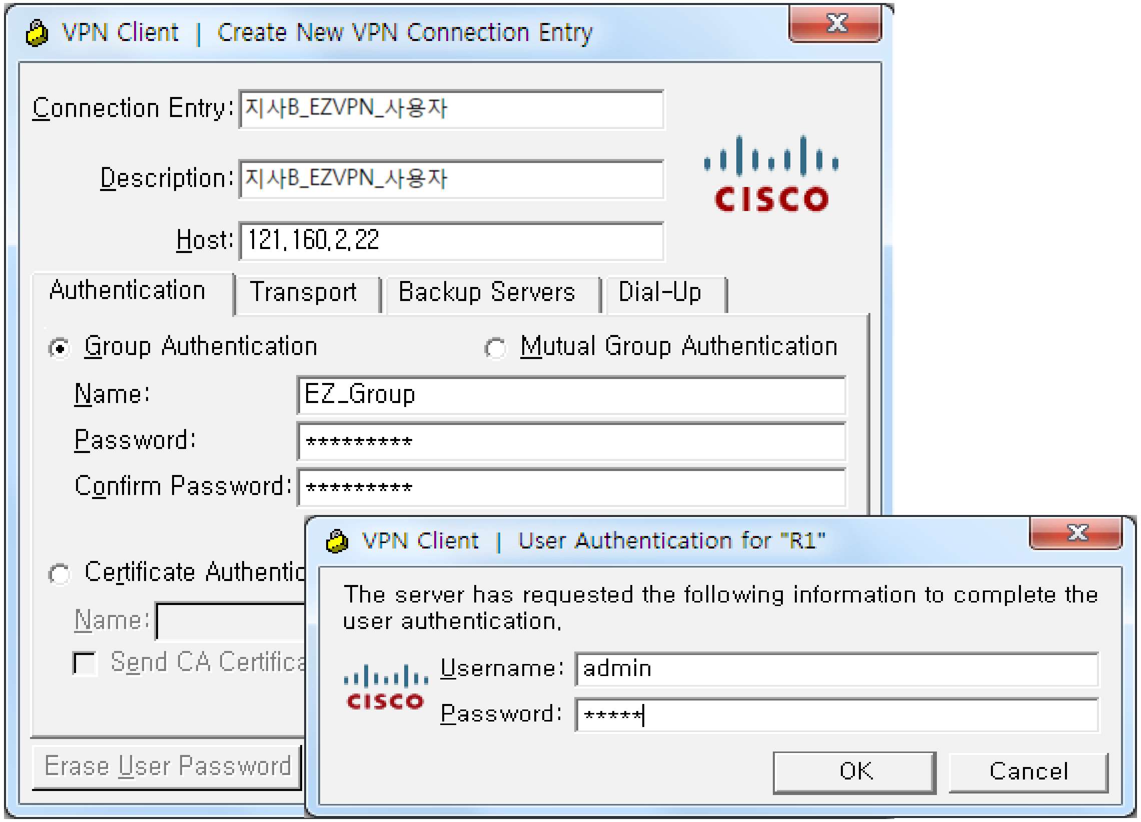
EZVPN

Easy VPN

구현 목표

- EZVPN 구성 (EX : 지사B)
- 자택근무자 / 이동 근무자들에게 원격으로 IPSec VPN을 손쉽게 사용

지사B_EZVPN_사용자 PC Setting



VPN Client | Create New VPN Connection Entry

Connection Entry: 지사B_EZVPN_사용자

Description: 지사B_EZVPN_사용자

Host: 121.160.2.22

Authentication | Transport | Backup Servers | Dial-Up

● Group Authentication ○ Mutual Group Authentication

Name: EZ_Group

Password: **********

Confirm Password: **********

○ Certificate Authentic

Name:

□ Send CA Certifica

Erase User Password

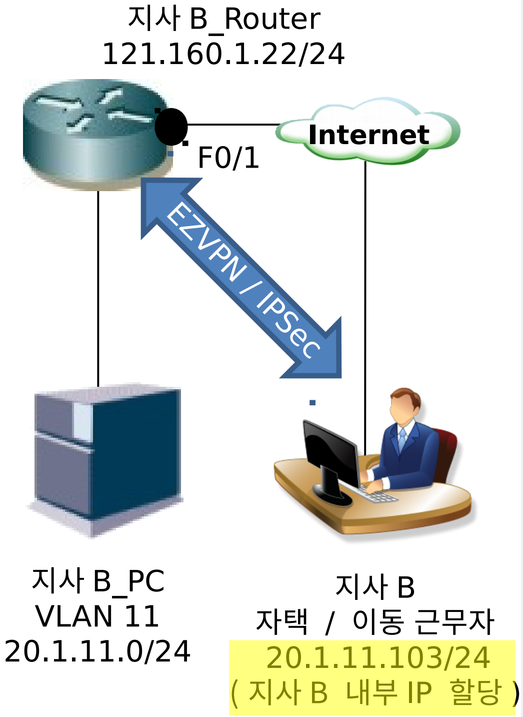
VPN Client | User Authentication for "R1"

The server has requested the following information to complete the user authentication.

Username: admin

Password: *****

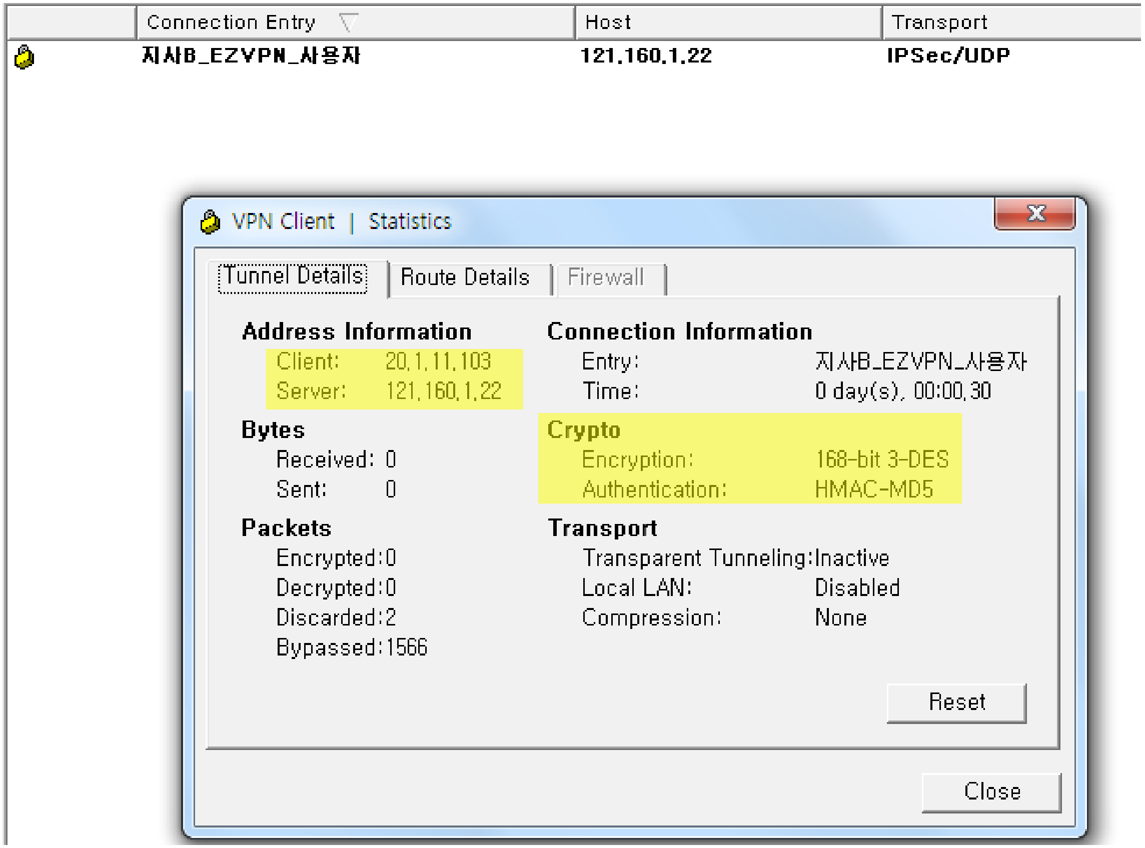
OK Cancel



구현 목표

- EZVPN 구성 (EX : 지사B)
- 자택근무자 / 이동 근무자들에게 원격으로 IPSec VPN을 손쉽게 사용

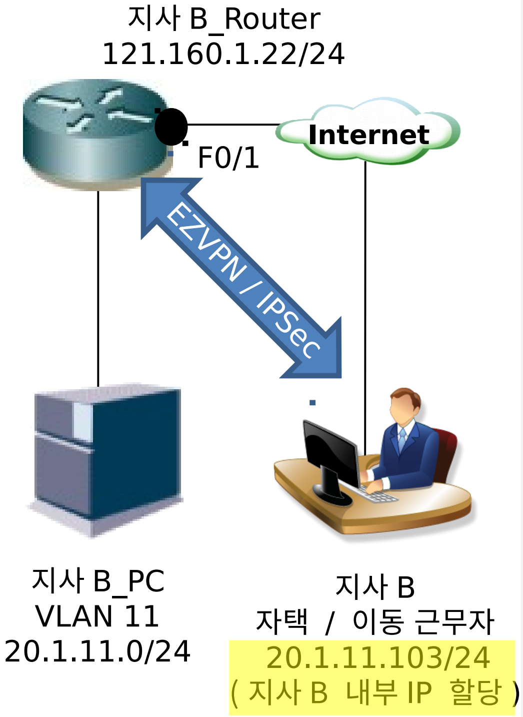
지사B_EZVPN_사용자 PC 연결확인 / IPSec 적용 확인



	Connection Entry	Host	Transport
	지사B_EZVPN_사용자	121.160.1.22	IPSec/UDP

VPN Client | Statistics

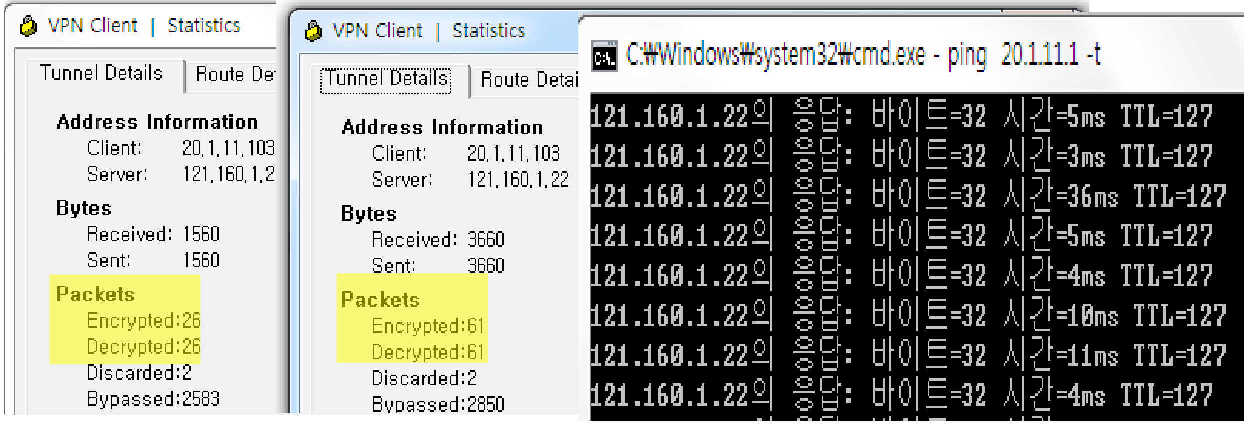
```
Address Information          Connection Information
  Client:   20.1.11.103        Entry:          지사B_EZVPN_사용자
  Server:   121.160.1.22       Time:           0 day(s), 00:00.30
Bytes                        Crypto
  Received: 0                  Encryption:     168-bit 3-DES
  Sent:     0                  Authentication: HMAC-MD5
Packets                      Transport
  Encrypted:0                  Transparent Tunneling:Inactive
  Decrypted:0                  Local LAN:      Disabled
  Discarded:2                  Compression:    None
  Bypassed:1566
```



구현 목표

- EZVPN 구성 (EX : 지사B)
- 자택근무자 / 이동 근무자들에게 원격으로 IPSec VPN을 손쉽게 사용

지사B_EZVPN_사용자 PC 와 지사B내부 연결확인 및 IPSec을 통한 암호화 복호화 증가

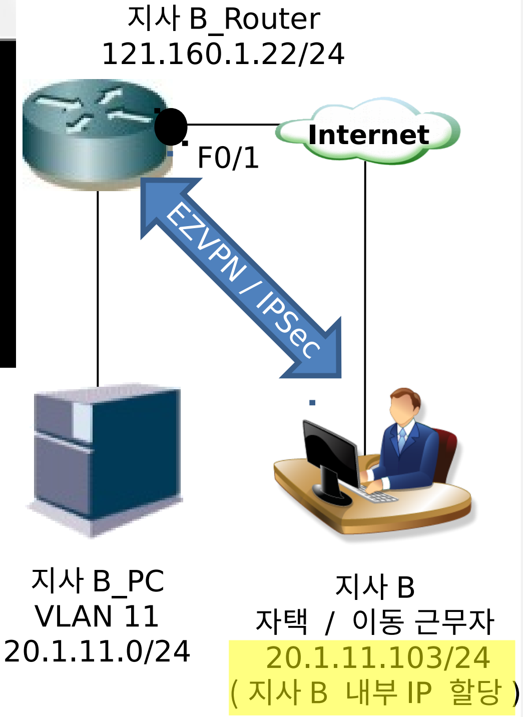


```
VPN Client | Statistics
Tunnel Details | Route De

Address Information
    Client:   20.1.11.103
    Server:   121.160.1.2
Bytes
    Received: 1560
    Sent:     1560
Packets
    Encrypted:26
    Decrypted:26
    Discarded:2
    Bypassed:2583
```

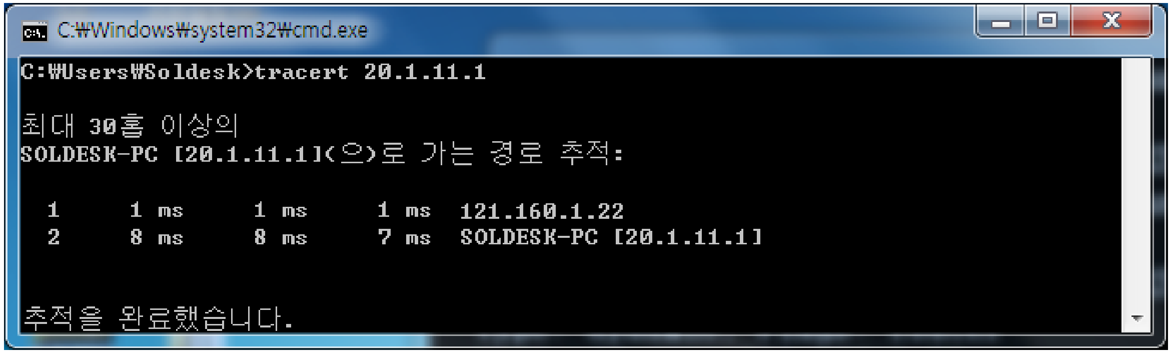
```
VPN Client | Statistics
Tunnel Details | Route Detai

Address Information
    Client:   20.1.11.103
    Server:   121.160.1.22
Bytes
    Received: 3660
    Sent:     3660
Packets
    Encrypted:61
    Decrypted:61
    Discarded:2
    Bypassed:2850
```

C:\Windows\system32\cmd.exe - ping 20.1.11.1 -t

```
121.160.1.22의 응답: 바이트=32 시간=5ms TTL=127
121.160.1.22의 응답: 바이트=32 시간=3ms TTL=127
121.160.1.22의 응답: 바이트=32 시간=36ms TTL=127
121.160.1.22의 응답: 바이트=32 시간=5ms TTL=127
121.160.1.22의 응답: 바이트=32 시간=4ms TTL=127
121.160.1.22의 응답: 바이트=32 시간=10ms TTL=127
121.160.1.22의 응답: 바이트=32 시간=11ms TTL=127
121.160.1.22의 응답: 바이트=32 시간=4ms TTL=127
```



지사B_EZVPN_사용자 PC 와 지사B내부 PC 간 Tracert



C:\Windows\system32\cmd.exe

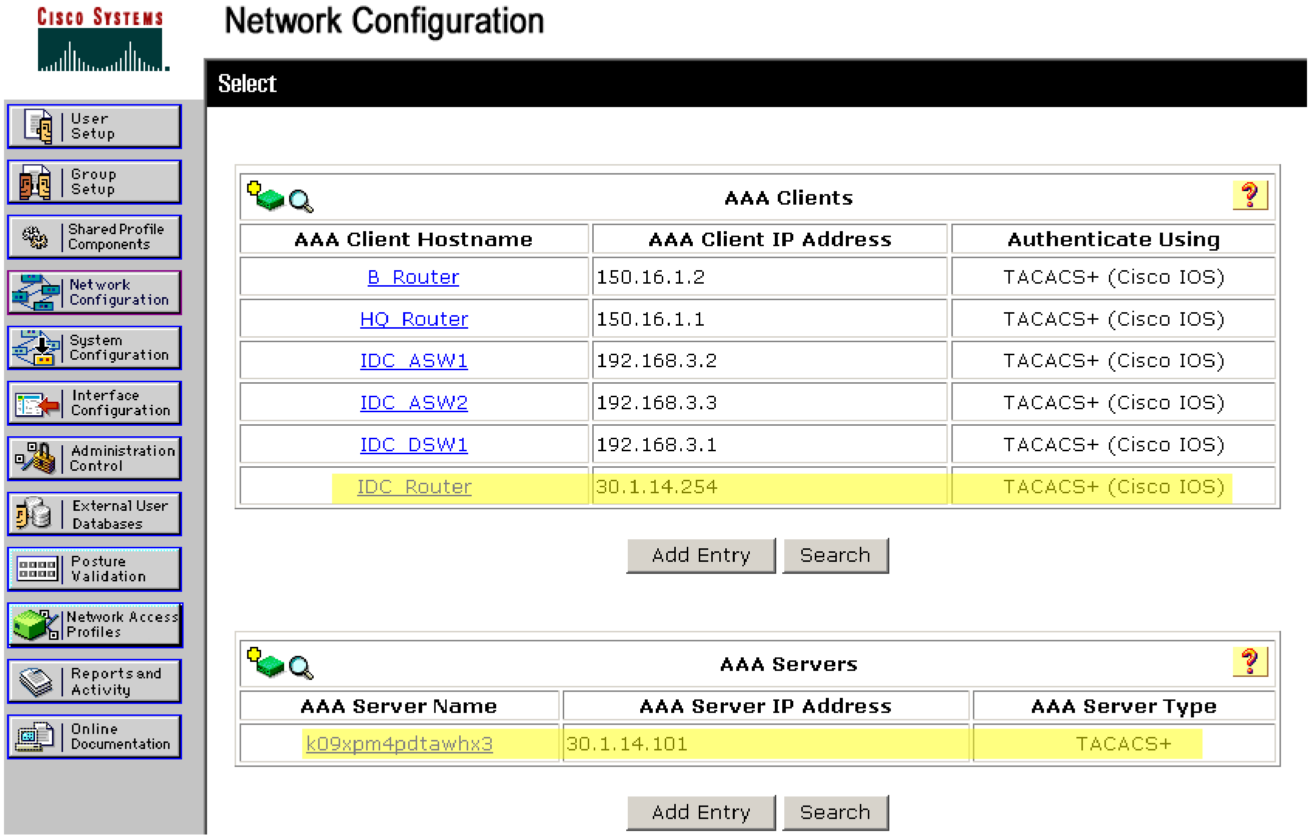
```
C:\Users\Soldesk>tracert 20.1.11.1

최대 30홉 이상의
SOLDESK-PC [20.1.11.1](으)로 가는 경로 추적:

  1     1 ms     1 ms     1 ms  121.160.1.22
  2     8 ms     8 ms     7 ms  SOLDESK-PC [20.1.11.1]

추적을 완료했습니다.
```

03 보안기술 내용_Tacacs+ Server

구현 목표

- Tacacs+ Server 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 라우터로 접속하는 사용자에 대한 인증 및 명령어 제한을 통한 보안 관련 기능 수행 (EX : IDC_Router)

AAA서버 및 클라이언트 구성



Network Configuration

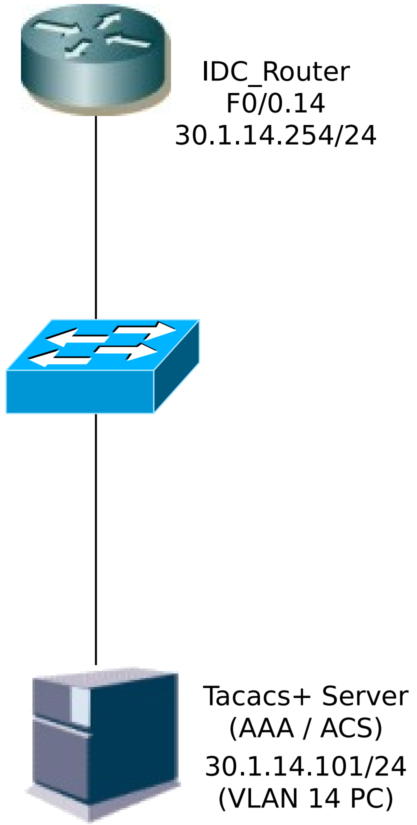
Select

AAA Clients

AAA Client Hostname	AAA Client IP Address	Authenticate Using
B_Router	150.16.1.2	TACACS+ (Cisco IOS)
HQ_Router	150.16.1.1	TACACS+ (Cisco IOS)
IDC_ASW1	192.168.3.2	TACACS+ (Cisco IOS)
IDC_ASW2	192.168.3.3	TACACS+ (Cisco IOS)
IDC_DSW1	192.168.3.1	TACACS+ (Cisco IOS)
IDC_Router	30.1.14.254	TACACS+ (Cisco IOS)

AAA Servers

AAA Server Name	AAA Server IP Address	AAA Server Type
k09xpm4pdtawhx3	30.1.14.101	TACACS+

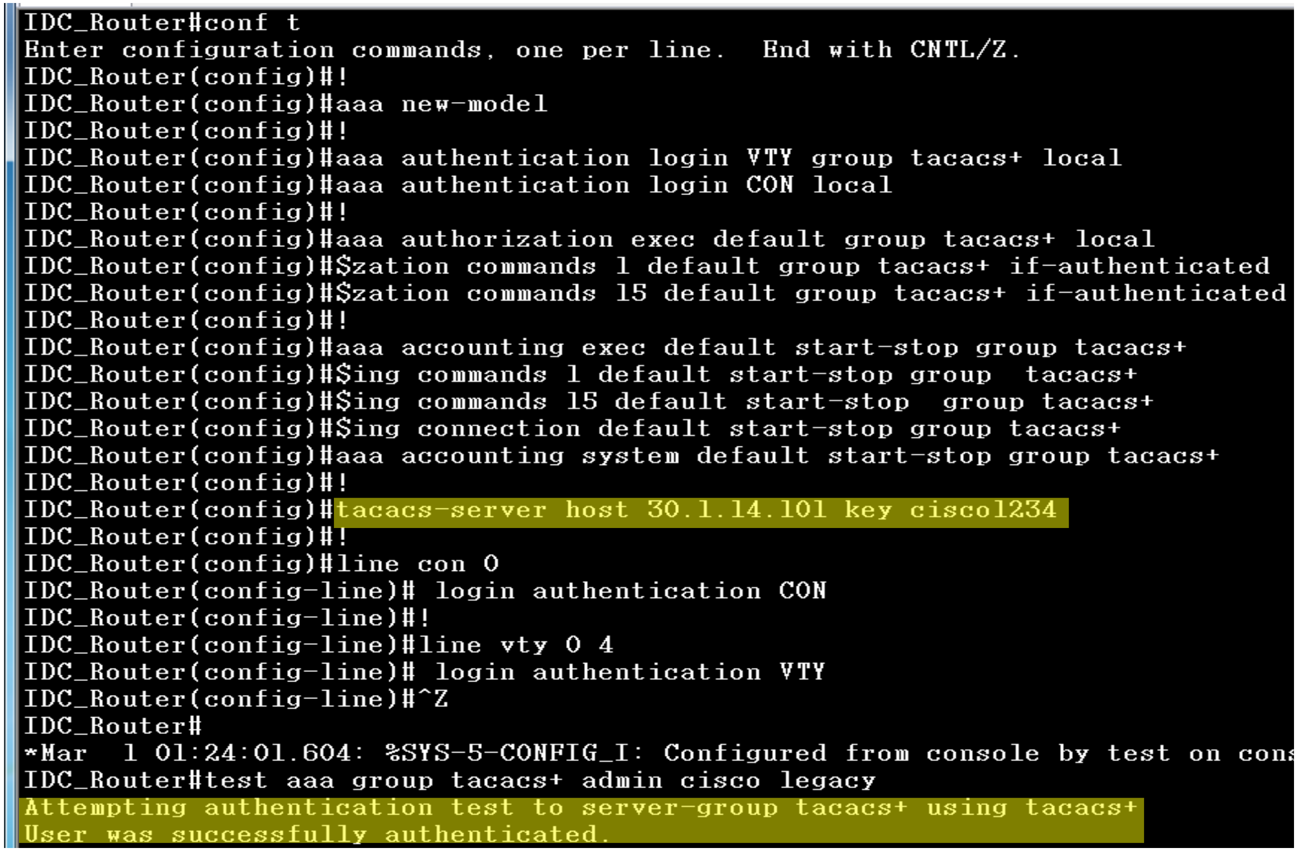


03 보안기술 내용_Tacacs+ Server

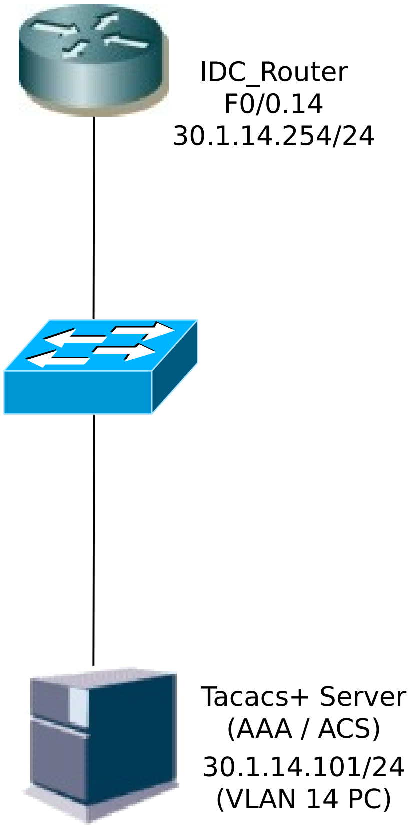
구현 목표

- Tacacs+ Server 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 라우터로 접속하는 사용자에 대한 인증 및 명령어 제한을 통한 보안 관련 기능 수행 (EX : IDC_Router)

IDC_Router AAA 설정 및 AAA 서버와 연동 TEST



```
IDC_Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IDC_Router(config)#!
IDC_Router(config)#aaa new-model
IDC_Router(config)#!
IDC_Router(config)#aaa authentication login VTY group tacacs+ local
IDC_Router(config)#aaa authentication login CON local
IDC_Router(config)#!
IDC_Router(config)#aaa authorization exec default group tacacs+ local
IDC_Router(config)#$zation commands 1 default group tacacs+ if-authenticated
IDC_Router(config)#$zation commands 15 default group tacacs+ if-authenticated
IDC_Router(config)#!
IDC_Router(config)#aaa accounting exec default start-stop group tacacs+
IDC_Router(config)#$ing commands 1 default start-stop group  tacacs+
IDC_Router(config)#$ing commands 15 default start-stop  group tacacs+
IDC_Router(config)#$ing connection default start-stop group tacacs+
IDC_Router(config)#aaa accounting system default start-stop group tacacs+
IDC_Router(config)#!
IDC_Router(config)#tacacs-server host 30.1.14.101 key cisco1234
IDC_Router(config)#!
IDC_Router(config)#line con 0
IDC_Router(config-line)# login authentication CON
IDC_Router(config-line)#!
IDC_Router(config-line)#line vty 0 4
IDC_Router(config-line)# login authentication VTY
IDC_Router(config-line)#^Z
IDC_Router#
*Mar  1 01:24:01.604: %SYS-5-CONFIG_I: Configured from console by test on cons
IDC_Router#test aaa group tacacs+ admin cisco legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

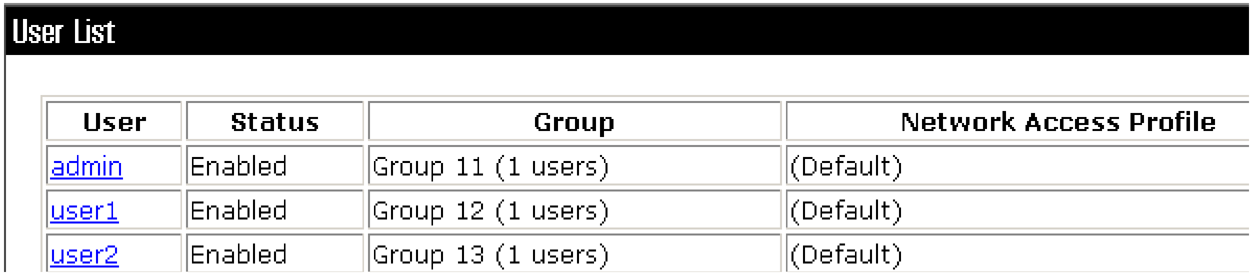


03 보안기술 내용_Tacacs+ Server

구현 목표

- Tacacs+ Server 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 라우터로 접속하는 사용자에 대한 인증 및 명령어 제한을 통한 보안 관련 기능 수행 (EX : IDC_Router)

User List 생성

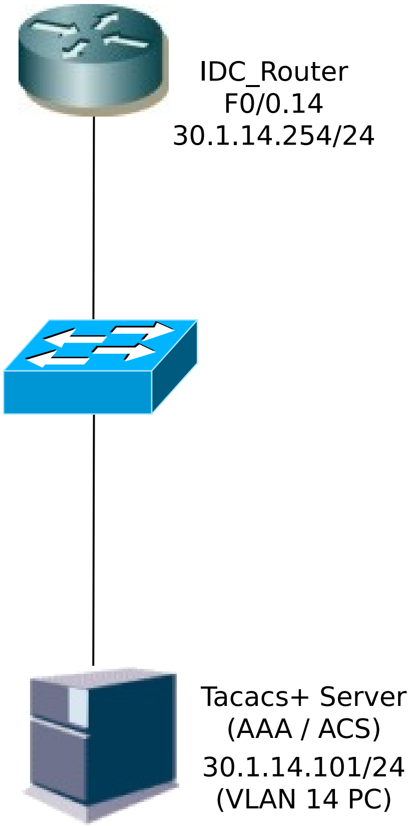


User List

User	Status	Group	Network Access Profile
admin	Enabled	Group 11 (1 users)	(Default)
user1	Enabled	Group 12 (1 users)	(Default)
user2	Enabled	Group 13 (1 users)	(Default)

User 계정 및 명령어 제한 설정

구분	계정	명령어 제한
주 - 관리자	admin	모든 명령어 가능
부 - 관리자	user1	Reload, copy, erase, delete 제외한 모든 명령어 가능
신입 직원	user2	show ip route, show ip int brief, show version 만 가능

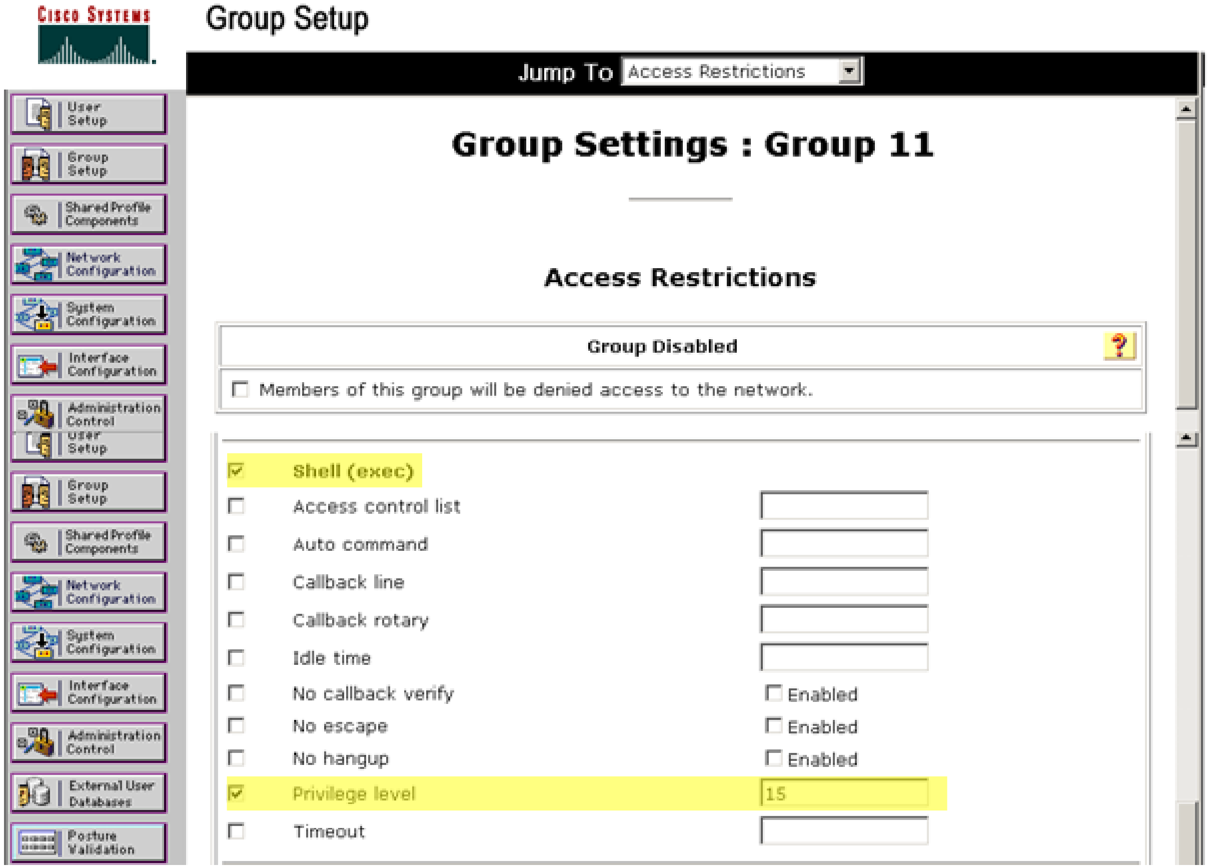


03 보안기술 내용_Tacacs+ Server

구현 목표

- Tacacs+ Server 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 라우터로 접속하는 사용자에 대한 인증 및 명령어 제한을 통한 보안 관련 기능 수행 (EX : IDC_Router)

- 각 User 명령어 제한 설정 (Group 11 : admin)



Group Setup

Jump To Access Restrictions

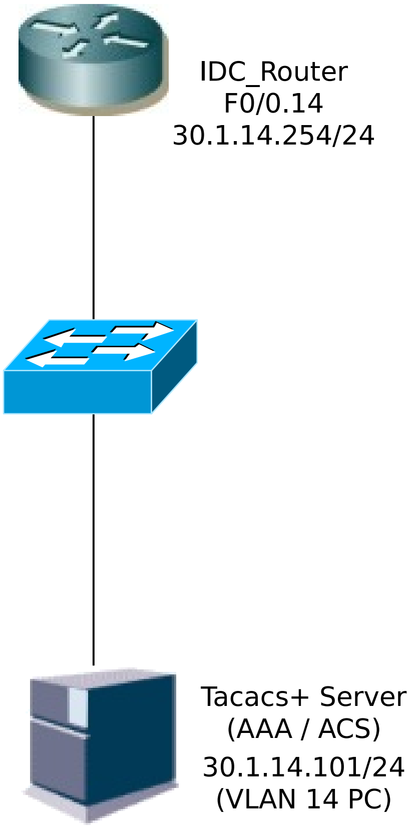
Group Settings : Group 11

Access Restrictions

Group Disabled

□ Members of this group will be denied access to the network.

☑	Shell (exec)	
□	Access control list	
□	Auto command	
□	Callback line	
□	Callback rotary	
□	Idle time	
□	No callback verify	□ Enabled
□	No escape	□ Enabled
□	No hangup	□ Enabled
☑	Privilege level	15
□	Timeout	

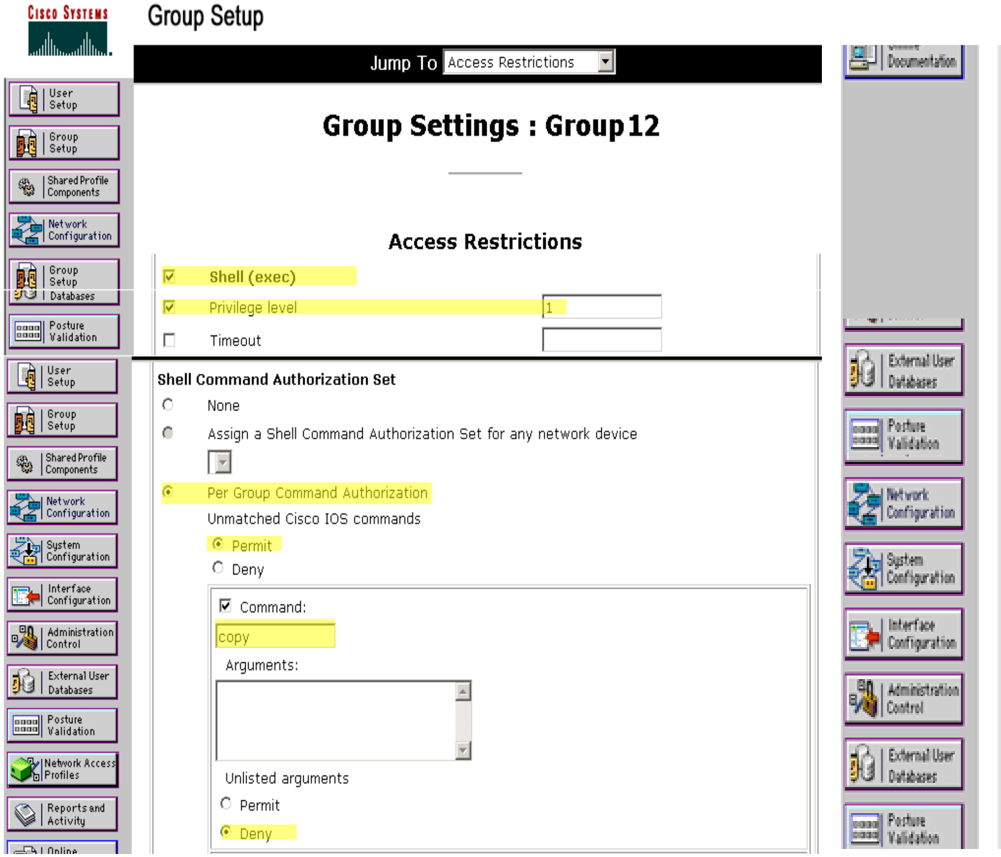


03 보안기술 내용_Tacacs+ Server

구현 목표

- Tacacs+ Server 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 라우터로 접속하는 사용자에 대한 인증 및 명령어 제한을 통한 보안 관련 기능 수행 (EX : IDC_Router)

각 User 명령어 제한 설정 (Group 12 : user1)



Group Setup

Jump To Access Restrictions

Group Settings : Group12

Access Restrictions

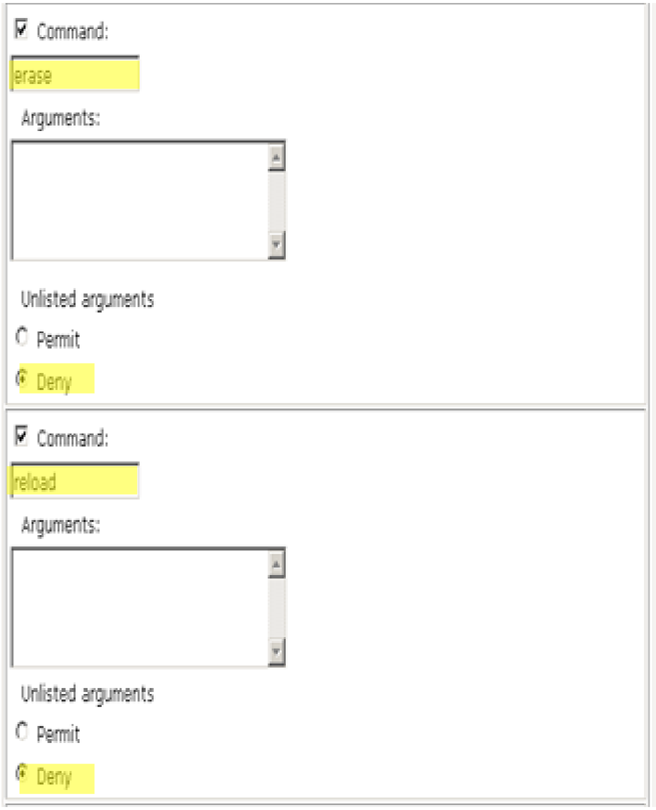
☑ Shell (exec)
☑ Privilege level 1
□ Timeout

Shell Command Authorization Set

○ None
○ Assign a Shell Command Authorization Set for any network device
● Per Group Command Authorization
Unmatched Cisco IOS commands
● Permit
○ Deny

☑ Command:
copy
Arguments:

Unlisted arguments
○ Permit
● Deny



☑ Command:
erase
Arguments:

Unlisted arguments
○ Permit
● Deny

☑ Command:
reload
Arguments:

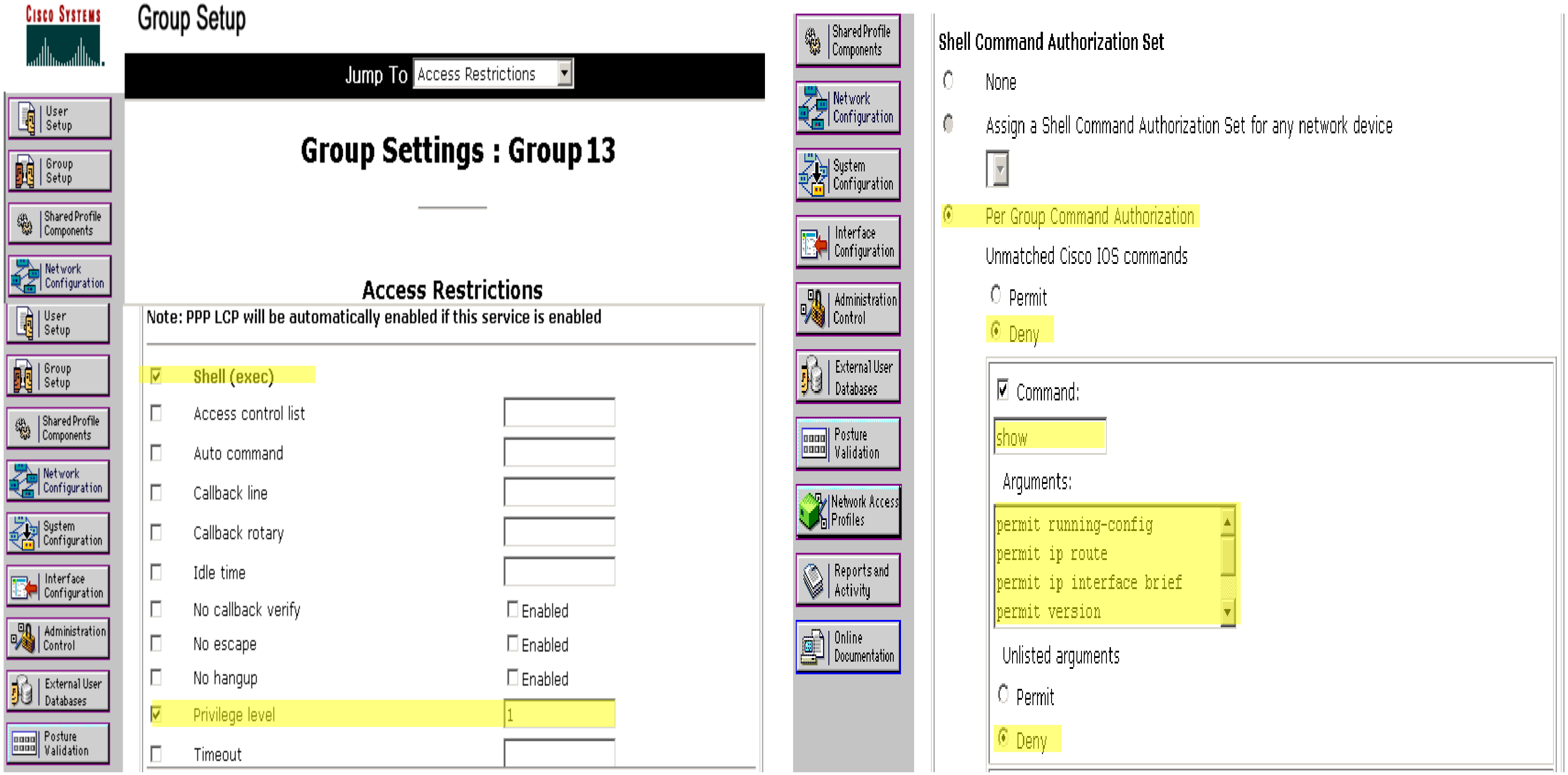
Unlisted arguments
○ Permit
● Deny

03 보안기술 내용_Tacacs+ Server

구현 목표

- Tacacs+ Server 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 라우터로 접속하는 사용자에 대한 인증 및 명령어 제한을 통한 보안 관련 기능 수행 (EX : IDC_Router)

각 User 명령어 제한 설정 (Group 13 : user2)



Group Setup

Jump To: Access Restrictions

Group Settings : Group 13

Access Restrictions

Note: PPP LCP will be automatically enabled if this service is enabled

☑ Shell (exec)
□ Access control list
□ Auto command
□ Callback line
□ Callback rotary
□ Idle time
□ No callback verify □ Enabled
□ No escape □ Enabled
□ No hangup □ Enabled
☑ Privilege level: 1
□ Timeout

Shell Command Authorization Set

○ None
○ Assign a Shell Command Authorization Set for any network device
● Per Group Command Authorization

Unmatched Cisco IOS commands
○ Permit
● Deny

☑ Command:
show

Arguments:

```
permit running-config
permit ip route
permit ip interface brief
permit version
```

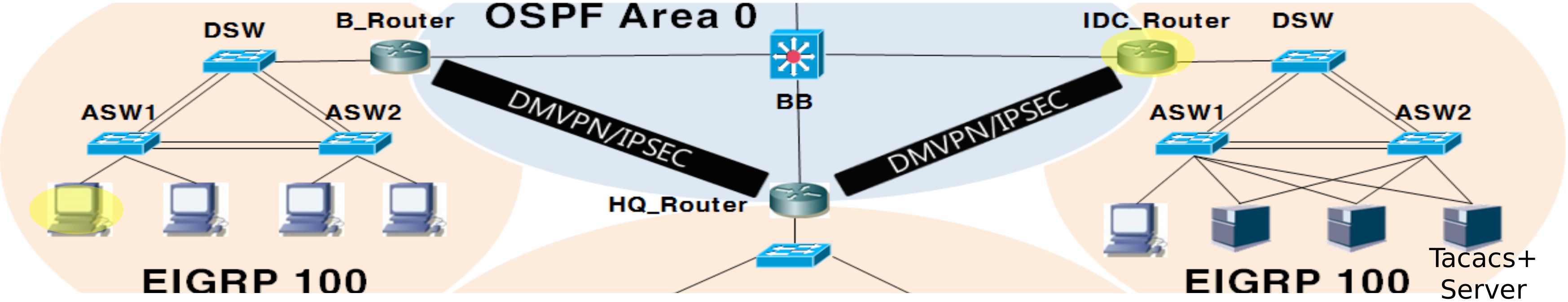
Unlisted arguments
○ Permit
● Deny

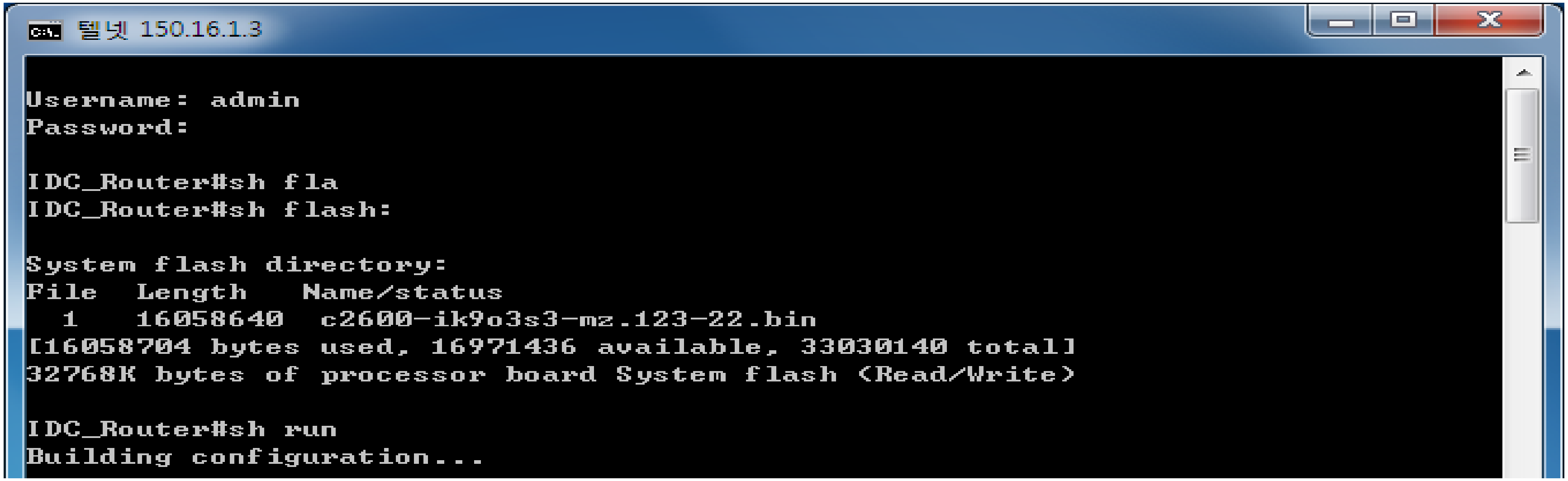
03 보안기술 내용_Tacacs+ Server

구현 목표

- Tacacs+ Server 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 라우터로 접속하는 사용자에 대한 인증 및 명령어 제한을 통한 보안 관련 기능 수행 (EX : IDC_Router)

- 각 User 명령어 제한 설정 TEST (EX : 지사B PC to IDC_Router Telnet 접속)





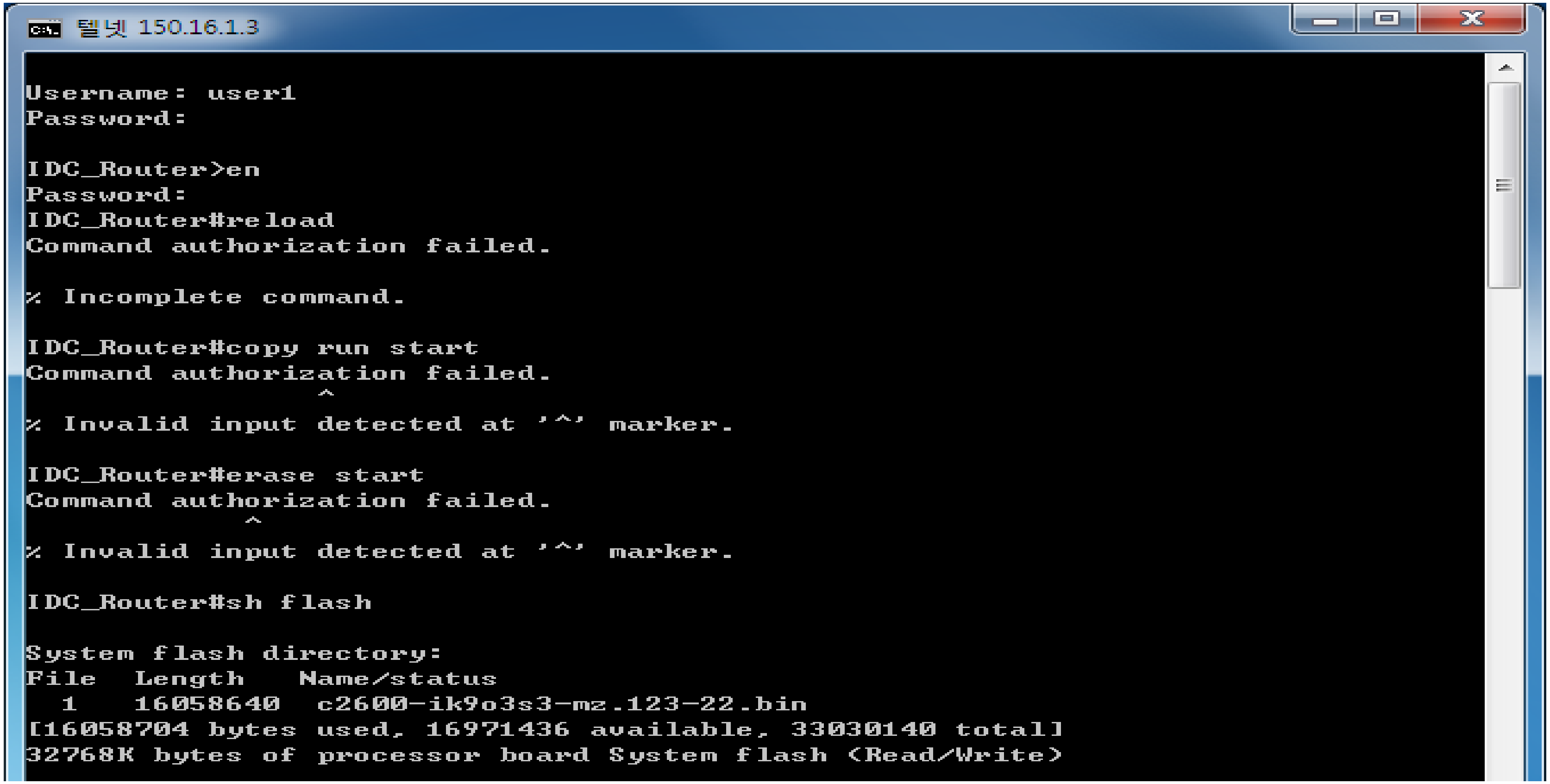
```
Username: admin
Password:

IDC_Router#sh fla
IDC_Router#sh flash:

System flash directory:
File  Length    Name/status
  1   16058640   c2600-ik9o3s3-mz.123-22.bin
[16058704 bytes used, 16971436 available, 33030140 total]
32768K bytes of processor board System flash (Read/Write)

IDC_Router#sh run
Building configuration...
```

03 보안기술 내용_Tacacs+ Server

구현 목표

- Tacacs+ Server 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 라우터로 접속하는 사용자에 대한 인증 및 명령어 제한을 통한 보안 관련 기능 수행 (EX : IDC_Router)

- 각 User 명령어 제한 설정 TEST (EX : 지사B PC to IDC_Router Telnet 접속)



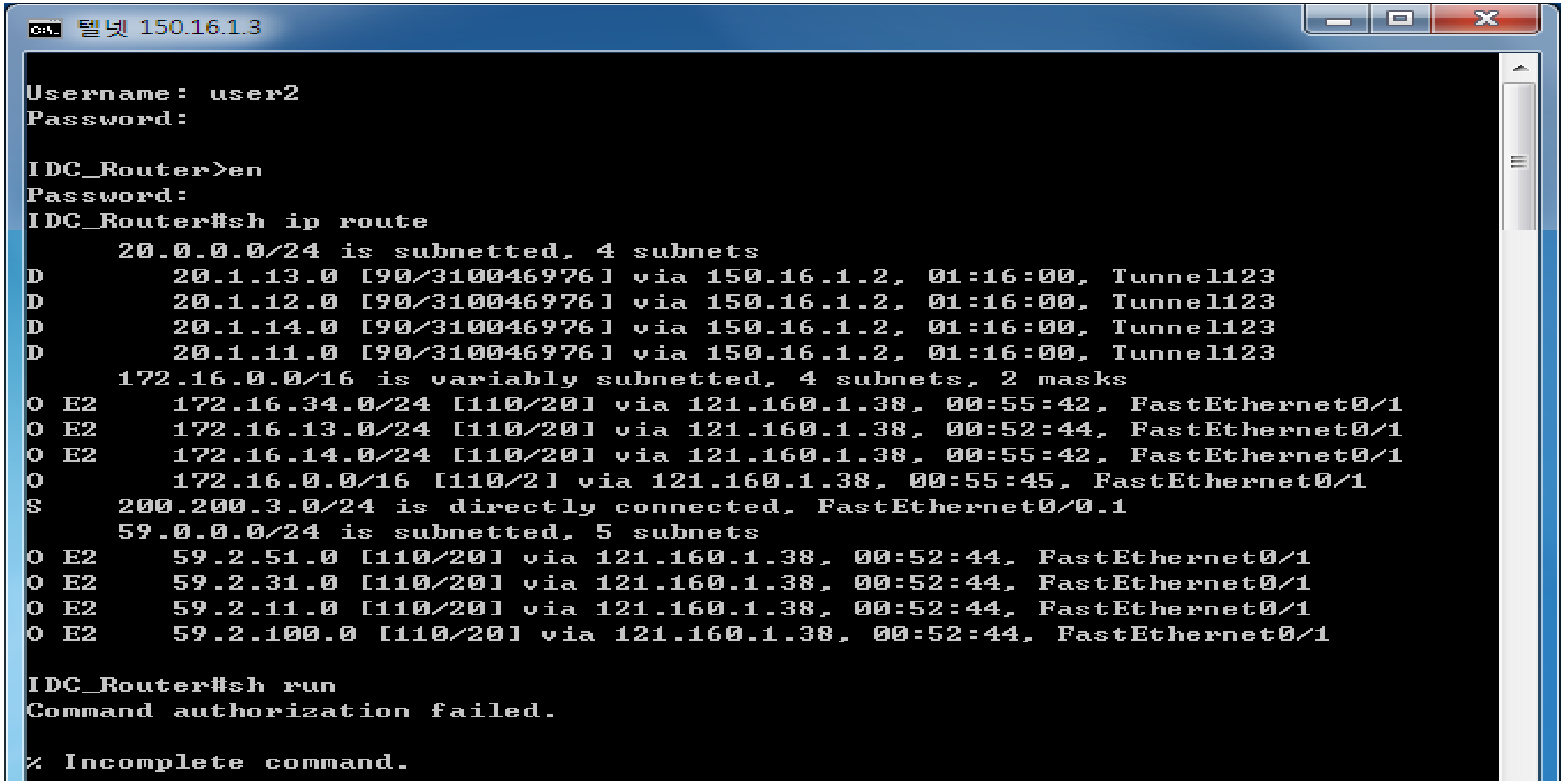
```
Username: user1
Password:

IDC_Router>en
Password:
IDC_Router#reload
Command authorization failed.

% Incomplete command.

IDC_Router#copy run start
Command authorization failed.
                ^
% Invalid input detected at '^' marker.

IDC_Router#erase start
Command authorization failed.
            ^
% Invalid input detected at '^' marker.

IDC_Router#sh flash

System flash directory:
File  Length   Name/status
  1   16058640  c2600-ik9o3s3-mz.123-22.bin
[16058704 bytes used, 16971436 available, 33030140 total]
32768K bytes of processor board System flash (Read/Write)
```

03 보안기술 내용_Tacacs+ Server

구현 목표

- Tacacs+ Server 구성 (IDC 서버지사의 VLAN14 PC의 VMware로 구성)
- 각 지사 라우터로 접속하는 사용자에 대한 인증 및 명령어 제한을 통한 보안 관련 기능 수행 (EX : IDC_Router)

- 각 User 명령어 제한 설정 TEST (EX : 지사B PC to IDC_Router Telnet 접속)



```
Username: user2
Password:

IDC_Router>en
Password:
IDC_Router#sh ip route
     20.0.0.0/24 is subnetted, 4 subnets
D       20.1.13.0 [90/310046976] via 150.16.1.2, 01:16:00, Tunnel123
D       20.1.12.0 [90/310046976] via 150.16.1.2, 01:16:00, Tunnel123
D       20.1.14.0 [90/310046976] via 150.16.1.2, 01:16:00, Tunnel123
D       20.1.11.0 [90/310046976] via 150.16.1.2, 01:16:00, Tunnel123
     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O E2    172.16.34.0/24 [110/20] via 121.160.1.38, 00:55:42, FastEthernet0/1
O E2    172.16.13.0/24 [110/20] via 121.160.1.38, 00:52:44, FastEthernet0/1
O E2    172.16.14.0/24 [110/20] via 121.160.1.38, 00:55:42, FastEthernet0/1
O       172.16.0.0/16 [110/2] via 121.160.1.38, 00:55:45, FastEthernet0/1
S    200.200.3.0/24 is directly connected, FastEthernet0/0.1
     59.0.0.0/24 is subnetted, 5 subnets
O E2    59.2.51.0 [110/20] via 121.160.1.38, 00:52:44, FastEthernet0/1
O E2    59.2.31.0 [110/20] via 121.160.1.38, 00:52:44, FastEthernet0/1
O E2    59.2.11.0 [110/20] via 121.160.1.38, 00:52:44, FastEthernet0/1
O E2    59.2.100.0 [110/20] via 121.160.1.38, 00:52:44, FastEthernet0/1

IDC_Router#sh run
Command authorization failed.

% Incomplete command.
```

기타 참조

05

- ✓ IP 할당 내역
- ✓ Configuration

01 IP 할당 내역

HQ

상세구간	장비	Interface	Channel Group	네트워크	IP Address	VLAN	비고
HQ_Router	Router	F0/1	-	121.160.1.16/30	121.160.1.17	-	공중망
		F0/0	-	10.1.1.0/28	10.1.1.1	-	
HQ_Core1	L2 SW	F0/10	-	-	-	-	
		F0/1, F0/3	5	-	-	-	
		F0/2, F0/4	6	-	-	-	
HQ_Core2	L3 SW	F0/1, F0/3	5	10.1.1.0/28	10.1.1.2	-	
		F0/19-20	4	-	-	-	
		F0/21-22	1	-	-	-	
		SVI	-	10.1.11.0/24	10.1.11.100	11	
		SVI	-	10.1.12.0/24	10.1.12.100	12	
		SVI	-	10.1.13.0/24	10.1.13.100	13	
		SVI	-	10.1.14.0/24	10.1.14.100	14	
HQ_Core3	L3 SW	F0/2, F0/4	6	10.1.1.0/28	10.1.1.3	-	
		F0/21-22	1	-	-	-	
		F0/23-24	2	-	-	-	
		SVI	-	10.1.11.0/24	10.1.11.200	11	
		SVI	-	10.1.12.0/24	10.1.12.200	12	
		SVI	-	10.1.13.0/24	10.1.13.300	13	
		SVI	-	10.1.14.0/24	10.1.14.400	14	
HQ_DSW1	L2 SW	F0/1-2. F0/4-5	-	-	-	-	
		F0/21-22	3	-	-	-	
		F0/23-24	4	-	-	-	

01 IP 할당 내역

HQ

상세구간	장비	Interface	Channel Group	네트워크	IP Address	VLAN	비고
HQ_DSW2	L2 SW	F0/1-2 F0/4-5	-	-	-	-	
		F0/21-22	3	-	-	-	
		F0/23-24	2	-	-	-	
HQ_ASW1	L2 SW	F0/1-2-	-	-	-	-	
		F0/10					User 1
HQ_ASW2	L2 SW	F0/1-2-	-	-	-	-	
		F0/10					User 2
HQ_ASW3	L2 SW	F0/1-2-	-	-	-	-	
		F0/10					User 3
HQ_ASW4	L2 SW	F0/1-2-	-	-	-	-	
		F0/10					User 4
User 1	PC	-	-	10.1.11.0/24	10.1.11.1	11	G.W 10.1.11.254
User 2	PC	-	-	10.1.12.0/24	10.1.12.1	12	G.W 10.1.12.254
User 3	PC	-	-	10.1.13.0/24	10.1.13.1	13	G.W 10.1.13.254
User 4	PC	-	-	10.1.14.0/24	10.1.14.1	14	G.W 10.1.14.254
Virtual Router		HSRP	-	10.1.11.0/24 10.1.12.0/24 10.1.13.0/24 10.1.14.0/24	10.1.11.254 10.1.12.254 10.1.13.254 10.1.14.254	11 12 13 14	Core 2-3

01 IP 할당 내역

Branch

상세구간	장비	Interface	Channel Group	네트워크	IP Address	VLAN	비고
B_Router	Router	F0/1	-	121.160.1.20/30	121.160.1.22	-	공중망
		F0/0	-	20.1.1.0/28	20.1.1.1	-	
B_Core	L2 SW	F0/10	-	-	-	-	
		F0/11-12	12	-	-	-	
		F0/15-16	23	-	-	-	
B_ASW1	L2 SW	F0/1	-	-	-	-	User 1
		F0/11-12	12	-	-		
		F0/13-14	13	-	-		
B_ASW2	L2 SW	F0/2	-	-	-	-	
		F0/13-14	13	-	-		
		F0/15-16	23	-	-		
User 1	PC	-	-	20.1.11.0/24	20.1.11.1	11	G.W 20.1.11.254
User 2	PC	-	-	20.1.12.0/24	20.1.12.1	12	G.W 20.1.12.254
User 3	PC	-	-	20.1.13.0/24	20.1.13.1	13	G.W 20.1.13.254
User 4	PC	-	-	20.1.14.0/24	20.1.14.1	14	G.W 20.1.14.254

01 IP 할당 내역

상세구간	장비	Interface	Channel Group	네트워크	IP Address	VLAN	비고
IDC_Router	Router	F0/1	-	121.160.1.36/30	121.160.1.37	-	공중망
				150.16.1.0/24	150.16.1.3	-	Tunnel 123
		F0/0.11	-	30.1.11.0/24	30.1.11.254	-	VLAN 11 G.W
		F0/0.12	-	30.1.12.0/24	30.1.12.254	-	VLAN 12 G.W
		F0/0.13	-	30.1.13.0/24	30.1.13.254	-	VLAN 13 G.W
		F0/0.14	-	30.1.14.0/24	30.1.14.254	-	VLAN 14 G.W
IDC_Core	L2 SW	F0/20	-	-	-	-	
		F0/11-12	12	-	-	-	
		F0/15-16	23	-	-	-	
IDC_ASW1	L2 SW	F0/1	-	-	-	-	User 1
		F0/11-12	12				
		F0/13-14	13				
IDC_ASW2	L2 SW	F0/2	-	-	-	-	User 4
		F0/13-14	13				
		F0/15-16	23				

01 IP 할당 내역

IDC
Internet Data Center

상세구간	장비	Interface	Channel Group	네트워크	IP Address	VLAN	비고
User 1	PC			30.1.11.0/24	30.1.11.1	11	G.W 30.1.11.254
User 2	PC			30.1.12.0/24	30.1.12.1	12	G.W 30.1.12.254
User 3	PC			30.1.13.0/24	30.1.13.1	13	G.W 30.1.13.254
User 4	PC			30.1.14.0/24	10.1.14.1	14	G.W 30.1.14.254
NTP Server	Router	Lo 0		200.200.3.0./24	200.200.3.1		
DHCP Server		F0/1		30.1.100.0/24	30.1.100.1	100	G.W 30.1.100.254
SYSLOG Server	VMware	F0/2		30.1.14.0/24	30.1.14.101	14	G.W 30.1.14.254
TACACS+ Server		F0/2		30.1.14.0/24	30.1.14.101	14	G.W 30.1.14.254

02 Configuration_HQ

HQ_Router

HQ_Router

```
Current configuration : 2465 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$SkUX$lRE1yxXRdxFkkQgqGY6Jp/
!
clock timezone KOREA 9
no aaa new-model
ip subnet-zero
ip cef
!
!
no ip domain lookup
!
ip inspect name CISCO tcp
ip inspect name CISCO udp
ip inspect name CISCO icmp
ip audit po max-events 100
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
```

```
crypto ipsec transform-set CISCO esp-3des esp-md5-hmac
!
crypto ipsec profile DMVPN
 set transform-set CISCO
!
!
crypto dynamic-map easyVPN 10
 set transform-set CISCO
 reverse-route
!
!
crypto map EZVPN 10 ipsec-isakmp dynamic easyVPN
!
!
!
interface Tunnel123
 ip address 150.16.1.1 255.255.255.0
 no ip redirects
 no ip next-hop-self eigrp 100
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 123
 no ip split-horizon eigrp 100
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile DMVPN
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
```

02 Configuration_HQ

HQ_Router

```
!
interface FastEthernet0/1
 ip address 121.160.1.17 255.255.255.252
 ip access-group IN_Traffic in
 ip nat outside
 ip inspect CISCO out
 duplex auto
 speed auto
!
router eigrp 100
 redistribute static
 redistribute ospf 1 metric 1544 2000 255 1 1500
 network 10.1.1.0 0.0.0.255
 network 150.16.1.1 0.0.0.0
 no auto-summary
!
router eigrp 10
 auto-summary
!
router ospf 1
 router-id 13.1.1.1
 log-adjacency-changes
 network 121.160.1.17 0.0.0.0 area 0
!
ip nat inside source list 10 interface FastEthernet0/1 overload
ip http server
no ip http secure-server
ip classless
!
!
!
ip access-list extended IN_Traffic
 permit eigrp any any
 permit ospf any any
 permit gre any any
 permit esp any any
 permit udp any any eq isakmp
 permit udp any eq ntp any eq ntp
 permit udp any eq syslog any eq syslog
 permit tcp any eq telnet any eq telnet
 permit tcp any eq tacacs any eq tacacs
 deny   ip any any
logging facility local1
logging source-interface Tunnel123
logging 30.1.14.101
access-list 10 permit 10.1.0.0 0.0.255.255
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 password ciscovty
 login
!
ntp clock-period 17179599
ntp server 30.1.100.1
!
end
```

02 Configuration_HQ

HQ_Core2

HQ_CORE2

```
Current configuration : 3789 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname HQ_CORE2
!
enable secret 5 $1$CwCj$kfhszneS6WdKJwMnBfY/v1
!
no aaa new-model
clock timezone KOREA 9
ip subnet-zero
ip routing
no ip domain-lookup
!
!
!
!
!
no file verify auto
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Tunnel123
 no ip address
!
```

```
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel4
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/1
 no switchport
 ip address 10.1.1.2 255.255.255.0
 channel-protocol lacp
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 4 mode active
!
!
```

02 Configuration_HQ

HQ_CORE2

```
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 4 mode active
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
!
interface Vlan11
 ip address 10.1.11.100 255.255.255.0
 ip helper-address 30.1.100.1
 standby 1 ip 10.1.11.254
 standby 1 priority 120
 standby 1 preempt
!
interface Vlan12
 ip address 10.1.12.100 255.255.255.0
 ip helper-address 30.1.100.1
 standby 2 ip 10.1.12.254
 standby 2 priority 120
 standby 2 preempt
!
interface Vlan13
 ip address 10.1.13.100 255.255.255.0
 ip helper-address 30.1.100.1
 standby 3 ip 10.1.13.254
 standby 3 preempt
!
interface Vlan14
 ip address 10.1.14.100 255.255.255.0
 ip helper-address 30.1.100.1
 standby 4 ip 10.1.14.254
 standby 4 preempt
!
router eigrp 100
 network 10.1.0.0 0.0.255.255
 network 192.168.1.0
 no auto-summary
!
ip classless
ip http server
ip http secure-server
!
logging facility local2
logging source-interface Tunnel123
logging 30.1.14.101
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password ciscovty
 login
line vty 5 15
 no login
!
ntp clock-period 17180155
ntp server 30.1.100.1
end
```

HQ_DSW1

HQ_DSW1

```
Current configuration : 5948 bytes
!
! Last configuration change at 12:58:19 KOREA Thu Apr 7 2016
! NVRAM config last updated at 13:11:47 KOREA Thu Apr 7 2016
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_ASW1
!
enable secret 5 $1$Ka.c$OHi0pfYyK5Pa/iQj3DyRB1
!
no aaa new-model
clock timezone KOREA 9
ip subnet-zero
no ip domain-lookup
!
!
!
crypto pki trustpoint TP-self-signed-3978664192
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3978664192
 revocation-check none
 rsakeypair TP-self-signed-3978664192
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
```

```
interface Tunnel123
 no ip address
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport access vlan 11
 switchport mode access
 spanning-tree portfast
!
interface Vlan1
 ip address 192.168.1.6 255.255.255.0
!
ip default-gateway 192.168.1.2
ip classless
ip http server
ip http secure-server
!
!
logging facility local4
logging source-interface Tunnel123
logging 30.1.14.101
!
control-plane
!
!
```

02 Configuration_HQ

HQ_DSW1

```
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password ciscovty
 login
line vty 5 15
 password ciscovty
 login
!
ntp clock-period 17180198
ntp server 30.1.100.1
ntp server 168.126.63.1
end
```

HQ_ASW1

HQ_ASW1

```
Current configuration : 5948 bytes
!
! Last configuration change at 12:58:19 KOREA Thu Apr 7 2016
! NVRAM config last updated at 13:11:47 KOREA Thu Apr 7 2016
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname HQ_ASW1
!
enable secret 5 $1$Ka.c$OHi0pfYyK5Pa/iQj3DyRB1
!
no aaa new-model
clock timezone KOREA 9
ip subnet-zero
no ip domain-lookup
!
!
!
crypto pki trustpoint TP-self-signed-3978664192
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3978664192
 revocation-check none
 rsakeypair TP-self-signed-3978664192
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
```

```
interface Tunnel123
 no ip address
!
interface FastEthernet0/1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport access vlan 11
 switchport mode access
 spanning-tree portfast
!
!
interface Vlan1
 ip address 192.168.1.6 255.255.255.0
!
ip default-gateway 192.168.1.2
ip classless
ip http server
ip http secure-server
!
!
logging facility local4
logging source-interface Tunnel123
logging 30.1.14.101
!
control-plane
!
```

02 Configuration_HQ

HQ_ASW1

```
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password ciscovty
 login
line vty 5 15
 password ciscovty
 login
!
ntp clock-period 17180198
ntp server 30.1.100.1
ntp server 168.126.63.1
end
```

02 Configuration_Branch

B_Router

B_Router

```
Current configuration : 4636 bytes
!
! Last configuration change at 04:56:36 UTC Fri Apr 8 2016 by admin
! NVRAM config last updated at 06:59:46 UTC Thu Apr 7 2016
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname B_Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$aPYr$3hctZzRRRiirQ9dsRrKF7/
!
no network-clock-participate slot 1
no network-clock-participate wic 0
aaa new-model
!
!
aaa authentication login EZVPN_Client local
aaa authentication login VTY group tacacs+ local
aaa authentication login CON local
aaa authorization exec default group tacacs+ local
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
aaa authorization network EZVPN_Group local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
!
ip inspect name CISCO tcp
ip inspect name CISCO udp
ip inspect name CISCO icmp
ip audit po max-events 100
!
!
!
!
username admin privilege 15 password 0 cisco
!
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
crypto isakmp client configuration group EZ_Group
 key cisco1234
 pool EZ_POOL
 acl 113
!
```

02 Configuration_Branch

B_Router

```
crypto ipsec transform-set CISCO esp-3des esp-md5-hmac
!
crypto ipsec profile DMVPN
 set transform-set CISCO
!
!
crypto dynamic-map EasyVPN 10
 set transform-set CISCO
 reverse-route
!
!
crypto map IPSEC client authentication list EZVPN_Client
crypto map IPSEC isakmp authorization list EZVPN_Group
crypto map IPSEC client configuration address respond
crypto map IPSEC 30 ipsec-isakmp dynamic EasyVPN
!
!
!
!
interface Loopback0
 no ip address
!
interface Tunnel123
 ip address 150.16.1.2 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast 121.160.1.17
 ip nhrp map 150.16.1.1 121.160.1.17
 ip nhrp network-id 123
 ip nhrp nhs 150.16.1.1
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile DMVPN
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.2.254 255.255.255.0
!
interface FastEthernet0/0.11
 encapsulation dot1Q 11
 ip address 20.1.11.254 255.255.255.0
 ip helper-address 30.1.100.1
 ip nat inside
!
interface FastEthernet0/0.12
 encapsulation dot1Q 12
 ip address 20.1.12.254 255.255.255.0
 ip helper-address 30.1.100.1
 ip nat inside
!
interface FastEthernet0/0.13
 encapsulation dot1Q 13
 ip address 20.1.13.254 255.255.255.0
 ip helper-address 30.1.100.1
 ip nat inside
!
interface FastEthernet0/0.14
 encapsulation dot1Q 14
 ip address 20.1.14.254 255.255.255.0
 ip helper-address 30.1.100.1
 ip nat inside
!
!
```

02 Configuration_Branch

B_Router

```
interface FastEthernet0/1
 ip address 121.160.1.22 255.255.255.252
 ip access-group IN_Traffic in
 ip nat outside
 ip inspect CISCO out
 duplex auto
 speed auto
 crypto map IPSEC
!
router eigrp 100
 network 20.1.11.0 0.0.0.255
 network 20.1.12.0 0.0.0.255
 network 20.1.13.0 0.0.0.255
 network 20.1.14.0 0.0.0.255
 network 150.16.1.2 0.0.0.0
 no auto-summary
!
router ospf 1
 router-id 14.1.1.1
 log-adjacency-changes
 network 121.160.1.22 0.0.0.0 area 0
!
ip local pool EZ_POOL 20.1.11.100 20.1.11.200
ip nat inside source list 10 interface FastEthernet0/1 overload
ip http server
no ip http secure-server
ip classless
!
ip access-list extended IN_Traffic
 permit eigrp any any
 permit ospf any any
 permit gre any any
permit tcp any eq tacacs any eq tacacs
 permit udp any any eq isakmp
 permit udp any eq ntp any eq ntp
 permit esp any any
 permit udp any eq syslog any eq syslog
 permit tcp any eq telnet any eq telnet
 deny   ip any any
logging facility local1
logging source-interface Tunnel123
logging 30.1.14.101
access-list 10 permit 20.1.11.0 0.0.0.255
access-list 10 permit 20.1.12.0 0.0.0.255
access-list 10 permit 20.1.13.0 0.0.0.255
access-list 10 permit 20.1.14.0 0.0.0.255
access-list 113 permit ip 20.1.11.0 0.0.0.255 any
!
tacacs-server host 30.1.14.101 key cisco1234
tacacs-server directed-request
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login authentication CON
line aux 0
line vty 0 4
 password ciscovty
 login authentication VTY
!
ntp clock-period 17207713
ntp server 30.1.100.1
!
end
```

02 Configuration_Branch

B_DSW

B_DSW

```
Current configuration : 2915 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname B_DSW
!
enable secret 5 $1$yoiJ$p84mqxg2ijAikE.n4zj660
!
no aaa new-model
ip subnet-zero
no ip domain-lookup
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Tunnel123
 no ip address
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
interface Port-channel2
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/10
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/19
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 2 mode active
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 2 mode active
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
```

02 Configuration_Branch

B_DSW

```
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface Vlan1
 ip address 192.168.2.3 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
logging facility local2
logging source-interface Tunnel123
logging 30.1.14.101
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password ciscovty
 login
line vty 5 15
 login
!
end
```

02 Configuration_Branch

B_ASW1

B_ASW1

```
Current configuration : 4721 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname B_ASW1
!
enable secret 5 $1$ir5m$8VTdEbTYc9rpQG6teQAeY1
!
no aaa new-model
ip subnet-zero
no ip domain-lookup
!
!
!
crypto pki trustpoint TP-self-signed-1178567424
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1178567424
 revocation-check none
 rsakeypair TP-self-signed-1178567424
!
!
crypto pki certificate chain TP-self-signed-1178567424
 certificate self-signed 01
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 11-12 priority 24576
!
vlan internal allocation policy ascending
!
```

```
interface Tunnel123
 no ip address
!
interface Port-channel1
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel3
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/1
 switchport access vlan 11
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/2
 switchport access vlan 12
 switchport mode access
 spanning-tree portfast
!
interface FastEthernet0/21
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
interface FastEthernet0/22
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 1 mode active
!
```

02 Configuration_Branch

B_ASW1

```
interface FastEthernet0/23
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 3 mode active
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 3 mode active
!
interface GigabitEthernet0/1
 switchport mode dynamic desirable
!
interface GigabitEthernet0/2
 switchport mode dynamic desirable
!
interface Vlan1
 ip address 192.168.2.1 255.255.255.0
!
ip classless
ip http server
ip http secure-server
!
!
logging source-interface Tunnel123
logging 30.1.14.101
!
control-plane
!
!
```

```
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 password ciscovty
 login
line vty 5 15
 login
!
ntp clock-period 17179650
ntp server 30.1.100.1
ntp server 192.168.2.254
ntp server 168.126.63.1
end
```

02 Configuration_IDC

IDC_Router

IDC_Router

```
Current configuration : 3766 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IDC_Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$WuUH$OsQ8ZjVTZOvea6CGdwuxO.
!
clock timezone KOREA 9
no network-clock-participate slot 1
no network-clock-participate wic 0
aaa new-model
!
!
aaa authentication login VTY group tacacs+ local
aaa authentication login CON local
aaa authorization exec default group tacacs+ local
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
aaa session-id common
ip subnet-zero
```

```
ip cef
!
no ip domain lookup
!
ip inspect name CISCO tcp
ip inspect name CISCO udp
ip inspect name CISCO icmp
ip audit po max-events 100
!
username test password 0 test
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
!
crypto ipsec transform-set CISCO esp-3des esp-md5-hmac
!
crypto ipsec profile DMVPN
 set transform-set CISCO
!
!
interface Tunnel123
 ip address 150.16.1.3 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map 150.16.1.1 121.160.1.17
 ip nhrp map multicast 121.160.1.17
 ip nhrp network-id 123
```

02 Configuration_IDC

IDC_Router

```
 ip nhrp nhs 150.16.1.1
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel key 123
 tunnel protection ipsec profile DMVPN
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.3.254 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.11
 encapsulation dot1Q 11
 ip address 30.1.11.254 255.255.255.0
 ip helper-address 30.1.100.1
 ip nat inside
!
interface FastEthernet0/0.12
 encapsulation dot1Q 12
 ip address 30.1.12.254 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0.13
 encapsulation dot1Q 13
 ip address 30.1.13.254 255.255.255.0
 ip nat inside
!
!
```

```
interface FastEthernet0/0.14
 encapsulation dot1Q 14
 ip address 30.1.14.254 255.255.255.0
 ip helper-address 30.1.100.1
 ip nat inside
!
interface FastEthernet0/0.100
 encapsulation dot1Q 100
 ip address 30.1.100.254 255.255.255.0
 ip nat inside
!
interface FastEthernet0/1
 ip address 121.160.1.37 255.255.255.252
 ip access-group IN_Traffic in
 ip nat outside
 ip inspect CISCO out
 duplex auto
 speed auto
!
router eigrp 100
 network 30.1.0.0 0.0.255.255
 network 150.16.1.3 0.0.0.0
 no auto-summary
!
router ospf 1
 router-id 13.3.3.3
 log-adjacency-changes
 network 121.160.1.37 0.0.0.0 area 0
!
ip nat inside source list 10 interface FastEthernet0/1 overload
ip http server
no ip http secure-server
ip classless
```

02 Configuration_IDC

IDC_Router

```
ip route 200.200.3.0 255.255.255.0 FastEthernet0/0.1
!
!
ip access-list extended IN_Traffic
 permit eigrp any any
 permit ospf any any
 permit gre any any
 permit udp any any eq isakmp
 permit esp any any
 permit tcp any eq tacacs any eq tacacs
 permit udp any eq ntp any eq ntp
 permit udp any eq syslog any eq syslog
 permit tcp any eq telnet any eq telnet
 deny   ip any any
logging facility local1
logging source-interface FastEthernet0/0
logging 30.1.14.101
access-list 10 permit 30.1.0.0 0.0.255.255
!
tacacs-server host 30.1.14.101 key cisco1234
tacacs-server directed-request
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login authentication CON
line aux 0
line vty 0 4
 password ciscovty
 logging synchronous
 login authentication VTY
!
end
```

02 Configuration_IDC

IDC_DSW

IDC_DSW

```
Current configuration : 4779 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IDC_DSW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$3rL9$f18vGuLCIhQ7aGvho0XeK/
!
username test password 0 test
aaa new-model
!
!
aaa authentication login VTY group tacacs+ local
aaa authentication login CON local
aaa authorization exec default group tacacs+ local
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
!
```

```
aaa session-id common
clock timezone KOREA 9
system mtu routing 1500
ip subnet-zero
no ip domain-lookup
!
!
!
!
crypto pki trustpoint TP-self-signed-3124101760
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3124101760
 revocation-check none
 rsakeypair TP-self-signed-3124101760
!
!
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
interface Port-channel12
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel23
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
!
!
```

02 Configuration_IDC

IDC_DSW

```
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 12 mode active
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 12 mode active
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 23 mode active
!
interface FastEthernet0/16
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 23 mode active
!
interface FastEthernet0/20
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast
!
interface Vlan1
 ip address 192.168.3.1 255.255.255.0
!
```

```
ip default-gateway 192.168.3.254
ip classless
ip http server
ip http secure-server
!
logging facility local2
logging source-interface FastEthernet0/16
logging 30.1.14.101
tacacs-server host 30.1.14.101 key cisco1234
tacacs-server directed-request
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login authentication CON
line vty 0 4
 password ciscovty
 login authentication VTY
line vty 5 15
 password ciscovty
!
ntp clock-period 36028159
ntp server 30.1.100.1
ntp server 168.126.63.1
end
```

02 Configuration_IDC

IDC_ASW1

IDC_ASW1

```
Current configuration : 5495 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IDC_ASW1
!
enable secret 5 $1$tsug$zLBGJq3MKg5F220thHtRb0
!
username test password 0 test
aaa new-model
!
!
aaa authentication login VTY group tacacs+ local
aaa authentication login CON local
aaa authorization exec default group tacacs+ local
aaa authorization commands 1 default group tacacs+ if-authenticated
aaa authorization commands 15 default group tacacs+ if-authenticated
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 1 default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+
aaa accounting connection default start-stop group tacacs+
aaa accounting system default start-stop group tacacs+
!
!
aaa session-id common
clock timezone KOREA 9
ip subnet-zero
no ip domain-lookup
```

```
crypto pki trustpoint TP-self-signed-3169475328
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3169475328
 revocation-check none
 rsakeypair TP-self-signed-3169475328
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
spanning-tree vlan 11-12 priority 4096
spanning-tree vlan 13-14 priority 8192
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface Port-channel12
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface Port-channel13
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/1
 switchport access vlan 11
 switchport mode access
 spanning-tree portfast
!
!
!
```

02 Configuration_IDC

IDC_ASW1

```
interface FastEthernet0/11
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 12 mode active
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 12 mode active
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 13 mode active
!
interface FastEthernet0/14
 switchport trunk encapsulation dot1q
 switchport mode trunk
 channel-protocol lacp
 channel-group 13 mode active
!
interface Vlan1
 ip address 192.168.3.2 255.255.255.0
!
ip default-gateway 192.168.3.254
ip classless
ip http server
ip http secure-server
!
!
```

```
logging facility local3
logging source-interface FastEthernet0/13
logging 30.1.14.101
tacacs-server host 30.1.14.101 key cisco1234
tacacs-server directed-request
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
 login authentication CON
line vty 0 4
 password ciscovty
 login authentication VTY
line vty 5 15
 password ciscovty
!
ntp clock-period 17180239
ntp server 30.1.100.1
end
```