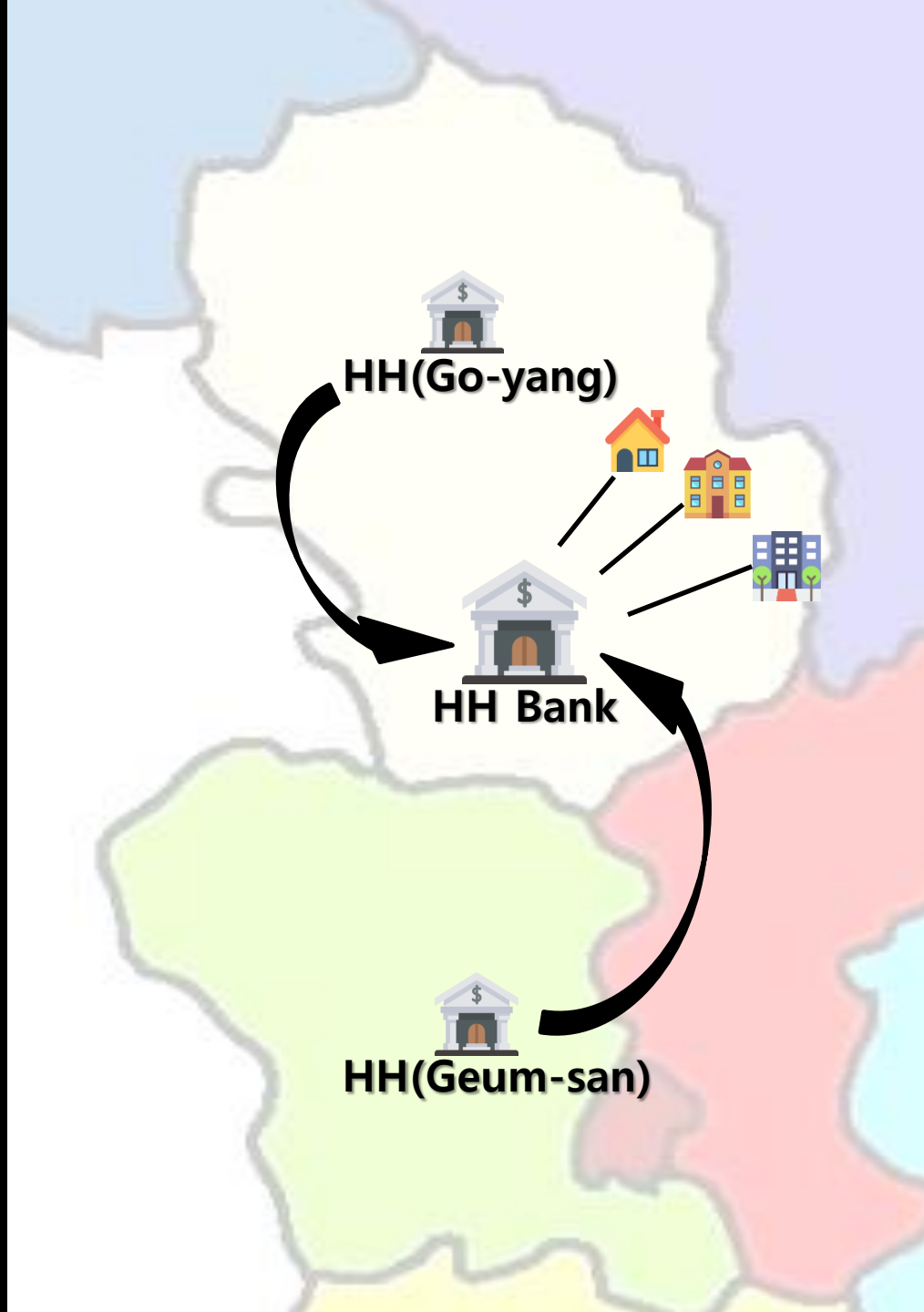
은행
Bank

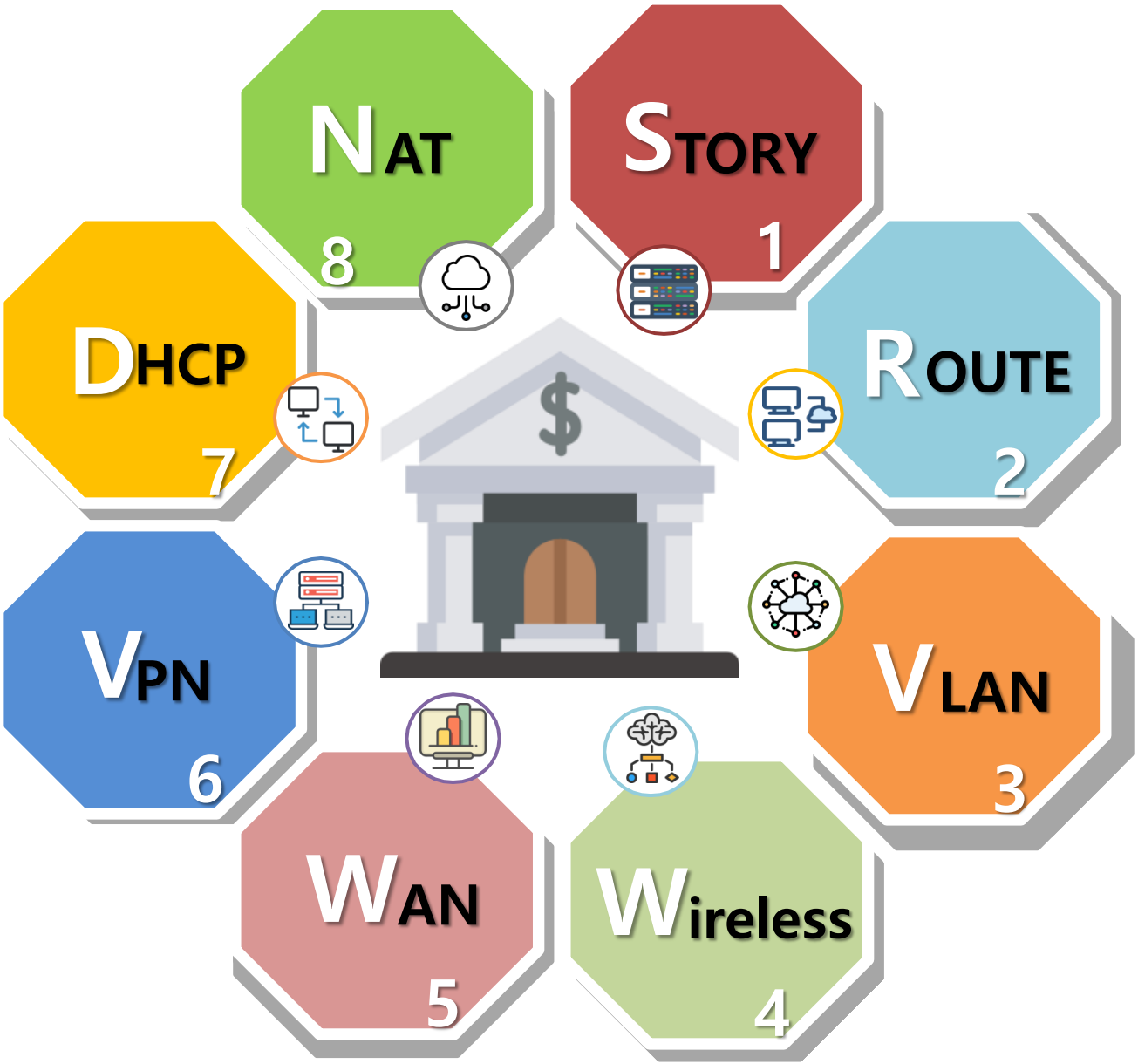
HH은행

정보보호학과
Information Security
이병천 교수님
Prof. ByungCheon Lee
네트워크 구축 및 보안운영
Computer Network Design and Security

권혁민 91416014
HYUK MIN
조현욱 91416416
HYEON WOOK

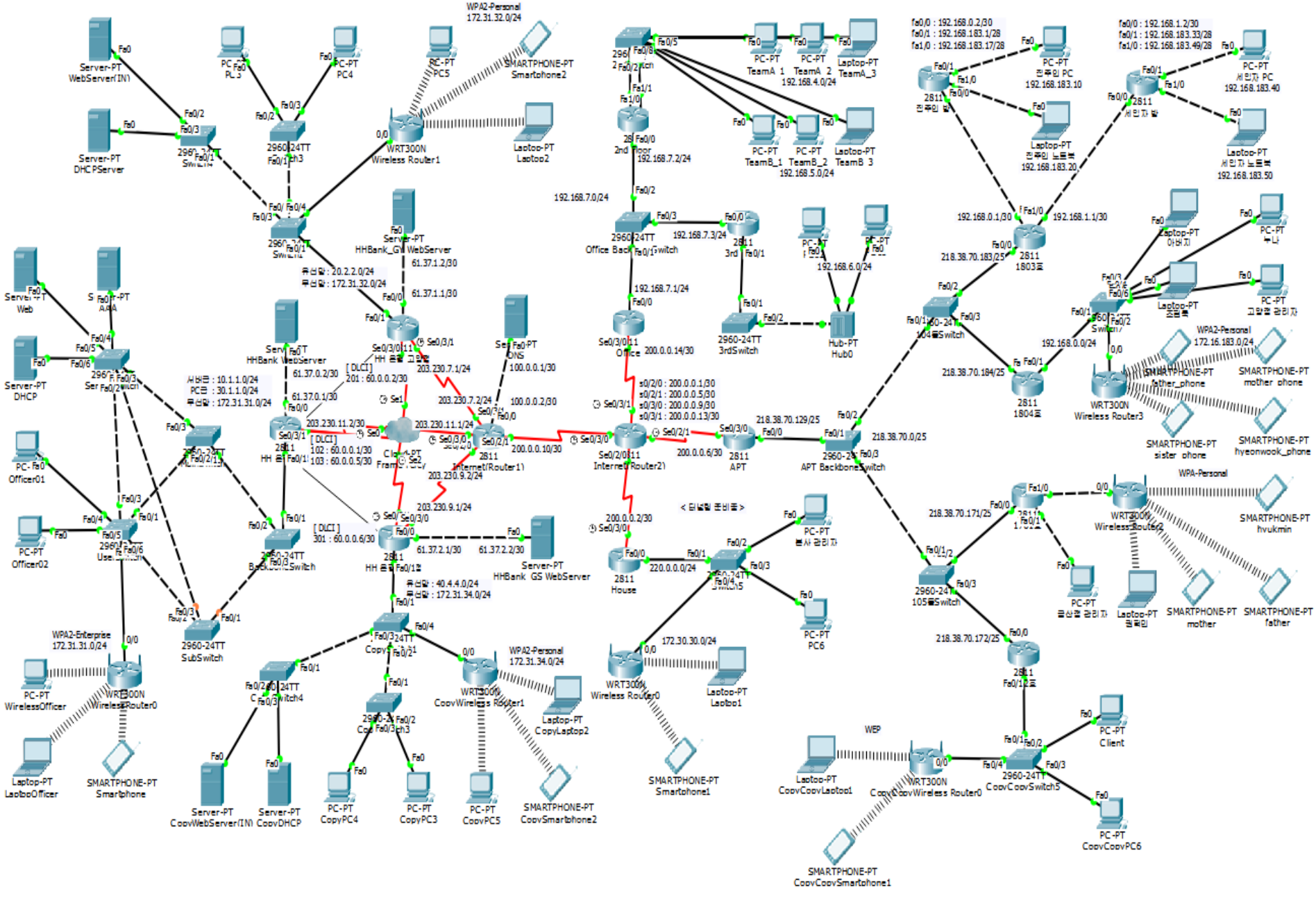


Contents

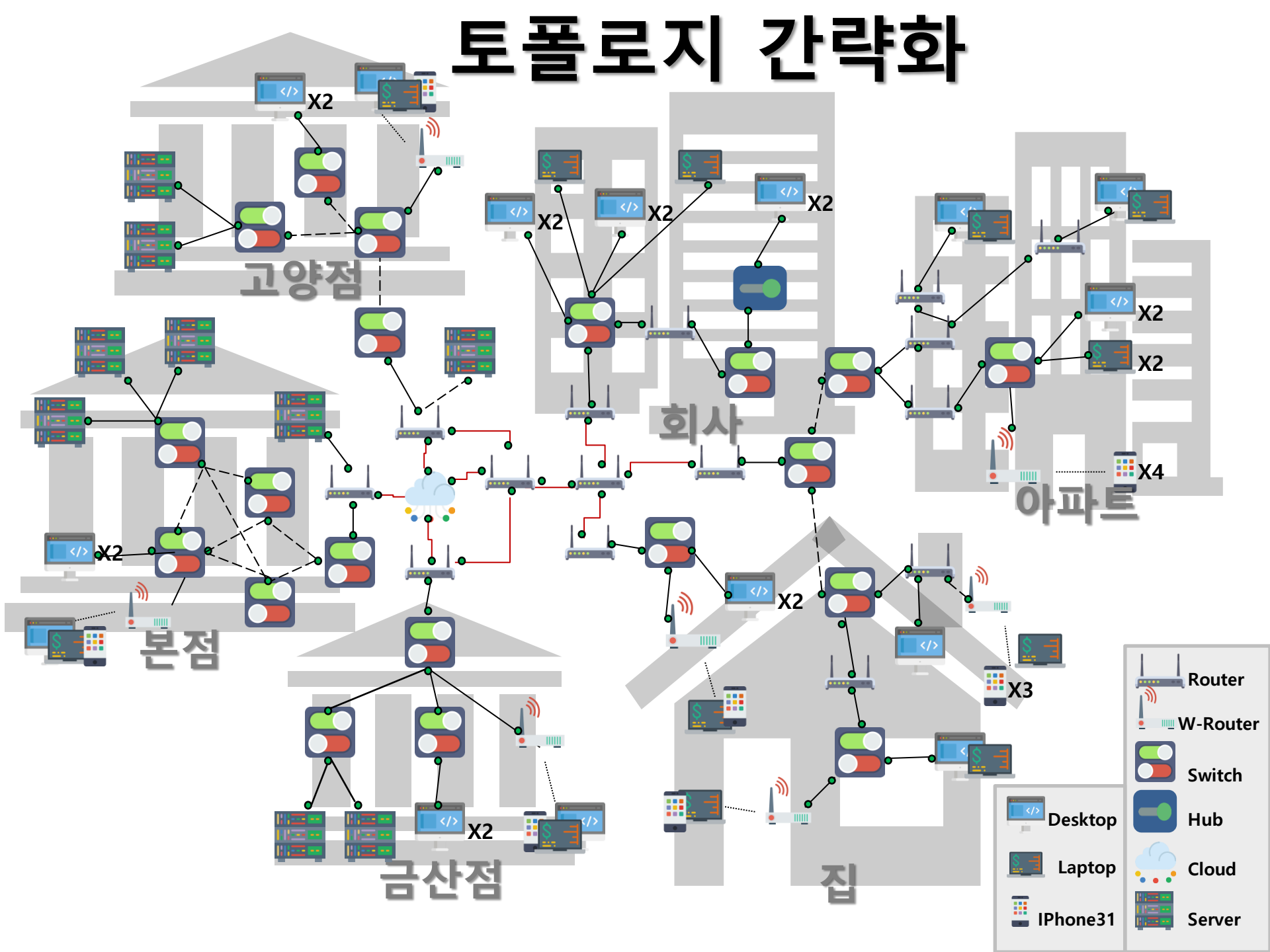


STORY

전체 토폴로지

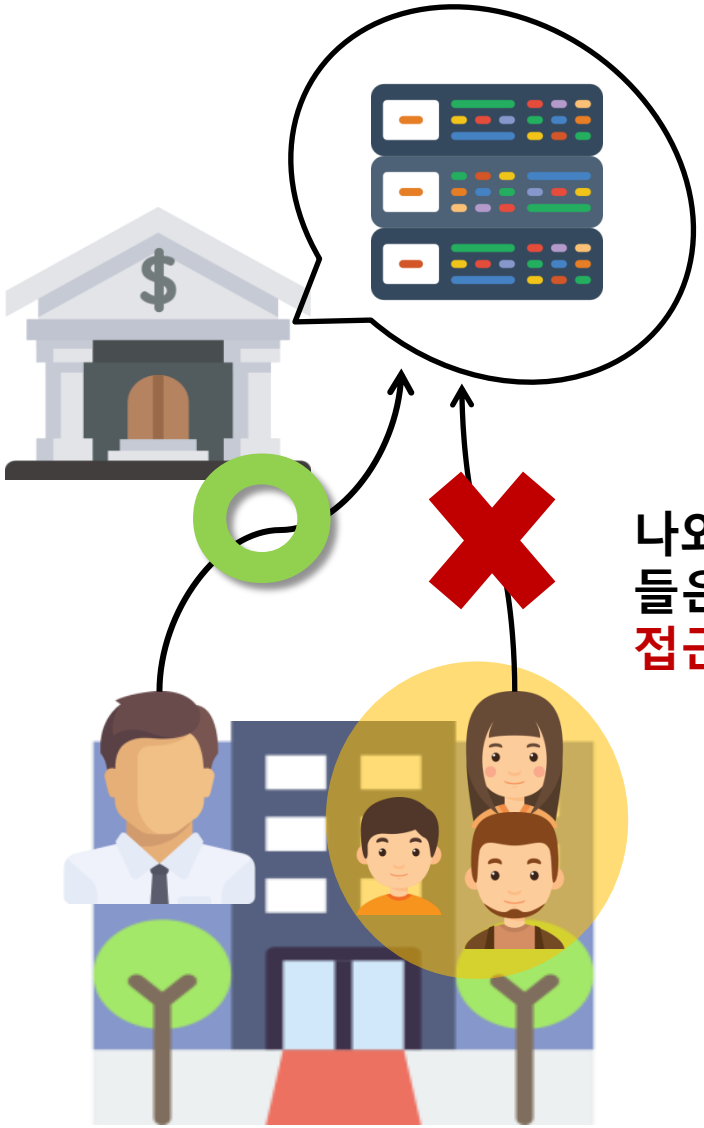

WPA2-Personal
172.31.32.0/24
Server-PT
WebServer(IN)
PC-PT
PC3
PC-PT
PC4
PC-PT
PC5
SMARTPHONE-PT
Smartphone2
Server-PT
DHCPServer
2960-24TT
Switch4
2960-24TT
Switch3
WRT300N
Wireless Router1
Laptop-PT
Laptop2
2960-24TT
Switch2
Server-PT
HHBank_GW WebServer
61.37.1.2/30
61.37.1.1/30
Server-PT
Web
Server-PT
AAA
Server-PT
DHCP
2960-24TT
Switch1
Server-PT
HHBank WebServer
61.37.0.2/30
61.37.0.1/30
Server-PT
DNS
100.0.0.1/30
100.0.0.2/30
203.230.7.1/24
203.230.7.2/24
203.230.11.2/30
203.230.11.1/24
203.230.10.1/24
203.230.9.2/24
203.230.9.1/24
2811
HH Router
Client-PT
Frame Relay
2811
Internet(Router1)
200.0.0.10/30
2811
Internet Router2
200.0.0.14/30
200.0.0.6/30
2811
APT
218.38.70.129/25
2960-24TT
APT BackboneSwitch
218.38.70.0/25
192.168.7.0/24
192.168.7.2/24
2960-24TT
Office Backbone Switch
192.168.7.3/24
2811
3rd Router
192.168.7.1/24
2960-24TT
3rdSwitch
192.168.6.0/24
Hub-PT
Hub0
200.0.0.2/30
220.0.0.0/24
2811
House
2960-24TT
Switch5
PC-PT
PC6
PC-PT
TeamA_1
PC-PT
TeamA_2
192.168.4.0/24
Laptop-PT
TeamA_3
PC-PT
TeamB_1
PC-PT
TeamB_2
192.168.5.0/24
Laptop-PT
TeamB_3
fa0/0 : 192.168.0.2/30
fa0/1 : 192.168.183.1/28
fa1/0 : 192.168.183.17/28
2811
192.168.0.1/30
192.168.1.1/30
2811
1803호
2960-24TT
104호Switch
218.38.70.183/25
218.38.70.184/25
2811
1804호
192.168.0.0/24
WRT300N
Wireless Router3
fa0/0 : 192.168.1.2/30
fa0/1 : 192.168.183.33/28
fa1/0 : 192.168.183.49/28
PC-PT
전무님 PC
192.168.183.10
Laptop-PT
전무님 노트북
192.168.183.20
PC-PT
사원자 PC
192.168.183.40
Laptop-PT
사원자 노트북
192.168.183.50
Laptop-PT
아버지
PC-PT
나
Laptop-PT
엄마
PC-PT
고양경 관리자
WPA2-Personal
172.16.183.0/24
SMARTPHONE-PT
father phone
SMARTPHONE-PT
mother phone
SMARTPHONE-PT
sister phone
SMARTPHONE-PT
hyeonwook_phone
2960-24TT
105호Switch
218.38.70.171/25
218.38.70.172/25
2811
1702호
WRT300N
Wireless Router2
WPA-Personal
SMARTPHONE-PT
hyukmin
PC-PT
홍사 관리자
Laptop-PT
컴퓨터
SMARTPHONE-PT
mother
SMARTPHONE-PT
father
2811
12호
PC-PT
Client
2960-24TT
CopyCopySwitch5
WRT300N
CopyCopyWireless Router0
Laptop-PT
CopyCopyLaptop1
PC-PT
CopyCopyPC6
SMARTPHONE-PT
CopyCopySmartphone1
WEP
Server-PT
HHBank GS WebServer
61.37.2.1/30
61.37.2.2/30
2811
HH 홍보
40.4.4.0/24
172.31.34.0/24
2960-24TT
SubSwitch
2960-24TT
BackboneSwitch
2960-24TT
CopySwitch4
2960-24TT
CopySwitch3
WRT300N
CopyWireless Router1
WPA2-Enterprise
172.31.31.0/24
WRT300N
Wireless Router0
WPA2-Personal
172.31.34.0/24
Laptop-PT
CopyLaptop2
Server-PT
CopyWebServer(IN)
Server-PT
CopyDHCP
PC-PT
CopyPC4
PC-PT
CopyPC3
PC-PT
CopyPC5
SMARTPHONE-PT
CopySmartphone2
PC-PT
Officer01
PC-PT
Officer02
PC-PT
WirelessOfficer
Laptop-PT
LaptopOfficer
SMARTPHONE-PT
Smartphone
WRT300N
Wireless Router0
Laptop-PT
Laptop1
SMARTPHONE-PT
Smartphone1
172.30.30.0/24
[DLCI]
201 : 60.0.0.2/30
[DLCI]
102 : 60.0.0.1/30
103 : 60.0.0.5/30
[DLCI]
301 : 60.0.0.6/30
s0/2/0 : 200.0.0.1/30
s0/2/1 : 200.0.0.5/30
s0/3/0 : 200.0.0.9/30
s0/3/1 : 200.0.0.13/30
서버팜 : 10.1.1.0/24
PC존 : 30.1.1.0/24
무선망 : 172.31.31.0/24
무선망 : 20.2.2.0/24
무선망 : 172.31.32.0/24
무선망 : 172.31.34.0/24

토폴로지 간략화


X2
고양점
X2
X2
X2
회사
X2
X2
X4
아파트
X2
본점
X2
X2
금산점
X3
집
Router
W-Router
Switch
Hub
Cloud
Server
Desktop
Laptop
IPhone31

STORY

시나리오



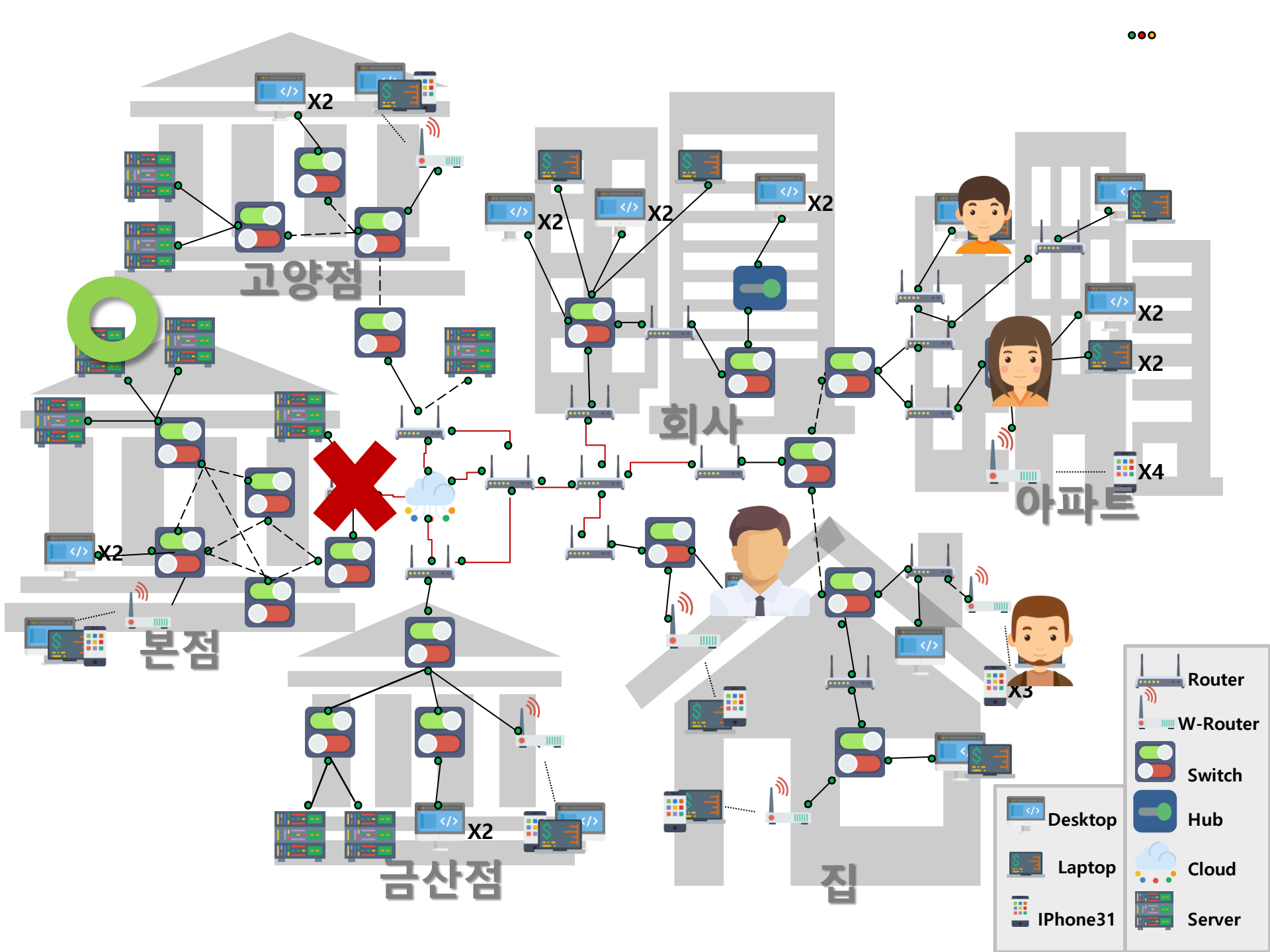
나는 은행 네트워크 **접근을 허용** 시켜 자택에서 근무를 할 수 있게 한다.

나와 같이 사는 주민들은 은행 네트워크에 **접근할 수 없다.**

STORY

시나리오

은행의 고객들은 은행의 서비스를 제공받을 수 있습니다.


X2
고양점
X2
X2
X2
회사
X2
X2
X4
아파트
X2
본점
X2
금산점
X3
집
Router
W-Router
Switch
Hub
Cloud
Server
Desktop
Laptop
IPhone31

ROUTER

STATIC

- 관리자가 경로를 직접 지정한다.
- 설정이 간단하다
- 토폴로지가 변경되면 관리자가 직접 변경해야 한다.
- 경로 설정을 유지하기 위한 라우팅 정보 교환이 불필요하다.
- 소규모 네트워크, 경로가 고정된 네트워크에 주로 사용한다.

RIPv2

Routing Information Protocol v2

- 클래스리스 라우팅 프로토콜
- 라우팅 업데이트시 서브넷마스크 정보도 전달한다.
- 자동요약은 설정/해제 선택 가능하다.
- RIPv2는 라우팅정보 전달시 멀티캐스트 주소 사용 (224.0.0.9)

EIGRP

Enhanced Interior Gateway Routing Protocol

EIGRP : 거리 벡터 라우팅 프로토콜

- 클래스리스
- 부분 업데이트가 가능하다.
- 224.0.0.10의 멀티캐스트 주소, 88번 포트 사용한다.
- 자동요약(auto-summary) 기능을 수행한다.
- Process-ID로 자율시스템번호(Autonomous System Number, 동일한 관리를 받는 라우터들의 집합 번호)를 사용한다.
- Process-ID가 서로 다른 여러 개의 EIGRP가 한 라우터 상에서 동작 가능하다.

OSPF

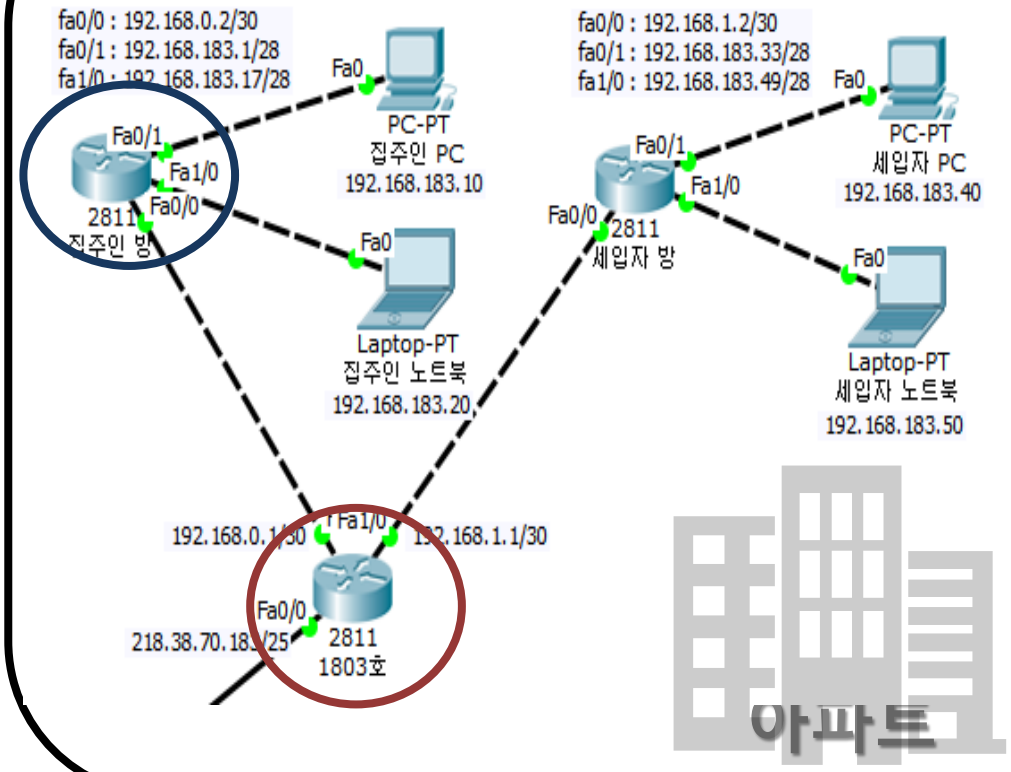
Open Shortest Path First

IP 헤더의 프로토콜 필드 89번을 사용한다.

- 네트워크 라우터에 변화가 생기는 즉시 전달한다.
- 수렴 시간이 짧고 홉수의 제한이 없다.
  ➔ 큰 네트워크 규모에 적합하다.
- Area개념 : 큰 전체 네트워크를 작은 영역으로 나누어 관리하여 빠른 업데이트, 효율적인 관리가 가능하다.
- VLSM을 지원하여 라우팅 테이블을 줄일 수 있다.
- 여러 개의 라우팅 경로를 하나로 묶는다.
- 네트워크 내 변화가 있을 경우에만 정보 전송한다.
- 링크 상태 라우팅 알고리즘을 사용한다.

ROUTE

STATIC

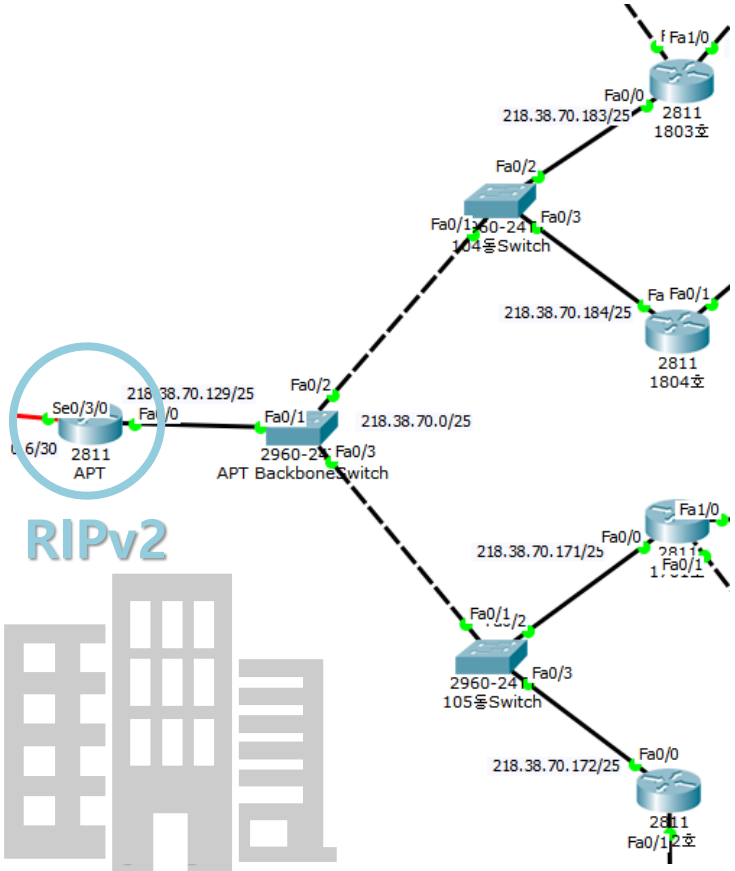



```
Owner(config)#interface fastEthernet 0/0
Owner(config-if)#ip address 192.168.0.2
255.255.255.252
Owner(config-if)#interface fastEthernet 0/1
Owner(config-if)#ip address 192.168.183.1
255.255.255.240
Owner(config-if)#interface fastEthernet 1/0
Owner(config-if)#ip address 192.168.183.17
255.255.255.240
Owner(config-if)#exit

Owner(config)#ip route 0.0.0.0 0.0.0.0 f0/0

1803(config)#ip route 192.168.183.0
255.255.255.224 fa0/1
1803(config)#ip route 192.168.183.32
255.255.255.224 f1/0
```

ROUTE

RIPv2

Routing Information Protocol



APT(config)#router rip
APT(config-router)#version 2
APT(config-router)#net 200.0.0.0
APT(config-router)#net 218.38.70.128
APT(config-router)#no auto-summary

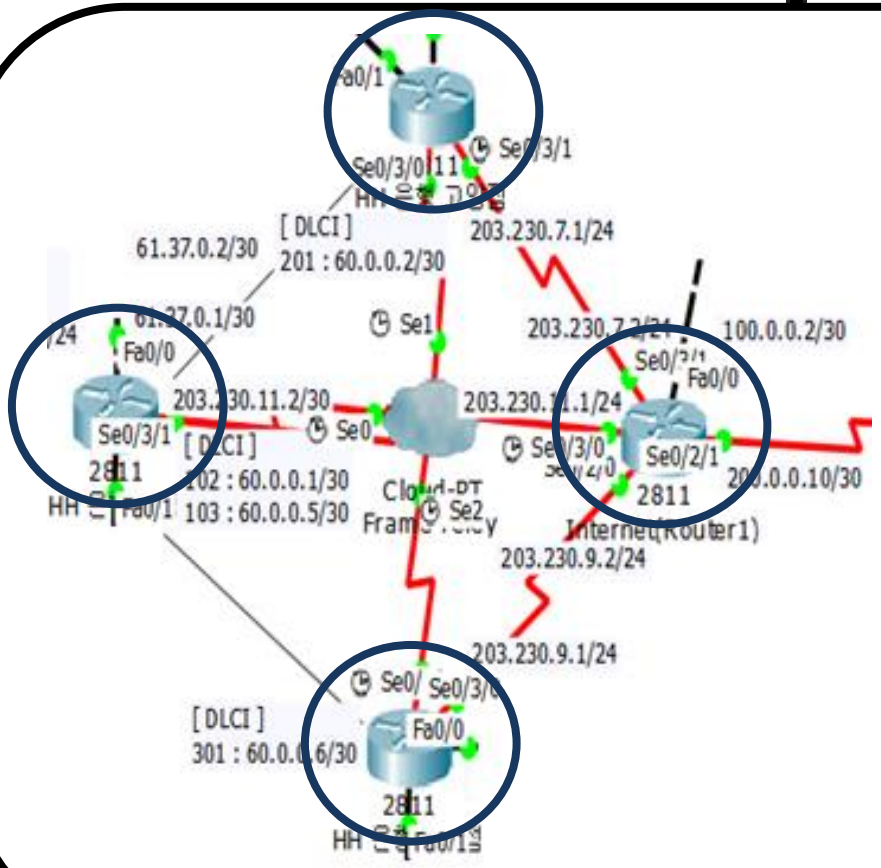
APT(config-router)#passive-interface fa0/0

패시브인터페이스
특정 인터페이스에 라우팅 업데이트 정보를 보내지 않도록 설정

ROUTE

EIGRP

Enhanced Interior Gateway Routing Protocol

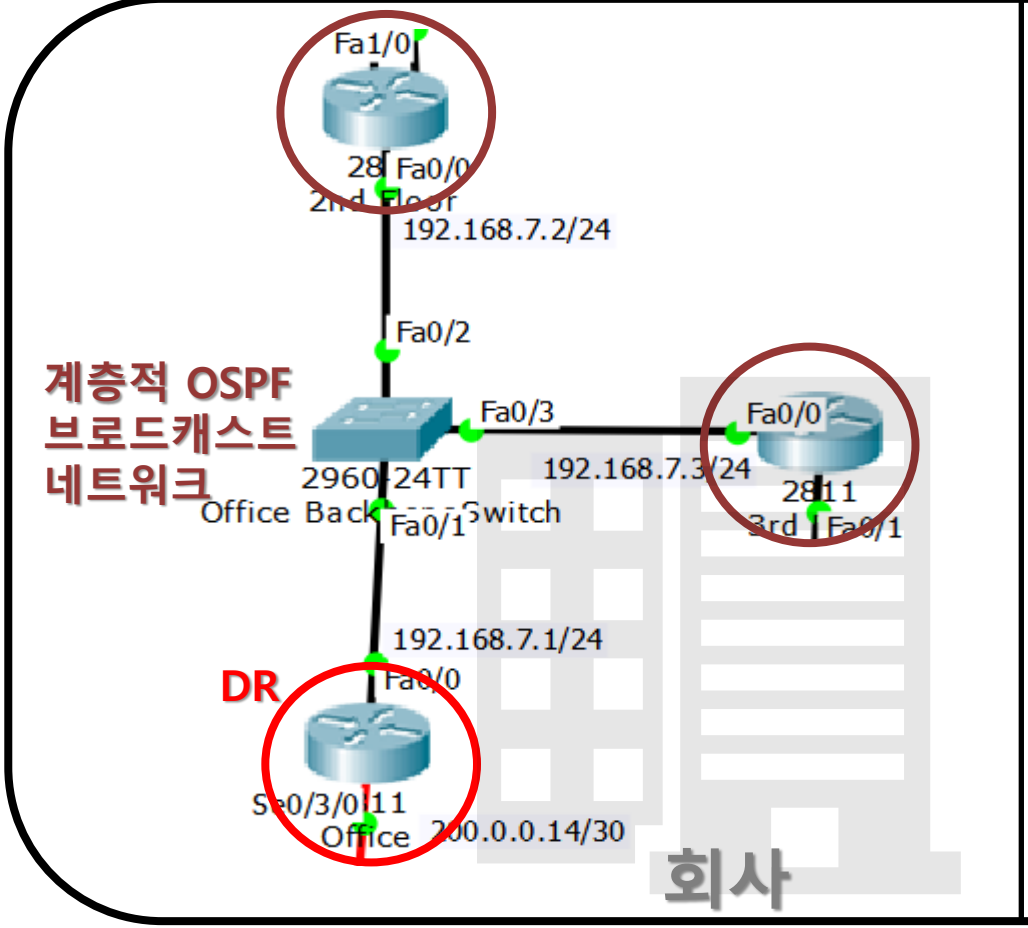



```
HH(config)#router eigrp 1
HH(config-router)#network 61.37.0.0
HH(config-router)#network 203.230.11.0
HH(config-router)#no auto-summary

HH_GY(config)#router eigrp 1
HH_GY(config-router)#network 61.37.1.0
HH_GY(config-router)#network 203.230.7.0
HH_GY(config-router)#no auto-summary

HH_GS(config)#router eigrp 1
HH_GS(config-router)#network 61.37.2.0
HH_GS(config-router)#network 203.230.9.0
HH_GS(config-router)#no auto-summary

Internet1(config)#router eigrp 1
Internet1(config-router)#network 100.0.0.0
Internet1(config-router)#network 200.0.0.8
Internet1(config-router)#network 203.230.7.0
Internet1(config-router)#network 203.230.9.0
Internet1(config-router)#network 203.230.11.0
Internet1(config-router)#no auto-summary
```

ROUTE

OSPF

Open Shortest Path First

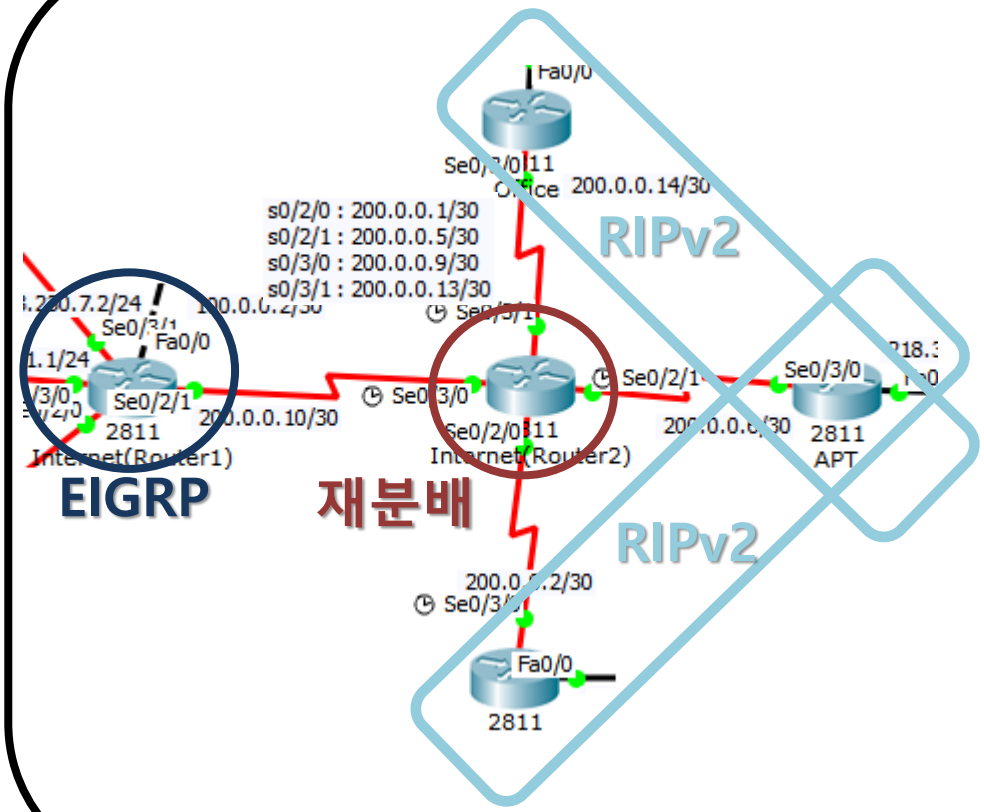



```
Office(config)#router ospf 1
Office(config-router)#network 192.168.7.0 0.0.0.255 area 0
Office(config-router)#network 200.0.0.12 0.0.0.3 area 0
Office(config-router)#exit
Office(config)#int f0/0
Office(config-if)#ip ospf priority 255 // DR로 설정

2ndRouter(config)#router ospf 1
2ndRouter(config-router)#network 192.168.4.0 0.0.0.255 area 2
2ndRouter(config-router)#network 192.168.5.0 0.0.0.255 area 2
2ndRouter(config-router)#network 192.168.7.0 0.0.0.255 area 0

3rdRouter(config)#router ospf 1
3rdRouter(config-router)#network 192.168.6.0 0.0.0.255 area 3
3rdRouter(config-router)#network 192.168.7.0 0.0.0.255 area 0

[ 재분배 ]
Internet2(config)#router rip
Internet2(config-router)#version 2
Internet2(config-router)#net 200.0.0.0
Internet2(config-router)#no auto-summary
Internet2(config-router)#redistribute eigrp 1 metric 4

Internet2(config)#router eigrp 1
Internet2(config-router)#network 200.0.0.0
Internet2(config-router)#no auto-summary
Internet2(config-router)#redistribute rip metric 1544 0 255 1 1500
```

ROUTE

재분배

redistribution




```
Internet2(config)#router rip
Internet2(config-router)#version 2
Internet2(config-router)#net 200.0.0.0
Internet2(config-router)#no auto-summary
Internet2(config-router)#redistribute eigrp 1 metric 4

Internet2(config)#router eigrp 1
Internet2(config-router)#network 200.0.0.0
Internet2(config-router)#no auto-summary
Internet2(config-router)#redistribute rip metric 1544 0
255 1 1500
```

재분배(RedisTribution)
서로 다른 라우팅 프로토콜을 사용하는 영역간의 라우팅이 가능하도록 설정하는 기능.

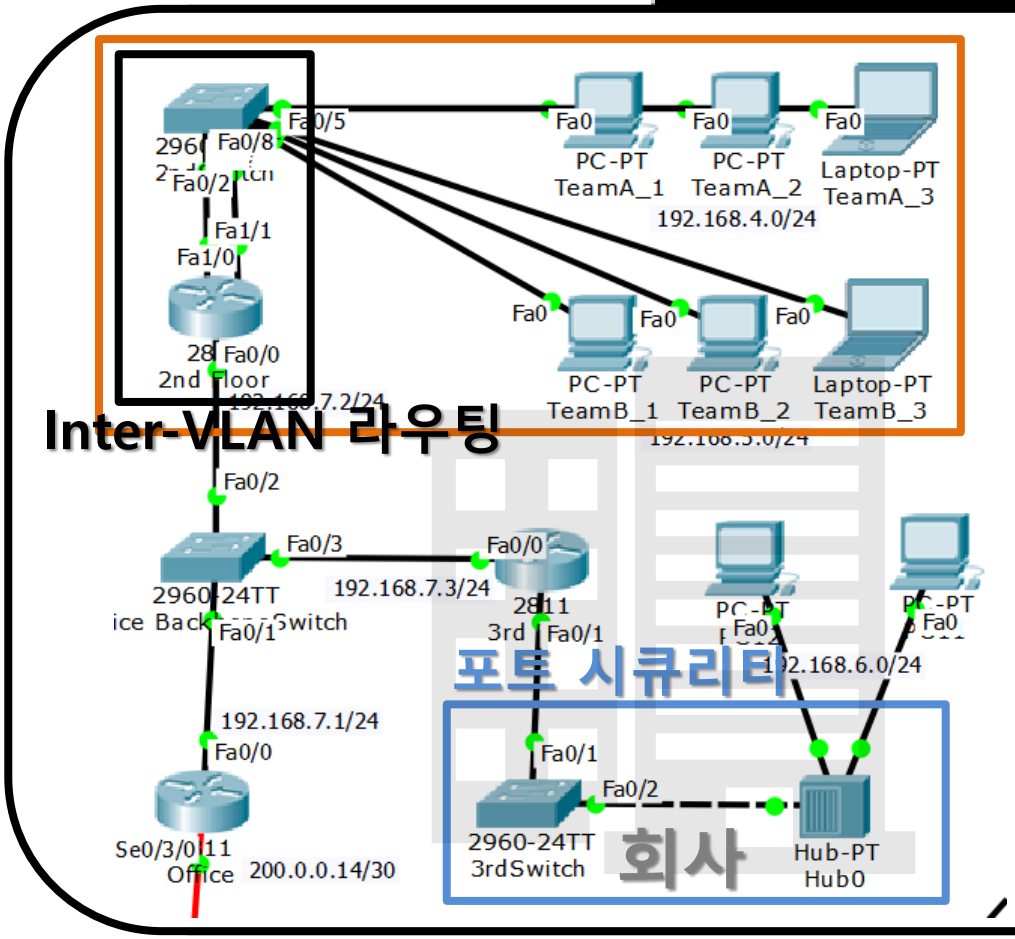
VLAN

VLAN

VLAN의 필요성
• 네트워크의 크기가 커지면 플러딩 데이터가 커짐
• 내부에서 권한이 없는 사용자가 제약없이 특정 장치에 접속 가능
VLAN의 역할
• 브로드캐스트 도메인을 분할하여 브로드캐스트 트래픽으로 인한 장비들의 성능저하를 막고자 함
• 서로 다른 VLAN에 속한 장치들은 통신이 불가능하여 보안에 도움
• 서로 다른 VLAN이 통신하려면 라우터나 L3 스위치가 필요
• 스위치의 모든 포트는 기본 VLAN 1번에 속해 있음

VLAN

VLAN

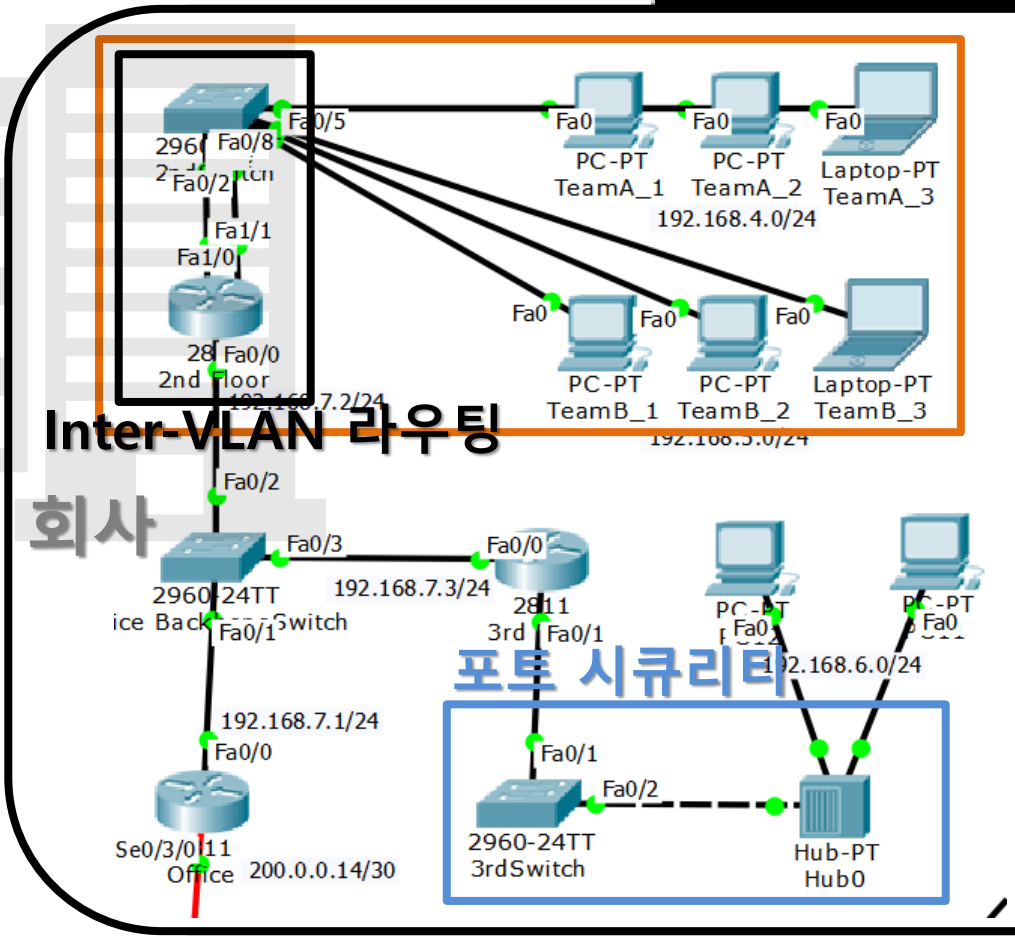


[VLAN]

```
2ndSwitch(config)#vlan 10
2ndSwitch(config-vlan)#name Team_A
2ndSwitch(config-vlan)#exit
2ndSwitch(config)#vlan 20
2ndSwitch(config-vlan)#name Team_B
2ndSwitch(config-vlan)#exit
2ndSwitch(config)#interface range fa0/3-5
2ndSwitch(config-if-range)#switchport
access vlan 10
2ndSwitch(config-if-range)#exit
2ndSwitch(config)#interface range fa0/6-8
2ndSwitch(config-if-range)#switchport
access vlan 20
2ndSwitch(config-if-range)#exit
```

VLAN

Inter-VLAN



[Inter-VLAN]

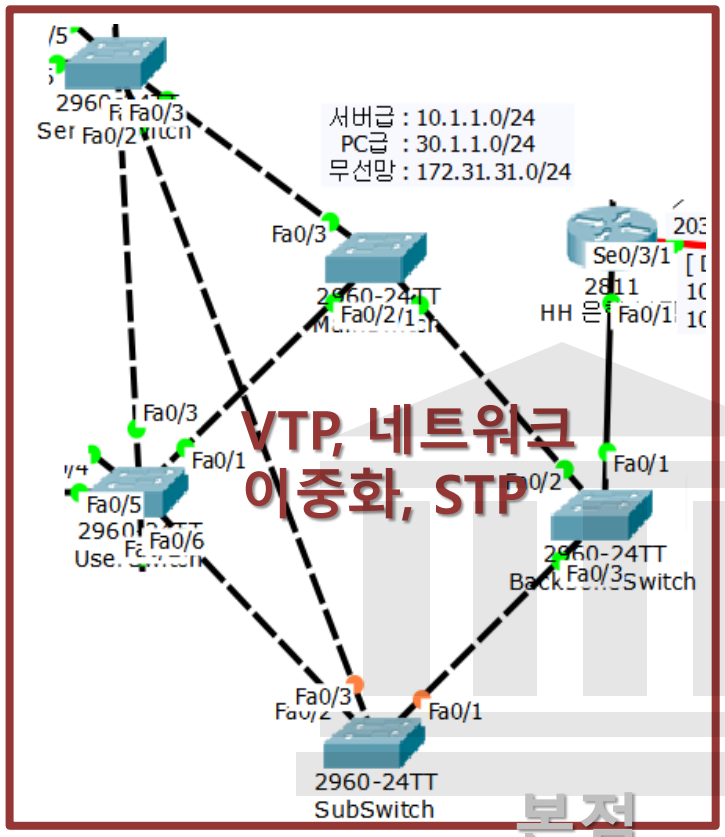
```
2ndSwitch(config)#interface fastEthernet 0/1
2ndSwitch(config-if)#switchport access vlan 10
2ndSwitch(config-if)#exit
2ndSwitch(config)#interface fastEthernet 0/2
2ndSwitch(config-if)#switchport access vlan 20
2ndSwitch(config-if)#exit
```

[Port-Security]

```
3rdSwitch(config)#interface fastEthernet 0/2
3rdSwitch(config-if)#switchport mode access
3rdSwitch(config-if)#switchport port-security
3rdSwitch(config-if)#switchport port-security maximum 2
3rdSwitch(config-if)#switchport port-security violation restrict
```

VLAN

VTP

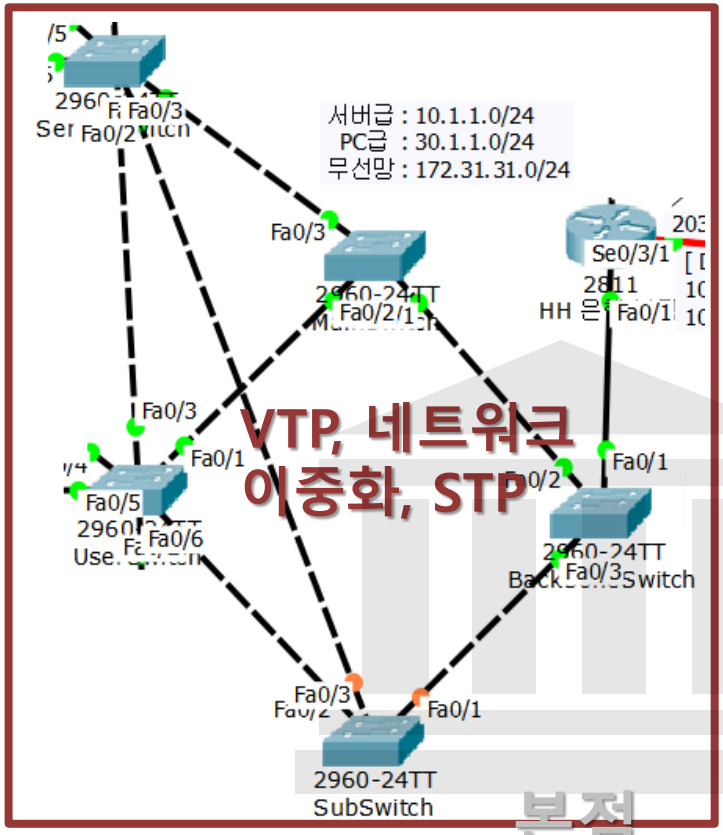


[VTP]

```
BBS(config)#vtp ver 2
BBS(config)#vtp mode server
BBS(config)#vtp domain HHbank
BBS(config)#vtp password headoffice
BBS(config)#int range fa0/1-3
BBS(config-if-range)#sw mode trunk
BBS(config-if-range)#exit

BBS(config)#vlan 10
BBS(config-vlan)#name Server
BBS(config-vlan)#exit
BBS(config)#vlan 30
BBS(config-vlan)#name User
BBS(config-vlan)#exit

MS(config)#vtp version 2
MS(config)#vtp mode client
MS(config)#vtp domain HHbank
MS(config)#vtp password headoffice
MS(config)#int range fa0/1-3
MS(config-if-range)#sw mode trunk
MS(config-if-range)#exit
```

VLAN

STP



[STP]
MS(config)#spanning-tree vlan 1 root primary
MS(config)#spanning-tree vlan 10 root primary
MS(config)#spanning-tree vlan 30 root primary

SS(config)#spanning-tree vlan 1 root secondary
SS(config)#spanning-tree vlan 10 root secondary
SS(config)#spanning-tree vlan 30 root secondary

Wireless

Wireless

WEP (Wired Equivalent Privacy)
- 고정된 비밀번호 사용
- 통신을 분석하여 암호키 획득 가능 (알고리즘이 취약)
- 확장성에 문제

WPA (WiFi Protected Access)
- TKIP (Temporal Key Integrity Protocol)
- AES (Advanced Encryption Standard)

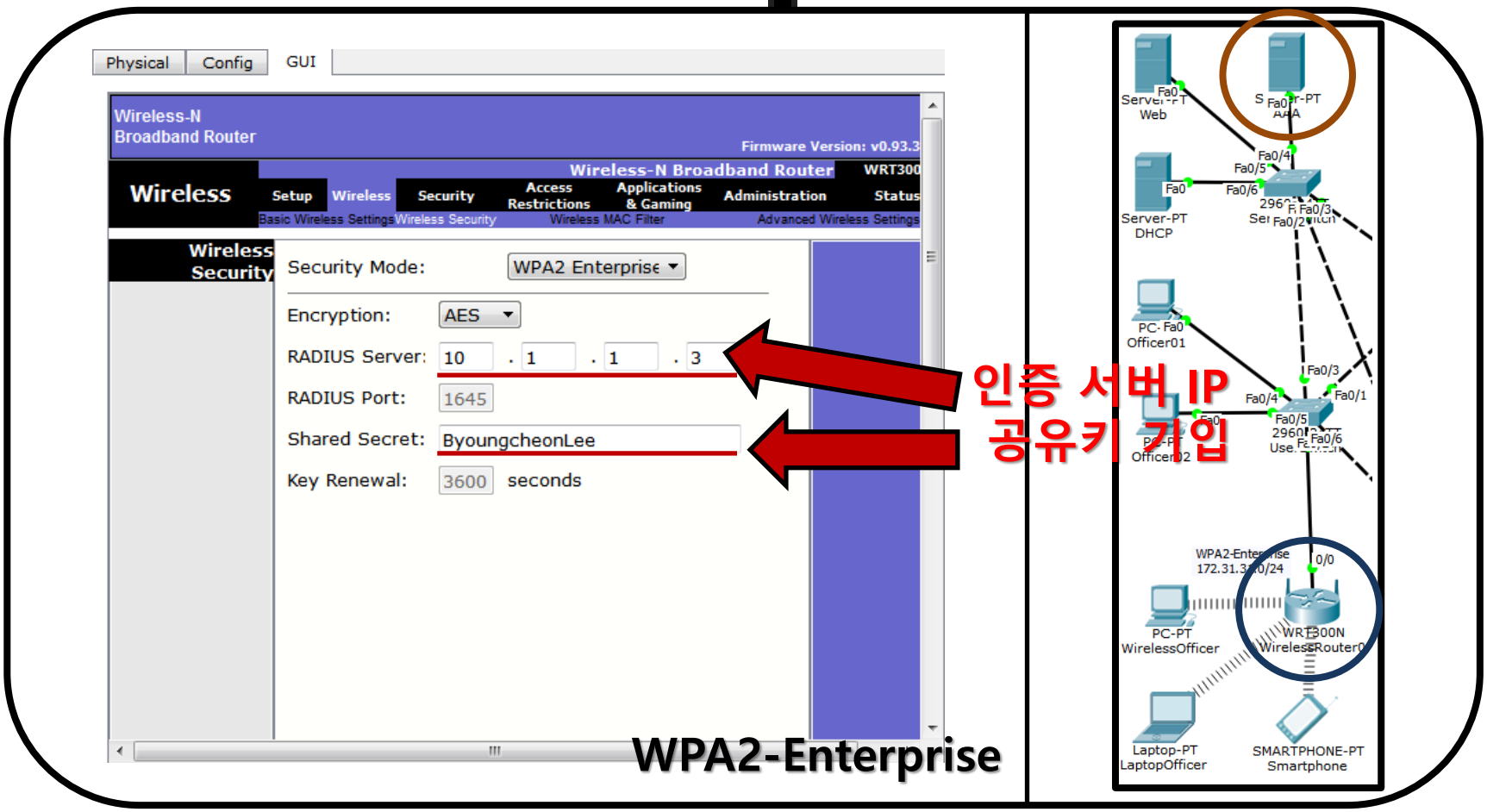
WPA2
- WPA의 개선된 버전

장점
- 무선 연결의 편리함.
- 이동성 제공. 사용의 유연성.
- 비용의 감소.

단점
- 정보의 누출 가능성. 무선랜 분석도구 이용.
- 무선랜 보안에 사용되는 암호화 키값의 추출 가능성
- 무선랜 해킹기술: spoofing, sniffing 등

Wireless

WPA2-Enterprise



Wireless

WPA2-Enterprise

Physical | Config | Services | Desktop | Software/Services

SERVICES
- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP

AAA

Service: On / Off Radius Port: 1645

Network Configuration

Client Name	Client IP	Server Type	Key
1 NHbank	30.1.1.254	Radius	Byoungche

Client Name: NHbank Client IP: 30.1.1.254
Secret: ByoungcheonLee ServerType: Radius

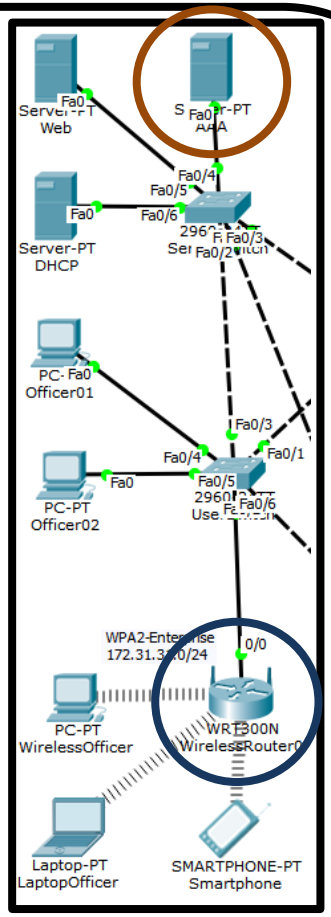
Add / Save / Remove

User Setup

Username Password

Username	Password
1 desktop	desktop00
2 laptop	laptop00
3 mobile	mobile00

Add / Save / Remove



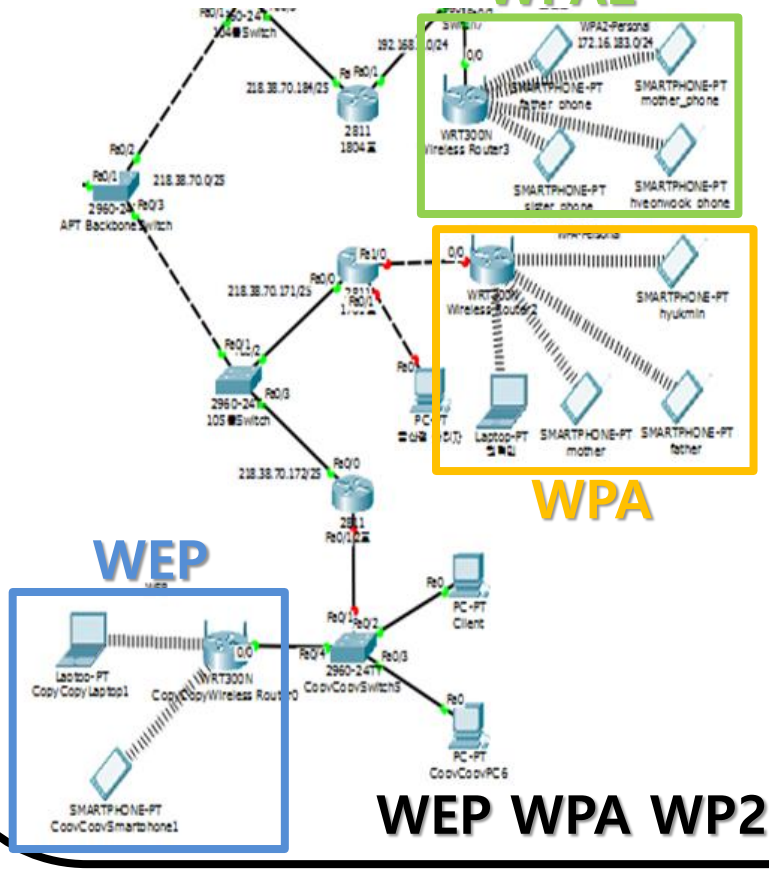
WPA2-Enterprise

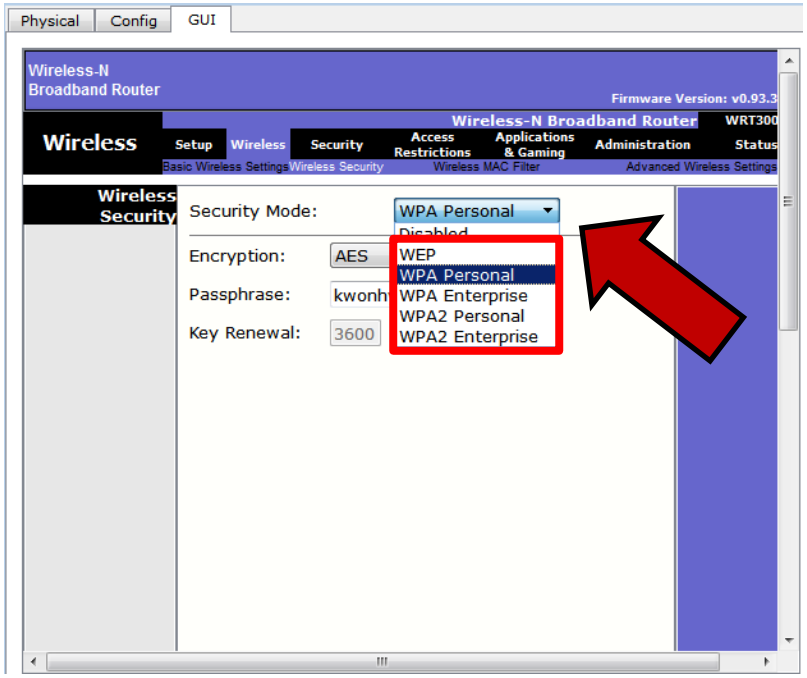
Wireless

WEP

WPA2

WPA



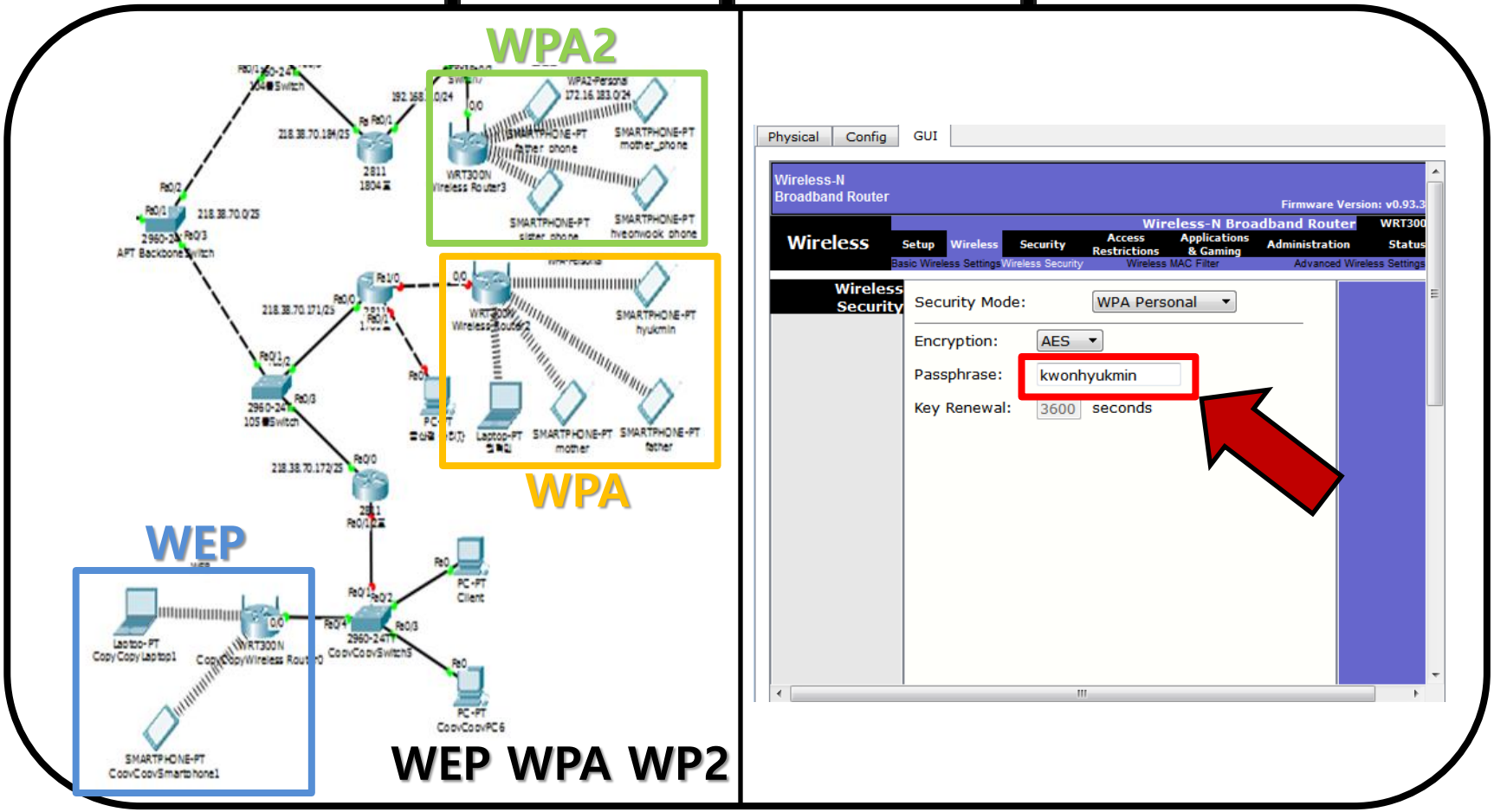


Wireless

WEP

WPA2

WPA

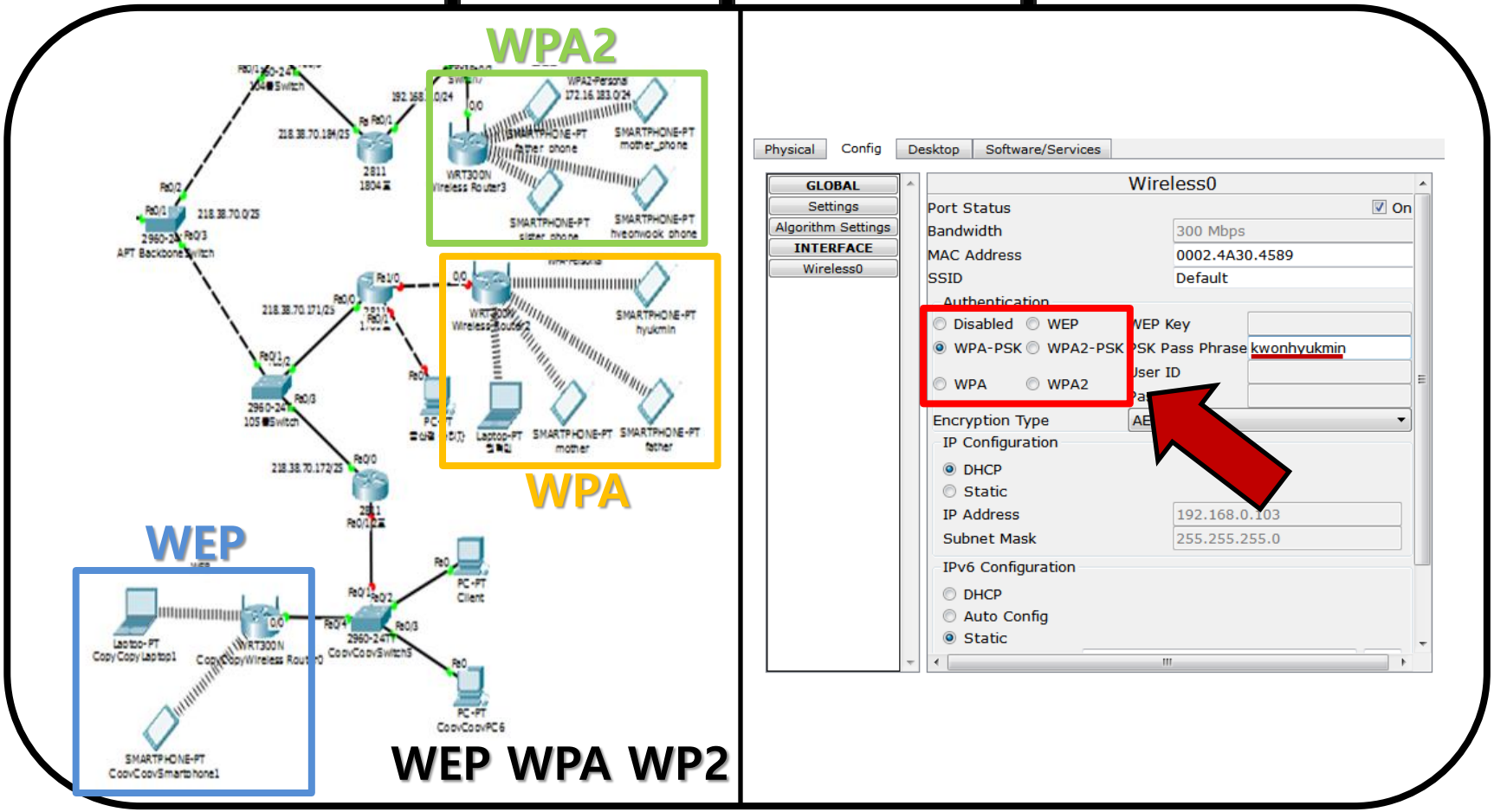


Wireless

WEP

WPA2

WPA



WAN

WAN

Wide Area Network

- LAN과 MAN을 포괄하는 광역 네트워크이다
- 라우터, 스위치 뿐만 아니라 다양한 장비들이 사용된다
- 다양한 접속기술과 접속장치들을 통해 네트워크를 구성한다

ATM (Asynchronous Transfer Mode)
- 데이터를 53바이트 길이의 셀로 나누어 전송
- 음성, 영상 등 실시간 데이터 전송에 효과적

프레임릴레이 (Frame-relay)
- 프레임이라 불리는 가변 길이 단위에 데이터를 넣고 재전송과 같은 필요한 오류 정정 기능은 단말 지점에 맡긴다. 이를 통해 전체 데이터 전송 속도를 향상시켰다.

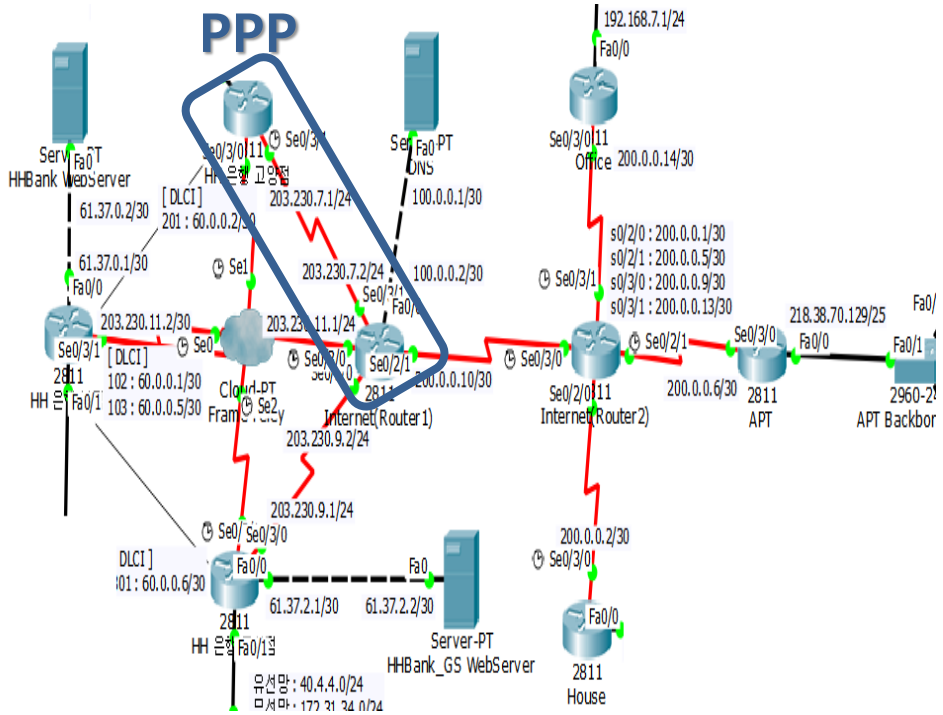
HDLC (High-level Data Link Control)
- 동기식 시리얼 전송
- 연결지향성, 비연결지향성 서비스를 모두 지원
- 시스코 전용, 시스코 라우터의 기본 캡슐화 방식

PPP (Point to Point)
- CHAP, PAP라는 보안설정이 가능한 WAN 캡슐화 방식

WAN

PPP

Point to Point



[PPP]

HH_GY(config)#username HH password bank

HH_GY(config)#int s0/3/1

HH_GY(config-if)#encapsulation ppp

HH_GY(config-if)#ppp authentication pap

HH_GY(config-if)#ppp pap sent-username Internet password router

Internet1(config)#username Internet password router

Internet1(config)#interface Serial0/3/1

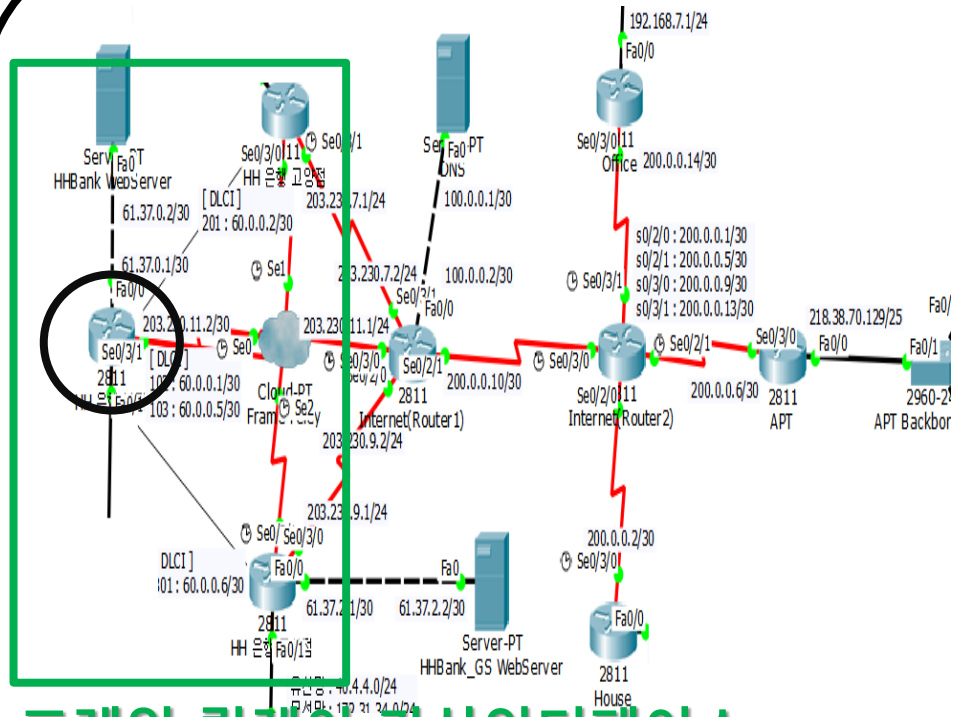
Internet1(config-if)#encapsulation ppp

Internet1(config-if)#ppp authentication pap

Internet1(config-if)#ppp pap sent-username HH password bank

WAN

Frame-relay



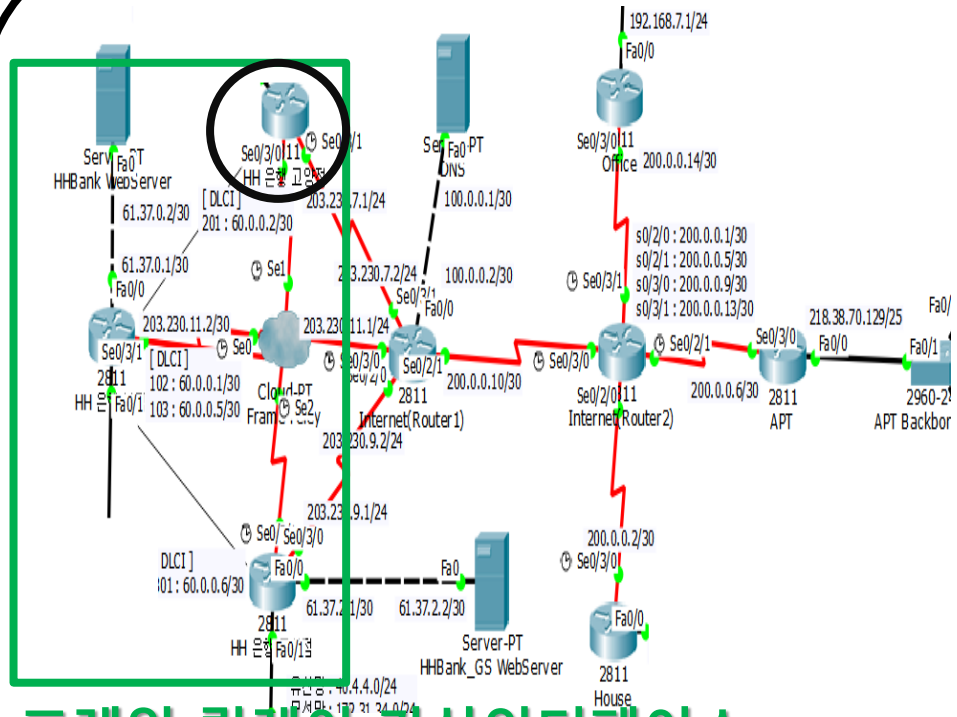
프레임 릴레이 가상인터페이스

[프레임릴레이 가상인터페이스]

```
HH(config)#interface Serial0/3/0
HH(config-if)#encapsulation frame-relay
HH(config-if)#no shutdown
HH(config-if)#exit
HH(config)#int s0/3/0.102 point-to-point
HH(config-subif)#ip add 60.0.0.1
      255.255.255.252
HH(config-subif)#frame-relay interface-dlci 102
HH(config-subif)#exit
HH(config)#int s0/3/0.103 point-to-point
HH(config-subif)#ip add 60.0.0.5
      255.255.255.252
HH(config-subif)#frame-relay interface-dlci 103
HH(config-subif)#exit
HH(config)#router rip
HH(config-router)#version 2
HH(config-router)#network 10.1.1.0
HH(config-router)#network 30.1.1.0
HH(config-router)#network 60.0.0.0
HH(config-router)#no auto-summary
```

WAN

Frame-relay

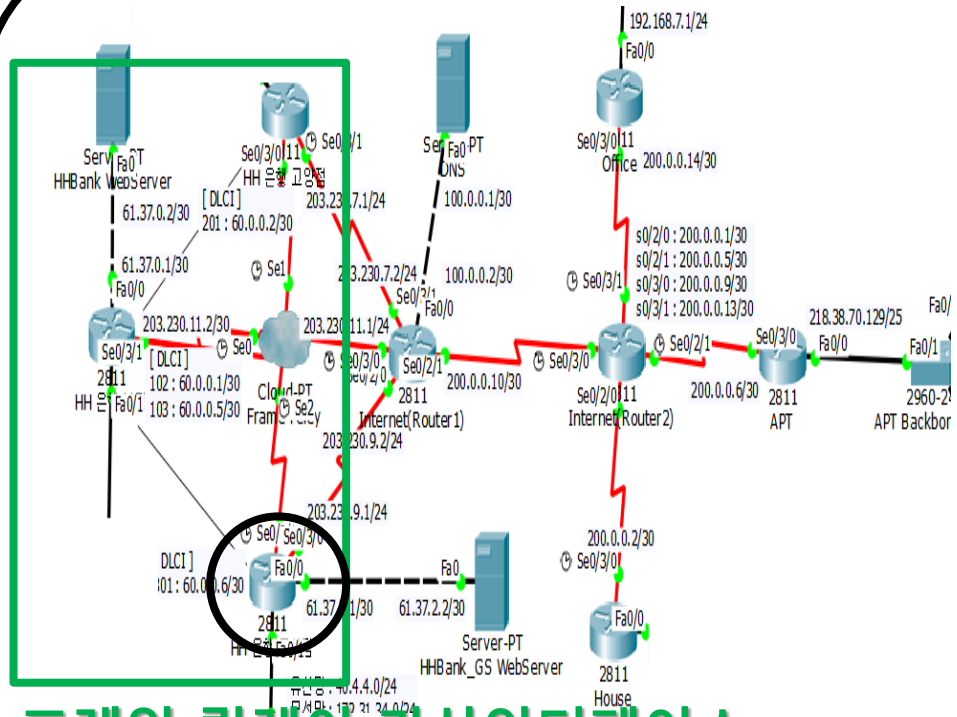


프레임 릴레이 가상인터페이스

```
HH_GY(config)#interface Serial0/3/0
HH_GY(config-if)#ip address 60.0.0.2
      255.255.255.252
HH_GY(config-if)#encapsulation frame-relay
HH_GY(config-if)#frame-relay map ip 60.0.0.1
      201 broadcast
HH_GY(config-if)#frame-relay map ip 60.0.0.6
      201 broadcast
HH_GY(config-if)#no shutdown
HH_GY(config-if)#exit
HH_GY(config)#router rip
HH_GY(config-router)#version 2
HH_GY(config-router)#network 20.2.2.0
HH_GY(config-router)#network 60.0.0.0
HH_GY(config-router)#no auto-summary
```

WAN

Frame-relay



프레임 릴레이 가상인터페이스

```
HH_GS(config-if)#interface Serial0/3/0
HH_GS(config-if)#ip add 60.0.0.6
      255.255.255.252
HH_GS(config-if)#encapsulation frame-relay
HH_GS(config-if)#frame-relay map ip 60.0.0.5
      301 broadcast
HH_GS(config-if)#frame-relay map ip 60.0.0.2
      301 broadcast
HH_GS(config-if)#no shutdown
HH_GS(config-if)#exit
HH_GS(config)#router rip
HH_GS(config-router)#version 2
HH_GS(config-router)#network 40.4.4.0
HH_GS(config-router)#network 60.0.0.4
HH_GS(config-router)#no auto-summary
```

VPN

VPN

Virtual Private Network

VPN의 응용

안전한 기업 업무환경 구축

- 본사-지사간의 안전한 네트워크 연결
- 재택근무: 집에서 회사 서버에 안전하게 접속 필요

VoIP 네트워크: 인터넷전화

IPTV, 비디오 회의

VPN의 보안 기능

암호프로토콜 이용하여 인증, 보안, 기밀성 유지

키의 이용

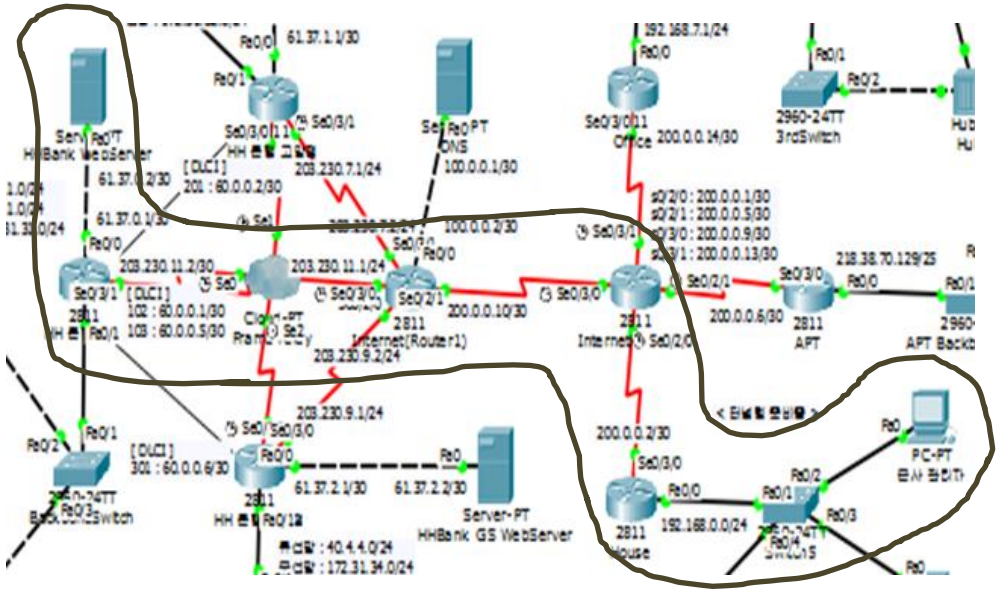
- 대칭키 암호화 (Symmetric Encryption):
  - PSK(Pre-shared key) – 공유키 이용
  - 디피-헬만(Diffie-Hellman) – 온라인 키합의 방식
- 비대칭키 암호화 (Asymmetric Encryption):
  - 인증서 이용

암호 알고리즘

- 대칭키 암호: DES, 3DES, AES
- 비대칭키 암호: RSA
- 해쉬암고리즘: HMAC, MD5, SHA-1

VPN

GRE+IPSec VPN

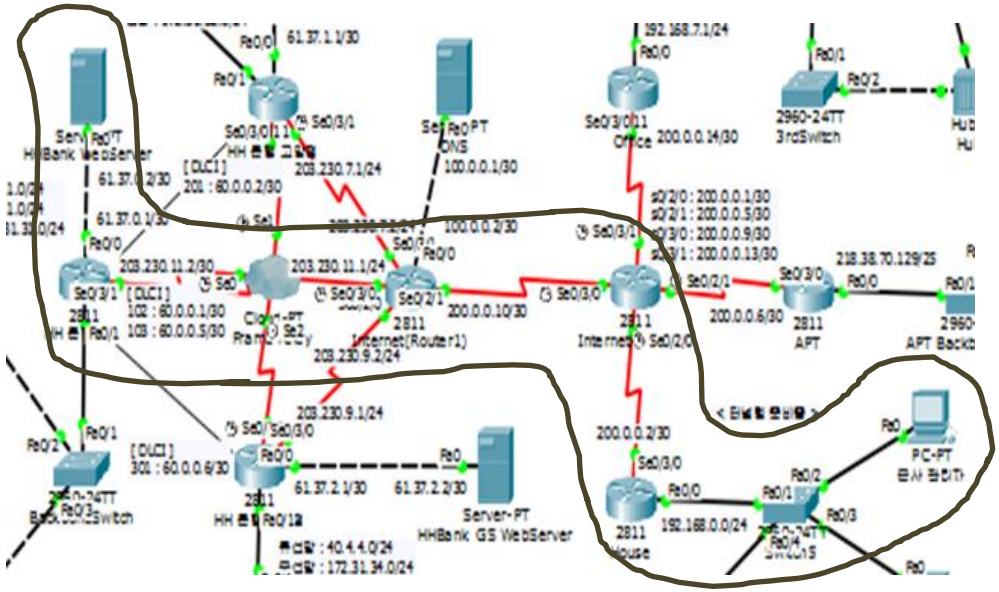


GRE+IPSec VPN

```
crypto isakmp policy 10
encr aes 256
authentication pre-share
lifetime 3600
hash sha
exit

crypto ipsec transform-set strong esp-3des esp-
      md5-hmac
crypto isakmp key hhbank001 address 0.0.0.0
      0.0.0.0

crypto map vpn 10 ipsec-isakmp
set peer 203.230.11.2
set transform-set strong
match address 110
exit

int s0/3/0
crypto map vpn
no shutdown
exit
```

VPN

GRE+IPSec VPN

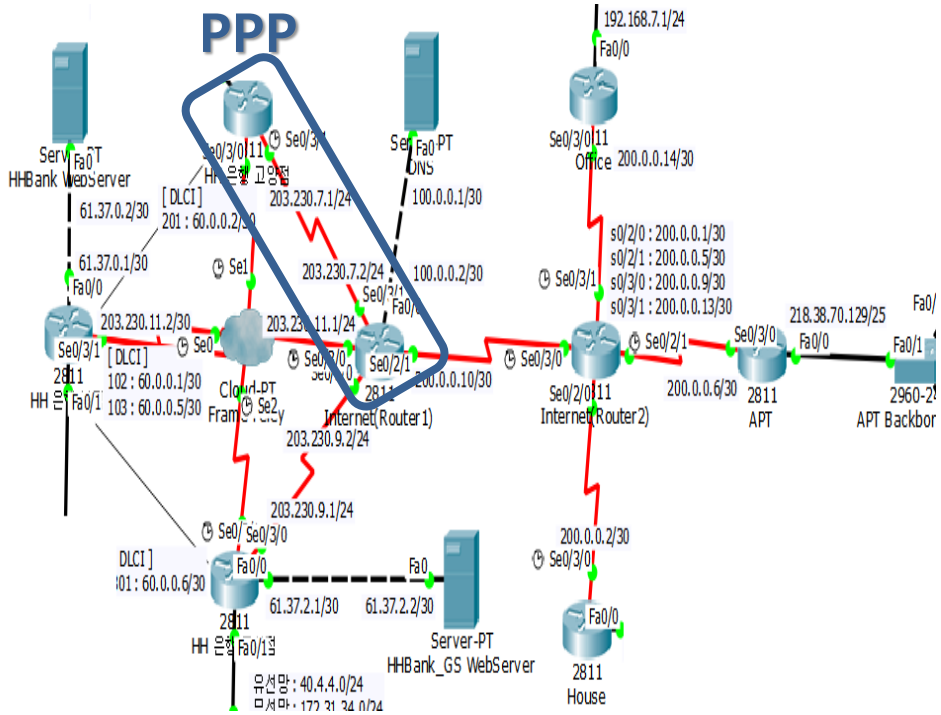


GRE+IPSec VPN

```
int tunnel 48
ip add 50.5.5.2 255.255.255.0
tunnel source s0/3/0
tunnel destination 203.230.11.2
exit

router rip
version 2
network 200.0.0.0
network 50.5.5.0
no auto-summary
exit

access-list 110 permit gre host 50.5.5.2 host
      50.5.5.1
```

VPN

VPN



[PPP]

HH_GY(config)#username HH password bank

HH_GY(config)#int s0/3/1

HH_GY(config-if)#encapsulation ppp

HH_GY(config-if)#ppp authentication pap

HH_GY(config-if)#ppp pap sent-username Internet password router

Internet1(config)#username Internet password router

Internet1(config)#interface Serial0/3/1

Internet1(config-if)#encapsulation ppp

Internet1(config-if)#ppp authentication pap

Internet1(config-if)#ppp pap sent-username HH password bank

DHCP

DHCP

Dynamic Host Configuration Protocol

DHCP(Dynamic Host Configuration Protocol)

- 동적 호스트 구성 프로토콜
- TCP/IP 통신을 실행하기 위해 필요한
- 정보를 자동적으로 할당하고 관리하기 위
- 통신 규약 (RFC 1541)
- IP주소의 자동관리로 관리의 편리성 향상
- IP주소의 가용성을 높여줌 – 할당만 하고 사용하지 않는 주소를 줄임

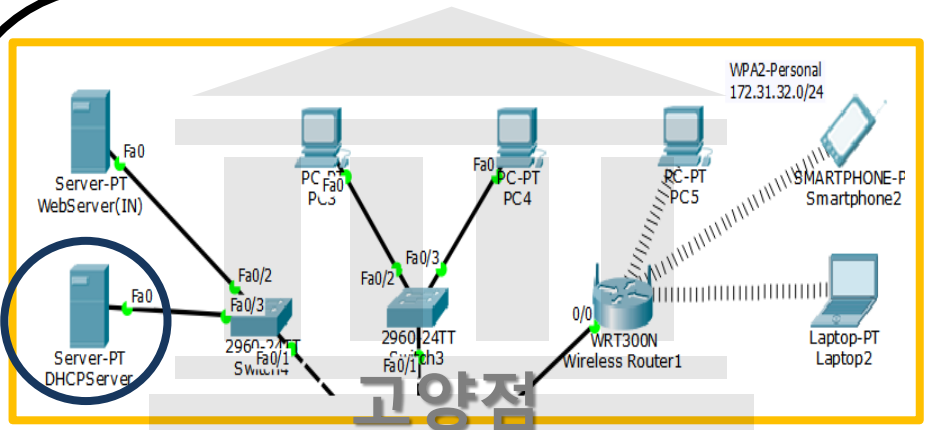
DHCP의 주소할당 방식

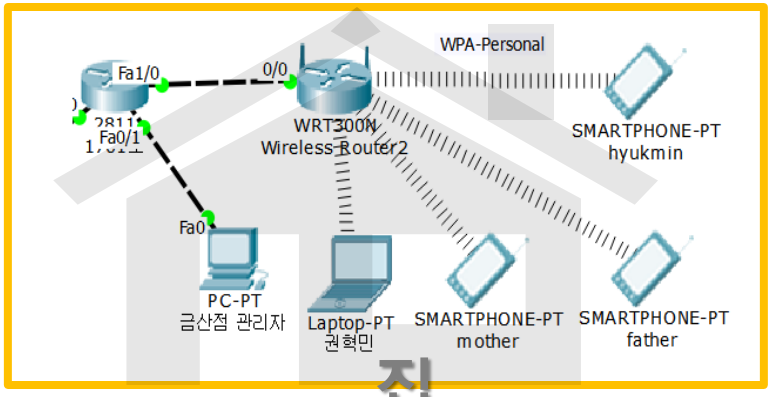
- 동적할당(Dynamic allocation): 주소를 할당 받는 장치에서 주소가 필요 없다는 메시지를 보낼 때까지 주소를 할당
- 자동할당(Automatic allocation): 주소를 영구적으로 할당
- 수동할당(Manual allocation): 미리 할당된 주소를 장치에게 전달하여 장치가 IP주소를 사용할 수 있도록 함

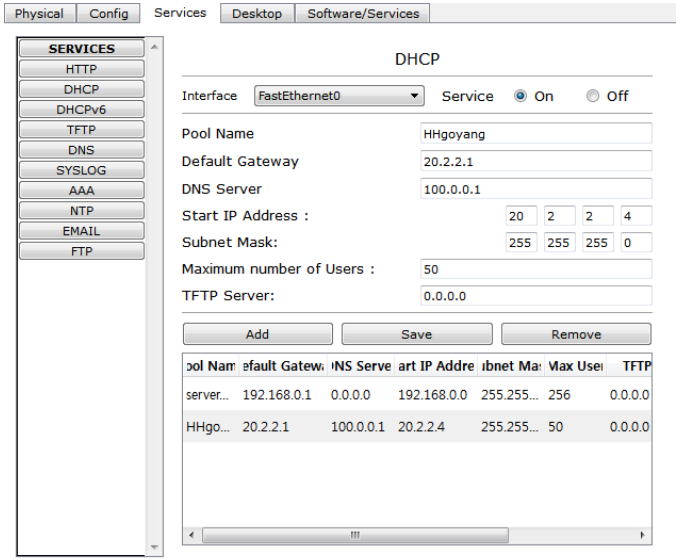
DHCP

DHCP

Dynamic **H**ost **C**onfiguration **P**rotocol



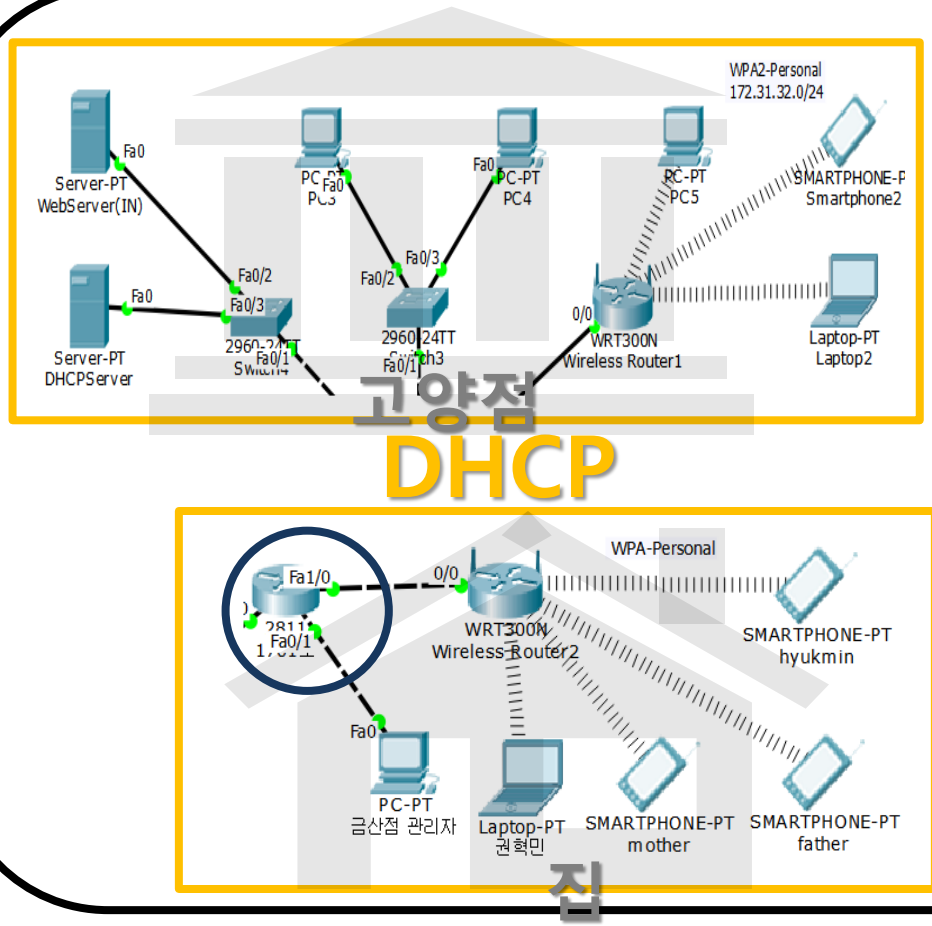




DHCP

DHCP

Dynamic Host Configuration Protocol



[DHCP 라우터]

```
1804(config)#ip dhcp excluded-address 192.168.0.1
1804(config)#ip dhcp excluded-address 192.168.0.255
1804(config)#ip dhcp pool router-dhcp
1804(dhcp-config)#network 192.168.0.0 255.255.255.0
1804(dhcp-config)#dns-server 100.0.0.1
1804(dhcp-config)#default-router 192.168.0.1
1804(dhcp-config)#exit
```


NAT

NAT

Network Address Translation

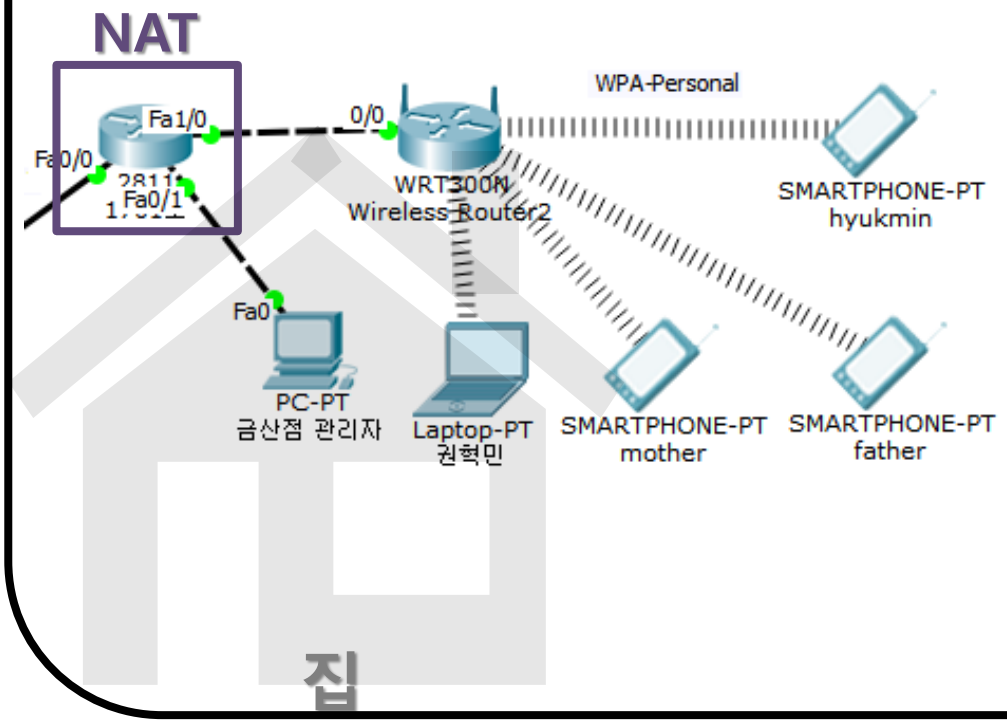
NAT란?

- 사설주소를 사용하는 장치가 공중네트워크와 통신하고자 할 때 사설IP주소를 공인IP주소로 변환해 주는 기술
- 내부 네트워크에서는 사설 IP주소를 사용하고, 외부 네트워크로 나가는 경우 공인 IP주소로 변환돼서 나가게 하는 기술

1. 정적 NAT
   - 사설IP주소와 공인IP주소가 1:1로 매칭. 고정된 IP주소를 가져야 하는 웹서버 등에 사용
   - 외부에서 내부 사설망을 접속하고자 할 때 사용
2. 동적 NAT
   - 클라이언트가 요청하는 순서대로 공인IP주소를 부여
   - 공인IP그룹과 사설IP그룹을 그룹 대 그룹으로 Mapping
3. NAT 오버로딩 = PAT(port address translation)
   - 여러 개의 사설IP주소를 하나의 공인IP주소(포트번호 이용)로 변환
   - 호스트마다 포트번호를 다르게 설정해서 하나의 공인 IP 주소로 외부와 통신가능

NAT

Network Address Translation



[NAT]

```
1804(config)#ip route 0.0.0.0 0.0.0.0
fastEthernet 0/0
1804(config)#ip nat inside source list 100
interface fa0/0 overload
1804(config)#access-list 100 permit ip
192.168.0.0 0.0.0.255 any
1804(config)#access-list 100 permit ip
172.16.183.0 0.0.0.255 any
1804(config)#int fastEthernet 0/1
1804(config-if)#ip nat inside
1804(config-if)#int fastEthernet 0/0
1804(config-if)#ip nat outside
```

TBANK YOU