10차시 수업
10/27 (목) 송준규

등교수업	10/27	목	15:30 ~ 18:30
등교수업			
등교수업			
등교수업	10/28	금	15:30 ~ 18:30
등교수업			
등교수업			
등교수업	11/1	화	16:30 ~ 18:30

이번 시간 (Frame-Relay, Server Service)

다음 시간 (Secret Challenge)

온라인 강의 대체 예정

9-1. VTP(Vlan Trunking Protocol)

Vlan :Switch에서만 지원 (Bridge, Hub 미지원)
:논리적으로 Broadcast Domain을 나눈다.

```
Switch# show vlan // vlan 정보 조회
Switch(config)# vlan [N] // 삭제시, no vlan [N]
Switch(config-vlan)# name [Name]
```

Vlan: Broadcast Domain을 나눈다.
VTP: Vlan 정보를 일치시켜 준다.
VTP: Trunk Port로만 전달 된다.
VTP Domain, VTP Password

VTP(Vlan Trunking Protocol): Switch간 vlan 정보를 항상 일치 시켜 주는 프로토콜
(Why? 모든 Switch에 Vlan 생성하는 것은 귀찮기 때문)

VTP 정보: **Trunk port** 로만 전달 가능
VTP: Domain, Password 값이 같아야 VTP 진행 가능

-다른 네트워크는 라우터를 통해야만 연결이 가능하다 (라우팅 필요)

9-2. VTP(VTP mode)

VTP mode
1. Server
2. Transparent
3. Client

VTP mode: Server / Transparent / Client
Server: 생성, 변경, 전달 가능
Transparent: 본인 저장 X, 전달만 가능
Client: 연결된 스위치에 전달, 수신 가능

Switch(config)#vtp mode server / transparent / client (3중1택)
Switch(config)#vtp domain [Domain]
Switch(config)#vtp password [Password]

#Deafult Value:
VTP Domain Name = null
VTP version = 1 (v2, Token ring vlan 지원)
VTP Mode = Server

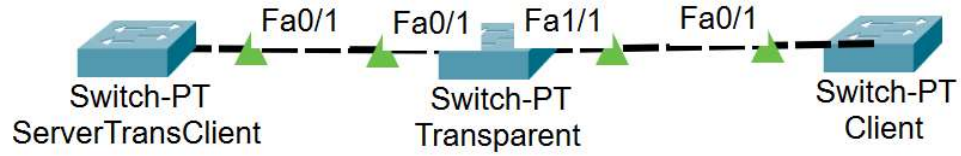
9-3. VTP(VTP mode)

VTP mode: Server / Transparent / Client

Server: 생성, 변경, 전달 가능

Transparent: 본인 저장 X, 전달만 가능

Client: 연결된 스위치에 전달, 수신 가능




```
Server#show vlan

VLAN Name
---- -----------
1    default

10   Red
20   Green
30   Blue
```

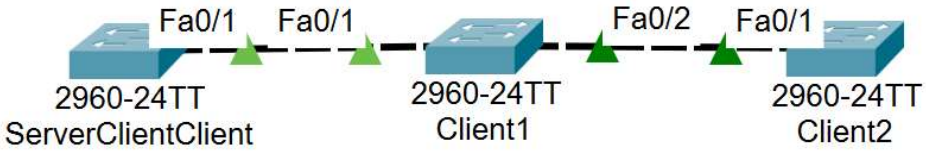
저장 o

```
Transparent#show vlan

VLAN Name
---- -----------
1    default
1002 fddi-default
1003 token-ring-default
1004 fddinet-default
1005 trnet-default
```

저장 x

```
Client#show vlan

VLAN Name
---- -----------
1    default

10   Red
20   Green
30   Blue
```

저장 o




```
Server#show vlan

VLAN Name
---- -----------
1    default

40   Hour
50   Minute
60   Second
```

저장 o

```
Client1#show vlan

VLAN Name
---- -----------
1    default
40   Hour
50   Minute
60   Second
```

저장 o

```
Client2#show vlan

VLAN Name
---- -----------
1    default

40   Hour
50   Minute
60   Second
```

저장 o

9-4. VTP(Switchport mode)

```
// 특정 Vlan 적용 시, (1개)
Switch(config)# int [interface]
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan [N]

// Trunk port 적용 시, (N개)
Switch(config)# int [interface]
Switch(config-if)# switchport mode trunk
```

요약: Trunk mode 설정 + Acces 설정
auto-auto, [Any]-Access 제외하고,
Trunk port로 사용 가능

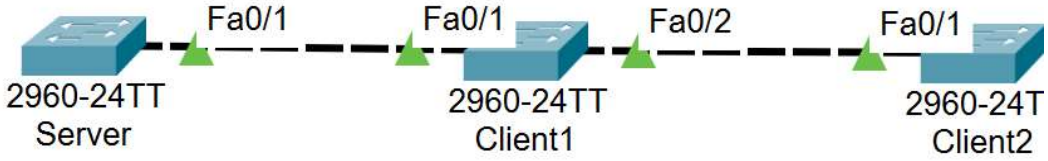
DTP(Dynamic Trunking Protocol)
1. access: Never trunk, Never DTP send
   : Switch(config-if)# switchport mode access
2. trunk: DTP send, 상대방 DTP ignore
   : Switch(config-if)# switchport mode trunk
3. dynamic (auto): DTP send X, DTP reply only // default
   : Switch(config-if)# switchport mode dynamic auto
4. dynamic (desirable): DTP send, DTP reply
   : Switch(config-if)# switchport mode dynamic desirable
5. Nonegotiate: disable DTP
   : Switch(config-if)# switchport nonegotiate

9-5. VTP(Lab)

요약: VTP 덕분에 귀찮은 작업을 줄일 수 있다.

Situation: VTP 덕분에 Server, Client, Client 상황에서 Vlan 6개의 정보를 서로 일치시키고 있다.

1. VTP Mode, Domain, Password 설정 (3*3=9)
2. VTP Server에 6개의 Vlan 정보 생성 (6)
3. 각 Segment 별로 Trunk port 지정 (2) // 17



If same Situation에서, VTP가 없다면?

1. Switch 별 Vlan 정보 생성 (6*3=18)
2. 각 포트별 Vlan 적용 (2*6*2=24) // 42
*. Vlan 정보 수정시 반영 X

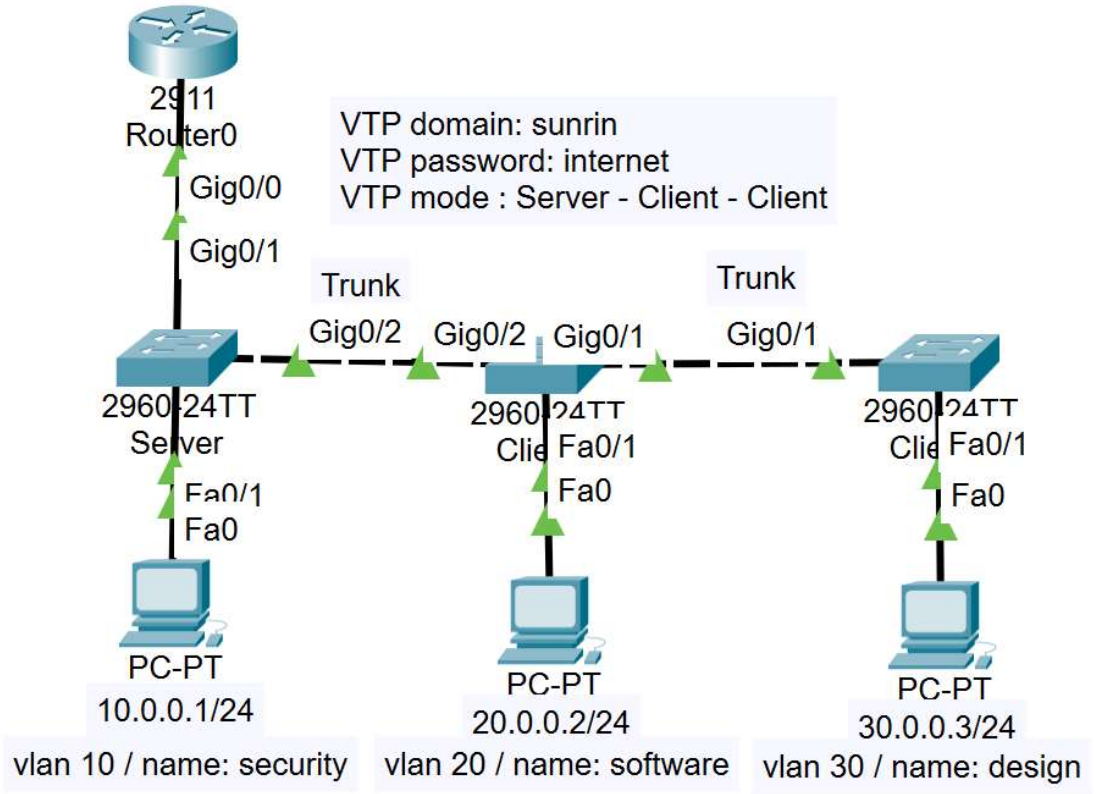
9-6. Inter-Vlan(Tutorial)

Inter-Vlan을 적용하여 모든 PC 끼리 통신이 가능하도록 설정합니다.
Gateway는 해당 네트워크의 사용가능한 마지막 IP를 사용합니다.
Routing protocol은 RIPv2를 사용합니다.

1. PC IP 부여 (생략)

2. Switch VTP Domain, Password, mode 설정 + VLAN 생성

```
//Switch Server
Server(config)# vtp mode server
Server(config)# vtp domain sunrin
Server(config)# vtp password internet
Server(config)# vlan 10
Server(config-vlan)# name security
Server(config-vlan)# vlan 20
Server(config-vlan)# name software
Server(config-vlan)# vlan 30
Server(config-vlan)# name design
//Switch Client 1
Client1(config)# vtp mode client
Client1(config)# vtp domain sunrin
Client1(config)# vtp password internet
//Switch Client 2
Client2(config)# vtp mode client
Client2(config)# vtp domain sunrin
Client2(config)# vtp password internet
```

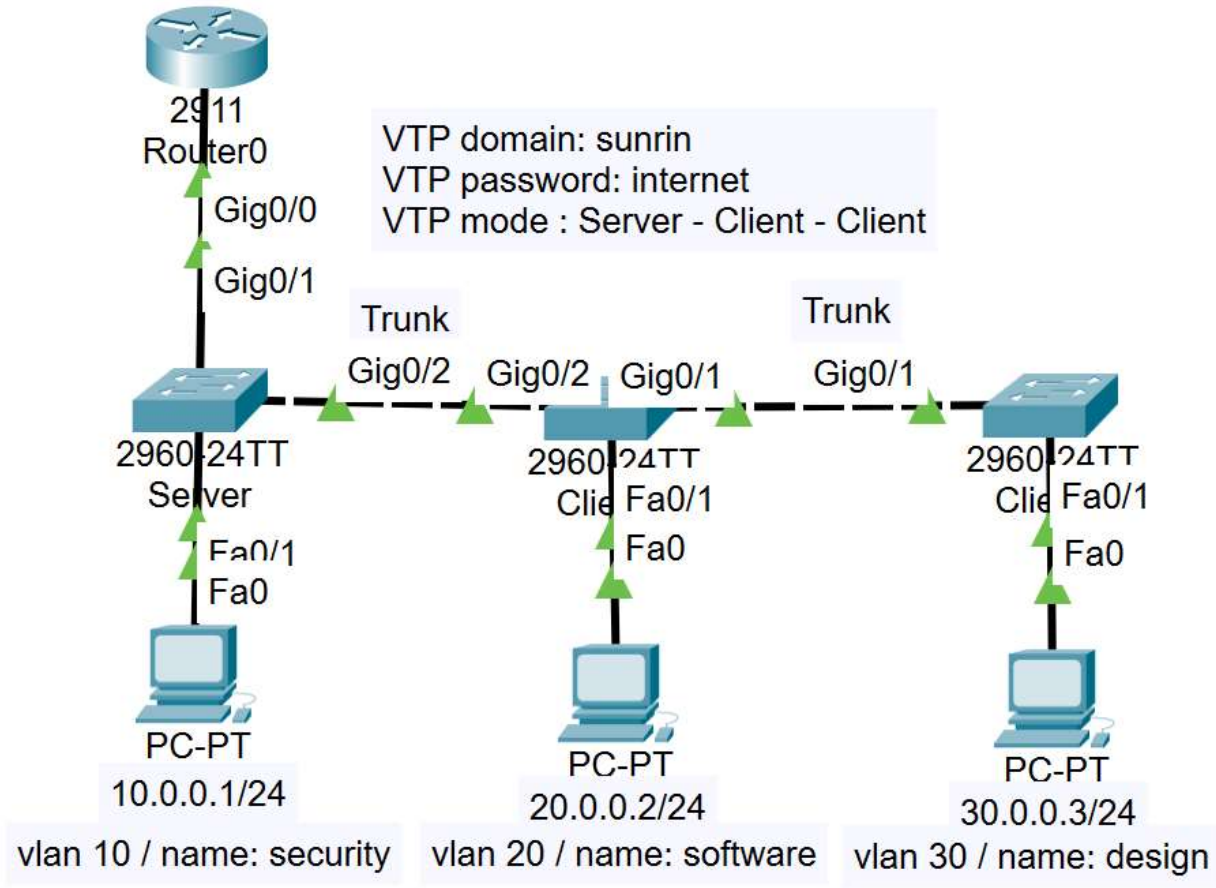


9-7. Inter-Vlan(Tutorial)

3. Trunk mode 설정
//Switch Server
Server(config)# int g0/2
Server(config-if)# switchport mode trunk
//Switch Client 1
Client1(config)# int g0/1
Client1(config-if)# switchport mode trunk

4. Vlan access 설정
//Switch Server
Server(config)# int fa0/1
Server(config-if)# switchport mode access
Server(config-if)# switchport access vlan 10
//Switch Client 1
Client1(config)# int fa0/1
Client1(config-if)# switchport mode access
Server(config-if)# switchport access vlan 20
//Switch Client 2
Client2(config)# int fa0/1
Client2(config-if)# switchport mode access
Server(config-if)# switchport access vlan 30

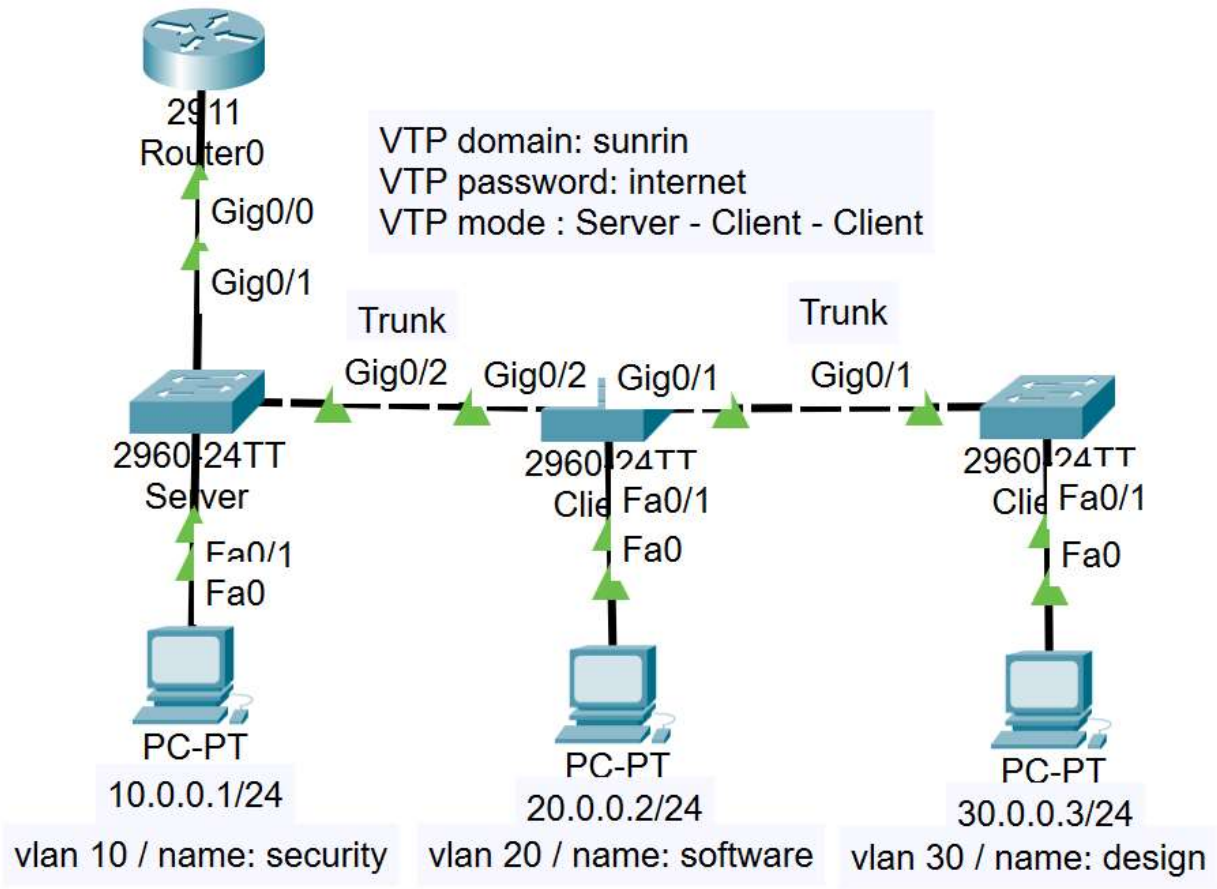
5. Router와 만나는 Switch: Trunk port 지정
//Switch Server
Server(config)# int gi0/1
Server(config-if)# switchport mode trunk



9-8. Inter-Vlan(Tutorial)

6. Router NO shutdown + Sub-Interface 생성
7. Sub-Interface에 vlan 정보 입력
// Router(config-subif)#encapsulation dot1Q [N]
8. Sub-Interface에 IP 정보 입력

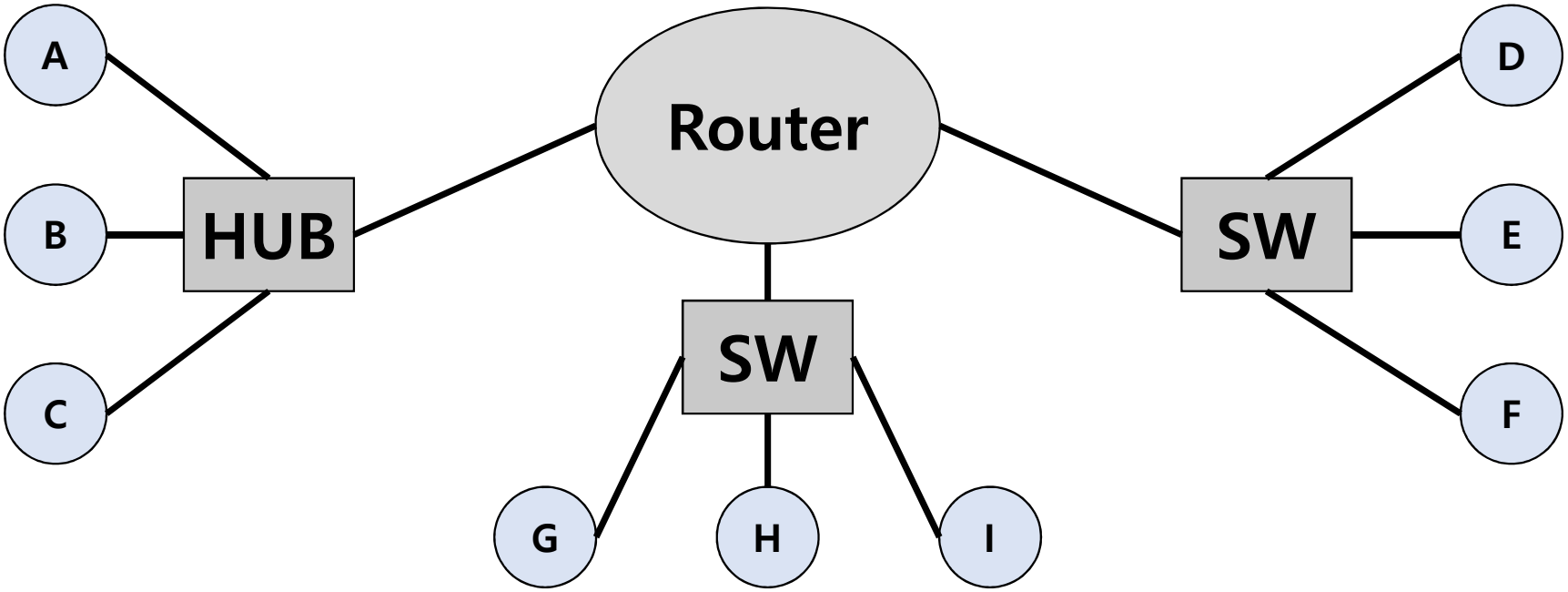
[6,7,8]
```
Router(config)# int gi0/0
Router(config-if)# no sh

Router(config)#int gi0/0.10
Router(config-subif)#encapsulation dot1Q 10
Router(config-subif)#ip add 10.0.0.254 255.255.255.0

Router(config-subif)#int gi0/0.20
Router(config-subif)#encapsulation dot1Q 20
Router(config-subif)#ip add 20.0.0.254 255.255.255.0

Router(config-subif)#int gi0/0.30
Router(config-subif)#encapsulation dot1Q 30
Router(config-subif)#ip add 30.0.0.254 255.255.255.0
// PC Gateway 주소로, .254 맞춰 주기
```
9. Routing table Update
```
Router(config)# router rip
Router(config)# version 2
Router(config)# net 10.0.0.0
Router(config)# net 20.0.0.0
Router(config)# net 30.0.0.0
Router(config)# no au
```



9-9. Summary + Quiz

Broadcast Domain은 Vlan 때문에 정확히 알기 어렵다.

Quiz : How many Broadcast domain, Collision Domain in this topology?



Vlan

10-1. WAN(Prepare)

요약: LAN처럼 WAN에도 2계층 Encapsulation 방식이 있고,
그 중에는 HDLC, PPP, Frame-Relay와 같은 방식(모양) 들이 있다.

WAN <-> LAN
WAN
: 멀리 떨어진 LAN과 LAN 사이 연결
: 직접 케이블을 깔 수 없을 때
3계층 <-> 2계층: 속도 차이

1. Leased Line: 전용선 (비용, 안정)
ㄴPPP, HDLC
2. Circuit Switching (예약 시간 비례/회선 회수)
ㄴPPP, HDLC
3. Packet Switching (패킷 비례/ 회선 공유)
ㄴFrame-Relay (Router 필요)
*. VPN <-> 전용선

Packet -> Router -> 2계층 Header를 벗김 -> 3계층 주소 확인 -> 2계층 새로운 정보 생성 -> 외부

WAN's 2계층 Protocol (Not 3계층) // encapsulation 방식

1. ATM (음성, 영상/ 53 byte Cell)
2. HDLC (High-level DataLink Control / Cisco 전용: Default / 표준 HDLC와 다름)
2. PPP (타사 장비 사용 가능/ PAP, CHAP / more better than HDLC / 기능)
3. Frame-Relay (오류 검출 drop -> 속도 get)

이론

10-2. WAN(PPP)

요약: PPP는 NCP, LCP를 통해 다양한 기능을 제공한다.
1. PAP, 2. CHAP 인증 기능 지원

PPP (Point to Point)
1. NCP (Netwok Control Protocol)
서로 다른 3계층 protocol encapsulation 지원
= Multi Protocol 지원
= 타사 장비 끼리 사용 가능하다

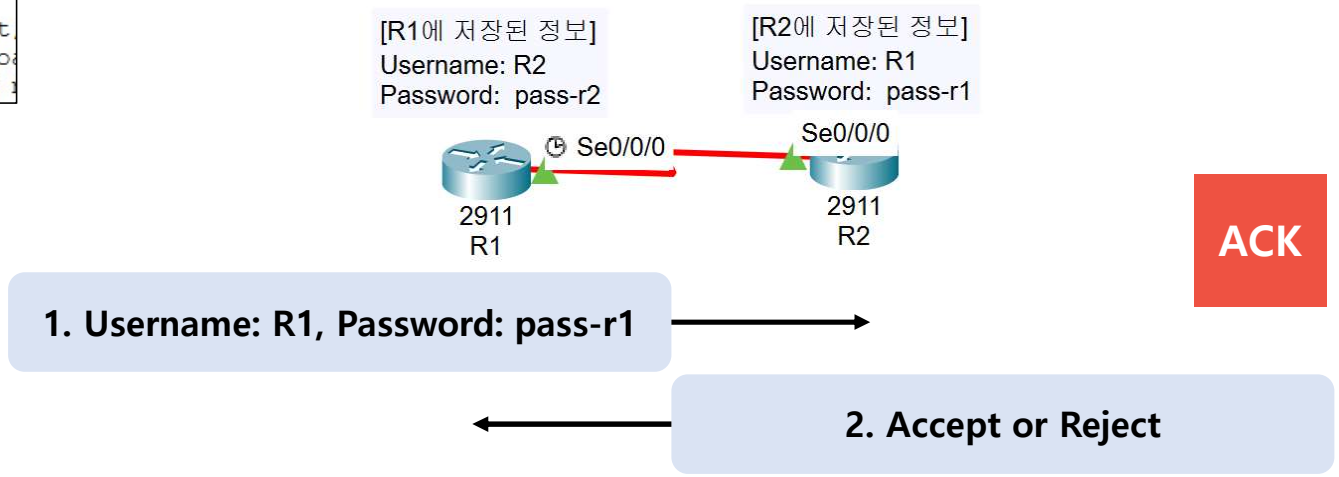
2. LCP (Link Control Protocol)
보안, 인증, 압축, 에러 검출, 다중 링크
- 2-1. PPP PAP
- 2-2. PPP CHAP

```
Router#show interfaces se0/0/0
Serial0/0/0 is administratively
(disabled)
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit,
     reliability 255/255, txlo
  Encapsulation HDLC, loopback
```

```
Router#show interfaces se0/0/0
Serial0/0/0 is administratively
(disabled)
  Hardware is HD64570
  MTU 1500 bytes, BW 1544 Kbit,
     reliability 255/255, txlo
  Encapsulation PPP, loopback
```

10-3. WAN(PPP PAP)

PAP (Password Authentication Protocol)
2-way hand shake 방식으로, 최초 연결 시에만 한번 인증 검사,
username, password 평문으로 전달

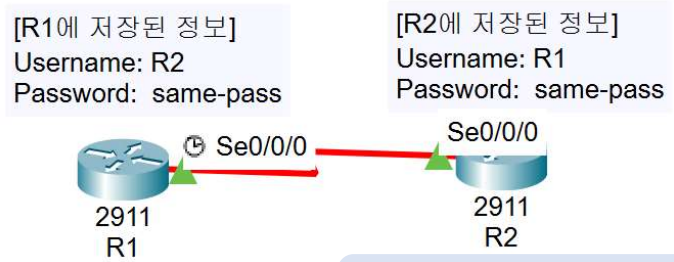



```
R1(config)# username R2 password pass-r2
R1(config)#int se0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication pap
R1(config-if)#ppp pap sent-username R1 password pass-r1
```

```
R2(config)# username R1 password pass-r1
R2(config)#int se0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication pap
R2(config-if)#ppp pap sent-username R2 password pass-r2
```

10-4. WAN(PPP CHAP)

CHAP (Challenge Handshake Authentication Protocol)
username, password MD5 hash값으로 전송
(톱 전송 -> 받은 톱으로 password 자르고 전송 -> 받은 잘라진값, 내가 내톱으로 자른값 비교)
hostname으로 peer 식별, 동일한 암호 사용



ACK

1. Challenge
(with Label.R2)

2. Response
(Lable.R2.same-pass.Hash with Lable.R1)

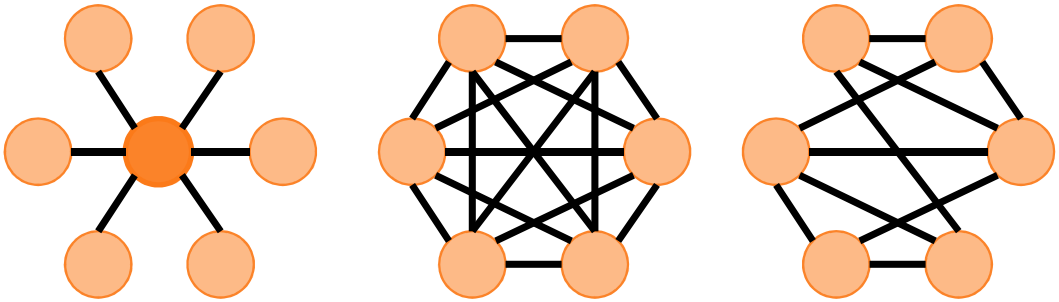
3. Accept or Reject
(Hash from R2 v.s. R1.same-pass.Hash)

```
Router(config)# hostname R1
R1(config)#username R2 password same-pass
R1(config)#int se0/0/0
R1(config-if)#encapsulation ppp
R1(config-if)#ppp authentication chap
```

```
Router(config)# hostname R2
R2(config)#username R1 password same-pass
R2(config)#int se0/0/0
R2(config-if)#encapsulation ppp
R2(config-if)#ppp authentication chap
```

10-5. Frame-Relay(Prepare)

Frame-Relay: WAN Encapsulation (가상 전용선 제공)
Routing X so, Router Needed for Routing(Packet Switching)
종류: Hub-And-Spoke, Full-mesh, Partial-mesh



X.25 Packet Switching의 overhead(오류 책임 X->다른 계층에 전담, Drop) 제거 -> Frame-Relay탄생

/*

cf) Frame-Relay 관련 용어 정리

이론

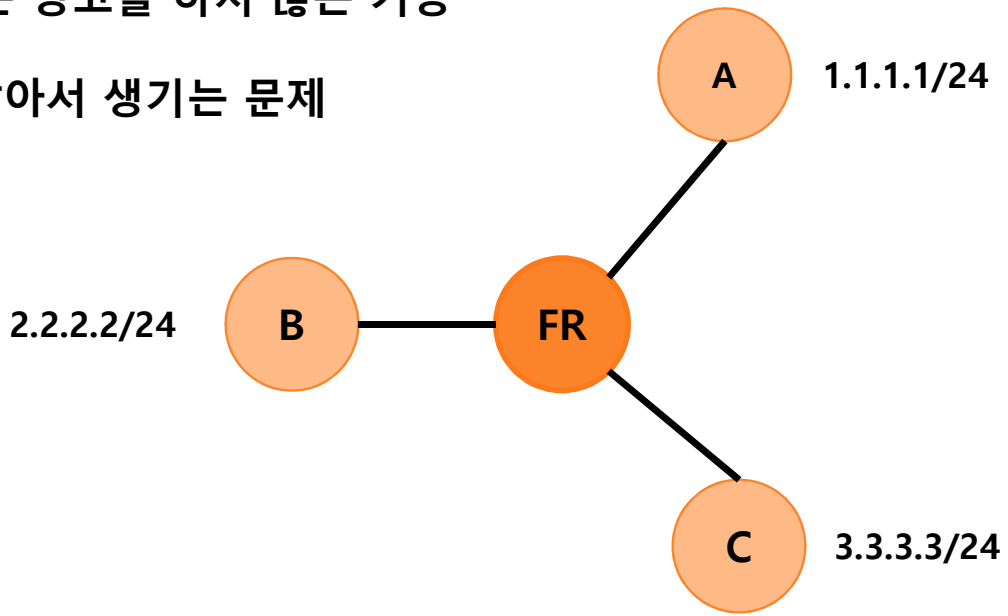
PVC (Permanent Virtual Circuit): 고정 가상 회선
DLCI (Data Link Connection Identifier): PVC 구별을 위한 식별 주소
LMI (Local Management Interface): PVC 상태 정보를 위한 Protocol
Inverse ARP (Address Resolution Protocol): DLCI, Router IP 자동 연동 Protocol // Dynamic Mapping
FECB (Forward Explicit Congestion Notification): 트래픽 혼잡시 데이터 수신 Router에 통지
BECN (Backward Explicit Congestion Notification): 트래픽 혼잡시 데이터 송신 Router에 통지
DE (Discard Eligiblity): 트래픽 혼잡시 가장 우선적으로 버려지는 Frame 설정 비트
CIR (Commited Information Rate): Frame-Relay에서 허용되는 전송 속도 */

10-6. Frame-Relay(Split-horizon)

Split-horizon: Distance Vector 알고리즘을 사용하는 라우터에서
특정 정보가 특정 포트에서 들어왔다면, 해당 포트로는 광고를 하지 않는 기능

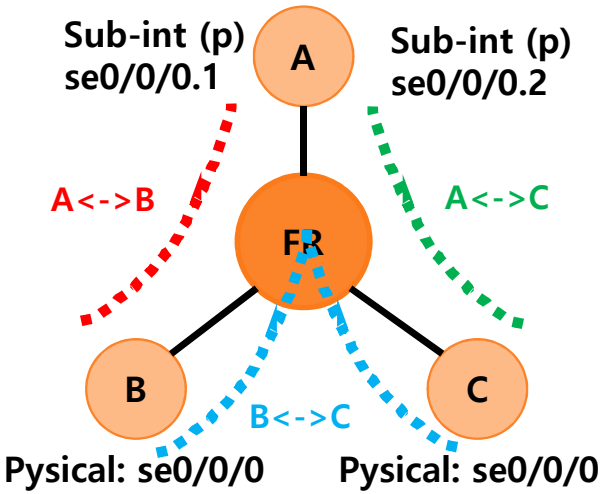
Frame-Relay의 정보가 들어온 port 나가는 port가 같아서 생기는 문제

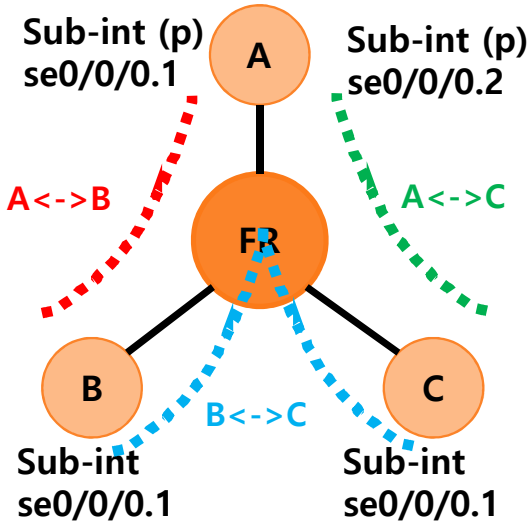
Solution 1. Sub-Interface를 선언하여, port 분리
Solution 2. Split horizion 기능 비활성화
Solution 3. Link State 방식 라우팅 사용

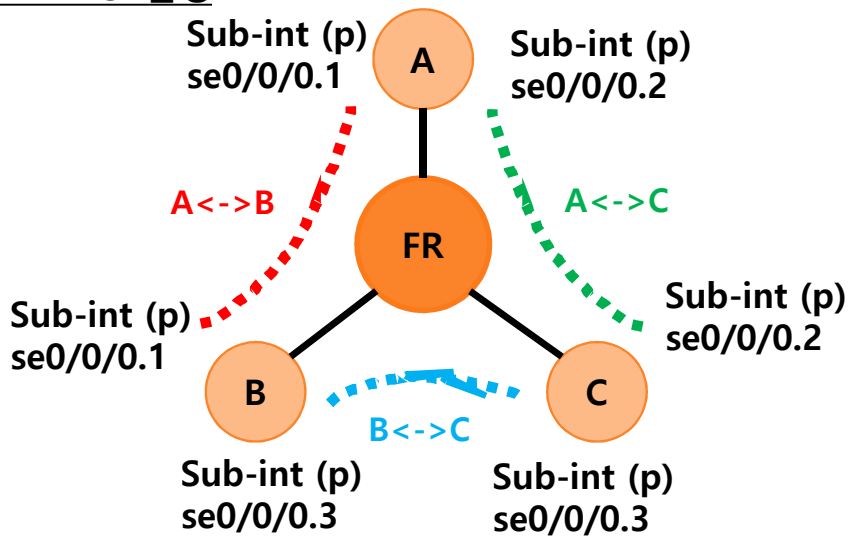


10-7. Frame-Relay(2 Types)

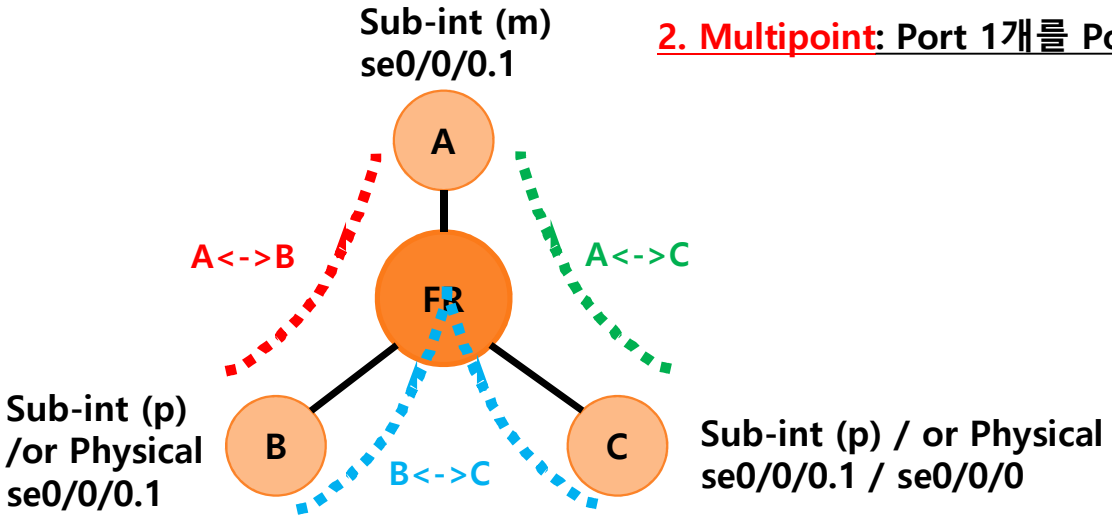
1. Point-to-Point: Port 1개와 port 1개를 1:1로 DLCI 설정

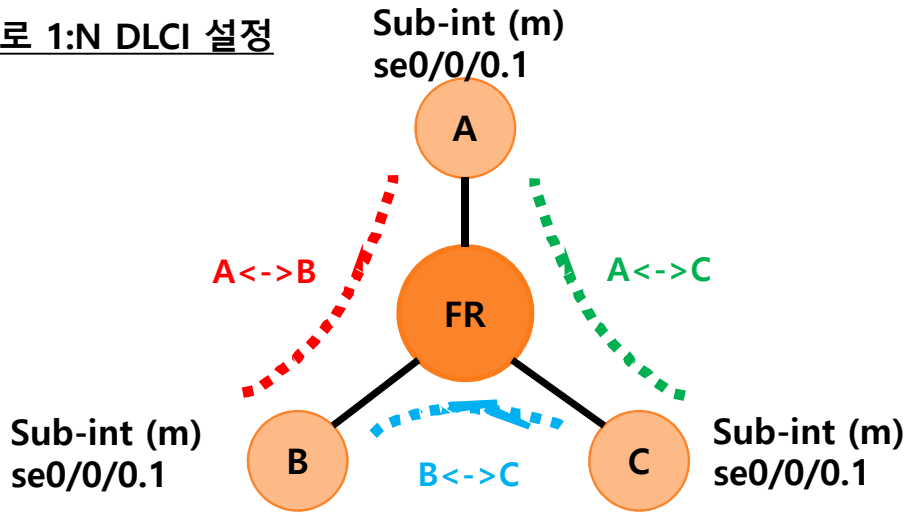






2. Multipoint: Port 1개를 Port 여러개로 1:N DLCI 설정





10-8-1. Frame-Relay(Point to Point Settings)

1. Point-to-Point: Port 1개와 port 1개를 1:1로 DLCI 설정 (via)

int se0/0/0
encapsulation frame-relay
no frame-relay inverse-arp // DLCI 자동 적용 방지

int se0/0/0.1 point-to-point // port 번호 상관 X
ip add [IP] [SM] // ip 부여 (Port 마다 다른 Subnet)
frame-relay interface-dlci [DLCI] // Sub-interface 에서만 사용 가능

[Routing]

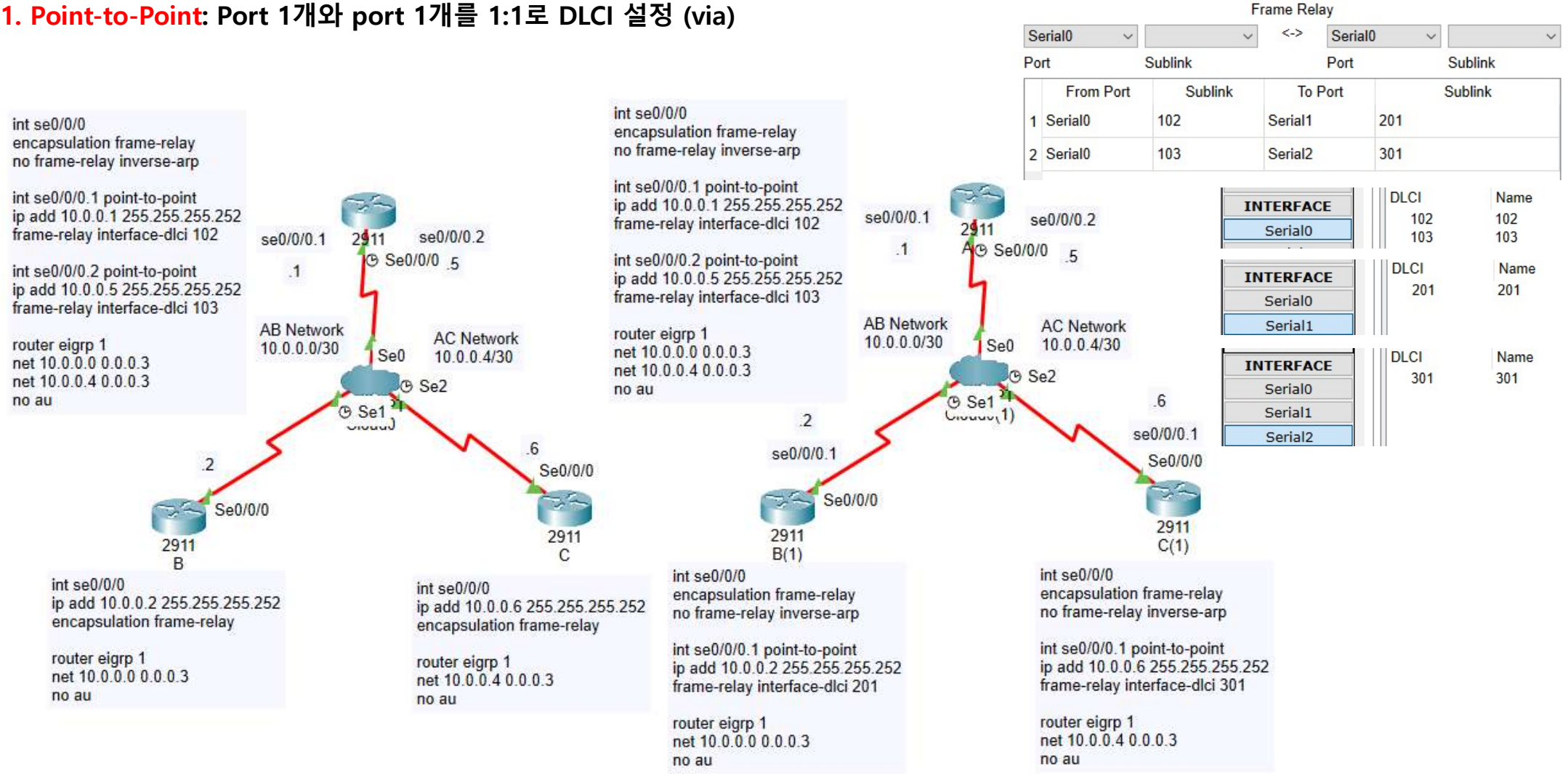
2. Multipoint: Port 1개와 port N개를 1:N로 DLCI 설정 (via)
int se0/0/0
encapsulation frame-relay
no frame-relay inverse-arp // DLCI 자동 적용 방지

int se0/0/0.1 multipoint
ip add [IP] [SM] // ip 부여 (동일한 Subnet)
frame-relay map ip [목적지 frame-relay ip] [DLCI] broadcast // broadcast+multicast 허용 / Physical, Multiport 일때

[Routing]

10-8-2. Frame-Relay(Point to Point via)

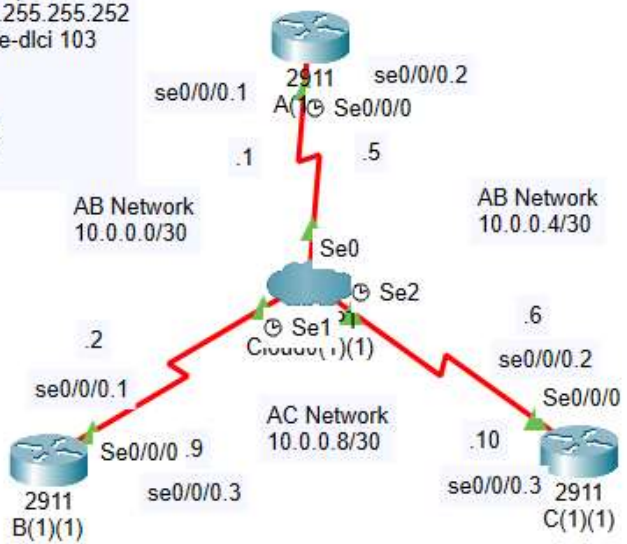
1. Point-to-Point: Port 1개와 port 1개를 1:1로 DLCI 설정 (via)



10-8-3. Frame-Relay(Point to Point mesh)

1. Point-to-Point: Port 1개와 port 1개를 1:1로 DLCI 설정 (mesh)

```
int se0/0/0
encapsulation frame-relay
no frame-relay inverse-arp

int se0/0/0.1 point-to-point
ip add 10.0.0.1 255.255.255.252
frame-relay interface-dlci 102

int se0/0/0.2 point-to-point
ip add 10.0.0.5 255.255.255.252
frame-relay interface-dlci 103

router eigrp 1
net 10.0.0.0 0.0.0.3
net 10.0.0.4 0.0.0.3
no au
```




```
int se0/0/0
encapsulation frame-relay
no frame-relay inverse-arp

int se0/0/0.1 point-to-point
ip add 10.0.0.2 255.255.255.252
frame-relay interface-dlci 201

int se0/0/0.3 point-to-point
ip add 10.0.0.9 255.255.255.252
frame-relay interface-dlci 203

router eigrp 1
net 10.0.0.0 0.0.0.3
net 10.0.0.8 0.0.0.3
no au
```

```
int se0/0/0
encapsulation frame-relay
no frame-relay inverse-arp

int se0/0/0.1 point-to-point
ip add 10.0.0.6 255.255.255.252
frame-relay interface-dlci 301

int se0/0/0.3 point-to-point
ip add 10.0.0.10 255.255.255.252
frame-relay interface-dlci 302

router eigrp 1
net 10.0.0.4 0.0.0.3
net 10.0.0.8 0.0.0.3
no au
```

Frame Relay

Serial0		<->	Serial0	
Port	Sublink		Port	Sublink

	From Port	Sublink	To Port	Sublink
1	Serial0	102	Serial1	201
2	Serial0	103	Serial2	301
3	Serial1	203	Serial2	302

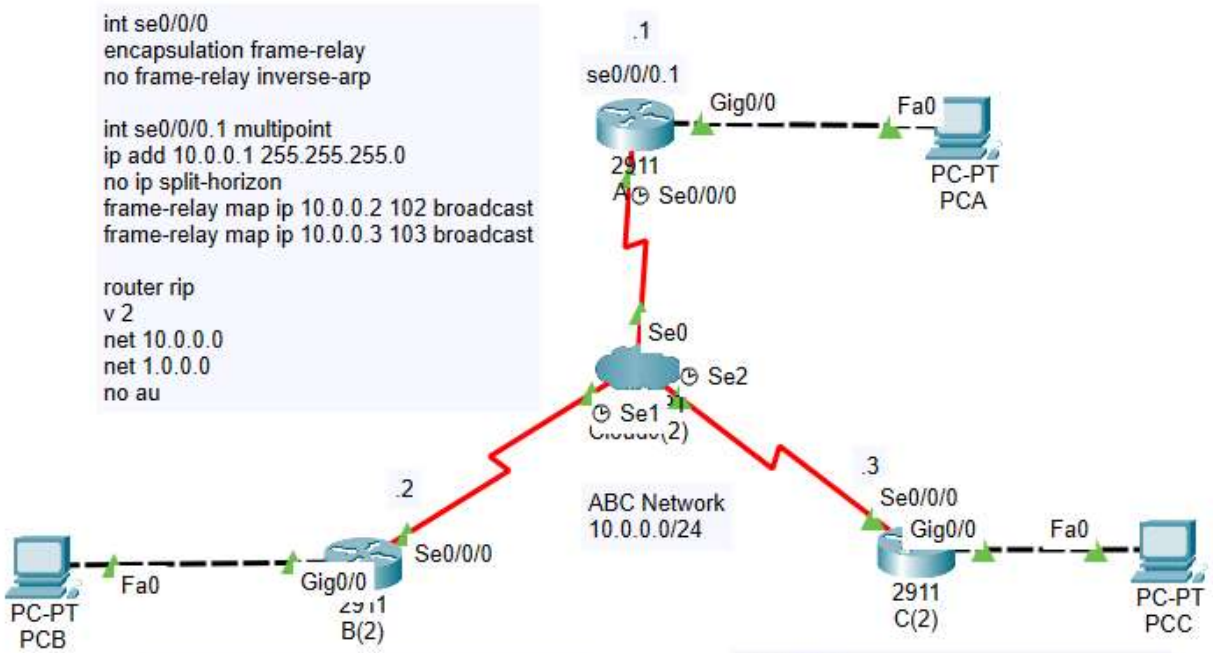
INTERFACE	DLCI	Name
Serial0	102	102
	103	103

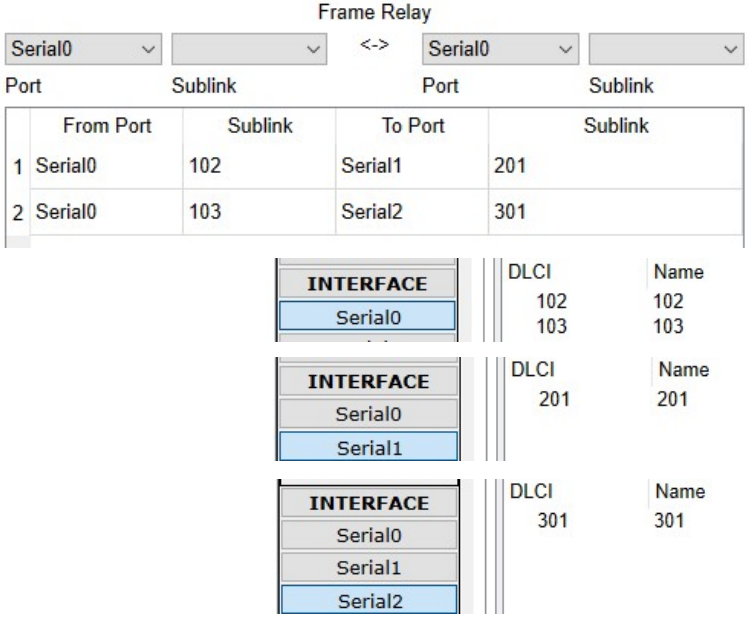
INTERFACE	DLCI	Name
Serial0	201	201
Serial1	203	203

INTERFACE	DLCI	Name
Serial0	301	301
Serial1	302	302
Serial2		

10-8-4. Frame-Relay(Multipoint via)

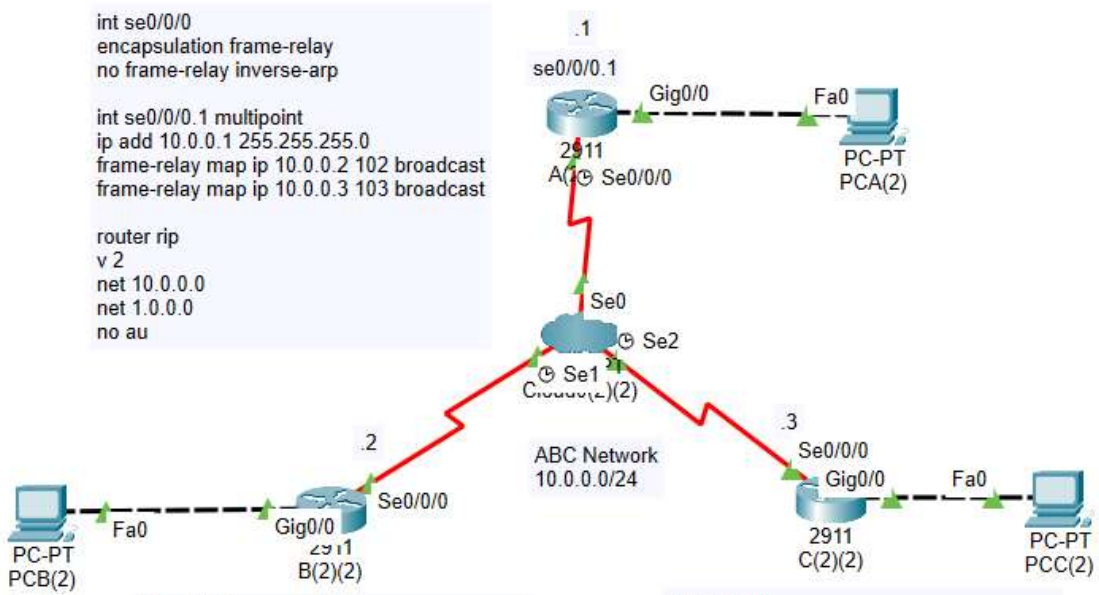
2. Multipoint: Port 1개와 port N개를 1:N로 DLCI 설정 (via)





10-8-5. Frame-Relay(Multipoint mesh)

2. Multipoint: Port 1개와 port N개를 1:N로 DLCI 설정 (mesh)



Frame Relay

Serial0		<->	Serial0	
Port	Sublink		Port	Sublink

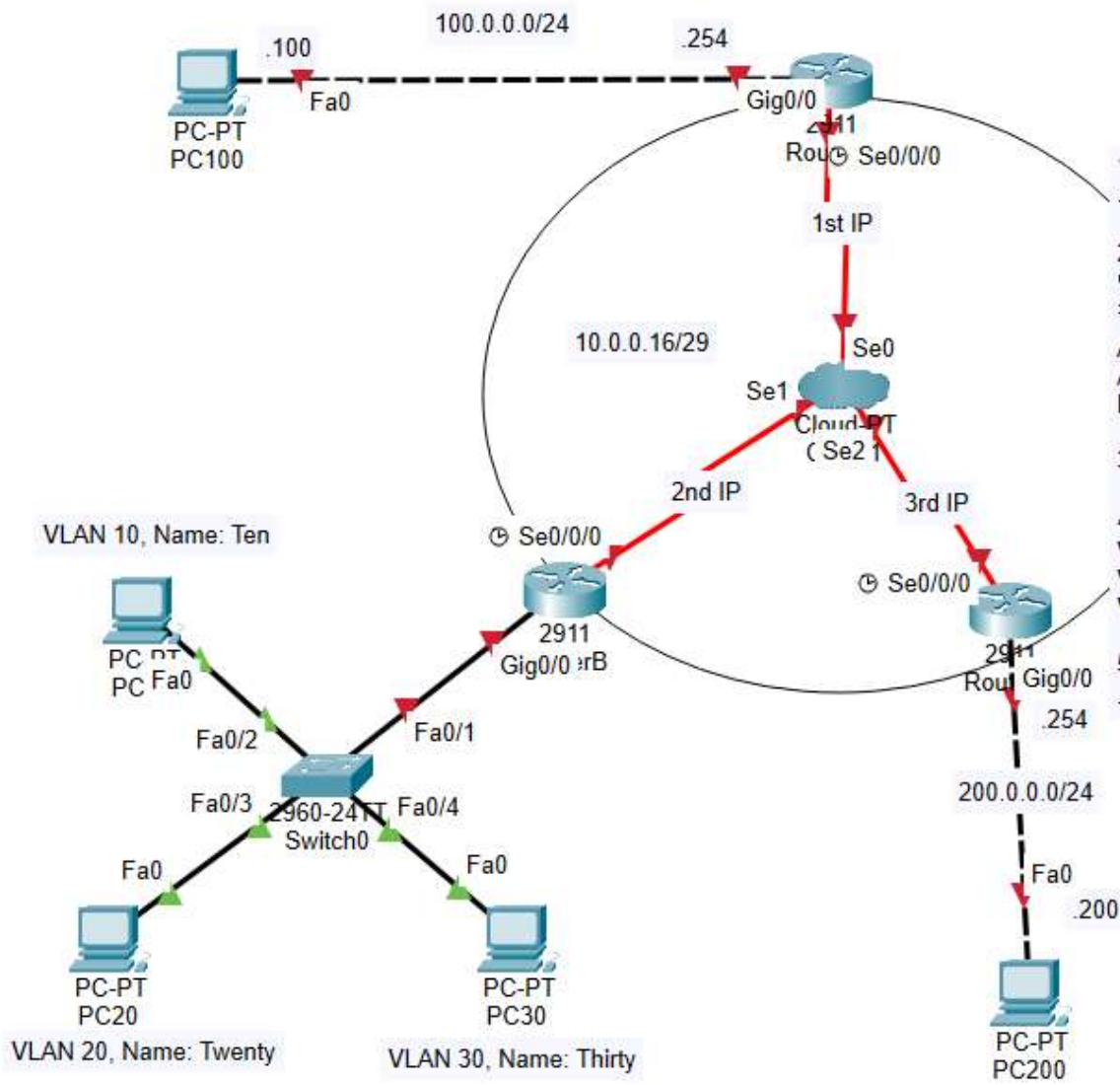
	From Port	Sublink	To Port	Sublink
1	Serial0	102	Serial1	201
2	Serial0	103	Serial2	301
3	Serial1	203	Serial2	302

INTERFACE	DLCI	Name
Serial0	102	102
	103	103

INTERFACE	DLCI	Name
Serial0	201	201
Serial1	203	203

INTERFACE	DLCI	Name
Serial0	301	301
Serial1	302	302
Serial2		

10-8-6. Frame-Relay(Practice)



1. RIP v2 Routing
모든 PC끼리 통신이 가능하도록 설정합니다.

2. Multipoint Frame-Relay를 구성합니다.
단, 모든 DLCI끼리 직접 연결이 가능해야 합니다.
필요한 DLCI는 아래와 같이 설정합니다.
A -> B : "102", B-> A : "201"
A -> C : "103", C -> A: "301"
B -> C : "203", C -> B: "302"

3. PC10, 20, 30에 각각 VLAN 10, 20, 30을 적용 시킵니다.

4. VLAN 지역을 위한 IP 대역입니다. 참고하여 설정합니다
VLAN 10: 110.0.0.0/24
VLAN 20: 120.0.0.0/24
VLAN 30: 130.0.0.0/24

5. 각 PC의 GW는 해당 네트워크의 사용 가능한 마지막 IP를 사용합니다.
또한 각 PC는 사용가능한 첫 IP를 사용합니다.

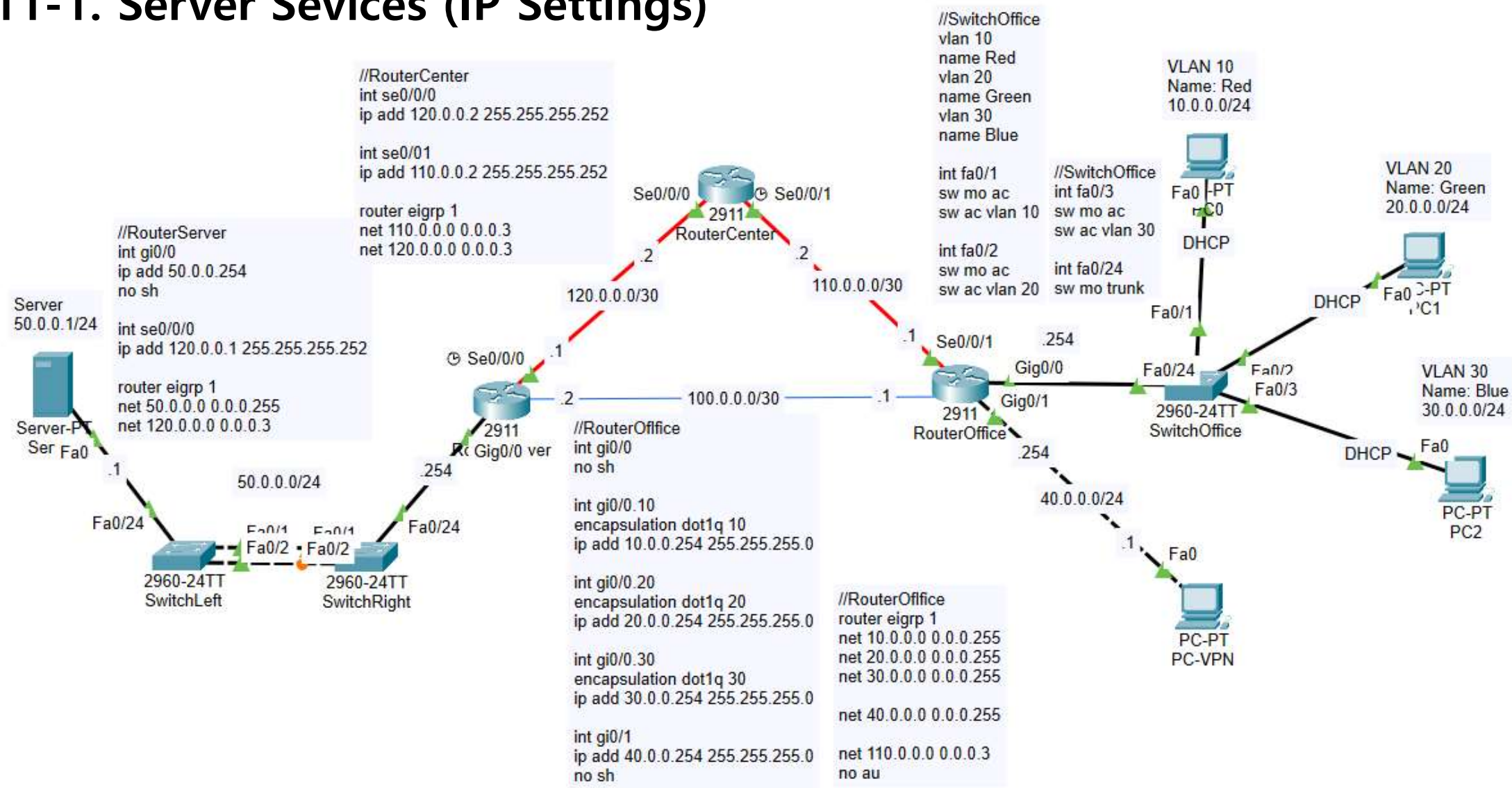
11. Server Sevices (Prepare)

프로그램 운영 계획					
차시	강의 내용	수업 방식	날짜	요일	시간
1	네트워크 개론	등교수업	9/20	화	16:30 ~ 18:30
2	OSI 7 Layer, TCP/IP 이론	등교수업			
3	IP & Subnetting 이론	등교수업	9/22	목	15:30 ~ 18:30
4	서브넷팅 문제 풀이	등교수업			
5	서브넷팅 문제 해설	등교수업			
6	서브넷팅 계산 문제 복습	등교수업	9/23	금	15:30 ~ 18:30
7	라우터 이론	등교수업			
8	정적 라우팅 이론 및 실습	등교수업			
9	RIPv2 라우팅 이론 및 실습	등교수업	9/27	화	16:30 ~ 18:30
10	EIGRP 라우팅 이론 및 실습	등교수업			
11	OSPF 라우팅 이론 및 실습	등교수업	9/29	목	15:30 ~ 18:30
12	스위치 및 L2 관련 이론	등교수업			
13	vlan 이론 설명	등교수업			
14	Inter-vlan 이론 및 실습	등교수업	9/30	금	15:30 ~ 18:30
15	VTP 이론 및 실습	등교수업			
16	ACL 이론 및 실습	등교수업			
17	PPP(pap, chap)	등교수업	10/4	화	16:30 ~ 18:30
18	Port-Security, Ether-Channel 구축	등교수업			
19	라우터, 스위치 내용 정리	등교수업	10/20	목	15:30 ~ 18:30
20	패킷트레이서 기타 명령어 정리	등교수업			
21	Server Service (HTTP, DNS)	등교수업			
22	Server Service (NTP, Syslog)	등교수업	10/25	화	16:30 ~ 18:30
23	Server Service (AAA, DHCP)	등교수업			
24	Frame-Relay 이론	등교수업	10/27	목	15:30 ~ 18:30
25	Frame-Relay 실습	등교수업			
26	트러블 슈팅 문제 풀이 및 해설	등교수업			
27	Secret Challenge 진행	등교수업	10/28	금	15:30 ~ 18:30
28	Secret Challenge 진행	등교수업			
29	Secret Challenge 풀이 및 해설	등교수업			
30	네트워크 학습 가이드 제시	등교수업	11/1	화	16:30 ~ 18:30

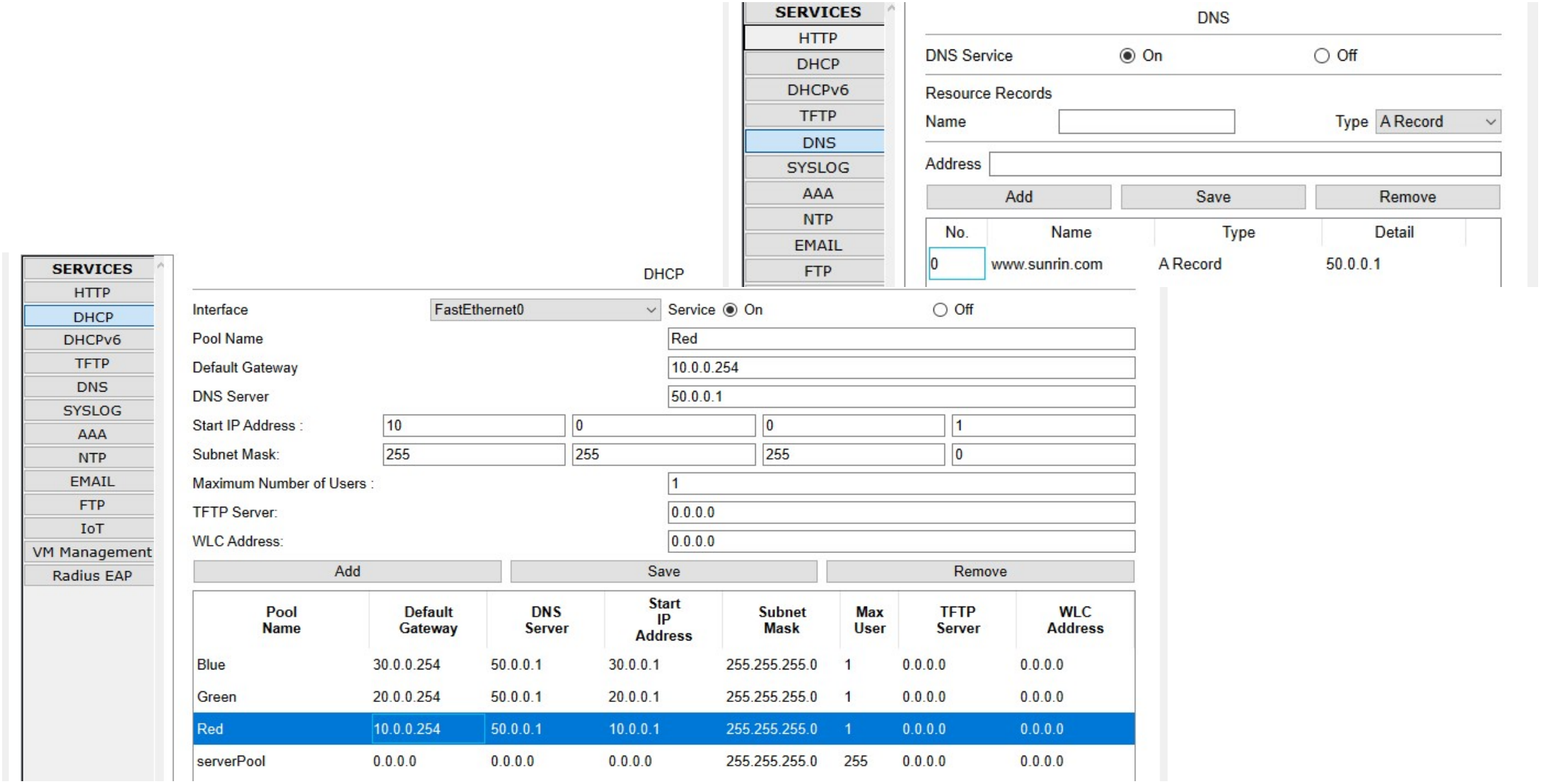
10/27 (목)
1. Server Services (DNS, HTTP, DHCP, AAA, NTP, Syslog)
2. ACL / 3. NAT / 4. VPN / 5. Port-Security / 6. Ether-Channel

10/28 (금)
Secret Challenge + Trouble Shooting

11-1. Server Sevices (IP Settings)



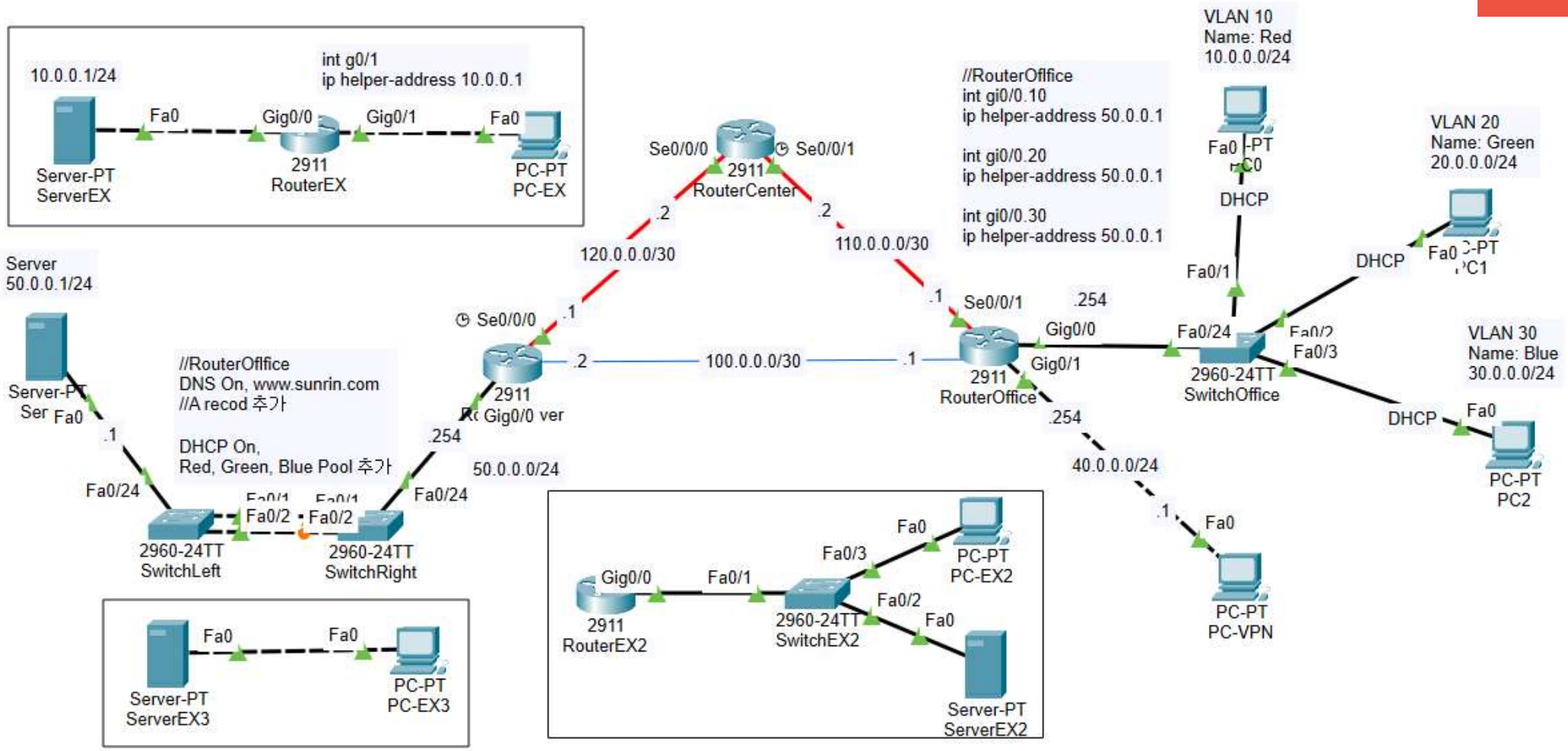
11-2-1. Server Sevices (DHCP, DNS)



11-2-2. Server Sevices (DHCP, DNS)

DNS:
PC -> Command Prompt -> "nslookup"

Option



11-3. Server Sevices (NTP, Syslog, HTTP)

Option

// Check Service On

1. NTP:

Router(config)# ntp server [ntp-server-ip]

2. Syslog:

Router(config)# logging on

Router(config)# logging host [syslog-server-ip]

3. HTTP:

PC -> Web Browser -> 확인 가능

11-4-1. Server Sevices (AAA Syntax)

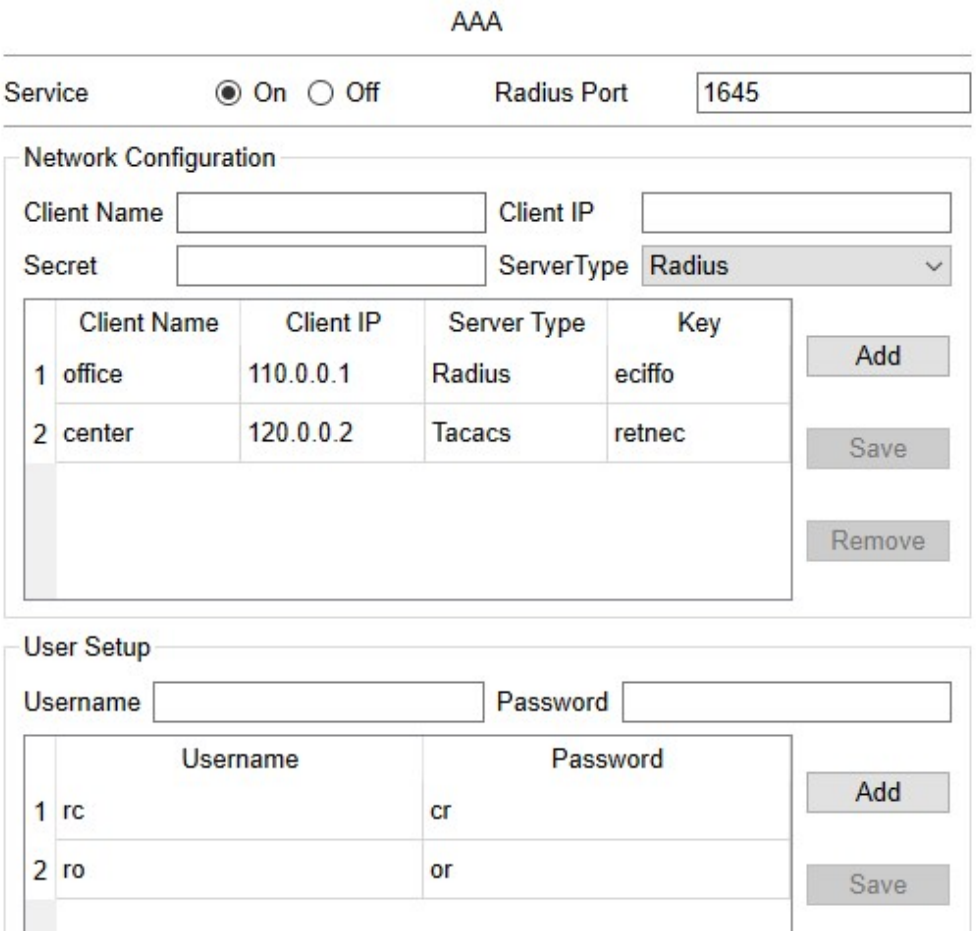
AAA(Authentication, Authorization, Account)

이론

Radius
TACACS+ / Telnet port 적용 / VPN 적용 / Options

Case 1) default(규칙 이름) + radius 조합 (부분 암호화)
aaa new-model // 외부 aaa 인증 장비를 사용합니다.
aaa authentication login default group radius
radius server [RadiusServer]
address ipv4 [radius-server-ip] auth-port 1645 // 변경 가능
key [shared-key]
line console 0
login authentication default

Case 2) Tacacs(규칙 이름) + Tacacs+ 조합 (Body 암호화)
aaa new-model // 외부 aaa 인증 장비를 사용합니다.
aaa authentication login Tacacs group tacacs
tacacs-server host [tacacs-server-ip]
tacacs-server key [shared-key]
line console 0
login authentication Tacacs

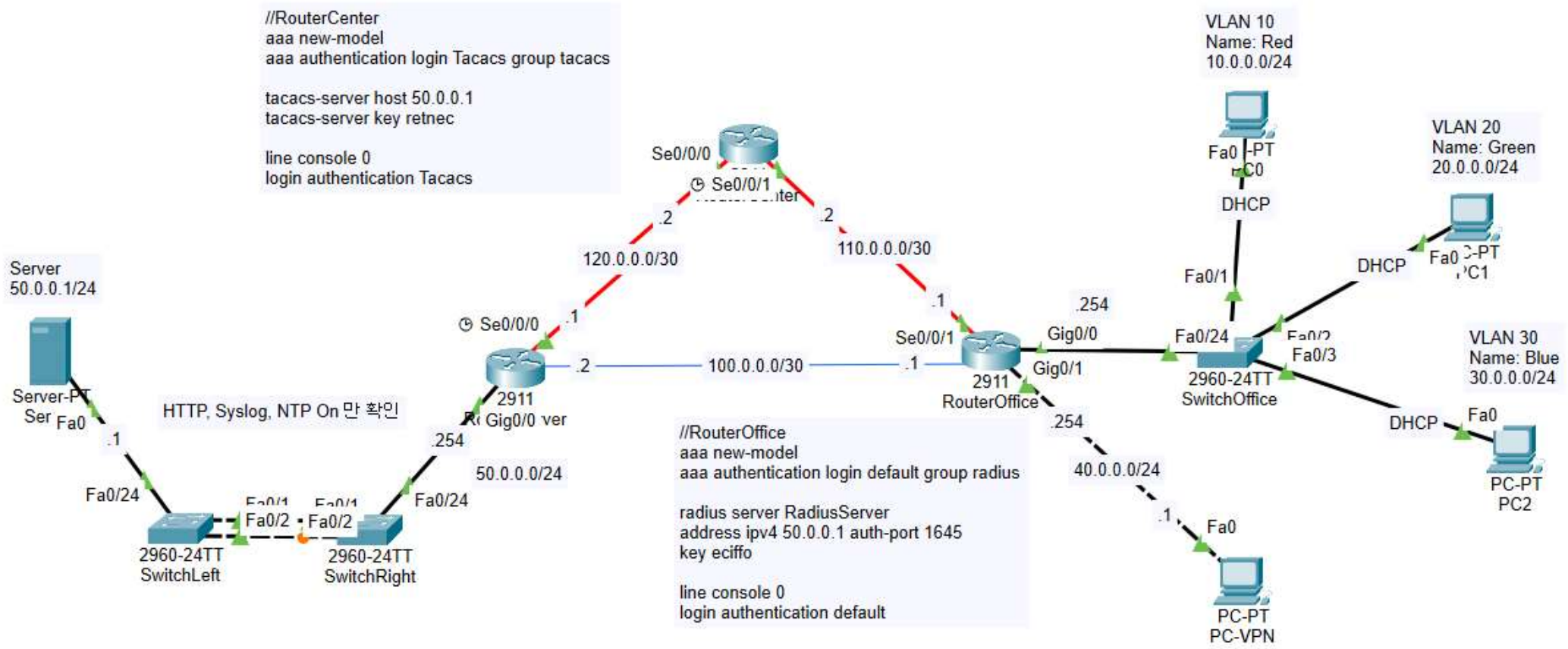


11-4-2. Server Sevices (AAA Practice)

AAA(Authentication, Authorization, Account)

이론

Radius
TACACS+ / Telnet port 적용 / VPN 적용 / Options



11-5-1. Server Sevices + Router (ACL Prepare)

ACL(Access Control List)

구글!

//Numberd
1. Standard ACL
2. Extended ACL
//Namded (규칙 설명)
3. Named Standard/Extended ACL

동작 방식 구분
1. Inbound: Get Packet -> Router -> ACL Filtering // 들어올 때 확인
2. Outbound: Send Packet -> Router -> ACL Filtering // 나갈 때 확인

주의사항: 위에서 부터 아래로 규칙 적용

11-5-2. Server Sevices + Router (ACL Syntax)

// Router(Config)#
1. Standard ACL (1~99)
#access-list [access-list-number] {permit | deny} {[src-net-id] [WM] | any}
// control only src
2. Extended ACL (100~199)
#access-list [access-list-number] {permit | deny} [protocol] [src-net-id] [WM] [dst-net-id] [WM] [port]
// control [src, dst, port]
3. Apply ACL to port
Router(config)# int [interface]
Router(config)# ip access-group [access-list-number] {in|out}

11-5-3. Server Sevices + Router (ACL Example)

// Router(Config)#
1. Standard ACL
#access-list [access-list-number] {permit | deny} {[src-net-id] [WM] | any}
2. Extended ACL
#access-list [access-list-number] {permit | deny} [protocol] [src-net-id] [WM] [dst-net-id] [WM] [port]
3. Apply ACL to port
Router(config)# int [interface]
Router(config)# ip access-group [access-list-number] {in|out}

//Standard ACL
1. 출발지가 192.168.0.0/24인 들어오는 Packet 차단
access-list 1 deny 192.168.0.0 0.0.0.255
access-list 1 permit any

int se0/0/0
ip access-group 1 in

//Standard ACL
2. 출발지가 192.168.0.0/24인 나가는 Packet만 허용
access-list 1 permit 192.168.0.0 0.0.0.255
access-list 1 deny any

int se0/0/0
ip access-group 1 out

//Extended ACL
1. 내부 192.168.0.0/24에서 외부로 나가는 Packet 중, 목적지가 1.1.1.1인 Packet만 허용
access-list 101 permit ip 192.168.0.0 0.0.0.255 host 1.1.1.1
access-list 101 deny any ip any any

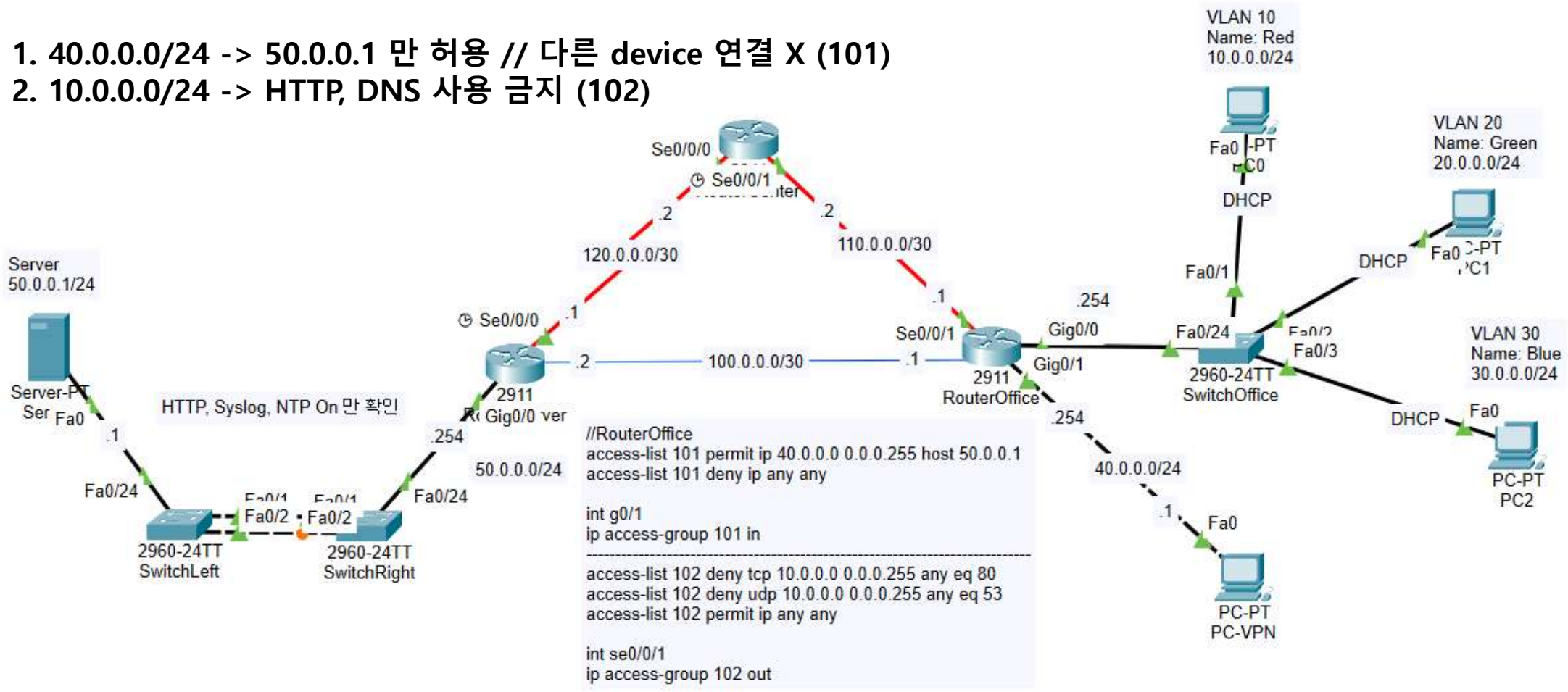
int fa0/0 // serial에 적용한다면?
ip access-group 101 in // out으로 적용한다면?

//Extended ACL
2. 출발지가 192.168.0.0/24인 외부로 통신 (HTTP, DNS) 들어오는 Packet 차단
access-list 101 deny tcp 192.168.0.0 0.0.0.255 any eq 80
access-list 101 deny udp 192.168.0.0 0.0.0.255 any eq 53
access-list 101 permit ip any any

int fa0/0
ip access-group 101 in

11-5-4. Server Sevices + Router (ACL Practice)

1. 40.0.0.0/24 -> 50.0.0.1 만 허용 // 다른 device 연결 X (101)
2. 10.0.0.0/24 -> HTTP, DNS 사용 금지 (102)

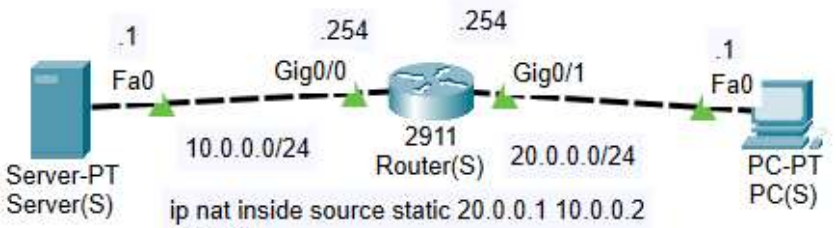



```
//RouterOffice
access-list 101 permit ip 40.0.0.0 0.0.0.255 host 50.0.0.1
access-list 101 deny ip any any

int g0/1
ip access-group 101 in
----------------------------------------------------------------------
access-list 102 deny tcp 10.0.0.0 0.0.0.255 any eq 80
access-list 102 deny udp 10.0.0.0 0.0.0.255 any eq 53
access-list 102 permit ip any any

int se0/0/1
ip access-group 102 out
```

11-6-1. Server Sevices + Router (NAT Syntax)

1. Static NAT(Network Address Translation) // 1:1

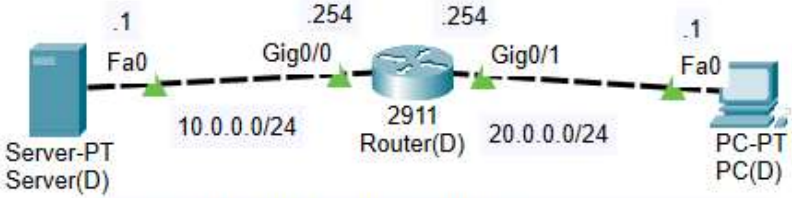
R1(config)# ip nat inside source static [사설 IP] [공인 IP]
R1(config)# int [사설-interface]
R1(config-if)# ip nat inside
R1(config)# int [외부-interface]
R1(config-if)# ip nat outside




```
ip nat inside source static 20.0.0.1 10.0.0.2
int g0/1
ip nat inside
int g0/0
ip nat ouside
```

2. Dynamic NAT // N

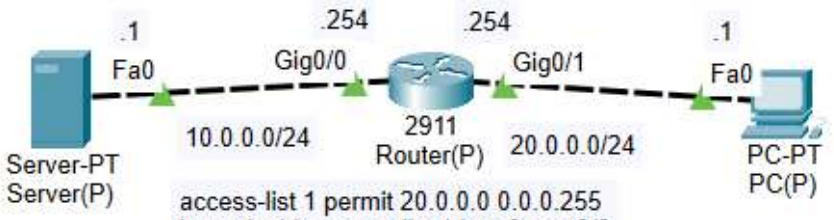
R2(config)# access-list [숫자] permit [사설-net-id] [WM]
R2(config)# ip nat pool [이름] [공인 first ip] [last ip] netmask [SM]
R2(config)# ip nat inside source list [숫자] pool [이름]
R2(config)# int [사설-interface]
R2(config-if)# ip nat inside
R2(config)# int [외부-interface]
R2(config-if)# ip nat outside




```
access list 1 permit 20.0.0.0 0.0.0.255
ip nat pool dynamic 10.0.0.2 10.0.0.10 netmask 255.255.255.0
ip nat inside source list 1 pool dynamic
int g0/1
ip nat inside
int g0/0
ip nat outside
```

3. PAT(Port Address Translation) // interface

R3(config)# access-list [숫자] permit [사설-net-id] [WM]
R3(config)# ip nat inside source list [숫자] interface [interface]
R3(config)# int [사설-interface]
R3(config-if)# ip nat inside
R3(config)# int [외부-interface]
R3(config-if)# ip nat outside



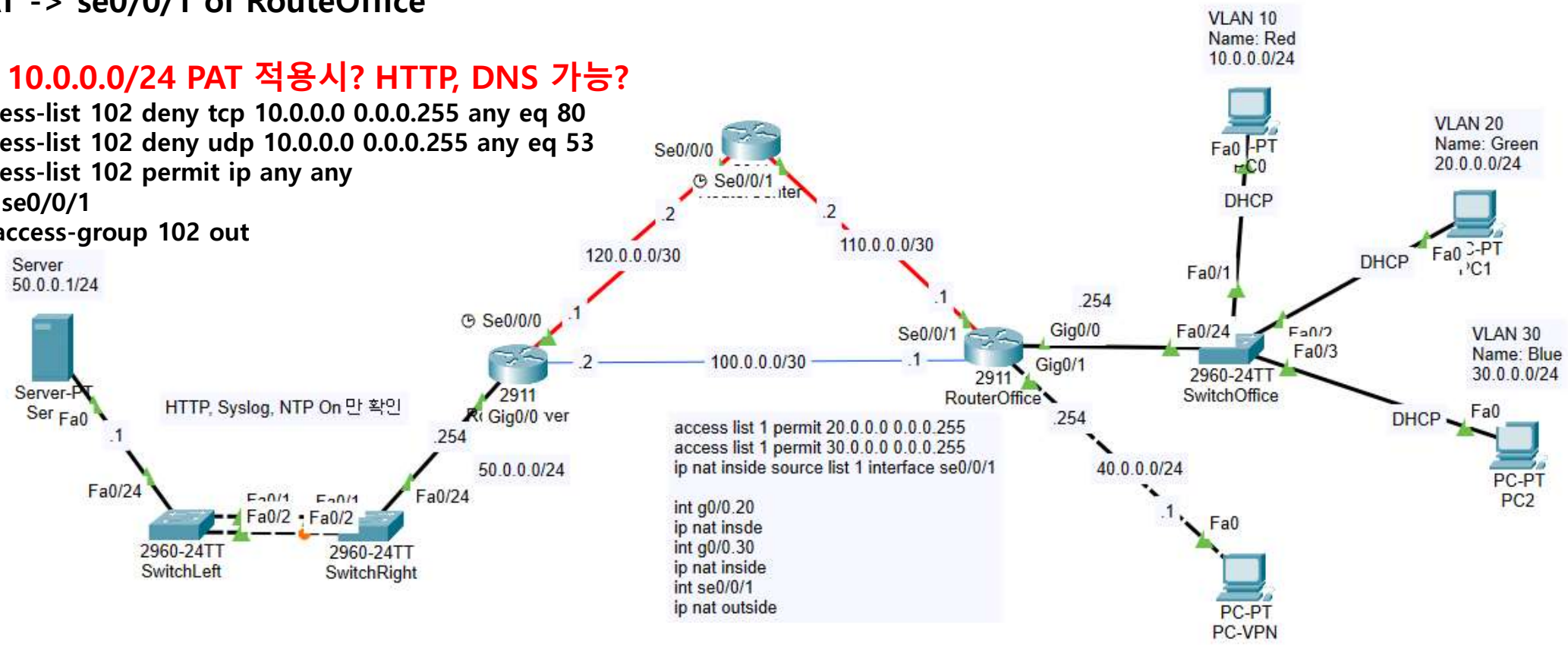

```
access-list 1 permit 20.0.0.0 0.0.0.255
ip nat inside source list 1 interface g0/0
int g0/1
ip nat inside
int g0/0
ip nat outside
```

11-6-2. Server Sevices + Router (NAT Practice)

20.0.0.0/24, 30.0.0.0/24 -> Out bound of RouterOffice
PAT -> se0/0/1 of RouteOffice

if) 10.0.0.0/24 PAT 적용시? HTTP, DNS 가능?

```
access-list 102 deny tcp 10.0.0.0 0.0.0.255 any eq 80
access-list 102 deny udp 10.0.0.0 0.0.0.255 any eq 53
access-list 102 permit ip any any
int se0/0/1
ip access-group 102 out
```



11-7-1. Server Sevices + Router (VPN / GRE Tunnel Syntax)

이웃하지 않은 네트워크를 이웃한 것 처럼 (By. GRE Tunnel Capsulation)

IPSec

//RouterLeft
(config)# interface tunnel 0
(config-if)# ip add 10.0.0.1 255.255.255.252
(config-if)# tunnel mode gre ip
(config-if)# tunnel source [외부로 향하는 Interface]
(config-if)# tunnel destination [받는 라우터 실제 주소]
(config)# ip route [건너편 내부-net-id] [SM] [건너편 Tunnel IP]

//RouterRight
(config)# interface tunnel 0
(config-if)# ip add 10.0.0.2 255.255.255.252
(config-if)# tunnel mode gre ip
(config-if)# tunnel source [외부로 향하는 Interface]
(config-if)# tunnel destination [받는 라우터 실제 주소]
(config)# ip route [건너편 내부-net-id] [SM] [건너편 Tunnel IP]

11-7-2. Server Sevices + Router (VPN / GRE Tunnel Practice)

PC -> Command Prompt -> tracert [IP]

```
C:\>tracert 50.0.0.1

Tracing route to 50.0.0.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      40.0.0.254
  2    17 ms     35 ms     38 ms     100.0.0.2
  3    14 ms     24 ms     15 ms     50.0.0.1
```

```
C:\>tracert 40.0.0.1

Tracing route to 40.0.0.1 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      50.0.0.254
  2    29 ms     2 ms      34 ms     100.0.0.1
  3    50 ms     25 ms     31 ms     40.0.0.1
```