Network 기초

■ Classful Address

Class	첫번째 옥텟의 범위	Network ID의 범위	사용가능한 Network ID의 개수	사용가능한 Host ID의 개수
A Class	1~126	1.0.0.0~126.0.0.0	$2^{(8-1)}-2=126$	$2^{24}-2=16,777,214$
B Class	128~191	128.0.0.0~191.255.0.0	$2^{(16-2)}=16,384$	$2^{16}-2=65,534$
C Class	192~223	192.0.0.0~223.255.255.0	$2^{(24-3)}=2,097,152$	$2^{8}-2=254$

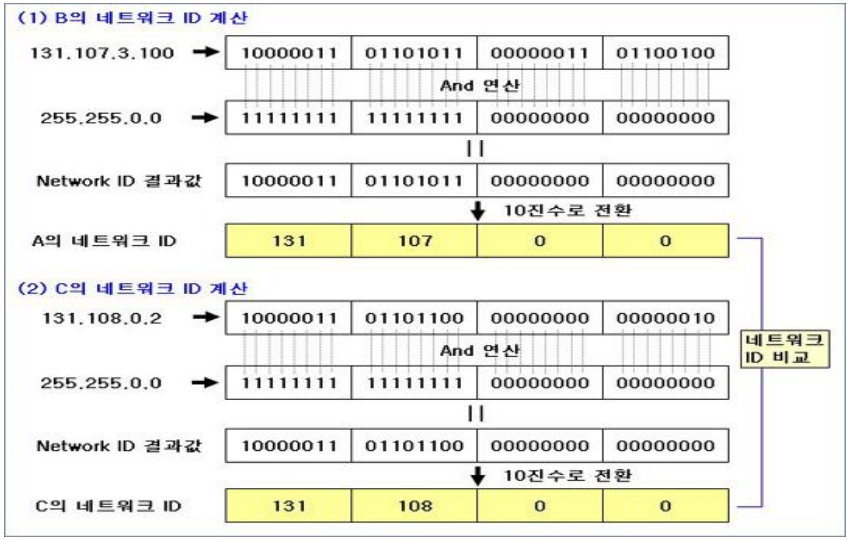
D class (예약된 멀티캐스트 주소) : 224-239
E class (예약된 연구용 주소) : 240-255

RFC 1918은 사설 주소 (사설 네트워크 내에서의 식별용 주소)로 사용하기 위한 세 개의 IP 주소 블럭을 설정해두었다.

- 10.0.0.0 ~ 10.255.255.255 (10/8 prefix)
- 172.16.0.0 ~ 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 ~ 192.168.255.255 (192.168/16 prefix)

- Subnet Mask

상대방 컴퓨터가 로컬인지 원격지인지를 구별



- Default Gateway

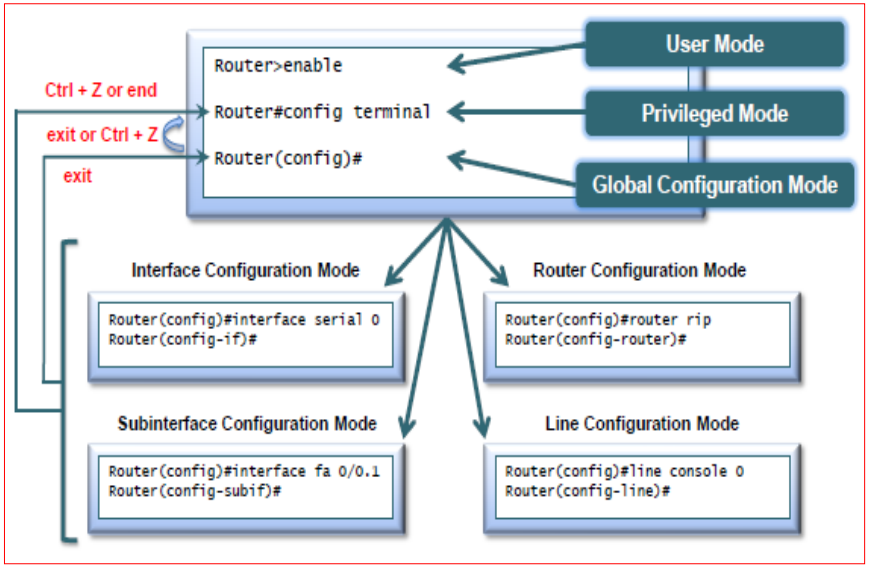
호스트가 TCP/IP통신을 할 때 가장 먼저 목적지 호스트가 자신과 같은 로컬에 있는지 원격지에 있는지를 판단한다고 했다. 이때 원격지에 있는 결과가 나오면 컴퓨터는 Default Gateway를 이용해서 통신을 하게 된다.

Router 기초

■ Router의 모드

```
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

Cisco 2621 (MPC860) processor (revision 0x200) with 253952K/8192K bytes of memor
y
.
Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
4 FastEthernet/IEEE 802.3 interface(s)
4 Low-speed serial(sync/async) network interface(s)
32K bytes of non-volatile configuration memory.
63488K bytes of ATA CompactFlash (Read/Write)


         --- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]:
```

Ctrl + Z



- User Mode (>)

. 테스트를 목적(ping이나 traceroute)으로 사용되며, 현재 상태만 확인해 볼 수 있다.
. show ?

- Priviledge Mode (#)

. 유저 모드에서 enable 명령어를 통해 전환되는 모드

. 운영자 모드로서 라우터의 모든 명령어가 가능하다.(라우터의 구성확인 및 변경 가능)

- Global Configure Mode ((config)#)

. Priviledge Mode에서 config terminal 명령어를 통해 전환되는 모드

. 라우터의 구성 파일을 변경하는 경우에 사용하는 모드

. 보통 config모드라고 하며 프리빌리지 모드를 통해서만 들어갈 수 있음

- Setup Mode(: 또는 ?)

. Configuration File이 없는 경우, 자동으로 나타나 Interactive한 라우터 설정이 가능하다

. 보통 라우터를 처음 동작시킬 때 라우터의 구성파일이 없기 때문에 라우터가 부팅하면서 자동으로 들어가는 모드(★)

. 라우터가 구성에 관계된 질문을 하나씩 던지고 사용자는 이 질문에 대답하면서 구성파일을 설정한다.

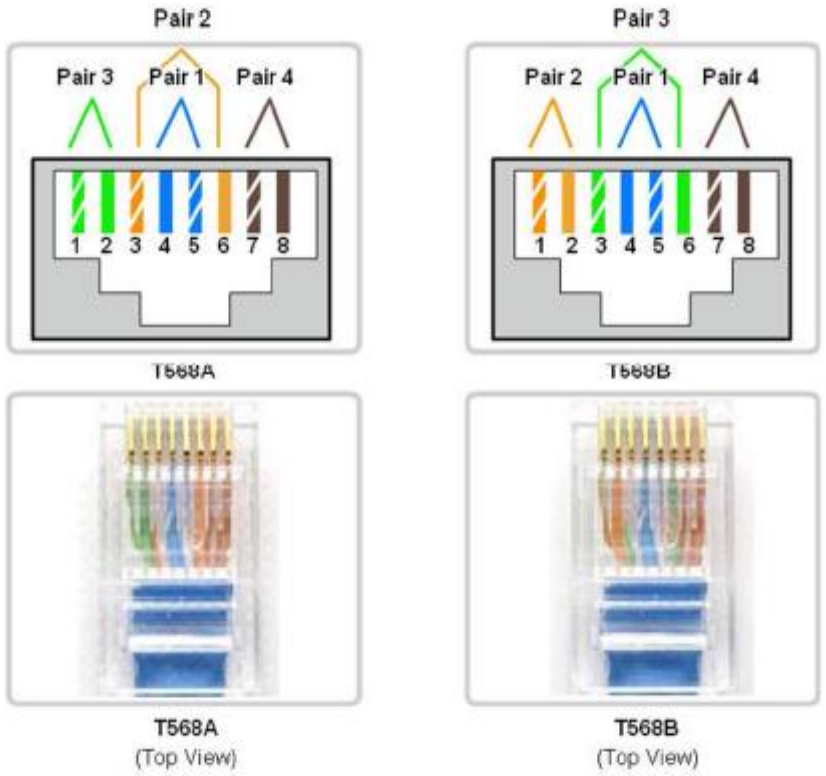
Cable

■ Ethernet Connectors

Pin Number	Signal
1	TD+ (Transmit Data, positive-going differential signal)
2	TD- (Transmit Data, negative-going differential signal)
3	RD+ (Receive Data, positive-going differential signal)
4	Unused
5	Unused
6	RD- (Receive Data, negative-going differential signal)
7	Unused
8	Unused

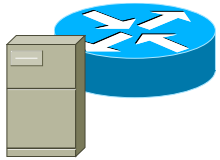
■ LAN 연결의 종류

황띠	황	초 띠	파	파 띠	초	갈 띠	갈
1	2	3	4	5	6	7	8



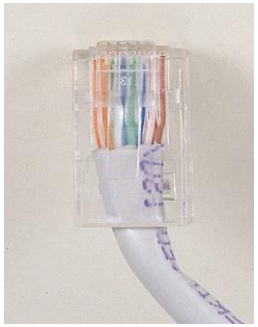
■ Straight-Through Cable (Direct)

Hub/Switch

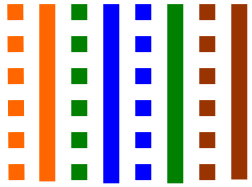


Server/Router

Pin	Label		Pin	Label
1	RD +	←	1	
2	RD -	←	2	
3	TD +	→	3	
4	NC		4	
5	NC		5	
6	TD -	→	6	
7	NC		7	
8	NC		8	



1 8



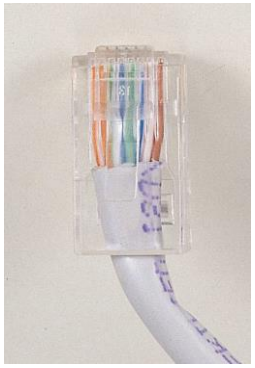
Pin	Color	Function	Pin	Color	Function
1	White/Green	TX+	1	White/Green	TX+
2	Green	TX-	2	Green	TX-
3	White/Orange	RX+	3	White/Orange	RX+
6	Orange	RX-	6	Orange	RX-

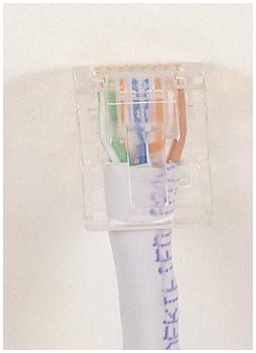
■ Crossover Cable

Hub/Switch

Hub/Switch

Pin	Label	Pin	Label
1	RD +	1	RD +
2	RD -	2	RD -
3	TD +	3	TD +
4	NC	4	NC
5	NC	5	NC
6	TD -	6	TD -
7	NC	7	NC
8	NC	8	NC

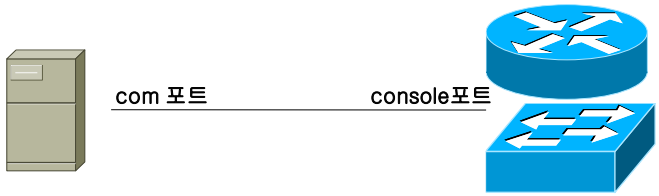




1→3, 2→6 케이블을 크로스 시킨다.

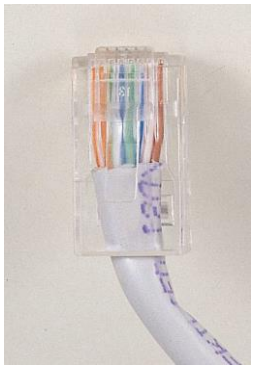
Pin	Color	Function	Pin	Color	Function
1	White/Green	TX+	3	White/Green	RX+
2	Green	TX-	6	Green	RX-
3	White/Orange	RX+	1	White/Orange	TX+
6	Orange	RX-	2	Orange	TX-

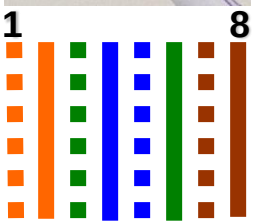
■ Rollover Cable(console)

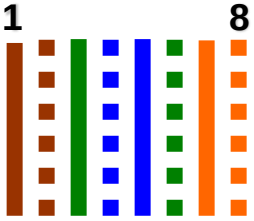


pc Hub/Switch

Pin	Label	Pin	Label
1	RD +	8	NC
2	RD -	7	NC
3	TD +	6	TD -
4	NC	5	NC
5	NC	4	NC
6	TD -	3	TD +
7	NC	2	RD -
8	NC	1	RD +







■ Serial Cable

DCE가 클럭신호를 보내는 쪽, DTE가 클럭신호를 받는 쪽 이다.

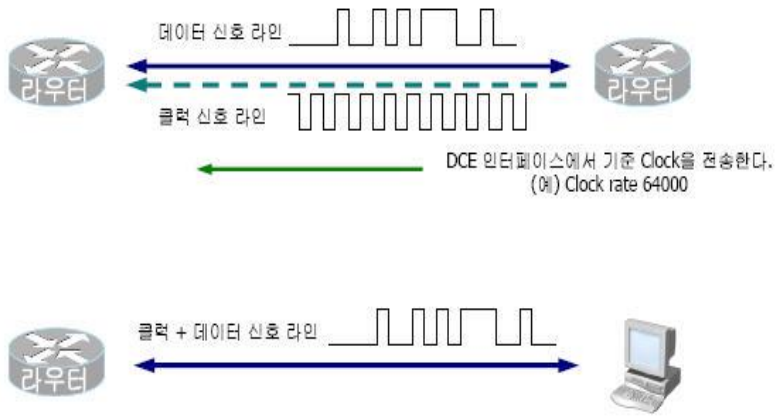
- Clock Rate 설정 이유

. 라우터에서 Clock Rate를 설정하는 이유는 위의 사진처럼 라우터끼리 Back-to-Back 구성 할 경우 Clock을 잡아주는 CSU/DSU가 없기 때문에 라우터 장비 둘 중 한쪽을 DCE로 설정하고 Clock 값을 지정해 주어야 한다.

. Clock Rate를 지정해주는 이유는 시리얼 인터페이스가 통신 시 어느 한쪽에서 "**통신 규격 속도를 지정**" 해주어야 하기 때문이다.

. DCE쪽에서 Clock을 잡아주면 DCE 인터페이스는 DTE인터페이스로의 **속도 동기화**가 이루어지는 것이다.

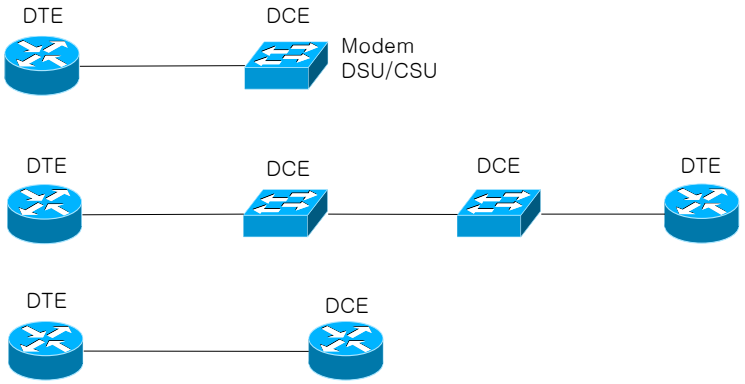
- Clock 신호 동기 방법



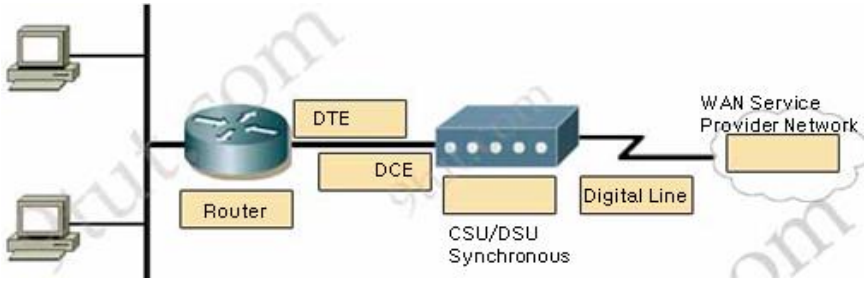
▶ DTE 와 DCE

Router# show controllers serial 0/0
장치의 케이블이 어떻게 연결되어 있는지, 케이블의 종류는 무엇인지 알 수 있다.

Router(config)#interface serial 0/0
Router(config-if)#clock rate 64000
DTE와 DCE 중 DCE의 클럭을 설정, 64k로 동작을 하게 만듬



<그림>



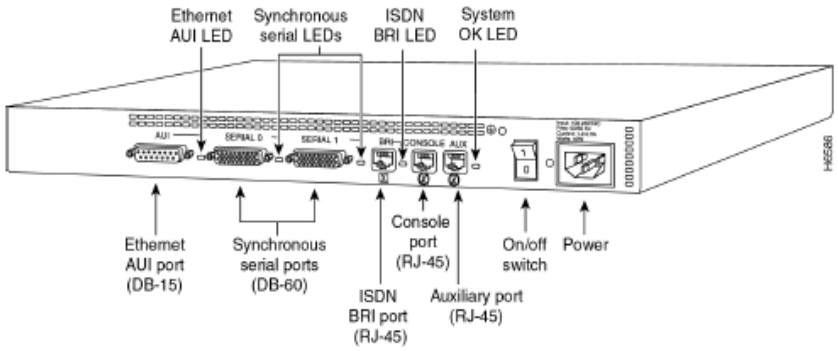
■ Router Interface Type

- Cisco 2500 Series

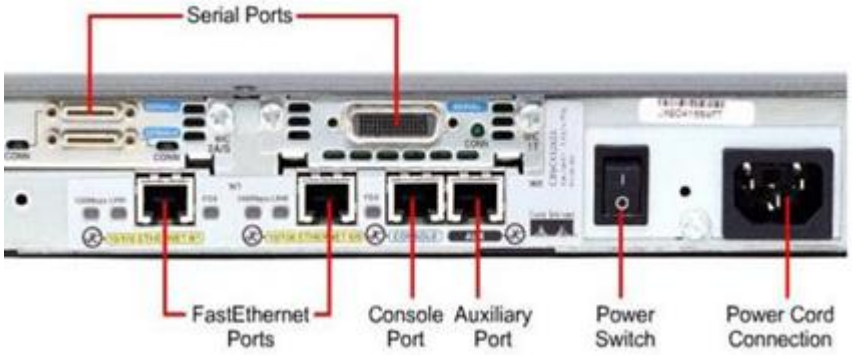
Cisco 라우터 2500series 장비 이다.
2500시리즈는 픽스형 인터페이스를 갖는데 이 픽스형이란, 고정형이라는 뜻이다. 즉 인터페이스 확장이 불가능하다.

2500시리즈 장비는 현장에선 쓸순 있지만 오래되었고 위에 언급한것과 같이 불편한점이 있다.

그래서 일반적으로 2600시리즈 장비를 많이 사용하고 있는추세이다.

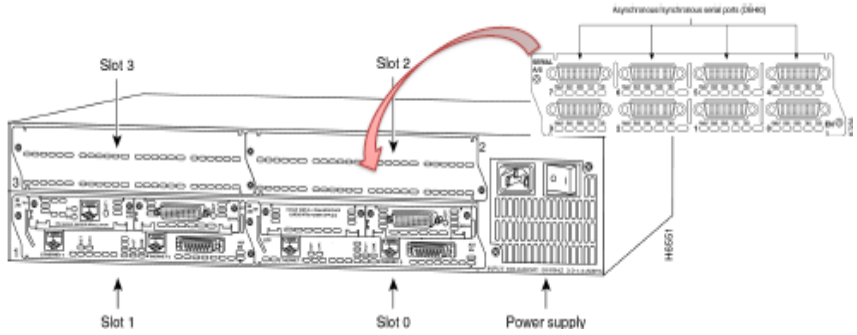


- Cisco 라우터 2600 Series

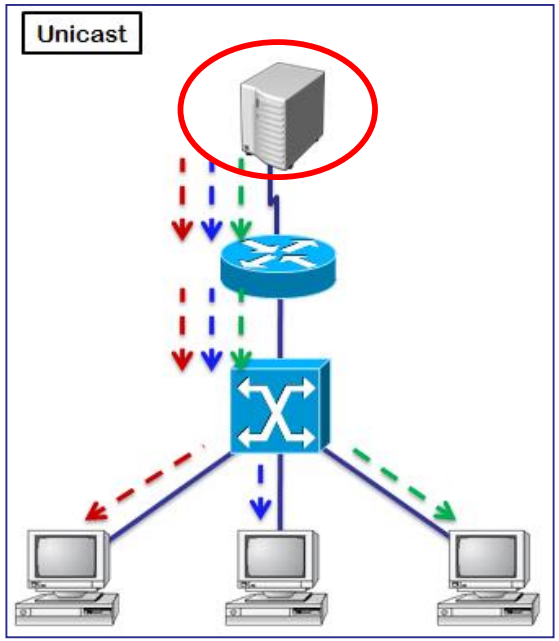


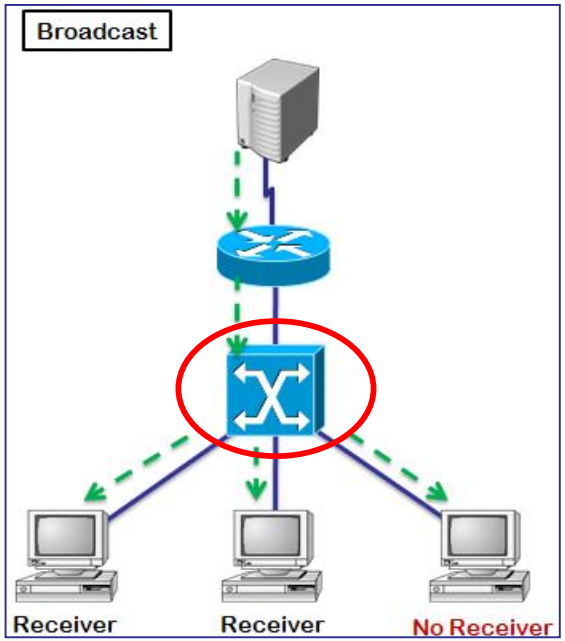
- Modular Interface (Cisco 3725)

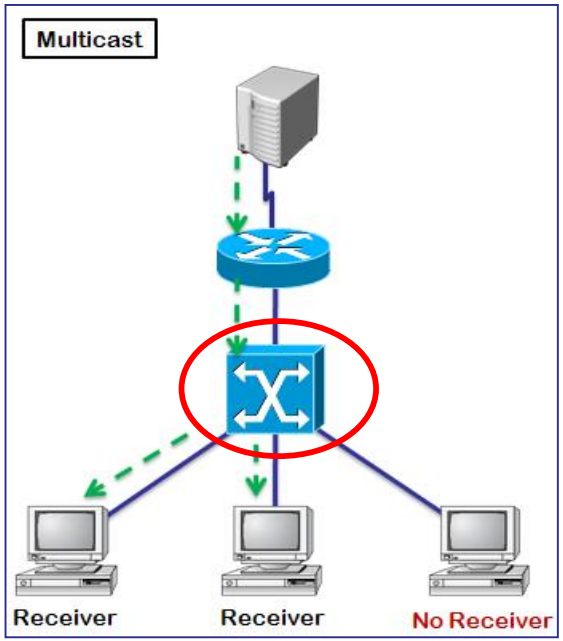
시리얼을 부를때 오른쪽에서 왼쪽으로 아래에서 위의 순서로 번호를 매긴다.(★)
S0/0 S0/1 S0/2 , S1/0 S1/1 S1/2



IPv4 통신 방법







. 하나의 트래픽을 발송 하더라도 다수의 Host에게 전달한다면 그 트래픽을 Host 수 만큼 복사하여 각 Host에게 전달한다.
신뢰성 있게 전송을 할 수 있으나 트래픽의 수 증가로 회선에 많은 부담을 갖는다. 다수의 Host에게 데이터 전달에 문제가 있다.

. 하나의 트래픽이 다수의 Host에게 발송할 때 하나의 트래픽으로 보낸다. 그리하여 회선의 부담을 주지 않는다. 그러나 네트워크 영역에서 다수의 Host들은 원하든 안원하든 모두 다 트래픽을 전달 받게 된다. No Receiver 입장에서는 그 트래픽이 불필요할 것이다.

. 원하는 Host에게만 데이터를 보내는 Unicast의 장점과 트래픽을 하나로 보내는 Broadcast 장점을 결합한 방식이 Multicast이다.

▶ Interface 상태보기

show interfaces
show interface serial 0/0
show ip int brief (★)

정상적 운영	serial 0/0 is up, line protocol is up
연결 문제 (data link 층 문제)	serial 0/0 is up, line protocol is down . clock rate 64000 생략한 경우(DCE) . encapsulation 다른 경우 (PPP, HDLC, Frame-relay) . no keepalive message are received
인터페이스 문제 (physical 층 문제)	serial 0/0 is down, line protocol is down . 잘못된 인터페이스 문제
비 사용 (관리자 shutdown)	serial 0/0 is administratively down, line protocol is down

▶ 패스워드 설정

- Console 패스워드 구성

line console 0
login
[no] password cisco

- Telnet 패스워드 구성

line vty 0 4
login
[no] password cisco

line vty 0 4
no login

- Enable 패스워드 구성

enable password cisco

enable Secret bsit

- 사용자 계정 구성

username admin password cisco

line vty 0 4
login local

line console 0
login local

- 패스워드 암호화

service password-encryption

Routing 개념

■ 라우터의 기능

라우터의 기능	설명
경로 결정 (Path Determination)	데이터 패킷이 출발지부터 목적지까지 갈 수 있는 경로를 검사하고 어떤 경로로 가는 것이 최선인지 결정
스위칭 (Switching)	경로 설정이 결정될 경우 데이터 패킷 스위칭 작업을 함

. 관리자에 의해 라우팅 프로토콜을 정의하고, 그 라우팅 알고리즘을 통해 경로설정과 스위칭을 한다

. 라우팅 알고리즘은 라우팅 테이블을 만들어 장치의 포트(인터페이스)별로 어디로 가야할지 지정을 한다

. 라우팅 구성은 라우터의 콘솔 포트를 사용하여 케이블을 연결한 후 설정한다.

▶ 라우팅(Routing)

. Routing은 한 네트워크에서 다른 네트워크로 패킷을 이동시키는 과정과 네트워크 안의 호스트에게 패킷들을 전달하는 과정을 의미함

. 라우팅의 종류로는 정적 라우팅(Static Routing), 디폴트 라우팅(Default Rouing), 동적 라우팅(Dynamic Routing)이 있다

▶ 라우티드 프로토콜(Routed Protocol)

. 수동의 의미로서 즉 라우팅 당하는 프로토콜, 라우터에 의해 라우팅을 당함

. 흔히 비유하는 택시(라우터)의 택시기사(라우팅 프로토콜)에 의해 운반되는 고객(라우티드 프로토콜)

. 위의 것을 실제적으로 말하자면 라우터 장치의 라우팅 프로토콜에 의해 어떻게 전송될지 결정하고 라우티드 프로토콜이 전송되는 것

▶ 라우팅 프로토콜(Routing Protocol)

. 능동의 의미로서 즉 라우팅 하는 프로토콜, 라우팅 알고리즘이라고도 함

. 어디로 전송해야할지에 대한 경로 정보를 가지고 있는 라우팅 테이블을 기억해둠

※ 라우팅 프로토콜과 라우티드 프로토콜의 종류

라우팅 프로토콜	RIP(Version1, Version2), IGRP, OSPF, EIGRP
라우티드 프로토콜	TCP/IP, IPX, Apple Talk

State Route

■ Static Routing 구성

. 네트워크 관리자가 수동으로 직접 목적지 별로 지정해 주는 경로를 의미

. 스태틱 라우팅 프로토콜은 외부 네트워크와 연결되는 경로가 하나뿐인 스텁(Stub) 네트워크에서 많이 사용한다

장점	.운영자가 경로로 직접 입력하기 때문에 라우터는 머리를 쓰지않아 CPU상에 부담이 없다 . 라우팅 테이블을 교환 및 업데이트 안하기 때문에 라우터들 간에 대역폭을 낭비하는 일이 없다 . 보안성이 있다
단점	. 라우터가 어떻게 연결되어 있는지를 알아야 한다. . 한 네트워크에 회선이 추가될 경우 추가된 경로를 설정해야 한다 . 동적 라우팅과는 달리 회선에 문제가 생겨도 다른길을 동적으로 찾지못하고 계속 불능이 된다.

▶ Static Route 설정하기

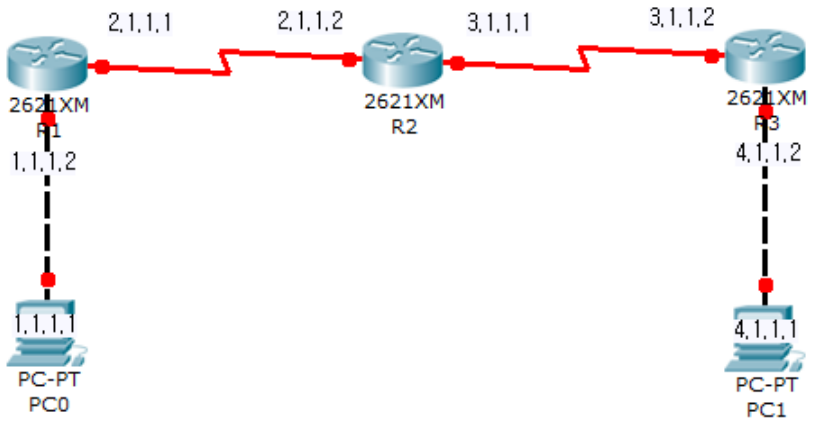
Router#(config) ip route
[destination_network] [subnet_mask] [next_hop_address] [distance]
① ② ③ ④

① 목적지 네트워크를 지정한다 (네트워크 주소임에 주의한다) - 가고 싶은곳의 주소

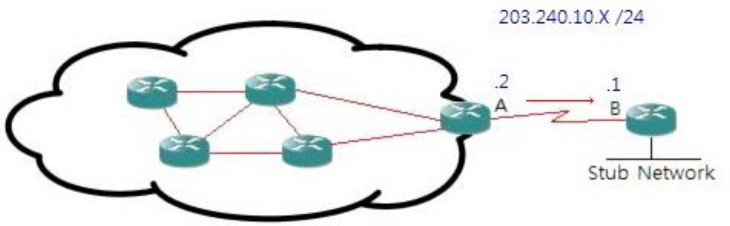
② 목적지 네트워크의 서브넷 마스크 지정 - 서브넷 마스크의 주소

③ 목적지 네트워크로 가기 위한 넥스트 홉 어드레스 지정 - 통해 갈곳의 주소
(넥스트 홉의 경우 1홉을 건너뛴 홉, 즉 자신의 건너편 라우터라고 생각하면 된다. 인터페이스를 쓸 경우 자신의 인터페이스를 적는다.)

④ 라우팅 정보의 가치로서 커지면 커질수록 가치가 떨어지게 되며, 명시하지 않아도 된다. (디폴트 값은 1이다)



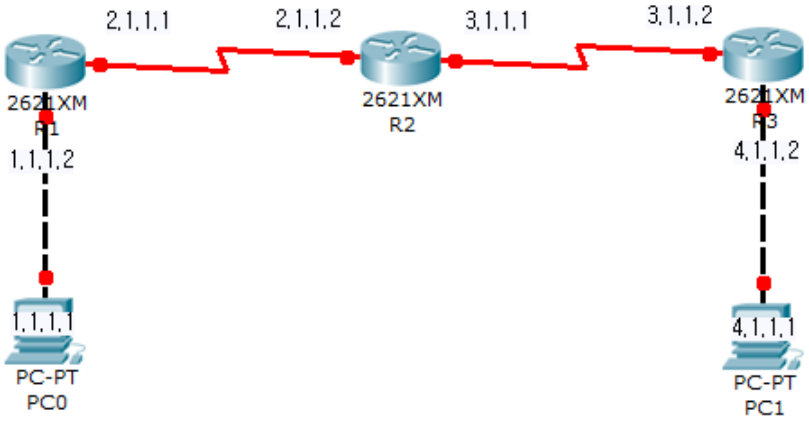
▶ Default Route



ip route 0.0.0.0 0.0.0.0 203.240.10.1

디폴트 네트워크 디폴트로 보낼 패킷 주소

ip default-network [classful ip]
- rip의 경우 자동으로 전달된다. (입력된 네트워크 주소가 아닌 0.0.0.0/0)
- IGRP, EIGRP도 자동으로 전달된다.(입력된 네트워크 주소로)



■ 라우팅 프로토콜 분류

◇ 다른 라우터에게 보내는 Routing Update의 내용에 따라 Distance Vector 및 Link State 라우팅 프로토콜로 분류

▷Distance Vector Routing Protocol (RIP, EIGRP, BGP)

전체 네트워크 토폴로지를 알지 못하며, 다만 "어떤 라우터를 통하면 목적지 네트워크까지의 Metric이 얼마이다." 라는 것만 알고 있다.

-Routing Update 전송시 포함되는 정보
(목적지 네트워크 + 목적지 네트워크의 Metric 값)
- Auto Summary
- Split Horizon

▷Link State Routing Protocol (OSPF)

전체 네트워크 구성도를 그리기 위한 모든 정보를 알려주며, 전체 네트워크의 토폴로지를 알며 각 라우터의 입장에서 목적지 네트워크까지의 최적경로를 계산한다. OSPF는 동일 Area 내에서는 인접 라우터에서 수신한 Routing-Update를 그대로 다른 라우터에게 전송한다.

◇ Routing Update에 서브넷 마스크 정보 포함 여부에 따라 Classful 및 Classless 라우팅 프로토콜로 분류

▷Classful Routing Protocol (RIPv1, IGRP) :
Routing Update 전송시 포함되는 정보 (Subnet Mask 정보가 없음)

▷Classless Routing Protocol (RIPv2, EIGRP, OSPF, BGP) :
Routing Update 전송시 포함되는 정보 (Subnet Mask 정보도 같이 전송)

◇ 동일한 조직(AS : Autonomous System) 내부 또는 서로 다른 조직간의 사용 여부에 따른 분류

▷ Interior Gateway Protocol (IGP) :
동일 AS 내부에서 사용되는 프로토콜 (RIP, EIGRP, OSPF, IS-IS)

▷ Exterior Gateway Protocol(EGP) :
다른 AS 간에 사용되는 프로토콜 (BGP)

■ 경로 결정 방법

1. 동일 라우팅 프로토콜내에서 특정 목적지로 가는 경로가 복수개 있을 때 메트릭 값이 가장 낮은 것이 선택된다.

2. 복수개의 라우팅 프로토콜들이 계산한 특정 네트워크가 라우팅 테이블에 저장될 때는 AD(Administrative Distance)값이 가장 낮은 것이 선택된다.

3. 일단 라우팅 테이블에 저장된 다음에는 패킷의 목적지 주소 와 라우팅 테이블에 있는 네트워크 주소가 가장 길게 일치되는 경로를 선택한다.
이것을 longest match rule 이라 한다.

<예 > longest match rule

show ip route (★)

s 1.0.0.0/8 s0/0
s 1.1.0.0/16 s0/1
s 1.1.1.0/24 s0/2

※ ip classless

. 어떤 major network 의 subnet으로 향하는 패킷을 수신한 경우 정확히 일치하는 route가 라우팅 테이블에 없을 때, 라우터는 이 패킷을 Default Route 로 보낸다.

. 반대로 정확히 일치하는 route가 라우팅 테이블에 없는 subnet을 향하는 패킷을 막기 위해서는 no ip classless 설정을 한다.

▶ 메트릭(Metric)

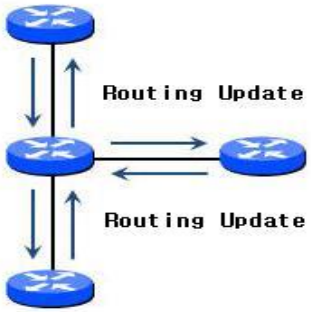
. 라우터는 작은 메트릭 값을 우선시 한다.

▶ AD(Administrative Distance)값

Route Source	Default Distance
Connected Interface	0
Static	1
EIGRP Summary Route	5
eBGP	20
EIGRP (Internal)	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP (External)	170
iBGP	200
Unknown	255

RIP

■ RIP (Routing Infomation Protocol)



. 다이나믹 라우팅 프로토콜로서 관리자가 일일이 경로를 지정하지 않아도 길을 찾아가는 프로토콜이다.

. AS내부를 구성하는 내부용 라우팅 프로토콜(IGP : Interior Gateway Protocol)이다.

. 디스턴스 벡터(Distance Vector) 라우팅 프로토콜로서 거리(홉)와 방향으로 길을 찾아가는 프로토콜이다.

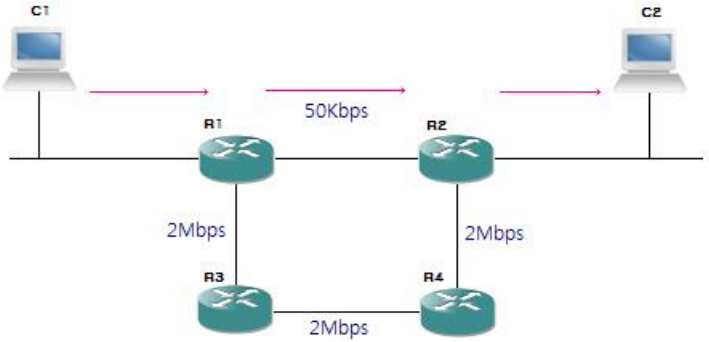
. RIP 라우팅 프로토콜에서 경로 설정 기준은 홉(Hop)카운트로서 최대 15개 까지 허용한다.

. 홉이 16이상이면 네트워크를 찾지 못하므로 데이터를 보내지 못하기 때문에 대규모 네트워크에서는 사용하는데 무리가 있다.

. 디폴트 라우팅 업데이트 주기는 30초이며 이를 통해 경로 이상이나 새로 생긴 경로등을 갱신한다.

. 디폴트 4부터 지정6까지 로드 밸런싱이 가능하다.
(경로가 4개 있을 경우 패킷을 4곳으로 나누어 보낼 수 있다.)

▶ RIP의 단점 : 홉(Hop)카운트 이용



▶ RIPv1 and RIPv2 비교

RIP v1	RIP v2
Classful routing protocol	Classless routing protocol
VLSM 지원 안함	VLSM 지원
No authentication support	Plain text or MD5 인증 지원
Broadcasts를 사용하여 광고	Multicasts를 사용하여 광고
자동 축약됨 (★) (불활성화 X, 수동 축약 X)	자동 축약됨(★) (불활성화 0, 수동 축약 0)

▶ RIP 구문

router rip
 network Classfull Network 주소
 version 2

▶ Loopback Interface

. 이는 가상의 인터페이스로 절대 down되지 않는다.

. 연결상태를 확인하기 매우 편하다.

interface loopback 0
  ip address x.x.x.x x.x.x.x

no interface loopback 0

▶ Passive Interface

. 불필요한 라우팅 정보를 보내지 않을 때 사용한다.

. f0/0에 패스브 인터페이스를 적용하여 RIP 라우팅 전파를 보내지 않음

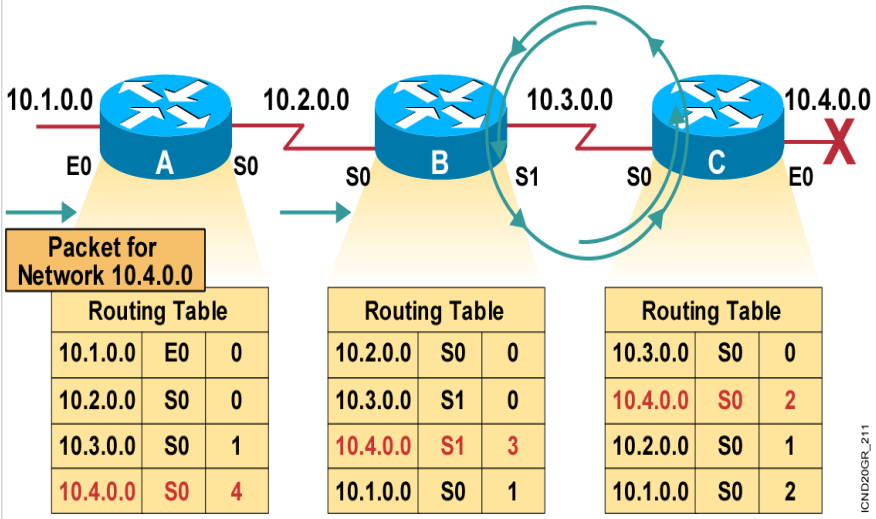
router rip
 version 2
 passive-interface f0/0

▶ Auto-summmary (RIP, IGRP, EIGRP)

Auto Summary 란 라우팅 정보에 포함된 네트워크 와
라우팅정보가 전송되는 인터페이스의 주 네트워크가 다른 지점에서 자동 축약이
일어나는 것이다.

router rip
 network Classfull Network 주소
 no auto-summary

▶ 디스턴스 벡터 (Distance Vector) 라우팅의 문제점



. RIP은 30초마다 새로운 정보를 갱신한다.

. 그런데 장애정보를 가지고 있는 라우터(C 라우터)보다 옆의 라우터(B라우터)가 갱신주기가 먼저 온다면, C라우터는 B라우터의 갱신정보를 보고 장애정보에 대해서 삭제하지 않고 홉카운트를 늘려서 갱신하게 된다.

. 또 C라우터가 B라우터에게 장애 네트워크의 정보를 갱신해주므로 장애 정보가 갱신되지 않는 문제로 인하여 무한 루프에 빠지게 된다.

▶ Looping 방지하기 위한 해결책

아래 루핑방지 기술들을 복합적으로 사용되는 경우가 많다.

. Maximum Hop Count를 15로 설정

15이상은 네트워크로 간주하지 않는다는 특징을 이용한 것으로 대규모 16홉이상의 네크워크에서는 적용이 힘들다

. Hold Down Timer

. Split Horizon(★)

. Route Poisoning

. Poison Reverse

. Triggered Update

해결책 1. Maximum Hop Count를 15로 설정

Network	Next Hop	Hop Count
A	R2	3
B	R2	2
C	--	1
D	--	1
E	R4	2

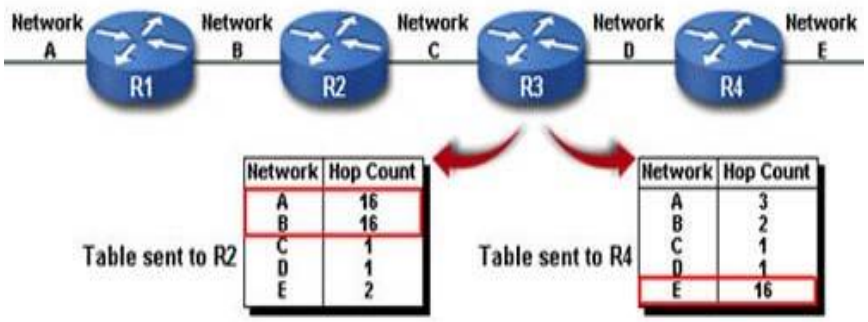


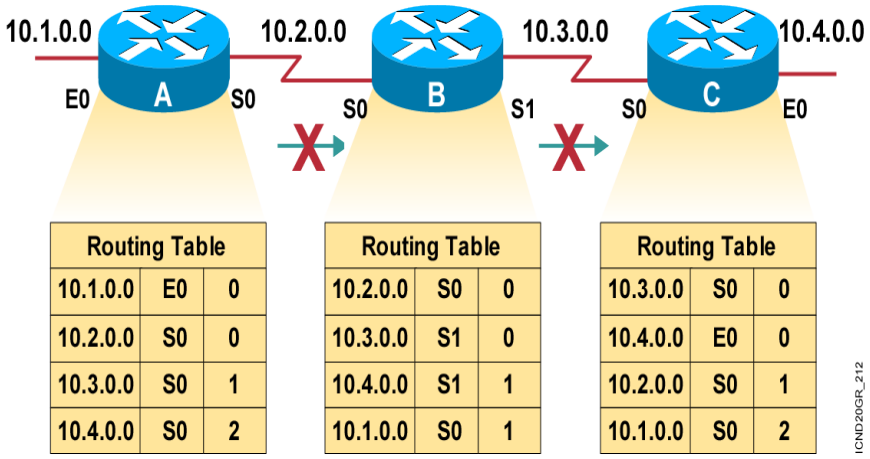
Table sent to R2

Network	Hop Count
A	16
B	16
C	1
D	1
E	2

Table sent to R4

Network	Hop Count
A	3
B	2
C	1
D	1
E	16

해결책 2. Split Horizon



Routing Table		
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

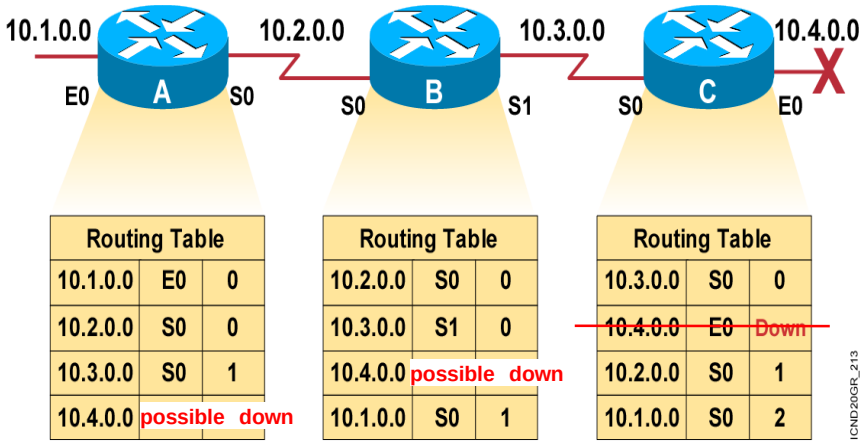
Routing Table		
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

. Network 정보를 받은 곳으로 그 Network 에 대한 라우팅 업데이트를 하지 않음
(즉 자신이 보낸 정보는 다시 되돌려 받지 않음)

(config-if)# no ip split-horizon

해결책 3. Route Poisoning

★ 장애가 발생되면 홉카운트를 16으로 해서 전송한다.



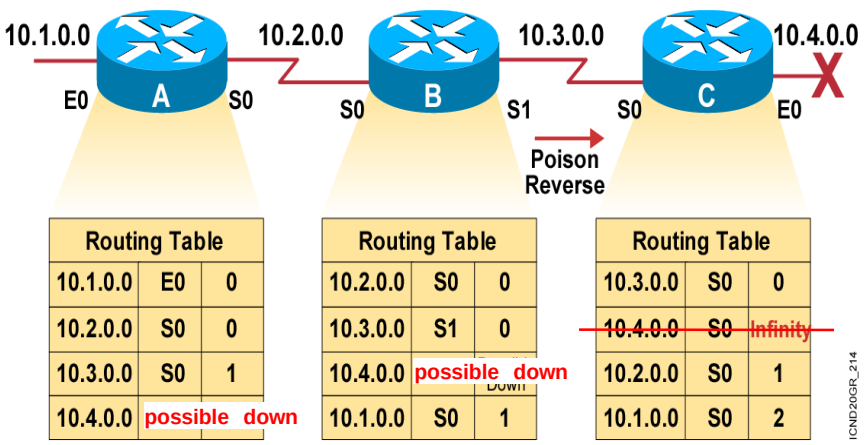
. Router C는 10.4.0.0에 대한 네트워크를 unreachable 이 라고 미리 설정하지만 이웃한 라우터인 Router A,B는 계속적으로 이 경로에 대한 라우팅 업데이트를 수행한다.

하지만 Router C는 문제가 생긴 경로를 미리 Unreachable이라고 지정했기 때문에 Router B에서 이 경로에 대한 업데이트가 들어 오더라도 무시한다.

. 다운 된 네트워크 값이 들어오면 메트릭 값을 16으로 바꾼다.
16으로 바꾸고 나서 다른 라우터에서 다운 된 네트워크 정보가 와도 무시한다.

해결책 4. Poison Reverse

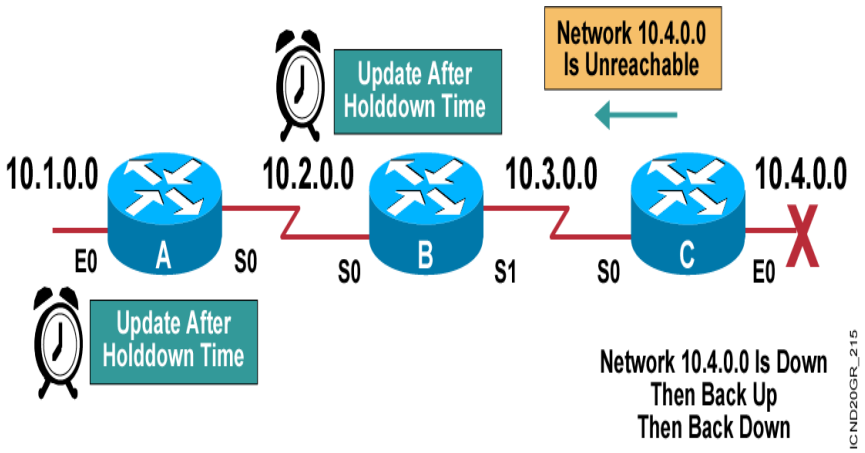
★ 16홉의 라우팅 값을 받으면 역으로 C 라우터가 고장났다고 알려주는 기능



. Router B 가 10.4.0.0의 경로가 inaccessible하다는 것을 라우터 C로부터 받았기 때문에 Router C에게 이에 대한 응답으로 Poison Reverse란 라우팅 업데이트를 Router C로 보낸다.

. Sprit Horizon 보다 우선순위가 높기 때문에 업데이트 정보가 Router C로 전달될 수 있다.(★)

해결책 5. Holddown Timers



. Router가 특정 Link의 Fail 을 전달 받은 후에 해당 경로를 Routing Table 에서 바로 제거하지 않고 특정 시간동안 그정보의 사실을 확인하기 위해 기다린다.
이는 Topology의 변화 정보를 검증하는 용도이다.

. 장애 네트워크가 연결이 됐다 안됐다 할때 그 장애의 계속되는 업데이트 정보로 인해 네트워크가 마비되는것을 방지한다.

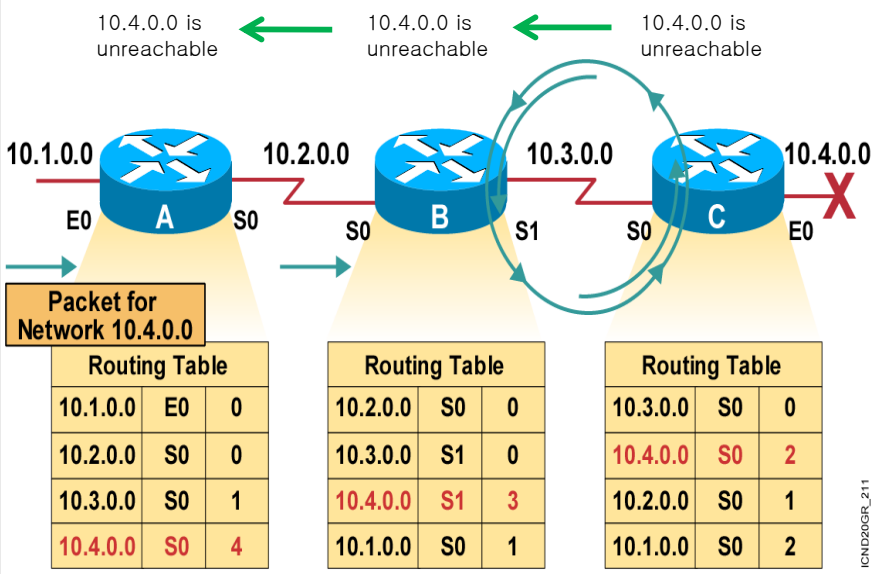
※ 라우팅 테이블 업데이트 하는 경우

1. Hold-down timers가 종료될 때

2. 좀 더 나은 metric 값을 가진 update가 수신될 때

3. 라우팅 테이블을 갱신시키는 Flush timers가 도달하여 라우팅 테이블에서 10.4.0.0 경로를 제거할때

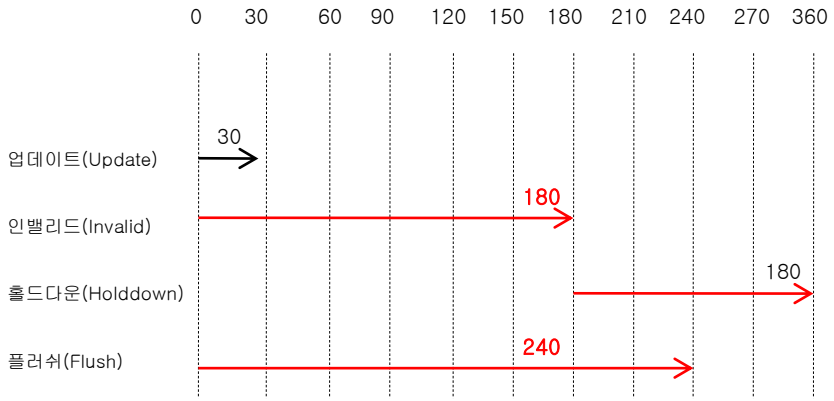
해결책 6. Triggered Update



.Topology의 변화를 즉시 이웃한 Router에게 알려준다.

. 계속되는 업데이트정보로 네트워크 마비의 문제점이 있음.

▶ 토폴로지 변화에 대한 RIP 동작



. Update

기본 값은 30초이다.
라우팅 정보를 받으면 업데이트 타이머는 항상 다시 0으로 리셋 된다.

. Invalid

기본값은 업데이트 타이머의 6배인 180초 이다.
인밸리드 타이머가 만료될 때까지 라우팅 정보를 받지 못하면 라우터는 홀드다운 상태로 들어간다.

. Holddown

기본값은 180초이다.
라우팅 루프가 발생하는 것을 방지하기 위하여 특정 기간동안 다른 라우터가 전송하는 라우팅 정보를 받아들이지 않는 것을 말한다.

그러나, 홀드다운 상태의 네트워크가 다시 살아나거나 대체 경로에 대한 광고를 받아도 이를 무시하고 홀드다운 상태가 계속된다.

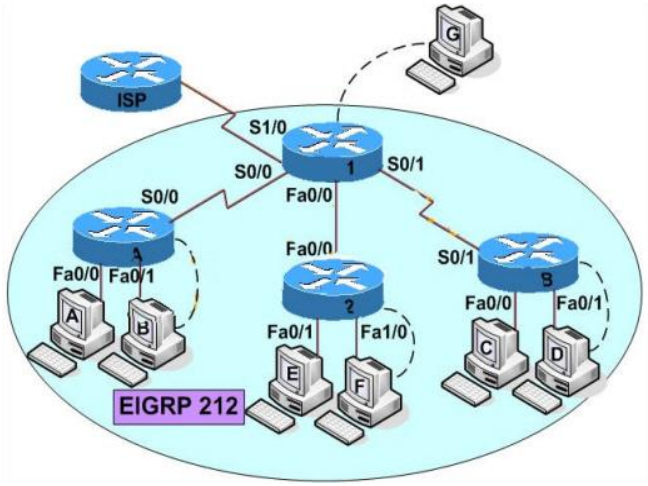
홀드다운 상태는 홀드다운타이머 자체가 만료되거나 플러시 타이머가 만료되어야 끝난다.

. Flush

기본값은 240초 이다.
플러시 타이머가 만료되면 홀드다운 상태에 있는 네트워크는 모두 라우팅 테이블에서 지워진다.

EIGRP

■ EIGRP (Enhanced Interior Gateway Routing Protocol)



- Cisco 사에서 만든 전용 프로토콜이므로 일반적으로 많이 사용하지는 않음

- IGP(Interior Gateway Protocol)중 하나이다.

- Advanced Distance Vector 라우팅 프로토콜로서, Hybrid 라우팅 프로토콜이라고도 한다. (디스턴스 벡터와 링크 스테이트의 장점을 결합)

- 구성(Configuration)이 쉬우며, VLSM과 Classless 라우팅을 지원한다.

- Rapid Conversence(빠른 변화 수렴)을 위해, DUAL(Diffusing Update Algorithm)을 사용하여 변화에 대해 빠르게 응답한다.

- Unequal Cost Load Balancing 를 지원한다.(★)

- 라우팅 업데이트에 있어 변화된 링크에 대한 정보만 업데이트 함으로서 대역폭을 적게 사용한다.

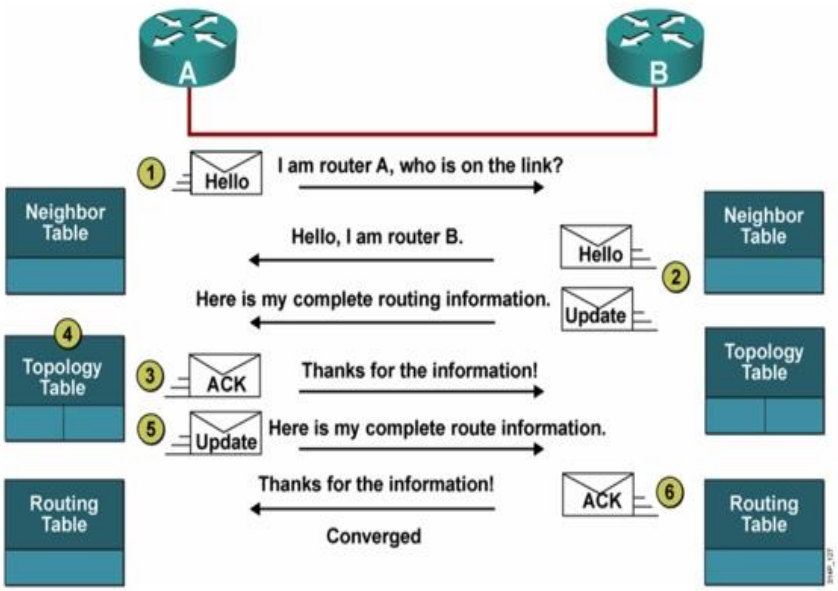
- Neighbor간에 교환되는 패킷을 MD5 Checksum을 이용하여 인증하게 할 수 있다.

- 멀티캐스트 사용 (테이블 교환 시 사용) : 브로드캐스트를 사용하면 다른 컴퓨터는 통신이 불가능하기 때문에 좋다

- 100% loop free : 루프가 안생기도록 기본적으로 Split horizon을 적용한다

- Auto Summarization : 자동적으로 요약해준다.

▶ EIGRP에서 사용하는 패킷



show ip eigrp neighbors EIGRP를 사용하는 이웃 라우터 정보

show ip eigrp topology EIGRP 토폴로지 테이블 정보

show ip route 라우팅 테이블 정보

- Hello

EIGRP 헬로 패킷은 네이버를 구성하고, 유지하기 위해 주기적으로 전송한다.
헬로 패킷은 멀티캐스트 주소인 224.0.0.10을 목적지 IP 주소로 사용한다.

헬로 주기의 3배에 해당되는 기간동안에 헬로 패킷을 받지 못하면 인접 라우터에 문제가 발생했다고 간주하고 관계를 해제하는데, 이 시간을 hold time 이라고 한다.

```
(config-if)# ip  hello-interval  eigrp 1  10
(config-if)# ip  hold-time  eigrp  1  30

# debug  eigrp  packet  hello
# debug  ip  packet
```

- Update

EIGRP 업데이트 패킷은 라우팅 정보를 전송 할 때 사용되는 패킷이다.

- Query

라우팅 정보요청 패킷은 라우팅 정보를 요청할 때 사용되는 패킷이다.

- Reply

응답 패킷은 요청 받은 라우팅 정보를 전송할 때 사용되는 패킷이다.

- Ack

Update, Query, Reply 패킷의 수신을 확인해 줄 때 사용된다.

▶ EIGRP 메트릭(혼합 메트릭)

. 벡터 메트릭중에서 MTU는 목적지까지 가는 각 인터페이스의 MTU중에서 가장 작은 것이 선택된다. 또 홉 카운트는 기본적으로 100 이다.
즉 홉 카운트가 100을 초과하면 도달 불가능한 경로로 간주한다.

. BW(bandwidth)는 목적지까지 가는 도중의 모든 인터페이스에 설정된 대역폭중에서 가장 낮은(느린) 값을 취한 후, 다음 공식에 대입한다.

BW=10^10 / 가장 느린 대역폭

. DLY(Delay)값은 목적지까지 가는 경로상의 모든 지연 값을 합친 다음 10으로 나눈다.

. 신뢰도(Reliability)는 인터페이스의 에러 발생율을 의미한다.

. 부하(load)는 인터페이스의 부하를 의미한다.

※ Default EIGRP Metric = (bandwidth + Delay) * 256

- bandwidth = 10,000,000 / minimum bandwidth in kbps

- delay = sum of delays of all interfaces in path in ten of millisecons

show ip protocols

show int s0/0

▶ EIGRP AD

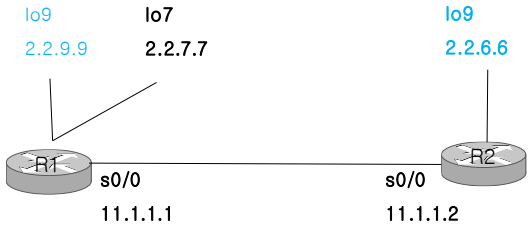
EIGRP 내부 네트워크의 AD는 90, 외부 네트워크는 170 이다.
EIGRP 네트워크를 축약하면 해당 라우터에서만 축약 네트워크의 AD 값이 5 이다.

▶ EIGRP 라우터 ID

EIGRP가 라우터 ID를 결정하는 방식은 OSPF 나 BGP 등과 동일하다. 즉

EIGRP 동작시 설정된 루프백의 IP 주소중에서 가장 높은 것을 라우터 ID로 결정한다.
만약, 루프백에 설정된 IP 주소가 없으면 물리적인 인터페이스에 설정된 IP 주소중에서 가장 높은 것을 선택한다.

자신과 동일한 라우터 ID를 가진 라우터가 전송한 외부 네트워크는 라우팅 테이블에 저장되지 않는다. (폐기함)



※ 직접 라우터 ID 지정하기

```
R1(config)# router  eigrp  1
            eigrp  router-id  2.2.1.1

R2(config)# router  eigrp  1
            eigrp  router-id  2.2.1.1
```

▶ EIGRP 설정

router eigrp *AS-number*
모든 라우터의 AS번호는 같아야 함!

network 네트워크주소 wildcard mask
Classful IP일때는 서브넷마스크를 안써도 됨!, 자신이 알리고자하는 Network 대역 정의!

※ Wild Card Mask 란?

1111 1111 . 1111 1111 . 1111 1111 . 0000 0000 => 255.255.255.0 Subnet Mask

0000 0000 . 0000 0000 . 0000 0000 . 1111 1111 => 0.0.0.255 Wild Card Mask
0000 0000 . 0000 0000 . 1111 1111 . 1111 1111 => 0.0.255.255

<R1>

-- 추천 구성 --

```
router eigrp 10
  network 1.1.1.1       0.0.0.0
  network 10.1.2.1      0.0.0.0
  network 192.168.1.1   0.0.0.0
  no auto-summary
```

-- 일반 구성 --

```
router eigrp 10
  network 1.0.0.0       0.255.255.255
  network 10.1.2.0      0.0.0.255
  network 192.168.1.0   0.0.0.3
  no auto-summary
```

-- 일반 구성 --

```
router eigrp 10
  network 1.0.0.0
  network 10.0.0.0
  network 192.168.1.0
  no auto-summary
```

-- 잘못된 구성 --

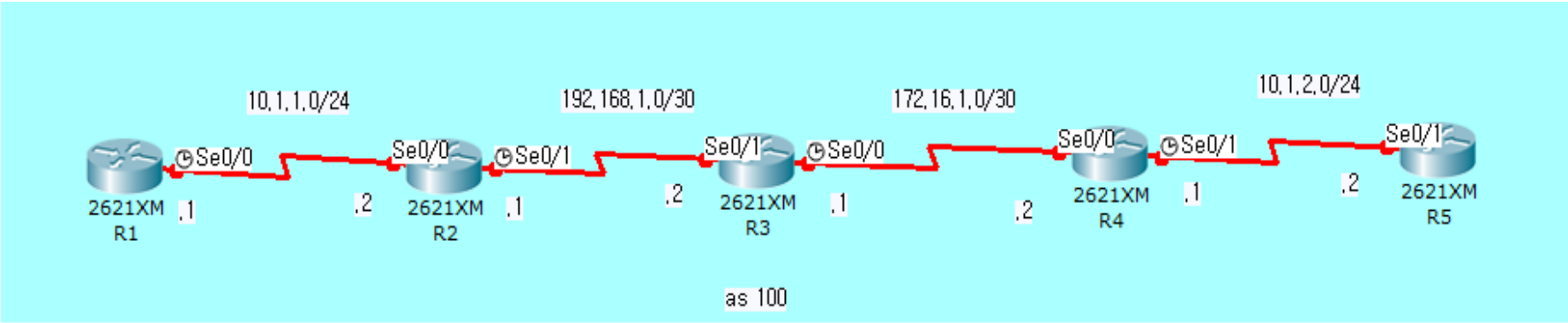
```
router eigrp 10
  network 1.0.0.0       0.0.0.0
  network 10.1.2.0      0.0.0.0
  network 192.168.1.0   0.0.0.0
  no auto-summary
```

※ 네이버 맺는 기준(★)

. as 번호가 같아야 한다.

. K-value 값이 같아야 한다. (기본값 1)

[실습] 같은 AS를 사용한 EIGRP




```
router eigrp 100
network 10.1.1.0 0.0.0.255
no auto-summary
```

```
router eigrp 100
 network 10.0.0.0
 no auto-summary
```

```
show ip eigrp neighbors
show ip eigrp topology
show ip route
```

```
show ip protocol
```

```
router eigrp 100
network 10.1.1.0 0.0.0.255
network 192.168.1.0 0.0.0.3
no auto-summary
```

```
router eigrp 100
 network 10.0.0.0
 network 192.168.1.0
 no auto-summary
```

```
# show ip eigrp neighbors
# show ip eigrp topology
# show ip route
```

```
# show ip protocol
```

```
router eigrp 100
network 192.168.1.0 0.0.0.3
network 172.16.1.0 0.0.0.3
no auto-summary
```

```
router eigrp 100
 network 192.168.1.0
 network 172.16.0.0
 no auto-summary
```

```
# show ip eigrp neighbors
# show ip eigrp topology
# show ip route
```

```
# show ip protocol
```

```
router eigrp 100
network 172.16.1.0 0.0.0.3
network 10.1.2.0 0.0.0.255
no auto-summary
```

```
router eigrp 100
 network 172.16.0.0
 network 10.0.0.0
 no auto-summary
```

```
# show ip eigrp neighbors
# show ip eigrp topology
# show ip route
```

```
# show ip protocol
```

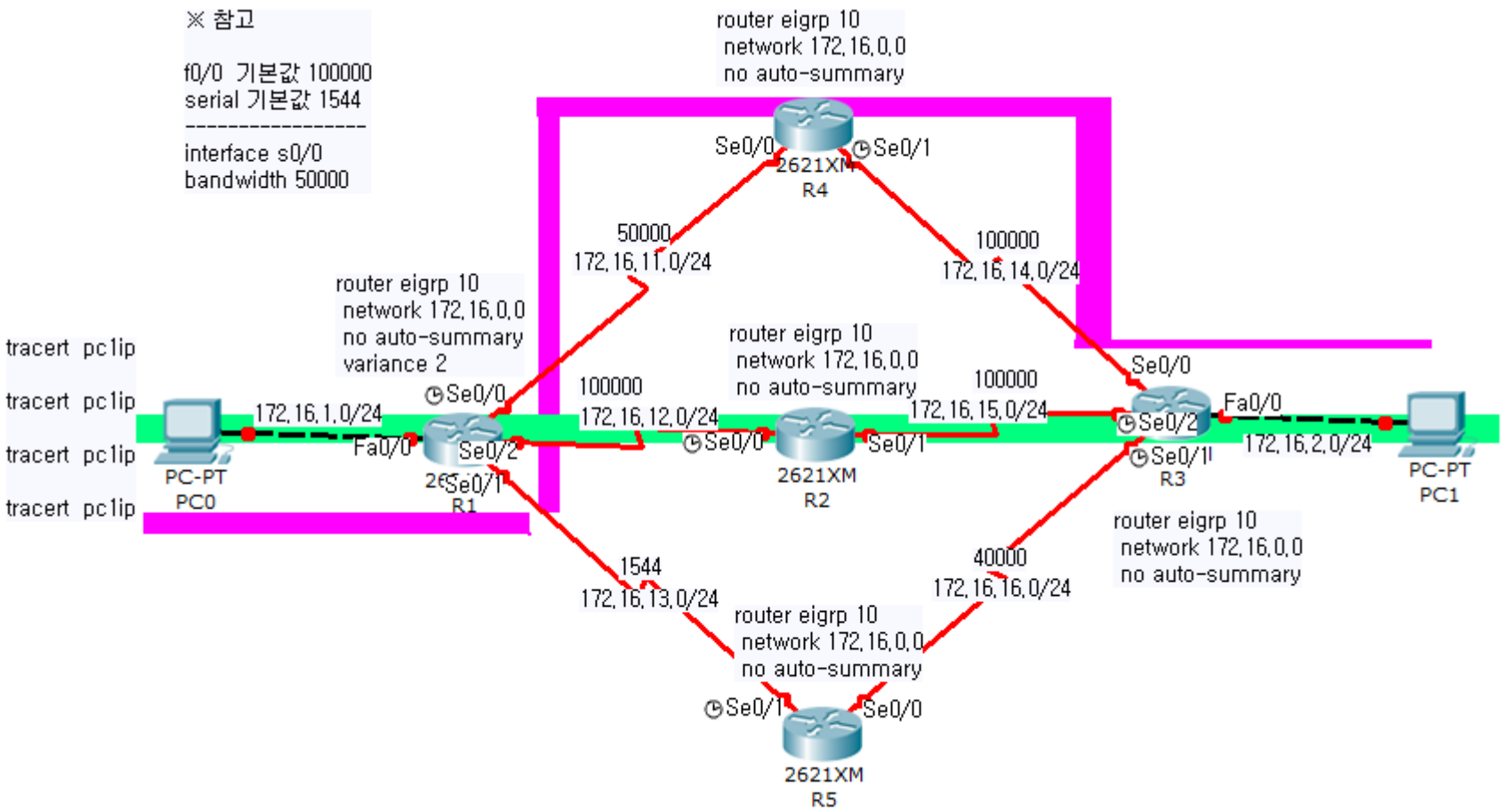
```
router eigrp 100
network 10.1.2.0 0.0.0.255
no auto-summary
```

```
router eigrp 100
 network 10.0.0.0
 no auto-summary
```

```
# show ip eigrp neighbors
# show ip eigrp topology
# show ip route
```

```
# show ip protocol
```

[실습] unequal-cost load balancing (128까지 가능)



OSPF

■ OSPF(Open Shortest Path First)

. OSPF는 규모가 크고 성장하는 Network를 위해 고안 되었다.
RIP의 한계를 극복하기 위해서 고안되었다.

. 각 라우터는 OSPF 데이터베이스를 토대로 Dijkstra Algorithm을 수행하여 최적경로를 산출하여 라우팅 테이블에 적재한다.

. IGP (Interior Gateway Protocol)이다.

. Open Architecture로서 특정 Vendor에 종속적이지 않다.

. Convergence의 속도는 Routing Change가 즉시 Flooding 되어 각 Router에서 병렬계산 되므로 대단히 빠르다. (Default : 5초 ~ 46초)

. VLSM 및 CIDR을 지원한다.

. OSPF는 Network 확장에 한계가 없다.

. Network에 변화가 있을 때만 Multicast (224.0.0.5)로 Link State Update를 하기 때문에 대역폭 사용이 적다.

. OSPF는 Bandwidth에 기초한 Cost Value 를 Path Selection Method로 사용한다. (OSPF는 Equal-Cost Multiple Path 를 최대 4 까지 지원함)

▶ OSPF 라우팅 테이블을 만들고 유지하는 과정은 개략적으로 아래와 같다.

. OSPF 가 설정된 라우터간에 헬로 패킷을 주고 받아 네이버 및 어드제이션트 네이버 관계를 구성한다.

다른 라우팅 프로토콜들과는 달리 OSPF는 모든 네이버간에 라우팅 정보를 교환하는 것은 아니다.

라우팅 정보를 교환하는 네이버를 어드제이션트 네이버라 한다.

. 어드제이션트 라우터끼리 라우팅 정보를 교환한다.

OSPF 에서는 라우팅 정보를 LSA(Link State Advertisement)라고 한다.(★)

각 라우터들은 전송받은 LSA를 링크 상태 데이터베이스에 저장한다.

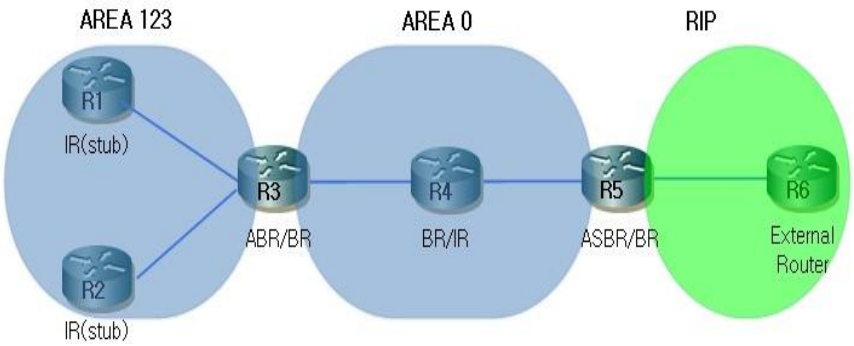
. LSA 교환이 끝나면 이를 근거로 SPF (Shortest Path First) 또는

디지크스트라(Dijkstra)라는 알고리즘을 이용하여 각 목적지가지의 최적 경로를 계산

하고 이를 라우팅 테이블에 저장한다.

. 이후 주기적으로 헬로 패킷을 전송하여 각 라우터가 정상적으로 동작하고 있음을 인접 라우터에게 알린다.

▶ AREA(영역) 개념



. OSPF에서는 네트워크를 여러 AREA로 나누고 OSPF 라우팅 정보를 몇 가지로 구분하여 적당히 작은 라우팅 테이블을 구현한다.

. AREA를 나누는데 있어서 중요한 기준 중 하나는 AREA 0 (중심이 되는 AREA)가 있어야 하며, 다른 AREA들은 모두 AREA 0와 붙어있어야 한다.(★)

. 만약 그렇게 되지 않은 경우, 가상링크(Virtual Link)를 통해 연결해야 한다.

- IR(Internal Router)

. AREA 내에 포함되어 있는 라우터를 IR이라 한다.

. IR의 인터페이스는 모두 해당 AREA의 번호를 가진다.

- ABR(Area Border Router)

. AREA와 AREA 경계선에 있는 라우터를 ABR이라 한다.

. ABR은 적어도 하나의 인터페이스는 AREA 0에 속해야 한다는 것이다.

. 만약 AREA에 붙지 못하는 경우 가상링크(Virtual Link)를 통해 속하게 한다.

- ASBR(Autonomous Systmem Border Router)

. 라우터의 인터페이스 중 일부가 OSPF영역 밖에 있는 경우의 라우터를 ASBR라고 한다.

. 예를 들면 RIP과 OSPF는 다른 프로토콜이므로 재분배를 해야하며 이럴때 ASBR이 된다.

- ABR/ASBR

. ABR이면서 ASBR인 경우로, AREA경계와 AS경계 모두 있는 경우 이다.

▶ OSPF 에서 사용하는 패킷

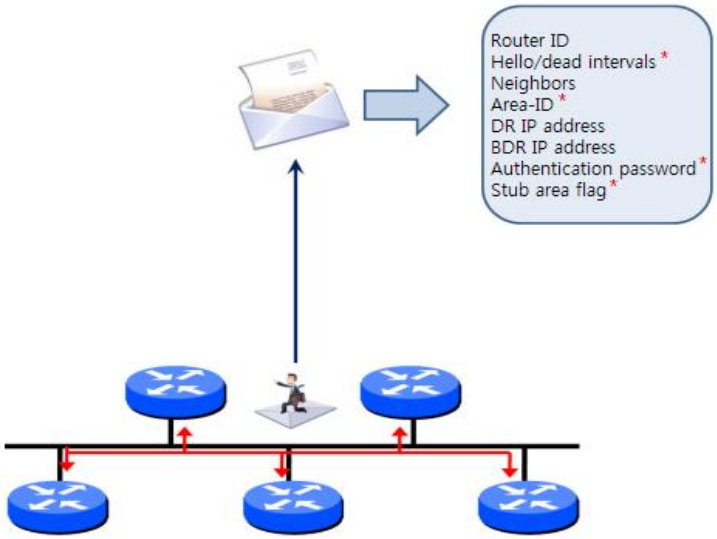
패킷 타입	패킷 이름	역할
1	hello	네이버 구성 및 유지
2	Database Description	데이터베이스 내용 요약
3	Link State Request	데이터베이스 상세내용 요청
4	Link State Update	데이터베이스 업데이트
5	Link State Ack	ACK 전송

- hello

. 헬로 패킷을 이용하여 인접한 라우터와 먼저 네이버를 구성한다.
. 물리적으로 직접 연결된 인터페이스를 통하여 네이버를 구성한다.(★)
. 물리적으로 직접 연결되어 있지 않으면 네이버 관계가 구성되지 않는다.

. OSPF 네이버를 형성하고 유지하는데 사용되는 패킷이다.
. 기본 값으로 hello패킷은 10초, 데드주기는 hello패킷의 4배를 사용한다.

※ HELLO 패킷의 데이터 값 중 반드시 일치해야하는 것들



- DDP(Link State Advertisement) = DBD

. OSPF의 네트워크 정보를 LSA라고 부른다.

. 자신이 만든 LSA 및 네이버에게서 수신한 LSA를 모두 링크 상태 데이터베이스라고 하는 곳에 저장한다.

. DDP는 OSPF 라우터의 링크 상태 데이터베이스에 있는 LSA들을 요약한 정보를 알려주는 패킷이다.

. OSPF 네이버 라우터간에 LSA들을 교환하기 전에 자신의 링크 상태 데이터베이스에 있는 LSA 목록을 상대 라우터에게 알려주기 위해서 사용한다.

- LSR(Link State Request)

. 상대 라우터가 보낸 DDP를 보고, 자신에게 없는 네트워크 정보(LSA)가 있으면, 상세한 내용(LSA)을 요청할 때 사용하는 패킷이다.

- LSU(Link State Update)

. 상대 라우터에게서 LSR을 받거나 네트워크 상태가 변했을 경우 해당 라우팅 정보를 전송할 때 사용하는 패킷이다. 즉 LSU는 LSA를 실어 나를 때 사용하는 패킷이다.

- LS ACK (Link State Acknowledgement)

. OSPF는 DDP, LSR, LSU 패킷을 수신하면 반드시 LS ACK 패킷을 사용하여 상대에게 정상적으로 수신했음을 알려야 한다.

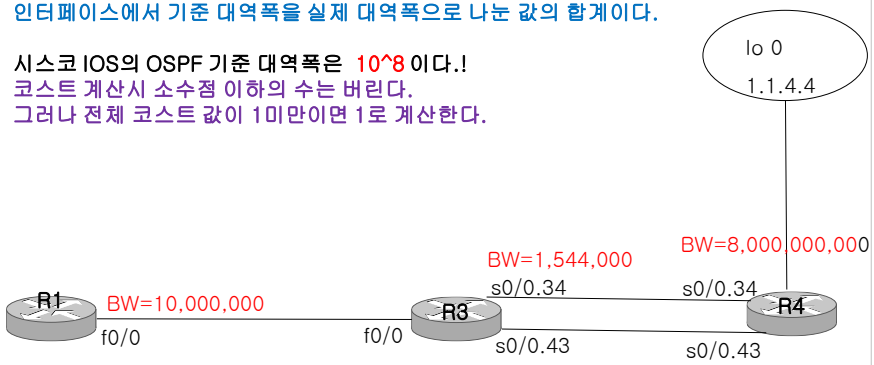
▶ OSPF 단계별 사용하는 OSPF 패킷 종류

INIT → 2WAY → EXSTART	→ EXCHANGE → LOADING → FULL
HELLO 패킷	DBD, LSR, LSU, LSAck 패킷

▶ OSPF 메트릭

OSPF 의 메트릭을 코스트(cost)라고 부르며, 출발지부터 목적지까지의 각 인터페이스에서 기준 대역폭을 실제 대역폭으로 나눈 값의 합계이다.

시스코 IOS의 OSPF 기준 대역폭은 10^8 이다.!
코스트 계산시 소수점 이하의 수는 버린다.
그러나 전체 코스트 값이 1미만이면 1로 계산한다.



< 예 > R1 에서 R4 의 1.1.4.4 네트워크에 대한 OSPF 코스트 값은 ?

f0/0 10(10^8/10,000,000), s0/0.34 64(10^8/1,544,000), lo0 1(10^8/8,000,000,000)

10 + 64 + 1 = 75 (cost)

▶ OSPF 구성하기

router ospf process-id

network networkIP Wildcardmask area 0

※ 프로세스 ID (Process ID)

- 라우터 내부적으로 사용하는 ID 이며, 다른 라우터와 동일한 필요가 없다.

- 운용상의 편리성을 위해 서로 동일하게 사용하는 것이 좋다.

- 한 라우터는 여러 개의 OSPF 프로세스를 운용할 수 있는데, 이는 여러 개의 OSPF 데이터베이스를 사용한다는 것이다

▶ DR 과 BDR

DR, BDR 은 브로드캐스트 및 논브로드캐스트 네트워크에서만 사용되며,
포인트 투 포인트 네트워크에서는 사용하지 않는다.

- DR이 다운되면 BDR이 DR이 되고, BDR을 새로 선출한다. BDR 이 다운되면 BDR을 새로 선출한다. DR, BDR이 아닌 라우터를 DROTHER 라우터라 한다.

- DR, BDR이 선출되면 DROTHER 라우터들은 DR 및 BDR 라우터와 라우팅 정보를 교환한다. 또 DR 과 BDR 도 서로 라우팅 정보를 교환한다.

  그러나 DROTHER 라우터끼리는 라우팅 정보를 교환하지 않는다.(★)

▶ OSPF의 주요 용어

- Neighbor

. 하나의 라우터에 있어 라우팅 정보를 교환하는 다른 라우터를 일컫는 말이다.

. 네이버를 잘 맺어야만, 비로소 라우팅 정보를 주고 받게 된다.

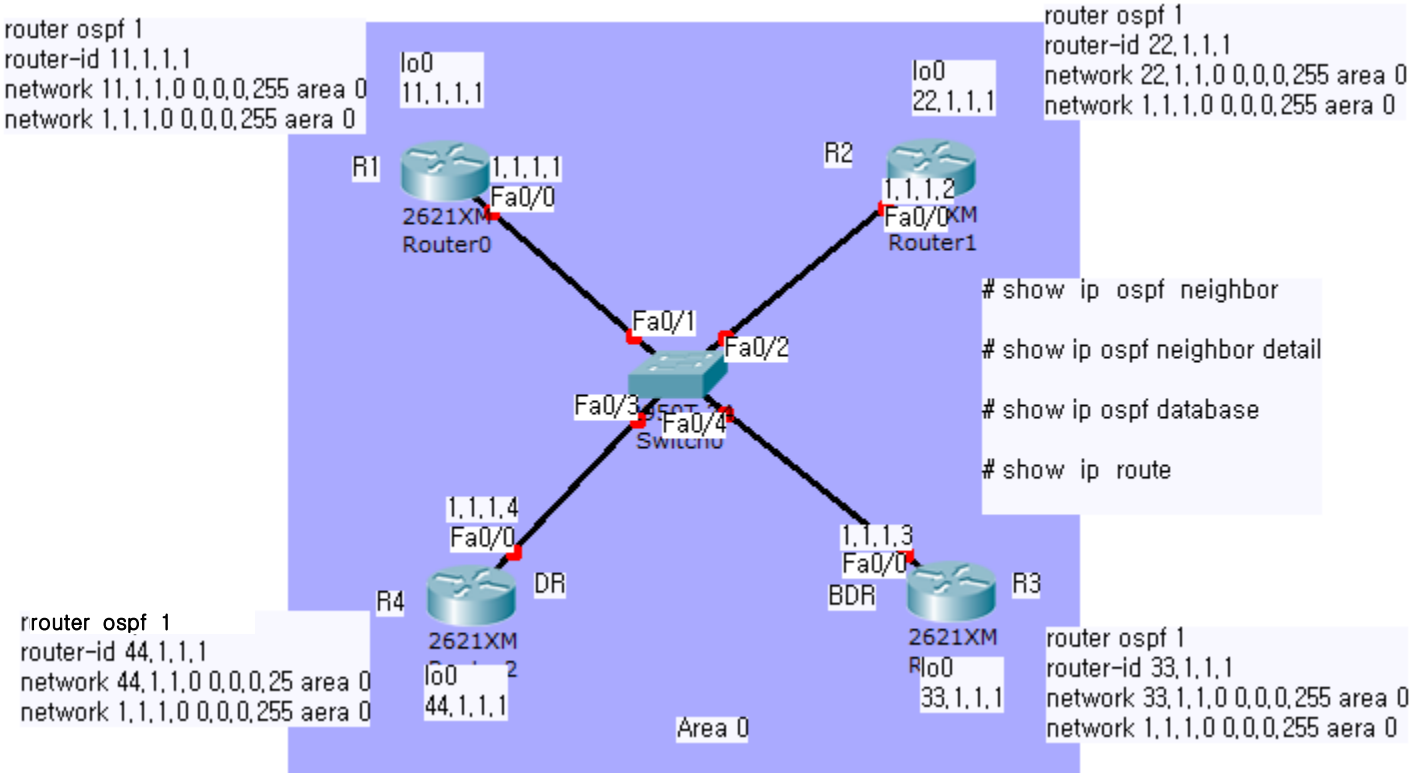
. 한 라우터를 기준으로 볼 때 직접 연결되어 있는 라우터를 말한다.

- Adjacency neighbor (★)

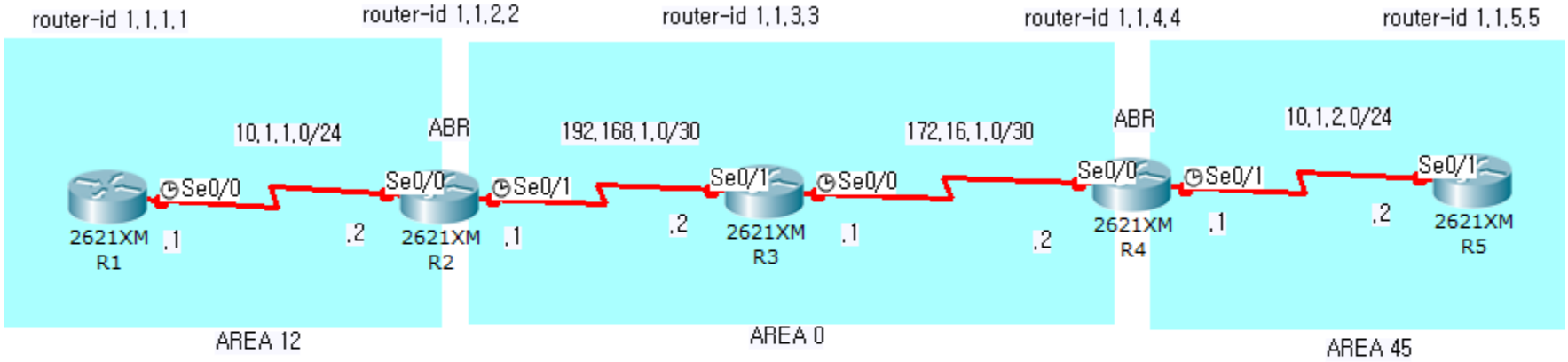
. OSPF 라우팅 정보를 주고 받는 네이버를 adjacency neighbor 라고 한다.

. 네이버가 아니면 adjacency neighbor 도 아니다.

<연습> DR / BDR / DROther 선출



[실습]




```
# show  ip  ospf  neighbor

# show ip ospf database

# show  ip  route

# debug  ip  ospf  adj
```

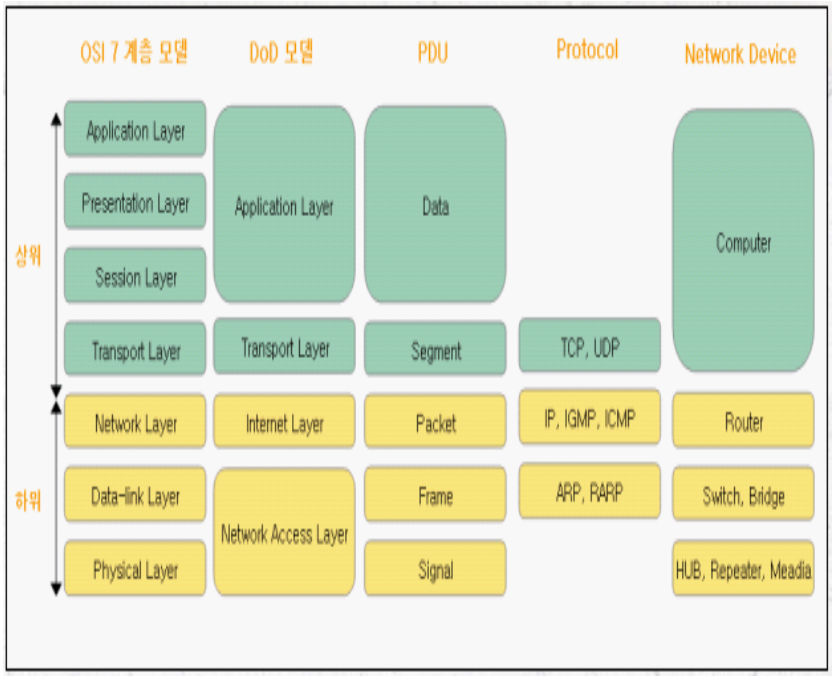
OSI

▶ OSI 7 Layer (Open System Interconnection)

국제 표준 기관(ISO)으로써 개방형 통신을 할 수 있게 OSI 7 Layer를 만들었다.

Upper Layer	Application	인터페이스 제공
	Presentation	데이터 인코딩 & 디코딩, 암호화 & 복호화
	Session	통신 장비간의 연결 관리
Lower Layer	Transport	흐름제어, 분할, 재조합, 에러관리
	Network	라우팅, 패킷 분할, 프로토콜 식별, 에러탐지
	Data link	장비 식별, 에러 체킹
	Physical	물리적, 전자적 특성, 아날로그 ↔ 디지털

▶ TCP / IP 4계층



※ Packet = datagram

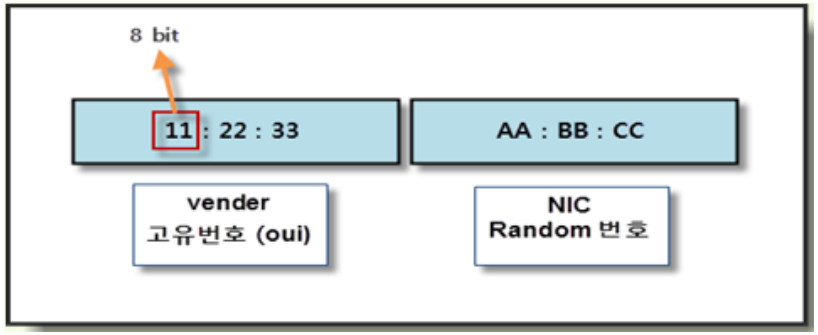
※ MTU (Maximum Transmission Unit : 대역폭)는 하나의 프레임이나 패킷이 한번에 전송가능한 데이터의 크기이다.

일반적으로 이더넷을 사용하기 때문에 최대 MTU 사이즈는 1500 바이트 이다.

- L1 (네트워크 인터페이스)

1. MAC 주소 (48bit)

MAC주소는 내부PC끼리 통신을 주고받을 시 이용되는 근거리 통신



10진수 = 0 1 2 3 4 5 6 7 8 9

16잔슈 = 0 1 2 3 4 5 6 7 8 9 A B C D E F

- L2 (인터넷 계층)

인터넷 계층은 IP를 이용한 Routing 과 Forwarding 기능이 존재한다.

. Routing
외부 통신을 위해 목적지까지 최적의 경로를 정하는 역할입니다.

. Forwarding
목적지주소로 가기위해 나가는 포트로 패킷을 이동시키는 역할입니다.

A Class : 1 - 126
B Class : 128 - 191
C Class : 192 - 223
D Class : 224 - 239

---

unicast (global unicast) : A , B , C = 유일한 MAC 주소

multicast : D = 0100-5e - 로 시작

broadcast : 255.255.255.255 , 1.255.255.255 = FFFF.FFFF.FFFF

---

loopback : 127.0.0.1

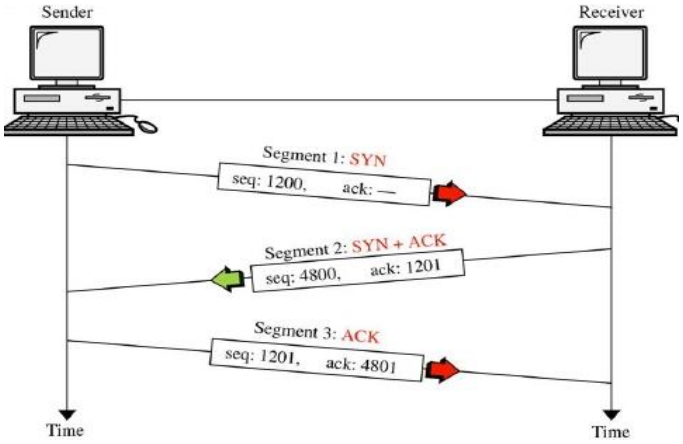
사설 주소

10.0.0.0 ~ 10.255.255.255 (10/8 prefix)
172.16.0.0 ~ 172.31.255.255 (172.16/12 prefix)
192.168.0.0 ~ 192.168.255.255 (192.168/16 prefix)

자동 사설주소 : 169.254.0.0/16

- L3 (전송 계층)

. TCP : 3way-handshake 사용 신뢰성이 높고 속도가 느리다.



. UDP : 신뢰성이 낮고 속도가 빠르다. 스트리밍(동영상) 서비스에 사용 .

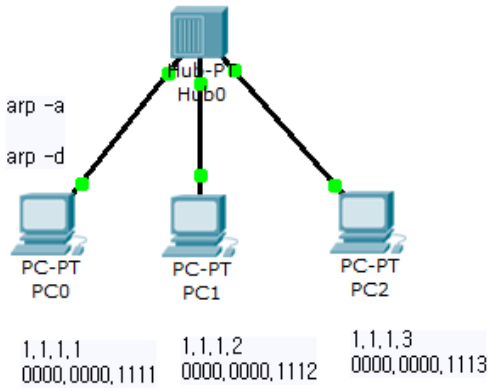
- L4 (응용 계층)

. 응용프로그램을 사용하는 계층으로 FTP, HTTP 등 있습니다.
. 프로그램상에서 수신측에 전달할 데이터가 만들어지는 곳입니다.

웹서버 = TCP 80
FTP서버 = TCP 21 (20)
Telnet서버 = TCP 23

DNS 서버 = TCP 53 , UDP 53

■ ARP (Address Resolution Protocol)



ping 1.1.1.2

스텝 1. 1.1.1.1 -> 1.1.1.2 경류할때

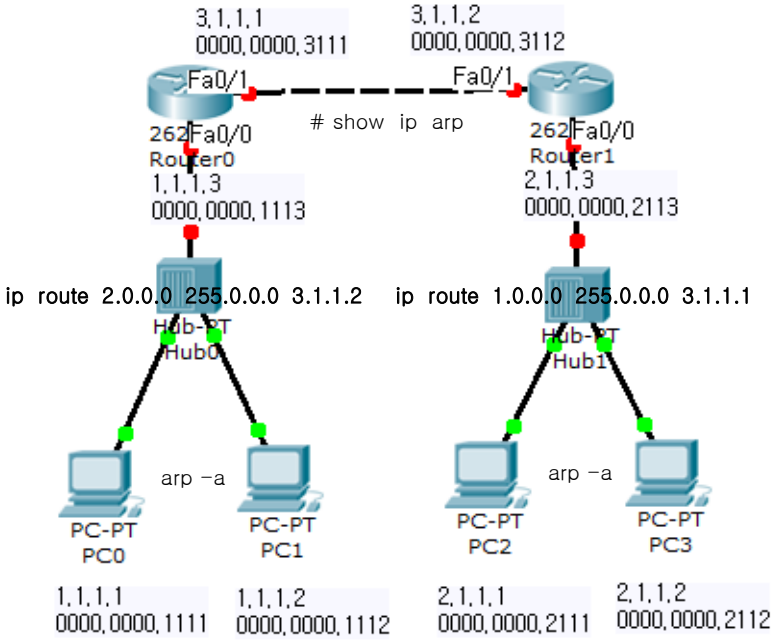
출발지 IP : 1.1.1.1 목적지 IP: 1.1.1.2
출발지 MAC: 0000.0000.1111 목적지 MAC: FFFF.FFFF.FFFF

스텝 2. 1.1.1.2 -> 1.1.1.1 경류할때

출발지 IP : 1.1.1.2 목적지 IP : 1.1.1.1
출발지 MAC: 0000.0000.1112 목적지 MAC: 0000.0000.1111

※ 라우터 맥주소 바꾸는 명령어

int fa0/1
mac-address 0000.0000.3111



ping 2.1.1.1

■ Collision 영역 과 Broadcast 영역

▶ Collision Domain (콜리전 도메인)

이더넷 방식의 LAN에서 전송매체를 공유하고 있는 단말 사이의 경쟁 (동시에 정보를 전송하는 등)이 생겼을 경우를 충돌이라한다. 이 때, 이 러한 충돌이 전파되어서 정보의 송,수신에 영향을 받는 영역을 Collision Domain이라 한다.

Collision Domain은 동일 매체에 연결된 장치들의 그룹니다.

스위치 및 브리지는 이러한 도메인을 더 작은 단위로 나눔으로써 네트 워크 내부의 Collision Domain을 분할 할 수 있도록 한다.

리피터, 허브등을 통하여 네트워크를 구성할 경우 이는 2계층 장비가 아니므로 Collision을 나눌 수 없다.

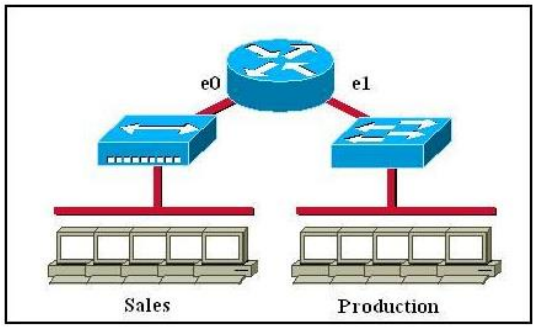
▶ Broadcast Domain (브로드캐스트 도메인)

Broadcast Domain은 네트워크상에 연결된 단말중 한 노드가 브로드 캐스트 패킷을 전송할 때 그 패킷을 수신 할 수 있는 노드들의 집합을 의미한다.

Broadcast Domain 분할이 가능한 장비는 3계층 장비인 라우터, VLAN등이 존재한다.

Collision Domain을 나누는 장비들은 Collision을 나눌수는 있지만 Broadcast 패킷을 전송하는 부분에는 대책이 없다. 이때 라우터에 이 러한 Domain을 연결함으로써 Broadcast Domain을 분할 가능하다.

<연습>



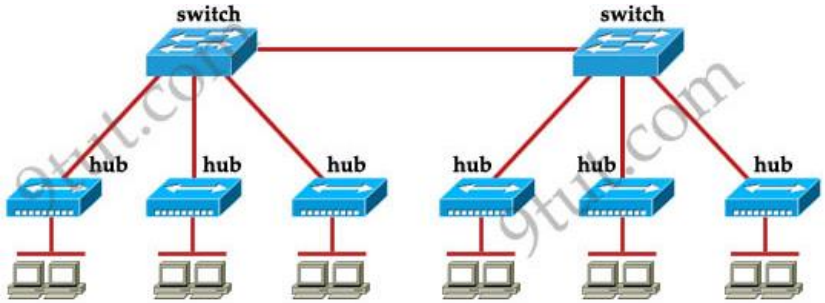
충 : 7

브 : 2

<연습>

충 : 7

브 : 1



Switch

■ 스위치(Switch)

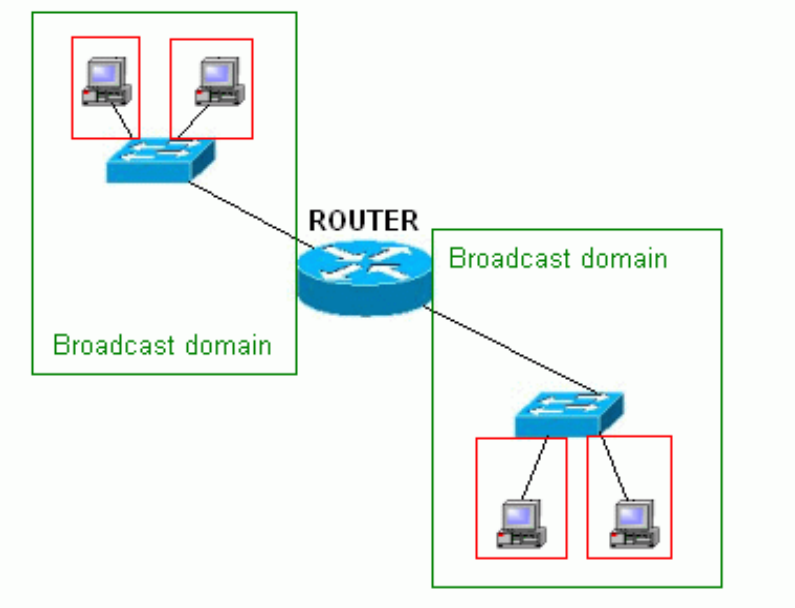
. 허브(Hub)장비의 단점인 콜리전 도메인(Collision Domain)문제를 해결하기 위해서 개발한 장치

. 그러나 여전히 브로드 캐스트 도메인(Broadcast Domain)문제는 해결되지 않았는데 라우터는 브로드 캐스트 도메인이 해결되었다.

. 허브는 콜리전 도메인으로 인해 다수의 네트워크를 허브로 연결한 한 PC에서 데이터를 보낼 시 다른 PC에서는 데이터 전송이 안되었다.

. 스위치는 이러한 문제점을 해결하여 특정 PC가 데이터를 송신하더라도 다른 PC에서 데이터 송신이 가능하다.

	허브	스위치	라우터
Collision Domain	1	port 별	port 별
Broadcast Domain	1	1	port 별



- 도메인의 의미(Domain)

. 지역(Area)을 의미함
. 보통 도메인 네임은 인터넷 주소로서 각각의 위치를 가리키는 이름

-충돌 도메인(Collision Domain) : Ethernet상에서 Collision이 발생 가능한 범위

. Ethernet 통신방법인 CSMA/CD(Carrier Sense Muliple Access / Collision Detection) 방식을 사용한다.

. 네트워크에서 둘 이상의 호스트가 통신을 하면 안되는 지역으로서 통신을 할 경우 충돌이 발생한다.

. 호스트들을 하나의 충돌 도메인으로 묶어주는 네트워크 장비로는 허브와 리피터가 있다. (물리계층 장비)

. 2계층 장비인 스위치는 충돌 발생을 막아주기 때문에 스위치 단위로 충돌 도메인을 나눌 수 있다. 허브는 1계층이므로 불가능 하다.

-브로드 캐스트 도메인(Broadcast Domain) : 네트워크 장비가 브로드케스트를 전달하지 않는 범위

. 라우터는 브로드캐스트를 전파하지 않기 때문에 라우터 단위로 브로드 캐스트 도메인을 나눌 수 있다.

▶ 스위치의 기본 동작 이해

ⅰ. Learning

브리지나 스위치는 자신의 포트에 연결된 PC가 통신을 위해서 프레임을 보내면 PC의 맥 어드레스를 읽어서 자신의 맥 어드레스 테이블(브리지 테이블)에 저장.

ⅱ. Flooding (broadcast:FFFF.FFFF.FFFF, multicast:0100-5e 로 시작)

들어온 포트를 제외한 나머지 모든 포트로 데이터를 뿌리는 것.

ⅲ. Forwarding

브리지가 목적지의 맥 어드레스를 자신의 브리지 테이블에 가지고 있고, 이 목적지가 출발지의 목적지와 다른 세그멘트에 존재하는 경우. 즉, 목적지가 어디 있는지 아는데 그 목적지가 다리를 건너야만 하는 경우 발생.

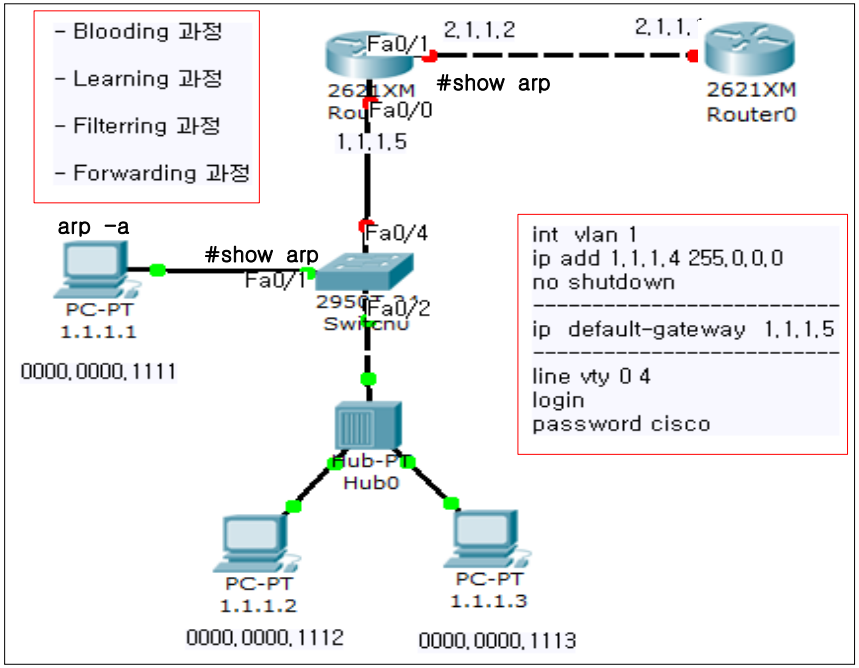
ⅳ. Filtering

브리지가 목적지의 맥 어드레스를 알고 있고 출발지와 목적지가 같은 세그먼트 상에 있는 경우, 필터링 기능 때문에 허브와는 다르게 콜리전 도메인을 나눌 수가 있다.

ⅴ.Aging

어떤 맥 어드레스를 브리지 테이블에 저장하고 나면, 그 때부터 Aging이 가동되어 저장 후 300초가 되어도 더 이상 그 출발지 주소를 가진 프레임이 들어오지 않으면 브리지 테이블에서 삭제.

<그림>



[ARP 과정]

1.1.1.1 -> 1.1.1.2 : S(1.1.1.1 – 0000.0000.1111), D(1.1.1.2 – FFFF.FFFF.FFFF)
1.1.1.2 -> 1.1.1.1 : S(1.1.1.2 – 0000.0000.1112). D(1.1.1.1 – 0000.0000.1111)

```
Switch#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0000.1111    DYNAMIC     Fa0/1
   1    0000.0000.1112    DYNAMIC     Fa0/2
   1    0000.0000.1113    DYNAMIC     Fa0/2
```

▶ 랜 스위칭 방법

- Store and Forward

처음부터 끝까지 이상이 있는지 없는지 확인 후 넘겨준다.
Store and Forward 스위칭 방식은 버퍼에 프레임 전체를 복사하여 CRC를 계산한 후 전송한다.

- Cut-Through (Real Time)

목적지 맥주소가 있는데 까지만 보고 그 다음 까지는 안본다.
이 방식은 버퍼에 프레임의 수신지 주소 Preamble 다음의 6바이트 만 복사한다.

- Fragment Free Store and Forward

총 64바이트까지 검사를 함 - 이 정도만 검사해도 90%이상의 데이터를 보장한다는 것을 확률적 계산에 의해 결정.

이 방식은 Cut-Through 방식을 보완한 방식이다.

▶ 포트 Duplex 구성하기(기본 값은 Auto)

Duplex는 스위치와 시스템 상호간 통신시 송신과 수신이 어떤 형식으로 이루어지는지에 대한 mode를 말한다.

기본 값은 Auto이고 자동으로 구성해준다.

Switch(config-if)#duplex ?

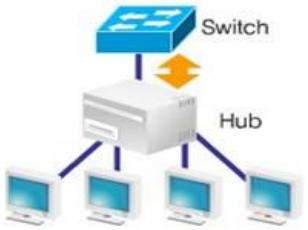
auto Enable AUTO duplex configuration
full Force full duplex operation
half Force half-duplex operation

- Half Duplex

. 단방향 data flow

. Collision이 발생할 확률이 높다.

. Hub 연결에 사용된다.

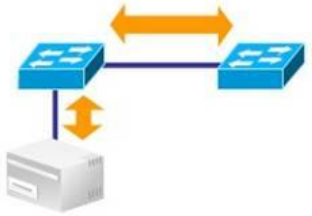


- Full Duplex

. 양방향 data flow

. Collision이 발생하지 않는다.

. Switch port에서 지원한다.



▶ Transparent bridging

이더넷 스위치는 mac 주소 테이블을 참조하여 이더넷 프레임을 목적지 방향으로 전송한다. 이때 mac 주소 테이블을 만들고, 유지하며, mac 주소 테이블을 참조하여 프레임을 전송하는 것을 트랜스패런트 브리징이라고 한다.

※ 참고

When the aging type is configured with the absolute keyword, all the dynamically learned secure addresses age out when the aging time expires

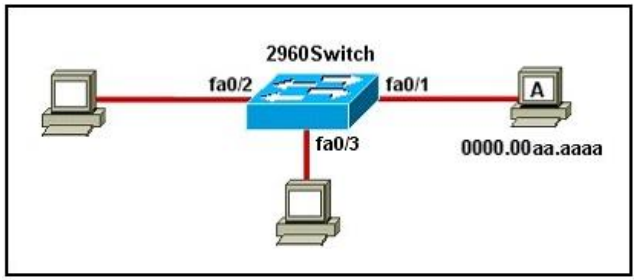
This is how to configure the secure MAC address aging type on the port:

Router(config-if)# switchport port-security aging type absolute

and configure the aging time (aging time = 120 minutes)

Router(config-if)# switchport port-security aging time 120

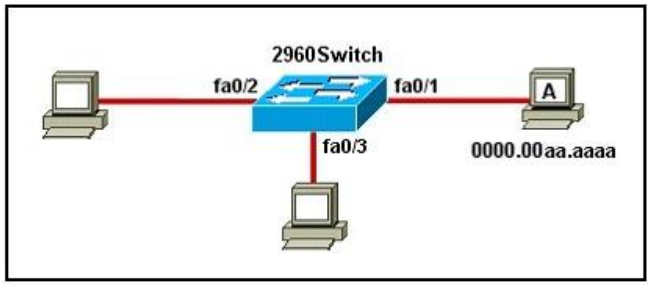
- Dynamic mac-address (출발지 주소만 배움)



show mac-address-table

- Static mac-address

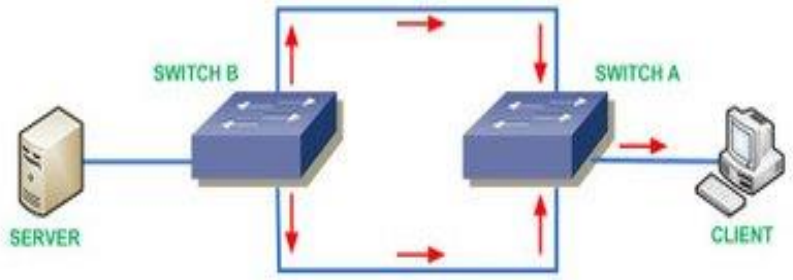
mac-address-table static 0000.00aa.aaa vlan 1 interface fa0/1



show mac-address-table

▶ STP(Spanning Tree Protocol)

– 문제점 : 루핑(Looping)

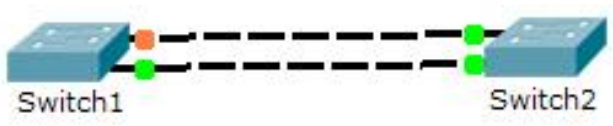


. 스위치나 브리지는 2개 이상의 경로가 만들어 질 경우 위의 그림같이 루핑(Looping)이 발생한다.

. 서버에서 브로드캐스트를 날리게되면 Switch B에서 브로드 캐스트를 날리고 Switch A에서 다시 브로드캐스트를 날리고 그것을 다시 Switch B가 브로드 캐스트를 날리는 것을 계속 반복한다. 이것을 루핑이라고 한다.

. 루핑이 계속 발생하면 이더넷의 특성상 네트워크가 프레임 전송이 없어야 보낼 수 있기 때문에 다른 전송이 불가능 하기에 치명적이다.

– 해결책 : STP(Spanning Tree Protocol)



. 스위치나 브리지에서 발생할 수 있는 루핑을 미리 막기 위해 두 개 이상의 경로가 발생하면 하나를 자동으로 막아두었다가 기존 경로에 문제가 생기면 막아놓은 경로를 풀어서 데이터를 전송하는 알고리즘

. 스패닝 트리가 세팅되어 있으면 스패닝 트리는 자동으로 루핑을 검색해서 이런 루핑이 발생할 수 있는 상황을 막아준다.

. 스위치 간의 두 개의 링크 중 하나를 끊어 놓는 것으로서, 위 그림과 같이 실제 링크는 2개이지만 데이터는 한쪽으로만 다니게 하는 것.

. 위와 같은 경우 STP가 설정되어 있기 때문에 Switch1에서 위쪽 포트 한쪽을 끊어놓아 루프를 방지한다.

. 실제 끊어진 것은 아니고 대기중인 링크이며, 사용중인 링크가 끊어지게 되면, 그 때 살아나서 데이터 전송을 맡아준다.

STP 프로토콜을 이해하기 위한 기본 개념

- Bridge ID와 Path Cost를 이해해야 한다.

Bridge Priority	맥 어드레스 (MAC Address)
8000	0260 8c01 1111
1000 0000 0000 0000	0000 0010 0110 0000 1000 1100 0000 0001 0001 0001 0001 0001

2바이트(16비트) 6바이트(48비트)

<1> 브리지 ID(Bridge ID)

. 브리지나 스위치들이 통신할 때 서로를 확인하기 위해 하나씩 가지고 있는 번호

. 브리지 ID는 브리지 우선순위(Bridge Priority) 와 브리지 맥 주소 (Bridge MAC Address)로 구성 (★)

. 우선순위의 경우 16비트로 만들어지기 때문에 0부터 2의 16제곱 -1 (0부터 65535) 까지 만들어진다. 기본 값은 32768이다.

. 우선 순위 값은 낮은 값일 수록 우선 순위가 높다.

. 맥 주소는 스위치에 고정되어 있는 값으로서 고유의 번호이다.
(이더넷 카드의 맥 주소를 생각하면 된다)

<2> Path Cost

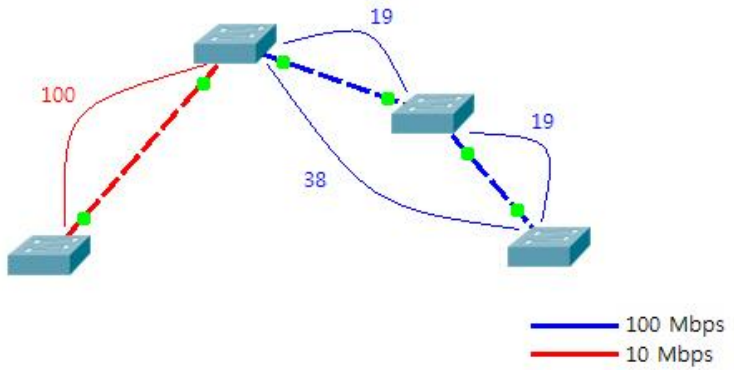
. 브리지가 얼마나 가까이, 그리고 빠른 링크로 연결되어있는지 알아내기 위한 값

. 따라서 두 스위치가 10Mbps로 연결되었다고 가정할 때,
Path Cost값은 1000/10 = 100 이 된다.

. 링크의 속도(대역폭)이 빠를수록 더 작은 값이 되며 10Gbps가 나오게 되면서 0.1이 되는데 기계는 소수를 계산하는데 오래걸리므로 개정했다.

※ 최신 **Path Cost**

Band Width(대역폭)	STP Cost(Path Cost)
4Mbps	250
10Mbps	100
16Mbps	62
45Mbps	39
100Mbps	19
155Mbps	14
622Mbps	6
1Gbps	4
10Gbps	2



-스패닝 트리를 위한 용어

Root Bridge	BID가 가장 낮은 브릿지
Non Root Bridge	루트 브릿지가 아닌 모든 브릿지
Root Port	비 루트 브릿지중 루트 브릿지에서 가장 가까운 포트 (Path Cost가 가장 작은것)
Designated Port	BPDU 송신
Non Designated Port	BPDU 수신, Block 되는 포트

※ BPDU(802.1d): 스패닝 트리 정보를 주고 받기 위한 특수 프레임

※ Root Bridge 선출 순서

. 네크워크당 하나의 Root Bridge 를 갖는다.

. 루트 브리지가 아닌 나머지 모든 브리지(Non Root Bridge)는 무조건 하나의 Root Port 를 갖는다.

. Segment 당 하나씩의 Designated Port 를 갖는다.

- 스패닝 트리 포트 상태

차단 (Blocking)
. BPDU 수신한다.
. 데이터 프레임을 송수신하지 않는다.
. 20 초이후 청취상태가 됨.

↓

청취 (Listening)
. 지정 포트라면 청취 상태에서 BPDU를 전송한다.
. 청취 상태에서 기본적으로 15초 지나면 학습 상태로 변경된다. (RP or DP 가 결정된 다음 차단에서 청취로 변경됨)

↓

학습 (Learning)
. 학습 상태에서 mac 주소 테이블을 채우기 시작한다.
. 학습 상태에서 기본적으로 15초가 경과하면 전송 상태로 변경된다.

↓

전송 (Forwarding)
. 전송 상태에서는 데이터 프레임을 송수신한다.
. POST -> 지정/루트 포트 결정 -> 청취상태

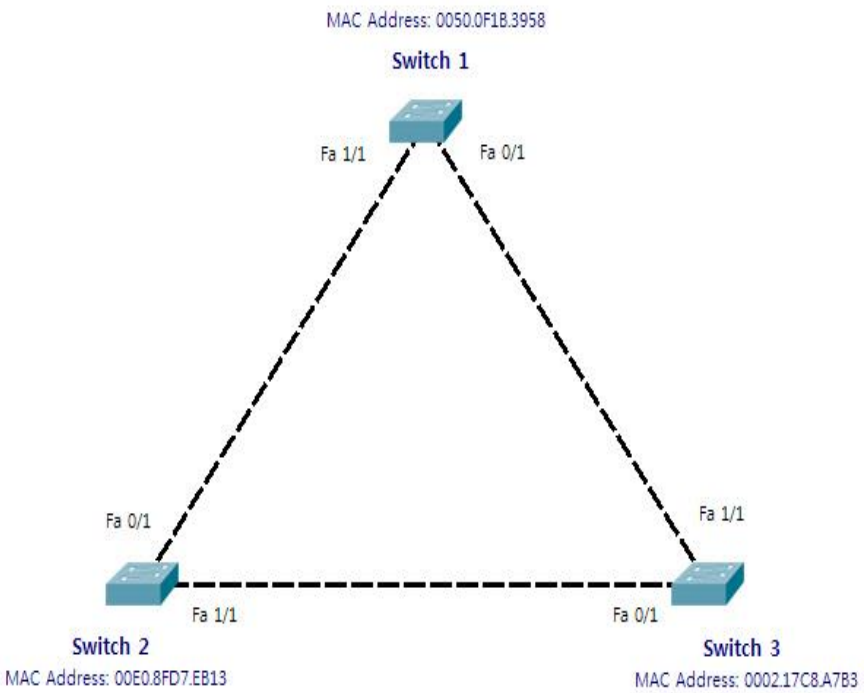
learning	populating the MAC address table but not forwarding data frames
forwarding	sending and receiving data frames
listening	preparing to forward data frames without populating the MAC address table
blocking	preventing the use of looped paths

※ portfast

포트 패스트는 단일 호스트가 접속된 포트에 설정해야 한다. 허브나 스위치 등에 설정하면 일시적인 루프가 발생할 수 있다.

```
int fa0/1
  spanning-tree portfast
```

[실습] 스패닝 트리 확인

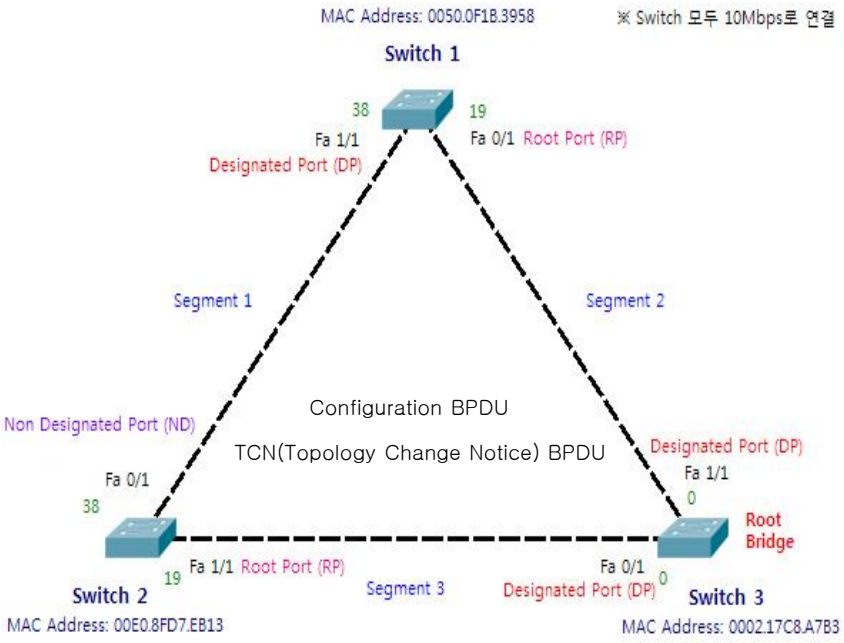


. 스위치의 MAC 주소 확인하기

Switch1 #show version

생략
Base ethernet MAC Address: 0050.0F1B.3958
생략-

★ RP의 반대쪽이 무조건 DP가 된다.



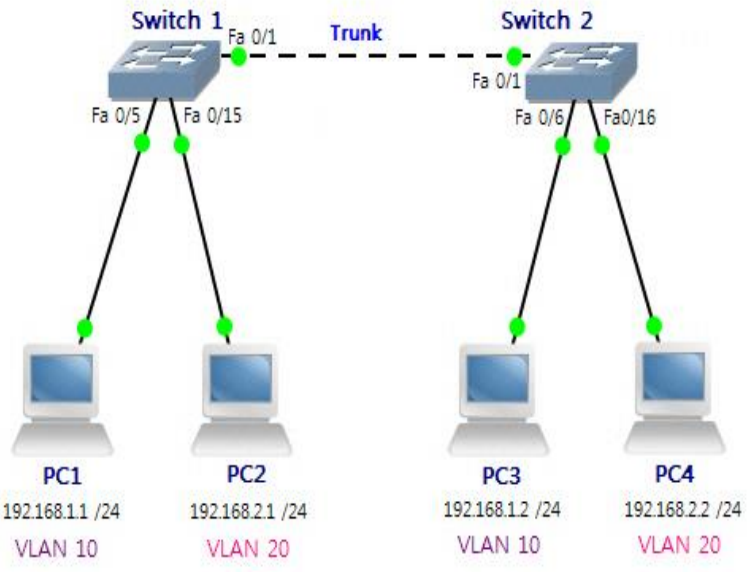
. 위의 포트들을 다 선출한 나머지가 바로 Non Designated Port 로서 비활성화되는 포트이다

show spanning-tree

★ 바로 옆 라인이 끊기면 listening and learning time이 15초씩 30초의 convegence 시 간이 걸린다.

하지만 건너편에 있는 라인이 끊기면 BPDU기다리는 시간 20초를 더해 50초의 학습 시간이 걸린다.

▶ VLAN (Virtual Local Area Network) = broadcast domain = network = subnet



show version

show spanning-tree interface fa0/5
show spanning-tree vlan 10

show mac-address-table

show vtp status

show vlan
show vlan brief
show interface trunk or show interfaces switchport

show cdp neighbor
show cdp neighbor detail

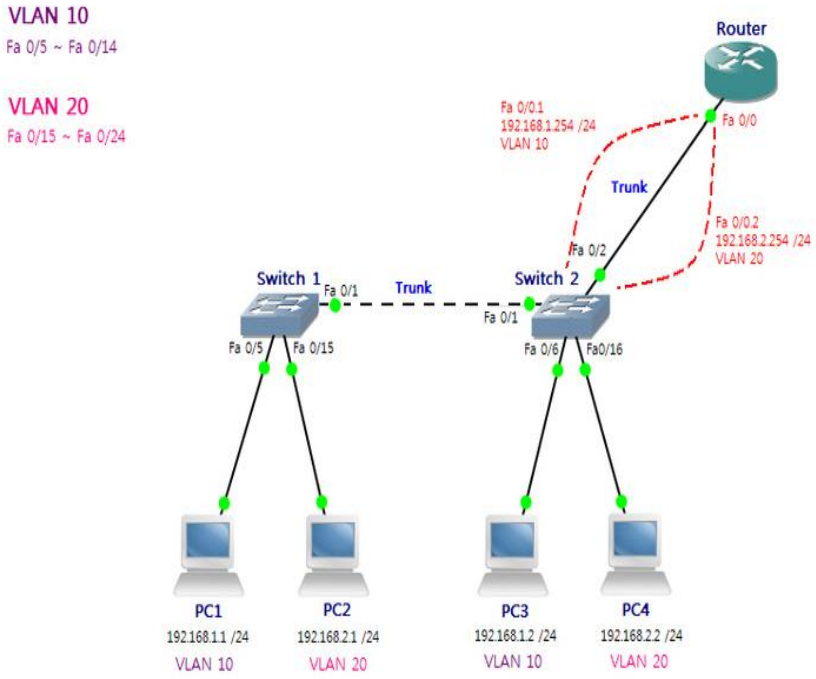
< switch 1 >

```
vlan 10
  name vlan10

vlan 20
  name vlan20


interface f0/5
  switchport mode access
  switchport access vlan 10

interface f0/15
  switchport mode access
  switchport access vlan 20

interface f0/1
   switchport mode trunk
```

< switch 2 >

```
vlan 10
  name vlan10

vlan 20
  name vlan20


interface f0/6
  switchport mode access
  switchport access vlan 10

interface f0/16
  switchport mode access
  switchport access vlan 20

interface f0/1
  switchport mode trunk
```

<실습 > VLAN 간 통신 연습



. VLAN10 (PC1과 PC3)끼리만 통신이 가능하고, VLAN20 (PC2과 PC4)끼리만 통신이 가능하였으나 라우터로 두 VLAN을 연결했으므로 통신이 가능하다.

. 따라서 PC1에서 PC2와 PC3에 ping명령어를 사용하면 두개의 PC 모두 응답이 온다

< switch 2 >

```
interface fastethernet 0/2
   switchport mode trunk
```

< router >

```
interface fastethernet 0/0
   no shutdown

interface fastethernet 0/0.10
   encapsulation  dot1Q  10
   ip address 192.168.1.254 255.255.255.0

interface fastehternet  0/0.20
   encapsulation dot1Q  20
   ip address192.168.2.254 255.255.255.0
```

```
show  version

show  spanning-tree interface  fa0/5
show  spanning-tree vlan 10

show  mac-address-table

show  vtp  status

show vlan
show  vlan  brief
show interface trunk

show cdp neighbor
show cdp neighbor detail
```

※ 스위치 트렁크 링크 확인하는 명령

```
show  interface  f0/2 switchport
show  interface  f0/2  trunk
```

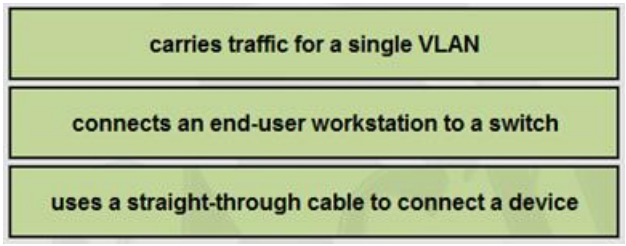
▶ VLAN Trunking

트렁크 또는 트렁크 포트란 복수개의 VLAN 에 소속된 포트를 말한다. 또 트렁크가 사용하는 프로토콜을 트렁킹(trunking) 프로토콜이라고 한다.

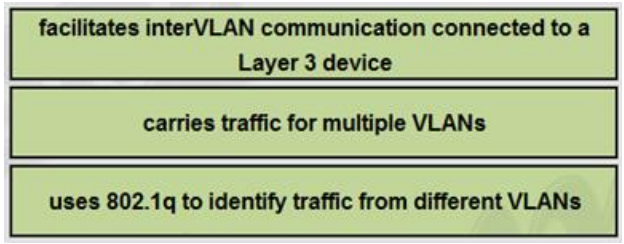
하나의 VLAN 에만 소속된 액세스 포트와 달리, 트렁크 포트는 복수개의 VLAN에 소속된 포트이다.

두 스위치에서 사용하는 VLAN 번호가 동일하다면 스위치 사이를 연결하는 포트도 액세스 포트로 설정할 수 있다.

- Access Port



- Trunk Port



show interface f0/2 switchport
show interface f0/2 trunk

- 트렁킹 프로토콜(Trunking Protocol)

트렁킹 프로토콜로는 시스코사에서 만든 ISL트렁킹 과 IEEE802.1Q트렁킹이 있다.

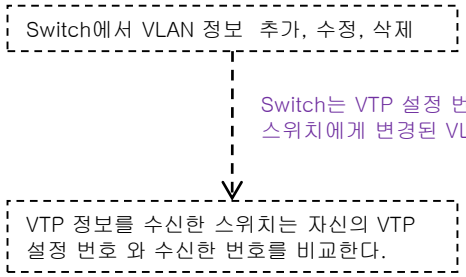
스위치 모델에 따라 두가지 방식 모두를 지원하는 것도 있고, 한 가지만 지원하기도 한다.

IEEE 802.1Q (Default)	. 트렁킹에 대한 표준 프로토콜 . 네이티브 VLAN 사용 가능 (VLAN 태그 붙이지 않음)
ISL	. 시스코에서 만든 트렁킹 프로토콜 . 시스코 장비끼리만

▶ VTP (VLAN Trunking Protocol)

VTP란 하나의 스위치에 설정된 VLAN 번호와 이름을 다른 스위치에게 알려줄 때 사용하는 프로토콜이다.

- VTP 동작원리



. 수신한 정보의 VTP 설정 번호가 더 높으면 자신의 VLAN 정보를 새로운 정보로 대체한다.

. 수신한 정보의 VTP 설정 번호와 자신의 번호가 동일하면 수신한 정보를 무시한다.

. 수신한 정보의 설정 번호가 자신의 번호보다 낮으면 자신의 VTP 정보를 전송한다.

- VTP의 모드

모드	VLAN 생성, 변경,삭제	VTP 정보전송	VTP 정보중계	VTP 정보동기
서버(default)	0	0	0	0
트랜스패런트	0	X	0	X
클라이언트	X	0	0	0

vtp domain domain-name(★)

vtp password password

vtp mode [server | client | transparent]

show vtp counters

show vtp status

show vlan-switch brief

show vlan-switch id VLAN번호

- VTP 설정 삭제 방법

VLAN 이나 VTP 를 설정하면 Flash 메모리에 vlan.dat 파일로 저장된다.

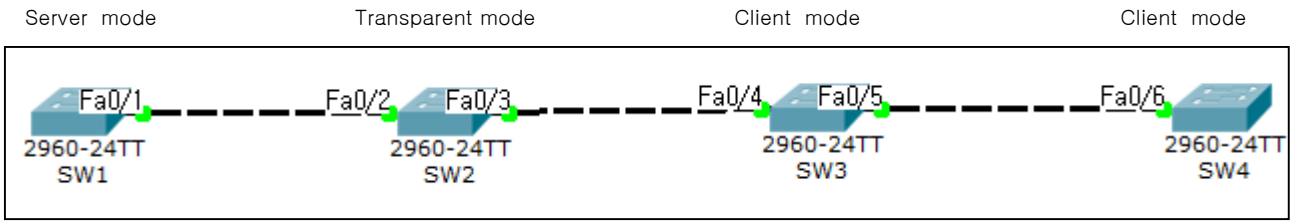
erase startup-config <-- NVRAM

delete vlan.dat

reload

<실습> VTP 연습

서버에서만 VLAN설정하도록 하며, 모든 스위치 포트에 트렁킹 설정을 한다.



스텝 1. trunk 구성

스텝 2. mode 구성 : vtp mode [server | client | transparent]

스텝 3. 도메인이름 : vtp domain itbank : SW1만

스텝 4. vlan 생성 : vlan 10, vlan 20 : SW1만

스텝 5. vtp password ciso

show running-config

show vtp status (★)

show vlan brief

show spanning-tree vlan 10

show interface trunk

show mac-address-table

▶ STP 와 RSTP

스패닝 트리 프로토콜은 장애 발생시 대체 경로가 동작하는 시간이 느리다.
그래서 STP를 보완한 RSTP(Rapid Spanning Tree Protocol)라는 프로토콜을 발표하였다. (STP의 단점인 convergence time을 획기적으로 단축시켜 준다.)

[STP]

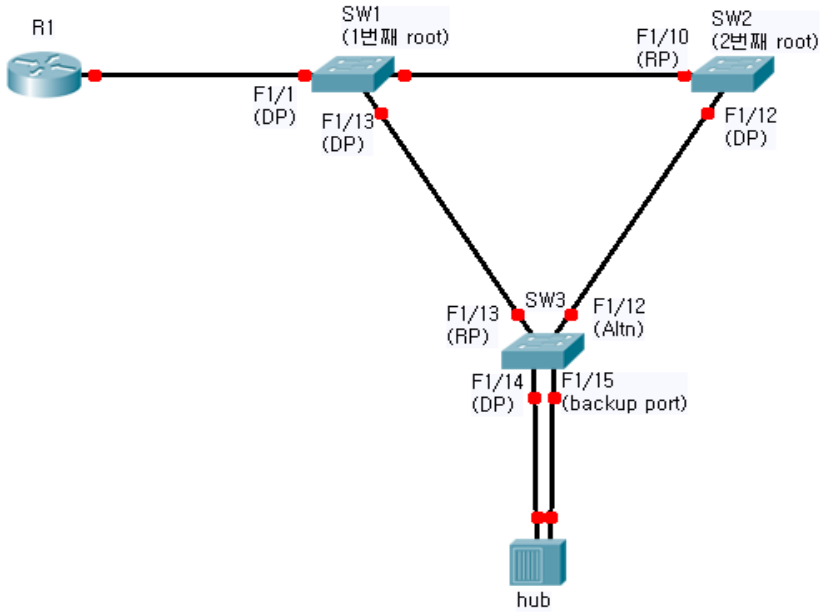
간접 링크 다운시 STP 에서는 대체 포트가 바로 전송 상태로 변경되지 않고 20초간 기다린다. 이후 다시 30초를 기다렸다가 전송 상태가 된다. 이렇게 기다리는 이유는 바로 전송 상태로 변경시 프레임 루프가 발생할 수 있기 때문이다.

[RSTP]

자신의 BPDU 정보가 우세하면 바로 자신이 지정 포트임을 주장하는 제안 BPDU 를 전송한다. 이것을 수신한 상대 포트는 이에 동의하여 자신은 루트포트가 되겠다는 동의 BPDU 를 보내면서 해당 포트를 바로 전송 상태로 변경한다.

동의 BPDU 를 수신한 지정 포트도 즉시 자신의 포트를 전송 상태로 변경한다. 결과적으로 거의 순간적으로 전송 상태로 변경된다.

- RSTP 포트 역할



. designated port
STP의 지정 포트와 동일하다.

. root port
STP의 루트 포트와 동일하다.

. alternate port
루트 포트가 다운되면 그 역할을 이어받는 포트를 말한다.
대체포트는 데이터 프레임을 송수신하지 않고, 차단 상태에 있다.

. backup port
지정포트가 다운되면 그 역할을 이어받는 포트를 말한다.
백업포트는 데이터 프레임을 송수신하지 않고, 차단 상태에 있다.
스위치가 자신이 보낸 BPDU를 다른 포트를 통하여 수신할 때 두 포트중 후순위의 포 트가 백업포트가 된다. 즉 허브와 복수 개의 링크로 접속 될 때 백업 포트가 생긴다.

. disabled
RSTP에서 역할이 없는 포트를 말한다.
셧다운된 포트 등 이 여기에 해당되다.

- RSTP 포트 상태

폐기 (discarding)
. STP 에서 blocking 상태와 동일
. BPDU 수신한다.
. 데이터 프레임을 송수신하지 않느다.

↓

학습 (learning)
. STP 에서 learning 상태와 동일
. 지정 포트라면 청취 상태에서 BPDU를 전송한다.
. mac 주소 테이블을 채운다.

↓

전송 (forwarding)
. STP 에서 forwarding 상태와 동일
. 데이터 프레임을 스위칭 한다.

- 포트 duplex에 따른 구분

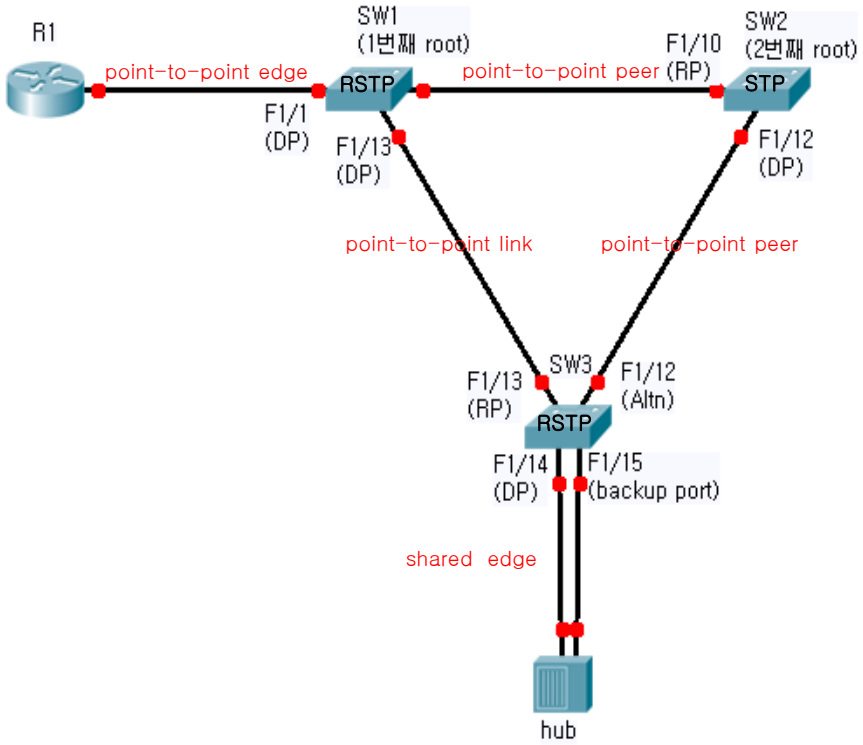
. point-to-point : full duplex로 동작하는 포트
. shared : half 로 동작하는 포트

- 상대 장비의 종류에 따른 구분

. link : 상대 장비도 RSTP로 동작하는 스위치와 연결된 포트
. edge : PC, 서버 등과 같이 스패닝 트리가 동작하지 않는 종단 장치와 연결된 포트
. peer : STP와 같이 RSTP가 아닌 프로토콜로 동작하는 스위치와 연결된 포트

STP로 동작하면서 full duplex인 링크는 point-to-point peer 로 표시된다.

RSTP 지정 포트는 edge port or point-to-point link 로 동작할 때에만 즉시 전송상태로 변경된다.



(config)# spanning-tree mode ?

. pvst Per-Vlan spanning tree mode
. rapid-pvst Per-Vlan rapid spanning tree mode

CDP

■ CDP(Cisco Discovery Protocol) 개요

. 2계층 프로토콜로서 연결된 CISCO 장비 간의 정보를 파악하기 위해 사용되는
CISCO 전용 프로토콜

. Multicast 주소를 사용해 네이버 정보 파악.

. 시스코 장비가 아닌 장비를 활성화 하면 기본적으로 비활성화 되어 있다.

. 같은 시스코 장비끼리 구성정보를 볼 수 있다.

. LLDP (Link Layer Discovery Protocol) : 다른 벤더 사의 장비를 찾는다. (표준)

```
config t
  cdp run
  no cdp run


config t
interface serial 0
  cdp enable
  no  cdp enable

show  cdp

show cdp neighbor
show cdp neighbor detail

show  cdp  entry  *

show cdp detail
show cdp trafic
show cdp interface
```

- show cdp neighbor detail 로 확인할 수 있는 정보

Device ID	장비의 hostname
Entry Address	Layer 3주소 정보
Platform	모델명
Capability	장비의 종류
Interface	연결 된 나의 인터페이스
Port ID	상대방의 인터페이스
Hold Time	홀드타임
Version	IOS정보

※ 참고

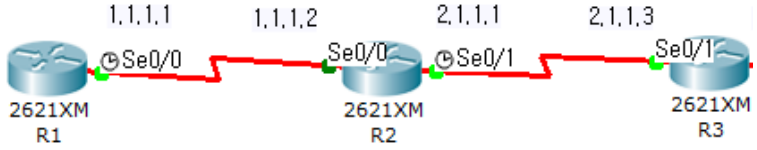
. Hold Time

호스트 이름 변경이나 구성 정보를 업데이트 했을 경우
180초까지만 저장하고 더 이상 CDP정보가 오지 않으면 정보를 버림

. Update Time

60초 마다 자신의 정보를 다른 장비에게 알림

< 실습 >



cdp run

clear cdp table

cdp run

clear cdp table

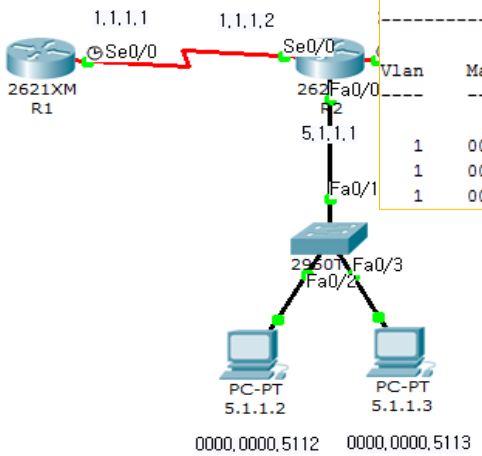
cdp run

clear cdp table

```
R1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2               Ser 0/0           156            R       C2600     Ser 0/0
```

```
R1#show cdp neighbors detail

Device ID: R2
Entry address(es):
  IP address : 1.1.1.2
Platform: cisco C2600, Capabilities: Router
Interface: Serial0/0, Port ID (outgoing port): Serial0/0
Holdtime: 155

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full
```

< 실습 >




```
SW1#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0000.0000.5112    DYNAMIC     Fa0/2
   1    0000.0000.5113    DYNAMIC     Fa0/3
   1    0001.63ca.3c01    DYNAMIC     Fa0/1
```

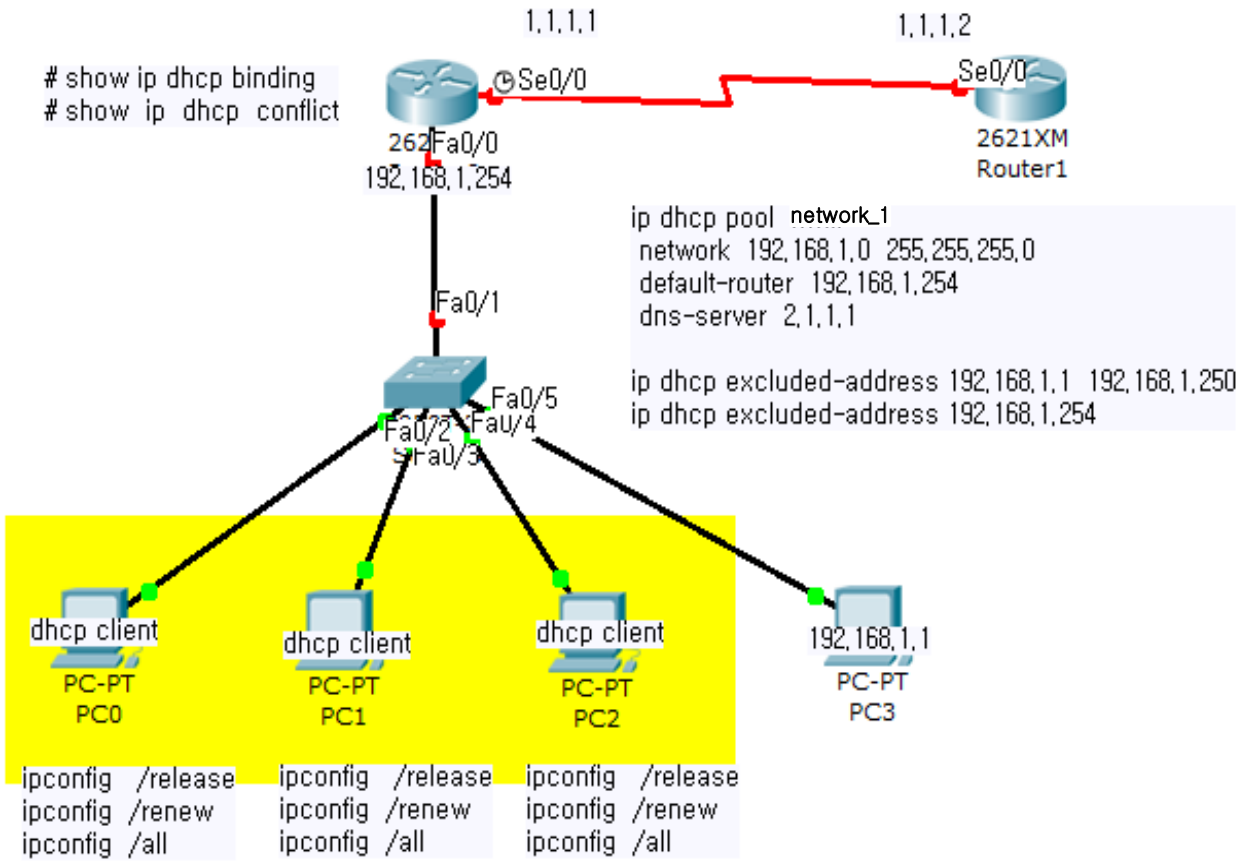
```
SW1#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
R2               Fas 0/1           154            R       C2600     Fas 0/0
```

```
SW1#show cdp neighbors detail

Device ID: R2
Entry address(es):
  IP address : 5.1.1.1
Platform: cisco C2600, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0
Holdtime: 142

Version :
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-I-M), Version 12.2(28), RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

advertisement version: 2
Duplex: full
```

DHCP

■ DHCP Server

Discover -> Offer -> Request -> Ack = broadcast (255.255.255.255)



ACL
(Access Control List)

■ 엑세스 리스트(Access List, ACL)

- 엑세스 리스트 제어방법에 따른 분류

Standard Access List	출입 통제 시 출발지 주소만을 참고
Extended Access List	출발지, 목적지, 프로토콜, 사용 포트 번호 참고

- 엑세스 리스트 숫자 와 이름에 따른 분류

Standard Access List	1-99, 1300~1999
Extended Access List	100-199, 2000~2699
Named Access List	이름 사용

- access-list 문 정의

. access-list 는 Interface별, Direction(in,out)별, Protocol별로 각각 하나씩 적용 가능

. 액세스 리스트는 명시한 순서대로 윗줄부터 순차적으로 수행한다

. 액세스 리스트는 암묵적으로 deny any 이 마지막으로 적용된다.

. 따라서 해당하지 않는 주소를 허용하려면 permit any를 명시해주어야 한다.

- access-list 문 갱신

. 엑세스리스트는 추가 될 경우 맨 마지막 라인에 추가 된다.

. 숫자 형태의 액세스리스트는 삭제한 액세스리스트 다음 모든 것이 삭제되나,
named 액세스리스트는 부분추가 삭제가 가능다.

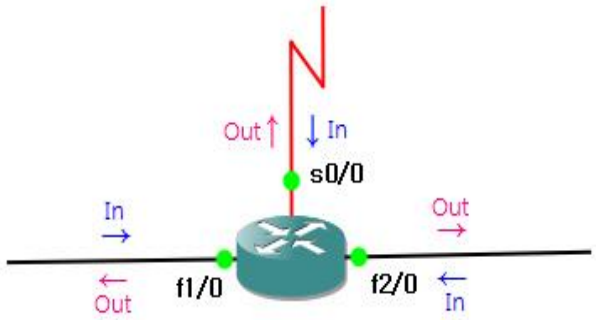
. Wildcard Mask 는 생략이 가능하지만,
생략이 가능한 경우는 0.0.0.0 인 경우다. (host 특정주소)

- access-list 문 interface 에 적용

. 인터페이스에 대한 엑세스 리스트의 정의가 되어 있지 않은 경우 결과는 permit any가 된다.

. Interface 의 기본값은 out 이다.

▶ 라우터 IN 과 OUT의 구분



※ Subnet Mask 와 Wildcard Mask 비고

. SubNet Mask -> 0 : 호스트 자리
-> 1 : 네트워크 자리

. Wildcard Mask -> 0 : 무엇이 오든 검사해라
-> 1 : 무엇이 오든 무시해라

<연습> 192.168.2.1 0.0.0.255
<연습> 192.168.2.2 0.0.0.255
<연습> 192.168.2.0 0.0.0.255

<연습> 192.168.10.4 0.0.0.3

▶ Standard Access-list

- 스텐더드 액세스 리스트 명령 형식

Router(config)#access-list access-list-number {permit | deny} {source-wildcard | any}
액세스 리스트 번호 (0~99)또는(1300~1999) 허용 또는 거부 와일드카드 마스크 또는 모든주소

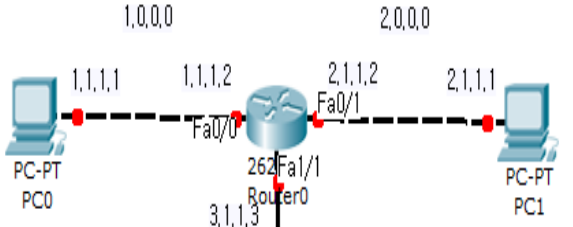
Router(config-if)#ip access-group access-list-number {in | out}
엑세스 리스트 번호 in 또는 out (디폴트값 out)

<주의>

access-list 1 deny 0.0.0.0 255.255.255.255
access-list 1 deny any

access-list 1 deny 1.1.1.1 0.0.0.0
access-list 1 deny host 1.1.1.1

[실습]




```
access-list 1 deny 3.1.1.1 0.0.0.0
access-list 1 permit 0.0.0.0 255.255.255.255

int f0/0
ip access-group 1 out
-------------------------------------
ip access-list standard cisco
deny 3.1.1.1 0.0.0.0
permit 0.0.0.0 255.255.255.255

int f0/0
ip access-group cisco out
```

```
access-list 2 deny 3.1.1.2 0.0.0.0
access-list 2 permit 0.0.0.0 255.255.255.255

int f0/1
ip access-group 2 out
-------------------------------------
ip access-list standard itwill
deny 3.1.1.2 0.0.0.0
permit 0.0.0.0 255.255.255.255

int f0/0
ip access-group itwill out
```

```
# show   access-list
# show  ip   access-lists
# show  ip  interface  [interface]   인터페이스에 액세스리스트 설정 확인
```

※ telnet 접근 제한

```
line  vty  0  4
 login
 password  cisco
 access-class   1   in   <---3.1.1.1 만  접속 불가
```

▶ Extended Access-list

- 스탠더드 액세스 리스트는 출발지 주소(Source Address)만으로 제어하는 반면, 익스텐디스 액세스리 리스트는 출발지 주소, 목적지 주소(Destination Address)까지 제어할 수 있다.

- 스탠더드 액세스 리스트는 전체 TCP/IP에 대한 제어만을 하는 반면, 익스텐디드 엑세스 리스트는 TCP, IP, udp, icmp, ftp 등 특정 프토토콜까지 지정하여 제어할 수 있다.

- 스탠더드 액세스 리스트는 (1~99), (1300~1999) 사용하고, 익스텐디드 액세스 리스트는 (100~199), (2000~2699) 사용한다.

- Well Known Port

20 (TCP)	File Transfer Protocol 데이타
21 (TCP)	FTP Control Data
23 (TCP)	Telnet
25 (TCP)	SMTP (Simple Mail Transport Protocol)
53 (TCP, UDP)	Domain Name System (DNS)
69 (UDP)	Trivial File Transfer Protocol(TFTP)
80 (TCP)	HyperText Transfer Protocol (HTTP)

- 익스텐디드 액세스 리스트 명령 형식

```
Router(config)#access-list access-list-number {permit | deny}
                           액세스 리스트 번호     허용 또는 거부
                        (100~199)또는(2000~2699)

protocol source source-wildcard [ operator port ]
프로토콜  출발지  출발지 와일드카드마스크
  지정     주소

destination destication-wildcard [ operator port ]  [ established ] [ log ]
도착지 주소  도착지 와일드 카드마스크



Router(config-if)#ip access-group access-list-number  { in | out }
                                  액세스 리스트 번호     in 또는 out
```

※ 암묵적으로 존재 :

access-list 100 deny ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
access-list 100 deny ip(tcp|udp|icmp) any any

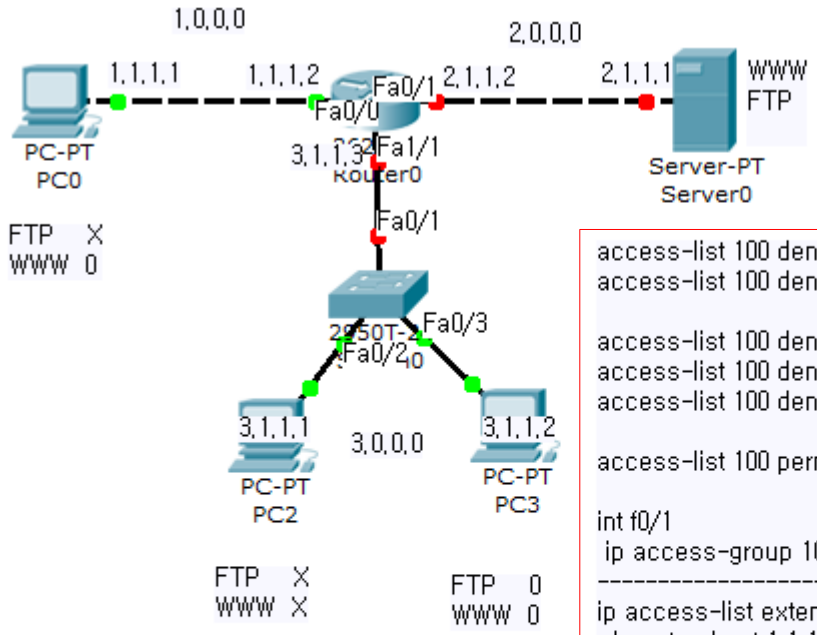
- protocol

IP 패킷에 실려서 전송될수 있는 상위계층 프로토콜을 필터링하며, ICMP, TCP, UDP 등을 지정한다.

- operator

gt (greater than)	~ 보다 크다.
lt (less than)	~ 보다 작다.
eq (equal)	~ 와 같다.
neq (not equal)	~ 와 같지 않다.

[실습]

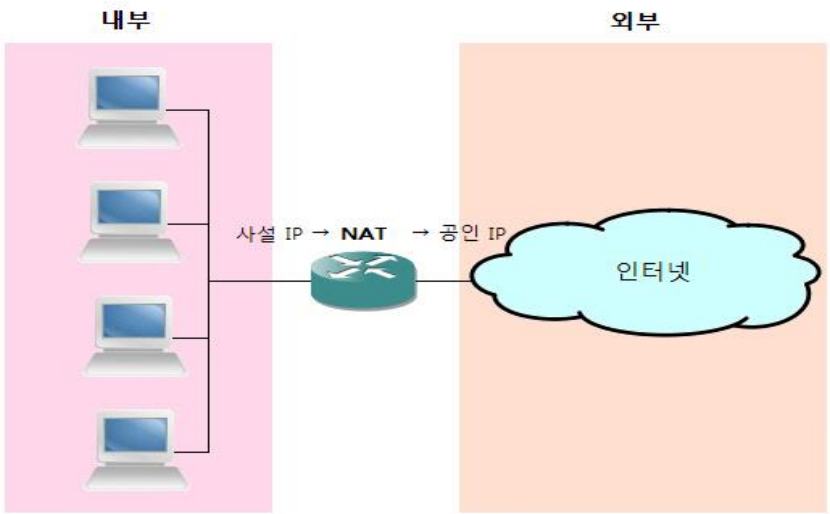



```
access-list 100 deny tcp host 1.1.1.1 host 2.1.1.1 eq 21
access-list 100 deny tcp host 1.1.1.1 host 2.1.1.1 eq 20

access-list 100 deny tcp host 3.1.1.1 host 2.1.1.1 eq 21
access-list 100 deny tcp host 3.1.1.1 host 2.1.1.1 eq 20
access-list 100 deny tcp host 3.1.1.1 host 2.1.1.1 eq 80

access-list 100 permit ip any any

int f0/1
 ip access-group 100 out
-----------------------------------------------
ip access-list extended cisco
 deny tcp host 1.1.1.1 host 2.1.1.1 eq 21
 deny tcp host 1.1.1.1 host 2.1.1.1 eq 20

 deny tcp host 3.1.1.1 host 2.1.1.1 eq 21
 deny tcp host 3.1.1.1 host 2.1.1.1 eq 20
 deny tcp host 3.1.1.1 host 2.1.1.1 eq 80

 permit ip any any

int f0/1
 ip access-group cisco out
```

access-list 100 deny icmp any host 2.1.1.1 echo

NAT

■ NAT(Network Address Translation)



Inside Local 주소 → 변환(NAT) → Inside Global 주소

- NAT의 사용이유는 대부분 내부 네트워크에서는 사설 IP를 사용하다가 공인 IP로 변경하여 사용하기 위해서 이다
- Inside Local주소 : 내부 네트워크에서 사용하는 비공인 주소 (예 : 사설 IP)
- Inside Global주소 : 외부 네트워크로 나갈 때 변환되어 나가는 주소(예 : 공인 IP)
- 어떠한 네트워크의 IP 주소가 다른 네트워크로 넘어갈 때 다른 IP로 변환이 되는 것을 말함

▶ NAT 운형

1. IP 변환에 사용 할 전역 주소 풀을 설정

ip nat pool *name* *start-ip* *end-ip* {netmask *Netmask* | Prefix-length *Prefix-length* }

임의지정 / 할당할 공인 IP의 시작과 끝 IP / 넷마스크 / 길이로 지정 (예 : /24)

2. 내부에서 IP 변환을 허용 할 주소를 Standard Access-list 정의한다.

access-list *number* permit *source-address [Wildcard-mask]*

번호지정 / 출발지 주소 / 와일드카드마스크

3. 동적 변환을 수립하기 위한 NAT 설정을 한다.

ip nat inside source list *Access-list-number* pool *name* overload

액세스 리스트 번호 / 지정한 이름

4. 각 인터페이스로 이동 후 내부와 외부를 각각 설정한다.

ip nat inside

NAT를 통해 들어가는 인터페이스

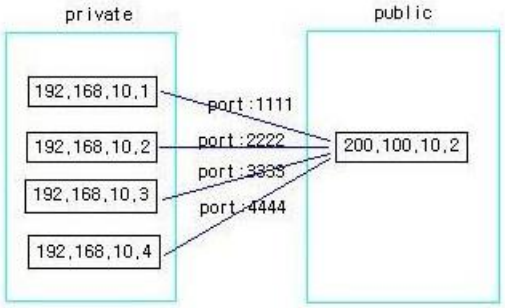
ip nat outside

NAT를 통해 나가는 인터페이스

▶ NAT 방식

☞ PAT(Port Address Translation)

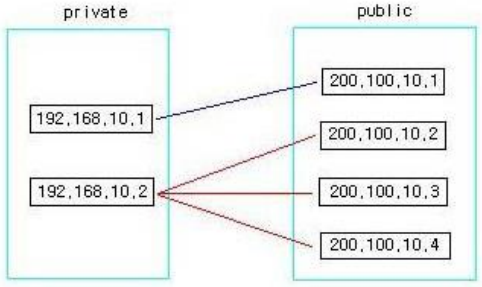
포트 변환을 통해서 NAT를 실행한다. Static NAT나 Dynamic NAT의 경우 사용할 수 있는 공인IP보다 사설IP의 수가 많다면 모자라는만큼 외부로 나갈 수 없는 사설IP가 많아진다. 하지만 PAT는 포트 변환을 하기때문에 공인IP가 하나만 있어도 많은 수의 사설IP가 외부로 나갈 수 있다.



위 경우 사용할 수 있는 공인IP는 한 개이지만 내부의 사설IP들은 각각 포트를 달리함으로써 개별적으로 외부로 나갈 수 있게 된다.

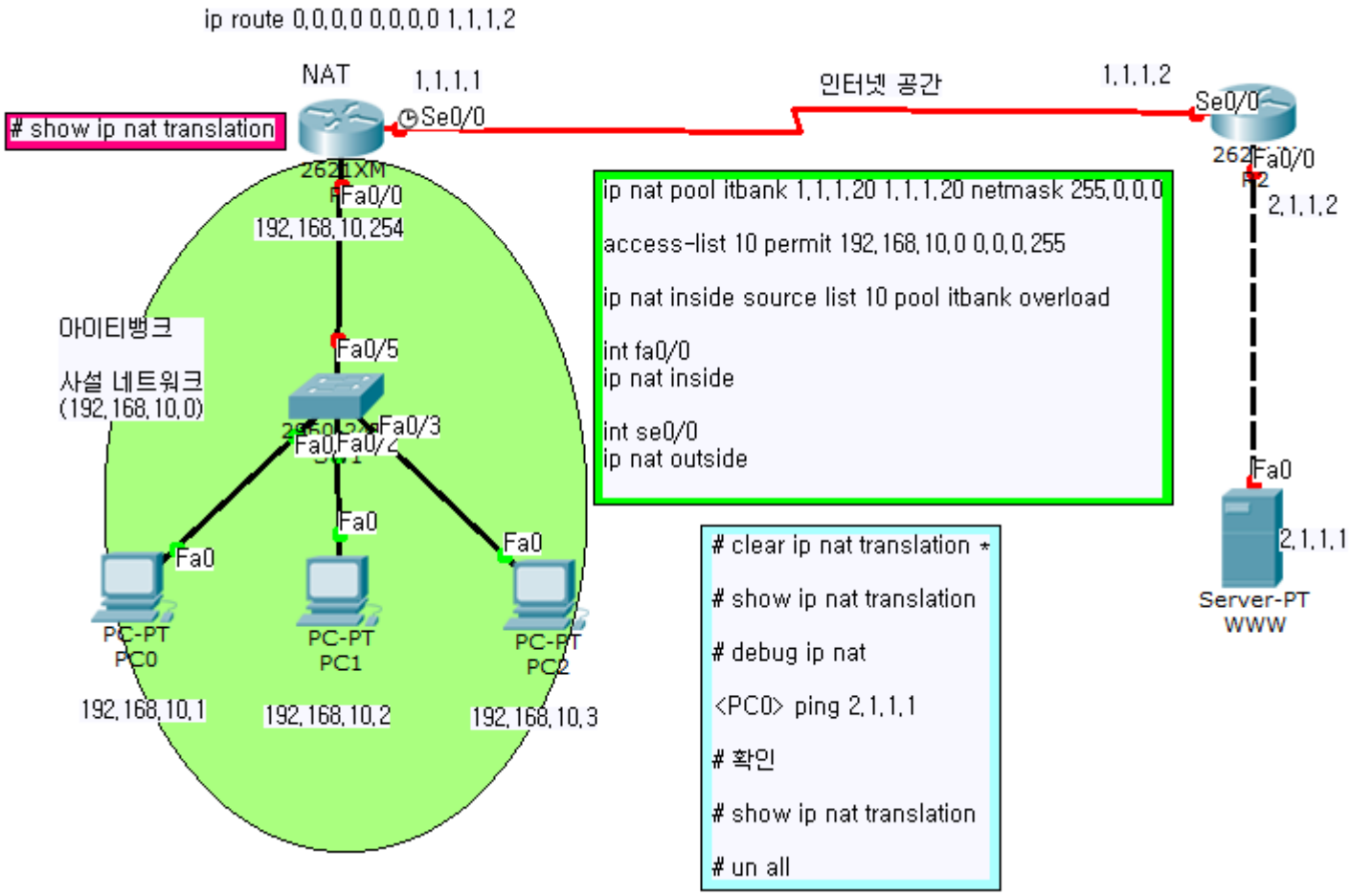
☞ Static NAT

특정 사설IP가 특정 공인IP만 사용하도록 관리자가 미리 정해놓는 방식, 외부로 서비스하는 서버는 대부분 Static NAT방식을 사용한다.

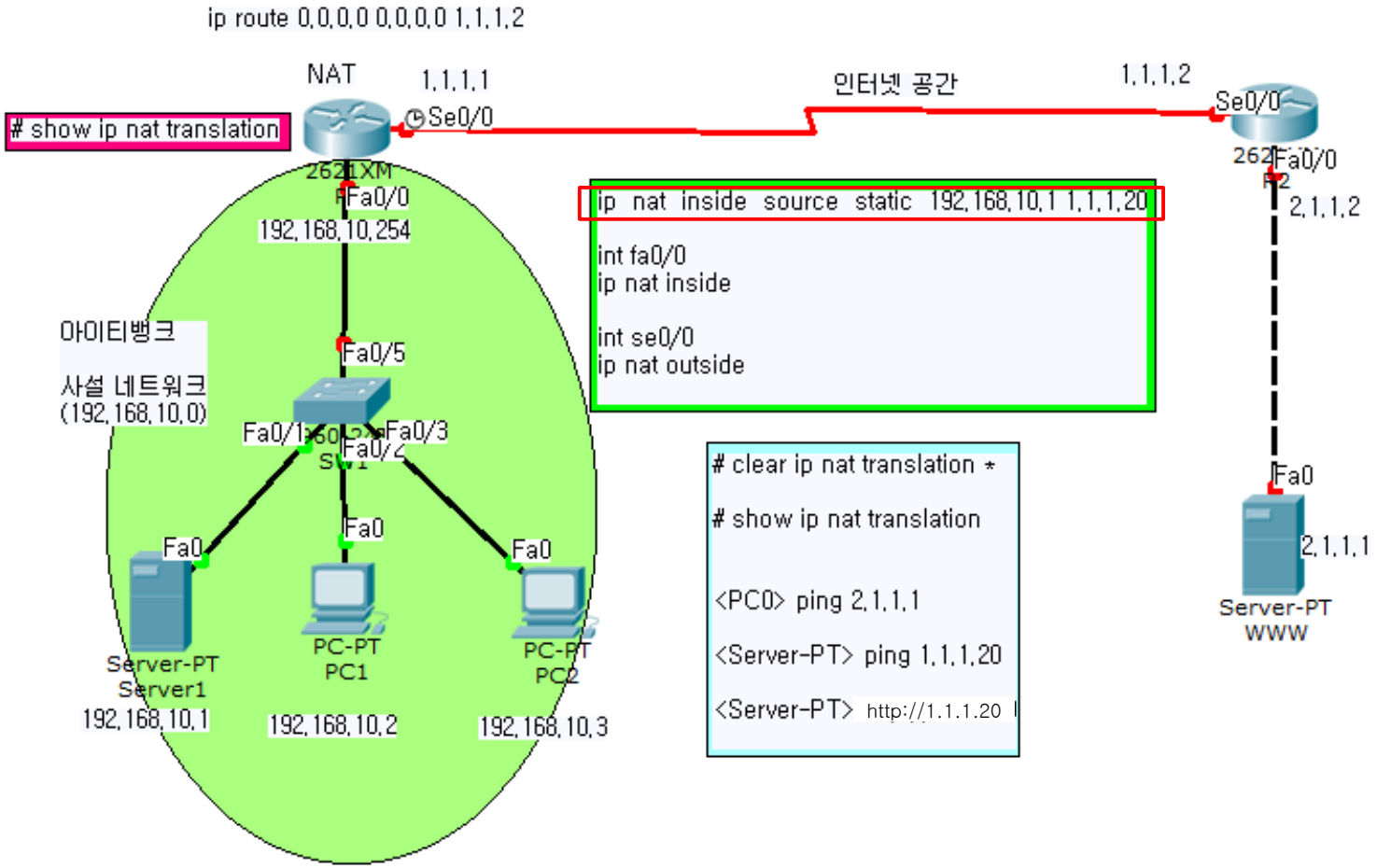


위에서 192.168.10.1은 200.100.10.1로만 무조건 매핑이 된다. 192.168.10.2는 나머지 200.100.10.2 ~ 4 중에서 하나를 사용하게 된다.

<실습> PAT


ip route 0.0.0.0 0.0.0.0 1.1.1.2
NAT
1.1.1.1
Se0/0
show ip nat translation
인터넷 공간
1.1.1.2
Se0/0
Fa0/0
2.1.1.2
Fa0
2.1.1.1
Server-PT
WWW
Fa0/0
192.168.10.254
아이티뱅크
사설 네트워크
(192.168.10.0)
Fa0/5
Fa0/3
Fa0
Fa0
Fa0
PC-PT
PC0
PC-PT
PC1
PC-PT
PC2
192.168.10.1
192.168.10.2
192.168.10.3
ip nat pool itbank 1.1.1.20 1.1.1.20 netmask 255.0.0.0
access-list 10 permit 192.168.10.0 0.0.0.255
ip nat inside source list 10 pool itbank overload
int fa0/0
ip nat inside
int se0/0
ip nat outside
clear ip nat translation *
show ip nat translation
debug ip nat
<PC0> ping 2.1.1.1
확인
show ip nat translation
un all

<실습> Static NAT



IPV6

■ IPV6 주소표기

1. 주소표기

- 16진수 콜론 표기법
- 128비트를 16비트씩 8개의 필드로 나누어 콜론(:)으로 구분

예> BEAF:2002:0221:F207:0000:0000:FFFF:4002

16bit:16bit:16bit:16bit:16bit:16bit:16bit:16bit = 128bit

네트워크 ID　　인터페이스 ID

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
F E D C B A 9 8 7 6 5 4 3 2 1 0

1 1 1 1　1 1 1 1　1 1 1 1　1 1 1 1
8 4 2 1　8 4 2 1　8 4 2 1　8 4 2 1

1 1 1 1　1 1 1 1　1 1 1 1　1 1 1 1
F　　F　　F　　F

2. 주소 프리픽스의 표현 방법

IPV6의 주소 뒤에 "/" 를 표기하고 프리픽스의 길이를 10진수의 숫자로 표기

예> BEAF:ABCD:0:FFFF::/64

3. "0" 의 값을 포함하는 주소에 대한 주소 생략법

- 상위 연속적 영일 경우 이를 생략 (중간이나 하위 영은 생략 불가)

Unabbreviated

FDEC : BA98 : 0074 : 3210 : 000F : BBFF : 0000 : FFFF

FDEC : BA98 : 74 : 3210 : F : BBFF : 0 : FFFF

Abbreviated

- 연속적인 영을 한 번 이상 생략 불가
  (0 으로만 나타난 연속된 필드는 0 를 모두 삭제하고 2개의 콜론(::)만으로 나타냄)

BEAF:0:0:0:0:ABCD:0:FFFF ==> BEAF::ABCD:0:FFFF

※ 주의

0000:0000:0000:0a2d:41c3:0000:0000:0000 ==> ::a2d:41c3:: 로 생략시 구별불가

. 0:0:a2d:41c3:0:0:0:0
. 0:0:0:a2d:41c3:0:0:0
. 0:0:0:0:a2d:41c3:0:0

■ IPV6 종류

▶ global unicast 주소 = 001/3 으로 시작하면 공인주소임 [0010(2), 0011(3)]

▶ site local = FEC0::/10 – FEFF::/10

▶ link local = FE80::/10 – FEBF::/10

▶ Multicast = FFxx::/8 로 시작하며, 브로드캐스트 주소는 사용하지 않는다.

▶ Anycast (1:nearest)

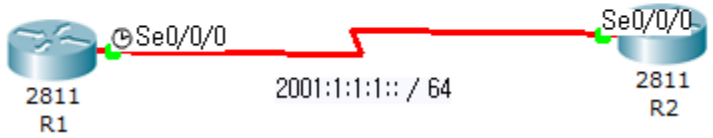
. 복수개의 라우터에 동일한 주소를 부여하는 것을 애니캐스트 주소라고 한다.
. 애니캐스트 주소를 부여할 때는 마지막에 anycast 라는 옵션을 사용한다.

▶ loopback = ::1/128

▶ Unspecified = : :

<연습>

```
show ipv6 route
show ipv6 interface brief
show ipv6 int s0/0/0
```



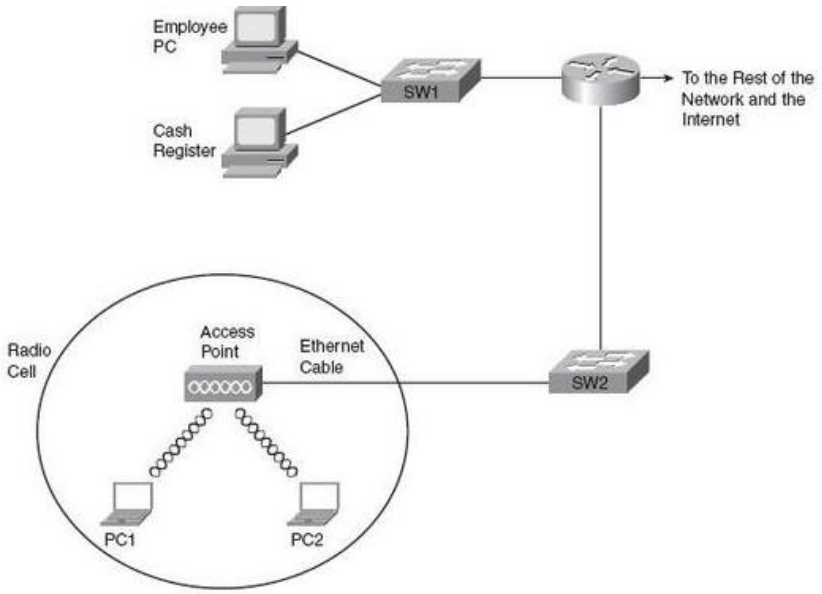

```
ipv6 unicast-routing

interface s0/0/0
  ipv6 enable
  ipv6 address 2001:1:1:1::1/64
  no shutdown
```

```
ipv6 unicast-routing

interface s0/0/0
  ipv6 enable
  ipv6 address 2001:1:1:1::2/64
  no shutdown
```

■ WLAN(Wireless LAN) 무선랜

- LAN과의 비교

Wireless LAN	Wired LAN
Radio Wave 로 통신한다.	Cable 로 전기 신호를 보내 통신한다.
HDX(half duplex), 송수신 동시에 불가능	FDX(full duplex)
CSMA/CA 알고리즘 사용	CSMA/CD 알고리즘 사용
(carrier sense multiple access with collision avoidance)	(carrier sense multiple access with collision detection)
AP(access point)가 필요	스위치에 연결



◇ CSMA/CA 알고리즘 요약 ◇

- 다른 장치가 같은 공간에서 전송매체(같은 대역의 라디오 전파)를 사용하는지 본다,(Listen)

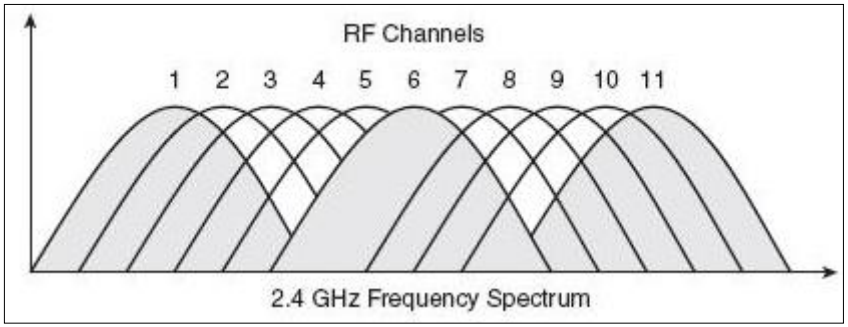
- 없으면 프레임을 보내기 전에 랜덤 시간을 정한다. - 현재 전파가 없다고 해서 모든 장치가 동시에 전파를 보내면 충돌이 일어나니 이를 줄이기 위해 랜덤 시간을 정하고 그 후에 보냄

- 랜덤 시간이 지나면 다시 전송매체가 사용중인지 보고, 사용중이 아니면 프레임을 보낸다. 만약 매체가 사용중이면 다시 1번

- 모든 프레임을 보내고 Acknowledgment 를 기다린다.

- 만약 Acknowledgment 가 정해진 시간 안에 안오면 1번으로 돌아가 다시 프레임을 보낸다.

- Acknowledgment 를 받으면 전송 완료.

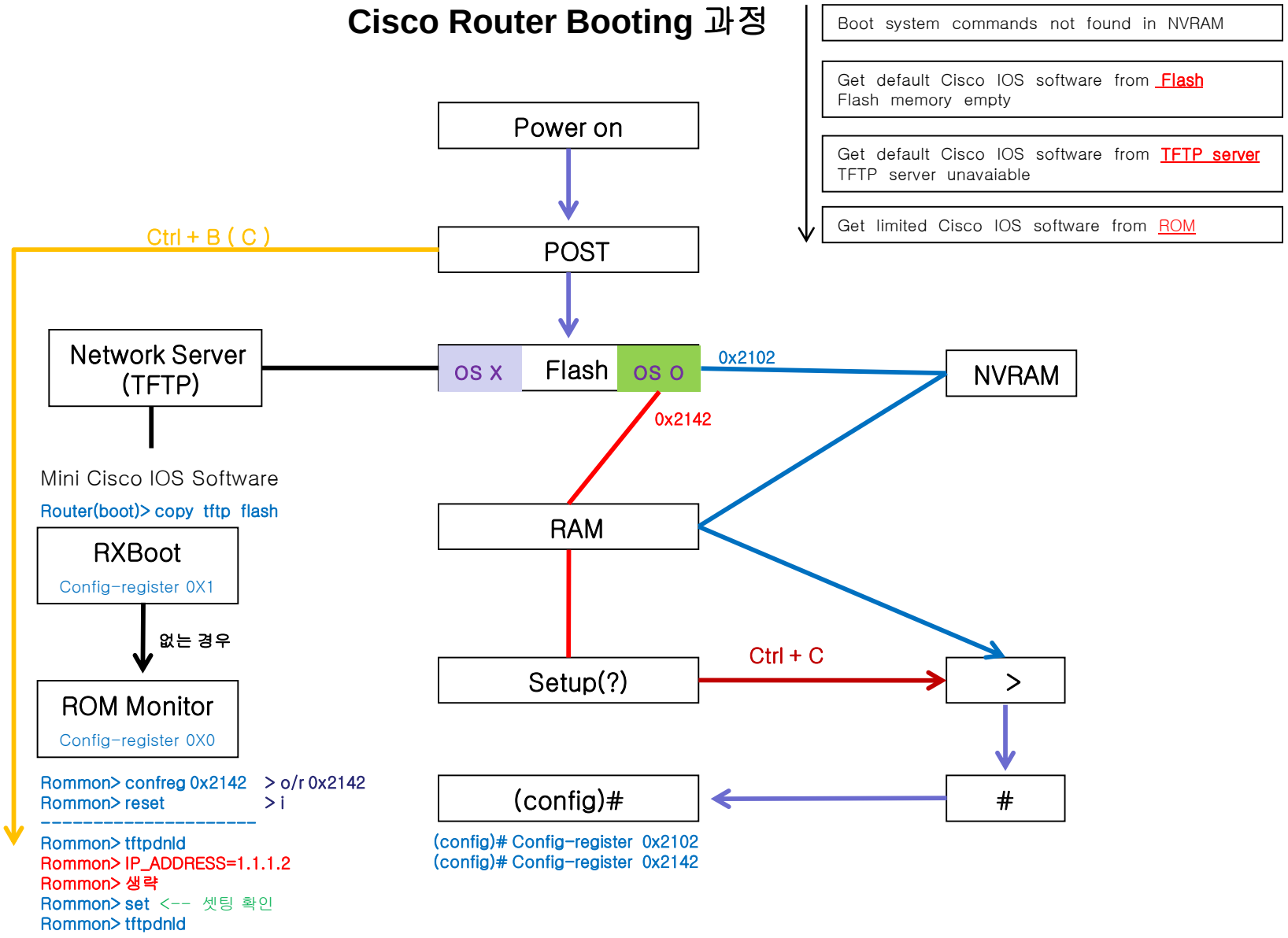


★ 이중 1, 6, 11 채널이 거의 간섭이 없다. (따라서 같은 공간의 WLAN에서 동시사용 가능) 따라서 ESS WLAN 을 구성 할 때 쓸 수 있다.

부록

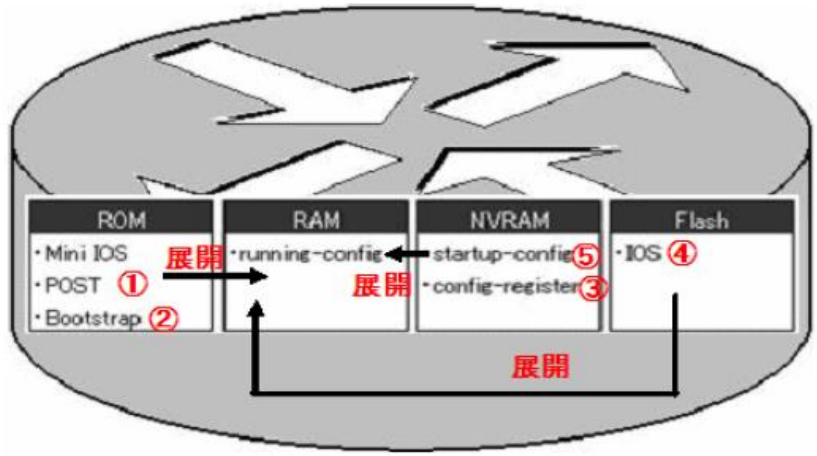
Router 부팅 / 백업 / 복구

Cisco Router Booting 과정



▶ CISCO 라우터 구성요소

Cisco 라우터는 ROM, RAM, NVRAM, Flash 4종류의 메모리를 내장하고 있다.



메모리	특징
ROM	읽기 전용, 전원을 내려도 지워지지 않는다.
RAM	읽고 쓰기 가능, 전원을 내리면 내용이 삭제된다.
NVRAM	읽고 쓰기 가능, 전원을 내려도 지워지지 않는다.
Flash	읽고 쓰기 가능, 전원을 내려도 지워지지 않는다. IOS가 담겨 있다

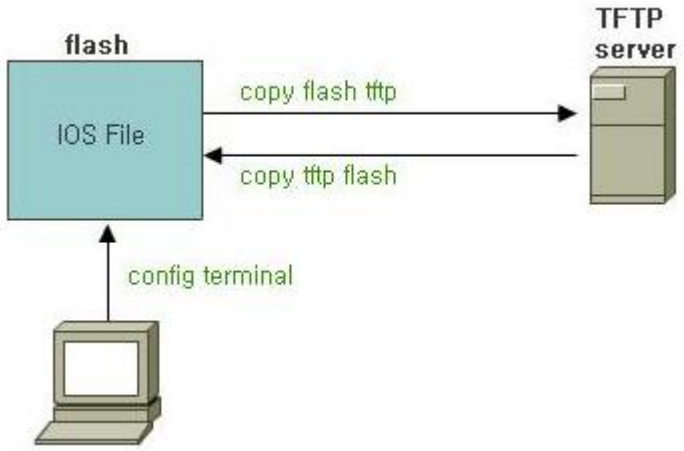
▶ 라우터 정보 확인 및 저장

. RAM 정보 확인 : show running-config

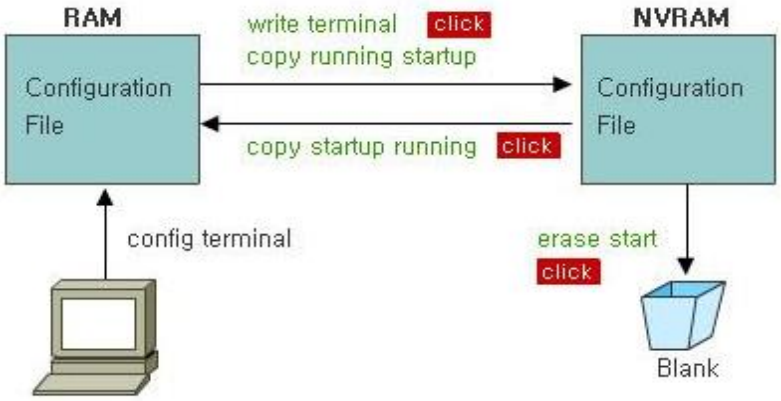
. NVRAM 정보 확인 : show startup-config

. Flash 정보 확인 : show flash

- IOS 백업 및 업그레이드

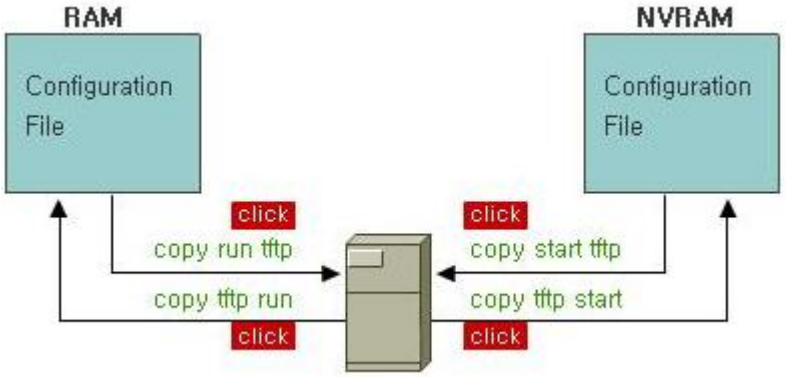


- RAM 파일 과 NVRAM 파일 교환



(1) RAM에 상주해 있는 Running Configuration 파일을 NVRAM의 startup configuration 파일로 저장
(2) Startup 파일을 Running 파일로 변환
(3) Startup 파일 지우기

- 백업



▶ 라우터 패스워드 복구 절차

스텝 1. 부팅시 Ctrl + Break 를 통해 rommon 모드 진입후 레지스터를 0x2142로 설정

```
rommon> confreg 0x2142
rommon> reset
```

or

```
> o/r 0x2142
> i
```

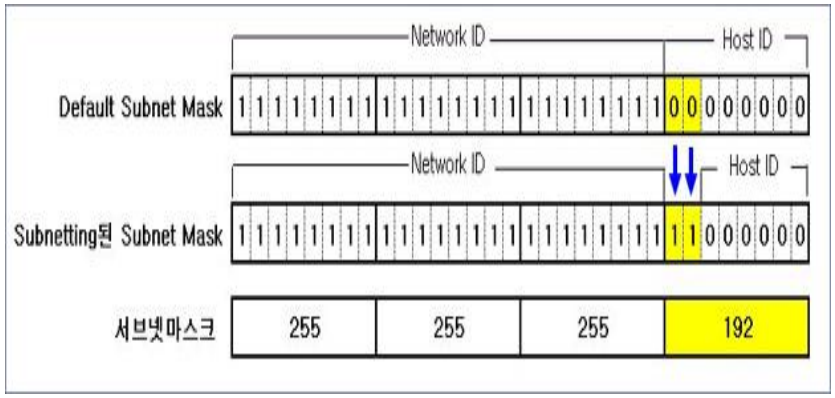
스텝 2. enable로 privilege모드 진입

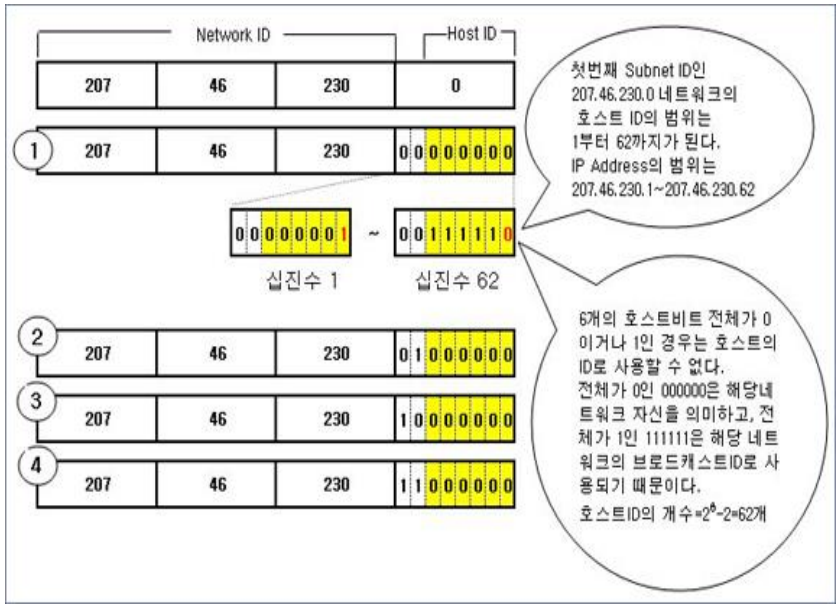
```
enable  password  cisco

config-register 0x2102

copy  run   sta
```

▶ 라우터 IOS 복구 절차

```
rommon> tftpdnld

rommon> IP_ADDRESS=1.1.1.2

rommon> IP_SUBNET_MASK= 255.0.0.0

rommon> DEFAULT_GATEWAY=1.1.1.2

rommon> TFTP_SERVER= 1.1.1.1

rommon> TFTP_FILE= R1_IOS

rommon> tftpdnld
```

■ Subnetting





(1) 회사에서 필요로 하는 네트워크의 수 결정

(2) 필요한 네트워크ID를 만들기 위해 전환할 bit수의 결정

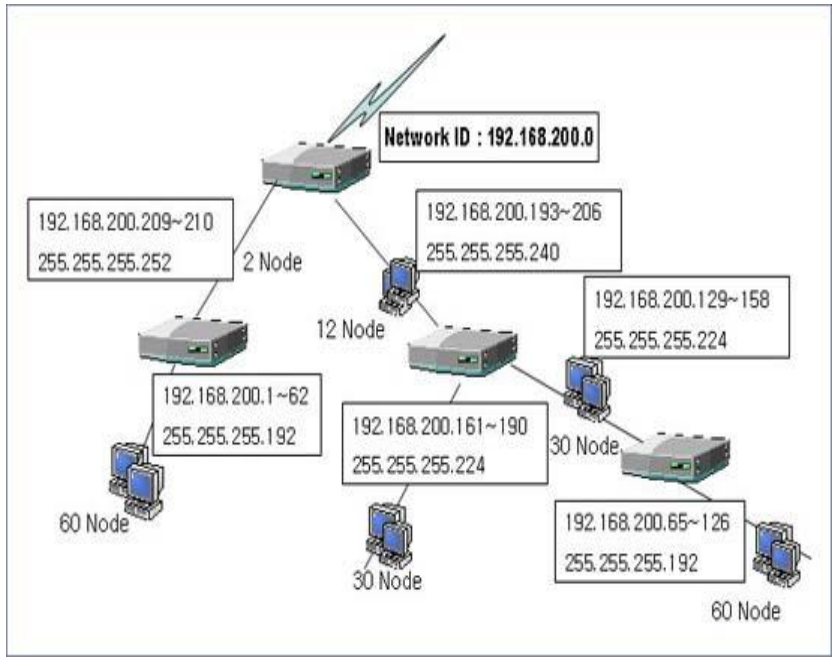
(3) 서브넷 마스크(User defined Subnet Mask) 계산

(4) 서브넷 ID 계산

(5) 서브넷별 호스트ID의 범위 계산

CIDR(ClasslessInter Domain Routing) = Subnetting + Suppernetting
CIDR 표기법: 207.46.230.2/26

■ VLSM (Variable Length Subnet Mask)



(1) 60개 호스트를 지원하기 위한 서브네팅

- 60개의 호스트를 지원하기 위해 필요한 호스트 비트수 = 6개 (2^6-2=62)
- 서브넷마스크는 11111111.11111111.11111111.11000000(남은 2비트로 서브네팅)
- 호스트ID의 범위 2개 : 192.168.200.1~62, 192.168.200.65~126 /26

(2) 30개 호스트를 지원하기 위한 서브네팅

- 30개의 호스트를 지원하기 위해 필요한 호스트 비트수 = 5개 (2^5-2=30)
- 서브넷마스크는 11111111.11111111.11111111.11100000 (남은 3비트로 서브네팅)
- 호스트ID의 범위 2개 : 192.168.200.129~158,192.168.200.161~190 /27
  (1~127까지는 이미 앞의 네트워크에서 사용되었음을 유의한다.)

(3) 12개 호스트를 지원하기 위한 서브네팅

- 12개의 호스트를 지원하기 위해 필요한 호스트 비트수 = 4개 (2^4-2=14)
- 서브넷마스크는 11111111.11111111.11111111.**1111**0000 (남은 4비트로 서브네팅)
- 호스트ID의 범위 1개를 구하면 -> 192.168.200.193~206 /28
  (1~191까지는 이미 다른 네트워크에서 사용되었음을 유의한다.)

(4) 2개 호스트를 지원하기 위한 서브네팅

- 2개의 호스트를 지원하기 위해 필요한 호스트 비트수 = 2개 (2^2-2=2)
- 서브넷마스크는 11111111.11111111.11111111.**111111**00 (남은 6비트로 서브네팅)
- 호스트ID의 범위 1개를 구하면 -> 192.168.200.209~210 /30
  (1~207까지는 이미 다른 네트워크에서 사용되었음을 유의한다.)

<연습>

문제> 192.168.1.0 255.255.255.0 Network에서 1개 부서에는 100Host를 2개의 부서에는 각각50Host를 만족하는 VLSM을 하시오

1Network 100Host (2^7=128)

1	0000000	255.255.255.128 /25
0	0000000 ~ 0 1111111	0~127
1	0000000 ~ 1 1111111	128~255

2Network 50Host (2^6=64)

11	000000	255.255.255.192 /26
10	000000 ~ 10 111111	128 ~ 191
11	000000 ~ 11 111111	192 ~ 255

<연습>

문제> 210.16.199.0 255.255.255.0을 사용하는 ITSTAR에서 마케팅 부서에는 100Host 강의장 1,2에는 30Host를 강사부와 관리부에는 10 Host를 경리부에는 5Host를 만족하는 VLSM을 하시오

마케팅부서 100Host (2^7=128)

1	0000000	255.255.255.128
0	0000000 ~ 0 1111111	0~127
1	0000000 ~ 1 1111111	128~255

1,2 강의장 30Host (2^5=32)

111	00000	255.255.255.224
100	00000 ~ 100 11111	128~159
101	00000 ~ 101 11111	160~191

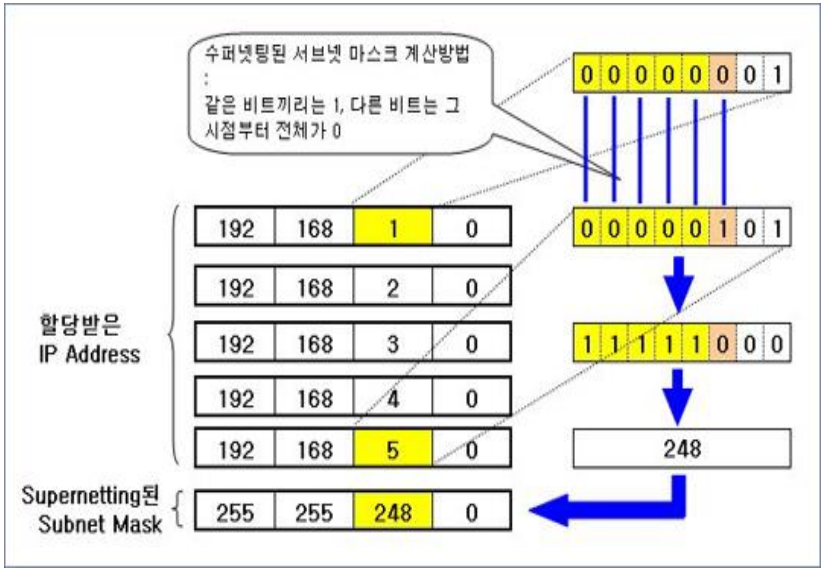
강사부,관리부 10Host (2^4=16)

1100	0000	255.255.255.240
1100	0000 ~ 1100 1111	192~207
1101	0000 ~ 1101 1111	208~223

경리부 5Host (2^3=8)

11111	000	255.255.255.248
11100	000 ~ 11100 111	224~231
11101	000 ~ 11101 111	232~239

■ Suppernetting = Aggregation = Summarization=축약



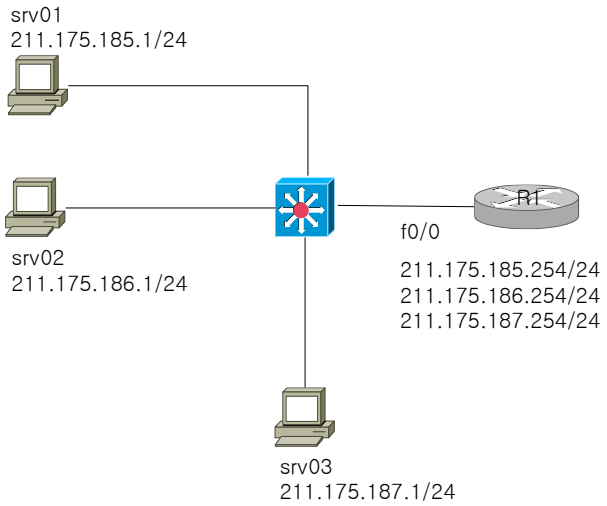
<연습>

network ID	host ID
211.175.10111001	(185).0
211.175.10111010	(186).0
211.175.10111011	(187).0

network 주소 : 211.175.184.0/22

subnet mask : 255.255.252.0

<연습> 211.175.185.0~211.175.187.0 (Suppernetting X)



<연습> 211.175.185.0~211.175.187.0 (Suppernetting 0)