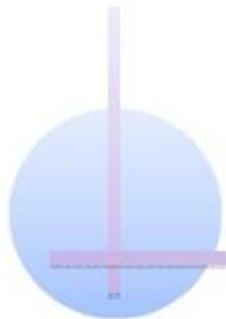




목차

- Chapter 01 TCP/IP Network 기초
- Chapter 02 Cisco 장비와 IOS 기초
- Chapter 03 Switching
- Chapter 04 VLAN
- Chapter 05 Routing
- Chapter 06 ACL과 NAT
- Chapter 07 WAN
- Chapter 08 IPv6
- Chapter 09 BGP

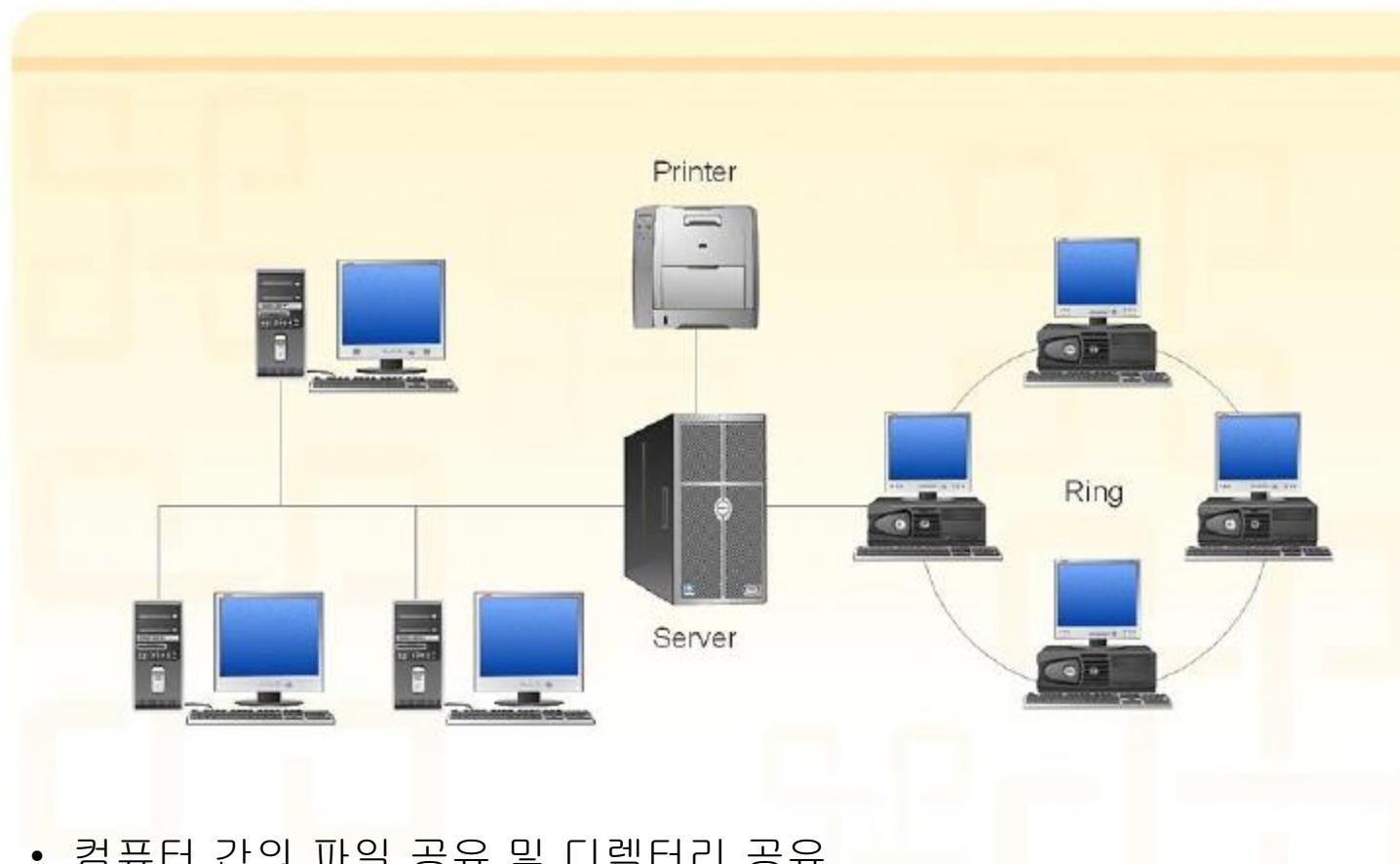


Chapter 01:

TCP/IP Network 기초



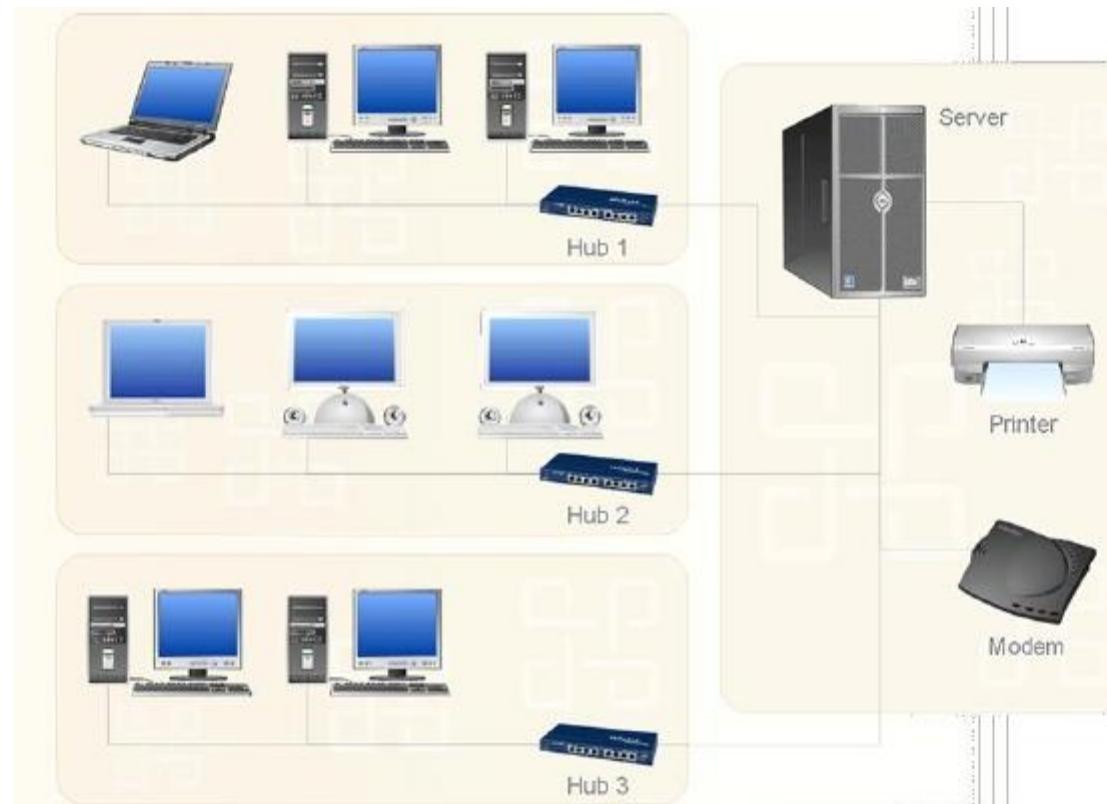
Computer Network 란



- 컴퓨터 간의 파일 공유 및 디렉터리 공유
- 전자 메일 등 커뮤니케이션 지원
- 전자 뉴스나 WWW에 의한 정보 공유



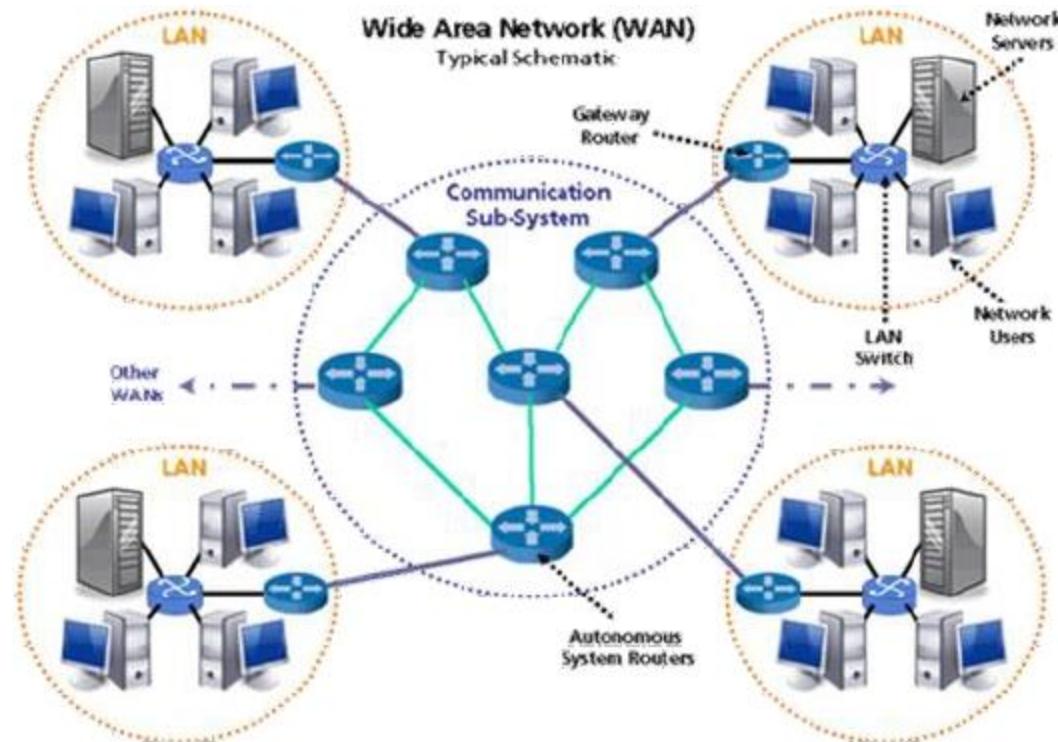
LAN (Local Area Network)



- 조직내부나 동일 건물 등 비교적 좁은 지역을 연결하기 위한 네트워크
- 비용 : 초기 투자 비용이 많이 들고 유지비용은 적게 든다.
- 관리자가 직접 관리하는 방식
- 속도 : 보통 100Mbps, 1Gbps, 10Gbps



WAN (Wide Area Network)

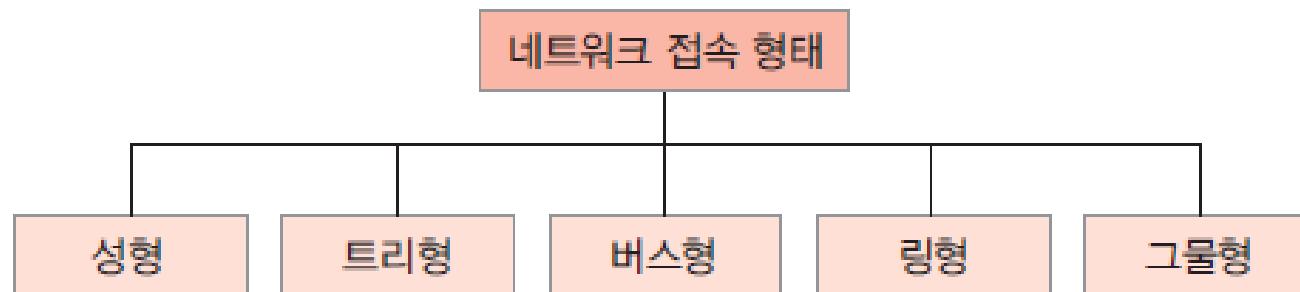


- 2개 이상의 LAN을 넓은 지역에 걸쳐 연결한 것을 가리킨다.
- 비용 : 초기 설치 비용은 적게 들지만 유지 비용이 많이 듈다.
- 관리 : 서비스 제공업체에서 관리를 하기 때문에 관리가 용이
- 속도 : 보통 느린 연결을 가진다. 56Kbps ~ T1 or E1 연결이 일반적이다.



네트워크 접속형태

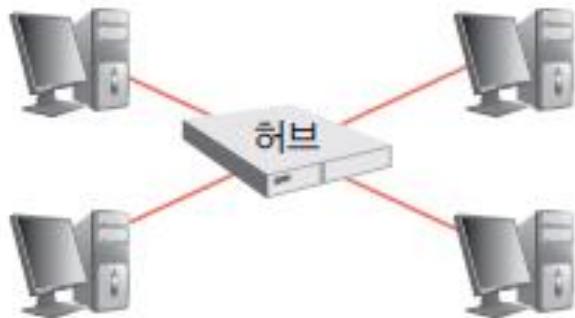
- 네트워크의構성을 '네트워크 토플로지'라고도 하는데, 이는 네트워크에 연결되어 있는 노드와 링크가 물리적 또는 논리적으로 배치되어 있는 방식을 말한다. 여기서 노드는 네트워크에 연결된 주소가 있는 통신 장치를 말하고 컴퓨터, 프린터, 복합기 등이 하나의 노드가 될 수 있다. 링크 하나에 2개 이상의 노드가 연결되며, 2개 이상의 링크가 접속 형태를 구성한다.
- 네트워크 접속 형태는 네트워크에 연결된 여러 노드의 물리적인 배열이 아닌 상호 연결 방법을 보여준다. 예를 들어 성형 접속 형태는 네트워크의 모든 노드가 별 모양인데, 이는 허브에 물리적으로 놓여 있는 모습이 아니라 상호 연결 방법을 나타낸다





네트워크 접속형태(성형)

- 가장 일반적인 네트워크 구성 형태다.
- 허브가 네트워크 중앙에 위치하여 다른 모든 노드를 연결한다.
- 모든 노드가 중앙의 허브에 연결되어 통신하므로 통신망의 처리 능력과 신뢰성은 허브가 좌우한다.
- 성형 접속 형태의 네트워크에서 하나의 케이블은 허브 같은 중앙의 네트워크 장치하고만 연결하므로, 배선 문제는 단지 해당 노드에만 영향을 줄 뿐 네트워크 전체에는 영향을 미치지 않는다.





네트워크 접속형태(성형)

■ 장점

- 성형 접속 형태에서 각 장치는 다른 장치와 연결하는 링크 한 개와 I/O 포트 한 개만 필요하므로 설치비용이 저렴하고, 중앙 집중적인 구조로 유지보수나 확장이 용이하다.
- 링크 하나가 끊어져 작동하지 않을 때 해당 링크만 영향을 받고 다른 링크들은 영향을 받지 않는다(안전성). 이러한 특징 덕분에 결함을 쉽게 식별하고 분리할 수 있기 때문에 허브는 링크에서 발생한 문제를 점검하여 결함이 발견된 링크를 우회하는 역할을 한다.

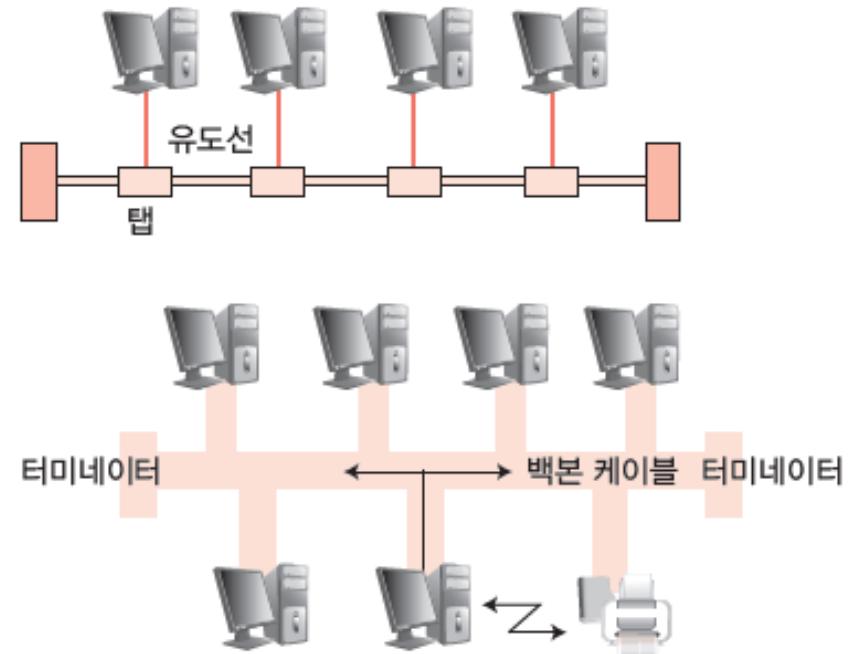
■ 단점

- 중앙에 있는 전송제어장치에 장애가 있으면 네트워크 전체가 동작할 수 없고, 통신량이 많으면 전송이 지연된다.
- 각 노드가 중앙 허브와 연결되어 있어야 하기 때문에 일부 다른 접속 형태(트리형, 링형, 버스형)보다 많은 케이블을 연결해야 한다.



네트워크 접속형태(버스형)

- 버스형은 모든 네트워크 노드와 주변 장치가 파이프 등의 일자형 케이블(버스)에 연결되어 있는 형태이다. 다음 그림과 같이 버스형에서는 하나의 긴 케이블이 네트워크의 모든 장치를 연결하는 중추 네트워크 역할을 한다. 모든 노드는 하나의 케이블에 연결되어 있고, 케이블의 시작과 끝에는 터미네이터라는 장치를 붙여서 신호가 케이블로 되돌아오는 것을 막는다.



NOTE 터미네이터(terminator)

LAN의 전기 신호가 양끝에서 반사되는 것을 방지하기 위해 덧붙이는 종단기이다.

NOTE 브로드캐스팅(broadcasting)

하나의 송신 측이 다수의 수신 측 단말을 지정하여 동일한 정보나 메시지를 동시에 전송하는 것을 말한다.



네트워크 접속형태(버스형)

■ 장점

- 설치가 간단하고 케이블 비용이 적게 듈다. 또한 장비를 추가하기 쉽고, 고장이 나도 전체 네트워크에 영향을 미치지 않는다.
- 중추 케이블을 가장 효과적으로 설치할 수 있고, 다양한 길이의 유도선으로 노드를 연결할 수 있기에 성형이나 트리형 접속 형태보다 사용하는 케이블양이 적다.

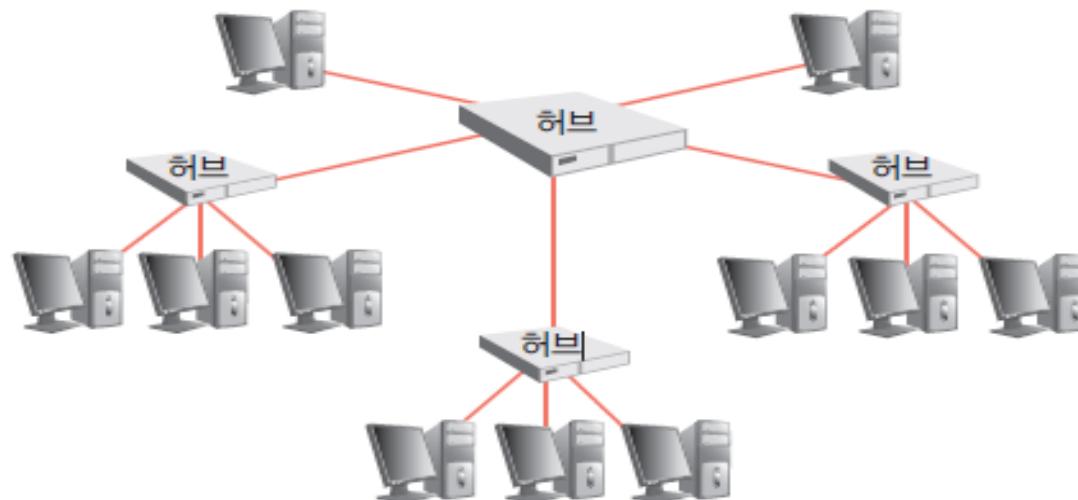
■ 단점

- 장비 수가 많아지면 네트워크 성능이 저하되고, 중앙 케이블이 고장 나면 네트워크 전체가 동작하지 않는다.
- 재구성이나 결합·분리가 어렵다.
- 베이스밴드 전송 방식에서는 케이블 거리가 멀어지면 신호가 점점 약해지기 때문에 중계기를 사용해야 한다.
- 한 노드에서 데이터를 전송할 때 다른 노드에서 이미 데이터를 전송하고 있으면 충돌이 발생하므로 나중에 다시 전송해야 한다.



네트워크 접속형태(트리형)

- 성형의 변형으로, 중앙에 있는 전송제어장치에 모든 장비를 연결한 것이 아니라 트리 형태의 노드에 전송제어장치를 두어 노드들을 연결하는 형태다.
- 상위 계층의 노드가 하위 노드들을 직접 제어하는 계층적인 네트워크에 적합하다.





네트워크 접속형태(트리형)

■ 장점

- 제어가 간단하여 관리나 네트워크 확장이 쉽다.
- 중앙에 있는 하나의 전송제어장치에 더 많은 장비를 연결할 수 있어 각 장비 간의 데이터 전송 거리를 늘릴 수 있다.
- 여러 컴퓨터를 분리하거나 우선순위를 부여할 수 있다.

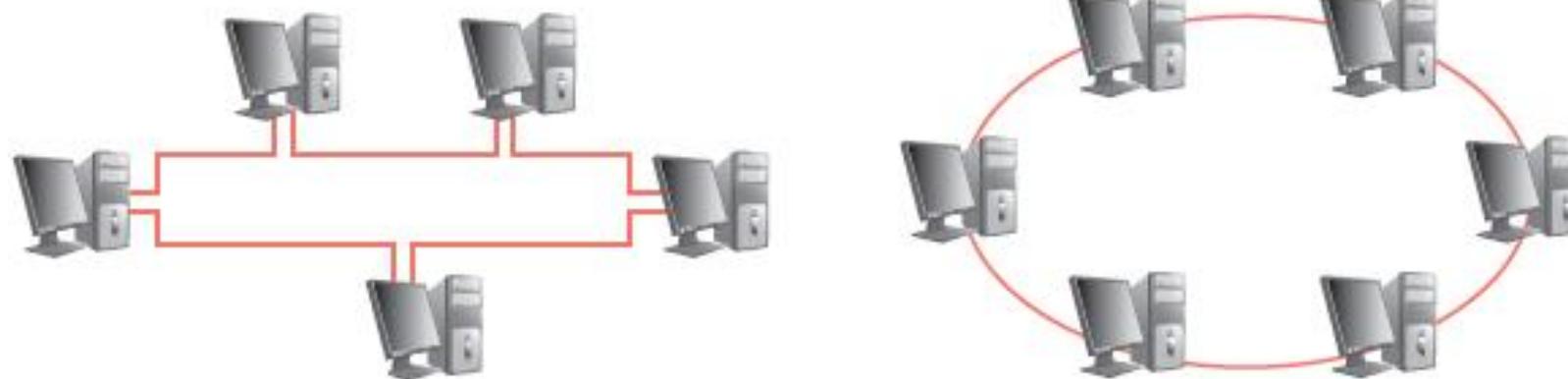
■ 단점

- 중앙에 트래픽이 집중되어 병목현상이 발생할 수 있고, 중앙의 전송제어장치가 다운되면 전체 네트워크에 장애가 발생한다.



네트워크 접속형태(링형)

- 노드가 링에 순차적으로 연결된 형태로, 모든 컴퓨터를 하나의 링으로 연결한다.
- 각 노드들은 인접한 노드 두 개하고만 연결되며, 전체 네트워크는 하나의 원을 형성한다.
- 링형 접속 형태에는 원의 한 방향으로만 데이터를 전송할 수 있는 단순 링형(Single Ring)과 양방향으로 전송할 수 있는 이중 링형(Double Ring)이 있다.





네트워크 접속형태(링형)

■ 장점

- 구조가 단순하여 설치와 재구성이 쉽고, 장애가 발생해도 복구시간이 빠르다.
- 각 장치는 바로 이웃하는 장치에만 연결되어 있고, 장치를 추가하거나 삭제할 때는 단지 연결선 두 개만 움직이면 된다.
- 보통 신호는 항상 순환되므로 한 장치가 특정한 시간 내에 신호를 받지 못하면 경보를 낼수 있다. 이 경보는 네트워크 운영자에게 문제의 발생 사실과 발생 위치를 알려준다.
- 성형보다 케이블 비용을 많이 줄일 수 있다.

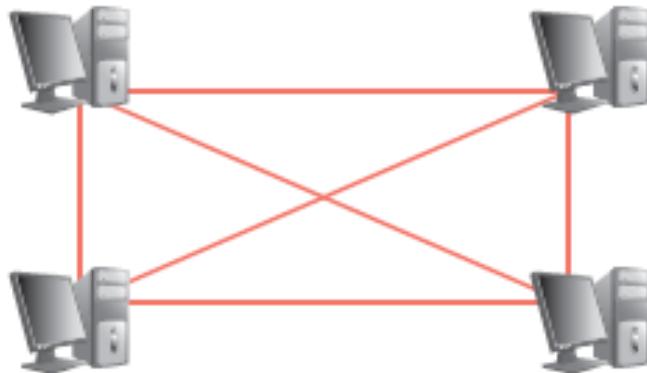
■ 단점

- 링을 제어하는 절차가 복잡하고, 새로운 장비를 연결하려면 링을 절단한 후 장비를 추가해야 한다.
- 단순 링형에서는 링에 결함(네트워크 내 한 장치가 사용 불가능한 경우)이 생기면 전체 네트워크를 사용할 수 없다.



네트워크 접속형태(그물형)

- 중앙에 제어하는 노드 없이 모든 노드가 상호 간에 전용의 점대점 형태로 연결되는 형태를 말한다.
- 전용이라는 것은 연결된 두 장치 간에 통신만 담당하는 링크가 있음을 의미하며, 그물형에서는 $n(n-1)/2$ 개의 물리적 채널이 필요하다.
- 네트워크가 복잡하고 많은 통신회선이 필요하기 때문에 비용이 많이 들지만, 신뢰성이 높아 중요한 네트워크에 주로 사용한다.





네트워크 접속형태(그물형)

■ 장점

- 전용 링크를 사용하면 각 연결회선이 원하는 자료를 전송할 수 있어 많은 장치를 공유하는 링크에서 발생하는 통신량 문제를 해결할 수 있다.
- 한 링크가 고장 나더라도 전체 시스템에는 큰 문제가 발생하지 않는다. 일부 통신회선에 장애가 발생하면 다른 경로를 통하여 데이터를 전송하면 된다.
- 모든 메시지는 전용선으로 보내기 때문에 원하는 수신자만 받을 수 있다. 따라서 비밀 유지와 보안에 유리하다.
- 결함의 식별과 분리가 비교적 쉽고, 전송에 문제가 있다고 생각되는 링크는 관리자가 우회하도록 설정할 수 있다. 즉 관리자는 문제가 발생한 곳을 쉽게 찾아 그 원인을 바로 해결할 수 있다.

■ 단점

- 노드를 다른 모든 노드와 연결해야 하므로 설치와 재구성이 어렵다.
- 실제 필요한 전선의 용적이 벽 속이나 천장, 바닥 아래 등 전선을 수용할 공간보다 커질 수 있다.
- 네트워크가 복잡하고 많은 통신회선이 필요하기 때문에 각 링크와 연결되는 하드웨어(I/O 포트와 전선)에 엄청난 비용이 들 수 있다.



네트워크 접속형태(혼합형)

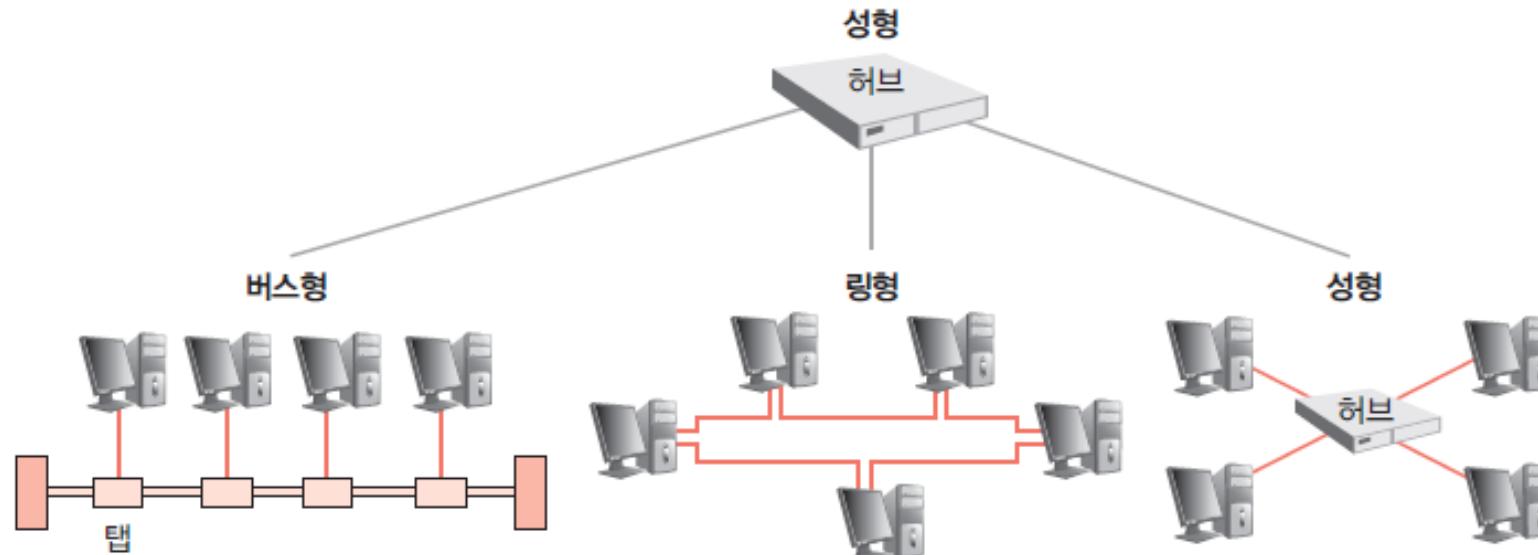
- 소규모 네트워크가 아니라면 순수한 버스형이나 링형, 성형접속 형태를 실제로 만나기는 어렵다.
- 노드 수가 상대적으로 큰 실제 네트워크에서는 효율을 높이고 결함 허용 능력을 증대시키려고 혼합형 접속 형태를 사용한다.
- 네트워크 서브넷이 서로 연결되어 규모가 큰 접속 형태가 되도록 여러 접속 형태를 결합할 수 있다.

NOTE 서브넷(subnet)

대규모 네트워크를 구성하는 개별 네트워크를 말한다.

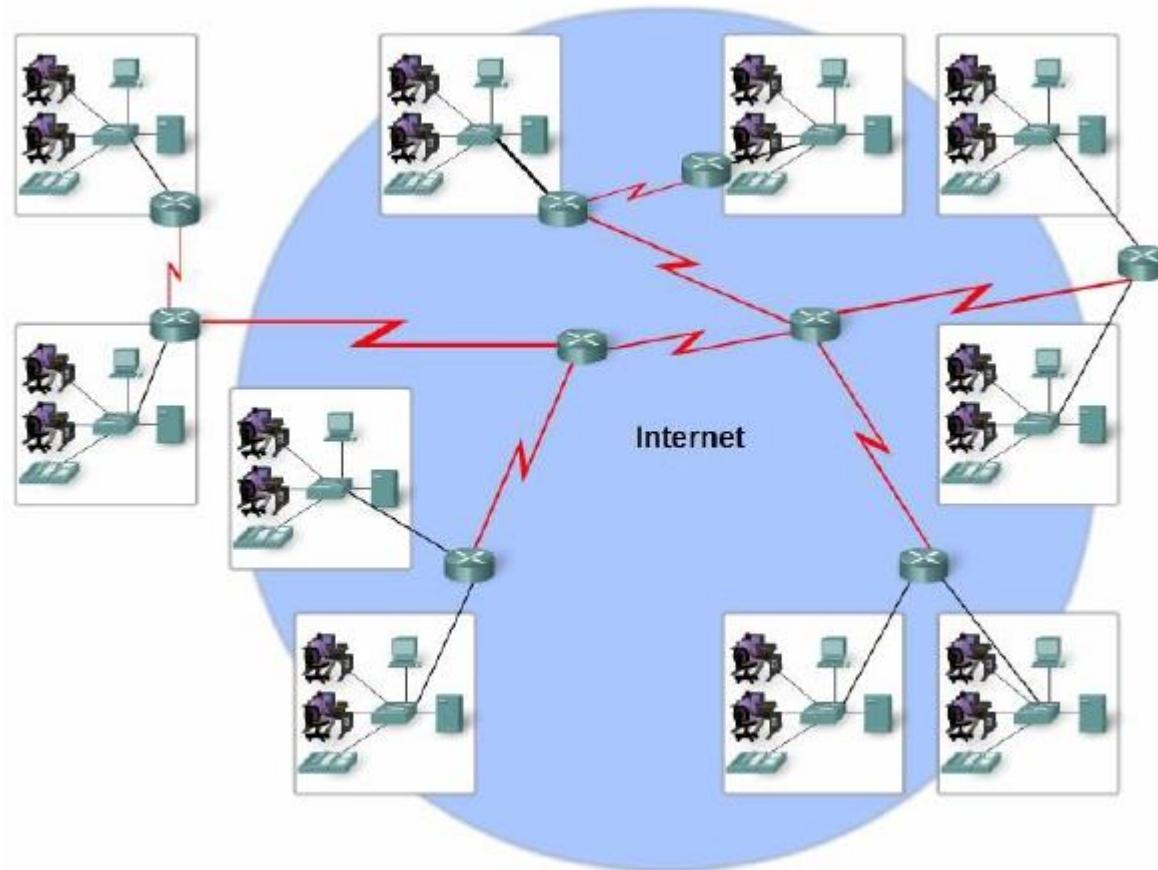


네트워크 접속형태(혼합형)





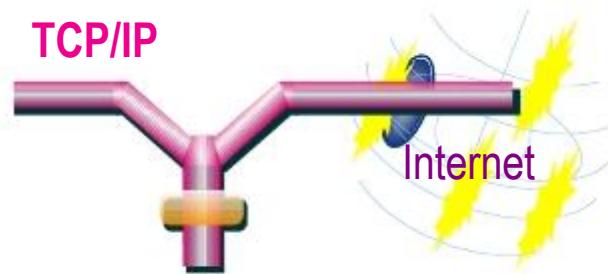
Internet ?



인터넷([영어](#): Internet, 누리망)은 [컴퓨터](#)를 연결하여 [TCP/IP](#)(Transmission Control Protocol/Internet Protocol)라는 [통신 프로토콜](#)을 이용해 정보를 주고받는 [컴퓨터 네트워크](#)이다. –위키백과-



프로토콜(Protocol)

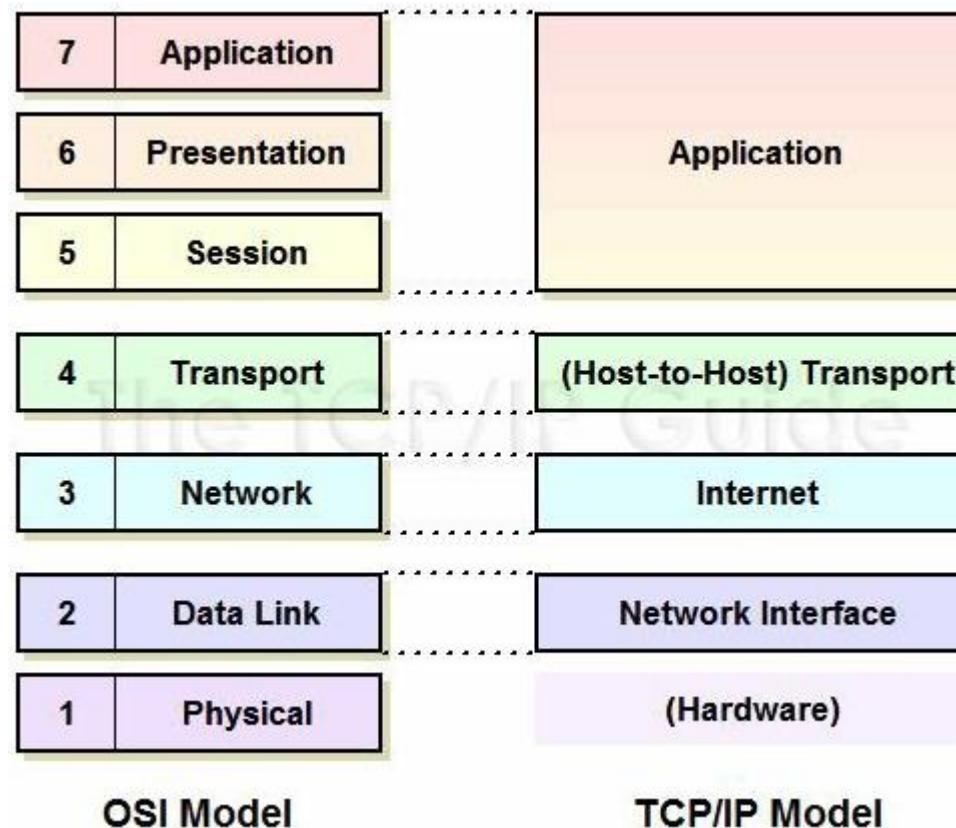


메이커명이나 조직명	아키텍쳐 또는 프로토콜명
Apple Computer	AppleTalk
DEC (현 Compaq)	DNA(DECnet)
IBM	SNA
ISO, CCITT (현 ITU-T)	OSI
Microsoft	NetBEUI
Novell	NetWare (IPX/SPX)
XEROX	XNS

- 프로토콜이란 네트워크 소프트웨어의 핵심으로 둘 이상의 통신 개체 사이에 교환되는 메시지의 형태, 의미, 전송순서, 그리고 메시지 송수신 및 기타 사건에 수행할 동작을 정의한 규약
- 많은 프로토콜의 정의나 설명이 RFC(Request For Comments)에 서로 정리되어 있으며 각 프로토콜의 역할과 구성이 명확이 정해져 있다.
www.ietf.org

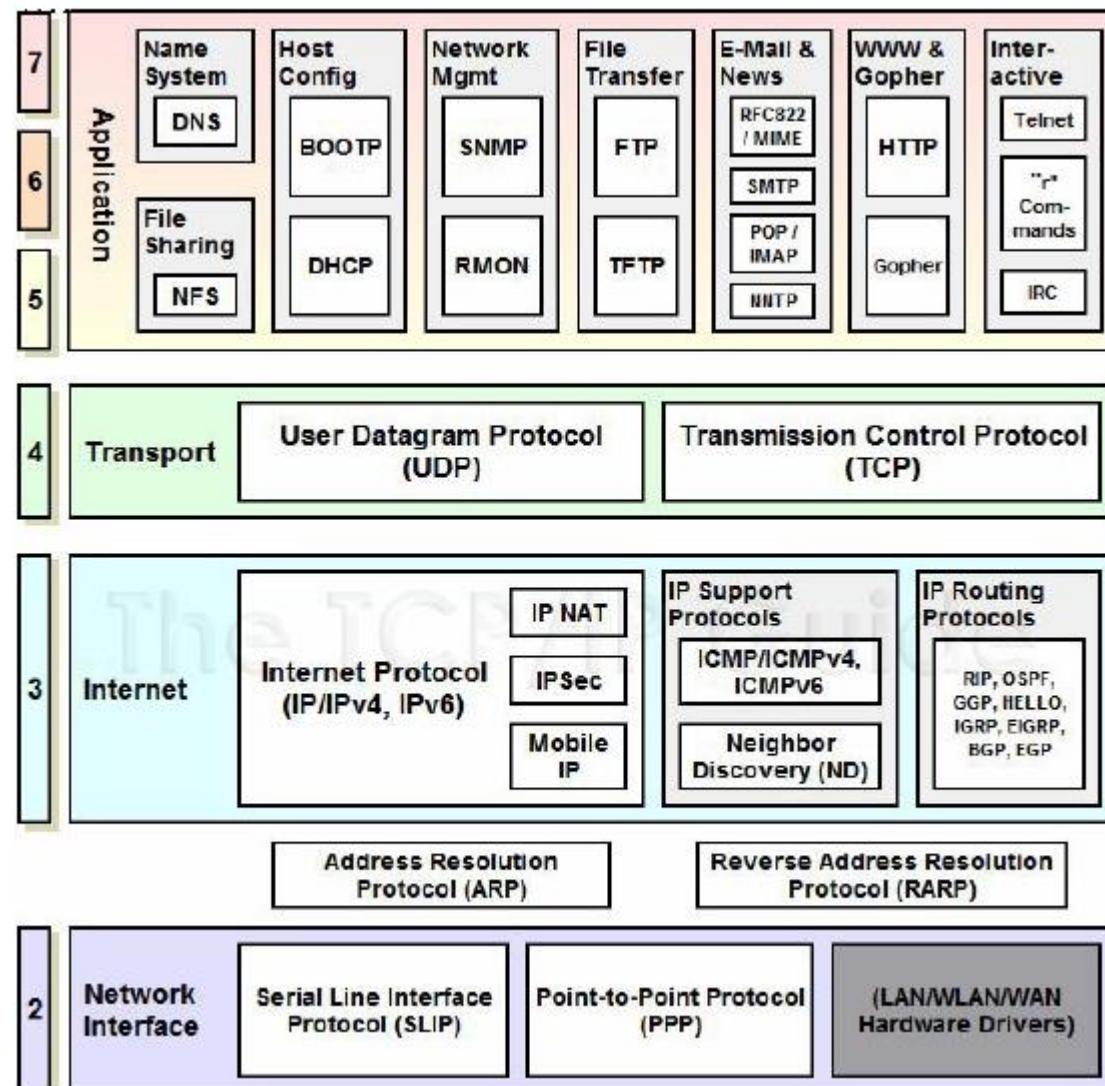


OSI 7 Layer vs TCP/IP Model Layer



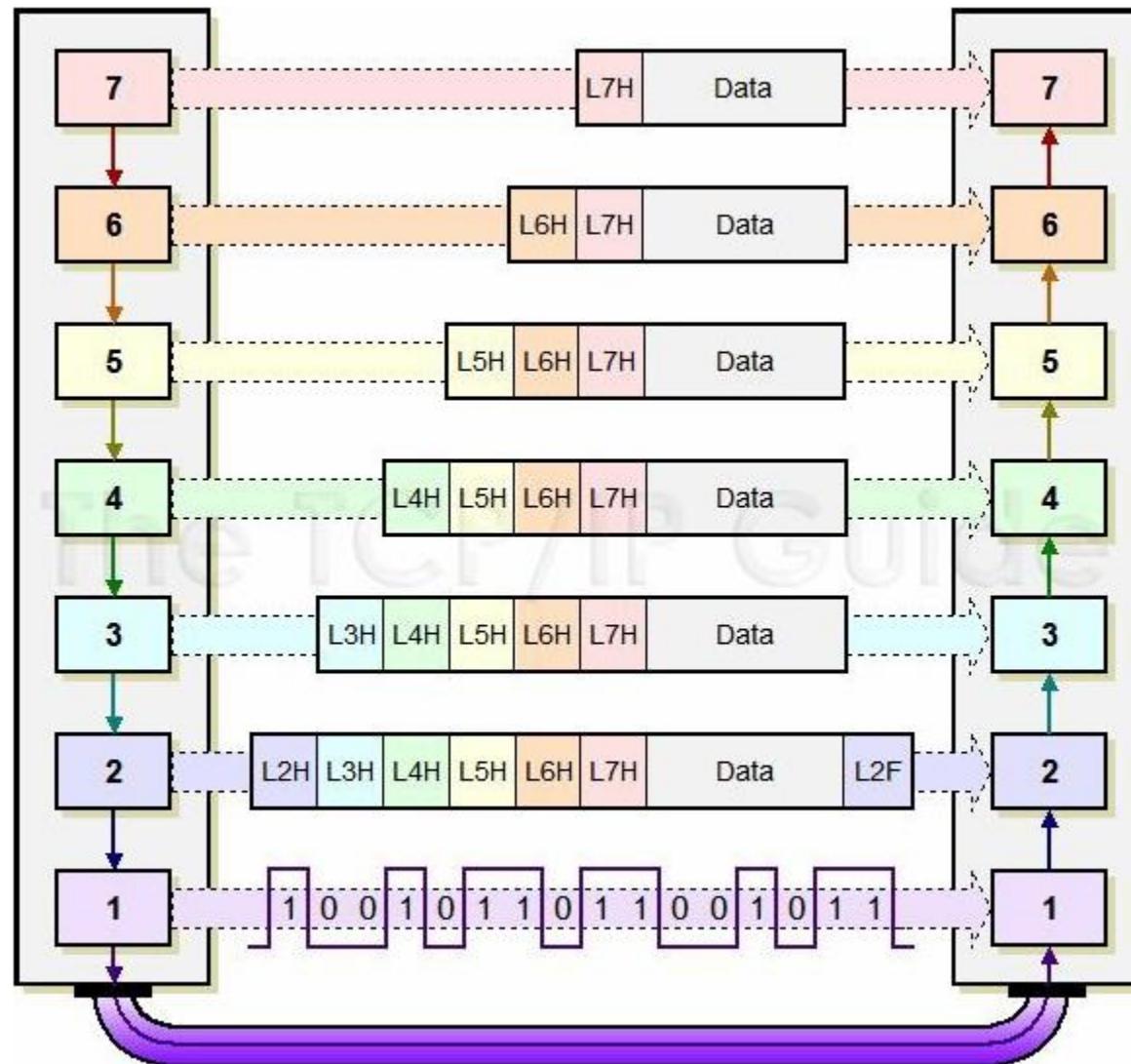


TCP/IP Protocol Stack(Suite)



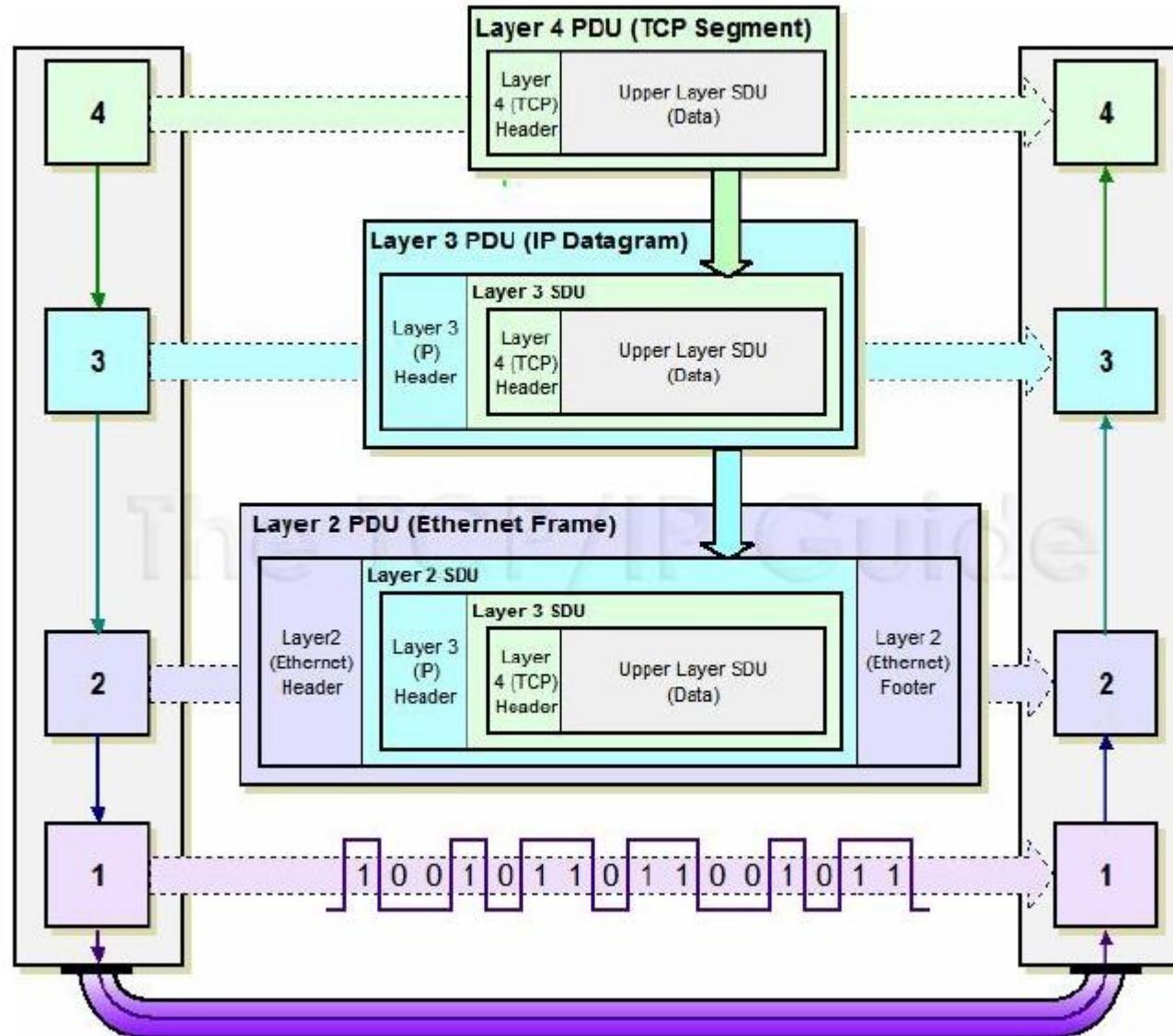


Data encapsulation & de-encapsulation





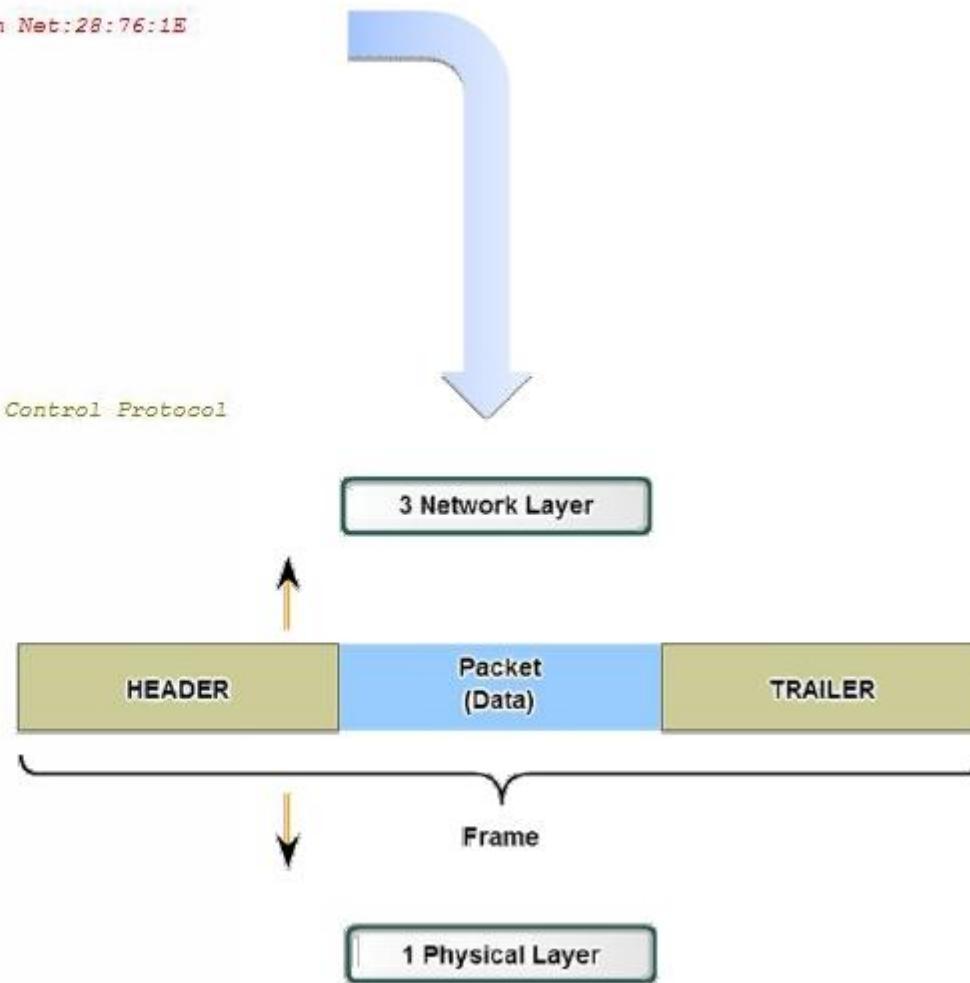
Data encapsulation & de-encapsulation





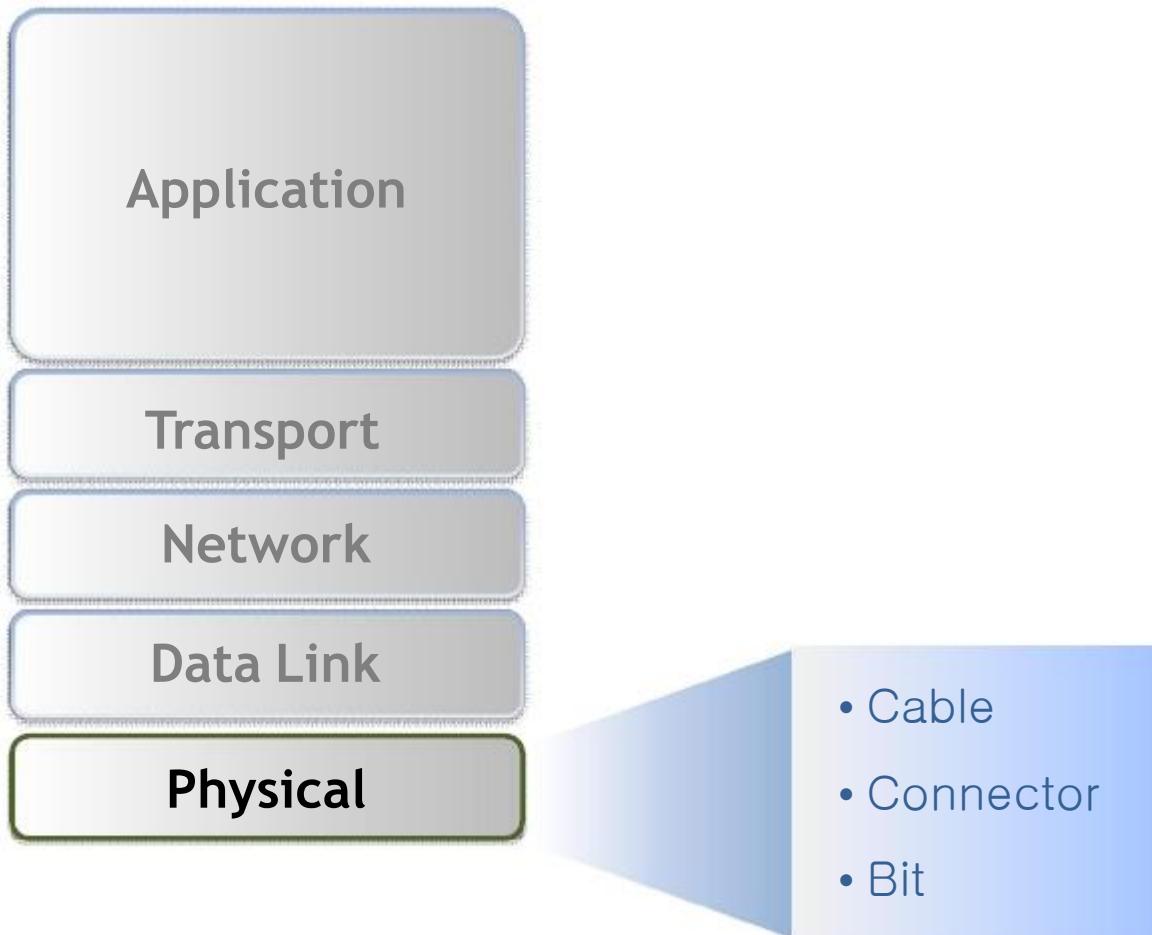
Packet의 구성요소

Ethernet Header	
Destination:	00:08:9F:28:76:1E Efm Net:28:76:1E
Source:	00:13:02:24:D8:56
Protocol Type:	0x0800 IP
IP Header - Internet Protocol Datagram	
Version:	4
Header Length:	5 (20 bytes)
Differentiated Services:	=00000000
Total Length:	40
Identifier:	47902
Fragmentation Flags:	=010
Fragment Offset:	0 (0 bytes)
Time To Live:	128
Protocol:	6 TCP - Transmission Control Protocol
Header Checksum:	0x3A7F
Source IP Address:	192.168.50.122
Dest. IP Address:	222.231.51.40
TCP - Transport Control Protocol	
Source Port:	1921 noadmin
Destination Port:	80 http
Sequence Number:	2358878175
Ack Number:	1711502834
TCP Offset:	5 (20 bytes)
Reserved:	=0000
F=	00010000 . . . A
Window:	17520
TCP Checksum:	0x55F2
Urgent Pointer:	0
No TCP Options	
Extra bytes	
Number of bytes:	(6 bytes)
FCS - Frame Check Sequence	
FCS:	0xDC6301CB Calculated





Physical Layer





Cable & Connector

TwistedPair

100BaseT



**Unshielded (UTP)
Shielded (STP)**

Coaxial



10Base2, 10Base5

**ThinNet
ThickNet**

FiberOptic

100BaseFx

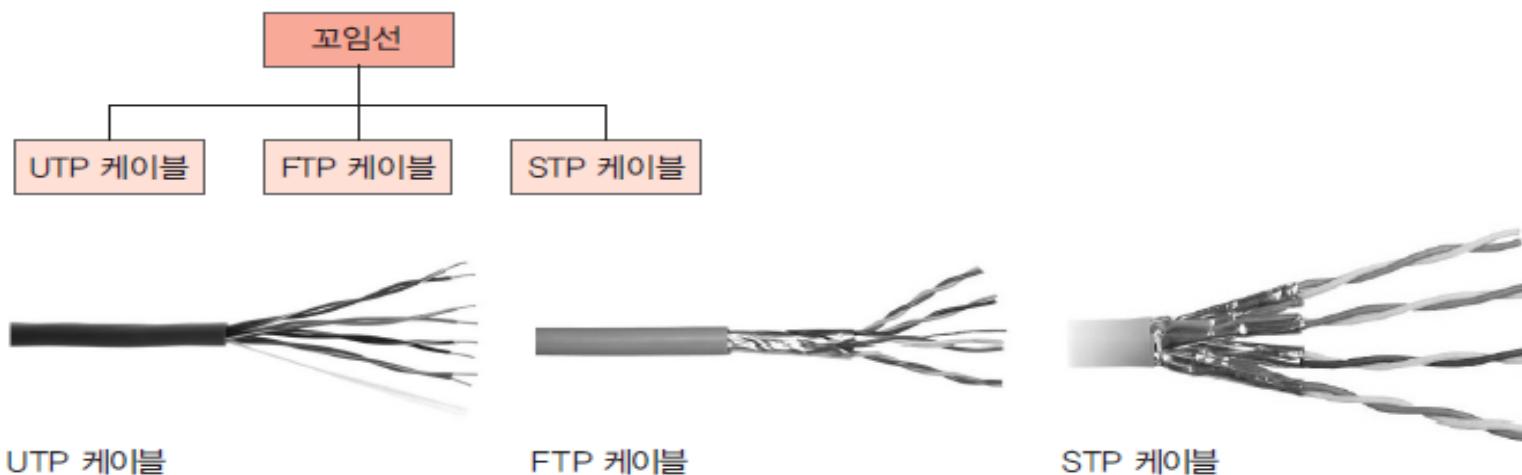
**Multi Mode
Single Mode**





꼬임선(Twisted Pair) : 이중 나선 케이블

- 꼬임선은 플라스틱으로 덮인 두 가닥의 절연된 구리선을 나선형으로 꼬아서 만든다.
- 한 쌍이 하나의 통신회선 역할을 하며, 여러 개의 쌍이 묶여 하나의 케이블을 형성하고 보호용 외피로 이를 감싸 완성한다.
- 구리선을 꼬는 이유는 두 선 사이의 전기적 간섭을 최소화하기 위해서다.
- 접속 형태 중 성형 구성에 많이 사용하며, 동축 케이블이나 광섬유 케이블에 비해 설치하기 쉽다.
- 꼬임선은 만들기 쉽고 비용이 저렴하기 때문에 다양한 전송매체에 사용한다.
- 꼬임선은 외부 신호의 간섭을 최소화하려고 금속망으로 전선을 감싸는 차폐 보호망을 사용하는데, 사용 여부에 따라 UTP(Unshielded Twist Pair) 케이블과 FTP(Foil Screened Twist Pair) 케이블, STP(Shielded Twist Pair) 케이블로 분류할 수 있다.

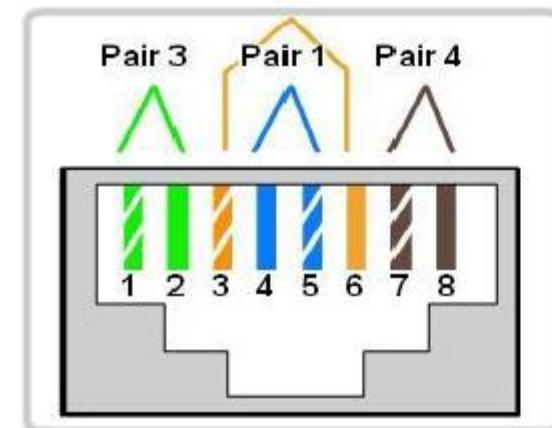




RJ-45를 이용한 UTP Connector 만들기

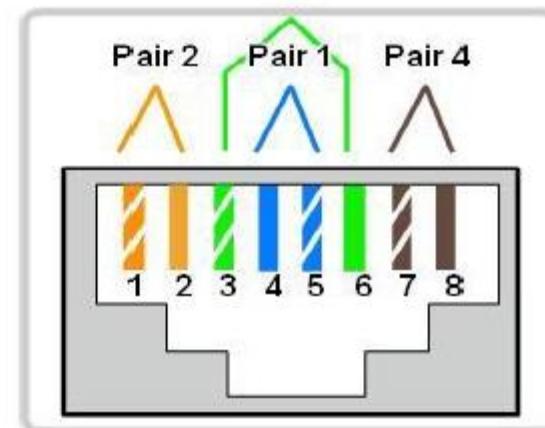
RJ45 T568A & T568B Termination

Pair 2

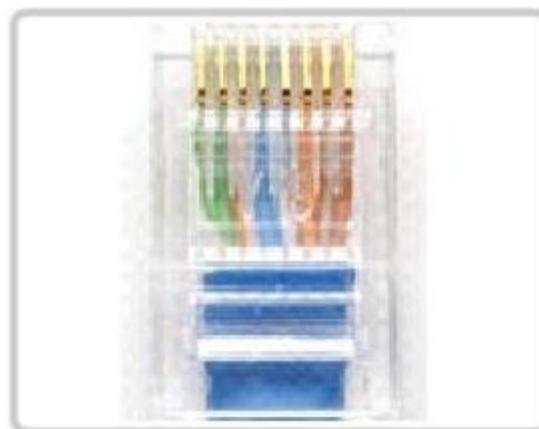


T568A

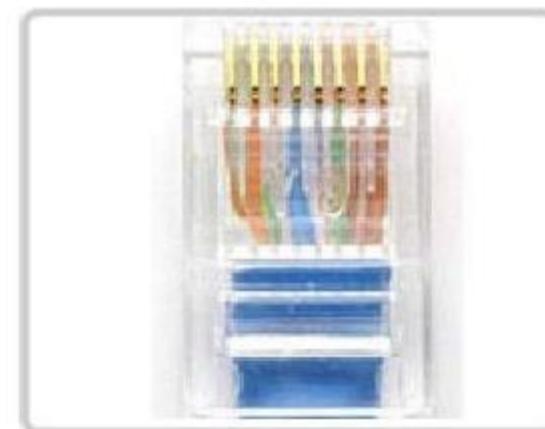
Pair 3



T568B



T568A
(Top View)



T568B
(Top View)



Fiber Optical

Fiber Media Modes

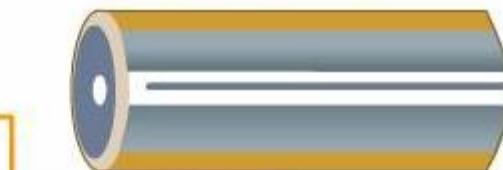
Single-Mode

Polymeric Coating



Glass Cladding
125 microns dia

Produces single straight path for light



Glass Core=8-10 microns

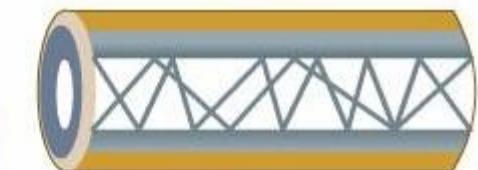
Multimode

Polymeric Coating



Glass Cladding
125 microns dia

Allows multiple paths for light



Glass Core=50/62.5 microns

Single-Mode

- 단일 경로
- 10미크론 이하
- 큰 정밀도
- 가격이 비싸다
- 50Gbps

Multimode

- 다중 경로
- 50~62.5미크론
- 가격이 싸다



Fiber Optical Connector



LC



SC



ST



FC



MTRJ

LC : Lucent Connector

SC : Subscriber Connector or Square Connector

ST : Straight Tip

FC : Fiber transmission system Connector

MTRJ : Mechanical transferable Registered Jack



UTP Cable Category

CAT 1	1Mbps 미만	아날로그 음성 (전화) ISDN BRI 연결용
CAT 2	4Mbps	주로 IBM의 토큰링에 사용
CAT 3	16Mbps	10BaseT Ethernet 데이터 및 음성 전송
CAT 4	20Mbps	16Mbps 토큰링에서 사용. 많이 사용하지 않음
CAT 5	100Mbps	100Mbps FastEthernet Network. 가장 보편적
CAT 6	200MHz~250MHz	1000Mbps를 구성하기 위해 만들어졌다

- EIA(Electronic Industries Alliance)
- EIA/TIA-568 표준 규격

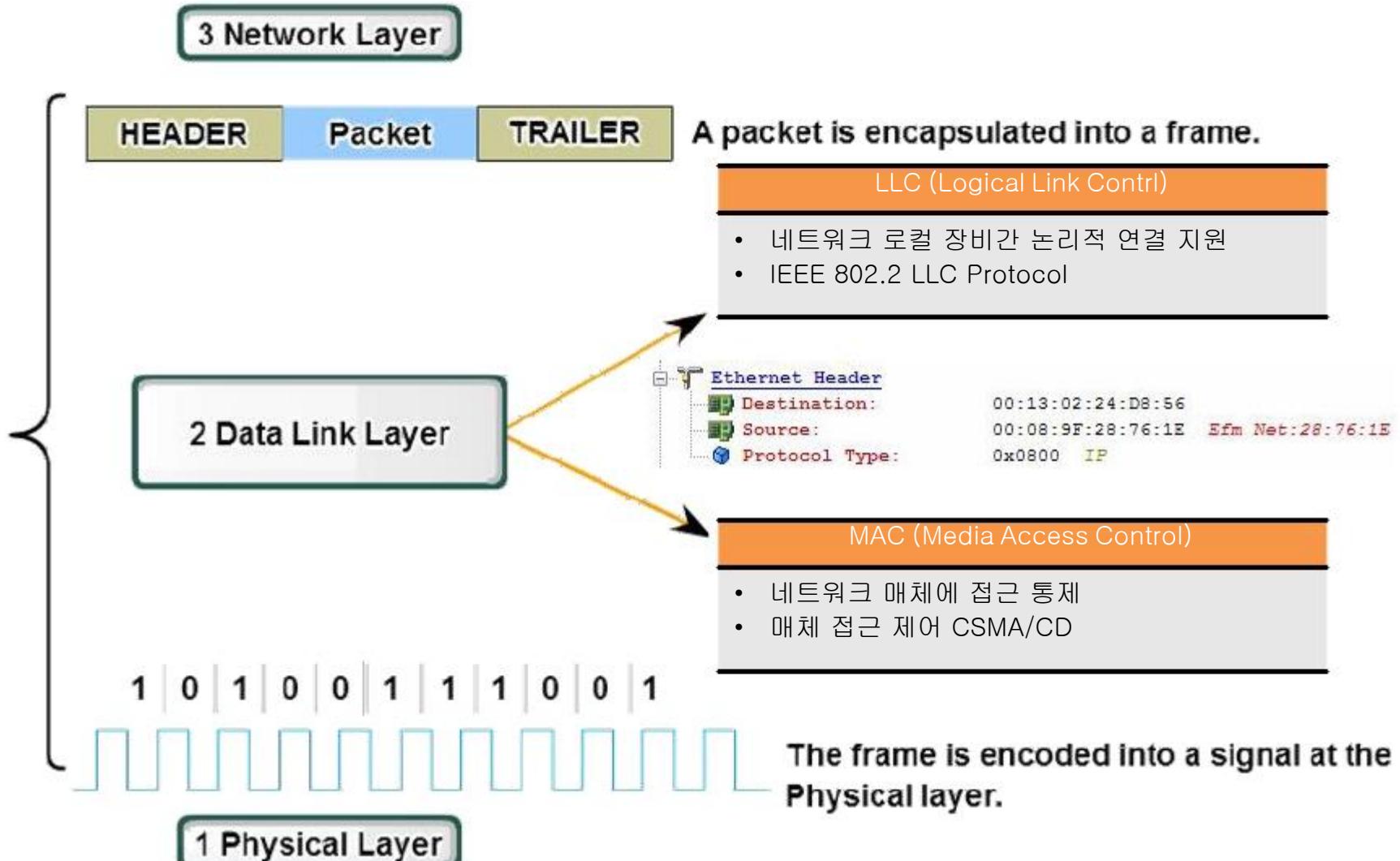


Type of Ethernet

Ethernet Type	Bandwidth	Cable Type	Duplex	Maximum Distance
10Base-5	10 Mbps	Thicknet Coaxial	Half	500 m
10Base-2	10 Mbps	Thinnet Coaxial	Half	185 m
10Base-T	10 Mbps	Cat3/Cat5 UTP	Half	100 m
100Base-TX	100 Mbps	Cat5 UTP	Half	100 m
100Base-TX	200 Mbps	Cat5 UTP	Full	100 m
100Base-FX	100 Mbps	Multimode Fiber	Half	400 m
100Base-FX	200 Mbps	Multimode Fiber	Full	2 km
1000Base-T	1 Gbps	Cat5e UTP	Full	100 m
1000Base-TX	1 Gbps	Cat6 UTP	Full	100 m
1000Base-SX	1 Gbps	Multimode Fiber	Full	550 m
1000Base-LX	1 Gbps	Single-Mode Fiber	Full	2 km
10GBase-CX4	10 Gbps	Twin-axial	Full	100 m
10GBase-T	10 Gbps	Cat6a/Cat7 UTP	Full	100 m
10GBase-LX4	10 Gbps	Multimode Fiber	Full	300 m
10GBase-LX4	10 Gbps	Single-Mode Fiber	Full	10 km

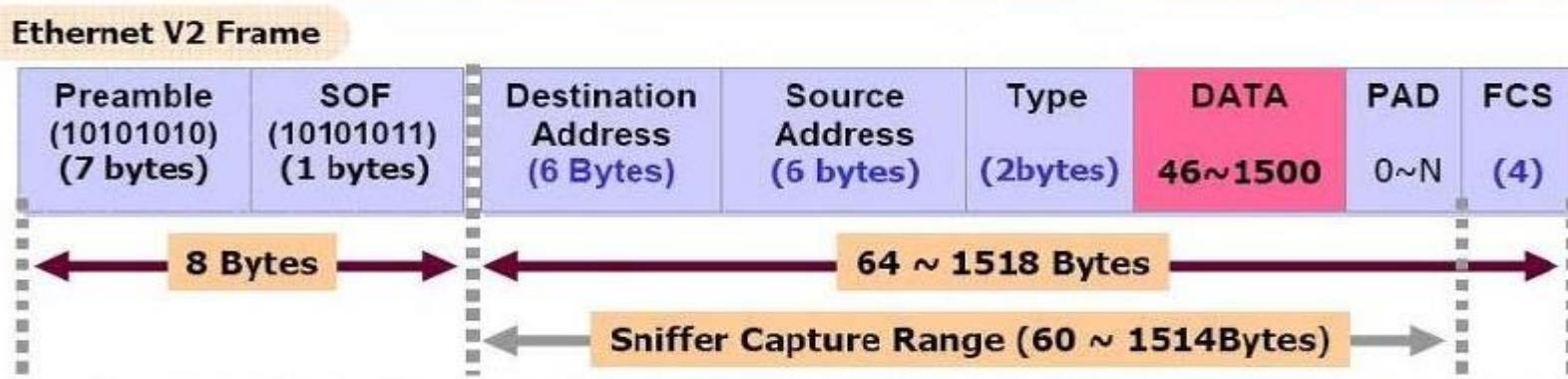


Data-Link Layer





Ethernet 프레임 포맷



- ▶ Preamble : 물리계층에서 전송된 비트 패턴이며, 송신자와 수신자의 동기(Synchronize)를 맞추는데 사용된다. 101010... 반복
- ▶ SOF (Start of Frame) : Ethernet Frame 시작을 알려주는 신호. 10101011
- ▶ Destination Address : Frame이 도착 되어야 할 MAC Address
- ▶ Source Address : Frame을 전송하는 Station의 MAC Address
- ▶ Type/Length : IEEE 802.3일 경우 ‘Length’가 Ethernet V2일 경우에는 ‘Type’이 된다.
- ▶ Data : 상위 계층으로부터 받은 데이터가 여기에 담기는데, 최소 46, 최대 1500 Bytes 크기를 갖는다.
- ▶ PAD : Data 필드의 최소값을 보정하는 기능으로, 46Bytes이하로 데이터가 들어올 때, 임의로 만들어 준다.
- ▶ FCS : CRC(Cyclic Redundancy Check)라고도 불리며, Frame의 오류 체크를 담당한다.



EUI-48 & EUI-64

- **EUI-48 (48-bit Extended Unique Identifier) :**

- 00-0E-35-05-80-6F
- 상위 24bit는 Company ID (제조 회사에 할당된 주소임.)
- 하위 24bit는 Extension ID (제조번호에 해당함.)
- 하나의 OUI는 $2^{24} = 16,777,216$ 개 MAC 사용.

- **EUI-64 (64-bit Extended Unique Identifier) :**

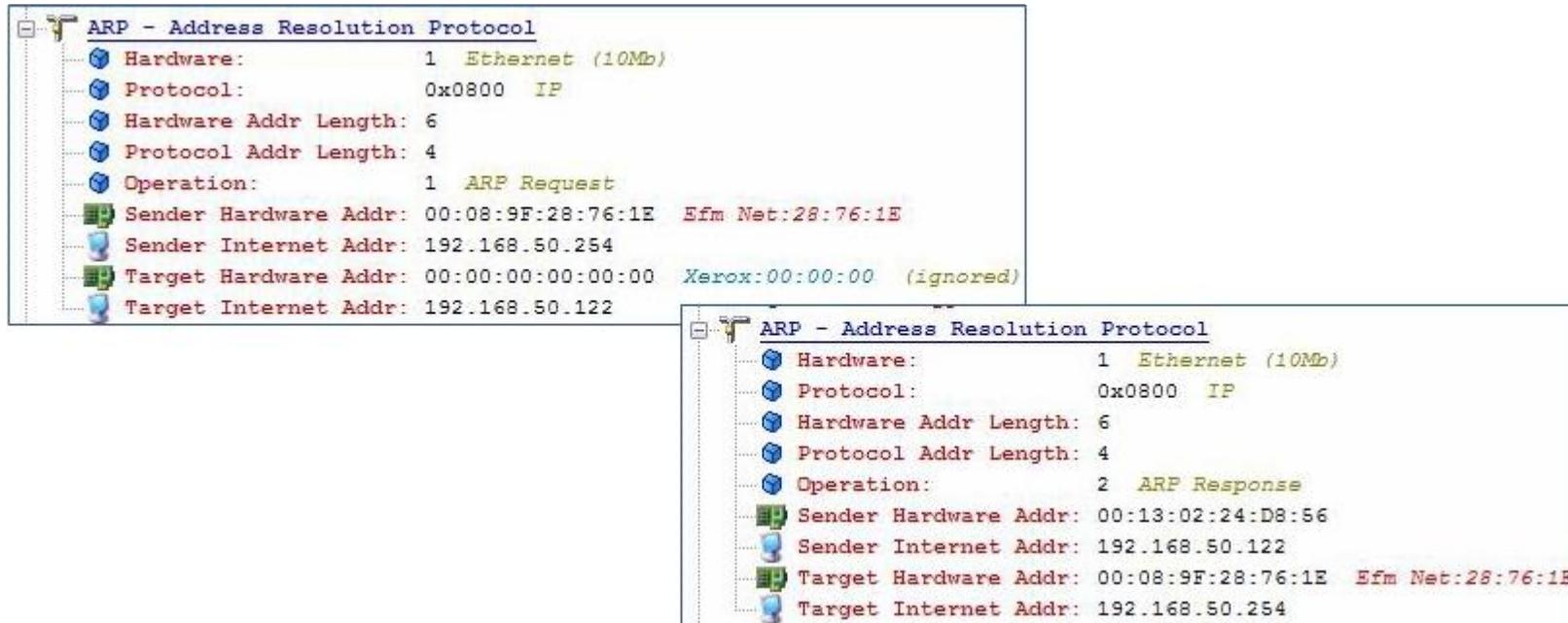
- 00-0E-35-FF-FE-05-80-6F
- 상위 24bit는 Company ID 이다. (제조회사)
- 하위 40bit는 Extension ID 이다. (제조번호)
- 하나의 OUI는 $2^{40} = 1,099,511,627,776$ 개 MAC 사용.

Company ID 확인 사이트

<http://standards.ieee.org/regauth/oui/index.shtml>



ARP (Address Resolution Protocol)



- 같은 네트워크 세그먼트에 있는 두 IP장비가 통신하는 경우에는 그 네트워크에서 이용하는 특정 매체에 적합하게 정의된 하위 계층 프로토콜과 주소 지정 (Addressing) 메커니즘을 사용한다.
- 예를 들어, 이더넷 장비는 통신할 때 이더넷에 특화된 주소를 사용한다. 반면 프레임 릴레이는 프레임릴레이에 특화된 주소를 사용한다. IP 시스템이 통신하기 위해서는 먼저 로컬 장비가 속한 네트워크에 연결된 다른 장비의 하드웨어 주소를 확인해야 한다. 주소 변환 프로토콜 (ARP, Address Resolution Protocol)은 이런 서비스를 제공한다.



ARP Cache

- ▶ ARP 요청을 보냈던 시스템은 ARP응답을 수신하면 질의 대상 시스템의 하드웨어 주소와 IP주소를 로컬 캐시(Cache)에 저장한다.
 - 시스템에서 다음 번 데이터를 보낼 때 로컬 캐시를 검사하여 엔트리를 찾으면 그것을 사용함으로써 또 다른 요청을 브로드캐스트 할 필요가 없어짐으로써 로컬 트래픽을 줄일 수 있다. 응답하는 시스템도 동일하게 로컬 Cache에 ARP정보를 저장한다.

```
C:\>arp -a

Interface: 192.168.50.122 --- 0x2
      Internet Address          Physical Address          Type
        192.168.50.254        00-08-9f-28-76-1e    dynamic
```



ARP Cache & Static ARP Table

- ARP Cache 확인

```
C:\>arp -a
Interface: 211.255.9.138 on Interface 0x1000004
Internet Address      Physical Address      Type
 211.255.9.130        00-e0-4c-ab-43-ee    dynamic
 211.255.9.254        00-10-7b-38-24-68    dynamic
```

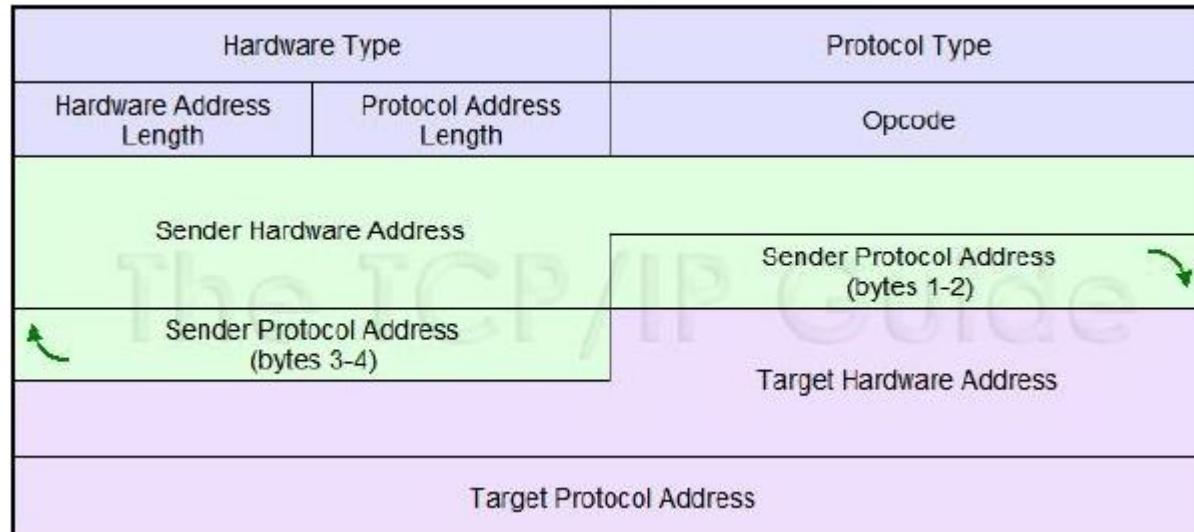
- Static ARP Table 만들기

```
C:\>arp -s 211.255.9.254 00-10-7b-38-24-68
C:\>arp -a
Interface: 211.255.9.138 on Interface 0x1000004
Internet Address      Physical Address      Type
 211.255.9.130        00-e0-4c-ab-43-ee    dynamic
 211.255.9.254        00-10-7b-38-24-68    static
```

```
netsh interface ipv4 set neighbors interface=15 address=192.168.100.1 00-21-a0-a1-46-c0
```



ARP Packet 구조



Hardware Type	요청된 하드웨어 주소 종류를 나타냄
Protocol Type	다루고 있는 상위 계층의 프로토콜 정보
Hardware Address Length	물리매체의 하드웨어 주소의 크기를 바이트 단위로 나타낸다
Protocol Address Length	상위 계층의 프로토콜 주소의 크기를 바이트 단위로 나타낸다
Operation	ARP Packet의 목적을 나타낸다. (요청 또는 응답)
Sender Hardware Address	ARP Broadcast를 전송하는 시스템의 하드웨어 주소
Sender Internet Address	ARP Broadcast를 전송하는 시스템의 상위 계층 프로토콜 주소
Target Hardware Address	ARP Broadcast를 수신하는 시스템의 하드웨어 주소
Target Internet Address	ARP Broadcast를 수신하는 시스템의 상위 계층 프로토콜 주소



Operation Code & Hardware Type

<Operation Code>

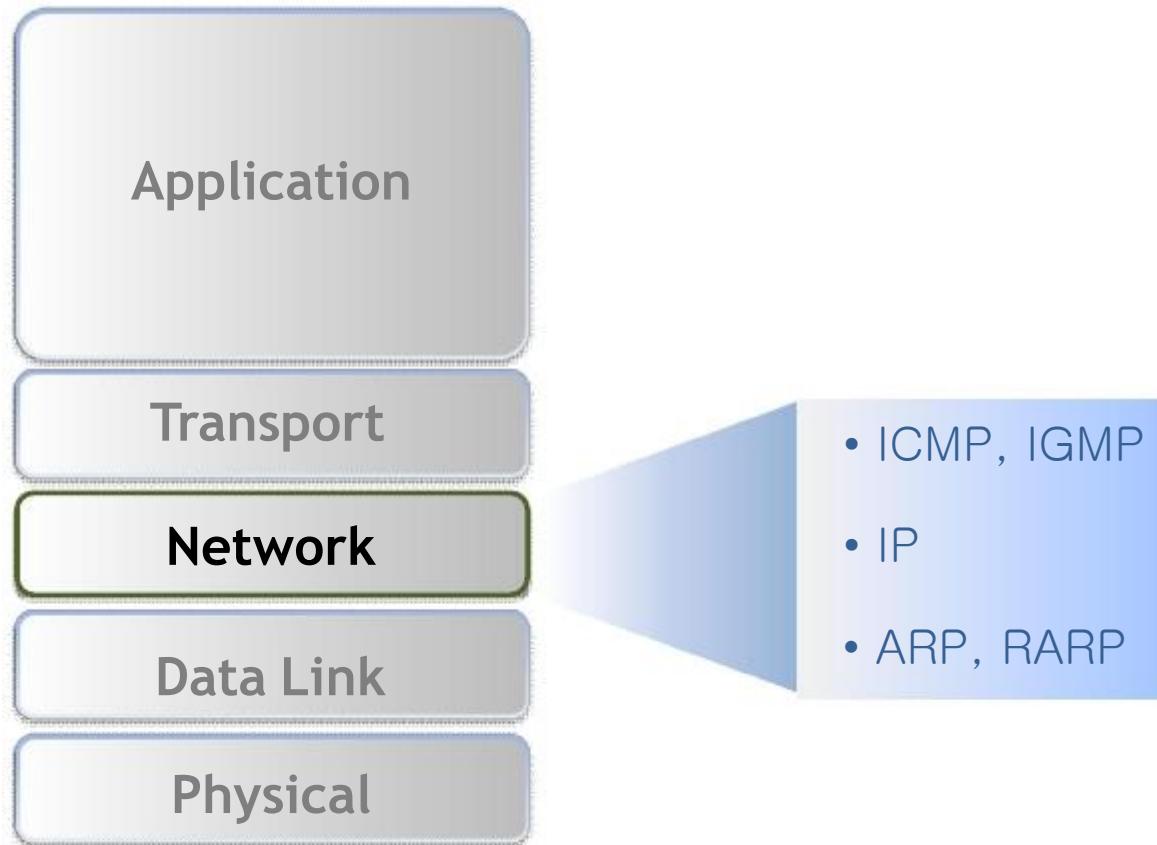
Opcode	ARP Message Type
1	ARP Request
2	ARP Reply
3	RARP Request
4	RARP Reply
5	DRARP Request
6	DRARP Reply
7	DRARP Error
8	InARP Request
9	InARP Reply

<Hardware Type>

HRD Value	Hardware Type
1	Ethernet (10 Mb)
6	IEEE 802 Networks
7	ARCNET
15	Frame Relay
16	Asynchronous Transfer Mode (ATM)
17	HDLC
18	Fibre Channel
19	Asynchronous Transfer Mode (ATM)
20	Serial Line



Internet Layer



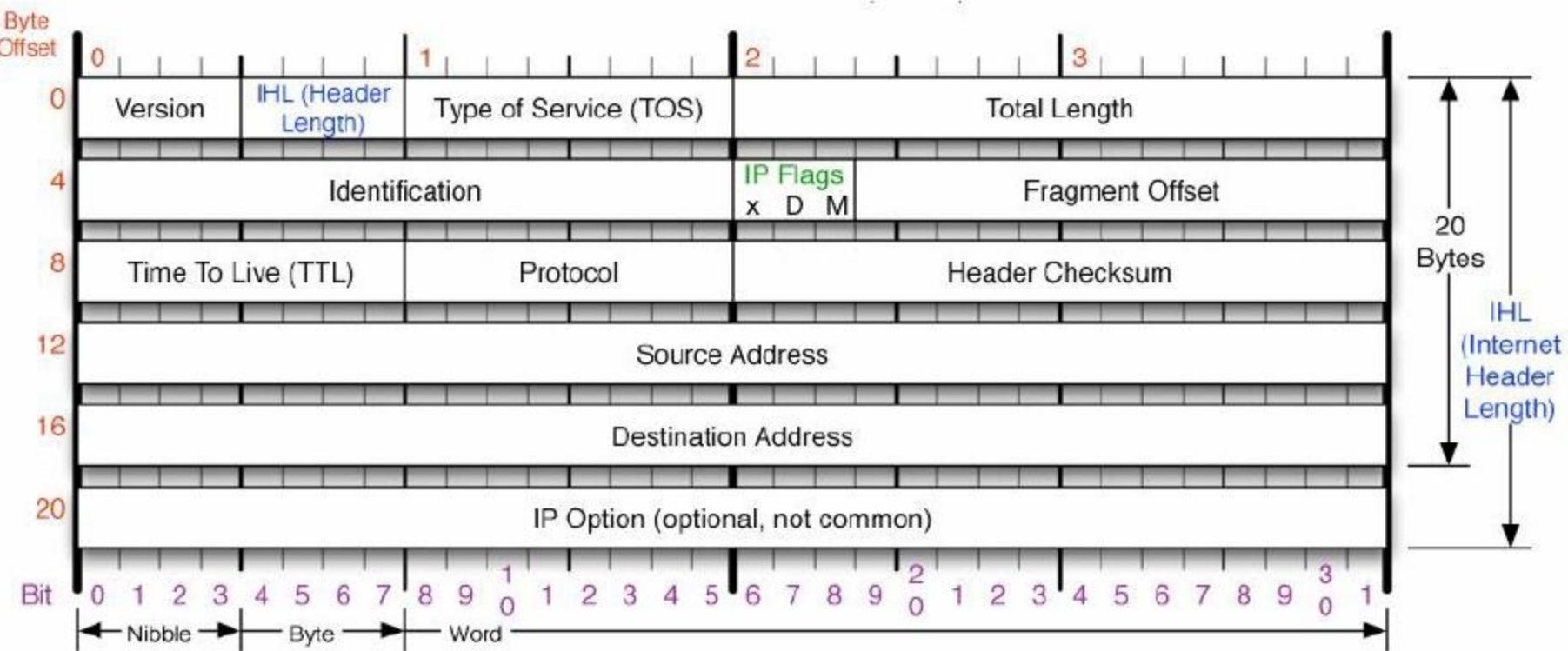


IPv4 Header

IP Header - Internet Protocol Datagram	
Version:	4
Header Length:	5 (20 bytes)
Differentiated Services:	\$00000000
	0000 00.. Default
00 Not-ECT
Total Length:	1500
Identifier:	28897
Fragmentation Flags:	\$010
	0.. Reserved
	.1. Do Not Fragment
	..0 Last Fragment
Fragment Offset:	0 (0 bytes)
Time To Live:	52
Protocol:	6 TCP - Transmission Control Protocol
Header Checksum:	0xCAE3
Source IP Address:	222.231.51.77
Dest. IP Address:	192.168.50.122



IP Header 포맷



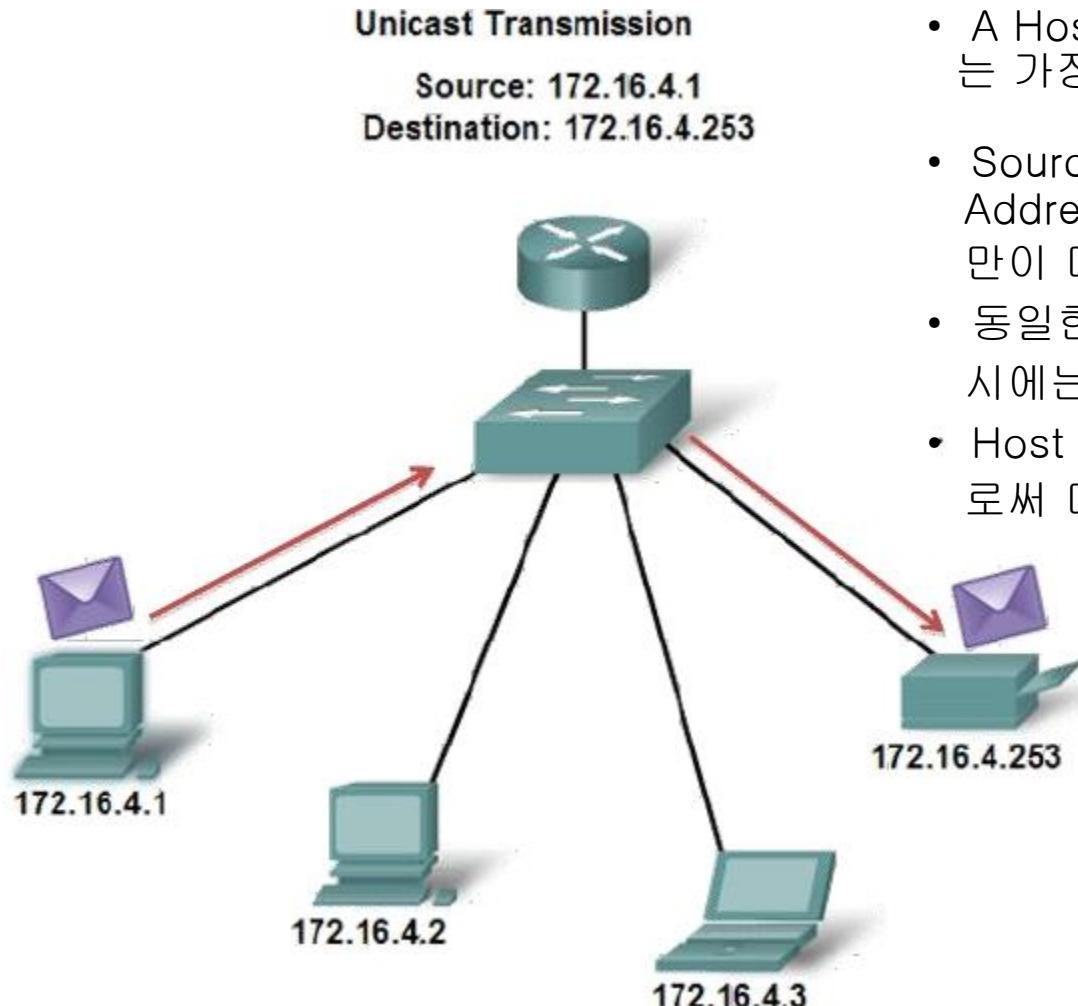


IP Header 설명

필드명	비트	역할
Version	4	IP Protocol Version 정보 현재 인터넷에서 사용되는 Version은 v4 이다.
Header Length	4	IP Header의 길이를 32비트 단위로 나타낸다. (Default 5) $5 \times 32 = 160\text{bit} = 20\text{Byte}$
Type-of-Service Flags	8	Internet의 Application, Host, 그리고 Router에 우선순위 서비스를 제공한다. 이 필드를 설정하여 Datagram의 처리순서를 빠르게 할 수 있다.
Total Packet Length	16	헤더와 몸체를 포함한 전체 IP Packet의 길이를 바이트 단위로 나타낸다.
Fragment Identifier	16	분열이 발생한 경우 조각을 다시 결합하는 일을 돋기 위한 조각들이 속한 원래의 Datagram을 나타낸다.
Fragmentation Flags	3	현재의 분열상태의 단서 제공 3Bit중 마지막2Bit만 사용 (첫번째 Bit는 예비용 두번째 Bit는 분열허용여부 (0 : 허용 1 : 허용 안됨) 세번째 Bit는 현재의 조각이 마지막인지 여부 표시 마지막 인 경우 0 더 있으면 1로 표기한다.
Fragmentation Offset	13	8바이트의 오프셋으로 조각에 저장된 원래 Datagram의 바이트 범위를 나타낸다.
Time-to-Live	8	Datagram이 전달 불가능한 것으로 판단되어 소멸되기 이전에 Datagram이 이동할 수 있는 단계의 수를 나타낸다.
Protocol Identifier	8	IP Datagram의 몸체에 저장된 상위 계층 프로토콜을 나타낸다.
Header Checksum	16	IP 헤더의 Checksum을 저장한다.
Source IP Address	32	Datagram을 전송한 원래 컴퓨터의 32비트의 IP Address이다.
Destination IP Address	32	Datagram 수신할 최종목적지의 32비트 IP Address이다.
Option	가변	IP가 Type-of-Service를 통해 우선순위 서비스를 제공하는 것처럼 Option 필드를 사용하여 특별한 처리 옵션을 추가로 정의할 수 있다. 보통의 경우에는 사용되지 않음.
Padding	가변	IP 헤더의 길이는 32비트 단위여야 한다. 헤더에 옵션이 추가되면 헤더는 32비트로 나눠 떨어지도록 부족분이 채워져야 한다.



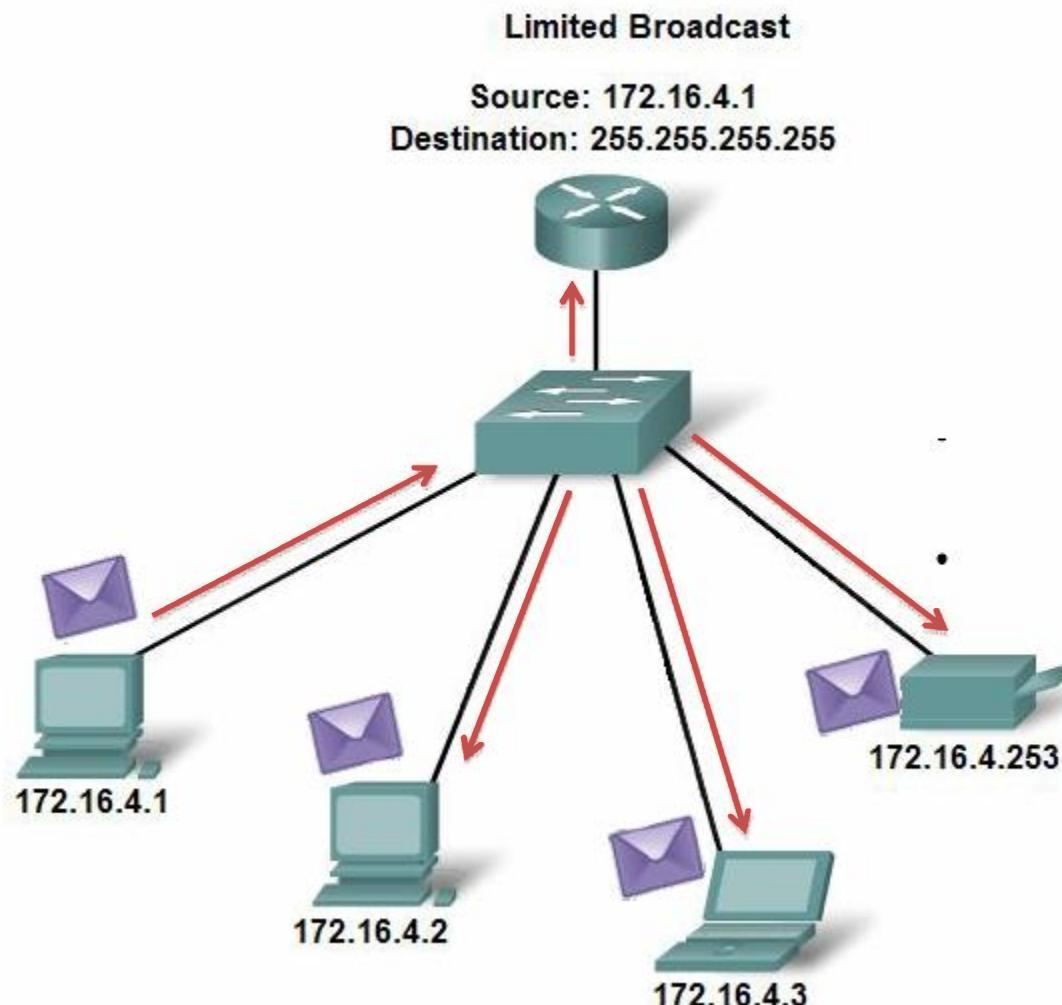
데이터 전송타입 (Unicast)



- A Host가 B Host에게 Data를 전달하는 가장 일반적인 방법이다.
- Source Address와 Destination Address를 명시하여 해당하는 장비만이 데이터를 처리하는 방법이다.
- 동일한 정보를 많은 호스트에 전달 시에는 비 효율적인 방법일수 있다.
- Host to Host 전달을 기반으로 함으로써 다른 Host에 부하는 주지 않는다.



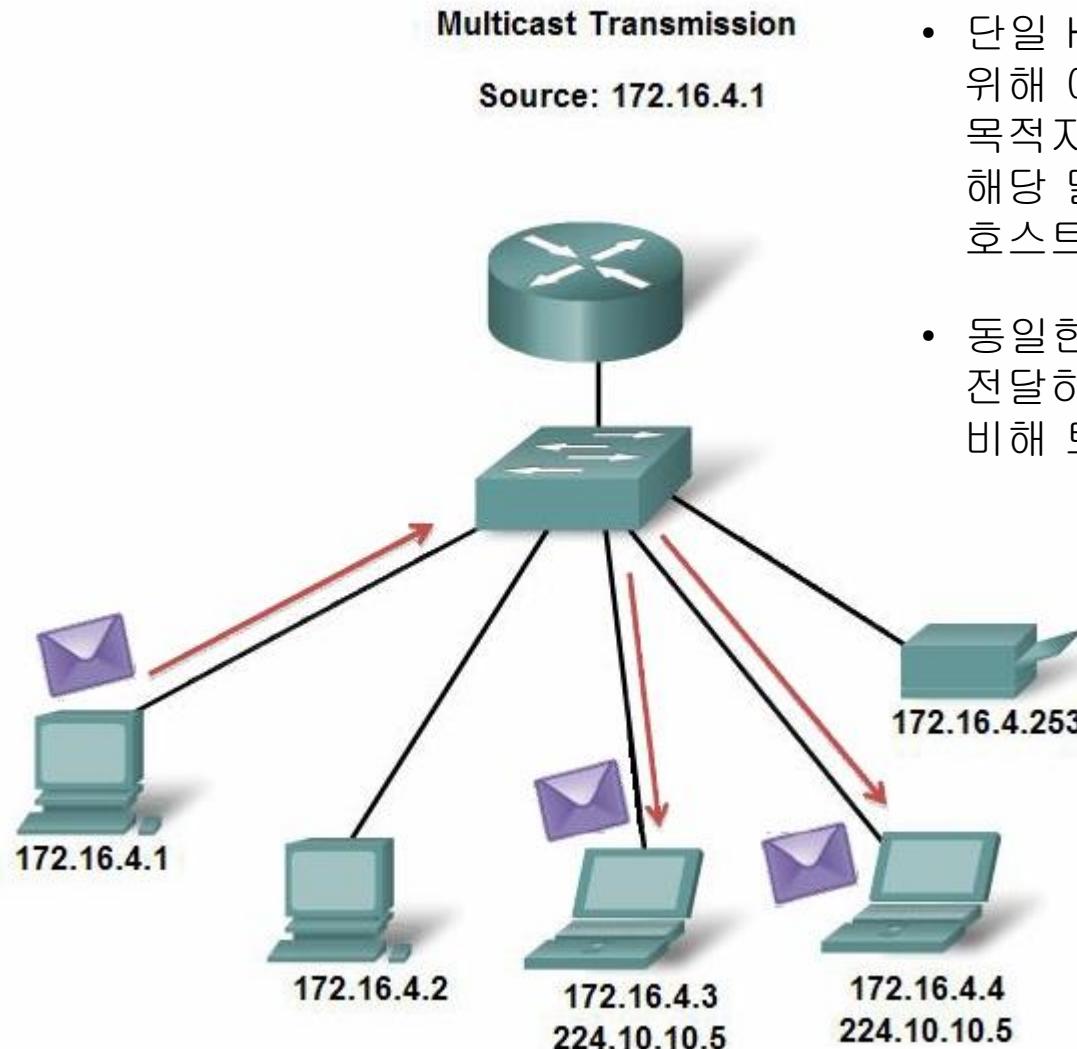
데이터 전송타입 (Broadcast)



- 단일 Host가 Segment에 모든 호스트를 대상으로 Data를 전달 시 사용된다.
- 목적지 주소를 각 주소에 예약된 Broadcast Address를 입력하여 전달한다. 모든 호스트는 이 메시지를 수신한다.
- 동일한 정보를 한번에 모든 호스트에게 전달하는 장점을 갖는다.
- 많은 Broadcast는 호스트의 성능저하를 가져온다.



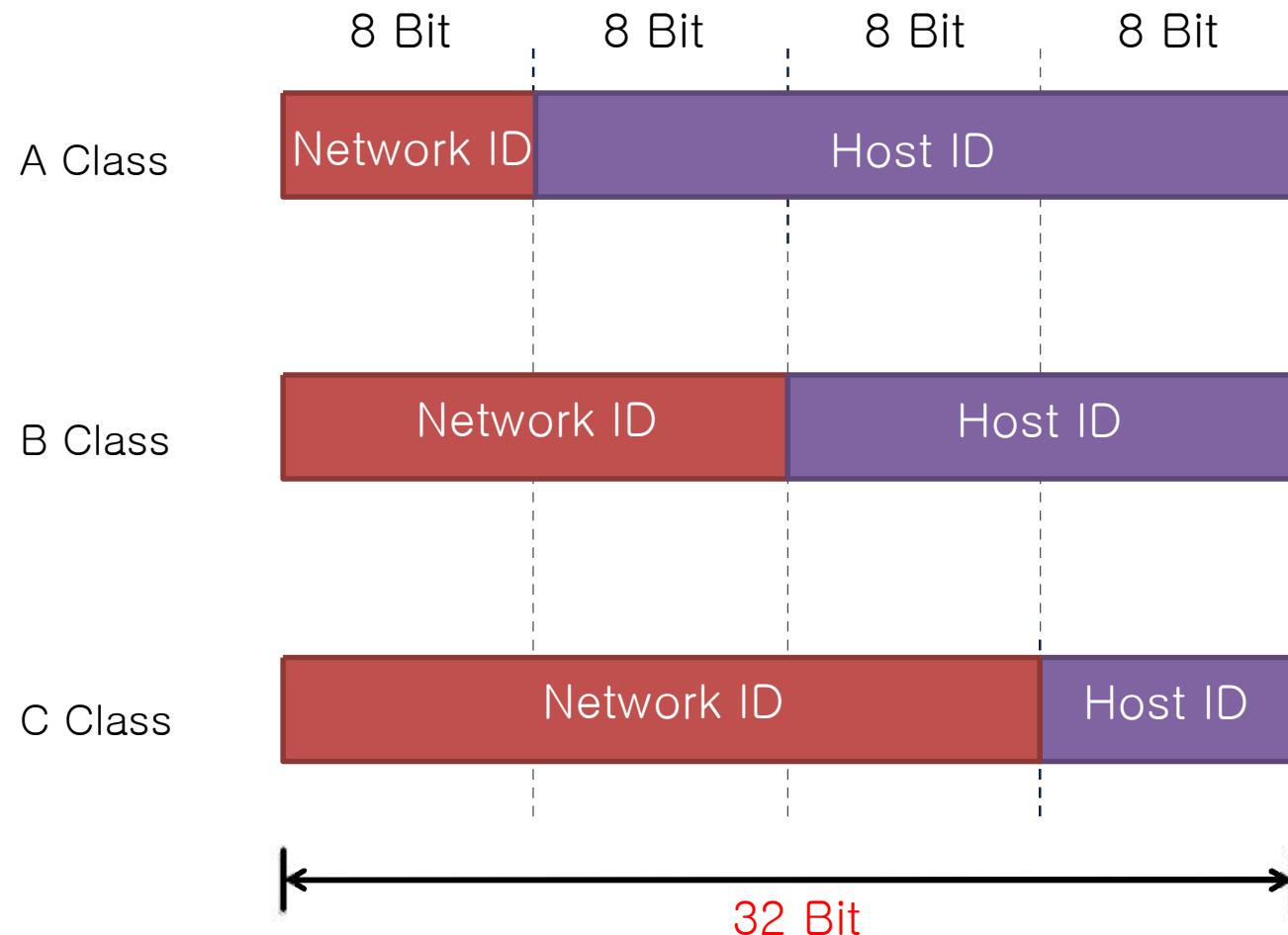
데이터 전송타입 (Multicast)



- 단일 Host가 여러 호스트에 데이터를 보내기 위해 예약된 주소 (Multicast Address)를 목적지 주소로 설정하여 전달 한다. 해당 멀티캐스트를 수신하도록 설정된 모든 호스트는 이 메시지를 수신한다.
- 동일한 정보를 한번에 여러 호스트에게 전달하는 장점을 갖는다. 특히 유니캐스트에 비해 트래픽을 현저히 줄일 수 있다.



IPv4 주소의 클래스



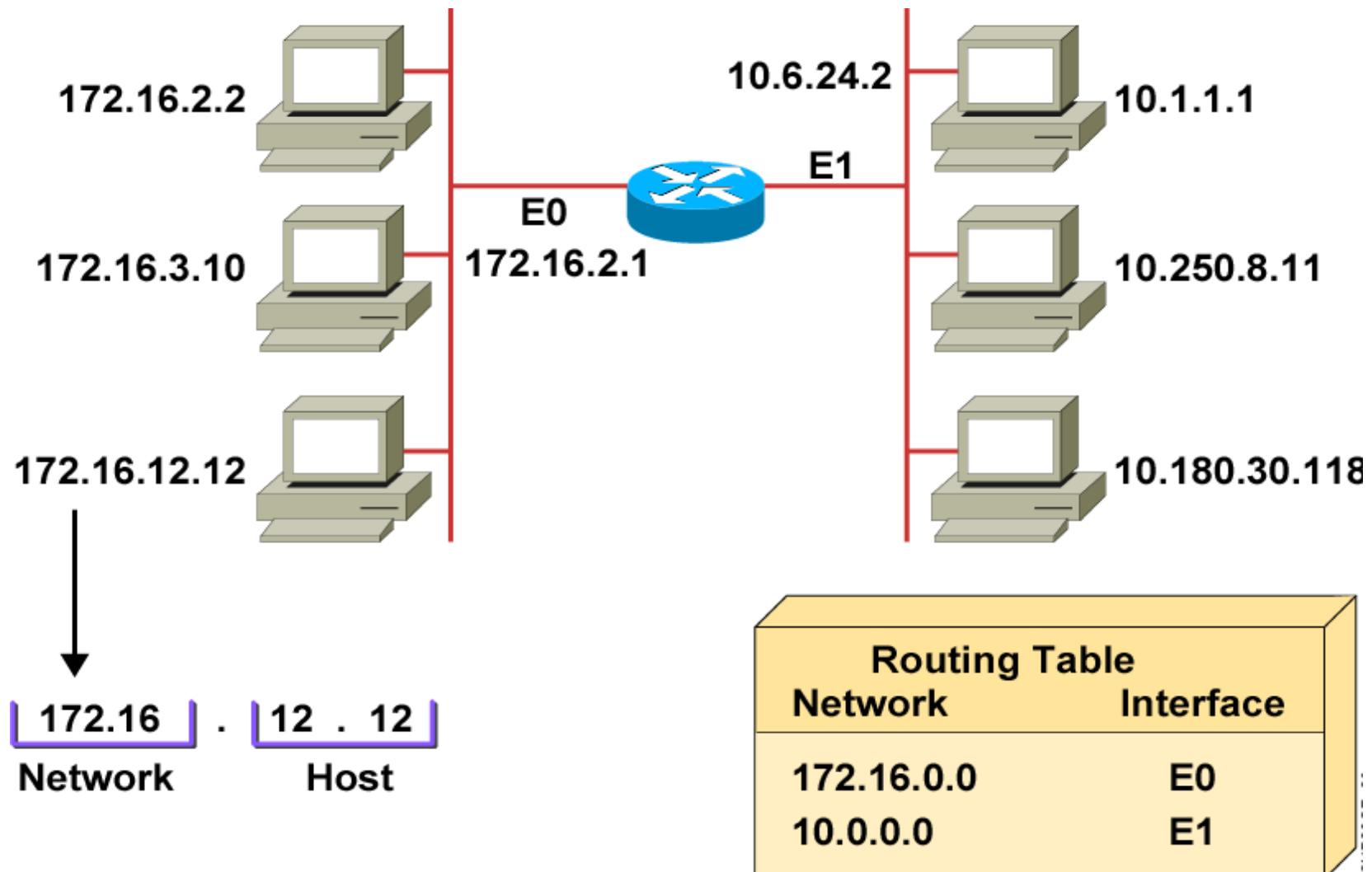


IP Address Class 구분 (사용 가능한 IP)

Class	IP 주소의 첫번째 옥텟	첫째 옥텟의 최소값 (2진수)	첫째 옥텟의 최대값 (2진수)	첫째 옥텟의 값의 범위 (10진수)	이론적 IP 주소 범위
A Class	0xxx xxxx	0000 0001	0111 1110	1 ~126	1.0.0.0 ~ 126.255.255.255
B Class	10xx xxxx	1000 0000	1011 1111	128 ~ 191	128.0.0.0 ~ 191.255.255.255
C Class	110x xxxx	1100 0000	1101 1111	192 ~ 223	192.0.0.0 ~ 223.255.255.255
D Class	1110 xxxx	1110 0000	1110 1111	224 ~ 239	224.0.0.0 ~ 239.255.255.255
E Class	1111 xxxx	1111 0000	1111 1111	240 ~ 255	240.0.0.0 ~ 255.255.255.255

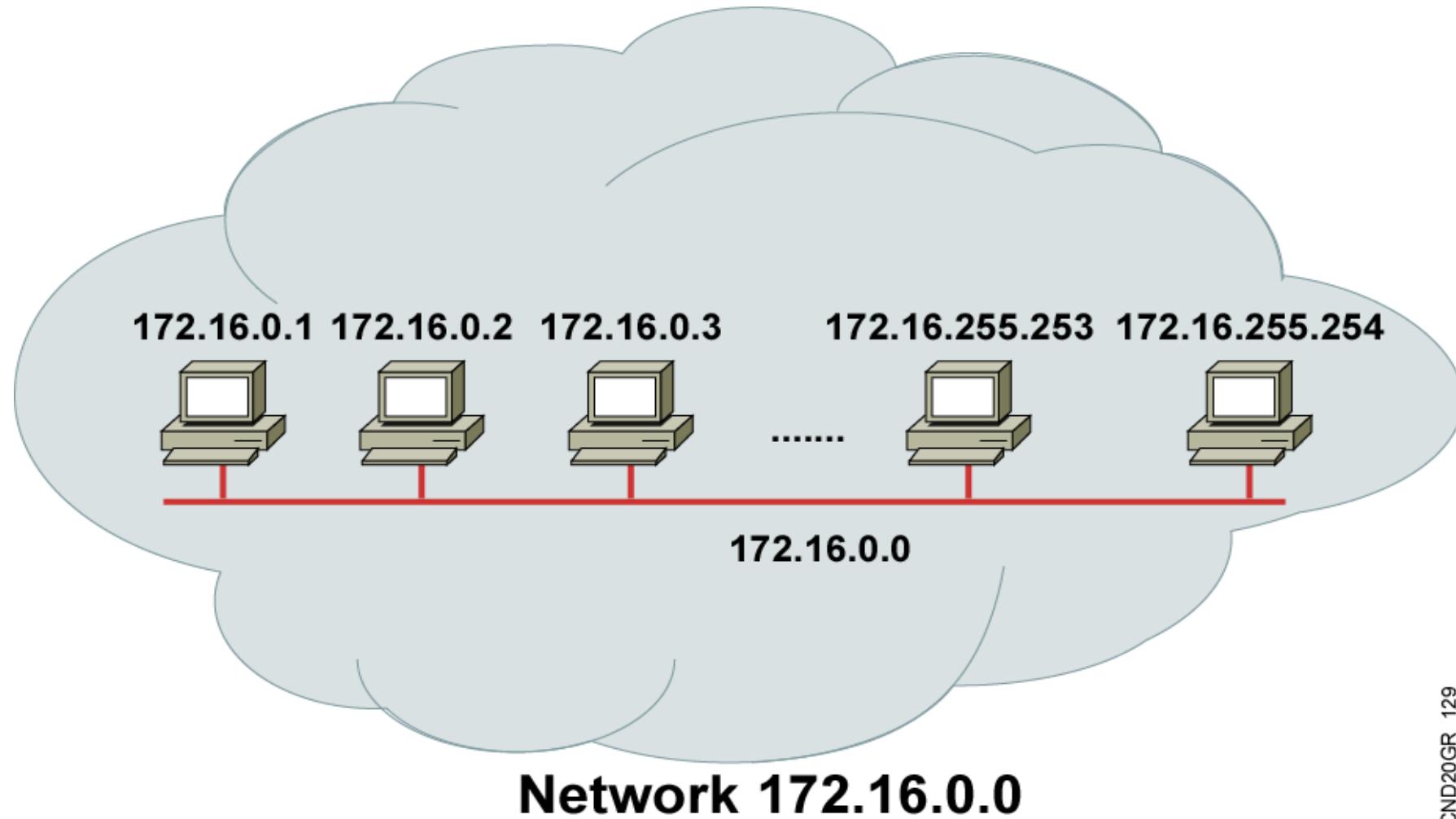


네트워크 주소와 호스트 주소



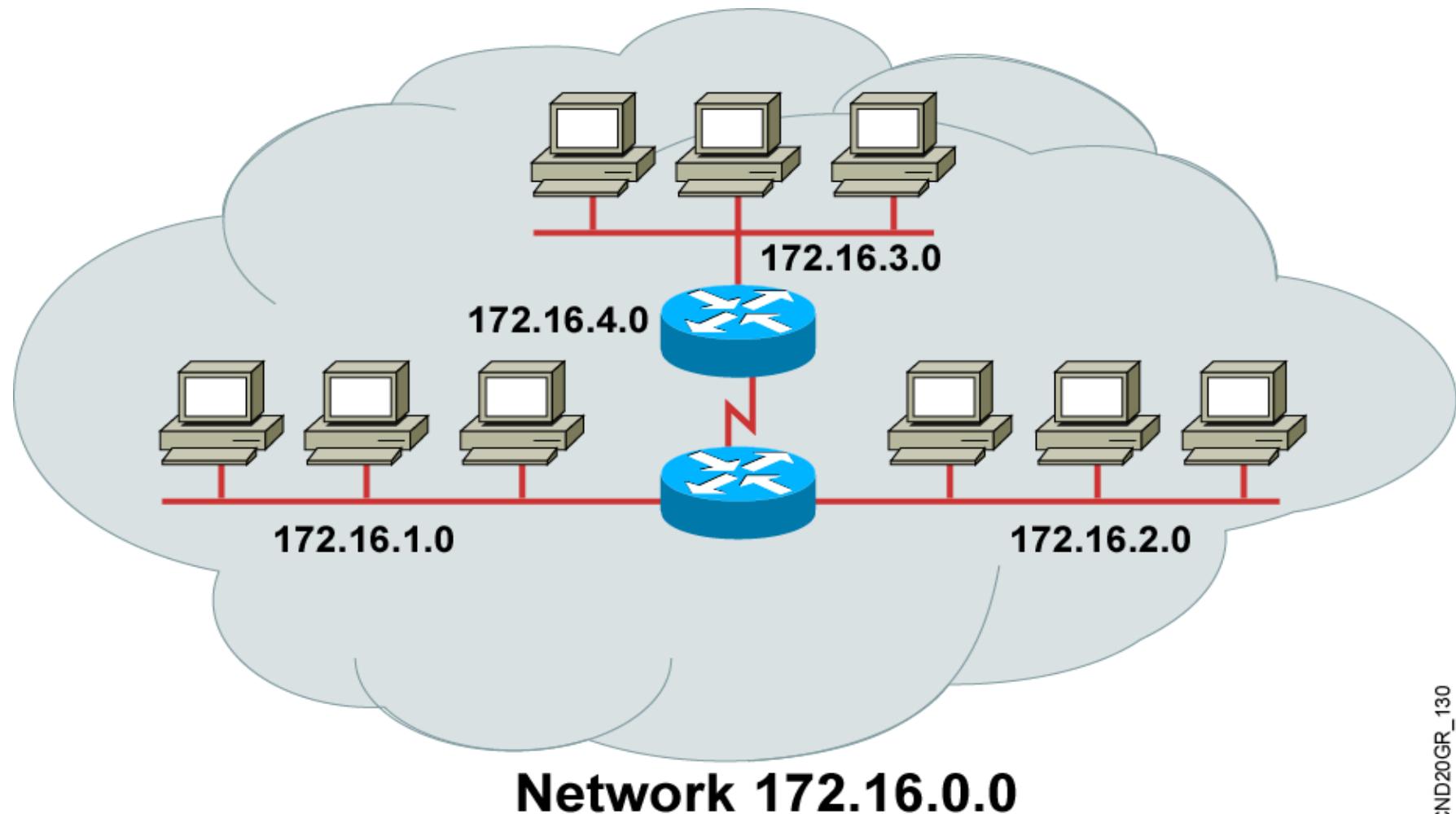


서브네팅하지 않고 IP주소 할당하는 경우



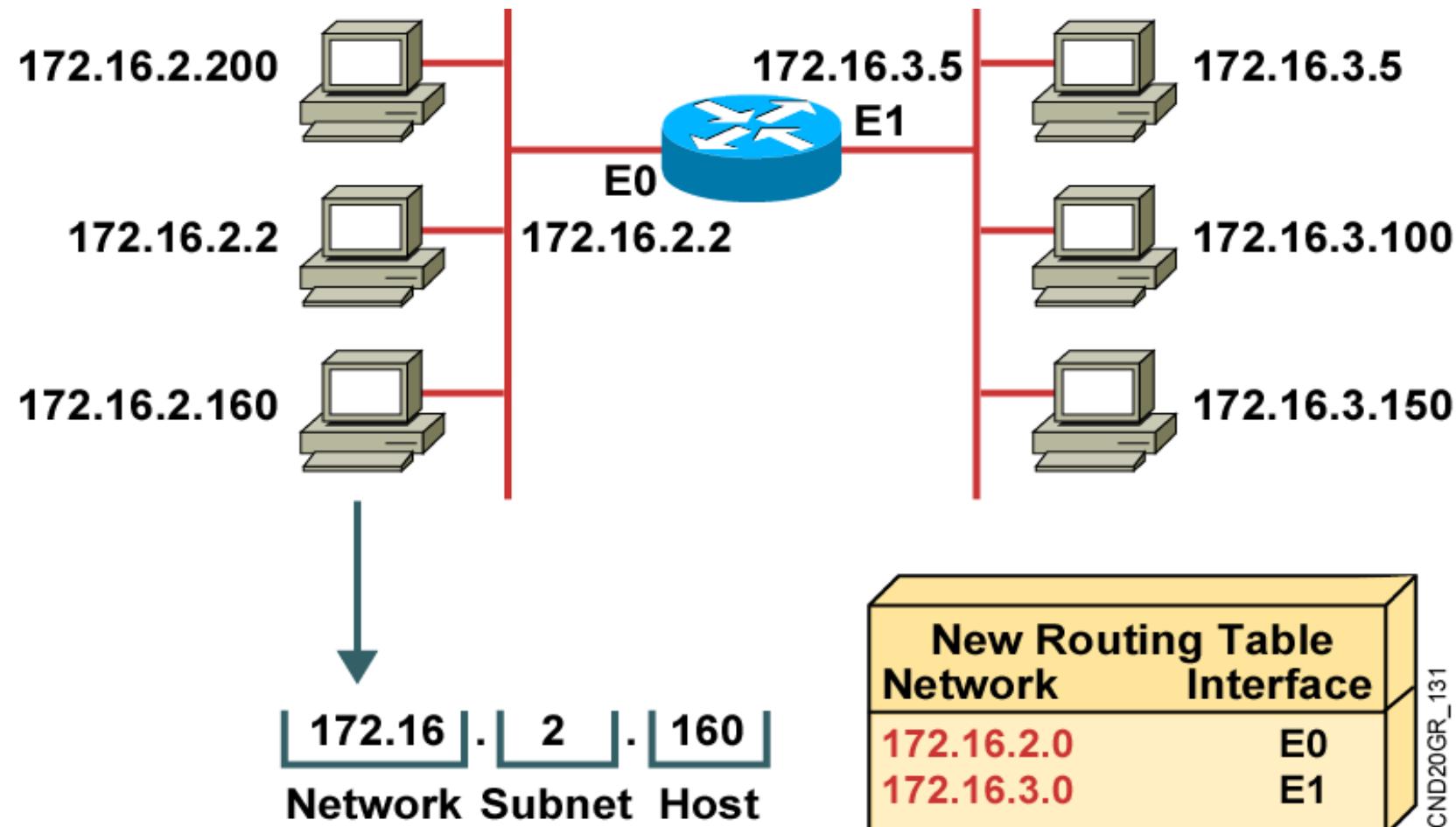


서브네팅을 이용하여 IP주소 할당하는 경우



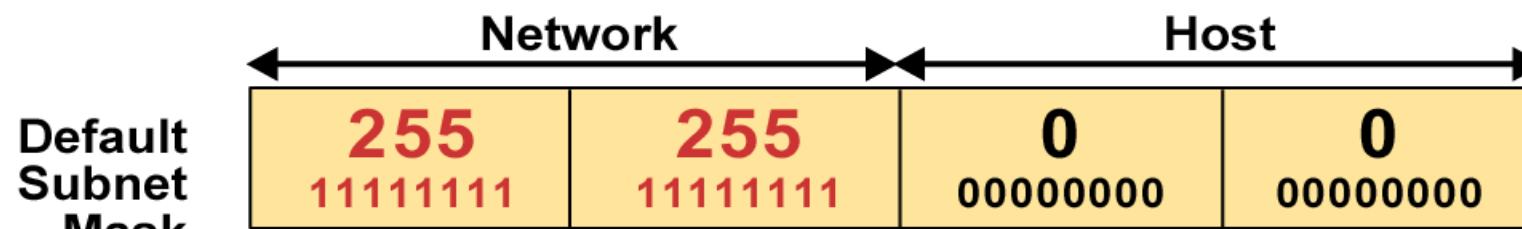
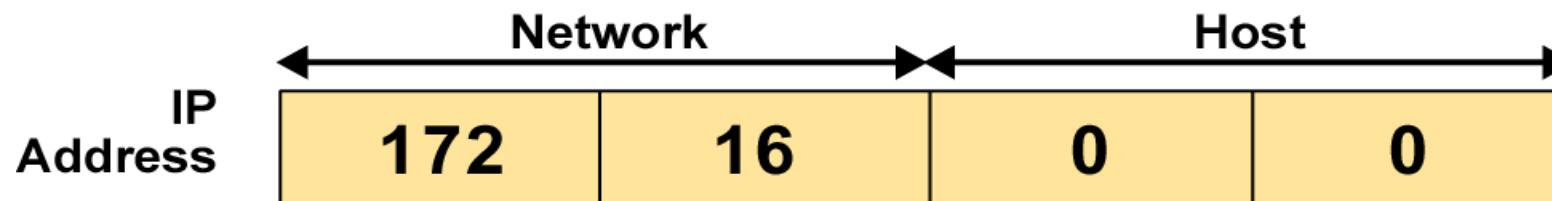


서브넷 주소 할당

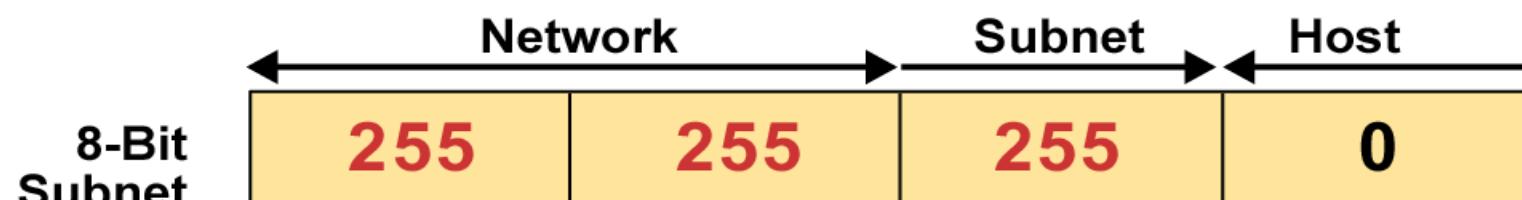




서브넷 마스크(Subnet Mask)



- Also written as “/16,” where 16 represents the number of 1s in the mask



- Also written as “/24,” where 24 represents the number of 1s in the mask



비트에 대응하는 10진수(2진수를 10진수로 변환)



Default Netmask

	Network			Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
	10101100	00010000	00000000	00000000
Network Number	172	16	0	0

- 기본적으로 클래스풀 네트워크에는 서브넷이 사용되지 않는다.
- 클래스풀 네트워크에서 네트워크부분을 가리키는 것이 디폴트 넷마스크이다.



Subnetmask를 이용한 Network Subnetting

	Network		Subnet	Host
172.16.2.160 255.255.255.0	10101100 11111111	00010000 11111111	00000010 11111111	10100000 00000000
	10101100	00010000	00000010	00000000
Network Number	172	16	2	0

- Network ID를 나타내는 비트의 개수가 16개에서 24개로 확장된다.



Subnetmask를 이용한 Network Subnetting (계속)

	Network		Subnet	Host
172.16.2.160	10101100	00010000	00000010	10100000
255.255.255.192	11111111	11111111	11111111	11000000
	10101100	00010000	00000010	10000000

Below the table, there is a diagram showing the binary representation of the IP address and subnet mask, with their decimal equivalents:

128	192	224	240	248	252	254	255
128	192	224	240	248	252	254	255

Network Number

172	16	2	128
-----	----	---	-----

- Network ID를 나타내는 비트의 개수가 24개에서 26개로 확장된다.



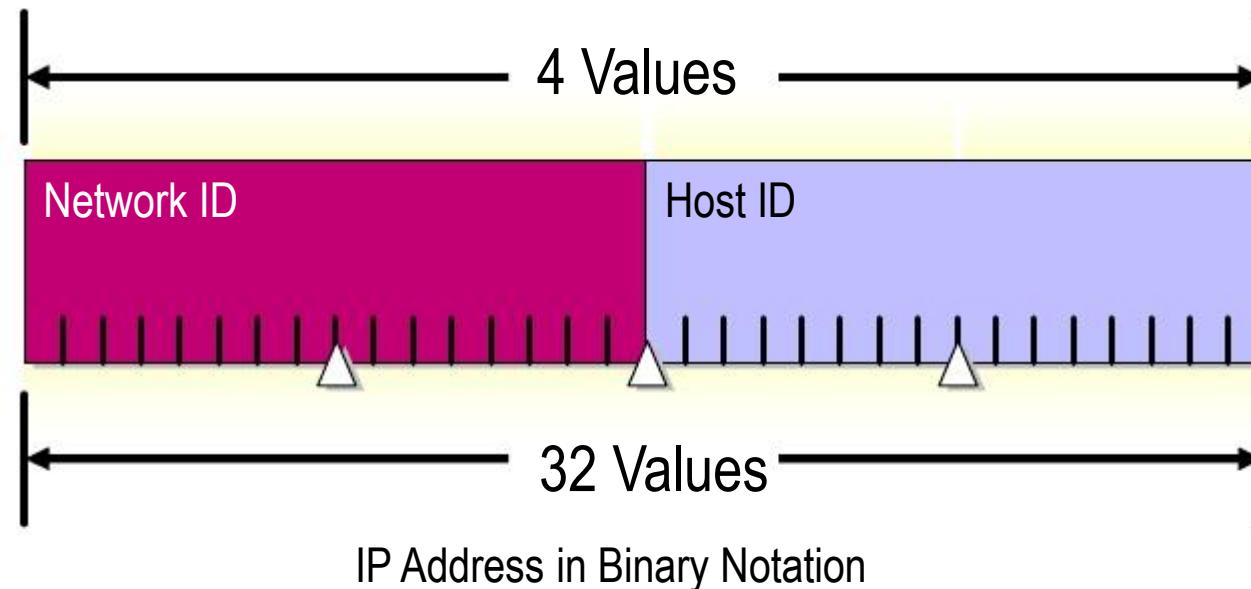
Multicast Address

범위 시작 주소	범위 끝 주소	설명
224.0.0.0	224.0.0.255	유명한 특수 멀티캐스트 주소로 예약
224.0.1.0	238.255.255.255	전역 범위 (인터넷 전체) 멀티캐스트 주소
239.0.0.0	239.255.255.255	관리용(로컬) 멀티캐스트 주소

주 소	설 명
224.0.0.0	예약됨. 쓰이지 않음
224.0.0.1	서브넷의 모든 장비
224.0.0.2	비 서브넷의 모든 라우터
224.0.0.3	예약됨.
224.0.0.4	DVMRP를 사용하는 모든 라우터
224.0.0.5	OSPF가 동작되는 모든 라우터
224.0.0.6	OSPF네트워크에서 DR로 지정된 라우터
224.0.0.9	RIP-2로 지정된 라우터
224.0.0.10	EIGRP를 사용하는 라우터
224.0.0.12	DHCP 서버/중계 애이전트



CIDR(Classless Inter-Domain Routing)



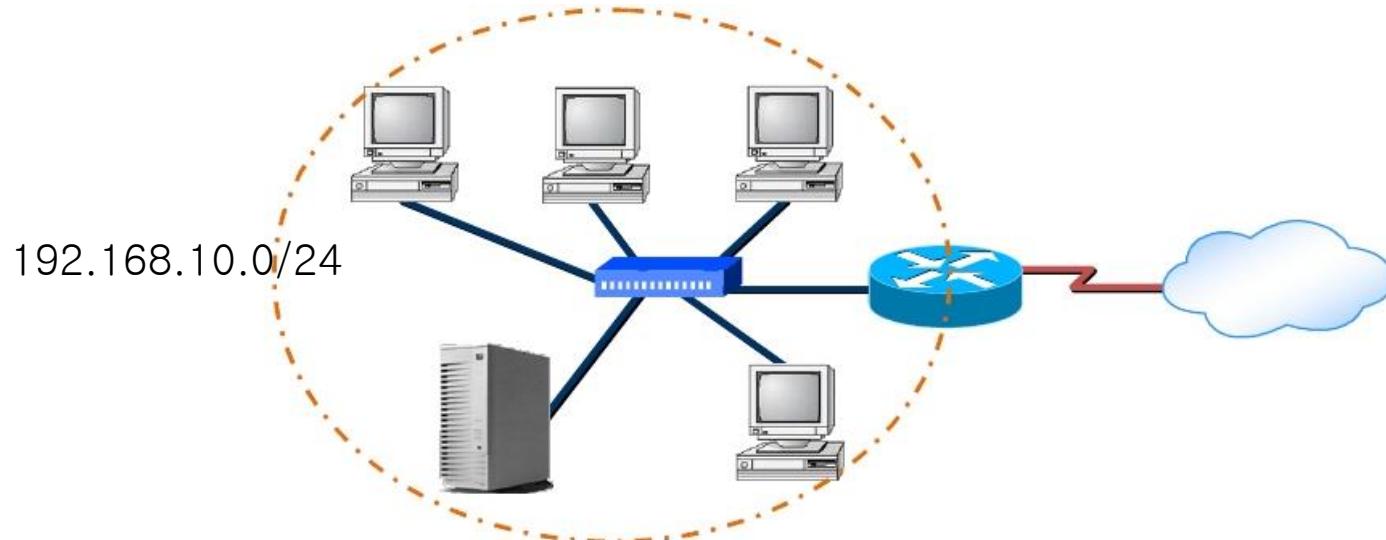
00001010 11011001

01111011 00000111

CIDR(Classless Inter-Domain Routing)은 클래스 없는 도메인 간 라우팅 기법으로 1993년 도입되기 시작한, IP 주소 할당 방법이다. 사이더는 기존의 IP 주소 할당 방식이었던 네트워크 클래스를 대체하였다. 사이더는 IP 주소의 영역을 여러 네트워크 영역으로 나눌 때 클래스별로 나누던 기존방식에 비해 유연성을 더해준다. 또한 급격히 부족해지는 IPv4 주소를 보다 효율적으로 사용할 수 있도록 해주었다. 접두어(Prefix)를 이용한 주소 지정 방식을 가지는 계층적 구조를 사용함으로써 인터넷 광역 라우팅의 부담을 줄여준다.



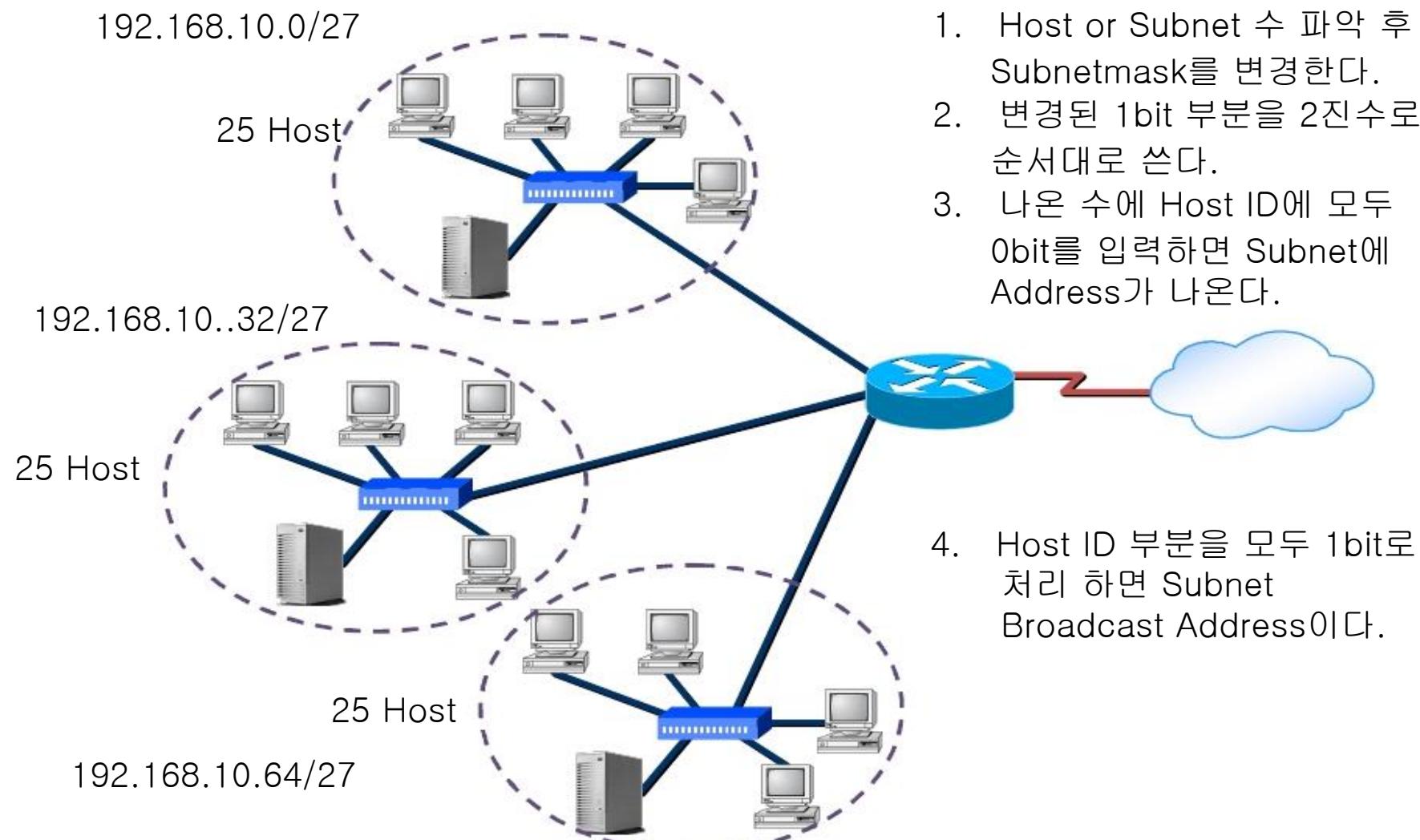
서브네팅(Subnetting)



- Broadcast Domain에 많은 호스트가 연결된 경우 호스트에서 발생한 Broadcast 트래픽이 모든 호스트에 전달되고 브로드캐스트를 받은 호스트는 무조건 해당 트래픽에 대한 처리를 해야한다. 이렇듯 브로드캐스트 도메인의 규모가 크면 그 내부에 있는 호스트들은 처리해야 할 브로드캐스트가 비약적으로 늘어난다. 따라서 브로드캐스트 도메인의 규모를 줄일 필요가 있다. 또한, 하나의 Broadcast Domain에서는 보안이 취약하기 때문에 Firewall이나 ACL과 같은 정책을 구현하기 위해서는 Network Segment를 나누는 것이 효율적이다.
이와 같이 클래스풀 네트워크를 작은 규모의 네트워크 세그먼트로 나누는 것을 서브네팅이라고 한다. 서브네팅을 하면 클래스풀 네트워크에 비해 IP를 효율적으로 할당할 수 있다.
- ISP업체에서는 회선을 임대한 기업들에 IP를 할당하기 위하여 Subnetting을 한 후에 IP를 할당하여 주소를 절약한다.



Subnet 구조





VLSM (Variable Length Subnet Mask)

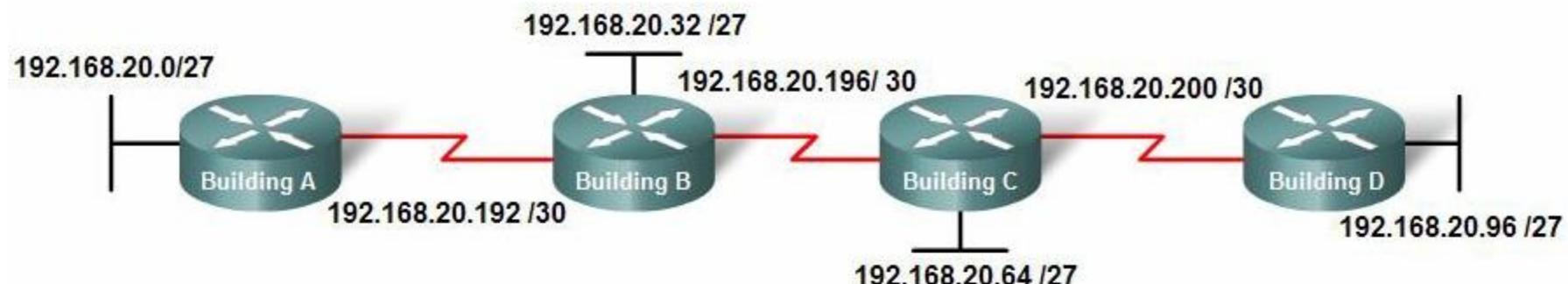
- ▶ VLSM : variable-length subnet mask (가변 길이 서브넷 마스크)

VLSM은 쉽게 말해 하나의 서브넷을 다시 서브네팅하는 것이다.

- 서로 다른 서브넷에서 동일한 네트워크 번호로 다른 서브넷 마스크를 지정할 수 있는 특성
- VLSM은 동일 네트워크 주소를 서브넷 마스크의 길이를 변경해 가며, 필요한 IP개수를 할당하기 때문에 가용 주소 공간을 최적화하는데 도움이 된다.



VLSM 예제



Subnet Number	Subnet Address
Subnet 0	192.168.20.0/27
Subnet 1	192.168.20.32/27
Subnet 2	192.168.20.64/27
Subnet 3	192.168.20.96/27
Subnet 4	192.168.20.128/27
Subnet 5	192.168.20.160/27
Subnet 6	192.168.20.192/27
Subnet 7	192.168.20.224/27

Subnet Number	Subnet Address
Subnet 0	192.168.20.192/30
Subnet 1	192.168.20.196/30
Subnet 2	192.168.20.200/30
Subnet 3	192.168.20.204/30
Subnet 4	192.168.20.208/30
Subnet 5	192.168.20.212/30
Subnet 6	192.168.20.216/30
Subnet 7	192.168.20.220/30



ICMP (Internet Control Message Protocol)

- ▶ IP는 신뢰성을 보장하지 않는다. 따라서 네트워크 장애나 중계 라우터 등의 에러에 대처 할 수 없다. 이런 경우 수신측에서 송신측으로 데이터의 사고에 대한 내용을 전달할 필요가 있다. ICMP는 이와 같은 오류 정보를 발견 송신측에 메시지를 전달하는 기능을 한다.

ICMP - Internet Control Messages Protocol	
ICMP Type:	8 Echo Request
ICMP Code:	0
ICMP Checksum:	0x2D5C
Identifier:	0x0200
Sequence Number:	0x001E
ICMP Data Area:	(32 bytes)

ICMP - Internet Control Messages Protocol	
ICMP Type:	0 Echo Reply
ICMP Code:	0
ICMP Checksum:	0x355C
Identifier:	0x0200
Sequence Number:	0x001E
ICMP Data Area:	(32 bytes)

Type	Message
0	에코 응답 (Echo Reply)
3	수신처 도달 불가 (Destination Unreachable)
4	발신제한 (Source Quench)
5	라우트 변경 (redirect)
8	에코 요청 (Echo Request)
11	시간 초과 (Time Exceeded)
12	파라미터 불량 (Parameter Problem)
13	타임 스탬프 요청 (Timestamp Request)
14	타임 스탬프 응답 (Timestamp reply)
15	정보 요구 (Information Request)
16	정보 응답 (Information Reply)
17	주소 마스크 요구 (Address Mask Request)
18	주소 마스크 응답 (Address Mask Reply)



ICMP Error Message

- ▶ ICMP 에러 메시지를 읽는 가장 쉬운 방법은 메시지를 다룰 수 있는 크기로 나누는 것이다.
 - 메시지의 첫 부분은 항상 보고되는 측정 ICMP 에러 메시지를 나타내며, 메시지의 나머지 부분은 실패한 IP 데이터그램의 헤더와 데이터 첫 8바이트를 포함한다.

Code	Message
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown

<http://www.iana.org/assignments/icmp-parameters>



ICMP Utility : Ping

- ▶ Ping 도구는 ICMP Echo Request 메시지를 전송하여 목적지시스템으로부터 ICMP Echo Reply 메시지로 응답을 받는데 걸린 시간을 측정함으로써 네트워크 연결을 검사할 수 있다.

```
C:\WINDOWS\system32\cmd.exe
C:\>ping www.yahoo.co.kr

Pinging yahoo.co.kr [211.115.99.172] with 32 bytes of data:

Reply from 211.115.99.172: bytes=32 time=22ms TTL=51
Reply from 211.115.99.172: bytes=32 time=23ms TTL=51
Reply from 211.115.99.172: bytes=32 time=22ms TTL=51
Reply from 211.115.99.172: bytes=32 time=22ms TTL=51

Ping statistics for 211.115.99.172:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 22ms, Maximum = 23ms, Average = 22ms
```

```
C:\WINDOWS\system32\cmd.exe
C:\>tracert 59.5.67.254

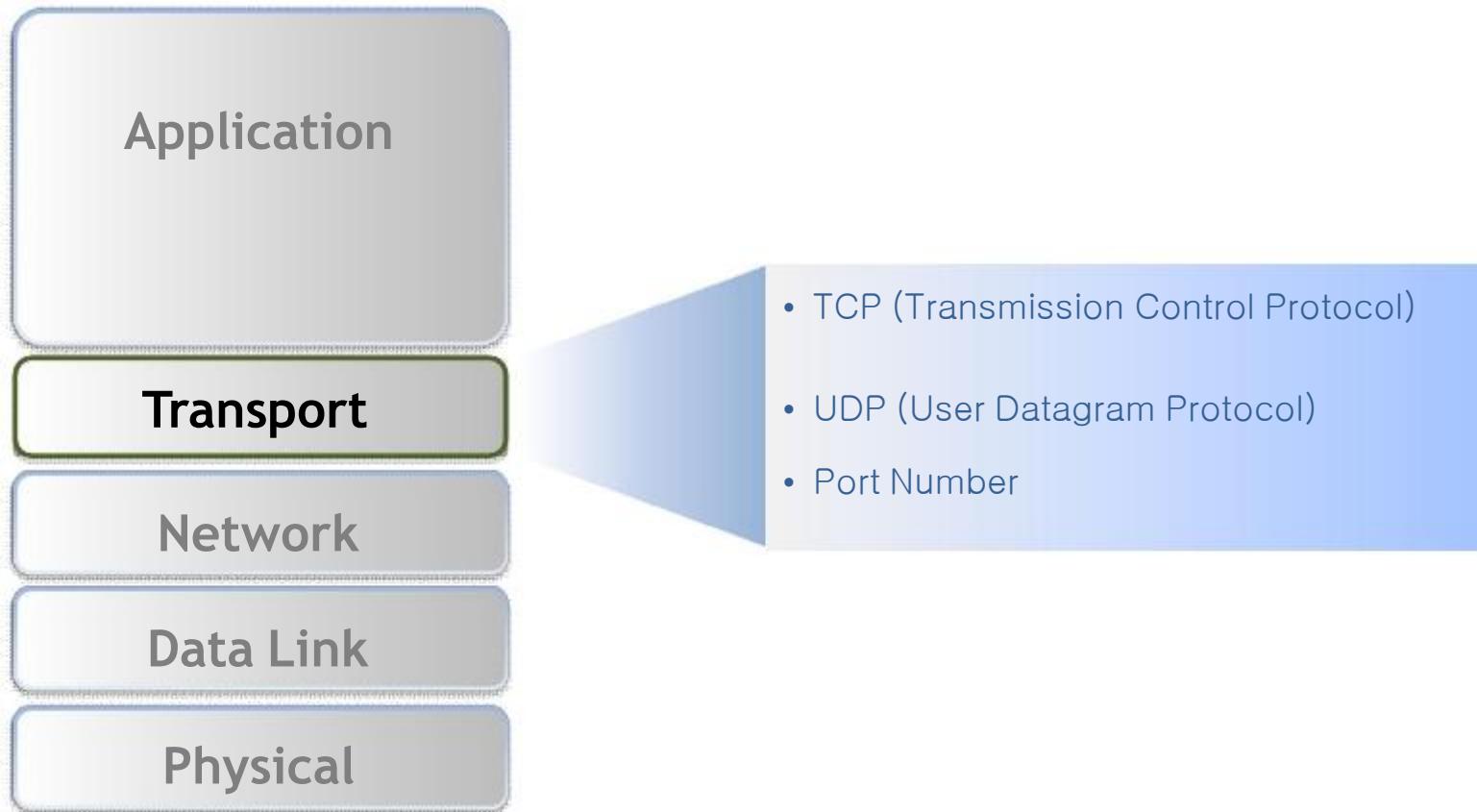
Tracing route to 59.5.67.254 over a maximum of 30 hops

  1      1 ms      <1 ms      1 ms  192.168.50.254
  2     21 ms      21 ms     21 ms  59.5.67.254

Trace complete.
```



전송계층(Transport Layer)





UDP (User Datagram Protocol)

- ▶ IP 네트워크에서 응용프로그램들은 서로 통신하기 위해서 TCP 나 UDP 표준전송 프로토콜을 사용한다. 그 중에서 UDP는 작고 신뢰성이 없지만 오버헤드가 적어서 빠른 전송 서비스를 제공하는 사용자 Datagram Protocol이다.

UDP - User Datagram Protocol	
Source Port:	1025 blackjack
Destination Port:	53 domain
Length:	38
UDP Checksum:	0xDC93

Port	Description
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
137	NetBIOS Name Service (WINS)
161	Simple Network Management Protocol (SNMP)

Source Port	송신 측 호스트의 포트번호
Destination Port	수신 측 호스트의 포트번호
Length	UDP 패킷의 옥텟 단위 길이. 이 길이는 UDP 헤더와 그 데이터를 포함한다. 길이 필드의 최소 값은 8이며 이는 0크기의 데이터 필드를 나타낸다.
UDP Checksum	UDP 헤더 데이터를 포함한 세그먼트 전체에 대하여 계산한 값. 에러 체크에 사용



TCP (Transmission Control Protocol)

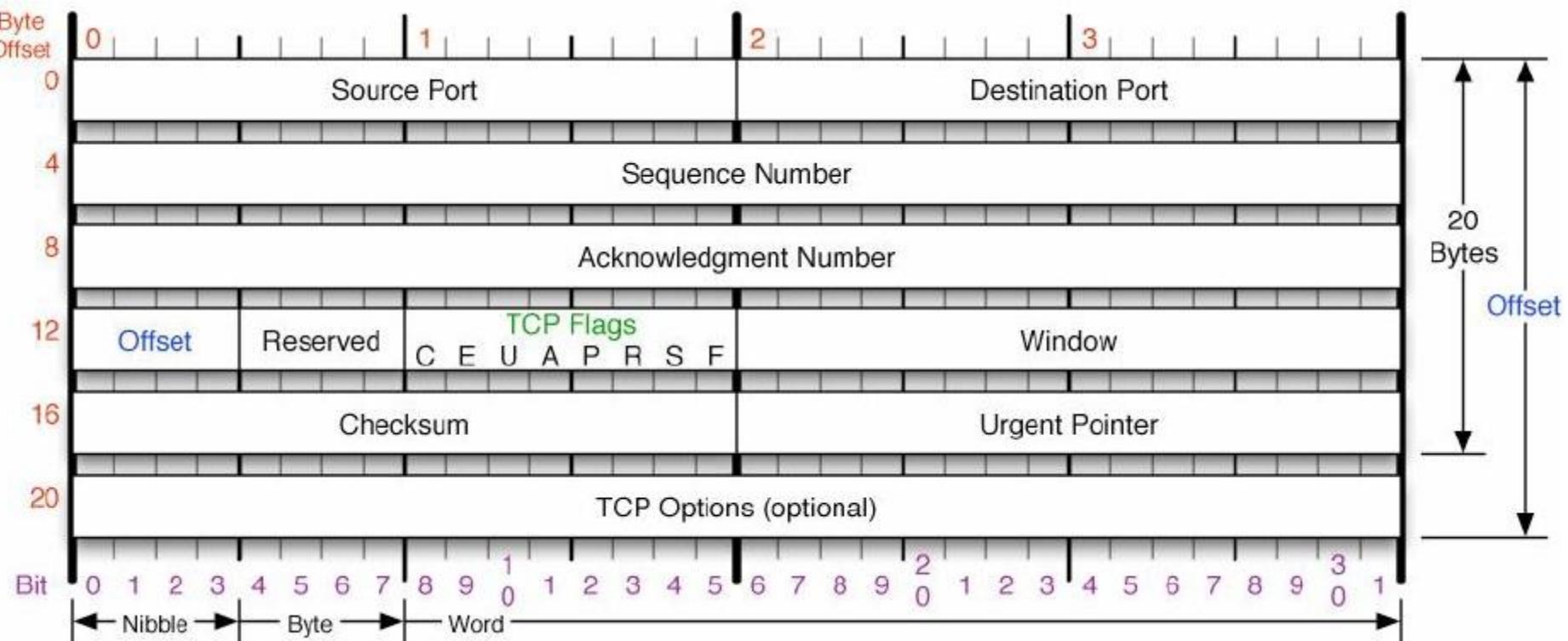
TCP - Transport Control Protocol

- Source Port: 80 http
- Destination Port: 1049 td-postman
- Sequence Number: 3915864790
- Ack Number: 1308743846
- TCP Offset: 5 (20 bytes)
- Reserved: \$0000
- TCP Flags:** \$000010000 ...A....
 - 0..... (No Congestion Window Reduction)
 - .0..... (No ECN-Echo)
 - .0..... (No Urgent pointer)
 - ..1.... Ack
 - ...0... (No Push)
 - ...0.. (No Reset)
 - ...0. (No SYN)
 - ...0 (No FIN)
- Window: 6944
- TCP Checksum: 0x8EC0
- Urgent Pointer: 0
- No TCP Options

Port	Service
21	FTP
23	Telnet
25	SMTP
80	HTTP
110	POP3
194	Internet Relay Chat (IRC)
443	Secure HTTP (HTTPS)
1863	MSN Messenger
8008	Alternate HTTP
8080	Alternate HTTP



TCP Header





TCP Header

- TCP Header :

① Source Port Number (16 bits) : 송신 시스템의 어플리케이션 포트번호

- 클라이언트인 경우 Well-known-port가 아닌 임의의 번호 부여

- 서버인 경우 Well-known-port 사용, HTTP (80), SMTP (20,21), Telnet (23)

② Destination Port Number (16 bits) : 수신할 시스템의 어플리케이션 포트번호

③ Sequence Number (32 bits) : 세그먼트에 들어있는 데이터의 첫 바이트 위치를 일련번호로 기록한다.

- 송.수신 시스템이 데이터를 잘 받았는지 확인하는 중요한 기능으로 사용

- 세그먼트 내의 바이트에 일련번호를 붙이는 기능이다. 데이터가 포함되지 않은 경우는 동일한 번호 사용

- 전송되는 데이터 크기만큼 번호가 증가한다.

- 통신을 개시할 때 처음 시작하는 일련번호를 Initial Sequence Number (ISN)라고 한다.

- Sequence Number는 시스템의 클럭에서 추출된 값을 부여한다.



TCP Header

- ④ Acknowledge Number (32bits) : 상대방으로 부터 수신하고자 하는 다음 데이터 바이트를 기록한다.
 - 데이터를 전송한 송신자에게 잘 받았다고 확인해 주는 번호이다.
(Sequence Number에 대한 확인/인정)
 - 상대방(Sender)이 다음에 전송하는 패킷의 Sequence Number이기도 하다.
- ⑤ Header Length / Data Offset (4bits) : TCP 헤더의 전체 길이를 32 bit 단위로 표현한다.
 - 이 필드는 32 bit의 단위로 사용하며, 최소 '5' (20 Bytes), 최대값 '15' (60 Bytes) 이다.



TCP Header

❖ TCP Flags :

1	A	P	R	S	F
---	---	---	---	---	---

Urgent (Hex:0x20) : Urgent Pointer 필드와 함께 사용되며 즉시 데이터를 처리해야 한다.

- Urgent Pointer가 지정한 일련 번호까지 긴급 데이터가 있으므로 최우선으로 처리해야 한다.

U	1	P	R	S	F
---	---	---	---	---	---

Acknowledge (Hex:0x10) : Synchronize에 대한 확인(인정)

- 모든 세그먼트에는 Ack가 설정되어야 한다.
- (3Way-Hand-Shake의 Syn 과정 및 Reset 제외)

U	A	1	R	S	F
---	---	---	---	---	---

Push (Hex:0x08) : 일반적으로 모든 데이터를 전송하고 나서 마지막에 보내는 신호이다. (전송 버퍼를 즉시 비워라)



TCP Header

U	A	P	1	S	F
---	---	---	---	---	---

Reset (Hex:0x04) : 연결 및 종료를 정상적으로 할 수 없을 때 사용
(주로 서버 메시지)

- 송신자가 유효하지 않은 소켓으로 연결을 시도할 때 이를 거부할 때도 사용된다.

U	A	P	R	1	F
---	---	---	---	---	---

Synchronize (Hex:0x02) : 통신을 시작할 때 연결을 요청한다.
(TCP-Half Open)

- SYN = 1 , ACK = 0 : 연결 패킷 (연결 요청)
- SYN = 1 , ACK = 1 : 연결 수신 통지 (연결 요청 응답)
- SYN = 0 , ACK = 1 : 데이터 또는 ACK 패킷

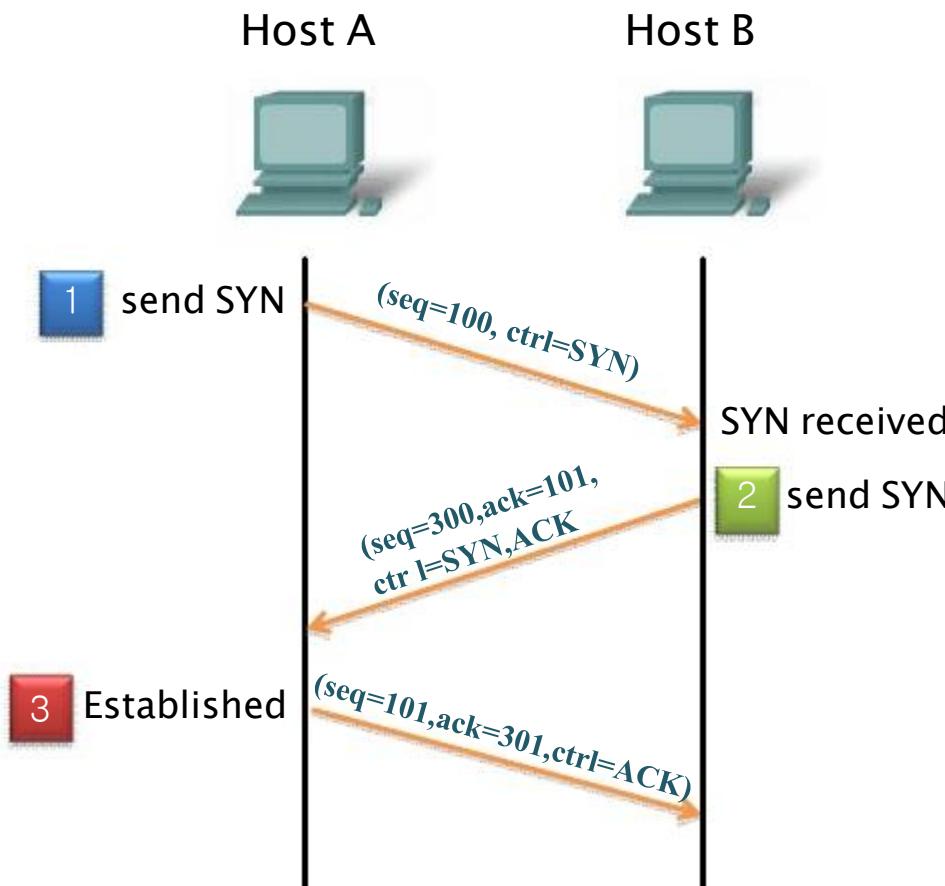
U	A	P	R	S	1
---	---	---	---	---	---

Finish (Hex:0x01) : 데이터가 정상적으로 교환되어 연결을 종료한다.

- 어플리케이션이 종료를 원할 경우 TCP의 FIN을 설정시켜 전송한다.
- TCP-FIN을 받은 시스템도 연결을 종료시킬 준비가 되었다면 TCP-FIN을 맞교환하고 종료한다.



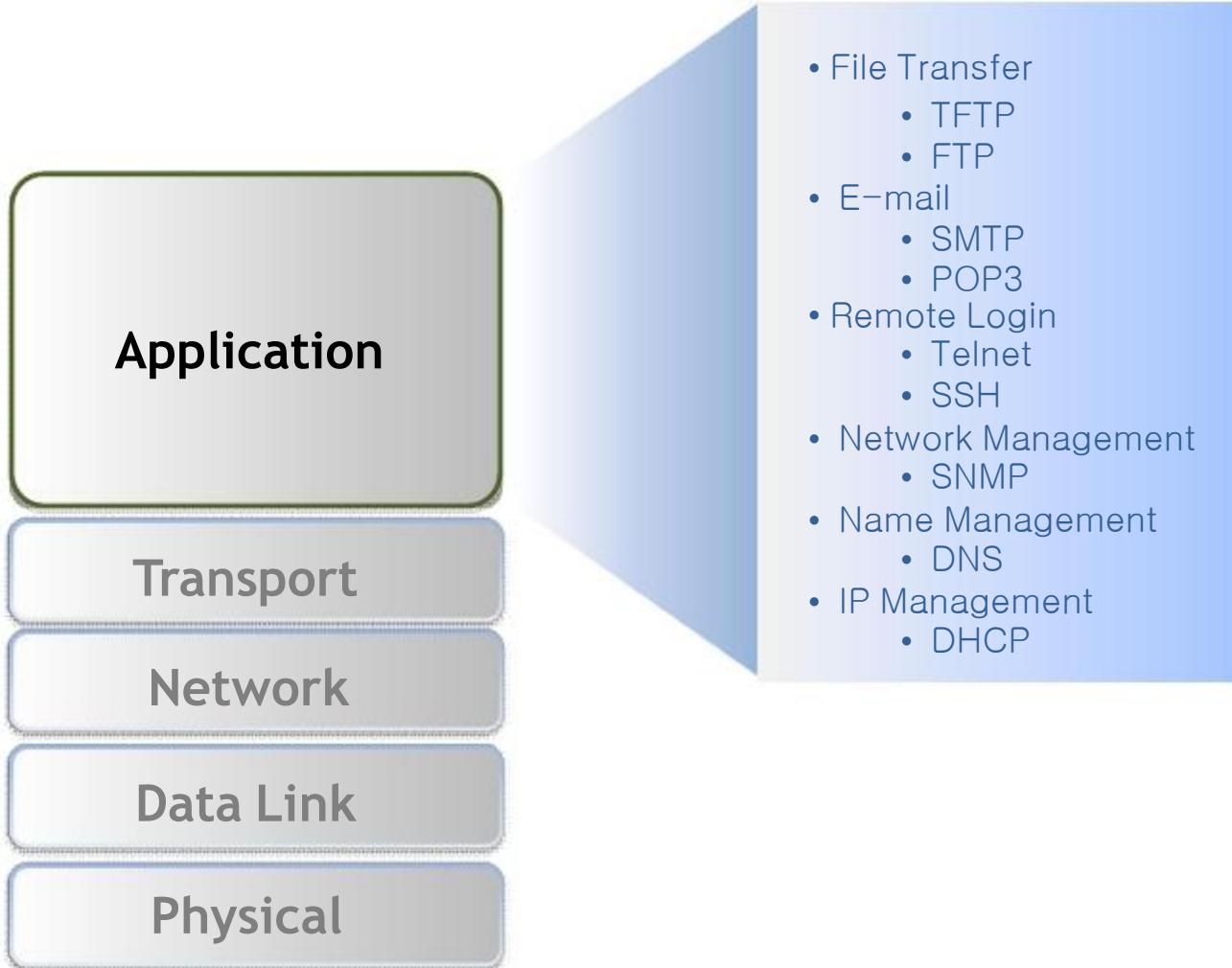
TCP Three way Handshake

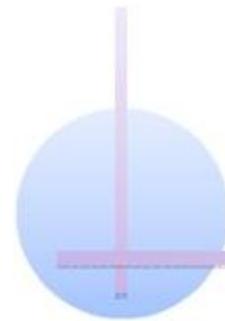


TCP - Transport Control Protocol	
Source Port:	1563 <i>cadabra-lm</i>
Destination Port:	21 <i>ftp</i>
Sequence Number:	677660227
Ack Number:	0
TCP Offset:	7 (28 bytes)
Reserved:	\$0000
+ F=00000010 S .	
Window:	16384
TCP Checksum:	0x5A1D
Urgent Pointer:	0
TCP - Transport Control Protocol	
Source Port:	21 <i>ftp</i>
Destination Port:	1563 <i>cadabra-lm</i>
Sequence Number:	3335109222
Ack Number:	677660228
TCP Offset:	7 (28 bytes)
Reserved:	\$0000
+ F=00010010 . . . A . . . S .	
Window:	16384
TCP Checksum:	0xD92B
Urgent Pointer:	0
TCP - Transport Control Protocol	
Source Port:	1563 <i>cadabra-lm</i>
Destination Port:	21 <i>ftp</i>
Sequence Number:	677660228
Ack Number:	3335109223
TCP Offset:	5 (20 bytes)
Reserved:	\$0000
+ F=00010000 . . . A	
Window:	16560
TCP Checksum:	0x04F0
Urgent Pointer:	0
No TCP Options	



Application Layer Overview





Chapter 02

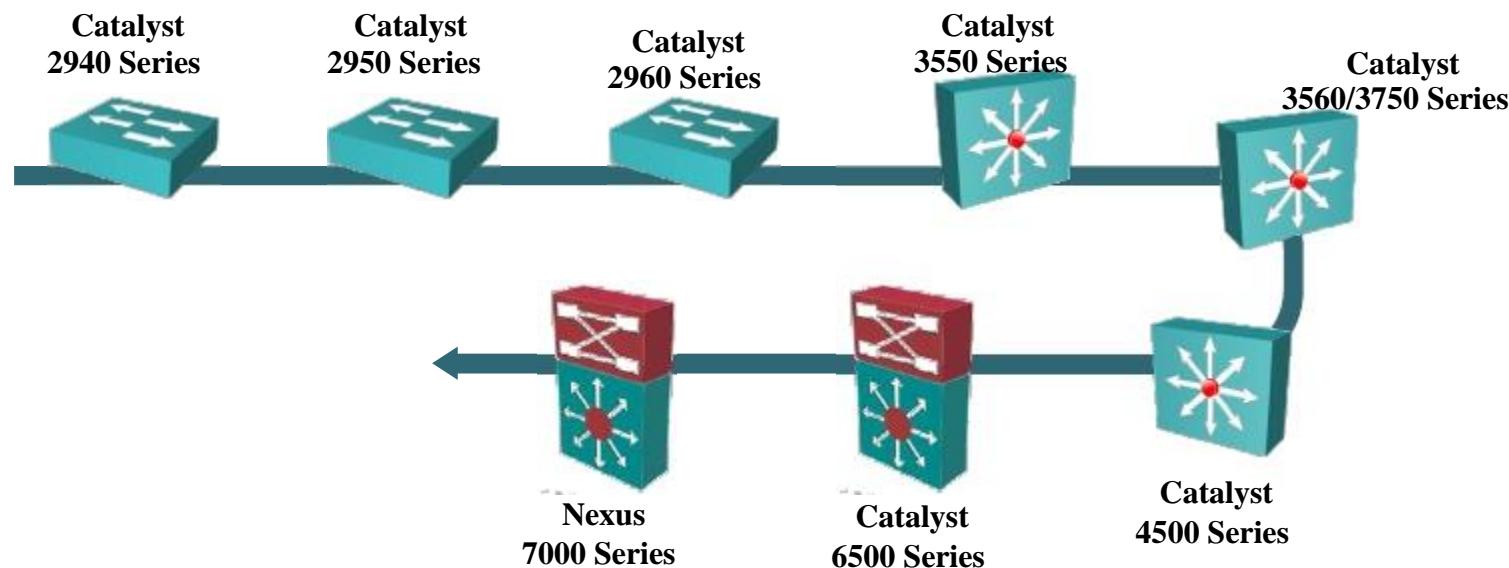
Cisco Device and IOS Basic



Cisco Switch

▶ 선택 기준 :

- 매체 속도 : 10Mbps, 100Mbps, 1000Mbps
- 스위치간 통신(trunking) 필요성
- Workgroup segmentation (VLANs)
- Port 밀도 요구사항





Catalyst Switch Type



**Catalyst
2940 Series**



**Catalyst
2960 Series**



**Catalyst
6500 Series**



**Catalyst
3560 Series**



**Catalyst
4500 Series**



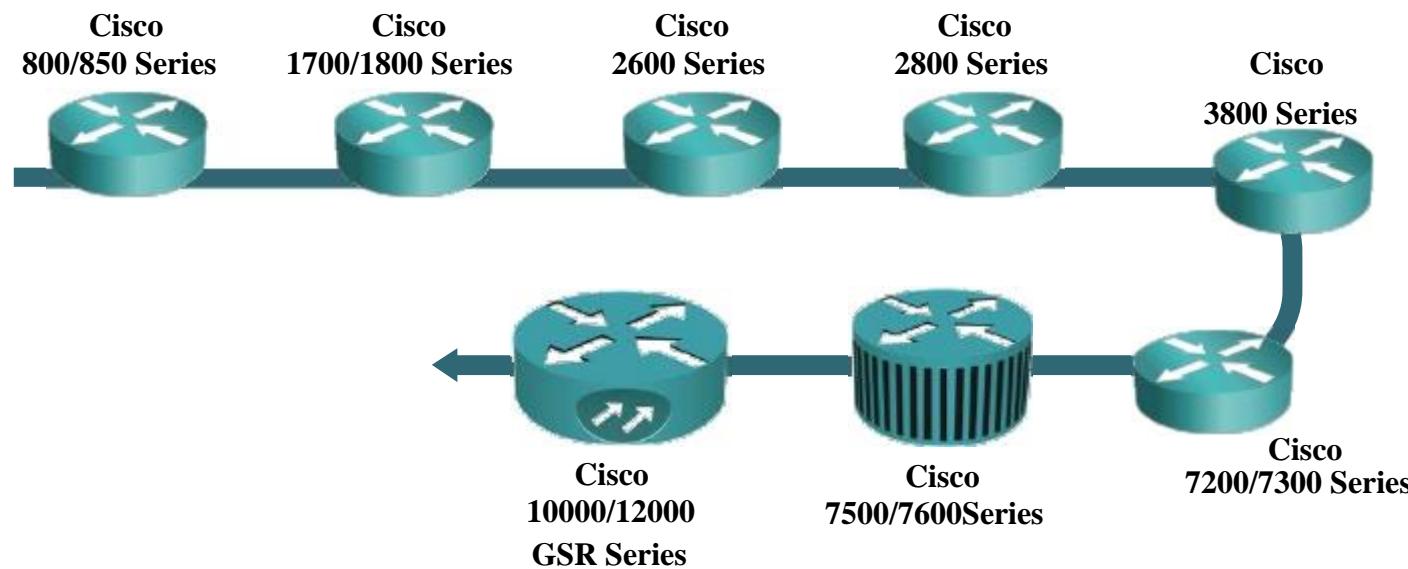
**Nexus
7000 Series**



Cisco Router

▶ 선택 기준 :

- 라우팅 특성 및 확장에 대한 필요성
- 포트 밀도 및 다양성 요구사항
- 일반적인 사용자 인터페이스
- 용량 및 성능





Cisco Router Type



Cisco
800/850 Series



Cisco
1700/1800 Series



Cisco
2600 Series



Cisco
2800 Series



Cisco
3800 Series



Cisco
7200/7300 Series



Cisco
7500/7600 Series

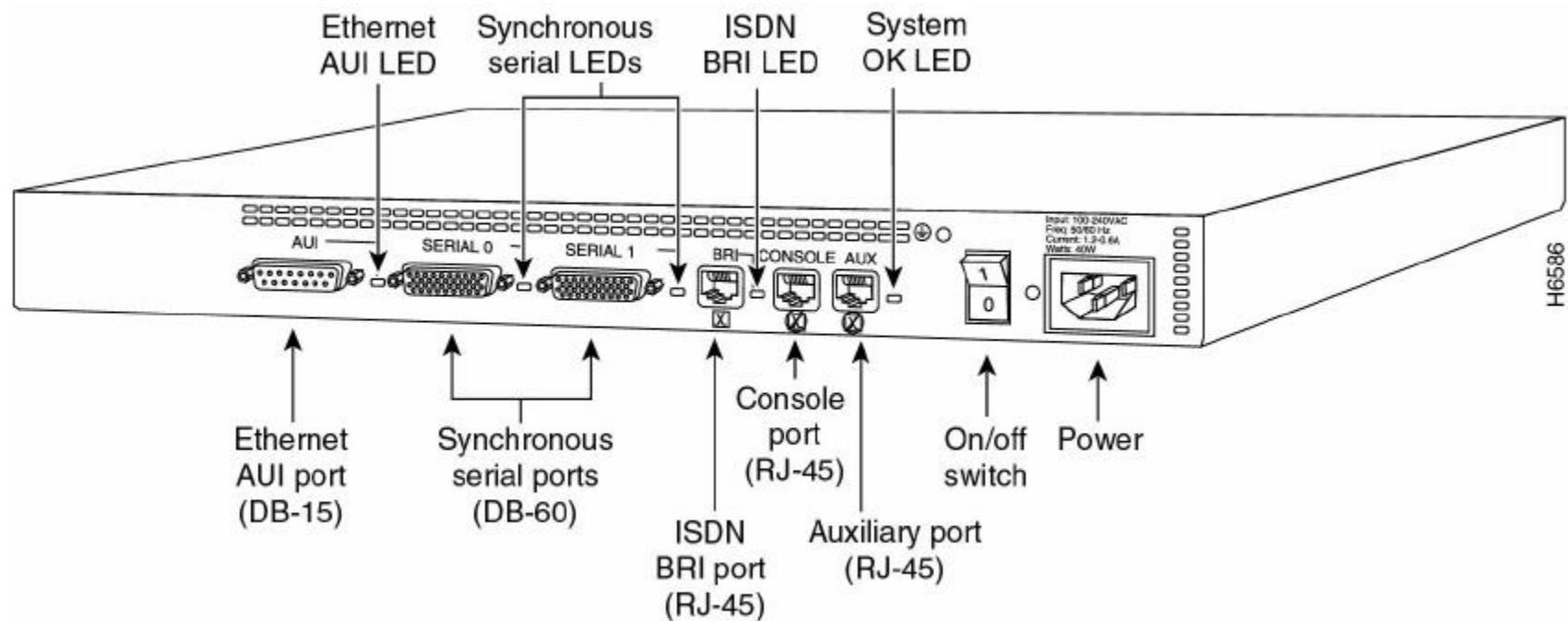


Cisco
10000/12000
GSR Series



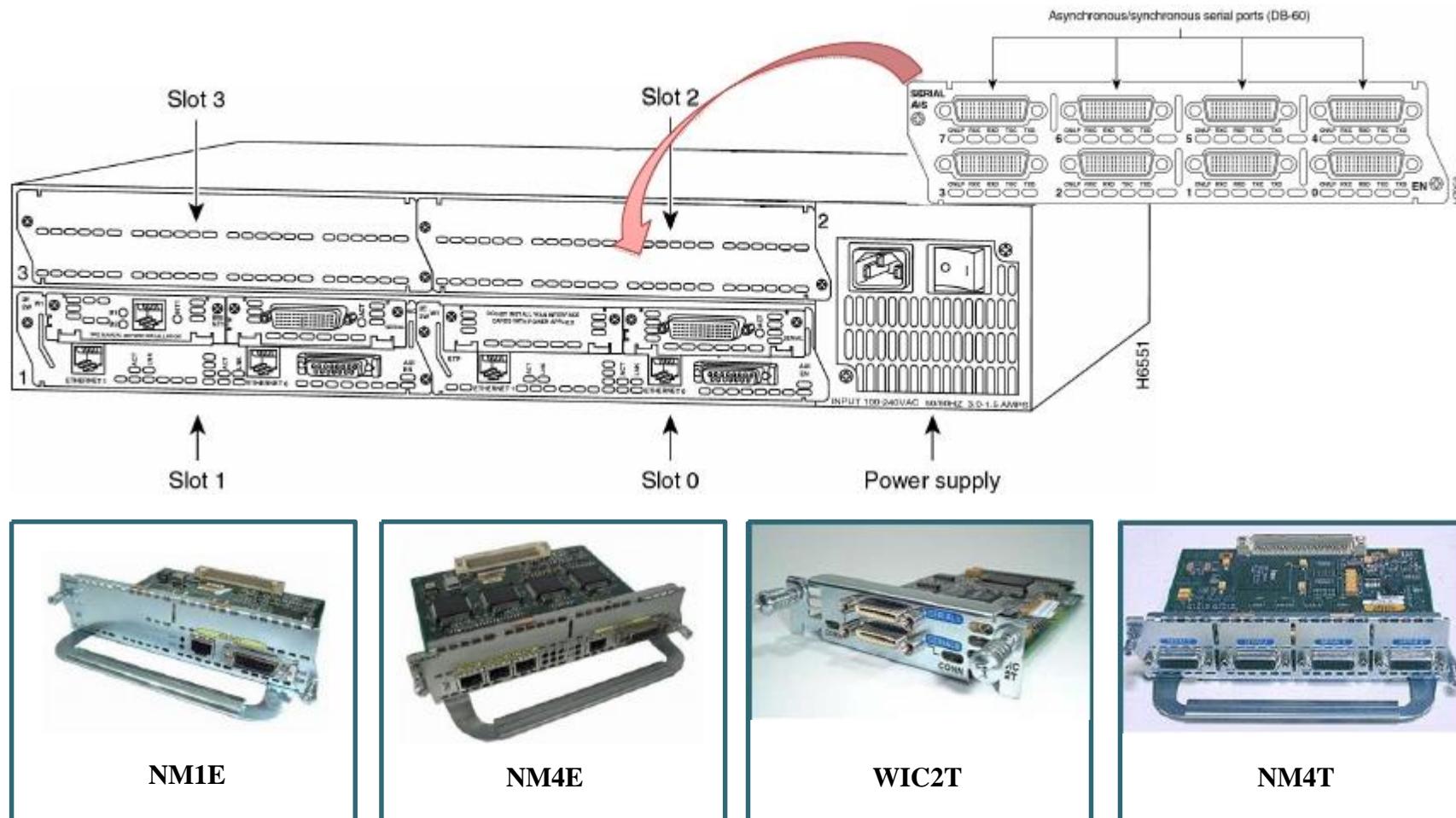


Cisco 2500 Series Router Interface Type



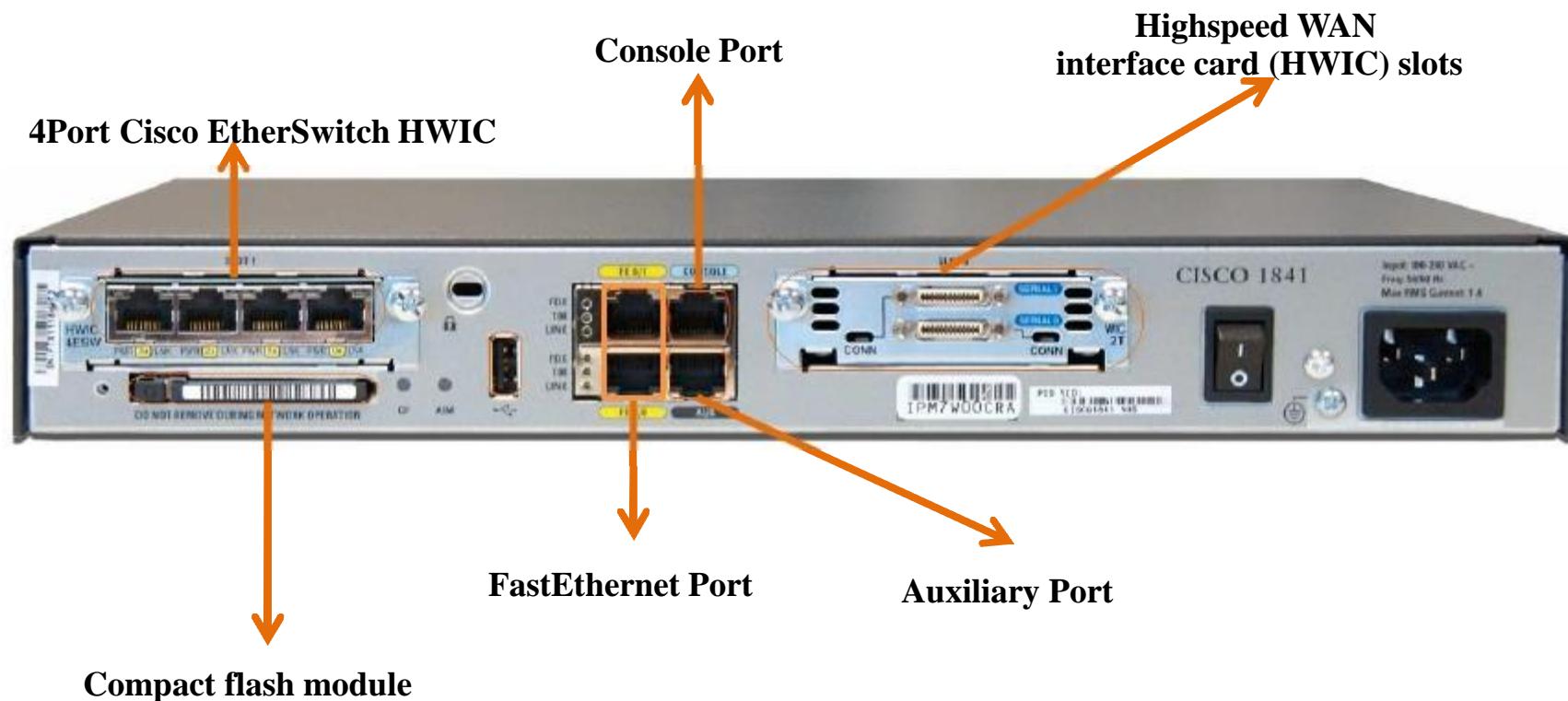


Modular Interface (Cisco 3725)





Cisco 1841 Router Interface





Cisco Router Cable

BToB(WIC 1T ↔ WIC 2T)



BToB(WIC 1T ↔ WIC 1T)





CSU/DSU & V.35 Cable



1751 CSU



V.35 Cable



CSU(Channel Service Unit)

DSU(Digital Service Unit)

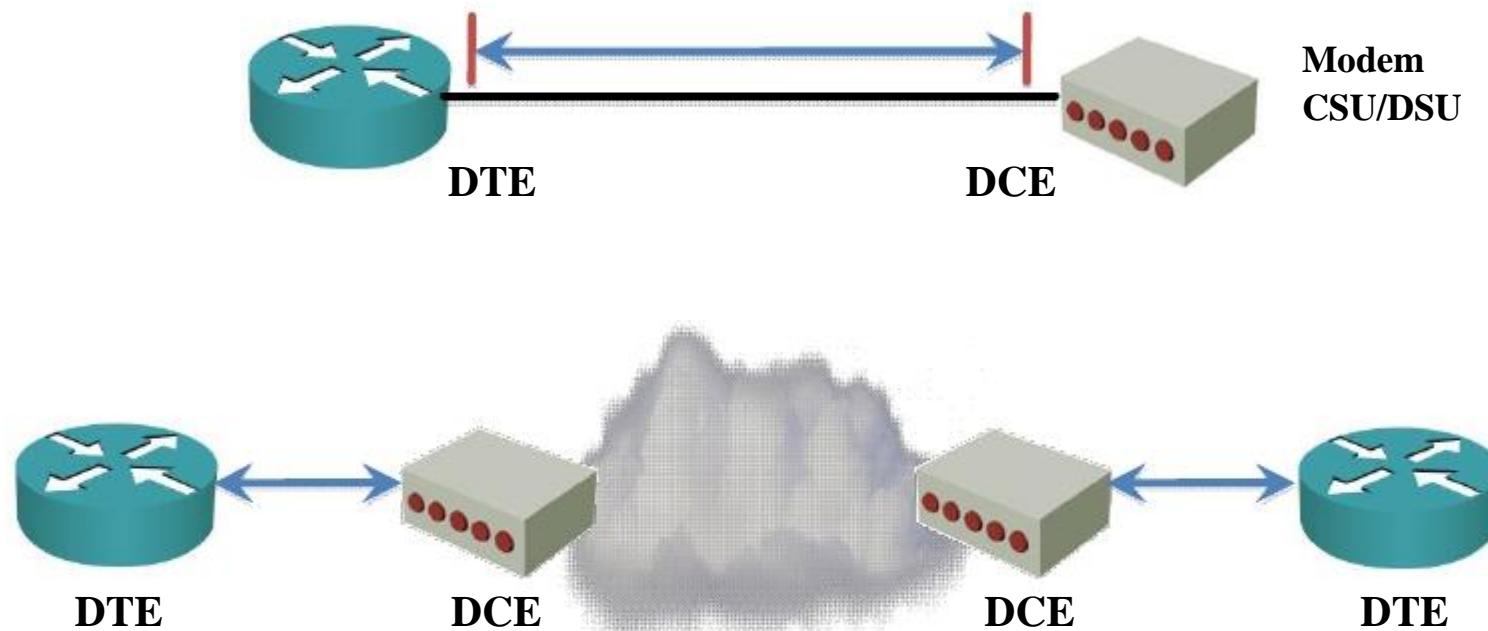


Router to CSU Connection





DTE/DCE 연결



DTE(Data Terminal Equipment)

DCE(Data Communication Equipment)

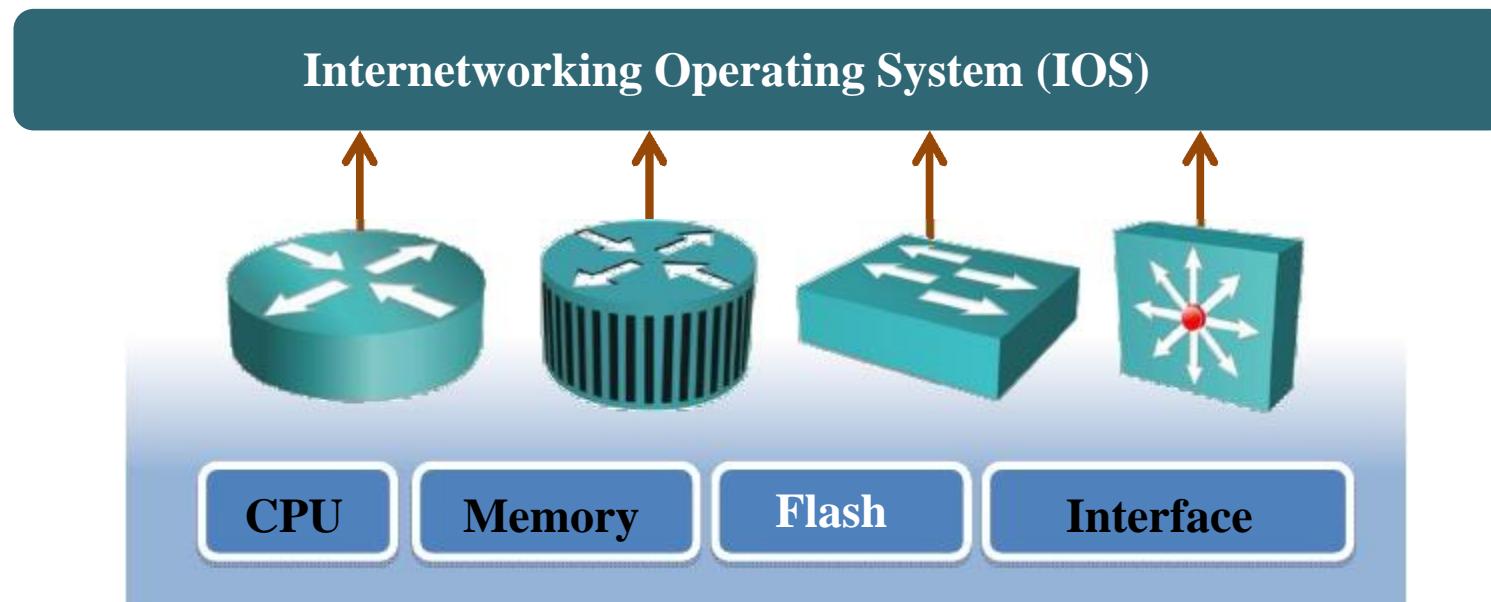
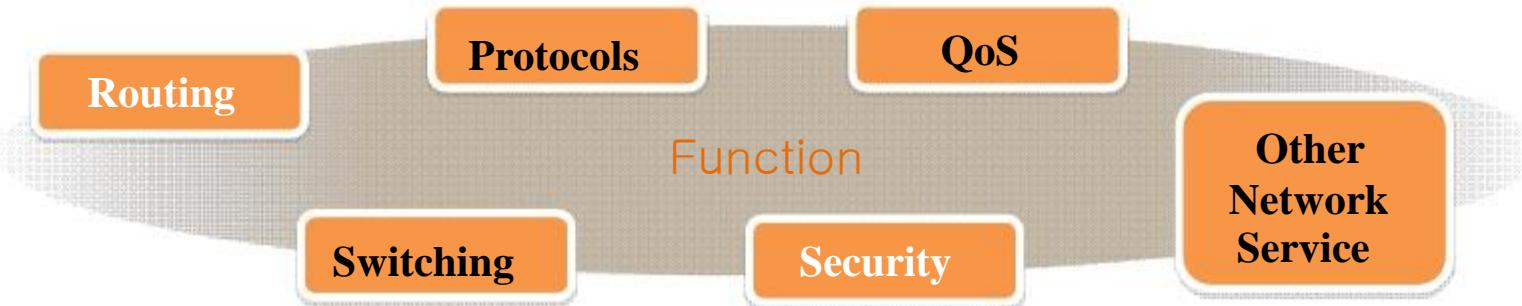


Cisco IOS Software 개요

- **Cisco IOS Software** 특징
- **IOS Device** 구성
- **IOS Device** 구성을 위한 외부 접근 방식
- **IOS Command Line Interface**의 기능
- **IOS**의 기본 실행(**EXEC**) 모드



Cisco IOS Software 특징





IOS Device의 구성 작업들

- Network에서 요구되는 다양한 정책 설정
- Protocol Address와 관련 Option 설정
- IOS Device 관리를 위한 관리 Option

Router는 초기구성
정보를 사용자가
지정해야 한다

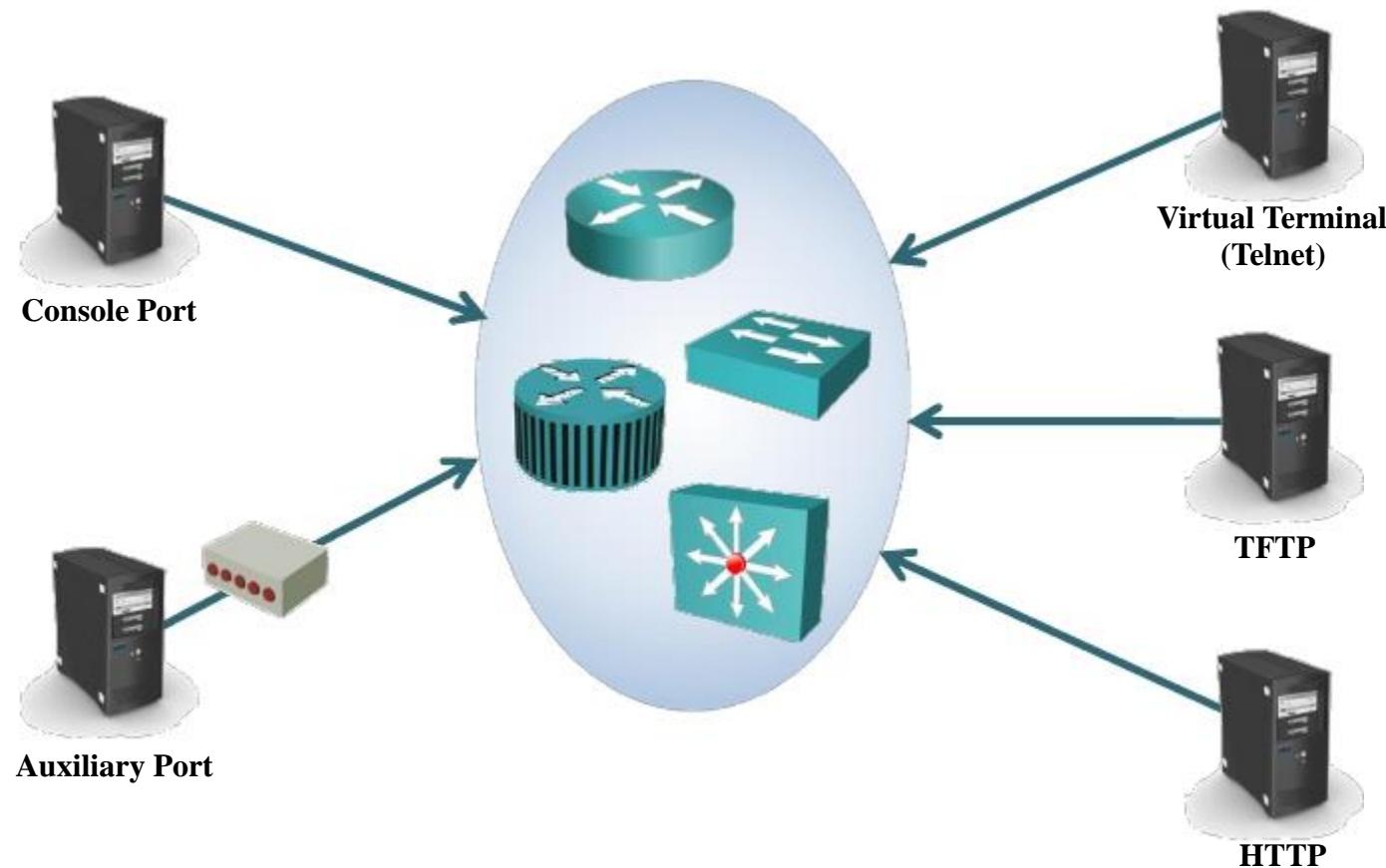


Switch는 초기구성
정보를 메모리에
저장하고 있다





IOS Device 구성을 위한 외부 접근 방식





IOS Command Line Interface의 기능

- IOS가 제공하는 가장 기본적인 사용자 **Interface**이다.
- CLI는 사용자가 명령어를 직접 입력하는 방식이다.
- IOS Device의 종류에 따라 다양한 명령어가 제공된다.
- Console안에서 명령어의 직접/간접 입력이 가능하다.
- 실행모드는 크게 **User Mode**와 **Privileged Mode**가 있다.
- 명령어 모드에 따라 다양한 **Prompt**를 제공한다.



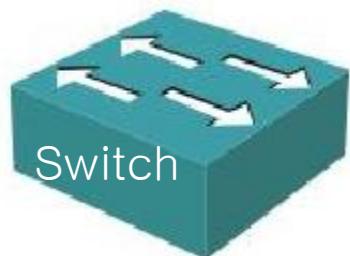
IOS의 기본 실행(EXEC) 모드 - User Mode

IOS의 기본 실행 모드이다.

- 제한된 명령어만을 사용할 수 있다.
- 다음과 같은 Prompt를 제공한다.



```
Router>  
Router>  
Router>
```

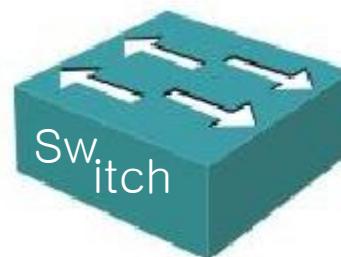
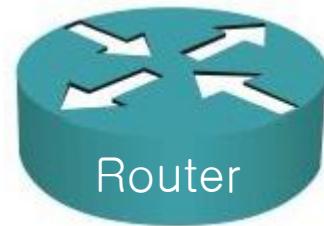


```
Switch>  
Switch>  
Switch>
```



IOS의 기본 실행(EXEC) 모드 - Privileged Mode

- IOS의 구성작업을 진행할 수 있는 실제 실행모드이다.
- IOS의 모든 명령어를 사용할 수 있다.
- IOS가 제공하는 다른 구성모드로 진입하기 위해서는 이 실행모드가 기본이 된다.
- 다음과 같은 Prompt를 제공한다.





Cisco Router의 초기 시동

```
System Bootstrap, Version 12.2(4r)XT2, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 2001 by cisco Systems, Inc.
c2691 processor with 131072 Kbytes of main memory

Main memory is configured to 64 bit mode with parity disabled
 Readonly ROMMON initialized
 rommon 1 > b
program load complete, entry point:0x80008000, size:0x6284dc
Self decompressing the image
:#####
##### [OK] 
.....
#####[OK]

Smart Init is enabled
Smart init is sizing iomem
      ID          MEMORY_REQ          TYPE
000259          0005F3C00      c2691 2NM Mainboard
0001AA          0X0025178C  1A DS3
                           0X0010AE00 public buffer pools
                           0X00211000 public particle pools
TOTAL: 0X00B6118C

If any of the above Memory Requirements are
"UNKNOWN", you may be using an unsupported
```

IOS Image Loading



Cisco Router의 초기 시동

```
Cisco Internetwork Operating System Software
IOS (tm) 2600 Software (C2691-I-M), version 12.2(4)XT, MAINTENANCE INTERIM
SOFTWARE
Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Thu 23-Aug-01 00:28 by uma
Image text-base:0x60008960, data-base:0x60AE4000

cisco 2691 (R7000) processor (revision 0.6) with 118784K/12288K bytes of memory.
Processor board ID 12345678901
R7000 CPU at 240Mhz, Implementation 39, Rev 3.3, 256KB L2 Cache
Bridging software.
X.25 software, version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
DRAM configuration is 64 bits wide with parity disabled.
55K bytes of non-volatile configuration memory.
15680K bytes of ATA System CompactFlash (Read/Write)
31360K bytes of ATA Slot0 CompactFlash (Read/Write)
```

IOS Software Version

Hardware Information



Cisco Router의 초기 시동

■ Setup Mode

```
--- System Configuration Dialog ---
```

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

```
At any point you may enter a question mark '?' for help.  
Use ctrl-c to abort configuration dialog at any prompt.  
Default settings are in square brackets '[]'.
```

```
Basic management setup configures only enough connectivity  
for management of the system, extended setup will ask you  
to configure each interface on the system
```

```
Would you like to enter basic management setup? [yes/no]: no
```

■ User Mode

```
Router con0 is now available  
Press RETURN to get started.
```

```
Router>
```



Router에 Login 하기





Router의 User Mode Command List

Router>?

Exec commands:

access-enable	Create a temporary Access-List entry
access-profile	Apply user-profile to interface
clear	Reset functions
connect	Open a terminal connection
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
exit	Exit from the EXEC
help	Description of the interactive help system
login	Log in as a particular user
logout	Exit from the EXEC
modemui	Start a modem-like user interface
mrinfo	Request neighbor and version information from a multicast router
mstat	Show statistics after multiple multicast traceroutes
mtrace	Trace reverse multicast path from destination to source
name-connection	Name an existing network connection
pad	Open a x.29 PAD connection
ping	Send echo messages
ppp	Start IETF Point-to-Point Protocol (PPP)
--More--	



Router의 Privileged Mode Command List

Router#?

Exec commands:

access-enable	Create a temporary Access-List entry
access-profile	Apply user-profile to interface
access-template	Create a temporary Access-List entry
archive	manage archive files
auto	Exec level Automation
bfe	For manual emergency modes setting
cd	Change current directory
clear	Reset functions
clock	Manage the system clock
configure	Enter configuration mode
connect	Open a terminal connection
copy	Copy from one file to another
debug	Debugging functions (see also 'undebbug')
delete	Delete a file
dir	List files on a filesystem
disable	Turn off privileged commands
disconnect	Disconnect an existing network connection
enable	Turn on privileged commands
erase	Erase a filesystem
exit	Exit from the EXEC

--More--



Router의 CLI Help 기능

▶ ContextSensitive Help :

- Command List를 제공
- 명령어 조합 및 각 단계마다 수행할 수 있는 명령만 표시

▶ Console Error Message :

- 라우터에서 발생할 수 있는 문제를 정의
- 문제를 수정할 수 있도록 도와준다

▶ Command History Buffer :

- 사용한 명령을 버퍼에 저장 (재사용)
- 버퍼의 크기 조절 가능



Console Error Message

- 일반적인 Error Message

- 불완전한 명령어 입력 시

```
Router#con  
% Ambiguous command: "con"  
Router#
```

- 오타로 인한 명령어 잘못 입력 시 오류

```
Router#conf v  
^  
% Invalid input detected at '^' marker.
```

- 현재 모드에 존재하지 않는 명령 입력 오류

```
Router(config)#conf  
% Incomplete command.  
Router(config)#
```



Router의 CLI Editing 기능

```
Router#config terminal  
Router(config)#interface ethernet 0/0  
Router(config-if)#ip address 1.1.12.1 255.255.255.0  
Router(config-if)#
```

(Automatic scrolling of long lines)	
Ctrl + A	Move to the beginning of the command line
Ctrl + E	Move to the end of the Command line
Ctrl + U	Erase a line
Ctrl + B	Move back one character
Ctrl + F	Move forward one character
Ctrl + H	Delete a single character



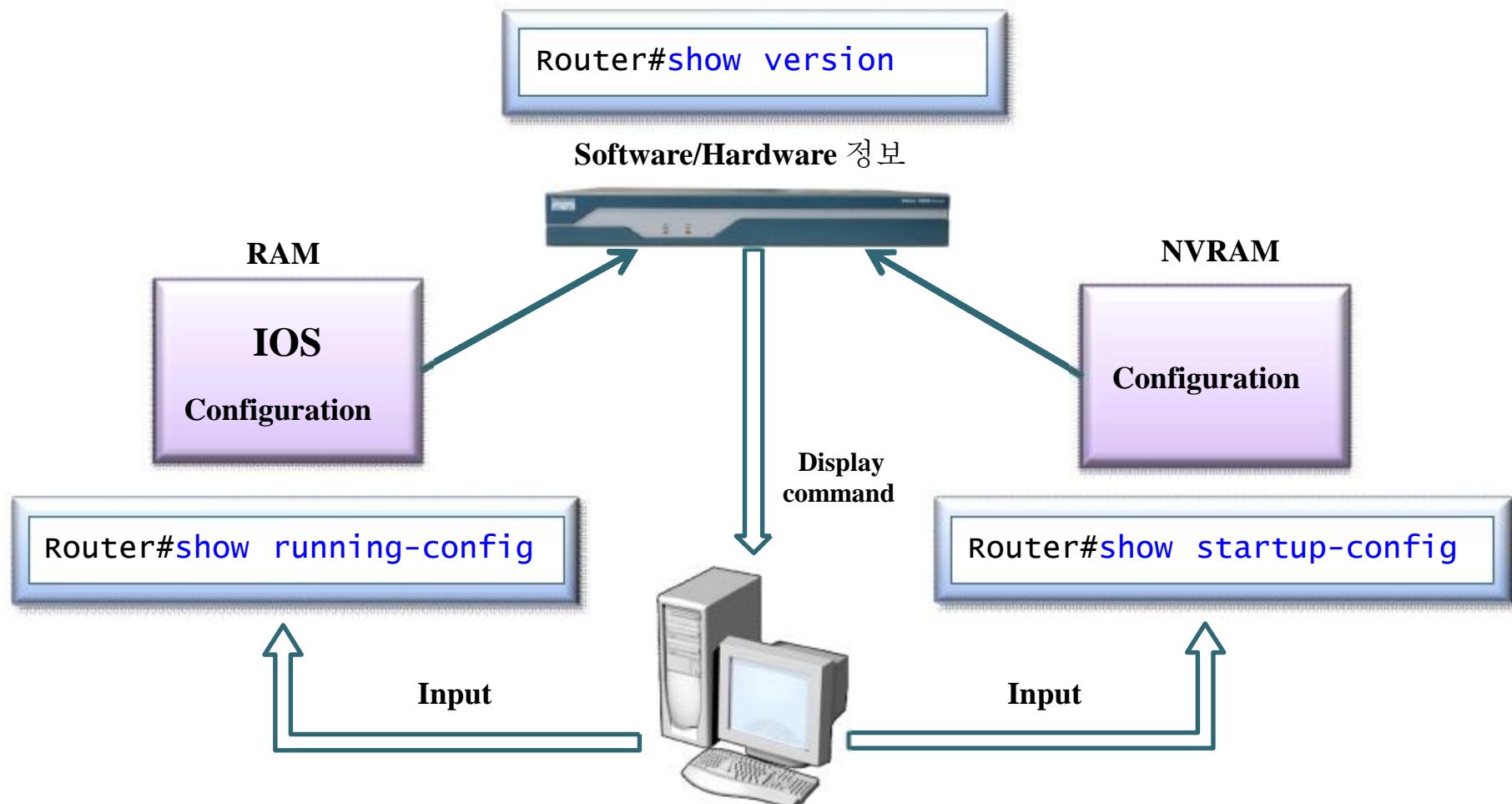
Router의 Command History

CtrlP or Up Arrow	Recalls last(previous) commands
CtrlN or Down Arrow	Recalls more recent commands
show history	Shows command buffer contents
history size line	Sets the buffer size permanently
terminal history size lines	Sets session command buffer size

```
Router#show history
  en
  conf t
  sh ip int brief
  show history
  end
  conf t
  show history
Router#
```



Router의 초기 상태 정보 검증





Router의 초기 상태 정보 검증

```
R11#show version
Cisco Internetwork Operating System Software
IOS (tm) 3700 Software (C3725-I-M), Version 12.3(1a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Fri 06-Jun-03 12:20 by dchih
Image text-base: 0x60008954, data-base: 0x60D52000

ROM: ROMMON Emulation Microcode
ROM: 3700 Software (C3725-I-M), Version 12.3(1a), RELEASE SOFTWARE (fc1)

R11 uptime is 1 hour, 7 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0,
      BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"

cisco 3725 (R7000) processor (revision 0.1) with 120832K/10240K bytes of memory.
Processor board ID XXXXXXXXXXXX
R7000 CPU at 80Mhz, Implementation 39, Rev 2.1, 256KB L2, 512KB L3 Cache
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
DRAM configuration is 64 bits wide with parity enabled.
55K bytes of non-volatile configuration memory.
16384K bytes of ATA System CompactFlash (Read/write)

Configuration register is 0x2102
```



Router의 초기 상태 정보 검증

In RAM

```
Router#show running-config
Building configuration...

Current configuration : 1117 bytes
!
version 12.3
service timestamps debug datetime msec
.......
```

In NVRAM

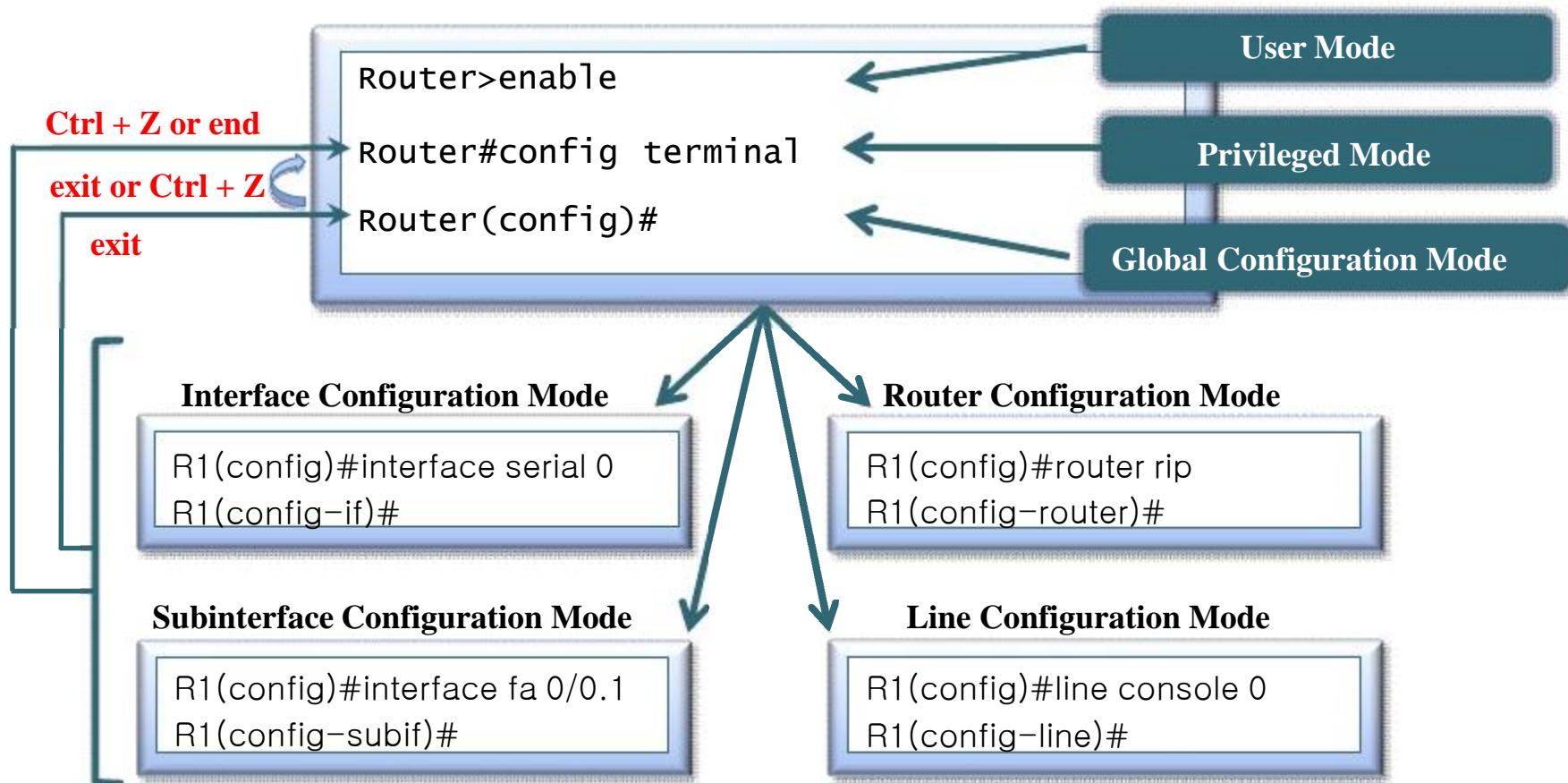
```
Router#show startup-config
Using 1027 out of 57336 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
.....
```

- 현재 DRAM에 저장된 정보를 표시
- 사용자가 수정한 정보는 running-config 파일에 저장
- Active Config 파일이므로 설정된 내용은 System에 적용되어 있음

- NVRAM에 저장된 정보를 표시
- “copy running-config startup-config” 명령을 사용하여 NVRAM에 저장
- 이 정보는 Router Reload시에 Router를 초기 구성에 사용



Router 구성 모드





CLI에서 Router 설정

- Router 이름 지정

```
Router(config)# hostname R11  
R11(config)#
```

- Banner MOTD 설정 (Message Of The DayBanner)

```
R11(config)#banner motd #  
외부 접근 사용자에게 보여질 문구 지정 #
```

- Interface Description (interface 식별을 위한 구문)

```
R11(config)#interface serial 0  
R11(config-if)#description ## To Busan Line ##
```



Banner 예제

```
Router(config)# banner motd #
```

```
=====
```

Welcome to my router!

Unauthorized access is prohibited by law.

```
=====#=
```

```
Router(config)#
```



CLI에서 Router Password 설정

•Console Password

```
Router(conf)#line console 0  
Router(conf-line)#login  
Router(conf-line)#password cisco
```

•Virtual Terminal Password

```
Router(conf)#line vty 0 4  
Router(conf-line)#login  
Router(conf-line)#password cisco
```

•Enable Password

```
Router(config)#enable password cisco
```

•Secret Password

```
Router(config)#enable secret cisco1
```

User Mode에서 Privileged Mode로 변경



CLI에서 Router 설정 – Console Option

- **Console Session Time** 설정(일정시간동안 입력이 없을시 로그아웃되지 않도록 함.)

```
Router(conf)#line console 0  
Router(conf-line)#exec-timeout 0 0
```

- **Console Input Message** 동기화 설정(Console에 메시지 출력 후, 엔터 효과)

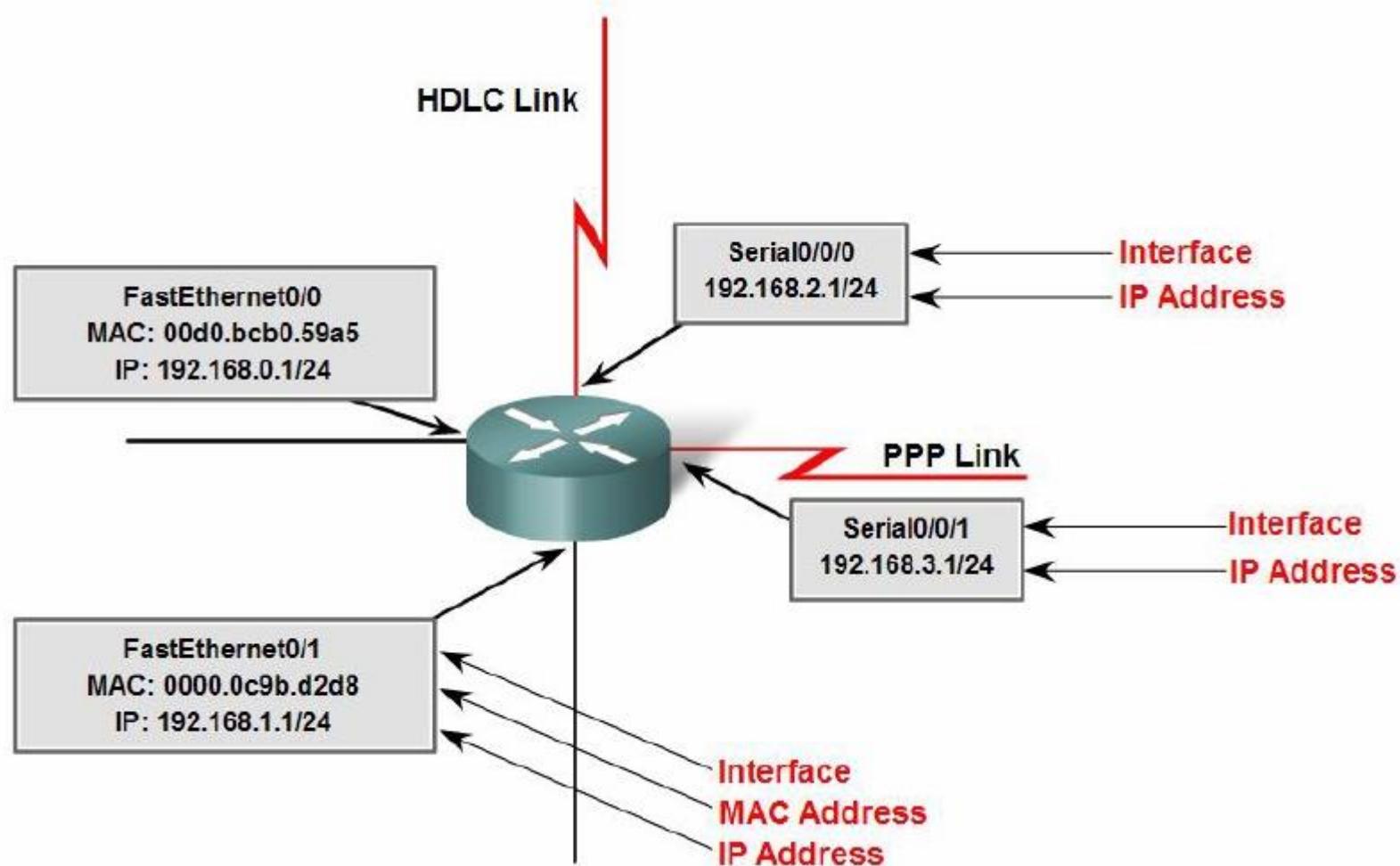
```
Router(conf)#line console 0  
Router(conf-line)#logging synchronous
```

- **Console** 인증 설정 : login 옵션중에 local user DB를 위한 설정

```
Router(conf)#Username student password korea  
Router(conf)#line console 0  
Router(conf-line)#login local
```



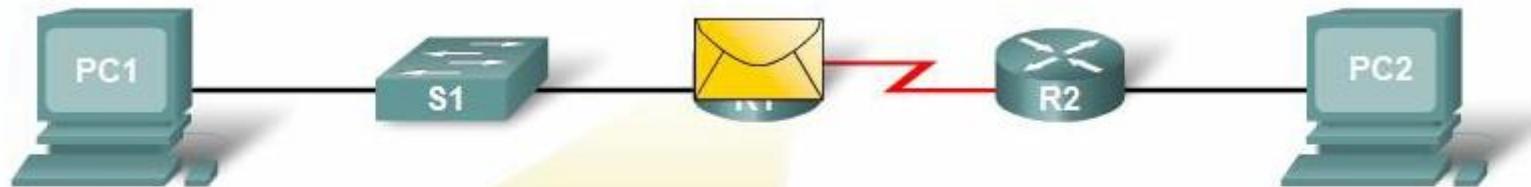
라우터 인터페이스





Router Packet Forwarding

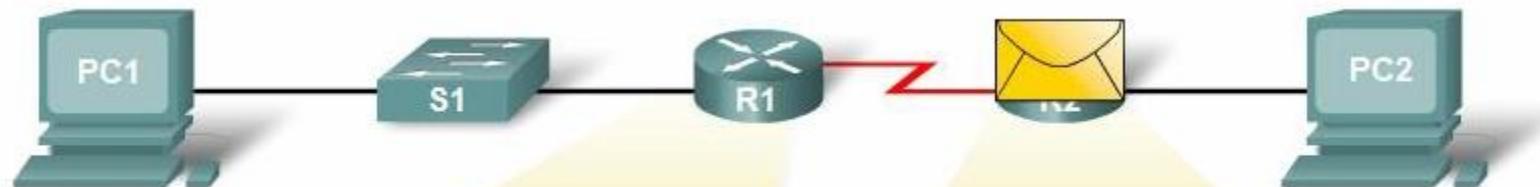
To: 192.168.3.10





Router Packet Forwarding

To: 192.168.3.10





Router의 Interface 설정

- **Interface Configuration Mode** 진입을 위한 **Interface Type** 이해

```
Router(conf)#interface type number  
Router(conf-if)#{}
```

Type = serial, ethernet, loopback, atm, fddi, null, token ring..
Number = interface를 구별하기 위한 번호

- **Fixed Interface Router**

```
Router(conf)#interface type number  
EX)  
Router(conf)#interface serial 0  
Router(conf-if)#{}
```

- **Module Interface Router**

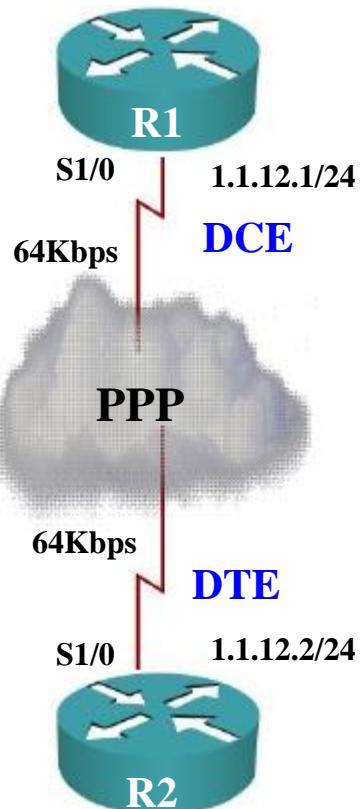
```
Router(conf)#interface type slot/port  
EX)  
Router(conf)#interface serial 1/0  
Router(conf-if)#{}
```



Router의 Interface 설정

- Interface configuration의 기본 단계

Serial Back to Back Connection



- 2계층 encapsulation 타입 설정하기
R1(conf)#interface serial 1/0
R1(conf-if)#encapsulation PPP
- Address 설정하기
R1(conf-if)#ip address 1.1.12.1 255.255.255.0
- Bandwidth 설정하기
R1(conf-if)#bandwidth 64
- Clock Rate 설정하기 (DCE Interface에서 설정)
R1(conf-if)#clock rate 64000
- Interface 동작 시키기
R1(conf-if)#no shutdown



Router Interface 구성 정보 검증

▪ Interface 상태정보 검증

```
R1#show interfaces serial 1/0
Serial1 is up, line protocol is up
Hardware is M4T
Internet address is 1.1.12.1/24
MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec,
  reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, crc 16, loopback not set
```

Carrier Detect

Keepalives

Operational	Serial1 is up, line protocol is up
Connection problem	Serial1 is up, line protocol is down
Interface problem	Serial1 is down, line protocol is down
Disabled	Serial1 is administratively down, line protocol is down



Router Interface 구성 정보 검증

- Serial1/0 is up, line protocol is down 0) 발생하는 경우
 - No keepalives
 - No clock rate set
 - 서로 다른 encapsulation type 설정
- Serial1/0 is administratively down, line protocol is down
 - " no shutdown " 으로 interface를 활성화를 시켜야 한다.



Router Interface 구성 정보 검증

▪ Serial Interface 상태정보 검증

```
R1# show interfaces serial 1/0
Serial1/0 is up, line protocol is up
  Hardware is M4T
  Internet address is 1.1.12.1/24
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 16, loopback not set
  Keepalive set (10 sec)
  Restart-Delay is 0 secs
  Last input 00:00:00, output 00:00:02, output hang never
  Last clearing of "show interface" counters never      => clear counter se 0/0
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
    Conversations 0/1/256 (active/max active/max total)
    Reserved Conversations 0/0 (allocated/max allocated)
    Available Bandwidth 768 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    2872 packets input, 210786 bytes, 0 no buffer
    Received 2871 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    2559 packets output, 110264 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    0 output buffer failures, 0 output buffers swapped out
    2 carrier transitions      DCD=up    DSR=up    DTR=up    RTS=up    CTS=up
```



Router Interface 구성 정보 검증

- Serial Interface의 Serial Cable Type 정보 확인

```
R1#show controllers serial 1/0
M4T: show controller:
PAS unit 0, subunit 0, f/w version 1-45, rev ID 0x2800001, version 1
idb = 0x61935618, ds = 0x61936DC8, ssb=0x619370FC
Clock mux=0x0, ucmd_ctrl=0x1C, port_status=0x7B
Serial config=0x8, line config=0x200
maxdgram=1608, bufpool=78Kb, 120 particles
    DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
line state: up

cable type : v.11 (X.21) DCE cable, received clockrate 128000

base0 registers=0x3D000000, base1 registers=0x3D002000
mxt_ds=0x61A89BA8, rx ring entries=78, tx ring entries=128
rxring=0x79BEFA0, rxr shadow=0x6193D6E8, rx_head=52
txring=0x79BF240, txr shadow=0x6193DABC, tx_head=80, tx_tail=80, tx_count=0
throttled=0, enabled=0
halted=0, last halt reason=0
Microcode fatal errors=0
rx_no_eop_err=0, rx_no_stp_err=0, rx_no_eop_stp_err=0
rx_no_buf=0, rx_soft_overrun_err=0, dump_err= 0, bogus=0, mxt_flags=0x0
tx_underrun_err=0, tx_soft_underrun_err=0, tx_limited=1(2)
tx_fullring=0, tx_started=2896
rx_int_count=3250, tx_int_count=2898
```



R1 라우터 기본 구성

```
Router#configure terminal
Router(config)#hostname R1
R1(config)#no ip domain-lookup
R1(config)#enable password cisco
R1(config)#line console 0
R1(config-line)#password cisco
R1(config-line)#exec-timeout 0 0
R1(config-line)#logging synchronous
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config)#interface loopback 0
R1(config-if)#ip address 1.1.1.1 255.255.255.0
R1(config)#interface Serial 1/0
R1(config-if)#no shutdown
R1(config-if)#ip address 1.1.12.1 255.255.255.0
```



R2 라우터 기본 구성

```
Router#config t
Router(config)#hostname R2
R2(config)#no ip domain-lookup
R2(config)#enable password cisco
R2(config)#line con 0
R2(config-line)#password cisco
R2(config-line)#exec-timeout 0 0
R2(config-line)#logging synchronous
R2(config)#line vty 0 4
R2(config-line)#password cisco
R2(config)#interface loopback 0
R2(config-if)#no shutdown
R2(config-if)#ip add 1.1.2.1 255.255.255.0
R2(config)#interface Serial 1/0
R2(config-if)#no shutdown
R2(config-if)#ip add 1.1.12.2 255.255.255.0
```



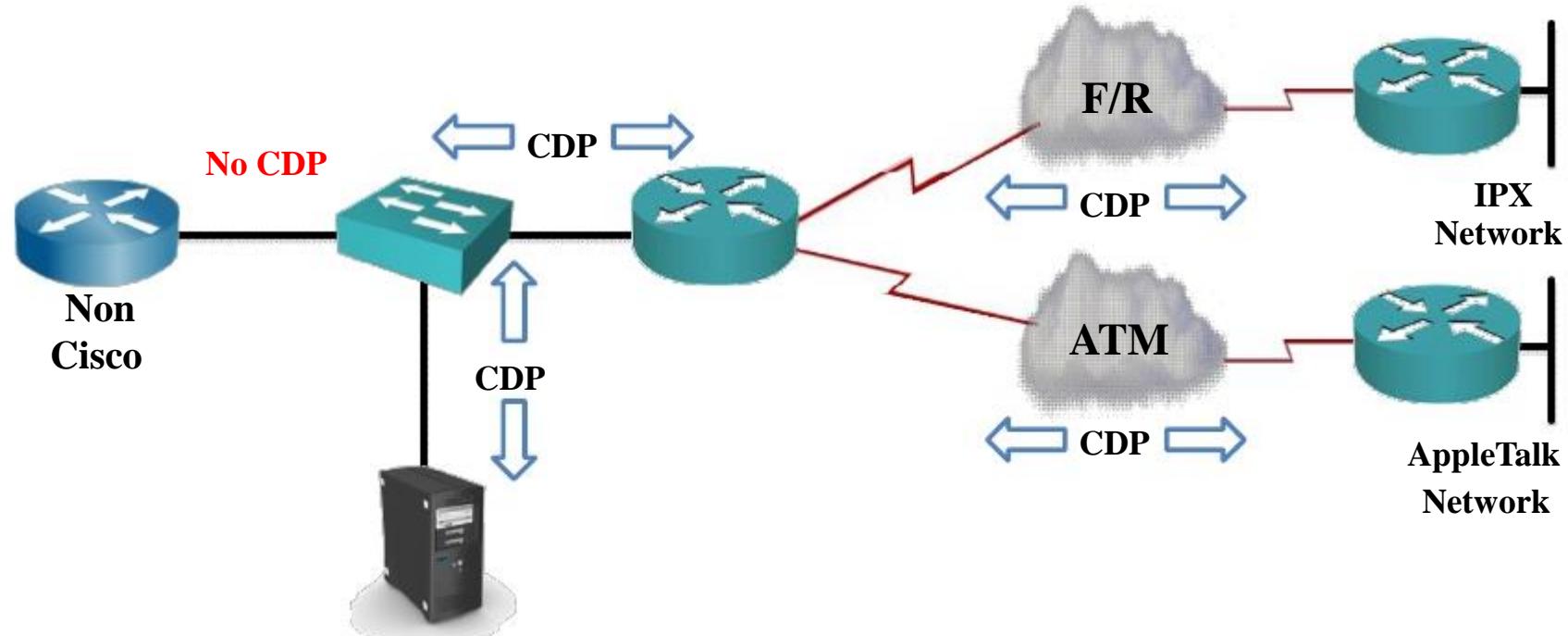
Neighbor Device 관리

- **CDP (Cisco Discovery Protocol)** 개요
- **CDP**를 이용한 정보 수집
- **CDP** 설정하기
- **CDP** 상태정보 검증
- **CDP**를 이용한 **Network** 구조 검증



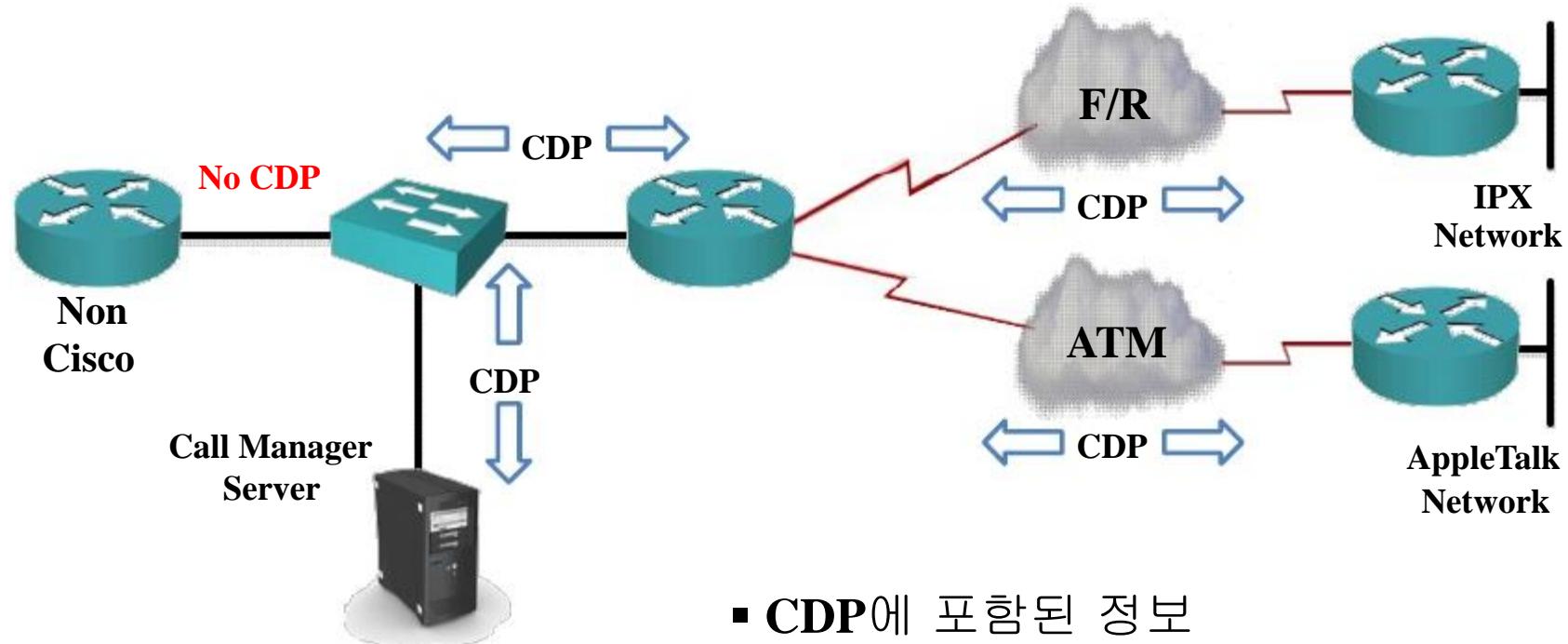
CDP(Cisco Discovery Protocol) 개요

3-계층 프로토콜	TCP/IP, Novel IPX, Apple Talk, Others
Cisco Proprietary Data-link Protocol	CDP는 Cisco Device에서만 동작하며 Cisco Device의 정보만을 주고 받는다
2-계층 프로토콜	LAN, Frame-relay, ATM, Others





CDP를 이용한 정보수집

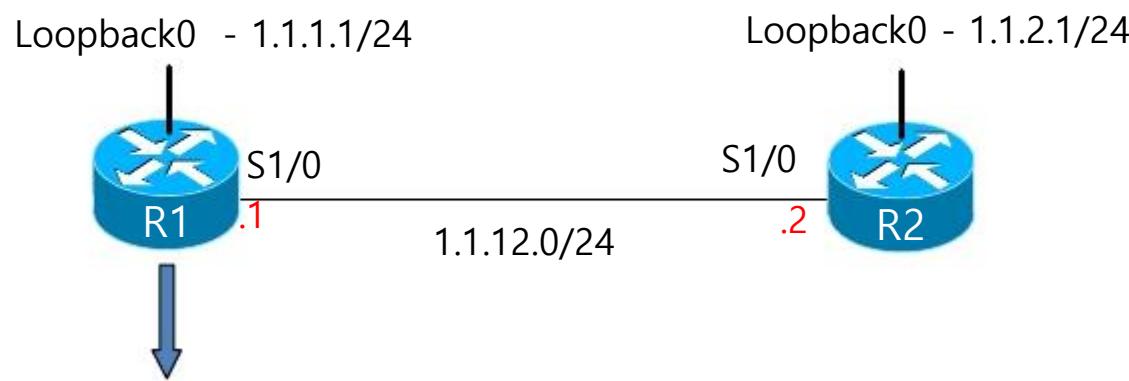


■ CDP에 포함된 정보

- Neighbor Device *Hostname*
- Neighbor Device *Address* 정보
- Neighbor Device *Port* 정보
- Neighbor Device 장비 성격
- Neighbor Device 기종



CDP를 이용한 정보 수집



R1#sh cdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

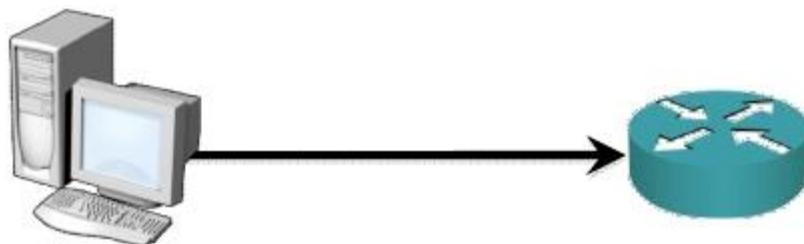
Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
R2	Ser 1/0	148	R	3640	Ser 1/0



CDP 설정하기

• CDP Option

```
Router#show cdp ?
```



• Global Configuration Mode

```
Rotuer#config terminal  
Router(config)#cdp run  
Router(config)#no cdp run
```

➡ CDP Enable
➡ CDP Disable

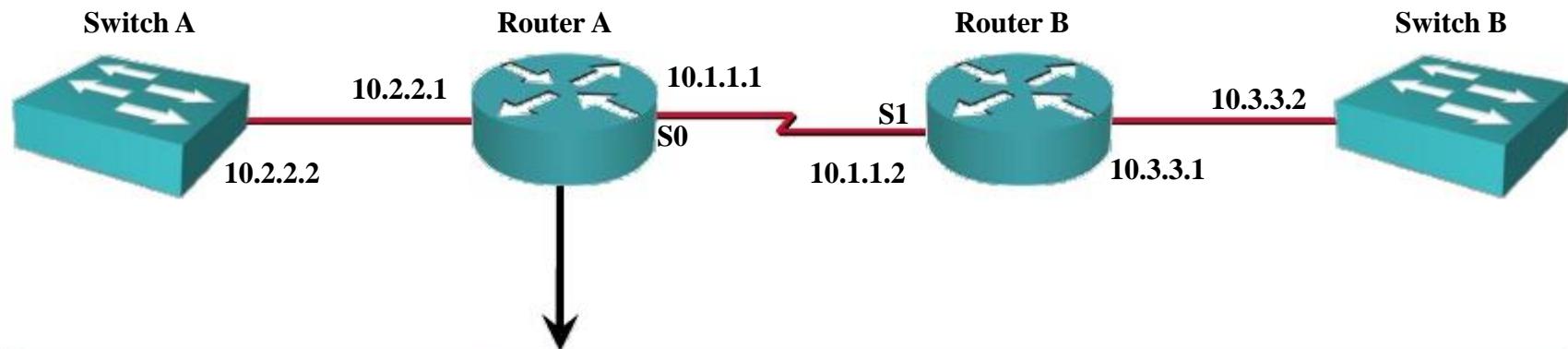
• Interface Configuration Mode

```
Router#config terminal  
Router(conf)#interface serial 0  
Router(conf-line)#cdp enable  
Router(conf-line)#no cdp enable
```

➡ CDP Enable
➡ CDP Disable



CDP상태정보 검증



```
RouterA#show cdp neighbor
```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
S - Switch, H - Host, I - IGMP, r - Repeater

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
routerB	Ser 0	148	R	2522	Ser 1
switchA	Eth 0	167	T S	1900	2

- CDP는 Router A에 물리적으로 직접 연결된 인접한 Device의 정보만을 보여준다.
따라서 물리적으로 직접 연결되지 않은 Switch B는 CDP를 이용한 정보수집이 불가능하다.



CDP상태정보 검증

- Show CDP entry Command

```
R1#show cdp entry * (or show cdp neighbor detail )  
  
Device ID: RouterB  
Entry address(es):  
  IP address: 1.1.12.2  
Platform: cisco 2522,  Capabilities: Router  
Interface: Serial0,  Port ID (outgoing port): Serial1  
Holdtime : 168 sec  
  
Version :  
Cisco Internetwork Operating System Software  
IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(3), RELEASE SOFTWARE  
(fci)  
Copyright (c) 1986-1999 by cisco Systems, Inc.  
Compiled Mon 08-Feb-99 18:18 by phanguye  
.
```



CDP상태정보 검증

- Show CDP entry Command

```
R1#show cdp traffic
CDP counters :
    Packets output: 56, Input: 38
    Hdr syntax: 0, Chksum error: 0, Encaps failed: 3
    No memory: 0, Invalid packet: 0, Fragmented: 0
```

```
R1#show cdp interface
BRI0 is administratively down, line protocol is down
    Encapsulation HDLC
    Sending CDP packets every 60 seconds
    Holdtime is 180 seconds
    .
```



Remote Device 관리

- Router Telnet 설정하기
- Telnet을 이용한 Remote Device 연결하기
- Telnet Session 관리



Router Telnet 설정

- **Virtual Terminal Configuration**

```
R1#config terminal  
R1(config)#line vty 0 4  
R1(config-line)#password cisco  
R1(config-line)#login
```

- **Local UserDB를 이용한 접속 설정**

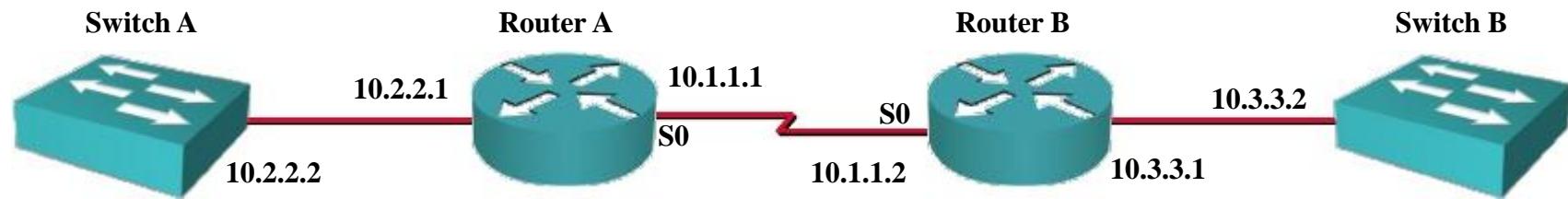
```
R1#config terminal  
R1(config)#username admin password cisco  
R1(config)#line vty 0 4  
R1(config-line)#login local
```

- 암호 입력 없이 **UserEXEC mode** 가지 접속 허용하기

```
R1#config terminal  
R1(config)#line vty 0 4  
R1(config-line)#no password  
R1(config-line)#no login
```



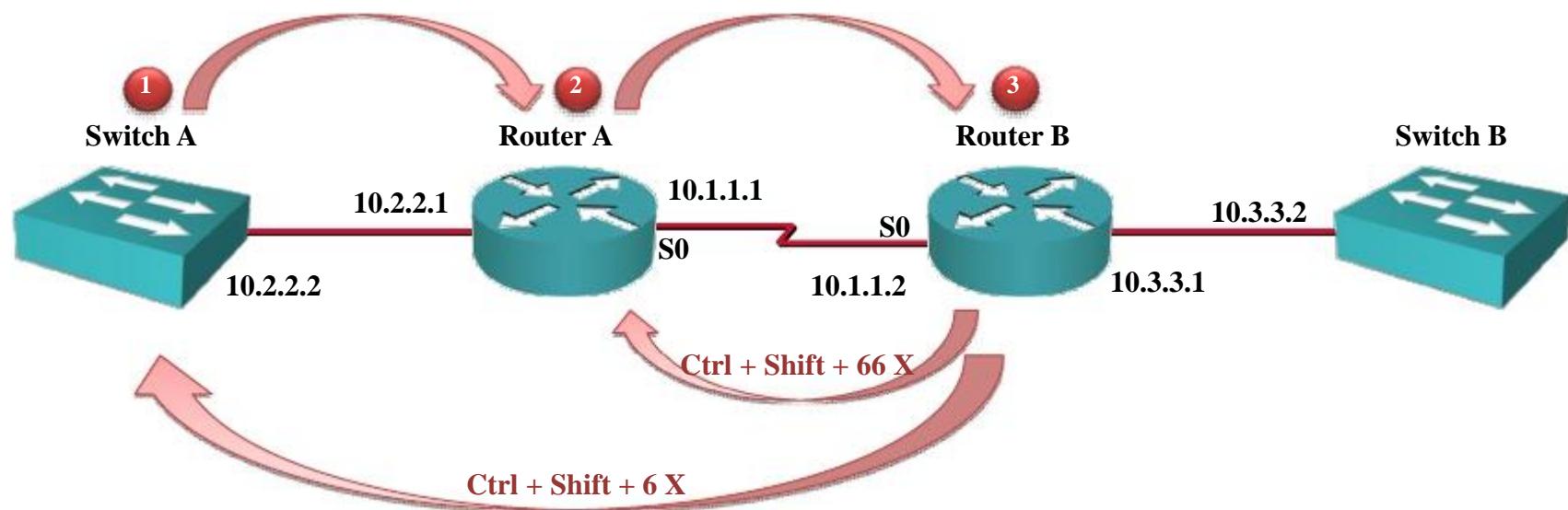
Telnet을 이용한 Remote Device 연결



```
RouterA#telnet 10.2.2.2
Trying 10.2.2.2 ... open
-----
Catalyst 1900 Management Console
Copyright (c) Cisco Systems, Inc. 1993-1998
All rights reserved.
Enterprise Edition Software
Ethernet Address: 00-90-86-73-33-40
PCA Number: 73-2239-06
PCA Serial Number: FAA02359H8K
Model Number: WS-C1924-EN
System Serial Number: FAA0237X0FQ
.
.
SwitchB>
```



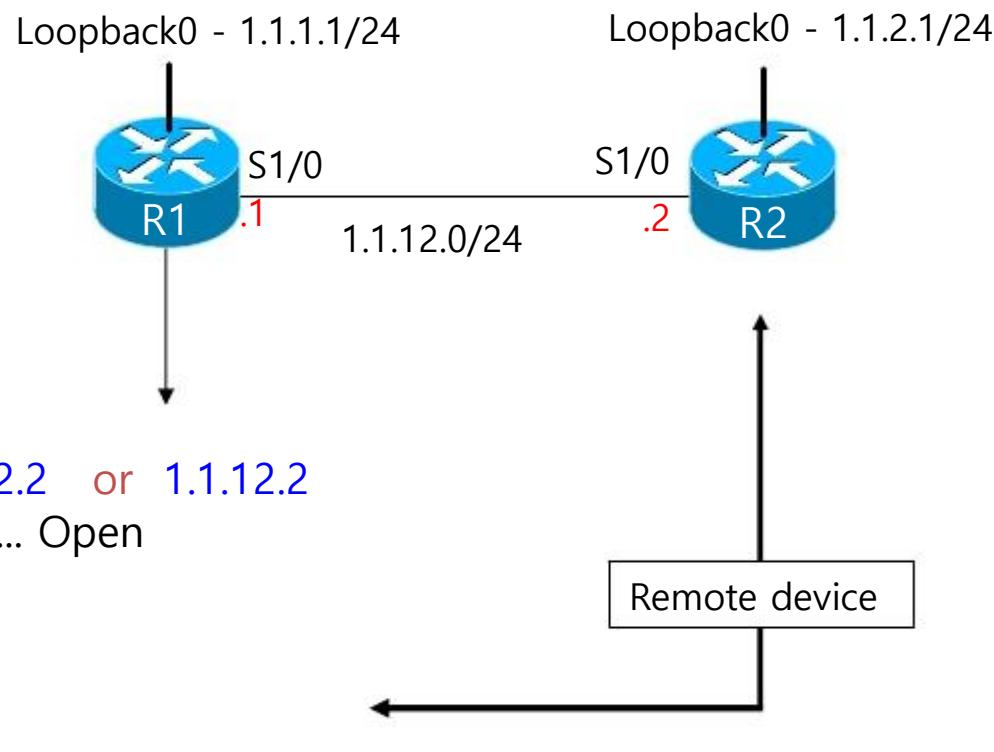
Telnet Session 관리



1. **Ctrl + Shift + 6 X**를 입력하면 telnet 접속되어 있는 현재 위치에서 처음 있었던 위치로 이동한다.
2. **Enter**를 2번 누르면 이전 위치로 이동한다.
3. **Ctrl + Shift + 66 X** 키를 누르면 2번째 위치로 이동한다. 엔터를 2번 연속 누르면 이전 위치로 이동하게 된다



Telnet 접속





Telnet 접속 해제

Conn	Host	Address	Byte	Idle	Conn Name
1	1.1.12.2	1.1.12.2	0	0	1.1.12.1
* 2	1.1.12.1	1.1.12.1	0	0	1.1.12.2

- 현재 라우터에서 원격 장비에 대한 연결을 보여준다. *는 마지막 연결을 나타낸다.

```
R1#disconnect      ----:로컬 디바이스에서 Telnet 세션 종료  
Closing connection to 1.1.12.1 [confirm]
```

R2#shuser				
Line	User	Host(s)	Idle	Location
* 0 con 0		idle	1w0d	
1 vty 0		idle	00:00:09	1.1.12.10

- 현재 라우터에 대한 다른 장비의 연결 및 Console, Aux에서의 연결을 보여주며 *는 현재 화면의 터미널을 나타낸다.

```
R2#clear line 1      ----: 외부 호스트와 연결된 Telnet 세션 종료  
[confirm]  
[OK]
```



Telnet 간편 접속

```
R1#conf t  
R1(config)#ip host R2 1.1.2.1  
R1(config)#ip host R3 1.1.3.1  
R1(config)#ip host R4 1.1.4.1  
R1(config)#exit
```

```
R1#R2  
Trying 1.1.2.1 ... Open  
. .  
Password :  
R2>
```



Router의 시동 및 구성 정보 관리

- Router의 부팅과정 소개
- Router의 내부 구성 요소
- IOS와 Configuration의 참조 동작
- Configuration register



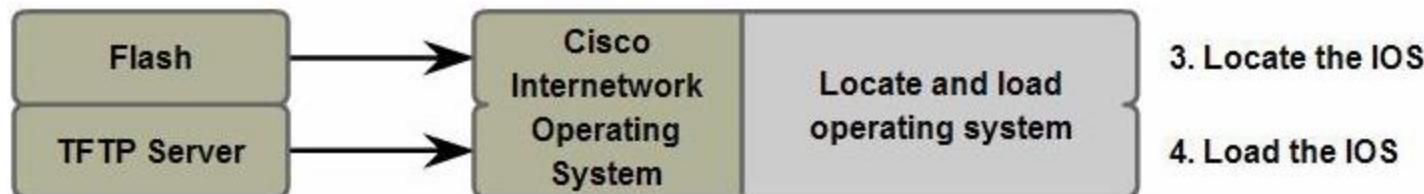
Router의 부팅 과정



```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2620 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
```



Router의 부팅 과정



```
System Bootstrap, Version 12.1(3r)T2, RELEASE SOFTWARE (fc1)
Copyright (c) 2000 by cisco Systems, Inc.
cisco 2620 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory
```

Self decompressing the image :

```
#####
##### [OK]
```



Router의 부팅 과정

Restricted Rights Legend

use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

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>

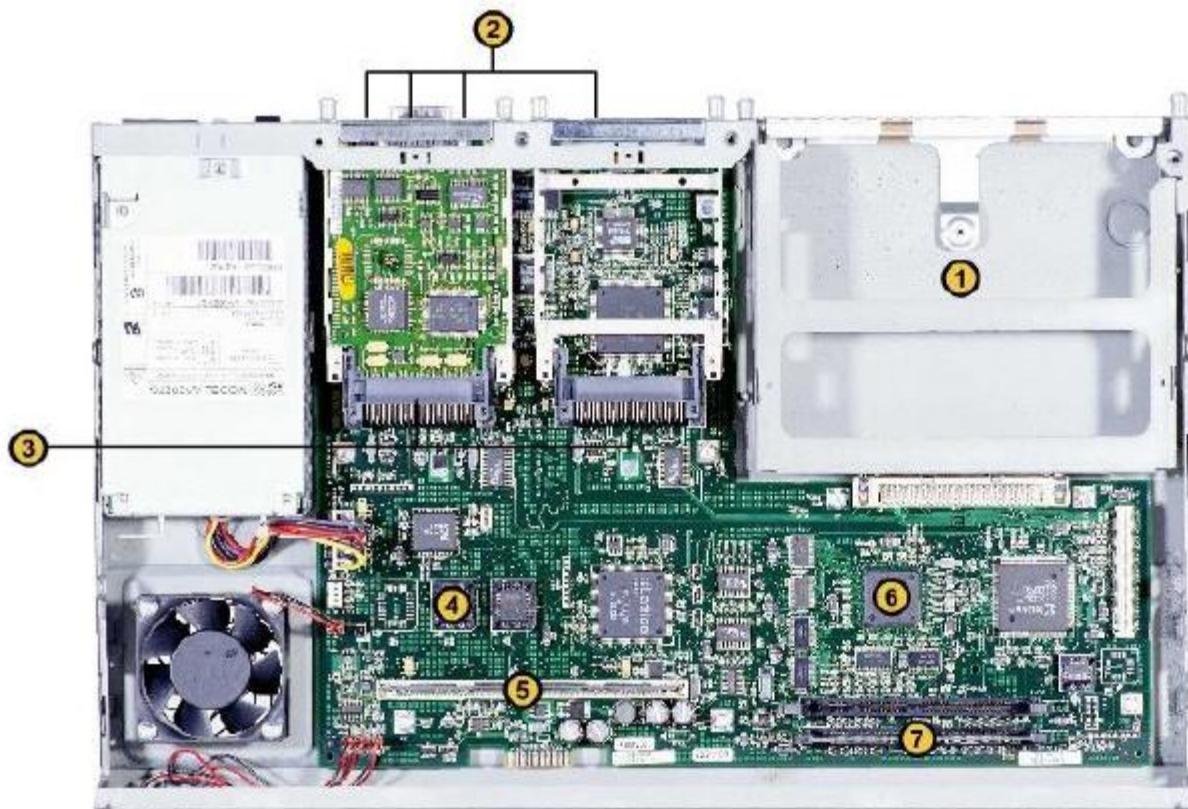
Copyright (c) 1986-2005 by cisco Systems, Inc.
Compiled Wed 27-Apr-04 19:01 by miwang

cisco 2620 (MPC860) processor (revision 0x200) with 60416K/5120K bytes of memory.

Processor board ID JAD05190MTZ (4292891495)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
1 FastEthernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/write)



Router의 내부 구성 요소



1. NM slot

2. Interface

3. WIC Slot

4. ROM

5. Flash

6. CPU

7. RAM



Configuration Register

```
R1# show version
Cisco Internetwork Operating System Software
IOS (tm) 3700 Software (C3725-I-M), Version 12.3(1a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2003 by cisco Systems, Inc.
Compiled Fri 06-Jun-03 12:20 by dchih
Image text-base: 0x60008954, data-base: 0x60D52000

ROM: ROMMON Emulation Microcode
ROM: 3700 Software (C3725-I-M), Version 12.3(1a), RELEASE SOFTWARE (fc1)

R1# uptime is 16 minutes
System returned to ROM by unknown reload cause - suspect boot_data[BOOT_COUNT] 0x0, BOOT_COUNT 0,
BOOTDATA 19
System image file is "tftp://255.255.255.255/unknown"

cisco 3725 (R7000) processor (revision 0.1) with 120832K/10240K bytes of memory.
Processor board ID XXXXXXXXXXXX
R7000 CPU at 80Mhz, Implementation 39, Rev 2.1, 256KB L2, 512KB L3 Cache
Bridging software.
X.25 software, Version 3.0.0.
2 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
DRAM configuration is 64 bits wide with parity enabled.
55K bytes of non-volatile configuration memory.
16384K bytes of ATA System CompactFlash (Read/write)
Configuration register is 0x2102
```

Configuration Register 

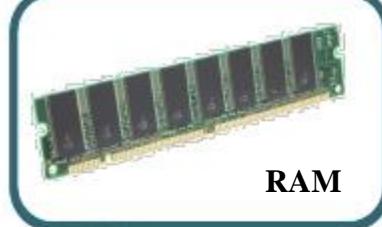


IOS Device의 기본 관리

- **IOS File System과 Device**
- **IOS Image 관리**
- **Device Configuration 정보 관리**
- **IOS Copy Command**
- **IOS Device에서 Debug 사용**



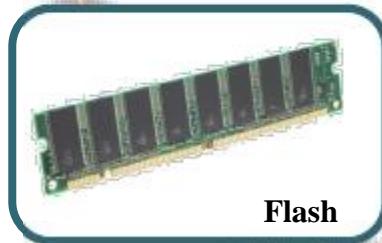
IOS File System & Device



RAM



NVRAM



Flash



TFTP



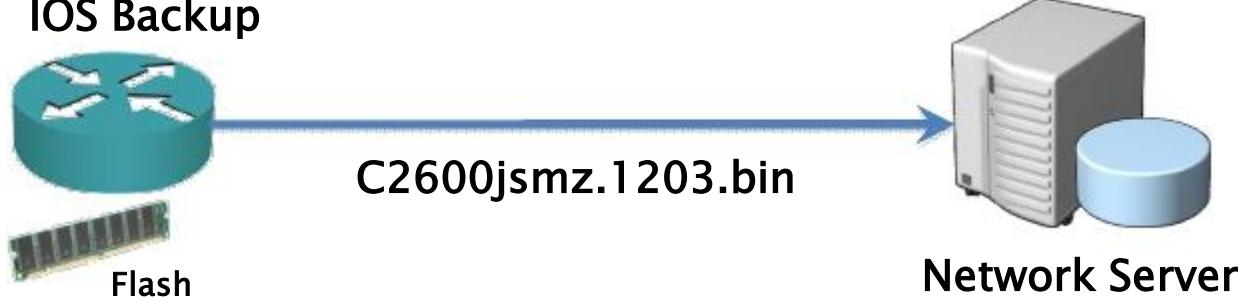
PCMCIA



IOS image 관리

- IOS Backup & Restore

- IOS Backup



- IOS Restore



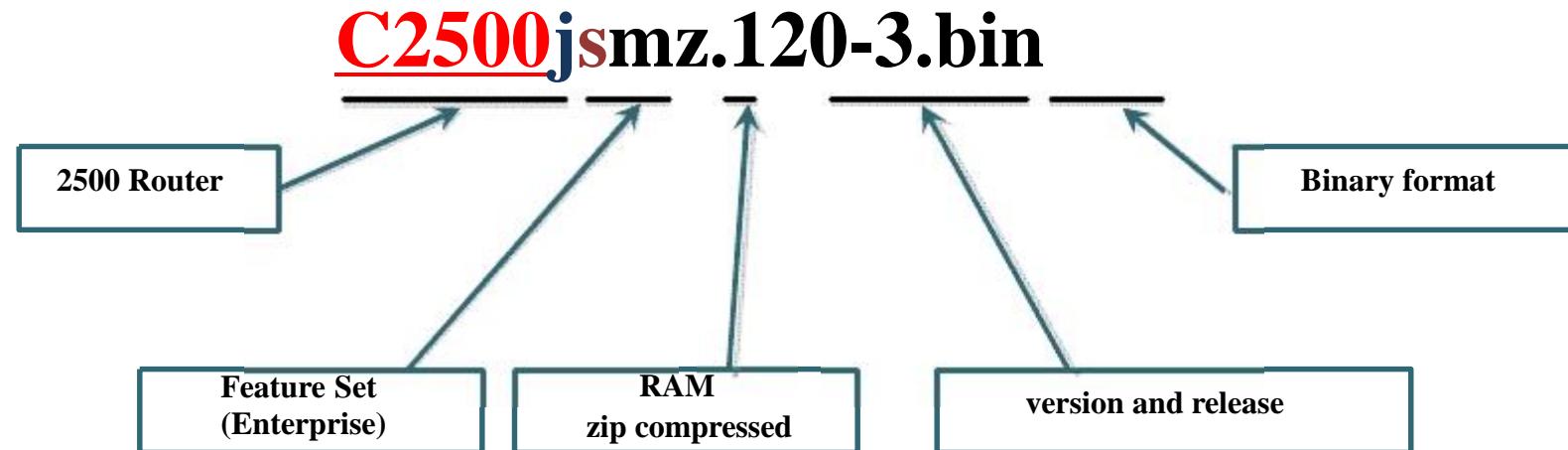
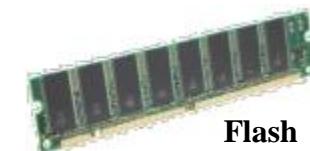


IOS image 관리

- IOS Image file Format Example

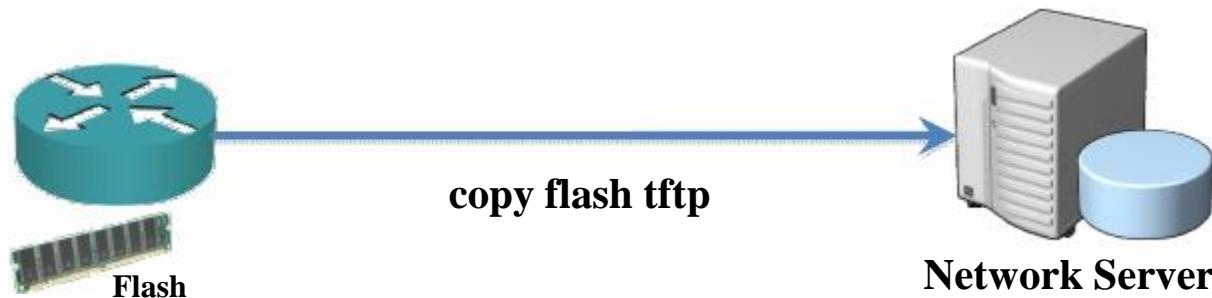
```
R1#show flash
System flash directory:
File  Length   Name/status
1    10084696  c2500-jsmz.120-3.bin

[10084760 bytes used, 6692456 available, 16777216 total]
16384K bytes of processor board system flash (Read ONLY)
```





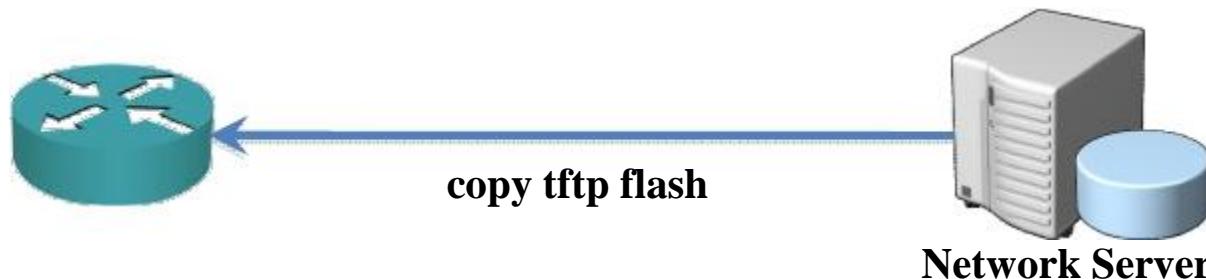
IOS image 관리 – IOS backup



```
R1#copy flash tftp
Source filename []? c2500-js-1_120-3.bin
Address or name of remote host []? 10.1.1.1
Destination filename [c2500-js-1_120-3.bin]?
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!
<output omitted>
10084696 bytes copied in 709.228 secs (14223 bytes/sec)
Router#
```



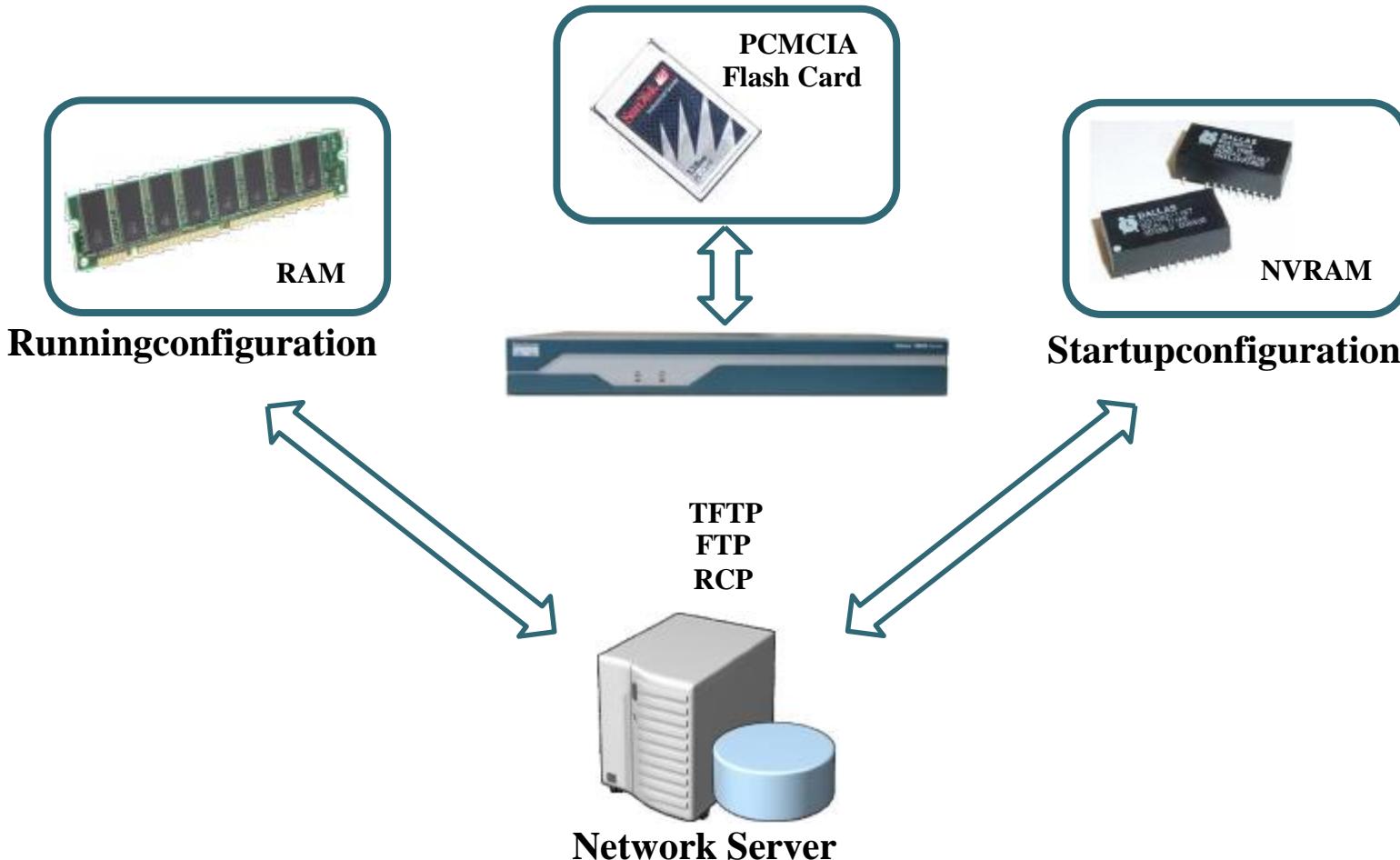
IOS image 관리 – Restore & Upgrade



```
R1#copy tftp flash
Address or name of remote host [10.1.1.1]?
Source filename []? c2500-js-l_120-3.bin
Destination filename [c2500-js-l_120-3.bin]?
Accessing tftp://10.1.1.1/c2500-js-l_120-3.bin...
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device... eeeee (output omitted) ...erased
Erase of flash: complete
Loading c2500-js-l_120-3.bin from 10.1.1.1 (via Ethernet0): !!!!!!!!!!!!!!!!
!!!!!!!!!!!!!! (output omitted)
[OK - 10084696/20168704 bytes]
Verifying checksum... OK (0x9AA0)
10084696 bytes copied in 309.108 secs (32636 bytes/sec)
Router#
```

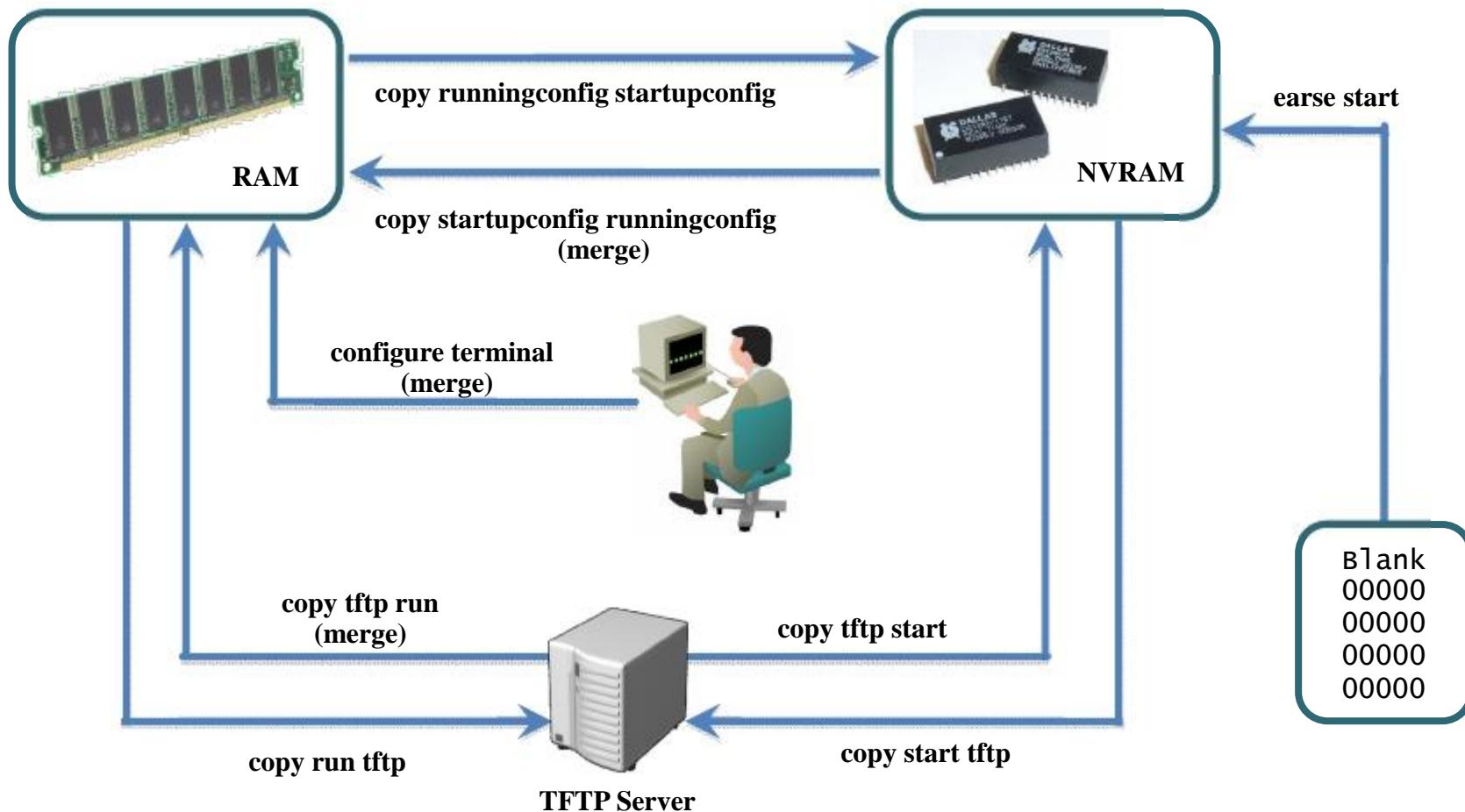


IOS device configuration 관리





IOS copy command





IOS copy command

Router의 runningconfig

```
Interface serial 0
 ip address 10.1.1.1 255.255.255.0
!
Interface ethernet 0
 ip address 10.2.2.2 255.255.255.0
!
Interface ethernet 1
 no ip address
```

TFTP Sever의 test.cfg

```
Interface ethernet 0
 ip address 172.16.1.1 255.255.255.0
!
Interface ethernet 1
 ip address 192.168.1.1 255.255.255.0
```

copy tftp runningconfig (merge)

copy 결과

```
Interface serial 0
 ip address 10.1.1.1 255.255.255.0
!
Interface ethernet 0
 ip address 172.16.1.1 255.255.255.0
!
Interface ethernet 1
 ip address 192.168.1.1 255.255.255.0
```



IOS copy command

- Configuration 정보 Copy

```
R1#copy running-config tftp
Address or name of remote host [ ] ? 10.1.1.1
Destination filename [running-config] ? wgrox.cfg
.!
1684 bytes copied in 13.300 sec (128 bytes / sec )

R1#copy tftp running-config
Address or name of remote host [ ] ? 10.1.1.1
Source filename [ ] ? wgrox.cfg
Destination filename [running-config] ?
Accessing tftp://10.1.1.1/wgrox.xfg....
Loading wgrox.cfg from 10.1.1.1 (via ethernet 0 ) : !!
[OK - 1684/3072 bytes]

1684 bytes copied in 17.692 secs (99 byte / sec)
```



IOS device에서 debug command 사용

▪ Show와 Debug Command의 비교

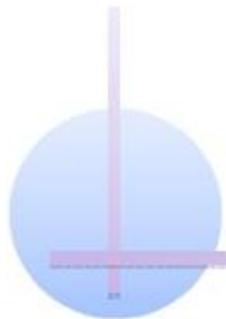
구분	show	debug
실행에 따른 구분	Static	Dynamic
실행에 따른 Overhead	Low	High
주된 사용 용도	상태정보 확인	특정 동작 과정 확인

▪ Show command

- interface, protocols, performance, media등의 정적이고, 부분적인 정보확인

▪ Debug command

- 각종 protocol들의 traffic의 흐름을 실시간으로 분석 할 수 있으며, configuration의 문제점 확인 가능



Chapter 03 Switching



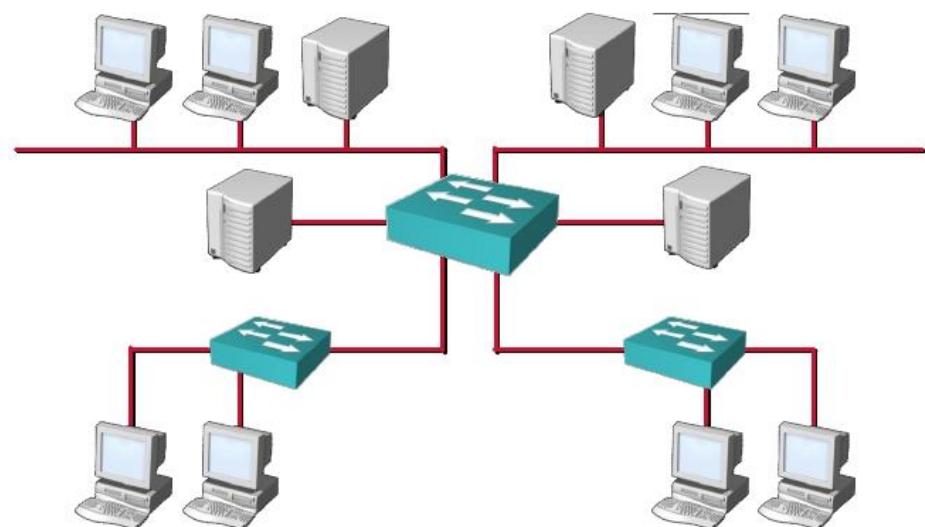
Ethernet Switches and Bridges

- 2계층 스위치의 세가지 주요 기능

-주소학습 : 각 포트로 들어오는 프레임의 출발지 MAC 주소와 포트 정보를 MAC 데이터베이스(mac-address-table)에 저장한다.

- 패킷 포워딩/필터링 : 스위치가 프레임을 수신하면 MAC 테이블을 참조하여 어떤 포트로 프레임을 내보낼 것인지를 결정한다. 포트가 결정되면 결정된 포트로만 프레임을 전송한다.

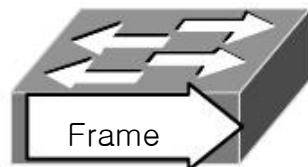
- 루프방지 : 스위치 네트워크의 이중화로 인해 발생되는 루프를 방지하는 기능을 가지고 있다.



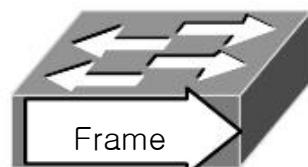


프레임 전송 방식

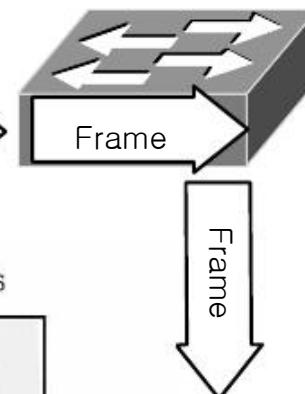
- Fragment-Free



- CUT-Through



- Store and Forward



6 bytes 1 byte 6 bytes 6 bytes 2 bytes up to 1500 bytes 4 bytes

Preamble	SFD	Destination hardware addresses	Source hardware addresses	Length	DATA	FCS
----------	-----	--------------------------------	---------------------------	--------	------	-----

Default switching
cut-through;
no error checking

CUT-Through:
checks for
collisions

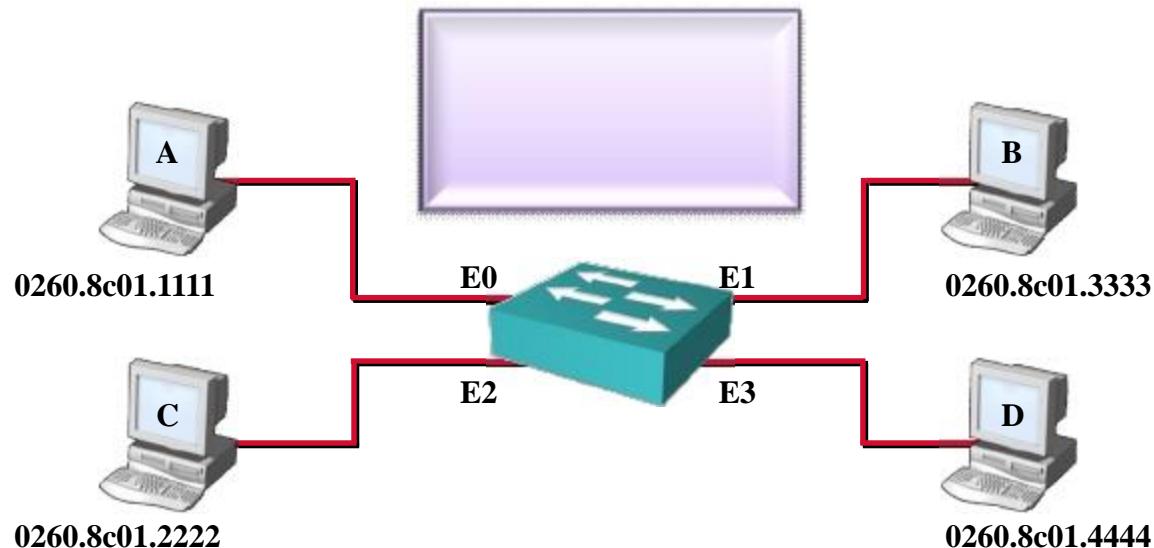
Store-and-forward:
all errors filtered;
has highest latency

- **Store and Forward** : 프레임이 포워딩 하기 전에 완전한 프레임을 수신해야 한다. 목적지 주소와 출발지 주소를 읽고 CRC를 수행한 후 프레임을 포워딩한다. 손상된 프레임은 버려진다. 지연시간은 프레임 길이에 따라 다르다.
- **Cut-through** : 프레임 헤더가 도착하자마자 목적지 주소를 검사하고 바로 프레임을 포워딩한다. 패킷의 지연시간은 엄청 줄어든다. 단점은 CRC 값에 오류가 있는 프레임이나 충돌된 프레임을 여전히 포워딩한다
- **Fragment-free** : 스위치가 프레임을 포워딩하기 전에 첫 번째 64bytes를 읽어 들여서 CRC 검사를 한 다음 이상이 없으면 포워딩 한다. 대개 프레임의 손상이나 충돌은 프레임의 첫 번째 64bytes에서 발생되기 때문이다.



MAC 주소 학습

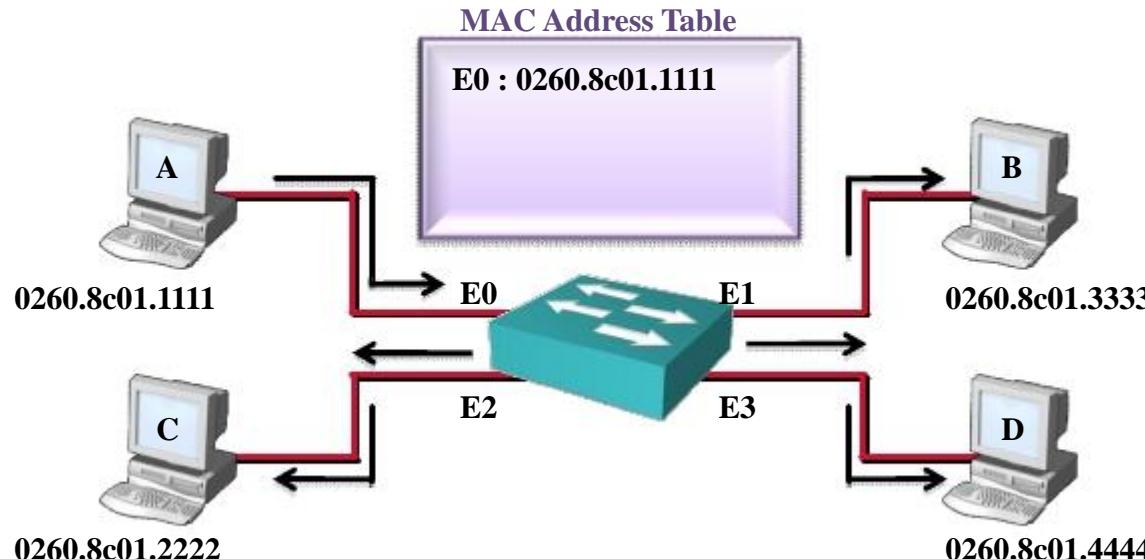
MAC Address Table



- 초기에는 MAC Address Table이 비어 있다



MAC 주소 학습

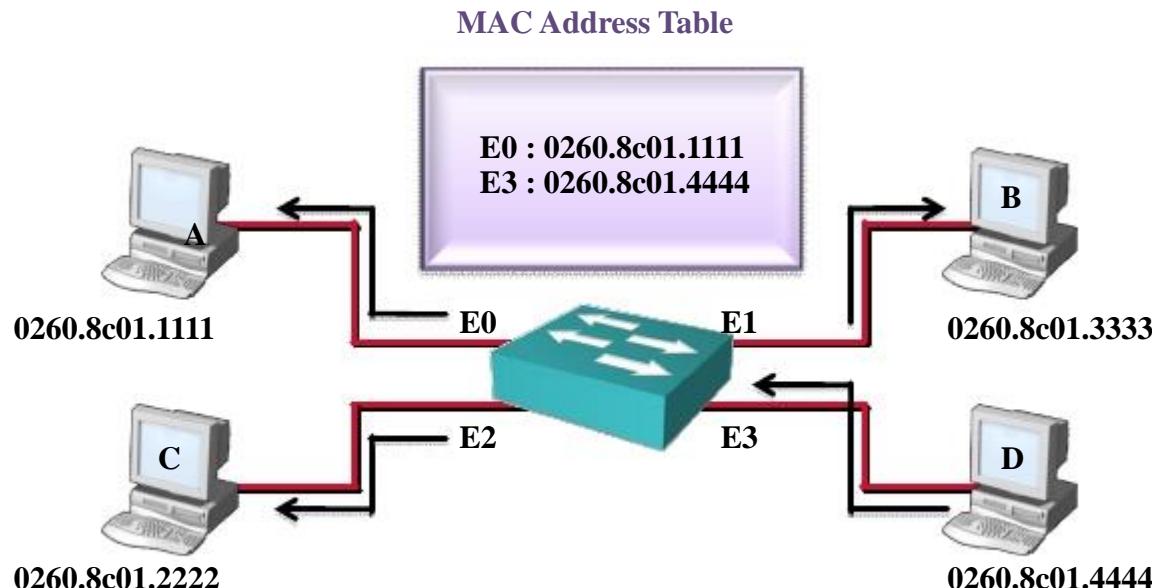


- Host A가 Host B에게 Frame을 전달한다.
- Switch는 MAC Address Table이 비어 있기 때문에 Frame을 모든 포트로 Flooding한다.
- Host A에서 온 Frame을 Flooding하는 동안 스위치는 E0에 Host A의 MAC Address를 학습한다.
- Host A에 대한 MAC Address Table 정보는 Cache에 저장된다. (Aging Time 300초)

참고) 플러딩(Flooding)이란 스위치로 들어온 프레임의 목적지 MAC주소에 대한 정보가 Mac-address-table에 저장되어 있지 않을 경우 해당 프레임이 들어온 포트를 제외한 나머지 모든 포트로 프레임을 내보내는 것을 가리킨다.



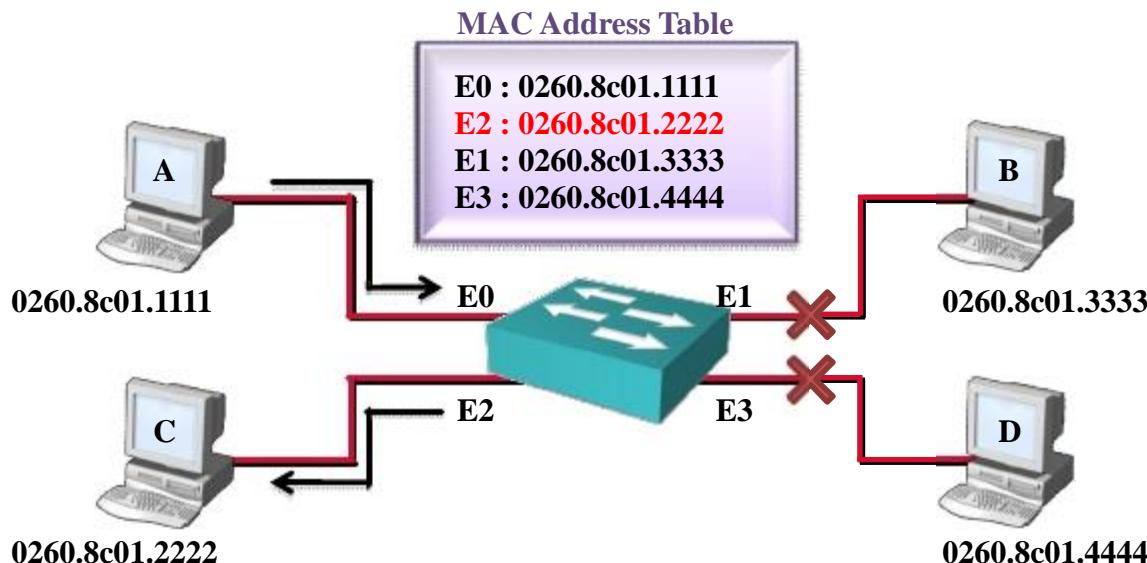
MAC 주소 학습(계속)



- Host D가 Host C에게 Frame을 전달한다.
- Switch는 MAC Address Table에 목적지 MAC Address에 대한 정보가 없기 때문에 Frame을 전달된 포트를 제외한 모든 포트로 Flooding한다.
- Host D에서 온 Frame을 Flooding하는 동안 스위치는 E3에 Host D의 MAC Address를 학습한다.
- Host D에 대한 MAC Address Table 정보는 Cache에 저장된다. (Aging Time 300초)



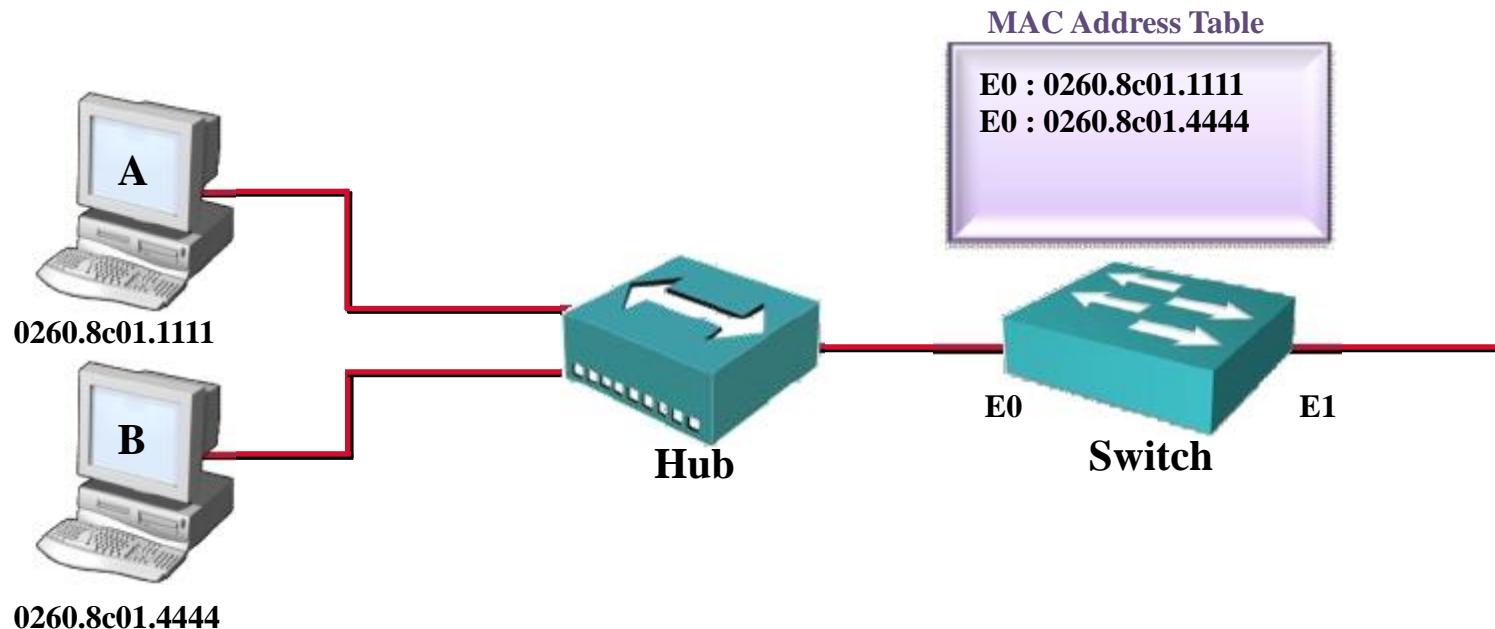
프레임 포워딩(Frame Forwarding)



- Host A가 Host C에게 Frame을 전달한다.
- Switch는 MAC Address Table에 목적지 MAC Address에 대한 정보를 찾아 해당하는 포트인 E2로 Frame을 전달한다.
- E2에 대한 Aging Time이 초기화 된다.



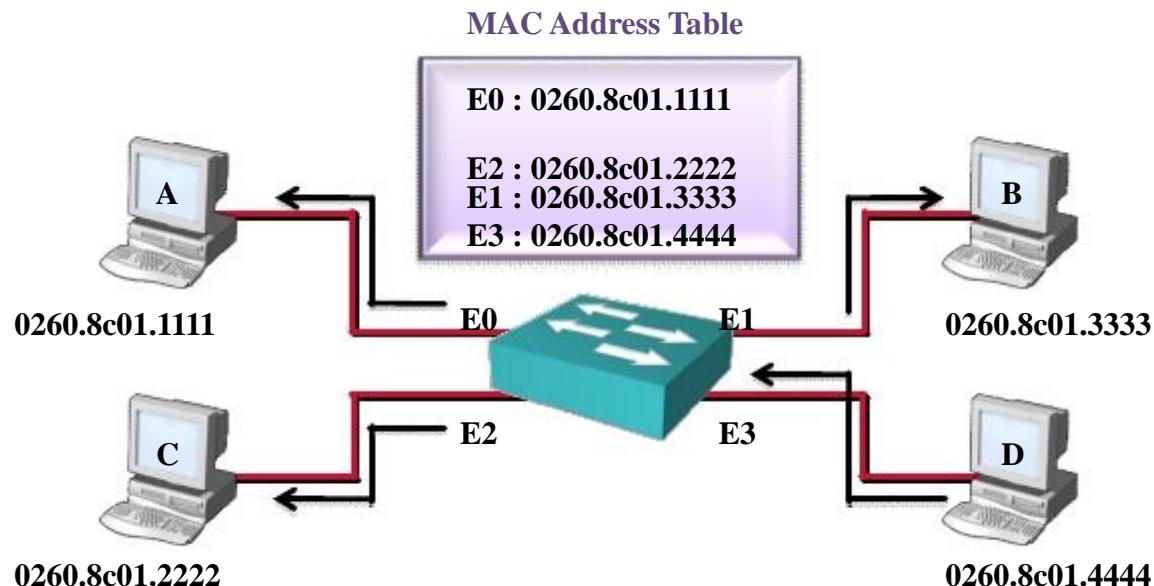
프레임 필터링(Frame Filtering)



- Host A가 Host B에게 Frame을 보낸다.
- Switch는 MAC Address Table에 Host B의 MAC Address를 추가한다.
- 이후에 Host A와 Host B가 통신을 할 때 스위치는 E0로 들어오는 프레임이 다른 포트로 전달되는 것을 차단하게 된다.



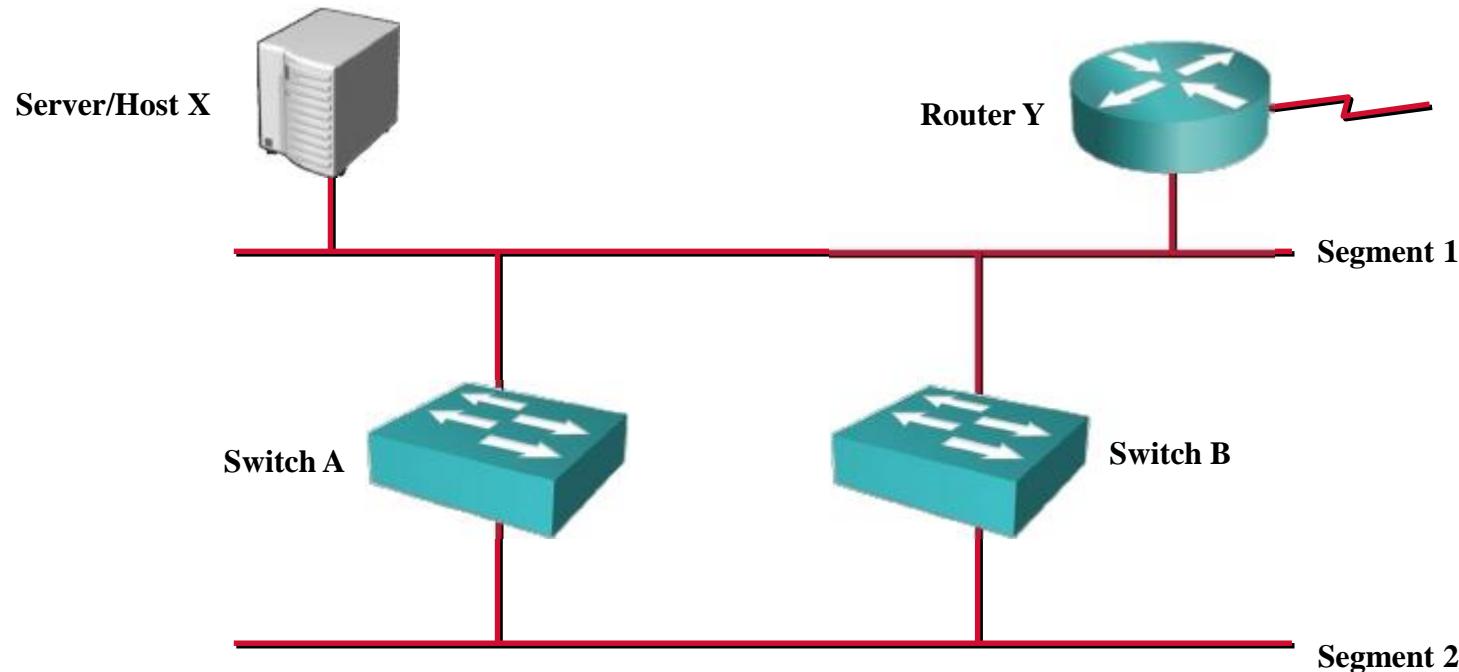
Broadcast와 Multicast 프레임 전송



- Host D가 Broadcast 또는 Multicast를 보낸다.
- Broadcast나 Multicast는 전달된 포트를 제외한 모든 포트로 Flooding 된다.



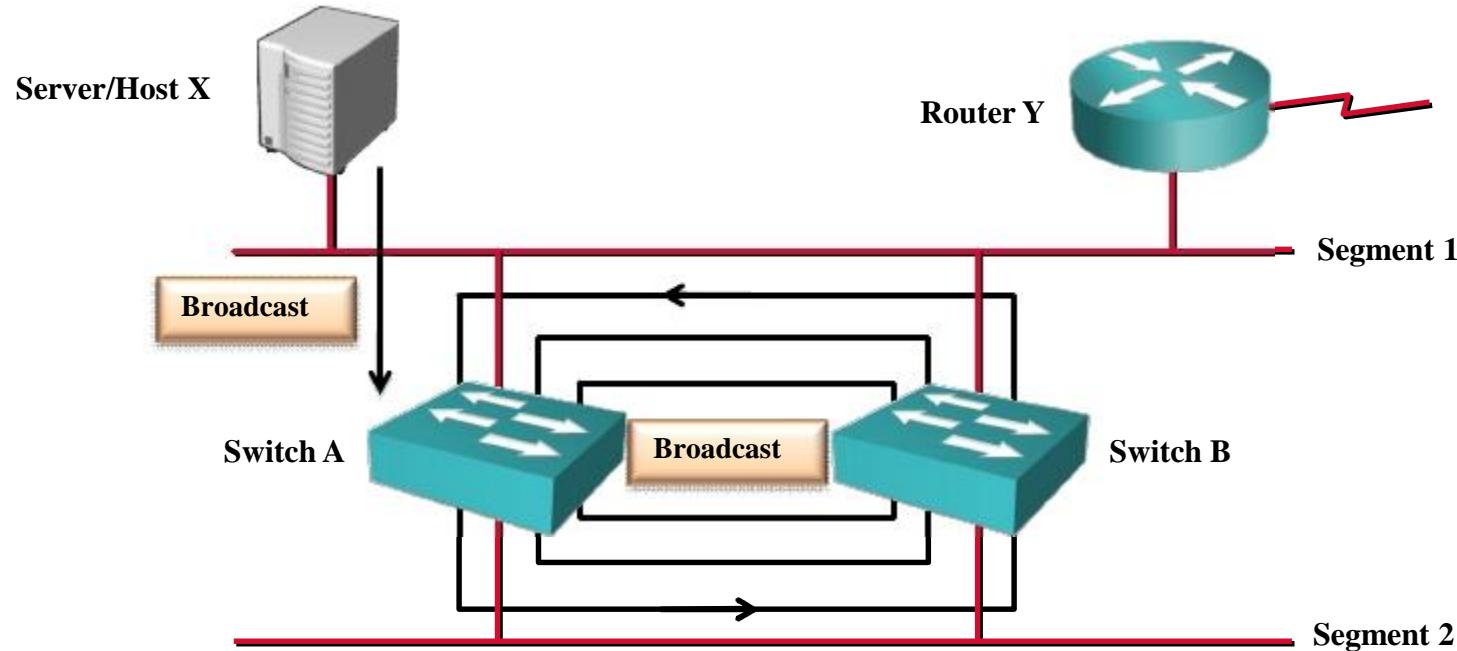
이중화 토플로지



- 링크 이중화는 한 지점에서의 장애로 인해 네트워크의 기능 상실을 방지한다
- 하지만 링크 이중화로 인해서 Broadcast Storm, Multiple frame 복사, MAC Address Table 불안정성 문제가 발생한다



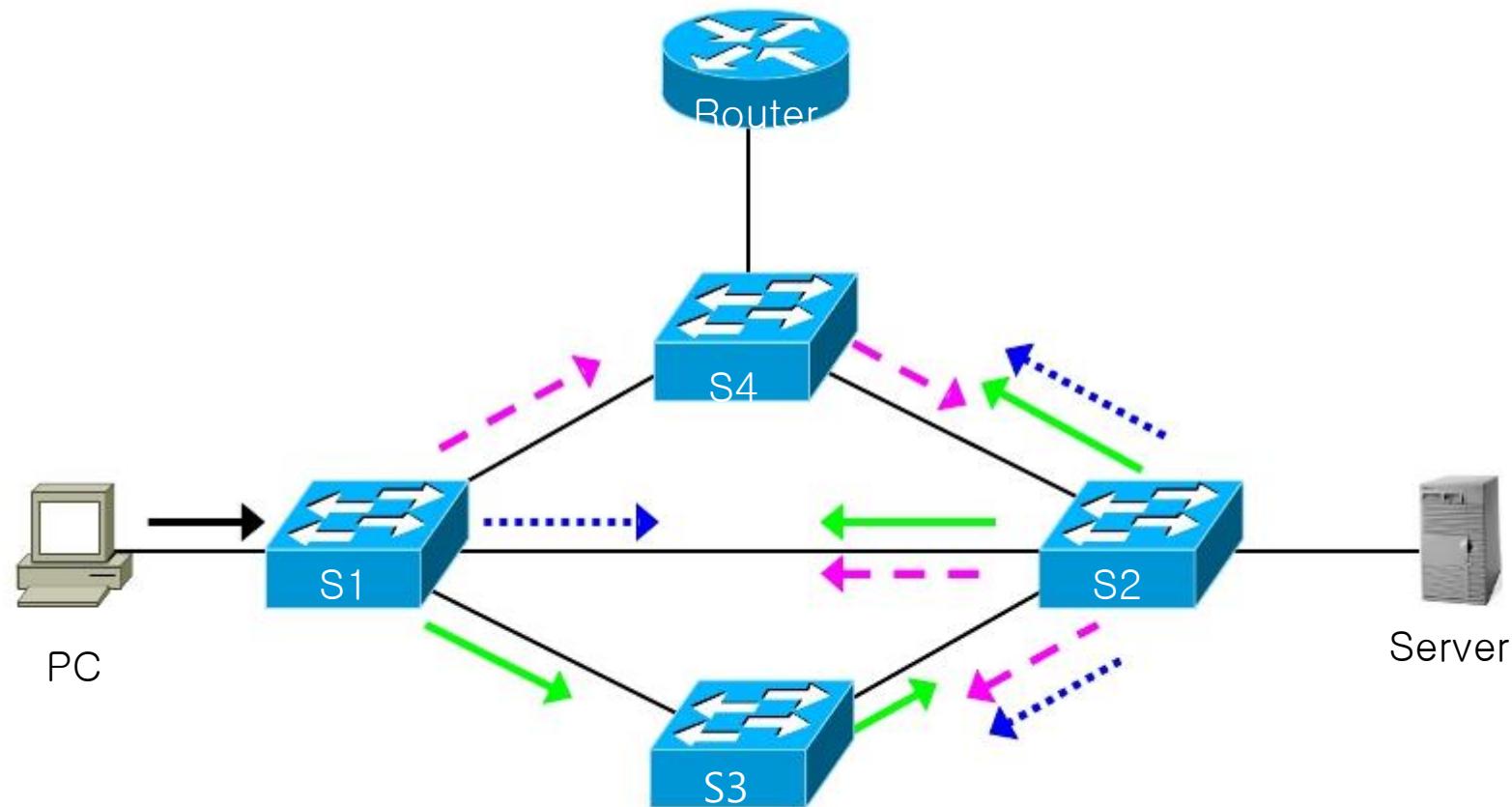
Broadcast Storm



- Host X가 Broadcast를 보낸다.
- Broadcast를 받은 Switch A는 플러딩을 하게 된다.
- Switch B 역시 Broadcast 프레임을 받게 되고, 계속해서 Broadcast traffic을 서로에게 전달한다.



Broadcast Storm



- S1에서 3개의 프레임이 브로드캐스트 되면 다시 6개가 되어 돌아온다. 이렇듯 브로드캐스트 트래픽은 기하급수적으로 늘어나게 되며, 결국 대역폭을 모두 소진할 때까지 늘어나고, 네트워크는 마비되게 된다.

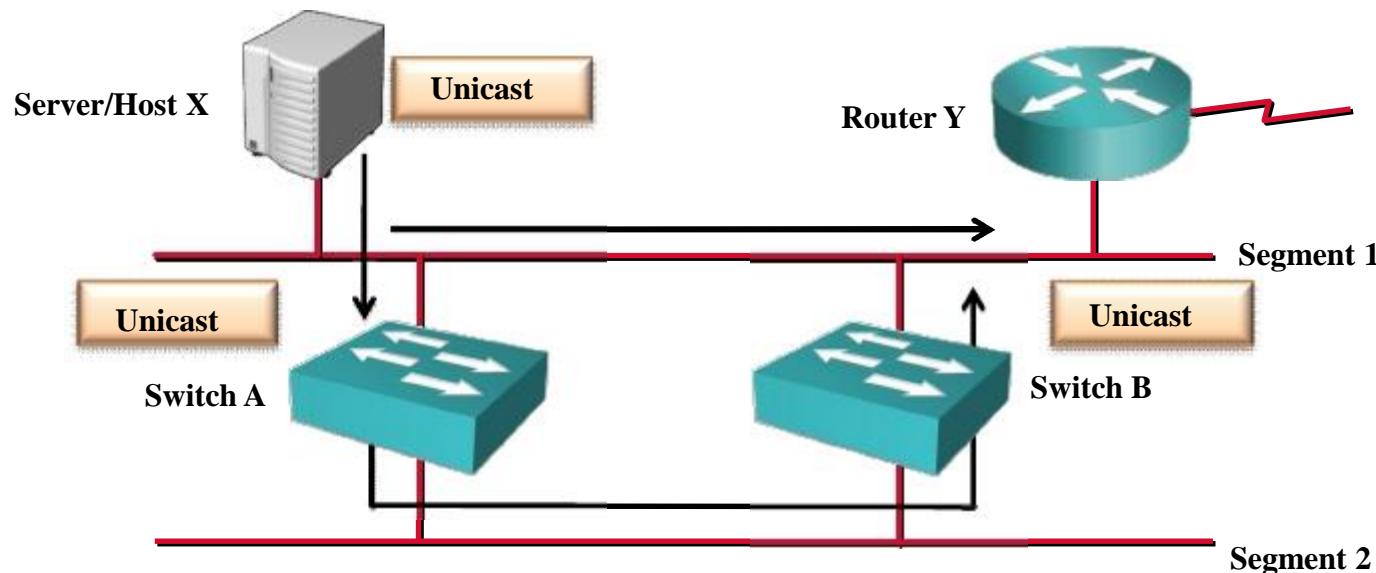


Broadcast Storm

- 스위치 네트워크를 이중화로 구성했을 때 발생할 수 있는 프레임 루프 문제를 살펴보자.
 - **IP 패킷** : 루프가 발생하면 TTL (Time To Live) 필드에 의해 무한정 루프 방지.
 - * 라우터간에 최대 255회의 루핑 후에 패킷이 폐기된다.
 - **이더넷 프레임** : IP의 TTL에 해당하는 필드가 없어서 무한 루핑 발생이 가능.
 - * 따라서 루프 발생시 인위적으로 차단하지 않으면 중단되지 않는다.
 - * 스위치에는 모두 STP가 작동하기 때문에 대부분의 루프 걱정은 없다.
 - **루프 발생시 증상** : * 큰 망에서는 수초 동안만 발생해도 스위치 다운된다.
 - * 스위치 LED가 빠른 속도로 깜박거림
 - * CPU 사용율이 급격히 상승 "[show process cpu](#)"
 - * 네트워크 속도가 느려지고 심하면 다운된다.
 - **루프 대처 방법** : * 스위치간 루프 발생 포트를 'shutdown' 시키거나
 - * 루프 발생 포트의 케이블을 잠시 뽑았다가 꽂아주면 된다.
 - 그런 다음 루프가 발생한 원인을 찾아 제거해 주어야 한다.



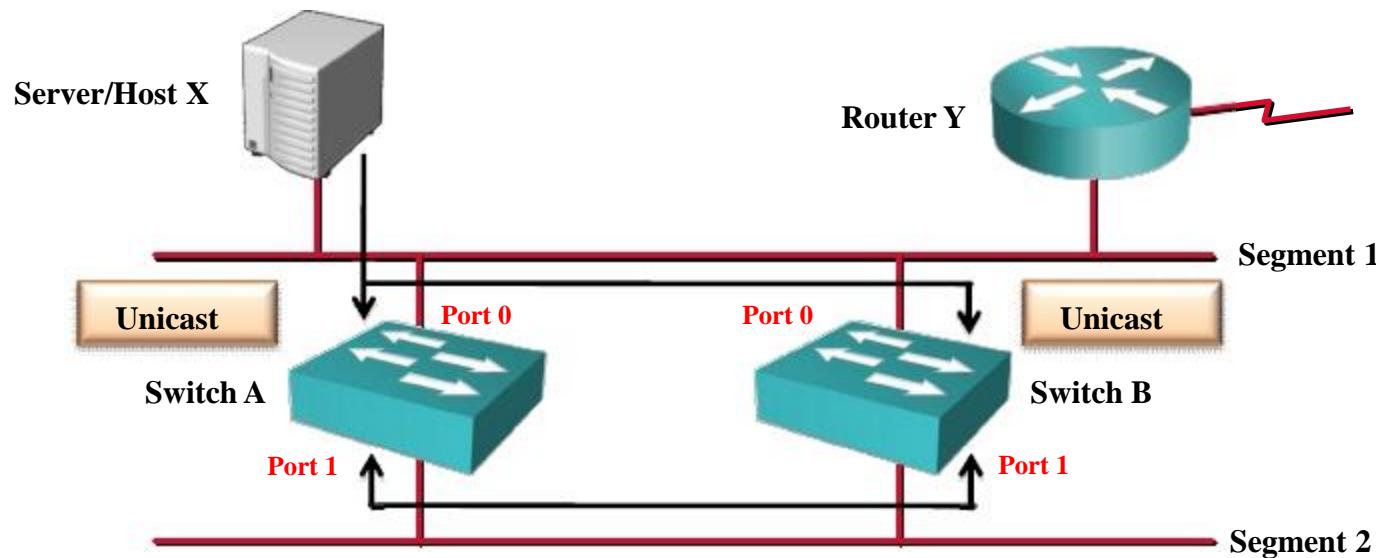
Multiple Frame 복사



- Host X가 Unicast Frame을 Router Y에게 보낸다.
- Router Y와 Switch A는 Frame을 받게 된다. Switch A는 MAC Table에 Host X에 대한 MAC Address가 없기 때문에 Flooding한다.
- Switch A로부터 Flooding된 Frame을 Switch B가 받아 다시 Flooding한다.
- Router Y는 복사된 동일한 Frame을 다시 받게 된다.



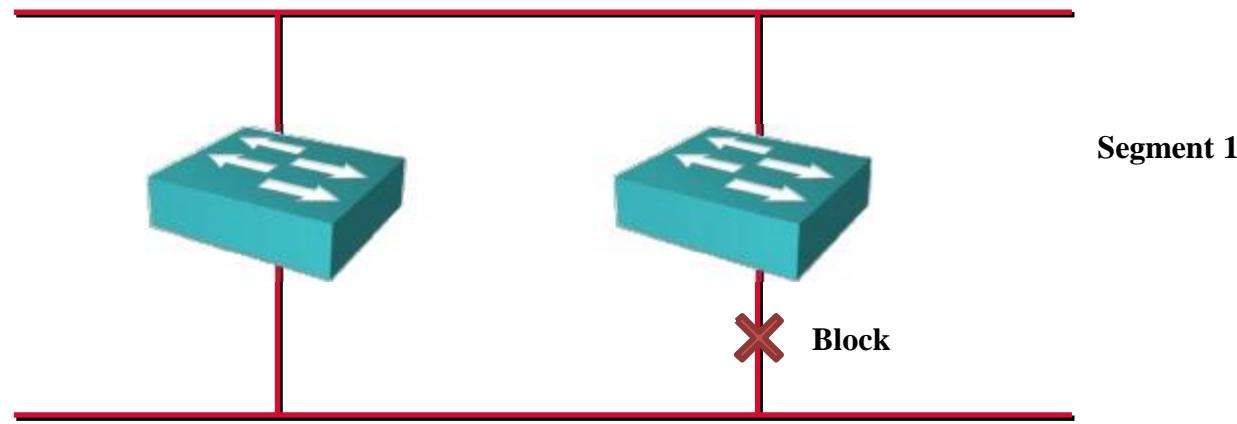
MAC Database 불안정성



- Host X가 Unicast Frame을 Router Y에게 보낸다.
- 아직 Router Y의 MAC Address를 학습한 Switch가 없다.
- Switch A와 Switch B는 Port 0에 Host X에 MAC Address를 학습한다.
- 두 Switch에서 Router Y로 가는 Frame이 Flooding 된다.
- Switch A와 Switch B가 Port 1에서 Host X에 MAC Address를 부정확하게 학습한다.



Spanning Tree Protocol



- STP는 Switch가 Topology내의 루프를 방지하기위해 하나의 경로만을 남기고 나머지 Link를 차단하여 Loop를 제거한다.
- STP는 포트를 계속 모니터링 하다가 다른 포트에 장애나 토플로지 변경이 발생하는 경우 포트를 재 설정하여 연결의 완전 손실이나 새로운 루프를 막는다.

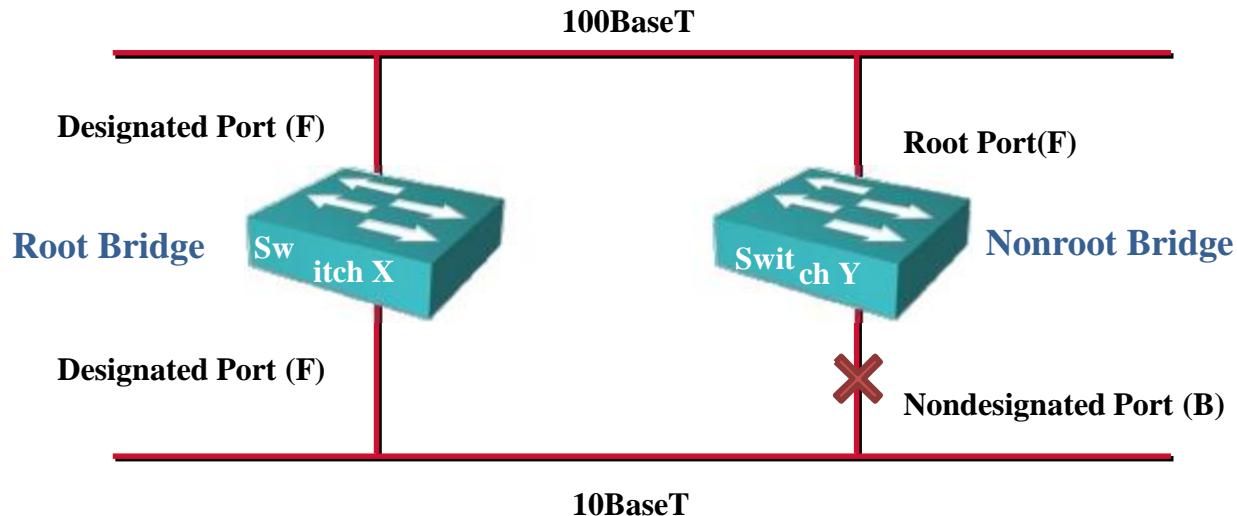


BPDU (802.1d)

802.1 - Bridge Spanning Tree	
♦ Protocol Identifier:	0 [17-18]
♦ Protocol Version ID:	0 [19]
♦ Message Type:	0 Configuration Message [20]
♦ Flags:	\$00000001 [21]
	Topology Change Notification Acknowledge
■ Root Priority/ID:	0x8000/ 00:0D:BC:9A:BF:81 [22-29]
♦ Cost Of Path To Root:	0x00000000 (0) [30-33]
■ Bridge Priority/ID:	0x8000/ 00:0D:BC:9A:BF:81 [34-41]
♦ Port Priority/ID:	0x80/ 0x03 [42-43 Mask 0x00FF]
♦ Message Age:	0/256 seconds (<i>exactly 0 seconds</i>) [44-45]
♦ Maximum Age:	5120/256 seconds (<i>exactly 20 seconds</i>) [46-47]
♦ Hello Time:	512/256 seconds (<i>exactly 2 seconds</i>) [48-49]
♦ Forward Delay:	3840/256 seconds (<i>exactly 15 seconds</i>) [50-51]



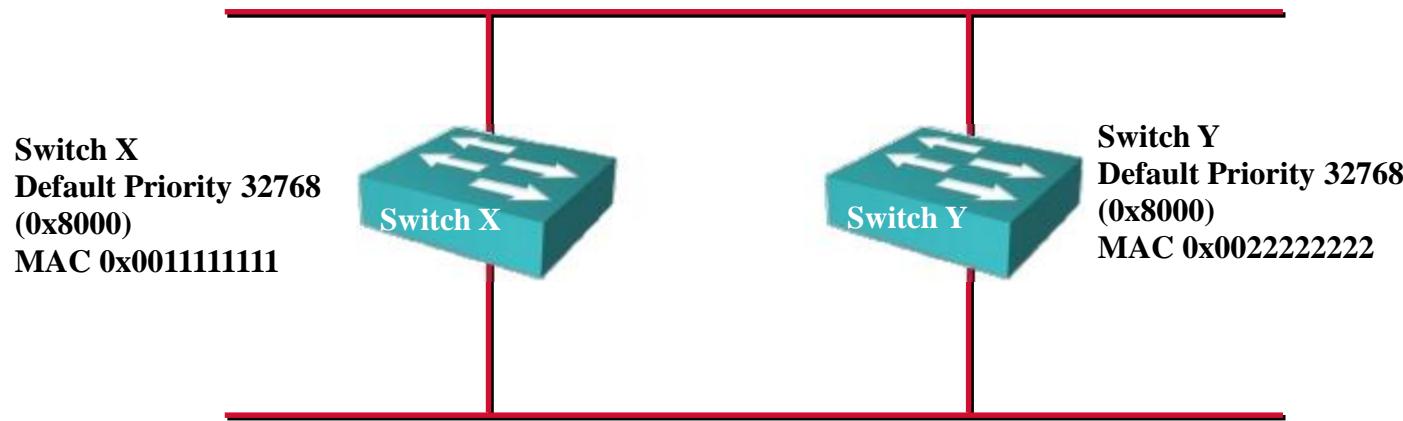
SpanningTree 동작



- Network당 하나의 Root Bridge를 가진다.
- NonRoot Bridge당 하나의 Root Port를 가진다.
- Segment당 하나의 Designated Port를 가진다.
- Nondesignated Port는 사용하지 않는다.



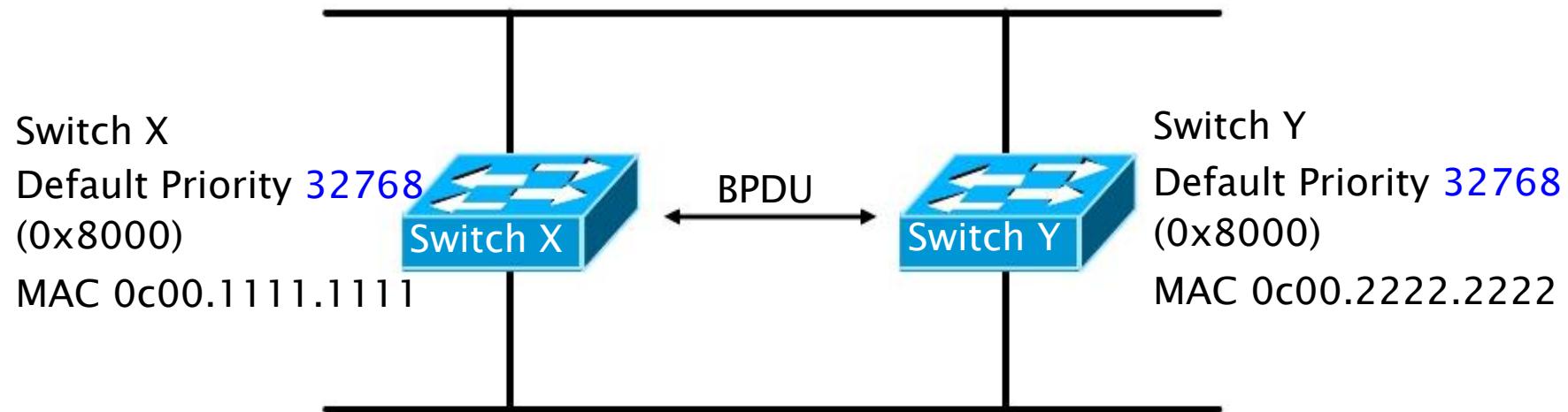
STP의 Root bridge 선택



- BPDU = Bridge Protocol Data Unit(Default = 매 2초마다 전송함)
- Root Bridge = Lowest Bridge ID를 갖는 Bridge
- Bridge ID = Bridge Priority + MAC Address



스페닝 트리 프로토콜 (STP) - 브리지 ID



- Root bridge : 가장 낮은 bridge ID를 선택한다.
 - Bridge ID는 우선순위와 브리지 MAC 주소로 구성되어 있다.
 - 디폴트 우선순위(IEEE 802.1d)는 32768 이다. (0 - 65535)
 - 디폴트 우선순위 값이 같으면 낮은 MAC 주소를 가진 것이 루트 브리지가 된다.



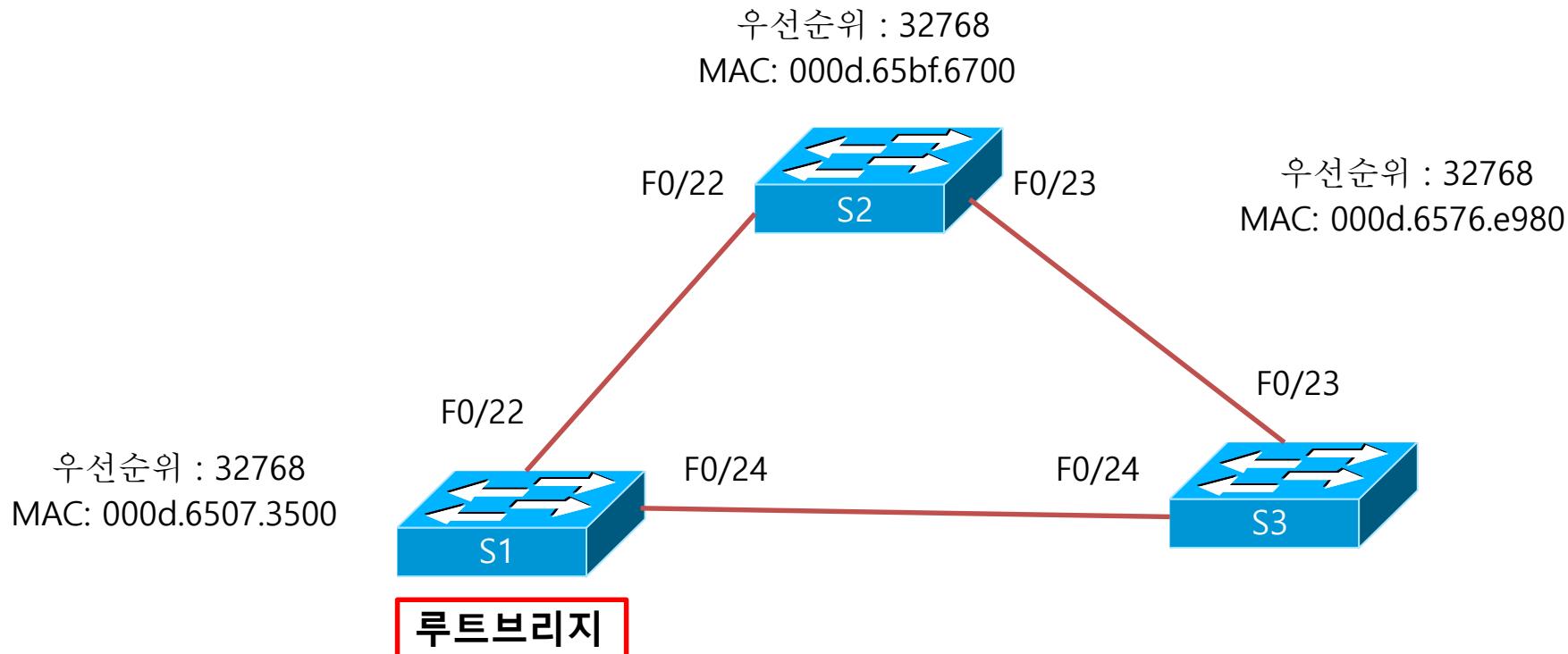
스페닝 트리 프로토콜 (STP) - 브리지 ID

우선순위 (2바이트)	MAC 주소 (6바이트)
-------------	---------------

- 브리지 ID는 2 바이트의 우선순위 (Priority)와 6 바이트의 MAC 주소로 이루어진다.
 - 브리지 ID에서 사용하는 우선순위는 기본값이 16진수로 8000이며 10진수로 변환하면 32768이다.
 - 따라서, 가장 작은 브리지 ID는 0, 가장 큰 값은 65535이다.
 - 우선순위가 낮을수록 루트 ID가 되고, 우선순위가 동일하면 MAC 주소가 낮을 수록 루트 ID가 된다.
 - VLAN당 별개의 스페닝 트리가 동작하는 PVST (Per-VLAN Spanning Tree)에서는 각 VLAN 별로 하나씩의 브리지 ID가 필요하다.
- => 결과적으로 VLAN 1000 개를 설정할 수 있는 스위치라면 서로 다른 MAC 주소 1000개가 있어야 한다.



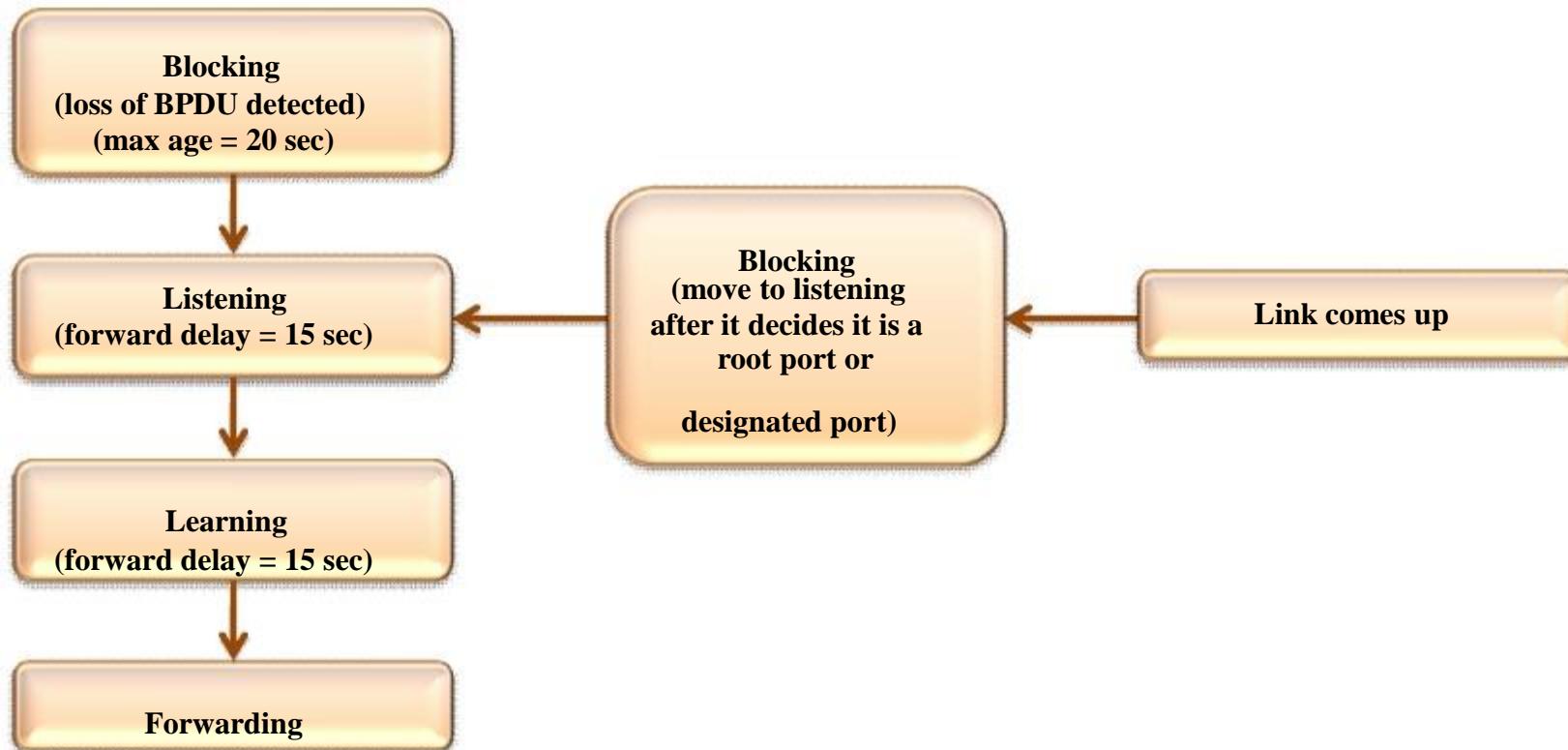
스패닝 트리 프로토콜 (STP) - 브리지 ID 확인하기



- 브리지 ID와 루트 ID는 '[show spanning-tree](#)' 명령어로 알 수 있다.
 - 이 네트워크에서 스위치 S1 이 MAC 주소가 가장 낮기 때문에 루트 스위치이다. 따라서 S1에서는 루트 ID와 브리지 ID가 동일하다.



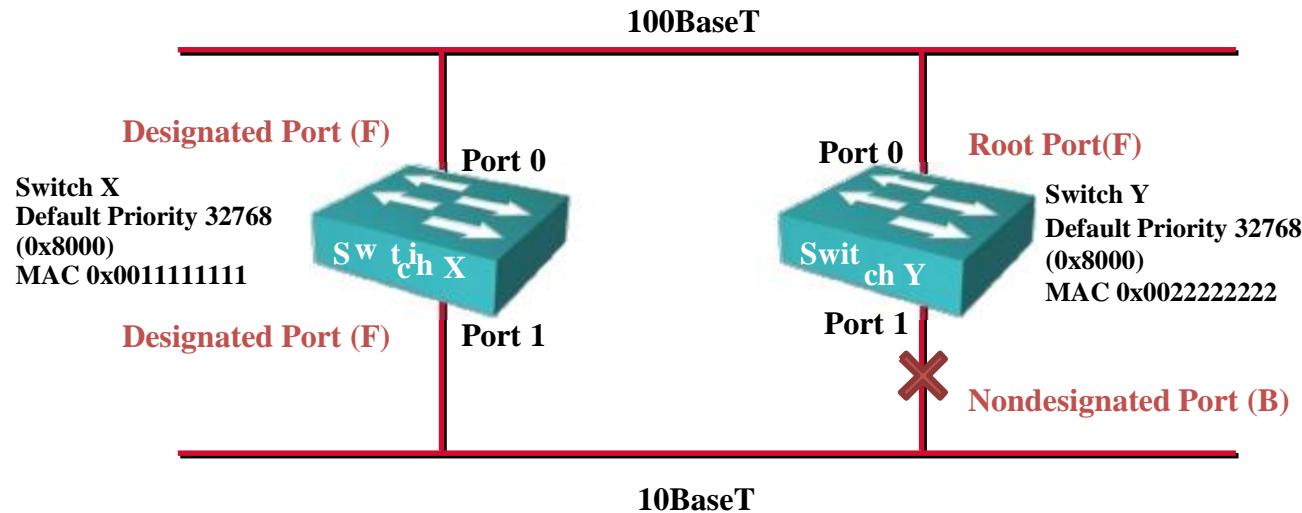
STP Port 상태



- Topology의 변화로 인하여 Blocking Mode에서 Forwarding State로 이행하는 데는 Default로 50초의 시간이 필요하며 이 기간 동안에는 프레임이 Forwarding 되지 못한다.



STP Port 상태



- Switch X(Root Bridge)는 모든 포트가 Designated Port가 된다.
- Switch Y는 cost가 더 낮은 Fastethernet port가 Root Port가 된다.
- Switch Y에 ethernet port는 Nondesignated Port가 된다.



STP 동작 방식 - 루트 포트 선택

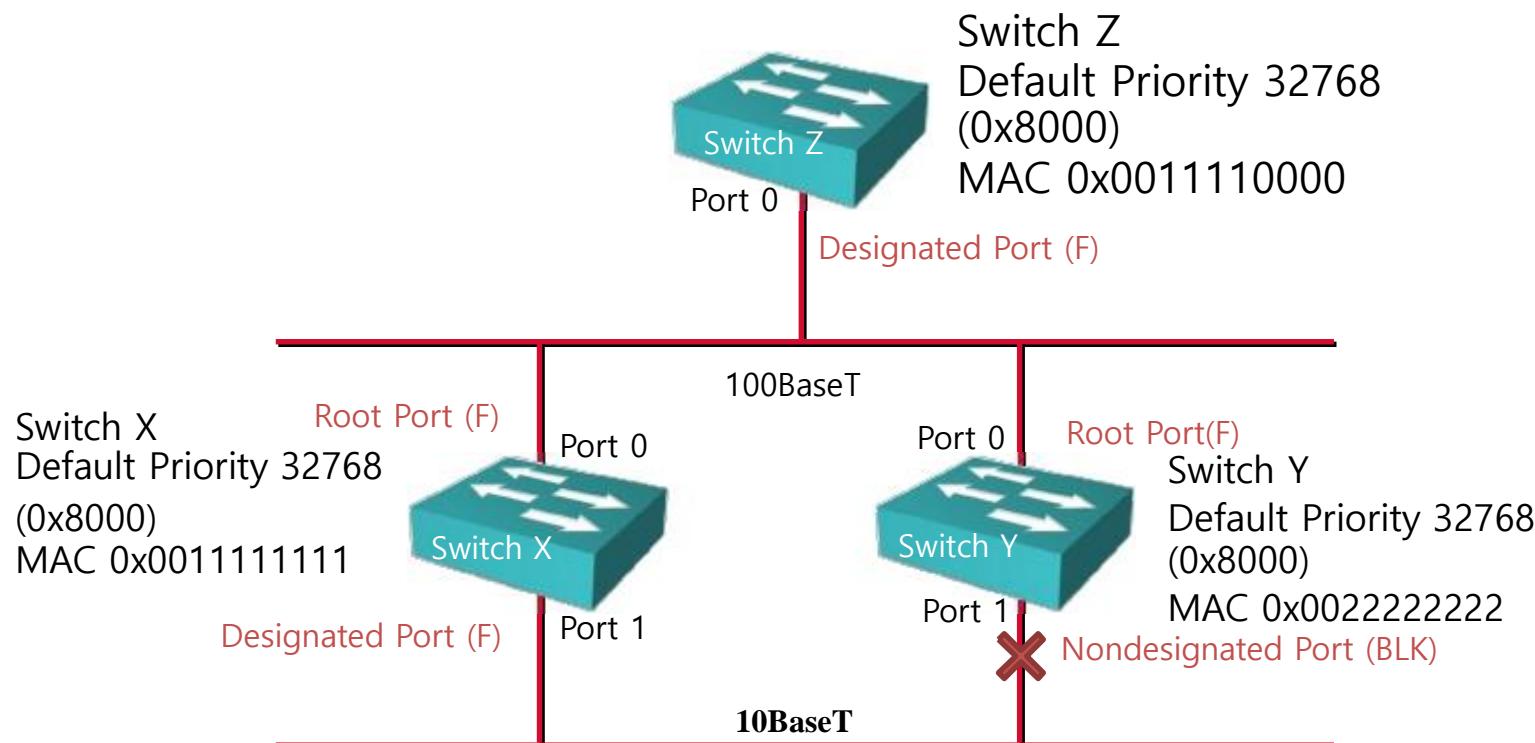
- 루트 스위치가 선택되면, 나머지 스위치에서 루트 포트를 선택해야 한다.
 - 루트 포트와 지정 포트를 선택할 때는 항상 경쟁 포트간에 다음 사항을 비교한다.
 1. 루트 스위치 ID
 2. 경로 값
 3. 브리지 ID
 4. 포트 ID

< SpanningTree Path Cost >

Link Speed	Cost (Revised IEEE Spec)	Cost (Previous IEEE Spec)
10 Gbps	2	1
1 Gbps	4	1
100 Mbps	19	10
10 Mbps	100	100

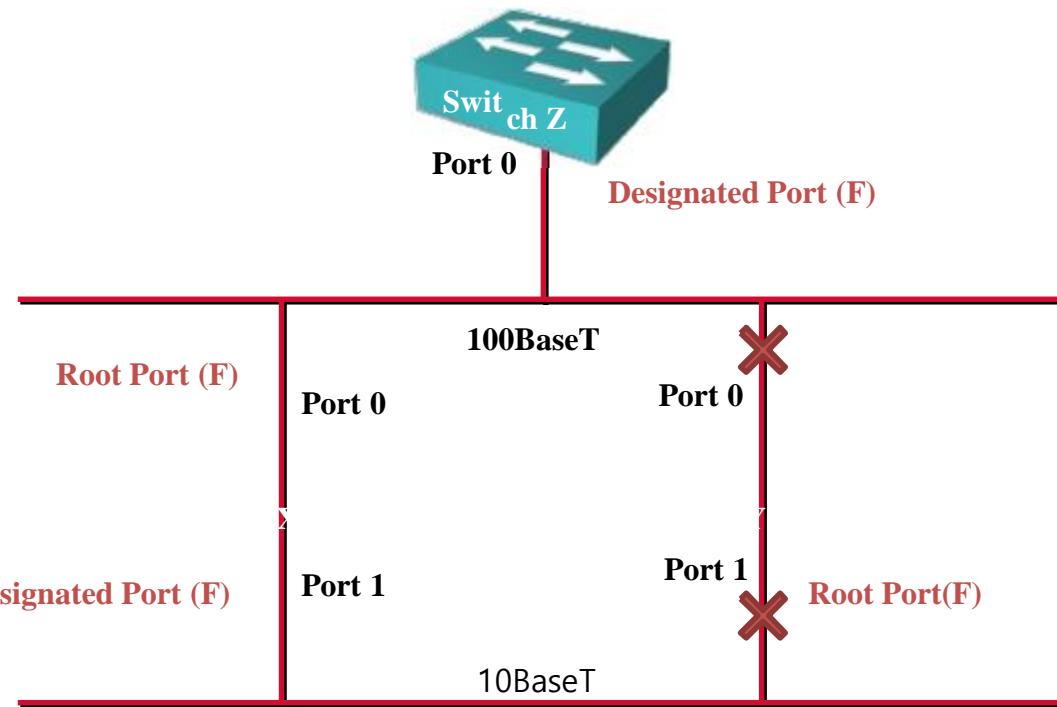


STP 동작 과정 – 예제





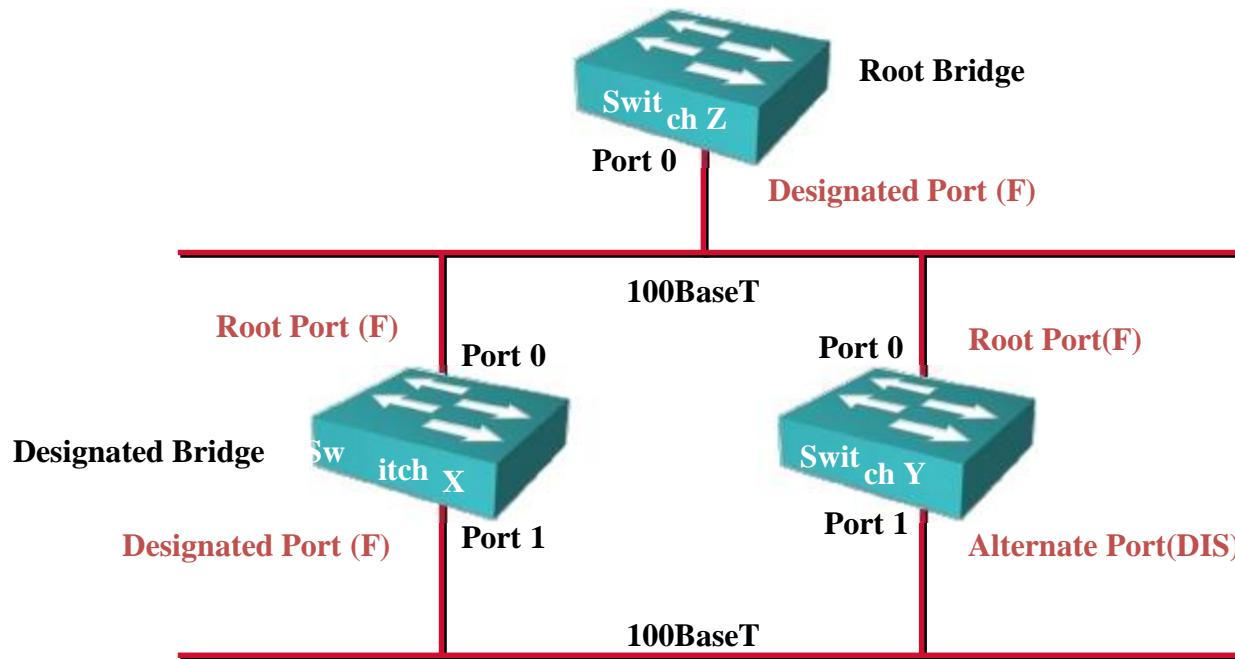
SpanningTree Recalculation



- 전달 포트에 대한 브리지 장애나 링크 장애로 인해 토폴로지가 변경될 때 STP는 Network Topology를 다시 조정해서 차단된 포트를 전달 상태로 변경하여 연결이 이루어 지도록 한다



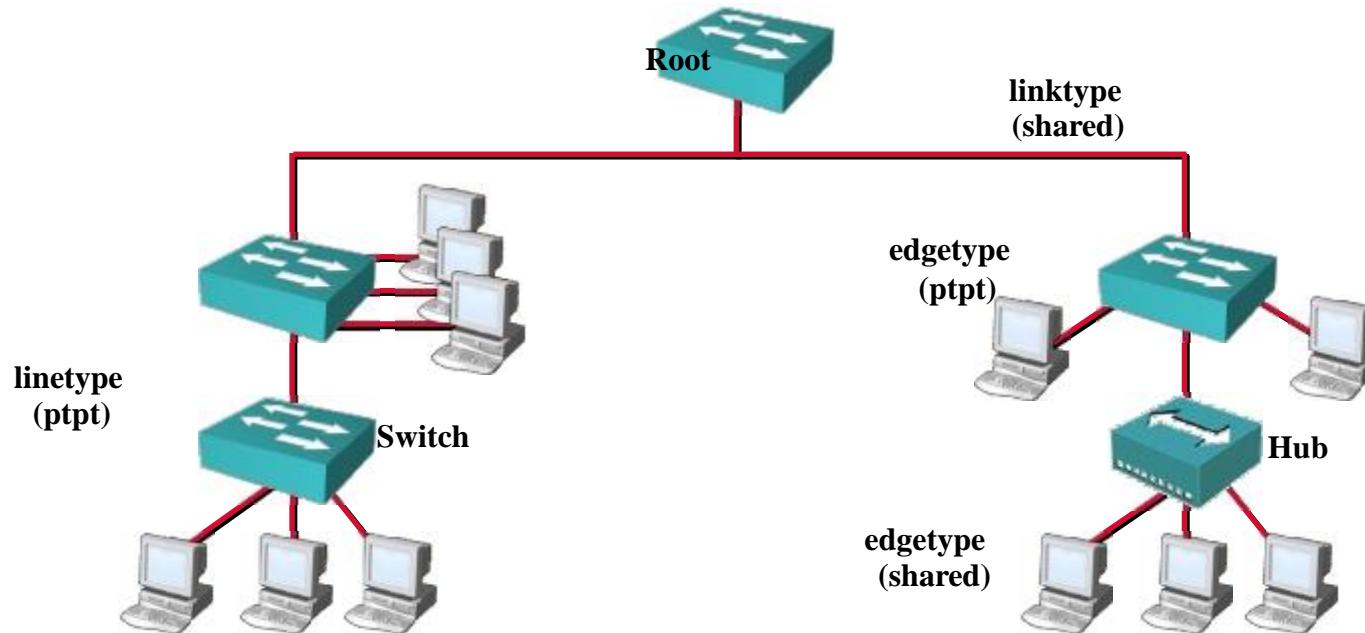
RSTP(Rapid SpanningTree protocol)



- 802.1w 표준을 RSTP(Rapid Spanning Tree Protocol)라고 부른다.
- RSTP는 링크 장애 시 빠르게 포트 변경이 이루어 진다 이전에 802.1d는 BPDU Time이 완료되기를 기다렸다가 포트를 변경하지만 802.1w는 포트 장애나 토플로지 변경 시 즉시 그 정보를 인접 장비에 전달하여 포트 선출을 하여 변경 즉시 토플로지에 적용된다.



RSTP의 포트 타입



- RSTP에서 Port Type은 Link-Type과 Edge-Type으로 구분한다.
- Line-Type은 다시 Shared or Pt-Pt로 구분된다. Shared인 경우 loop발생 여지가 있는 경우이고, Pt-Pt는 단일 Line로 연결되어 loop가 발생하지 않는 환경을 정의 한다.
- Edge-Type도 Shared와 Pt-Pt로 분리하는데 Shared는 Collision Domain인 경우이고, Pt-Pt는 서버나, 라우터와 연결되어 loop가 발생되지 않는다.



Catalyst 2950 기본 설정

- IP Address : 0.0.0.0
- CDP : enabled
- 100BaseT Port : auto negotiate duplex mode
- Spanning tree : enable
- Console password : none



Catalyst 2950 Switch의 포트 명칭

```
ASW2950#show run
```

```
Building configuration...
Current configuration:
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
```

```
ASW2950#show spanning-tree
```

```
VLAN 0001
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 000b.5f2a.5a00
This bridge is the root
Hello Time 2 sec MAX Age 20 sec Forward
Delay 15 sec
```

```
ASW2950#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24



스위치의 IP주소 구성하기

```
ASW2950(config-if)#ip address {ip_address} {mask}
```

```
ASW2950(config)#interface vlan 1  
ASW2950(config-if)#ip address 1.1.1.1 255.255.255.0
```

- Switch에 VLAN1 Interface에 IP Address와 Subnet mask를 설정한다.



스위치의 Default Gateway 구성하기

```
ASW2950(config-if)#ip default-gateway {ip_address}
```

- Catalyst 2950 Switch에 Default Gateway 설정

```
ASW2950(config)#ip default-gateway 1.1.1.254  
ASW2950(config)#
```



Switch의 IP 주소 확인하기

```
ASW2950#show interface vlan 1
  vlan1 is up, line protocol is up
    Hardware is Cat5k Virtual Ethernet, address is 0010.f6a9.9800 (bia 0010.f6a9.9800)
      Internet address is 1.1.1.1/24
      Broadcast address is 255.255.255.255
      ...
ASW2950#
```



NVRAM에 저장된 설정 삭제하기

```
ASW2950#erase startup-config
```

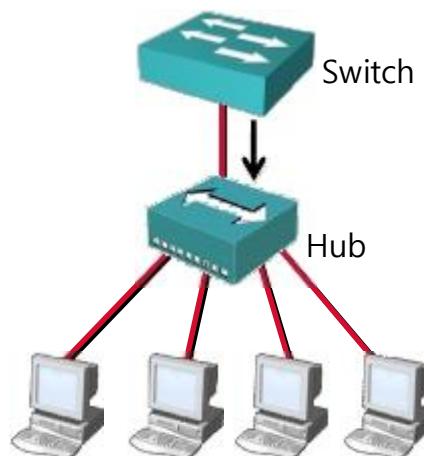
- Startupconfig 파일을 제거하면 모든 구성정보가 제거된다
- Reload를 하면 초기화된 상태로 부팅하게 된다



Duplex

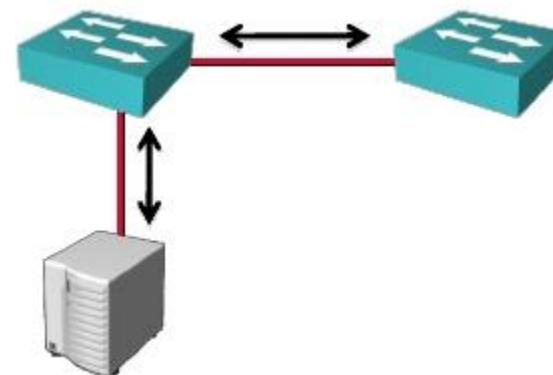
- Half Duplex (CSMA/CD)

- 단 방향 Data 흐름
- Collision 가능성이 더 높음
- Hub 연결



- Full Duplex

- PointtoPoint only
- 전용 switched port에 연결
- 양쪽에서 fullduplex 지원 필수
- Collisionfree
- Collision 감지 회선 비활성





Speed와 Duplex 변경하기

```
ASW2950(config)#interface fa1/1
ASW2950(config-if)#speed {10 | 100 | auto}
ASW2950(config-if)#duplex {auto | full | half}
```



Duplex 상태 확인하기

```
ASW2950#show interfaces fastethernet1/1
```

```
FastEthernet0/3 is up, line protocol is down
Hardware is Fast Ethernet, address is 0000.0000.0003 (bia 0000.0000.0003)
MTU 1500 bytes, BW 100000 kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)

Half-duplex, 10Mb/s
input flow-control is off, output flow-control is off
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```



MAC Address Table 관리

```
ASW2950#show mac-address-table
```

```
Dynamic Address Count: 1  
Secure Address Count: 0  
Static Address (User-defined) Count: 0  
System Self Address Count: 25  
Total MAC addresses: 26  
Maximum MAC addresses: 8192  
Non-static Address Table:
```

Destination Address	Address Type	VLAN	Destination Port
0050.0f02.3372	Dynamic	1	FastEthernet0/2



Static MAC Address 설정하기

```
ASW2950(config)#mac-address-table secure hw-addr interface [vlan vlan_id]
```

```
ASW2950(config)#mac-address-table secure 0003.3333.3333 fa 0/1 vlan 1
```

```
ASW2950#show mac-address-table
```

Dynamic Address Count:	1
Secure Address Count:	1
Static Address (User-defined) Count:	1
System Self Address Count:	25
Total MAC addresses:	28
Maximum MAC addresses:	8192

```
Non-static Address Table:
```

Destination Address	Address Type	VLAN	Destination Port
0050.0f02.3372	Dynamic	1	FastEthernet0/2
0003.3333.3333	Secure	1	FastEthernet0/1

```
Static Address Table:
```

Destination Address	VLAN	Input Port	Output Ports
2222.2222.2222	1	ALL	Fa0/1

한 포트에 mac-address-table secure 가 설정된 상태에서 다른 포트에 같은 mac으로 secure 포트를 만들면 기존의 설정은 삭제된다. 즉, 스위치에서 오로지 하나의 mac을 한 포트에만 설정 가능하다. static 보다 더 안전하다.



Port Security 설정하기

```
ASW2950(config-if)#switchport port-security
```

```
ASW2950(config)#interface fa0/1
ASW2950(config-if)#switchport mode access
ASW2950(config-if)#switchport port-security mac-address
```

- 스위치 포트의 보안 설정은 2가지가 있고, 위반시 처리방법을 설정할 수 있다.
- 보안설정 방법 : mac-address H.H.H => 수동으로 mac 설정
mac-address sticky => 자동으로 입력되는 mac으로 설정
maximum => mac 테이블에 저장될 수 있는 최대 갯수 지정
- 보안설정 위반시 처리방법 설정

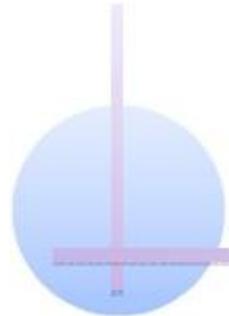
```
ASW2950(config-if)#switchport port-security violation {action}
```

- violation protect => 위반이후에 들어오는 프레임 폐기
restrict => 위반이후에 들어오는 프레임 폐기하고 count 증가
shutdown => 위반시 포트를 비활성화 시킴



Port Security 확인하기

```
ASW2950#show port-security interface fastethernet 0/1
```

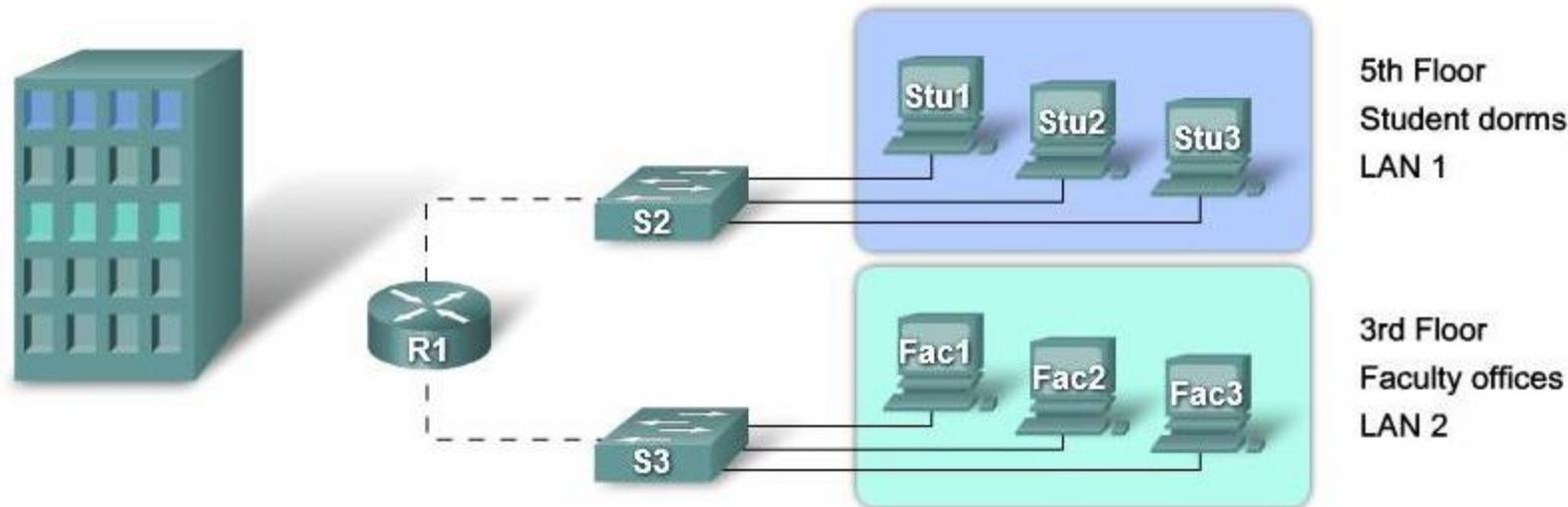


Chapter 04 VLAN 과 VTP



VLAN 개요

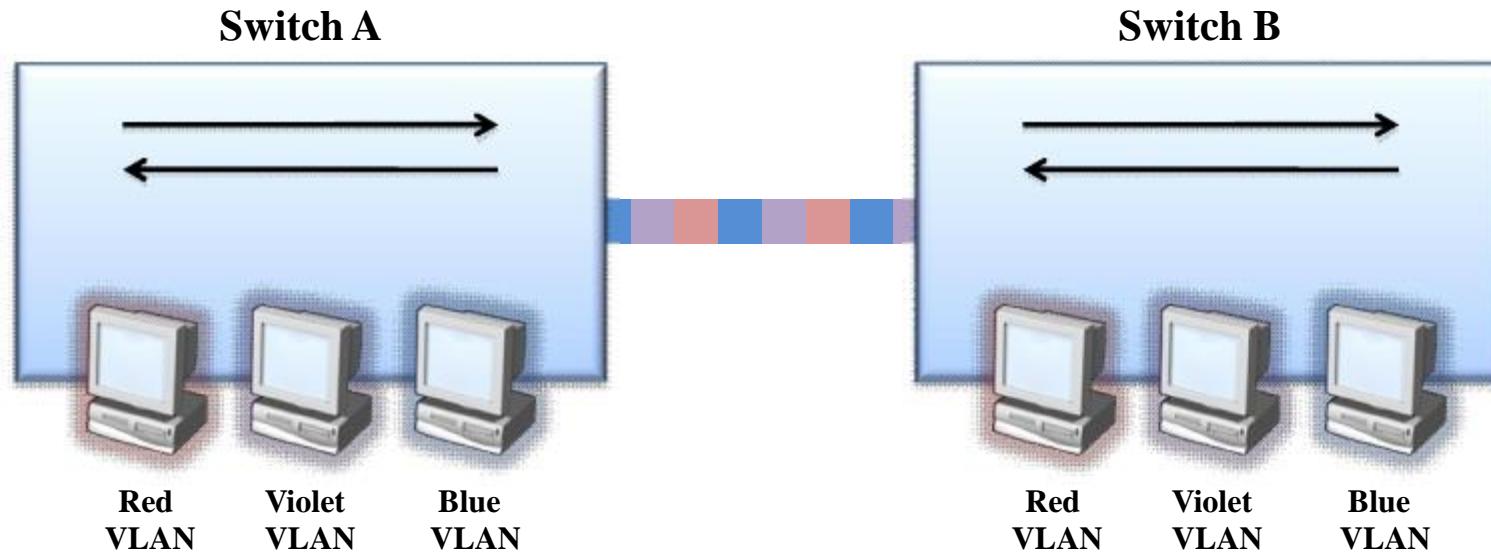
A VLAN = A Broadcast Domain = Logical Network (Subnet)



- Segmentation
- Flexibility
- Security



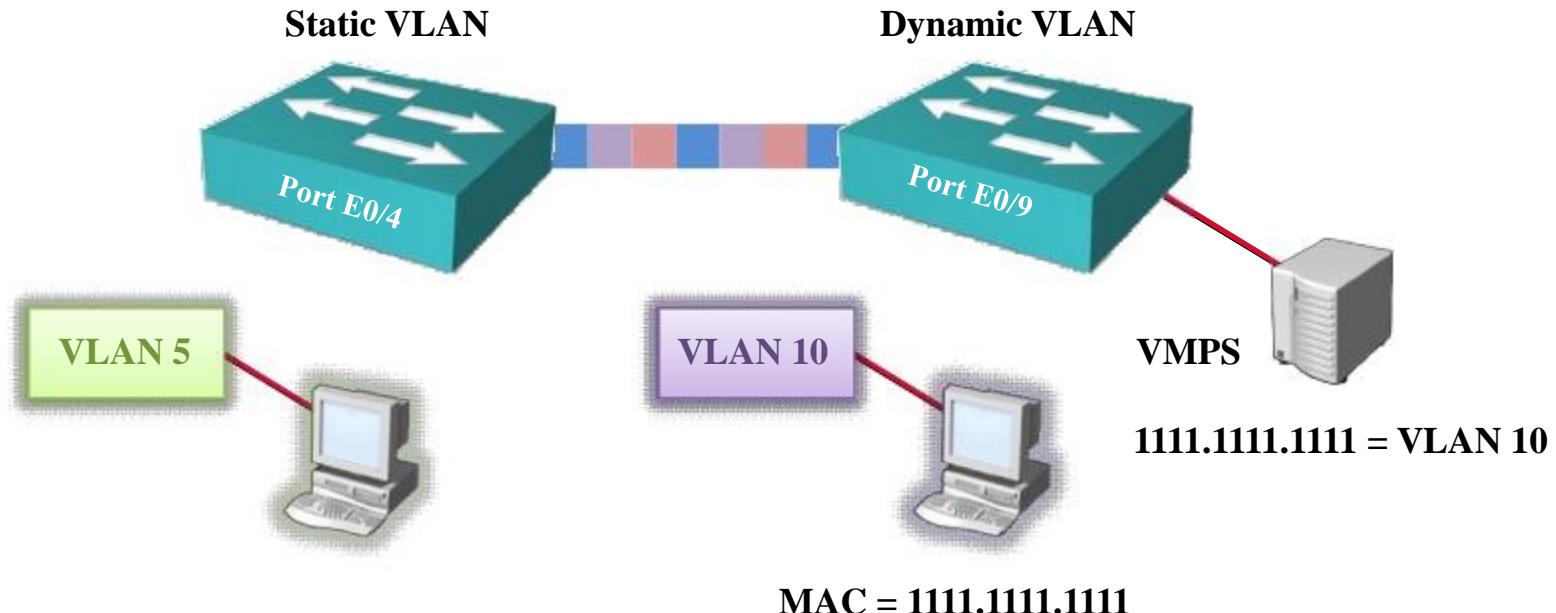
VLAN 동작



- 각각의 Logical VLAN은 별도의 Physical Bridge와 동일하다.
- VLAN을 여러대의 Switch로 확장할 수 있다.
- Trunk Link는 여러 VLAN Traffic을 전달한다.



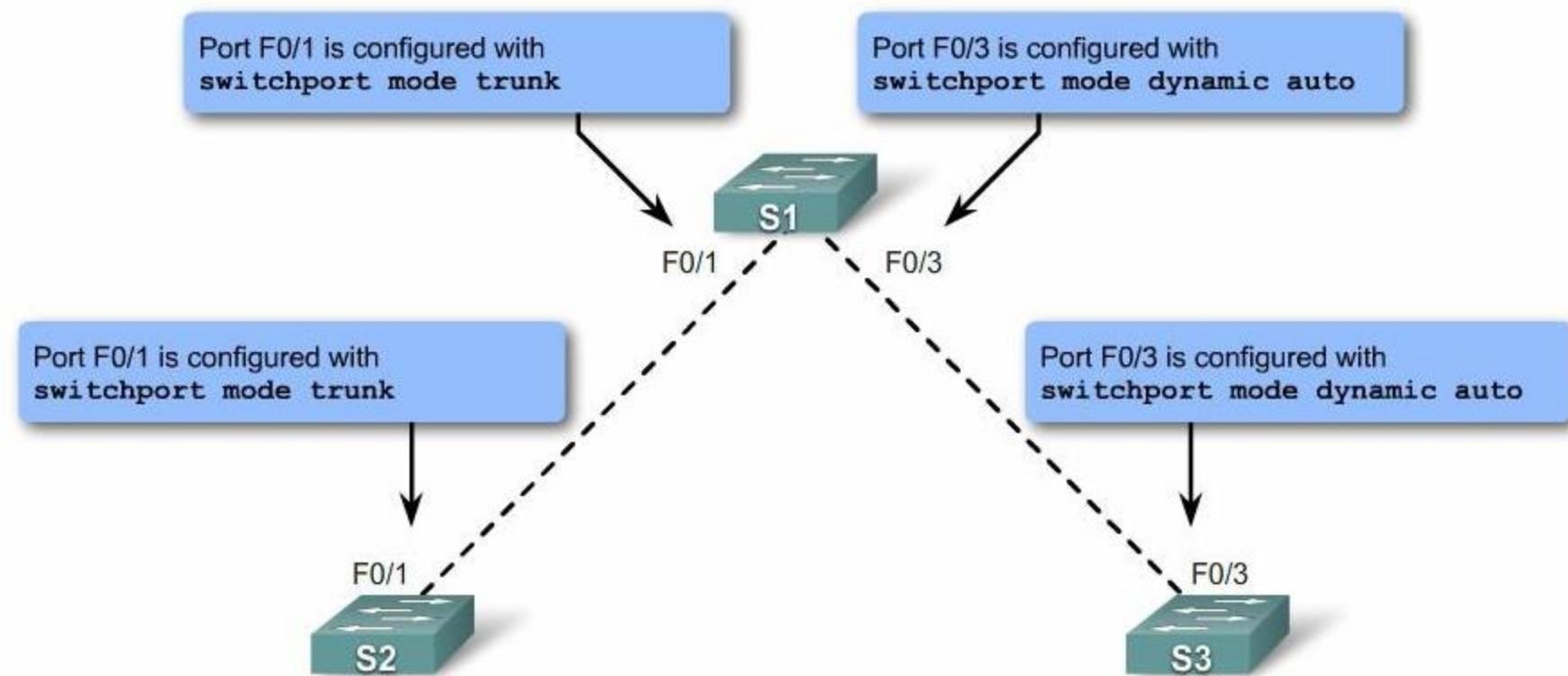
VLAN Membership Type



- Static VLAN
 - 관리자가 직접 하나의 포트에 VLAN을 할당하는 VLAN이다.
- Dynamic VLAN
 - VMPS(VLAN Membership Policy Server)를 사용하여 포트에 연결된 호스트에 MAC Address를 기반으로 Switch가 VMPS에 질의하여 해당 포트에 VLAN을 결정한다.



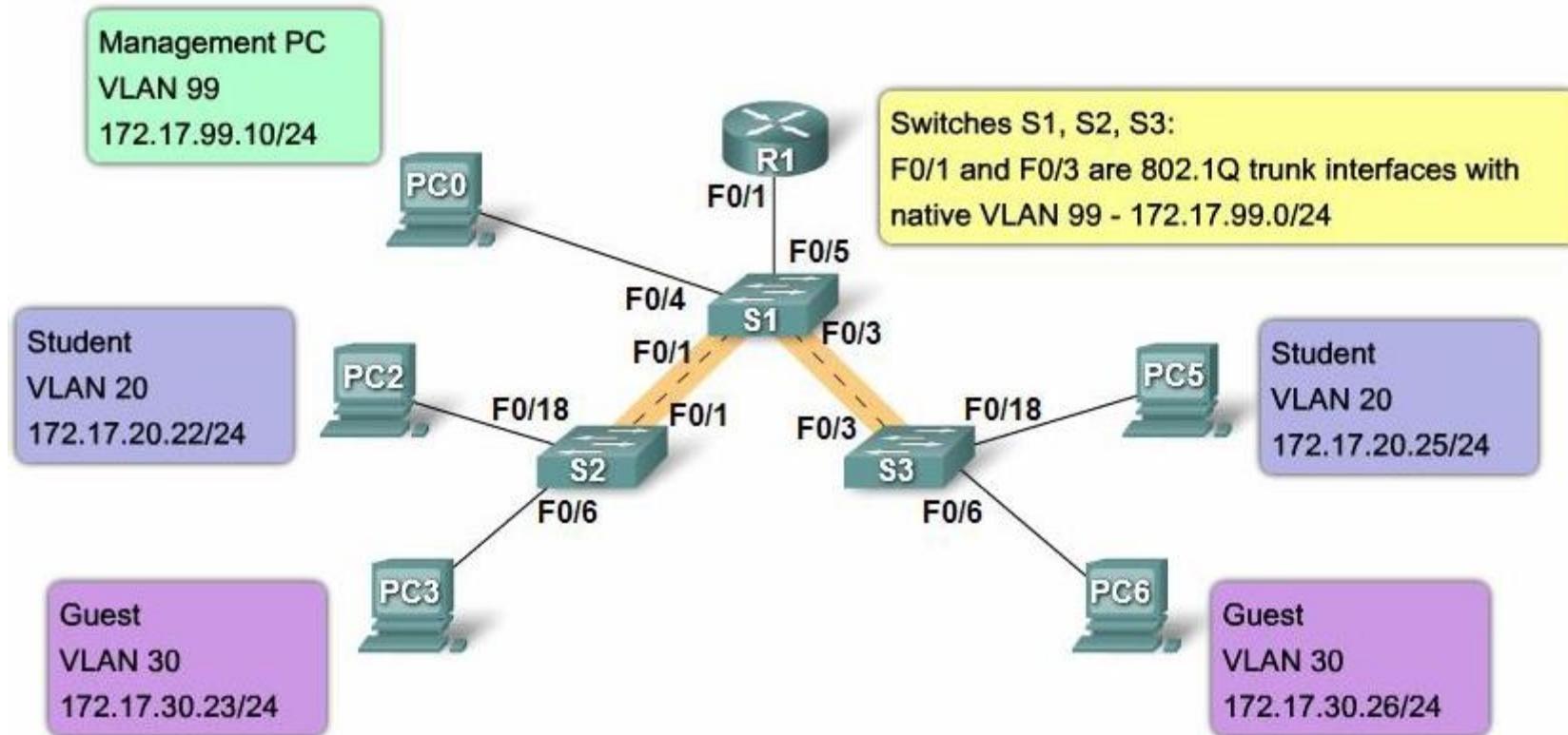
802.1Q Trunking



- 스위치 간 또는 스위치와 라우터사이에 다중 VLAN 트래픽을 처리한다.
- Cisco에서는 FastEthernet과 GigabitEthernet Interface에 대해 IEEE 802.1Q를 지원.
- Cisco Switch에서는 802.1Q를 일반적으로 dot1q라고 부른다.



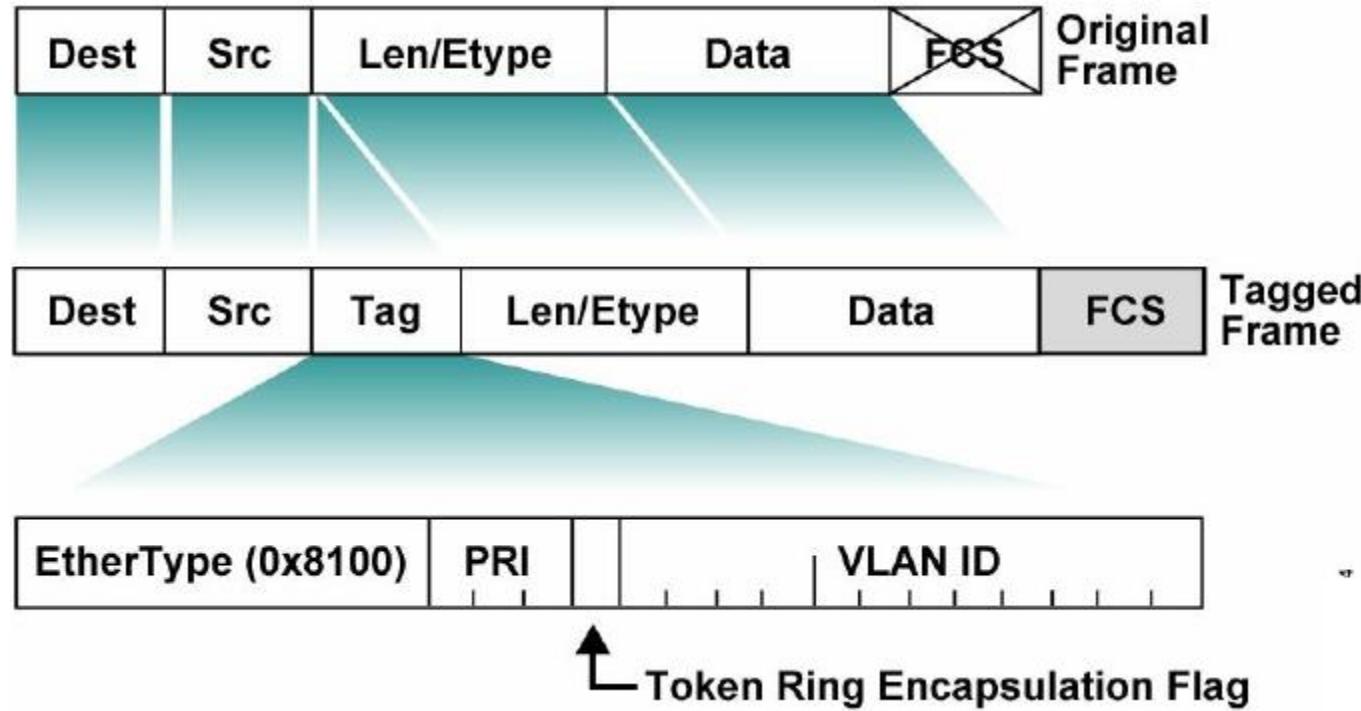
Native VLAN



- Ethernet이 공유매체이고 대화하지 않더라도 통신은 할 수 있어야 한다. 이러한 이유로 인해 802.1Q를 Native VLAN으로 정의하기도 한다. Native VLAN은 Tag되지 않은 Frame을 전달하는 VLAN을 정의한다. 트렁킹을 인식하지 못하는 장비 사용시 필요.



802.1Q Frame

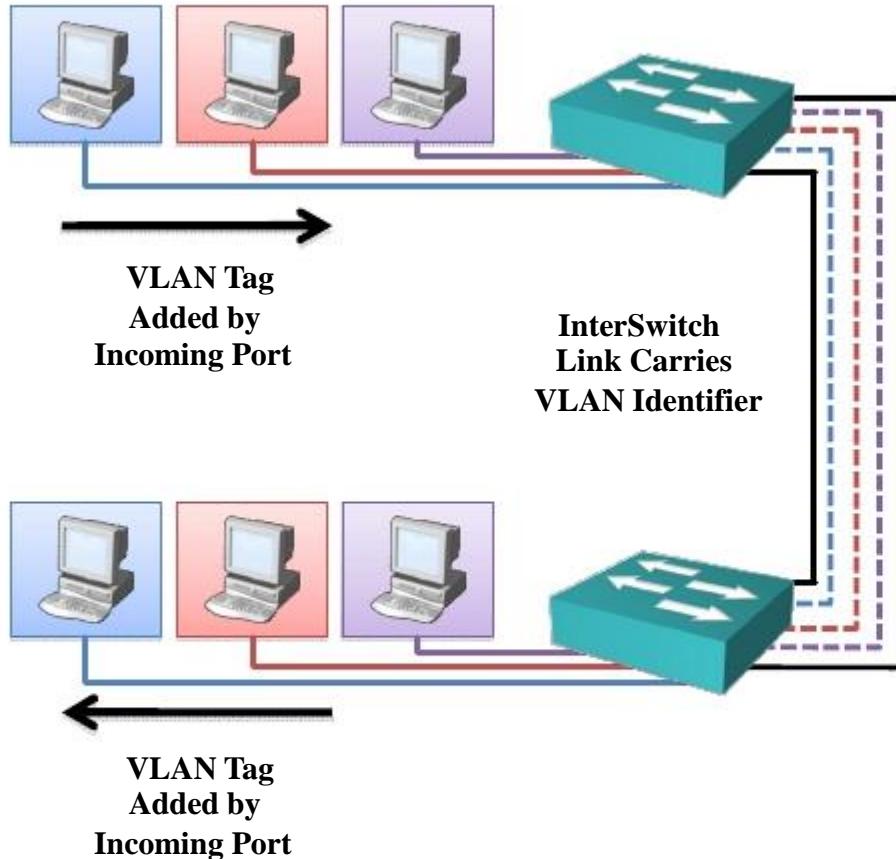


- 802.1Q Frame Tag : 4Byte = 2Byte(TPID) + 2Byte(TCI)
 - TPID(Tag Protocol ID) : 0x8100 (이 값은 802.1Q 호환 장비는 0x8100값을 보고 이 프레임에 태그가 붙어 있으며, 다음 2Byte가 802.1Q 정보용으로 사용된다고 인식한다.)
 - TCI (Tag control Information) : Priority(3bit) QoS용도, CFI(1bit) 0인 경우 Ethernet, 1인 경우 Tokenring을 의미함, CFI의 마지막 12bit는 VLAN ID이다.

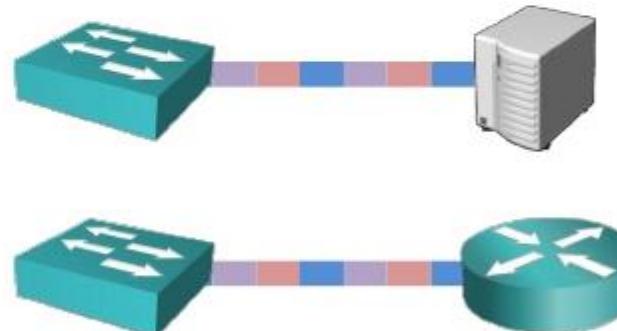


ISL Tagging

ISL trunks enable VLANs across a backbone

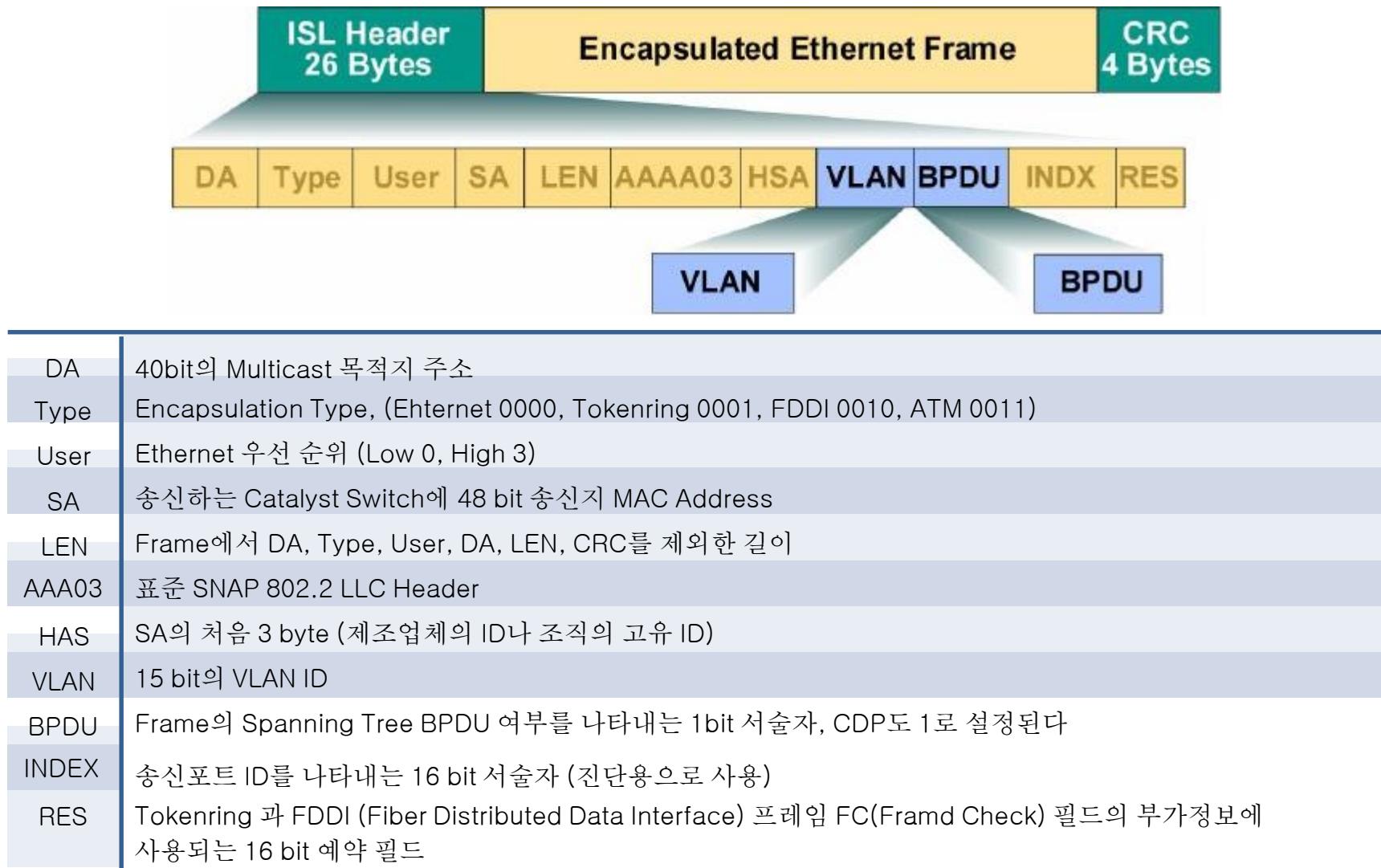


- ASIC (Application Specific Integrated Circuits)와 함께 수행
- Client는 ISL 헤더를 알지 못함.
- Switch 사이, Router와 Switch 사이, Switch와 ISL NIC가 장착된 Server 사이에서 효과적이다.





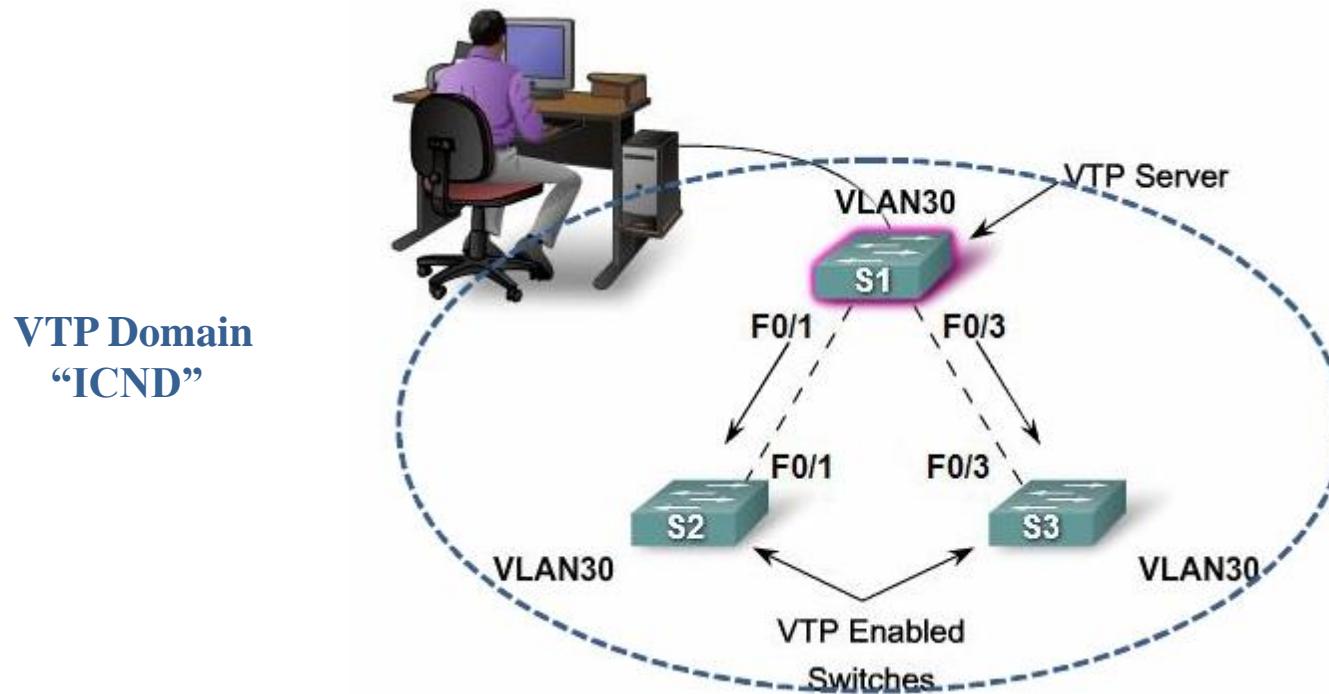
ISL Encapsulation





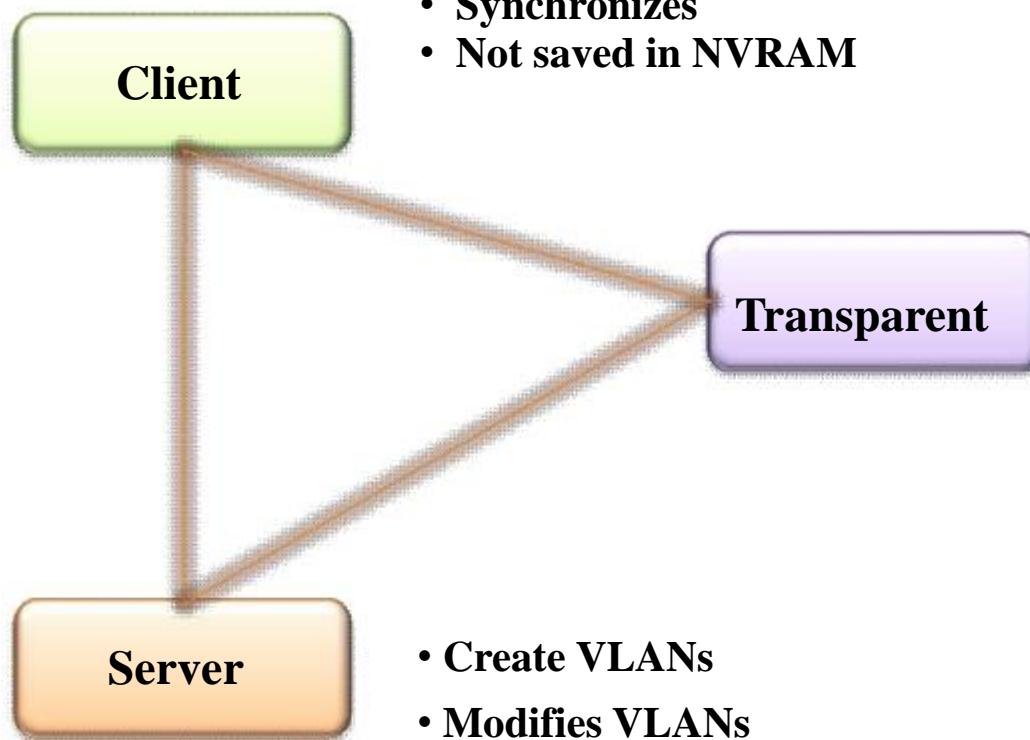
VTP Protocol 특징

- VTP는 Switch Network 전체에 설정되어 있는 VLAN에 관해 확인한 정보를 분배하고 동기화 하기 위해 사용되는 Protocol이다.
- Switch Network에서 일관된 VLAN 설정을 손쉽게 한다.
- VTP Server에 의해 생성된 VLAN 정보는 Trunk를 통해 모든 스위치로 분배된다.





VTP 모드



- Forwards advertisements
- Synchronizes
- Not saved in NVRAM

Transparent

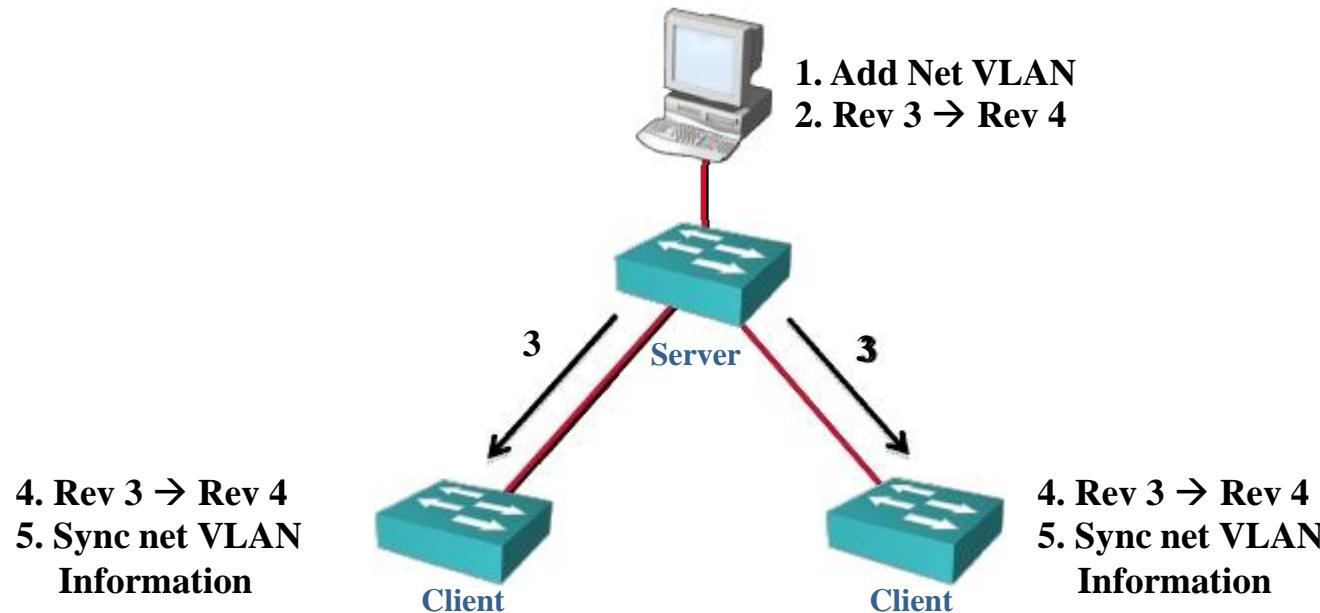
- Creates VLANs
- Modifies VLANs
- Deletes VLANs
- Forward advertisements
- Does not synchronize
- Saved in NVRAM

- Create VLANs
- Modifies VLANs
- Deletes VLANs
- Sends/forwards advertisements
- Synchronized
- Saved in NVRAM



VTP 동작

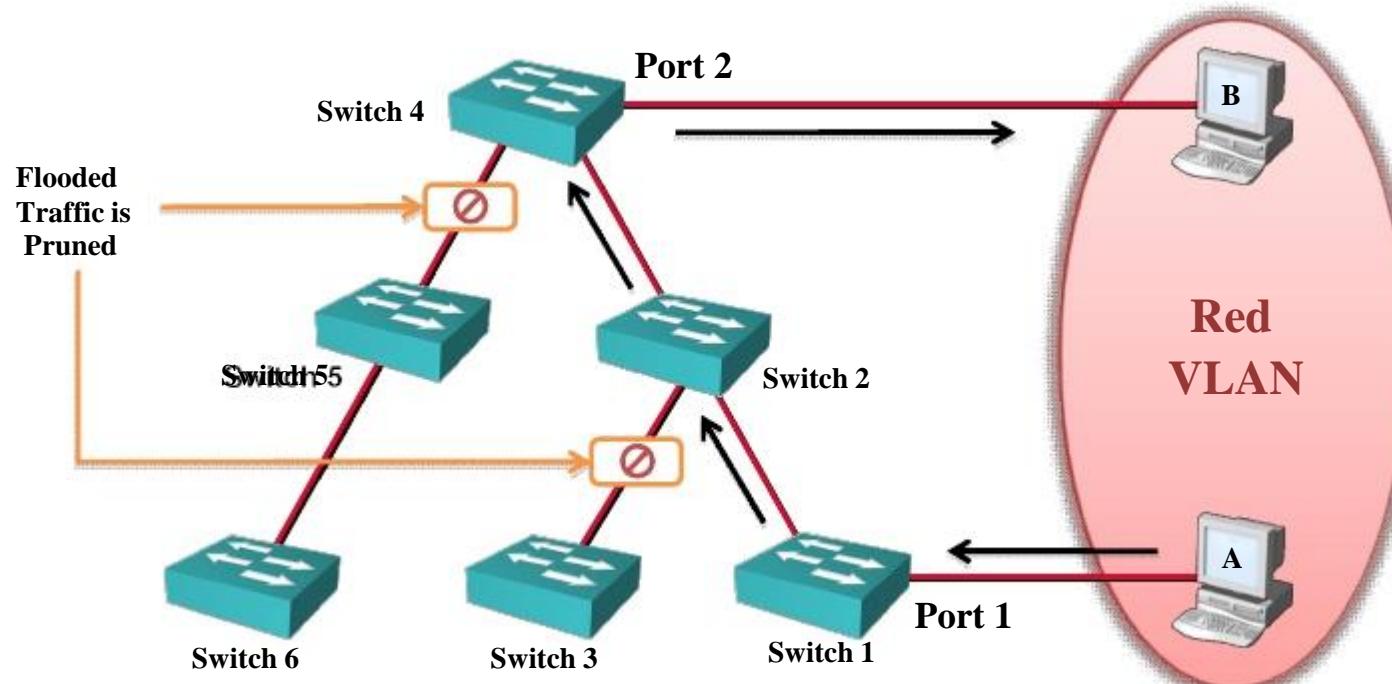
- VTP 광고는 Multicast Frame으로 전달된다.
- VTP Server와 Client는 Revision Number가 큰 값이 더 최근 정보로 간주된다.
- VTP 광고는 변경이 없어도 매 5분마다 정기적으로 전달한다.





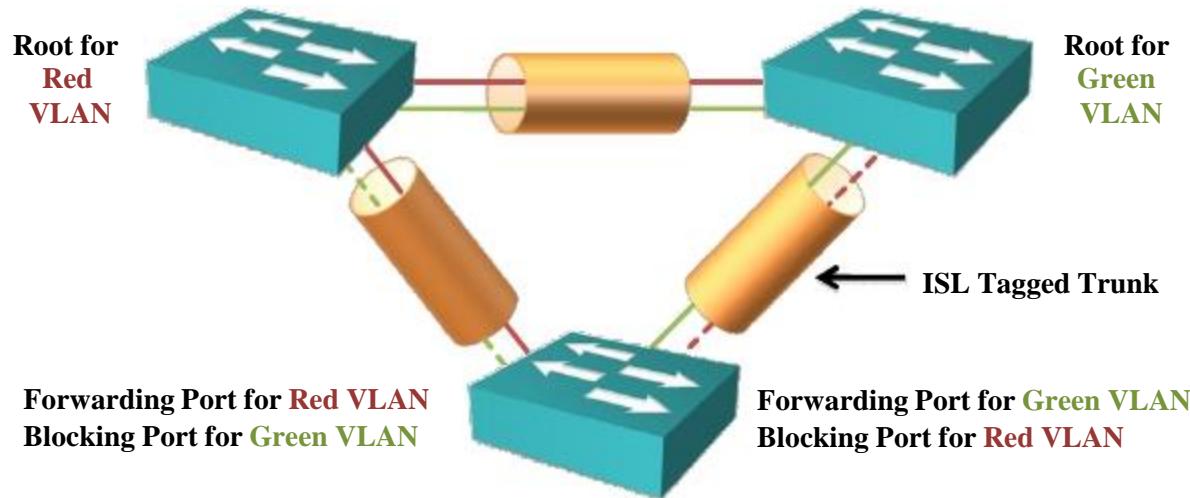
VTP Pruning

- 일부 traffic을 운반할 필요가 없는 Link들을 가로질러 필요 없이 Flooding되는 traffic을 차단하는 기능이다.
- Host A와 Host B는 같은 VLAN에 있기 때문에 호스트 A에서 전달한 traffic이 Switch 1, Switch 2, Switch 4를 통해서 전달되어야 한다. 그러나 Switch 3, Switch 5, Switch 6은 Red VLAN이 없기 때문에 Traffic이 전달되지 않는다.





PVST(PerVLAN Spanning Tree)



- VLAN에서 고려해야 할 한가지 사항은 STP (Spanning Tree Protocol)이다.
- 802.1Q 표준에서는 네트워크의 모든 VLAN이 한 개의 Spanningtree를 운영한다.
- 802.1Q에서 한 개의 Spanningtree는 Native VLAN에서 동작하여 비 호환 스위치와도 통신할 수 있다. (이 단일 Interface를 CST(Common Spanning Tree)라고 한다)
- PVST는 시스코에 의해 만들어지며 VLAN마다 Spanningtree를 운영한다.
- PVST는 ISL이나 802.1Q를 사용하여 링크관리 및 STP에 의한 병렬 링크들 간 트래픽 로드 밸런싱을 구현할 수 있다.



VLAN 설정 구성도

Vlan1 : 1.1.1.1/24

Vlan10 : 10.1.1.1/24 Fa1/2, Fa1/12

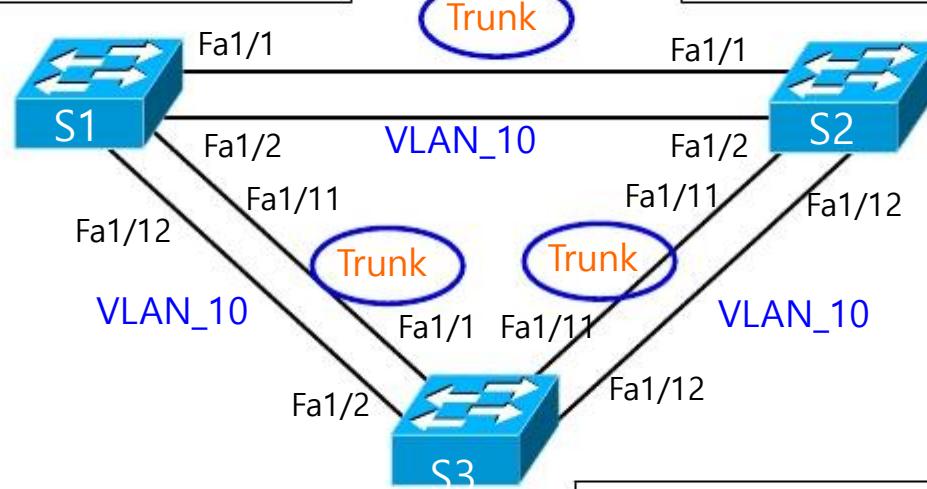
Vlan20 : 20.1.1.1/24 Fa1/5 - 7

Vlan1 : 1.1.1.2/24

Vlan10 : 10.1.1.2/24 Fa1/2, Fa1/12

Vlan20 : 20.1.1.2/24 Fa1/5 - 7

Priority : 0



Vlan1 : 1.1.1.3/24

Vlan10 : 10.1.1.3/24 Fa1/2, Fa1/12

Vlan20 : 20.1.1.3/24 Fa1/5 - 7



VLAN 설정 순서

- VLAN을 설정하려면 전체 설정모드에서
 - 1) VLAN 번호를 설정하고 (생성하고)
 - 2) 인터페이스 설정모드에서 포트가 속하는 VLAN 번호를 지정하고
 - 3) VLAN 인터페이스에 IP를 부여하면 된다. (VLAN 인터페이스에 IP 주소를 부여하는 것은 관리 목적이다.)



VLAN 추가하기

- Catalyst 2950

```
ASW2950(config)# vlan vlan_ID  
ASW2950(config-vlan)# name <word>
```

```
ASW2950#vlan database  
% warning: It is recommended to configure VLAN from config  
mode, as VLAN database mode is being deprecated. Please consult  
user documentation for configuring VTP/VLAN in config mode.
```

```
ASW2950(vlan)#vlan 10 name sales
```



VLAN 추가하기

```
S1#conf t                                     => Cisco Switch 설정방식
S1(config)#vlan 10
S1(config-vlan)#name aaa_10                  => VLAN 이름 부여

S1(config-vlan)#vlan 20
S1(config-vlan)#name bbb_20                  => VLAN 이름 부여
S1(config-vlan)#end
```

```
S1#vlan database                               => Cisco Router 설정방식
S1(vlan)#vlan 10 name aaa_10
VLAN 10 modified:
  Name: aaa_10
S1(vlan)#vlan 20 name bbb_20
VLAN 20 modified:
  Name: aaa_20
S1(vlan)#exit
```



VLAN에 스위치 포트 할당하기

- Catalyst 2950

```
ASW2950(config)# interface fa1/2  
ASW2950(config-if)#switchport access vlan <vlan_id>
```

- **fa0/1**번 포트부터 **10**번 포트까지 , **fa0/15**부터 **19**번 포트까지 설정을 한번에 구성하기

```
ASW2950(config)# interface range fa1/1-10, fa1/15-19  
ASW2950(config-if-range)#switchport access vlan <vlan_id>
```



VLAN에 스위치 포트 할당하기 - 예제

```
S1(config)#interface range fastEthernet 1/2 , 12
```

```
S1(config-if-range)#switchport mode access
```

```
S1(config-if-range)#switchport access vlan 10
```

```
S1(config)#interface range fastEthernet 1/5 - 7
```

```
S1(config-if-range)#switchport mode access
```

```
S1(config-if-range)#switchport access vlan 20
```



VLAN 구성 확인

S1#show vlan brief

=> Cisco 스위치에 적용 명령어

S1#[show vlan-switch brief](#)

=> Cisco 라우터에 적용 명령어

VLAN	Name	Status	Ports
1	default	active	Fa1/11, Fa1/12, Fa1/13, Fa1/14 Fa1/15
10	aaa_10	active	Fa1/2, Fa1/12
20	bbb_20	active	Fa1/5, Fa1/6, Fa1/7
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet	active	



VLAN 설정 – VLAN IP 설정하기

```
S1(config)#interface vlan 10  
S1(config-if)#ip address 10.1.1.1 255.255.255.0
```

```
S1(config)#interface vlan 20  
S1(config-if)#ip address 20.1.1.1 255.255.255.0
```



VLAN 설정 – VLAN IP 확인 하기

```
S1#sh ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	1.1.1.1	YES	NVRAM	up	up
Vlan10	10.1.1.1	YES	manual	up	up
Vlan20	20.1.1.1	YES	manual	up	down

```
S1#sh inter vlan 10
```

Vlan10 is up, line protocol is up

Hardware is EtherSVI, address is c400.0f50.0000 (bia c400.0f50.0000)

Internet address is 10.1.1.1/24

MTU 1500 bytes, BW 100000 Kbit, DLY 1000000 usec,
reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:01:58, output never, output hang never

Last clearing of "show interface" counters never

(생략)



VLAN에 할당된 포트 확인하기

```
ASW2950#show vlan brief
```

```
ASW2950#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21
5	VLAN5	active	Fa0/3
9	VLAN9	active	Fa0/22, Fa0/23
1002	fdci-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

```
ASW2950#show interfaces interface switchport
```



VLAN에서 동작하는 STP 확인하기

```
ASW2950#show spanning-tree vlan [vlan#]
```

```
ASW11#show spanning-tree vlan 1
```

VLAN0001

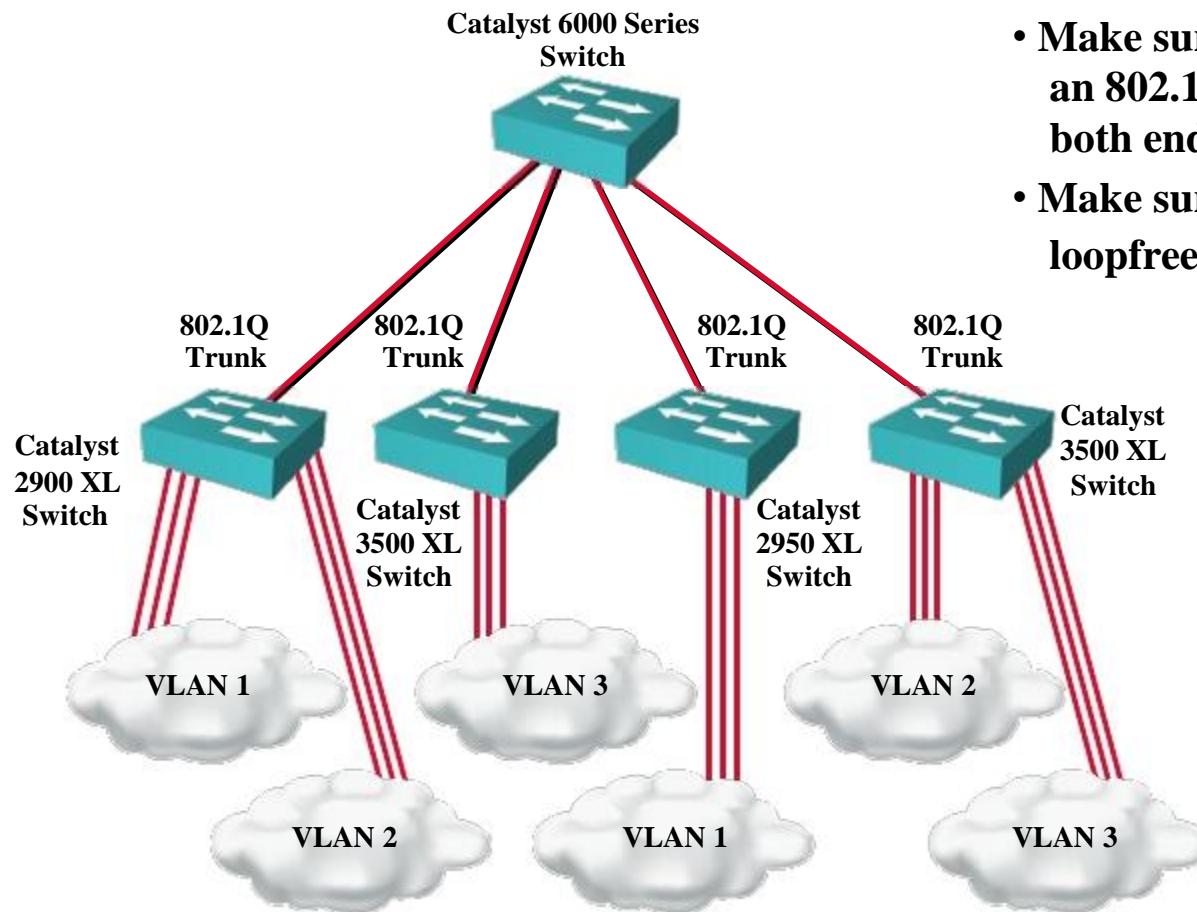
Spanning tree enabled protocol ieee
Root ID Priority 32769
Address 0007.5044.4980
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address 0007.5044.4980
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Aging Time 300

Interface	Role	Sts	Cost	Prio.Nbr	Type
Fa0/23	Desg	FWD	19	128.23	P2p



802.1Q Trunking Limitations



- Make sure the native VLAN for an 802.1Q trunk is the same on both ends of the trunk link
- Make sure your network is loopfree before disabling STP



Configuring 802.1Q Trunking

- Configures the port as a VLAN trunk

```
ASW3550(config-if)#switchport trunk encapsulation dot1q  
ASW3550(config-if)#switchport mode trunk
```

- Catalyst 3550 등은 trunk encapsulation type을 지정해야 수동 설정이 가능하다
- ASW(configif)#switchport trunk encapsulation {dot1q | isl}을 이용하여 설정하면 된다.



Trunk 설정 구성도

Vlan1 : 1.1.1.1/24

Vlan10 : 10.1.1.1/24 Fa1/2, Fa1/12

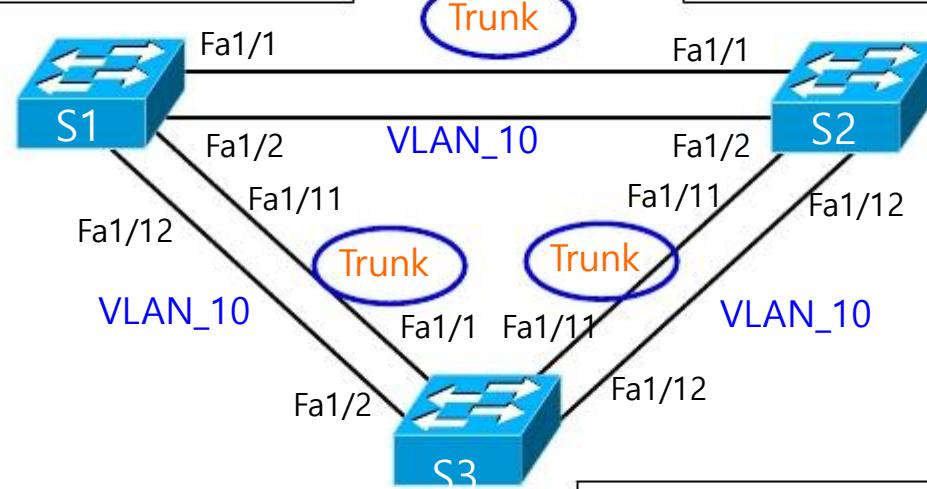
Vlan20 : 20.1.1.1/24 Fa1/5 - 7

Vlan1 : 1.1.1.2/24

Vlan10 : 10.1.1.2/24 Fa1/2, Fa1/12

Vlan20 : 20.1.1.2/24 Fa1/5 - 7

Priority : 0



Vlan1 : 1.1.1.3/24
Vlan10 : 10.1.1.3/24 Fa1/2, Fa1/12
Vlan20 : 20.1.1.3/24 Fa1/5 - 7



Trunk 설정

```
S1(config)#interface range fastEthernet 1/1, 11  
S1(config-if-range)#switchport trunk encapsulation dot1q  
S1(config-if-range)#switchport mode trunk
```

```
S2(config)#interface range fastEthernet 1/1, 11  
S2(config-if-range)#switchport trunk encapsulation dot1q  
S2(config-if-range)#switchport mode trunk
```

```
S3(config)#interface range fastEthernet 1/1, 11  
S3(config-if-range)#switchport trunk encapsulation dot1q  
S3(config-if-range)#switchport mode trunk
```



트렁크 포트 상태 확인하기

S1#**show interface trunk**

Port ①	Mode ②	Encapsulation ③	State ④	Native vlan ⑤
Fa1/1	on	802.1q	trunking	1
Fa1/11	on	802.1q	trunking	1
Fa1/24	desirable	n-802.1q	trunking	1

① **Port** : 트렁크로 동작하는 포트번호를 나타낸다.

② **Mode** : 포트의 옵션 상태를 나타낸다.

③ **Encapsulation** : 사용중인 트렁킹 프로토콜을 나타낸다.

ex) n-802.1q : 양측포트에서 DTP를 사용하여 협상한 결과 802.1q로 설정되었음을 나타낸다. 802.1q는 앞에 'n-'표시가 없으므로 관리자가 직접 지정했음을 알려준다.

④ **상태 (State)** : 현재 트렁크로 사용 중 (trunking)임을 나타낸다.

⑤ **네이티브 VLAN** : 해당 트렁크 포트에 설정된 네이티브 VLAN 번호를 나타낸다.



Verifying a Trunk

```
ASW2950#show interface interface switchport
```

```
wg_sw_2950#show interface fa1/1 switchport
Name: Fa0/2
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
...
```



VTP 구성시 주의사항

- VTP domain name – Default None
- VTP mode (server/client/transparent) – VTP server mode is the default
- VTP pruning – Default Disabled
- VTP password – None
- VTP trap – Default Disabled

➤ 주의 : 기존 도메인에 새로운 스위치를 추가할 때 스위치에 대한 설정 개정 번호가 0 인지를 확인하여 새로운 스위치가 부정확한 VLAN 정보를 전파하지 못하도록 한다.

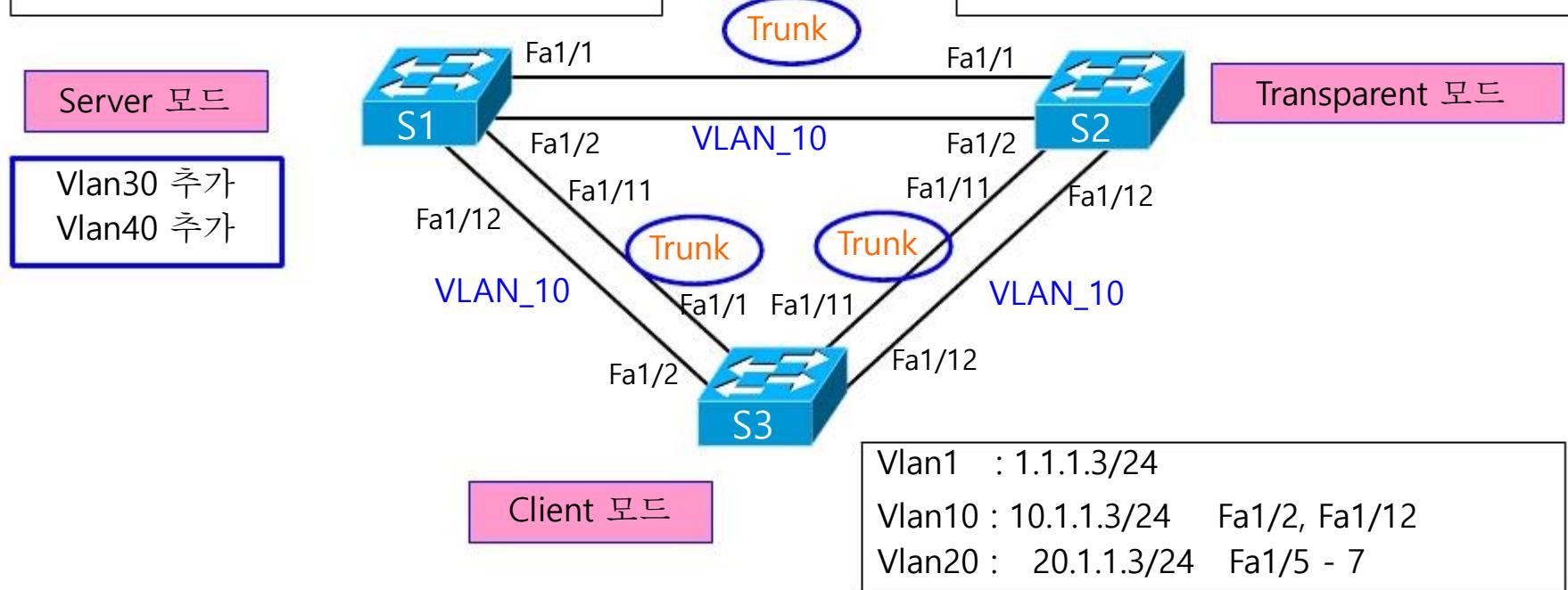
(새로운 스위치에 VTP 설정 개정 번호를 Reset하여 VTP에 추가한다)



VTP 설정 구성도

Vlan1 : 1.1.1.1/24
Vlan10 : 10.1.1.1/24 Fa1/2, Fa1/12
Vlan20 : 20.1.1.1/24 Fa1/5 - 7

Vlan1 : 1.1.1.2/24
Vlan10 : 10.1.1.2/24 Fa1/2, Fa1/12
Vlan20 : 20.1.1.2/24 Fa1/5 - 7





VTP 도메인 생성하기

```
ASW2950(config)#vtp domain domain-name
ASW2950(config)#vtp password password
ASW2950(config)#vtp pruning
ASW2950(config)#vtp snmp-server enable traps vtp
ASW2950(config)#vtp mode [ server | client | transparent ]
```



VTP modes – Server Mode

- Server Mode :
 - VLAN을 만들거나, 지우거나 또는 VLAN의 이름을 변경할 수 있으며, VTP 정보를 다른 스위치에게 전송한다. 그리고 설정은 NVRAM에 저장된다.
 - 다른 스위치에게서 받은 정보와 자신의 정보를 일치시키며, 이를 다른 스위치에게 중계한다.
 - 스위치의 디폴트 VTP 모드가 서버이다.
 - VTP Domain 별로 최소 하나의 VTP Server가 존재하여야 한다.

```
S1#conf t  
S1(config)#vtp mode server
```

=> Cisco 스위치 적용명령어

```
S1#vlan database  
S1(vlan)#vtp server
```

=> Cisco Router 적용명령어



VTP modes – Client Mode

- **Client Mode**

- VLAN을 만들고, 변경하고, 제거할 수 없다.

그러나, 자신의 VTP 정보를 다른 스위치에게 전송하며, 다른 스위치에게서 받은 정보와 자신의 정보를 일치시키고, 이를 다른 스위치에게 중계한다.

- VLAN Database를 NVRAM에 저장하지 않는다. => Server에서 받으므로...
- 서버에서 VLAN을 만들어야 클라이언트 스위치의 포트에 VLAN을 할당할 수 있다.

```
S3#conf t  
S3(config)#vtp mode client
```

=> Cisco 스위치 적용명령어

```
S3#vlan database  
S3(vlan)#vtp client
```

=> Cisco Router 적용명령어



VTP modes – Transparent Mode

- **Transparent Mode :**
 - 자신의 VTP 정보를 다른 스위치에게 전송하지 않으며, 다른 스위치에게서 받은 정보와 일치 시키지 않는다.
 - 그러나, 다른 스위치에게서 받은 VTP 정보를 중계하며, 자신이 사용할 VLAN을 만들거나 삭제할 수 있다.
 - VTP Transparent Switch는 자신의 Local Database에 VLAN을 만들고, 변경하고, 제거할 수 있다. **설정한 VLAN은 자신에게만 영향을 미친다.** 데이터베이스를 다른 스위치와 공유할 수 없다.(= Does not synchronize)

```
S2#conf t  
S2(config)#vtp mode transparent => Cisco 스위치 적용명령어
```

```
S2#vlan database  
S2(vlan)#vtp transparent => Cisco Router 적용명령어
```



VTP 정보 확인하기

```
S1 # show vtp status
```

- ① VTP version : 2
- ② Configuration revision : 8
- ③ Maximum VLANs supported locally : 1005
- ④ Number of existing VLANs : 7
- ⑤ VTP Operating Mode : Sever
- ⑥ VTP domain name : aaa
- ⑦ VTP pruning mode : Disabled
- ⑧ VTP V2 Mode : Disabled
- ⑨ VTP traps generation : Disabled
- ⑩ MD5 digest : 0x3D 0x02 0xD4 0x3A 0xC4 0x46 0xA1 0x03
- ⑪ Configuration last modified by: 1.1.1.10 at 02-21-2008 17:05:05
- ⑫ Local updater ID is 1.1.1.1 on interface VLAN 1 (first interface found)



VTP 정보 확인하기

- ① VTP 버전을 표시한다.
- ② VTP 설정번호 (configuration Revision)을 표시한다.
- ③ 이 스위치에 설정할 수 있는 최대 VLAN 수를 의미한다.
- ④ 현재 설정되어 있는 VLAN 수를 의미하다.
- ⑤ VTP 모드를 표시한다.
- ⑥ VTP 도메인 이름을 표시한다.
- ⑦ VTP 프루닝 모드를 나타낸다.
- ⑧ VTP 버전 2 모드의 사용여부를 표시한다.
- ⑨ SNMP용 VTP 트랩 전송여부를 나타낸다.
- ⑩ VTP 패스워드를 암호화시켜 나타낸다.
- ⑪ 가장 최근에 VTP 정보를 전송한 스위치의 IP 주소와 전송한 시간 및 날짜를 표시.
- ⑫ 스위치가 VTP 정보를 전송할 때 사용하는 IP 주소와 인터페이스를 표시한다.



VLAN 추가하기

```
S1#conf t  
S1(config)#vlan 30  
S1(config-vlan)#name aaa_30
```

=> Cisco Switch 설정방식
=> VLAN 이름 부여

```
S1(config-vlan)#vlan 40  
S1(config-vlan)#name bbb_40  
S1(config-vlan)#end
```

=> VLAN 이름 부여

```
S1#vlan database  
S1(vlan)#vlan 30 name aaa_30  
VLAN 30 modified:  
    Name: aaa_30  
S1(vlan)#vlan 40 name bbb_40  
VLAN 40 modified:  
    Name: aaa_40  
S1(vlan)#exit
```

=> Cisco Router 설정방식



VLAN 설정 확인

S1#show vlan brief

=> Cisco 스위치에 적용 명령어

S1#[show vlan-switch brief](#)

=> Cisco 라우터에 적용 명령어

VLAN	Name	Status	Ports
1	default	active	Fa1/11, Fa1/12, Fa1/13, Fa1/14 Fa1/15
10	aaa_10	active	Fa1/2, Fa1/12
20	bbb_20	active	Fa1/5, Fa1/6, Fa1/7
30	aaa_30	active	
40	bbb_40	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet	active	



VLAN 설정 확인

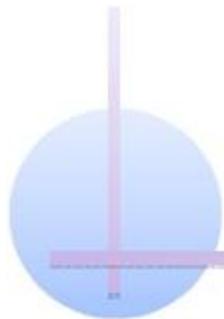
S2#show vlan brief

=> Cisco 스위치에 적용 명령어

S2#[show vlan-switch brief](#)

=> Cisco 라우터에 적용 명령어

VLAN	Name	Status	Ports
1	default	active	Fa1/11, Fa1/12, Fa1/13, Fa1/14 Fa1/15
10	aaa_10	active	Fa1/2, Fa1/12
20	bbb_20	active	Fa1/5, Fa1/6, Fa1/7
30	aaa_30	active	
40	bbb_40	active	
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet	active	

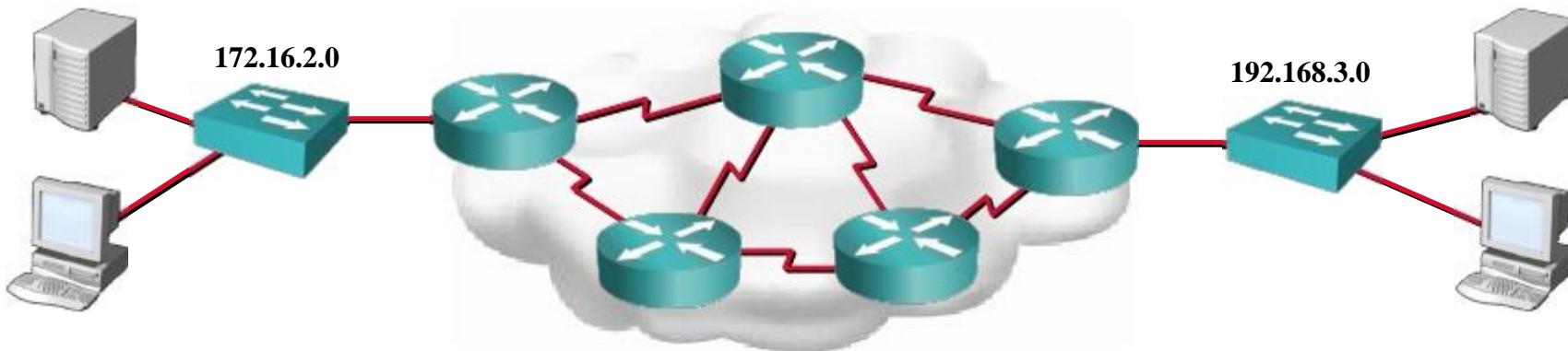


Chapter 05 Routing

Routing의 개념 소개

- **Routing** 개요
- **Static & Dynamic Routing**
- **Static Route** 설정하기
- **Default Route** 설정하기
- **Dynamic Routing** 개요

Routing 개요



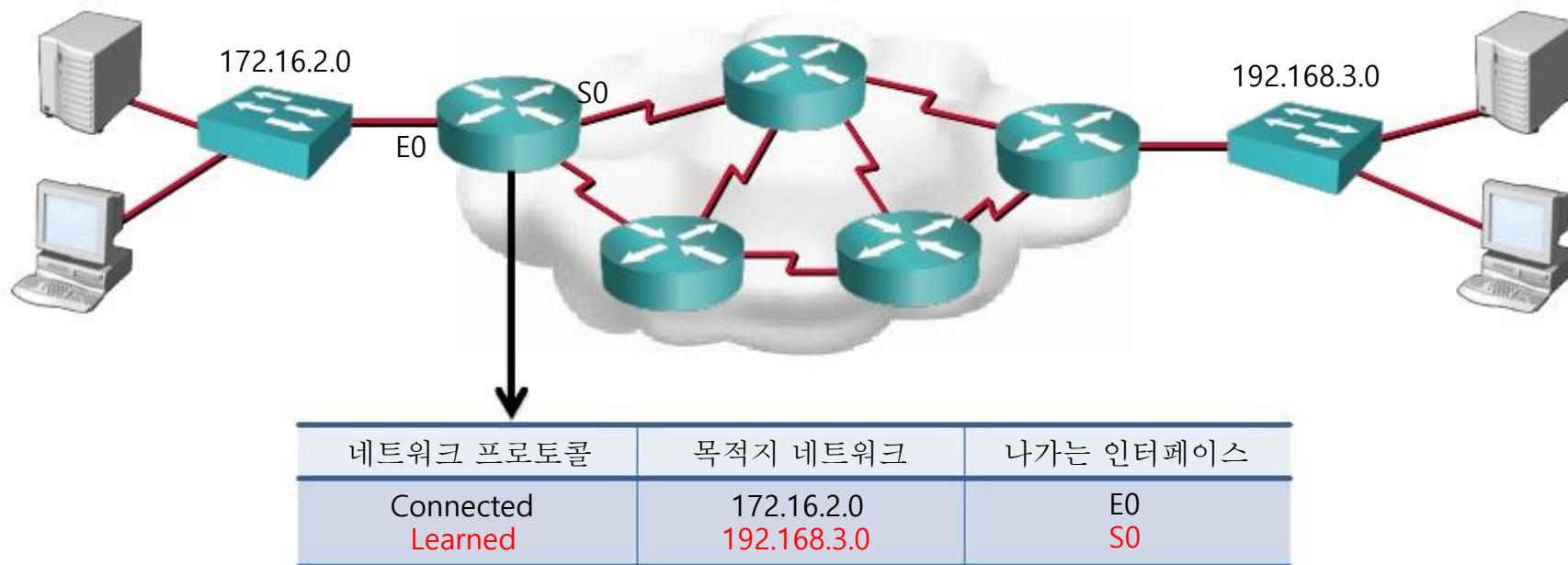
데이터를 최적의 경로를 선택하여 목적지까지 이송하는 모든 절차

IP Protocol이 올라가 있는 Router, Computer or Host, L3 Ethernet Switch 들이 이러한 작업이 가능

▶ 라우터가 데이터를 Routing하기 위하여 알아야 하는 것

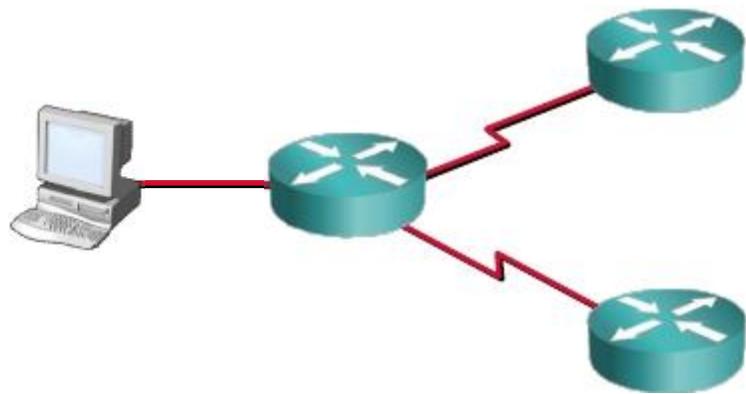
- 소스와 목적지 주소
- 입/출력 인터페이스 형태
- 가능성 있는 모든 경로(route)들에 대한 정보 수집
- 가능성 있는 모든 경로 중에서 최적의 경로 선택
- 지속적인 네트워크 상태를 확인하고 유지하는 것

Routing 개요



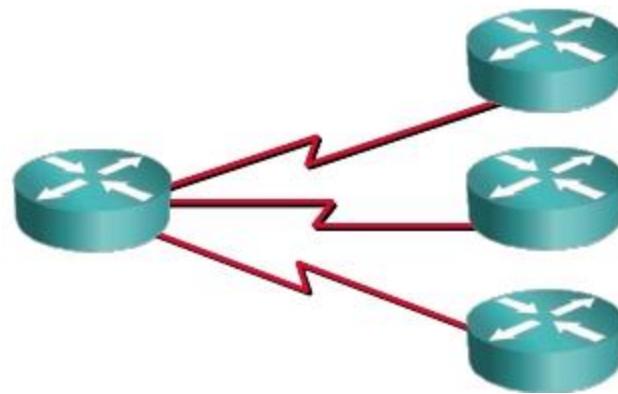
라우터는 인터페이스로 들어온 패킷의 목적지 주소를 확인한 후에 라우팅 테이블에서 해당 네트워크에 대한 정보가 있는지를 찾아서 일치하는 정보가 있다면 해당 인터페이스로 패킷을 내보낸다(라우팅한다.) 직접 연결된 네트워크 이외의 다른 목적지에 대해서는 반드시 Static, Dynamic Routing Protocol, Redistribution과 같은 다양한 방법으로 학습할 수 있다.

Static & Dynamic Routing



Static Routing

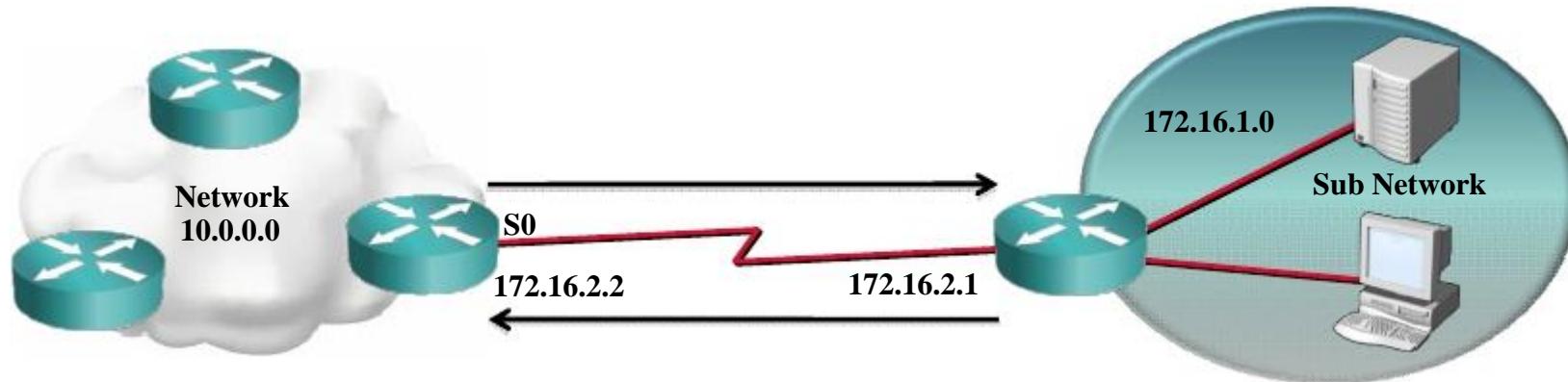
관리자가 직접 수동으로 Router에게 필요한 Route 정보들을 입력한다
Network의 변화에 대해 Router가 자동으로 반응하지 못하며 관리자가 직접 Network의 변화를 Router에 설정해야 한다.



Dynamic Routing

Routing Protocol을 이용하여 자동으로 Route 정보를 수집한다.
Network 변화에 대해 자동으로 반응한다.

Static Route 설정하기



```
Router(config)#ip route network mask {address|interface} [distance] [permanent]
```

Network

도착지 Network

Mask

도착지 Network의 Subnet mask

Address

도착지 network로 도달하기 위한 Nexthop address

Interface

도착지 network로 도달하기 위한 Nexthop Router와 연결된 local interface

Distance

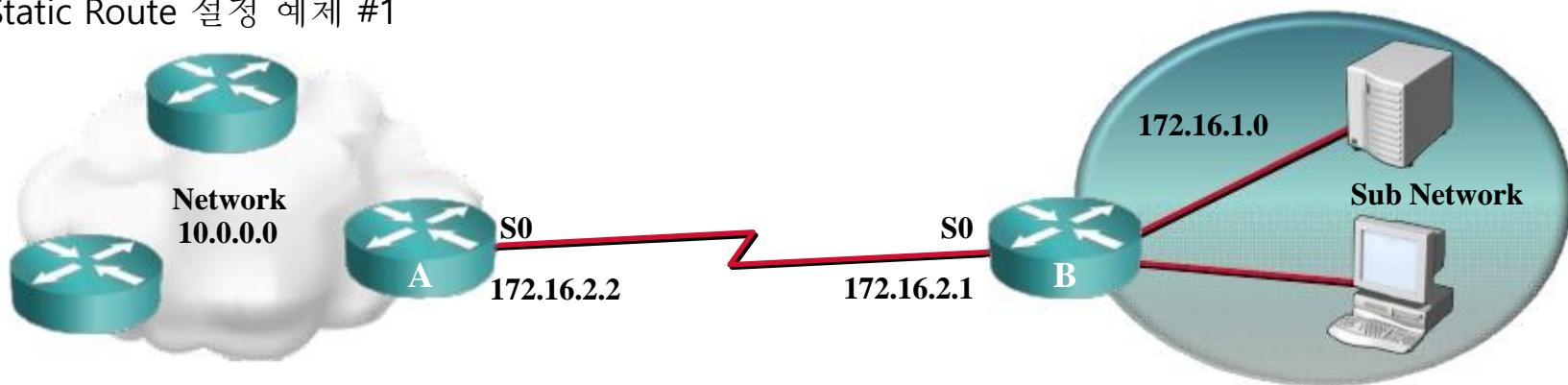
정의된 Route의 Administrator Distance 값

Permanent

정의된 Static Route가 Routing table에서 제거되지 않도록 한다.

Static Route 설정하기

- Static Route 설정 예제 #1



- RouterA

```
Router(config)#ip route 172.168.1.0 255.255.255.0 172.16.2.1
```

- RouterB

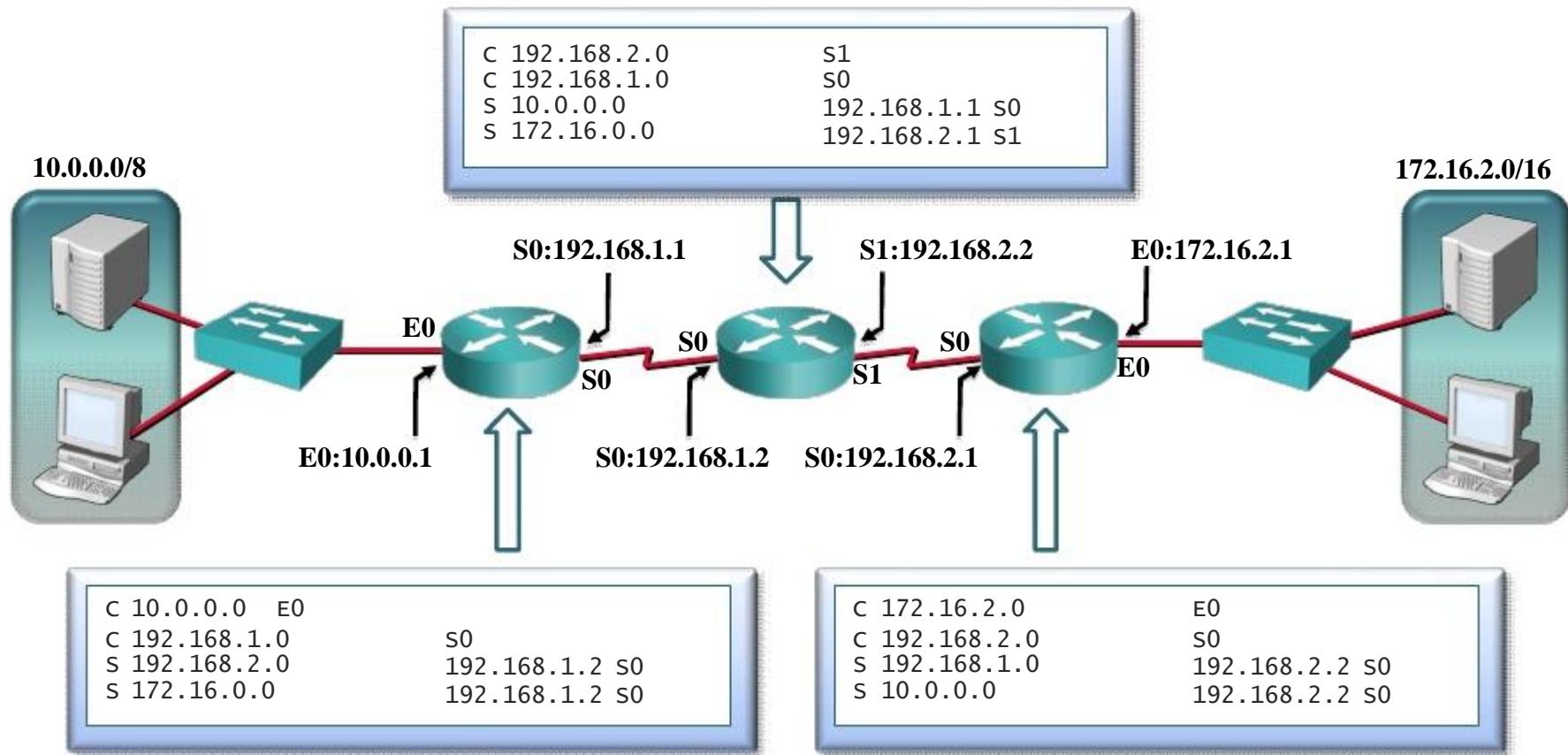
```
Router(config)#ip route 10.0.0.0 255.0.0.0 172.168.2.2
```

or

```
Router(config)#ip route 10.0.0.0 255.0.0.0 serial 0
```

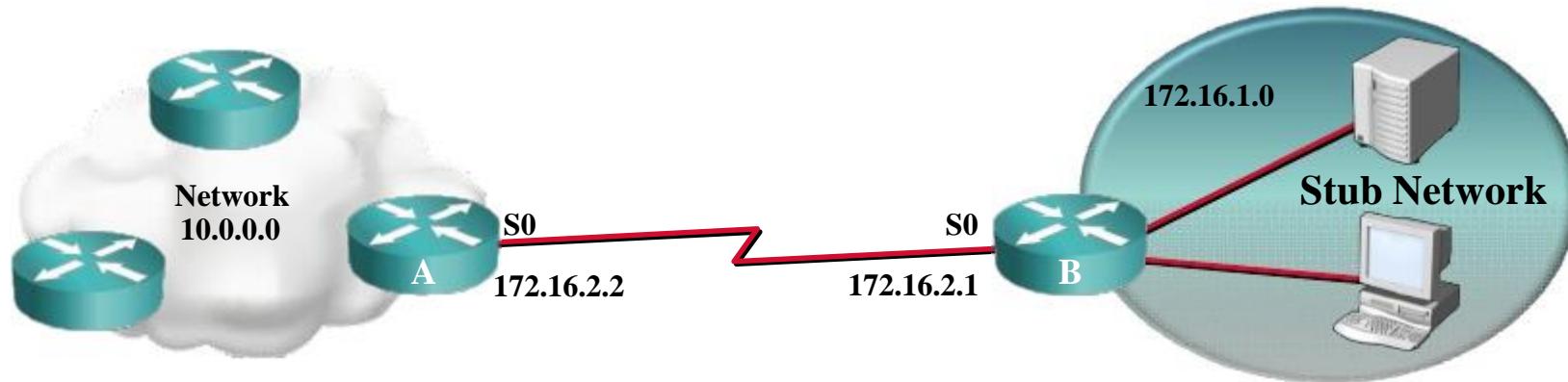
Static Route 설정하기

- Static Route 설정 예제 #2



Default Route 설정하기

- Default Route 설정 예제



- RouterA

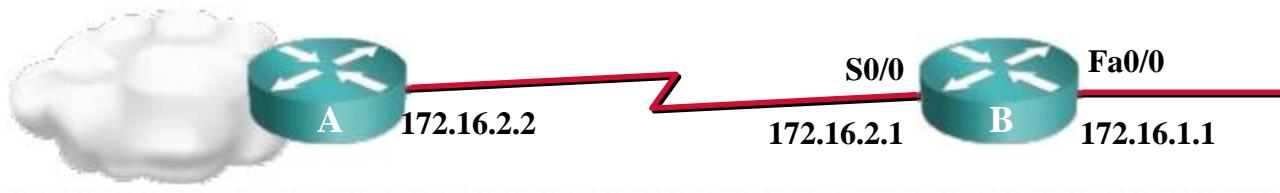
```
Router(config)#ip route 172.168.1.0 255.255.255.0 172.16.2.1
```

- RouterB

```
Router(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
```

Default Route 설정하기

- Default Route 설정 확인

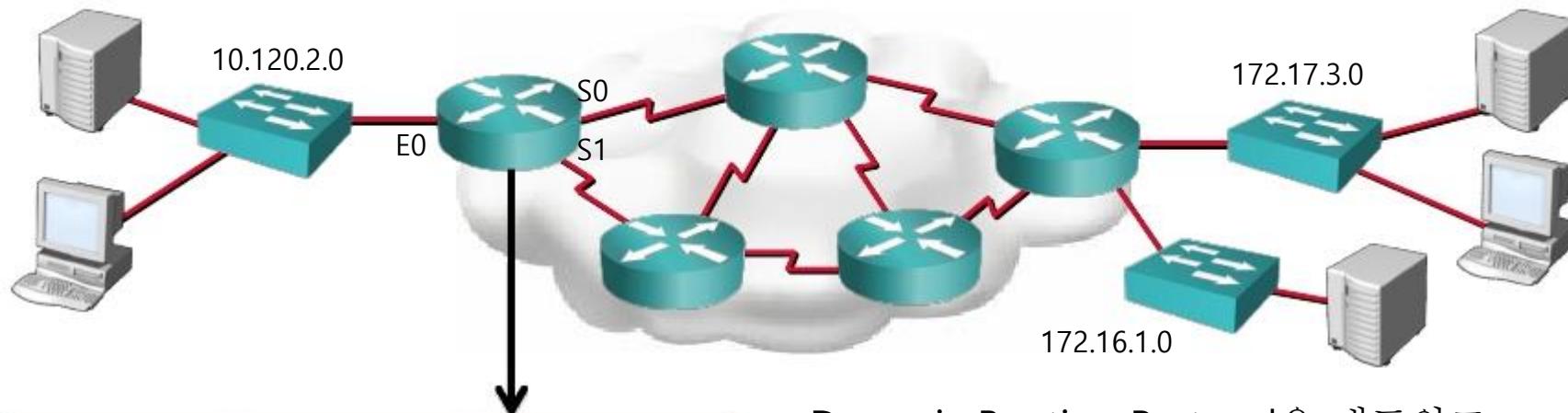


```
Router-B#config t
Router-B(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2
Router-B(config)#exit
Router-B#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
        * - candidate default, U - per-user static route, o - ODR
        P - periodic downloaded static route

Gateway of last resort is not set

C 172.16.0.0/24 is subnetted, 3 subnets
C    172.16.1.0 is directly connected, FastEthernet0/0
C    172.16.2.0 is directly connected, Serial0/0
S*  0.0.0.0/0 [ 1/0 ] via 172.16.2.2
Router-B#
```

Dynamic Routing 개요



라우팅 프로토콜	목적지 네트워크	나가는 인터페이스
Connected RIP	10.120.2.0 172.16.2.0	E0 S0

Dynamic Routing Protocol은 네트워크 정보를 교환하여 최적의 경로를 결정하고, 라우팅 테이블을 지속적으로 유지한다. 하나의 경로가 결정되면 라우터는 Routed Protocol들을 라우트 할 수 있다.

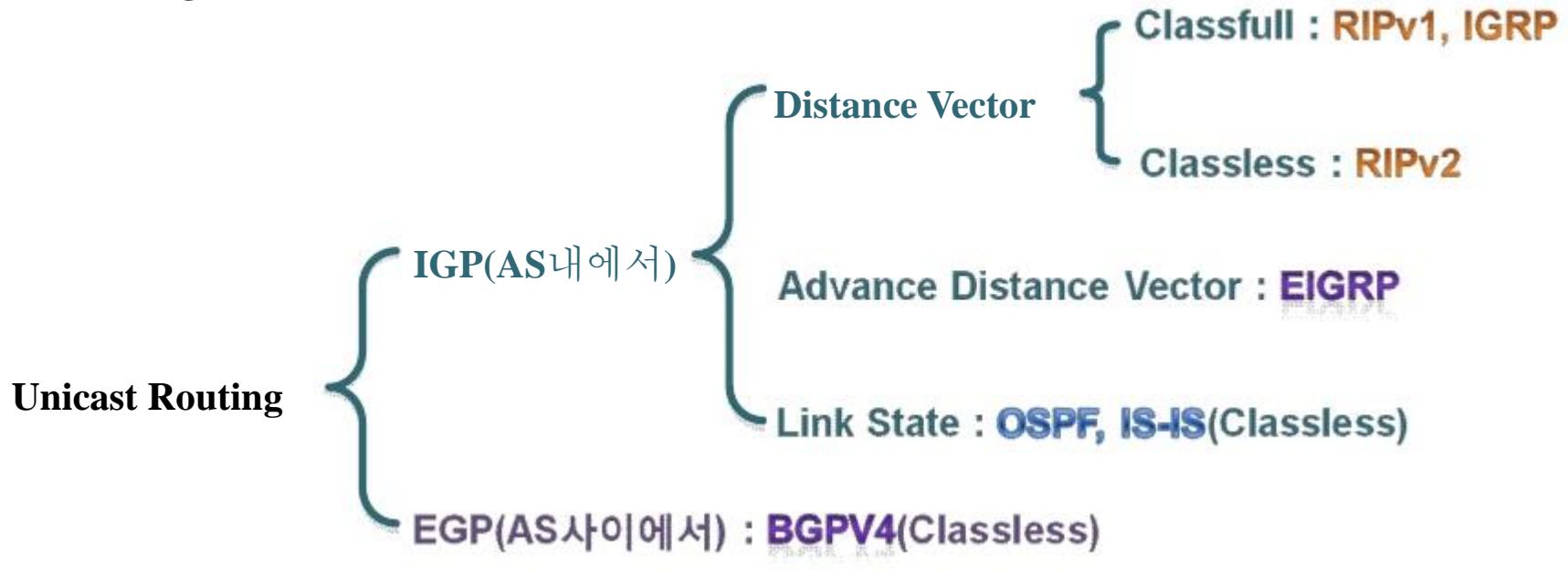
- **Routed Protocol** : IP, IPX, Apple Talk
- **Routing Protocol** : RIP, IGRP, EIGRP, OSPF, ISIS, BGP, DBMRP (Distance-Vector Multicast-Routing Protocol) , MOSPF, PIM Dense & Sparse

Routing Protocol 종류

1. 라우팅 정보를 수집하는 방식에 따라 static routing 과 dynamic routing
 - static : default, static routing
 - dynamic : rip, eigrp, ospf ...
2. 다른 라우터에 보내는 라우팅 정보의 내용에 따라 distance vector 와 link state
 - distance vector : rip, igrp
 - link state : ospf, is-is
 - Hybrid : eigrp
3. 라우팅 정보에 서브넷 마스크 정보 포함 여부에 따라서 classful 과 classless
 - classful : rip v1, igrp
 - classless : rip v2, eigrp , ospf, is-is
4. 동일한 조직 (AS : Autonomous System) 내부 또는 서로 다른 조직간에 사용되는지 여부에 따라 IGP (interior gateway protocol) 또는 EGP (exterior gateway protocol)
 - IGP : rip, eigrp, ospf, is-is
 - EGP : BGPv4

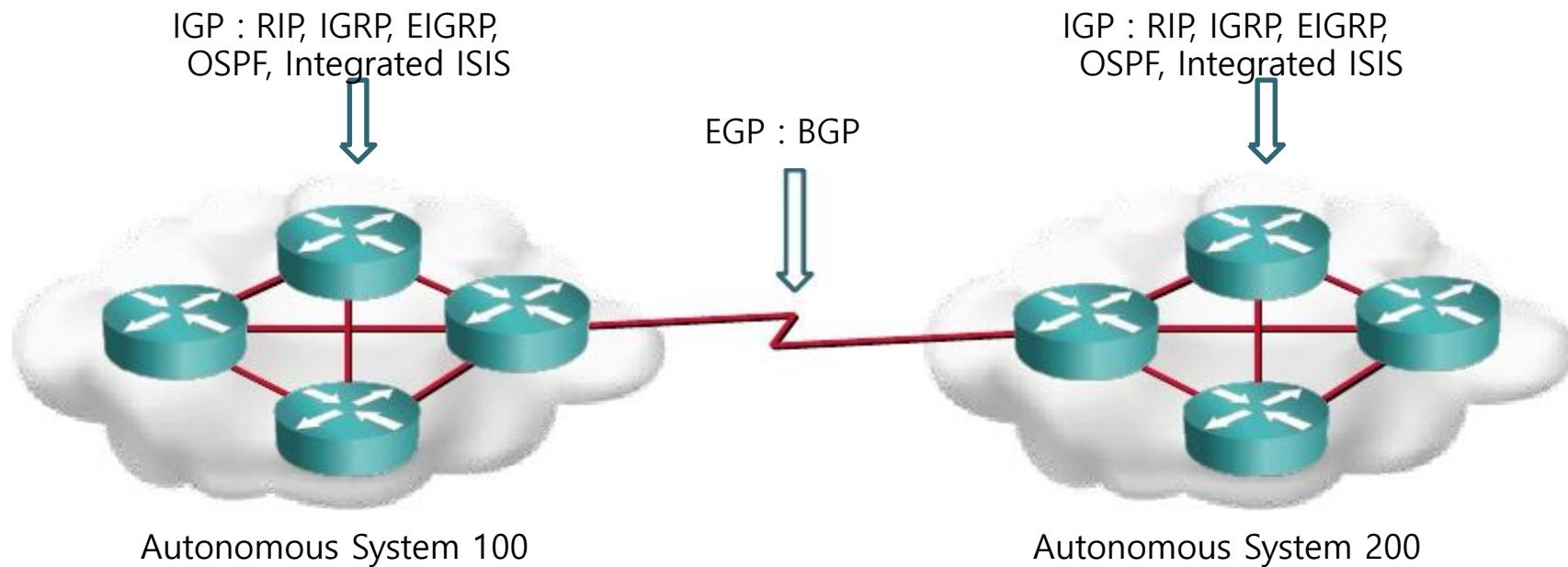
Dynamic Routing 개요

- IP Routing Protocol의 종류



Multicast Routing : DVMRP, MOSPF, PIM Dense & Sparse

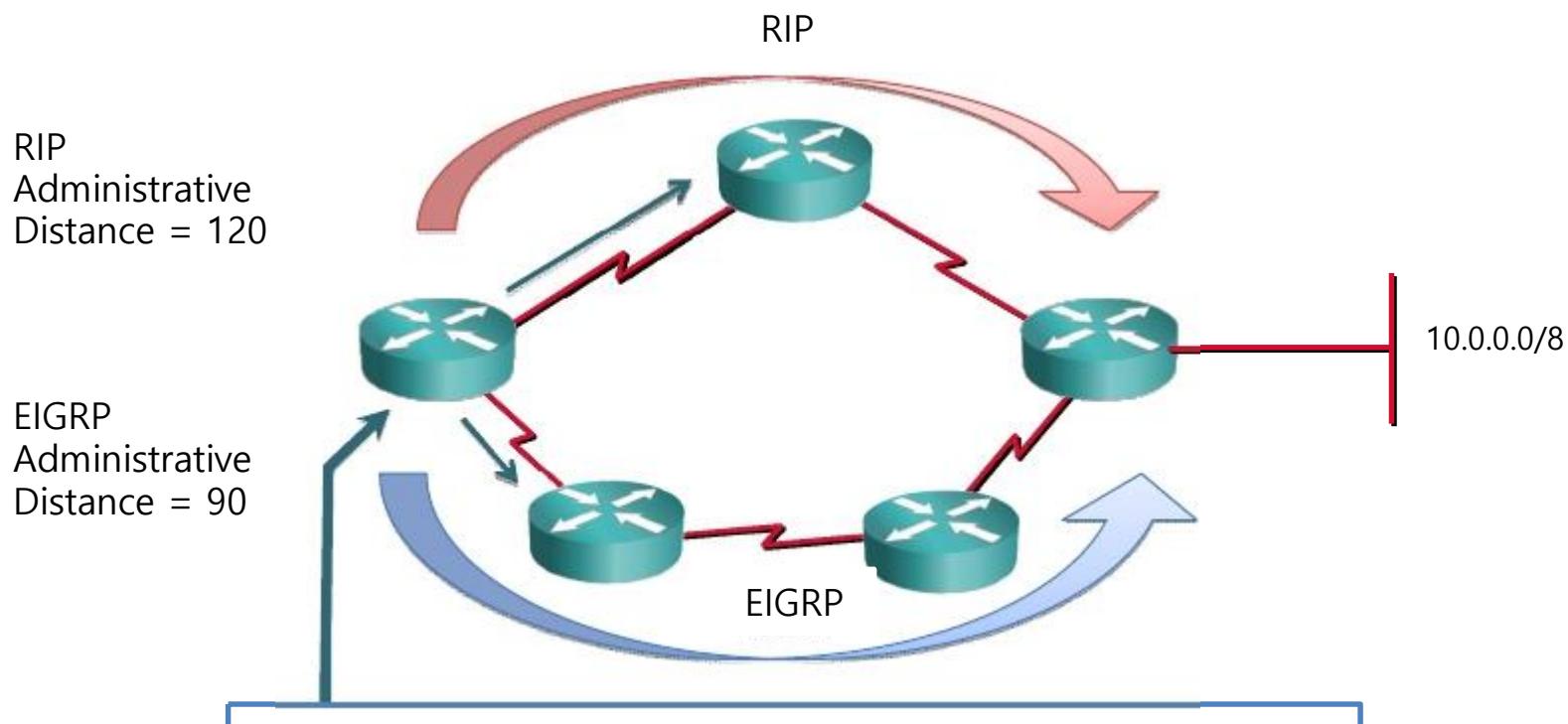
Dynamic Routing 개요



- Autonomous System은 일반적인 관리 영역하에 있는 네트워크들의 집합
- IGP들은 Autonomous System안에서 운영
- EGP들은 다른 Autonomous System간의 운영

Dynamic Routing 개요

- Administrative Distance



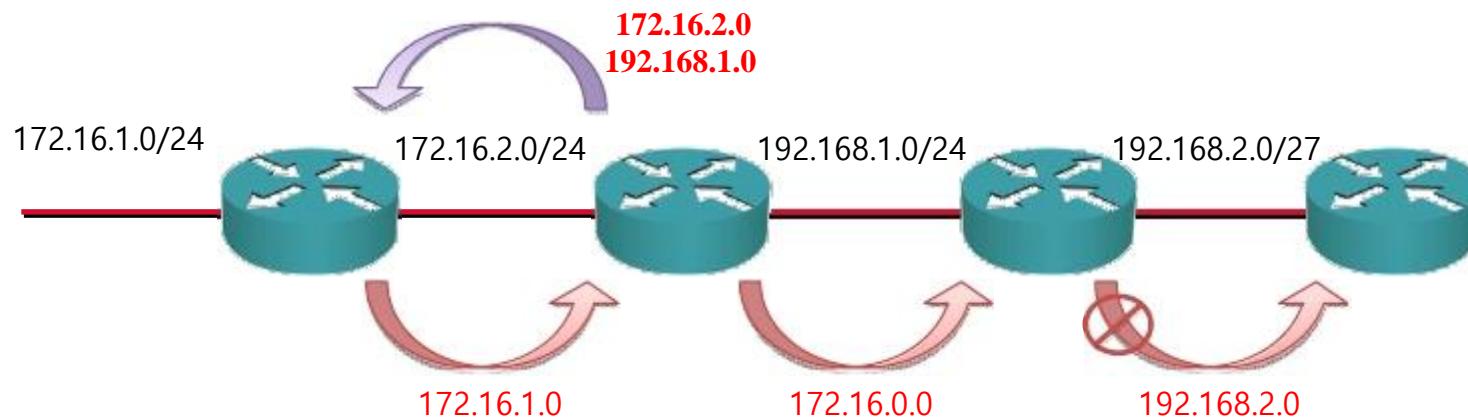
10.0.0.0/8로 가기 위해서 어떤 Routing Protocol이 학습한 경로를
더 신뢰할 것인가??

Administrative Distance 값들

RouteSource	DefaultDistance
Connectedinterface	0
StaticRoute	1
eBGP	20
InternalEIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
ExternalEIGRP	170
iBGP	200
Unknown	255

Dynamic Routing 개요

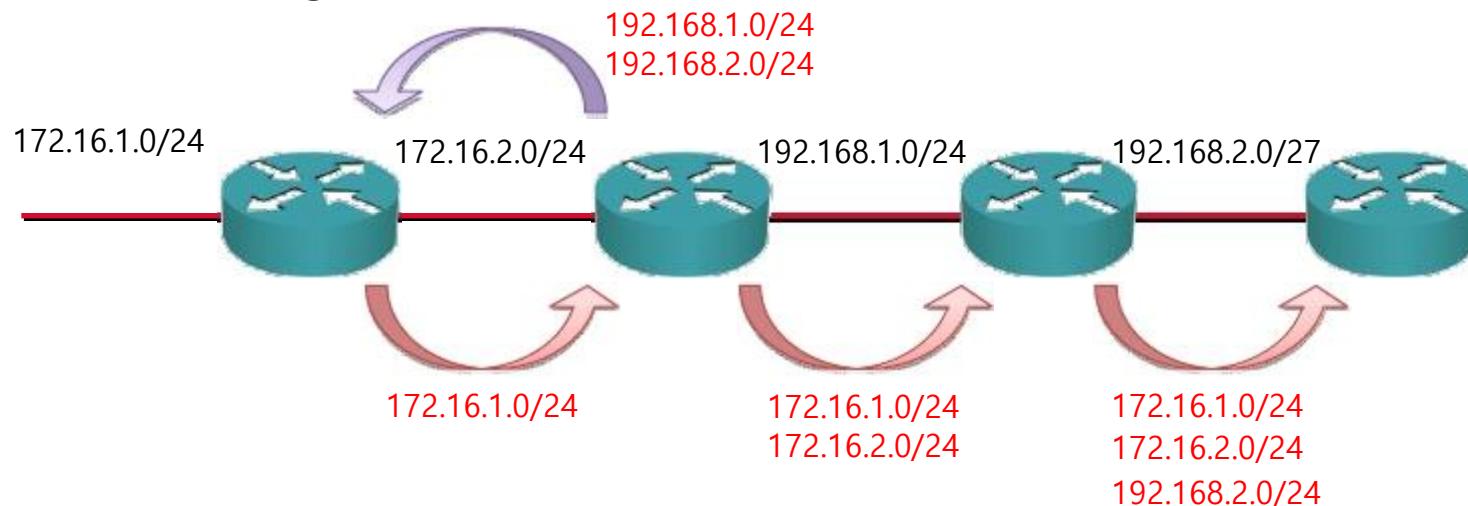
- Classful Routing



- Routing 정보 전달 시에 Subnet mask 정보를 전달하지 않는다
- 같은 network에 연결된 Router들은 같은 Subnet mask로 설정되어 있다고 가정한다
- Network이 다른 router와 Routing 정보 교환 시에는 자동으로 Classfull 경계를 기반으로 Summary된 정보를 전달한다
- RIP Version 1과 IGRP가 여기 속한다

Dynamic Routing 개요

- Classless Routing



- Routing 정보 전달 시에 Subnet mask 정보를 함께 전달한다
- Network에 연결된 Router들은 다양한 Subnet mask로 설정되어 있을 수 있다 (VLSM 지원)
- Network이 다른 router와 Routing 정보 교환 시에는 수동적으로 Summary된 정보를 전달 할 수도 있다
- RIP Version 1과 IGRP를 제외한 모든 Routing Protocol이 이를 지원한다

Dynamic Routing 개요

- Routing Protocol들의 비교 #1

특 징	RIPv1	RIPv2	IGRP	EIGRP**	OSPF
Distance vector	O	O	O	O	
LinkState					O
Classful(auto route summ.)	O	O	O	O	
Classless(VLSM support)		O		O	O
Proprietary			O	O	
Scalability	Small	Small	Med.	Large	Large
Convergence time	Slow	Slow	Slow	Fast	Fast

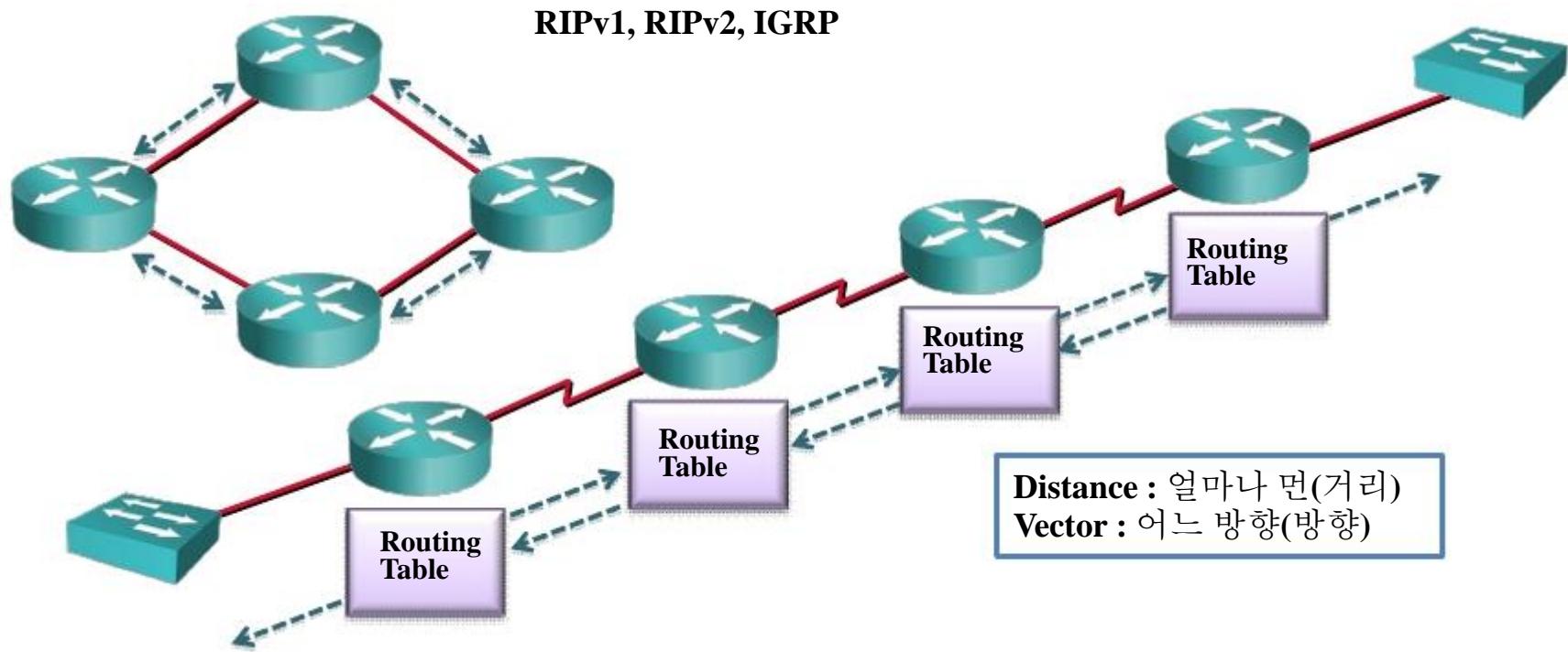
Dynamic Routing 개요

- Routing Protocol들의 비교 #2

특 징	RIPv1	RIPv2	IGRP	EIGRP**
Count to infinity	O	O	O	
Split horizon	O	O	O	O
Holddown timer	O	O	O	
Triggered updates with route poisoning	O	O	O	O
Load balancingEqual paths	O	O	O	O
Load balancingUnequal paths			O	O
VLSM support		O		O
Routing algorithm	BF	BF	BF	Dual
Metric	Hops	Hops	Comp	Comp
Hop count limit	16	16	100	100
Scalability	Med	Med	Large	Large

** EIGRP는 Advanced Distance Vector Protocol (Hybrid)

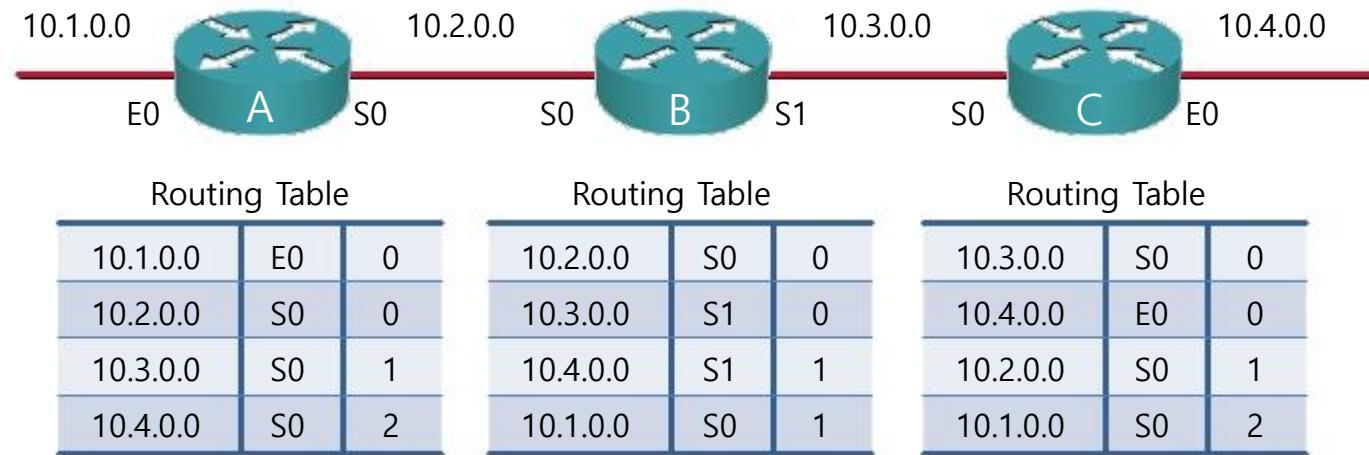
Distance Vector Routing의 개요



- 최적의 라우팅 리스트를 만든 후, 주기적으로 라우팅 테이블을 인접관계에 있는 라우터에게 전달

Distance Vector Routing의 개요

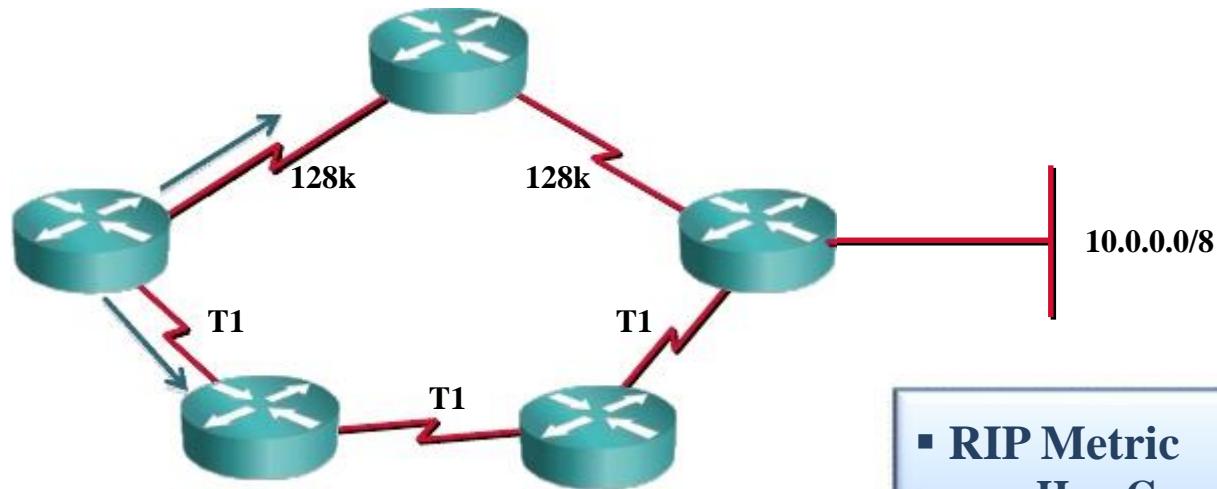
- Distance Vector의 경로 정보 수집



- Router들은 Network상에 각 Destination에 대해 최적의 경로를 선택 후 이를 관리 및 유지 한다.

Distance Vector 의 경로 선택

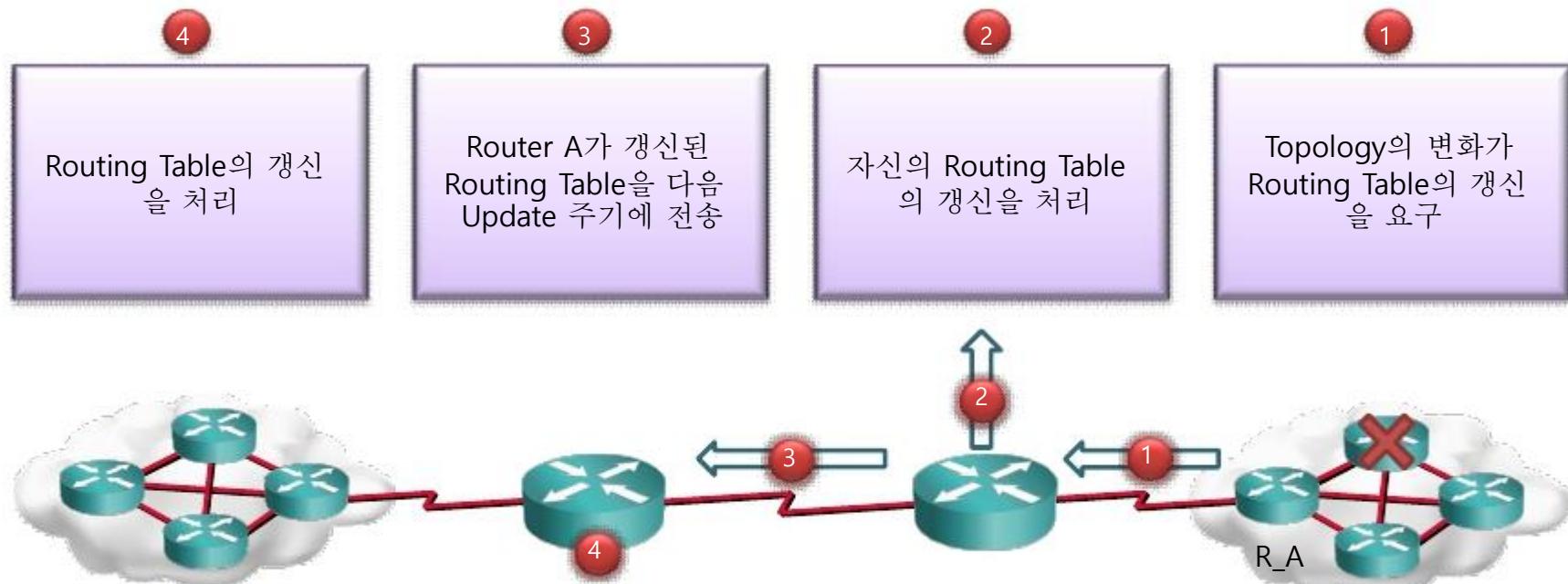
- Distance Vector의 Metric



▪ RIP Metric
• Hop Count

▪ IGRP Metric
▪ Bandwidth, Delay
▪ Load, Reliability, MTU

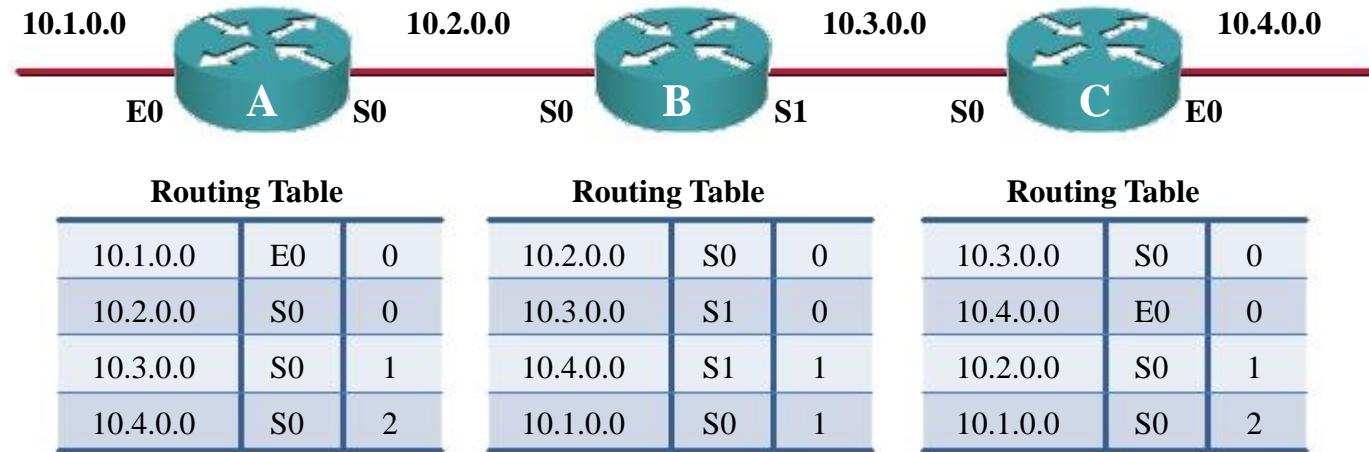
Routing 정보 관리



- Update 절차는 라우터에서 다른 라우터로 StepbyStep으로 진행

Distance Vector의 Routing Loop

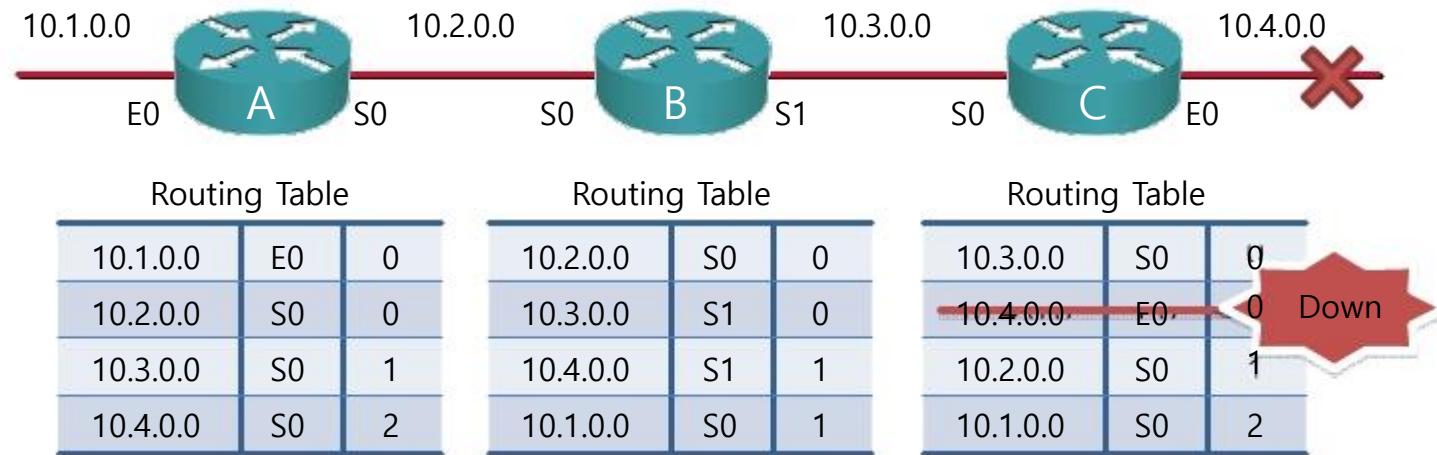
- Routing Loop 예제



일반적인 상황에서의 Routing Table

Distance Vector의 Routing Loop

- Routing Loop 예제 (계속)

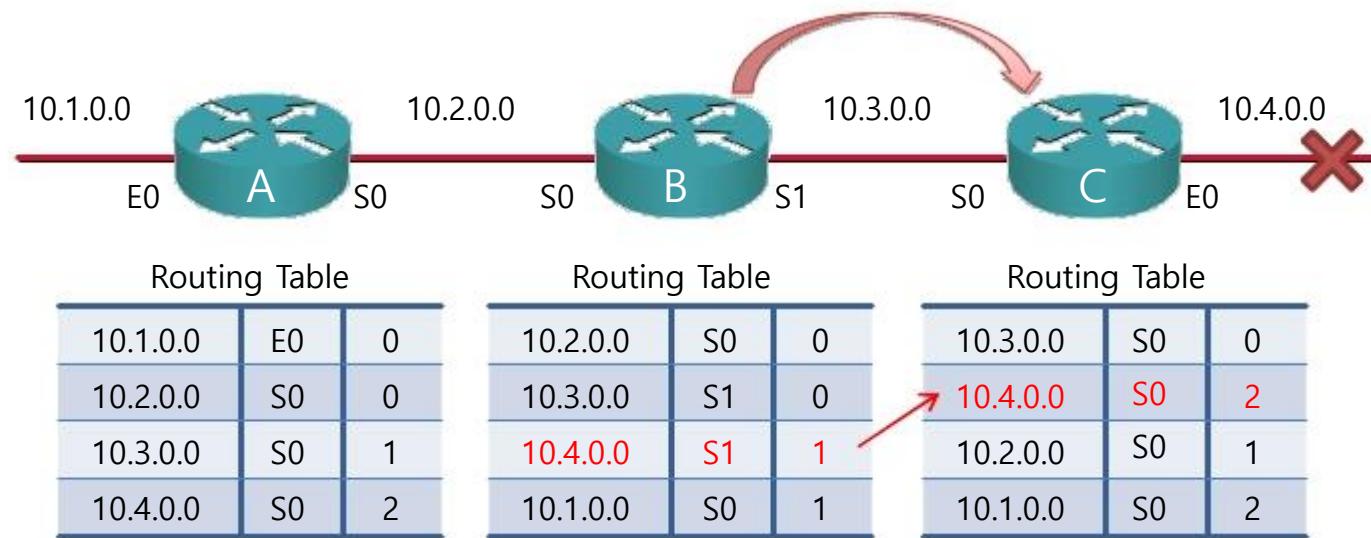


RouterC에서 Down된 Ethernet 구간은 Routing Table에서 경로 제거

이러한 Topology의 변화가 다른 Router에게 얼마나 빨리 전달되는가 ?

Distance Vector의 Routing Loop

- Routing Loop 예제 (계속)

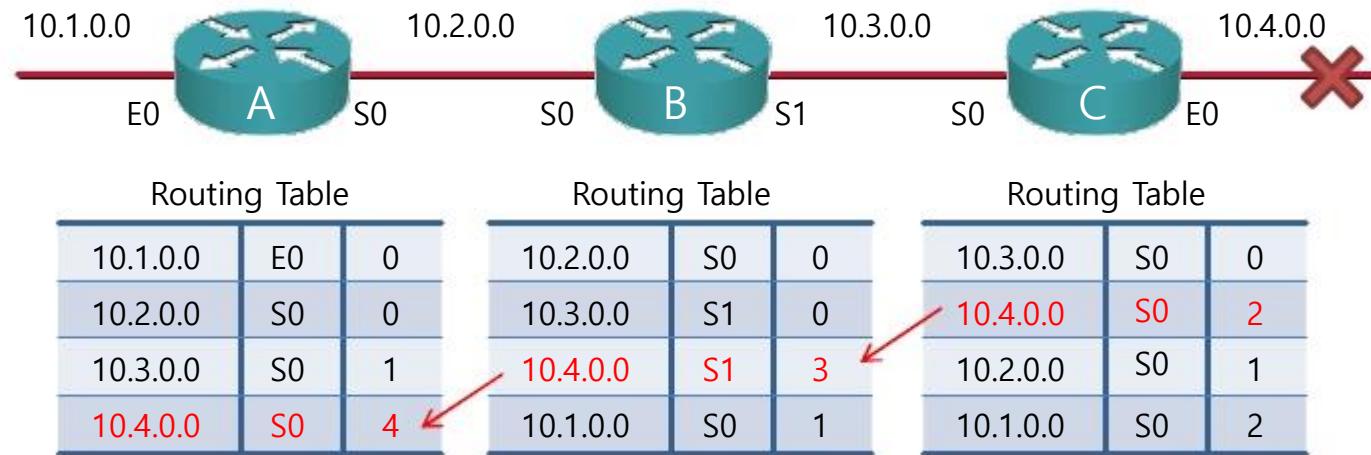


Distance Vector는 Network Topology를 이해하지 못한다

RouterC는 RouterB에서 받은 Routing 정보를 기반으로 10.4.0.0에 도달할 수 있는 또 다른 경로가 있다고 판단한다

Distance Vector의 Routing Loop

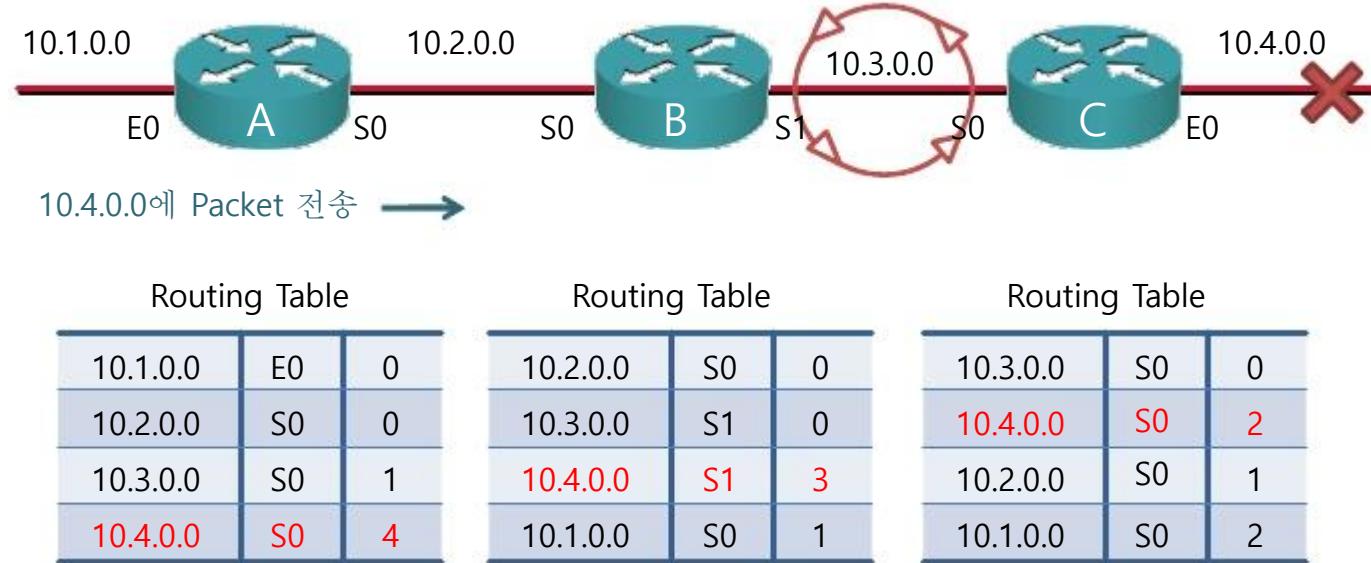
- Routing Loop 예제 (계속)



결국 Hop Count가 Maximum=16까지 증가되어서야 10.4.0.0의 Network이 도달할 수 없음을 모든 Router가 인지하게 된다

Hop Count가 Maximum까지 증가되면 Routing Table에서 해당 경로를 제거한다

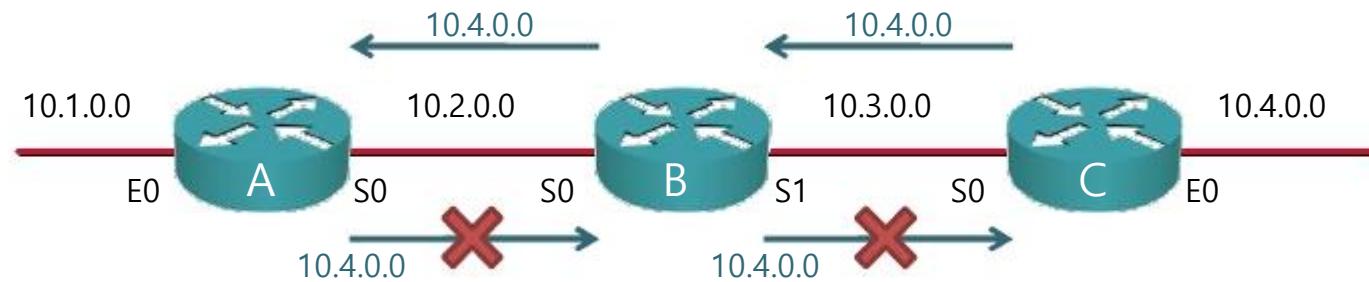
Distance Vector의 Routing Loop



RouterB와 RouterC 사이에서 Routing Loop 발생

Routing Loop 문제 해결

- Split Horizon



Routing Table		
Network	Interface	Hop Count
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	2

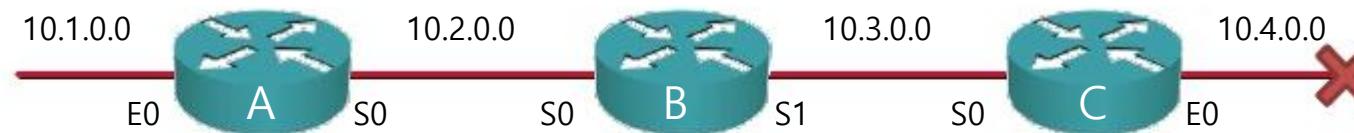
Routing Table		
Network	Interface	Hop Count
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	1
10.1.0.0	S0	1

Routing Table		
Network	Interface	Hop Count
10.3.0.0	S0	0
10.4.0.0	E0	0
10.2.0.0	S0	1
10.1.0.0	S0	2

특정 interface에서 받아온 Route 정보는 차후에 그 interface를 통해 다시 전달되지 않는다.

Routing Loop 문제 해결

- Route Poisoning



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	16

Routing Table		
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	16
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

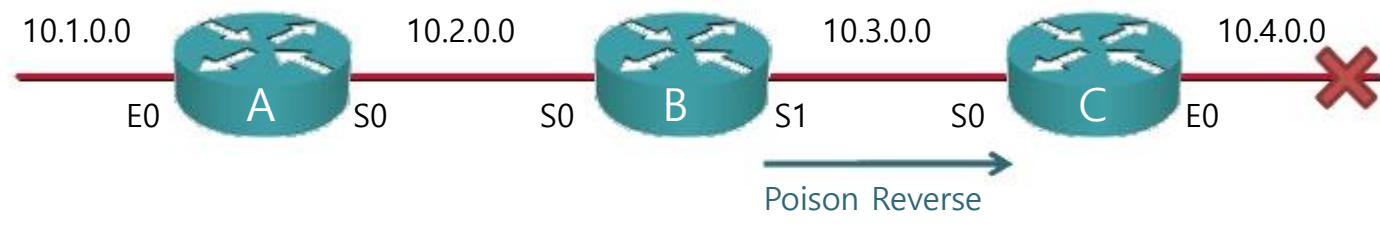
Down

hop = 16

hop = 16

Routing Loop 문제 해결

- Poison Reverse



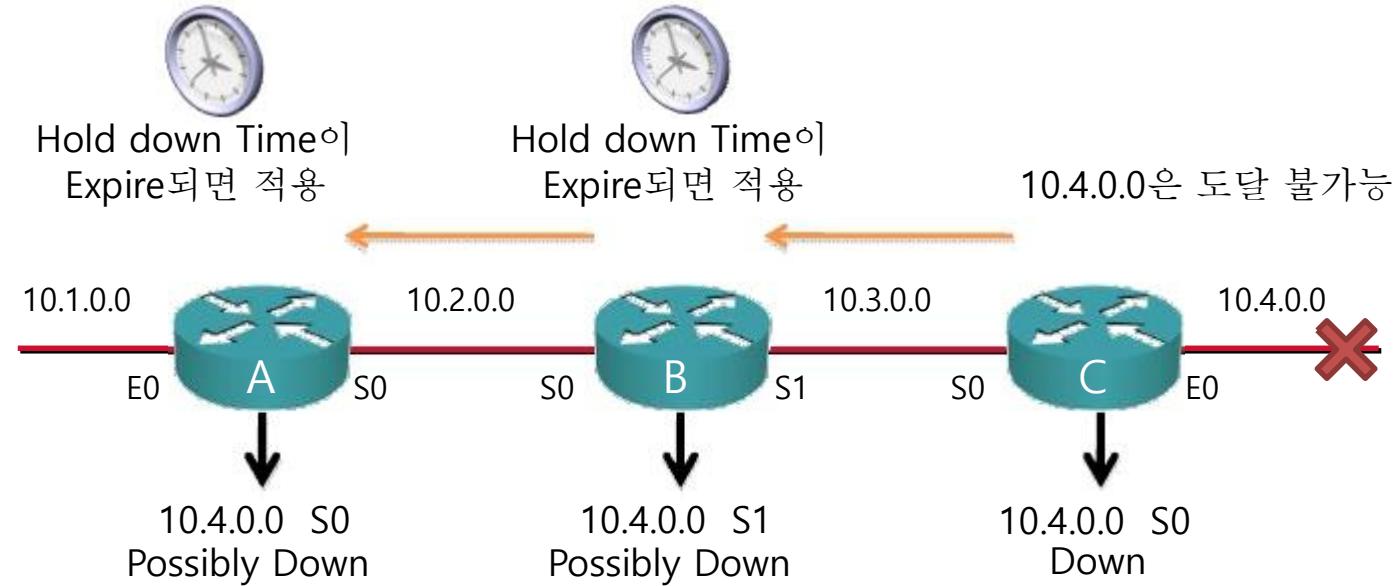
Routing Table		
Network	Interface	Hop Count
10.1.0.0	E0	0
10.2.0.0	S0	0
10.3.0.0	S0	1
10.4.0.0	S0	16

Routing Table		
Network	Interface	Hop Count
10.2.0.0	S0	0
10.3.0.0	S1	0
10.4.0.0	S1	Possibly Down
10.1.0.0	S0	1

Routing Table		
Network	Interface	Hop Count
10.3.0.0	S0	0
10.4.0.0	E0	Infinity
10.2.0.0	S0	1
10.1.0.0	S0	2

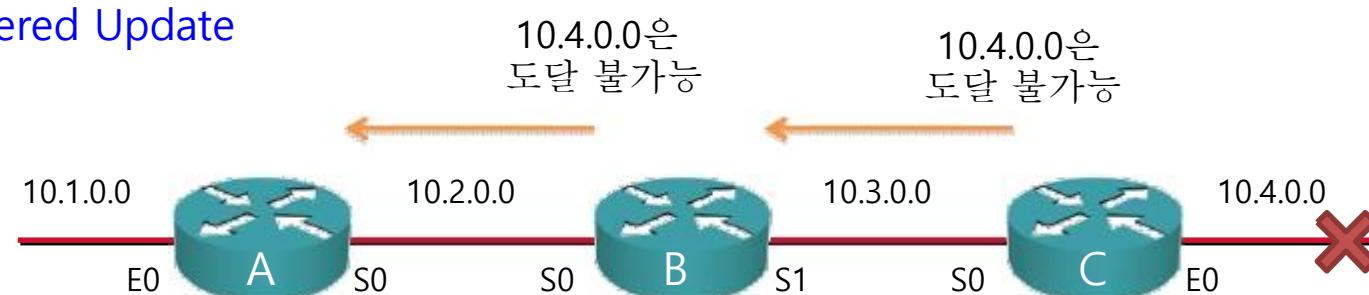
Routing Loop 문제 해결

- Hold down Timer



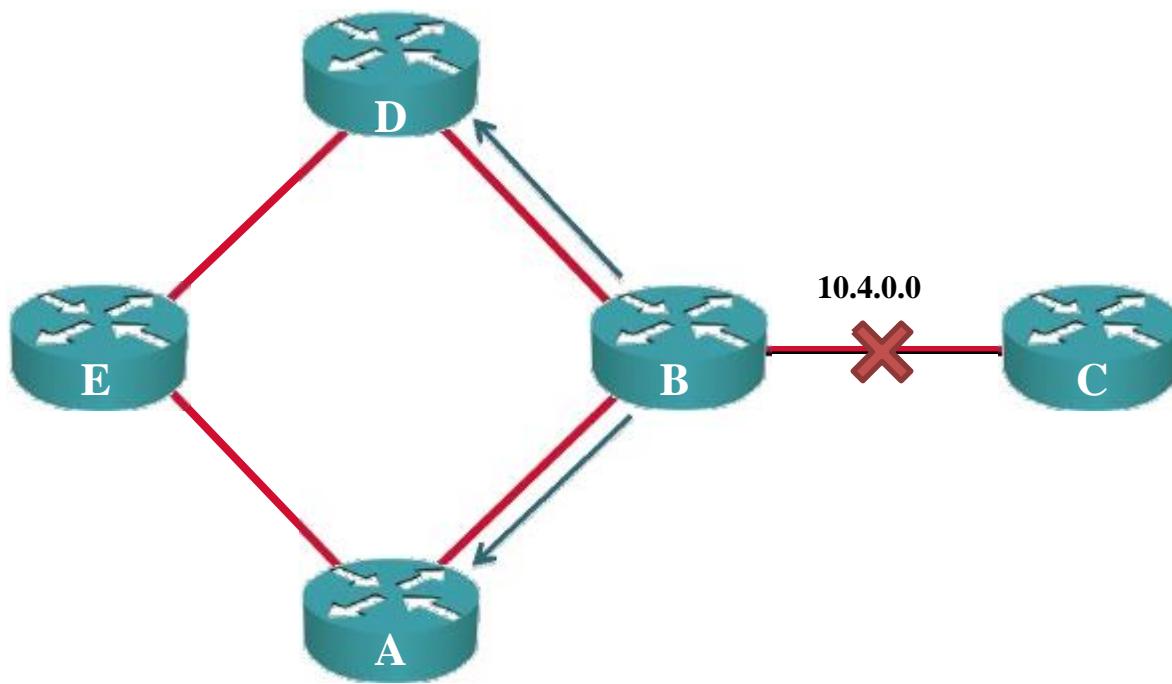
Router가 특정 Link의 Fail을 전달 받은 후에 해당 경로를 Routing Table에서 바로 제거하지 않고 특정 시간 동안 그 정보의 사실을 확인하기 위해 기다린다. 이는 Topology의 변화 정보를 검증하는 용도이다.

- Triggered Update

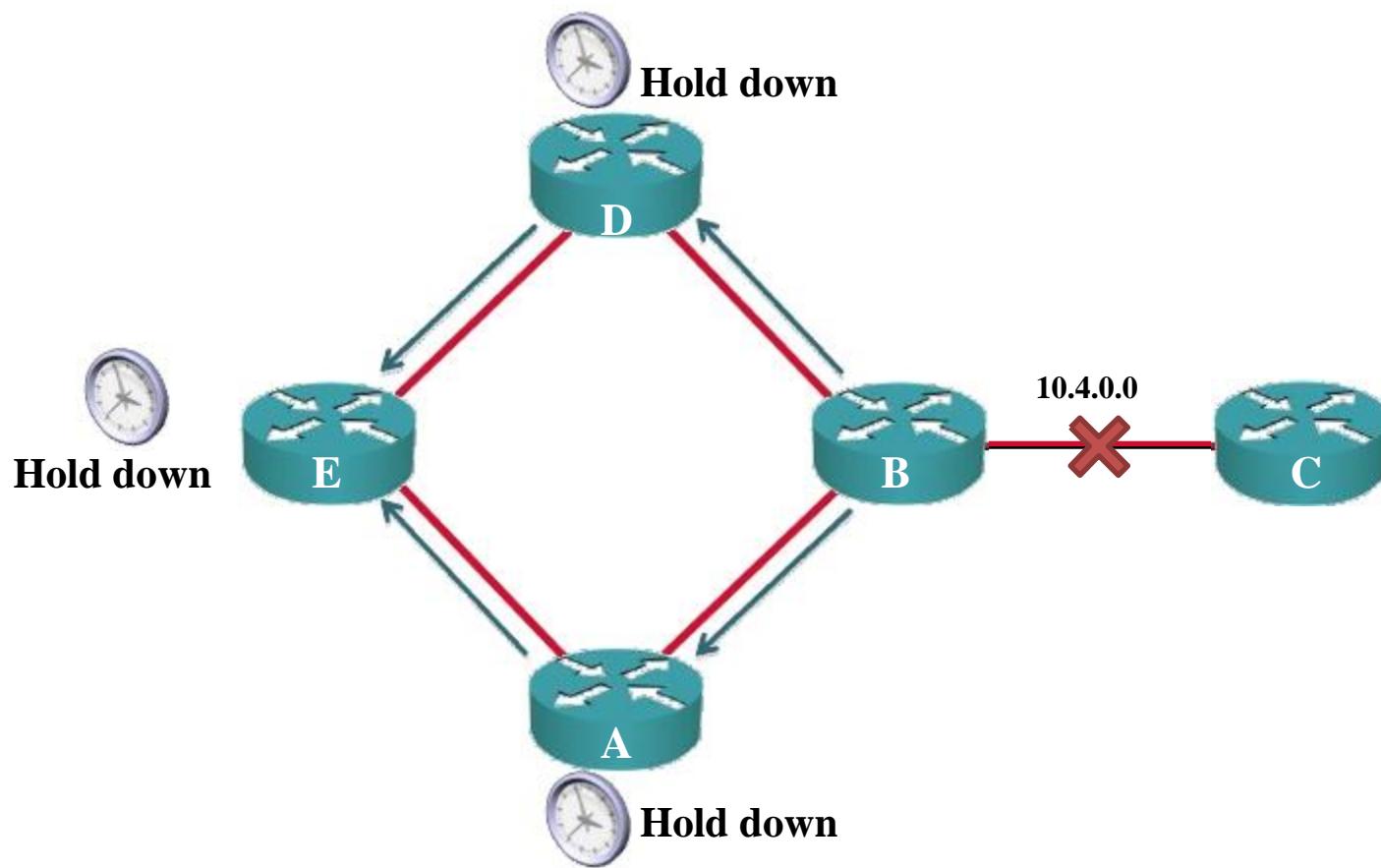


Topology의 변화를 즉시 이웃한 Router에게 알려준다

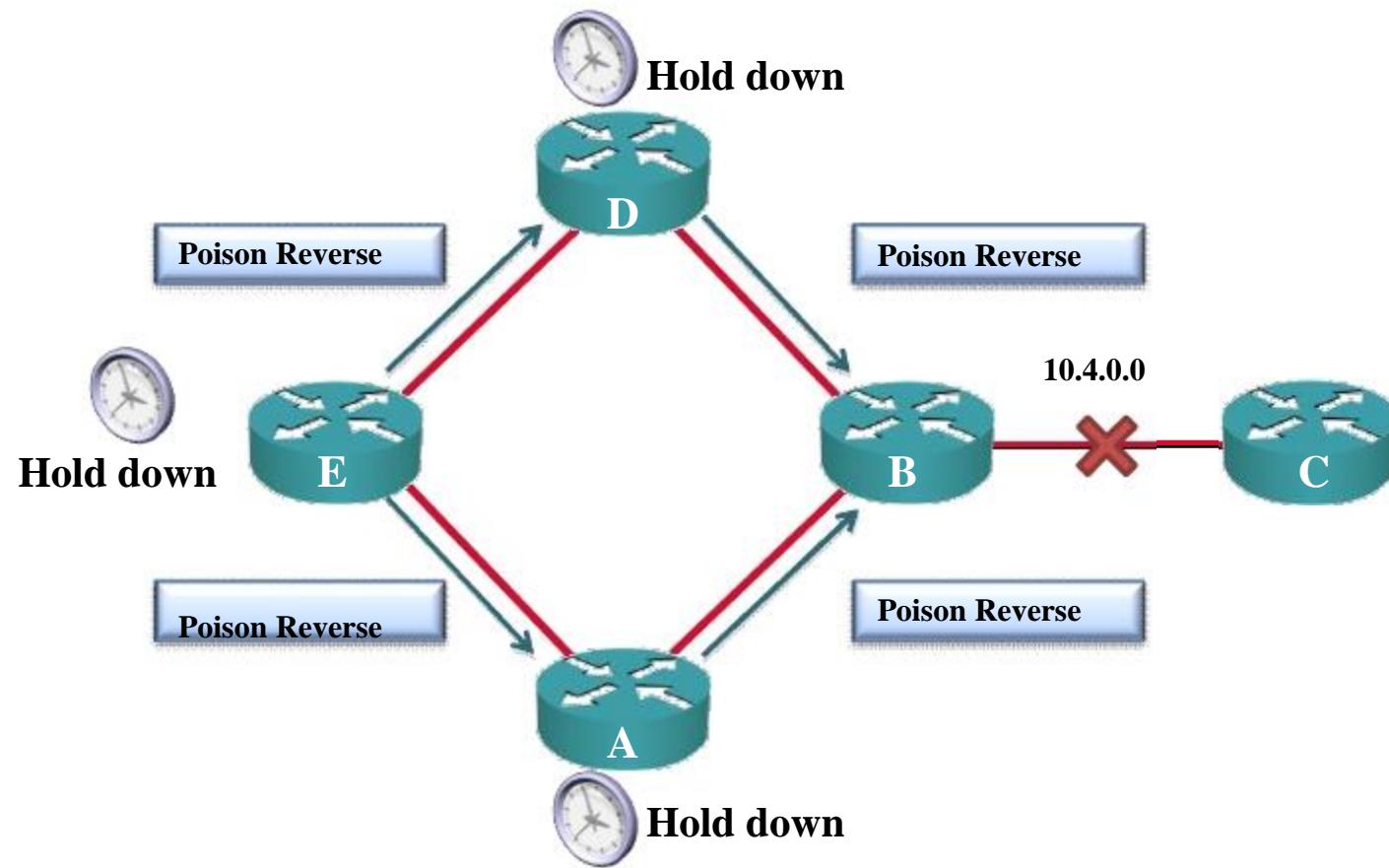
Distance Vector Operation



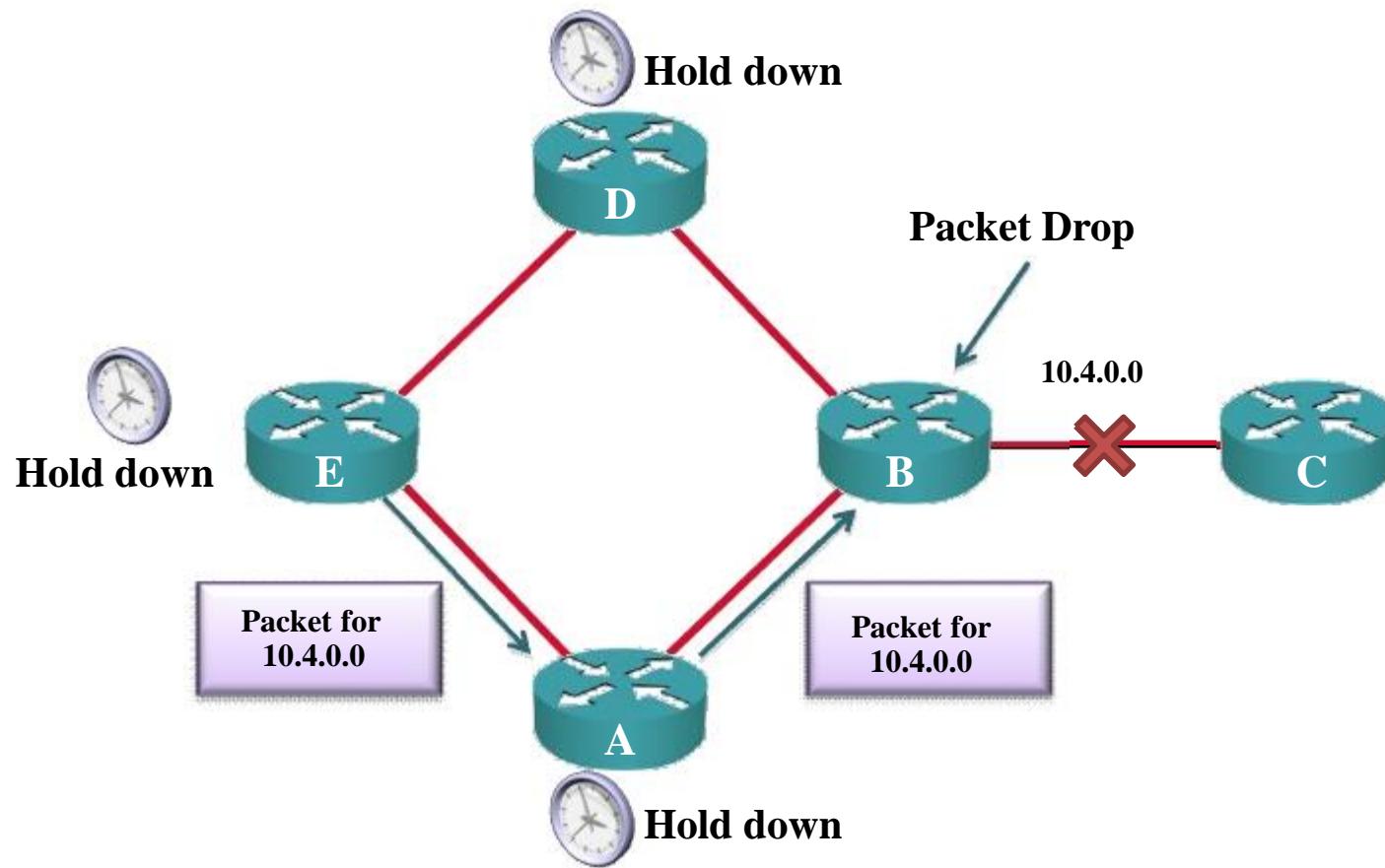
Distance Vector Operation



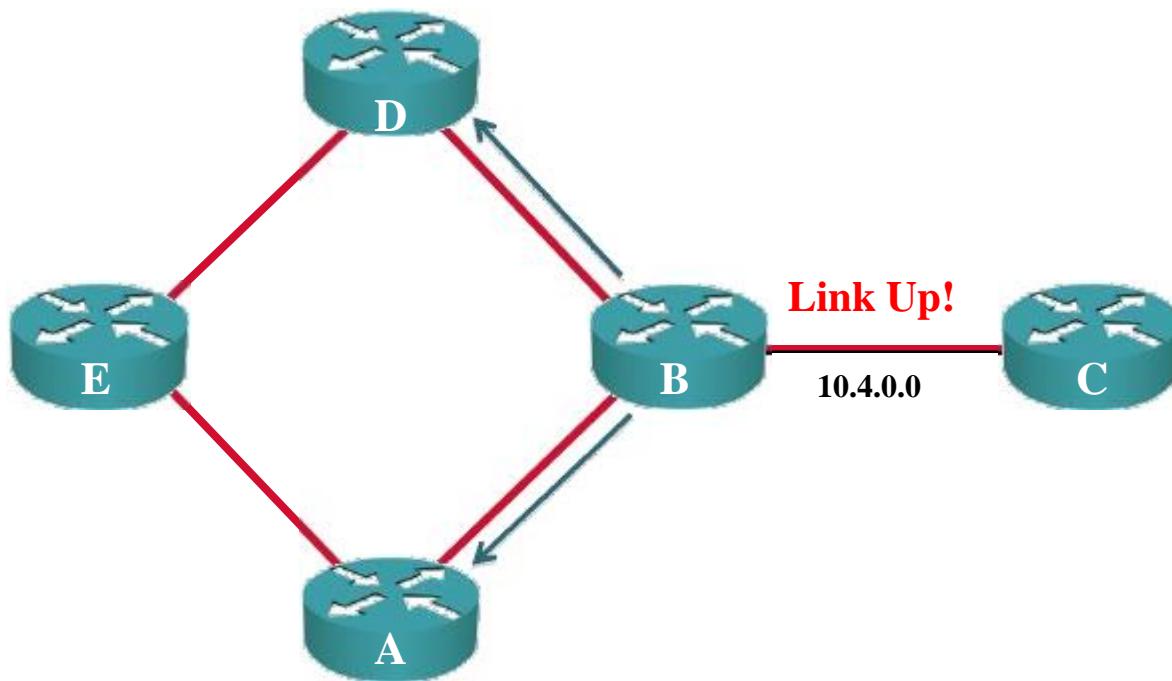
Distance Vector Operation



Distance Vector Operation



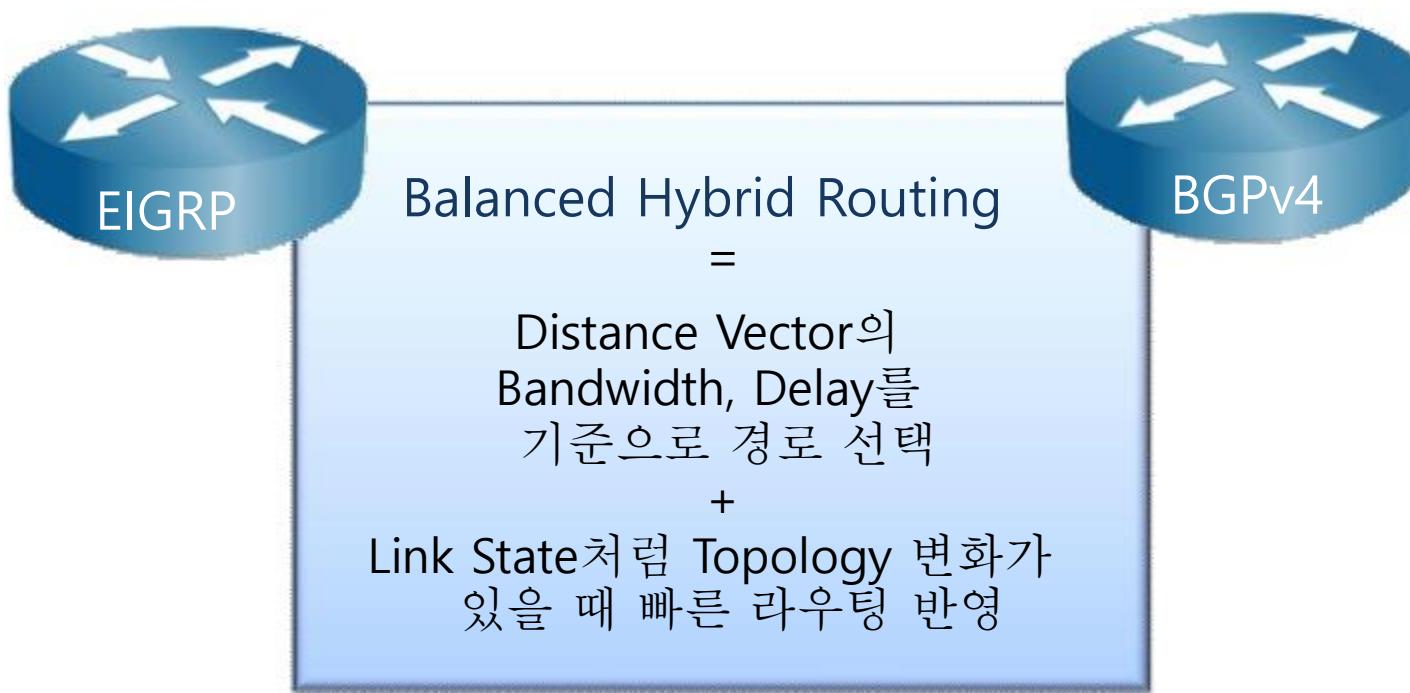
Distance Vector Operation



Hybrid Routing & LinkState

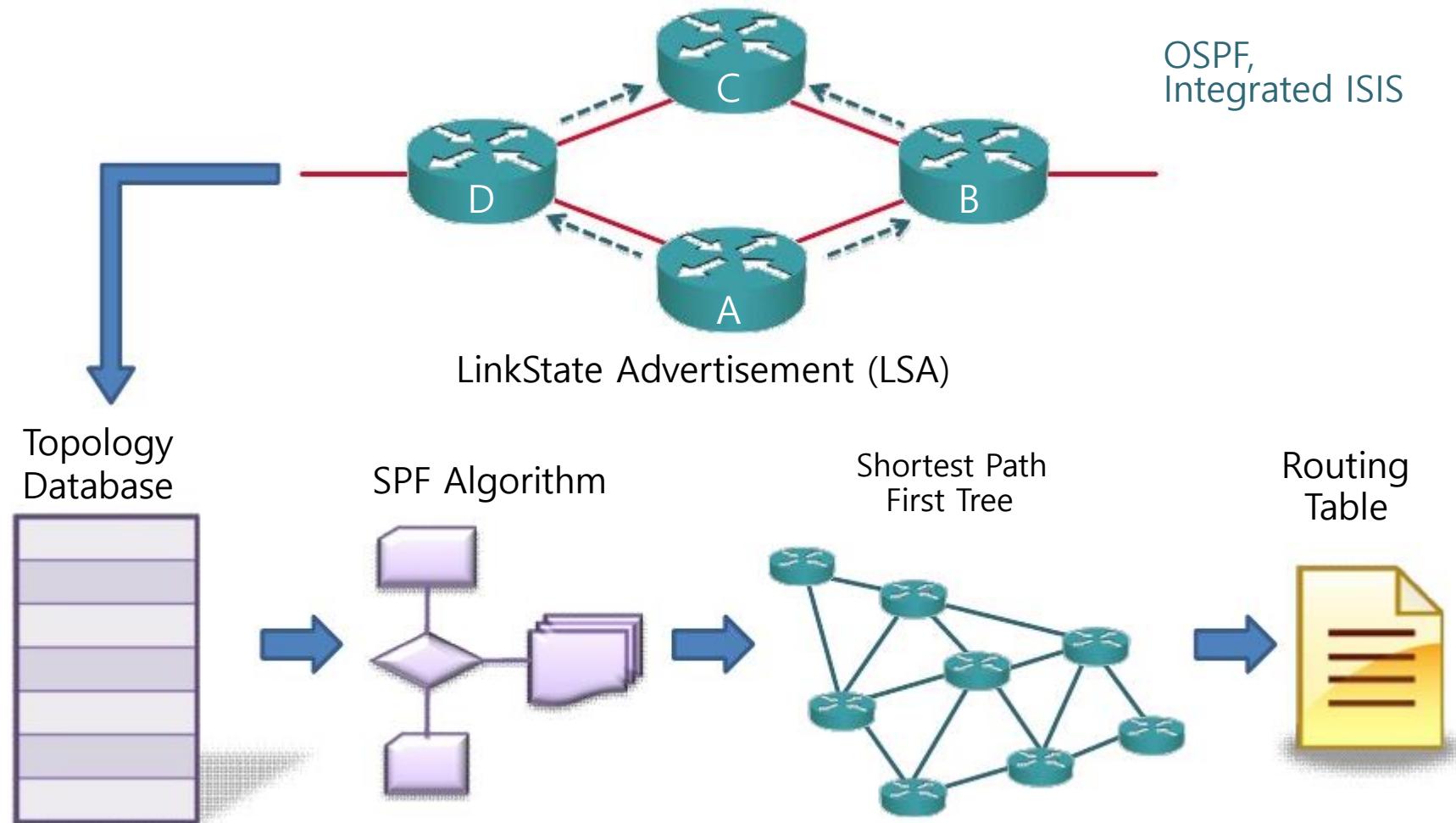
- Hybrid Routing Protocol
- LinkState Routing Protocol 개요
- LinkState의 SPF 알고리즘
- LinkState의 계층적 구조

Hybrid Routing Protocol



Distance Vector와 LinkState 특성을 공유

LinkState Routing Protocol



LinkState Routing Protocol

■ LinkState Routing Protocol의 장점 :

Fast Convergence :

Topology의 변화에 빠른 반응을 수행한다.

Routing Loop :

Topology를 이해하므로 SPF 알고리즘에서 Routing Loop를 방지한다.

계층적 Design에 따라 Network 확장성이 보장된다.

■ LinkState Routing Protocol의 단점 :

Router의 내부 Resource 소모가 많다.

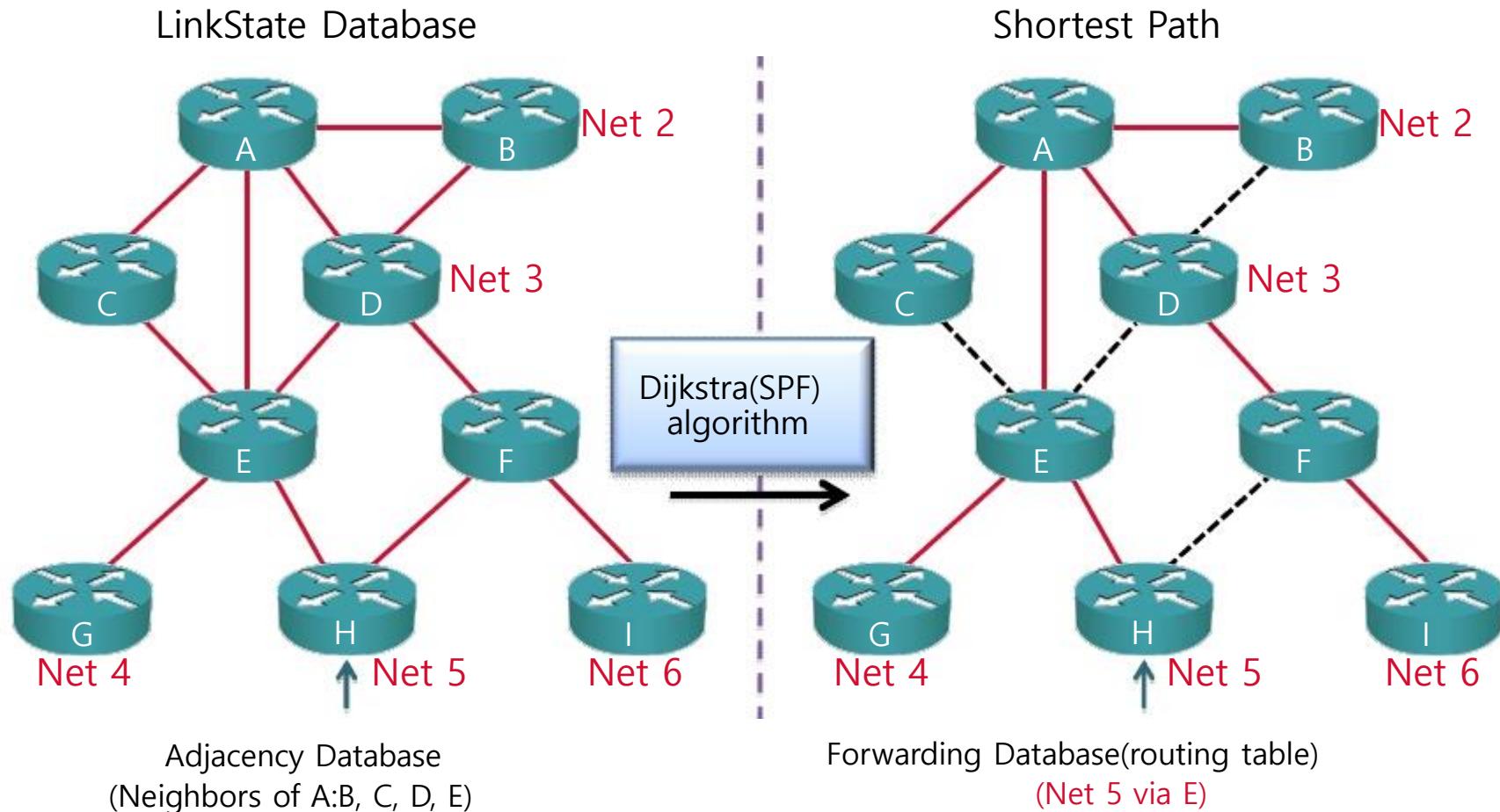
CPU가 네트워크에 변경사항 발생시 잦은 SPF 알고리즘 수행

Network Topology 정보 관리를 위해 요구되는 Memory가 많다.

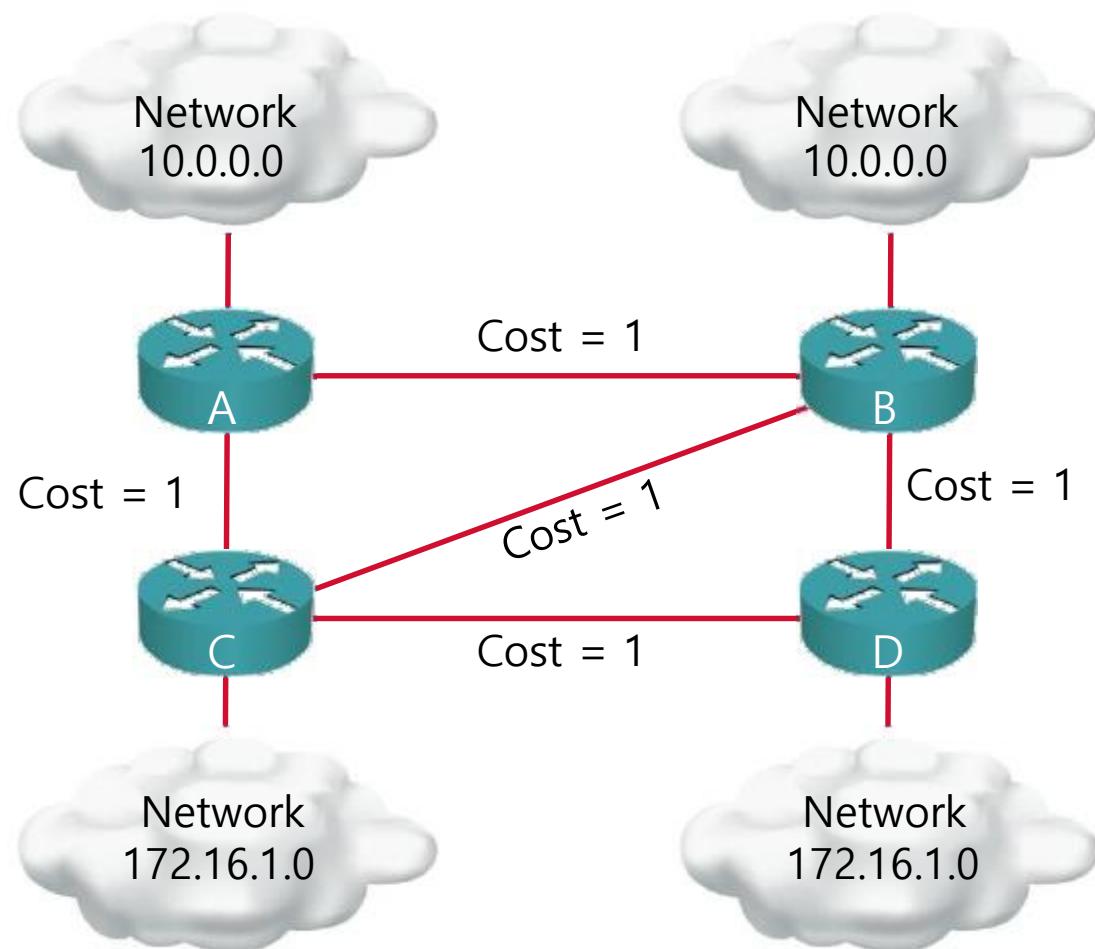
반드시 계층적 Design Rule을 따라야 한다.

경우에 따라서는 많은 Tuning Option을 이해해야 한다.

Link-State의 SPF 알고리즘



Link-State의 SPF 알고리즘



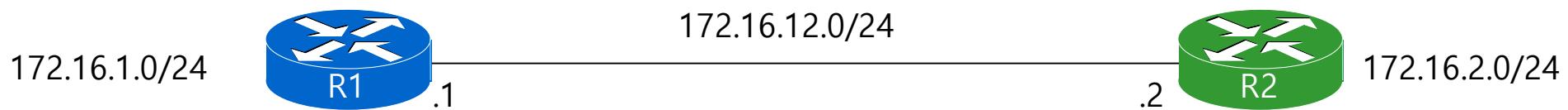
RIP 개요

RIP에는 V1, V2가 있으며, RIP V1는 Classful Routing 을 하며, 모든 벤더들의 제품에서 동작을 한다.

- ❖ RIP V1은 UDP Port number 520번을 사용한다.
- ❖ RIP V1은 Routing Update를 할 때 Broadcast를 사용한다.
- ❖ RIP에는 Request Message and Response Message 두 메시지 형식이 있다.
- ❖ RIP은 Update, Invalid, Holddown, Flush timer를 이용하여 라우팅테이블을 업데이트한다.
- ❖ RIP은 최적의 경로를 선택할 때 Metric은 Hop Count를 사용을 한다.
- ❖ RIP은 최대 15개까지 허용을 한다.
- ❖ RIP은 Administrative Destination 120.

RIP Configuration

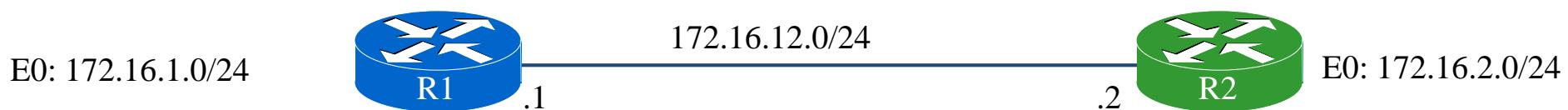
Cisco router에서 default로 RIP v1을 지원하며, 전역설정 모드에서 "router"라는 명령어를 사용하여 설정을 할 수가 있다.



```
Router(config)#router routing_protocol
Router(config-router)#network classful_network
```

RIP v1 Routing Update Address

RIP V1은 라우팅정보를 전파할 때 브로드캐스트를 한다. 또한, UDP Port Number 520번을 사용하여 Neighbor와 Routing Update가 이루어진다.

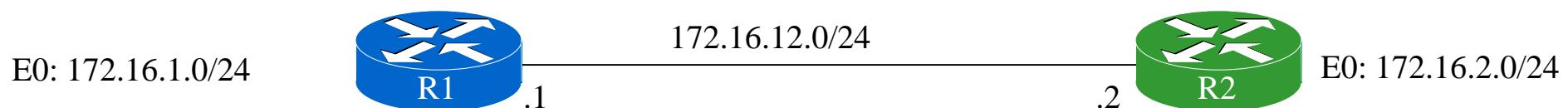


```
R1#debug ip rip
RIP protocol debugging is on
R1#
02:19:10: RIP: sending v1 update to 255.255.255.255 via Serial0 (172.16.12.1)
02:19:10: RIP: build update entries
02:19:10:     subnet 172.16.1.0 metric 1

02:19:38: RIP: sending v1 update to 255.255.255.255 via Serial0 (172.16.12.1)
02:19:38: RIP: build update entries
02:19:38:     subnet 172.16.1.0 metric 1
```

RIP v1 Passive-interface

특정 Interface로 Routing Update가 전송되는 것을 방지하기 위해서 사용되는 것이 “Passive-interface” 명령어 이다.



[Command type]

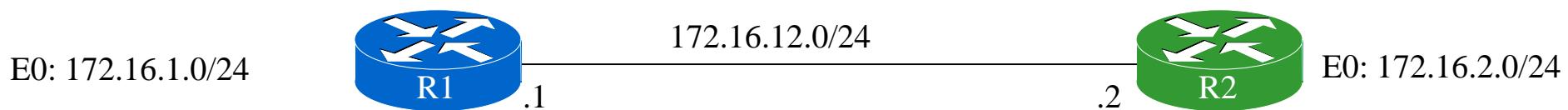
```
R1(config)#router rip  
R1(config-router)#passive-interface interface_type
```

[Configuration Example]

```
R1(config)#router rip  
R1(config-router)#passive-interface s0
```

RIP v1 Passive-interface

특정 Interface로 Routing Update가 전송되는 것을 방지하기 위해서 사용되는 것이 “**Passive-interface**” 명령어이다.



```
02:09:46: RIP: sending v1 update to 255.255.255.255 via Ethernet0 (172.16.1.1)
```

```
02:09:46: RIP: build update entries
```

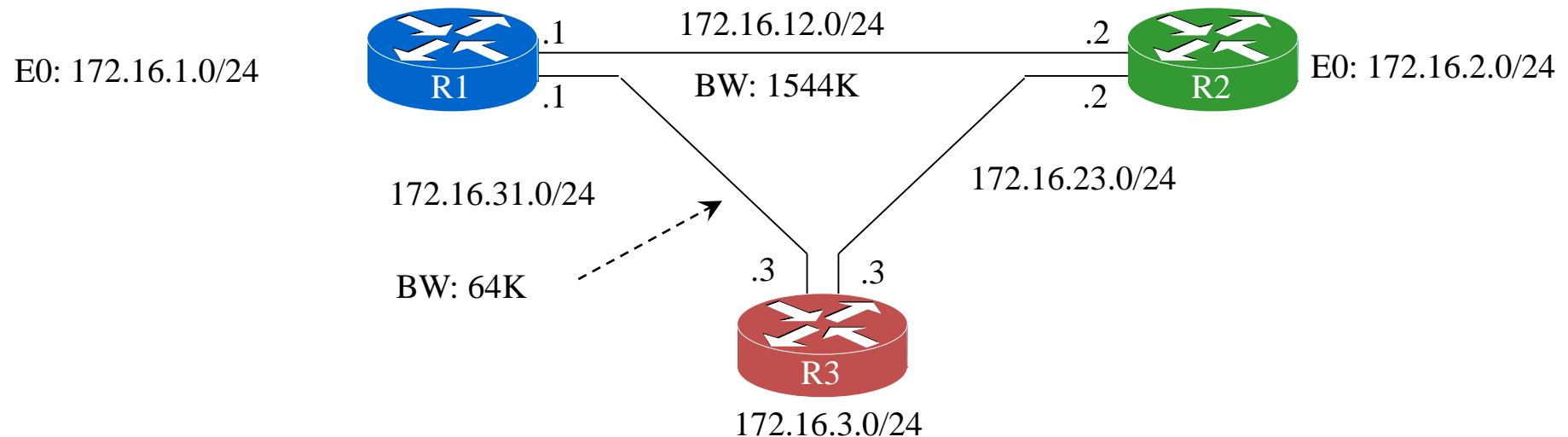
```
02:09:46:     subnet 172.16.2.0 metric 2
```

```
02:09:46:     subnet 172.16.12.0 metric 2
```

```
02:09:48: RIP: received v1 update from 172.16.12.2 on Serial0
```

```
02:09:48:     172.16.2.0 in 1 hops
```

RIP v1 Metric Value

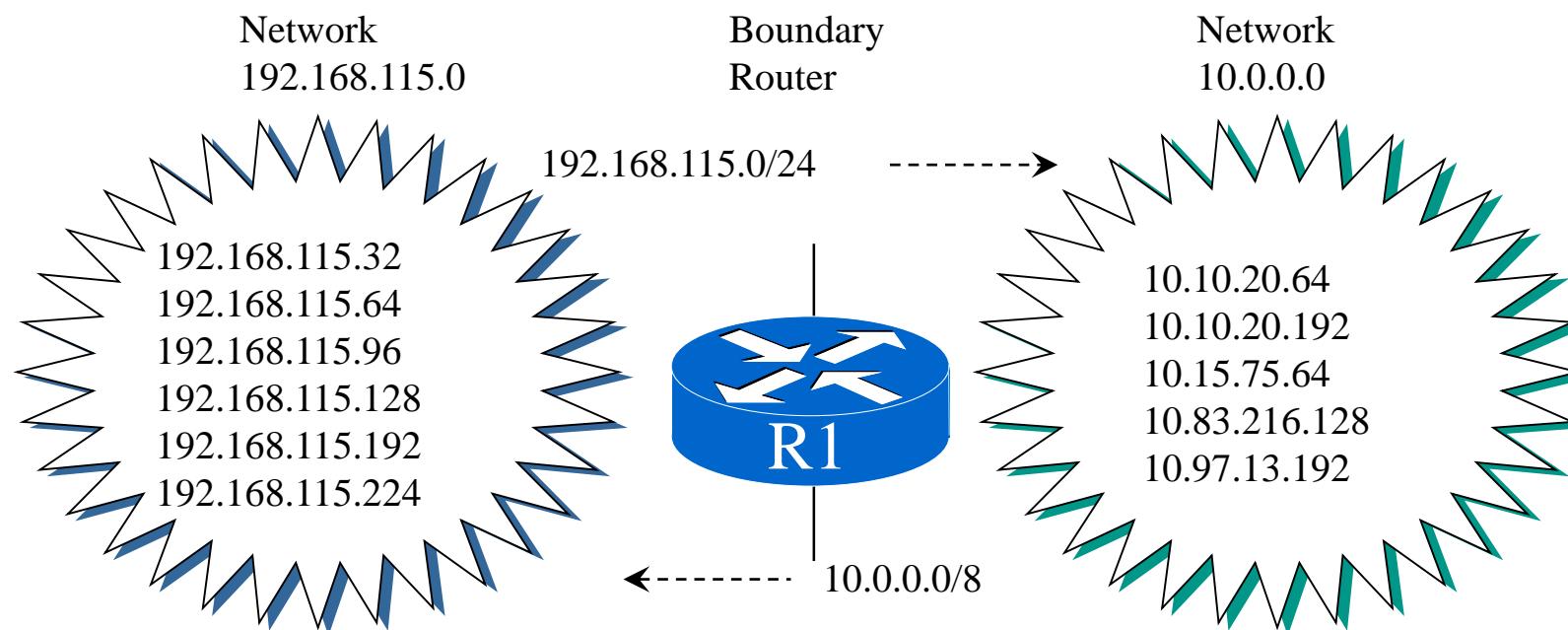


```
R1#sh ip route
```

```
172.16.0.0/24 is subnetted, 6 subnets
C 172.16.31.0 is directly connected, Serial1
R 172.16.23.0 [120/1] via 172.16.12.2, 00:00:22, Serial0
C 172.16.12.0 is directly connected, Serial0
C 172.16.1.0 is directly connected, Loopback0
R 172.16.2.0 [120/1] via 172.16.12.2, 00:00:22, Serial0
R 172.16.3.0 [120/1] via 172.16.12.2, 00:00:05, Serial0
R1#
```

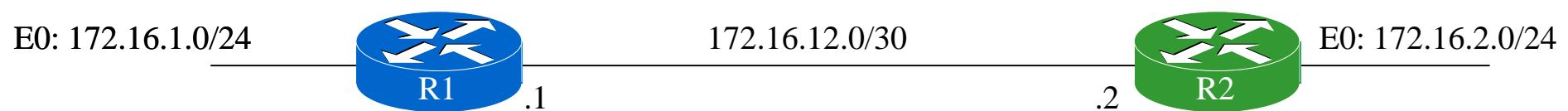
RIP v1과 Subnet Mask

Classful Routing Protocol은 Routing Update를 전송할 때 Subnet Mask까지 전송을 하지 않는다.



RIP v1과 Subnet Mask

전송되는 Interface의 major network가 같고 Subnet mask 길이가 다르면, 해당 정보를 전송하지 않는다.

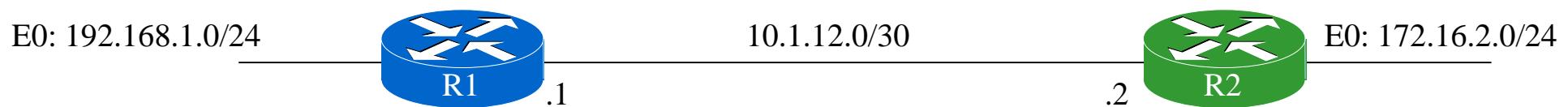


```
R1#debug ip rip
RIP protocol debugging is on
R1#
RIP: sending v1 update to 255.255.255.255 via Ethernet0 (172.16.1.1) suppressing null update
RIP: sending v1 update to 255.255.255.255 via Serial0 (172.16.12.1) suppressing null update
```

```
R2#debug ip rip
RIP protocol debugging is on
R2#
RIP: sending v1 update to 255.255.255.255 via Ethernet0 (172.16.2.1) suppressing null update
RIP: sending v1 update to 255.255.255.255 via Serial0 (172.16.12.2) suppressing null update
```

RIP v1과 Subnet Mask

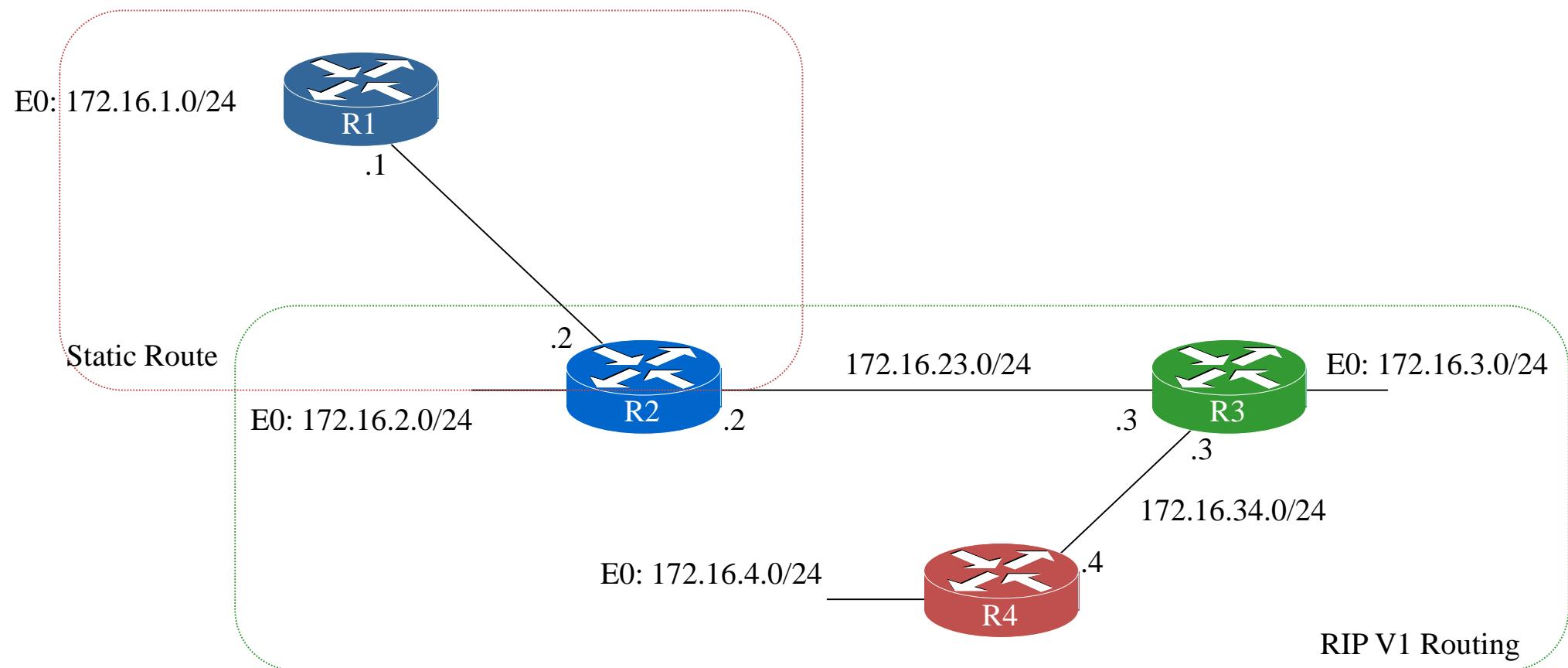
전송되는 Interface의 major network가 다를 경우 자동적으로 summary을 하여 전송을하게 된다.



```
R1#debug ip rip
RIP protocol debugging is on
R1#
RIP: sending v1 update to 255.255.255.255 via Ethernet0 (192.168.1.1)
RIP: build update entries
    network 172.16.0.0 metric 2
    network 10.0.0.0 metric 1
RIP: sending v1 update to 255.255.255.255 via Serial0 (10.1.12.1)
RIP: build update entries
    network 192.168.1.0 metric 1
```

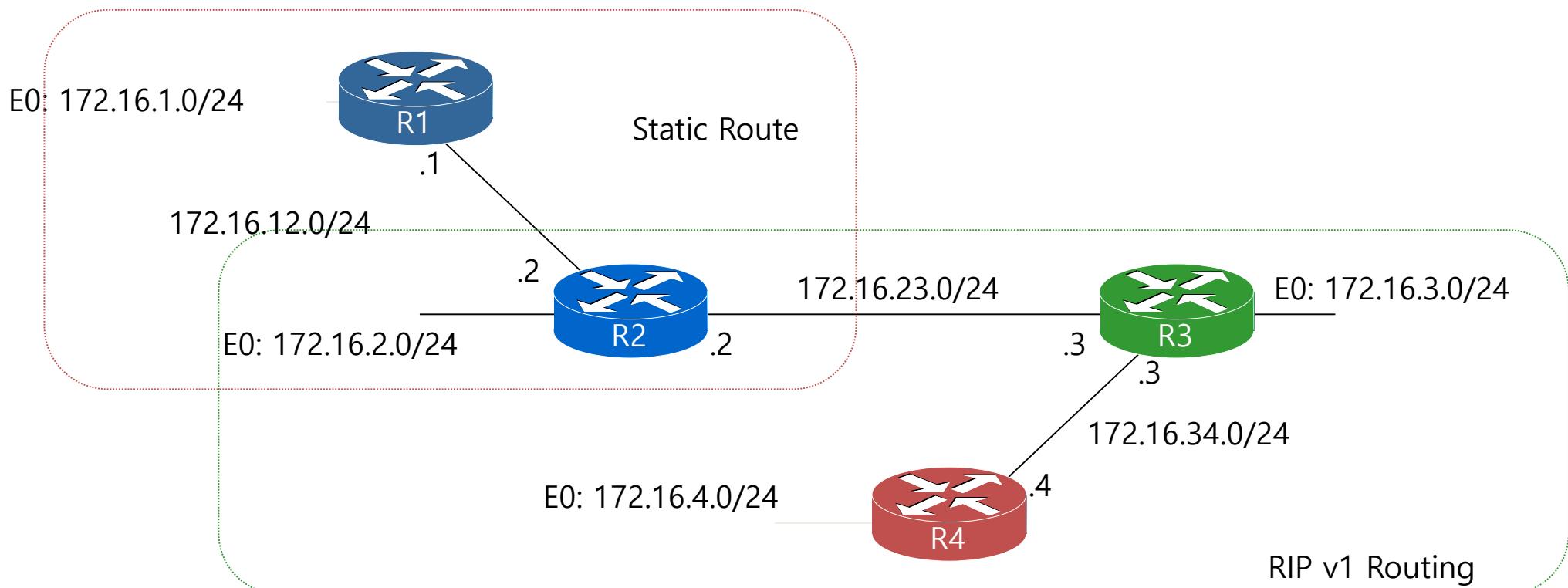
RIP v1과 Default Network

Default Network를 이용하여 Routing table의 크기를 줄 일 수가 있으며, 안정화를 시킬 수가 있다.



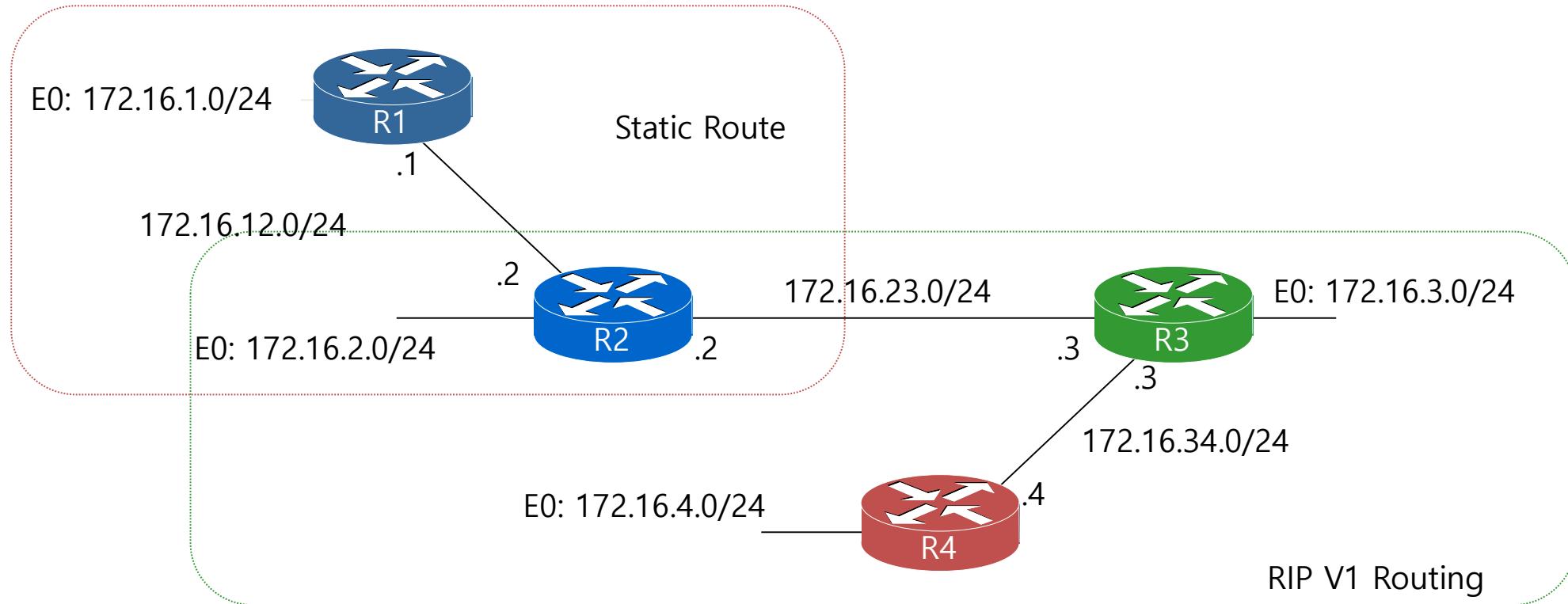
Default-information originate Command

Default-information originate는 RIP 설정모드에서 사용할 수 있으며, Neighbor로 Default Route를 전송하게 된다.



```
R2(config)#router rip  
R2(config-router)#default-information originate
```

Default-information originate Command



```
R3#sh ip route rip
 172.16.0.0/24 is subnetted, 6 subnets
 R    172.16.12.0 [120/1] via 172.16.23.2, 00:00:02, Serial0
 R    172.16.4.0 [120/1] via 172.16.34.4, 00:00:08, Serial1
 R    172.16.2.0 [120/1] via 172.16.23.2, 00:00:02, Serial0
 R*   0.0.0.0/0 [120/1] via 172.16.23.2, 00:00:02, Serial0
R3#
```

RIP v2 개요

RIP v2는 RIP v1의 문제점을 개선하여 만든 라우팅 프로토콜이다.

- ❖ RIP v2는 Classless Routing Protocol이다.
- ❖ RIP v2는 목적지주소로 Multicast Address 224.0.0.9를 사용한다.
- ❖ RIP v2는 Authentication을 할 수 있다.
- ❖ RIP v2는 Auto Summary를 비활성화 할 수 있다.

RIP v2 Configuration

RIP V2는 RIP V1과 설정방법이 비슷하며, RIP 설정모드에서 "version 2"라고 지정을 해 주면 된다.

[RIP V2 Command type]

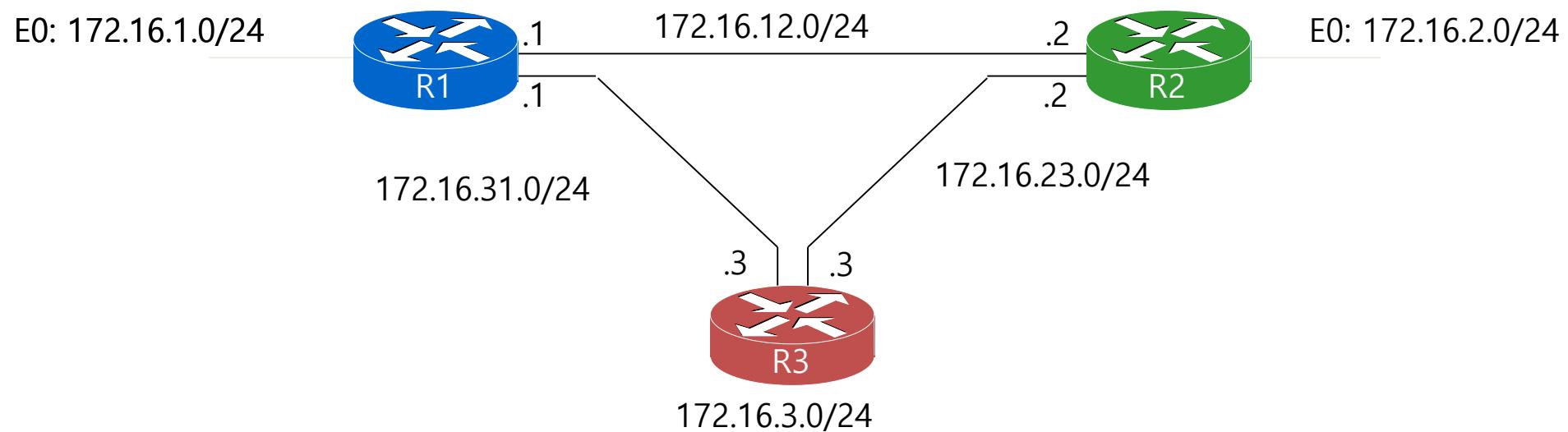
```
Router(config)#router rip  
Router(config-router)#version 2  
Router(config-router)#network network_number
```

[RIP V1, V2 Command type]

```
Router(config)#int s0  
Router(config-if)#ip rip send version 1 2  
Router(config-if)#ip rip receive version 2
```

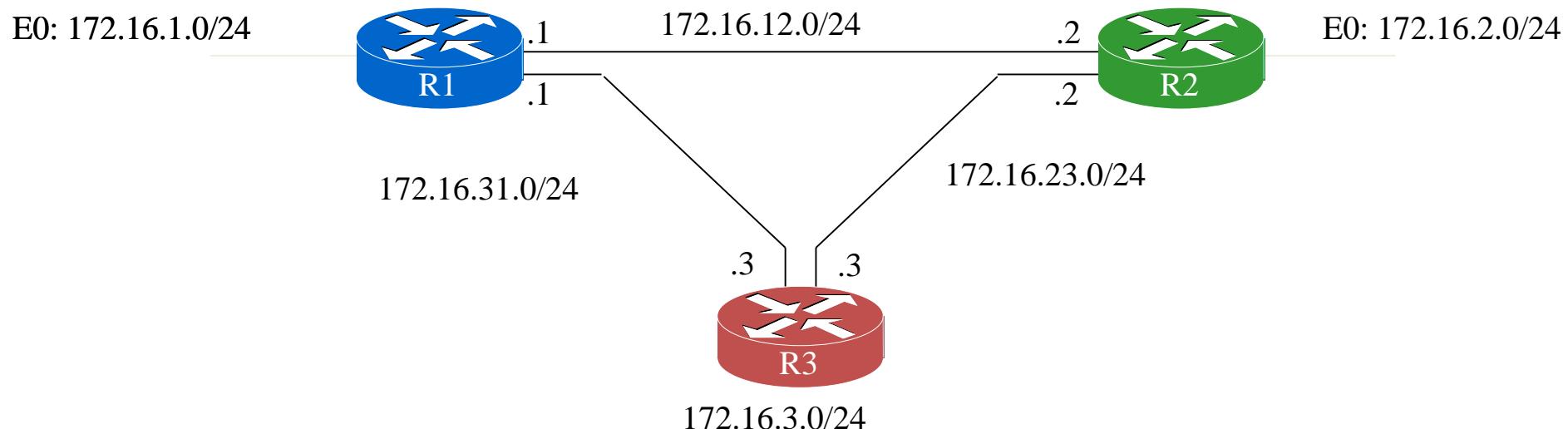
RIP v2 Configuration

RIP 설정모드에서 Version 2 명령어를 사용하여 간단하게 RIP V2를 설정해 보도록 하자.



```
R1(config)#router rip  
R1(config-router)#version 2  
R1(config-router)#network 172.16.0.0
```

RIP v2 Configuration



02:18:01: RIP: received v2 update from 172.16.12.2 on Serial0

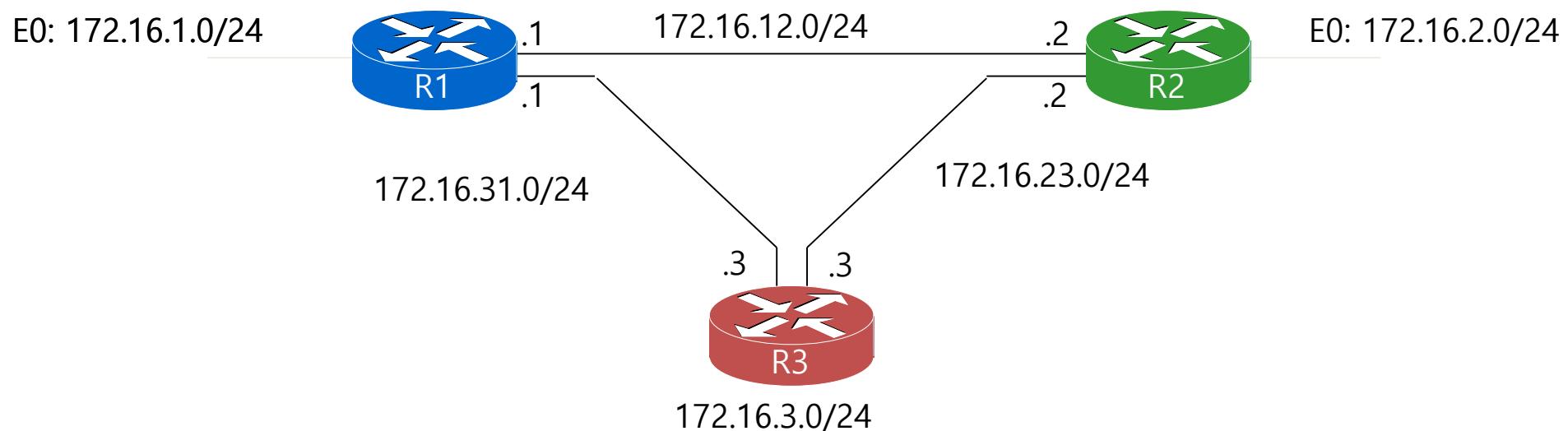
02:18:01: 172.16.2.0/24 via 0.0.0.0 in 1 hops
02:18:01: 172.16.3.0/24 via 0.0.0.0 in 2 hops
02:18:01: 172.16.23.0/24 via 0.0.0.0 in 1 hops

02:18:02: RIP: sending v2 update to 224.0.0.9 via Serial1 (172.16.31.1)

02:18:02: RIP: build update entries
02:18:02: 172.16.1.0/24 via 0.0.0.0, metric 1, tag 0
02:18:02: 172.16.2.0/24 via 0.0.0.0, metric 2, tag 0
02:18:02: 172.16.3.0/24 via 0.0.0.0, metric 3, tag 0
02:18:02: 172.16.12.0/24 via 0.0.0.0, metric 1, tag 0
02:18:02: 172.16.23.0/24 via 0.0.0.0, metric 2, tag 0

RIP v1, v2 Configuration

R1과 R3 Router는 RIP V1으로만 통신을 하며, 나머지는 모두 RIP v2로 설정해 보도록 하자.



```
R1(config)#int s1
R1(config-if)#ip rip send version 1
R1(config-if)#ip rip receive version 1
R1(config-if)#int s0
R1(config-if)#ip rip send version 2
R1(config-if)#ip rip receive version 2
```

RIP v1, v2 Debugging

02:39:52: RIP: sending v2 update to 224.0.0.9 via Serial0 (172.16.12.1)

02:39:52: RIP: build update entries

02:39:52: 172.16.1.0/24 via 0.0.0.0, metric 1, tag 0

02:39:52: 172.16.3.0/24 via 0.0.0.0, metric 2, tag 0

02:39:52: 172.16.31.0/24 via 0.0.0.0, metric 1, tag 0

02:39:52: RIP: sending v1 update to 255.255.255.255 via Serial1 (172.16.31.1)

02:39:52: RIP: build update entries

02:39:52: subnet 172.16.1.0 metric 1

02:39:52: subnet 172.16.2.0 metric 2

02:39:52: subnet 172.16.12.0 metric 1

02:39:58: RIP: received v2 update from 172.16.12.2 on Serial0

02:39:58: 172.16.2.0/24 via 0.0.0.0 in 1 hops

02:39:58: 172.16.3.0/24 via 0.0.0.0 in 2 hops

02:39:58: 172.16.23.0/24 via 0.0.0.0 in 1 hops

02:40:03: RIP: received v1 update from 172.16.31.3 on Serial1

02:40:03: 172.16.2.0 in 2 hops

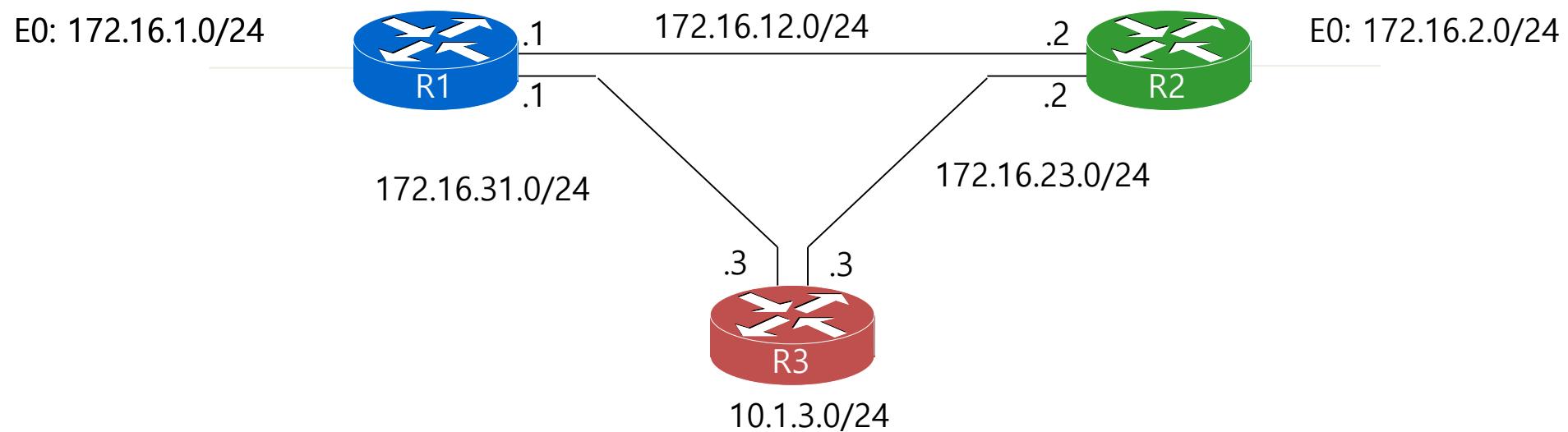
02:40:03: 172.16.3.0 in 1 hops

02:40:03: 172.16.23.0 in 1 hops

R1#

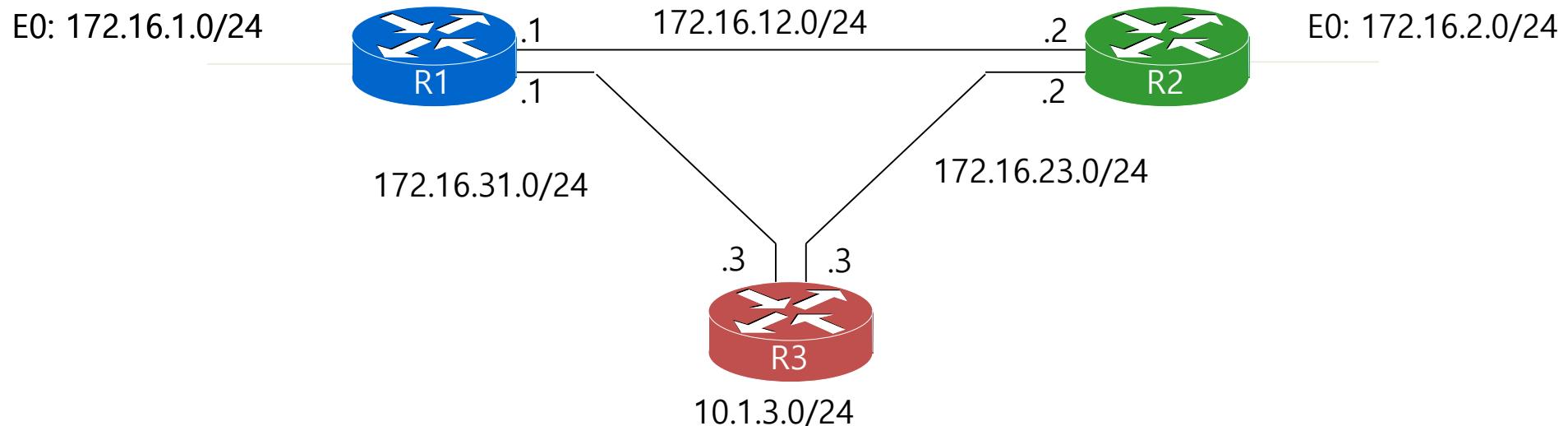
RIP v2 Summary

RIP V2는 RIP V1과 다르게 Auto Summary 기능을 비활성화할 수가 있다.



```
R1(config)#router rip  
R1(config-router)#no auto-summary
```

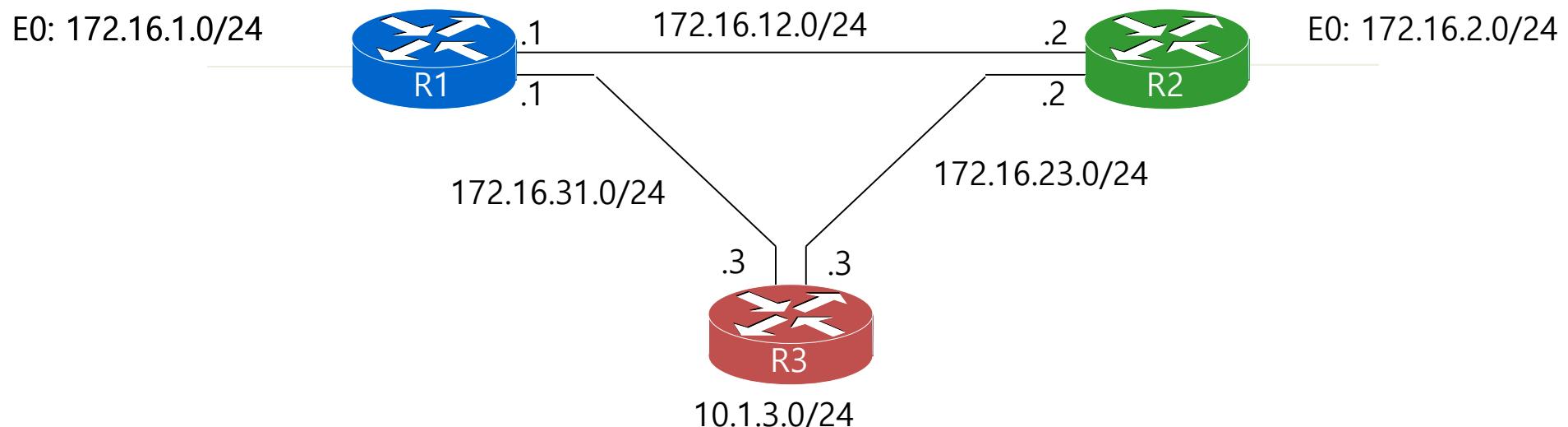
RIP v2 Summary



```
R2#sh ip route
```

```
172.16.0.0/24 is subnetted, 5 subnets
R    172.16.31.0 [120/1] via 172.16.12.1, 00:00:18, Serial0
                  [120/1] via 172.16.23.3, 00:00:17, Serial1
R    172.16.1.0 [120/1] via 172.16.12.1, 00:00:18, Serial0
R    10.0.0.0/8 [120/1] via 172.16.23.3, 00:00:17, Serial1
R2#
```

RIP v2 Summary



```
R2#sh ip route
```

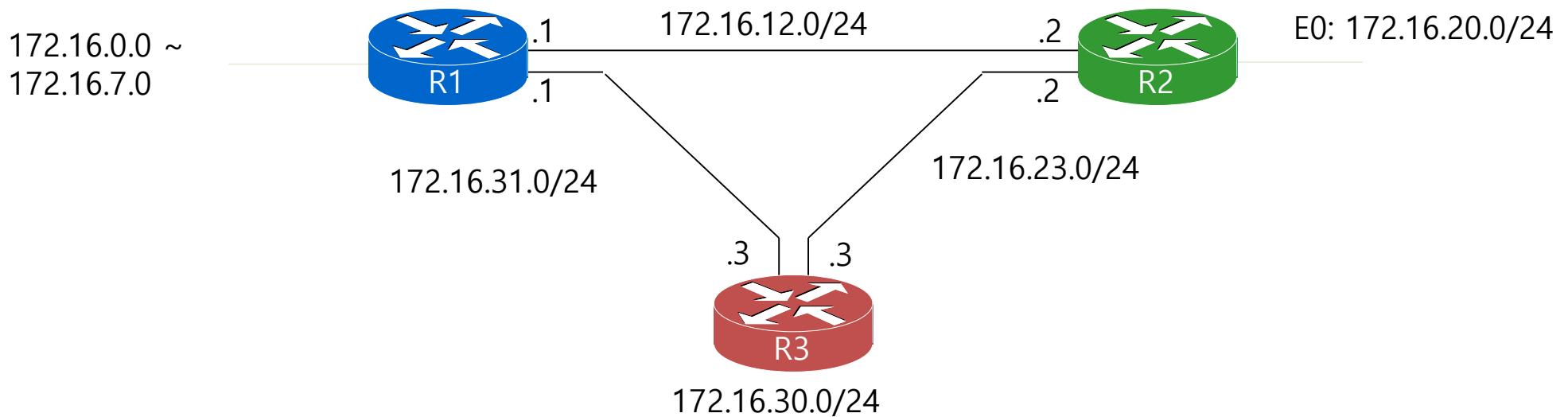
```
172.16.0.0/24 is subnetted, 5 subnets
R    172.16.31.0 [120/1] via 172.16.23.3, 00:00:03, Serial1
                  [120/1] via 172.16.12.1, 00:00:17, Serial0
R    172.16.1.0  [120/1] via 172.16.12.1, 00:00:17, Serial0

10.0.0.0/24 is subnetted, 1 subnets
R    10.1.3.0 [120/1] via 172.16.23.3, 00:00:03, Serial1
```

```
R2#
```

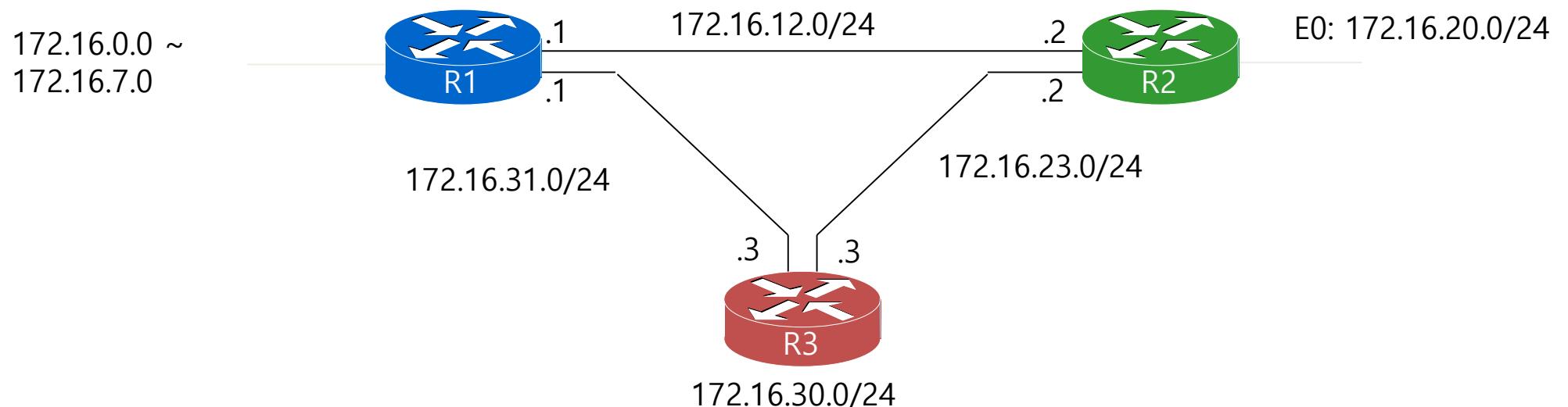
RIP v2 수동 Summary

RIP V2는 네트워크 관리자가 직접 명령어를 사용하여 수동으로 Summary를 할 수가 있다.



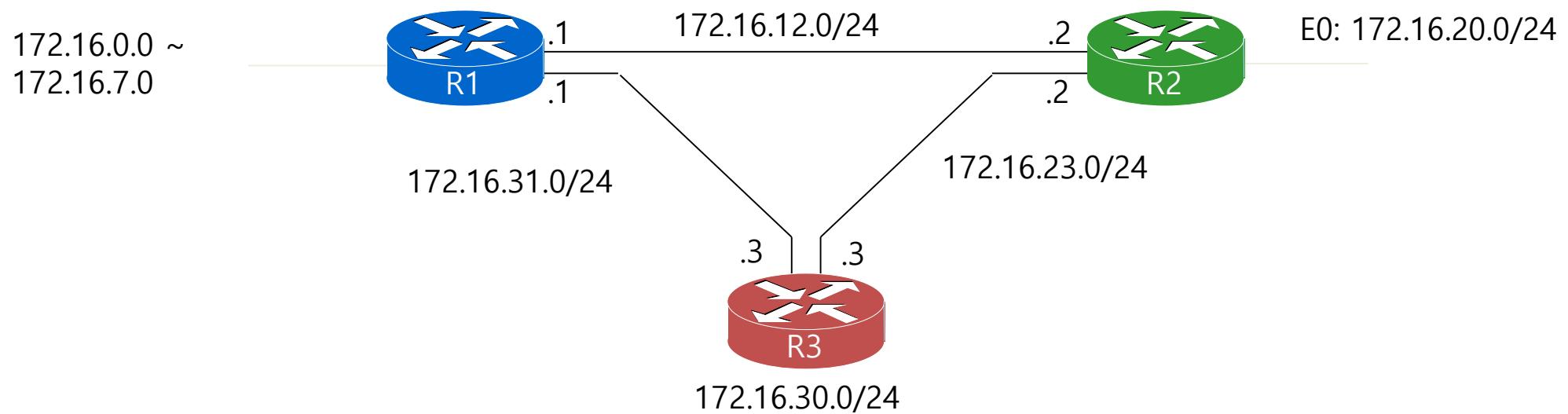
```
R1(config)#int s0
R1(config-if)#ip summary-address rip network_number subnet_mask
```

RIP v2 수동 Summary



```
R2#sh ip route
 172.16.0.0/24 is subnetted, 12 subnets
R  172.16.30.0 [120/1] via 172.16.23.3, 00:00:04, Serial1
R  172.16.31.0 [120/1] via 172.16.23.3, 00:00:04, Serial1
              [120/1] via 172.16.12.1, 00:00:07, Serial0
R  172.16.4.0 [120/1] via 172.16.12.1, 00:00:07, Serial0
R  172.16.5.0 [120/1] via 172.16.12.1, 00:00:07, Serial0
R  172.16.6.0 [120/1] via 172.16.12.1, 00:00:07, Serial0
R  172.16.7.0 [120/1] via 172.16.12.1, 00:00:07, Serial0
R  172.16.1.0 [120/1] via 172.16.12.1, 00:00:07, Serial0
R  172.16.2.0 [120/1] via 172.16.12.1, 00:00:07, Serial0
R  172.16.3.0 [120/1] via 172.16.12.1, 00:00:07, Serial0
R2#
```

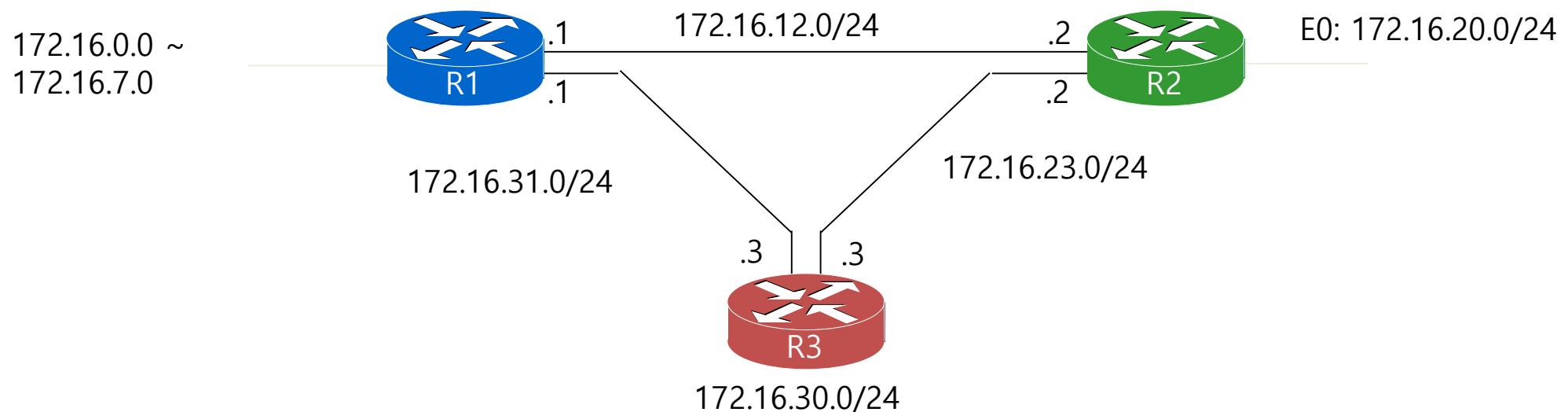
RIP v2 수동 Summary



```
R1(config)#int s0
R1(config-if)#ip summary-address rip 172.16.0.0 255.255.248.0
```

```
R1(config)#int s1
R1(config-if)#ip summary-address rip 172.16.0.0 255.255.248.0
```

RIP v2 수동 Summary



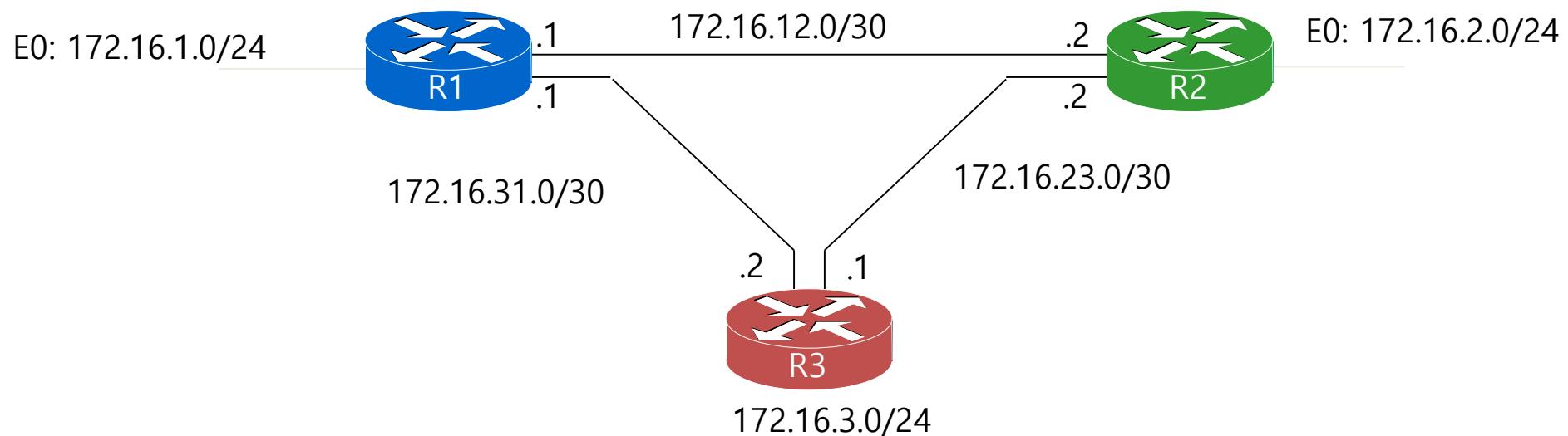
```
R2#sh ip route
```

```
172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
```

```
R 172.16.30.0/24 [120/1] via 172.16.23.3, 00:00:03, Serial1
R 172.16.31.0/24 [120/1] via 172.16.23.3, 00:00:03, Serial1
[120/1] via 172.16.12.1, 00:00:15, Serial0
R 172.16.0.0/21 [120/1] via 172.16.12.1, 00:00:15, Serial0
R2#
```

RIP v2 VLSM

RIP v2는 Classless Routing Protocol이기 때문에 서로 다른 subnet mask를 사용하는 VLSM (Variable Length Subnet Mask)를 사용할 수가 있다.



EIGRP 소개



■ EIGRP Support :

- Network Topology 변화에 수렴 시간이 빠르다.
- Multiple Routed Protocol (IP, IPX, Apple talk)을 지원한다.
- EIGRP는 Auto Summary 및 Manual Summary를 지원한다.
- 정상 운용 중에 적은 Network 자원을 이용해 Routing Table을 유지한다.
- Classless Routing 지원

EIGRP 특징

- 시스코 전용(Cisco Proprietary) Routing Protocol이다.
- Hybrid Protocol이다.:
 - Link State와 Distance Vector Routing Protocol의 장점을 결합했다.
 - Advanced Distance Vector Routing Protocol이다.
- 빠른 수렴: Rapid Convergence와 라우팅 루프 방지를 위하여 DUAL(Diffusing Update Algorithm)을 사용한다.
- Bandwidth 적게 사용한다.
 - 주기적인 업데이트를 하지 않는다.
 - Destination에 대한 Path나 Metric에 변화가 있을 때만(Incremental update) 즉시 Partial Update를 한다.

EIGRP 패킷

▶ Hello :

- 네이버관계를 형성하기 위해 사용.
- Ack 번호를 0을 가지고 multicast (224.0.0.10)

▶ Update :

- 라우팅 업데이트를 보낼 때 사용
- New neighbor 발견 시 topology table 동기화 : unicast
- Topology Change 발견 시 : multicast

▶ Query :

- 라우팅 정보에 대해 네이버에게 물어볼 때 사용 : 항상 multicast

▶ Reply :

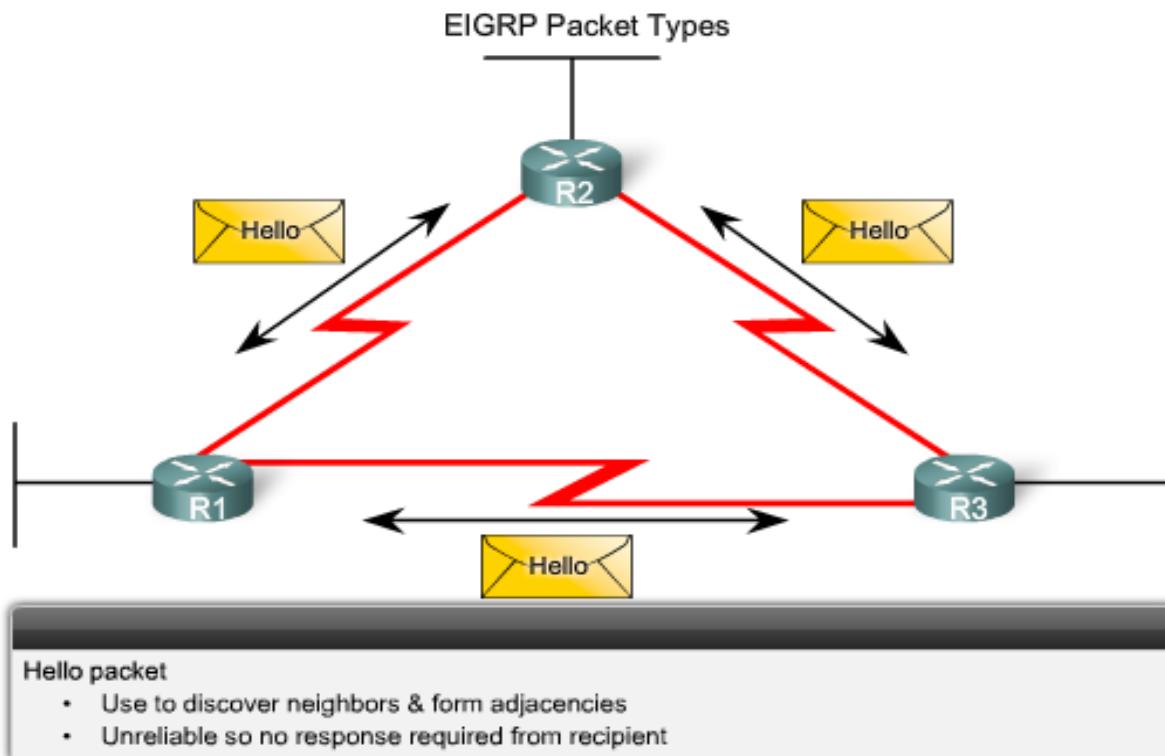
- 라우팅 정보에 대한 Query에 응답할 때 사용 : unicast

▶ ACK :

- 신뢰를 요구하는 패킷들(update, query, reply)에 대한 확인.
- Nonzero ack 번호를 가진 unicast

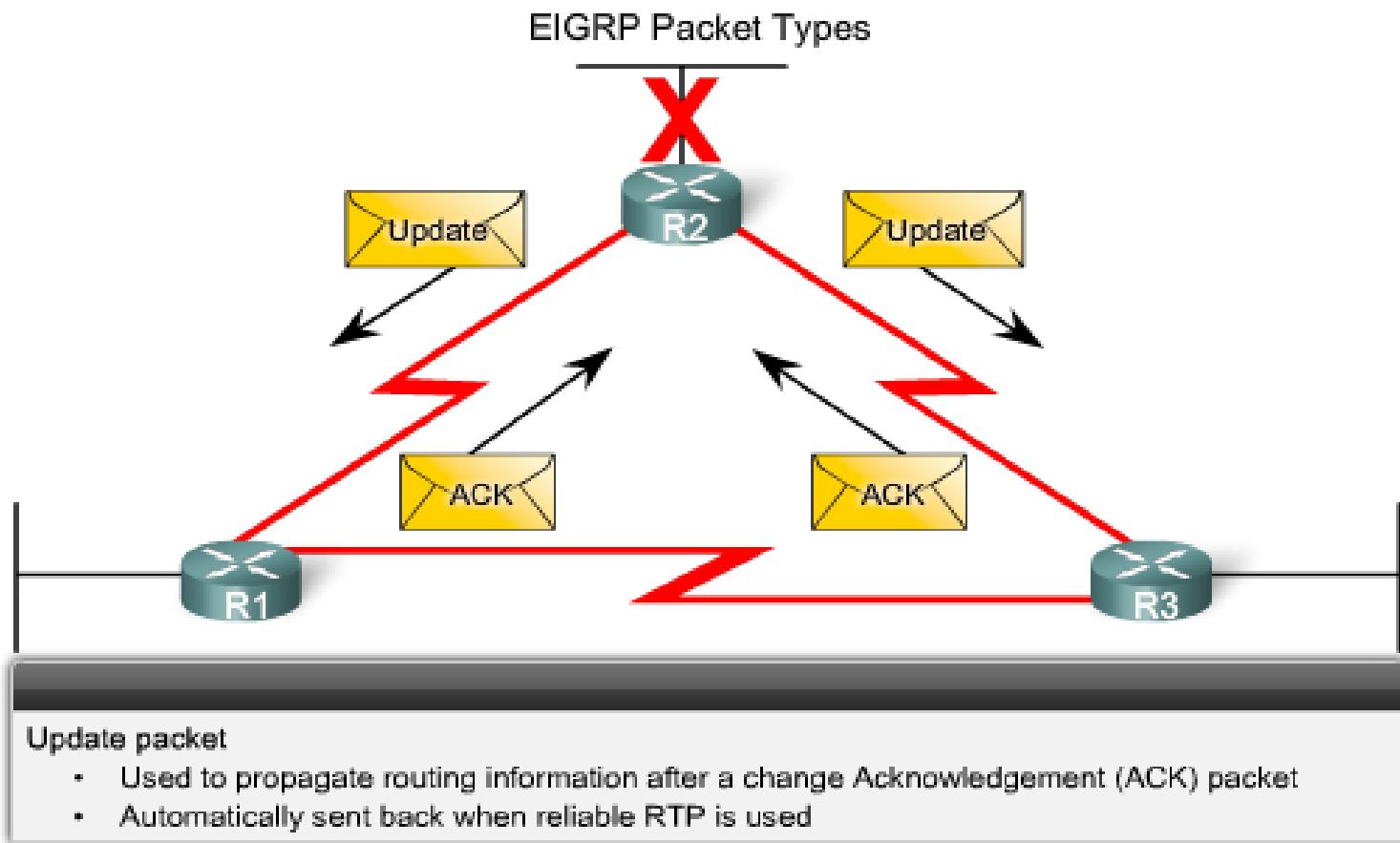
EIGRP 패킷

- **Hello 패킷**
 - 네이버를 찾고 인접관계(adjacency)를 형성하기 위해



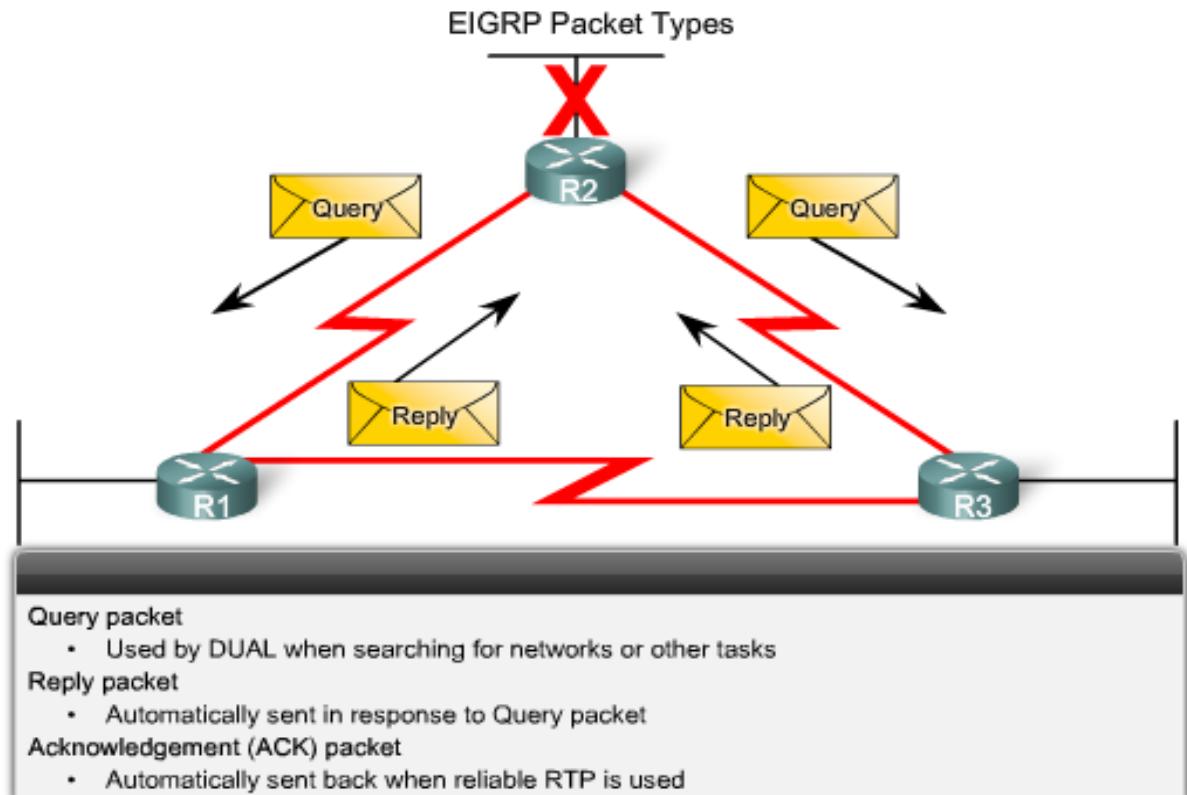
EIGRP 패킷

- **Update 패킷**
 - 라우팅 정보를 전파하기 위해 사용



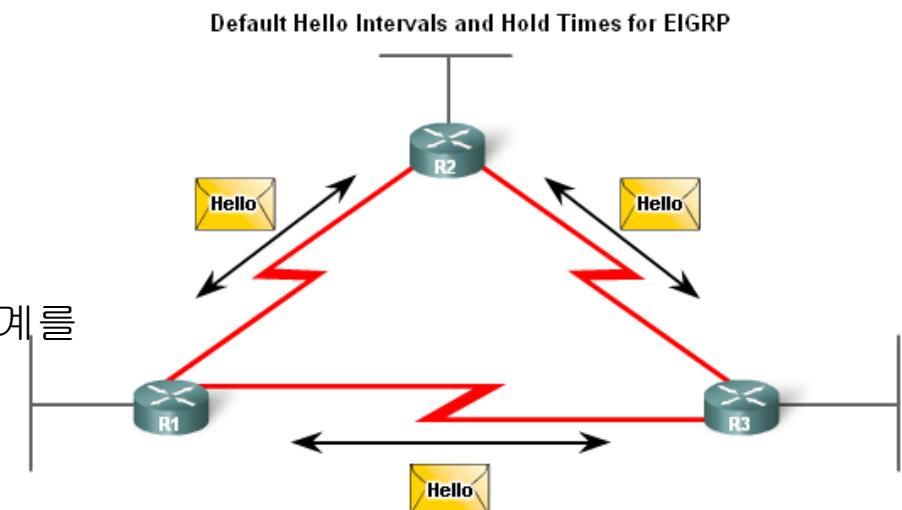
EIGRP 패킷

- **Query 패킷**
 - 네트워크를 찾기 위해 DUAL에 의해 사용됨.
 - Unicast 또는 Multicast
- **Reply 패킷**
 - Query에 대한 응답 packet
 - Unicast
- **Acknowledgement 패킷**
 - Update, Query, Reply 패킷을 받았다는 확인을 하기 위해 사용



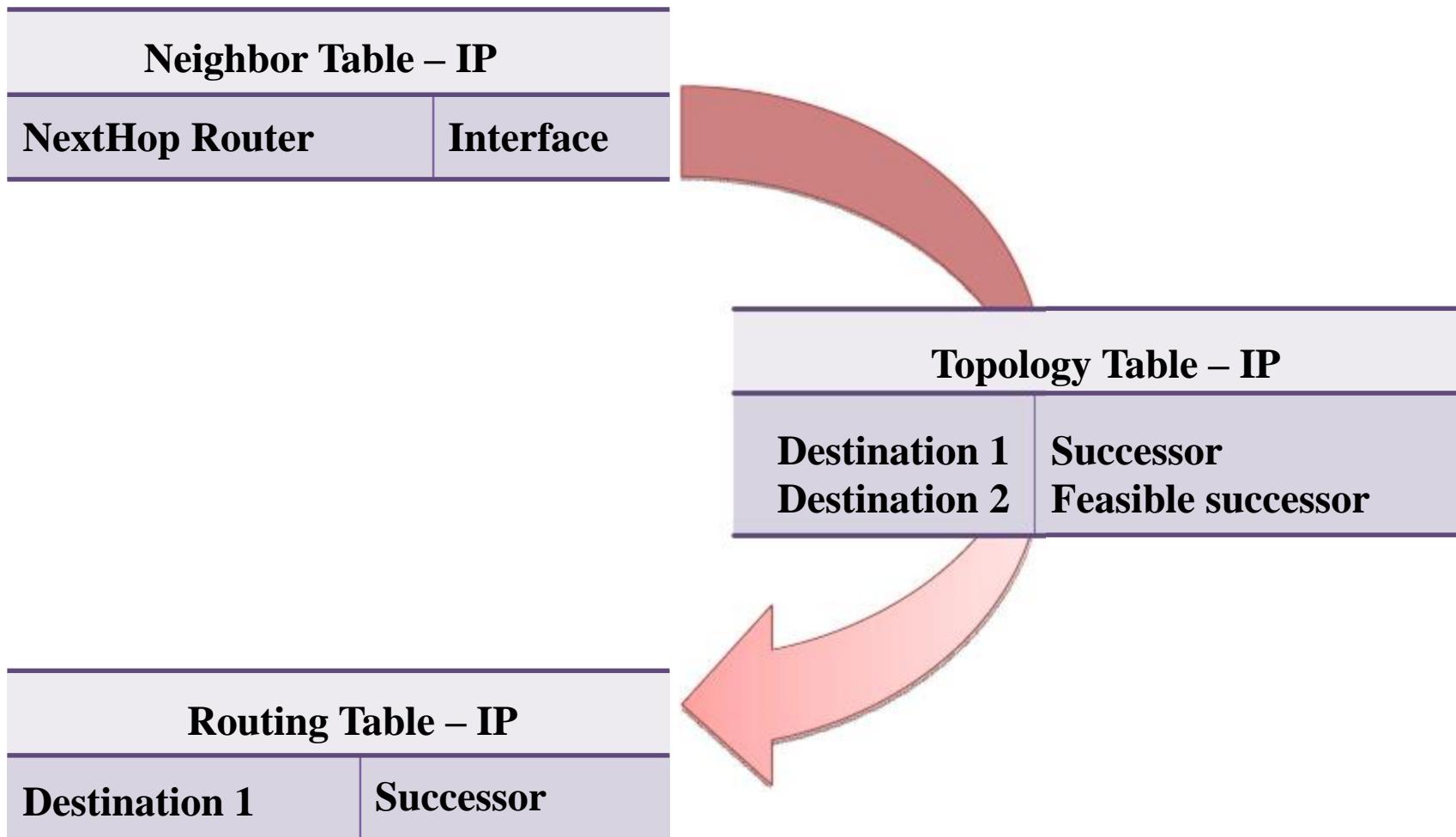
EIGRP 패킷

- **Hello 패킷의 목적**
 - 네이버 라우터를 찾고 인접(adjacency) 관계를 형성하기 위해서.
- **Hello 패킷의 특징**
 - Hello 패킷 주기
 - 대부분의 네트워크 : 매 5초
 - 멀티포인트 NMBA 네트워크 : 매 60초
 - Holdtime
 - Hello 패킷이 도착하지 않아도 네이버 관계를 유지하는 시간
 - 기본 holdtime
 - Hello 주기의 3배



Bandwidth	Example Link	Default Hello Interval	Default Hold Time
1.544 Mbps	Multipoint Frame Relay	60 seconds	180 seconds
Greater than 1.544 Mbps	T1, Ethernet	5 seconds	15 seconds

EIGRP 테이블



EIGRP 용어

Neighbor Table	EIGRP router는 인접 Router(직접 연결된 neighbor router)에 대한 table을 보유하여 인접 router간의 양방향 통신을 확립한다. 지원하는 프로토콜(IP, IPX, AppleTalk)별로 각각의 Neighbor Table을 유지한다
Topology Table	EIGRP router는 routing 정보교환에 의하여 알게 된 모든 네트워크에 대한 Topology Table을 유지한다. 지원하는 프로토콜 별로 각각의 Topology Table을 유지한다
Routing Table	EIGRP router는 Topology Table을 기초로 하여 Destination에 대한 최적의 경로를 routing table에 보유한다. 지원하는 프로토콜 별로 각각의 Routing Table을 유지한다
Successor route	Destination에 대한 Primary Route이다. Routing Table에 유지된다.
Feasible Successor route	Destination에 대한 Backup Route이다. Feasible Successor는 Successor와 동시에 선택되는데 Topology Table에 보유된다. Destination에 대해서 여러 개의 Feasible Successor를 보유할 수 있다

EIGRP – Metric 요소들

- 벡터 메트릭 (Vector metric) or 혼합 메트릭 (Composite metric)
 - 대역폭 (bandwidth) : 경로에서 가장 적은 대역폭
 - 지연 (delay) : 경로를 따라 누적한 인터페이스의 지연 시간 (누적 값/10)
 - 신뢰도 (Reliability) : 인터페이스의 에러 발생율
 - 부하 (load) : 인터페이스의 부하
 - MTU (Maximum transmission unit) : 경로의 Maximum Transfer Unit 값이다.
 - * 목적지까지 가는 각 인터페이스의 MTU 중 가장 작은 것이 선택한다.
 - EIGRP 의 흡 카운트는 기본적으로 100 이다. (show ip protocol로 확인)

EIGRP Metric 계산

- EIGRP Composite Metric과 K 값
 - EIGRP는 복합 메트릭으로 다음 값을 이용한다.
 - Bandwidth, delay, reliability, load
 - EIGRP에 의해 이용되는 복합 메트릭
 - 기본식은 다음 상수값을 갖는다.
 - $K_1 \& K_3 = 1$
 - all other K values = 0

EIGRP Composite Metric

Default Composite Formula:
 $\text{metric} = [K_1 * \text{bandwidth} + K_3 * \text{delay}]$

Complete Composite Formula:
 $\text{metric} = [K_1 * \text{bandwidth} + (K_2 * \text{bandwidth}) / (256 - \text{load}) + K_3 * \text{delay}] * [K_5 / (\text{reliability} + K_4)]$
(Not used if "K" values are 0)

Default values:
K1 (bandwidth) = 1
K2 (load) = 0
K3 (delay) = 1
K4 (reliability) = 0
K5 (reliability) = 0

} "K" values can be changed with the **metric weights** command.

```
Router(config-router) #metric weights tos k1 k2 k3 k4 k5
```

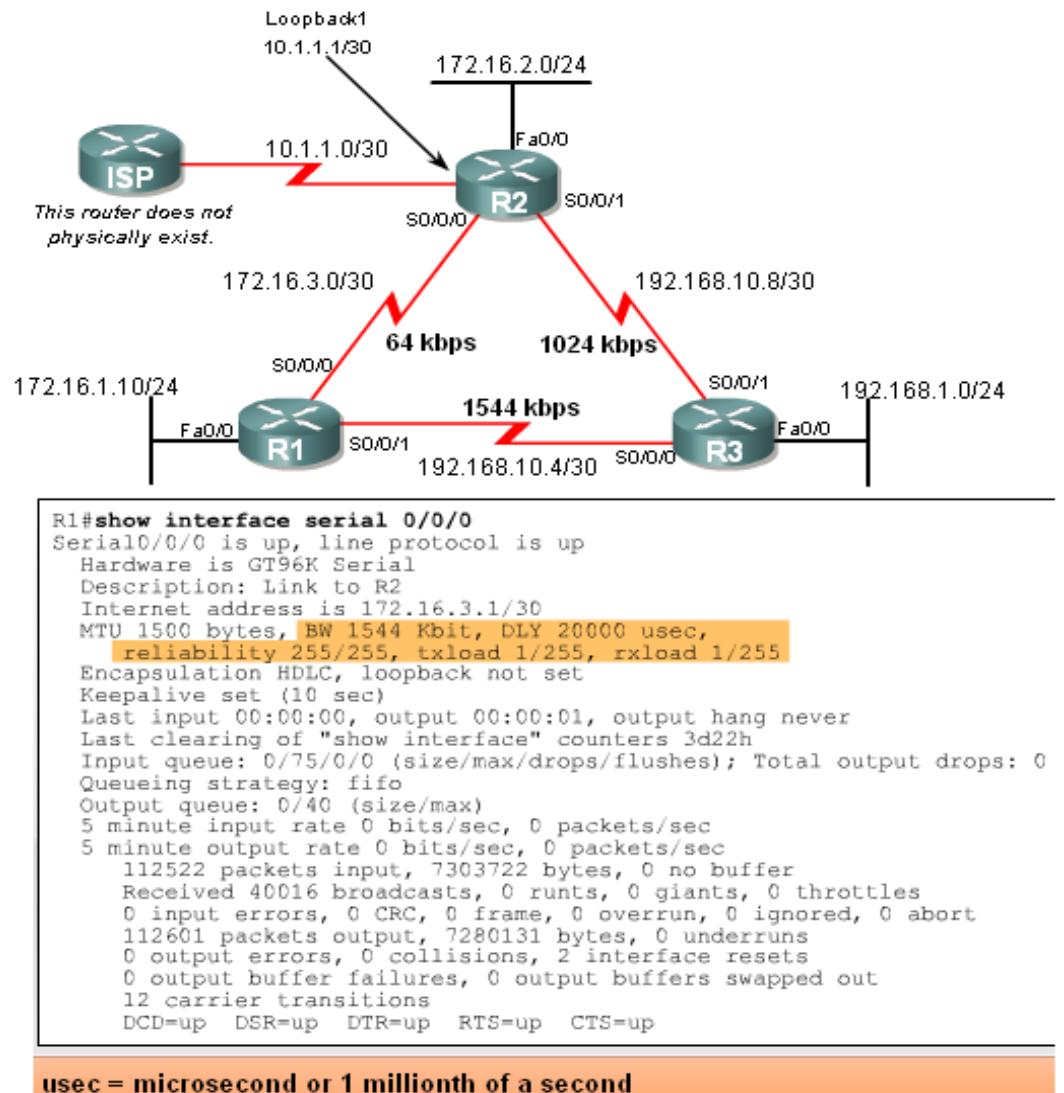
EIGRP Metric 계산

- show ip protocols 명령으로 K 상수값을 확인할 수 있다.

```
R1#show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.10.0/24 for FastEthernet0/0, Serial0/0/0
      Summarizing with metric 2169856
    172.16.0.0/16 for Serial0/0/1
      Summarizing with metric 28160
  Maximum path: 4
  Routing for Networks:
    172.16.0.0
    192.168.10.0
  Routing Information Sources:
    Gateway          Distance      Last Update
    (this router)      90          00:03:29
    192.168.10.6      90          00:02:09
    Gateway          Distance      Last Update
    172.16.3.2        90          00:02:12
  Distance: internal 90 external 170
```

EIGRP Metric 계산

- EIGRP 메트릭
 - **show interfaces** command 를 이용하여 메트릭 확인
 - EIGRP 메트릭
 - **Bandwidth** – EIGRP는 메트릭을 계산하기 위해 고정 bandwidth를 계산한다.
 - 대부분의 serial interface는 기본 bandwidth로 1.544Mbps(T1)가 설정되어 있다.



EIGRP Metric 계산

- EIGRP 메트릭
 - Delay는 패킷이 출발해서 돌아오는데 걸리는 시간을 나타낸다.
 - 연결된 인터페이스의 타입에 따라 기본적으로 고정값이 할당되어 있다.

Delay Values in Microseconds

Media	Delay
100M ATM	100 μs
Fast Ethernet	100 μs
FDDI	100 μs
1HSSI	20,000 μs
16M Token Ring	630 μs
Ethernet	1,000 μs
T1 (Serial Default)	20,000 μs
512K	20,000 μs
DSO	20,000 μs
56K	20,000 μs

EIGRP Metric 계산

- Reliability (기본 EIGRP metric 산출시 제외)
 - 링크가 실패할 가능성 측정
 - 1에서 255까지 나타낼 수 있으며 255일 때 신뢰도가 100%이다.
- Load (기본 EIGRP metric 산출시 제외)
 - 얼마나 많은 양의 트래픽이 링크를 사용하는지를 나타내는 숫자
 - 1에서 255까지 나타낼 수 있으며 1일 때 부하가 가장 적음을 나타낸다.

Reliability and Load Values

```
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec,
```

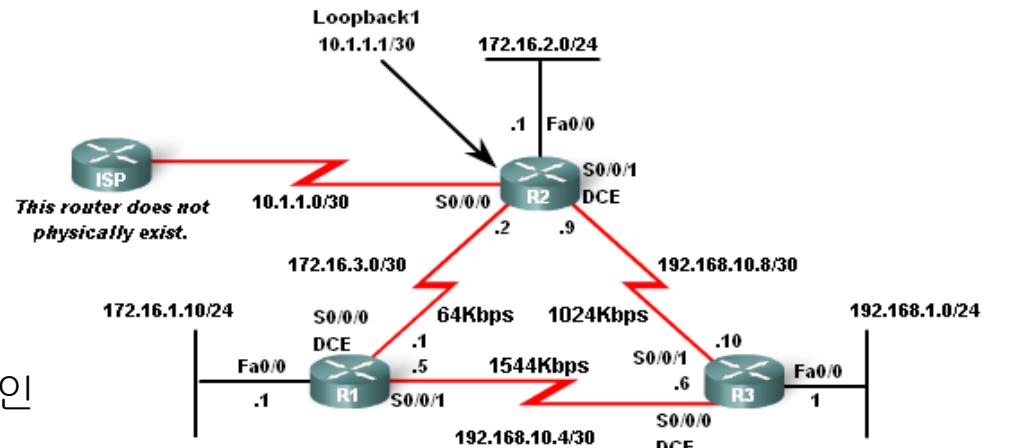
```
reliability 255/255, txload 1/255, rxload 1/255
```

Reliability Value

Load Value

EIGRP Metric 계산

- Bandwidth Command
 - interface bandwidth 변경하기
 - **bandwidth** command 사용
 - 예)
 - Router(config-if)#**bandwidth** kilobits
 - bandwidth 확인하기
 - **show interface** command 사용
 - 참고 – bandwidth command가 링크의 물리적인 bandwidth를 변경하는 것은 아니다.



The bandwidth Command

```
R1(config)#inter s 0/0/0
R1(config-if)#bandwidth 64
```



```
R2(config)#inter s 0/0/0
R2(config-if)#bandwidth 64
R2(config)#inter s 0/0/1
R2(config-if)#bandwidth 1024
```



```
R3(config)#inter s 0/0/1
R3(config-if)#bandwidth 1024
```

Verifying Bandwidth Value

```
R2#show interface serial 0/0/0
Serial0/0/0 is up, line protocol is up
Hardware is PowerQUICC Serial
Internet address is 172.16.3.2/30
MTU 1500 bytes, BW 64 Kbit, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
<some output omitted>
```

Note: The actual bandwidth of the link between R1 and R3 matches the default value for serial interfaces (1544 kbps).

EIGRP Metric 계산

- EIGRP metric는 bandwidth와 delay에 의해 결정된다.

Calculating the EIGRP Default Metric

Default metric = [K1*bandwidth + K3*delay]

Since K1 and K3 both equal 1, the formula simplifies to: **bandwidth + delay**

bandwidth = speed of slowest link in route to the destination

delay = sum of the delays of each link in route to the destination

Slowest bandwidth: $(10,000,000/\text{bandwidth kbps}) * 256$

Plus the sum of the delays $+ (\text{sum of delay}/10) * 256$

$= \text{EIGRP metric}$

```
R2#show ip route
<output omitted>
D    192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:02:14, Serial0/0/1
```

EIGRP Metric 계산

- EIGRP는 메트릭 계산시에 가장 낮은 bandwidth (BW)를 사용한다.
 - Calculated BW = reference BW / lowest BW(kbps)
- Delay는 EIGRP는 경로상의 모든 링크의 지연값을 합한다.
 - Calculated Delay = the sum of outgoing interface delays
- EIGRP Metric = calculated BW + calculated delay

EIGRP Metric 계산

Finding the Slowest Bandwidth

```
R2#show inter ser 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 192.168.10.9/30
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec,
<remaining output omitted>
```

```
R3#show inter fa 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0002.b9ee.5ee0 (bia 0002.b9ee.5ee0)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<remaining output omitted>
```

$$\text{bandwidth} = (10,000,000/1024) = 9765 * 256 = 2499840$$

Summing the Delays

```
R2#show inter ser 0/0/1
Serial0/0/1 is up, line protocol is up
  Hardware is PowerQUICC Serial
  Internet address is 192.168.10.9/30
  MTU 1500 bytes, BW 1024 Kbit, DLY 20000 usec,
<remaining output omitted>

<remaining output omitted>
```

```
R3#show inter fa 0/0
FastEthernet0/0 is up, line protocol is up
  Hardware is AmdFE, address is 0002.b9ee.5ee0 (bia 0002.b9ee.5ee0)
  Internet address is 192.168.1.1/24
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
<remaining output omitted>
```

$$\text{delay} = [(20000/10) + (100/10)] * 256 = 514560$$

$$\text{EIGRP Metric} = \text{bandwidth} + \text{delay} = 2499840 + 514560 = 3014400$$

```
R2#show ip route
<code output omitted>

Gateway of last resort is not set

      192.168.10.0/24 is variably subnetted, 3 subnets, 2 masks
D        192.168.10.0/24 is a summary, 00:00:15, Null0
D        192.168.10.4/30 [90/21024000] via 192.168.10.10, 00:00:15, Serial0/0/1
C        192.168.10.8/30 is directly connected, Serial0/0/1
      172.16.0.0/16 is variably subnetted, 4 subnets, 3 masks
D        172.16.0.0/16 is a summary, 00:00:15, Null0
D        172.16.1.0/24 [90/40514560] via 172.16.3.1, 00:00:15, Serial0/0/0
C        172.16.2.0/24 is directly connected, FastEthernet0/0
C        172.16.3.0/30 is directly connected, Serial0/0/0
      10.0.0.0/30 is subnetted, 1 subnets
C          10.1.1.0 is directly connected, Loopback1
D        192.168.1.0/24 [90/3014400] via 192.168.10.10, 00:00:15, Serial0/0/1
```

EIGRP 설정하기

- EIGRP 설정

```
Router(config)#router eigrp autonomous-system  
Router(config-router)#  
Router(config-router)#{
```

- network command를 이용하여 Network 광고하기

```
Router(config-router)# network network-number  
Router(config-router)# network network-number wildcard-mask  
Router(config-router)# network network-number subnet-mask  
Router(config-router)# network int-address 0.0.0.0
```

EIGRP 설정 확인하기

- Neighbor Table 확인

```
Router# sh ip eigrp neighbors
```

- Topology Table 확인

```
Router# sh ip eigrp topology
```

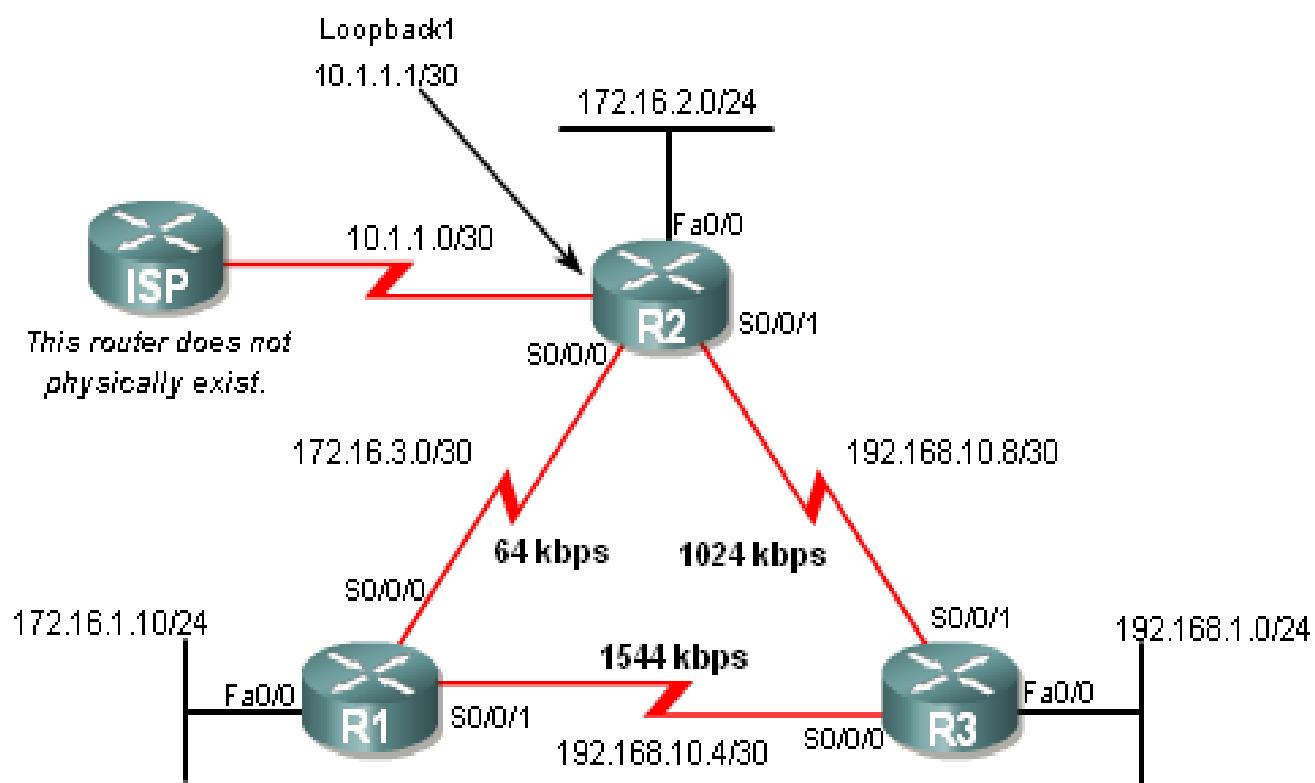
- Topology Table 확인 - 모든 토폴로지 데이터 확인

```
Router# sh ip eigrp topology all-links
```

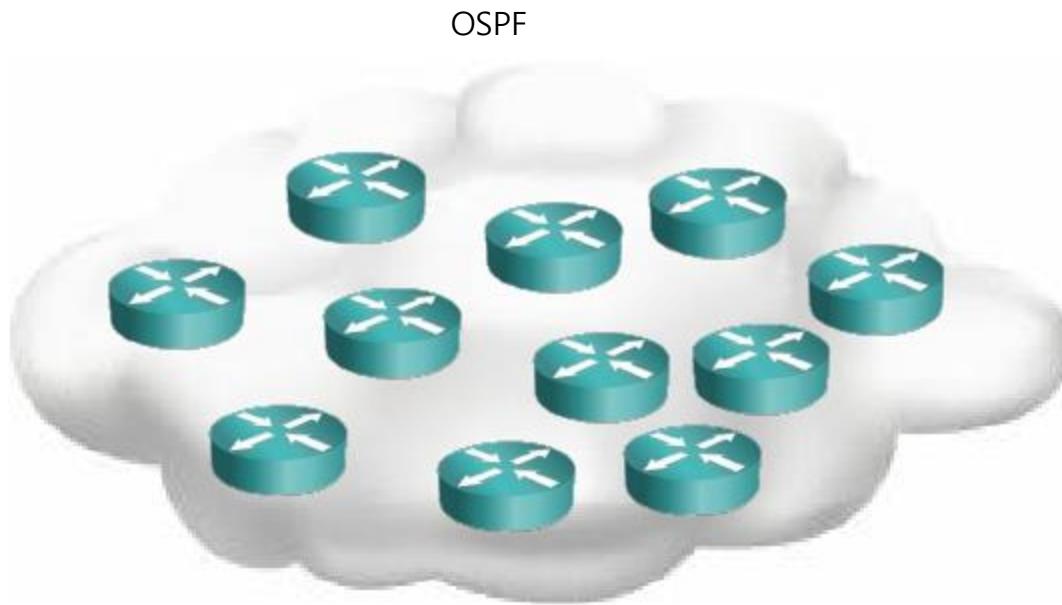
- Routing Table 확인

```
Router# sh ip route eigrp
```

EIGRP 설정 Lab



OSPF 소개

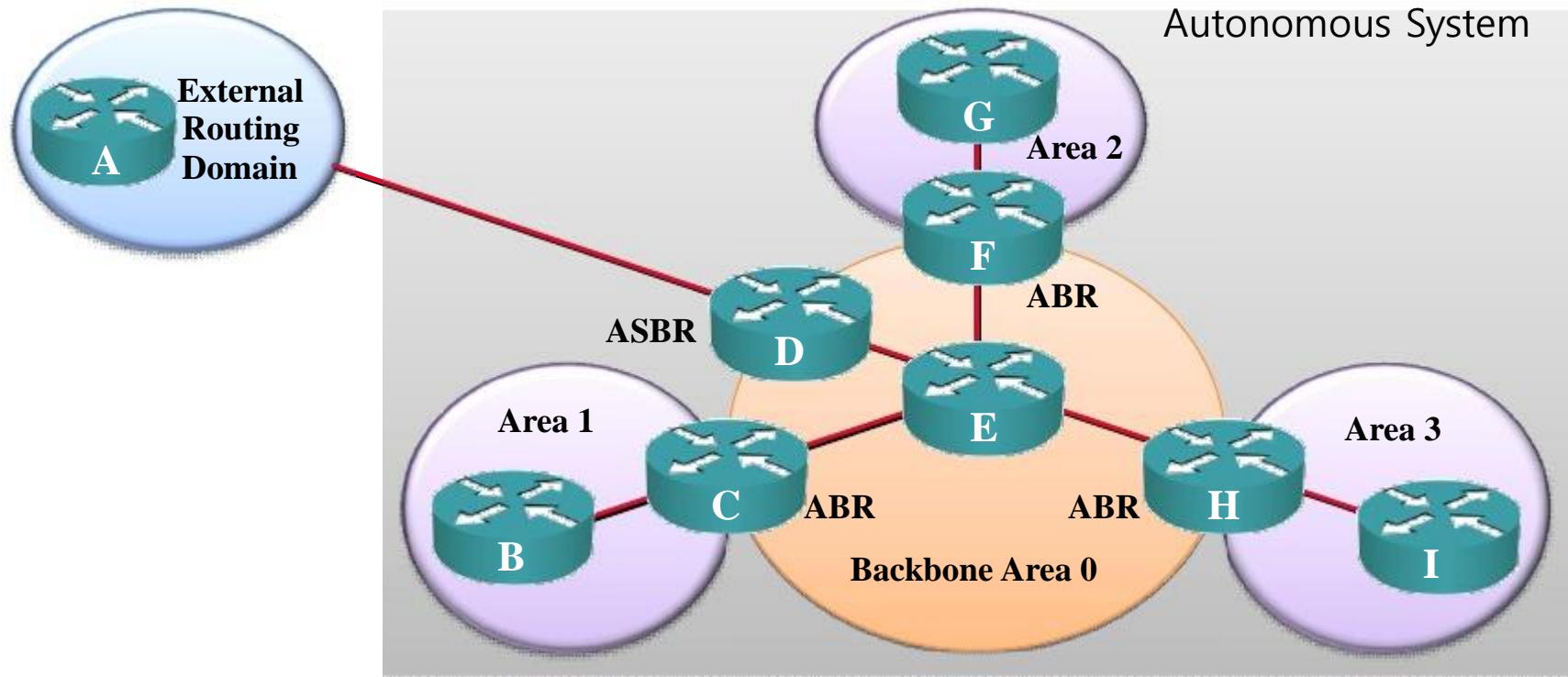


- OSPF는 IETF 표준이다 (RFC 2328)
- Shortest Path First (SPF) 알고리즘을 사용한다.
- Linkstate Routing Protocol 이다.

OSPF 특징

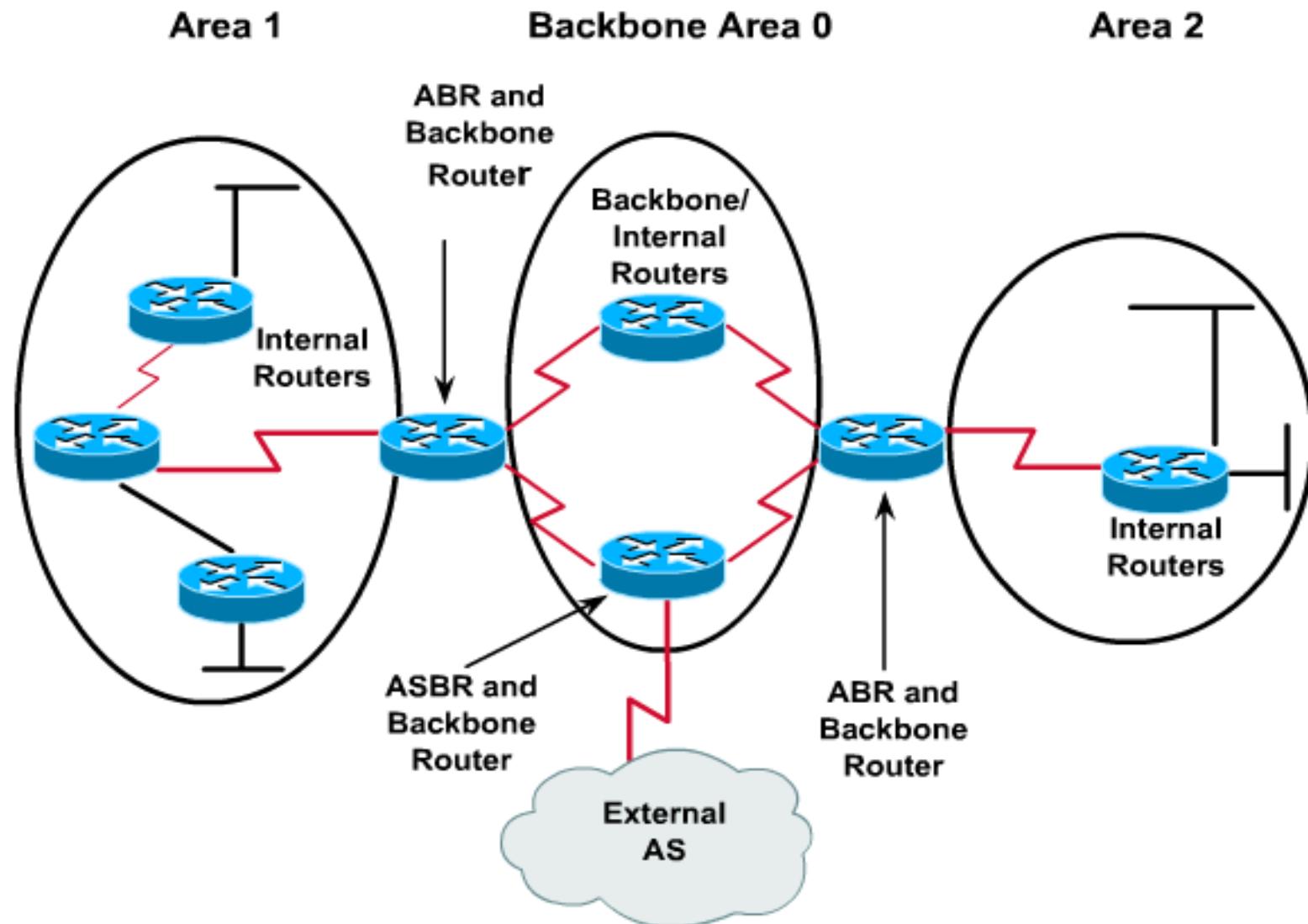
- OSPF는 Routing Table을 Update하지 않고 LinkState정보를 광고한다
- OSPF는 동일한 Area내의 다른 모든 Router에게 LSA (LinkState Advertisement)의 전송을 요청한다
- OSPF는 LinkState Database에 상태가 변경되면 즉시 LSA를 전달하여 다른 Router에게 알린다
- OSPF는 목적지 경로에 대한 최적의 정보를 SPF 알고리즘을 사용하여 계산한다.
- Link = router interface
- State = Interface와 Neighbor 연결 관계를 설명한다.

OSPF 의 계층적 Routing

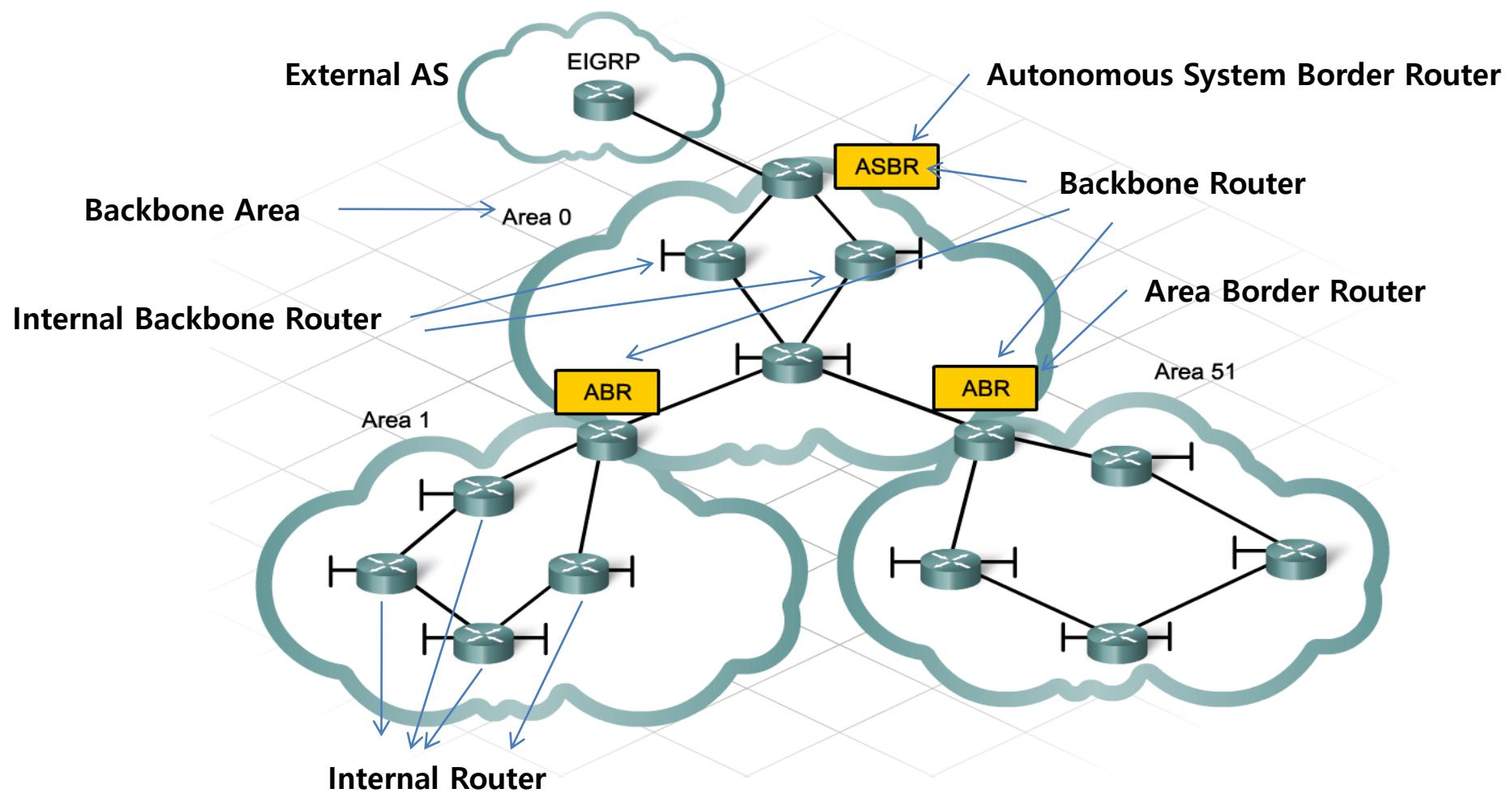


- 효과적인 Route Summarization을 통해 Routing Table Size 절감
- Area안에서 Topology 변화와 관련된 Traffic을 지역적으로 제한
- Router의 Processor와 Memory 자원 절감. SPF 계산빈도 줄어듦.
- Routing Update Traffic 줄임

OSPF Router Types



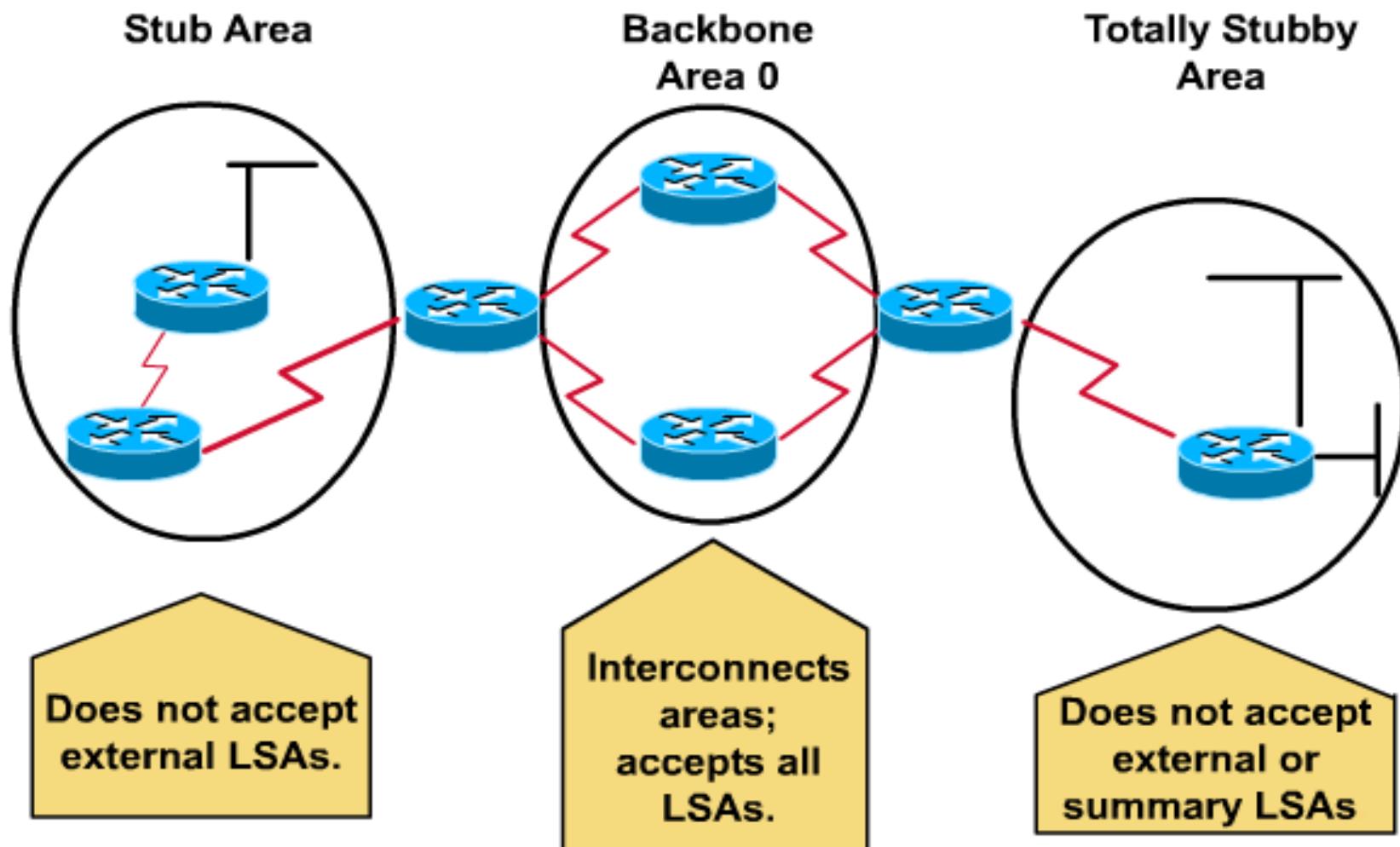
Area 개념



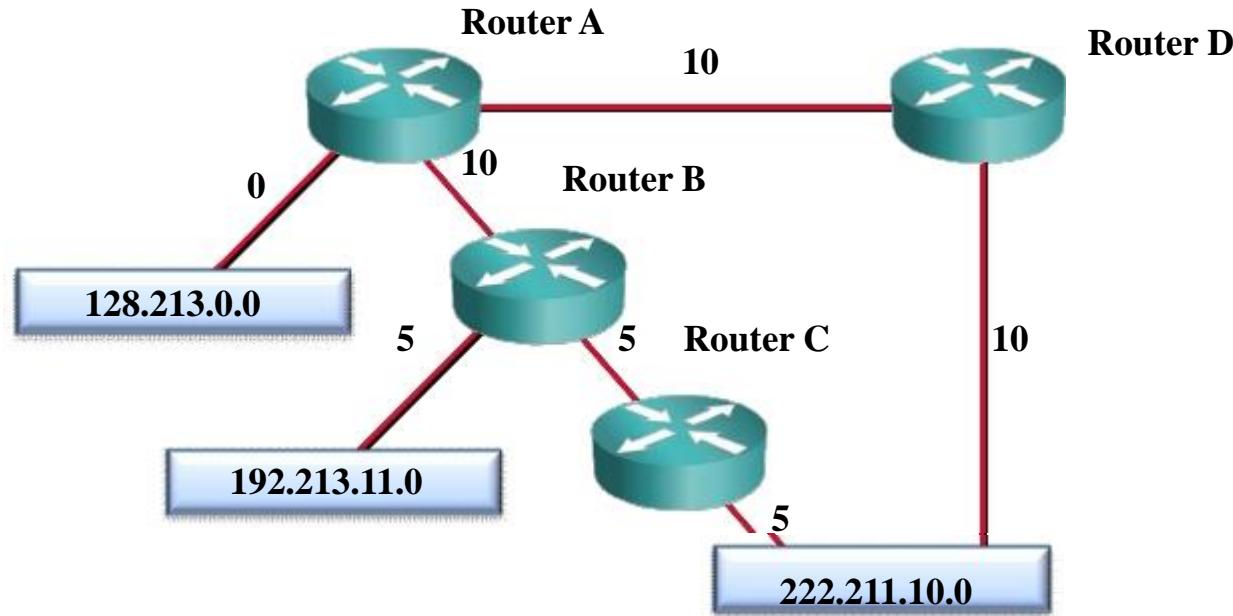
OSPF Area 탑입

- Backbone area (Area 0) - 모든 traffic이 통과하는 Area
- Non-backbone area - 보통의 OSPF Area
- Stub area - External정보를 받지 않는 Area
- Totally stubby area - External 정보와 Internal 정보 모두 받지 않는 Area
- Not-so-stubby area (NSSA) - AS내에 External정보를 가지는 Stub Area

Area Type



Shortest Path First Algorithm



- SPF 알고리즘에서는 Tree의 Root에 각 라우터를 두고 수신지에 도달하는데 필요한 누적 Cost를 기반으로 각 Node로 가는 최단 경로를 계산한다.
- $\text{Cost} = 10^8 / \text{bandwidth (bps)}$

OSPF 동작방식

- 1) OSPF를 설정한 Router끼리 Hello packet을 교환해서 Neighbor 혹은 adjacent Neighbor를 맺는다.
 - * adjacent Neighbor → 라우팅 정보(LSA)를 교환하는 네이버
 - * LSA(Link State Advertisement) → OSPF에서의 라우팅 정보
- 2) adjacent 네이버인 Router간에 라우팅 정보(LSA)를 서로 교환.
전송 받은 LSA를 Link-state DataBase에 저장.
- 3) LSA를 모두 교환하고 SPF(Shortest Path First) 또는 Dijkstra 알고리즘을 이용해서 각 목적지까지의 최적 경로를 계산 후 Routing Table에 올린다.
- 4) 그 후에도 주기적으로 Hello packet을 교환하면서 정상 동작을 확인
- 5) 네트워크의 상태가 변하면 다시 위의 과정을 반복해서 Routing Table을 생성

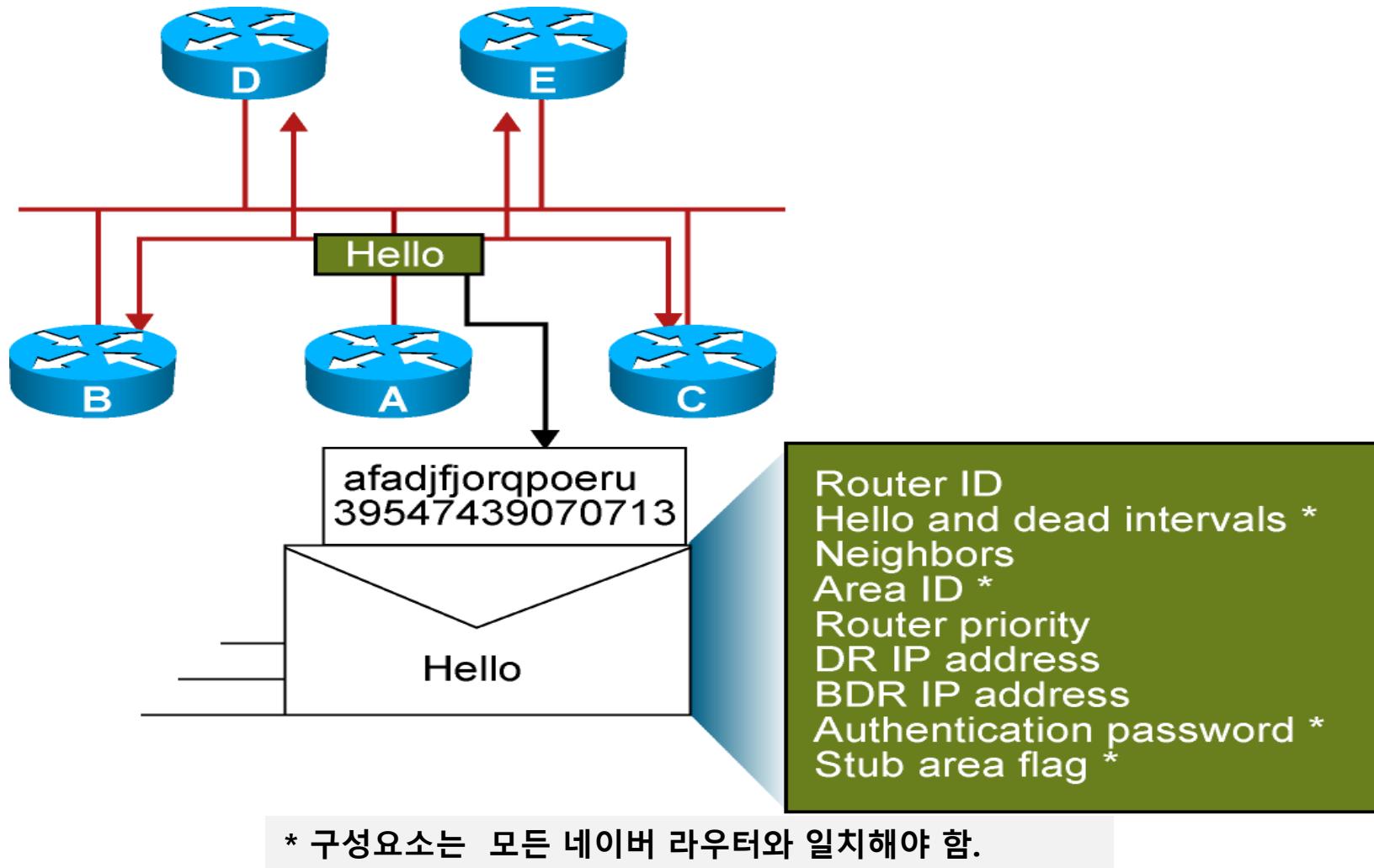
Adjacent 네이버

- OSPF에서 라우팅 정보(LSA)를 서로 교환하는 Neighbor를 adjacent 네이버라고 한다.
 - 1) DR과 다른 Router
 - 2) BDR과 다른 Router
 - 3) Point - to - point 네트워크로 연결된 두 Router
 - 4) Point - to - Multipoint로 연결된 두 Router
 - 5) Virtual-link로 연결된 두 Router

OSPF 패킷 타입

OSPF Packet Type	Description
Type 1 – Hello Packet	인접한 Router간 Neighbor 관계를 형성하고 Neighbor 관계를 유지하는데 사용
Type 2 – DBD Packet (Database Description Packet)	OSPF의 네트워크 정보인 LSA들의 요약된 정보를 알려줄 때 사용
Type 3 – LSR Packet (Link-State Request)	Neighbor에게서 수신한 DBD에 자신이 모르는 네트워크가 있을 때 상세 정보를 요청할 때 사용
Type 4 – LSU Packet (Link-State Update)	LSR을 받거나 자신이 알고 있는 네트워크 상태가 변했을 때 해당 네트워크 정보를 전송할 때 사용
Type 5 – LSAck Packet (Link-State Acknowledgement)	OSPF packet을 정상적으로 수신했음을 알려줄 때 사용 (DBD, LSR, LSU일 경우에만 응답)

Hello 패킷



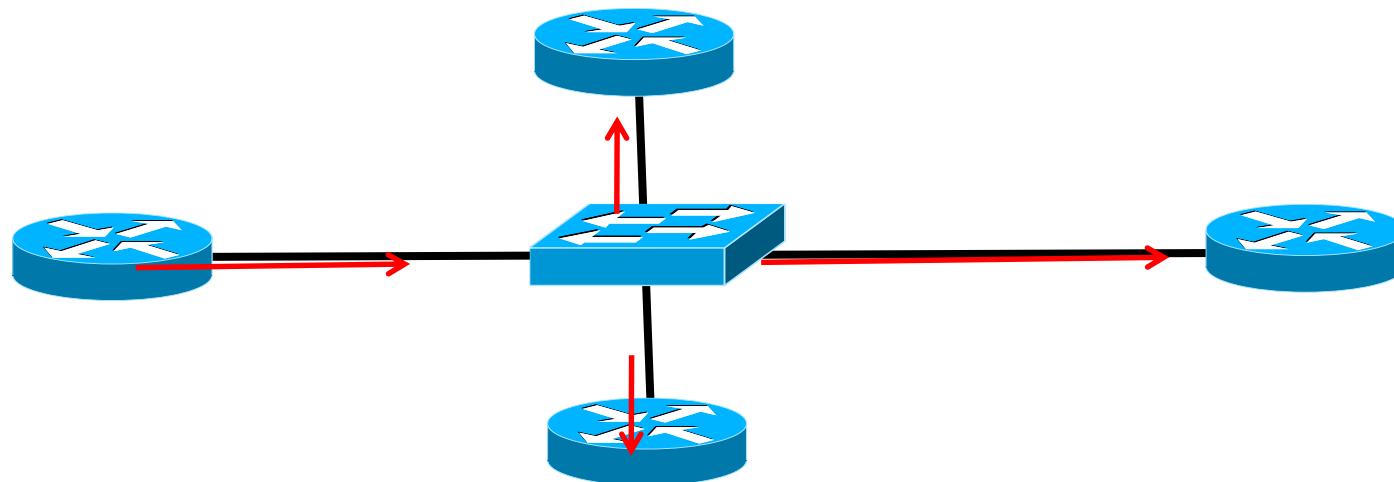
OSPF 네이버 상태

- Down 상태에서 시작해서 Neighbor와 Routing 정보 교환을 끝내고 Full 상태로 완료
- 1) Down 상태 → OSPF가 설정되고 Hello packet을 전송했지만 아직 상대방의 Hello packet을 받지 못한 상태
 - 2) Init 상태 → 근접 Router에게 Hello packet을 받았지만 상대 Router가 아직 내가 보낸 Hello packet을 받지 못한 상태
 - * 즉, 상대방이 전송한 Hello packet안의 네이버 리스트에 내 Router-ID가 없는 경우
 - 3) Two-way 상태 → Neighbor와 쌍방향 통신이 이루어진 상태
 - Multi Access 네트워크일 경우 이 단계에서 DR/BDR 선출
 - * 즉, 서로 전송한 Hello packet안의 네이버 리스트에 서로의 Router-ID가 있는 경우
 - 4) Exstart 상태 → adjacent neighbor가 되는 첫번째 단계. Master와 Slave Router를 선출. (Router-ID가 높은 Router가 Master)
 - 5) Exchange 상태 → 각 Router가 자신의 Link-state Database에 저장된 LSA의 Header만을 DBD Packet에 담아 상대방에게 전송
 - * DBD packet을 수신한 라우터는 자신의 database 내용과 비교한 후 자신에게 없거나 자신의 것보다 더 최신 정보일 경우 상대방에게 상세 정보(즉, LSA)를 요청하기 위해 Link State Request list에 기록한다.
 - 6) Loading 상태 → DBD packet 교환이 끝난 후 자신에게 없는 정보를 LSR packet으로 요청한다. LSR을 받은 Router는 정보를 LSU packet에 담아서 전송해준다.
 - 7) Full 상태 → adjacent neighbor간 라우팅 정보 교환이 모두 끝난 상태

네트워크 타입

1) Broadcast Multi Access

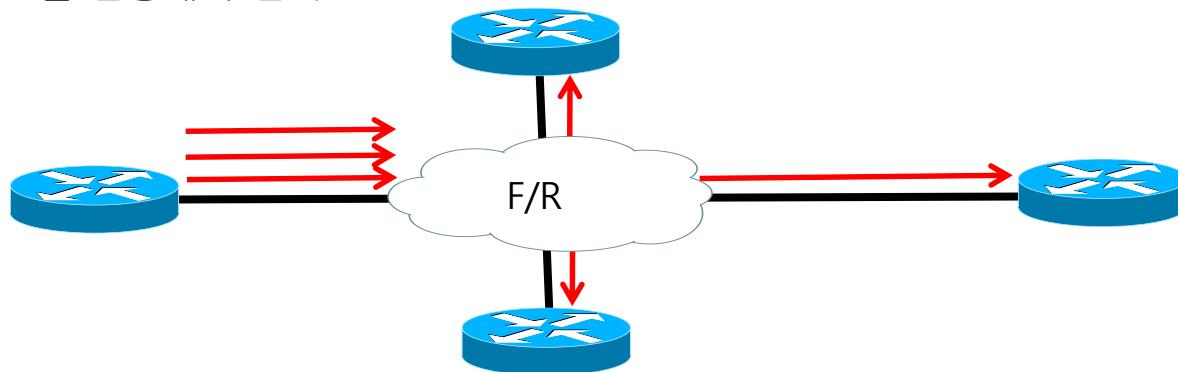
- 하나의 Broadcast 패킷을 전송할 경우 동일 네트워크 상의 모든 장비에게 전달되는 네트워크를 Broadcast 네트워크, 하나의 인터페이스를 통해 다수의 장비와 연결된 네트워크를 Multi Access 네트워크라 한다. (ex. Ethernet)
- Broadcast나 Multicast 방식을 사용해 하나의 packet만 전송해도 연결된 모든 장비에게 전송된다.



네트워크 타입

2) Non Broadcast Multi Access (NBMA)

- Broadcast가 지원되지 않는 Multi Access 네트워크를 의미한다.
(ex. ATM, X.25, Frame Relay)
- 대부분 내부에 Virtual Circuit (가상 회로) 방식을 사용
- NBMA에서는 Broadcast 를 사용하여 전송할 경우 가상회로 하나당 하나씩 Broadcast packet을 전송해야 한다.



3) Point-to-Point

- 하나의 Interface와 연결된 장비가 하나뿐인 네트워크
(ex. HDLC, PPP, F/R의 sub interface 중 point-to-point)

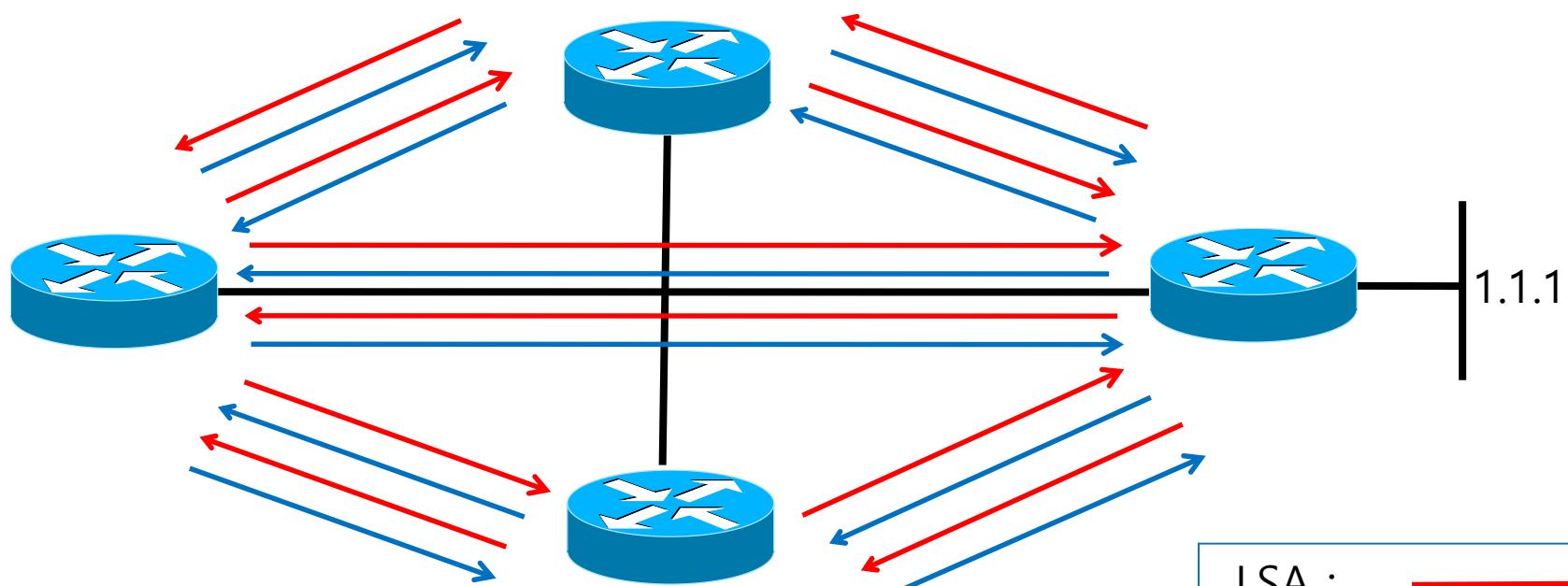


네트워크 타입

네트워크 타입	네이버	DR	Hello / Dead 주기	기본 인터페이스
Broadcast	자동	선출	10초 / 40초	Ethernet, Token ring, FDDI
Point-to-Point	자동	X	10초 / 40초	HDLC, PPP, F/R의 point-to-point 서브 인터페이스
Non Broadcast	지정	선출	30초 / 120초	Frame relay, ATM, X.25

DR(Designated Router)/BDR(Backup DR)

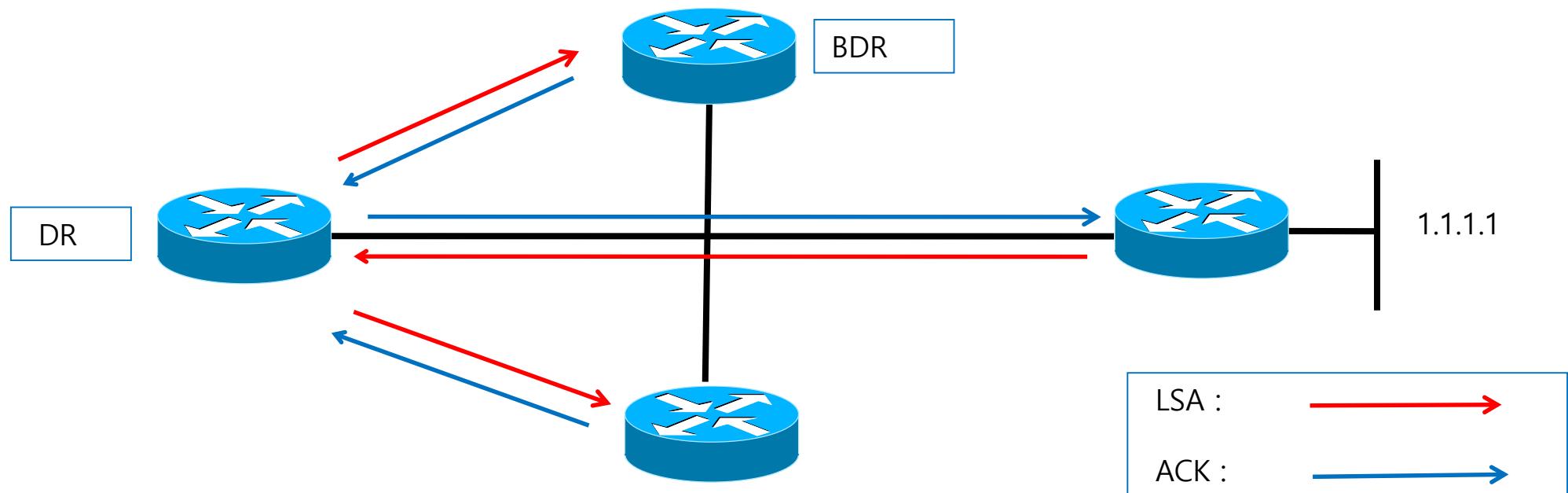
- Ethernet, NBMA 등의 Multi Access 네트워크에 접속된 Router가 1:1로 LSA를 교환할 경우 중복된 LSA와 ACK가 많이 발생



LSA :
ACK :

DR(Designated Router)/BDR(Backup DR)

- 중계 역할을 하는 DR(Designated Router)를 선출하고, DR에 문제가 발생할 경우를 대비해서 Backup용으로 BDR(Backup DR)을 선출한다.
- DR, BDR은 Broadcast 및 Non Broadcast의 MultiAccess 네트워크에서만 사용.
(Point-to-Point 네트워크에서는 사용하지 않는다.)



DR 선출 방법

- 1) OSPF priority가 가장 높은 Router가 DR로 선출
(다음으로 높은 Router가 BDR로 선출된다.)
- 2) OSPF priority가 동일할 경우 Router-ID가 높은 것이 DR, BDR로 선출
- 3) DR, BDR이 선출 된 후에 더 높은 순위의 Router가 추가되어도 DR,BDR이 변경되지 않는다.
(Router를 재부팅하거나 clear ip ospf process 명령어를 사용하면 변경)
- 4) DR이 다운될 경우 BDR이 DR이 되고 다시 BDR을 선출
(DR과 BDR이 아니 Router를 DROTHER라고 한다.)

Router ID와 설정

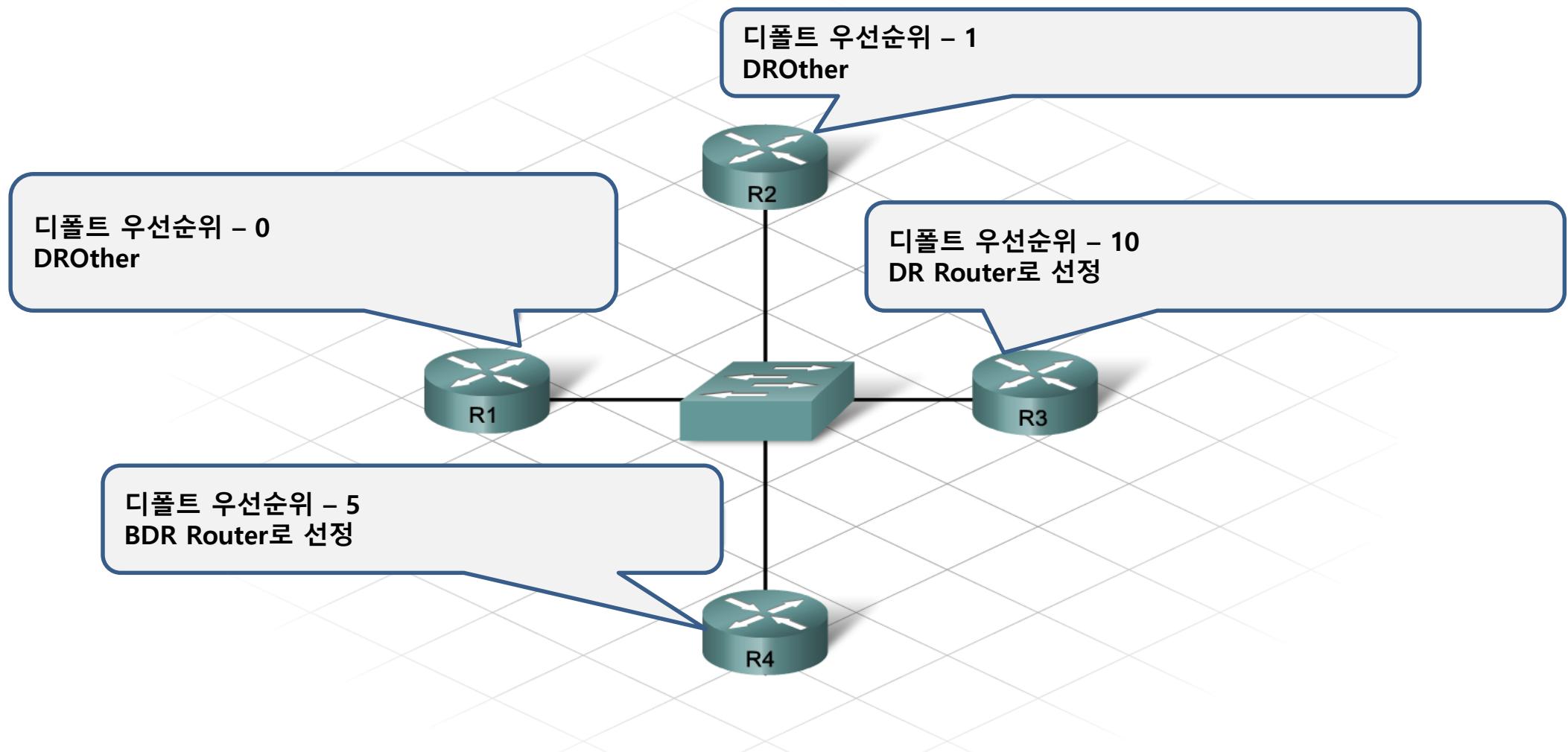
1) 라우터 ID

- OSPF는 라우터ID로 네이버 라우터를 식별
 - 라우터ID로 특정 네이버 식별
 - LSDB에 라우터ID별로 LSA 관리
- 32비트의 점이 있는 10진수로 표기
 - IP주소를 라우터ID로 사용

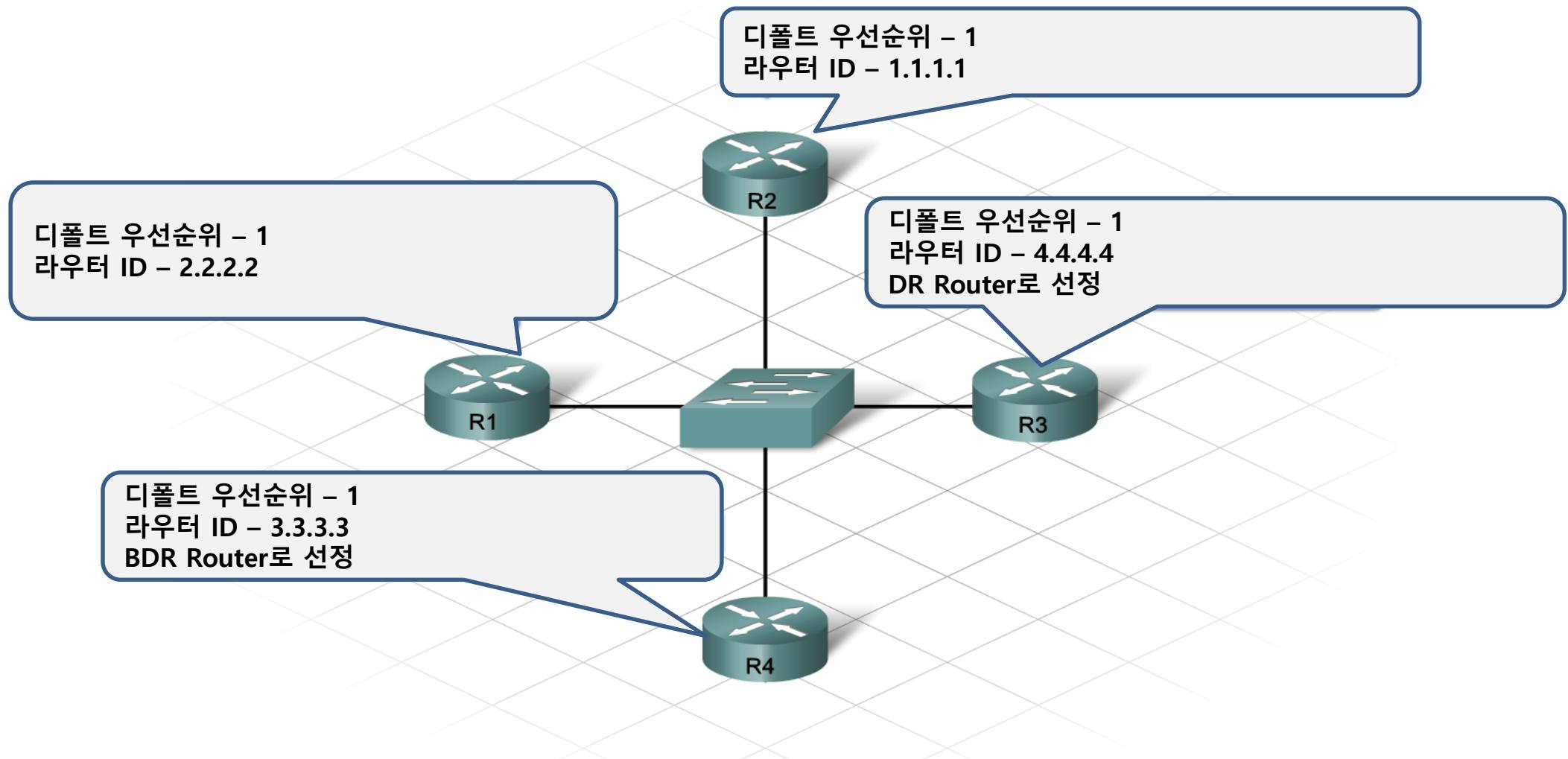
2) 라우터 ID 설정

- 라우터의 인터페이스에 할당된 IP 주소 중에 가장 높은 IP 주소가 라우터ID가 됩니다.
- Loopback 인터페이스가 활성화되어 있고, IP 주소가 할당되어 있다면 다른 인터페이스에 우선하여 Loopback 인터페이스의 IP 주소가 라우터ID가 됩니다.
- 라우팅 프로토콜 설정 모드에서 router-id 명령을 이용하여 관리자가 직접 지정할 수 있습니다.

우선순위에 의한 DR/BDR 선정



Router ID 의한 DR/BDR 선정



OSPF 단일 Area 설정

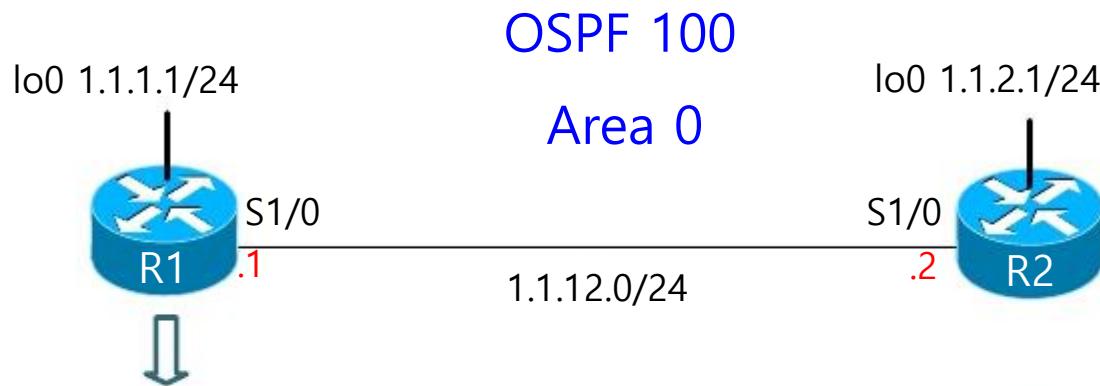
- router ospf 명령을 사용하여 OSPF routing process를 시작하고, Network 명령을 사용하여 광고할 네트워크 혹은 인터페이스를 포함시킨다. 마지막으로 해당 네트워크나 인터페이스가 포함될 area를 지정한다.

```
Router(config)# router ospf process-id
```

```
Router(config-router)# network network-address wildcard-mask area area-id
```

```
Router(config-router)#{
```

OSPF 단일 Area 설정하기



```
R1(config)#router ospf 100
R1(config-router)#network 1.1.1.0 0.0.0.255 area 0
R1(config-router)#network 1.1.12.0 0.0.0.255 area 0
```

```
R2(config)#router ospf 100
R2(config-router)#network 1.1.12.0 0.0.0.255 area 0
R2(config-router)#network 1.1.2.0 0.0.0.255 area 0
```

OSPF 설정 확인

```
R1#sh ip route
```

Gateway of last resort is not set

1.0.0.0/8 is variably subnetted, 7 subnets, 2 masks

C 1.1.1.0/24 is directly connected, Loopback0

O 1.1.2.1/32 [110/11] via 1.1.12.2, 00:01:05, Serial1/0

C 1.1.12.0/24 is directly connected, Serial1/0

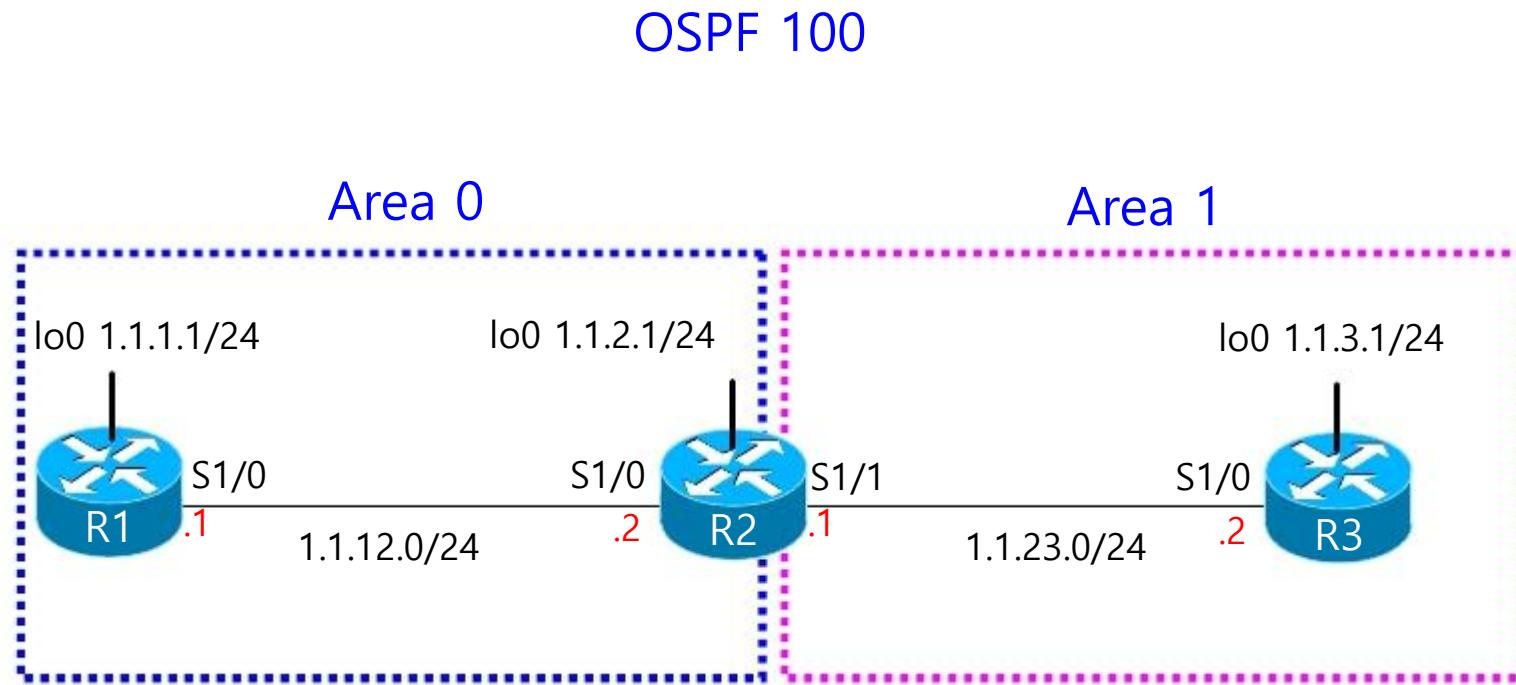
```
R1#show ip ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
1.1.2.1	0	FULL/ -	00:00:36	1.1.12.2	Serial 1/0

OSPF 설정 확인

```
R1# show ip ospf database
```

OSPF 멀티 Area 설정하기



OSPF 멀티 Area 설정하기

```
R1(config)#router ospf 100
R1(config-router)#router-id 1.1.1.1
R1(config-router)#network 1.1.1.0 0.0.0.255 area 0
R1(config-router)#network 1.1.12.0 0.0.0.255 area 0
```

```
R2(config)#router ospf 100
R2(config-router)#router-id 1.1.2.1
R2(config-router)#network 1.1.12.0 0.0.0.255 area 0
R2(config-router)#network 1.1.2.0 0.0.0.255 area 0
R2(config-router)#network 1.1.23.0 0.0.0.255 area 1
```

```
R3(config)#router ospf 100
R3(config-router)#router-id 1.1.3.1
R3(config-router)#network 1.1.23.0 0.0.0.255 area 1
R3(config-router)#network 1.1.3.0 0.0.0.255 area 1
```

OSPF 멀티 Area 설정 확인

```
R1#sh ip route
```

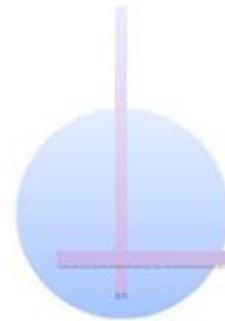
Gateway of last resort is not set

1.0.0.0/8 is variably subnetted, 7 subnets, 2 masks

- C 1.1.1.0/24 is directly connected, Loopback0
- O 1.1.2.1/24 [110/11] via 1.1.12.2, 00:01:05, Serial1/0
- O IA 1.1.3.1/24 [110/75] via 1.1.12.2, 00:01:05, Serial1/0
- C 1.1.12.0/24 is directly connected, Serial1/0
- O IA 1.1.23.0/24 [110/74] via 1.1.12.2, 00:01:05, Serial1/0

OSPF 멀티 Area 설정 확인

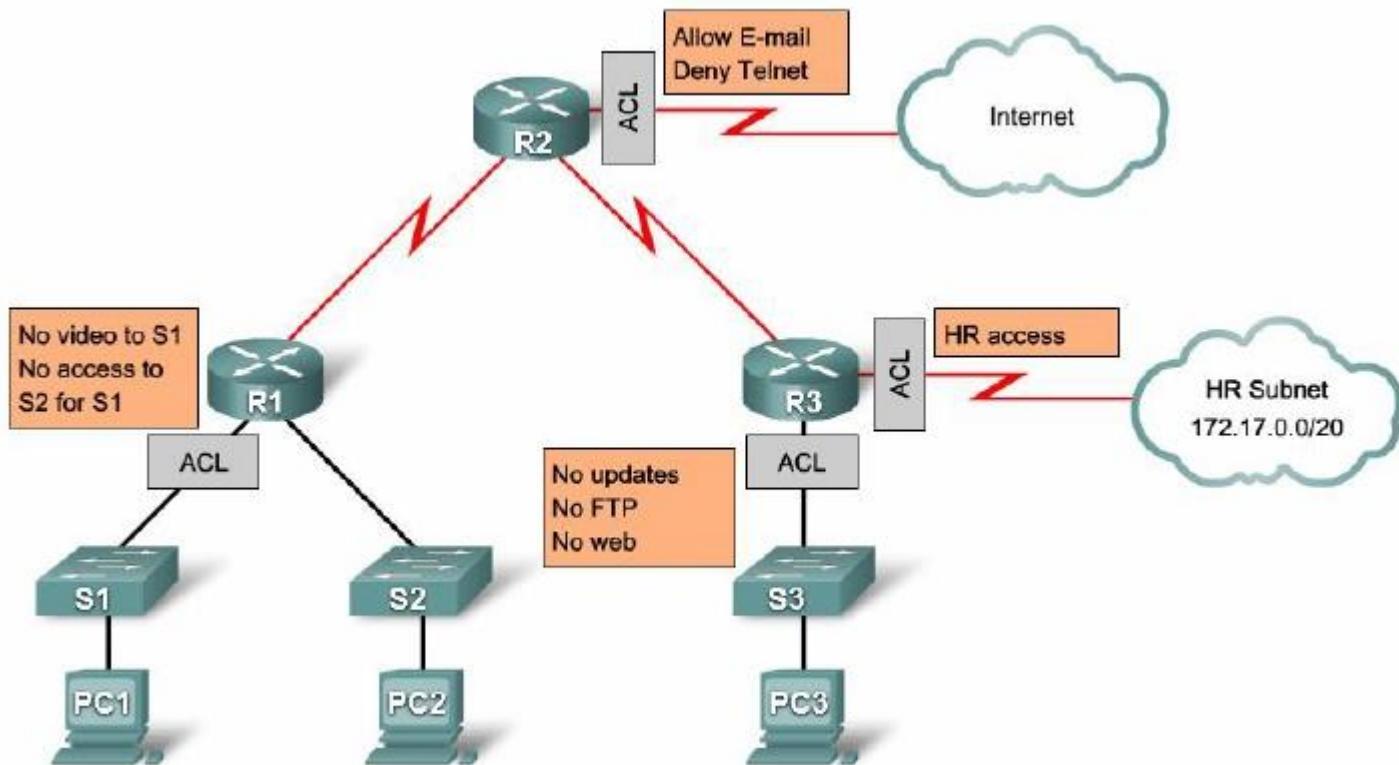
```
R1# sh ip ospf database
```



Module 06

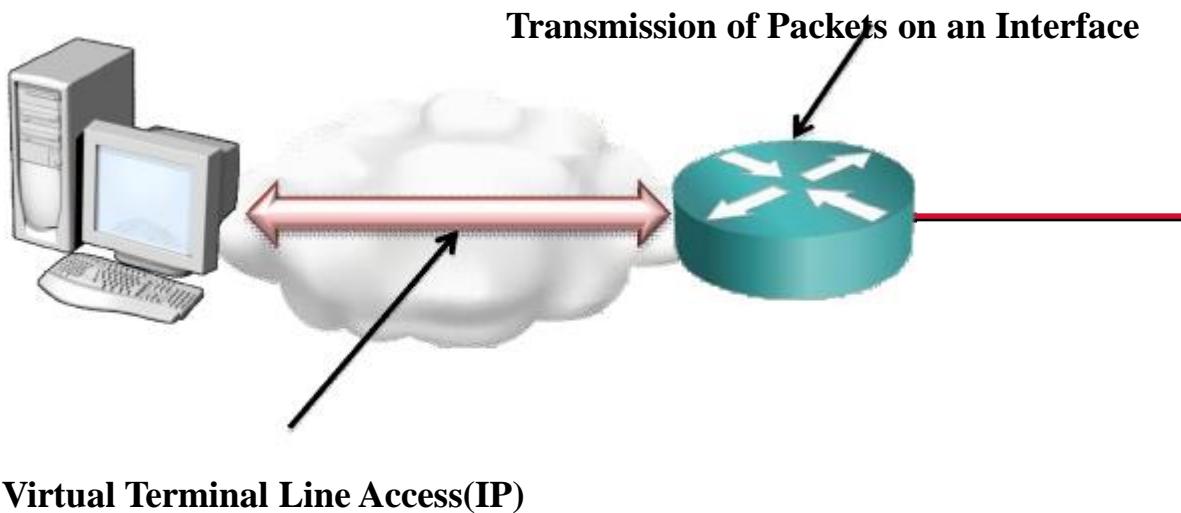
ACL과 NAT를 이용한 IP Traffic 관리

Why Use Access Lists ?



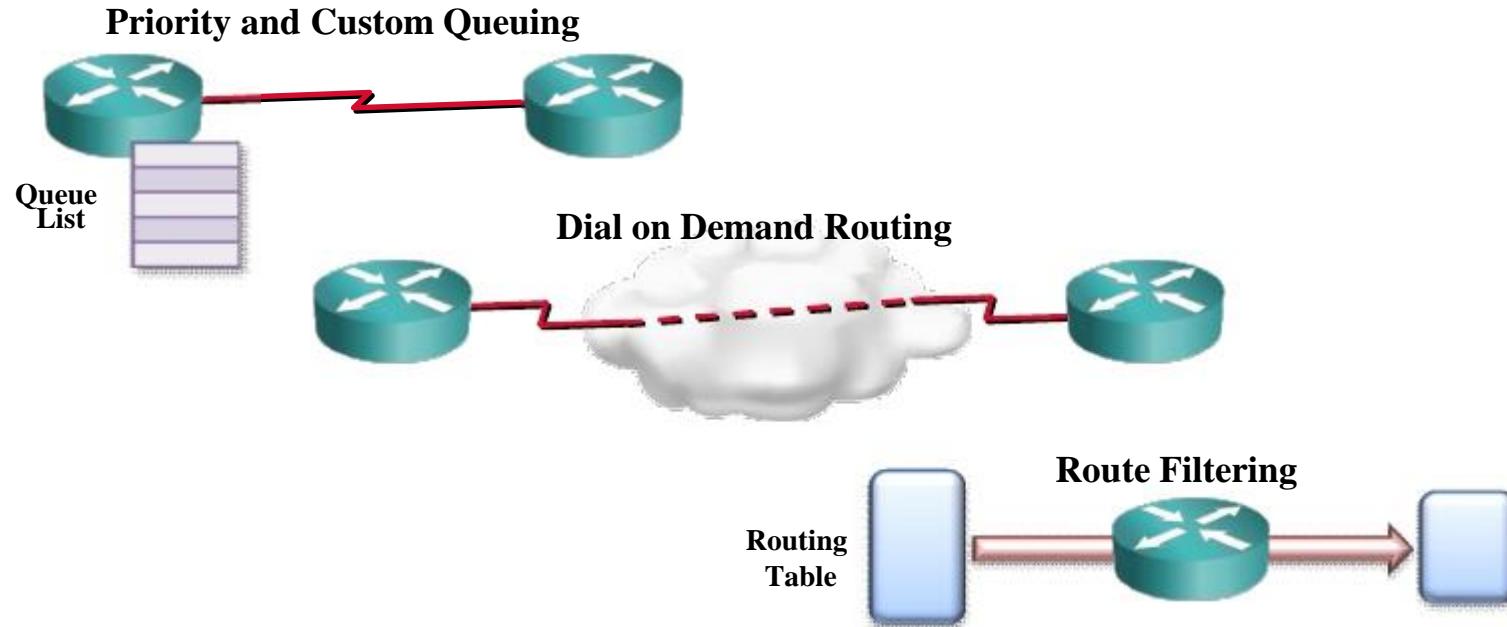
- Router에서는 ACL (Access Control List)을 사용하여 트래픽 식별, 필터링, 암호화, 분류, 변환 작업을 수행할 수 있다
- Router를 경유하는 Packet을 Filtering한다

Access List Applications



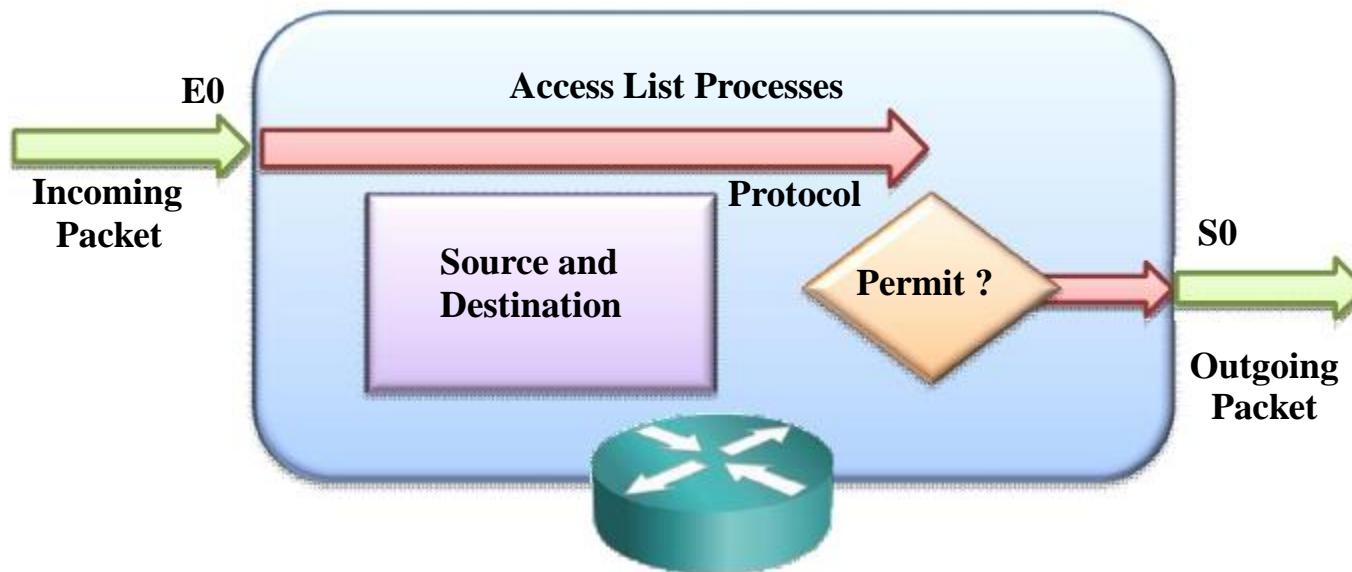
- Packet Filtering을 활용하여 네트워크에서의 Packet 이동을 제어 할 수 있다
- Router에 VTY 포트로 들어오거나 VTY 포트에서 나가는 Telnet Traffic을 허용(Permit)하거나 거부(Deny)할 수 있다

ACL을 이용하는 기술들



- Access List를 다양한 방식으로 활용할 수 있다
 - Priority and Custom Queuing
 - Dial on Demand Routing (DDR)
 - Route Filtering

ACL의 탑입



- Standard Access List :

Source Address를 검사한다

검사결과에 따라 전체 Protocol Suite에 대한 Packet 출력을 허용하거나 거부한다

- Extended Access List :

Source Address와 Destination Address를 모두 검사한다

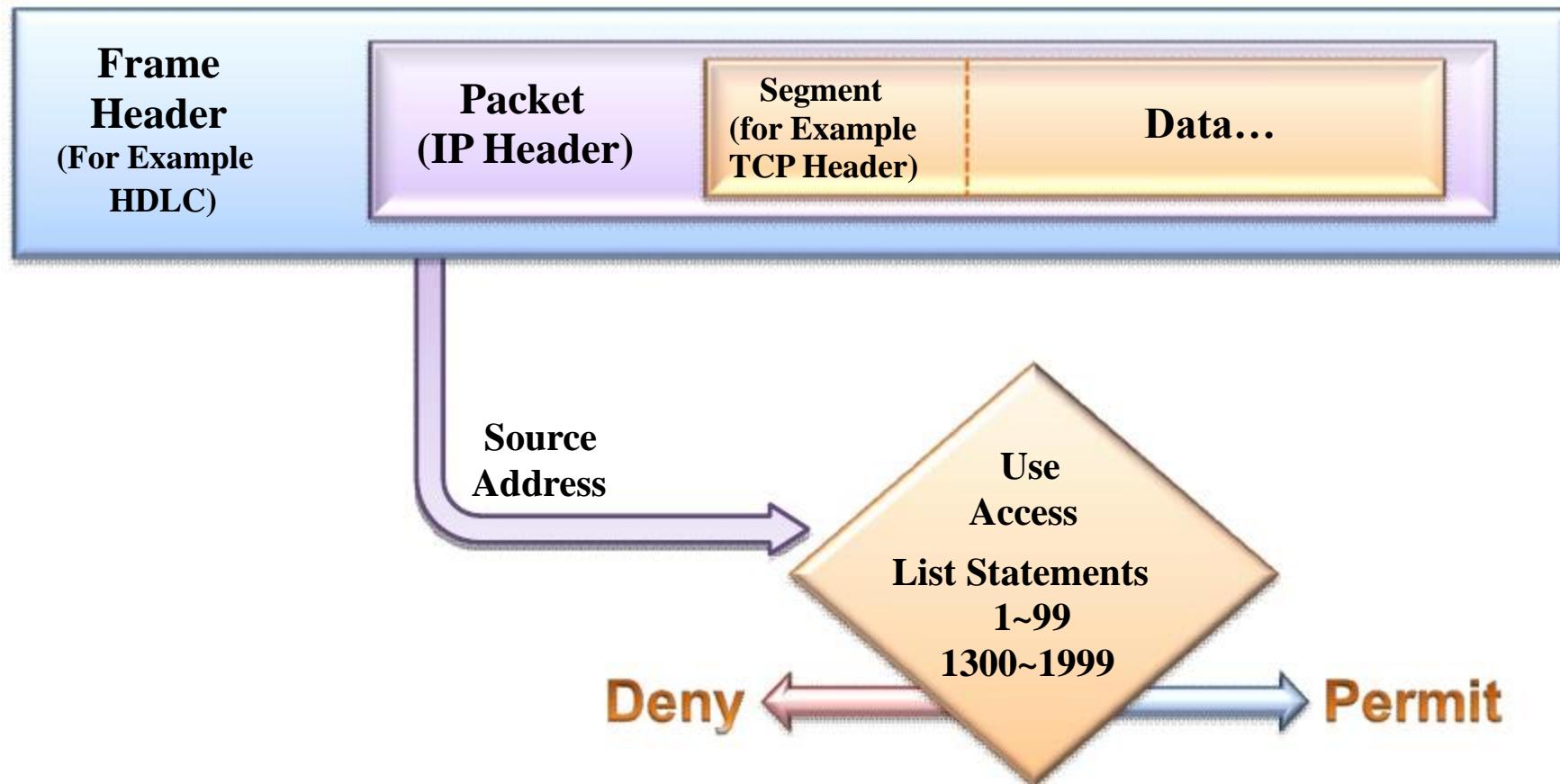
특정 Protocol, Port번호, 다른 매개변수를 검사하여 유연하게 제어가 가능하다

ACL 식별하기

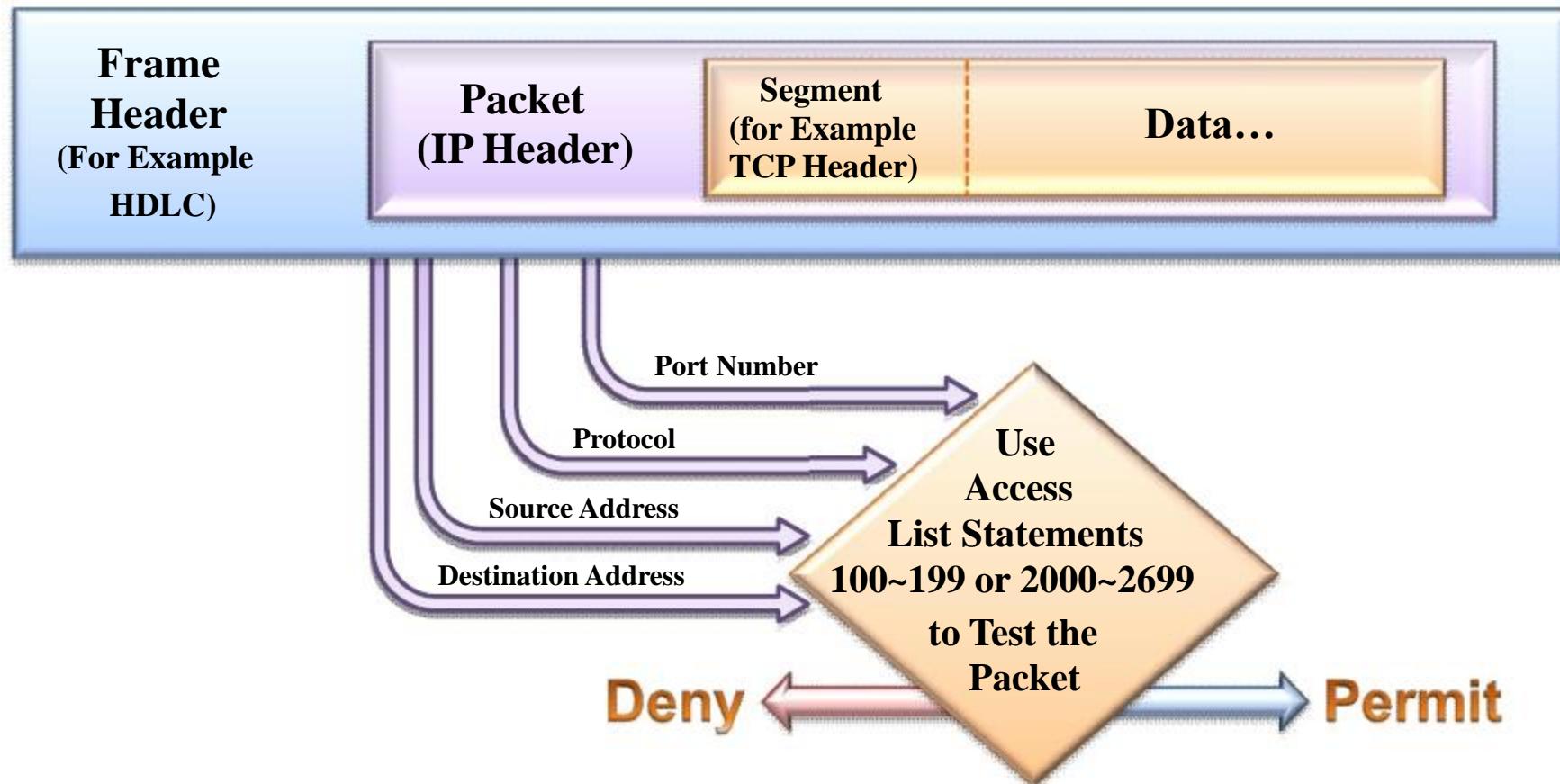
Access List Type	Number Range/Identifier
IP Standard	1~99, 1300~1999
Extended	100~199, 2000~2699
Named	Name

- Standard IP List (1~99)는 IP Packet에 Source Address를 조건으로 가진다
- Extended IP List (100~199)는 Source and Destination Address와 특정 TCP/IP Protocol Suite Protocol과 Destination Port를 조건으로 가진다
- Standard List (1300~1999) (Expanded Range)
- Extended IP List (2000~2699) (Expanded Range)
- Named IP List는 Standard와 Extended 이름으로 선어하여 각 조건을 검사한다

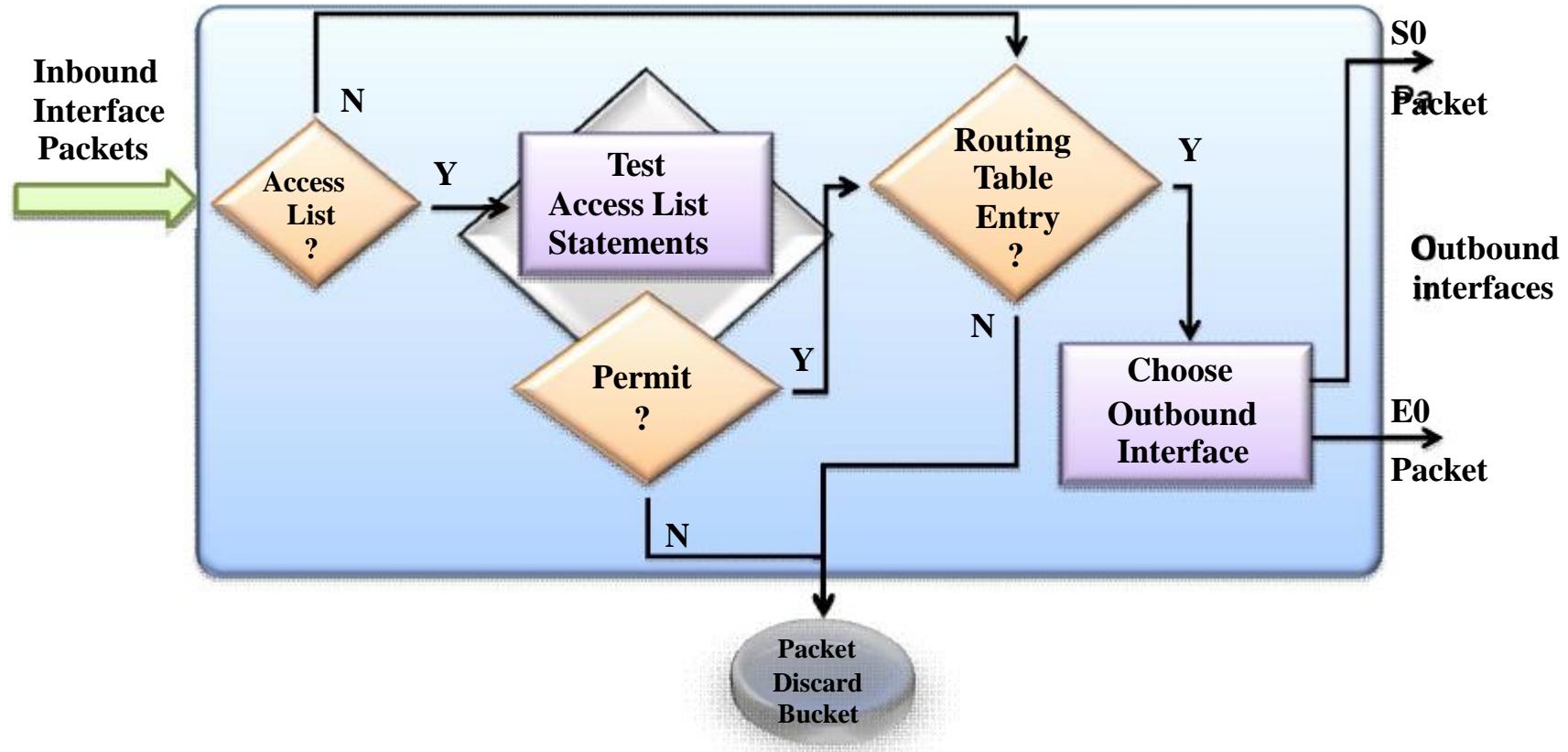
표준 ACL의 패킷 필터링



확장 ACL의 패킷 필터링

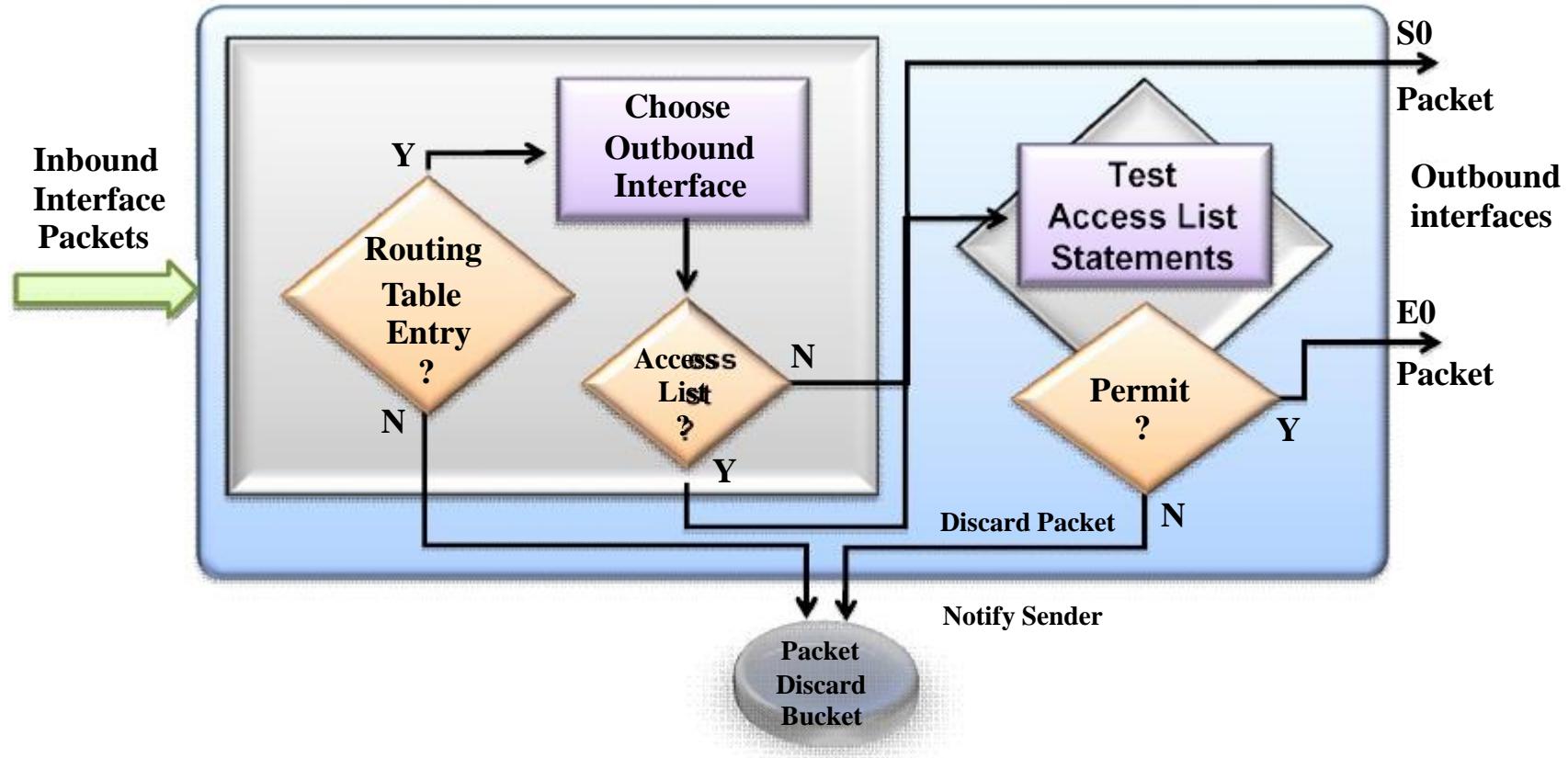


인바운드 ACL의 동작과정



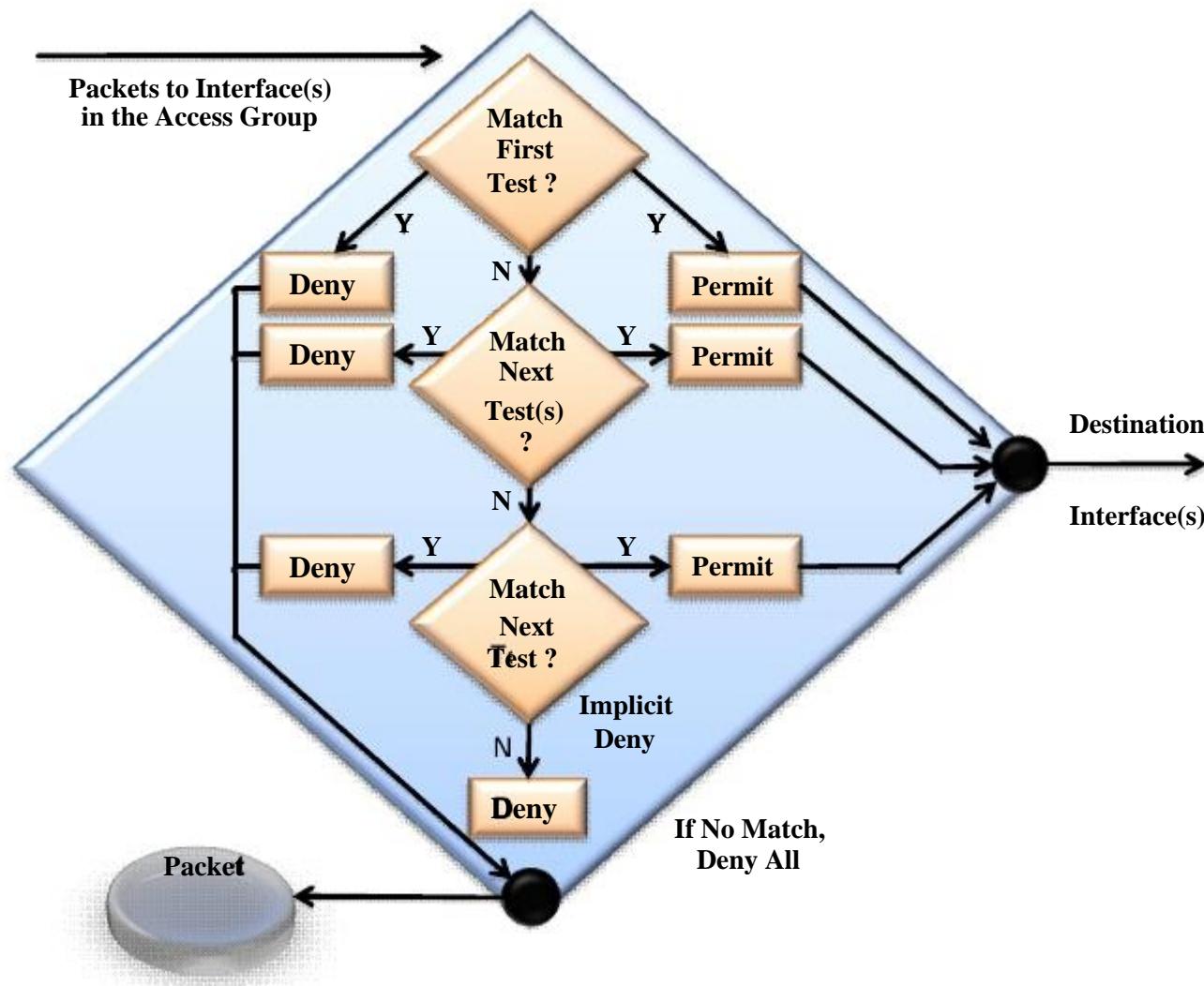
- Access List에 매치되지 않는 모든 Packet은 암묵적으로 거부된다

아웃바운드 ACL의 동작과정

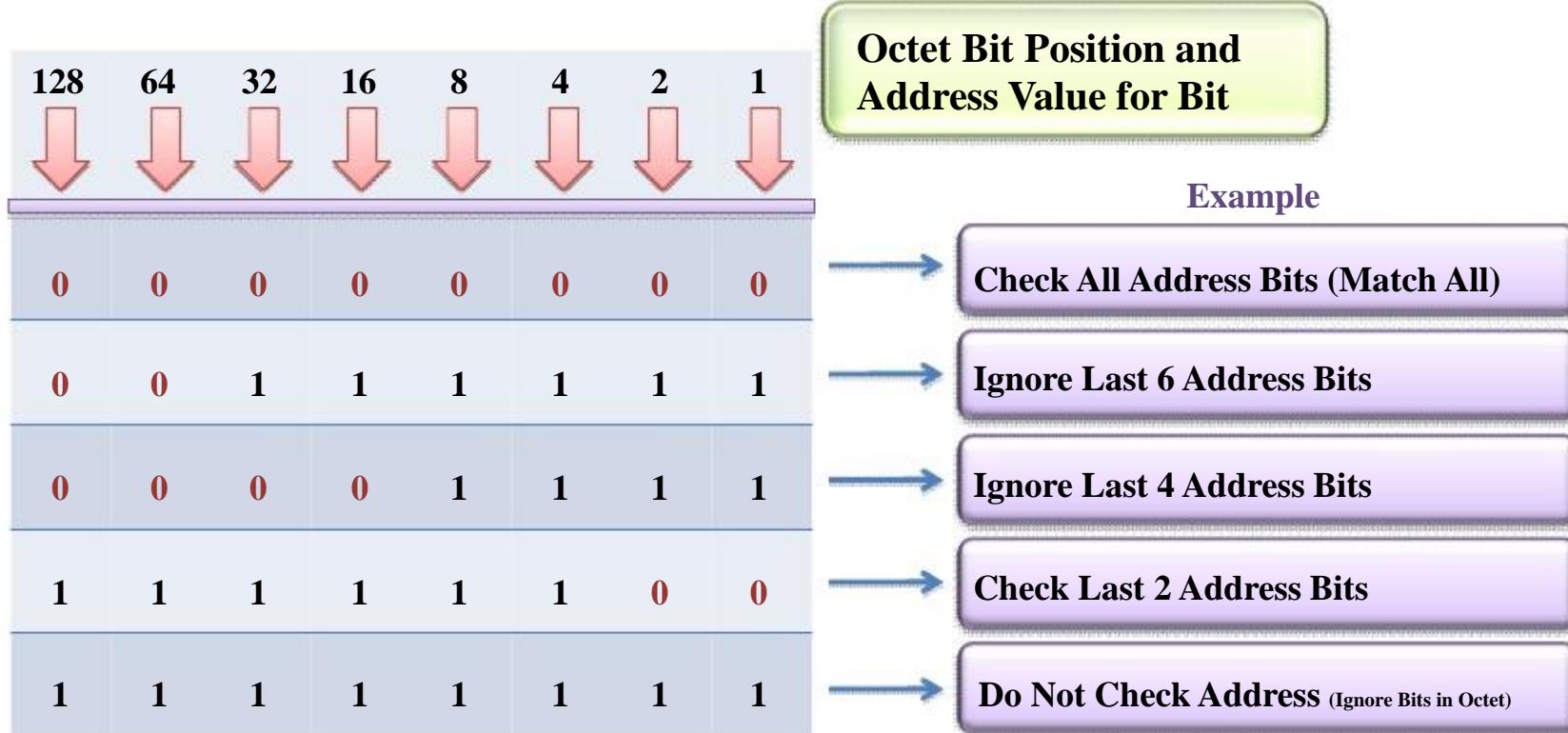


- Access List에 매치되지 않는 모든 Packet은 암묵적으로 거부된다

ACL 엔트리의 패킷 검사 : Deny, Permit



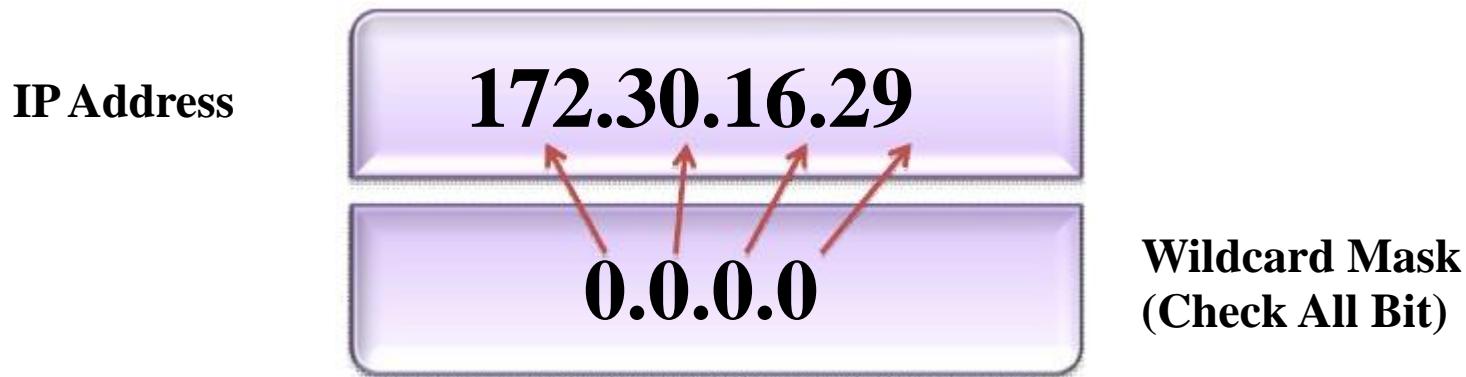
Wildcard mask : 특정 주소에 해당하는지 검사



- Wildcard mask bit 0은 대응 bit값을 검사하라는 것을 의미한다
- Wildcard mask bit 1은 대응 bit값을 검사하지 말고 무시하라는 것을 의미한다

특정 IP 호스트를 나타내는 Wildcard mask

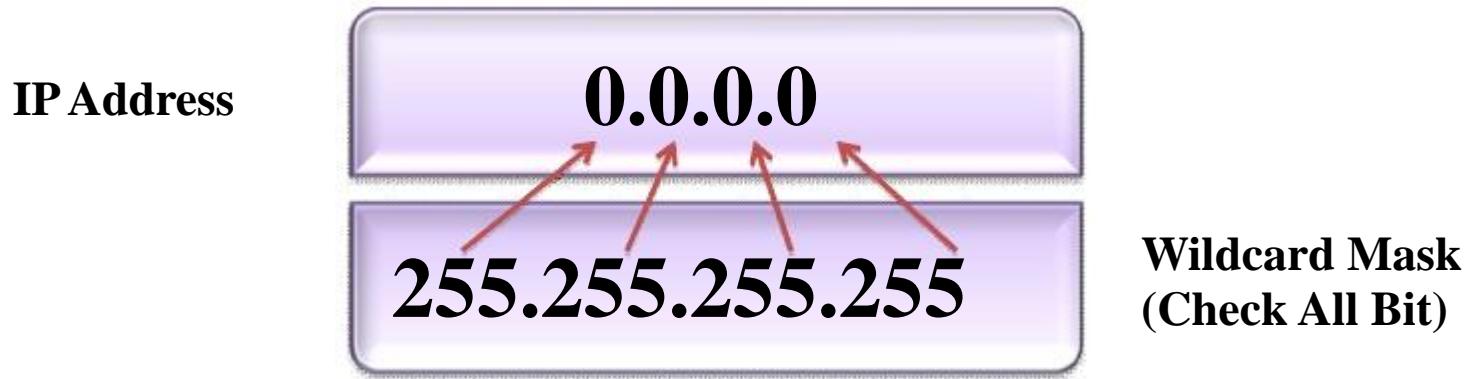
- Test 조건 : 모든 Address Bit 검사 (모두 일치)
(1개의 IP Host Address만 검사)



- 172.30.16.29 0.0.0.0은 모든 Address를 검사해서 매치되는 주소 즉, 172.30.16.29를 갖는 호스트를 지정한다
- 하나의 IP를 알리기 위해 IP Address 앞에 약어 host를 사용할 수 있다. 예를 들어 "172.30.16.29 0.0.0.0" 대신 "host 172.20.16.29"를 사용할 수도 있다

모든 주소를 나타내는 Wildcard mask

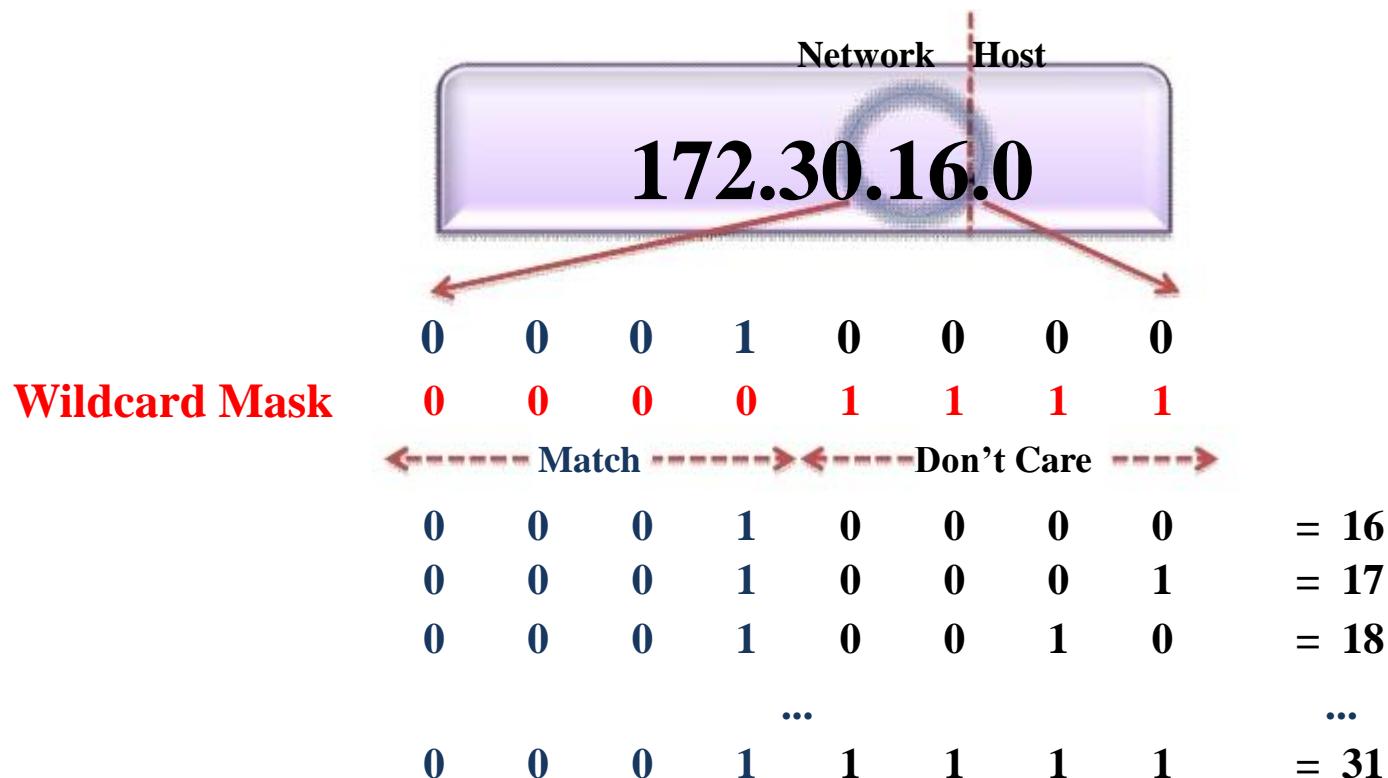
- Test 조건 : 모든 Address Bit 무시 (Match Any)
(모든 IP Address)



- 모든 Address를 받아들이려면 IP Address는 0.0.0.0을 입력하고 Wildcard mask는 모든 값을 무시(검사 없이 허용)하려면 255.255.255.255를 지정한다
- 관리자는 모든 주소를 지정할 목적으로 0.0.0.0 255.255.255.255를 명시하는 대신 **any**라는 문자를 사용할 수 있다

특정 IP 서브넷을 나타내는 Wildcard mask

- 172.30.16.0/24에서 172.30.31.0/24까지의 IP Subnet 검사하기
 - Address와 wildcard mask : 172.30.16.0 0.0.15.255



ACL command 개요

- Step 1 : accesslist 명령어로 IP Traffic Filter list에 Entry를 만든다

```
Router(config)#access-list access-list-number {permit | deny} {test_conditions}
```

- Step 2 : IP accessgroup 명령으로 기준 AccessList를 Interface에 적용한다

```
Router(config-if)#{protocol} access-group access-list-number {in | out}
```

표준 ACL 설정

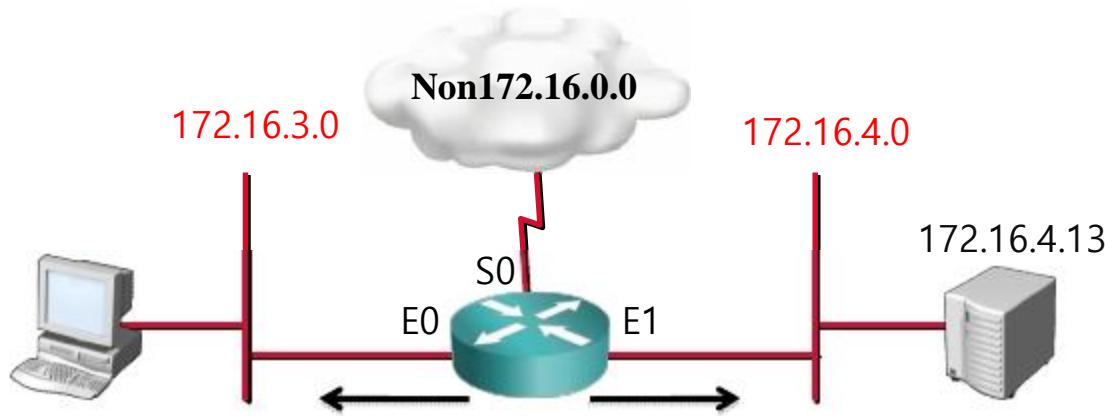
```
Router(config)#access-list access-list-number {permit | deny} source [mask]
```

- Accesslistnumber : Entry가 속할 list 번호 설정. 1~99, 1300~1999사이의 번호가 들어간다
- permit | deny | remark는 해당 Entry에 매치되면 취할 Action을 정의
- Source는 송신지 IP Address를 정의 한다
- mask는 Wildcard mask를 사용하여 Address 필드의 어느 비트들이 일치되어야 하는지 설정한다

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

- List를 적용할 Interface에서 설정한다
- Inbound또는 Outbound시 검사하도록 설정한다
- Default = outbound
- Interface에서 "no ip accessgroup *accesslistnumber*" 명령을 사용하여 적용된 Accesslist를 제거한다

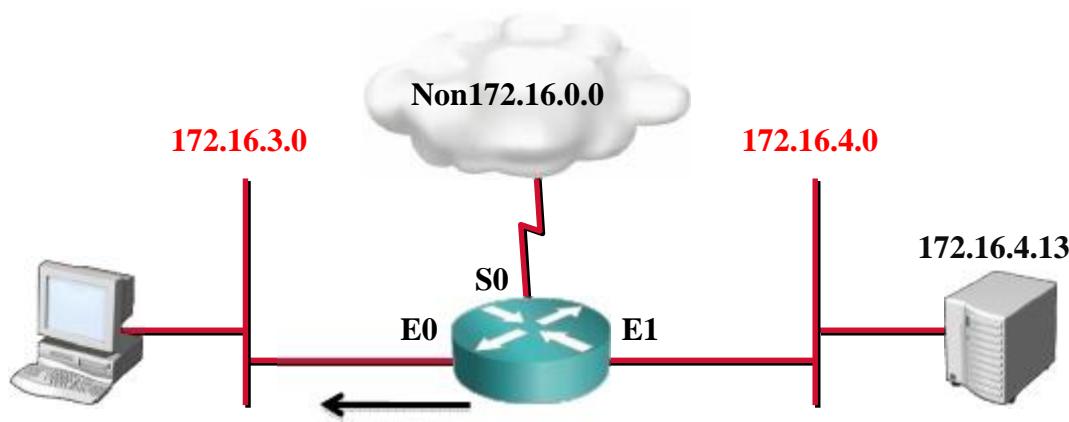
표준 ACL 설정 예제 1



```
Router(config)#access-list 1 permit 172.16.0.0 0.0.255.255
(ACL 엔트리에 명시적으로 추가하지 않아도 마지막 라인에 다음과 같이 모든 패킷을 거부하라는
엔트리가 포함됨)
(access-list 1 deny 0.0.0.0 255.255.255.255)

Router(config)#interface ethernet 0
Router(config-if)#ip access-group 1 out
Router(config)#interface ethernet 1
Router(config-if)#ip access-group 1 out
```

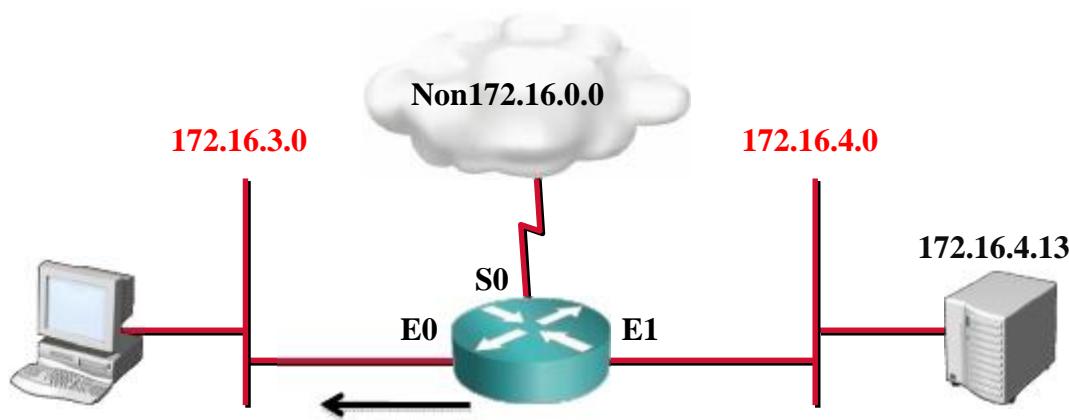
표준 ACL 설정 예제 2



```
Router(config)#access-list 1 deny 172.16.4.13 0.0.0.0
Router(config)#access-list 1 permit 0.0.0.0 255.255.255.255
(ACL 엔트리에 명시적으로 추가하지 않아도 마지막 라인에 다음과 같이 모든 패킷을 거부하라는 엔트리가 포함됨)
(access-list 1 deny 0.0.0.0 255.255.255.255)
```

```
Router(config)#interface ethernet 0
Router(config-if)#ip access-group 1 out
```

표준 ACL 설정 예제 3



```
Router(config)#access-list 1 deny 172.16.4.0 0.0.0.255  
Router(config)#access-list 1 permit any
```

(ACL 엔트리에 명시적으로 추가하지 않아도 마지막 라인에 다음과 같이 모든 패킷을 거부하라는 엔트리가 포함됨)

(access-list 1 deny 0.0.0.0 255.255.255.255)

```
Router(config)#interface ethernet 0  
Router(config)#ip access-group 1 out
```

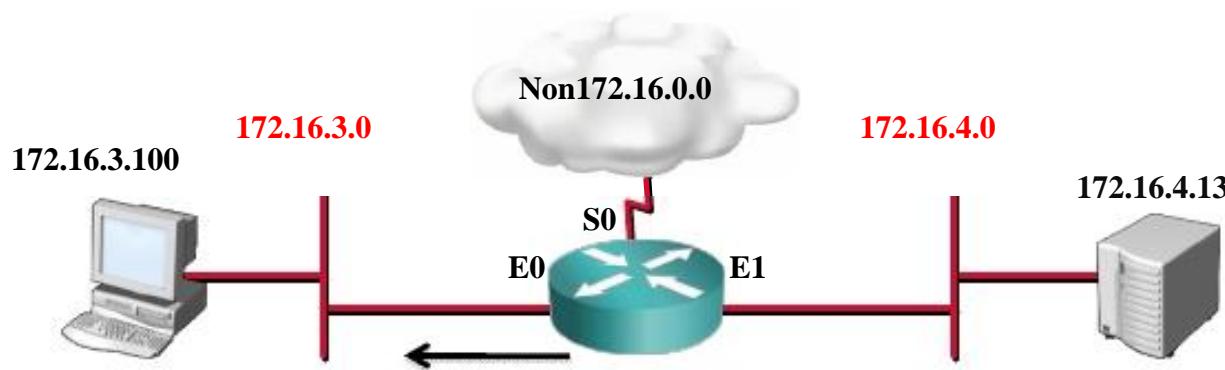
확장 ACL 설정

```
Router(config)#access-list access-list-number
{permit | deny} protocol source source-wildcard [operator port]
destination destination-wildcard [operator port] [established] [log]
```

- Accesslistnumber : Entry가 속할 list 번호 설정. 100~199, 2000~2699사이의 번호가 들어간다.
- permit | deny | remark는 해당 Entry에 매치되면 취할 Action을 정의.
- Source와 Destination은 송수신지 IP Address를 정의한다.
- mask는 Wildcard mask를 사용하여 Address 필드의 어느 비트들이 일치되어야 하는지 설정한다.
- Operator port는 lt(less than), gt(greater than), eq(equal to), neq(not equal to)와 Protocol Port번호를 명시한다.
- established는 Inbound TCP에 대해서만 사용된다.
- log는 Console로 log Message를 보낸다.

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

확장 ACL 설정 예제 1



```
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21  
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20  
Router(config)#access-list 101 permit ip any any
```

(ACL 엔트리에 명시적으로 추가하지 않아도 마지막 라인에 다음과 같이 모든 패킷을 거부하라는 엔트리가 포함됨)

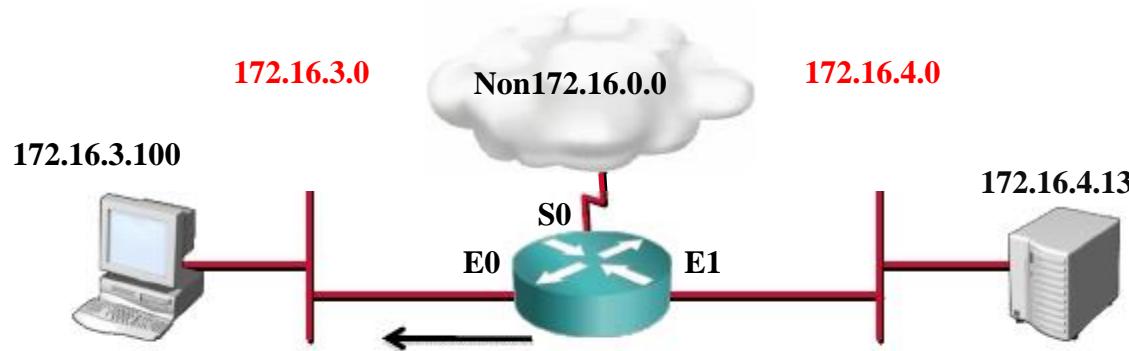
(access-list 101 deny 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

```
Router(config)#interface ethernet 0
```

```
Router(config-if)#ip access-group 101 out
```

- deny list는 172.16.4.0 Subnet에서 172.16.3.0 subnet으로 가는 FTP Traffic을 거부한다.
- permit은 다른 모든 IP Traffic이 E0 Interface로 나가는 것을 허용한다.

확장 ACL 설정 예제 2



```
Router(config)#access-list 101 deny tcp 172.16.4.0 0.0.0.255 any eq 23
```

```
Router(config)#access-list 101 permit ip any any
```

(ACL 엔트리에 명시적으로 추가하지 않아도 마지막 라인에 다음과 같이 모든 패킷을 거부하라는 엔트리가 포함됨)

(access-list 101 deny 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255)

```
Router(config)#interface ethernet 0
```

```
Router(config-if)#ip access-group 101 out
```

- deny list는 172.16.4.0 Subnet에서 E0 Interface로 나가는 Telnet Traffic을 거부한다.
- permit은 다른 모든 IP Traffic이 E0 Interface로 나가는 것을 허용한다.

Named ACL

- Named IP Access list 고려사항

- Named IP Access list는 IOS 11.2 이전 version에서는 호환되지 않는다
- 여러 개의 액세스 리스트에 같은 이름을 사용할 수 없다

- Named IP Access list 생성 단계

- Named IP Accesslist Mode로 이동한다

```
Router(config)#ip access-list {stanard | extended} name
```

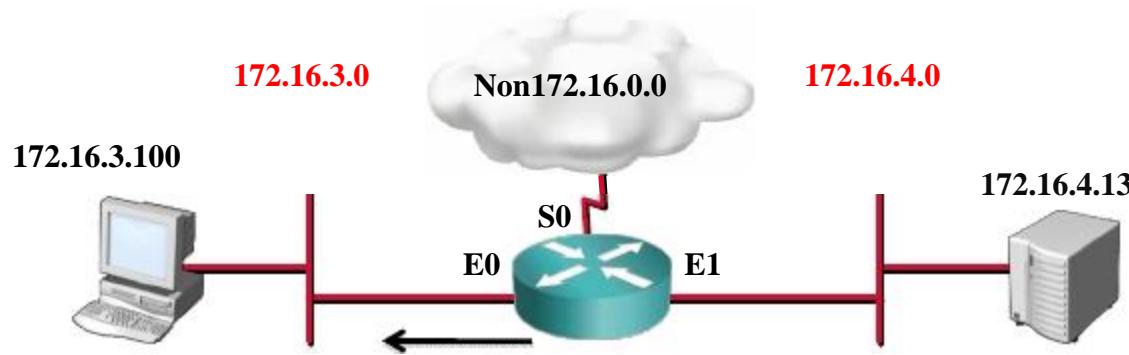
- Test 조건을 입력한다

```
Router(config-{std|ext})#{permit|deny} {test conditions}  
Router(config-{std|ext})#no {permit|deny} {test conditions}
```

- 해당 Accesslist를 Interface에 적용하기

```
Router(config-if)#ip access-group name {in | out}
```

Named ACL 설정

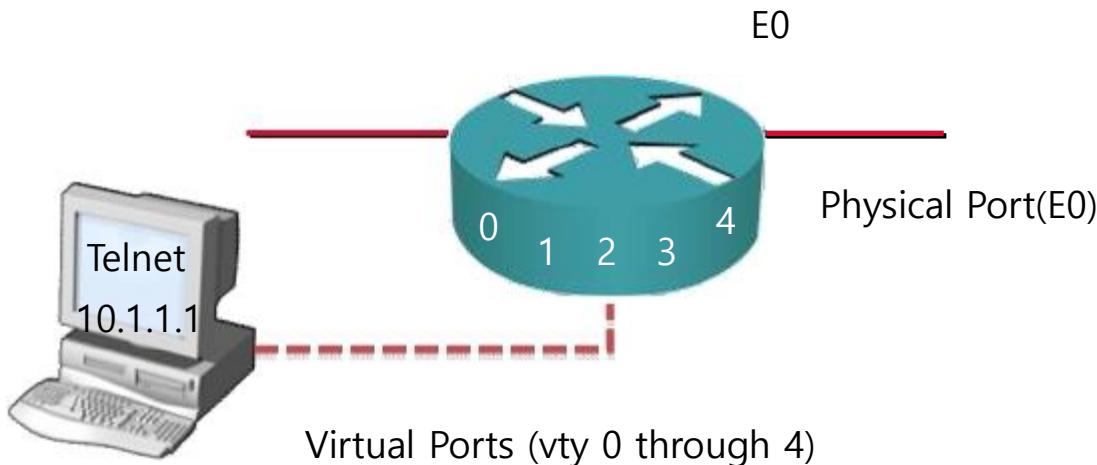


```
Router(config)#ip access-list extended screen
Router(config-ext-nacl)#deny  tcp  172.16.4.0  0.0.0.255  172.16.3.0  0.0.0.255  eq  23
Router(config-ext-nacl)#permit ip any any
```

```
Router(config)#interface ethernet 0
Router(config-if)#ip access-group screen out
```

- deny는 172.16.4.0 Subnet에서 E0 Interface로 나가는 Telnet Traffic을 거부하는 Named Access List이다.
- permit은 다른 모든 IP Traffic이 E0 Interface로 나가는 것을 허용한다.

ACL을 이용한 텔넷 접속 제한하기



- VTY는 라우터에 Telnet 접속을 위해 할당된 가상 포트이다.
- Interface를 경우해서 지나가는 트래픽이 아니기 때문에 Interface에서 제어할 수 없으므로 line vty 0 4에서 제어한다.

텔넷 접속 제한 설정

- 접속 제어 할 포트 번호를 활성화 한다

```
Router(config)#line vty {vty# | vty-range}
Router(config)#
```

- 적용할 Accesslist를 적용한다

```
Router(config-line)#access-class access-list-number {in | out}
Rotuer(config-line)#

```

텔넷 접속 제한 설정 예제

- Controlling Inbound Access

```
Router(config)#access-list 12 permit 192.168.1.0 0.0.0.255  
(implicit deny all)
```

```
Router(config)#line vty 0 4  
Router(config-line)#access-class 12 in  
Router(config-line)#{
```

- 192.168.1.0/24 Subnet에 해당하는 IP Address를 갖는 호스트만 접속을 허용한다

ACL문 모니터링

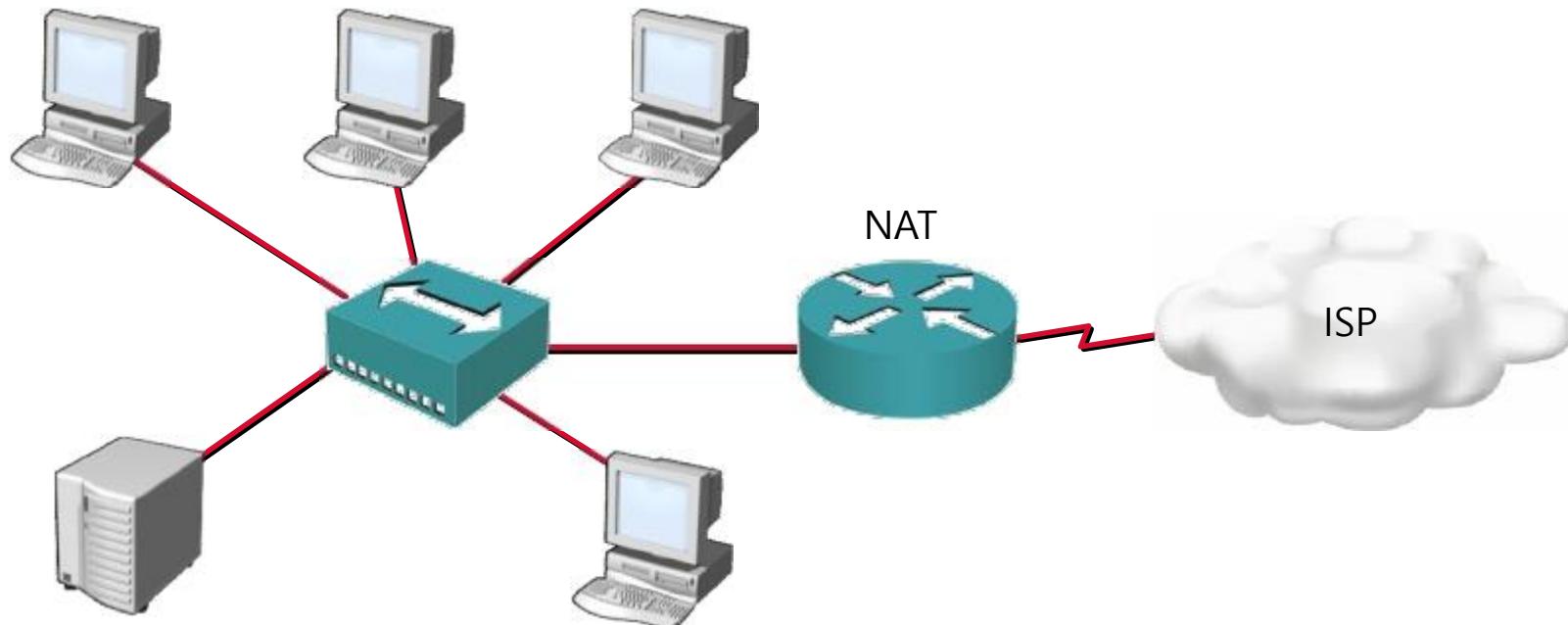
```
Router#show {protocol} access-list {access-list number}
```

```
Router#show access-list {access-list number}
```

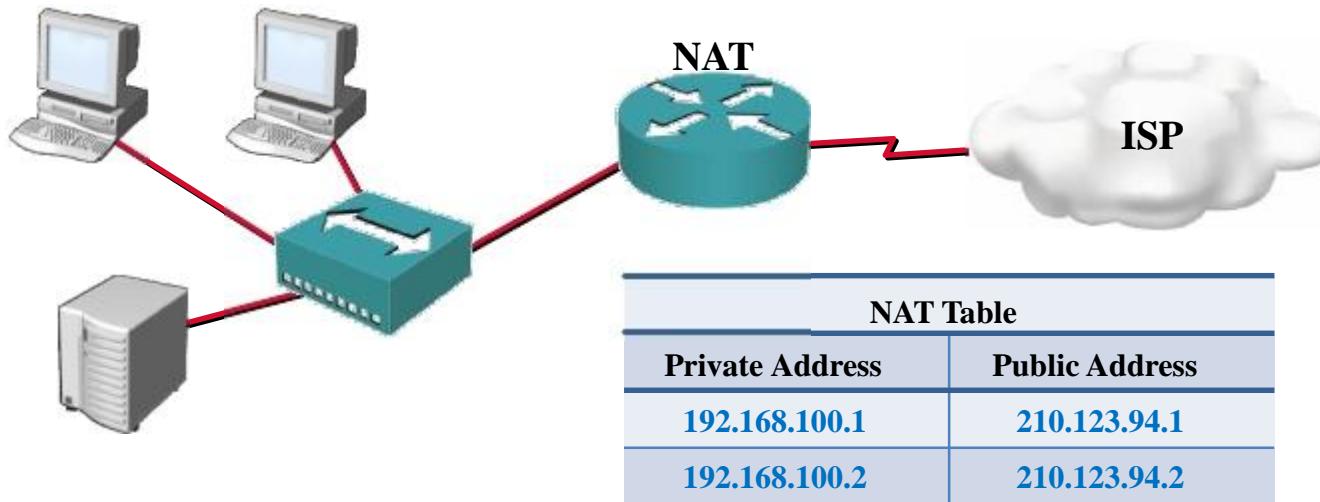
```
Router#show access-lists
Standard IP access list 1
    permit 10.2.2.1
    permit 10.3.3.1
    permit 10.4.4.1
    permit 10.5.5.1
Extended IP access list 101
    permit tcp host 10.22.22.1 any eq telnet
    permit tcp host 10.33.33.1 any eq ftp
    permit tcp host 10.44.44.1 any eq ftp-data
```

NAT (Network Address Translation)

- NAT는 RFC 1631에 정의된 것으로 IP Header의 주소를 다른 주소로 바꾸는 기술이다.
NAT는 사설주소(RFC 1918)를 사용하는 호스트들이 인터넷에 서비스를 이용할 수 있도록 하기 위해 사용한다

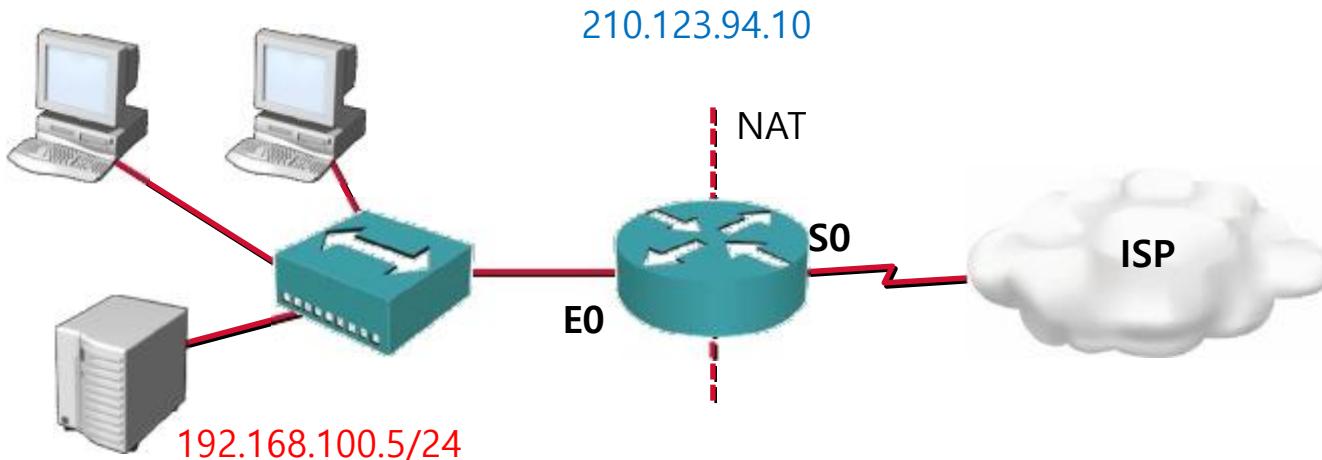


Static NAT와 Dynamic NAT



- 정적 NAT는 외부주소로 들어온 요청을 내부 서버로 전달 될 수 있도록 목적지 주소를 변환하는 기능이다. 이 방법으로 사설망 서버를 구현하고 외부 주소로 들어오는 연결을 내부 서버로 전달할 수 있다.
- 동적 NAT는 호스트가 요구하는 Traffic을 받으면 IP 주소내에서 사설 IP를 라우터에 설정된 주소 Pool에 있는 공인 IP로 변환한 후 외부로 전달한다. 외부에서 응답 신호가 라우터로 돌아오면 NAT라우터는 NAT Table에 있는 이전 정보로 들어온 주소를 사설 IP로 변환해서 내부망으로 전달한다.

Static NAT 설정



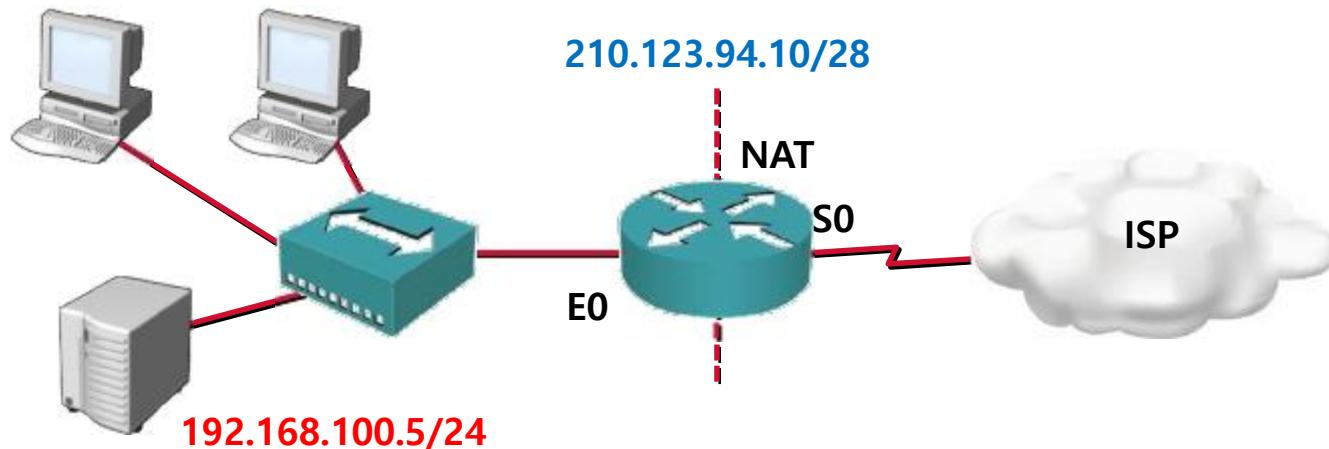
- 정적 변환을 수립하기 위한 **NAT** 설정을 한다.

```
Router(config)#ip nat inside source Static local-ip global-ip
```

- 각 인터페이스로 이동 후 내부와 외부를 각각 설정한다.

```
Router(config-if)#ip nat inside  
Router(config-if)#ip nat outside
```

Static NAT 설정 예제



```
NAT(config)#ip nat inside source static 192.168.100.5 210.123.94.10  
  
NAT(config)#int e0  
NAT(config-if)#ip nat inside  
NAT(config-if)#int s0  
NAT(config-if)ip nat outside
```

Dynamic NAT Configuration

- IP 변환에 사용할 전역 주소풀을 설정한다.

```
Router(config)#ip nat pool name start-ip end-ip {netmask Netmask |  
prefix-length Prefix-length}
```

- 내부에서 IP변환을 허용할 주소를 Standard Accesslist로 정의한다.

```
Router(config)#Access-list number permit source-address [Wildcard-mask]
```

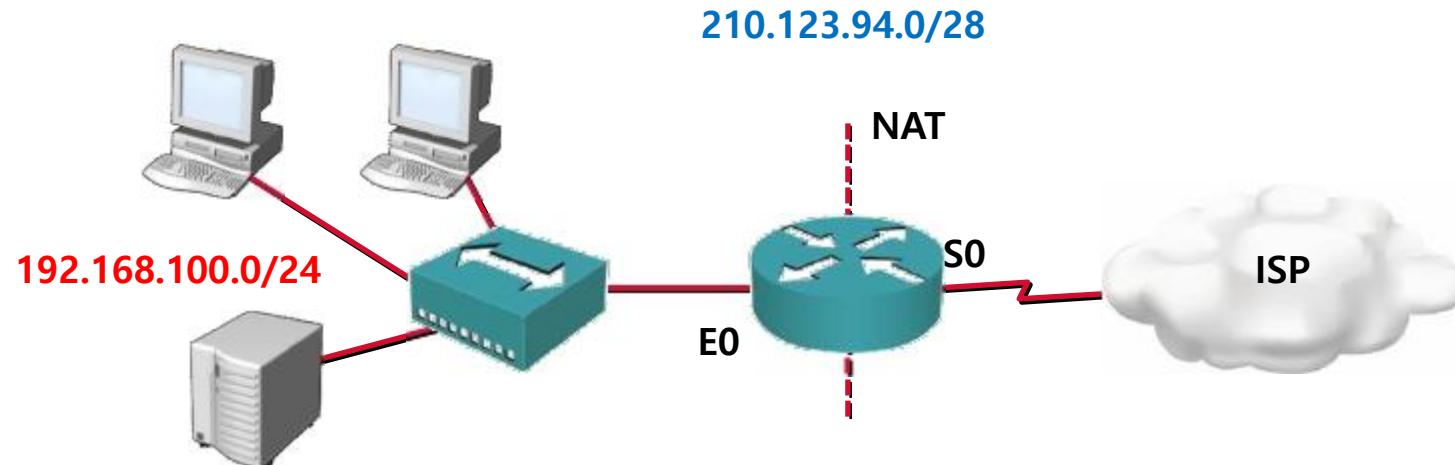
- 동적 변환을 수립하기 위한 NAT 설정을 한다.

```
Router(config)#ip nat inside source list Access-list-number pool name  
[overload]
```

- 각 인터페이스로 이동 후 내부와 외부를 각각 설정한다.

```
Router(config-if)#ip nat inside  
Router(config-if)#ip nat outside
```

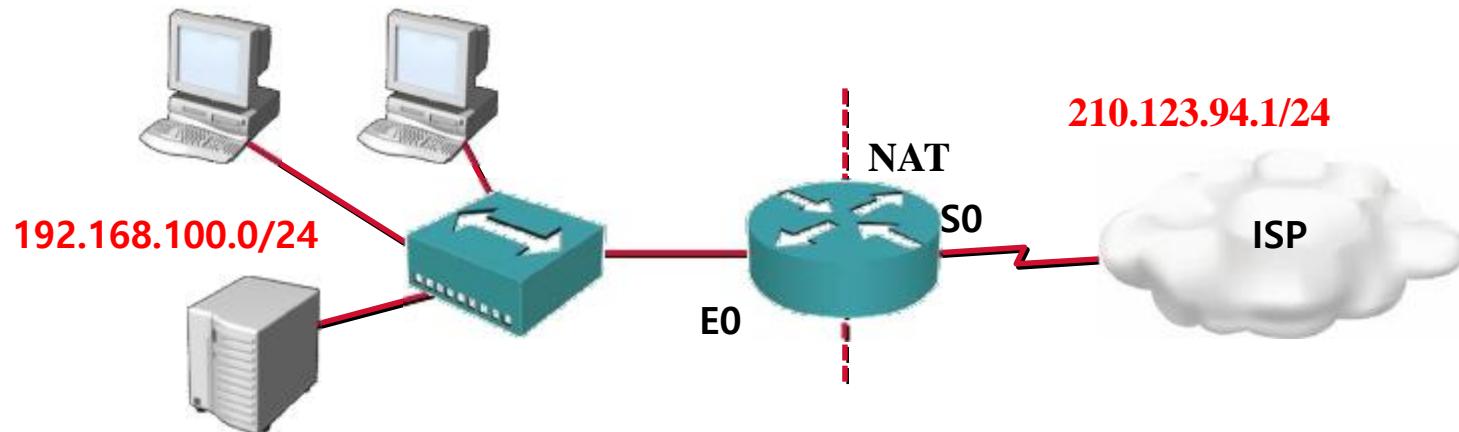
Dynamic NAT 예제



```
NAT(config)#ip nat pool Pub_IP 210.123.94.1 210.123.94.14 netmask 255.255.255.240  
NAT(config)#access-list 50 permit 192.168.100.0 0.0.0.255  
NAT(config)#ip nat inside source list 50 pool Pub_IP
```

```
NAT(config)#int e0  
NAT(config-if)#ip nat inside  
NAT(config-if)#int s0  
NAT(config-if)#ip nat outside
```

Dynamic NAT 예제



```
NAT(config)#ip nat inside source list 1 interface serial 0 overload  
NAT(config)#access-list 1 permit 192.168.100.0 0.0.0.255
```

```
NAT(config)#int e0  
NAT(config-if)#ip nat inside  
NAT(config-if)#int s0  
NAT(config-if)#ip nat outside
```

NAT 모니터링

- NAT 변환테이블 삭제

```
Router#clear ip nat translation *
```

- 활성화된 변환 정보 보기

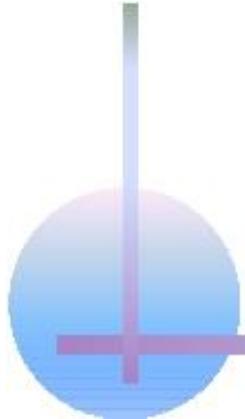
```
Router#show ip nat translations
```

- 변환된 통계 정보 보기

```
Router#show ip nat statistics
```

- NAT 변환 상태 모니터링

```
Router#debug ip nat
```



Module 07

WAN Service

WAN(Wide Area Network) 개요

WAN은 LAN(Local Area Network)과는 달리 거리가 먼 지역에서도 데이터를 전송할 수 있도록 해준다. LAN은 소규모 지역이나 빌딩 안의 워크스테이션, 주변 장치, 터미널 그리고 기타 장비들을 연결하는 네트워크다.

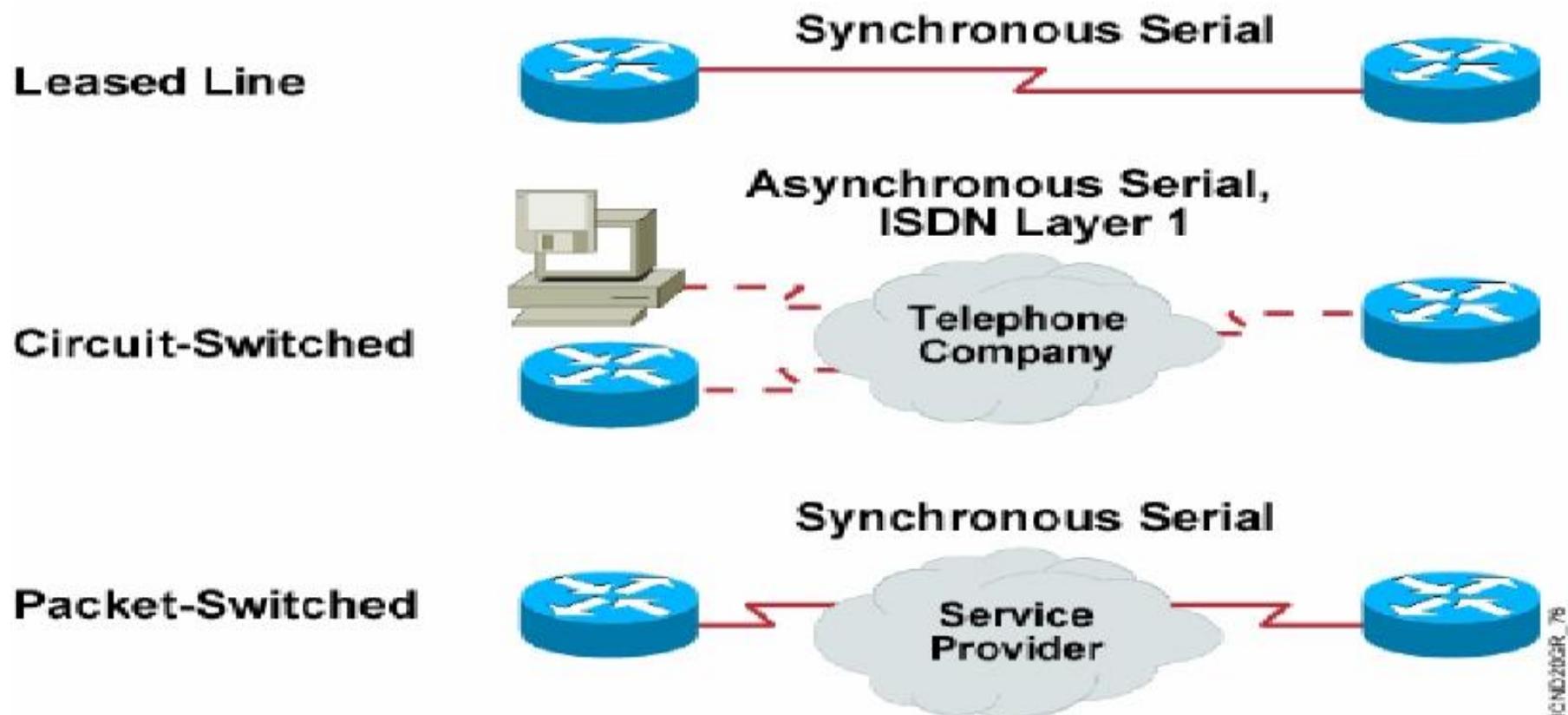
기업들은 아래 그림과 같이 멀리 떨어져 있는 기업 내의 사이트들 간에 정보를 주고받을 수 있도록 WAN 연결 서비스를 이용한다.



이러한 커넥션은 사용자의 요구사항과 비용 그리고 이용가능성에 의존적이다.

WAN 연결 옵션

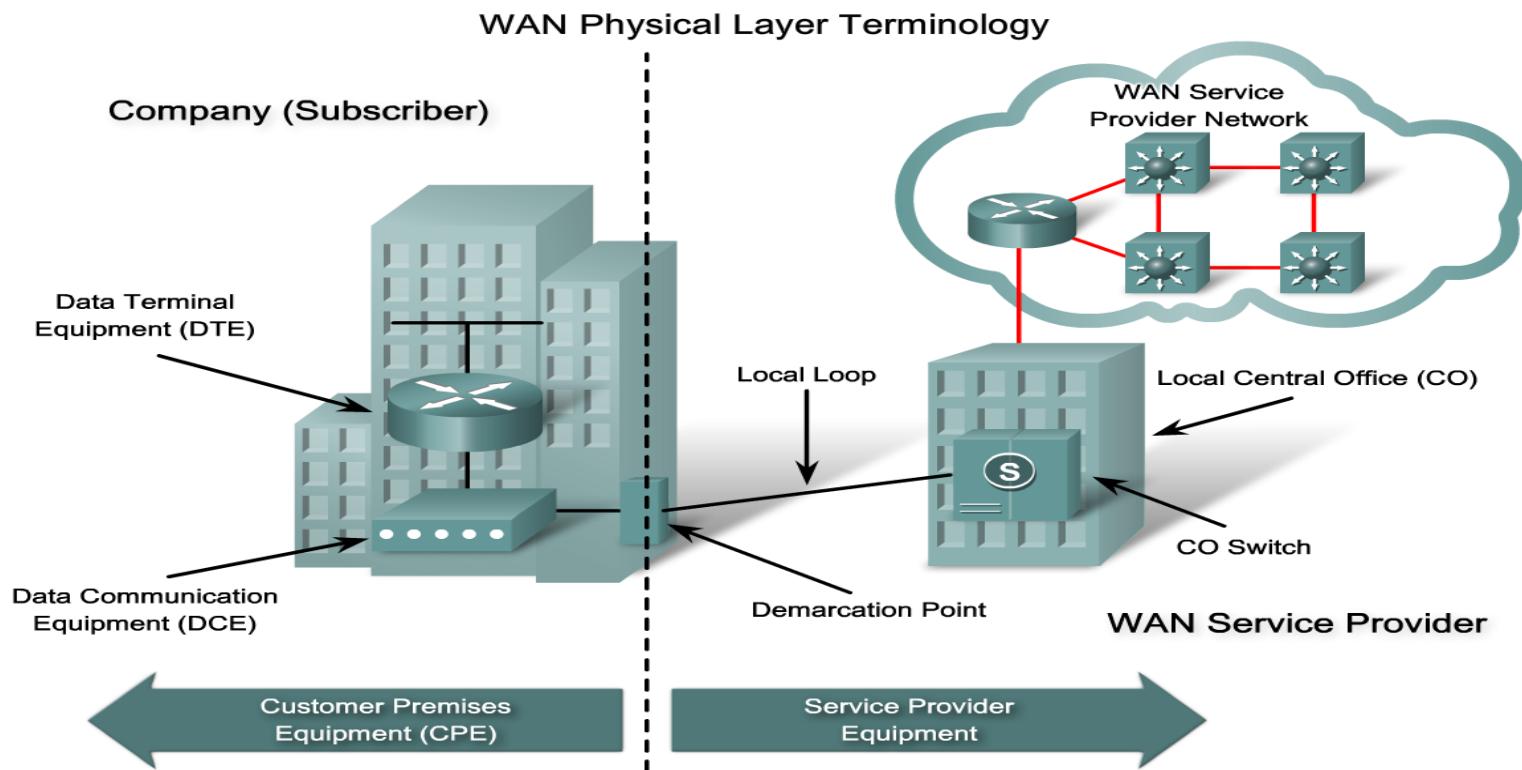
WAN 연결에서 많은 옵션을 선택할 수 있다. 그러나 모든 지역에서 이러한 서비스를 모두 제공할 수 있는 것은 아니다. 다음에 세 가지 유형의 WAN연결 서비스를 보여준다. 각각 다음과 같은 특징을 갖는다.



- **임대 회선** : 사용 고객만 전용으로 이용할 수 있도록 서비스 제공 업체에서 보장한다. 임대 회선을 사용하면 네트워크 망을 공유하면서 고려해야 하는 프라이버시, 보안, 그리고 연결 과정과 연결 종료 과정 등을 고려하지 않아도 되지만 그만큼 많은 비용을 지불해야 한다. 대부분 동기 시리얼 연결로 T3/E3 또는 45Mbps의 대역폭 서비스를 지원하며, 이 속도는 항시 보장된다.
- **회선 교환** : 회선 교환은 서비스 제공업체에서 사용하는 방법으로 기본 전화 서비스 또는 ISDN과 같은 서비스를 제공할 때 이용된다. 전화 접속 요청이 이루어질 때마다 송수신자 간의 회선이 확립된다. 이 연결은 사용자가 회선을 사용하는 동안 계속 유지되지만, 재 연결을 할 때마다 같은 회선을 사용하는 것은 아니다. 회선 교환 연결은 일반적으로 백업 링크 혹은 작은 대역폭을 요구하는 연결과 같이 산발적인 WAN 연결이 필요할 때 주로 사용된다.
- **패킷 교환** : 서비스 제공업체에서 제공하는 공유된 인터네트워크 망을 이용해서 송신지에서 수신지로 패킷을 전달할 때, 단일 점 대 점 연결이나 점 대 다중점 링크를 공유하는 네트워크 장비에서 사용하는 WAN 스위칭 방법이다. 패킷 교환 인터네트워크는 END-TO-END 연결을 위한 방법으로 PVC나 SVC를 이용한다.
- **셀 교환** : 패킷 교환 방법과 비슷하지만 가변적인 길이의 패킷을 이용하는 것이 아니라 고정된 길이의 셀을 이용하며, 가상 회선을 통해 전송한다. 셀 교환 연결은 구리 케이블을 이용할 경우 T1에서 DS3(45Mbps)까지의 속도를 제공하며, 광 케이블을 이용할 경우 OC-192(약 10Gbps)까지의 속도를 제공한다. 셀 교환 방법의 특징은 빠른 속도와 더불어 질 높은 QoS 제공 및 음성이나 비디오와 같은 멀티미디어에 적합하다는 점이다. 대표적인 셀 교환 서비스로 ATM을 꼽을 수 있다.

WAN 기술 용어

WAN 기술에 관련된 서비스와 장비들을 설명하는 많은 용어와 개념이 있다.
몇몇 기본적인 용어들은 반드시 이해하고 있어야 한다.



기업에서 인터넷워크 자원을 활용하기 위해 외부 서비스 제공업체로부터 WAN 서비스를 제공 받을 때, 서비스 제공업체는 기업에 WAN 링크를 구성할 수 있도록 여러 가지 매개 변수를 할당한다.

WAN Serial Line 표준

시리얼 임대 회선이나 프레임 릴레이 연결과 같은 패킷 교환 WAN 연결을 이용한 동기 전송을 위해서 시스코에서는 다음과 같은 물리적 계층의 시리얼 표준을 지원한다.

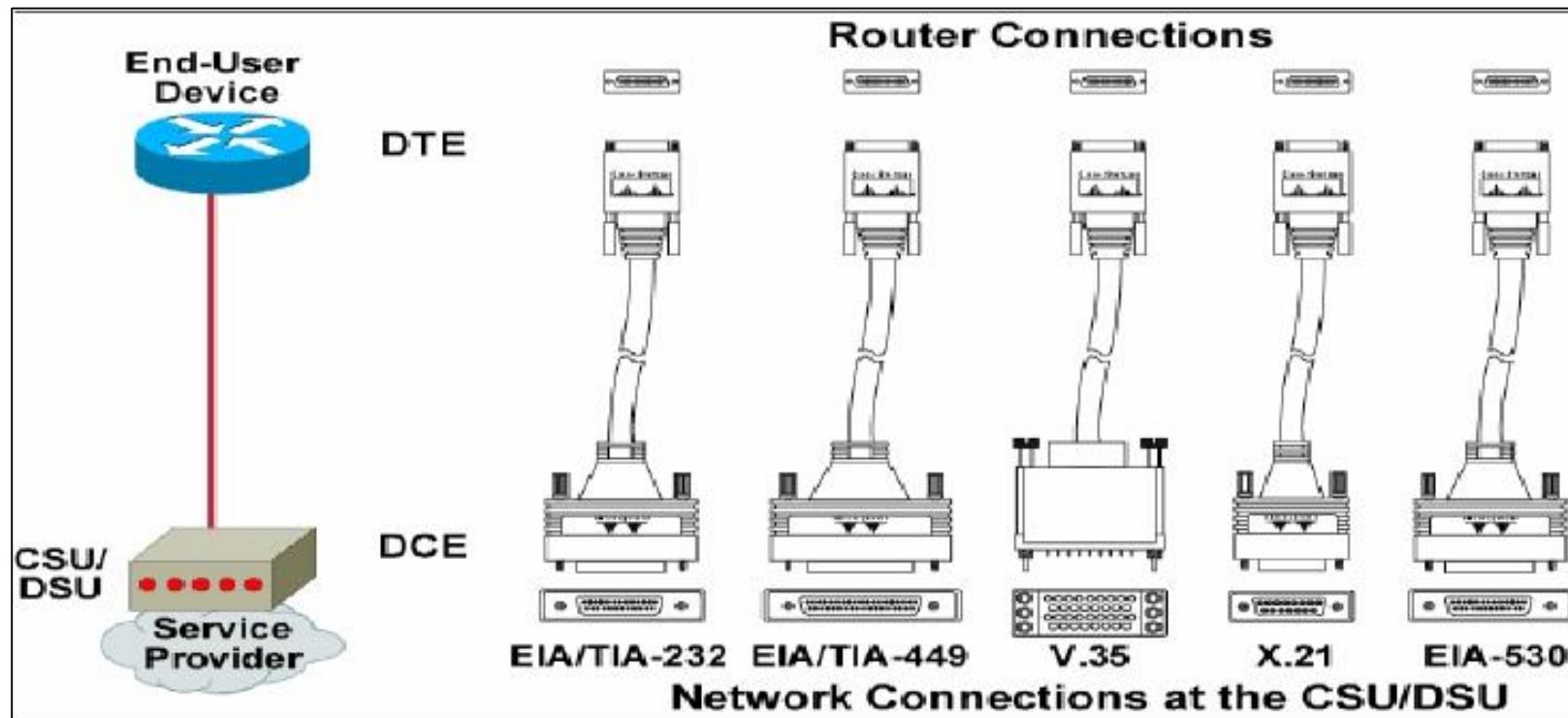
EIA/TIA-232

EIA-TIA-449

V.35

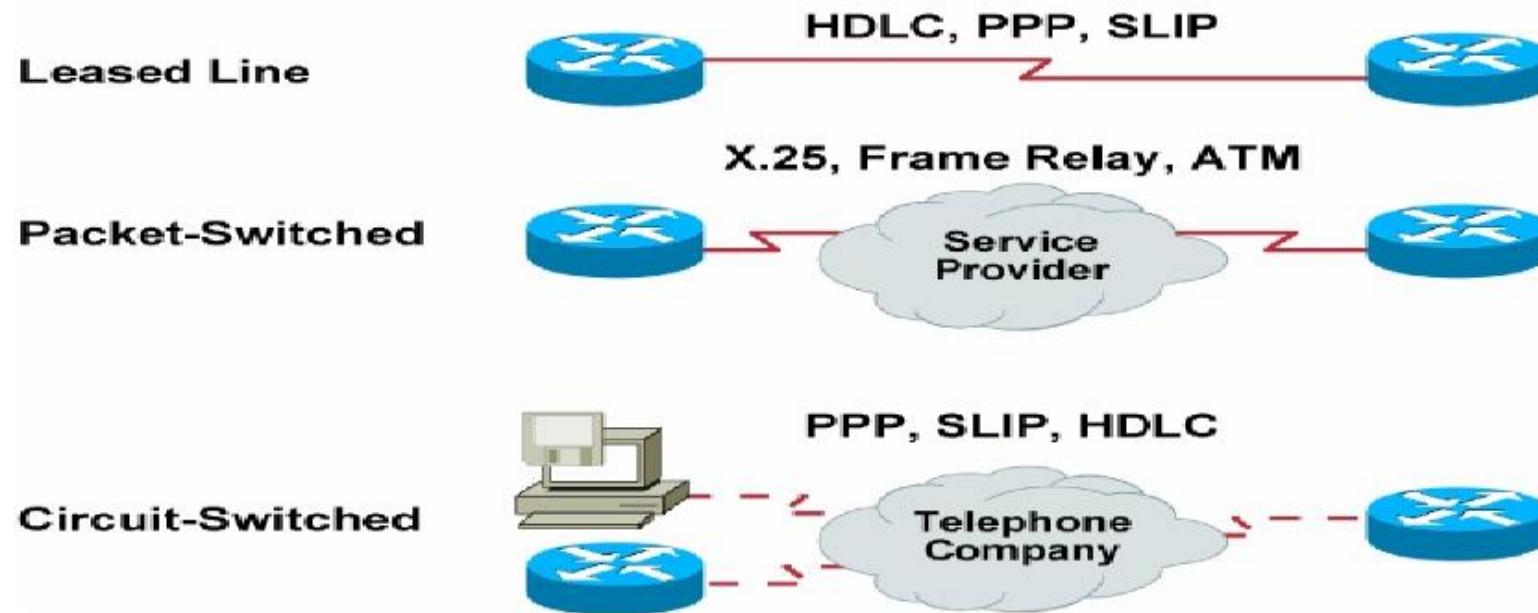
X.21

EIA-530



WAN 2계층 캡슐화

OSI 모델에서 물리적 계층에서부터 상위 계층으로 전이하는 경우, 시리얼 장비에서는 반드시 데이터 링크 계층(2계층)에서 프레임 형식으로 데이터를 캡슐화해야 한다. 적합한 프로토콜을 사용하려면 적절한 데이터 링크 계층의 캡슐화 방법을 반드시 설정해야 한다. 프로토콜은 WAN 기술과 통신 장비에 따라 다양하게 선택될 수 있다.



시스코 HDLC : 시스코 라우터에서는 cHDLC가 기본 캡슐화 방법이며, 이는 점 대 점 연결과 회선 교환 연결 방식에 이용된다. 시스코 HDLC는 시스코 장비간의 통신을 위해 사용되는 동기 방식의 데이터 링크 프로토콜이다.

WAN 2계층 캡슐화

- PPP : PPP는 동기와 비동기 회선을 포함하여 다양한 물리적 인터페이스 표준을 통해 라우터 사이와 호스트 및 네트워크 사이의 연결에 사용되는 표준 프로토콜이다. PPP는 IP와 같이 다양한 네트워크 계층 프로토콜과 연동될 수 있도록 고안되었다. 그리고 PAP와 CHAP와 같은 보안 메커니즘을 포함한다.
- SLIP : SLIP는 TCP/IP를 이용하는 점 대 점 시리얼 연결 표준 프로토콜이다. PPP가 보편적으로 사용되면서 SLIP를 대체하였다.
- X.25/LAPB : LAPB는 ITU-T 표준 프로토콜이며, DTE와 DCE 간의 연결 상태와 원격 터미널 접속 유지 그리고 불안정한 링크 사이의 컴퓨터 통신 제어 등을 정의한다. X.25는 데이터 링크 프로토콜로 LAPB를 이용한다.
- 프레임 릴레이 : 프레임 릴레이는 다중 가상 회선을 제어하는 ISDN 프레임 기술을 토대로 패킷 교환 방법을 정의하는 산업 표준 데이터링크 계층 프로토콜이다. 프레임 릴레이는 X.25를 보다 발전시킨 것으로, 기존의 불안정한 통신 링크 간의 에러 제어나 흐름 제어와 같은 불필요한 기능들을 제거하여 빠른 전송 속도를 보장할 수 있도록 하였다.
- ATM : ATM은 다양한 서비스 유형의 데이터(음성, 비디오, 데이터)를 포함한 셀을 전달하는 국제 표준이며, 고정 길이의(53바이트) 셀을 교환한다. 고정된 길이로 셀을 나누는 과정은 하드웨어에서 일어나며, 전송 지연을 줄이는 장점이 있다. ATM은 T3, E3 그리고 SONET과 같은 초고속 전송 미디어의 장점을 이용할 수 있도록 고안되었다.

HDLC 캡슐화 설정

다음은 ISO 표준 HDLC와 시스코 전용 HDLC 프레임을 나타낸다.

Cisco HDLC

Flag	Address	Control	Proprietary	Data	FCS	Flag
------	---------	---------	-------------	------	-----	------

Standard HDLC

Flag	Address	Control	Data	FCS	Flag
------	---------	---------	------	-----	------

CISCO HDLC에는 Proprietary Data 필드가 있으며, 이는 다중 상위 프로토콜을 지원하기 위함이다.

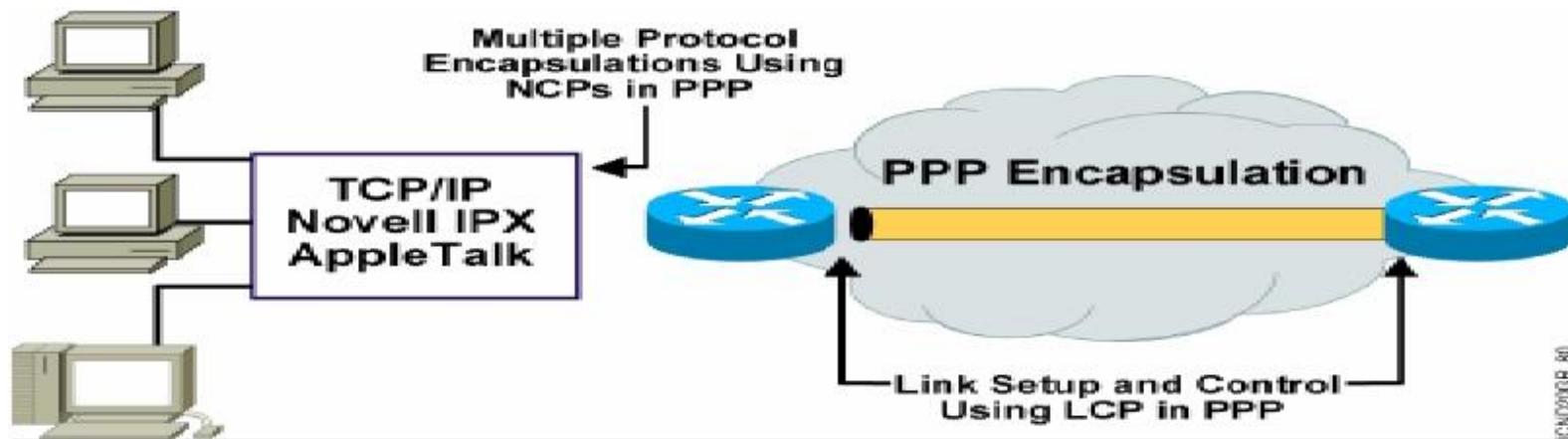
표준 HDLC는 1개의 상위 프로토콜만을 지원한다.

기본적으로 시스코 라우터에서는 동기 시리얼 라인에 시스코 HDLC 시리얼 캡슐화 방법을 사용한다. 그러나 시리얼 인터페이스에 이미 다른 캡슐화 프로토콜이 설정되어 있는 상태에서 HDLC 캡슐화 프로토콜을 사용하려면 변경하려는 인터페이스 설정 모드로 들어가서 HDLC로 변경해야 한다. 아래에는 구성하는 명령어를 보여준다.

```
Router(config-if)#encapsulation hdlc
```

PPP 캡슐화

PPP는 HDLC와는 달리 특정 장비에서만 사용되는 프로토콜이 아니며, 프레임 내부에 PPP임을 식별하는 필드를 포함한다. 이러한 특징 때문에 다른 벤더의 장비 사이에서 PPP를 사용할 수 있다.

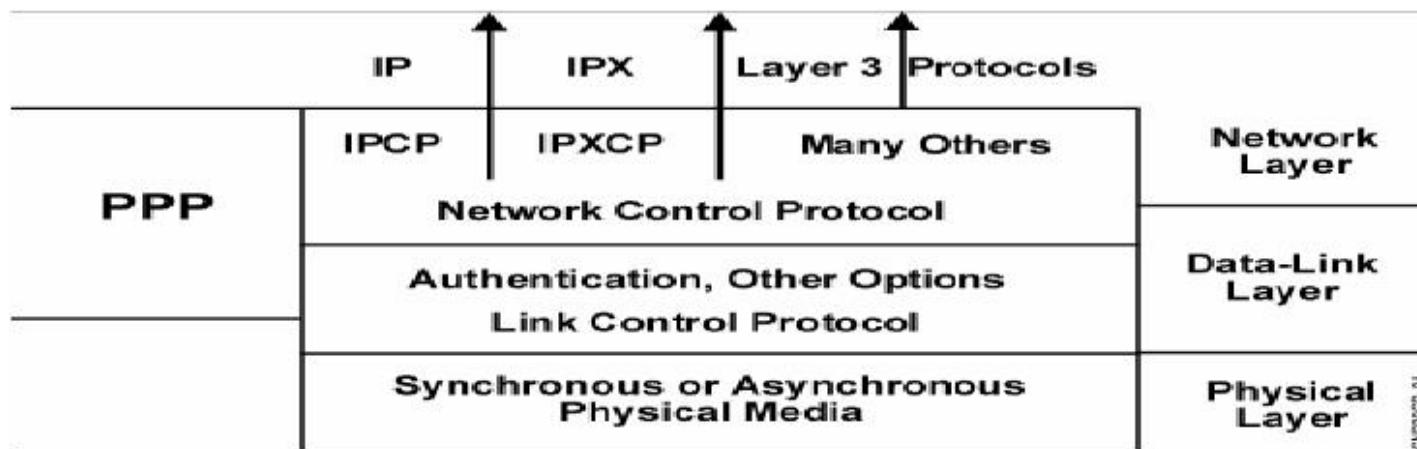


인터넷 개발자는 점 대 점 링크 연결을 위해 PPP를 고안했다.
아래와 같은 물리적 인터페이스에서 PPP를 설정할 수 있다.

- 비동기 시리얼 인터페이스
- ISDN
- 동기 시리얼 인터페이스
- HSSI(High-Speed Serial Interface)

PPP 구성요소 : NCP와 LCP

기능적인 관점에서 PPP는 데이터 링크 프로토콜 역할을 담당하지만, 네트워크 계층 서비스를 협상할 수 있는 기능도 가지고 있다. 이러한 이유로 PPP는 2개의 하위 계층으로 나누어진다. 이러한 하위 계층은 PPP의 기능을 더욱 확장시켰다.



PPP는 다중 상위 프로토콜을 캡슐화하기 위해 PPP의 구성 요소인 NCP를 이용한다. 또한 PPP는 WAN 데이터 링크 연결을 위한 옵션의 협상 및 초기 연결 설정을 위해 중요한 구성 요소인 LCP를 이용한다.

이러한 하위 계층 기능을 통해 PPP는 다음의 매체를 이용할 수 있다.

- 동기 연결을 이용하는 매체
- 모뎀을 이용한 전화 연결 서비스와 같은 비동기 연결을 이용하는 매체
- ISDN

PPP 구성요소 : NCP와 LCP

PPP는 데이터 링크 설정을 제어하는 풍부한 서비스를 제공한다. 이러한 서비스들은 LCP의 옵션 필드에서 구현되며, 일반적으로 관리자가 의도하는 점 대 점 연결을 위해 프레임을 검사하고 옵션을 협상한다.

인증을 포함한 다양한 옵션들을 이용할 수 있는 PPP는 캡슐화 계층 프로토콜로서 전화 접속 네트워크 연결에 상당히 유용하다.

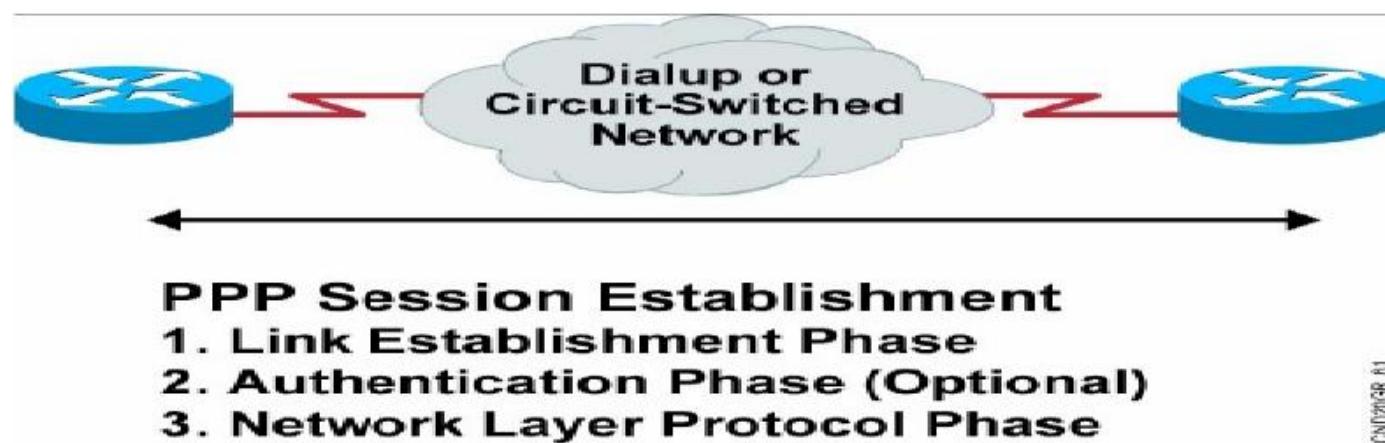
상위 계층 프로토콜을 지정할 수 있는 기능을 이용하여, PPP는 NCP를 통해 다양한 네트워크 계층 프로토콜들을 전송할 수 있다. 이와 같은 기능을 담당하는 필드는 PPP가 캡슐화하는 네트워크 계층 프로토콜을 지정하는 표준 코드를 포함한다.

LCP 옵션

특징	프로토콜	구현과정
인증	PAP CHAP	패스워드가 필요하다. 요구핸드쉐이크를 사용한다.
압축	Stacker 또는 Predictor	송신지에서 데이터를 압축하며 수신지에서 압축을 해제한다.
에러검출	MagicNumber Quality	링크에서 제거되는 데이터를 모니터한다. 프레임 루프을 방지한다.
다중링크	다중링크프로토콜	다중링크를 통해 로드밸런싱을 구현한다.

PPP 연결 확립 과정

PPP를 이용하여 장비 간에 통신을 하려면 프로토콜은 먼저 세션을 만들어야 한다. 아래 그림은 연결 확립 과정을 단계별로 보여준다.



- PPP세션은 다음의 세 단계를 거쳐 연결된다.

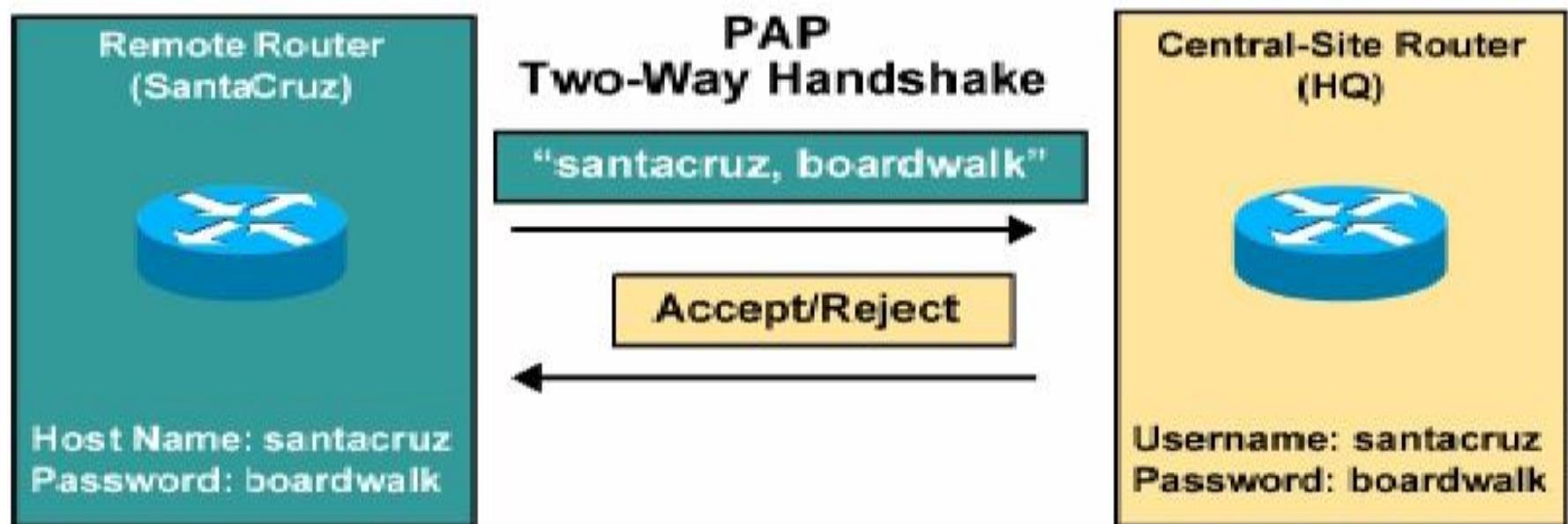
1. 링크 연결 확립 단계
2. 인증 확인 단계(옵션)
3. 네트워크 계층 프로토콜 연계 단계

PPP 캡슐화와 인증방법 설정

PAP과 CHAP 인증 방법

PAP 인증방법

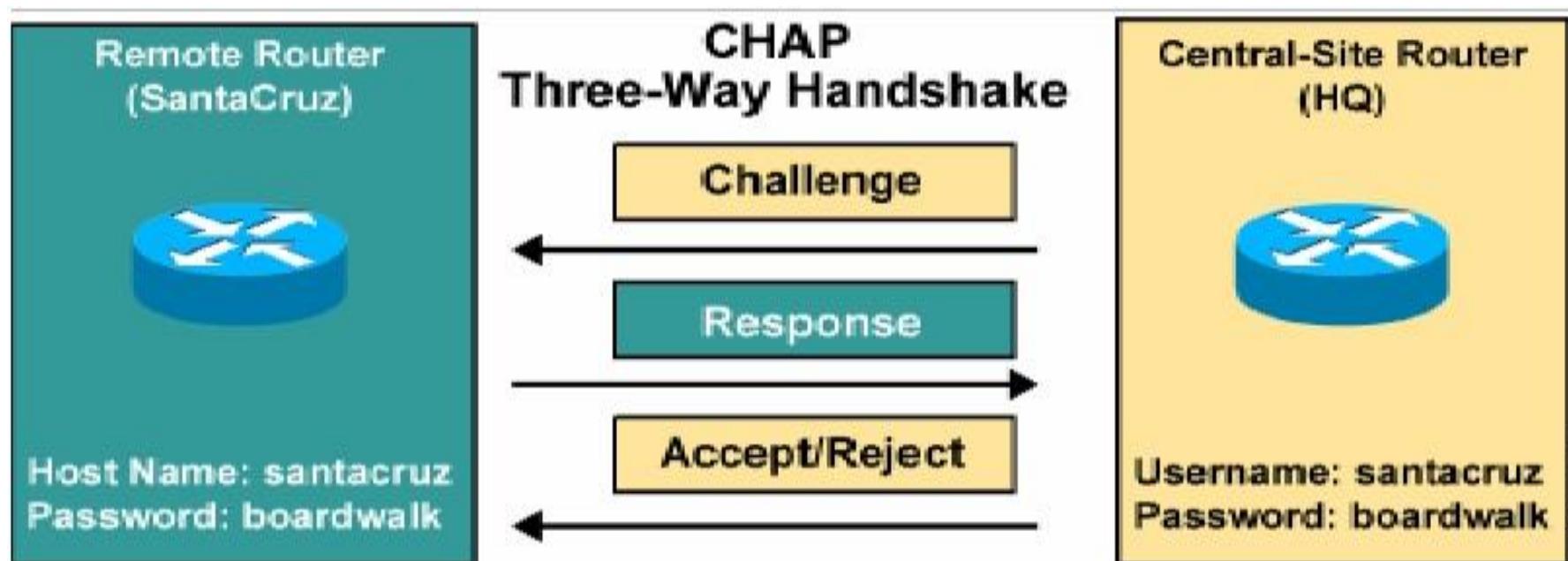
PAP는 양방향 인증 과정을 통해 원격 사용자를 확인하는 간단한 인증 방법을 제공한다. 그러나 처음 연결하는 과정에서만 인증 과정을 거치기 때문에 CHAP에 비해 보안성이 약하다.



PPP 캡슐화와 인증방법 설정

CHAP 인증 방법

CHAP는 PAP에 비해 보안성이 뛰어난 인증 방법이다. CHAP는 초기 링크의 연결 과정에서 사용되며 신뢰성 있는 원격지 노드인지를 확인하기 위해서 주기적으로 쓰리웨이 핸드쉐이크 방법을 사용한다.



PPP 캡슐화와 인증(PAP/CHAP) 구현

PPP 인증을 설정하기 전에 인터페이스에 PPP 캡슐화를 설정해야 한다. 인터페이스 설정 모드에서 PPP캡슐화를 설정한다. 인터페이스 설정 모드에서 encapsulation PPP 명령어를 입력하여 해당 인터페이스에서는 PPP를 캡슐화 방법으로 사용한다는 것을 지정한다.

```
Router(config-if)#encapsulation ppp
```

그리고 다음과 같이 PAP 또는 CHAP의 인증 방법을 설정할 수 있다.

1단계 : 우선 각 라우터의 호스트 이름을 확인한다. 호스트 이름은 상대편 라우터에서 인증을 확인하는 데 사용하게 된다. 라우터가 상대편에서 'username'을 이용해서 전송한 호스트 이름을 수신하면 지역의 데이터 베이스에서 해당하는 패스워드를 검색한다. 호스트 이름을 설정하려면 글로벌 모드에서 hostname **name** 을 입력하면 된다.

2단계 : 각 라우터에서는 글로벌 모드에서 username **name** password **password** 명령어를 이용하여 상대편 라우터의 호스트 이름과 해당하는 패스워드를 정의한다.

PPP 캡슐화와 인증(PAP/CHAP) 구현

```
Router(config)#hostname name
```

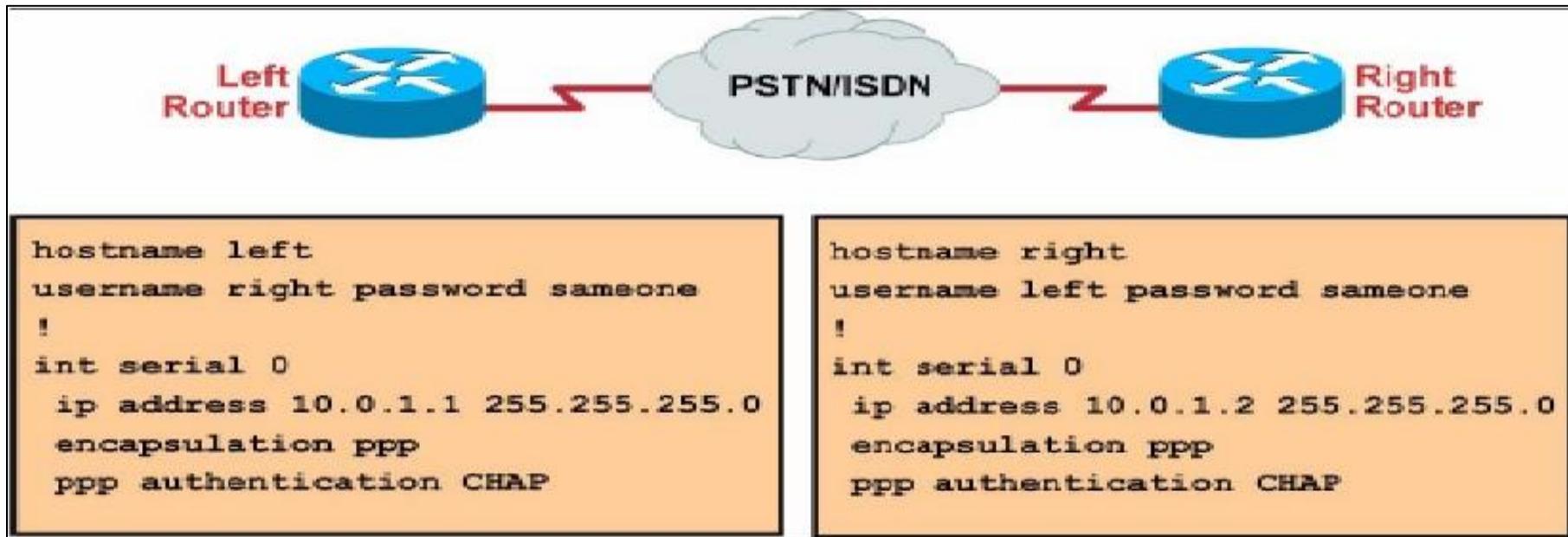
```
Router(config)#username name password password
```

Name은 상대편 라우터의 호스트 이름에 해당한다. 대소문자를 구별하기 때문에 유의하도록 한다.
password 옵션은 연결 과정에서 사용할 패스워드다. 반드시 양쪽 사이에 동일한 패스워드를 지정해야 한다.

3단계 : 인터페이스 설정 모드에서 ppp authentication 명령어를 입력하여 PPP 인증 방법을 지정한다.
다음과 같이 입력하면 된다.

```
Router(config-if)# ppp authentication {chap | chap pap | pap chap | pap }
```

PAP/CHAP 구현 예제

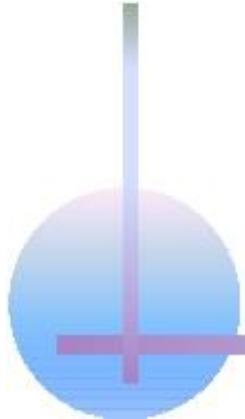


점 대 점 CHAP 인증 설정을 나타낸다. 두 라우터 모두 상대편 라우터에 인증을 요청하고 또 요청을 수락해야 한다. CHAP 인증 명령어를 보면 서로 반대되는 것을 확인할 수 있다. 지역 라우터의 호스트 이름과 패스워드는 반드시 상대편 라우터에서 지정하는 **username name** **password password** 명령어와 일치해야 한다. 다시 말하면, CHAP에서 지정하는 **username**은 상대방 라우터의 호스트 이름에 해당한다. 아울러 두 라우터에서는 모두 동일한 패스워드를 설정해야 한다.

PPP 캡슐화 설정 확인

PPP를 설정하고 링크에서 이를 사용할 때는 show interface 명령어를 수행하여 LCP와 NCP 상태를 점검해야 한다. show interface 명령어를 사용하면 이를 확인할 수 있다. 다음은 show interface 명령어를 수행했을 때의 결과 값을 나타낸다.

```
Router#show interface s0
Serial0 is up, line protocol is up
Hardware is HD64570Internet address is 10.140.1.2/24
MTU 1500 bytes, BW 1544 Kbit, DLY 20000 usec, rely 255/255, load 1/255
Encapsulation PPP, loopback not set, keepalive set (10 sec)
LCP Open
Open: IPCP, CDPCP
Last input 00:00:05, output 00:00:05, output hang never
Last clearing of "show interface" counters never
Queueing strategy: fifo
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
38021 packets input, 5656110 bytes, 0 no buffer
Received 23488 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
38097 packets output, 2135697 bytes, 0 underruns
0 output errors, 0 collisions, 6045 interface resets
0 output buffer failures, 0 output buffers swapped out
482 carrier transitionsDCD=up DSR=up RTS=up CTS=up
```



Module 08 IPv6

IPv6의 필요성

- 1) 스마트폰 등 IP를 요구하는 다양한 기기의 등장으로 IPv4 주소 고갈
- 2) 보안 취약성 해소
- 3) 멀티미디어/실시간 트래픽 처리 능력 개선

IPv6 주요특징

- **Larger address space:** Global reach capability, flexibility, aggregation, multihoming, autoconfiguration, “plug-and-play,” renumbering
- **Simpler header:** Routing code streamlined, simpler processing in hardware
- **Security and mobility:** Built into the standard, not as extensions
- **Transition richness:** Several mechanisms available, including “dual-stacking”

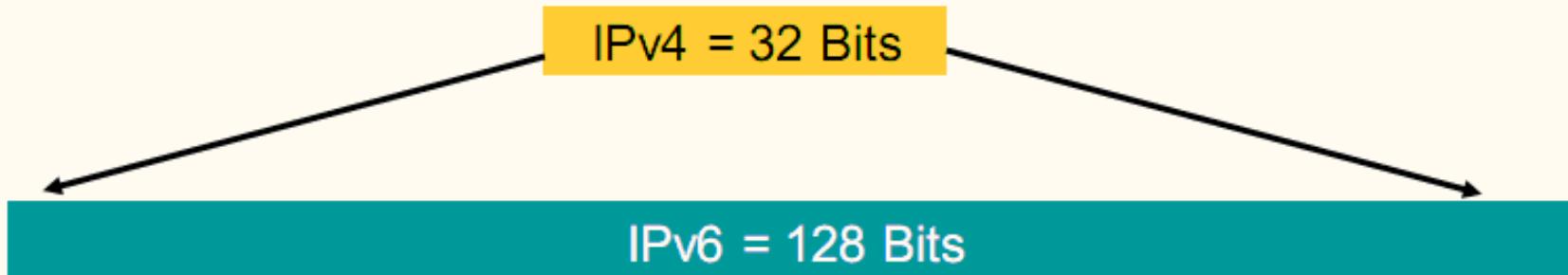
넓은 주소공간

IPv4:

- 32 bits
- = 4,294,967,296 possible addressable nodes

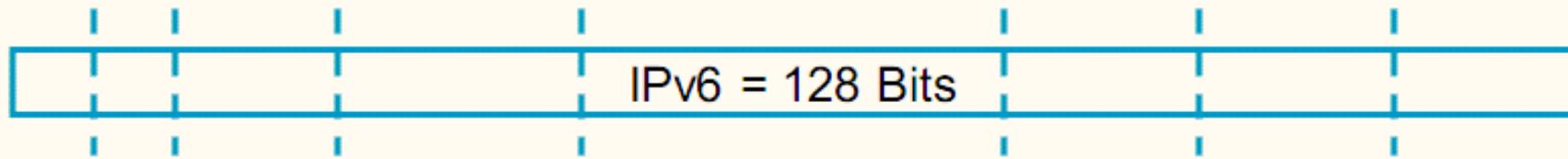
IPv6:

- 128 bits: 4 times larger in bits
- = $\sim 3.4 \times 10^{38}$ possible addressable nodes
- = 340,282,366,920,938,463,463,374,607,431,768,211,456



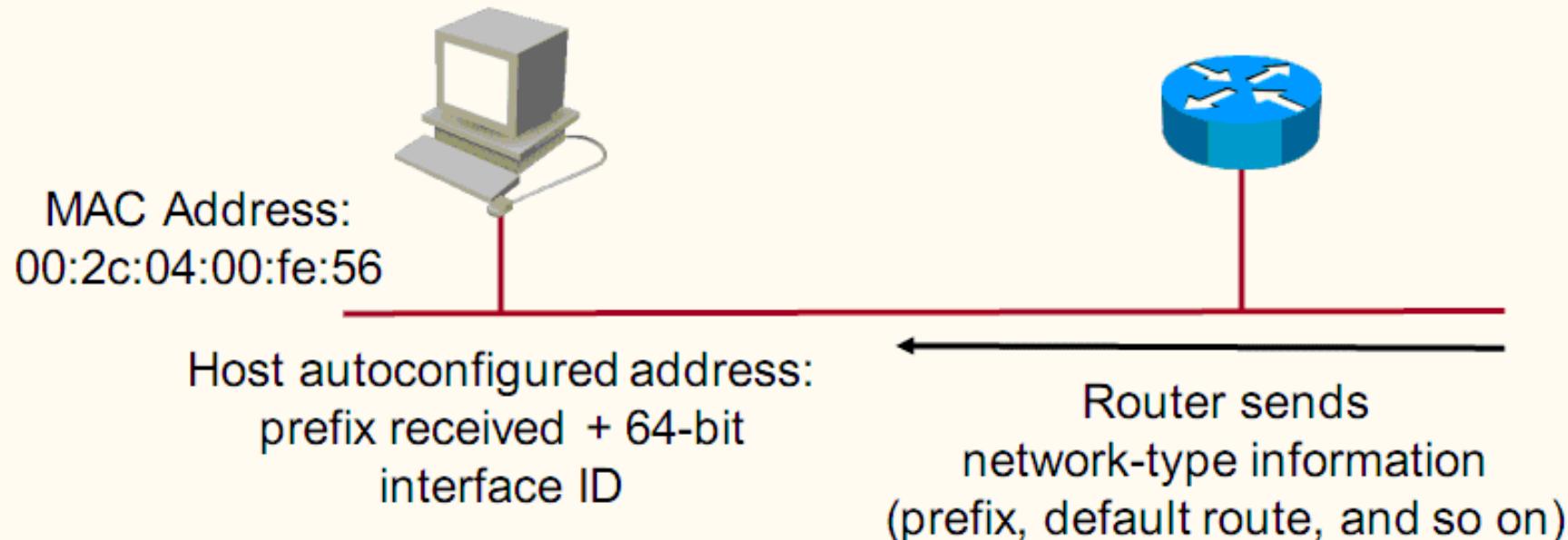
주소의 계층적 구조

- Multiple levels of hierarchy inside the address space allow better segmentation of the network to follow organizational structure (/48 or /56 given to end users)
- More flexibility, more privacy, new functionalities



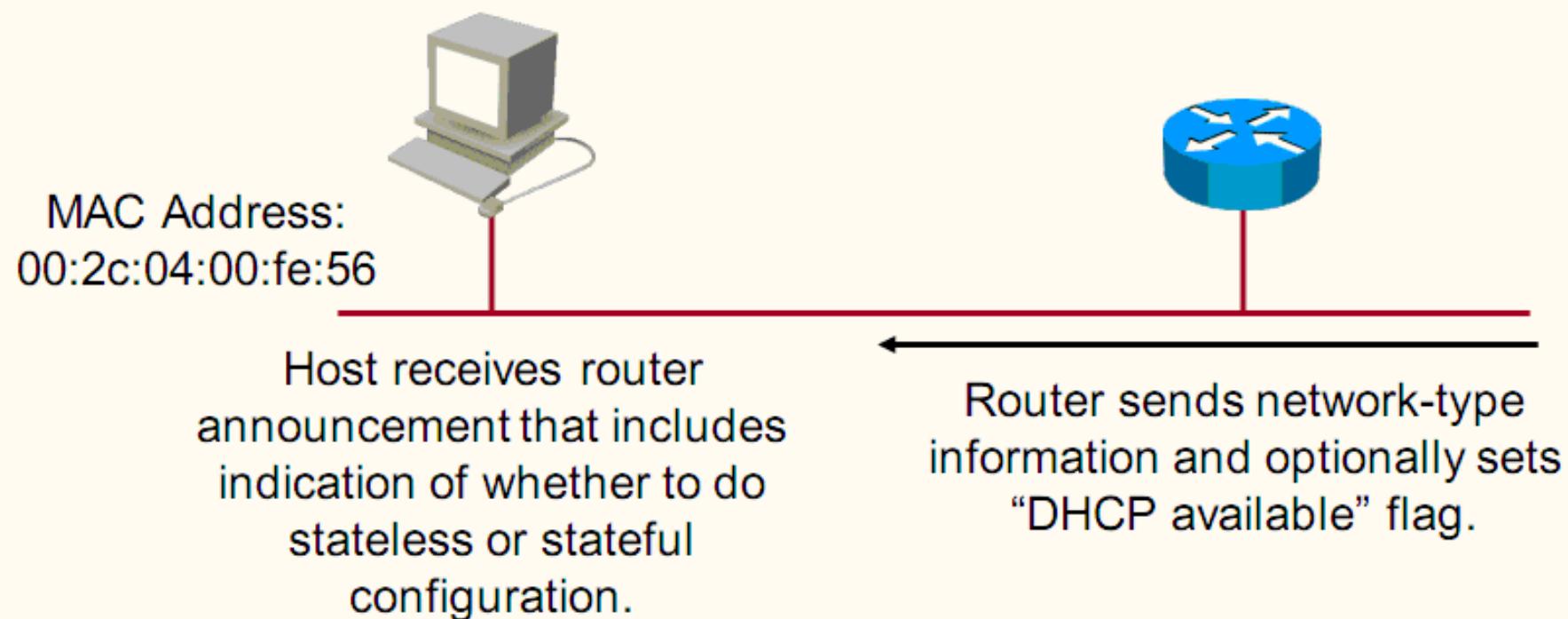
Stateless Autoconfiguration(비상태보존형 자동설정)

- Often uses Layer 2 identifier (derived from OUI)
- Autoconfiguration with no collisions
- “Plug-and-play”
- Suitable for embedded networks for industrial use (dispersed seismic sensors, etc.), but lack of capability to communicate DNS settings



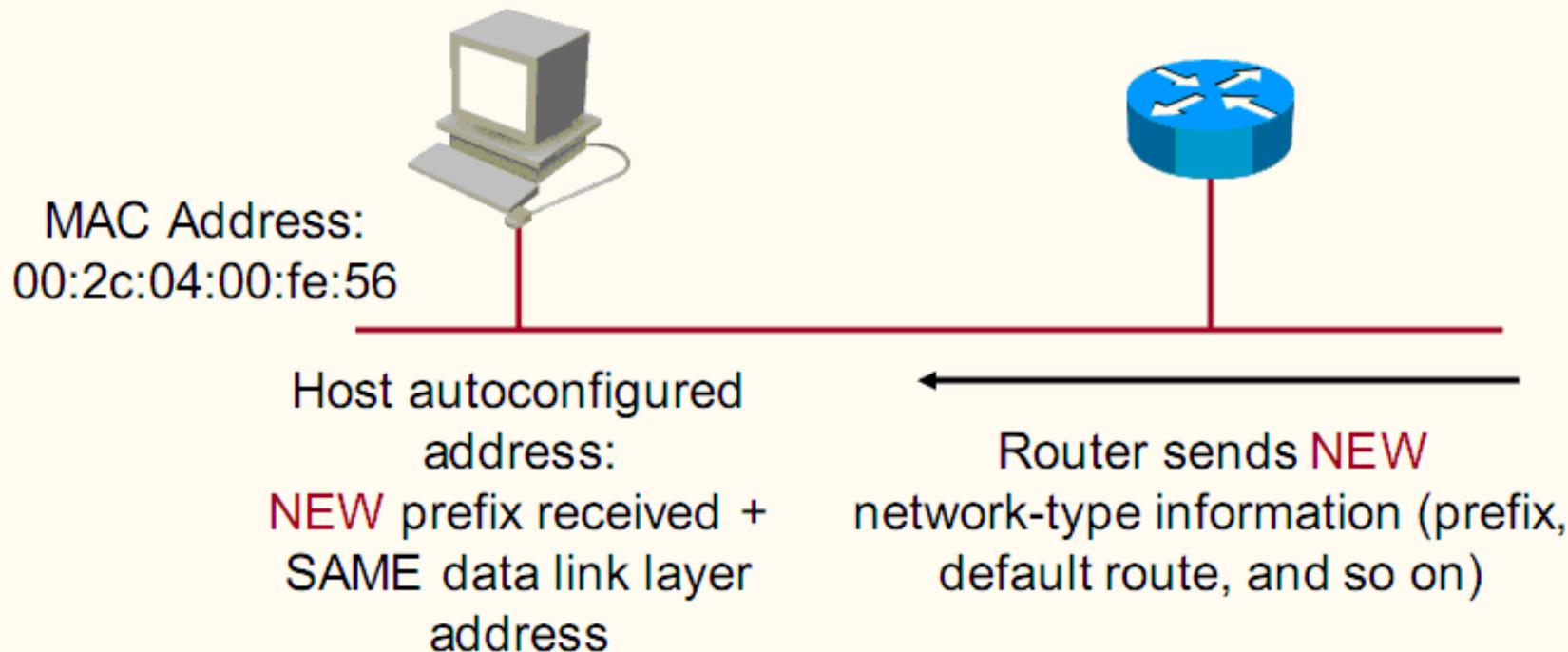
Stateful Autoconfiguration (상태보존형 자동설정)

- Router announcement can indicate to hosts whether or not additional configuration parameters are available via stateful configuration (DHCPv6), such as DNS, IP options, and so on.



Renumbering(주소 재지정)

- Renumbering, using autoconfiguration and multiple addresses
- Old address still held for a time for possible incoming traffic; new address is used for outgoing connections first

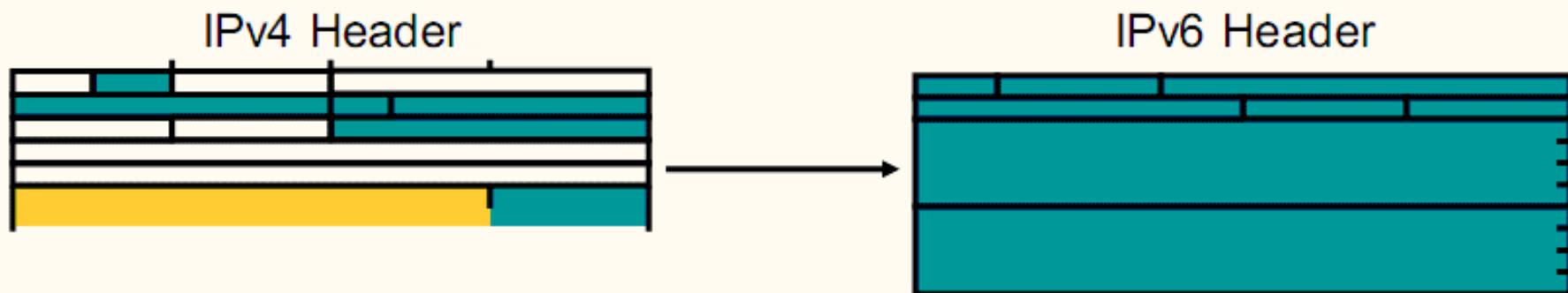


Multicast 사용

- Broadcasts in IPv4:
 - Interrupt all computers on the LAN, even if the destination is only one or two computers
 - Can completely bring down a network (“broadcast storm”)
- No broadcast in IPv6:
 - Replaced by scoped multicast
- Multicast:
 - Enables efficient use of the network
 - Has much larger address range

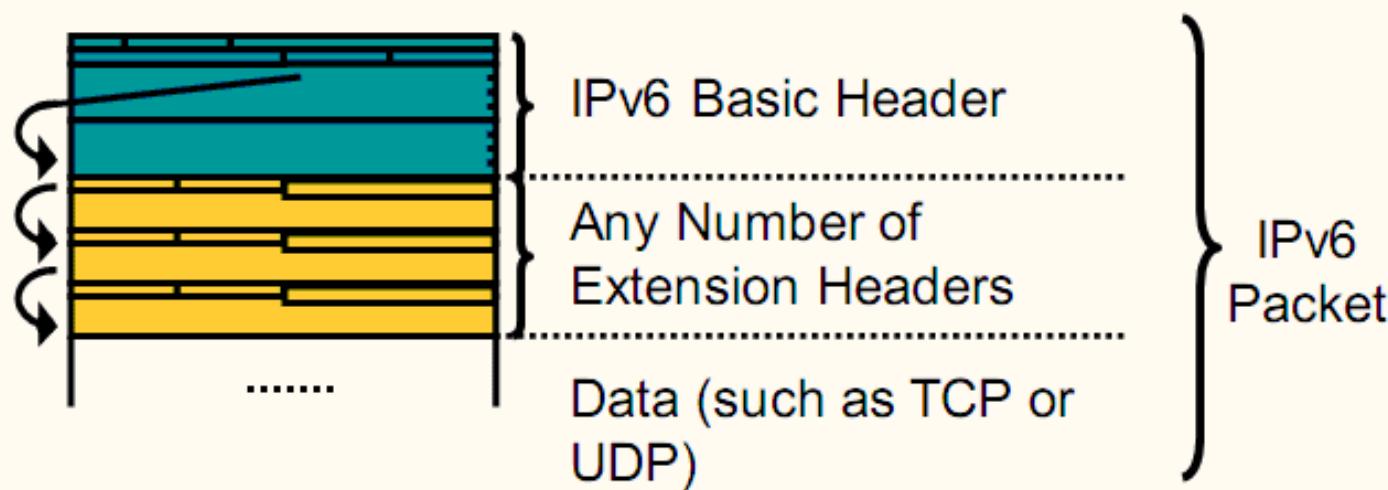
단순하고 효율적인 헤더

- 64-bit aligned fields and fewer fields
- Hardware-based, efficient processing
- Improved routing efficiency, performance, and forwarding rate scalability



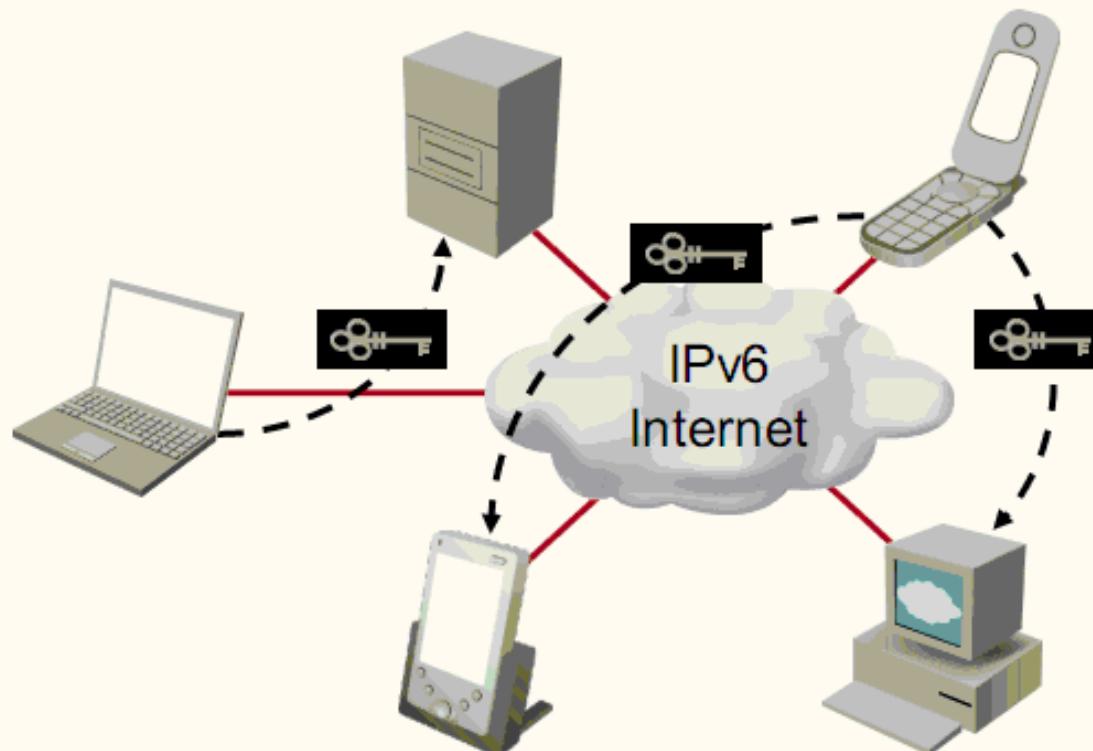
Extension Headers (확장 헤더)

- Flexible extension headers
- More efficient handling of IP options
- Faster forwarding rate and end-node processing



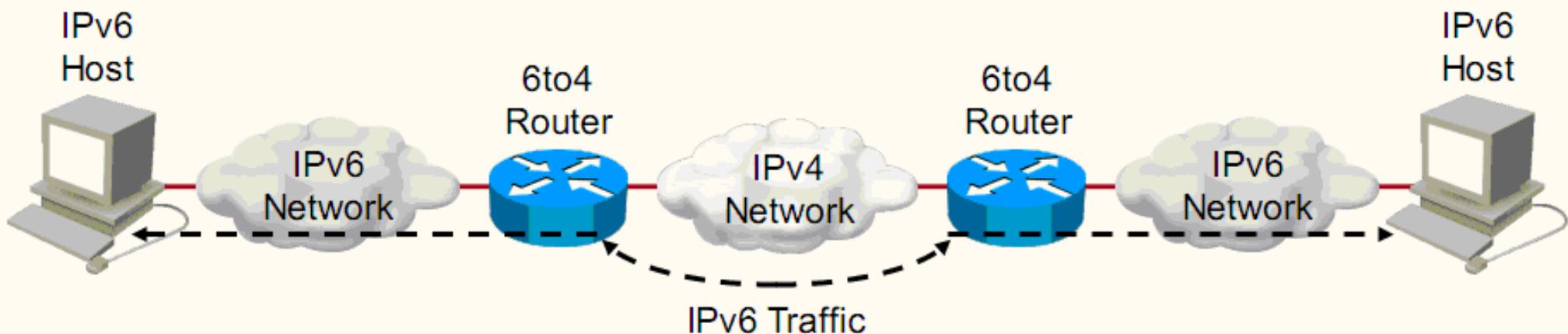
Security (보안성)

- End-to-end network security (integrity, authentication, confidentiality)
- Inherent (built-in) with IPv6—usable by any node



Transition Richness (IPv4에서 IPv6 변환)

- No fixed day to convert, no need to convert all at once
- Different transition mechanisms available:
 - Smooth integration of IPv4 and IPv6
- Different compatibility mechanisms:
 - Communication between IPv4 and IPv6 nodes



IPv6 vs IPv4 Technology 비교

IP Service	IPv4 Solution	IPv6 Solution
Addressing Range	32-bit, Network Address Translation	128-bit, multiple scopes
Autoconfiguration	DHCP	Stateless, Stateful (DHCPv6)
Security	IPsec	IPsec-mandated, works end-to-end
Mobility	Mobile IP	Mobile IP with optimized routing
QoS	Differentiated service, integrated service	Differentiated service, integrated service
IP Multicast	IGMP, PIM, Multicast BGP	MLD, PIM, multicast BGP, scope identifier

IPv6 address 표기법

Address Representation: Format

- x:x:x:x:x:x:x, where x is a 16-bit hexadecimal field:
 - Example: 2001:0DB8:010F:0001:0000:0000:0000:0ACD
 - Case-insensitive
- Leading zeros in a field are optional:
 - Example: 2001:DB8:10F:1:0:0:0:ACD
- Successive fields of 0 are represented as “::”, but only once in an address:
 - Example: 2001:DB8:10F:1::ACD

IPv6 address 표기법

Address Representation: Example

- Full address:
 - 2001:0DB8:0000:0000:FFFF:0000:0000:0ADC
- Correct representations:
 - 2001:DB8::FFFF:0:0:ADC
 - 2001:DB8:0:0:FFFF::AD
- Incorrect representation:
 - 2001:DB8::OFF::AD

IPv6 address 표기법

Address Representation: Further Examples

Full Address	Correct Representation
FF02:0:0:0:0:0:1	FF02::1
FF15:0:0:0:0:1:c001	FF15::1:C001
0:0:0:0:0:0:1	::1
0:0:0:0:0:0:0	::

IPv6 address 표기법

URL

`http://2001:DB8:1003::F:8080/index.html`

- Is 8080 part of the address or a port number?

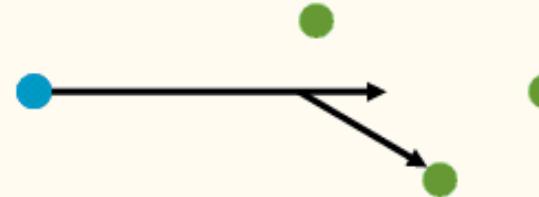
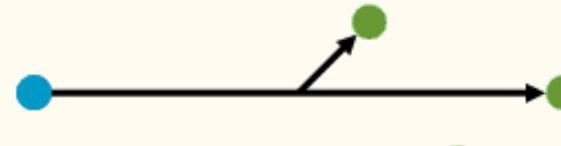
In a URL, the address is enclosed in brackets:

- Example: `http://[2001:DB8:1003::F]:8080/index.html`
- Not a new concept: works with IPv4 addresses
- Cumbersome for users
- Mostly for diagnostic purposes
- Use FQDNs whenever possible

Address 형태

Address Types

- Unicast
- Multicast
- Anycast
- No broadcast in IPv6



Unicast

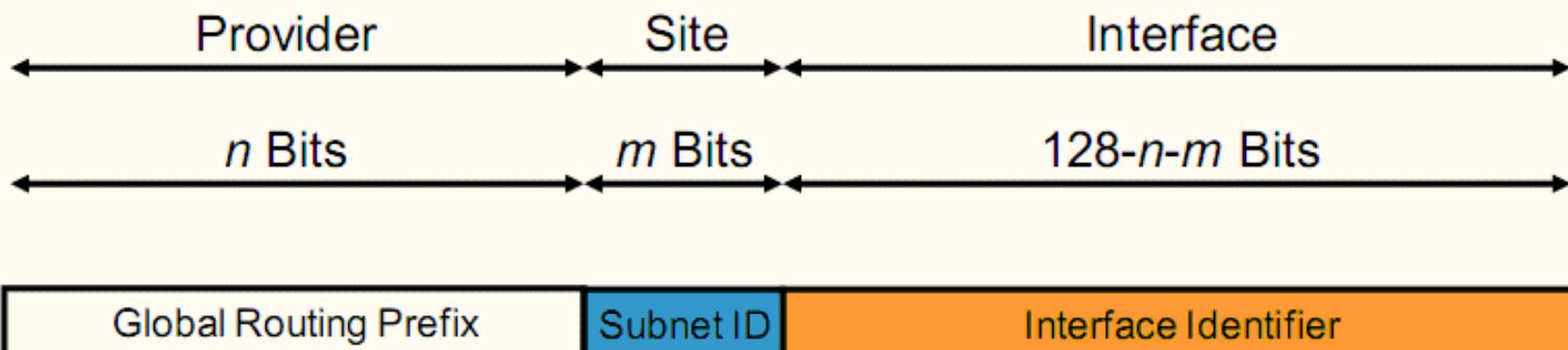
Unicast

- Unicast addresses are used in a one-to-one context.
- IPv6 unicast addresses:
 - Global unicast addresses
 - Link-local addresses
 - Unique local addresses
 - Special-purpose unicast:
 - Unspecified
 - Loopback
 - IPv4-mapped

Global Unicast 주소

Global Unicast Addresses

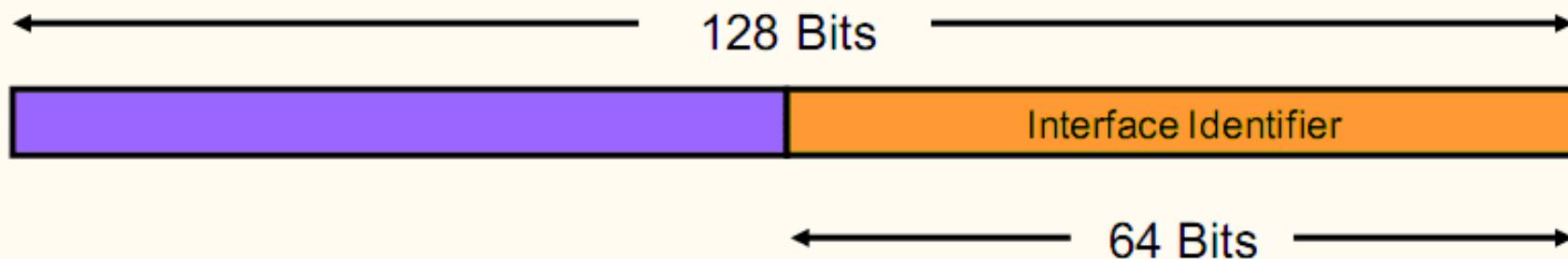
- Global unicast addresses are addresses for generic use of IPv6
- Interface identifier should be kept at 64 bits



Interface Identifiers

Interface Identifiers

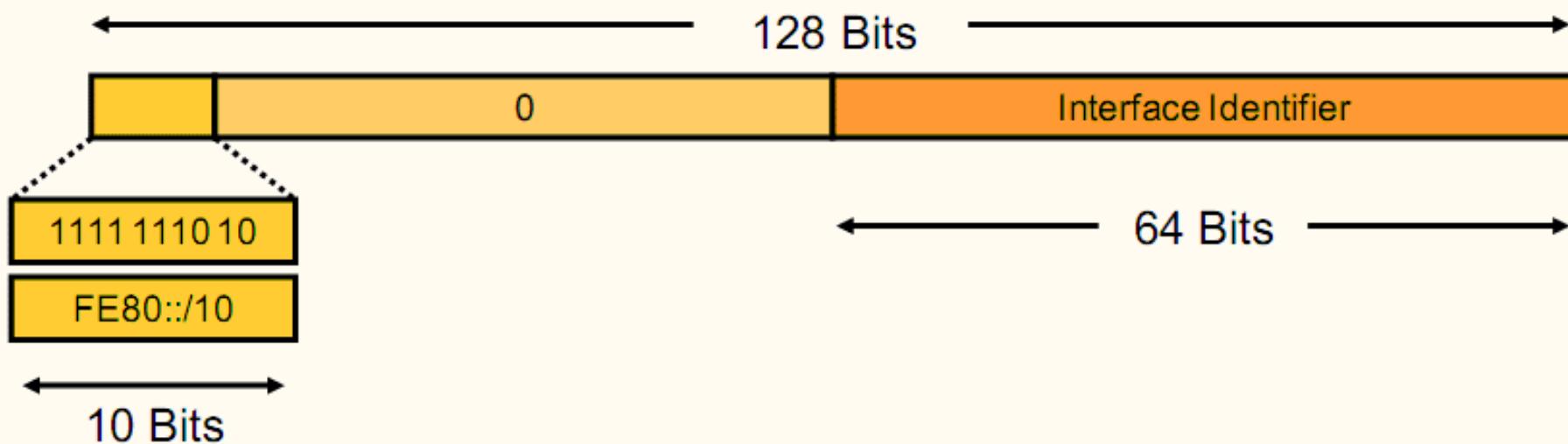
- Used to identify interfaces on a link:
 - Must be unique on that link
 - Can be globally unique
- Unicast addresses should have a 64-bit interface ID:
 - Except for unicast addresses that start with binary 000
 - Interface ID constructed in modified EUI-64 format



Link-Local 주소

Link-Local Addresses

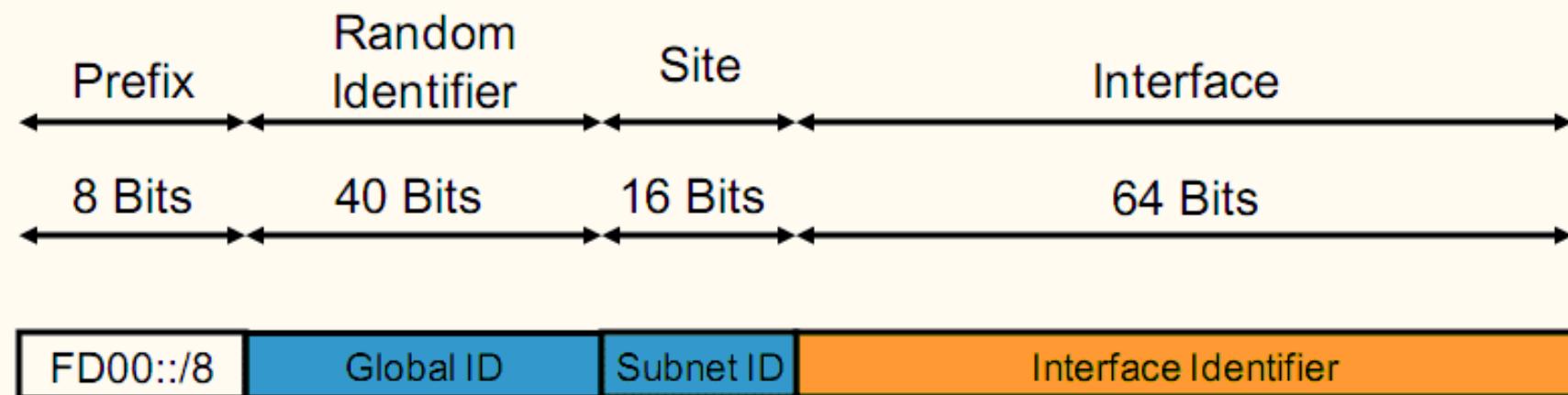
- Have a scope limited to the link
- Are automatically configured with the interface ID
- When used, must be paired with outgoing interface information



Unique Local Unicast 주소

Unique Local Unicast Addresses (RFC 4193)

- FC00::/7
 - FC00::/8 planned to be globally managed
 - FD00::/8 assigned locally by network administration
- For network in which only internal IPv6 communication is required
- Not routable on the Internet



Unspecified and Loopback 주소

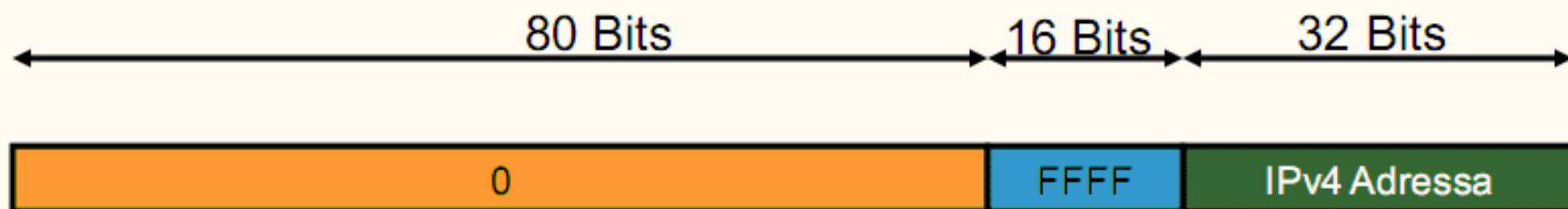
Unspecified and Loopback Addresses

- Unspecified address:
 - 0:0:0:0:0:0:0
 - Used as a placeholder when no address is available (initial DHCP request, DAD)
- Loopback address:
 - 0:0:0:0:0:0:1
 - Same as 127.0.0.1 in IPv4
 - Identifies self

IPv4-Mapped 변환 주소

IPv4-Mapped Addresses

- Used to represent the addresses of IPv4 nodes as IPv6 addresses
- Used for next-hop representation in 6PE and 6VPE
- Used in network stacks when both address families are processed internally as IPv6 (e.g., Linux)



0:0:0:0:FFFF:192.0.2.100

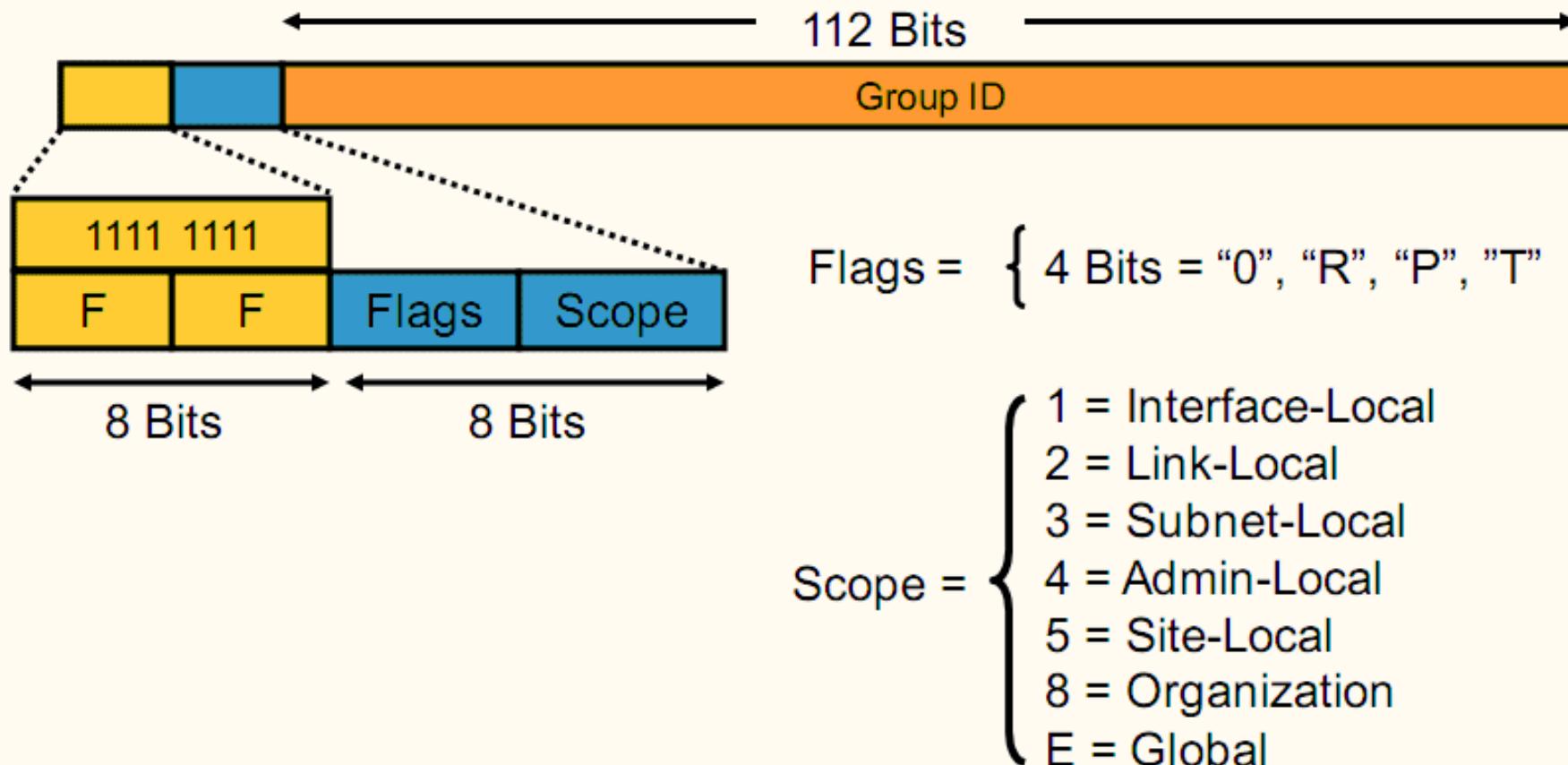
= ::FFFF:192.0.2.100

= ::FFFF:C000:0246

Multicast 주소

Multicast Addresses

- Multicast is used in the context of one to many.
- Explicit multicast scope is a new concept in IPv6.



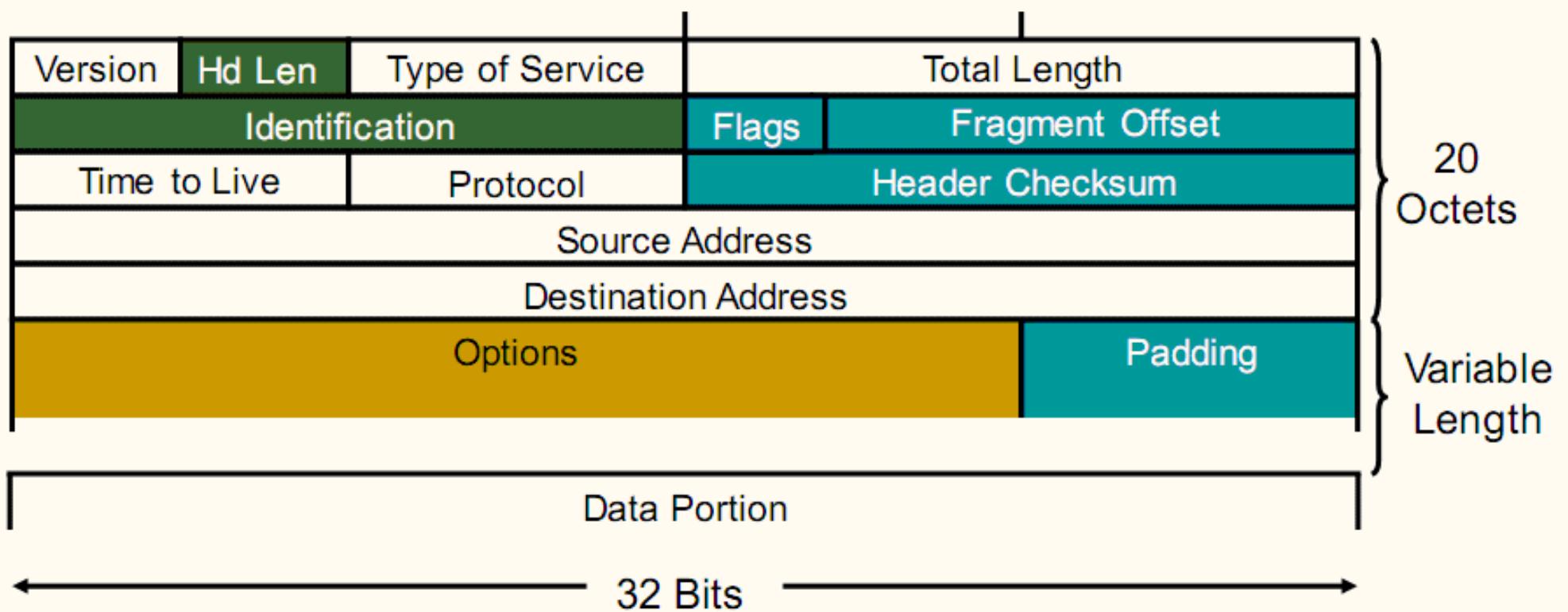
예약된 Multicast 주소

Multicast Assigned Addresses (RFC 2375)

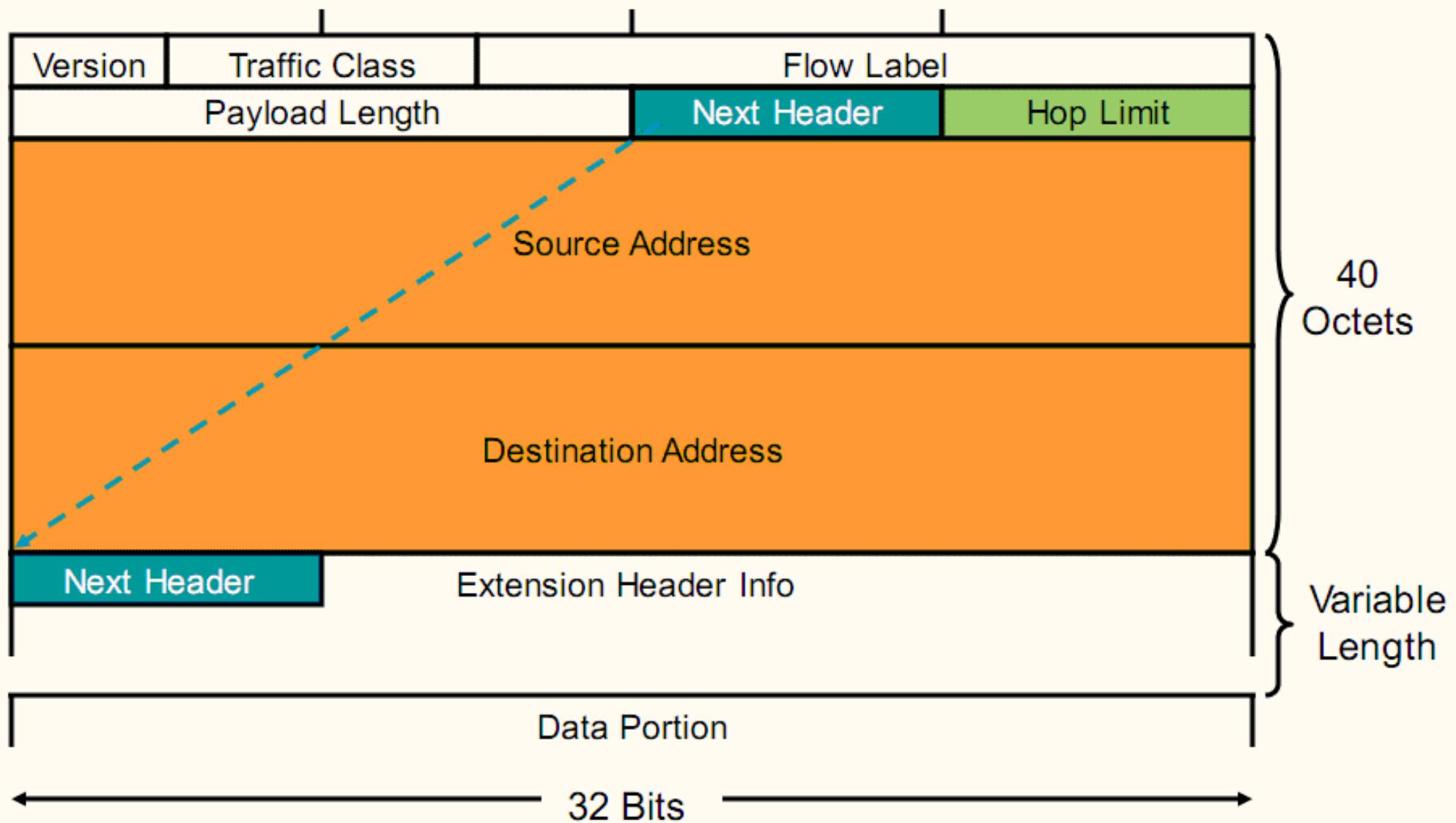
- FF0X:: is reserved (X is from the range from 0 to F).
- Inside this range, the following addresses are assigned:

Address	Meaning	Scope
FF02::1	All nodes	Link-local
FF02::2	All routers	Link-local
FF02::9	All RIP routers	Link-local
FF02::1:FFXX:XXXX	Solicited-node	Link-local
FF05::101	All NTP servers	Site-local
FF05::1:3	All DHCP servers	Site-local
FF0X::127	CISCO-RP-ANNOUNCE	Any scope
FF0X::128	CISCO-RP-DISCOVERY	Any scope

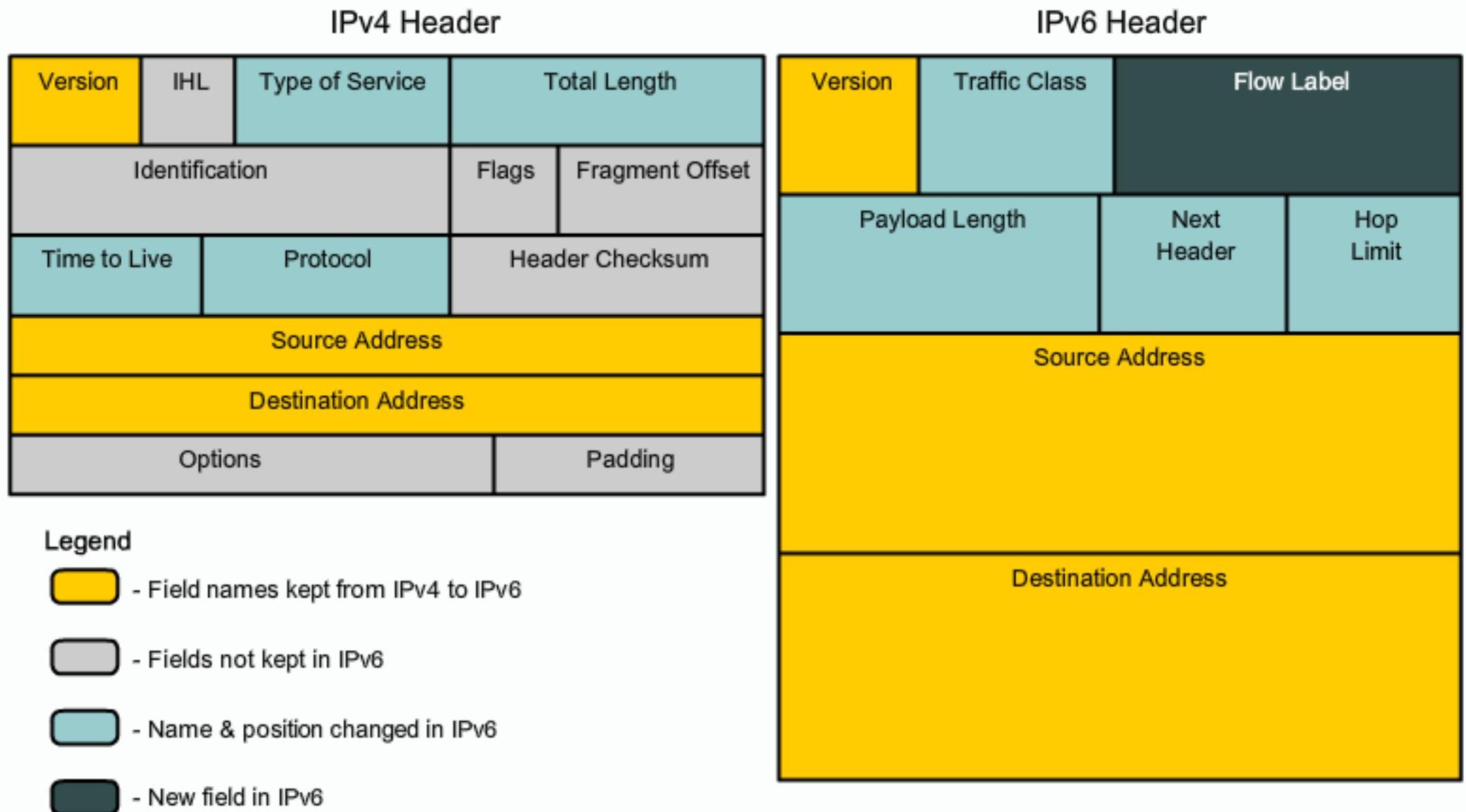
IPv4 Header 형태



IPv6 Header 형태



IPv4 and IPv6 Header 비교



Cisco Router에서 IPv6 활성화

To enable IPv6 on Cisco IOS routers, enable IPv6 unicast packet forwarding:

```
router(config)#  
ipv6 unicast-routing
```

- Enable IPv6 traffic forwarding

Enabling IPv6 on Cisco Catalyst switches might require changing the switch database management template.

```
switch(config)#  
sdm prefer dual-ipv4-and-ipv6 default
```

- Enable IPv6 TCAM support (advance IP Services feature set is required)

IPv6 Address 설정

The **ipv6 address** command:

- Enables IPv6 on the interface
- Configures the interface IPv6 address

```
router(config-if)#
```

```
  ipv6 enable
```

- Enables IPv6 support on an interface when no explicit address has been configured

```
router(config-if)#
```

```
  ipv6 address <ipv6prefix>/<prefixlength> [eui-64]
```

- Configures an IPv6 address on an interface and starts sending out route advertisements for the configured prefix

IPv6 Address 설정

```
router(config-if)#
  ipv6 unnumbered <interface>
```

- Assigns address from another interface

```
router(config-if)#
  ipv6 address <fe80::suffix> link-local
```

- Configures link local address to an arbitrary value

```
router(config-if)#
  ipv6 address autoconfig [default]
```

- Configures stateless autoconfiguration on the interface
- Default route is added, based on route advertisement information, if the **default** keyword is added.

IPv6 Address 설정

LAN: 2001:DB8:C18:1::/64

Ethernet0



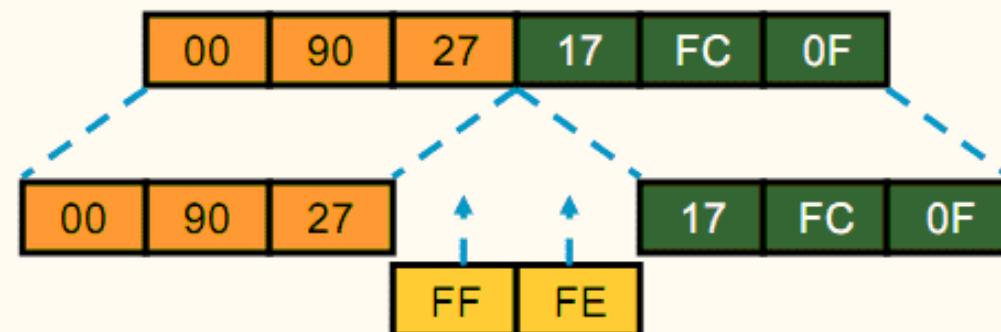
```
ipv6 unicast-routing  
interface Ethernet0  
    ipv6 address 2001:db8:c18:1::/64 eui-64
```

MAC Address: 0060.3E47.1530

```
router# show ipv6 interface Ethernet0  
Ethernet0 is up, line protocol is up  
    IPv6 is enabled, link-local address is FE80::260:3EFF:FE47:1530  
    Global unicast address(es):  
        2001:DB8:C18:1:260:3EFF:FE47:1530, subnet is 2001:DB8:C18:1::/64  
    Joined group address(es):  
        FF02::1:FF47:1530  
        FF02::1  
        FF02::2  
    MTU is 1500 bytes
```

Modified EUI-64 Format

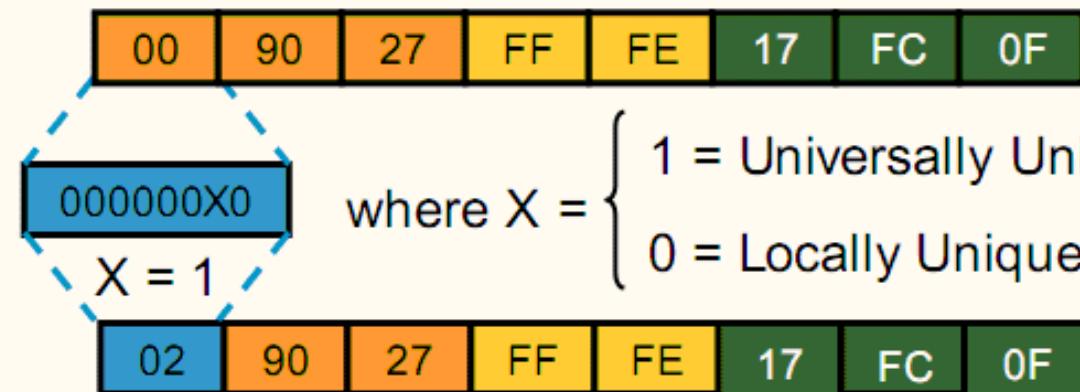
Ethernet MAC Address
(48 Bits)



64-Bit Version

U/L Bit

Modified EUI-64 Address



A modified EUI-64 address is formed by inserting “FFFE” and complementing a bit that identifies the uniqueness of the MAC address.

Cisco IOS show 명령어

- Send IPv6 ICMP echo request to the default router:

```
router# ping 2001:DB8:C18:1:260:3EFF:FE47:1530
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:C18:1:260:3EFF:FE47:1530, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

- Display the neighbor discovery cache on the router:

```
router# show ipv6 neighbors
IPv6 Address                               Age Link-layer Addr State Interface
FE80:: 260:3EFF:FE47:1530                  26 0060.3e47.1530 REACH Ethernet0
2001:DB8:C18:1:260:3EFF:FE47:1530          0 0060.3e47.1530 REACH Ethernet0
```

RIPng for IPv6 개요

RIPng has the same main features as RIP for IPv4:

- Distance vector routing protocol
- Maximum radius of 15 hops
- Routing loop prevention using split horizon and poison reverse
- Uses UDP port 521 for communication
- Periodic routing updates and same timer values
- Derived from RIPv2, but not compatible due to IPv6-specific messages

RIPng for IPv6 개요

Updated RIPng Features for IPv6

- Able to carry IPv6 prefixes, next-hop IPv6 link-local address, next-hop interface.
- Uses the all-RIP-routers multicast group, FF02::9, as the destination address for RIP updates.
- Uses IPv6 for transport.
- Enabled per-interface, not per-network:
 - Enabled and used on the interface.
 - The **network** command deprecated.
- Several instances allowed on the router (up to four).

Cisco IOS RIPng 설정

```
router(config) #
```

```
  ipv6 router rip tag
```

- Creates and enters RIP router submode

```
router(config-rtr) #
```

```
  redistribute static | bgp | rip tag
```

- Redistributions routes from other routing processes

```
router(config-if) #
```

```
  ipv6 rip tag enable
```

- Configures RIP on an interface

```
router(config-if) #
```

```
  ipv6 rip tag default-information originate
```

- Originates the default route (::/0) from an interface

Cisco IOS RIPng 설정

Cisco IOS RIPng Commands

```
router#
```

```
show ipv6 rip
```

- Displays status of the various RIP processes

```
router#
```

```
show ipv6 rip database
```

- Displays the RIP database

```
router#
```

```
show ipv6 route rip
```

- Shows RIP routes in the IPv6 route table

```
router#
```

```
debug ipv6 rip
```

- Displays RIP packets sent and received

OSPF for IPv6 개요

- Router ID is no longer based on an IPv4 address of the router:
 - It is configured in the routing process
 - It is still a 32-bit number, written in four octets
 - It is used to sign routing updates
- Adjacencies and next-hop attributes use link-local addresses (exception: virtual links).
- IPv6 is used for transport of the LSA.
- Enabled per-link, not per-network.
- OSPFv3 requires Cisco Express Forwarding.

OSPF for IPv6 개요

- Router ID, area ID, and link-state ID remain 32 bits:
 - Not derived from an IPv4 address
- Router LSA and network LSA do not contain IPv4 addresses, these are only 32-bit identifiers.
- LSAs now have a flooding scope defining a radius:
 - Link-local
 - Area
 - Autonomous system
- Handling and forwarding of unknown LSAs is supported—to handle future OSPF extensions.
- Uses IPv6 link-local multicast addresses:
 - FF02::5 OSPF routers
 - FF02::6 OSPF-designated routers

OSPF for IPv6 개요

- Two LSAs have been renamed:
 - Interarea Prefix LSAs (Type 3)
 - Interarea Router LSAs (Type 4)
- Two new LSAs have been added to OSPFv3:
 - Link LSAs (Type 8)
 - Intra-Area Prefix LSAs (Type 9)

Cisco IOS OSPFv3 설정 확인

router#

```
show ipv6 ospf [process-id] [area-id] interface [int]
```

- Displays OSPF-related interface information

router#

```
show ipv6 ospf [process-id] [area-id]
```

- Displays general information about OSPF processes

router(config-if)#

```
clear ipv6 ospf [process-id] {process |force-spf |  
redistribution | counters [neighbor [neighbor-interface]]}
```

- Triggers SPF recalculations

EIGRP for IPv6 개요

- Advanced distance vector mechanism with some features common to link-state protocols
- Uses protocol-dependent modules to support multiple protocols:
 - IPv4
 - IPX
 - AppleTalk
- Easy to configure
- Fast convergence
- Supports IPv6 as a separate routing context

Cisco IOS EIGRP for IPv6 설정

```
router(config)#
```

```
ipv6 router eigrp as-number
```

- Creates and enters EIGRP router submode

```
router(config-rtr) #
```

```
no shutdown
```

- Starts EIGRP for IPv6 without changing interface

```
router(config-rtr) #
```

```
default-information originate [route-map route-map]
```

- Advertises default route, with an optional route map

```
router(config-rtr) #
```

```
maximum-paths number
```

- Configures maximum number of paths to the same destination that will be installed in the routing table

Cisco IOS EIGRP for IPv6 설정

```
router(config-if) #
```

```
  ipv6 eigrp as-number
```

- Configures EIGRP for IPv6 on an interface

```
router(config-if) #
```

```
  ipv6 summary-address eigrp as-number prefix/mask [AD]
```

- Configures summarization on an interface

```
router(config-if) #
```

```
  no ipv6 split-horizon eigrp as-number
```

- Disables split horizon on an interface

```
router(config-if) #
```

```
  ipv6 bandwidth-percent eigrp as-number percent
```

- Configures the percentage of bandwidth EIGRP uses

Cisco IOS EIGRP for IPv6 설정 확인

```
router#
```

```
show ipv6 eigrp topology
```

- Displays entries in the EIGRP IPv6 topology table

```
router#
```

```
show ipv6 eigrp neighbors
```

- Displays the neighbors discovered by EIGRP for IPv6

```
router#
```

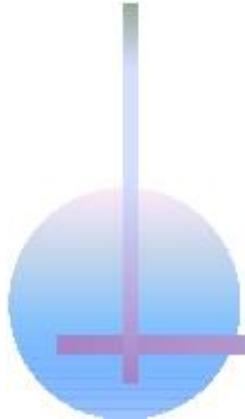
```
show ipv6 route eigrp
```

- Shows EIGRP routes in the IPv6 routing table

```
router#
```

```
debug ipv6 eigrp
```

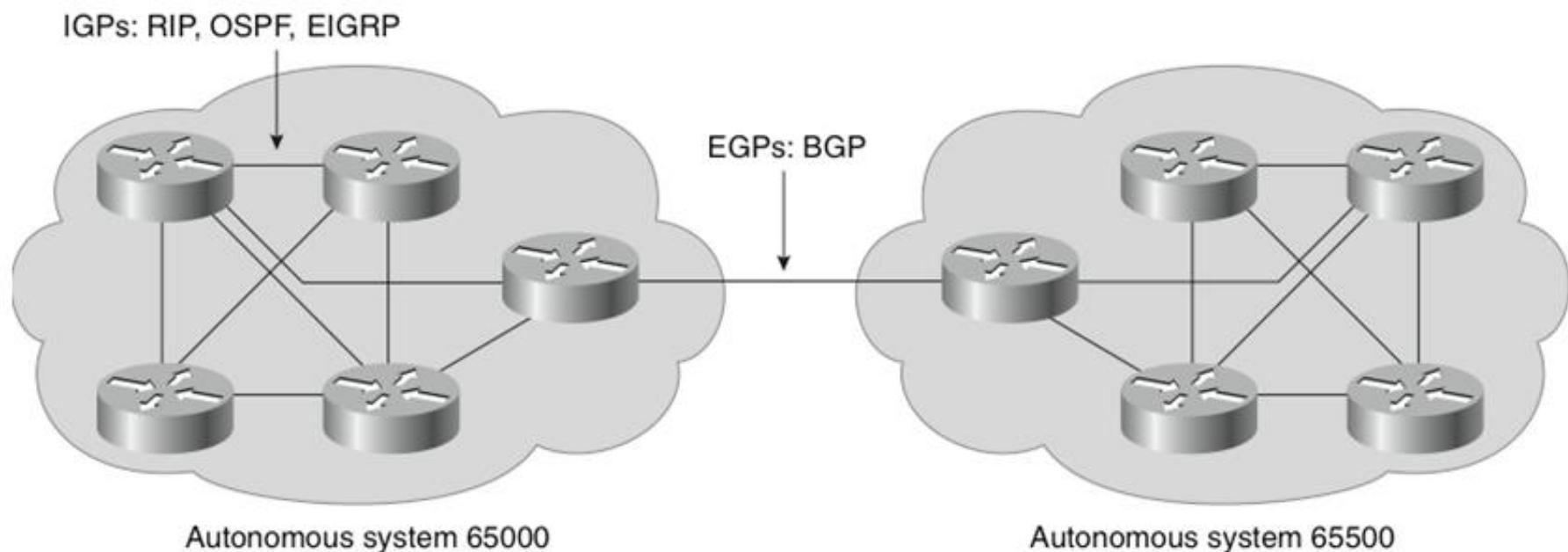
- Displays information about EIGRP for IPv6 protocol



Module 09 BGP

IGP vs. EGP

- **Interior gateway protocol (IGP)**
 - 자율 시스템(AS) 내에서 작동하는 라우팅 프로토콜.
 - RIP, OSPF, IGRP는 IGP이다.
- **Exterior gateway protocol (EGP)**
 - 서로 다른 AS 사이에서 작동하는 라우팅 프로토콜.
 - BGP는 도메인 간 라우팅 프로토콜 (IDRP)이며 EGP이다.



Autonomous Systems (AS)

- AS는 유사한 라우팅 정책을 공유하고 단일 관리 도메인 내에서 작동하는 라우터 그룹이다.
- AS는 일반적으로 하나의 조직에 속한다.
- AS 내에서 단일 또는 다중 내부 게이트웨이 프로토콜 (IGP)이 사용될 수 있다.
- 두 경우 모두 외부에서는 전체 AS를 하나의 개체로 간주한다.
- AS가 BGP와 같은 외부 게이트웨이 프로토콜을 사용하여 공용 인터넷에 연결하는 경우 IANA (Internet Assigned Numbers Authority)에서 관리하는 고유 한 AS 번호가 할당되어야 한다.
- AS 번호는 1에서 65,535 사이 일 수 있습니다. RIR은 1과 64,512 사이의 AS 번호를 관리한다. 64,512 - 65,535 개의 번호는 개인 용도로 예약되어 있다 (IP 개인 주소와 유사). IANA는 단일 공급자에 연결하는 조직이 개인 풀의 AS 번호를 사용하는 정책을 시행한다.
 - IETF는 RFC 4893과 RFC 5398을 발표했다. 이 RFC는 2 옥텟 (16 비트) 필드에서 4 옥텟 (32 비트) 필드로 AS 번호를 늘려 풀 크기를 65,536에서 4,294,967,296 값으로 늘리는 BGP 확장을 설명한다.

BGP 기초

- 인터넷은 서로 통신 할 수 있도록 상호 연결된 자율 시스템 모음이다.
 - BGP는 이러한 자율 시스템 간의 라우팅을 제공한다.
- BGP is a path vector protocol.
- TCP를 사용하는 유일한 라우팅 프로토콜이다.
 - OSPF 및 EIGRP는 IP를 통해 직접 작동합니다. IS-IS는 네트워크 계층에 있다.
 - RIP는 해당 전송 계층에 대해 UDP (User Datagram Protocol)를 사용한다.
- BGP 버전 4 (BGP-4)는 최신 버전의 BGP이다.
 - 슈퍼네팅, CIDR 및 VLSM 지원.
- BGP4 및 CIDR이 인터넷 라우팅 테이블이 너무 커지지 않도록 방지.

BGP Basics

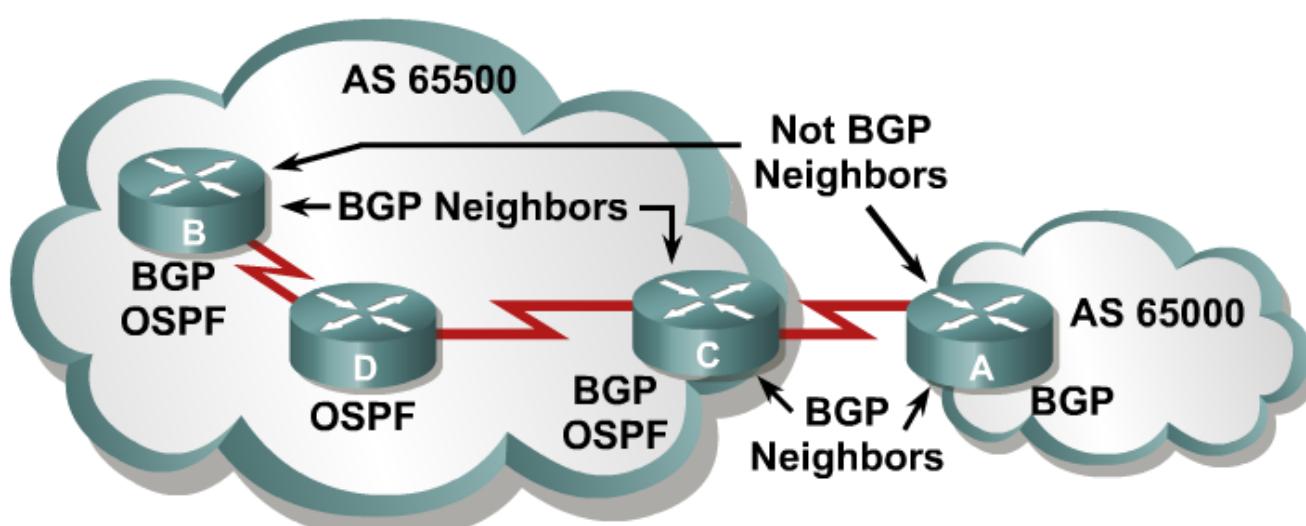
- 2019년 7월 11일 현재 인터넷 코어 라우터의 라우팅 테이블에는 435,211개의 경로가 있다.

<http://bgpupdates.potaroo.net/instability/bgpupd.html>

Number of BGP Update Messages:	11380351
Number of Prefix Updates:	6761935
Number of Prefix Withdrawals:	287835
Average Prefixes per BGP Update:	0.62
Average BGP Update Messages per second:	9.41
Average Prefix Updates per second:	5.83
Peak BGP Update Message Rate per second:	24853 (01:14:19 Wed, 10-Jul-2019)
Peak Prefix Update Rate per second:	10763 (06:45:13 Sat, 13-Jul-2019)
Peak Prefix Withdraw Rate per second:	22106 (05:37:58 Thu, 11-Jul-2019)
Prefix Count:	802838
Updated Prefix Count:	435211
Stable Prefix Count:	367627
Origin AS Count:	65233
Updated Origin AS Count:	44781
Stable Origin AS Count:	20452
Unique Path Count:	456027
Updated Path Count:	338798
Stable Path Count:	117229

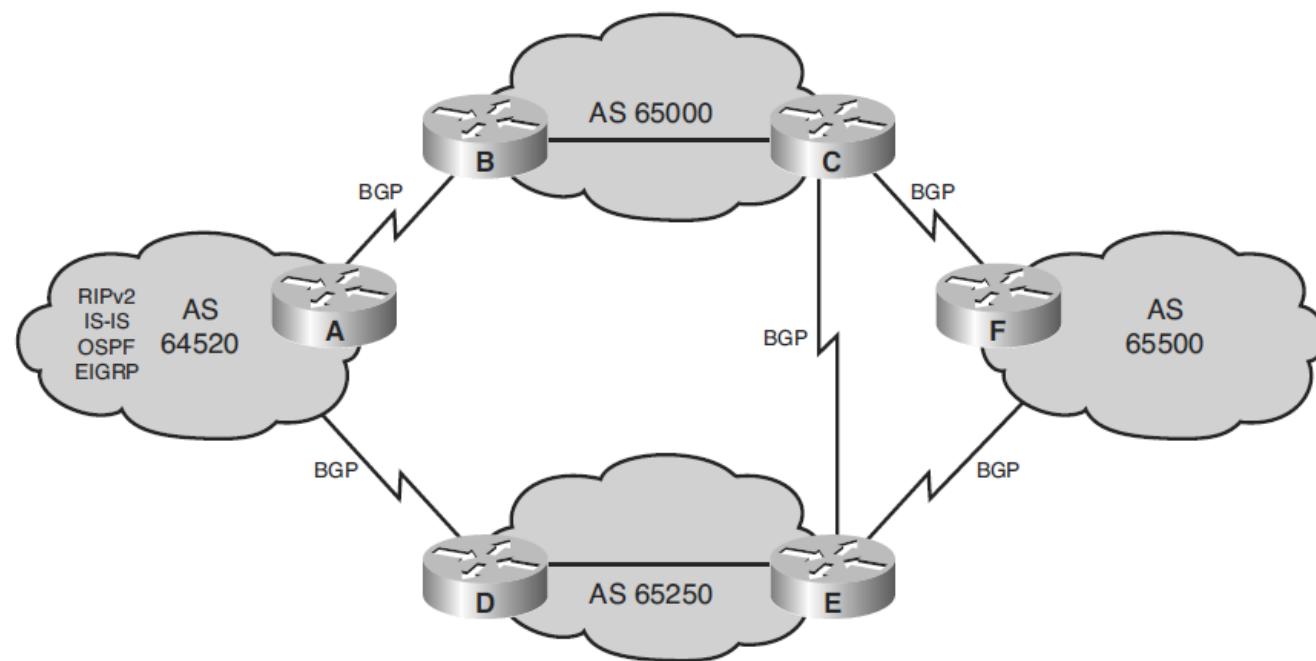
BGP 동작 개요

- 두 개의 라우터가 TCP 사용 가능 BGP 연결을 설정하면 이웃 또는 피어라고 한다.
 > 피어 라우터가 여러 연결 메시지 교환.
- BGP를 실행하는 각 라우터를 BGP 스피커라고 한다.
- "BGP 피어"("BGP 이웃"이라고도 함)는 인접 관계를 설정 한 BGP 스피커에 사용되는 특정 용어이다.
- BGP 라우팅 정보를 교환하기 위해 TCP 연결을 구성한 두 라우터를 BGP 피어 또는 BGP 이웃이라고 한다.
- BGP 이웃이 처음 연결을 설정하면, 모든 후보 BGP 경로를 교환한다.
 > 이 초기 교환 후 네트워크 정보가 변경되면 증분 업데이트가 전송된다.



BGP Use Between AS

- BGP는 자율 시스템 간의 라우팅 정보의 루프없는 교환을 보장하는 도메인 간 라우팅 시스템을 제공한다.



Comparing IGPs with BGP

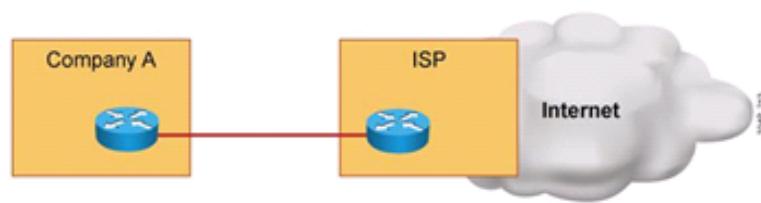
Protocol	Interior or Exterior	Type	Hierarchy Required?	Metric
RIP	Interior	Distance vector	No	Hop count
OSPF	Interior	Link state	Yes	Cost
IS-IS	Interior	Link state	Yes	Metric
EIGRP	Interior	Advanced distance vector	No	Composite

BGP	Exterior	Path vector	No	Path vectors (attributes)

Connection Redundancy

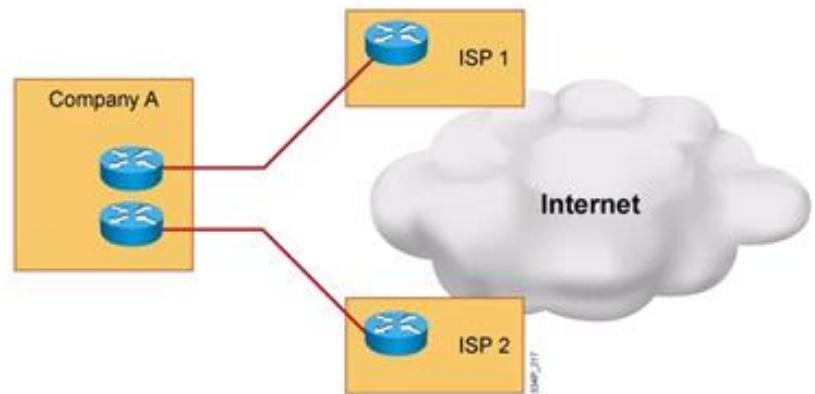
Connecting to One ISP

Single-homed

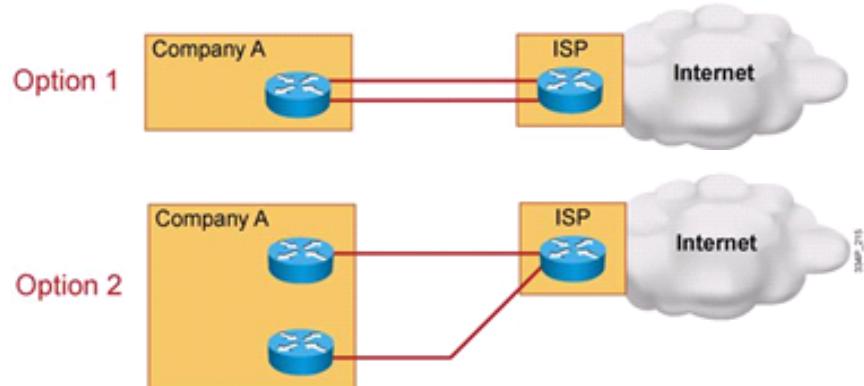


Connecting to Two or more ISPs

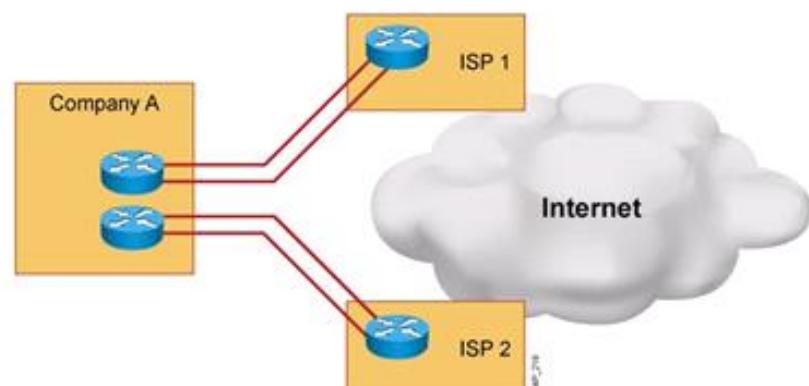
Multihomed



Dual-homed

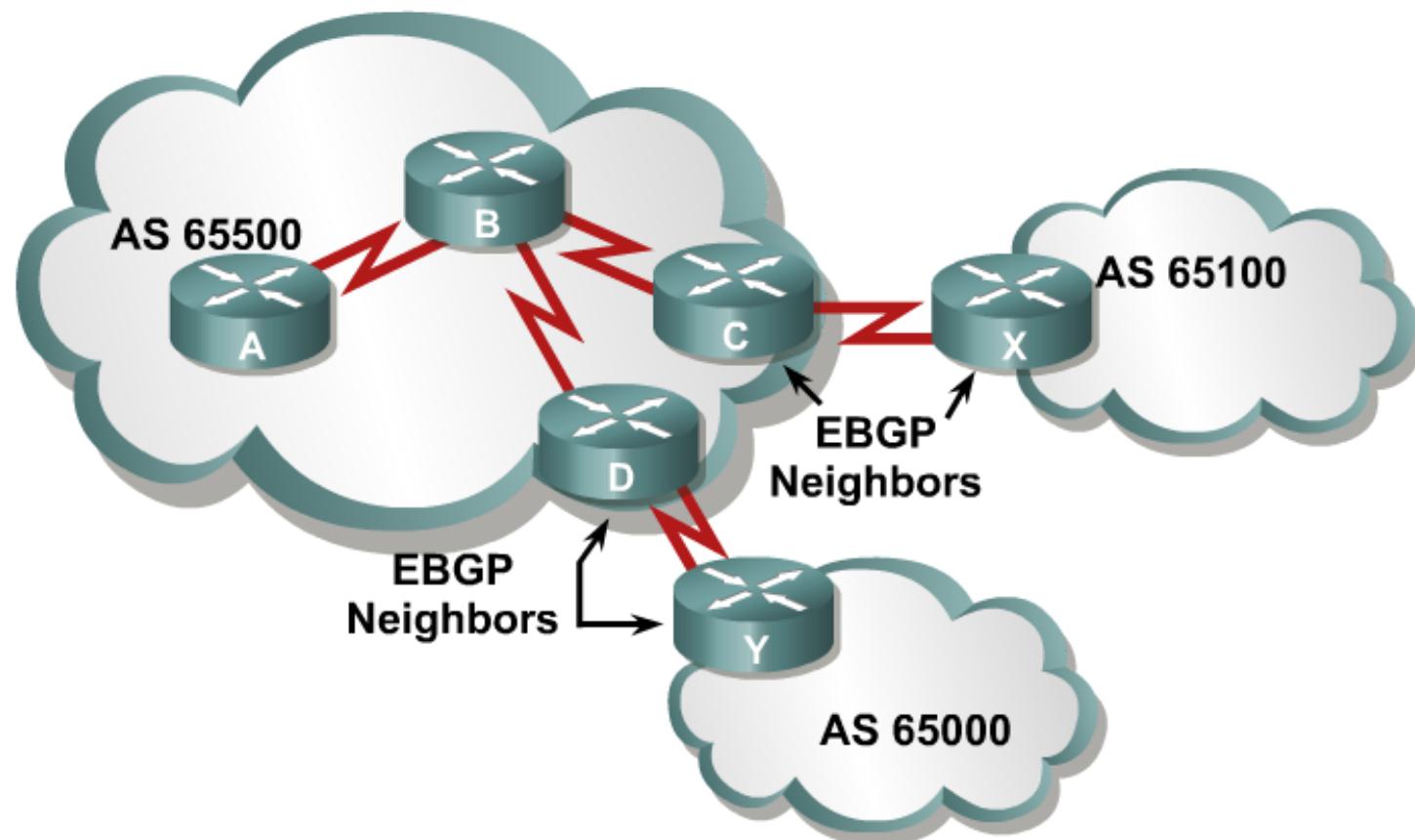


Dual-multihomed



EBGP(External BGP)

- EBGP 네이버는 다른 AS에 있다.
 - EBGP 네이버는 직접 연결될 필요가 있다.

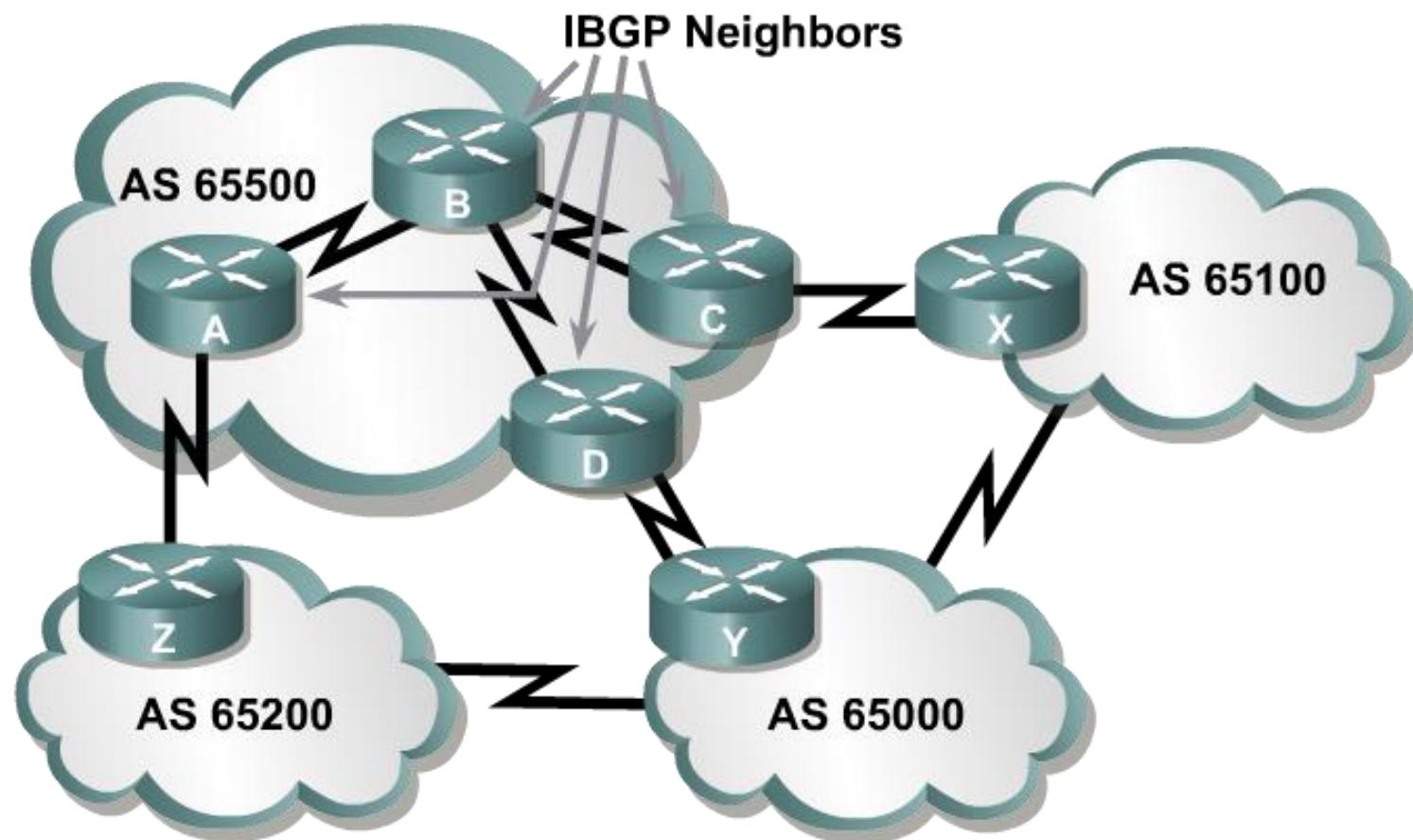


EBGP 네이버 형성을 위한 요구사항

- 네이버 정의:
 - BGP 라우팅 업데이트 교환을 시작하기 전에 TCP 세션 (3 방향 핸드 쇼이크)을 수립해야 한다.
- 도달가능성:
 - EBGP 네이버는 대개 직접 연결된다.
- 서로다른 AS번호:
 - EBGP 네이버는 서로 다른 AS번호를 가지고 있어야한다.

IBGP(Internal BGP)

- IBGP 네이버는 같은 AS내에 있다.
 - IBGP 네이버는 직접 연결될 필요가 없다.

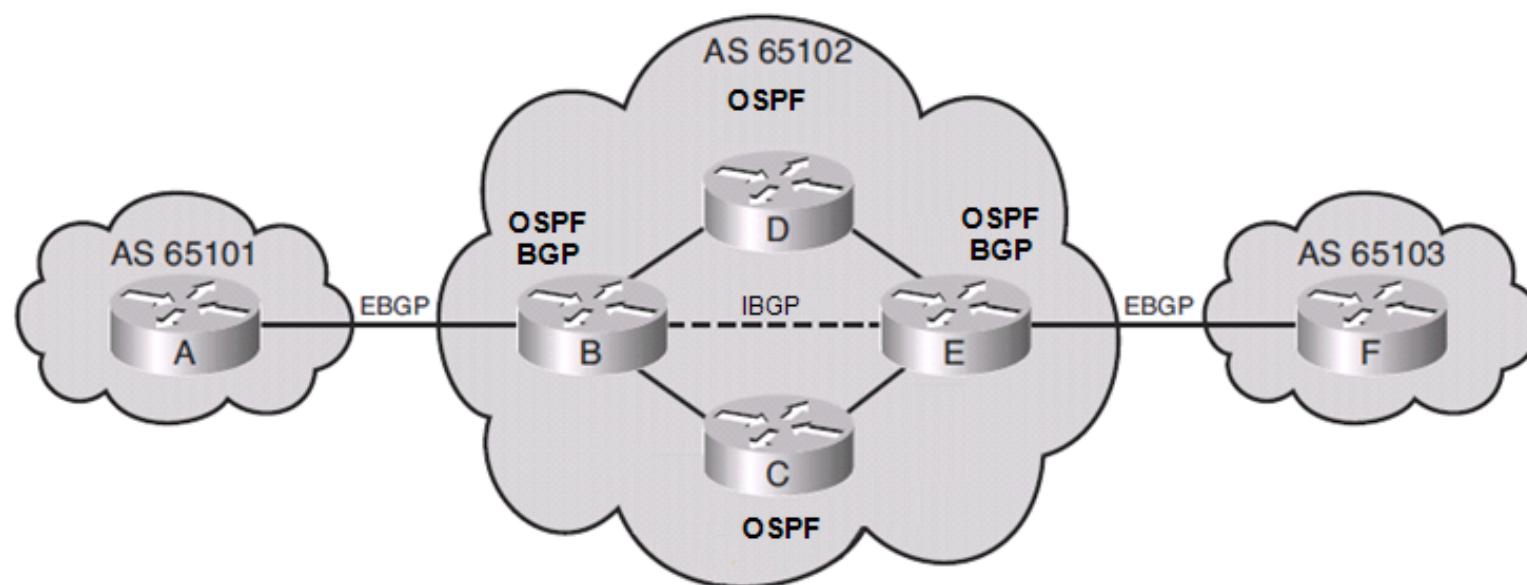


IBGP 네이버 형성을 위한 요구사항

- **네이버 정의:**
 - BGP 라우팅 업데이트 교환을 시작하기 전에 TCP 세션 (3 방향 핸드 쇼이크)을 수립해야 합니다.
- **도달가능성:**
 - IBGP 네이버는 일반적으로 IGP를 이용해 도달가능해야 한다.
 - Loopback IP주소가 보통 IBGP네이버를 식별하기 위해 사용된다.
- **같은 AS번호:**
 - IBGP 네이버는 같은 AS번호를 사용해야 한다.

IBGP in a Transit AS

- Transit AS는 한 외부 AS에서 다른 외부 AS로 트래픽을 라우팅하는 AS입니다.
- 아래 예에서 AS 65102는 service provider network이다.
 - 두개의 edge 라우터(router B and E)만 BGP가 운용되고 있고, OSPF를 이용하여 IBGP 네이버 관계를 수립한다.
 - EBGP 경로는 OSPF에 재분배 될 수 있지만 잠재적인 BGP 경로 수는 OSPF를 압도할 수 있으므로 권장되지 않는다.



BGP Routing 활성화하기

- BGP 설정하기

Router(config) #

```
router bgp autonomous-system
```

- *autonomous-system* 번호는 공인AS번호 또는 사설AS번호가 될 수 있다..
 - 라우터에 하나의 AS번호만 설정할 수 있다..
 - AS번호의 범위는 1에서 65535이다.

Defining BGP Neighbors

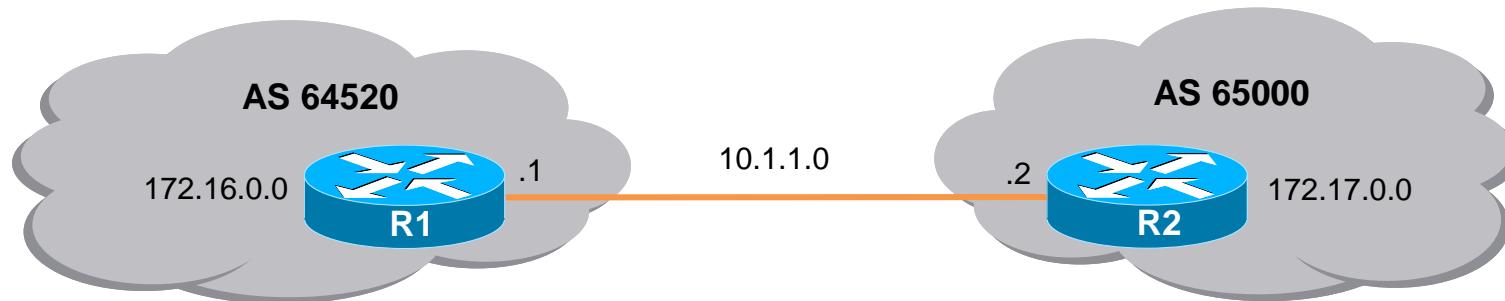
- BGP 세션을 수립하기 위해 neighbor 설정하기

```
Router(config-router) #
```

```
neighbor {ip-address | peer-group-name} remote-as  
autonomous-system
```

- *ip-address*는 BGP 피어의 목적지 주소이다.
 - BGP 관계를 설정하기 전에 주소에 도달할 수 있어야 한다.
- *Autonomous-System* 값은 세션이 내부 BGP (IBGP) 피어 또는 외부 BGP (EBGP) 피어와 관련되어 있는지 식별하는 데 사용된다.
 - 값이 라우터의 AS와 동일하면 IBGP 세션이 시도된다.
 - 값이 라우터의 AS와 같지 않으면 EBGP 세션이 시도된다.

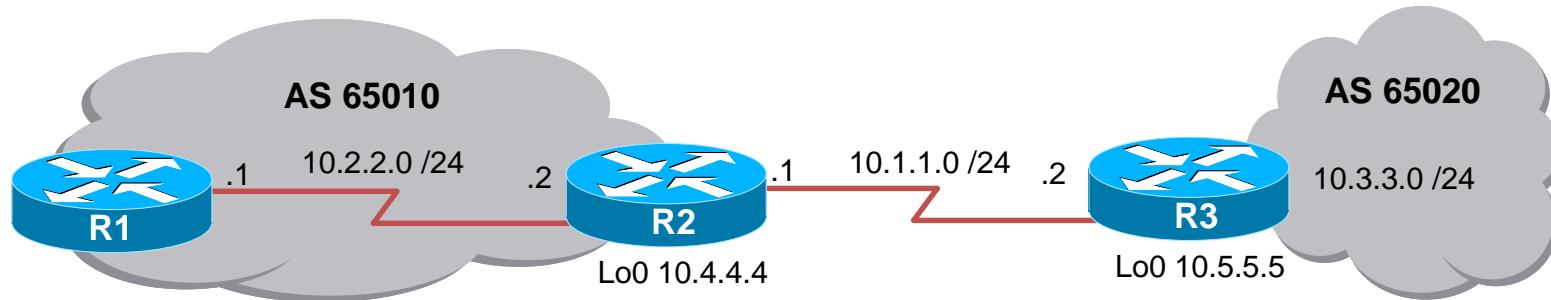
BGP Configuration Example #1



```
R1(config)# router bgp 64520
R1(config-router)# neighbor 10.1.1.2 remote-as 65000
R1(config-router)# network 172.16.0.0
```

```
R2(config)# router bgp 65000
R2(config-router)# neighbor 10.1.1.1 remote-as 64520
R2(config-router)# network 172.17.0.0
```

BGP Configuration Example #2



```
R2(config)# router bgp 65010
R2(config-router)# neighbor 10.1.1.2 remote-as 65020
R2(config-router)# network 10.2.2.0 mask 255.255.255.0
R2(config-router)# network 10.4.4.0 mask 255.255.255.0
R2(config-router) #
```

BGP 기본설정

router bgp AS번호

neighbor x.x.x.x(상대IP주소) remote-as 상대AS번호

network 클래스풀네트워크 : netmask가 필요치 않음.

network 서브네트워크 mask x.x.x.x : netmask 필요.

<Next-hop 문제 해결>

eBGP로 전달받은 정보를 다시 iBGP로 전달할 경우 next-hop이 바뀌지 않아 해당 경로를 사용할 수 없는 문제가 발생하는데 이를 해결하기 위해서 iBGP네이버 설정시 next-hop을 자신의 IP주소로 변경한다.

단, eBGP와 iBGP가 동작하는 라우터에서만 필요

router bgp 200

neighbor x.x.x.x remote-as 200

neighbor x.x.x.x next-hop-self

BGP 블랙홀 현상

AS내에 BGP가 동작하지 않는 라우터가 존재할 경우 해당 라우터는 BGP에 의한 라우팅정보를 알 수 없으므로 패킷이 폐기되는 현상

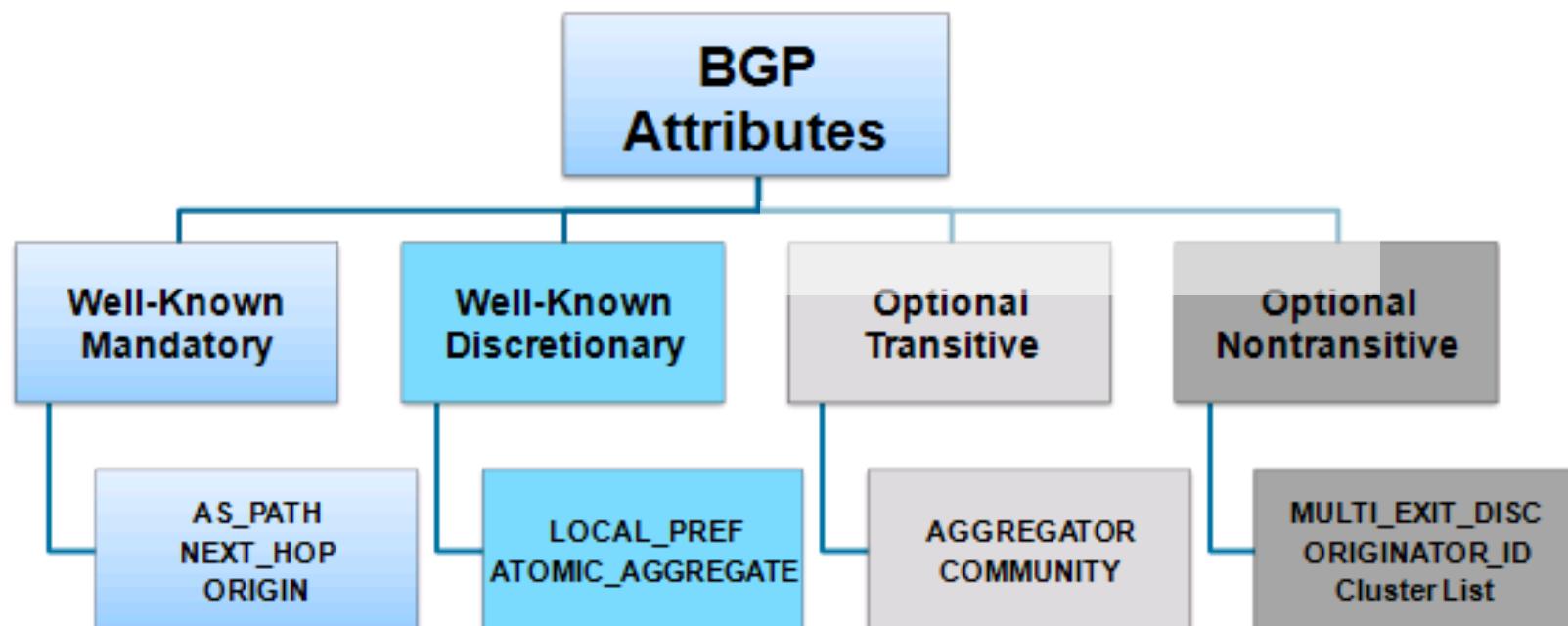
- >> 블랙홀 현상을 방지하기 위해 AS내의 모든 라우터에 BGP설정을 한다.
이 경우 iBGP 네이버간에 라우팅 루프를 방지하기 위해서 BGP Split-horizon규칙이 동작한다.
- >> BGP Split-horizon : iBGP간 라우팅 루프를 방지하기 위한 규칙
iBGP로 전달받은 정보는 다시 iBGP로 전달하지 않는다.
- >> AS내에 라우터들 간에 선형으로 네이버를 맺었을 때 BGP Split-horizon규칙에 의해 라우팅정보가 차단되는 현상이 생긴다.
이를 해결하는 방법
 - 1)Full Mesh => 라우터 개수가 늘어나면 Session이 많이 필요함. 따라서 잘 사용하지 않음.
 - 2)Confederation
 - 3)Route Reflector

Path Attributes

- 경로 속성은 네트워크 경로를 설명하는 BGP 메트릭 집합이다.(route).
 - BGP는 경로 속성을 사용하여 네트워크에 가장 적합한 경로를 결정한다.
 - 일부 속성은 필수이며 업데이트 메시지에 자동으로 포함되는 반면 다른 속성은 수동으로 구성 가능.
- BGP 속성을 사용하여 라우팅 정책을 시행 할 수 있다.
- BGP 속성을 구성하면 관리자에게 더 많은 경로 제어 옵션이 제공된다.
 - 예를 들어 경로정보 필터링, 특정 경로 선호, BGP동작 커스터마이징 등

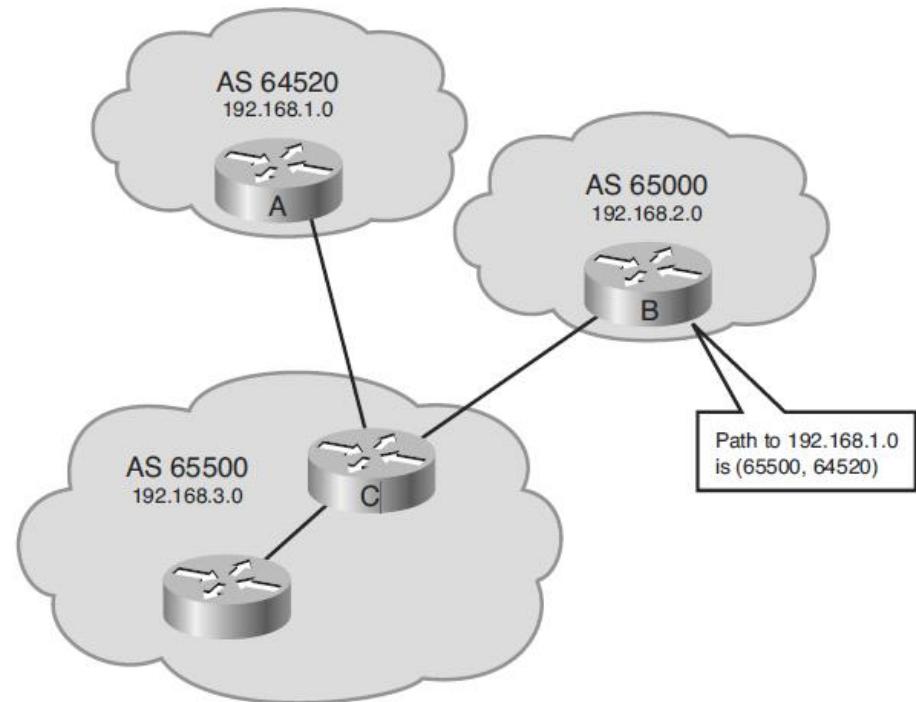
Path Attributes

- 4가지 속성 타입이 있다.
 - 모든 벤더가 모든 BGP속성을 인식하는 것은 아니다.



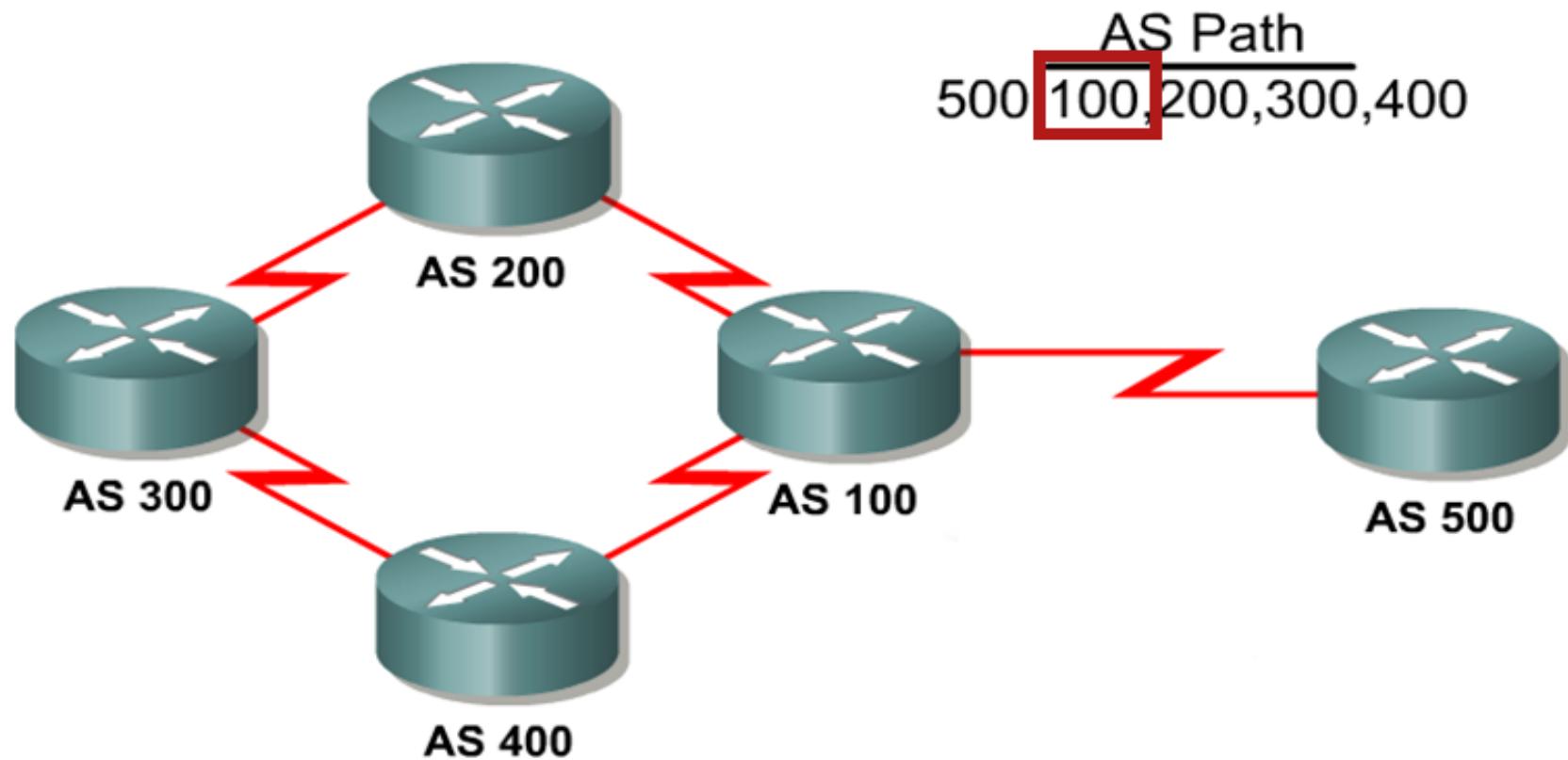
Well-Known Mandatory: AS_PATH

- AS_PATH 속성에는 경로에 도달하기 위한 AS 번호 목록이 포함된다.
- 라우트 업데이트가 AS를 통과 할 때마다 AS 번호는 다음 EBGP 인접 노드에 알리기 전에 AS_PATH 속성의 시작 부분에 추가된다.



Well-Known Mandatory: AS_PATH

- BGP always includes the AS_PATH attribute in its update.



Well-Known Mandatory: NEXT_HOP

- NEXT_HOP 속성은 목적지에 도달하는 데 사용되는 IP 주소를 나타낸다.
- IP 주소는 해당 목적지 네트워크에 대한 경로를 따라 다음 AS로 가기 위한 진입점이다.
 - 따라서 EBGP의 경우 다음 흙 주소는 업데이트를 보낸 네이버의 IP 주소이다.

Well-Known Mandatory: ORIGIN

- ORIGIN attribute 해당 경로가 어떻게 BGP에 포함되었는지를 나타낸다.:
 - **IGP:**
 - 해당 경로는 bgp의 network 명령에 의해 포함된 것을 가리킨다..
 - BGP table에 "i"로 표시된다.
 - **EGP:**
 - EGP 라우팅 프로토콜에 의해 학습된 경로를 나타내지만 현재는 사용되고 있지 않음.
 - BGP table에 "e"로 표시됨.
 - **Incomplete:**
 - 해당 경로가 재분배에 의해 BGP에 포함되었다는 것을 나타냄.
 - BGP table에 "?"로 표시됨.

Well-Known Mandatory: ORIGIN

```
R1# show ip bgp
BGP table version is 24, local router ID is 172.16.1.2
Status codes: s suppressed, d damped, h history, * valid, > k
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 192.208.10.0	192.208.10.5	0		0	300 i
*> 172.16.1.0	0.0.0.0		0	32768	i

```
R1# show ip bgp
<output omitted>
```

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 10.1.1.0/24	0.0.0.0	0		32768	?
*> 192.168.1.0/24	10.1.1.2	84		32768	?
*> 192.168.2.0/24	10.1.1.2	74		32768	?

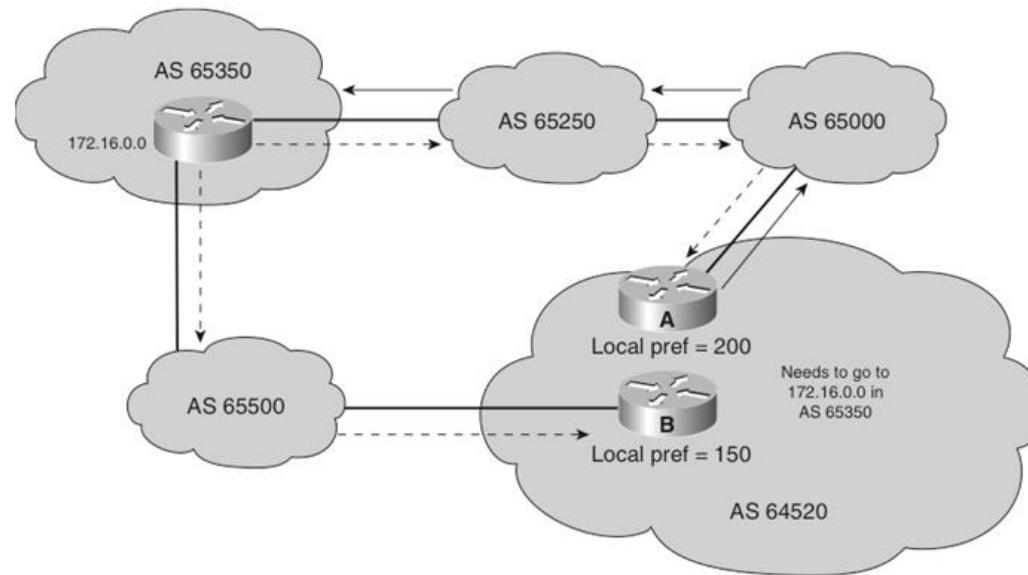
i = Route generated by the **network** command.

? = Route generated by unknown method (usually redistributed).

Well-Known Discretionary: LOCAL_PREF

- Local Preference 속성은 AS내에 있는 iBGP피어간에 전달되며 외부로 나가는 경로를 결정하는 값으로 사용된다..
 - 더 높은 local preference값을 갖는 경로가 선호된다.
 - 시스코 라우터에서 local preference의 기본값은 100이다.
- IBGP 라우터 사이에서만 사용되고 EBGP 피어로는 전달되지 않음.

Well-Known Discretionary: LOCAL_PREF



- 라우터 A와 B는 AS 64520의 IBGP 네이버이며 둘 다 다른 방향에서 네트워크 172.16.0.0에 대한 업데이트를 수신합니다..
 - The local preference on router A is set to 200.
 - The local preference on router B is set to 150.
- 라우터 A의 로컬 선호도 설정이 높기 때문에 AS 64520에서 선호되는 출구로 선택됩니다..

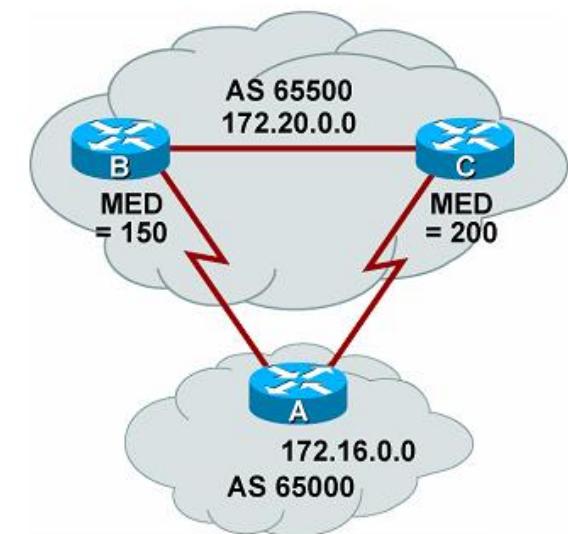
Optional Nontransitive: MED

- 메트릭이라고도하는 MED (Multiple Exit Discriminator) 속성은 여러 경로 중에 AS에서 선호하는 경로를 EBGP 피어에게 알린다.
 - 더 낮은 MED 더 높은 MED보다 선호된다.
- MED가 EBGP 피어에게 전송되고 해당 라우터는 AS 내에 MED를 전파한다.
 - AS 내의 라우터는 MED를 사용하지만 다음 AS로 전달하지는 않는다.
 - 동일한 업데이트가 다른 AS로 전달되면 메트릭은 기본값인 0으로 다시 설정된다.

- 라우터 B와 C는 라우터 A의 업데이트에 MED 속성을 포함합니다.

Router B MED attribute is set to 150.

Router C MED attribute is set to 200.

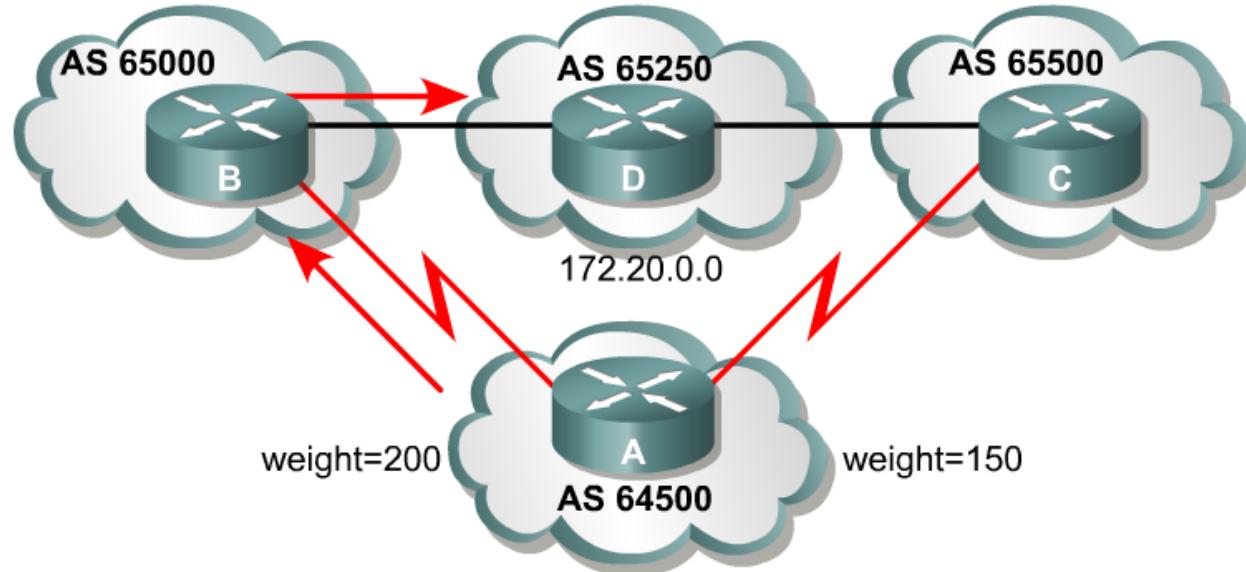


- A가 B와 C로부터 업데이트를 수신하면 라우터 B가 MED가 낮아서 다음으로 가장 좋은 다음 흡으로 선택합니다.

Cisco Weight Attribute

- Weight attribut는 Cisco proprietary 속성이다.
- Weight attribut은 하나의 라우터에 출구가 여러 개 일때 선호하는 출구를 결정하는 값이다.
 - Local preferenc는 라우터가 2대 이상일 경우에 사용됨.
- Weight값은 다른 라우터로 전달되지 않으며, 더 높은 weigh값을 갖는 경로를 선호한다.
- Weight는 0에서 65535 사이의 값을 갖는다.
 - 라우터가 생성하는 경로는 기본값으로 32768을 가지고 다른 경로들은 기본값으로 0을 가짐.

Cisco Weight Attribute



- 라우터 B와 C는 AS 65250에서 네트워크 172.20.0.0에 대해 알아보고 라우터 A에 업데이트를 전파한다.
 - 따라서 라우터 A에는 172.20.0.0에 도달하는 두 가지 방법이 있다..
- 라우터 A는 다음과 같이 업데이트의 weight를 설정한다. :
 - 라우터 B에서 오는 업데이트는 200으로 설정된다.
 - 라우터 C에서 오는 업데이트는 150으로 설정된다.
- 라우터 A는 더 높은 weight 때문에 라우터 B를 사용한다.

BGP 경로 선택 과정

- BGP 최적 경로 결정은 업데이트에 포함된 속성 값과 기타 BGP 구성 가능 요소.
- BGP는 AS 루프가 없는 동기화 된 경로와 유효한 다음 흡 주소만을 고려한다.

