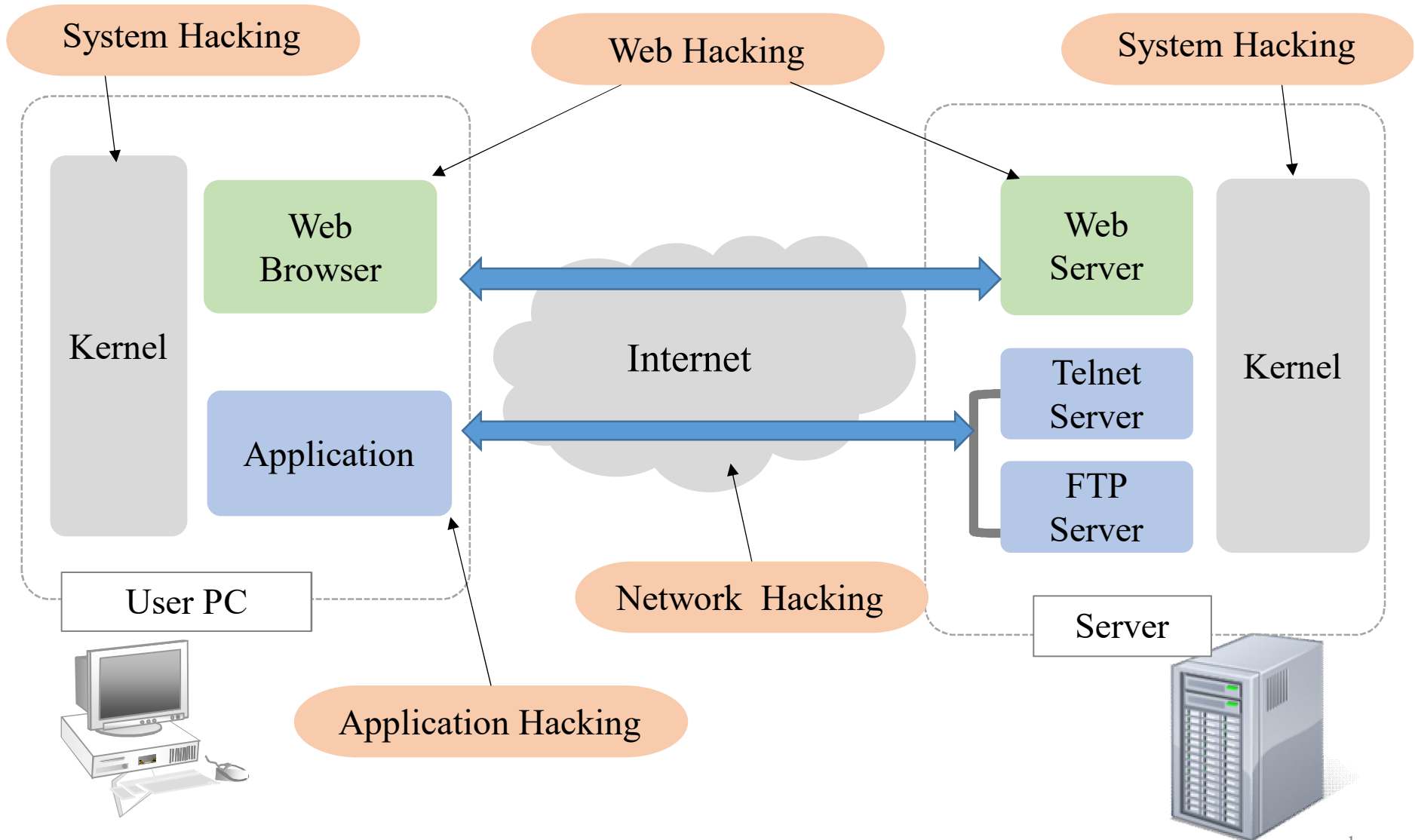
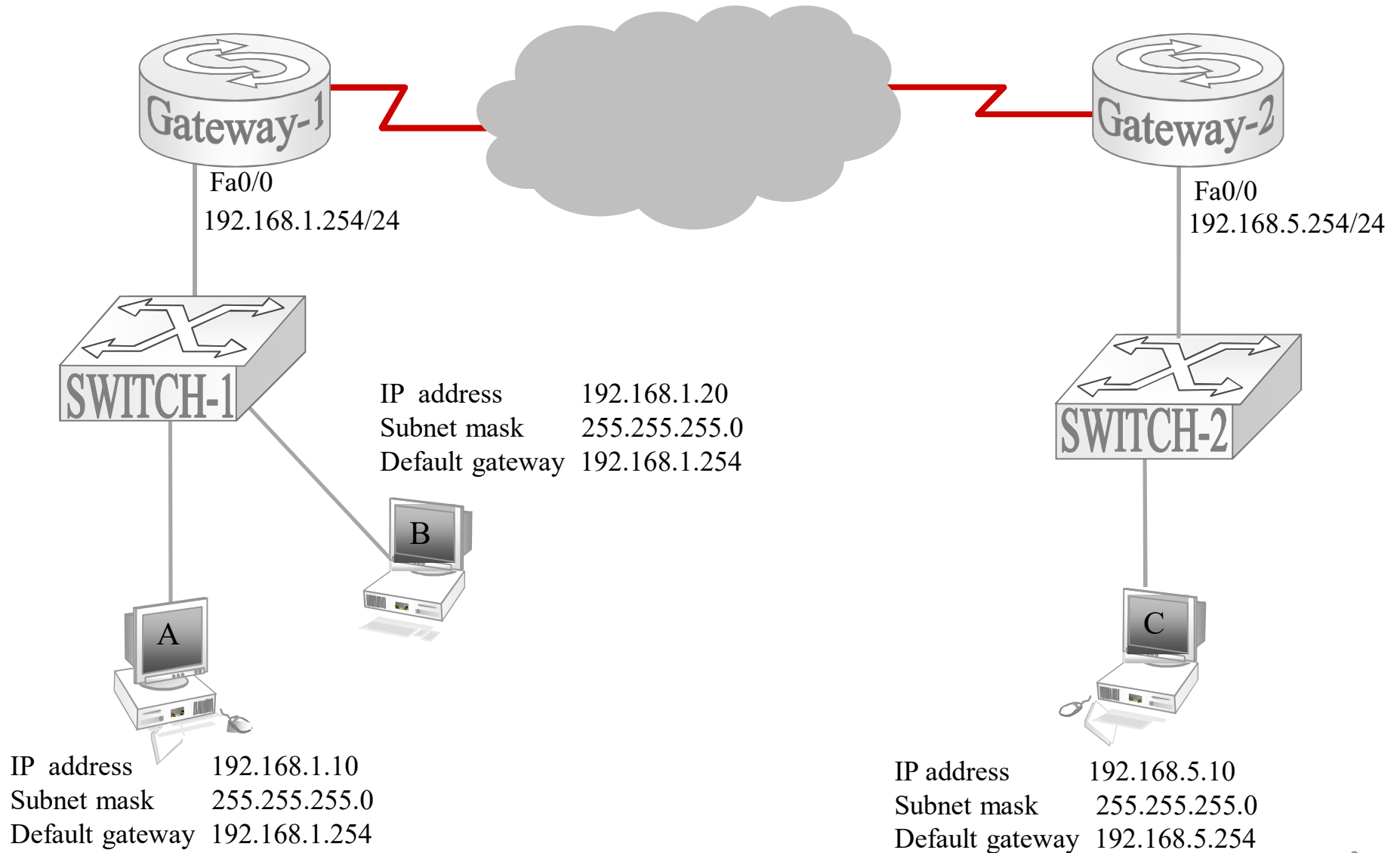


Attack 종류



네트워크 개요



1) 네트워크 주소

- FQDN
- Port number
- IP Address
- MAC Address

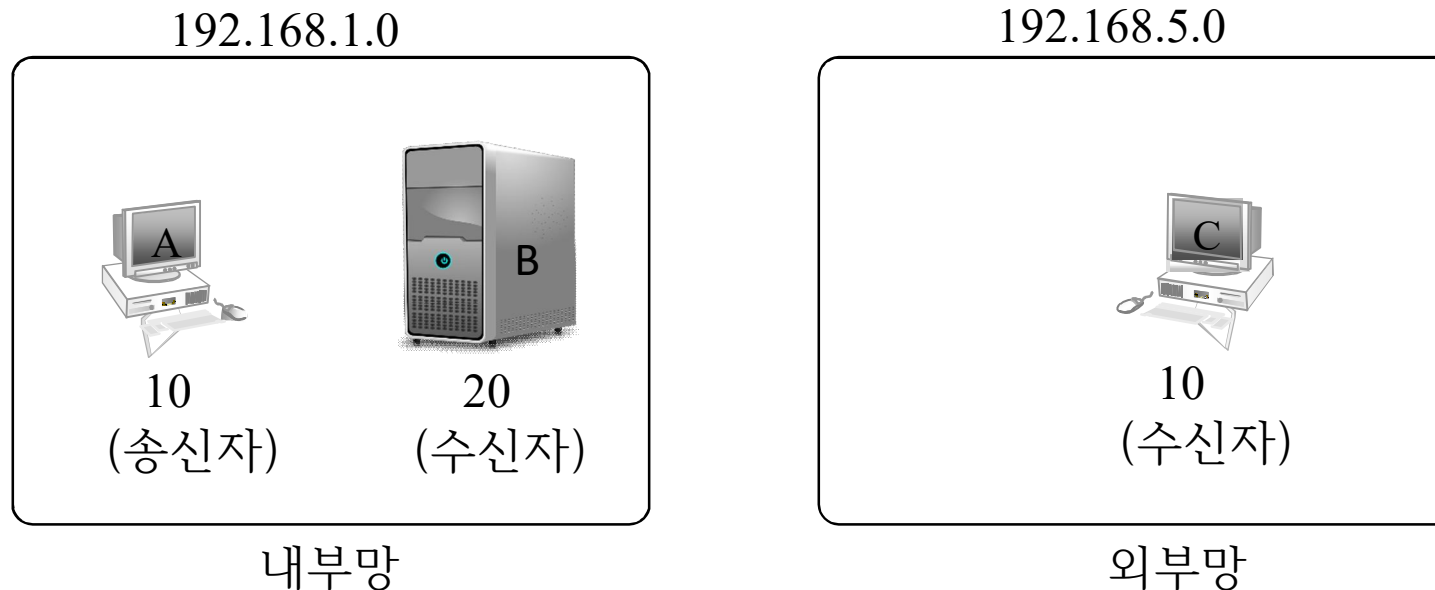
논리적 주소(3계층주소)

- IP address 구성
Network ID + Host ID
- Subnet Mask 기능
 - IP address의 Network ID와 Host ID 구분

IP address	192.168.1.10	255==1 & == X
& Subnet mask	& 255.255.255.0	
<hr/>		
Network ID	192.168.1. 0	

내부망과 외부망

- 송신자 : 데이터를 보내는 측 / 수신자 : 데이터를 받는 측

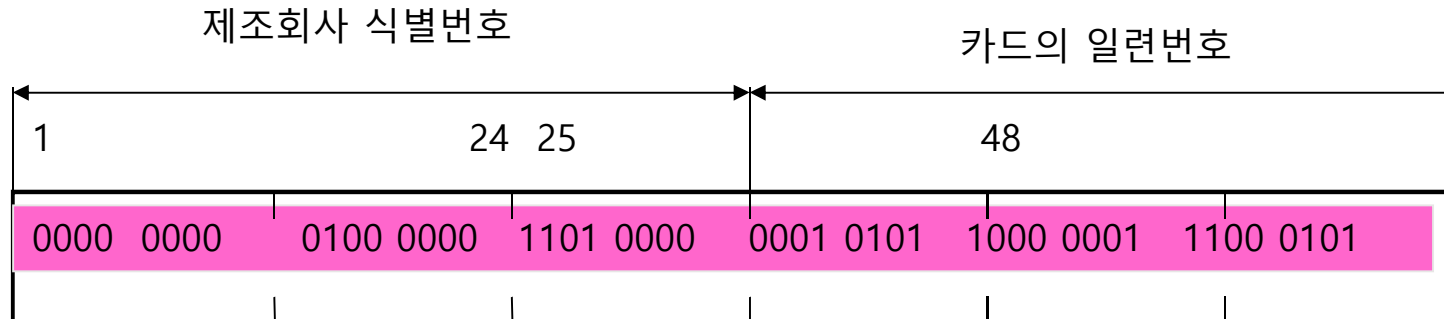


- 내부망 : 송수신자가 동일한 네트워크 ID를 사용
- 외부망 : 송수신자가 서로 다른 네트워크 ID를 사용

물리적 주소(2계층주소)

- Network Interface Card (NIC) 또는 Ethernet Card
- 데이터링크계층의 MAC 계층에 의해 사용되는 48비트의 하드웨어 주소

MAC 주소(16진수 표현) : 00-40-D0-15-81-C5



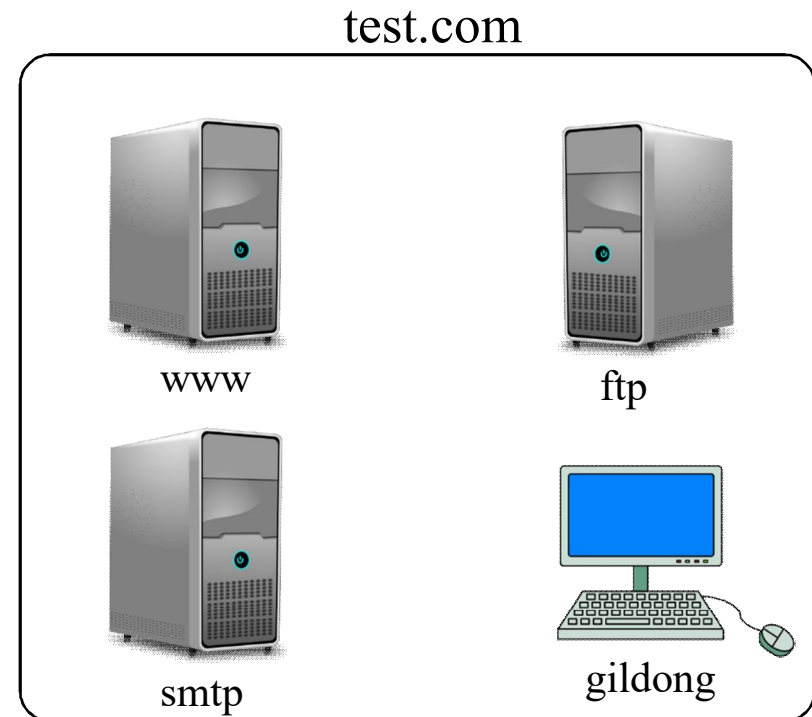
대표적인 제조회사 식별 번호의 예

- Intel: 00-A0-C9
- 3Com: 00-50-DA
- Realtek: 00-40-D0

Fully Qualified Domain Name (FQDN, 7계층 주소)

Host Name + Domain Name

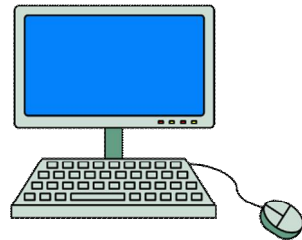
예) www.test.com



MAC/IP/FQDN Address

- MAC 주소 구성=제조회사+일련번호
- IP 주소 구성=네트워크ID+호스트ID
- FQDN 주소 구성=호스트명+도메인명

그룹주소+고유번호(명)



Client PC A

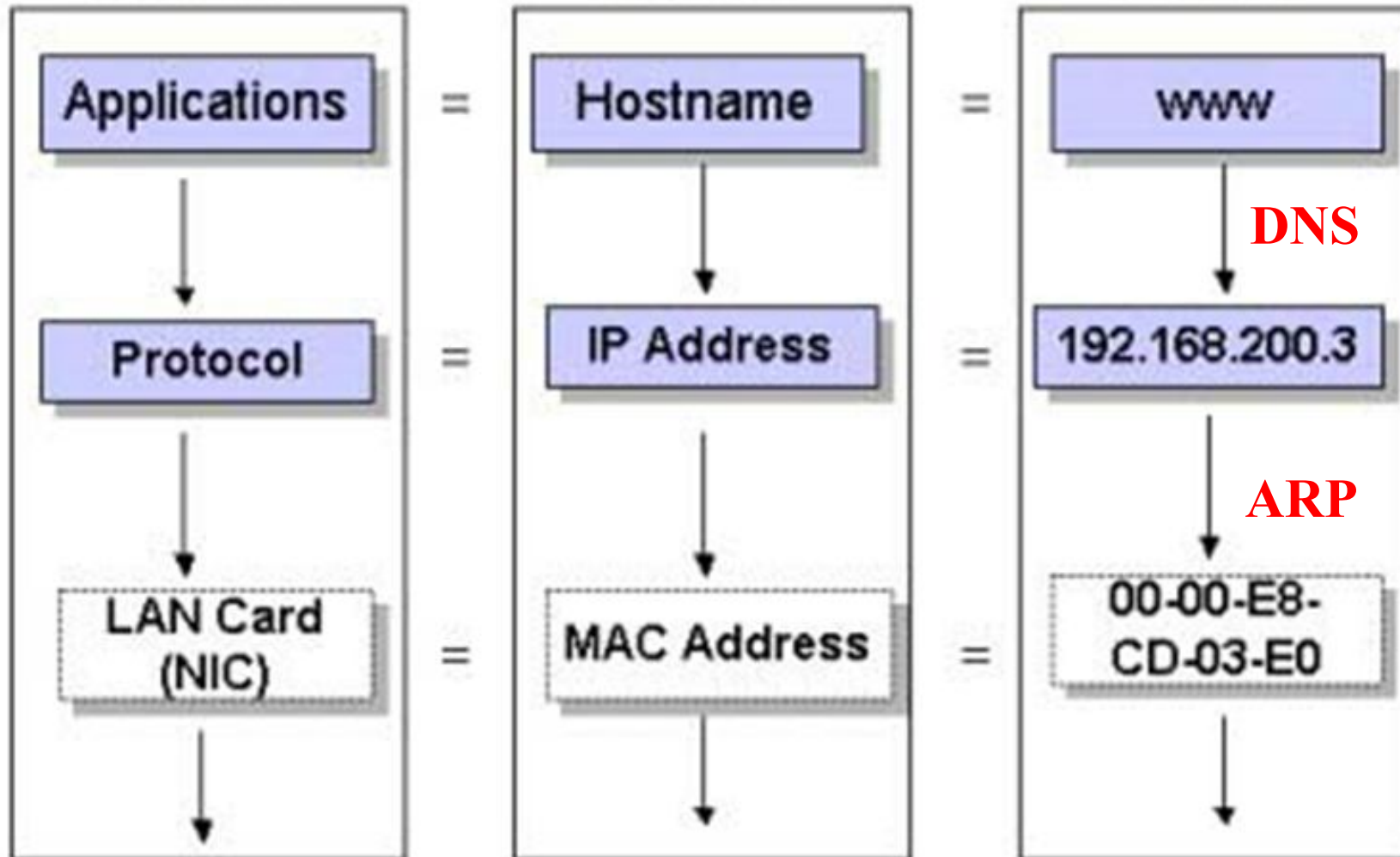
192.168.1.10
1111.2222.3333



Server B

www.test.com
192.168.1.20
3333.4444.5555

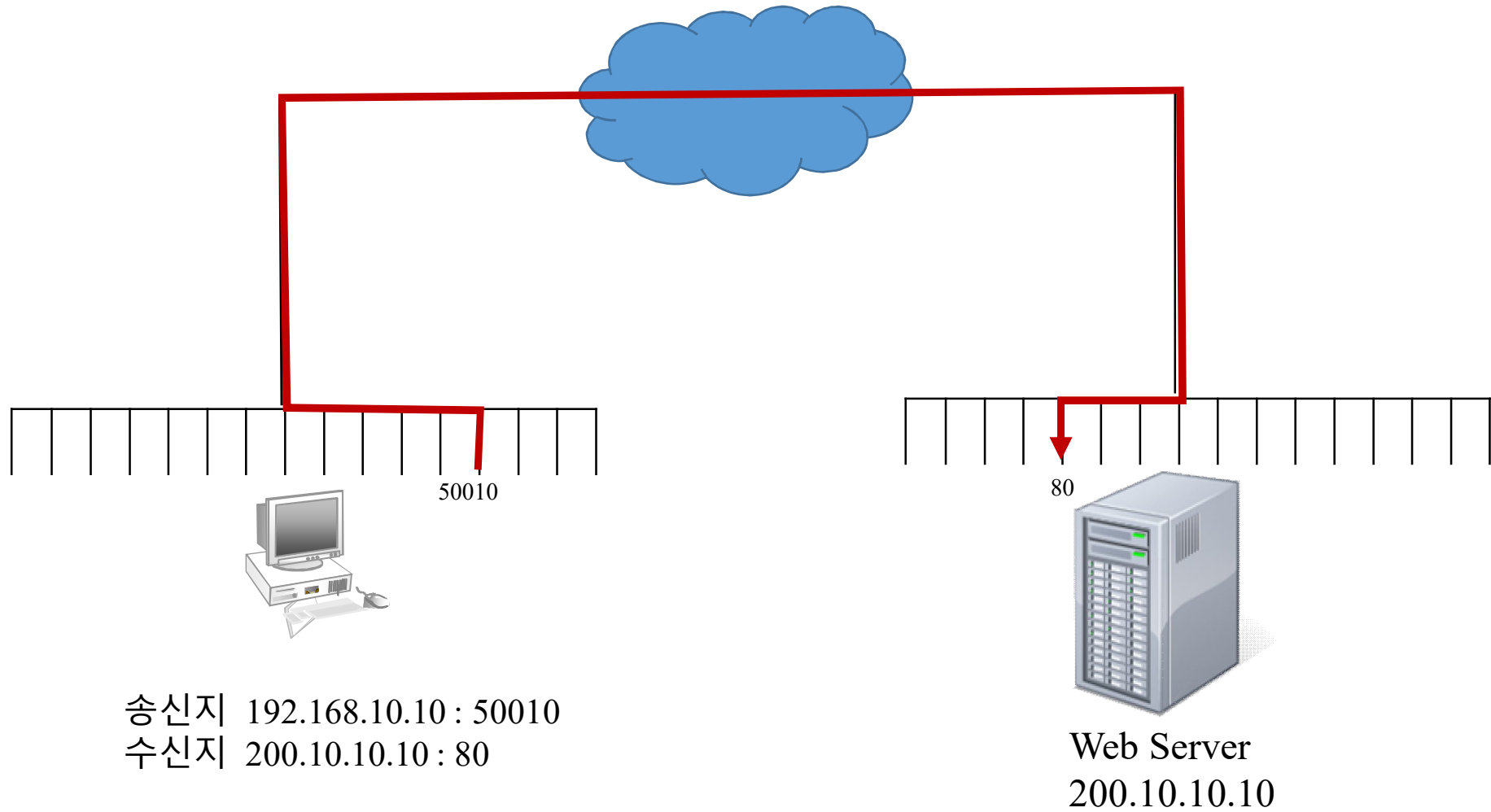
DNS & ARP



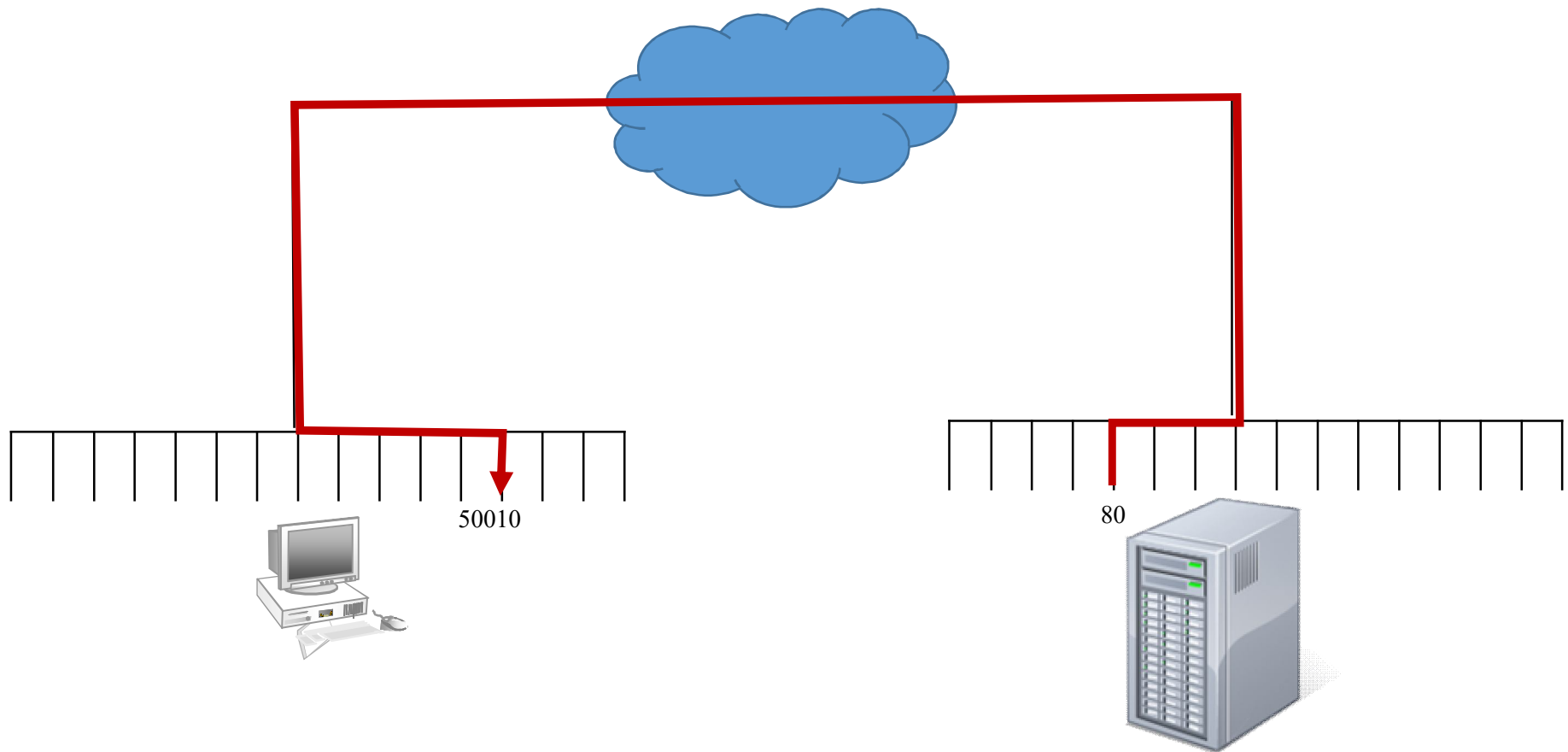
포트번호(4계층 주소)

- 데이터 송수신 번호
- 서비스 번호 또는 애플리케이션 번호
- 애플리케이션에서 부착해 전송
 - Well-Known Port : 1-1023
 - Registered Port : 1024-49151
 - Dynamic Port : 49152-65535

포트주소 (송신)



포트주소(수신)

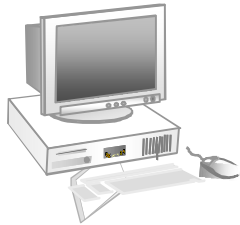


송신지 200.10.10.10 : 80
수신지 192.168.10.10 : 50010

2) 전송모드

- Unicast 1 : 1
- Broadcast 1 : m (불특정다수)
- Multicast 1 : n (특정다수)

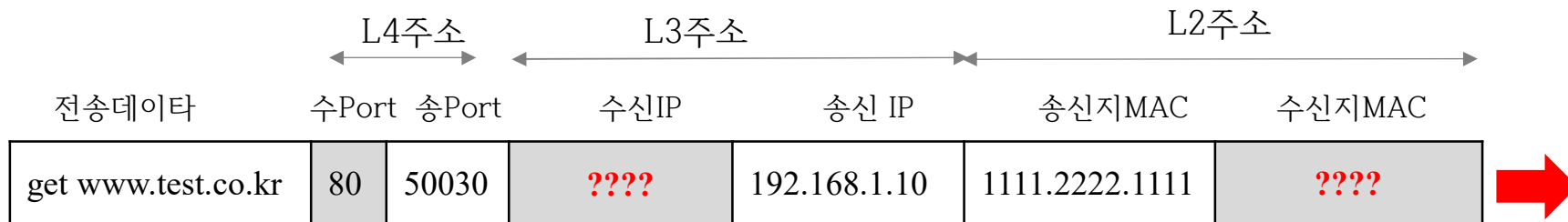
Unicast 전송모드



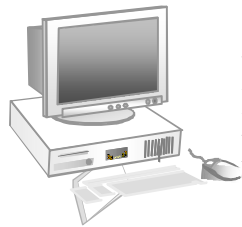
클라이언트(송신지)
IP 192.168.1.10
MAC 1111.2222.1111



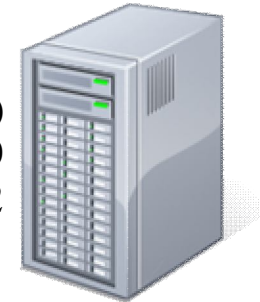
서버(수신지)
www.test.com
IP 192.168.1.20
MAC 1111.2222.2222



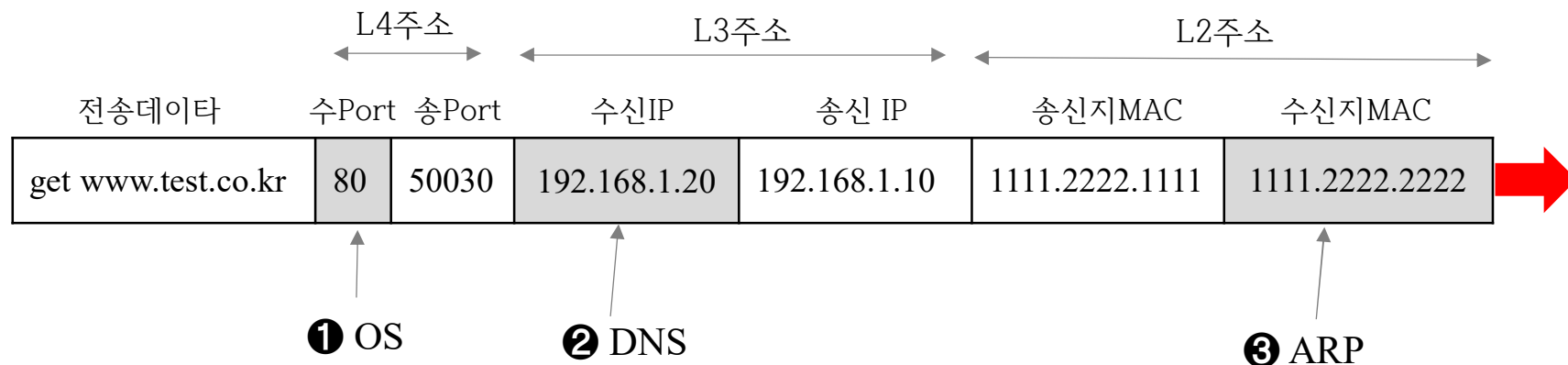
Unicast 전송모드



클라이언트(송신지)
IP 192.168.1.10
MAC 1111.2222.1111

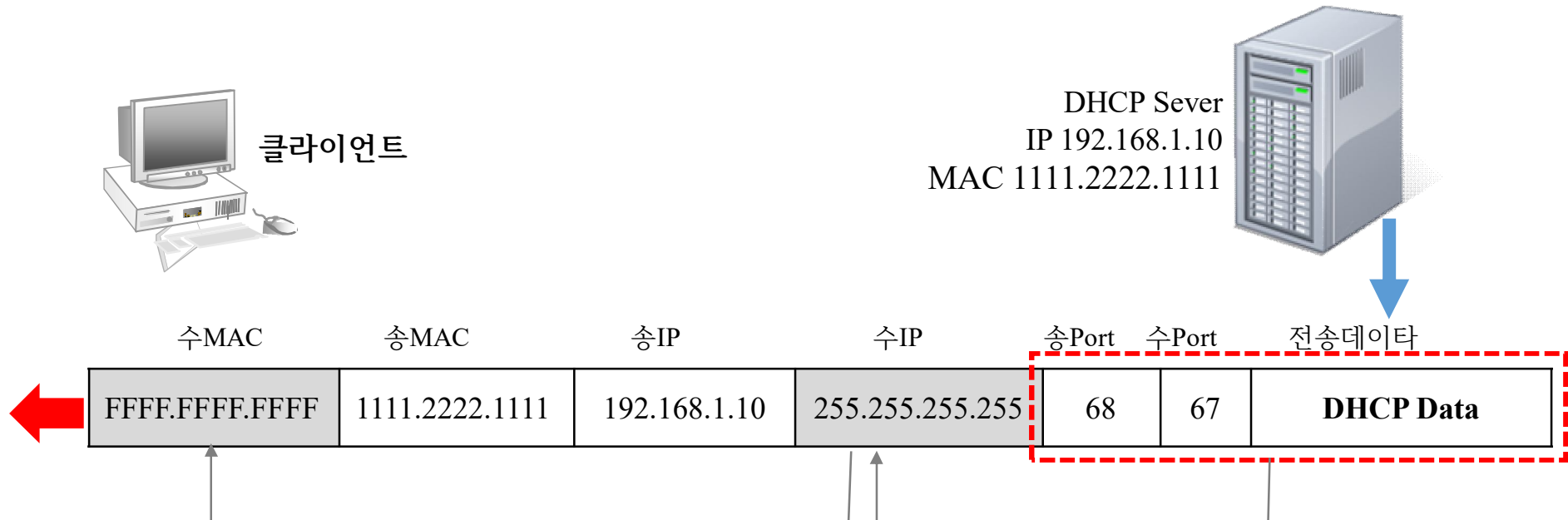


서버(수신지)
IP 192.168.1.20
MAC 1111.2222.2222

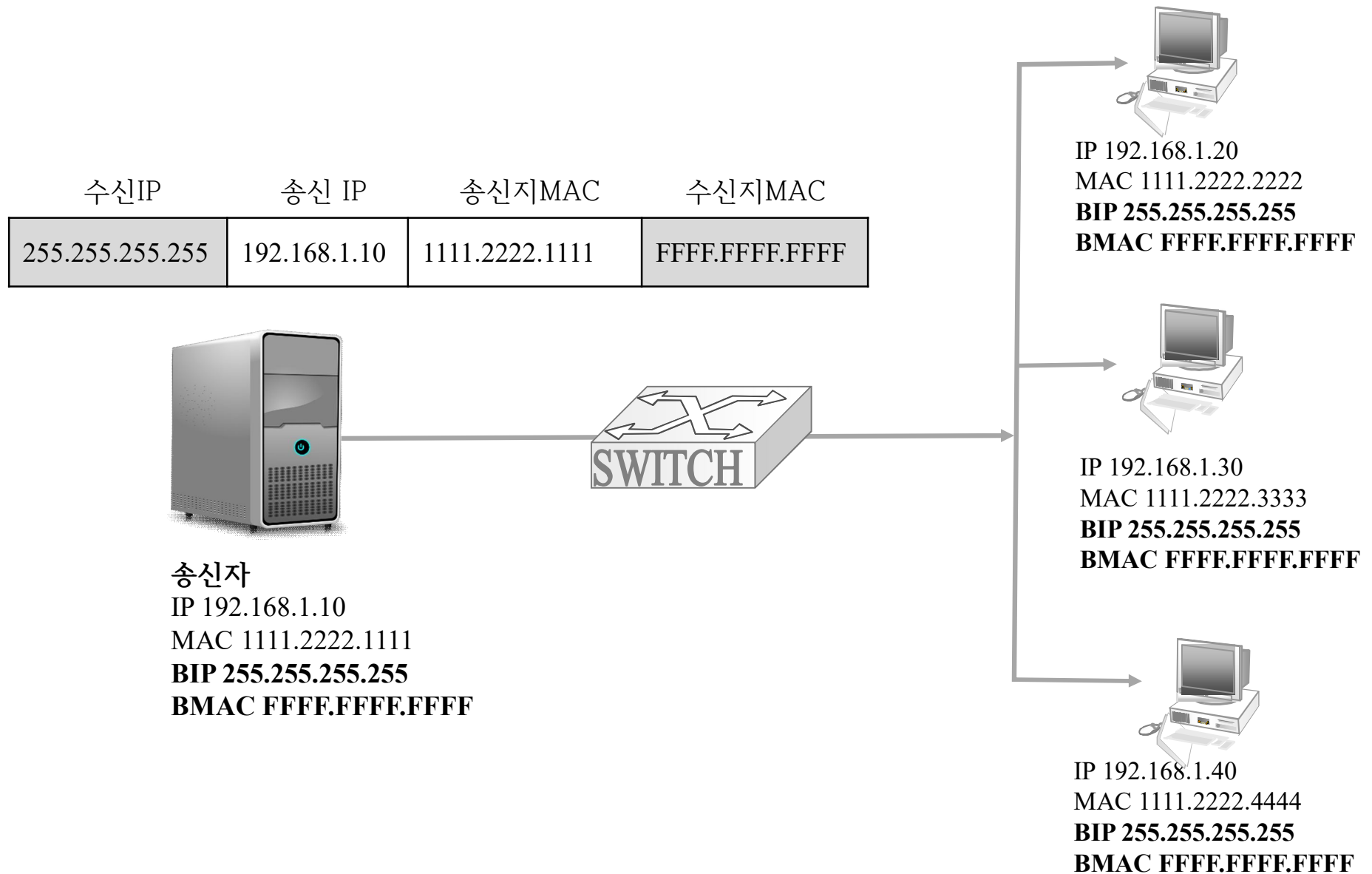


Broadcast 전송모드

- Broadcast IP 주소
 - Limited Broadcast(local broadcast) : 255.255.255.255
 - Directed Broadcast : 192.168.1.255/24
- Broadcast MAC 주소
 - FFFF.FFFF.FFFF

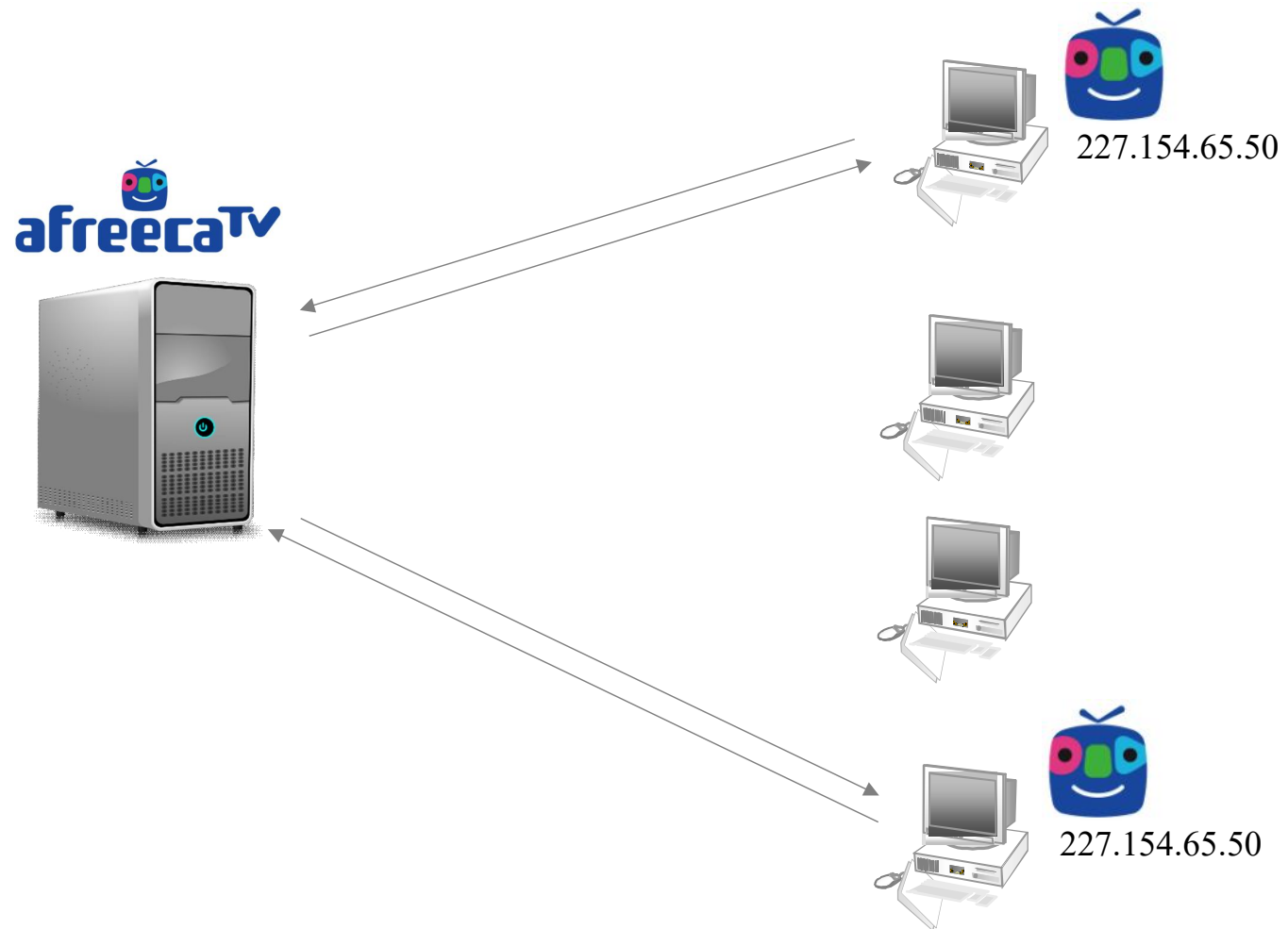


브로드캐스트 전송 예제



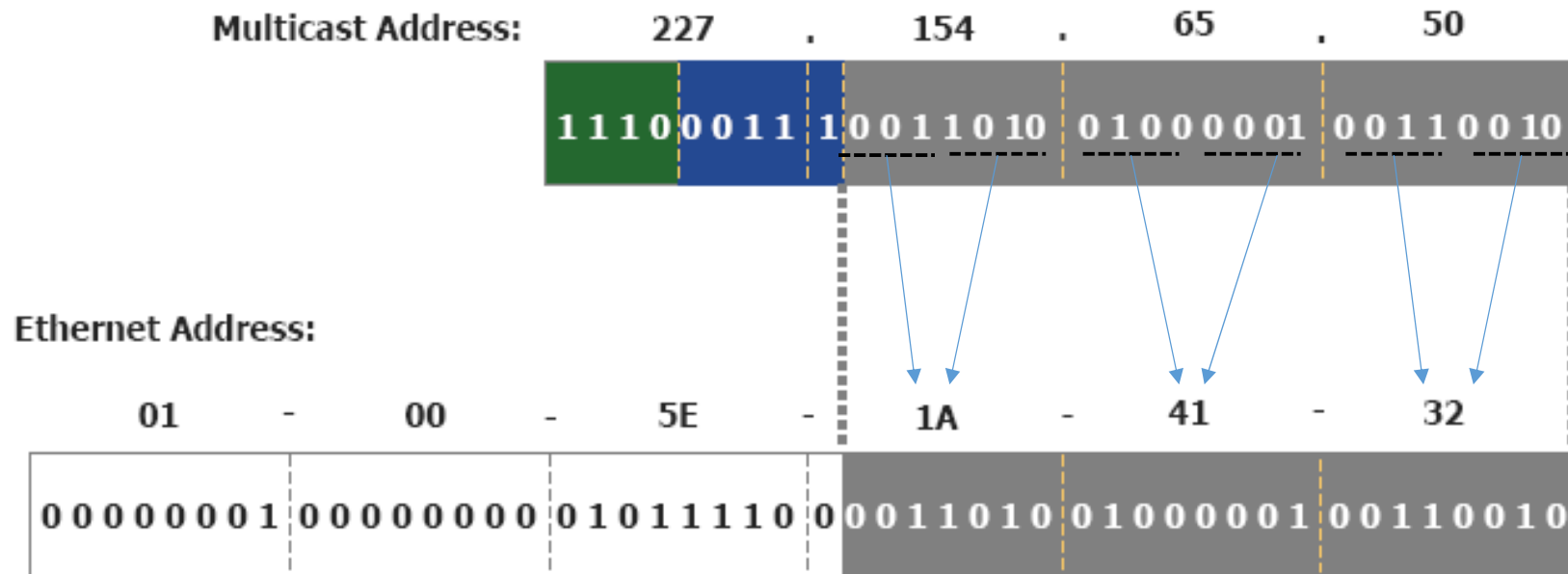
Multicast 전송모드

- Multicast IP 주소
 - **224-239**.X.X.X (예) 230.10.10.10



Multicast MAC 주소 형식 : 0100.5EXX.XXXX

- Multicast주소에 대한 MAC address Mapping 적용 예



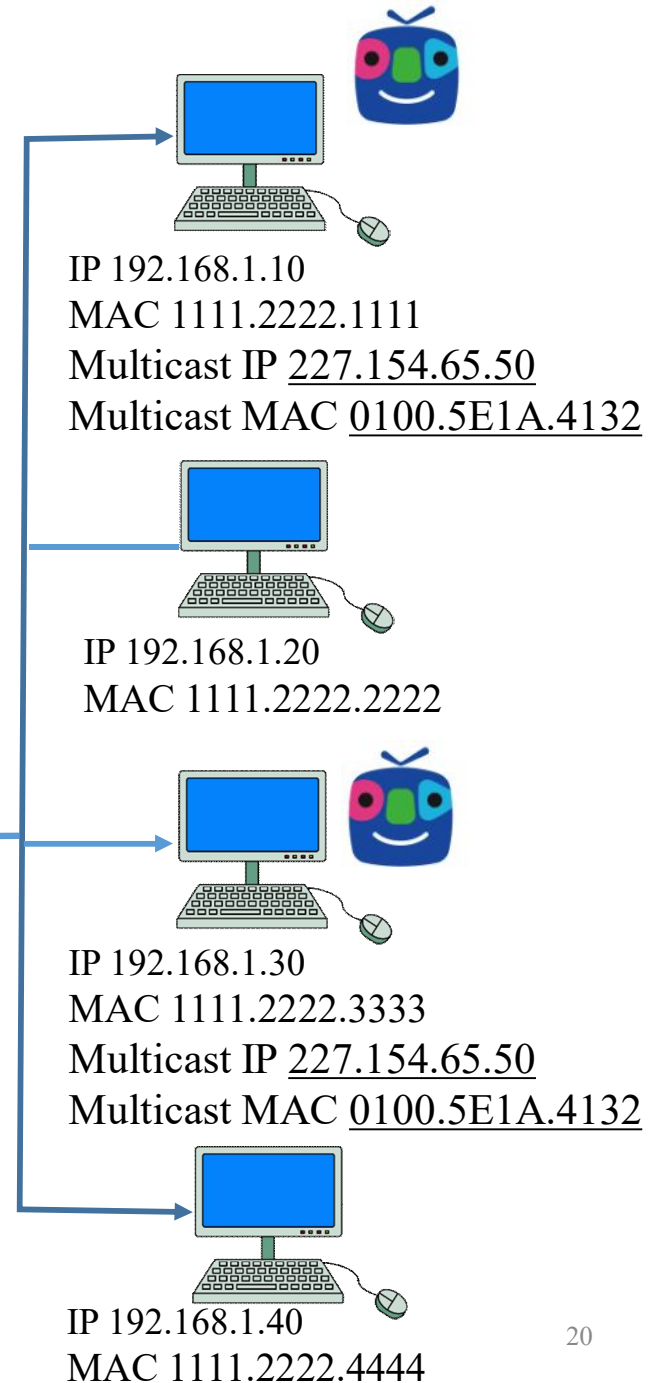
227.154.65.50 → 0100.5E1A.4132

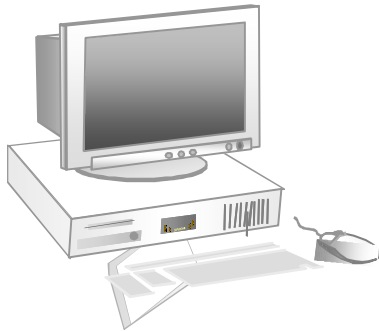
멀티캐스트 전송 예제

L3주소		L2주소	
수신IP	송신 IP	송신지MAC	수신지MAC
227.154.65.50	200.10.10.10	2222.4444.6666	0100.5E1A.4132



IP 200.10.10.10
MAC 2222.4444.6666
(라디오서버)





- Uni IP address / MAC address
 - 192.168.1.10/ MAC 1111.2222.1111
- Broadcast IP Address/ MAC Address
 - 255.255.255.255/ ffff.ffff.ffff
 - 192.168.1.255 / ffff.ffff.ffff
- Multicast IP Address/ MAC address
 - 224.0.0.22 (IGMPv3)/01-00-5e-00-00-16
 - 239.255.255.250(Device discovery)/01-00-5e-7f-ff-fa

ARP(Address Resolution Protocol)

- IP 주소에 대응 되는 MAC 주소를 조회 변환해 주는 서비스
- ARP 패킷 종류

① ARP request 패킷

- 송신지가 수신지의 MAC 주소를 조회하기 위해 보내는 질의 패킷
- 브로드캐스트 방식으로 운영

② ARP reply 패킷

- ARP request에 대해 응답 패킷
- 유니캐스트 방식으로 운영

ARP Cache Table

- IP주소와 MAC 주소의 대응 관계를 저장한 테이블
- ARP 캐시 테이블 확인 명령어 : arp -a

```
C:\#>arp -a
```

```
인터페이스: 192.168.35.131 --- 0x4
```

```
인터넷 주소
```

```
물리적 주소
```

```
192.168.35.1
```

```
00-23-aa-83-11-69
```

```
192.168.35.115
```

```
38-8c-50-9a-9b-b1
```

```
192.168.35.211
```

```
04-b4-29-bf-07-09
```

```
192.168.35.255
```

```
ff-ff-ff-ff-ff-ff
```

```
224.0.0.22
```

```
01-00-5e-00-00-16
```

```
224.0.0.251
```

```
01-00-5e-00-00-fb
```

```
224.0.0.252
```

```
01-00-5e-00-00-fc
```

```
239.255.255.250
```

```
01-00-5e-7f-ff-fa
```

```
255.255.255.255
```

```
ff-ff-ff-ff-ff-ff
```

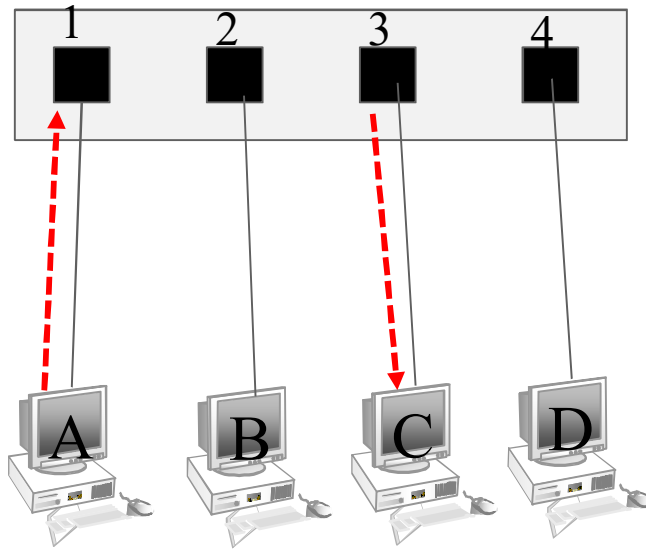
유형적
동적
정적
정적
정적
정적

3) 계층별 장비

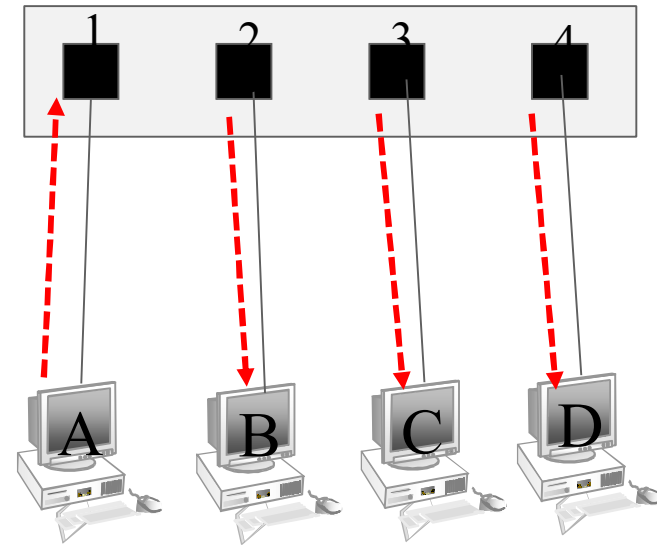
- Switch
- Router
- Hub

Forwarding과 Flooding

- Forwarding : 하나의 송신지 포트에서 하나의 수신지 포트에 트래픽 전송
- Flooding : 송신지 포트를 제외한 나머지 포트들로 트래픽 전송



Forwarding(포워딩)

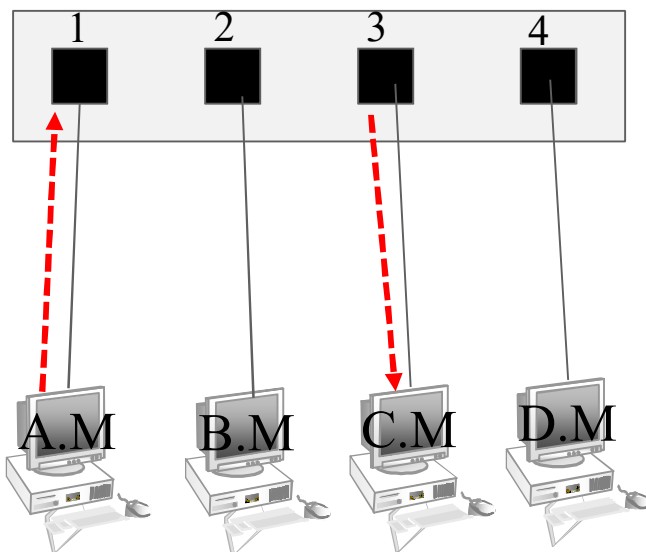


Flooding(플러딩)

Switch(2계층 장비)

MAC Address Table

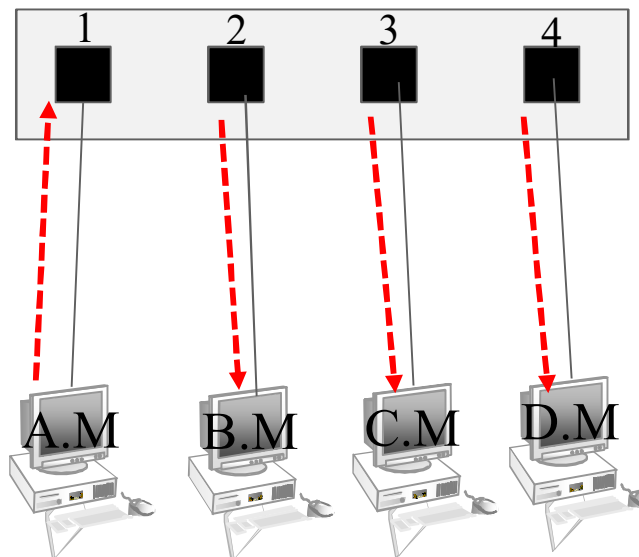
목적지	출구번호
A.M	1
B.M	2
C.M	3



A.M	C.M
송MAC	수MAC

MAC Address Table

목적지	출구번호
A.M	1
B.M	2
C.M	3

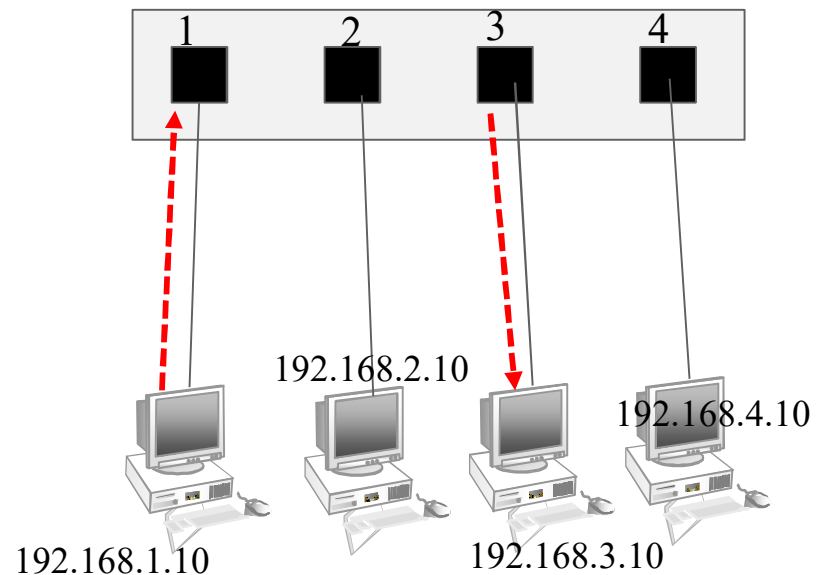


A.M	D.M
송MAC	수MAC

Router(3계층 장비)

Routing Table

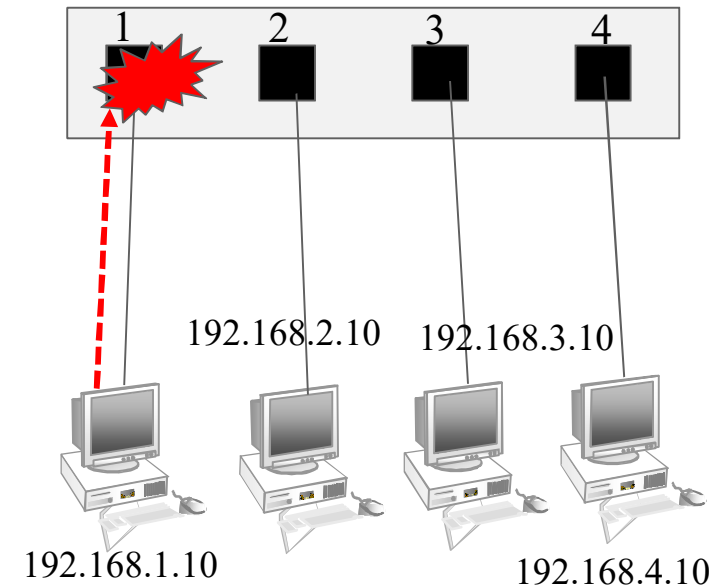
목적지	출구번호
192.168.1.0	1
192.168.2.0	2
192.168.3.0	3



192.168.1.10	192.168.3.10
송신지IP	수신지IP

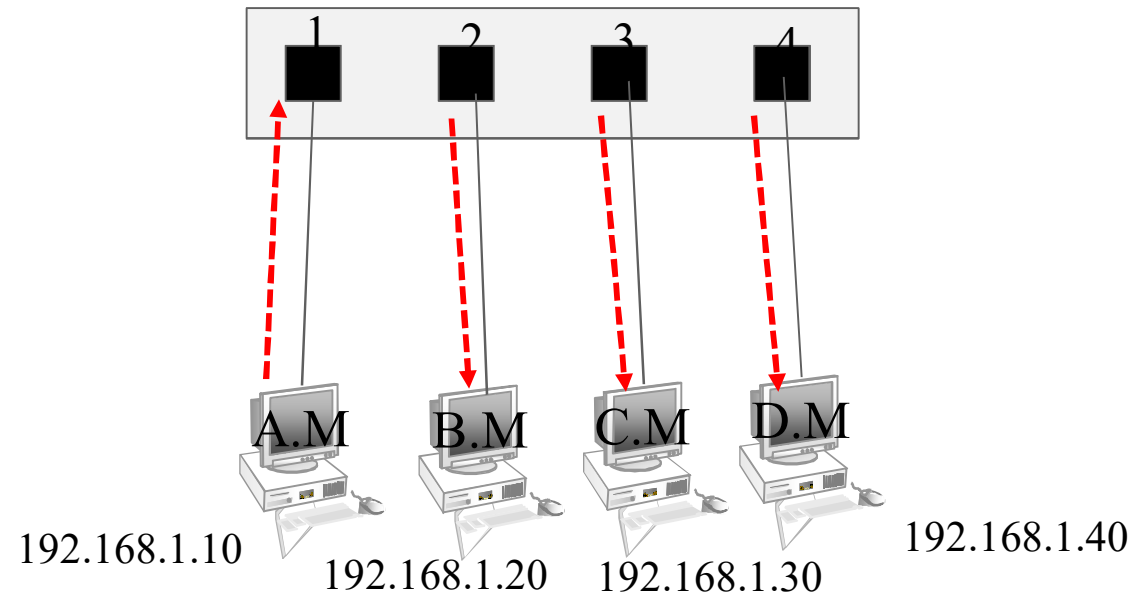
Routing Table

목적지	출구번호
192.168.1.0	1
192.168.2.0	2
192.168.3.0	3



192.168.1.10	192.168.4.10
송신지IP	수신지IP

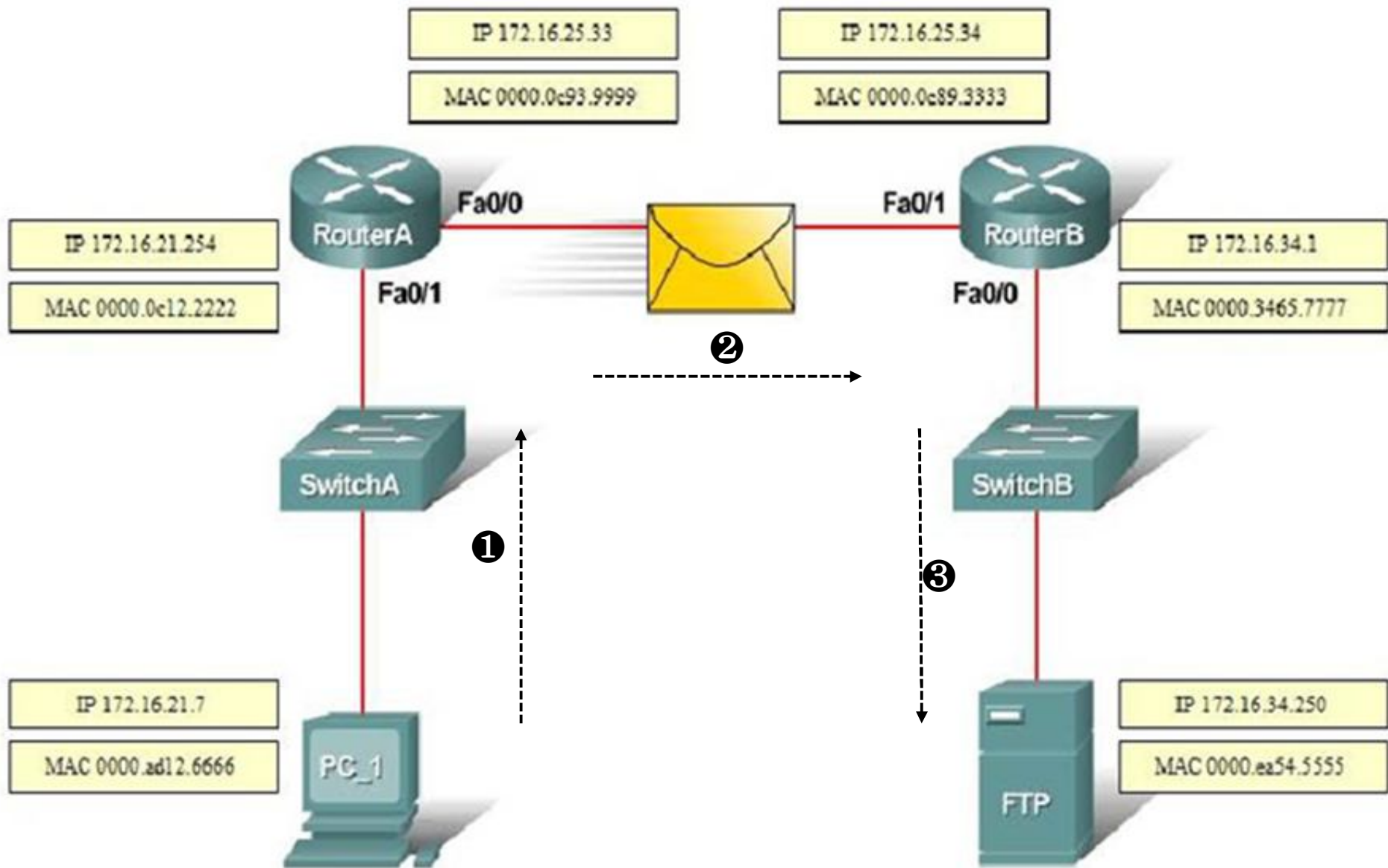
Hub(1계층 장비)



192.168.1.10	192.168.4.10	A.M	D.M
송신지IP	수신지IP	송MAC	수MAC

Media Translation

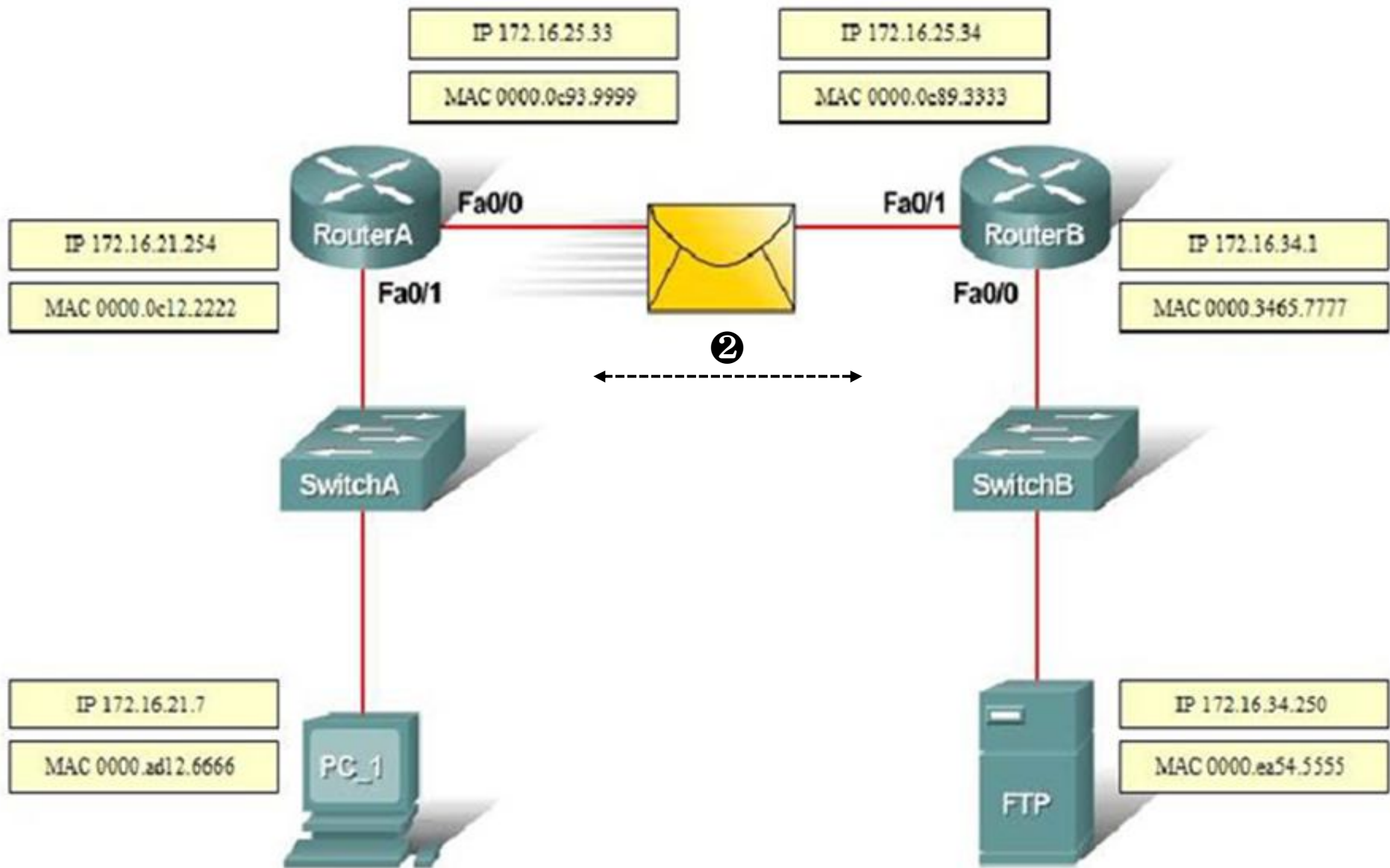
- 3계층 이상의 장비에서 처리
- 패킷이 출발지에서 목적지까지 가는 동안 3계층 장비를 거칠 때마다 L2 헤더 (프레임 헤더) 변경
 - 3계층 주소(IP주소) 변환 없음
 - 2 계층주소는 스위칭 환경에 따라 변환



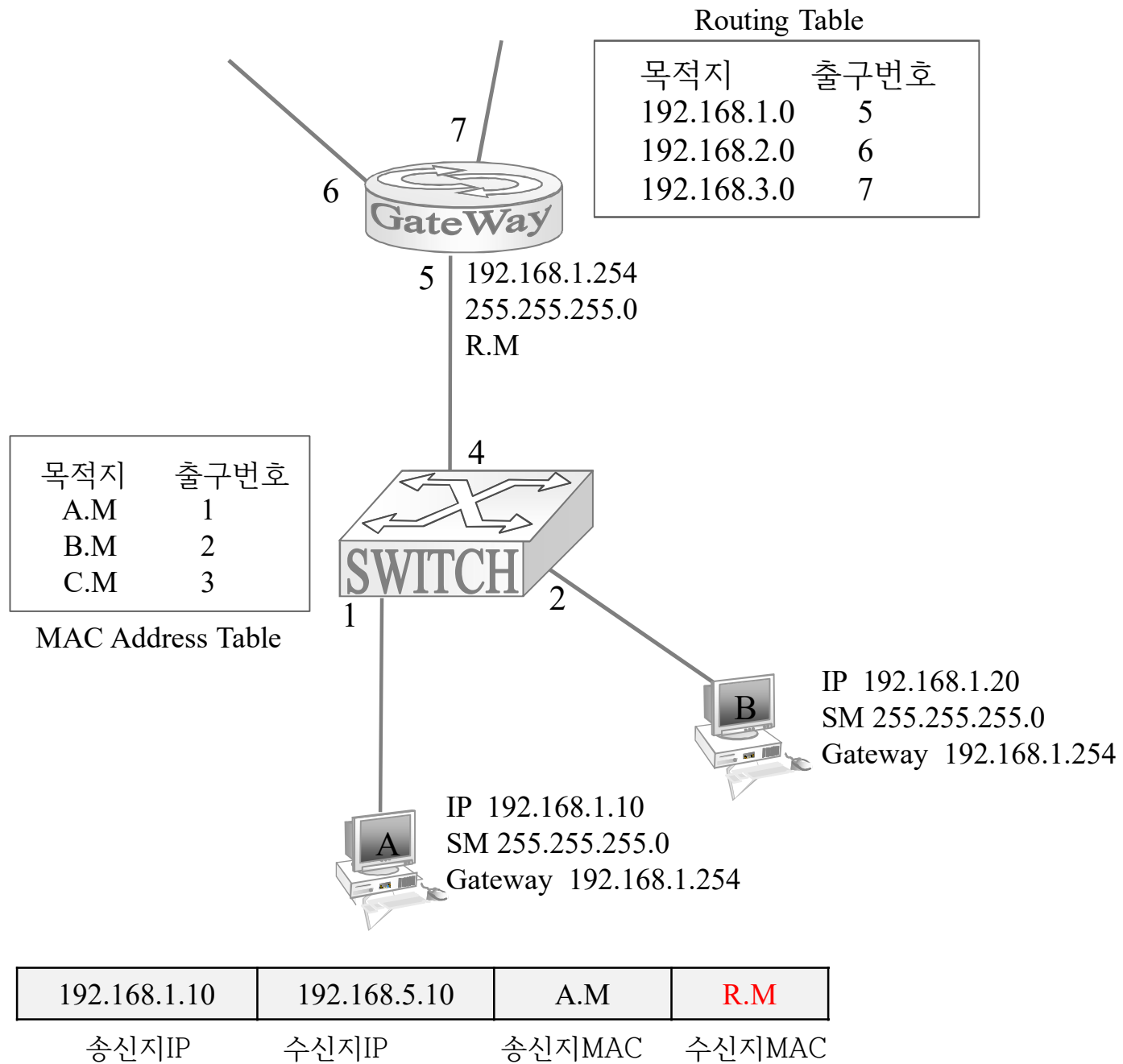
Source MAC	Destination MAC	Source IP	Destination IP

Media Translation

	Source IP	Destination IP	Source MAC	Destination MAC
PC-1 → RA	172.16.21.7	172.16.34.250	6666	2222
RA → RB	172.16.21.7	172.16.34.250	9999	3333
RB → FTP	172.16.21.7	172.16.34.250	7777	5555



Source MAC	Destination MAC	Source IP	Destination IP



4) 트래픽 흐름

- 내부망 트래픽 흐름
- 외부망 트래픽 흐름

트래픽 흐름(내부망)

1 단계. DNS를 이용하여 수신지 IP 주소 조회

- DNS 캐시 조회 (c:\> ipconfig /displaydns)
- Hosts.txt 파일 조회 (\windows\system32\drivers\etc\hosts)
- DNS 서버 이용

2 단계. 송신자 서브넷 마스크를 이용하여 수신지가 (내부망/외부망)에
존재하는지 확인

3 단계. 수신지 MAC 주소 조회

- ARP 캐쉬 조회
- ARP Request/Reply 를 이용

4단계. 수신지로 트래픽 전송

트래픽 흐름(외부망)

1 단계. DNS를 이용하여 수신지 IP 주소 조회

- DNS 캐시 조회 (c:\> ipconfig /displaydns)
- Hosts.txt 파일 조회 (windows\system32\drivers\etc\hosts)
- DNS 서버 이용

2 단계. 송신자 서브넷 마스크를 이용하여 수신지가 (내부망/외부망)에 존재하는지 확인

3 단계. GateWay의 MAC 주소 조회

- ARP 캐쉬 조회
- ARP Request/Reply 전송

4단계. Media Translation 방법으로 수신지로 트래픽 전송