

# 네트워크프로그래밍-2주

## TCP/IP 환경의 이해

### 프로토콜 분석

정인환교수

# 1주 TCP/IP 환경의 이해

- ▶ TCP/IP 환경 - 공인 IP / 사설 IP
- ▶ TCP/IP 환경의 이해 - 고정 IP 사용 환경
  - 한성대학교 네트워크 구성도
- ▶ TCP/IP 환경의 이해 - 공유기 사용하는 환경
  - 구성예 1 ~ 4
  - 공유기 동작 원리 NAT
- ▶ 라우팅의 원리
- ▶ TCP/IP 환경에서 라우팅
  - DATA 교환 순서, ARP 동작 순서
- ▶ 프로토콜분석 실습
  - ARP 분석
  - TCP 분석
  - IP 분석
  - DNS 분석
  - HTTP Web Data 분석
- ▶ Web Server 설치 및 HTTP 프로토콜 분석

# TCP/IP 환경 - 공인 IP / 사설 IP

## ▶ 공인 IP (Public IP)

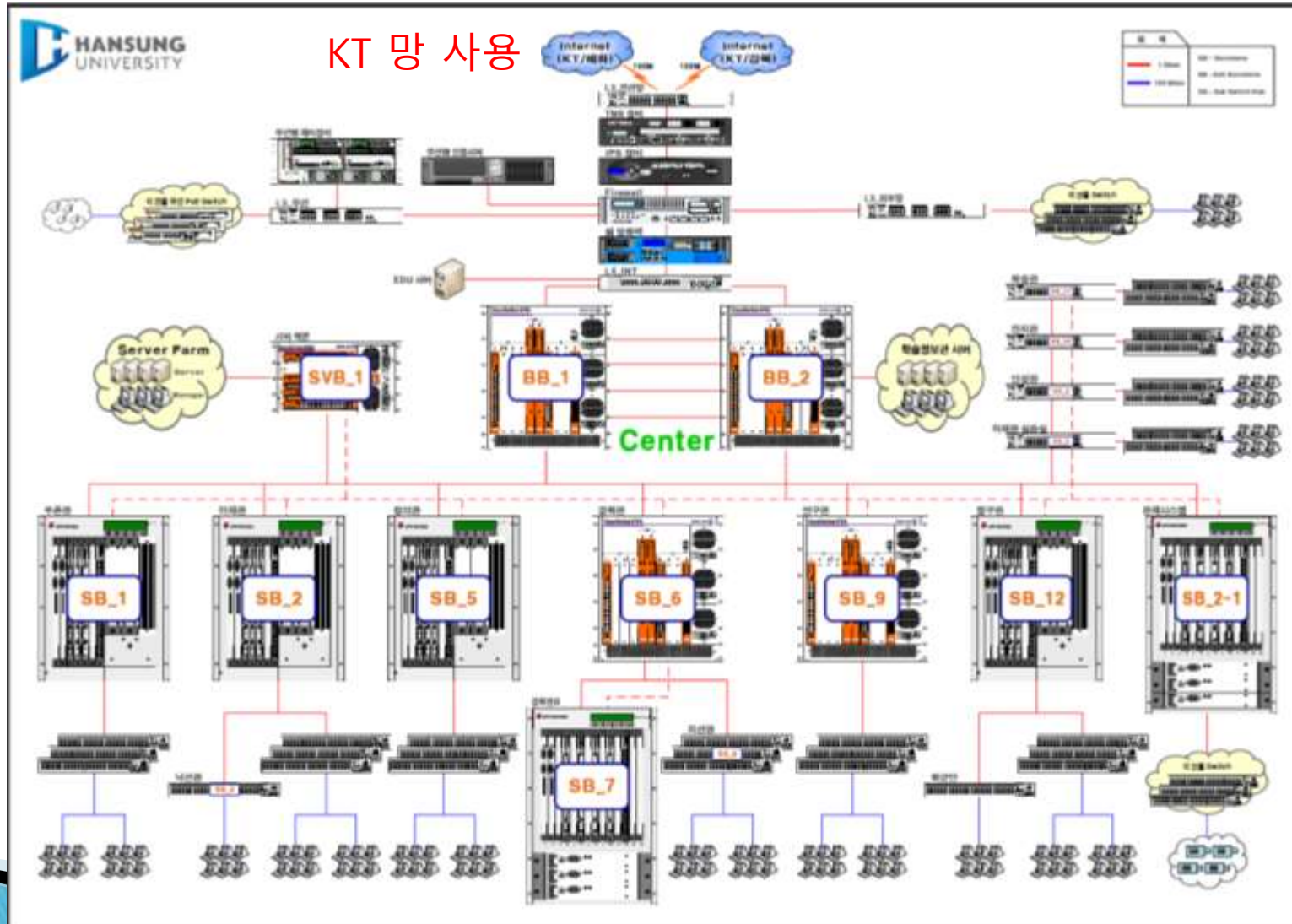
- 전세계 유일한 고유 IP 주소
- 외부 망에서 직접 연결 가능한 주소
- IPv4 : 4 bytes
- IPv6 : 16 bytes
- IPv4 주소가 부족하게 됨

## ▶ 사설 IP/비공인 IP (private IP) - 공유기 사용하여 IP를 공유함

- 공인 IP 부족을 해결하는 방법
- 하나의 공인 IP를 다수의 비공인(사설) IP 들이 공유
- 공유기 (Home Router) 사용 환경 - 강의노트 6 ~ 10
  - NAT : Network Address Translation 기능
  - 비공인 IP 영역
    - 10.XXX.XXX.XXX
    - 172.16.XXX.XXX ~ 172.31.XXX.XXX
    - 192.168.0.XXX ~ 192.168.255.XXX

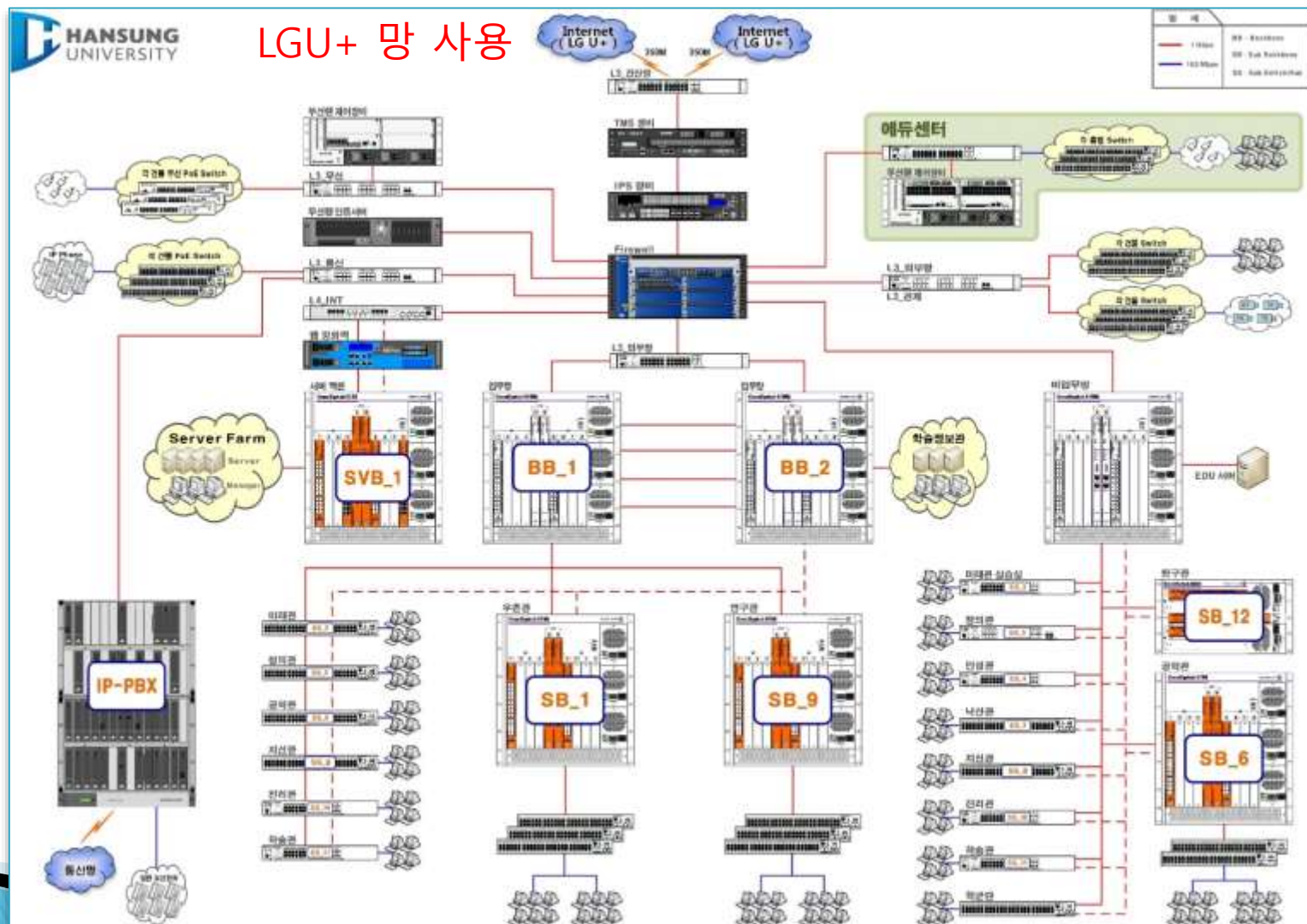
# TCP/IP 환경의 이해 - 공인 IP 사용환경

## ▶ 한성대학교 네트워크 구성도 - 2011 까지



# TCP/IP 환경의 이해 - 공인 IP 사용환경

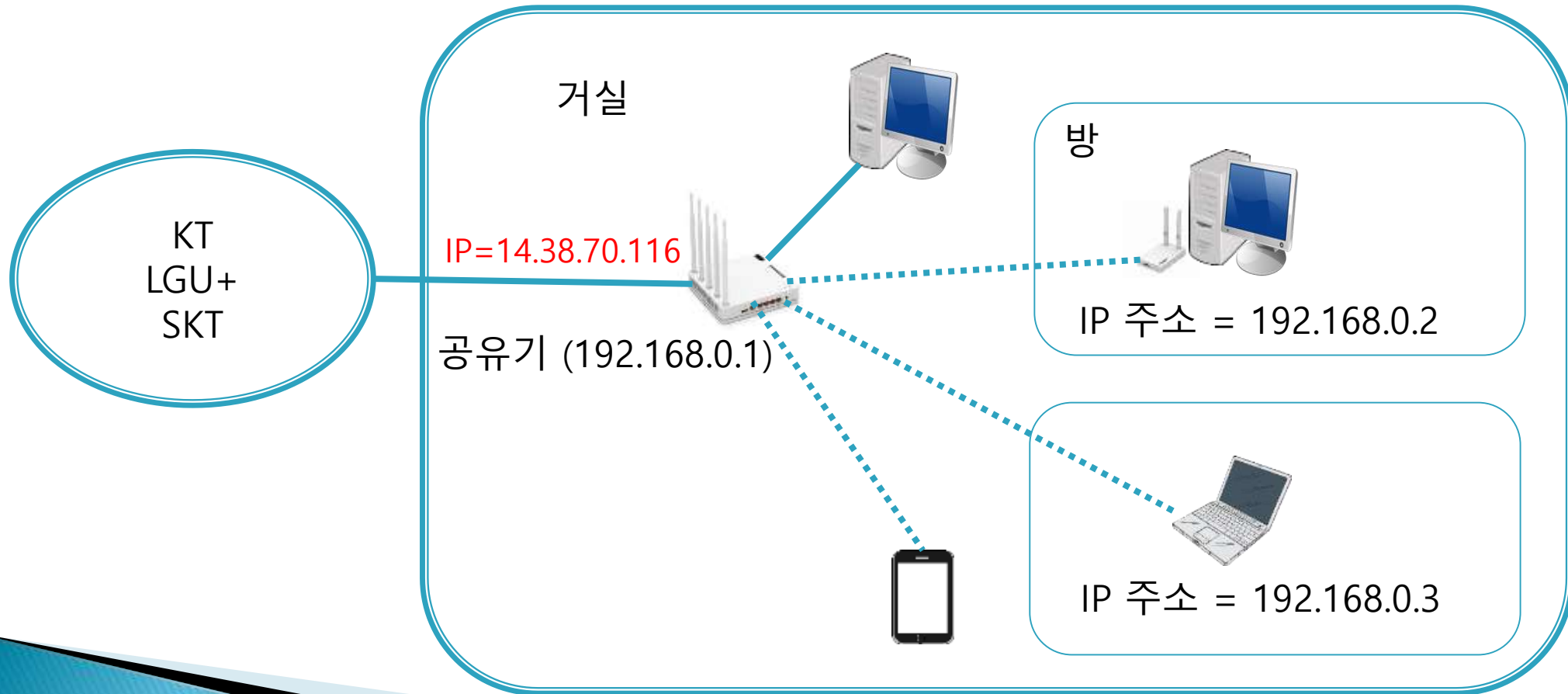
## ▶ 한성대학교 네트워크 구성도 - 2012 이후





# TCP/IP 환경의 이해

- ▶ 공유기 사용 환경 예 1 - KT 인터넷 1회선만 사용, IPTIME 공유기
  - IPTIME 공유기로 모두 유/무선 연결



# 공유기 원리 NAT(Network Address Translation)

192.168.0.2



Connection Table

IP	Port	IP	Port
192.168.0.2	1234	220.66.102.11	80

공유기

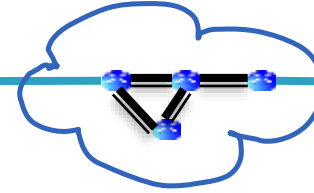
192.168.0.1



NAT Table

IP	Port	IP	Port	IP	Port
192.168.0.2	1234	14.38.70.116	5678	220.66.102.11	80

14.38.70.116



www.hansung.ac.kr  
220.66.102.11

Connection Table

IP	Port	IP	Port
14.38.70.116	5678	220.66.102.11	80

192.168.0.3



NAT (Network Address Translation)

IP	Port	IP	Port
192.168.0.3	5555	A.B.C.D	PP

IP	Port	IP	Port	IP	Port
192.168.0.3	5555	14.38.70.116	6666	A.B.C.D	PP

14.38.70.116

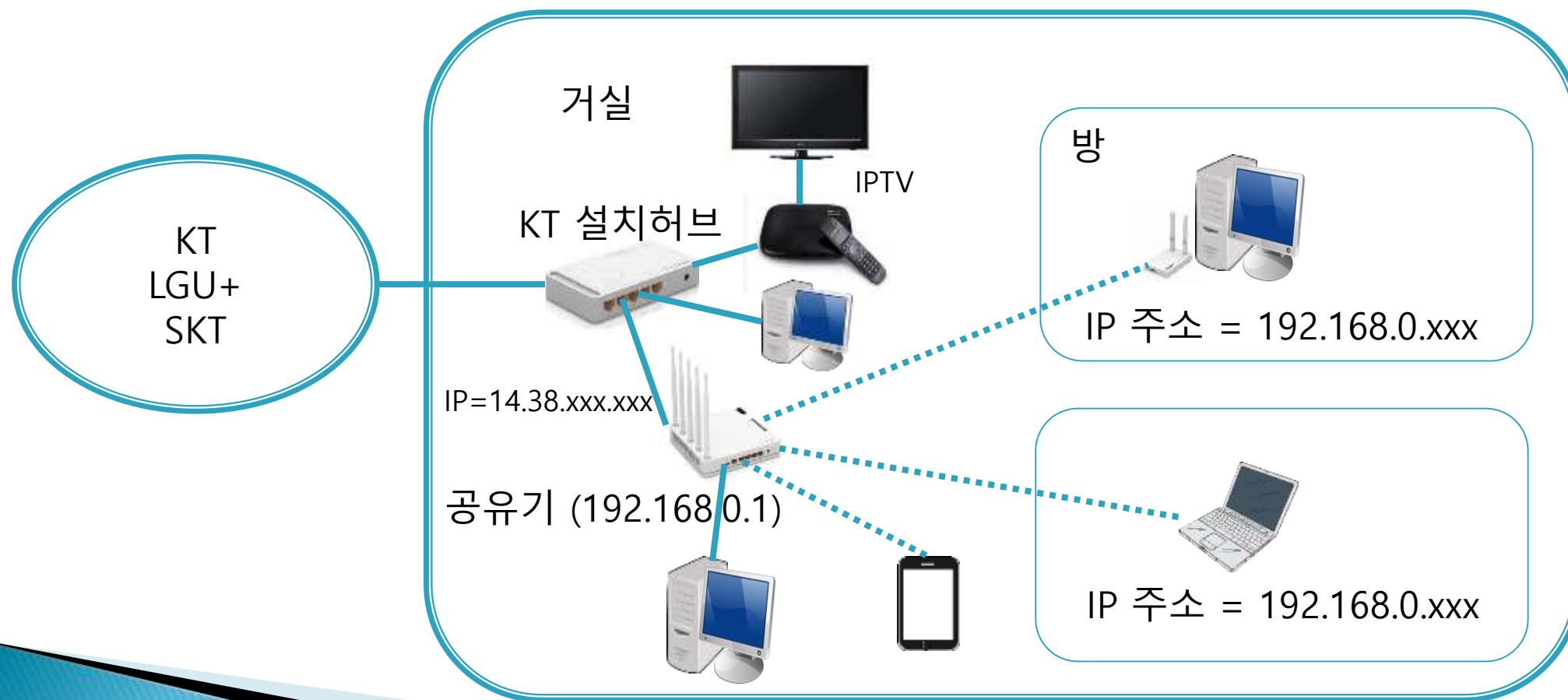
Internet Server  
IP = A.B.C.D Port = PP

IP	Port	IP	Port
14.38.70.116	6666	A.B.C.D	PP

14.38.70.116

# TCP/IP 환경의 이해

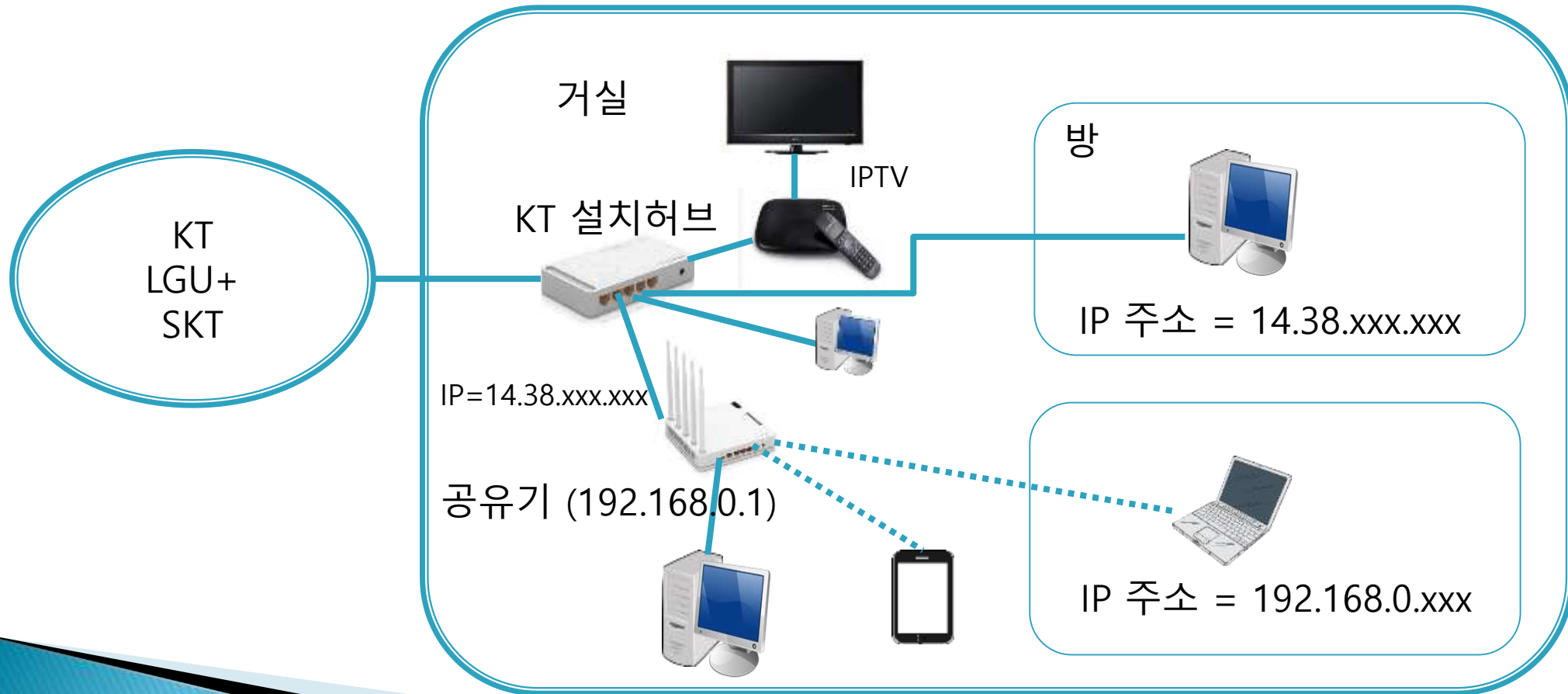
- ▶ 공유기 사용 환경 예 2 - KT 인터넷, IPTV 사용, IPTIME 공유기 사용
  - IPTIME 공유기로 모두 유/무선 연결





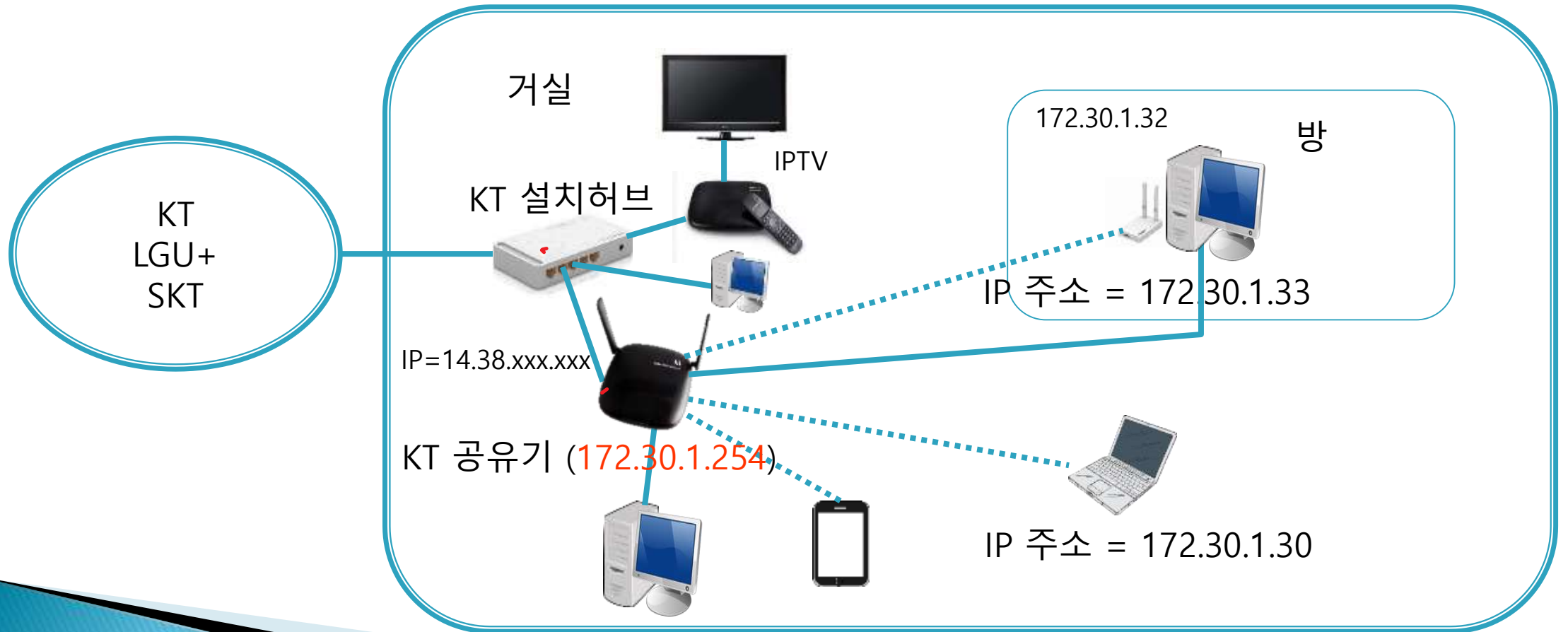
# TCP/IP 환경의 이해

- ▶ 공유기 사용 환경 예 3 - KT 인터넷, IPTV 사용, IPTIME 공유기 사용
  - PC는 유선 KT 연결, IPTIME 공유기에 유/무선으로 PC, 노트북, 스마트폰



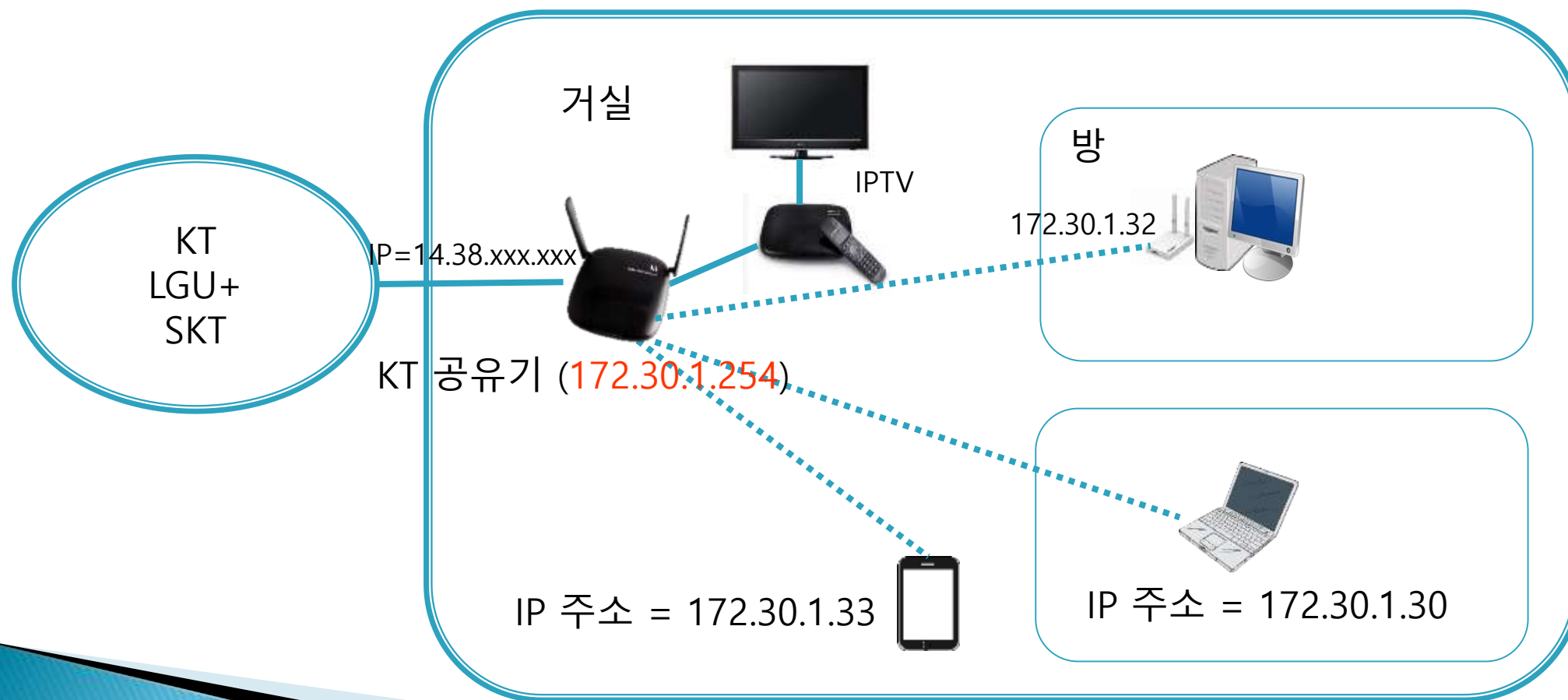
# TCP/IP 환경의 이해

- ▶ 공유기 사용 환경 예 4 - KT 인터넷, IPTV 사용, KT 허브, 공유기 사용
  - **KT 공유기**에 PC는 유/무선 연결, 노트북, 스마트폰은 무선 연결



# TCP/IP 환경의 이해

- ▶ 공유기 사용 환경 예 5 - KT 인터넷, IPTV 사용, KT 공유기 사용
  - **KT 공유기**에 PC는 유/무선 연결, 노트북, 스마트폰은 무선 연결



# 공유기 원리 NAT(Network Address Translation)

172.30.1.33



Connection Table

IP	Port	IP	Port
172.30.1.33	1234	220.66.102.11	80

공유기

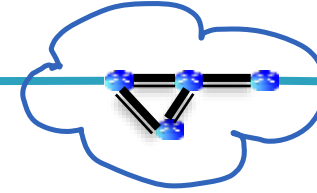
172.30.1.254



14.38.70.102

NAT Table

IP	Port	IP	Port	IP	Port
172.30.1.33	1234	14.38.70.116	5678	220.66.102.11	80



www.hansung.ac.kr  
220.66.102.11

Connection Table

IP	Port	IP	Port
14.38.70.116	5678	220.66.102.11	80

172.30.1.30



NAT (Network Address Translation)

IP	Port	IP	Port
172.30.1.30	5555	A.B.C.D	PP

IP	Port	IP	Port	IP	Port
172.30.1.30	5555	14.38.70.116	6666	A.B.C.D	PP

Internet Server  
IP = A.B.C.D Port = PP

IP	Port	IP	Port
14.38.70.116	6666	A.B.C.D	PP

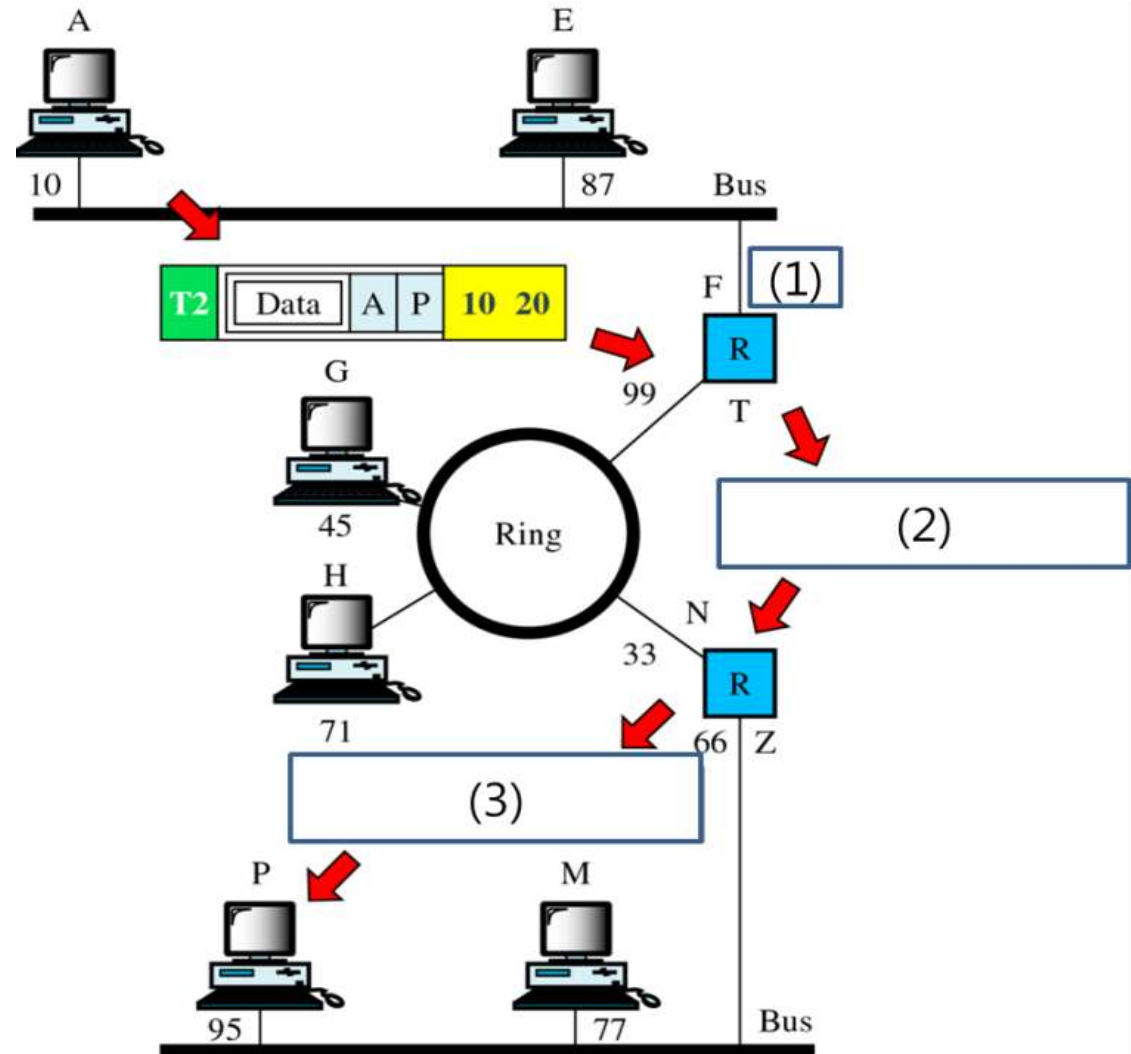
# 라우팅의 원리

## ▶ L2 Address

- 10, 20 ...
- Data Link Layer
- Physical Address
- 1:1 전달용
- MAC Address

## ▶ L3 Address

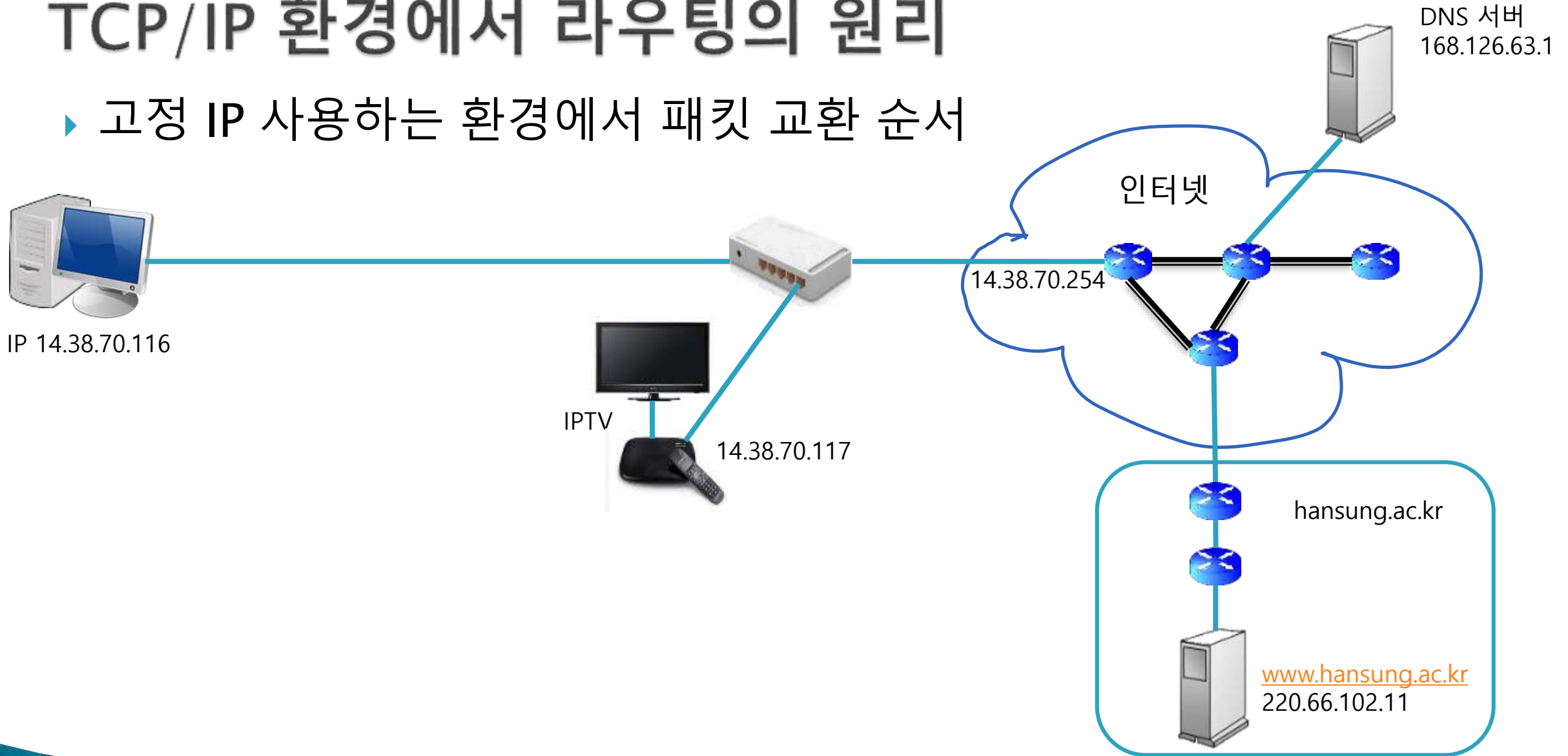
- A~P ...
- Network Layer
- Router 거쳐서 전달용
- Logical Address
- IP Address

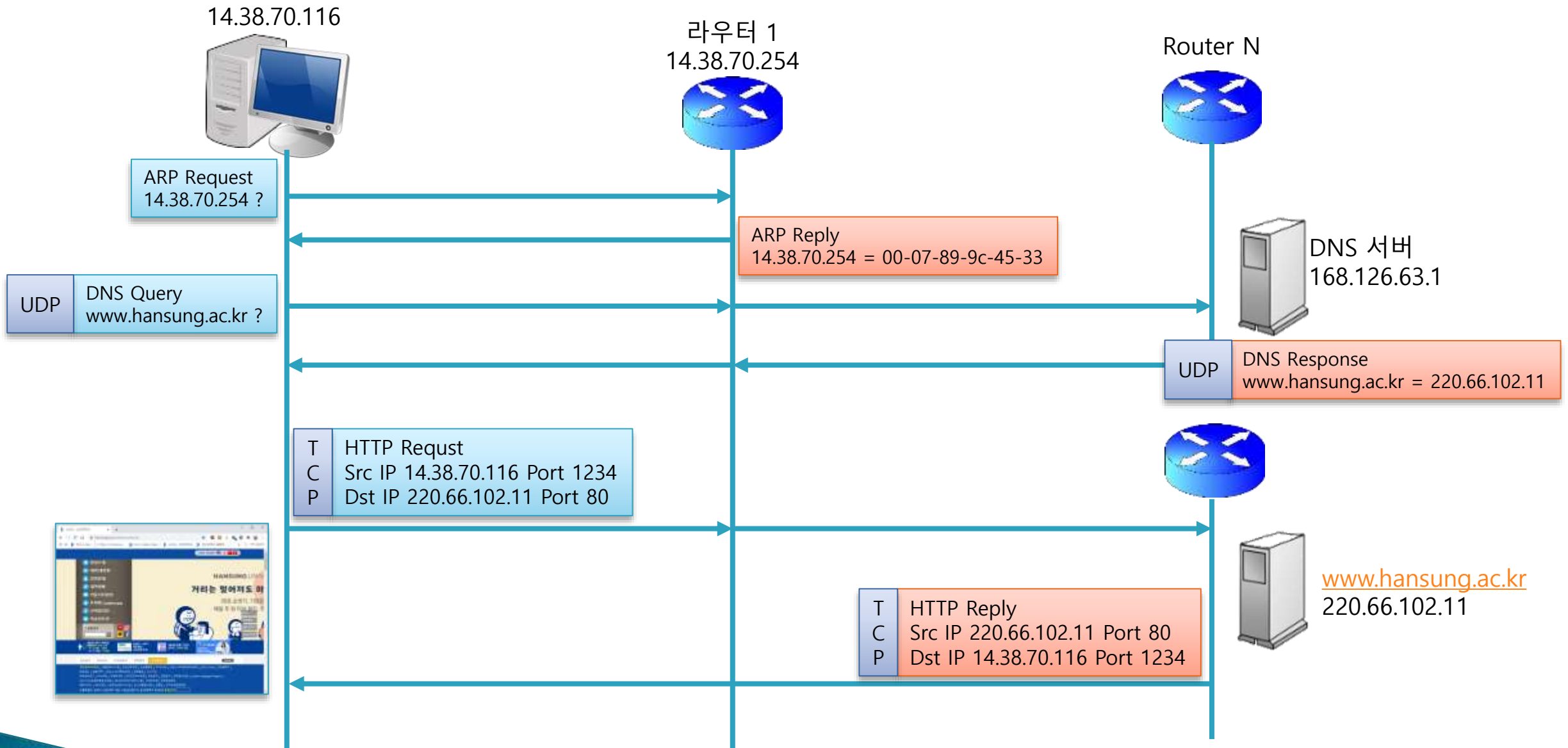


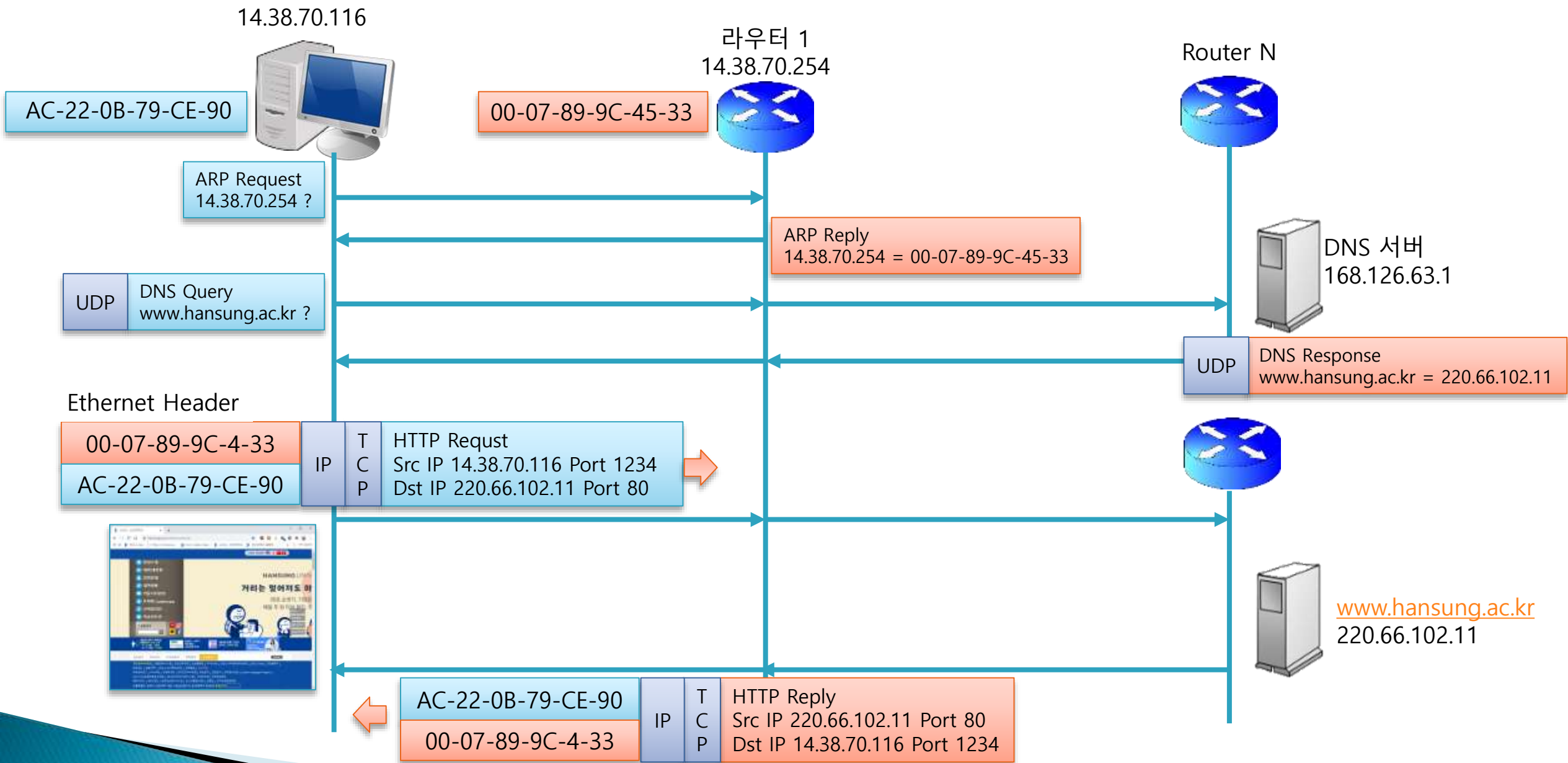


# TCP/IP 환경에서 라우팅의 원리

- ▶ 고정 IP 사용하는 환경에서 패킷 교환 순서





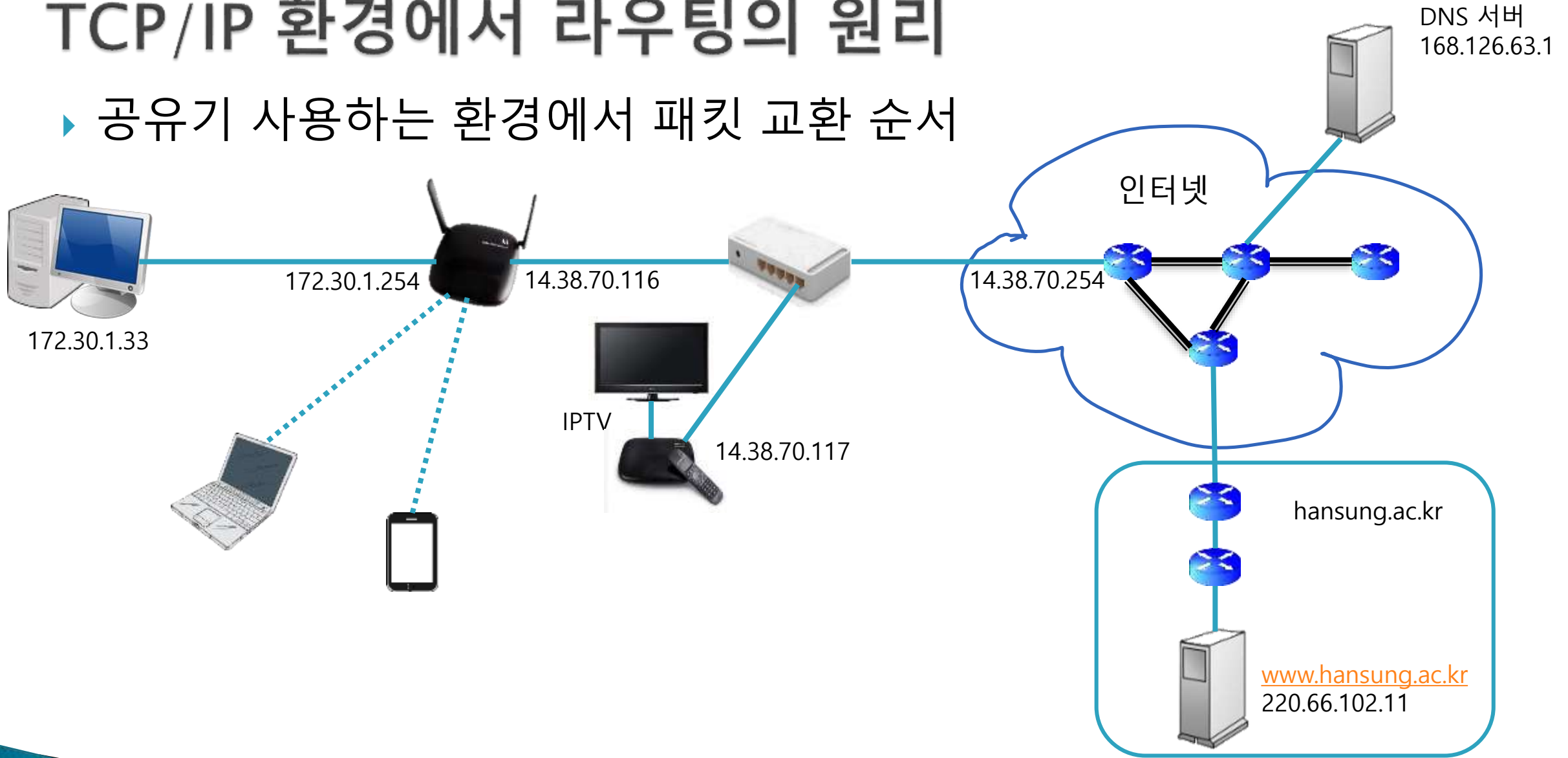


# TCP/IP 프로토콜 동작 순서

- ▶ ARP Protocol
  - IP → MAC Address 조회
  - ARP Request (Broadcasting) / ARP Reply (1:1)
- ▶ DNS Protocol (UDP and port 53)
  - Domain Name → IP Address
  - DNS Query / DNS Reply
- ▶ Analyzer를 이용한 인터넷 동작 순서 확인
  - ARP → DNS → Web Data 순서인 이유
    - Web 서버와 통신하려면 연결이 필요하고
    - www.hansung.ac.kr → IP 로 변환해야 함
    - 이름 → IP 변환을 위해 DNS 서버와 통신 필요
    - DNS 서버와 통신하려면 Router 도움이 필요함
    - Router의 MAC 주소 필요
    - ARP 가 먼저 동작해야 함 (Router의 MAC Address 조회)

# TCP/IP 환경에서 라우팅의 원리

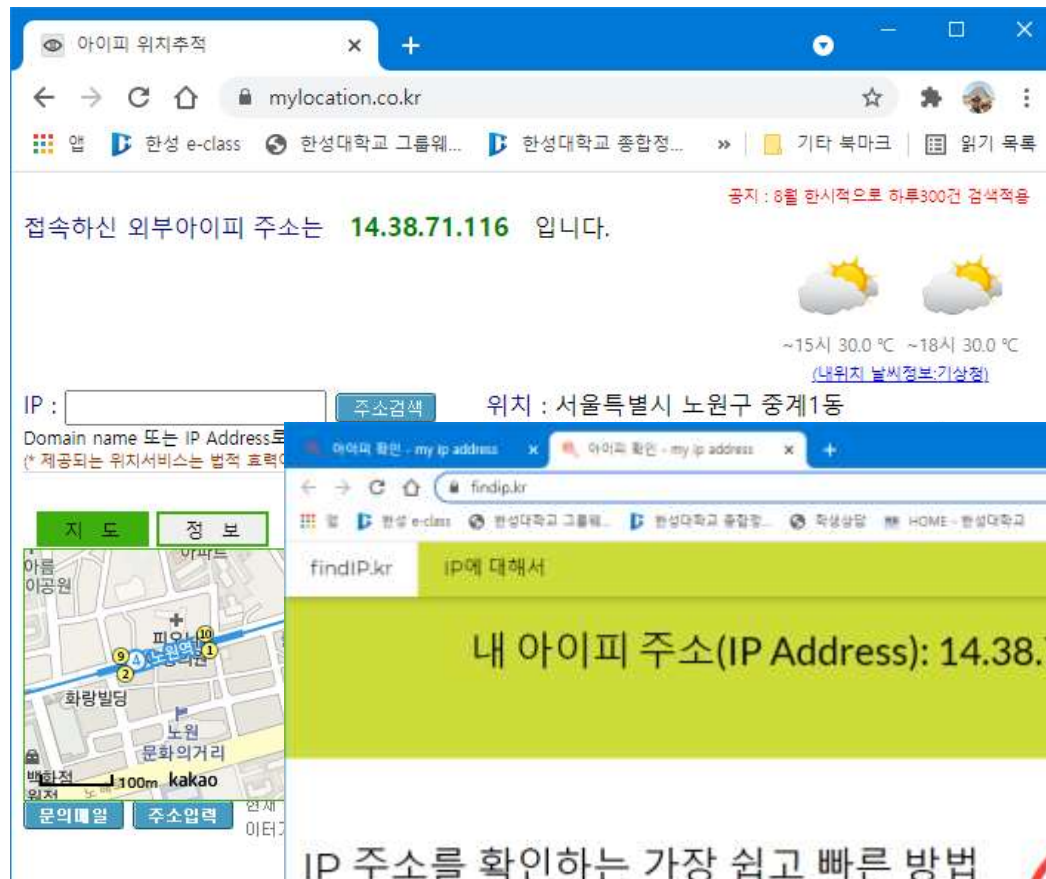
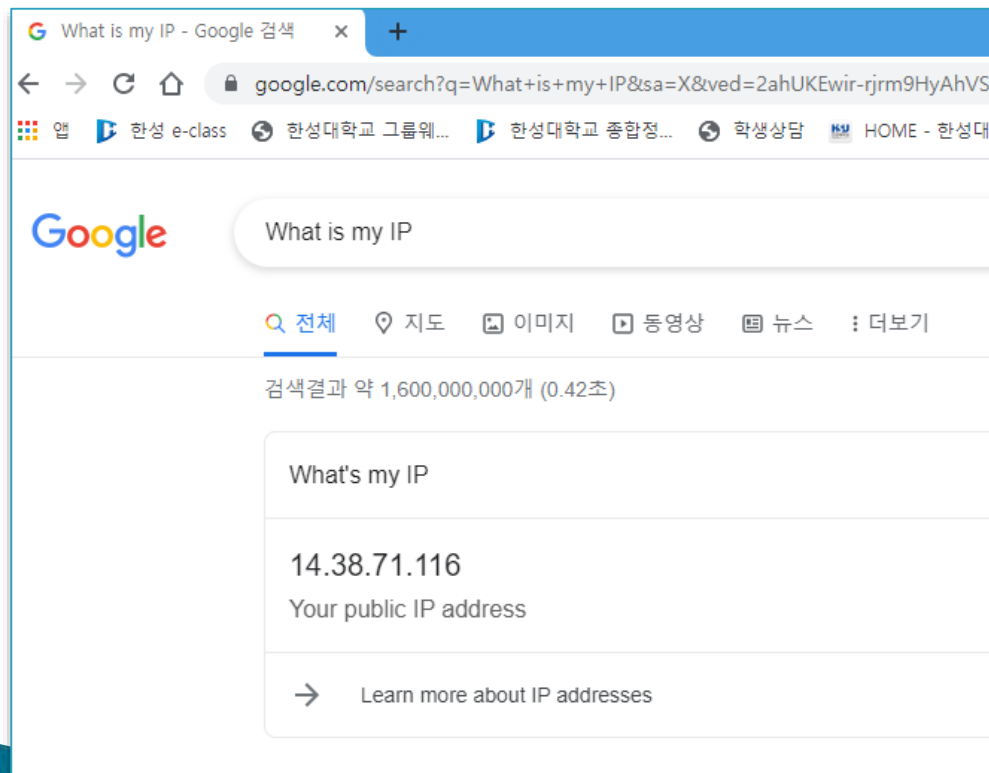
- ▶ 공유기 사용하는 환경에서 패킷 교환 순서





# 내 PC의(공유기) 공인 IP 확인하는 방법

- ▶ google 검색창에 What is my IP
- ▶ mylocation.co.kr
- ▶ findip.kr



# PC 에서 인터넷으로 연결되는 라우터들 IP 확인하기

- ▶ `tracert -d www.hansung.ac.kr` 로 처음 몇 개는 확인 가능

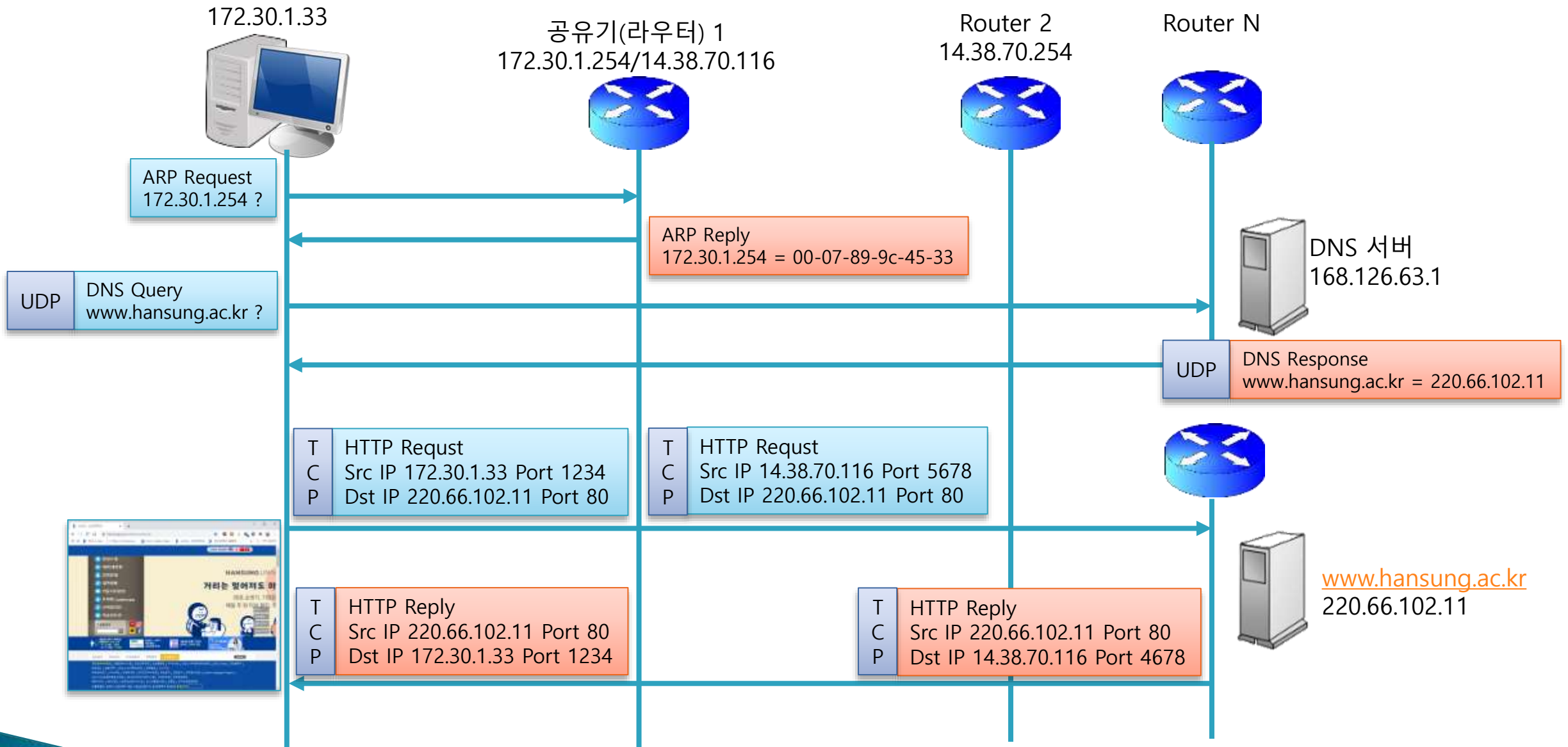
```
C:\> 관리자: 명령 프롬프트

C:\Windows\system32>tracert -d www.hansung.ac.kr

최대 30홉 이상의
www.hansung.ac.kr [220.66.102.11](으)로 가는 경로 추적:

 1  <1 ms    <1 ms    <1 ms    172.30.1.254
 2    4 ms    4 ms    4 ms    14.38.70.254
 3    2 ms    3 ms    2 ms    220.116.62.33
 4    2 ms    2 ms    1 ms    112.188.24.45
 5    3 ms    1 ms    2 ms    112.188.16.21
 6    *      *      *      요청 시간이 만료되었습니다.
 7    2 ms    2 ms    2 ms    112.174.10.118
 8    3 ms    2 ms    7 ms    203.233.35.105
 9    2 ms    3 ms    3 ms    1.208.167.49
10    3 ms    4 ms    3 ms    1.213.107.86
11    3 ms    3 ms    3 ms    1.213.141.78
12    5 ms    3 ms    3 ms    1.213.140.234
13    *      *      *      요청 시간이 만료되었습니다.
14    *      ^C

C:\Windows\system32>
C:\Windows\system32>
```

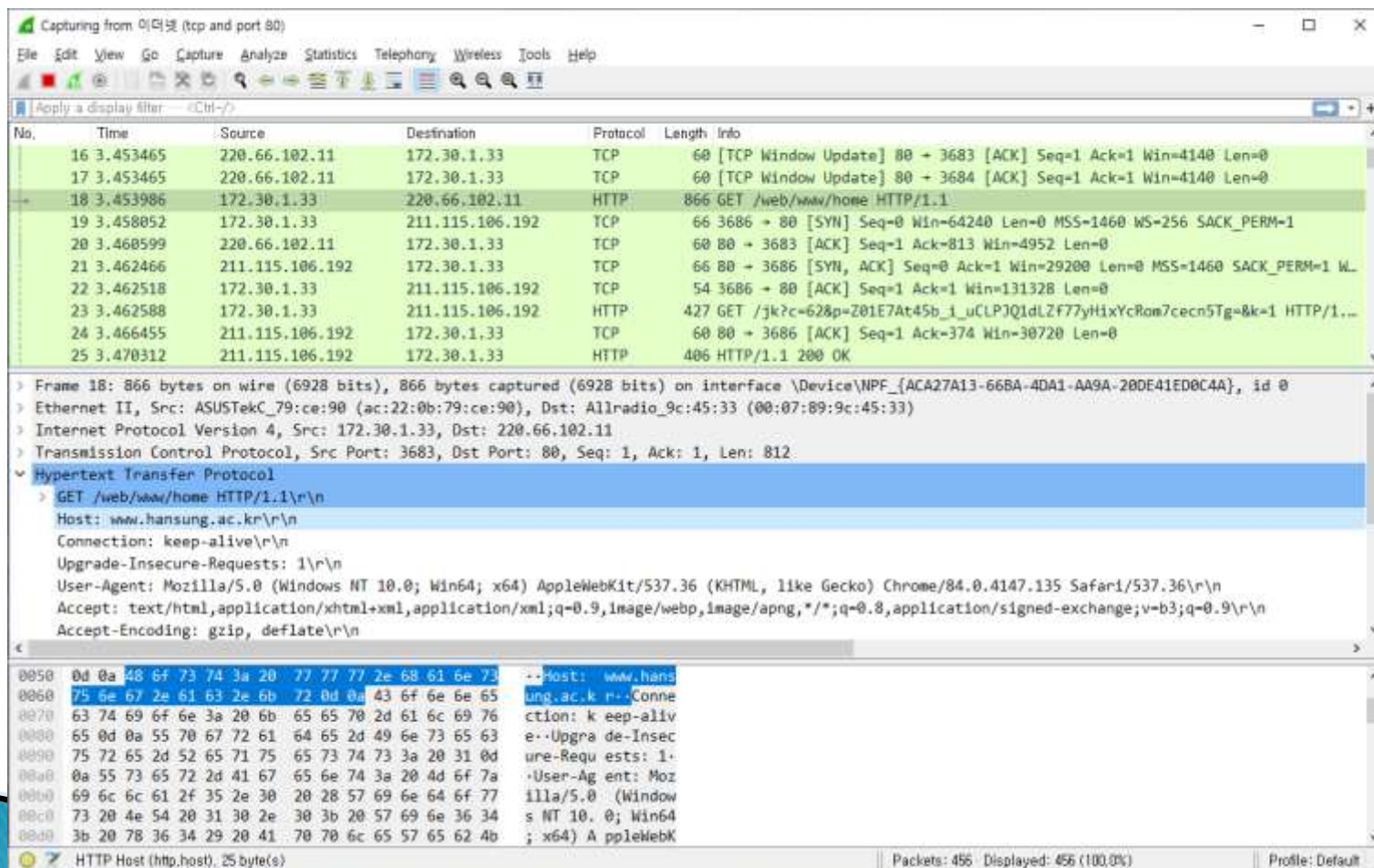


# 실습: 프로토콜 분석기 실습

- ▶ 프로토콜 분석기
  - TCP/IP 패킷을 Low Level 로 볼수 있는 프로그램
  - Data 가 오고가는 모습을 볼 수 있다
  - 네트워크프로그래밍 디버깅에 필수
- ▶ 종류
  - WireShark
- ▶ WireShark 설치
  - <https://www.wireshark.org/#download>
- ▶ 실습
  - HTTP 데이터 분석 (PC  $\leftrightarrow$  Web Server)
  - Mobile 데이터 분석 (H.P  $\leftrightarrow$  PC)

# 프로코콜 분석기 Wireshark

- ▶ <https://www.wireshark.org/#download>
  - 최신버전 설치





Wireshark - Capture Interfaces

Input Output Options

Interface	Traffic	Link-layer Header	Promi	Snapplen	Buffer (T	Monit	Capture Filter
> VMware Network Adapter VMnet8	_____	Ethernet	<input type="checkbox"/>	default	2	—	
로컬 영역 연결* 10	_____	Ethernet	<input type="checkbox"/>	default	2	—	
> 이더넷	_____	Ethernet	<input checked="" type="checkbox"/>	default	2	—	tcp and port 80
> VMware Network Adapter VMnet1	_____	Ethernet	<input type="checkbox"/>	default	2	—	
로컬 영역 연결* 9	_____	Ethernet	<input type="checkbox"/>	default	2	—	
로컬 영역 연결* 8	_____	Ethernet	<input type="checkbox"/>	default	2	—	
Adapter for loopback traffic capture	_____	BSD loopback	<input type="checkbox"/>	default	2	—	

☒ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces:

Manage Interfaces... Compile BPFs

Start Close Help

Frame 1: 60 bytes on wire (480 bits) captured (0.000000000 seconds) on interface 이더넷  
 Ethernet II, Src: 08:00:27:00:00:00, Dst: 08:00:27:00:00:00  
 Configuration Test Protocol  
 Data (40 bytes)

0000 cf 00 00 9c 45 33  
 0010 01 00 03 00 00 00 00 00 00 00 00 00 00 00 00  
 0020 00 00 00 00 00 00 00 00 00 00 00 00 00 00  
 0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00

wireshark\_이더넷\_20200824193606\_a03264.pcapng

Packets: 3155 · Displayed: 3155 (100.0%)

Profile: Default

# Network Data 구조

## ▶ ARP

Ethernet Header Type = 0x0806	ARP Header + Data
14	42 ~ 60

## ▶ IP

Ethernet Header	IP Header Protocol ?	TCP/UDP Header	DATA (HTTP, FTP, DNS, RTP, ...)
14	20	20/8	0 ~ 1472

## ▶ ICMP

Ethernet Header Type = 0x0800	IP Header Protocol 1	ICMP Header + Data
14	20	0 ~ 1480

## ▶ TCP

Ethernet Header Type = 0x0800	IP Header Protocol 6	TCP Header	DATA (HTTP, FTP, Telnet, ..)
14	20	20	0 ~ 1460

## ▶ UDP

Ethernet Header Type = 0x0800	IP Header Protocol 17	UDP Header	DATA (DNS, RTP, ...)
14	20	8	0 ~ 1472

# Ethernet Frame 구조

Ethernet Frame

Pre- amble	S F D	이더넷 헤더			데이터	F C S
		목적지 주소	근원지 주소	타입 길이		
7 (바이트)	1	6	6	2	46~1500	4

Ethernet Header

목적지 주소	근원지 주소	타입	데이터
6(바이트)	6	2	46~1500

802.3 Frame Header

목적지 주소	근원지 주소	데이터 길이	LLC헤더			SNAP ID		타입	데이터
			DS AP	SS AP	ct rl	OUI			
6	6	2	1	1	1	3	2		38~1500(바이트)

- ▶ Preamble
  - 동기화 기능
- ▶ SFD(Start of frame delimiter)
  - 프레임의 시작을 표시
- ▶ 근원지 MAC 주소
  - 데이터를 보내는 기계의 MAC 주소
- ▶ 목적지 MAC 주소
  - 데이터를 수신할 기계의 MAC 주소
- ▶ Type
  - 상위 계층 프로토콜 종류를 표시
  - 0x0806 ARP
  - 0x0800 IP Packet 이 뒤에 온다
  - 0x0800 미만이면 802.3 Frame
- ▶ 데이터 필드
  - 상위 프로토콜 데이터 패킷
- ▶ FCS (Frame Check Sequence)
  - 프레임에 문제가 있는지 판별에 사용

# Ethernet Frame 예

Wireshark packet capture showing an Ethernet II frame (Frame 16) with an IPv4 payload. The frame is from 172.30.1.33 to 220.67.231.144. The packet list shows a sequence of SSDP and TCP packets. The packet details pane shows the Ethernet II header and the IPv4/TCP payload. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination	Protocol	Length	Info
11	1.195432	fe80::95c2:8db1:aa3...	ff02::c	SSDP	511	NOTIFY * HTTP/1.1
12	1.469414	08:07:89:9c:45:33	cf:00:00:9c:45:33	LOOP	60	Reply
13	1.647619	220.67.231.144	172.30.1.33	TCP	105	80 → 5484 [PSH, ACK] Seq=1 Ack=1 Win=47952 Len=51
14	1.675340	172.30.1.33	239.255.255.250	SSDP	490	NOTIFY * HTTP/1.1
15	1.675629	fe80::95c2:8db1:aa3...	ff02::c	SSDP	520	NOTIFY * HTTP/1.1
16	1.689860	172.30.1.33	220.67.231.144	TCP	54	5484 → 80 [ACK] Seq=1 Ack=52 Win=62863 Len=0
17	1.953294	172.30.1.33	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
18	1.954965	172.30.1.254	172.30.1.33	SSDP	434	HTTP/1.1 200 OK

Frame 16: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF\_{ACA27A13-66BA-4DA1-AA9A-20DE41ED0C4A}, id 0

Ethernet II, Src: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90), Dst: Allradio\_9c:45:33 (00:07:89:9c:45:33)

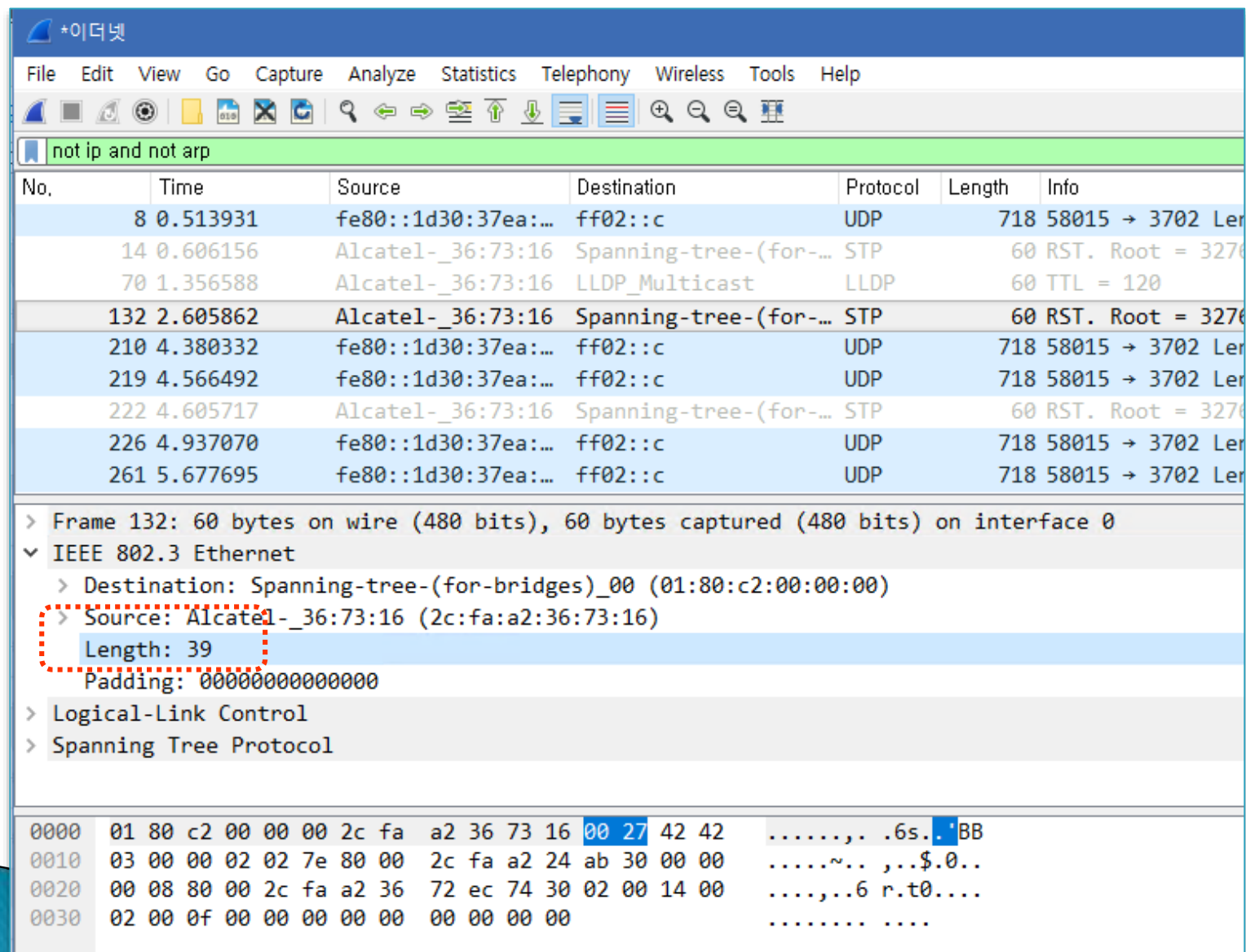
- Destination: Allradio\_9c:45:33 (00:07:89:9c:45:33)
- Source: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90)
- Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 172.30.1.33, Dst: 220.67.231.144

Transmission Control Protocol, Src Port: 5484, Dst Port: 80, Seq: 1, Ack: 52, Len: 0

0000 00 07 89 9c 45 33 ac 22 0b 79 ce 90 08 00 45 00 ....E3..y...E.  
0010 00 28 f0 74 40 00 80 06 99 47 ac 1e 01 21 dc 43 .(t@...G...!C  
0020 e7 90 15 6c 00 50 74 d3 18 b5 d3 78 a3 3f 50 10 ...lPt...x.P  
0030 f5 8f 2f 34 00 00 .../4..

# 802.3 Frame 예



Wireshark packet capture showing an IEEE 802.3 Ethernet frame. The frame details show a source MAC of Alcatel-\_36:73:16 and a length of 39 bytes. The packet bytes are displayed at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
8	0.513931	fe80::1d30:37ea:...	ff02::c	UDP	718	58015 → 3702 Ler
14	0.606156	Alcatel-_36:73:16	Spanning-tree-(for-...	STP	60	RST. Root = 3270
70	1.356588	Alcatel-_36:73:16	LLDP_Multicast	LLDP	60	TTL = 120
132	2.605862	Alcatel-_36:73:16	Spanning-tree-(for-...	STP	60	RST. Root = 3270
210	4.380332	fe80::1d30:37ea:...	ff02::c	UDP	718	58015 → 3702 Ler
219	4.566492	fe80::1d30:37ea:...	ff02::c	UDP	718	58015 → 3702 Ler
222	4.605717	Alcatel-_36:73:16	Spanning-tree-(for-...	STP	60	RST. Root = 3270
226	4.937070	fe80::1d30:37ea:...	ff02::c	UDP	718	58015 → 3702 Ler
261	5.677695	fe80::1d30:37ea:...	ff02::c	UDP	718	58015 → 3702 Ler

> Frame 132: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

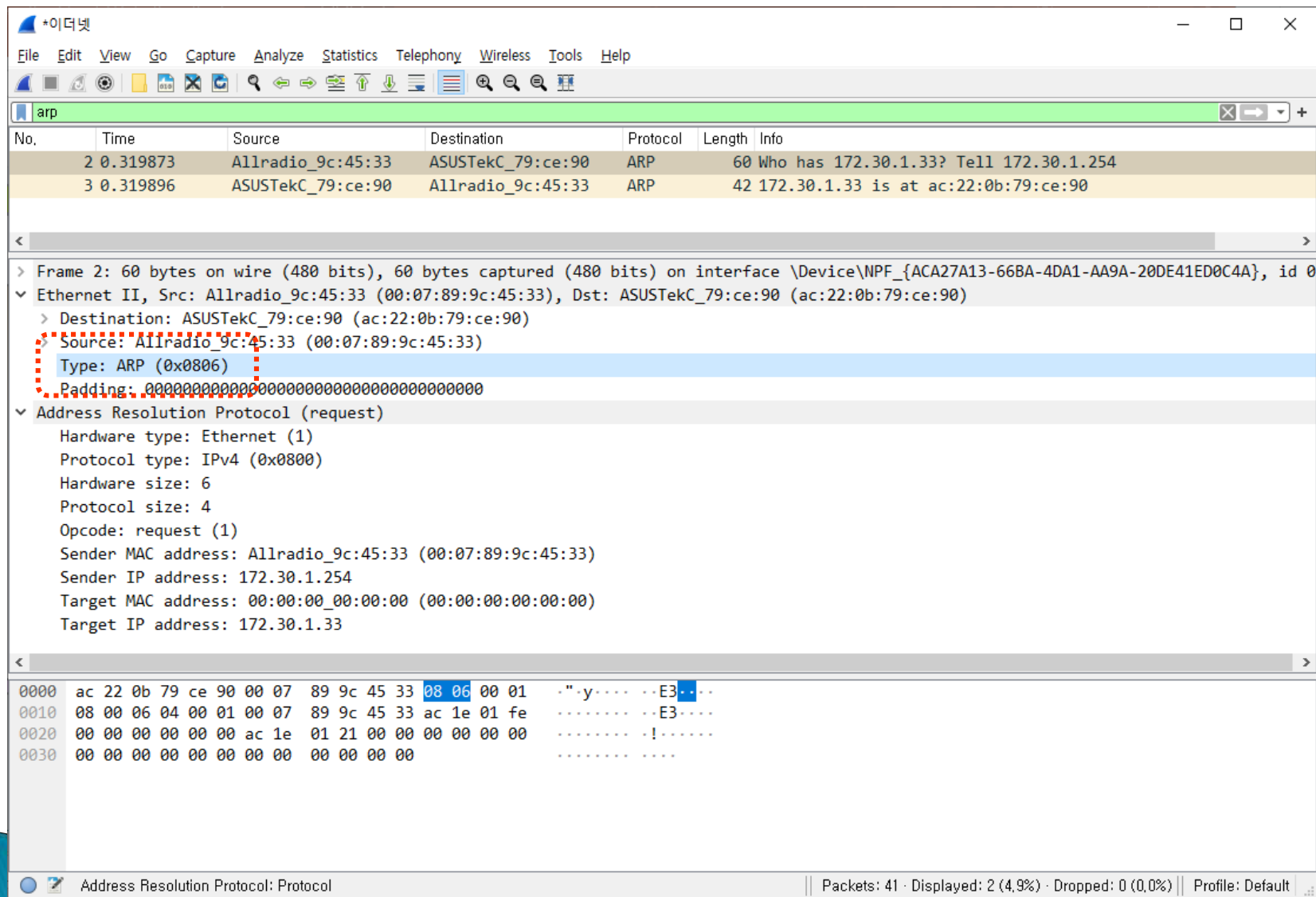
▼ IEEE 802.3 Ethernet

- > Destination: Spanning-tree-(for-bridges)\_00 (01:80:c2:00:00:00)
- > Source: Alcatel-\_36:73:16 (2c:fa:a2:36:73:16)
- Length: 39
- Padding: 0000000000000000
- > Logical-Link Control
- > Spanning Tree Protocol

Offset	Bytes	Hex	ASCII
0000	01 80 c2 00 00 00 2c fa a2 36 73 16 00 27 42 42	01 80 c2 00 00 00 2c fa a2 36 73 16 00 27 42 42	....., .6s. BB
0010	03 00 00 02 02 7e 80 00 2c fa a2 24 ab 30 00 00	03 00 00 02 02 7e 80 00 2c fa a2 24 ab 30 00 00	.....~.. ,..\$.0..
0020	00 08 80 00 2c fa a2 36 72 ec 74 30 02 00 14 00	00 08 80 00 2c fa a2 36 72 ec 74 30 02 00 14 00	....., .6 r.t0....
0030	02 00 0f 00 00 00 00 00 00 00 00 00	02 00 0f 00 00 00 00 00 00 00 00 00	.....

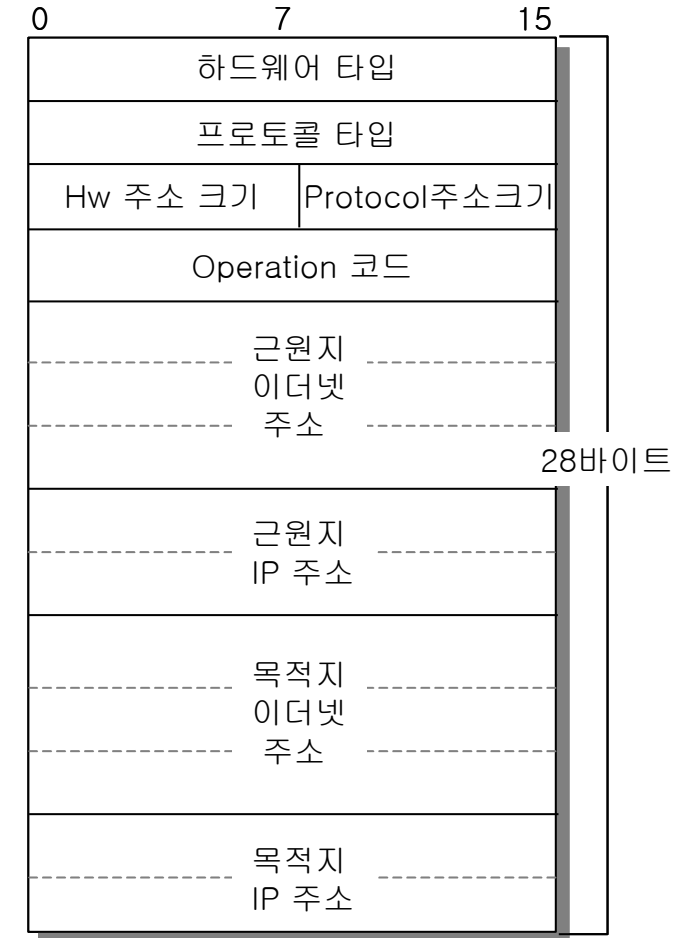
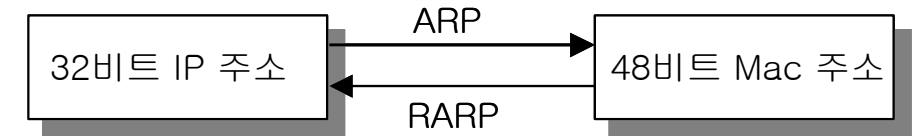
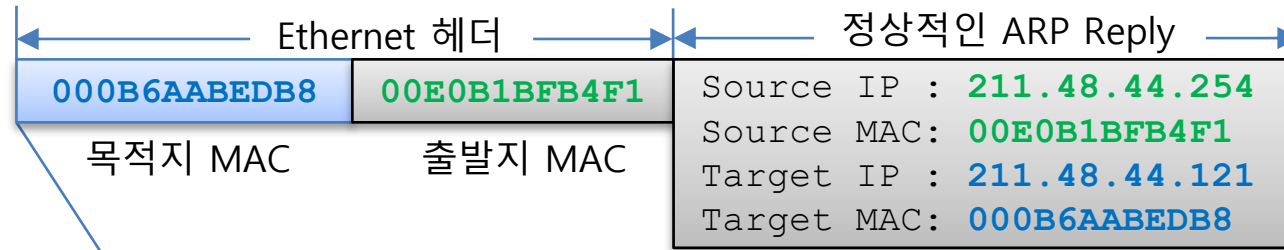


## ARP Frame 예

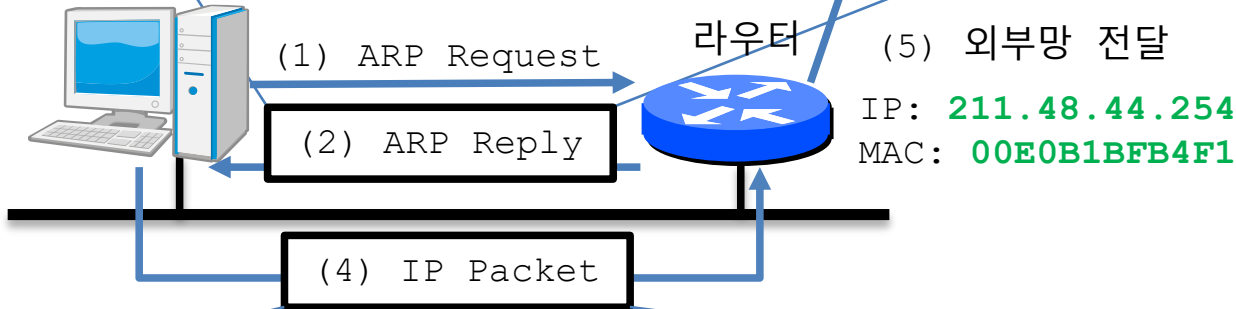


# ARP 프로토콜 분석

Ethernet Header Type = 0x0806	ARP Header + Data
14	42 ~ 60



IP: 211.48.44.121  
MAC: 000B6AABEDB8



(3) 정상적인 ARP Table

Internet Address	Physical Address	Type
211.48.44.254	00-E0-B1-BF-B4-F1	Dynamic

# Network Interface, Routing Table

```
관리자: 명령 프롬프트
C:\Windows\system32>ipconfig

Windows IP 구성

무선 LAN 어댑터 로컬 영역 연결* 2:

    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사 . . . . :

무선 LAN 어댑터 로컬 영역 연결* 12:

    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사 . . . . :

이더넷 어댑터 이더넷:

    연결별 DNS 접미사 . . . . :
    링크-로컬 IPv6 주소 . . . . : fe80::95c2:8db1:aa34:1b54%15
    IPv4 주소 . . . . . : 172.30.1.33
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . : 172.30.1.254

이더넷 어댑터 VMware Network Adapter VMnet1:

    연결별 DNS 접미사 . . . . :
    링크-로컬 IPv6 주소 . . . . : fe80::d1a8:7a11:815d:4d2f%21
    IPv4 주소 . . . . . : 192.168.237.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

이더넷 어댑터 VMware Network Adapter VMnet8:

    연결별 DNS 접미사 . . . . :
    링크-로컬 IPv6 주소 . . . . : fe80::6463:3a4b:5f95:e458%8
    IPv4 주소 . . . . . : 192.168.126.1
    서브넷 마스크 . . . . . : 255.255.255.0
    기본 게이트웨이 . . . . . :

무선 LAN 어댑터 Wi-Fi:

    미디어 상태 . . . . . : 미디어 연결 끊김
    연결별 DNS 접미사 . . . . :

C:\Windows\system32>
```

```
명령 프롬프트
C:\Users\Daddy>netstat -nr

=====
인터페이스 목록
16...92 9f 33 0f a5 40 .....Microsoft Wi-Fi Direct Virtual Adapter #2
17...90 9f 33 0f a5 40 .....Microsoft Wi-Fi Direct Virtual Adapter #3
15...ac 22 0b 79 ce 90 .....Realtek PCIe GbE Family Controller
21...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
8...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
13...90 9f 33 0f a5 40 .....Realtek 8812AU Wireless LAN 802.11ac USB NIC
1.....Software Loopback Interface 1
=====

IPv4 경로 테이블

=====
활성 경로:
네트워크 대상    네트워크 마스크    게이트웨이    인터페이스    메트릭
0.0.0.0          0.0.0.0            172.30.1.254  172.30.1.33    35
127.0.0.0        255.0.0.0
127.0.0.1        255.255.255.255
127.255.255.255  255.255.255.255
172.30.1.0       255.255.255.0
172.30.1.33      255.255.255.255
172.30.1.255     255.255.255.255
192.168.126.0    255.255.255.0
192.168.126.1    255.255.255.255
192.168.126.255  255.255.255.255
192.168.237.0    255.255.255.0
192.168.237.1    255.255.255.255
192.168.237.255  255.255.255.255
224.0.0.0        240.0.0.0
224.0.0.0        240.0.0.0
224.0.0.0        240.0.0.0
224.0.0.0        240.0.0.0
255.255.255.255  255.255.255.255
255.255.255.255  255.255.255.255
255.255.255.255  255.255.255.255
255.255.255.255  255.255.255.255

=====
영구 경로:
없음
```

# ARP Protocol : arp 명령어 (arp table 확인, 삭제)

arp table 보기

```
C:\Users\Daddy>arp -a
```

인터페이스: 192.168.126.1 --- 0x8	인터넷 주소	물리적 주소	형식
192.168.126.254	00-50-56-f3-83-3f	정적	유형
192.168.126.255	ff-ff-ff-ff-ff-ff	정적	정적
224.0.0.2	01-00-5e-00-00-02	정적	정적
224.0.0.22	01-00-5e-00-00-16	정적	정적
224.0.0.251	01-00-5e-00-00-fb	정적	정적
224.0.0.252	01-00-5e-00-00-fc	정적	정적
239.192.152.143	01-00-5e-40-98-8f	정적	정적
239.255.255.250	01-00-5e-7f-ff-fa	정적	정적

인터페이스: 172.30.1.33 --- 0xf	인터넷 주소	물리적 주소	형식
172.30.1.254	00-07-89-9c-45-33	정적	유형
172.30.1.255	ff-ff-ff-ff-ff-ff	정적	정적
224.0.0.2	01-00-5e-00-00-02	정적	정적
224.0.0.22	01-00-5e-00-00-16	정적	정적
224.0.0.251	01-00-5e-00-00-fb	정적	정적
224.0.0.252	01-00-5e-00-00-fc	정적	정적
239.192.152.143	01-00-5e-40-98-8f	정적	정적
239.255.255.250	01-00-5e-7f-ff-fa	정적	정적

인터페이스: 192.168.237.1 --- 0x15	인터넷 주소	물리적 주소	형식
192.168.237.254	00-50-56-f6-71-9d	정적	유형
192.168.237.255	ff-ff-ff-ff-ff-ff	정적	정적
224.0.0.2	01-00-5e-00-00-02	정적	정적
224.0.0.22	01-00-5e-00-00-16	정적	정적
224.0.0.251	01-00-5e-00-00-fb	정적	정적
224.0.0.252	01-00-5e-00-00-fc	정적	정적
239.192.152.143	01-00-5e-40-98-8f	정적	정적
239.255.255.250	01-00-5e-7f-ff-fa	정적	정적

```
C:\Users\Daddy>
```

arp table 삭제 후 다시 보기, cmd 창 관리자 권한으로 실행

```
C:\Windows\system32>type con > aaa.bat
arp -d
arp -a
^Z
```

batch 명령어로 해야 시간 차이 없이 삭제된 것을 확인 할 수 있다

```
C:\Windows\system32>aaa
```

```
C:\Windows\system32>arp -d
```

```
C:\Windows\system32>arp -a
```

인터페이스: 192.168.126.1 --- 0x8	인터넷 주소	물리적 주소	형식
224.0.0.22	01-00-5e-00-00-16	정적	유형
239.192.152.143	01-00-5e-40-98-8f	정적	정적

인터페이스: 172.30.1.33 --- 0xf	인터넷 주소	물리적 주소	형식
224.0.0.2	01-00-5e-00-00-02	정적	유형
224.0.0.22	01-00-5e-00-00-16	정적	정적
239.192.152.143	01-00-5e-40-98-8f	정적	정적

172.30.1.254 MAC 주소 삭제됨

인터페이스: 192.168.237.1 --- 0x15	인터넷 주소	물리적 주소	형식
224.0.0.22	01-00-5e-00-00-16	정적	유형
239.192.152.143	01-00-5e-40-98-8f	정적	정적

```
C:\Windows\system32>
```

# ARP Table 자동 생성 - network 사용하면 생성

```
관리자: 명령 프롬프트
C:\Windows\system32>arp -a

인터페이스: 192.168.126.1 --- 0x8
  인터넷 주소      물리적 주소      유형
192.168.126.254    00-50-56-f3-83-3f  동적
192.168.126.255    ff-ff-ff-ff-ff-ff  정적
224.0.0.2          01-00-5e-00-00-02  정적
224.0.0.22         01-00-5e-00-00-16  정적
224.0.0.251        01-00-5e-00-00-fb  정적
224.0.0.252        01-00-5e-00-00-fc  정적
239.192.152.143    01-00-5e-40-98-8f  정적
239.255.255.250    01-00-5e-7f-ff-fa  정적

인터페이스: 172.30.1.33 --- 0xf
  인터넷 주소      물리적 주소      유형
172.30.1.254      00-07-89-9c-45-33  동적
172.30.1.255      ff-ff-ff-ff-ff-ff  정적
224.0.0.2          01-00-5e-00-00-02  정적
224.0.0.22         01-00-5e-00-00-16  정적
224.0.0.251        01-00-5e-00-00-fb  정적
224.0.0.252        01-00-5e-00-00-fc  정적
239.192.152.143    01-00-5e-40-98-8f  정적
239.255.255.250    01-00-5e-7f-ff-fa  정적

인터페이스: 192.168.237.1 --- 0x15
  인터넷 주소      물리적 주소      유형
192.168.237.254    00-50-56-f6-71-9d  동적
192.168.237.255    ff-ff-ff-ff-ff-ff  정적
224.0.0.2          01-00-5e-00-00-02  정적
224.0.0.22         01-00-5e-00-00-16  정적
224.0.0.251        01-00-5e-00-00-fb  정적
224.0.0.252        01-00-5e-00-00-fc  정적
239.192.152.143    01-00-5e-40-98-8f  정적
239.255.255.250    01-00-5e-7f-ff-fa  정적

C:\Windows\system32>
```



# ARP Request

The image shows a Wireshark packet capture window titled "이더넷". The filter bar shows "arp". The packet list displays two packets:

No.	Time	Source	Destination	Protocol	Length	Info
144	0.865206	ASUSTekC_79:ce:90	Broadcast	ARP	42	Who has 172.30.1.254? Tell 172.30.1.33
145	0.865670	Allradio_9c:45:33	ASUSTekC_79:ce:90	ARP	60	172.30.1.254 is at 00:07:89:9c:45:33

The packet details pane shows the selected packet (144) expanded, revealing the following information:

- Frame 144: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF\_{ACA27A13-66BA-4DA1-AA9A-20DE41ED0C4A}, id
- Ethernet II, Src: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  - Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  - Source: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90)
  - Type: ARP (0x0806)
- Address Resolution Protocol (request)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: request (1)
  - Sender MAC address: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90)
  - Sender IP address: 172.30.1.33
  - Target MAC address: 00:00:00\_00:00:00 (00:00:00:00:00:00)
  - Target IP address: 172.30.1.254

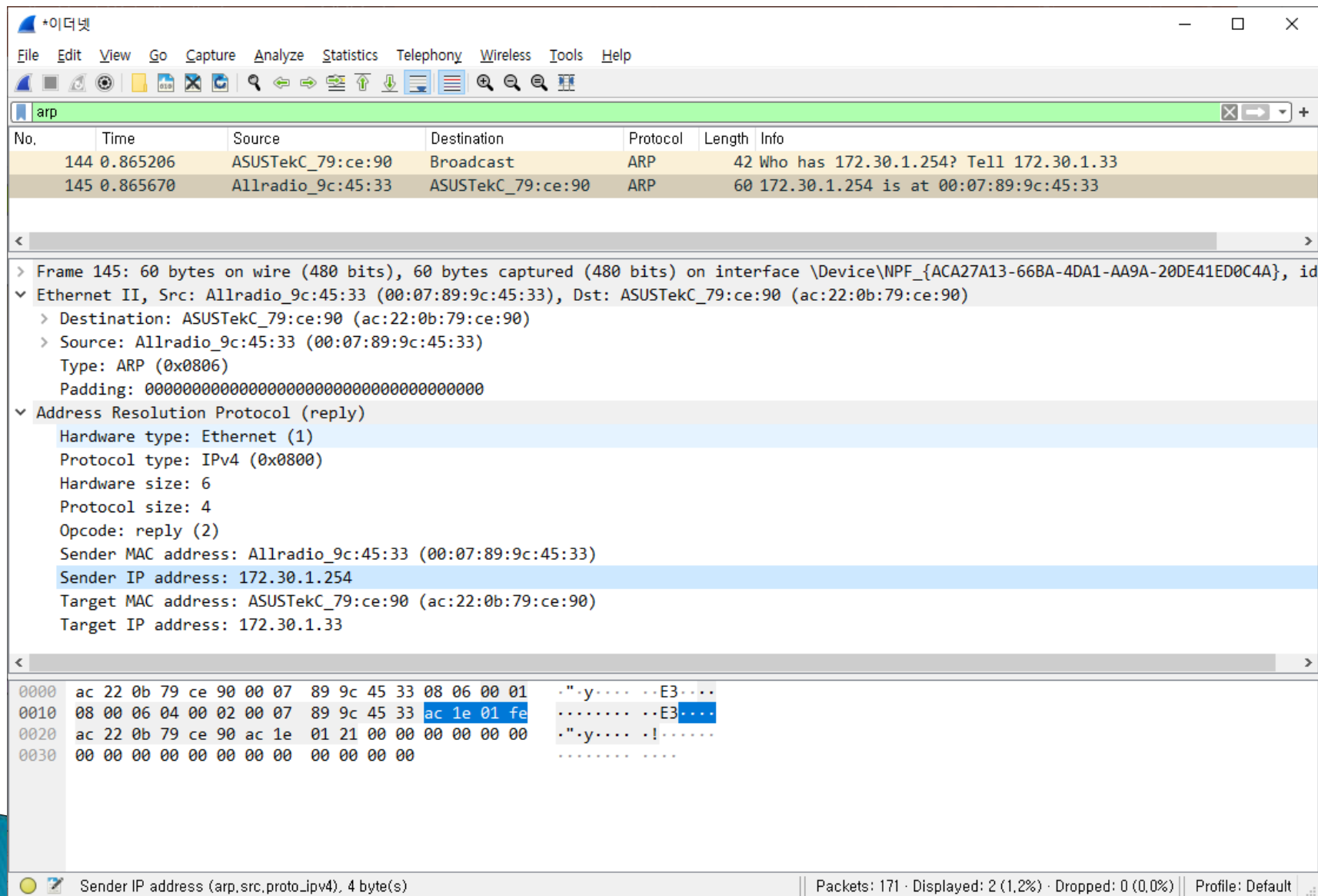
The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 ff ff ff ff ff ff ac 22 0b 79 ce 90 08 06 00 01 ..... " .y....
0010 08 00 06 04 00 01 ac 22 0b 79 ce 90 ac 1e 01 21 ..... " .y.....!
0020 00 00 00 00 00 00 ac 1e 01 fe ..... ..
```

The status bar at the bottom indicates: Address Resolution Protocol (arp), 28 byte(s) | Packets: 171 · Displayed: 2 (1,2%) · Dropped: 0 (0,0%) | Profile: Default



# ARP Reply



Wireshark packet capture showing an ARP Reply.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
144	0.865206	ASUSTekC_79:ce:90	Broadcast	ARP	42	Who has 172.30.1.254? Tell 172.30.1.33
145	0.865670	Allradio_9c:45:33	ASUSTekC_79:ce:90	ARP	60	172.30.1.254 is at 00:07:89:9c:45:33

Packet Details (Frame 145):

- Ethernet II, Src: Allradio\_9c:45:33 (00:07:89:9c:45:33), Dst: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90)
  - Destination: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90)
  - Source: Allradio\_9c:45:33 (00:07:89:9c:45:33)
  - Type: ARP (0x0806)
  - Padding: 00000000000000000000000000000000
- Address Resolution Protocol (reply)
  - Hardware type: Ethernet (1)
  - Protocol type: IPv4 (0x0800)
  - Hardware size: 6
  - Protocol size: 4
  - Opcode: reply (2)
  - Sender MAC address: Allradio\_9c:45:33 (00:07:89:9c:45:33)
  - Sender IP address: 172.30.1.254
  - Target MAC address: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90)
  - Target IP address: 172.30.1.33

Packet Bytes:

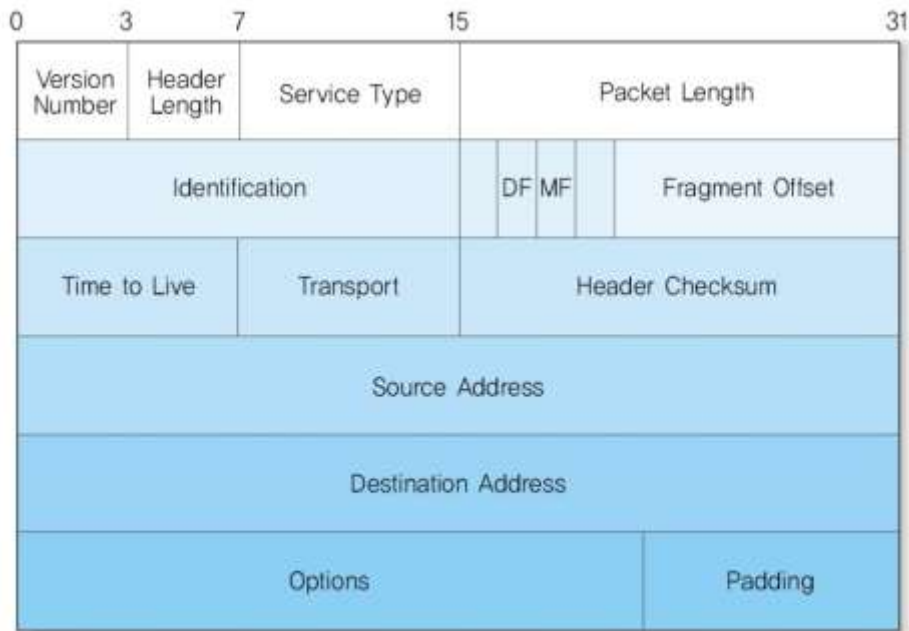
Offset	Hex	ASCII
0000	ac 22 0b 79 ce 90 00 07 89 9c 45 33 08 06 00 01	..".y.... ..E3...
0010	08 00 06 04 00 02 07 89 9c 45 33 ac 1e 01 fe	..... ..E3....
0020	ac 22 0b 79 ce 90 ac 1e 01 21 00 00 00 00 00 00	..".y.... ..!.....
0030	00 00 00 00 00 00 00 00 00 00 00 00	.....

Sender IP address (arp.src.proto\_ipv4), 4 byte(s)

Packets: 171 · Displayed: 2 (1,2%) · Dropped: 0 (0,0%) | Profile: Default

# IP 프로토콜 분석

Ethernet Header Type = 0x0800	IP Header Protocol ?	TCP/UDP Header	DATA (HTTP, FTP, DNS, RTP, ...)
14	20	20/8	0 ~ 1472



[그림 7-9] IP 헤더



# IP Header 내용

- ▶ 버전
  - 데이터그램을 생성한 IP의 버전(현재 4 혹은 6을 사용)
- ▶ 헤더길이
  - IP 헤더의 길이
- ▶ 서비스 유형
  - 데이터그램의 우선순위를 나타냄
- ▶ 전체길이
  - IP 헤더를 포함한 전체길이
- ▶ 식별자
  - IP가 단편화 될 때 단편들을 구분하기 위한 번호
- ▶ 플래그
  - 단편화 여부, 단편의 조각이 첫번째 조각인지, 중간 혹은 마지막 조각인지를 구분함
- ▶ 단편오프셋
  - 조각난 단편들의 원래 IP 데이터그램에서의 위치정보를 나타내는 포인터
- ▶ 수명
  - 데이터그램이 폐기되기 전 인터넷에서 얼마나 존속할 수 있는지를 지시하는 값
- ▶ 프로토콜
  - 데이터그램이 싣고 가는 데이터의 종류
  - 예) ICMP:1, TCP:6, UDP:17
- ▶ 체크섬
  - 전송 도중 IP 헤더의 손상여부를 확인
- ▶ 근원지주소
  - 보내는 편의 IP 주소
- ▶ 목적지주소
  - IP 데이터그램의 최종 목적지 주소
- ▶ 옵션
  - 경로설정, 타이밍, 관리, 정렬 등의 부수적인 기능처리

# IP Packet 예 (172.30.1.33 <-> 220.66.102.11)

The image shows a Wireshark packet capture window titled '\*이더넷 (host 220.66.102.11)'. The packet list shows three packets:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.30.1.33	220.66.102.11	TCP	66	7796 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
2	0.000161	172.30.1.33	220.66.102.11	TCP	66	7797 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
3	0.004704	220.66.102.11	172.30.1.33	TCP	60	80 → 7796 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=14

The packet details pane shows the structure of the selected packet (Frame 1):

- Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF\_{ACA27A13-66BA-4DA1-AA9A-20DE41ED0C4A}, id 0
- Ethernet II, Src: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90), Dst: Allradio\_9c:45:33 (00:07:89:9c:45:33)
  - Destination: Allradio\_9c:45:33 (00:07:89:9c:45:33)
  - Source: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90)
  - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.30.1.33, Dst: 220.66.102.11
  - 0100 .... = Version: 4
  - .... 0101 = Header Length: 20 bytes (5)
  - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  - Total Length: 52
  - Identification: 0x1ece (7886)
  - > Flags: 0x4000, Don't fragment
  - Fragment offset: 0
  - Time to live: 128
  - Protocol: TCP (6)
  - Header checksum: 0xec68 [validation disabled]
  - [Header checksum status: Unverified]
  - Source: 172.30.1.33
  - Destination: 220.66.102.11
- > Transmission Control Protocol, Src Port: 7796, Dst Port: 80, Seq: 0, Len: 0

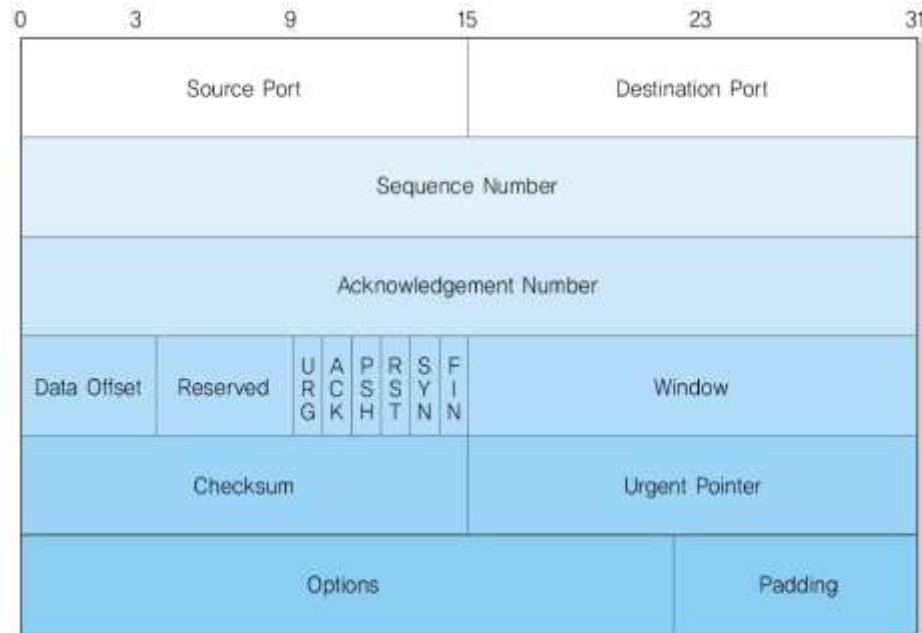
The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 00 07 89 9c 45 33 ac 22 0b 79 ce 90 08 00 45 00  ....E3." .y....E.
0010 00 34 1e ce 40 00 80 06 ec 68 ac 1e 01 21 dc 42  -4..@... .h...!.B
0020 66 0b 1e 74 00 50 d0 0f 54 f2 00 00 00 00 80 02  f..t.P.. T.....
0030 fa f0 40 cc 00 00 02 04 05 b4 01 03 03 08 01 01  ..@.....
0040 04 02  ..
```

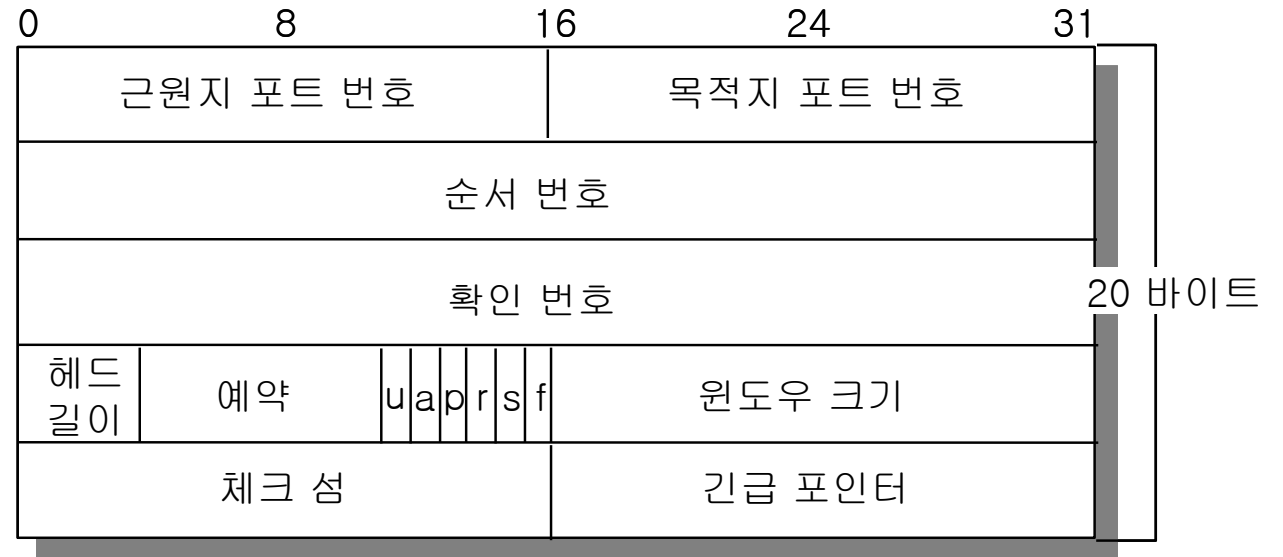
The status bar at the bottom indicates: Internet Protocol Version 4 (ip), 20 byte(s) | Packets: 14213 · Displayed: 14213 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

# TCP 프로토콜 분석

Ethernet Header Type = 0x0800	IP Header Protocol 6	TCP Header	DATA (HTTP, FTP, Telnet, ..)
14	20	20	0 ~ 1460



[그림 9-8] TCP 헤더



# TCP Header 내용

- ▶ 근원지 포트 번호
  - 근원지 컴퓨터에서 사용하는 것으로 인터넷 응용 프로그램이 사용하는 포트번호
- ▶ 목적지 포트 번호
  - 목적지 컴퓨터에서 사용하는 것으로 인터넷 응용 프로그램이 사용하는 포트번호
  - 포트 번호에 따라 상위 응용 프로토콜을 구별
    - 예) HTTP : 80, SMTP : 25, Telnet : 23, FTP 데이터 접속 : 20, SSH : 22
- ▶ 순서 번호
  - TCP 데이터 전송 순서번호를 나타냄
- ▶ 확인 번호
  - 제어 6 비트 중 ACK 비트가 설정되어 있을 때, 다음에 받아야 하는 순서번호를 나타냄



# TCP Header 내용

- ▶ 헤더 길이
  - 4바이트 기준으로 표기, 5(hex)일 경우 20바이트임
- ▶ 예약
  - 아직 사용되지 않는 필드
- ▶ 제어 6 비트

URG	세팅되면 긴급포인터의 내용 실행
ACK	세팅되면 확인번호 필드가 유효함
PSH	세팅되면 송신자에게 높은 처리율을 요구함
RST	세팅되면 TCP 연결을 다시 연결함
SYN	세팅되면 연결요청, 연결설정, 확인응답에서 순서번호 동기화에 사용
FIN	세팅되면 TCP 연결 종료

- ▶ 윈도우 크기
  - 슬라이딩 윈도우 크기를 정함
- ▶ 체크섬
  - TCP 헤더 내부의 오류 검사
- ▶ 긴급 포인터
  - 긴급 포인터의 끝과 일반데이터의 시작을 나타냄

# TCP Packet 예 (172.30.1.3:7796 <-> 220.66.102.11:80)

The image shows a Wireshark packet capture window. The top pane displays a list of captured packets. Packet 5 is selected, showing a GET request from 172.30.1.3 to 220.66.102.11. Packet 6 is a SYN-ACK response from 220.66.102.11 to 172.30.1.3. The bottom pane shows the detailed view of packet 6, which is a TCP SYN-ACK packet. The details include source and destination ports, sequence and acknowledgment numbers, flags (PSH, ACK), window size, and checksum. The packet length is 1098 bytes. The bottom status bar indicates the packet is a Transmission Control Protocol (tcp) packet, 20 bytes in size.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.004704	220.66.102.11	172.30.1.33	TCP	60	80 → 7796 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=14
4	0.004779	172.30.1.33	220.66.102.11	TCP	54	7796 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
5	0.005039	172.30.1.33	220.66.102.11	HTTP	1152	GET / HTTP/1.1
6	0.006166	220.66.102.11	172.30.1.33	TCP	60	80 → 7796 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=14

Frame 5: 1152 bytes on wire (9216 bits), 1152 bytes captured (9216 bits) on interface \Device\NPF\_{ACA27A13-66BA-4DA1-AA9A-20DE41ED0C4A}

Ethernet II, Src: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90), Dst: Allradio\_9c:45:33 (00:07:89:9c:45:33)

Internet Protocol Version 4, Src: 172.30.1.33, Dst: 220.66.102.11

Transmission Control Protocol, Src Port: 7796, Dst Port: 80, Seq: 1, Ack: 1, Len: 1098

- Source Port: 7796
- Destination Port: 80
- [Stream index: 0]
- [TCP Segment Len: 1098]
- Sequence number: 1 (relative sequence number)
- Sequence number (raw): 3490665715
- [Next sequence number: 1099 (relative sequence number)]
- Acknowledgment number: 1 (relative ack number)
- Acknowledgment number (raw): 1938310715
- 0101 .... = Header Length: 20 bytes (5)
- Flags: 0x018 (PSH, ACK)
- Window size value: 64240
- [Calculated window size: 64240]
- [Window size scaling factor: -2 (no window scaling used)]
- Checksum: 0x5c7b [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- [SEQ/ACK analysis]
- [Timestamps]
- TCP payload (1098 bytes)

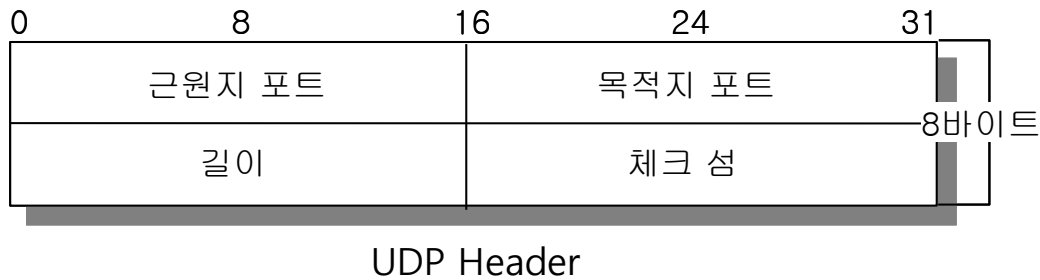
Hypertext Transfer Protocol

0020 66 0b 1e 74 00 50 d0 0f 54 f3 73 88 46 3b 50 18 f..t.P..T.s.F;P.  
0030 fa f0 5c 7b 00 00 47 45 54 20 2f 20 48 54 54 50 ..\{..GE T / HTTP

Transmission Control Protocol (tcp), 20 byte(s) | Packets: 14213 - Displayed: 14213 (100.0%) - Dropped: 0 (0.0%) | Profile: Default

# UDP/DNS 프로토콜 분석

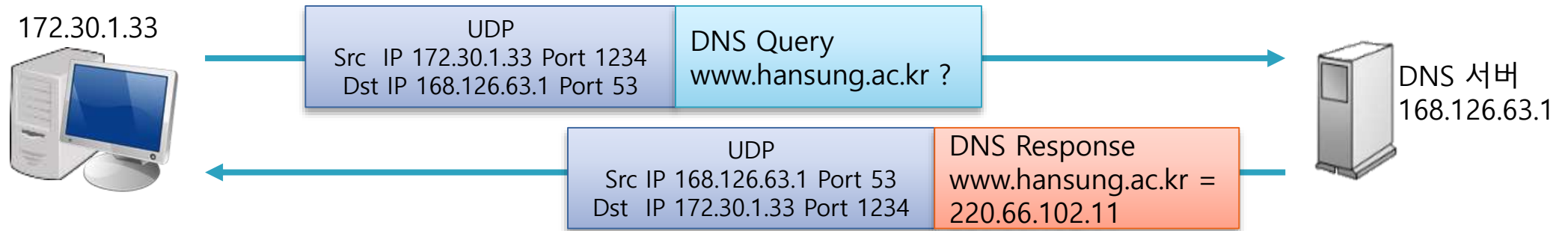
Ethernet Header Type = 0x0800	IP Header Protocol 17	UDP Header	DATA (DNS, RTP, ...)
14	20	8	0 ~ 1472



C:\> 관리자: 명령 프롬프트

```
C:\Windows\system32>nslookup www.hansung.ac.kr
서버: kns.kornet.net
Address: 168.126.63.1
```

```
권한 없는 응답:
이름: www.hansung.ac.kr
Address: 220.66.102.11
```



# DNS Query (www.hansung.ac.kr ? )

The image shows a Wireshark packet capture window titled '\*이더넷'. The packet list pane shows three packets, with packet 11 selected. The packet details pane shows the structure of the selected packet, which is a DNS query for www.hansung.ac.kr. The packet bytes pane shows the raw data of the packet, with the query data highlighted in blue.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
9	1.233931	172.30.1.33	168.126.63.1	DNS	85	Standard query 0x0001 PTR 1.63.126.168.in-addr.arpa
10	1.237970	168.126.63.1	172.30.1.33	DNS	183	Standard query response 0x0001 PTR 1.63.126.168.in-addr.arpa
11	1.240339	172.30.1.33	168.126.63.1	DNS	77	Standard query 0x0002 A www.hansung.ac.kr

Packet Details:

- Frame 11: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface \Device\NPF\_{ACA27A13-66BA-4DA1-AA9A-20DE41ED0C4A}, id 0
- Ethernet II, Src: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90), Dst: Allradio\_9c:45:33 (00:07:89:9c:45:33)
- Internet Protocol Version 4, Src: 172.30.1.33, Dst: 168.126.63.1
- User Datagram Protocol, Src Port: 57016, Dst Port: 53
  - Source Port: 57016
  - Destination Port: 53
  - Length: 43
  - Checksum: 0xf270 [unverified]
  - [Checksum Status: Unverified]
  - [Stream index: 2]
  - [Timestamps]
- Domain Name System (query)
  - Transaction ID: 0x0002
  - Flags: 0x0100 Standard query
  - Questions: 1
  - Answer RRs: 0
  - Authority RRs: 0
  - Additional RRs: 0
  - Queries
    - www.hansung.ac.kr: type A, class IN

Packet Bytes:

```
0000 00 07 89 9c 45 33 ac 22 0b 79 ce 90 08 00 45 00  ....E3..y....E.
0010 00 3f 56 15 00 00 80 11 4f da ac 1e 01 21 a8 7e  ?V.....0....!~
0020 3f 01 de b8 00 35 00 2b f2 70 00 02 01 00 00 01  ?...5.+..p.....
0030 00 00 00 00 00 00 03 77 77 77 07 68 61 6e 73 75  ....w ww.hansu
0040 6e 67 02 61 63 02 6b 72 00 00 01 00 01         ng-ac-kr .....
```

# DNS Response (www.hansung.ac.kr = 220.66.102.11)

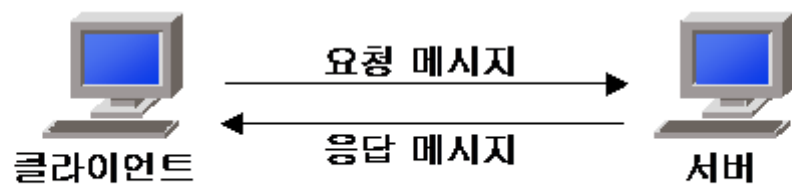
The image shows a Wireshark packet capture window with the following details:

- Filter:** dns
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
10	1.237970	168.126.63.1	172.30.1.33	DNS	183	Standard query response 0x0001 PTR 1.63.126.168.in-add
11	1.240339	172.30.1.33	168.126.63.1	DNS	77	Standard query 0x0002 A www.hansung.ac.kr
12	1.242635	168.126.63.1	172.30.1.33	DNS	205	Standard query response 0x0002 A www.hansung.ac.kr A 2
13	1.245431	172.30.1.33	168.126.63.1	DNS	77	Standard query 0x0003 AAAA www.hansung.ac.kr
- Packet Details:**
  - Frame 12: 205 bytes on wire (1640 bits), 205 bytes captured (1640 bits) on interface \Device\NPF\_{ACA27A13-66BA-4DA1-AA9A-20DE41ED0C4A}
  - Ethernet II, Src: Allradio\_9c:45:33 (00:07:89:9c:45:33), Dst: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90)
  - Internet Protocol Version 4, Src: 168.126.63.1, Dst: 172.30.1.33
  - User Datagram Protocol, Src Port: 53, Dst Port: 57016
    - Source Port: 53
    - Destination Port: 57016
    - Length: 171
    - Checksum: 0x793b [unverified]
    - [Checksum Status: Unverified]
    - [Stream index: 2]
    - [Timestamps]
  - Domain Name System (response)
    - Transaction ID: 0x0002
    - Flags: 0x8180 Standard query response, No error
    - Questions: 1
    - Answer RRs: 1
    - Authority RRs: 3
    - Additional RRs: 3
  - Queries
    - www.hansung.ac.kr: type A, class IN
  - Answers
    - www.hansung.ac.kr: type A, class IN, addr 220.66.102.11
      - Name: www.hansung.ac.kr
      - Type: A (Host Address) (1)
- Packet Bytes:**

Offset	Hex	ASCII
0040	6e 67 02 61 63 02 6b 72 00 00 01 00 01 c0 0c 00	ng-ac-kr .....
0050	01 00 01 00 00 4b 46 00 04 dc 42 66 0b c0 10 00	.....KF..Bf....
0060	02 00 01 00 01 22 3d 00 06 03 6e 73 32 c0 10 c0	....."=...ns2...
0070	10 00 02 00 01 00 01 22 3d 00 05 02 6e 73 c0 10	....."=...ns...
0080	c0 10 00 02 00 01 00 01 22 3d 00 11 03 6e 73 32	....."=...ns2

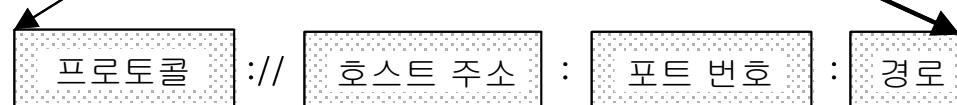
# HTTP 프로토콜 분석



요청 라인
헤더 (일반헤더   요청헤더   엔터티헤더)
공백 라인
본 문 (요청 메시지)

상태 라인
헤더 (일반헤더   요청헤더   엔터티헤더)
공백 라인
본 문 (응답 메시지)

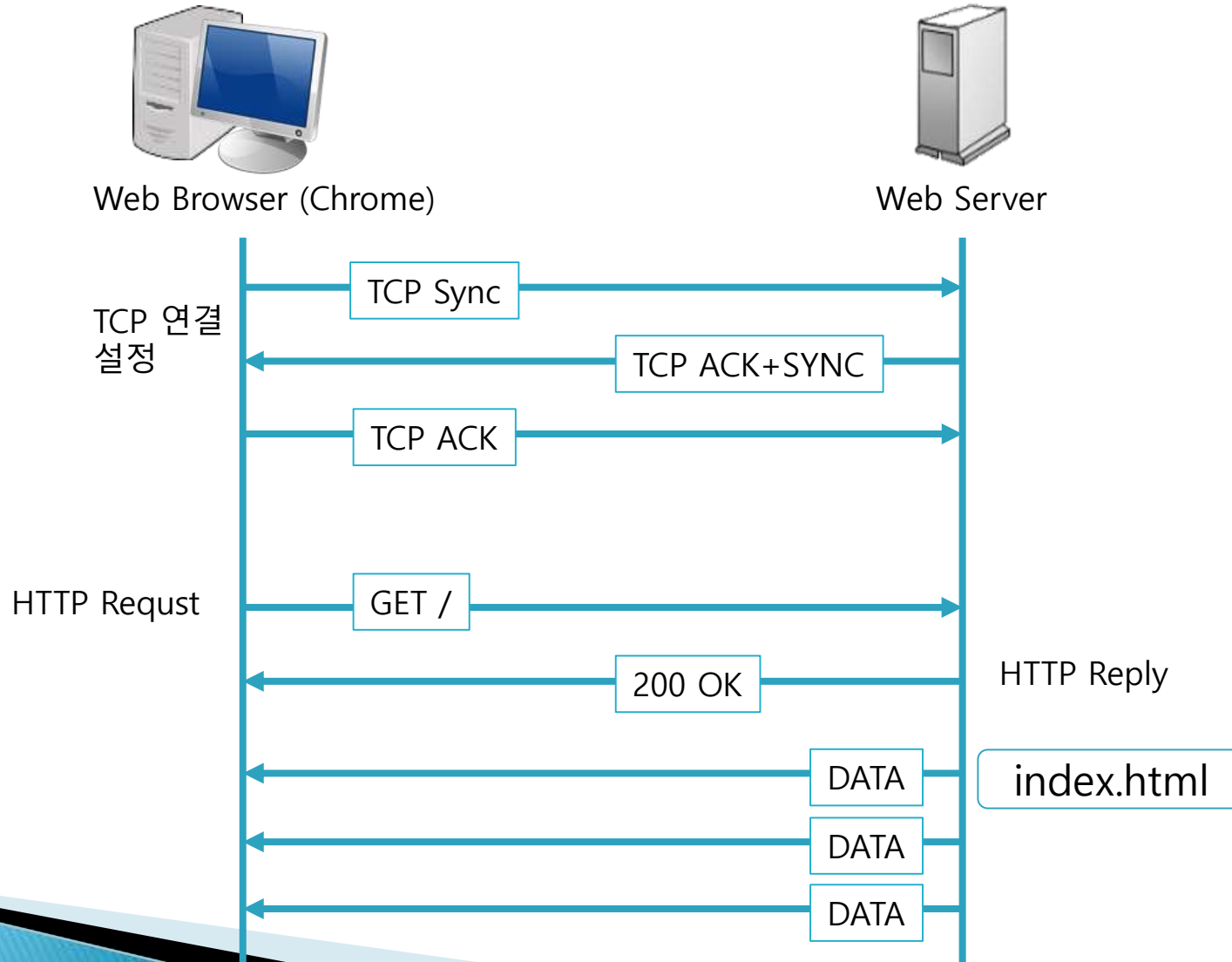
메소드(요청타입)	S	URL	P	HTTP 버전	C	L
					R	F



HTTP 버전	S	상태코드	P	상태설명	C	L
					R	F



# HTTP Request/Reply 흐름



# HTTP Data 예 (PC → Web Server)

The image shows a Wireshark packet capture window. The top pane displays a list of network packets. Packet 75 is selected, showing an HTTP GET request. The bottom pane displays the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
69	6.289886	172.30.1.33	220.66.102.11	TCP	66	8431 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
70	6.290098	172.30.1.33	220.66.102.11	TCP	66	8432 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256
71	6.298454	220.66.102.11	172.30.1.33	TCP	60	80 → 8432 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=14
72	6.298454	220.66.102.11	172.30.1.33	TCP	60	80 → 8431 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 MSS=14
73	6.298564	172.30.1.33	220.66.102.11	TCP	54	8432 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
74	6.298588	172.30.1.33	220.66.102.11	TCP	54	8431 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
75	6.301078	172.30.1.33	220.66.102.11	HTTP	506	GET / HTTP/1.1
76	6.302622	220.66.102.11	172.30.1.33	TCP	60	[TCP Window Update] 80 → 8431 [ACK] Seq=1 Ack=1 Win=41

> Frame 75: 506 bytes on wire (4048 bits), 506 bytes captured (4048 bits) on interface \Device\NPF\_{ACA27A13-66BA-4DA1-AA9A-20DE41ED0C4A},  
> Ethernet II, Src: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90), Dst: Allradio\_9c:45:33 (00:07:89:9c:45:33)  
> Internet Protocol Version 4, Src: 172.30.1.33, Dst: 220.66.102.11  
> Transmission Control Protocol, Src Port: 8432, Dst Port: 80, Seq: 1, Ack: 1, Len: 452  
v Hypertext Transfer Protocol  
 > GET / HTTP/1.1\r\n  
 Host: 220.66.102.11\r\n  
 Connection: keep-alive\r\n  
 Upgrade-Insecure-Requests: 1\r\n  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.83 Safari/537.36\r\n  
 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;\r\n  
 Accept-Encoding: gzip, deflate\r\n  
 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7\r\n  
 \r\n  
 [Full request URI: http://220.66.102.11/]  
 [HTTP request 1/18]  
 [Response in frame: 80]  
 [Next request in frame: 82]

0030 fa f0 c4 16 00 00 47 45 54 20 2f 20 48 54 54 50 .....GE T / HTTP  
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 32 32 30 2e /1.1..Ho st: 220.  
0050 36 36 2e 31 30 32 2e 31 31 0d 0a 43 6f 6e 6e 65 66.102.1 1..Conne  
0060 63 74 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 ction: k eep-aliv  
0070 65 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 e..Upgra de-Insec

Text item (text), 16 byte(s) | Packets: 2489 · Displayed: 2180 (87.6%) · Dropped: 0 (0.0%) | Profile: Default

# HTTP Data 예 (Web Server → PC)

Wireshark packet capture showing an HTTP GET request from a web server to a PC. The capture is filtered by `ip.addr == 220.66.102.11`.

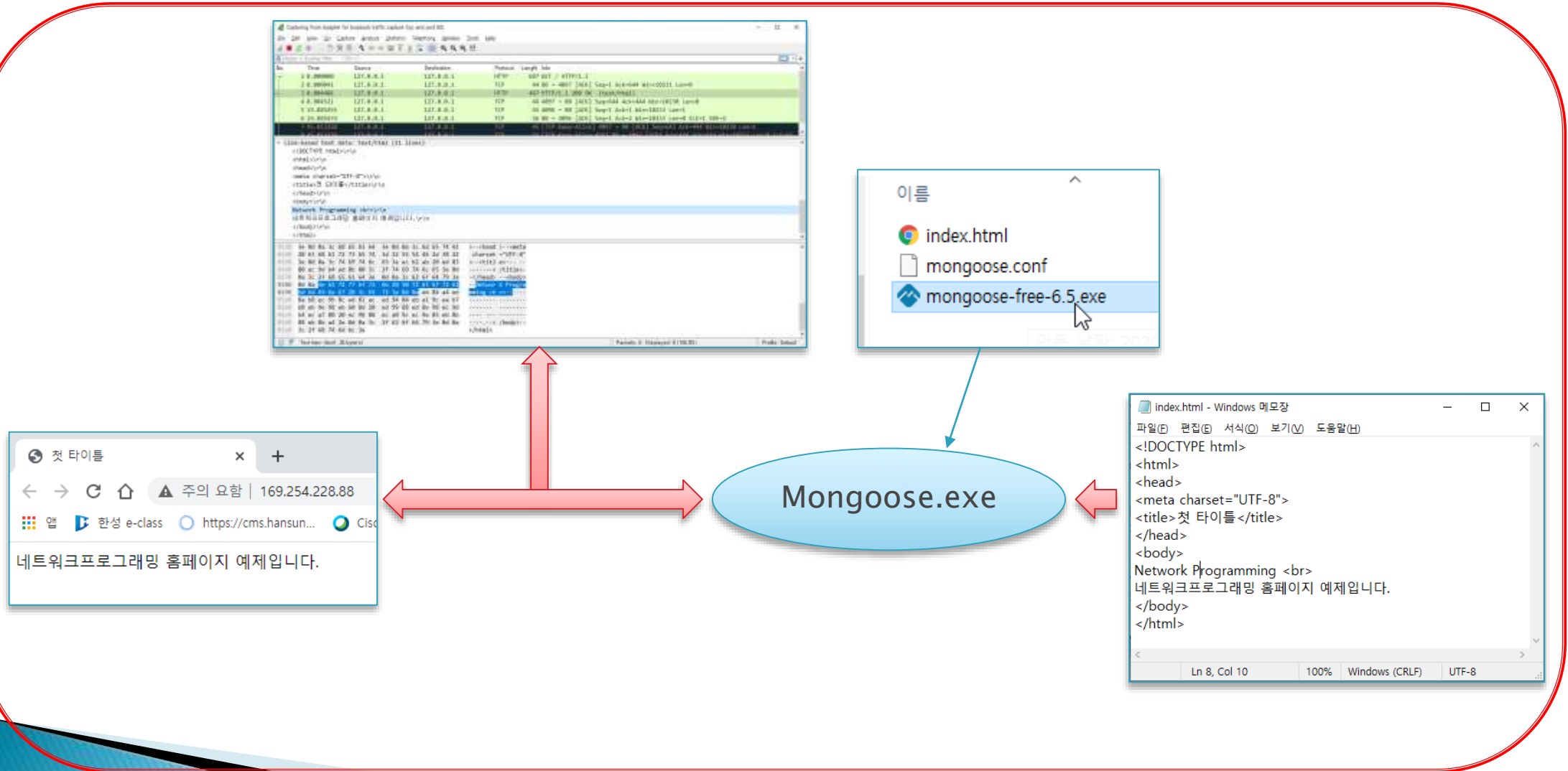
No.	Time	Source	Destination	Protocol	Length	Info
23	0.880223	172.30.1.33	220.66.102.11	HTTP	944	GET /web/www/home HTTP/1.1
24	0.882314	220.66.102.11	172.30.1.33	TCP	60	[TCP Window Update] 80 → 9551 [ACK] Seq=1 Ack=1 Win=4140
25	0.885420	220.66.102.11	172.30.1.33	TCP	60	80 → 9547 [ACK] Seq=1 Ack=891 Win=5030 Len=0
27	1.315828	220.66.102.11	172.30.1.33	TCP	1434	80 → 9547 [ACK] Seq=1 Ack=891 Win=5030 Len=1380 [TCP segment of data stream 0]
28	1.315828	220.66.102.11	172.30.1.33	TCP	1434	80 → 9547 [ACK] Seq=1381 Ack=891 Win=5030 Len=1380 [TCP segment of data stream 0]
29	1.315828	220.66.102.11	172.30.1.33	TCP	978	80 → 9547 [PSH, ACK] Seq=2761 Ack=891 Win=5030 Len=924 [TCP segment of data stream 0]
30	1.315828	220.66.102.11	172.30.1.33	TCP	1434	80 → 9547 [ACK] Seq=3685 Ack=891 Win=5030 Len=1380 [TCP segment of data stream 0]
31	1.315828	220.66.102.11	172.30.1.33	TCP	585	80 → 9547 [PSH, ACK] Seq=5065 Ack=891 Win=5030 Len=531 [TCP segment of data stream 0]

Frame 27: 1434 bytes on wire (11472 bits), 1434 bytes captured (11472 bits) on interface \Device\NPF\_{ACA27A13-66BA-4DA1-AA9A-20DE41ED} Ethernet II, Src: Allradio\_9c:45:33 (00:07:89:9c:45:33), Dst: ASUSTekC\_79:ce:90 (ac:22:0b:79:ce:90) Internet Protocol Version 4, Src: 220.66.102.11, Dst: 172.30.1.33 Transmission Control Protocol, Src Port: 80, Dst Port: 9547, Seq: 1, Ack: 891, Len: 1380

Source Port: 80  
Destination Port: 9547  
[Stream index: 3]  
[TCP Segment Len: 1380]  
Sequence number: 1 (relative sequence number)  
Sequence number (raw): 1510720018  
[Next sequence number: 1381 (relative sequence number)]  
Acknowledgment number: 891 (relative ack number)  
Acknowledgment number (raw): 4213672026  
0101 .... = Header Length: 20 bytes (5)  
Flags: 0x010 (ACK)  
Window size value: 5030  
[Calculated window size: 5030]  
[Window size scaling factor: -1 (unknown)]  
Checksum: 0x0f43 (unverified)

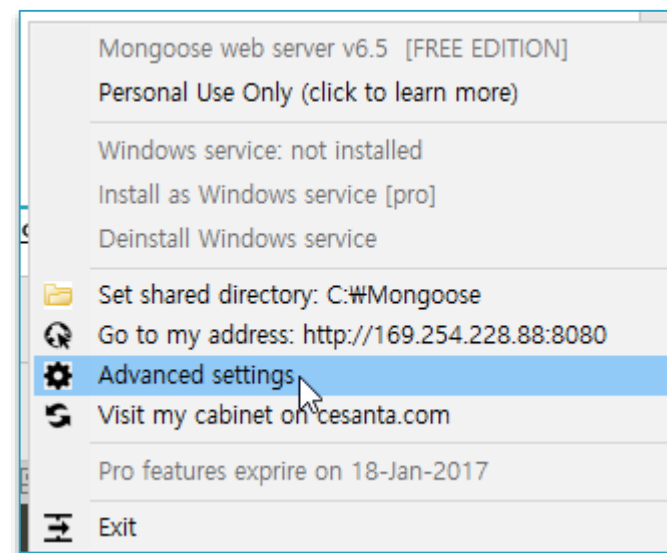
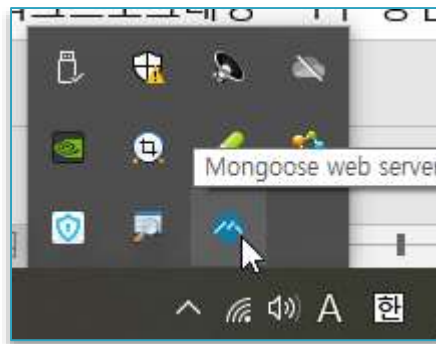
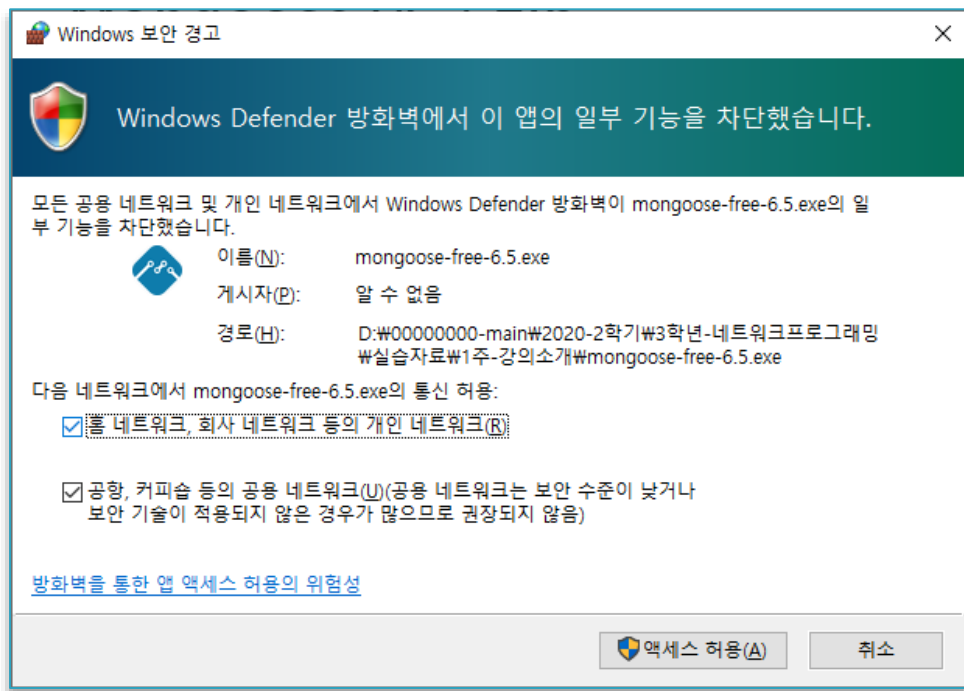
0000 ac 22 0b 79 ce 90 00 07 89 9c 45 33 08 00 45 00 .".y...-E3..E.  
0010 05 8c 10 be 40 00 f1 06 84 20 dc 42 66 0b ac 1e ....@...-Bf...  
0020 01 21 00 50 25 4b 5a 0b c2 12 fb 27 88 5a 50 10 .!.P%KZ-...'.ZP.  
0030 13 a6 0f 43 00 00 48 54 54 50 2f 31 2e 31 20 32 ...C..HT TP/1.1 2  
0040 30 30 20 4f 4b 0d 0a 58 2d 58 53 53 2d 50 72 6f 00 OK..X -XSS-Pro

# HTTP Web Sever 설치 및 Header 분석



# Mongoose 웹서버 설치(실행) 및 설정

- ▶ Mongoose v6.5zip
  - C:\Mongoose\Mongoose-free-6.5.exe



# Mongoose 웹서버 설정, restart

## Mongoose web server settings

Current Settings

access\_control\_list  
auth\_domain mydomain.com  
cgi\_pattern \*\*.cgi\$|\*\*.pl\$|\*\*.php\$  
dav\_root  
document\_root C:\Mongoose  
error\_log\_file  
extra\_mime\_types  
hide\_files\_patterns  
index\_files index.html,index.htm,index.shtml,index.cgi,index.p  
run\_as\_user  
ssl\_certificate  
start\_browser yes

access\_log\_file  
cgi\_interpreter  
dav\_auth\_file  
debug 0  
enable\_directory\_listing yes  
extra\_headers  
global\_auth\_file  
hexdump\_file  
listening\_port 80  
ssi\_pattern \*\*.shtml\$|\*\*.shtm\$  
ssl\_ca\_certificate  
url\_rewrites

(1) 80 port 로 변경

Config file location: C:\Mongoose\mongoose.conf (exists)

Done. Please restart Mongoose.

Reset Defaults

Save Settings

(2)

(3) 종료

Set shared directory: C:\Mongoose  
Go to my address: http://169.254.228.88:80  
Advanced settings  
Visit my cabinet on cesanta.com  
Pro features expire on 18-Jan-2017  
Exit

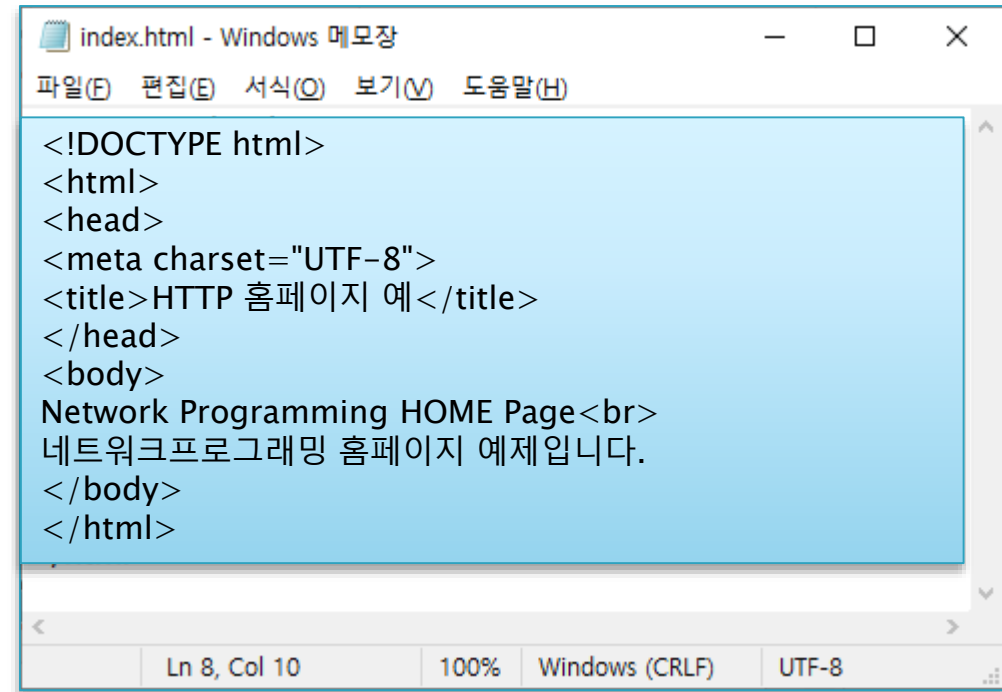
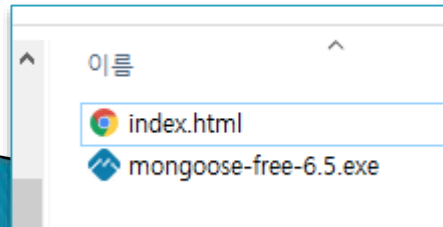
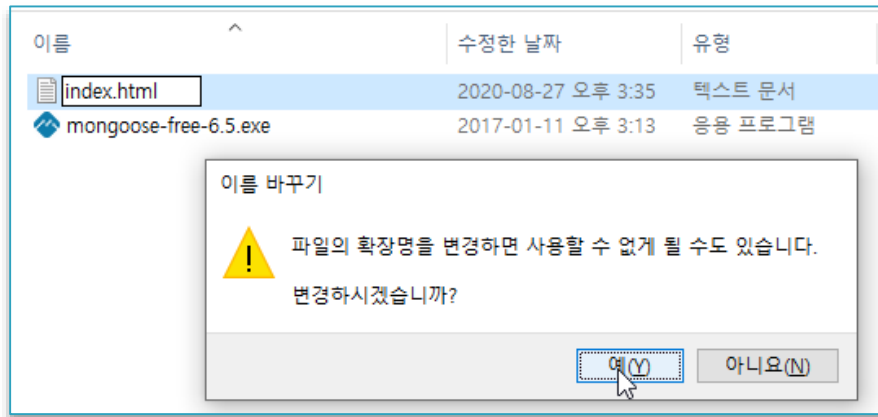
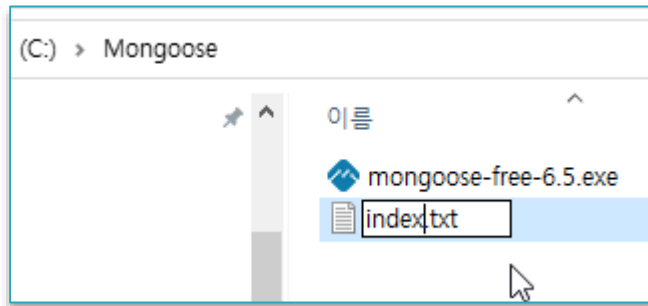
이름  
index.html  
mongoose.conf  
mongoose-free-6.5.exe

(4) 재시작



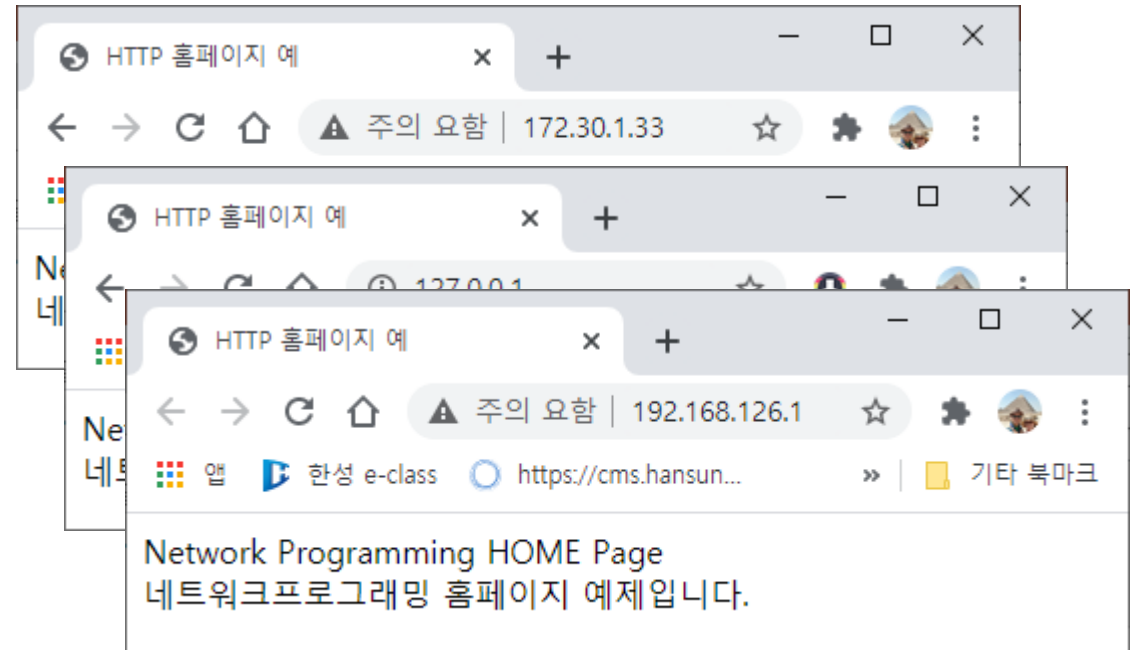
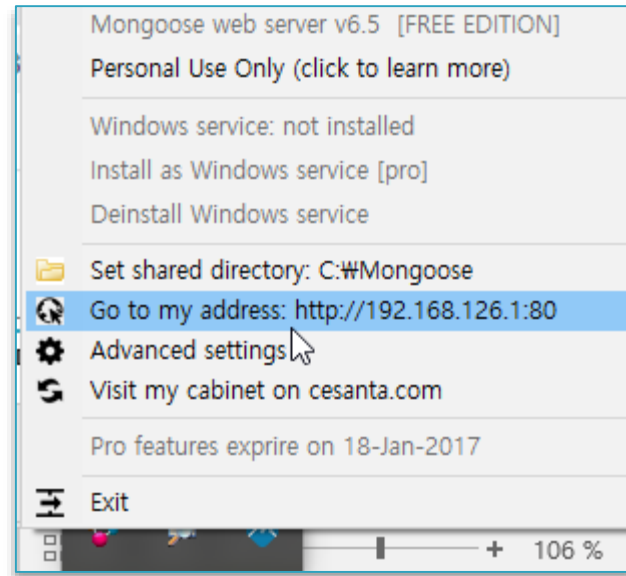
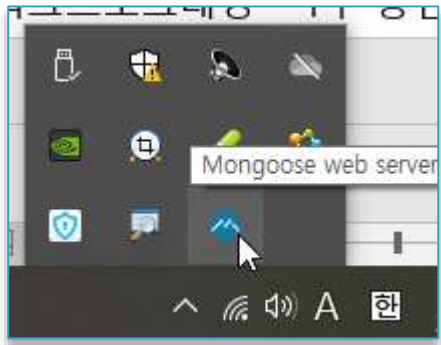
# Home Page : index.html 작성

- ▶ notepad 이용 index.txt → index.html

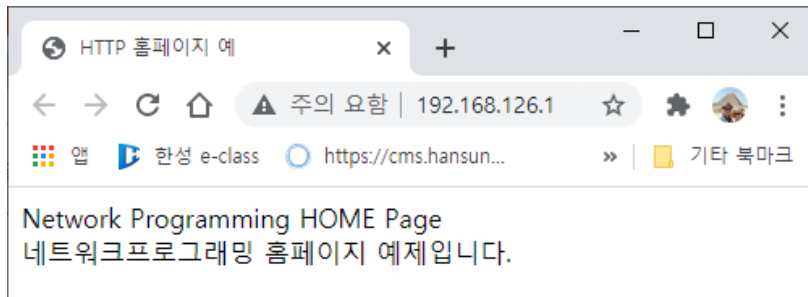
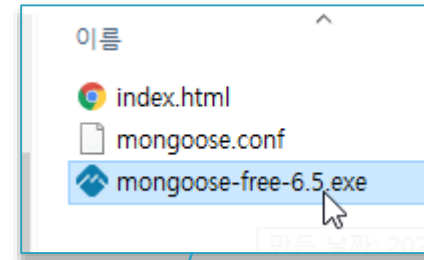
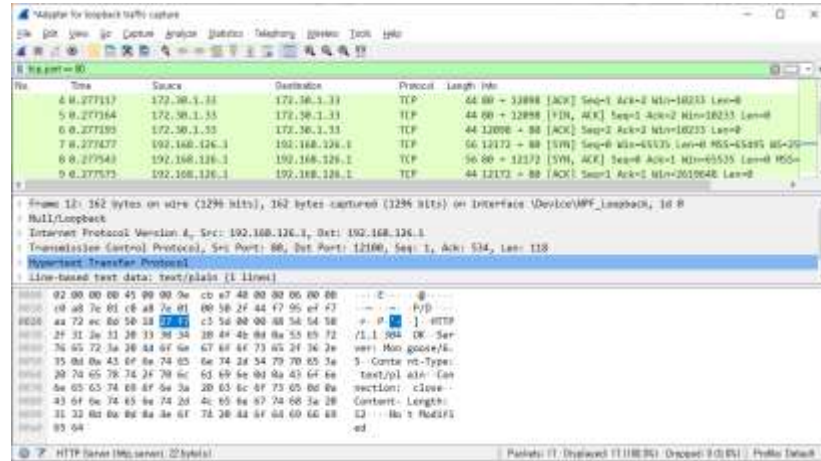


# Home page 확인

- ▶ 모든 IP 주소로 확인 (예)
  - 192.168.126.1 (Vmware 에서 설정한 기본 ip 주소)
  - 127.0.0.1 (Local Loopback)
  - 172.30.1.33 (공유기에서 설정한 IP 주소, 외부 통신용, ipconfig 에서 확인)

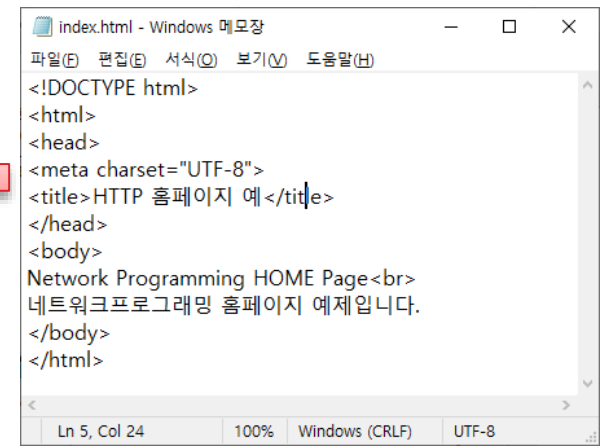


# Wireshark TCP/IP 헤더 분석 - HTTP Web Data



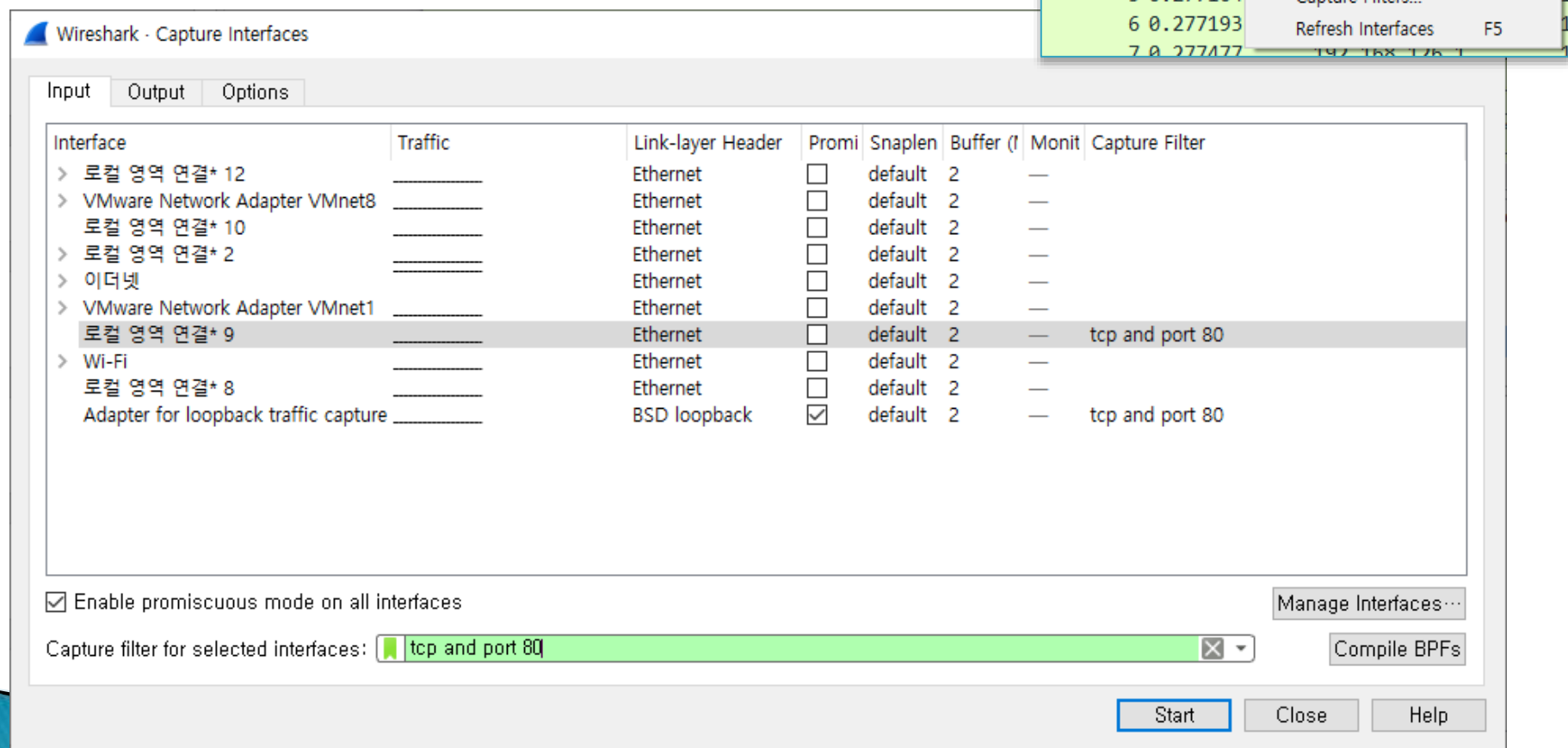
Mongoose.exe

192.168.126.1  
127.0.0.1  
172.30.1.1

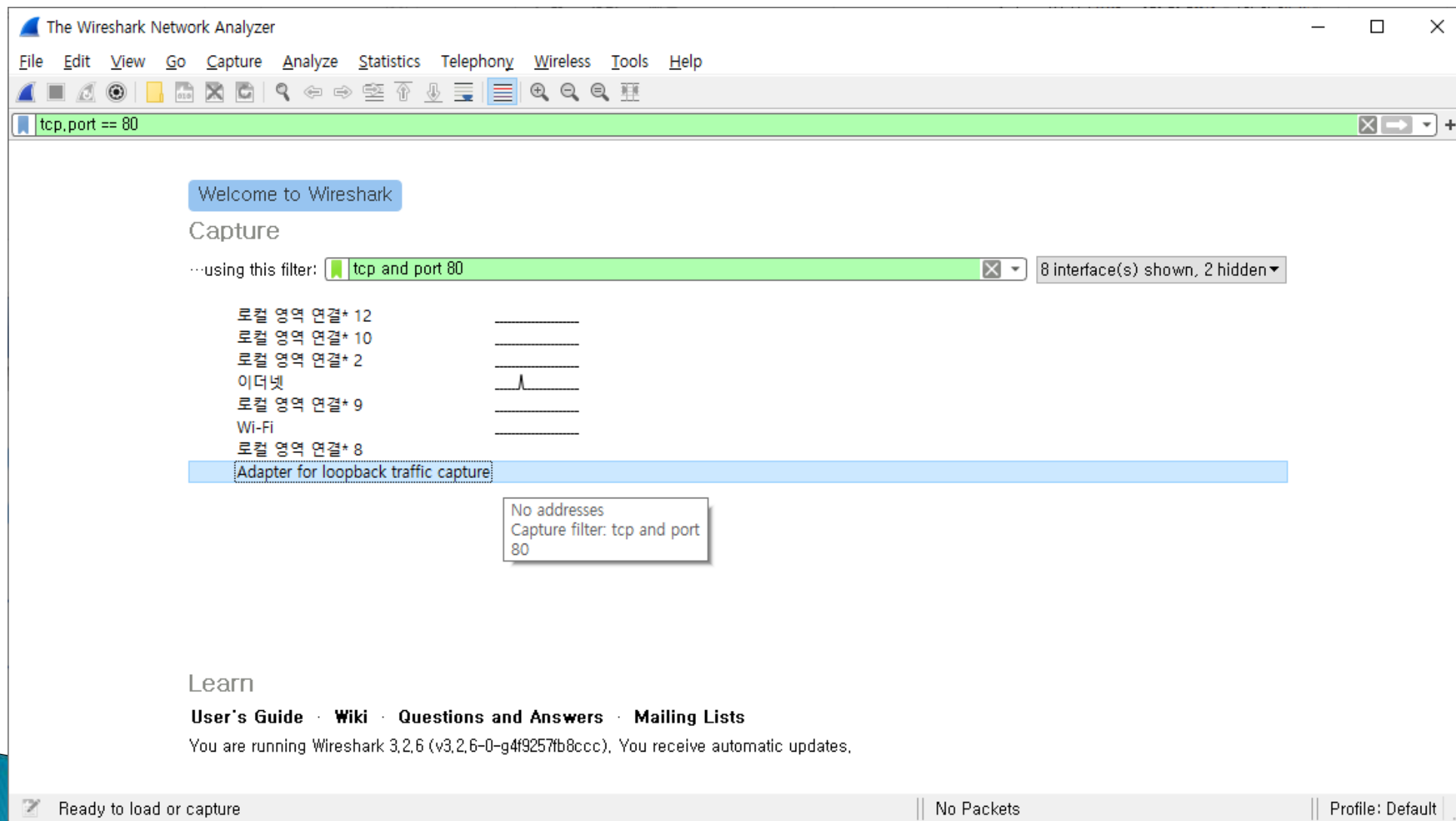


# Wireshark 실행 화면

- ▶ Capture > Option > filter 설정
- ▶ tcp and port 80



# Wireshark 실행 화면 - filter = tcp and port 80



# HTTP Data (Chrome → Web Server)

Capturing from Adapter for loopback traffic capture (tcp and port 80)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
10	0.000821	192.168.126.1	192.168.126.1	TCP	44	12849 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
11	0.001901	192.168.126.1	192.168.126.1	HTTP	603	GET / HTTP/1.1
12	0.001931	192.168.126.1	192.168.126.1	TCP	44	80 → 12848 [ACK] Seq=1 Ack=560 Win=2619648 Len=0
13	0.002730	192.168.126.1	192.168.126.1	HTTP	162	HTTP/1.1 304 OK (text/plain)
14	0.002752	192.168.126.1	192.168.126.1	TCP	44	12848 → 80 [ACK] Seq=560 Ack=119 Win=2619648 Len=0
15	0.002779	192.168.126.1	192.168.126.1	TCP	44	80 → 12848 [FIN, ACK] Seq=119 Ack=560 Win=2619648 Len=0
16	0.002798	192.168.126.1	192.168.126.1	TCP	44	12848 → 80 [ACK] Seq=560 Ack=120 Win=2619648 Len=0
17	0.002909	192.168.126.1	192.168.126.1	TCP	44	12848 → 80 [FIN, ACK] Seq=560 Ack=120 Win=2619648 Len=0
18	0.002946	192.168.126.1	192.168.126.1	TCP	44	80 → 12848 [ACK] Seq=120 Ack=561 Win=2619648 Len=0

> Frame 11: 603 bytes on wire (4824 bits), 603 bytes captured (4824 bits) on interface \Device\NPF\_{Loopback}, id 0

> Null/Loopback

> Internet Protocol Version 4, Src: 192.168.126.1, Dst: 192.168.126.1

> Transmission Control Protocol, Src Port: 12848, Dst Port: 80, Seq: 1, Ack: 1, Len: 559

▼ Hypertext Transfer Protocol

> GET / HTTP/1.1\r\n

Host: 192.168.126.1\r\n

Connection: keep-alive\r\n

Cache-Control: max-age=0\r\n

Upgrade-Insecure-Requests: 1\r\n

0020 cc 5f 77 ce 50 18 27 f9 e2 3c 00 00 47 45 54 20 . \_ w . P . ' . . < . . . GET

0030 2f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 / HTTP/1 .1 . . Host

0040 3a 20 31 39 32 2e 31 36 38 2e 31 32 36 2e 31 0d : 192.16 8.126.1.

0050 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 .Connect ion: kee

0060 70 2d 61 6c 69 76 65 0d 0a 43 61 63 68 65 2d 43 p-alive . Cache-C

0070 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 67 65 3d ontrol: max-age=

0080 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 0 . Upgra de-Insec

0090 75 72 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d ure-Requ ests: 1.

00a0 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a .User-Ag ent: Moz

00b0 69 6c 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 illa/5.0 (Window

00c0 73 20 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 s NT 10. 0; Win64

00d0 3b 20 78 36 34 29 20 41 70 70 6c 65 57 65 62 4b ; x64) A ppleWebK

Text item (text), 16 byte(s)

Packets: 18 · Displayed: 18 (100.0%)

Profile: Default



# Wireshark 분석 결과

\*Adapter for loopback traffic capture (tcp and port 80)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.126.1	192.168.126.1	TCP	56	12698 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SAC
2	0.000081	192.168.126.1	192.168.126.1	TCP	56	80 → 12698 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495
3	0.000120	192.168.126.1	192.168.126.1	TCP	44	12698 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
4	0.000342	192.168.126.1	192.168.126.1	TCP	56	12699 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SAC
5	0.000402	192.168.126.1	192.168.126.1	TCP	56	80 → 12699 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495
6	0.000430	192.168.126.1	192.168.126.1	TCP	44	12699 → 80 [ACK] Seq=1 Ack=1 Win=2619648 Len=0
7	0.010920	192.168.126.1	192.168.126.1	HTTP	496	GET / HTTP/1.1
8	0.010955	192.168.126.1	192.168.126.1	TCP	44	80 → 12699 [ACK] Seq=1 Ack=453 Win=2619648
9	0.012008	192.168.126.1	192.168.126.1	HTTP	504	HTTP/1.1 200 OK (text/html)
10	0.012039	192.168.126.1	192.168.126.1	TCP	44	12699 → 80 [ACK] Seq=453 Ack=461 Win=261913

<

```
<meta charset="UTF-8">\r\n
<title>HTTP 홈페이지 예</title>\r\n
</head>\r\n
<body>\r\n
Network Programming HOME Page<br>\r\n
네트워크프로그래밍 홈페이지 예제입니다.\r\n
</body>\r\n
</html>
```

0140 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 charset ="UTF-8"  
0150 3e 0d 0a 3c 74 69 74 6c 65 3e 48 54 54 50 20 ed >...<titl e>HTTP .  
0160 99 88 ed 8e 98 ec 9d b4 ec a7 80 20 ec 98 88 3c ..... <...<  
0170 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e /title>...</head>  
0180 0d 0a 3c 62 6f 64 79 3e 0d 0a 4e 65 74 77 6f 72 ..<body> ..Networ  
0190 6b 20 50 72 6f 67 72 61 6d 6d 69 6e 67 20 48 4f k Progra mming HO  
01a0 4d 45 20 50 61 67 65 3c 62 72 3e 0d 0a eb 84 a4 ME Page< br>...  
01b0 ed 8a b8 ec 9b 8c ed 81 ac ed 94 84 eb a1 9c ea .....  
01c0 b7 b8 eb 9e 98 eb b0 8d 20 ed 99 88 ed 8e 98 ec .....  
01d0 9d b4 ec a7 80 20 ec 98 88 ec a0 9c ec 9e 85 eb .....  
01e0 8b 88 eb 8b a4 2e 0d 0a 3c 2f 62 6f 64 79 3e 0d .....</body>..  
01f0 0a 3c 2f 68 74 6d 6c 3e .....</html>

Text item (text), 35 byte(s)

Packets: 10 · Displayed: 10 (100.0%) · Dropped: 0 (0.0%) Profile: Default

index.html - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

```
<!DOCTYPE html>
<html>
<head>
<meta charset="UTF-8">
<title>HTTP 홈페이지 예</title>
</head>
<body>
Network Programming HOME Page<br>
네트워크프로그래밍 홈페이지 예제입니다.
</body>
</html>
```

Ln 1, Col 16 100% Windows (CRLF) UTF-8

## 2주 과제 - 별도 과제 제출용 PPT 제공

- ▶ 본인 집 네트워크 구성 확인하고 구성도 그리기
  - 강의노트 6~9 page 중 본인 집의 구성도와 같은 page를 기준, 또는 새로운 구성도를 ppt로 작성
  - 특히, 본인 PC의 IP 주소를 확인해서 네트워크 구성도를 완성할 것
- ▶ 본인 집에서 Wireshark 실습
  - 본인 집에서 [www.hansung.ac.kr](http://www.hansung.ac.kr) 와 통신하는 경우 프로토콜 분석
  - 강의노트와 같은 방법으로 프로토콜 별로 분석 화면 Capture 제출
    - ARP, IP, TCP, UDP/DNS, HTTP
- ▶ Mongoose Web Server 설치 및 Protocol 분석
  - Local Address 기준 (예: 192.68.126.1, 127.0.0.1, 172.30.1.33) 테스트
- ▶ 과제 제출용 PPT 파일 참조