과목명	컴퓨터 네트워크
담당교수	조경산 교수님
학과	소프트웨어학과
학번	32153180
이름	이상민
제출일자	2019.05.20

Chapter 20~24

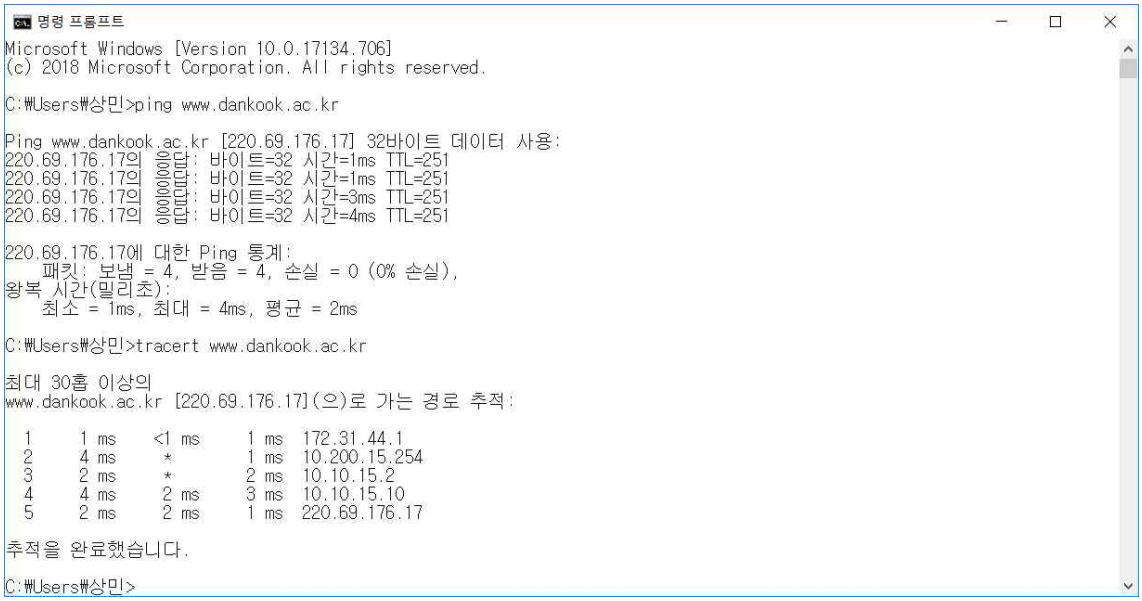
1. Execute the following network commands, and explain the network commands with captured screens.

ping www.dankook.ac.kr

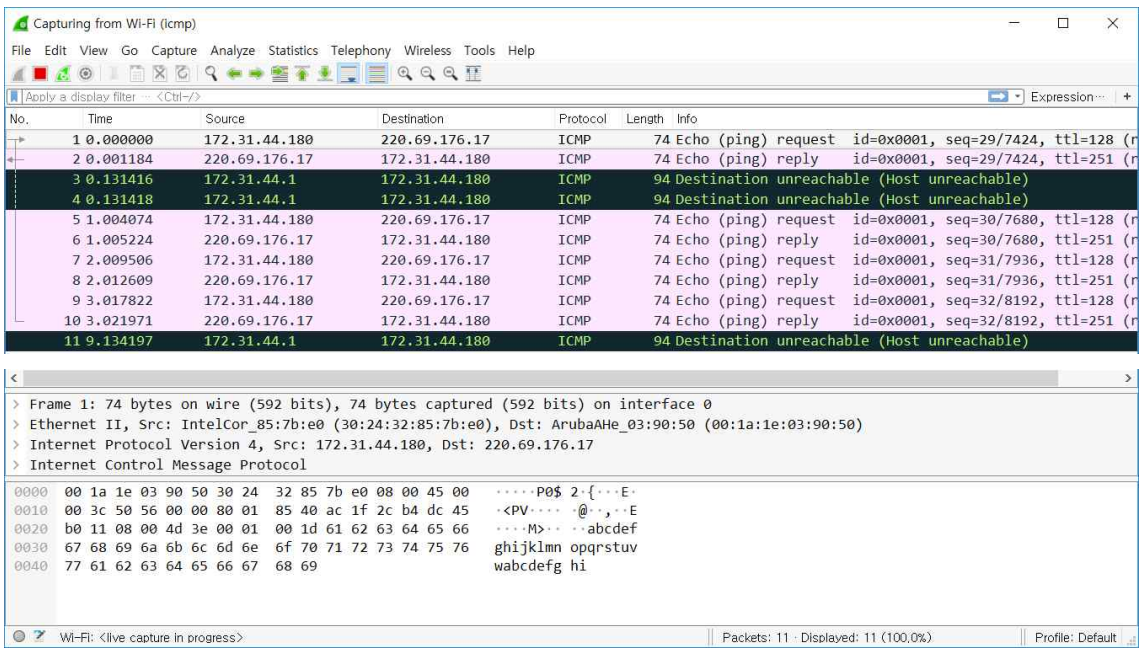
tracert www.dankook.ac.kr

Execute “wireshark” with capture filtering of “icmp”

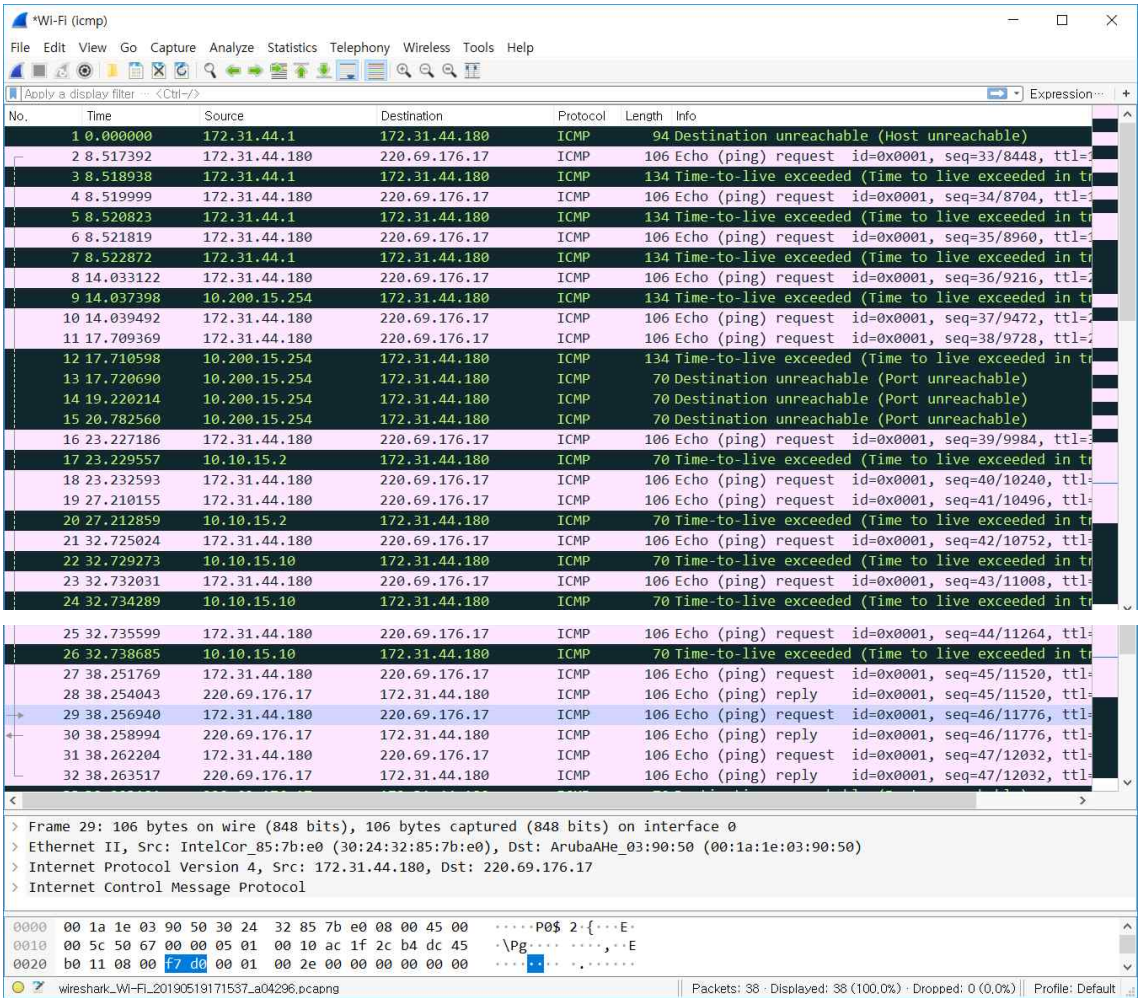
->

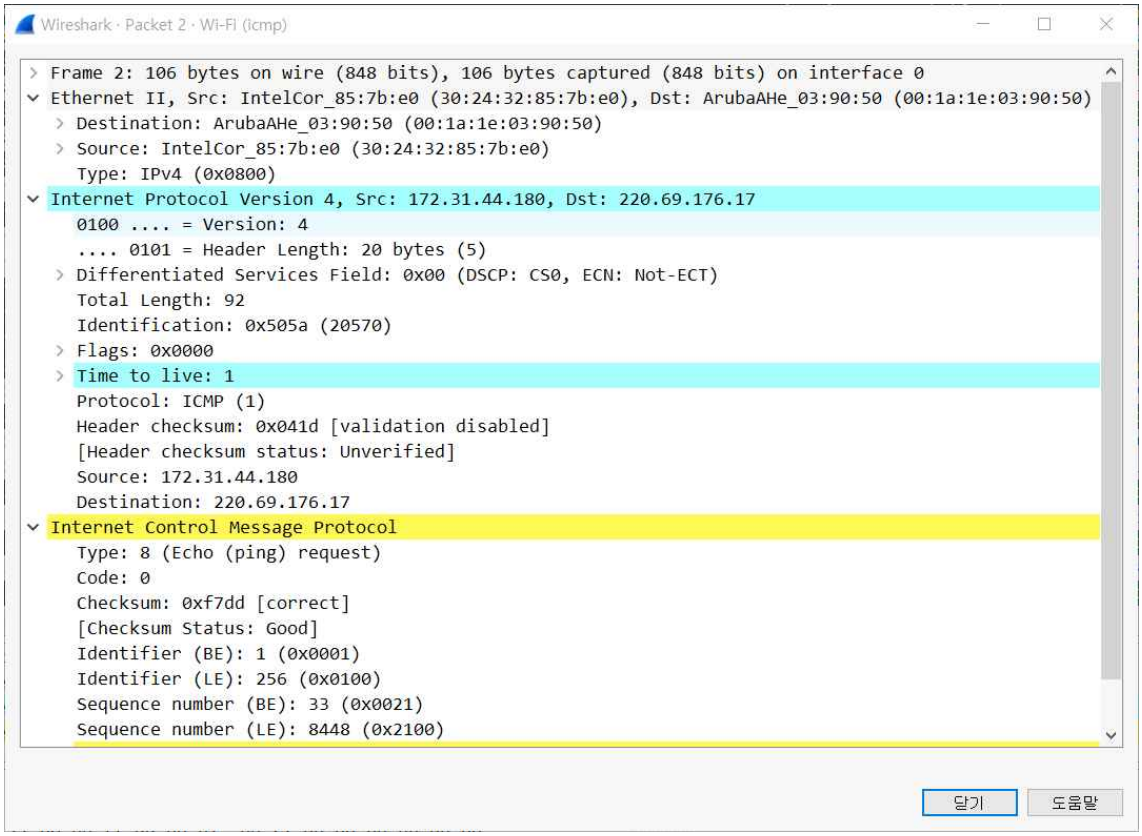


<ping>



<tracert>


*Wi-Fi (icmp)
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 0.000000 172.31.44.1 172.31.44.180 ICMP 94 Destination unreachable (Host unreachable)
2 8.517392 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=33/8448, ttl=
3 8.518938 172.31.44.1 172.31.44.180 ICMP 134 Time-to-live exceeded (Time to live exceeded in tr
4 8.519999 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=34/8704, ttl=
5 8.520823 172.31.44.1 172.31.44.180 ICMP 134 Time-to-live exceeded (Time to live exceeded in tr
6 8.521819 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=35/8960, ttl=
7 8.522872 172.31.44.1 172.31.44.180 ICMP 134 Time-to-live exceeded (Time to live exceeded in tr
8 14.033122 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=36/9216, ttl=
9 14.037398 10.200.15.254 172.31.44.180 ICMP 134 Time-to-live exceeded (Time to live exceeded in tr
10 14.039492 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=37/9472, ttl=
11 17.709369 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=38/9728, ttl=
12 17.710598 10.200.15.254 172.31.44.180 ICMP 134 Time-to-live exceeded (Time to live exceeded in tr
13 17.720690 10.200.15.254 172.31.44.180 ICMP 70 Destination unreachable (Port unreachable)
14 19.220214 10.200.15.254 172.31.44.180 ICMP 70 Destination unreachable (Port unreachable)
15 20.782560 10.200.15.254 172.31.44.180 ICMP 70 Destination unreachable (Port unreachable)
16 23.227186 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=39/9984, ttl=
17 23.229557 10.10.15.2 172.31.44.180 ICMP 70 Time-to-live exceeded (Time to live exceeded in tr
18 23.232593 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=40/10240, ttl=
19 27.210155 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=41/10496, ttl=
20 27.212859 10.10.15.2 172.31.44.180 ICMP 70 Time-to-live exceeded (Time to live exceeded in tr
21 32.725024 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=42/10752, ttl=
22 32.729273 10.10.15.10 172.31.44.180 ICMP 70 Time-to-live exceeded (Time to live exceeded in tr
23 32.732031 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=43/11008, ttl=
24 32.734289 10.10.15.10 172.31.44.180 ICMP 70 Time-to-live exceeded (Time to live exceeded in tr
25 32.735599 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=44/11264, ttl=
26 32.738685 10.10.15.10 172.31.44.180 ICMP 70 Time-to-live exceeded (Time to live exceeded in tr
27 38.251769 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=45/11520, ttl=
28 38.254043 220.69.176.17 172.31.44.180 ICMP 106 Echo (ping) reply id=0x0001, seq=45/11520, ttl=
29 38.256940 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=46/11776, ttl=
30 38.258994 220.69.176.17 172.31.44.180 ICMP 106 Echo (ping) reply id=0x0001, seq=46/11776, ttl=
31 38.262204 172.31.44.180 220.69.176.17 ICMP 106 Echo (ping) request id=0x0001, seq=47/12032, ttl=
32 38.263517 220.69.176.17 172.31.44.180 ICMP 106 Echo (ping) reply id=0x0001, seq=47/12032, ttl=
Frame 29: 106 bytes on wire (848 bits), 106 bytes captured (848 bits) on interface 0
Ethernet II, Src: IntelCor_85:7b:e0 (30:24:32:85:7b:e0), Dst: ArubaAHe_03:90:50 (00:1a:1e:03:90:50)
Internet Protocol Version 4, Src: 172.31.44.180, Dst: 220.69.176.17
Internet Control Message Protocol
0000 00 1a 1e 03 90 50 30 24 32 85 7b e0 08 00 45 00
0010 00 5c 50 67 00 00 05 01 00 10 ac 1f 2c b4 dc 45
0020 b0 11 08 00 f7 d0 00 01 00 2e 00 00 00 00 00 00
wireshark_Wi-Fi_20190519171537_a04296.pcapng
Packets: 38 · Displayed: 38 (100.0%) · Dropped: 0 (0.0%)
Profile: Default



두 번째 패킷은 위 사진과 같다. 간단하게 보면 frame 크기는 106byte이고 Ethernet frame의 source와 destination의 MAC address가 나와있다. type은 IPv4로 0800이다.

또한 IP datagram의 정보들도 들어있다. source와 destination의 IP address가 나와있다. header length는 5이므로 5*4=20byte이다. total length는 92이므로 data가 92-20=72byte로 예상된다. flag값은 0이므로 fragmented 하지 않는다. TTL은 1이다.

ICM protocol을 보면 type 값은 8이고, code 값은 0 그리고 checksum status는 good 즉, error가 없다는 정보들이 들어있다.

2. An IP datagram has the following partial information.

45000054 00030000 2006.....

a) What is the size of the header and the data?

-> 45000054에서 두 번째 5는 header length를 나타내고, 0054는 total length를 나타낸다. header = 5*4 = 20byte이고, data = total length – header = 54-20 = 34byte이다.

b) Is the packet fragmented?

-> 00030000에서 flag는 3bit로 표현되는데 그 값이 0이다. 따라서 DF(Do not Fragment) 값이 0, MF(More Fragment) 값이 0이므로 fragmented 하지 않는다.

c) What is the protocol number of the payload being carried by the packet?

-> 2006.....에서 06은 protocol type을 뜻한다. 따라서 TCP protocol이다.

d) How many more routers can the packet travel to?

-> 2006.....에서 20은 TTL(Time To Live)을 뜻한다. TTL은 길을 찾아주는데, datagram이 방문할 최대 router 개수를 의미한다. 최대 20개의 router를 방문할 수 있다.

3. An organization is granted the block 14.24.74.0/24. The organization needs to create 3 subnets. Assume that one subnet of 10 addresses, one subnet of 60 addresses, and one subnet of 120 addresses. Design 3 address sub-bocks with the first and last addresses.
-> 가장 큰 sub-block은 120개의 주소가 필요하다. 따라서 2^7=128개의 주소를 할당해야 한다. subnet mask = 32-7 = 25이다. 이 sub-block의 first address는 14.24.74.0/25이고, last address는 14.24.74.128/25이다.
그 다음 sub-block은 60개의 주소가 필요하므로 2^6=64개의 주소를 할당해야 한다. subnet mask = 32-6 = 26이다. 이 sub-block의 first address는 14.24.74.129/26이고, last address는 14.24.74.191/26이다.
마지막 sub-block은 10개의 주소가 필요하므로 2^4=16개의 주소를 할당해야 한다. subnet mask = 32-4 = 28이다. 이 sub-block의 first address는 14.24.74.192/28이고, last address는 14.24.74.207/28이다.

4. An IP fragment has arrived with a fragment offset value of 100. How many bytes of data were originally sent by the source before the data in this fragment?
-> offset 값은 항상 8로 나눠서 저장하기 때문에 원래 보낸 data는 800byte이다.

5. Will an ICMP error message is generated if error is found in
a) a datagram having a multicast address?
-> multicast address인 경우에는 error message를 만들지 않는다.
b) a datagram carrying an ICMP error message?
-> ICMP error message를 전달하는 과정에서 발생된 error에 대해서는 또다시 error message를 만들지 않는다.
c) a fragmented datagram that is not the first datagram?
-> fragmented datagram 중 첫 번째 datagram을 제외하고는 error message를 만들지 않는다.

6. Suppose a computer receives two ARP replies from a single request: MAC address is M1 and MAC address is M2. How does ARP handle the replies?
-> 처음 M1을 MAC address로 설정한 뒤 그 다음 받은 M2를 MAC address로 설정한다.

7. Distinguish between multicasting and multiple-unicasting – in terms of the number of the copies(copy) of the message from the sender and destination address.
-> 기본적으로 unicast와 multicast는 정보 전송 방법이다. unicast는 하나의 송신자가 하나의 수신자로만 정보를 전송하는 one-to-one communication이고, multicast는 하나의 송신자가 여러 수신자로 정보를 전송하는 one-to-many communication이다.
multiple-unicast는 말 그대로 다수의 unicast를 뜻하므로 여러 송신사자 여러 수신자에게 정보를 전송하는데 그것들은 각각 일대일 통신이다.

8. How can the error of IP datagram be found?
-> 우선 header checksum을 통해 error를 확인한다. 또한 TTL(Time To Live)이 초과할 경우 ICMP를 통해 error report를 받는다. 이때 ICMP message에는 어느 부분에서 오류가 났는지, 왜 오류가 발생했는지 등에 대한 정보가 들어 있다.

9. Compare NAT and DHCP. Both can solve the problem of a shortage of addresses in an organization, but by using different strategies.
-> NAT(Network Address Translation)는 실제 송신 시 private IP address를 global IP address로 바꿔주는데 사용하는 주소 변환기이다. 이렇게 하는 이유는 global IP address가 부족하기 때문이다.
DHCP(Dynamic Host Configuration Protocol)는 인터넷에 연결되어 사용하려 할 때마다 주소를 할당한다. 복잡하다는 단점이 있지만 주소를 효율적으로 할당할 수 있다.

10. What is the purpose of including the header and portion of payload of the IP datagram in the error-reporting ICMP message?
-> IP protocol은 error 발생 시 고칠 수 있는 능력이 없기 때문에 무조건 버린다. 따라서 ICMP message를 IP datagram을 이용해 전송한다. 그래서 IP protocol과 ICMP protocol은 co-dependent하다고 볼 수 있다.

11. Explain IP spoofing. Can IPSec protect IP datagram from IP spoofing?
-> IP spoofing은 해커가 자신의 IP를 악용하고자 하는 호스트의 IP 주소로 바꾼 뒤, 이를 통해 해킹하는 것이다. IPSec은 IP security protocol의 약자로 안전에 취약한 인터넷에서 안전한 통신을 실현하는 통신 규약이다. 기본적으로 IP에서는 IP spoofing과 같은 취약점을 해결하지 못했기 때문에 이러한 보안상의 문제를 해결하기 위해 IPSec이라는 별도의 protocol을 만든 것이다. IP를 암호화해주기 때문에 IP protocol과 함께 사용해서 보호해준다.

12. Explain advantages and disadvantages of classful addressing of IPv4 addresses.
-> IPv4에서는 3개의 class로 나눠서 IP 주소를 관리한다. 이렇게 하면 많은 network를 효율적으로 관리할 수 있다는 장점이 있다. 하지만 수많은 네트워크에서는 주어진 class에서 할당하는 수보다 훨씬 적은 수의 컴퓨터를 사용한다. 그래서 많은 IP 주소들이 낭비된다는 단점이 있다.