Wireshark 를 이용한 DHCP 와 IPv6 활용 현황 분석

목차

제출자

201323148

소프트웨어학과

이제호

1. 관찰 환경

아주대학교 중앙도서관 4층 열람실에서 본인의 노트북으로 관찰하였다.
관찰 기간 : 약 617초

2. DHCP 활용 현황 분석

IPv4의 경우 Host가 IPv4 주소를 할당 받기 위해서 다음 두 가지 방법을 사용할 수 있다. 첫 번째는 manual configuration으로 system admin에 의해 수동으로 할당하는 방법이다. 두 번째는 DHCP를 통한 할당 방법으로 DHCP server는 특정 subnet network에 연결하고 싶은 host에게 IPv4 주소를 임대해준다. 이 과정은 자동으로 이뤄지며, 첫 번째 방법보다 현재 더 많이 사용되는 방법이다. DHCP는 host를 위한 IP주소뿐 만 아니라, first-hop router, local DNS server의 IP주소 정보 또한 제공한다. 즉, 호스트는 인터넷을 사용하기 위해 필요한 parameters를 DHCP를 통해 얻을 수 있다. 다음 capture 결과를 통해 DHCP 메시지 구조와 흐름을 살펴보자.

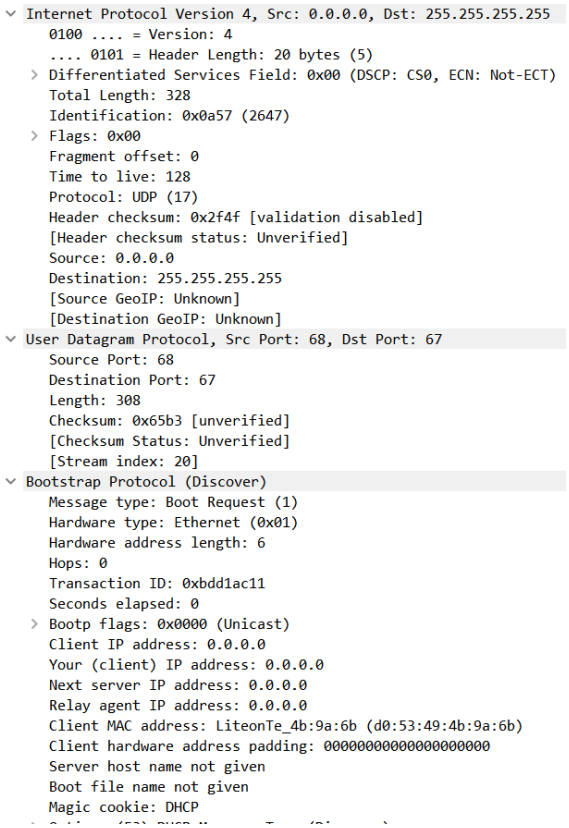
<사진 1 - DHCP messages>

bootp.dhcp

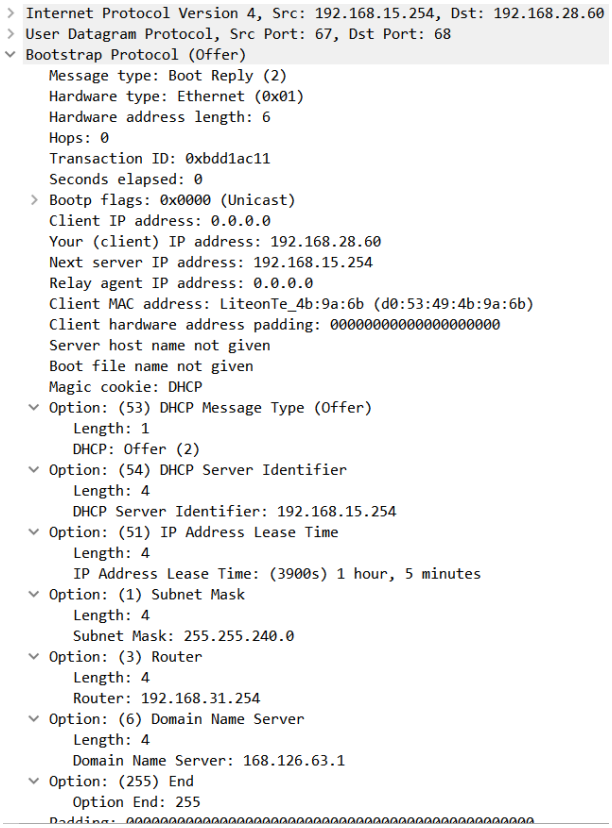
No.	Time	Source	Destination	Protocol	Length	Info
10	0.065461	192.168.28.60	192.168.15.254	DHCP	342	DHCP Release - Transaction ID 0xeaecea46
1154	69.201052	0.0.0.0	255.255.255.2…	DHCP	342	DHCP Discover - Transaction ID 0xbdd1ac11
1235	70.208563	192.168.15.254	192.168.28.60	DHCP	342	DHCP Offer - Transaction ID 0xbdd1ac11
1236	70.211751	0.0.0.0	255.255.255.2…	DHCP	354	DHCP Request - Transaction ID 0xbdd1ac11
1237	70.217678	192.168.15.254	192.168.28.60	DHCP	342	DHCP ACK - Transaction ID 0xbdd1ac11

위 사진은 wireshark filter값을 bootp.dhcp로 하여 filtering된 메시지로써, capture 과정에서 발생한 5개의 DHCP(over UDP/IPv4) 메시지를 나타낸다.

위 메시지들의 교환 과정을 살펴보기 전에 DHCP 메시지를 통해 DHCP 메시지 구조와 IPv4 header 구조를 살펴보겠다.



<DHCP Discover message>



<DHCP Offer message>

왼쪽의 사진은 DHCP Discover Message로 IPv4, UDP, DHCP part 모두 펼쳐 놓았다. 이 메시지는 DHCP client 측에서 server에게 보내는 **요청** 메시지이다. 오른쪽의 사진은 DHCP Offer message로 DHCP part만 나타내도록 하였다. 이 메시지는 DHCP server 측에서 client에게 보내는 **응답** 메시지이다.

(1) IPv4 header 와 DHCP message 구조

우선 왼쪽의 DHCP Discover message를 보며 IPv4 header 구조를 분석하도록 하겠다.

<IPv4 header format>

IP version number	IPv4 또는 IPv6 공통으로 사용하는 field이다. 현재는 IPv4를 나타내고 있으며, 수신 측에서 받은 패킷의 IP version을 지원하지 않으면 해당 패킷은 버려진다.
Header length	IP header의 길이를 나타낸다. Header의 길이는 Option field에 따라 가변적이며 기본은 20 bytes 이다.

Type of service	해당 packet을 특별하게 처리 해달라는 요청에 대한 정보이다.	
Total length	Datagram의 총 bytes 수를 나타낸다.	
16-bit identifier	Fragmentation info	여러 개의 datagram으로 fragmentation 된 segment을 재조합 하기 위해 사용된다.
Flags		Fragmentation에 대한 추가 정보를 위해 사용된다.
Fragment offset		수신자 측에서 segment로 재조합 할 때 data의 순서를 나타낸다.
Time to live	해당 패킷이 routing loop에 의해 네트워크에 오랜 시간 돌아다니지 않게 하기 위해 사용된다. TTL은 router를 거칠 때 마다 1씩 감소되고 0이 되면 해당 패킷은 폐기되며, ICMP를 통해 sender에게 폐기되었다는 정보를 알린다.	
Upper layer protocol	상위 계층의 protocol이 무엇인지 나타내는 필드로 UDP는 00010001 (17) 이다.	
Header checksum	IP header의 오류를 검출하기 위해 사용된다.	
Source IP address, Destination IP address	IP에서 가장 중요한 요소로, 출발지와 목적지의 IP 주소를 나타낸다. IPv4의 주소 길이는 32 bit이다.	
Options	Option field는 IP header를 확장해 추가 정보를 명시하는 field로 해당 field 때문에 IPv4 header의 길이가 가변적이다.	

다음으로 DHCP 메시지의 구조를 분석하는데, 중요한 field들만 다루도록 하겠다.

<DHCP message format>

Message type	DHCP 메시지의 타입을 나타낸다. DHCP 요청은 0x01, DHCP 응답은 0x02이다.
Hardware type	Physical link의 타입을 나타낸다. Ethernet은 0x01이다.
Transaction ID	DHCP client측에서 생성되며 DHCP server와 client가 서로 주고받는 메시지를 ID를 통해 식별할 수 있다.
Client IP address	Client의 현재 IP address를 나타내며, IP의 임대 기간을 갱신하거나 반납할 때 사용한다. DHCP Discover 메시지의 경우에 client는 IP 주소를 할당 받은 상태가 아니므로 0.0.0.0이다.
Your IP address	DHCP server로부터 할당 받는 IP 주소를 나타낸다. DHCP 요청을 받은 DHCP server는 DHCP 응답 메시지의 해당 field에 client가 사용 할 IP 주소를 포함시킨다.
Next server IP address	DHCP server의 IP주소를 나타낸다. DHCP server측에서 해당 field를 포함시켜 응답한다.
Relay agent IP address	DHCP client와 server 사이에 있는 relay agent router의 IP 주소를 나타낸다. Relay agent router는 서로 다른 subnet에 위치한 DHCP client와 server가 서로 통신할 수 있도록 해준다.
Options	DHCP client가 network에 참여하기 위해 필요한 부가 정보들을 나타내는 field이다. 각각의 option은 8-bit의 숫자로 구분된다. 중요한 몇 가지 option들을 살펴보는데, 우선 DHCP client측에서 보낸 요청 메시지에만 포함될 수 있는 option을 보도록 하겠다. 1. **Requested IP Address** - client 측에서 원하는 특정 IP 주소 혹은 과거에 할당 받은 IP주소를 나타낸다. 2. **Parameter Request List** - DHCP client가 server 측에 요청하는 부가적인 network 정보가 무엇인지 나타낸다. Local DNS server의 주소와 subnet mask 등을 포함한다. 다음은 DHCP server 측에서만 보낸 응답 메시지에만 포함될 수 있는 option이다.

	1. **IP Address Lease Time** - 요청을 보내온 DHCP client에게 할당한 IP주소의 임대 기간을 나타낸다. 2. **Subnet Mask** - DHCP client가 속한 network의 subnet mask를 나타낸다. 3. **Router** - DHCP client가 속한 subnet의 first-hop router 주소를 나타낸다. 4. **Domain Name Server** - DHCP client를 위한 local DNS server의 주소를 나타낸다.

(2) DHCP message 교환 과정

위 <사진 1>은 임대 받은 IP주소를 release하고 다시 IP주소를 할당 받는 과정을 나타내며, ipconfig 명령어를 사용해 얻은 결과이다.

첫 번째 메시지는 **DHCP Release 메시지**로 `ipconfig/release` 명령어를 입력한 직후에 나타난 메시지이다. DHCP release 메시지를 보낸 후 연결되어 있던 무선 LAN의 연결이 끊겼다. Capture를 시작하는 시점에서 인터넷에 연결되어 있었기 때문에 DHCP client는 이미 IP 주소를 할당 받았고, DHCP server의 IP 주소 또한 알고 있다. 따라서 DHCP release 메시지에는 source와 destination의 IP 주소가 명확히 나타나있다.

다음 4개의 DHCP 메시지는 `ipconfig/renew` 명령어를 입력한 후 발생한 메시지로, lease renewal 과정이며 다시 IP주소를 할당 받아 다시 인터넷을 사용할 수 있었다. 두 번째 메시지는 **DHCP Discover 메시지**로 DHCP client가 주소를 할당 받기 위해 보내는 첫 메시지이다. 이 시점에서 할당 받은 주소가 없으므로 source IP 주소는 0.0.0.0이고, DHCP server의 주소 또한 알지 못하므로 dest IP 주소를 255.255.255.255로 설정하여 보낸다. 255.255.255.255는 broadcasting IP 주소를 의미하며, subnet에 연결된 모든 노드로 broadcasting 된다. 다음 세 번째 메시지는 **DHCP Offer 메시지**로 DHCP Discover 메시지를 받은 DHCP server가 보내는 메시지이다. DHCP Offer 메시지에는 transaction ID, client에게 할당할 IP 주소, subnet mask, IP 주소 lease time, local DNS server IP 주소 등의 정보가 포함된다. DHCP client가 이러한 정보들을 받아들이게 되면, 인터넷을 사용하는데 필요한 parameter로 설정할 수 있다. 이 DHCP 메시지에서 주목할 점은 destination IP 주소가 broadcasting IP 주소가 아닌 특정 IP주소를 나타내는 unicast IP 주소라는 것이다. 이것은 **DHCP relay/proxy**가 있기 때문에 발생하는 결과이다.

DHCP relay/proxy는 많은 broadcast 메시지로 인해 네트워크 traffic이 증가하는 것을 방지하는 목적으로 설계된 것이다. DHCP relay/proxy는 DHCP relay agent로 동작하는 router 또는 switch에 proxy 기능이 추가된 것을 의미한다. 초기 임대 설정 시, DHCP client가 broadcast하는 DHCP Discover 메시지는 DHCP relay/proxy가 받게 되고 해당 요청 메시지를 여러 개로 복사해서 DHCP relay/proxy에 등록되어있는 DHCP server(s)에게 전달한다. 또한 DHCP relay/proxy는 client의 상태를 trace하기 위해 client 정보를 저장한다. 요청 메시지를 받은 DHCP server들은 DHCP relay/proxy에게 DHCP offer 메시지를 전송하고 DHCP relay/proxy는 그 중 가장 첫 번째로 받은 DHCP offer 메시지를 선택해 DHCP client 측에 전송한다. 이때 DHCP relay/proxy는 해당 offer 메시지의 DHCP server IP주소를 자신의 IP주소로 교체해서 보낸다. DHCP offer 메시지를 받은 client는 임대 받을 IP주소를 명시하여 **DHCP Request 메시지**를 broadcast 전송한다. DHCP request 메

시지를 받은 DHCP relay/proxy는 다시 DHCP server에게 해당 메시지를 전달하고, 전달 받은 DHCP server는 최종적으로 client를 위한 configuration parameters를 포함한 **DHCP ACK 메시지**를 보낸다. DHCP ACK 메시지를 받은 DHCP relay/proxy는 해당 메시지를 DHCP client에게 전달하고, DHCP client는 메시지에 포함된 configuration 정보들을 저장한다. 이렇게 초기의 임대 IP 주소를 설정하는 과정을 거치면 DHCP relay/proxy는 client의 상태를 trace하고 있으므로, DHCP server와 client 사이에서 이후에 발생하는 address lease renewal 또는 release 과정에서 unicast 전송이 가능하게 된다.

3. IPv6 활용 현황 분석

Protocol	Percent Packets	Packets	Percent Bytes	Bytes
Frame	100.0	3906	100.0	1189046
Ethernet	100.0	3906	4.6	54684
Internet Protocol Version 4	73.2	2858	4.8	57320
User Datagram Protocol	42.4	1655	1.1	13240
Transmission Control Protocol	29.7	1159	39.1	464628
Internet Group Management Protocol	1.0	40	0.1	696
Internet Control Message Protocol	0.1	4	0.0	208
Internet Protocol Version 6	26.1	1021	3.4	40840
User Datagram Protocol	25.0	975	0.7	7800
Simple Service Discovery Protocol	23.6	923	9.4	111683
Multicast Domain Name System	0.6	23	0.1	900
Link-local Multicast Name Resolution	0.4	15	0.0	377
Data	0.4	14	0.8	9184
Internet Control Message Protocol v6	1.2	46	0.1	1428

위 사진은 Protocol Hierarchy기능을 통해 살펴본 계층 구조이고, 전체 packet대비 Ipv6 packet의 비중은 26%정도이고 Ipv4 packet은 73%로 별다른 인터넷 작업을 하지 않았음에도 Ipv6 packet의 비중이 적었다. 만약 같은 시간 동안 다양한 인터넷 작업을 한다면, Ipv6 packet의 비중은 현저히 낮아질 것이다.

<사진 2 – IPv6를 사용하는 protocol message>

```
1267 70.565851   fe80::449b:93… ff02::fb   MDNS     93 Standard query 0x0000 ANY LeeJeHo.local, "QM" question
1268 70.566497   fe80::449b:93… ff02::fb   MDNS    131 Standard query response 0x0000 AAAA fe80::449b:9346:311b:c31b A 192.168.28.60
1270 70.566847   fe80::449b:93… ff02::1:3  LLMNR    87 Standard query 0x3ac6 ANY LeeJeHo
1274 70.676791   fe80::449b:93… ff02::16   ICMPv6  110 Multicast Listener Report Message v2
1400 71.776991   fe80::449b:93… ff02::c    SSDP    183 M-SEARCH * HTTP/1.1
```

위 사진은 wireshark filter 값을 ipv6로 두고 나타난 packet의 일부이다. 5개의 packet만 가져온 이유는 실제로 IPv6를 사용하는 protocol은 4 종류만 관찰되었기 때문이다.
Capture된 packet들의 모든 source IPv6 주소는 fe80::449b:9346:311b:c31b로, 아주대학교 중앙도서관 열람실의 무선 LAN에 연결된 본인이 사용하는 노트북의 IPv6 주소이다. 위 IPv6 주소를 풀어 쓰면 fe80:0000:0000:0000:449b:9346:311b:c31b와 같다.

위 4개의 protocol 모두 multicast IPv6 address를 지원하는 protocol이고, 본인의 장치에 연결된 network 장치는 IPv6를 지원하지 않기 때문에 발생하는 IPv6 메시지는 모두 prefix로 ff02::를 가진다. ff02::는 multicast address scope이 link local을 나타내는 prefix로, ff02::가 prefix인 IPv6주소를 destination으로 설정한 packet은 해당 subnet 내부로만 multicast 전송된다. 즉, 해당 subnet 바깥으로 routing이 불가능하다.
연결된 network 장치는 IPv6를 지원하지 않기 때문에 capture 과정에서 특정 link local IPv6 주소를 destination IP주소로 설정하여 전송하는 메시지도 발생하지 않았고, routing 가능한 multicast address scope을 가진 IPv6 주소로 설정된 메시지 또한 발생하지 않았다.

(1) Protocol messages over IPv6 and IPv6 packet header

위 <사진 2>의 IPv6를 사용하는 3개의 서로 다른 protocol 메시지를 통해 어떤 protocol이 있는지 살펴보고 각 protocol의 기능이 무엇인지 간단하게 살펴볼 것 이다. 또한 이 메시지들을 통해 IPv6 header 구조를 분석하고 비교해보겠다.

1 `1268 70.566497 fe80::449b:93… ff02::fb MDNS 131 Standard query response 0x0000 AAAA f`

위 packet은 MDNS (Multicast DNS) protocol over UDP/IPv6을 나타낸다. MDNS는 특정 장치의 host name을 매칭되는 IP 주소로 변환해주는 service이다. Local DNS server가 없는 작은 network 내에 존재하는 장치로부터 발생하며, DHCP server 또는 DNS server와 같은 configuration server의 개입 없이 network configuration이 가능하도록 하는 zero-configuration service이다. 장치의 host name에 매핑되는 IPv6 주소를 얻기 위해 MDNS client는 dest IPv6 주소를 ff02::fb로 설정하여 query 메시지를 multicast 전송한다. MDNS는 오직 ".local"로 끝나는 host name에 대해서만 매핑 서비스를 제공해주는데, ".local"은 pseudo-top-level domain을 나타내고 이는 world-wide official Domain Name System에 참여하고 있지 않는 private network를 표현하는 label이다.
MDNS는 Apple사의 MacOS 또는 iOS 환경의 장치에서 사용하는 name resolution protocol로 설계되었고, 현재 Microsoft사의 Window 10부터는 MDNS를 사용할 수 있도록 업데이트 되었는데 프린트 또는 주변 장치와의 연결을 위해 사용된다.

2 `1270 70.566847 fe80::449b:93… ff02::1:3 LLMNR 87 Standard query 0x3ac6 ANY LeeJeHo`

위 packet은 LLMNR (Link-Local Multicast Name Resolution) over UDP/IPv6 protocol을 나타낸다. LLMNR은 MDNS와 마찬가지로 DNS를 기반으로 하는 protocol이며, 같은 local link에 존재하는 IPv4와 IPv6 host에 대해 name resolution을 제공해준다. LLMNR은 MDNS와는 다르게 어떤 domain name도 query에 포함시킬 수 있다. 장치의 host name에 매핑되는 IPv6 주소를 얻기 위해 LLMNR client는 dest IPv6 주소를 ff02::1:3으로 설정하여 query 메시지를 multicast 전송한다.

LLMNR은 Window 환경에서 동작하도록 설계되었다.

3 1274 70.676791 fe80::449b:93… ff02::16 ICMPv6 110 Multicast Listener Report Message v2

위 packet은 ICMPv6 protocol을 나타낸다. ICMPv6는 IPv6에서 동작하는 ICMP로 IPv6 메시지의 payload에 포함되어 전송한다. ICMP 메시지는 error 메시지와 information 메시지로 나뉘고 각각의 메시지는 ICMP header의 Type field에 의해 구별된다. 예를 들어 "Destination unreachable", "Packet Too Big"등의 error report type과 위 메시지의 "Multicast Listener Report"와 같은 informational type의 ICMPv6 메시지가 있다. Capture 과정에서 발생한 모든 ICMPv6 메시지는 위와 같은 Multicast Listener Report Message v2 Type의 메시지였고, 이러한 type의 메시지는 MLDv2(Multicast Listener Discovery ver. 2) protocol로 정의되어 있으며 ICMPv6의 subset-protocol이다. MLDv2는 multicast packet을 받기 원하는 link상 인접한 multicast listener(device)를 찾거나, 그런 인접한 노드들이 어떤 multicast address를 원하는지 찾을 수 있게 해주는 protocol이다.

다음으로 위 1, 2, 3번 메시지의 내용과 구조를 분석해보도록 하겠다.

1 - MDNS

```
bytes on wire (1048 bits), 131 bytes captured (1048 bits)
c: LiteonTe_4b:9a:6b (d0:53:49:4b:9a:6b), Dst: IPv6mcast_f
Internet Protocol Version 6, Src: fe80::449b:9346:311b:c31b, Dst: ff02::f
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: C
    .... .... .... 0100 0011 0100 0101 1011 = Flow Label: 0x4345b
    Payload Length: 77
    Next Header: UDP (17)
    Hop Limit: 1
    Source: fe80::449b:9346:311b:c31b
    Destination: ff02::fb
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
    Source Port: 5353
    Destination Port: 5353
    Length: 77
    Checksum: 0x7abe [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
Multicast Domain Name System (response)
    [Request In: 1267]
    [Time: 0.000646000 seconds]
    Transaction ID: 0x0000
  > Flags: 0x8400 Standard query response, No error
    Questions: 0
    Answer RRs: 2
    Authority RRs: 0
    Additional RRs: 0
  v Answers
    > LeeJeHo.local: type AAAA, class IN, addr fe80::449b:9346:311b:c31b
    > LeeJeHo.local: type A, class IN, addr 192.168.28.60
```

2 - LLMNR

```
s on wire (696 bits), 87 bytes captured (696 bits) on in
iteonTe_4b:9a:6b (d0:53:49:4b:9a:6b), Dst: IPv6mcast_01:
Internet Protocol Version 6, Src: fe80::449b:9346:311b:c31b, Dst: ff02::1:3
    0110 .... = Version: 6
  > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00 (DSCP: CS0
    .... .... .... 0011 1110 1001 1000 1011 = Flow Label: 0x3e98b
    Payload Length: 33
    Next Header: UDP (17)
    Hop Limit: 1
    Source: fe80::449b:9346:311b:c31b
    Destination: ff02::1:3
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 64438, Dst Port: 5355
    Source Port: 64438
    Destination Port: 5355
    Length: 33
    Checksum: 0xeb1b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 23]
Link-local Multicast Name Resolution (query)
    Transaction ID: 0x3ac6
  > Flags: 0x0000 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  v Queries
    v LeeJeHo: type ANY, class IN
        Name: LeeJeHo
        [Name Length: 7]
        [Label Count: 1]
        Type: * (A request for all records the server/cache has available)
        Class: IN (0x0001)
```

위 2개의 메시지는 각각 MDNS over UDP/IPv6, LLMNR over UDP/IPv6 protocol이고 IPv6 header의 길이는 40 bytes이며 추가적인 extension header field가 없다. 또한 두 protocol 모두 UDP 통신 기반이므로 IPv6 datagram의 data field에 UDP segment가 포함된다.

3 – ICMPv6

```
Frame 1274: 110 bytes on wire (880 bits), 110 bytes captured (880
Ethernet II, Src: LiteonTe_4b:9a:6b (d0:53:49:4b:9a:6b), Dst: IPv
Internet Protocol Version 6, Src: fe80::449b:9346:311b:c31b, Dst:
   0110 .... = Version: 6
 > .... 0000 0000 .... .... .... .... .... = Traffic Class: 0x00
   .... .... .... 0000 0000 0000 0000 0000 = Flow Label: 0x00000
   Payload Length: 56
   Next Header: IPv6 Hop-by-Hop Option (0)
   Hop Limit: 1
   Source: fe80::449b:9346:311b:c31b
   Destination: ff02::16
   [Source GeoIP: Unknown]
   [Destination GeoIP: Unknown]
 v IPv6 Hop-by-Hop Option
      Next Header: ICMPv6 (58)
      Length: 0
      [Length: 8 bytes]
    v Router Alert
       > Type: Router Alert (0x05)
         Length: 2
         Router Alert: MLD (0)
    > PadN
Internet Control Message Protocol v6
   Type: Multicast Listener Report Message v2 (143)
   Code: 0
   Checksum: 0x9fdb [correct]
   [Checksum Status: Good]
   Reserved: 0000
   Number of Multicast Address Records: 2
 v Multicast Address Record Changed to exclude: ff02::fb
      Record Type: Changed to exclude (4)
      Aux Data Len: 0
      Number of Sources: 0
      Multicast Address: ff02::fb
 v Multicast Address Record Changed to exclude: ff02::1:3
      Record Type: Changed to exclude (4)
      Aux Data Len: 0
      Number of Sources: 0
      Multicast Address: ff02::1:3
```

왼쪽의 메시지는 ICMPv6 메시지로 위 1, 2번 메시지와 다르게 extension header field가 존재한다. 기본 IPv6 header의 길이는 40 bytes로 같지만, 추가적인 extension header field의 길이는 8 bytes이다. 앞서 분석한 IPv4는 추가적인 header 정보를 명시하기 위해 IPv4 header에 Options field를 두어 header의 길이가 가변적인 반면, IPv6 header에서는 IPv4 방식에서 발생하는 overhead 문제를 없애고자 기본 IPv6 header의 길이는 고정시키고 추가 header 정보는 extension header를 추가하는 방식을 택했다. 따라서 IPv6의 header는 기본 header로부터 chain으로 연결되어 있는 형태를 가진다. 또한 위 1, 2번 메시지는 IP datagram의 payload에 UDP segment (transport layer)가 포함되어 있지만, 왼쪽 3번 메시지는 payload에 ICMPv6 protocol message 자체를 포함하고 있다.

왼쪽 3번 ICMPv6 메시지를 통해 IPv6 header 구조를 분석하고 IPv4와의 차이점 또한 다루도록 하겠다.

<IPv6 header format>

IP version number	IP version을 나타내는 4bit field로 IPv4 header에도 존재한다. 0110(binary) = 6(decimal), 즉 IPv6임을 나타낸다.
Traffic Class	IPv4의 TOS와 유사하며, 특정 IP packet을 지정한 Class에 따라 우선순위를 두는데 사용되는 8-bit field이다.
Flow Label	각각의 패킷 flow를 구분할 수 있는 식별용 label을 나타낸다. 예를 들어 실시간 서비스와 같은 특별한 처리를 요구하는 sender에 대해 특정 flow에 속하는 packet을 labeling하는데 사용할 수 있다.
Payload length	IP datagram의 data field(=payload) 길이를 나타낸다. 위 datagram의 payload 길이는 36 bytes이다. 36 bytes (payload) = 8 bytes (extension header) + 28 bytes (ICMPv6 data)
Next Header	Datagram payload에 포함된 protocol을 명시하는 1 byte field로, 1, 2번 메시지의 경우 next header는 UDP에 해당하는 식별 번호 17(decimal)인 반면, 3번 ICMPv6메시지는 0(decimal)이다. 0(decimal)은 "IPv6 Hop-by-Hop Option"을 나타내며, 기본 IPv6 header 40 bytes 뒤에 따라오는 extension header field가 존재한다.
Hop Limit	IPv4의 TTL field와 같다.
Source IP address, Destination IP address	출발지와 목적지 IPv6 주소를 나타낸다. IPv6 주소의 길이는 128 bit로 IPv4의 주소 부족 현상을 해결하고도 충분히 남는 숫자이다. 주소 부족 현상을 해결할 수 있다는 큰 장점이 있지만, NAT에 의해 주소 부족 현상을 해결할 수 있고 sensor network에서와 같이 작은 device에서 주소 길이만 32 bytes를 사용해야 한다는 등의 이유 때문에 IPv6의 도입이 늦어지고 있다.

[Extension Header]	Hop-by-Hop Option이란 해당 packet이 거치는 매 router 마다 처리해야 하는 option을 뜻한다. 따라서 거치는 모든 router들은 extension header를 처리해야 한다. Extension header의 length 단위는 8 bytes로 한 개의 option만을 가진 extension header의 길이는 8 bytes이다.	
IPv6 Hop-by-Hop Option	**Next Header**	base IPv6 header의 Next Header field는 extension header의 Type을 명시하는데 사용되었고, 해당 extension header의 Next Header field는 실제로 datagram payload에 포함되는 protocol을 명시하는데 사용하거나 또 다른 extension header의 type을 명시하는데 사용된다. 58(decimal)은 payload에 포함되는 protocol인 ICMPv6를 나타낸다.
	Length	Length field는 extension header의 실제 길이를 명시하는 것이 아니고, 첫 8 bytes를 제외한 8 bytes block 단위로 표현한 길이를 나타낸다. 현재 option은 한 개 밖에 없으므로 length field는 0이고 8 bytes임을 나타낸다.
	Option	Packet이 거치는 매 router들이 추가적으로 처리할 option이 무엇인지 명시하는 field이다. 현재 option type은 "Router Alert" option type(0x05)을 나타내고, Router Alert 중에서도 Multicast Listener Discovery (MLD) type을 Option field의 마지막 2 bytes를 통해 명시한다. 이는 payload에서 ICMPv6의 type이 MLDv2 인 것과 연관이 있다.
	PadN	8 bytes block 간의 경계를 두기 위해 사용되는 field이다.

4. 새로 알게 된 지식

DHCP offer 메시지에서 destination IP 주소가 broadcasting IP 주소가 아닌 unicast IP 주소였는데, 이 부분을 이해하는데 많은 시간을 투자했다. 구글링을 통해 어느 정도 이해하고 보니 컴퓨터 네트워크를 수강하면서 많이 접했던 개념인 proxy 기능이 접목되어 있었다. 즉, 지금까지 배운 Web proxy 또는 DNS proxy의 목적은 네트워크의 메시지 수를 줄이는 것인데 DHCP에서도 마찬가지로 해당 목적을 위해 DHCP relay/proxy가 설계되어 있었다. DHCP server와 client간에 DHCP relay/proxy를 통해 DHCP 메시지를 주고 받는 경우 다음과 같은 장점이 있다.
우선 다수의 DHCP server에게서 받은 DHCP offer 메시지들을 DHCP relay/proxy가 받으면 하나의 DHCP offer 메시지만 DHCP client에게 전달되므로 network traffic이 줄어드는 효과가 있다.
또한 DHCP relay/proxy에서 DHCP offer 메시지를 DHCP client에게 보낼 때 DHCP server의 IP주소를 DHCP relay/proxy 자신의 IP주소로 바꿔 보내기 때문에 DHCP client는 실제 DHCP server의 IP 주소를 알지 못한다. 따라서 Dos 공격을 예방할 수 있는 장점이 있다.

ICMPv6 메시지 분석에서 MLDv2에 대해 다뤘는데, MLDv2 for IPv6에 대해 더 알아보겠다.
MLDv2는 IPv6 router가 link상 인접한 multicast listener node를 발견하는데 사용되거나 그런 node들이 어떤 multicast address를 원하는지 찾을 수 있게 해주는데 사용되며, 마치 IGMPv3와 비슷하다. MLDv2는 독립적인 protocol이 아닌, ICMPv6에 포함된 protocol임을 ICMPv6 메시지 분석을 통해 확인할 수 있었다. MLD를 통해 수집된 정보는 어떤 multicast routing protocol을 사용하는 router에게든 제공되어야 하는데, 특정 multicast 전송된 packet을 원하는 모든 link상의

listener node가 해당 packet을 받을 수 있어야 하기 때문이다. <사진 2>에서 MDNS와 LLMNR 메시지가 포착된 직후 MLDv2 in ICMPv6 메시지가 포착되었는데, 주목할 점은 MLDv2 메시지에 있는 Multicast address record field의 address가 MDNS와 LLMNR 메시지의 destination 주소라는 것이다. 즉, 해당 multicast 주소에 대해 관심이 있다는 것을 link 상 인접한 node들에게 알리는 기능을 하는 것이다. 이렇게 MLDv2 메시지는 multicast address를 destination 주소로 설정하는 protocol 메시지와 상호적이다.

5. 관찰 후 소감

이번 3차 과제는 특정 시나리오 없이 일정 시간 동안 capture가 진행되므로 처음에 큰 어려움이 없을 것이라 생각했다. 하지만 명료하고 이해하기 쉬운 메시지들이 송수신되는 1, 2차 과제의 protocol과는 달리, 3차 과제에서 분석하는 protocol은 메시지에 포함된 내용이 무엇을 의미하는지 이해하고 알아보는데 많은 시간을 썼다. 게다가 1, 2차 과제의 protocol들에 비해 실제로 많이 접할 수 없는 protocol들을 다루었기 때문에 해당 protocol이 무엇인지부터 알아봐야 했다. 과제 중에 왜 강의 주 교재가 top-down approach를 하는지 깨닫게 되었다.
1차부터 3차까지 wireshark 분석을 통해 흥미로웠던 것은 Network를 위한 많은 protocol, service들의 RFC 문서를 찾아보고 문서의 내용과 실제 capture된 packet의 내용이 매치되는 것을 확인할 수 있다는 점이었다. 3번의 과제를 통해 Network에 대해 이해할 수 있었음은 물론이고, 이해되지 않는 내용을 영문으로 된 문서와 자료를 읽어가며 이해하는 과정이 흥미로웠고 도움이 많이 됐다.