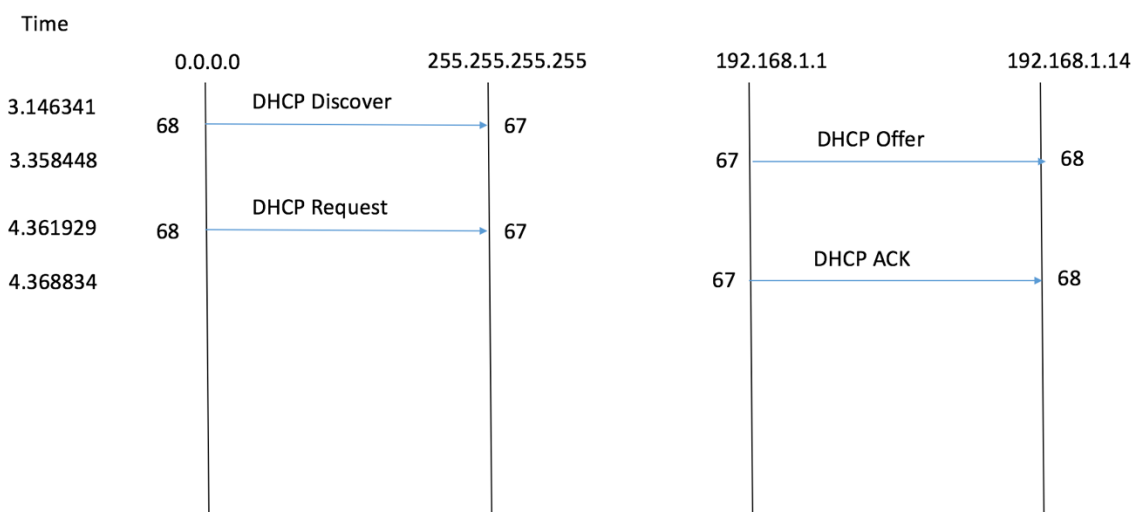# EE450

Lab1

Session 2

Yin-Hsia Yen

Q1: Are DHCP messages sent over UDP or TCP?

DHCP sent message through UDP

```
▶ Frame 141: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶ Ethernet II, Src: Apple_1b:1e:96 (8c:85:90:1b:1e:96), Dst: Sagemcom_4f:46:ea (e8:ad:a6:4f:46:ea)
▶ Internet Protocol Version 4, Src: 192.168.1.14, Dst: 192.168.1.1
▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
▶ Dynamic Host Configuration Protocol (Release)
```

Q2: Draw a timing datagram illustrating the sequence of the first four-packet Discover/Offer/Request/ACK DHCP exchange between the client and server. For each packet, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?

The port numbers are the same

Time
```
                0.0.0.0            255.255.255.255      192.168.1.1            192.168.1.14
                     DHCP Discover
3.146341    68  |---------------------▶|  67
                                                          DHCP Offer
3.358448                                          67  |---------------------▶|  68
                     DHCP Request
4.361929    68  |---------------------▶|  67
                                                          DHCP ACK
4.368834                                          67  |---------------------▶|  68
```

Q3: What is the link-layer (e.g., Ethernet) address of your host?

The link-layer address of my host is 8c:85:90:1b:1e:96

```
▶ Frame 141: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
▶ Ethernet II, Src: Apple_1b:1e:96 (8c:85:90:1b:1e:96), Dst: Sagemcom_4f:46:ea (e8:ad:a6:4f:46:ea)
▶ Internet Protocol Version 4, Src: 192.168.1.14, Dst: 192.168.1.1
▶ User Datagram Protocol, Src Port: 68, Dst Port: 67
▶ Dynamic Host Configuration Protocol (Release)
```

Q4: What values in the DHCP discover message differentiate this message from the DHCP request message?

It can be distinguished by Option (53) DHCP Message Type


```
▶ Option: (53) DHCP Message Type (Discover)
▶ Option: (53) DHCP Message Type (Offer)
```

Q5: What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set (Request/ACK) set of DHCP messages? What is the purpose of the Transaction-ID field?

The value of Transaction-ID in the first set (Discover/Offer/Request/ACK): 0xb79829b
The value of Transaction-ID in the second set (Request/ACK): 0x89ae0ecc
Transaction-ID allows the client to recognize which DHCP response correspond to which request

No.	Time	Source	Destination	Protocol	Length	Info
74	3.146341	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover – Transaction ID 0xb79829b
80	3.358448	192.168.1.1	192.168.1.14	DHCP	342	DHCP Offer – Transaction ID 0xb79829b
86	4.361929	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request – Transaction ID 0xb79829b
87	4.368834	192.168.1.1	192.168.1.14	DHCP	342	DHCP ACK – Transaction ID 0xb79829b
141	6.413956	192.168.1.14	192.168.1.1	DHCP	342	DHCP Release – Transaction ID 0xb79829c
142	6.414745	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover – Transaction ID 0x89ae0ecc
143	6.423921	192.168.1.1	192.168.1.14	DHCP	342	DHCP Offer – Transaction ID 0x89ae0ecc
146	7.429765	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request – Transaction ID 0x89ae0ecc
147	7.509173	192.168.1.1	192.168.1.14	DHCP	342	DHCP ACK – Transaction ID 0x89ae0ecc
409	10.127152	192.168.1.14	192.168.1.1	DHCP	342	DHCP Release – Transaction ID 0x89ae0ecd

Q6: A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange! If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK DHCP), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

If the IP address is not set yet, the client uses 0.0.0.0 as source IP, 255.255.255.255 as destination IP; while DHCP server uses its actual IP as source IP and 255.255.255.255 as destination IP.

It can be shown as follows:

	Source IP	Destination IP
DHCP- Discover	0.0.0.0	255.255.255.255
DHCP- Offer	192.168.1.1	255.255.255.255
DHCP- Request	0.0.0.0	255.255.255.255
DHCP- ACK	192.168.1.1	255.255.255.255

Q7: What is the IP address of your DHCP server?

The IP address of my DHCP server is 192.168.1.1

Q8: What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

The DHCP server offers 192.168.1.14 to the client

```
▶ Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.1.14
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Apple_1b:1e:96 (8c:85:90:1b:1e:96)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▶ Option: (53) DHCP Message Type (Offer)
```

Q9: In the example screenshot in this assignment, there is no relay agent between the host and the DHCP server. What values in the trace indicate the absence of a relay agent? Is there a relay agent in your experiment? If so what is the IP address of the agent?

There is no relay agent in my experiment.

```
▶ Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 192.168.1.14
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: Apple_1b:1e:96 (8c:85:90:1b:1e:96)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▶ Option: (53) DHCP Message Type (Offer)
```

Q10: Explain the purpose of the router and subnet mask lines in the DHCP offer message.

The router in the DHCP offer message tells you the Gateway IP address which can be used to connect to another network.

The subnet mask lines tell you how to get the Net ID from an IP address

```
▶ Option: (54) DHCP Server Identifier (192.168.1.1)
▶ Option: (51) IP Address Lease Time
▼ Option: (1) Subnet Mask (255.255.255.0)
    Length: 4
    Subnet Mask: 255.255.255.0
▼ Option: (3) Router
    Length: 4
    Router: 192.168.1.1
```

Q11: In the DHCP trace file noted in footnote 2, the DHCP server offers a specific IP address to the client (see also question 8. above). In the client's response to the first server OFFER message, does the client accept this IP address? Where in the client's RESPONSE is the client's requested address?

Yes. The client accepts the IP address.

```
▶ Option: (53) DHCP Message Type (Request)
▶ Option: (55) Parameter Request List
▶ Option: (57) Maximum DHCP Message Size
▶ Option: (61) Client identifier
▼ Option: (50) Requested IP Address (192.168.1.14)
      Length: 4
      Requested IP Address: 192.168.1.14
▶ Option: (54) DHCP Server Identifier (192.168.1.1)
▶ Option: (12) Host Name
▶ Option: (255) End
  Padding: 00000000
```

Q12: Explain the purpose of the lease time. How long is the lease time in your experiment?

The client can own this IP address in the lease time.
Once the lease time is expired or the client releases this IP address, DHCP can assign it to others.

```
▼ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (259200s) 3 days
```

Q13: What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgment of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

The purpose of the DHCP release message:

1. The client asks to release this IP address so that another client can use it
2. The leasing time is expired and the client needs to ask for a new one.

The DHCP server does not send an ACK to the clients.

When the DHCP release message is lost, DHCP server needs to wait till the leasing time expired so that it can assign it to another client.

Q14: Clear the *bootp* filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet-exchange period? If so, explain the purpose of those ARP packets.

There is no ARP packet happened between the DHCP packet-exchange period.
(No. 74 ~87, DHCP Discover/Offer/Request/ACK)

No.	Time	Source	Destination	Protocol	Length	Info
73	2.506319	192.168.1.1	192.168.1.14	DNS	80	Standard query response 0xc18f No such name PTR lb._dns-sd._udp.home
74	3.146341	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb79829b
75	3.149520	192.168.1.1	192.168.1.14	ICMP	62	Echo (ping) request id=0x9892, seq=0/0, ttl=64 (no response found!)
76	3.156085	2605:e000:1525:441…	2607:f8b0:4007:80c…	TCP	86	53807 → 443 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=2738417055 TSecr=3279020737
77	3.175478	2607:f8b0:4007:80c…	2605:e000:1525:441…	TCP	86	443 → 53807 [FIN, ACK] Seq=1 Ack=2 Win=270 Len=0 TSval=3279063726 TSecr=2738417055
78	3.175550	2605:e000:1525:441…	2607:f8b0:4007:80c…	TCP	86	53807 → 443 [ACK] Seq=2 Ack=2 Win=4096 Len=0 TSval=2738417074 TSecr=3279063726
79	3.346376	fe80::8d0:28e0:5cc…	ff02::fb	MDNS	424	Standard query 0x0000 PTR _airplay._tcp.local, "QU" question PTR _airplay._tcp.local, "QU" questio
80	3.358448	192.168.1.1	192.168.1.14	DHCP	342	DHCP Offer - Transaction ID 0xb79829b
81	3.659053	2605:e000:1525:441…	2607:f8b0:400e:c09…	TCP	86	53803 → 5228 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=2738417552 TSecr=781073095
82	3.685082	Sagemcom_4f:46:ef	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/e8:ad:a6:4f:46:ea Cost = 0 Port = 0x8003
83	3.954568	2605:e000:1525:441…	2607:f8b0:400e:c09…	TCP	86	[TCP Retransmission] 53803 → 5228 [FIN, ACK] Seq=1 Ack=1 Win=4096 Len=0 TSval=2738417844 TSecr=781?
84	3.994496	2607:f8b0:400e:c09…	2605:e000:1525:441…	TCP	74	5228 → 53803 [RST] Seq=1 Win=0 Len=0
85	4.353915	fe80::8d0:28e0:5cc…	ff02::fb	MDNS	424	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _airplay._tcp.local, "QM" questio
86	4.361929	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xb79829b
87	4.368834	192.168.1.1	192.168.1.14	DHCP	342	DHCP ACK - Transaction ID 0xb79829b
88	4.369496	Apple_1b:1e:96	Broadcast	ARP	42	Who has 192.168.1.14? Tell 0.0.0.0
89	4.694750	Apple_1b:1e:96	Broadcast	ARP	42	Who has 192.168.1.14? Tell 0.0.0.0
90	5.015177	Apple_1b:1e:96	Broadcast	ARP	42	Who has 192.168.1.14? Tell 0.0.0.0
91	5.054854	fe80::8d0:28e0:5cc…	fe80::eaad:a6ff:fe…	ICMPv6	86	Neighbor Solicitation for fe80::eaad:a6ff:fe4f:46ea from 8c:85:90:1b:1e:96
92	5.056826	fe80::eaad:a6ff:fe…	fe80::8d0:28e0:5cc…	ICMPv6	78	Neighbor Advertisement fe80::eaad:a6ff:fe4f:46ea (rtr, sol)
93	5.340418	Apple_1b:1e:96	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.14 (Request)
94	5.665691	Apple_1b:1e:96	Broadcast	ARP	42	Gratuitous ARP for 192.168.1.14 (Request)
95	5.733011	Sagemcom_4f:46:ef	Spanning-tree-(for…	STP	60	Conf. Root = 32768/0/e8:ad:a6:4f:46:ea Cost = 0 Port = 0x8003