

Computer Networks 1

Lab 4b

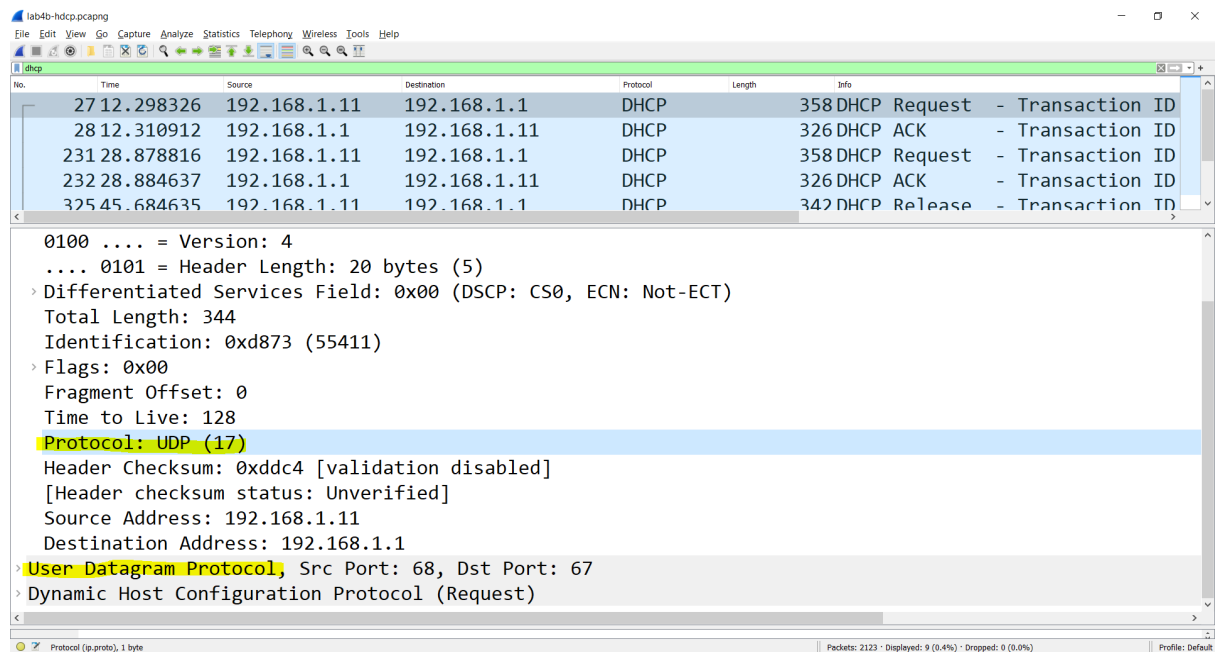
Wireshark Lab: DHCP v8.0

Student Name: Nguyễn Quý Hải

Student No.: 2052974

- Q1: Are DHCP messages sent over UDP or TCP?

Answer: DHCP messages sent over UDP.



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

Answer: (chưa trả lời)

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

Answer: Client MAC address: a4:97:b1:e3:90:0b

No.	Time	Source	Destination	Protocol	Length	Info
27	12.298326	192.168.1.11	192.168.1.1	DHCP	358	DHCP Request - Transaction ID
28	12.310912	192.168.1.1	192.168.1.11	DHCP	326	DHCP ACK - Transaction ID
231	28.878816	192.168.1.11	192.168.1.1	DHCP	358	DHCP Request - Transaction ID
232	28.884637	192.168.1.1	192.168.1.11	DHCP	326	DHCP ACK - Transaction ID
375	45.684635	192.168.1.11	192.168.1.1	DHCP	342	DHCP Release - Transaction ID

Dynamic Host Configuration Protocol (Request)

Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x73320d45
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.11
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
Client hardware address padding: 0000000000000000
Server host name not given

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

Answer: DHCP discover message: 1, DHCP request message: 3

- 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?

Answer: The purpose of the Transaction-ID field is to differentiate between the groups of messages.

lab1b-hdcp.capng

FileEditViewGoCaptureAnalysisStatisticsTelephonyWirelessToolsHelp

idhcp

No.	Destination	Protocol	Length	Info
2.168.1.11	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0x73320d45
2.168.1.1	192.168.1.11	DHCP	326	DHCP ACK - Transaction ID 0x73320d45
2.168.1.11	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0x8494516
2.168.1.1	192.168.1.11	DHCP	326	DHCP ACK - Transaction ID 0x8494516
2.168.1.11	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x5c2bdec4
0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xb9a40312
2.168.1.1	192.168.1.11	DHCP	326	DHCP Offer - Transaction ID 0xb9a40312
0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb9a40312
2.168.1.1	192.168.1.11	DHCP	326	DHCP ACK - Transaction ID 0xb9a40312

Seconds elapsed: 0

> Bootp flags: 0x0000 (Unicast)

Client IP address: 192.168.1.11

Your (client) IP address: 0.0.0.0

Next server IP address: 0.0.0.0

Relay agent IP address: 0.0.0.0

Client MAC address: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)

Client hardware address padding: 00000000000000000000

Server host name not given

- 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.

Answer:

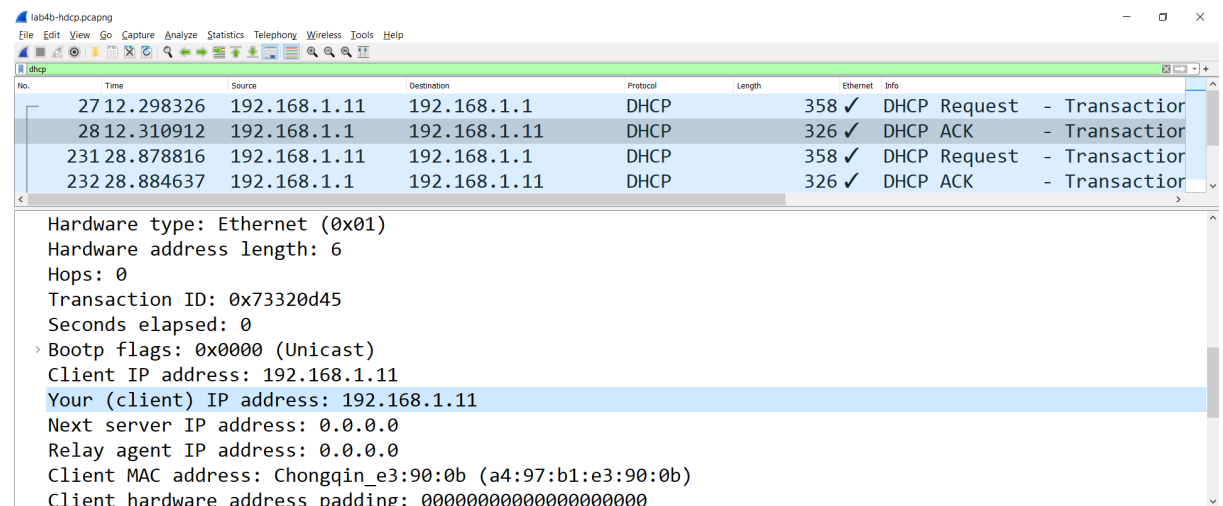
- Discover Src – 0.0.0.0, Dst – 255.255.255.255
- Offer Src – 192.168.1.1, Dst – 255.255.255.255
- Request Src – 0.0.0.0, Dst – 55.255.255.255
- ACK DHCP – 192.168.1.1, Dst – 255.255.255.255

- Q7. What is the IP address of your DHCP server?

Answer: 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.

Answer: The IP address which DHCP server is offering to my host in the DHCP Offer message is: 192.168.1.11. DHCP message contains address offered by server



No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
27	12.298326	192.168.1.11	192.168.1.1	DHCP	358	✓	DHCP Request - Transaction ID: 0x73320d45
28	12.310912	192.168.1.1	192.168.1.11	DHCP	326	✓	DHCP ACK - Transaction ID: 0x73320d45
231	28.878816	192.168.1.11	192.168.1.1	DHCP	358	✓	DHCP Request - Transaction ID: 0x73320d45
232	28.884637	192.168.1.1	192.168.1.11	DHCP	326	✓	DHCP ACK - Transaction ID: 0x73320d45

Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x73320d45
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.1.11
Your (client) IP address: 192.168.1.11
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
Client hardware address padding: 000000000000000000000000

- 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?

Answer: It is 0.0.0.0, and it exists in my experiment and the value is also 0.0.0.0

lab4b-hdcp.pcapng

No.	Time	Source	Destination	Protocol	Length	Info
27	12.298326	192.168.1.11	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0x7
28	12.310912	192.168.1.1	192.168.1.11	DHCP	326	DHCP ACK - Transaction ID 0x7
231	28.878816	192.168.1.11	192.168.1.1	DHCP	358	DHCP Request - Transaction ID 0x8
232	28.884637	192.168.1.1	192.168.1.11	DHCP	326	DHCP ACK - Transaction ID 0x8
325	45.684635	192.168.1.11	192.168.1.1	DHCP	342	DHCP Release - Transaction ID 0x5
606	54.056426	0.0.0.0	255.255.255.255	DHCP	344	DHCP Discover - Transaction ID 0xt
607	54.061072	192.168.1.1	192.168.1.11	DHCP	326	DHCP Offer - Transaction ID 0xt
608	54.061650	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xt
609	54.069143	192.168.1.1	192.168.1.11	DHCP	326	DHCP ACK - Transaction ID 0xt

> Bootp flags: 0x0000 (Unicast)
 Client IP address: 0.0.0.0
 Your (client) IP address: 0.0.0.0
 Next server IP address: 0.0.0.0
 Relay agent IP address: 0.0.0.0
 Client MAC address: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Root file name not given

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

Answer

The subnet mask line tells the client which subnet mask to use.

The router indicates where client should send messages by default

- 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?

Answer: The client accepts the IP address given in the offer message within the request message. After being offered the IP address 192.168.1.11 in the offer message, my client sent back a message further requesting that specific IP address.

lab4b-hdcp.pcapng

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
607	54.061072	192.168.1.1	192.168.1.11	DHCP	326	✓	DHCP Offer - Transaction
608	54.061650	0.0.0.0	255.255.255.255	DHCP	370	✓	DHCP Request - Transaction
609	54.069143	192.168.1.1	192.168.1.11	DHCP	326	✓	DHCP ACK - Transaction

Relay agent IP address: 0.0.0.0
Client MAC address: Chongqin_e3:90:0b (a4:97:b1:e3:90:0b)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Request)
> Option: (61) Client identifier
~ Option: (50) Requested IP Address (192.168.1.11)
Length: 4
Requested IP Address: 192.168.1.11
~ Option: (54) DHCP Server Identifier (192.168.1.1)

0120 a4 97 b1 e3 90 0b 32 04 c0 a8 01 0b 36 04 c0 a82.6..
0130 01 01 0c 0f 44 45 53 4b 54 4f 50 2d 46 36 54 43 ...DESK TOP-F6TC
0140 4b 31 35 51 12 00 00 00 44 45 53 4b 54 4f 50 2d K15Q... DESKTOP-
0150 46 36 54 43 4b 31 35 3c 08 4d 53 46 54 20 35 2e F6TK15<-MSFT 5.

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

Answer: The purpose of lease time is to tell the client how long they can use the specific IP address assigned by the server before they will have to be assigned a new one. In my experiment, it is 86400s (1 day)

lab4b-hdcp.pcapng

No.	Time	Source	Destination	Protocol	Length	Ethernet	Info
607	54.061072	192.168.1.1	192.168.1.11	DHCP	326	✓	DHCP Offer - Transaction
608	54.061650	0.0.0.0	255.255.255.255	DHCP	370	✓	DHCP Request - Transaction
609	54.069143	192.168.1.1	192.168.1.11	DHCP	326	✓	DHCP ACK - Transaction

Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (ACK)
> Option: (54) DHCP Server Identifier (192.168.1.1)
~ Option: (51) IP Address Lease Time
Length: 4
IP Address Lease Time: (86400s) 1 day
> Option: (1) Subnet Mask (255.255.255.0)
> Option: (3) Router
> Option: (6) Domain Name Server
> Option: (15) Domain Name

0110 00 00 00 00 00 00 63 82 53 63 35 01 05 36 04 c0c. Sc5..6..
0120 a8 01 01 33 04 00 01 51 80 01 04 ff ff ff 00 03 ...3...Q
0130 04 c0 a8 01 01 06 08 7b 1a 1a 1a 7b 17 17 0f{ ...{....
0140 04 48 6f 6d 65 ffHome.

- 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?

Answer: The purpose of the release message is to release the IP address back to the server. There is no verification that the release message has been received by the server. If the message is lost, the client releases the IP address, but the server will not reassign that address until the clients lease on the address expires.

- 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.

Answer: Yes, they appear to be broadcasts sent out by the network to build up the known IP addresses by the clients network.

