CSC358H5: Principles of Computer Networking — Winter 2025

Wireshark Lab 2: DHCP

Due Date: Sunday, March 16, 11:59 PM

1 What is DHCP?

We always know our own MAC address, because it's burned into the hardware. But, when a computer first joins a network, How does it obtain the information required for connecting to the Internet? First, let's see what information do we need.

- We need to be allocated an **IP address** so we can send and receive packets. Recall that IP addresses are allocated geographically. So, it cannot be burned into the hardware. Our IP address depends on which network we are connected to. While our IP address does not have to be globally unique, it must be unique in the local network we are connected to.
- We need the IP address of the router on the local network, so that we can send any non-local packets to the router. This router is commonly known as the **default gateway**.[1]
- What about local packets? Where should we send them to? There's no need to send them to the router. They are in our own local network and we know how to send a packet to a device in our local area network. Just simply send the packet directly to the MAC address of that device in the local network. The L2 switches will take care of it. But how do we know if an IP packet is local or non-local? We need to learn the **subnet mask** so that we can learn the range of local IP addresses.[2]
- What's the point of connecting to the internet if we cannot use it? We need to be able to translate Domain Names to IP addresses.So, we need to learn where the DNS recursive resolver is located for this network.

We could manually configure these values every time we first join the network. This is time-consuming, and the average Internet user probably has no idea how to configure these values manually.[3] The Dynamic Host Configuration Protocol (DHCP) allows new hosts to automatically learn these values (and possibly other useful information).

DHCP has four steps:

1. **DHCP Discover** - The client sends a broadcast **Discover** message to find a DHCP server.
2. **DHCP Offer** - Any DHCP server who can help would unicast an **Offer** (*i.e.*, IP address and subnet mask, gateway address, DNS address).
3. **DHCP Request** - The client sends a *broadcast* **Request** message to indicate which offer was accepted. This message is broadcasted to ensure all DHCP servers are notified of the accepted offer so that they do not assign conflicting IPs and to allow the rejected offers to be freed up for future clients..
4. **DHCP ACK** - The server sends an **Acknowledgment** confirming the request was granted.

In smaller networks, such as home networks, the router typically functions as the DHCP server. In larger networks, a dedicated machine may serve this role. Since DHCP operates within the local network, the server must be on the same network as the client. However, in large-scale networks, running a DHCP server on every router may not be ideal. Instead, local routers can forward DHCP requests to a centralized remote DHCP server that handles the protocol. DHCP servers listen on a fixed port, UDP port 67, for requests from new machines.

IP addresses are assigned to hosts on a temporary lease, typically lasting for a limited period (*e.g.*, hours or days). To continue using the address, the host must renew the lease. While an IP address is leased to a host,

[1] Why don't we need to obtain the MAC address of the default gateway? That's because we already know how to translate IP addresses to MAC addresses, *i.e.*, ARP.

[2] Given the mask, we can bitwise AND the mask with our own IP address to learn the local IP prefix.

[3] That said, manual configuration does sometimes work for machines like routers, which don't move around often.

the DHCP server cannot assign it to another client. Additionally, DHCP can be configured to always provide the same IP address to a specific host each time it connects or to assign a different temporary IP address upon each connection.

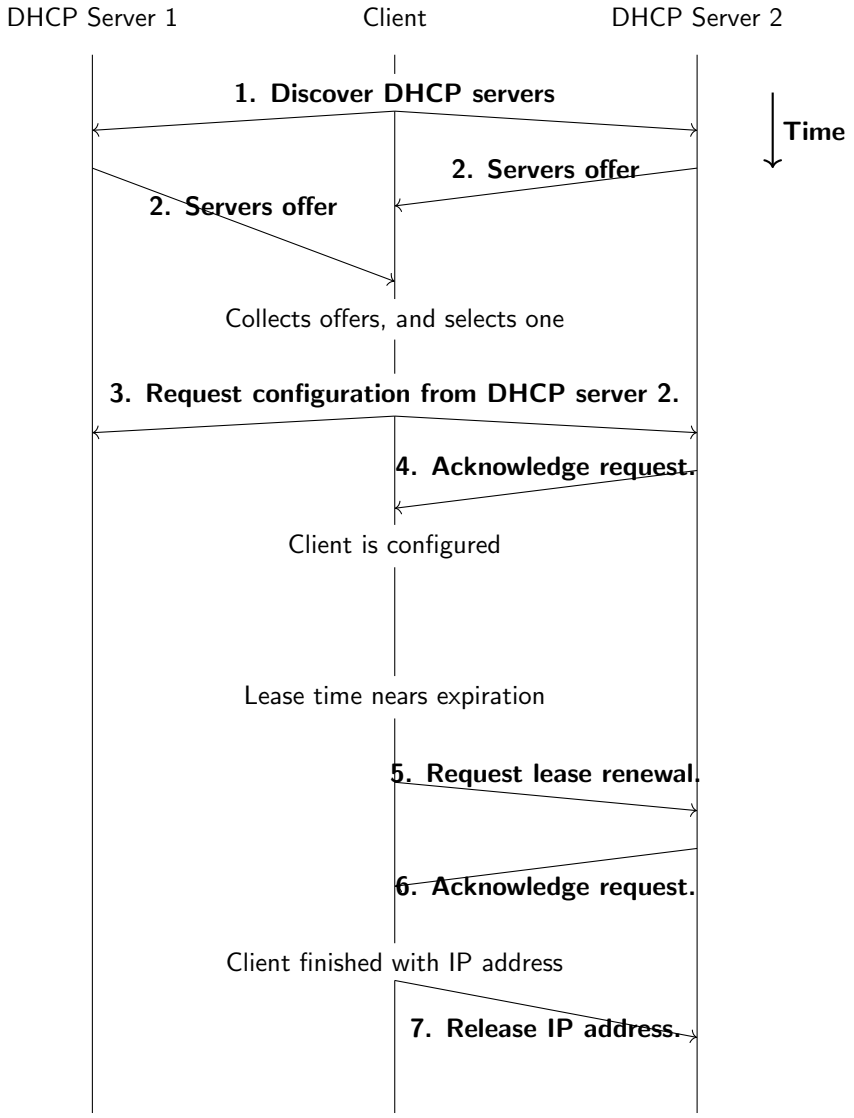

Figure 1: DHCP Client-Server Interaction

Note that DHCP is a Layer 7 application protocol, and it runs on top of UDP, which itself runs on top of IP. In step 1, it sends a packet with destination IP of 255.255.255.255 (all ones), which is the IPv4 broadcast address. When this packet is passed down to Layer 2, instead of translating this IP address using ARP, the IPv4 broadcast address is mapped to the Ethernet broadcast address of FF-FF-FF-FF-FF-FF (all ones). Then, the packet can get broadcast across the network at Layer 2. As the client does not have an IP address yet, it sets the source IP to be 0.0.0.0.

If there's no source IP, how do the DHCP servers know how to unicast the offers? The DHCP servers could either broadcast the offers, or use the client's MAC address to unicast the offers.

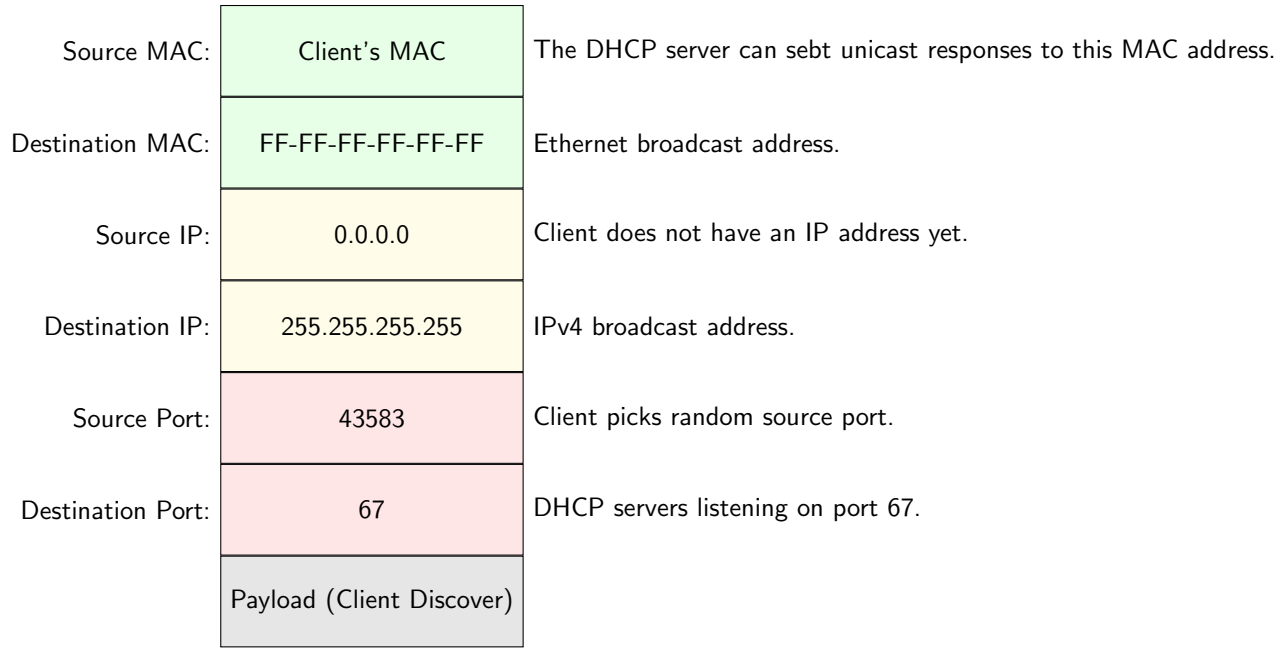

Figure 2: A DHCP discovery message.

2 Gathering a Packet Trace

This section is not required for you to complete the lab, but is encouraged for learning purposes. To setup for this exercise first disable the network on the interface en0, where the packets will be captured. The following commands can be run.

- **Linux:**

```
sudo ip addr flush en0
sudo dhclient -r
```

- **Windows:** `ipconfig /release`
- **Mac:** `sudo ipconfig set en0 none`

Now, begin the Wireshark capture. To see the DHCP packets, we must re-enable the network on the `en0` interface. Run the following commands to restore network connectivity:

- **Linux:** `sudo dhclient en0`
- **Windows:** `ipconfig /renew`
- **Mac:** `sudo ipconfig set en0 dhcp`

Now wireshark will capture the DHCP packets which can be found by adding the dhcp filter as shown in Figure 3.

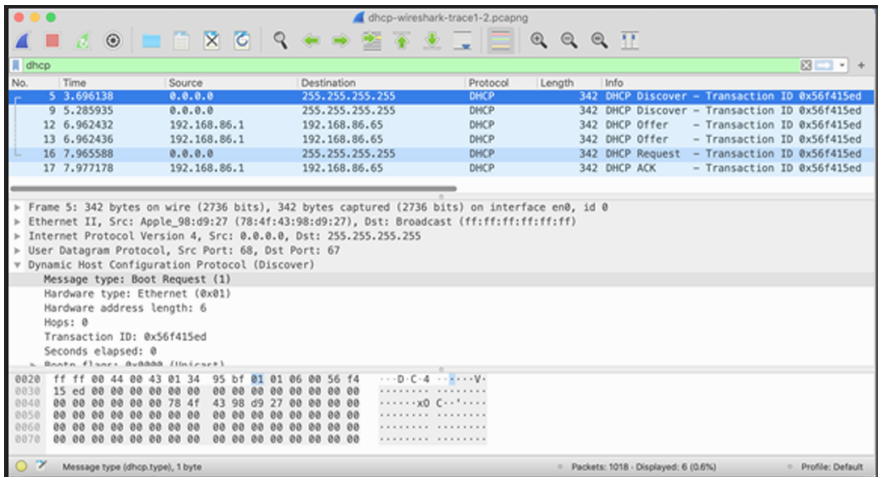

Figure 3: Wireshark Capture of DHCP Packets

3 DHCP Questions

Download `dhcp-wireshark-trace1-1.pcapng` from Quercus, available under the section Files/Wireshark Labs/Lab 2, and open it in Wireshark to answer the following questions.

3.1 DHCP Discover Message

Locate the IP datagram containing the first Discover message in your trace and answer the following:

Q1. Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?

Q2. What is the source IP address used in the IP datagram containing the Discover message?

Q3. What is the destination IP address used in the datagram containing the Discover message?

Q4. What is the value in the transaction ID field of this DHCP Discover message?

Q5. Inspect the options field in the DHCP Discover message. What are five pieces of information, listed under "Parameter Request List," that the client is requesting from the DHCP server as part of this DHCP transaction.

3.2 DHCP Offer Message

Locate the IP datagram containing the DHCP Offer message sent by a DHCP server in response to the Discover message.

Q6. How do you know that this Offer message is being sent in response to the DHCP Discover message?

Q7. What is the source IP address used in the IP datagram containing the Offer message?

Q8. What is the destination IP address used in the datagram containing the Offer message?

Q9. Inspect the options field in the DHCP Offer message. List five pieces of information that the DHCP server is providing to the DHCP client.

3.3 DHCP Request Message

Locate the IP datagram containing the first DHCP Request message in your trace.

Q10. What is the UDP source port number in the IP datagram containing the first DHCP Request message? What is the UDP destination port number?

Q11. What is the source IP address in the IP datagram containing this Request message?

Q12. What is the destination IP address used in the datagram containing this Request message?

Q13. What is the value in the transaction ID field of this DHCP Request message? Does it match the transaction IDs of the earlier Discover and Offer messages?

Q14. (Not for grades) Inspect the options field in the DHCP Request message and examine the `Parameter Request List`. Compare the entries in this list in the Request message with those in the earlier Discover message. What differences do you notice?

3.4 DHCP ACK Message

Locate the IP datagram containing the first DHCP ACK message in your trace.

Q15. What is the source IP address in the IP datagram containing this ACK message?

Q16. What is the destination IP address used in the datagram containing this ACK message?

Q17. What is the name of the field in the DHCP ACK message (as indicated in the Wireshark window) that contains the assigned client IP address?

Q18. For how many days has the DHCP server assigned this IP address to the client, *i.e.*, what is the "lease time"?

Q19. What is the IP address (returned by the DHCP server to the DHCP client in this DHCP ACK message) of the first-hop router on the default path from the client to the rest of the Internet?