

IT304

LAB 10

Understanding of DHCP using wireshark and packet tracer

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automate the process of configuring devices on IP networks, thus allowing them to use network services such as DNS, NTP, and any communication protocol based on UDP or TCP. DHCP is an enhancement of an older protocol called BOOTP.

1 Experiment

1. Begin by opening the Windows Command Prompt application (which can be found in your Accessories folder). Enter “ipconfig /release”. The executable for ipconfig is in C/windows/system32. This command releases your current IP address, so that your host’s IP address becomes 0.0.0.0.
2. Start up the Wireshark packet sniffer, as described in the introductory Wireshark lab and begin Wireshark packet capture.
3. Now go back to the Windows Command Prompt and enter “ipconfig /renew”. This instructs your host to obtain a network configuration, including a new IP address.
4. Wait until the “ipconfig /renew” has terminated. Then enter the same command “ipconfig /renew” again.
5. When the second “ipconfig /renew” terminates, enter the command “ipconfig/release” to release the previously-allocated IP address to your computer.
6. Finally, enter “ipconfig /renew” to again be allocated an IP address for your computer.
7. Stop Wireshark packet capture.

You should hand in a screen shot of the Command Prompt window. Whenever possible, when answering a question below, you should hand in a printout of the packet(s) within the trace that you used to answer the question asked. Annotate the printout to explain your answer. To print a packet, use File->Print, choose Selected packet only, choose Packet summary line, and select the minimum amount of packet detail that you need to answer the question.

2 Questions

1. Are DHCP messages sent over UDP or TCP?
2. 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, indicated the source and destination port numbers. Are the port numbers the same as in the example given in this lab assignment?
3. What is the link-layer (e.g., Ethernet) address of your host?

4. What values in the DHCP discover message differentiate this message from the DHCP request message?
5. 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?
6. 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.
7. What is the IP address of your DHCP server?
8. 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.
9. 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?
10. Explain the purpose of the router and subnet mask lines in the DHCP offer message.
11. In the example screenshots in this assignment, the host requests the offered IP address in the DHCP Request message. What happens in your own experiment?
12. Explain the purpose of the lease time. How long is the lease time in your experiment?
13. 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?
14. 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.

3 Experiment2: Implementing DHCP server in a router

1. Implement following topology in packet tracer

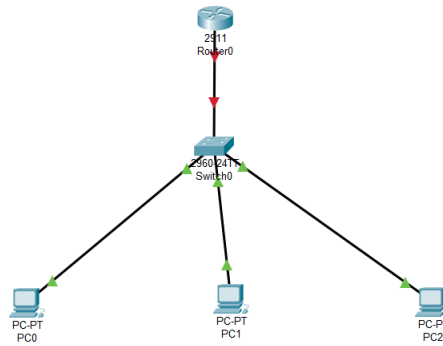


Figure 1: Caption

2. Set ip address of router as 192.168.1.1/24.
3. Turn on port of router
4. Run following code in router configuration

```
Router(config)#  
Router(config)#ip dhcp pool MY_LAN  
Router(dhcp-config)#network 192.168.1.0 255.255.255.0  
Router(dhcp-config)#default-router 192.168.1.1  
Router(dhcp-config)#dns-server 192.168.1.10
```

Figure 2: Caption

5. Also add following commands in router configuration
Router(config)#ip dhcp excluded-address 192.168.1.1 192.168.1.10
6. configure all PCs as following:
(a) Click PC1->Desktop->IP configuration. Then enable DHCP
7. Check which ip addresses are assigned to pc by DHCP server