**Hands-On Project 7-1: Examine a DHCP Boot Sequence**

**Objective:** Examine a DHCP boot sequence on a Windows client computer.

**Description:** This project shows you the different options that a client provides and requests when requesting an IP address from a DHCP server. In addition, you explore the different messages exchanged between a client and DHCP server.

1. Start Wireshark. (In Windows 7, click the Start button, point to All Programs, and then click Wireshark. In Windows 10, click the Start button, click All apps, and then click Wireshark. Alternately, use the Start menu search box [Windows 7] or the Search box on the taskbar [Windows 10], type Wireshark, and then click Wireshark in the resulting list.)
2. Click File on the menu bar, click Open, select the ch07\_Hands-on\_Project\_trace\_file\_ DHCPboot.pcapng, and click Open.
3. Click Packet #1 to open the decode window. Answer the following questions:
   1. What value is contained in the Client Identifier field?
   2. How can you verify that the Client Identifier value is the same as the client’s hardware address?
   3. What is the host name?
   4. Can this client accept unicast replies during the boot process?
   5. List the option codes (and their names) used in this DHCP packet.
4. Click through each packet trace in the summary window until you locate the DHCP Offer, Request, and ACK packets. Examine each DHCP packet. This is a normal DHCP boot sequence.
5. Close Wireshark.

**Hands-On Project 7-2: Examine DHCP Renewal, Rebind, and Reinitialize Sequences**

**Objective:** Review the process of DHCP renewal, rebind, and reinitialize sequences on an existing network-connected client.

**Description:** In this project, you will review the process of DHCP renewal, rebind, and reinitialize sequences by examining a trace file in Wireshark.

1. Start Wireshark. (In Windows 7, click the Start button, point to All Programs, and then click Wireshark. In Windows 10, click the Start button, click All apps, and then click Wireshark. Alternately, use the Start menu search box [Windows 7] or the Search box on the taskbar [Windows 10], type Wireshark, and then click Wireshark in the resulting list.)
2. Click File, click Open, select the ch07\_Hands-on\_Project\_trace\_file\_DHCPboot2.pcapng, and click Open.
3. Click Packet #3 to populate the decode window. Answer the following questions about this packet:
   1. Does this DHCP client already have an IP address?
   2. What message type is used in this packet?
   3. What is the purpose of this packet?
   4. Does the client receive a reply to this packet?
   5. What DHCP process is the client performing at this time?
4. Click through the packet capture summary window until you see Packet #5. Answer the following questions about this packet:
   1. Does this DHCP client still have an IP address?
   2. What is the message type used in this packet?
   3. What is the primary difference between this packet and Packet #3?
   4. Does the client receive a reply to this packet?
   5. What DHCP process is the client performing at this time?
5. Click through the packet capture summary window until you see Packet #10. Answer the following questions about this packet:
   1. Does this DHCP client still have an IP address?
   2. What is the message type used in this packet?
   3. Does the client receive a reply to this packet?
   4. What DHCP process is the client performing at this time?
6. Examine the remaining DHCP packets in the trace file. Did the client get the requested IP address?
7. Close Wireshark.

**Hands-On Project 7-3: Examine a DHCPv6 Boot Sequence**

**Objective:** Examine a DHCPv6 boot sequence on a Windows client computer.

**Description:** This project shows you the different options that a client provides and requests when requesting an IPv6 address from a DHCPv6 server. In addition, you explore the different messages exchanged between a client and a DHCPv6 server.

1. Start Wireshark. (In Windows 7, click the Start button, point to All Programs, and then click Wireshark. In Windows 10, click the Start button, click All apps, and then click Wireshark. Alternately, use the Start menu search box [Windows 7] or the Search box on the taskbar [Windows 10], type Wireshark, and then click Wireshark in the resulting list.)
2. Click File, click Open, select the ch07\_Hands-on\_Project\_trace\_file\_DHCPv6boot.pcapng, and click Open.
3. Click Packet #4 to populate the decode window. Answer the following questions about this packet:
   1. Does this DHCPv6 client have an IPv6 global unicast address?
   2. What message type is used in this packet?
   3. What is the host name? (Hint: Look for domain.)
   4. Does the client receive a reply to this packet?
   5. What DHCPv6 process is the client performing at this time?
4. Click through each packet trace in the summary window until you locate the DHCPv6 Solicit, Advertise, Request, and Reply packets. Examine each DHCPv6 packet. This is a normal DHCPv6 boot sequence.
   1. What is the packet number where the DHCPv6 provides the final approval for an IPv6 address, and what is that IPv6 address assigned to the client?
5. Which packet is the DAD verification process for the client’s global unicast address?
6. Close Wireshark.

Pyles, James; Carrell, Jeffrey L.; Tittel, Ed. Guide to TCP/IP: IPv6 and IPv4 (Page 432). Course Technology. Kindle Edition.