

# LAB-8

Name: Jashanpreet Singh

ID: 2018A7PS0134G

1) Show a round of execution of the DHCP protocol.

Filter = dhcp

Wireshark packet capture showing a DHCP transaction. The packet list shows four packets: 628 (DHCP Discover), 634 (DHCP Offer), 635 (DHCP Request), and 636 (DHCP ACK). The packet details for packet 628 show the Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (DHCP Discover) layers. The packet bytes show the hexadecimal representation of the DHCP Discover message.

No.	Time	Source	Destination	Protocol	Data length	Total Length	Info
628	2021-04-12 12:12:56.797608918	0.0.0.0	255.255.255.255	DHCP	328	328	DHCP Discover - Transaction ID 0x94614b78
634	2021-04-12 12:12:56.801382397	192.168.29.1	192.168.29.187	DHCP	328	328	DHCP Offer - Transaction ID 0x94614b78
635	2021-04-12 12:12:56.801709318	0.0.0.0	255.255.255.255	DHCP	328	328	DHCP Request - Transaction ID 0x94614b78
636	2021-04-12 12:12:56.805890284	192.168.29.1	192.168.29.187	DHCP	328	328	DHCP ACK - Transaction ID 0x94614b78

Frame 628: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface wlp0s20f3, id 0  
Ethernet II, Src: IntelCor\_e6:5b:c7 (c8:b6:f9:e6:5b:c7), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255  
User Datagram Protocol, Src Port: 68, Dst Port: 67  
Dynamic Host Configuration Protocol (Discover)

0000 ff ff ff ff ff ff c0 b6 f9 e6 5b c7 00 00 45 10 .....E  
0010 01 40 00 00 00 00 00 11 39 96 00 00 00 00 ff ff ..H.....9.....  
0020 ff ff 00 44 00 43 01 34 86 4b 01 01 06 00 94 61 ...D.C.4.K.....a  
0030 4b 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 KX.....[.....  
0040 00 00 00 00 00 00 c0 b6 f9 e6 5b c7 00 00 00 00 .....[.....  
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

DHCP server IP: 192.168.29.1

DHCP client IP: 192.168.29.187

This is found from dhcp offer since this is sent by dhcp server.

2) Show a round of execution of the ARP protocol.

Filter = arp

Wireshark packet capture showing ARP protocol execution. The packet list shows a series of ARP requests and replies. Packet 641 is highlighted, showing an ARP reply from the IntelCor\_e6:5b:c7 interface to the a8:da:0c:07:5d:af interface.

No.	Time	Source	Destination	Protocol	Data length	Total Length	Info
469	2021-04-12 12:12:50.038657398	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
479	2021-04-12 12:12:51.062705924	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
497	2021-04-12 12:12:52.086442550	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
557	2021-04-12 12:12:53.110370996	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
587	2021-04-12 12:12:54.134373910	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
600	2021-04-12 12:12:54.953621458	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
615	2021-04-12 12:12:55.966548523	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
640	2021-04-12 12:12:56.822887219	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.1? Tell 192.168.29.187
641	2021-04-12 12:12:56.824063620	a8:da:0c:07:5d:af	IntelCor_e6:5b:c7	ARP			192.168.29.1 is at a8:da:0c:07:5d:af
2145	2021-04-12 12:12:58.977391496	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
2624	2021-04-12 12:13:00.004898870	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
3116	2021-04-12 12:13:01.024907431	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
4084	2021-04-12 12:13:03.977948820	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
4451	2021-04-12 12:13:04.992974548	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
4720	2021-04-12 12:13:06.016983268	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
6118	2021-04-12 12:13:08.977450926	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
6618	2021-04-12 12:13:09.980977610	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187

Frame 641: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp0s20f3, id 0  
Ethernet II, Src: a8:da:0c:07:5d:af (a8:da:0c:07:5d:af), Dst: IntelCor\_e6:5b:c7 (c0:b6:f9:e6:5b:c7)  
Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: a8:da:0c:07:5d:af (a8:da:0c:07:5d:af)  
Sender IP address: 192.168.29.1  
Target MAC address: IntelCor\_e6:5b:c7 (c0:b6:f9:e6:5b:c7)  
Target IP address: 192.168.29.187

0000 c0 b6 f9 e6 5b c7 a8 da 0c 07 5d af 08 06 00 01 .....  
0010 08 00 06 04 00 02 a8 da 0c 07 5d af c0 a8 1d 01 .....  
0020 c0 b6 f9 e6 5b c7 c0 a8 1d bb .....  
.....

Address Resolution Protocol: Protocol Packets: 8167 · Displayed: 22 (0.3%) · Dropped: 0 (0.0%) Profile: Default

MAC Address of Replier = a8:da:0c:07:5d:af

3) Find the MAC address and the IP address of the Gateway router .

Filter = arp

Wireshark packet capture showing ARP traffic. The packet list shows frame 641 as an ARP reply from the gateway router. The packet details show the sender MAC as a8:da:0c:07:5d:af and the sender IP as 192.168.29.1. The packet bytes show the MAC address a8:da:0c:07:5d:af at offset 0000.

No.	Time	Source	Destination	Protocol	Data length	Total Length	Info
67	2021-04-12 12:12:46.113654137	a8:da:0c:07:5d:af	IntelCor_e6:5b:c7	ARP			Who has 192.168.29.187? Tell 192.168.29.1
291	2021-04-12 12:12:47.113714126	a8:da:0c:07:5d:af	IntelCor_e6:5b:c7	ARP			Who has 192.168.29.187? Tell 192.168.29.1
496	2021-04-12 12:12:48.113616832	a8:da:0c:07:5d:af	IntelCor_e6:5b:c7	ARP			Who has 192.168.29.187? Tell 192.168.29.1
499	2021-04-12 12:12:50.038657398	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
479	2021-04-12 12:12:51.062705924	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
497	2021-04-12 12:12:52.086442550	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
557	2021-04-12 12:12:53.118370996	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
587	2021-04-12 12:12:54.134373919	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
600	2021-04-12 12:12:54.953621458	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
615	2021-04-12 12:12:55.966548523	a8:da:0c:07:5d:af	Broadcast	ARP			Who has 192.168.29.187? Tell 192.168.29.1
640	2021-04-12 12:12:56.822887219	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.1? Tell 192.168.29.187
641	2021-04-12 12:12:56.824063620	a8:da:0c:07:5d:af	IntelCor_e6:5b:c7	ARP			192.168.29.1 is at a8:da:0c:07:5d:af
2145	2021-04-12 12:12:58.977391496	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
2624	2021-04-12 12:13:00.004898870	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
3116	2021-04-12 12:13:01.024907431	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
4084	2021-04-12 12:13:03.977948820	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187
4451	2021-04-12 12:13:04.992974548	IntelCor_e6:5b:c7	Broadcast	ARP			Who has 192.168.29.223? Tell 192.168.29.187

Frame 641: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface wlp0s20f3, id 0  
Ethernet II, Src: a8:da:0c:07:5d:af (a8:da:0c:07:5d:af), Dst: IntelCor\_e6:5b:c7 (c0:b6:f9:e6:5b:c7)  
Address Resolution Protocol (reply)  
Hardware type: Ethernet (1)  
Protocol type: IPv4 (0x0800)  
Hardware size: 6  
Protocol size: 4  
Opcode: reply (2)  
Sender MAC address: a8:da:0c:07:5d:af (a8:da:0c:07:5d:af)  
Sender IP address: 192.168.29.1  
Target MAC address: IntelCor\_e6:5b:c7 (c0:b6:f9:e6:5b:c7)  
Target IP address: 192.168.29.187

0000 c0 b6 f9 e6 5b c7 a8 da 0c 07 5d af 08 06 00 01 .....[...].  
0010 08 00 06 04 00 02 a8 da 0c 07 5d af c0 a8 1d 01 .....[...].  
0020 c0 b6 f9 e6 5b c7 c0 a8 1d bb .....[...]

Sender MAC address (arp.src\_hw\_mac), 6 bytes

Packets: 8167 · Displayed: 22 (0.3%) · Dropped: 0 (0.0%)

Profile: Default

Here the reply is given by router so the mac address and ip shown are of the gateway router.

MAC Address: a8:da:0c:07:5d:af  
IP Address: 192.168.29.1