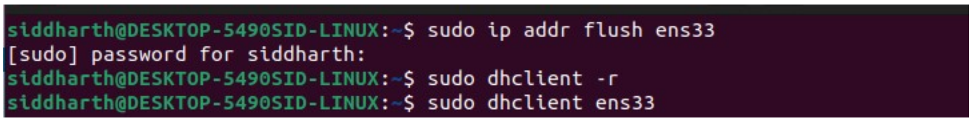
CS315: Lab Assignment 9

B Siddharth Prabhu
200010003@iitdh.ac.in

07 March 2023

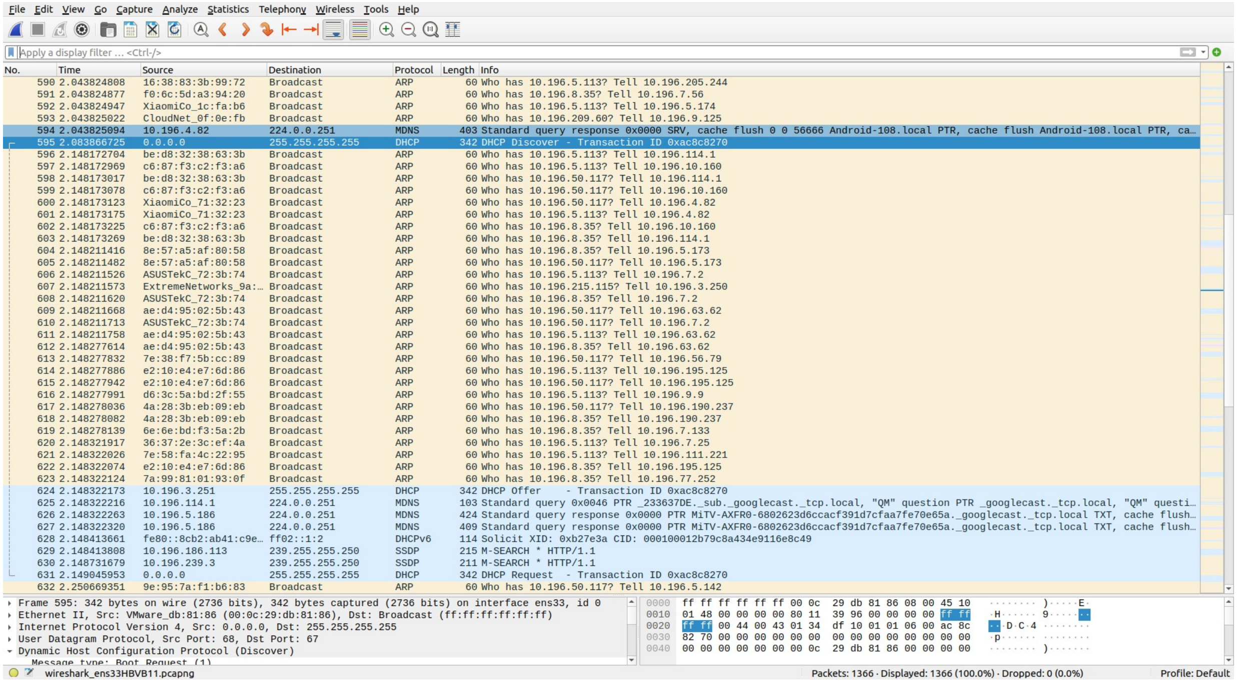
1 Gathering Packet Trace: Getting all DHCP Message Types

In this lab, we explore DHCP (Dynamic Host Configuration Protocol), which is used extensively in corporate, university and home-network wired and wireless LANs to dynamically assign IP addresses to hosts, as well as to configure other network configuration information. Note that this lab has been done on a Linux Virtual Machine. Below is a screenshot of the commands used to remove the existing IP address of the interface, and release any existing DHCP address leases, followed by a screenshot of the packet trace when IP address is requested and received.



```
siddharth@DESKTOP-5490SID-LINUX:~$ sudo ip addr flush ens33
[sudo] password for siddharth:
siddharth@DESKTOP-5490SID-LINUX:~$ sudo dhclient -r
siddharth@DESKTOP-5490SID-LINUX:~$ sudo dhclient ens33
```

Figure 1: Flush IP address and Request



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time        Source               Destination      Protocol Length Info
 590 2.043824808 16:38:83:3b:99:72    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.205.244
 591 2.043824877 f0:6c:5d:a3:94:20    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.7.56
 592 2.043824947 XiaomiCo_1c:fa:b6    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.5.174
 593 2.043825022 CloudNet_0f:0e:fb    Broadcast        ARP        60 Who has 10.196.209.60? Tell 10.196.9.125
 594 2.043825094 10.196.4.82          224.0.0.251      MDNS      403 Standard query response 0x0000 SRV, cache flush 0 0 56666 Android-108.local PTR, cache flush Android-108.local PTR, ca…
 595 2.083866725 0.0.0.0              255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0xac8c8270
 596 2.148172704 be:d8:32:38:63:3b    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.114.1
 597 2.148172969 c6:87:f3:c2:f3:a6    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.10.160
 598 2.148173017 be:d8:32:38:63:3b    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.114.1
 599 2.148173078 c6:87:f3:c2:f3:a6    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.10.160
 600 2.148173123 XiaomiCo_71:32:23    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.4.82
 601 2.148173175 XiaomiCo_71:32:23    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.4.82
 602 2.148173225 c6:87:f3:c2:f3:a6    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.10.160
 603 2.148173269 be:d8:32:38:63:3b    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.114.1
 604 2.148211416 8e:57:a5:af:80:58    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.5.173
 605 2.148211482 8e:57:a5:af:80:58    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.5.173
 606 2.148211526 ASUSTekC_72:3b:74    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.7.2
 607 2.148211573 ExtremeNetworks_9a:… Broadcast        ARP        60 Who has 10.196.215.115? Tell 10.196.3.250
 608 2.148211620 ASUSTekC_72:3b:74    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.7.2
 609 2.148211668 ae:d4:95:02:5b:43    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.63.62
 610 2.148211713 ASUSTekC_72:3b:74    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.7.2
 611 2.148211758 ae:d4:95:02:5b:43    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.63.62
 612 2.148277614 ae:d4:95:02:5b:43    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.63.62
 613 2.148277832 7e:38:f7:5b:cc:89    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.56.79
 614 2.148277886 e2:10:e4:e7:6d:86    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.195.125
 615 2.148277942 e2:10:e4:e7:6d:86    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.195.125
 616 2.148277991 d6:3c:5a:bd:2f:55    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.9.9
 617 2.148278036 4a:28:3b:eb:09:eb    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.190.237
 618 2.148278082 4a:28:3b:eb:09:eb    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.190.237
 619 2.148278139 6e:6e:bd:f3:5a:2b    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.7.133
 620 2.148321917 36:37:2e:3c:ef:4a    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.7.25
 621 2.148322026 7e:58:fa:4c:22:95    Broadcast        ARP        60 Who has 10.196.5.113? Tell 10.196.111.221
 622 2.148322074 e2:10:e4:e7:6d:86    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.195.125
 623 2.148322124 7a:99:81:01:93:0f    Broadcast        ARP        60 Who has 10.196.8.35? Tell 10.196.77.252
 624 2.148322173 10.196.3.251         255.255.255.255  DHCP      342 DHCP Offer    - Transaction ID 0xac8c8270
 625 2.148322216 10.196.114.1         224.0.0.251      MDNS      103 Standard query 0x0046 PTR _233637DE._sub._googlecast._tcp.local, "QM" question PTR _googlecast._tcp.local, "QM" questi…
 626 2.148322263 10.196.5.186         224.0.0.251      MDNS      424 Standard query response 0x0000 PTR MiTV-AXFR0-6802623d6ccacf391d7cfaa7fe70e65a._googlecast._tcp.local TXT, cache flush…
 627 2.148322320 10.196.5.186         224.0.0.251      MDNS      409 Standard query response 0x0000 PTR MiTV-AXFR0-6802623d6ccacf391d7cfaa7fe70e65a._googlecast._tcp.local TXT, cache flush…
 628 2.148413661 fe80::8cb2:ab41:c9e… ff02::1:2        DHCPv6    114 Solicit XID: 0xb27e3a CID: 000100012b79c8a434e9116e8c49
 629 2.148413808 10.196.186.113       239.255.255.250  SSDP      215 M-SEARCH * HTTP/1.1
 630 2.148731679 10.196.239.3         239.255.255.250  SSDP      211 M-SEARCH * HTTP/1.1
 631 2.149045953 0.0.0.0              255.255.255.255  DHCP      342 DHCP Request  - Transaction ID 0xac8c8270
 632 2.250669351 9e:95:7a:f1:b6:83    Broadcast        ARP        60 Who has 10.196.50.117? Tell 10.196.5.142
```

```
› Frame 595: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface ens33, id 0
› Ethernet II, Src: VMware_db:81:86 (00:0c:29:db:81:86), 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)
    Message type: Boot Request (1)
```

```
0000  ff ff ff ff ff ff 00 0c  29 db 81 86 08 00 45 10   ········ )·····E·
0010  01 48 00 00 00 00 80 11  39 96 00 00 00 00 ff ff   ·H······ 9·······
0020  ff ff 00 44 00 43 01 34  df 10 01 01 06 00 ac 8c   ···D·C·4 ········
0030  82 70 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·p······ ········
0040  00 00 00 00 00 00 00 0c  29 db 81 86 00 00 00 00   ········ )·······
```

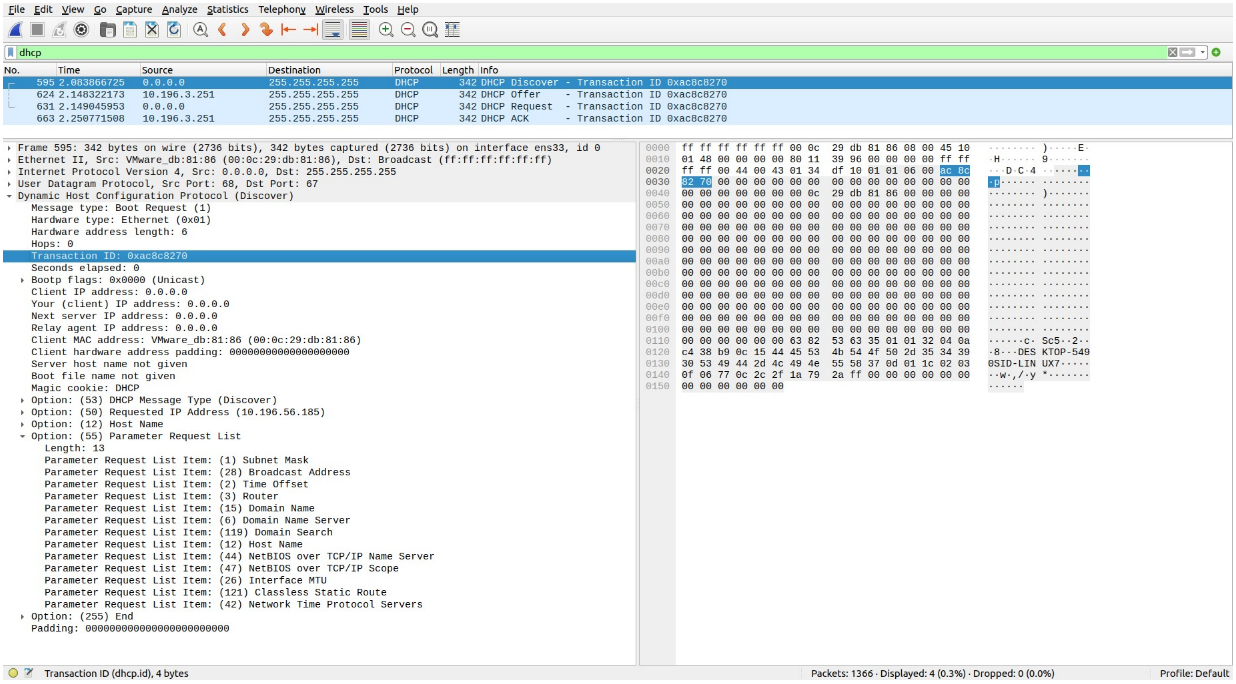
wireshark_ens33HBVB11.pcapng
Packets: 1366 · Displayed: 1366 (100.0%) · Dropped: 0 (0.0%)
Profile: Default

Figure 2: Packet Trace with DHCP

Then, we can filter out all DHCP messages by entering 'dhcp' in the display filter field.

2 Exploring DHCP

Firstly, let's focus on the **DHCP Discover** message. The packet details for the same are shown in Figure (3).



```
No.  Time           Source        Destination      Protocol  Length Info
 595 2.083866725    0.0.0.0       255.255.255.255  DHCP      342 DHCP Discover - Transaction ID 0xac8c8270
 624 2.148322173    10.196.3.251  255.255.255.255  DHCP      342 DHCP Offer    - Transaction ID 0xac8c8270
 631 2.149045953    0.0.0.0       255.255.255.255  DHCP      342 DHCP Request  - Transaction ID 0xac8c8270
 663 2.250771508    10.196.3.251  255.255.255.255  DHCP      342 DHCP ACK      - Transaction ID 0xac8c8270
```

```
› Frame 595: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface ens33, id 0
› Ethernet II, Src: VMware_db:81:86 (00:0c:29:db:81:86), 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)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xac8c8270
    Seconds elapsed: 0
  › 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: VMware_db:81:86 (00:0c:29:db:81:86)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  › Option: (53) DHCP Message Type (Discover)
  › Option: (50) Requested IP Address (10.196.56.185)
  › Option: (12) Host Name
  ⌄ Option: (55) Parameter Request List
      Length: 13
      Parameter Request List Item: (1) Subnet Mask
      Parameter Request List Item: (28) Broadcast Address
      Parameter Request List Item: (2) Time Offset
      Parameter Request List Item: (3) Router
      Parameter Request List Item: (15) Domain Name
      Parameter Request List Item: (6) Domain Name Server
      Parameter Request List Item: (119) Domain Search
      Parameter Request List Item: (12) Host Name
      Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
      Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
      Parameter Request List Item: (26) Interface MTU
      Parameter Request List Item: (121) Classless Static Route
      Parameter Request List Item: (42) Network Time Protocol Servers
  › Option: (255) End
    Padding: 000000000000000000000000
```

```
0000  ff ff ff ff ff ff 00 0c  29 db 81 86 08 00 45 10   ········ )·····E·
0010  01 48 00 00 00 00 80 11  39 96 00 00 00 00 ff ff   ·H······ 9·······
0020  ff ff 00 44 00 43 01 34  df 10 01 01 06 00 ac 8c   ···D·C·4 ········
0030  82 70 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·p······ ········
0040  00 00 00 00 00 00 00 0c  29 db 81 86 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   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 01 32 04 0a   ······c· Sc5··2··
0120  c4 38 b9 0c 15 44 45 53  4b 54 4f 50 2d 35 34 39   ·8···DES KTOP-549
0130  30 53 49 44 2d 4c 49 4e  55 58 37 0d 01 1c 02 03   0SID-LIN UX7·····
0140  0f 06 77 0c 2c 2f 1a 79  2a ff 00 00 00 00 00 00   ··w·,/·y *·······
0150  00 00 00 00 00 00                                  ······
```

Transaction ID (dhcp.id), 4 bytes   Packets: 1366 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%)   Profile: Default

Figure 3: Packet Details for DHCP Discover Packet

(1) Is this DHCP Discover message sent out using UDP or TCP as the underlying transport protocol?

The DHCP Discover message is sent out using **UDP (User Datagram Protocol)** as the underlying transport layer protocol. DHCP requests and responses can be quite small, so using UDP instead of TCP helps to conserve bandwidth.

(2) What is the source IP address used in the IP datagram containing the Discover message? Is there anything special about this address? Explain.

The source IP address used in the IP datagram containing the Discover message is `0.0.0.0` . The host uses 0.0.0.0 as its own source address in IP since it has not yet been assigned an address.

(3) What is the destination IP address used in the datagram containing the Discover message. Is there anything special about this address? Explain.

The destination IP address used in the IP datagram containing the Discover message is `255.255.255.255` . This IP address is used when the host broadcasts the DHCPDISCOVER message on the subnet. When a DHCP server receives such a message, it replies to it with a DHCPOFFER message; other devices ignore the broadcast. Also, routers do not forward this message to any external network.

(4) What is the value in the transaction ID field of this DHCP Discover message?

The value in the transaction ID field of this DHCP Discover message is `0xac8c8270` .

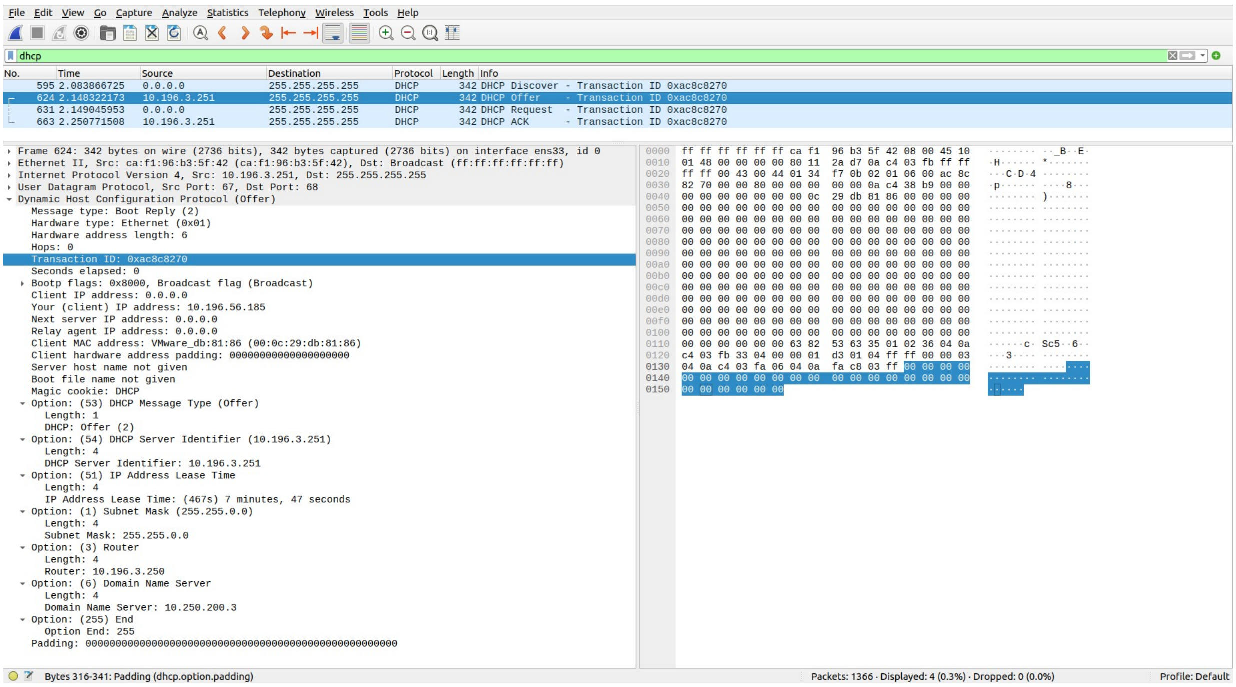
(5) What are five pieces of information (beyond an IP address) that the client is suggesting or requesting to receive from the DHCP server as part of this DHCP transaction?

Five pieces of information that the client is seen to be requesting to receive from the DHCP server as part of the DHCP transaction are as follows:

- Subnet Mask
- Router
- Domain Name Server
- Network Time Protocol Servers
- Classless Static Route

Others include: NetBIOS over TCP/IP Scope, NetBIOS over TCP/IP Name Server, Time Offset, Domain Name, Domain Search, etc.

Now, let's look at the **DHCP Offer** message. The packet details for the same are shown in Figure (4) below.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp

```
No.    Time          Source          Destination       Protocol  Length  Info
   595 2.083866725   0.0.0.0         255.255.255.255   DHCP         342 DHCP Discover - Transaction ID 0xac8c8270
   624 2.148322173   10.196.3.251    255.255.255.255   DHCP         342 DHCP Offer    - Transaction ID 0xac8c8270
   631 2.149045953   0.0.0.0         255.255.255.255   DHCP         342 DHCP Request  - Transaction ID 0xac8c8270
   663 2.250771508   10.196.3.251    255.255.255.255   DHCP         342 DHCP ACK      - Transaction ID 0xac8c8270
```

```
› Frame 624: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface ens33, id 0
› Ethernet II, Src: ca:f1:96:b3:5f:42 (ca:f1:96:b3:5f:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Internet Protocol Version 4, Src: 10.196.3.251, Dst: 255.255.255.255
› User Datagram Protocol, Src Port: 67, Dst Port: 68
▾ Dynamic Host Configuration Protocol (Offer)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xac8c8270
    Seconds elapsed: 0
  › Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.196.56.185
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: VMware_db:81:86 (00:0c:29:db:81:86)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▾ Option: (53) DHCP Message Type (Offer)
      Length: 1
      DHCP: Offer (2)
  ▾ Option: (54) DHCP Server Identifier (10.196.3.251)
      Length: 4
      DHCP Server Identifier: 10.196.3.251
  ▾ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (467s) 7 minutes, 47 seconds
  ▾ Option: (1) Subnet Mask (255.255.0.0)
      Length: 4
      Subnet Mask: 255.255.0.0
  ▾ Option: (3) Router
      Length: 4
      Router: 10.196.3.250
  ▾ Option: (6) Domain Name Server
      Length: 4
      Domain Name Server: 10.250.200.3
  ▾ Option: (255) End
      Option End: 255
    Padding: 000000000000000000000000000000000000000000000000000
```

```
0000  ff ff ff ff ff ff ca f1  96 b3 5f 42 08 00 45 10   ········ ··_B··E·
0010  01 48 00 00 00 00 80 11  2a d7 0a c4 03 fb ff ff   ·H······ *·······
0020  ff ff 00 43 00 44 01 34  f7 0b 02 01 06 00 ac 8c   ···C·D·4 ········
0030  82 70 00 00 80 00 00 00  00 00 0a c4 38 b9 00 00   ·p······ ····8···
0040  00 00 00 00 00 00 00 0c  29 db 81 86 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   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 02 36 04 0a   ······c· Sc5··6··
0120  c4 03 fb 33 04 00 00 01  d3 01 04 ff ff 00 00 03   ···3···· ········
0130  04 0a c4 03 fa 06 04 0a  fa c8 03 ff 00 00 00 00   ········ ········
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0150  00 00 00 00 00 00                                  ······
```

```
Bytes 316-341: Padding (dhcp.option.padding)        Packets: 1366 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%)        Profile: Default
```

Figure 4: Packet Details for DHCP Offer Packet

(6) How do you know that this Offer message is being sent in response to the DHCP Discover message you studied in questions 1-5 above?

We can conclude that this Offer message is being sent in response to the DHCP Discover message, since the transaction ID (0xac8c8270) of the DHCP Offer message is the identical to that of the Discover message used in questions 1-5 above.

(7) What is the source IP address used in the IP datagram containing the Offer message? Is there anything special about this address? Explain.

The source IP address used in the IP datagram containing the DHCP Offer message is `10.196.3.251` . This is same as the DHCP Server identifier. This is required since there may be multiple DHCP servers in the network, so the client must know which server is sending the offer message.

(8) What is the destination IP address used in the datagram containing the Offer message? Is there anything special about this address? Explain.

The destination IP address used in the IP datagram containing the DHCP Offer message is `255.255.255.255` . This means that the DHCP server is broadcasting the DHCP Offer message as well. This is because the client doesn't have an assigned IP address yet. The client understands that the Offer is meant for it due to the transaction ID being the same.

(9) Now inspect the options field in the DHCP Offer message. What are five pieces of information that the DHCP server is providing to the DHCP client in the DHCP Offer message?

The information that the DHCP server is providing to the DHCP client in the DHCP Offer message is as follows:

- DHCP Server Identifier (10.196.3.251)
- IP Address Lease Time (467 seconds)
- Subnet Mask (255.255.0.0)
- Router (10.196.3.250)
- Domain Name Server (10.250.200.3)

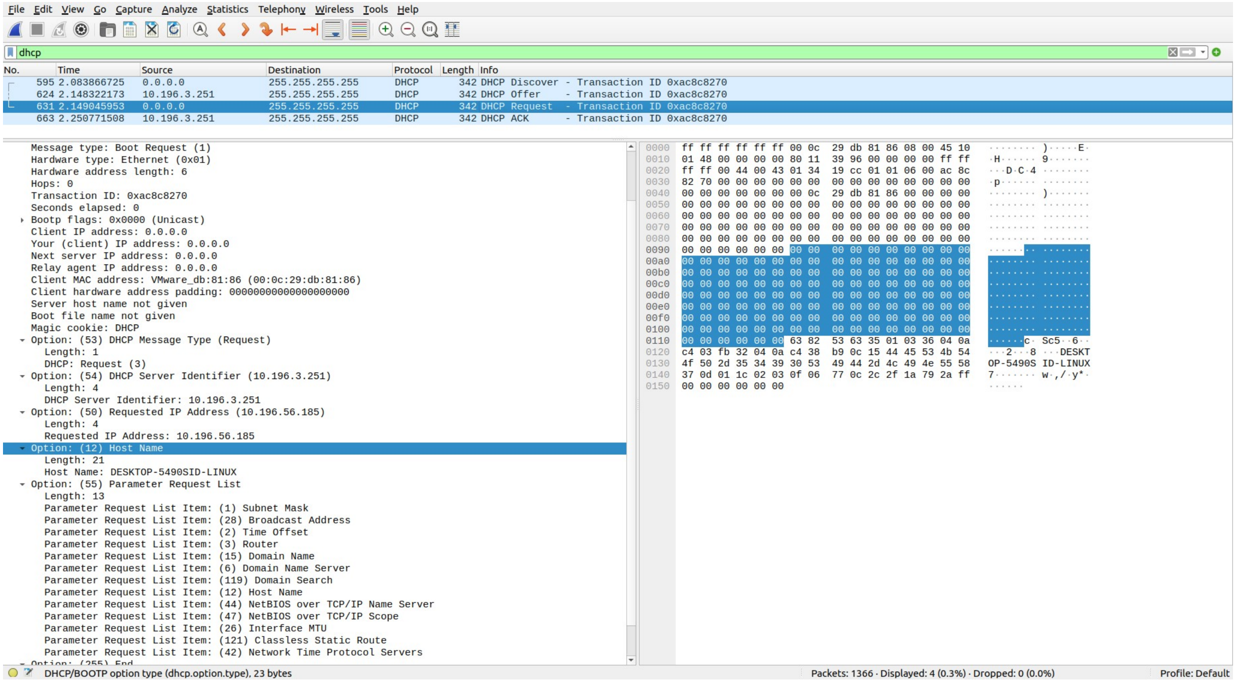
The client may have received OFFERs from multiple DHCP servers and so a second phase is needed, with two more mandatory messages – the client-to-server DHCP Request message, and the server-to-client DHCP ACK message is needed. But at least the client knows there is at least one DHCP server out there! So, let's take a look at the **DHCP Request** message, remembering that although we've already seen a Discover message in our trace, that is not always the case when a DHCP request message is sent. (Refer to Figure (5) for the Packet Details of the DHCP Request message.)

(10) What is the UDP source port number in the IP datagram containing the first DHCP Request message in your trace? What is the UDP destination port number being used?

The UDP source port number in the IP datagram containing the first DHCP Request message is `68` . The UDP destination port number being used is `67` .

(11) What is the source IP address in the IP datagram containing this Request message? Is there anything special about this address? Explain.

The source IP address used in the IP datagram containing the Request message is `0.0.0.0` . The host uses 0.0.0.0 as its own source address in IP since it still has not yet been assigned an address.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
dhcp
```

```
No.   Time         Source         Destination      Protocol Length Info
  595 2.083866725  0.0.0.0        255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0xac8c8270
  624 2.148322173  10.196.3.251   255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0xac8c8270
  631 2.149045953  0.0.0.0        255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0xac8c8270
  663 2.250771508  10.196.3.251   255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xac8c8270
```

```
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xac8c8270
    Seconds elapsed: 0
  ▸ 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: VMware_db:81:86 (00:0c:29:db:81:86)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▾ Option: (53) DHCP Message Type (Request)
      Length: 1
      DHCP: Request (3)
  ▾ Option: (54) DHCP Server Identifier (10.196.3.251)
      Length: 4
      DHCP Server Identifier: 10.196.3.251
  ▾ Option: (50) Requested IP Address (10.196.56.185)
      Length: 4
      Requested IP Address: 10.196.56.185
  ▾ Option: (12) Host Name
      Length: 21
      Host Name: DESKTOP-5490SID-LINUX
  ▾ Option: (55) Parameter Request List
      Length: 13
      Parameter Request List Item: (1) Subnet Mask
      Parameter Request List Item: (28) Broadcast Address
      Parameter Request List Item: (2) Time Offset
      Parameter Request List Item: (3) Router
      Parameter Request List Item: (15) Domain Name
      Parameter Request List Item: (6) Domain Name Server
      Parameter Request List Item: (119) Domain Search
      Parameter Request List Item: (12) Host Name
      Parameter Request List Item: (44) NetBIOS over TCP/IP Name Server
      Parameter Request List Item: (47) NetBIOS over TCP/IP Scope
      Parameter Request List Item: (26) Interface MTU
      Parameter Request List Item: (121) Classless Static Route
      Parameter Request List Item: (42) Network Time Protocol Servers
  ▾ Option: (255) End
```

```
0000  ff ff ff ff ff ff 00 0c  29 db 81 86 08 00 45 10   ········ )·····E·
0010  01 48 00 00 00 00 80 11  39 96 00 00 00 00 ff ff   ·H······ 9·······
0020  ff ff 00 44 00 43 01 34  19 cc 01 01 06 00 ac 8c   ···D·C·4 ········
0030  82 70 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ·p······ ········
0040  00 00 00 00 00 00 00 0c  29 db 81 86 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   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 36 04 0a   ······c· Sc5··6··
0120  c4 03 fb 32 04 0a c4 38  b9 0c 15 44 45 53 4b 54   ···2···8 ···DESKT
0130  4f 50 2d 35 34 39 30 53  49 44 2d 4c 49 4e 55 58   OP-5490S ID-LINUX
0140  37 0d 01 1c 02 03 0f 06  77 0c 2c 2f 1a 79 2a ff   7······· w·,/·y*·
0150  00 00 00 00 00 00                                  ······
```

DHCP/BOOTP option type (dhcp.option.type), 23 bytes

Packets: 1366 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%)

Profile: Default

Figure 5: Packet Details for DHCP Request Packet

(12) What is the destination IP address used in the datagram containing this Request message. Is there anything special about this address? Explain.

The destination IP address used in the IP datagram containing the Request message is `255.255.255.255` . This IP address is used when the host broadcasts the DHCPREQUEST message on the subnet, letting all DHCP servers know which one the client has chosen to get serviced by.

(13) 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?

The value in the transaction ID field of this DHCP Request message is `0xac8c8270` . Yes, it matches the transaction IDs of the earlier Discover and Offer messages.

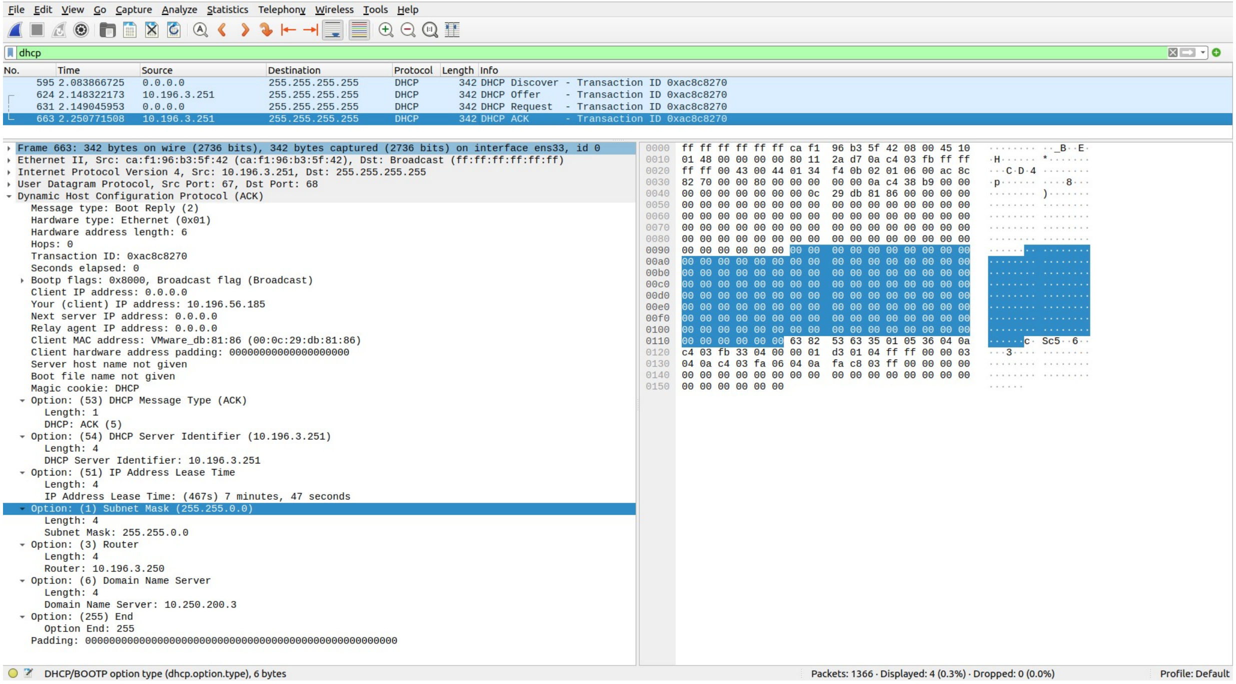
(14) What differences do you see between the entries in the 'parameter request list' option in this Request message and the same list option in the earlier Discover message?

There are **no differences** in the 'parameter request list' option in this Request message and the same list option in the earlier Discover message.

Lastly, let's look at the DHCP ACK message. This is the last message in the IP address allocation procedure, and the packet details of the same are in Figure (6).

(15) What is the source IP address in the IP datagram containing this ACK message? Is there anything special about this address? Explain.

The source IP address used in the IP datagram containing the DHCP ACK message is `10.196.3.251` . This is same as the DHCP Server identifier.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dhcp

```
No.     Time         Source         Destination      Protocol Length Info
    595 2.083866725  0.0.0.0        255.255.255.255  DHCP     342 DHCP Discover - Transaction ID 0xac8c8270
    624 2.148322173  10.196.3.251   255.255.255.255  DHCP     342 DHCP Offer    - Transaction ID 0xac8c8270
    631 2.149045953  0.0.0.0        255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0xac8c8270
    663 2.250771508  10.196.3.251   255.255.255.255  DHCP     342 DHCP ACK      - Transaction ID 0xac8c8270
```

```
› Frame 663: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface ens33, id 0
› Ethernet II, Src: ca:f1:96:b3:5f:42 (ca:f1:96:b3:5f:42), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Internet Protocol Version 4, Src: 10.196.3.251, Dst: 255.255.255.255
› User Datagram Protocol, Src Port: 67, Dst Port: 68
⌄ Dynamic Host Configuration Protocol (ACK)
    Message type: Boot Reply (2)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xac8c8270
    Seconds elapsed: 0
  › Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 10.196.56.185
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: VMware_db:81:86 (00:0c:29:db:81:86)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⌄ Option: (53) DHCP Message Type (ACK)
      Length: 1
      DHCP: ACK (5)
  ⌄ Option: (54) DHCP Server Identifier (10.196.3.251)
      Length: 4
      DHCP Server Identifier: 10.196.3.251
  ⌄ Option: (51) IP Address Lease Time
      Length: 4
      IP Address Lease Time: (467s) 7 minutes, 47 seconds
  ⌄ Option: (1) Subnet Mask (255.255.0.0)
      Length: 4
      Subnet Mask: 255.255.0.0
  ⌄ Option: (3) Router
      Length: 4
      Router: 10.196.3.250
  ⌄ Option: (6) Domain Name Server
      Length: 4
      Domain Name Server: 10.250.200.3
  ⌄ Option: (255) End
      Option End: 255
    Padding: 000000000000000000000000000000000000000000000000000000
```

```
0000  ff ff ff ff ff ff ca f1  96 b3 5f 42 08 00 45 10   ········ ··_B··E·
0010  01 48 00 00 00 00 80 11  2a d7 0a c4 03 fb ff ff   ·H······ *·······
0020  ff ff 00 43 00 44 01 34  f4 0b 02 01 06 00 ac 8c   ···C·D·4 ········
0030  82 70 00 00 80 00 00 00  00 00 0a c4 38 b9 00 00   ·p······ ····8···
0040  00 00 00 00 00 00 00 0c  29 db 81 86 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   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 36 04 0a   ······c· Sc5··6··
0120  c4 03 fb 33 04 00 00 01  d3 01 04 ff ff 00 00 03   ···3···· ········
0130  04 0a c4 03 fa 06 04 0a  fa c8 03 ff 00 00 00 00   ········ ········
0140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0150  00 00 00 00 00 00                                  ······
```

DHCP/BOOTP option type (dhcp.option.type), 6 bytes   Packets: 1366 · Displayed: 4 (0.3%) · Dropped: 0 (0.0%)   Profile: Default

Figure 6: Packet Details for DHCP ACK Packet

(16) What is the destination IP address used in the datagram containing this ACK message. Is there anything special about this address? Explain.

The destination IP address used in the IP datagram containing the ACK message is `255.255.255.255`. This IP address is used by the DHCP Server to broadcast the message, since the client still doesn't have an IP address of its own, and from here on out, the client will be referred to using the IP address assigned to it in this message.

(17) 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?

The name of the field in the DHCP ACK message that contains the assigned client IP address is `Your (client) IP address` and can be referred in the display filter field using `dhcp.ip.your`.

(18) For how long a time (the so-called "lease time") has the DHCP server assigned this IP address to the client?

The DHCP server assigned this IP address to the client for a duration of **467 seconds** (7 minutes, 47 seconds). This information is in Option (51), which is called 'IP Address Lease Time'.

(19) 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?

The IP address of the first-hop router on the default path from the client to the rest of the Internet is found to be `10.196.3.250`. This information is in Option (3), which is called 'Router'.