



LAB 2 DHCP (Dynamic Host Configuration Protocol)

CMPE 208: NETWORK ARCHITECTURE AND PROTOCOL

Prof. Shai Silberman

Submitted by

Team 12

Team Members

Akash Kumar Athghara

akash.athghara@sjsu.edu
010757929

Kshama Shalini

kshama.shalini@sjsu.edu
010763792

Gunveet Singh Arora

gunveet.singh@sjsu.edu
010641904

Sashank Malladi

sashank.malladi@sjsu.edu
010466651

Contribution by each team member

Akash Kumar Athghara: Packet Format, Sessions and Signalling Records

Gunveet Singh Arora: Introduction, Overview, Lab setup, What is DHCP and DHCP Handshake

Kshama Shalini: How DHCP works, Protocol Components, DHCP Snooping and Standards.

Sashank Malladi: QoS, Packet Header and Conclusion.

Lab Setup

In this Lab Setup, we use a windows host machine and a Guest Linux Virtual Machines to perform the operations required.

On the Linux Virtual Machines we install **WIRESHARK** which is a free open source software to capture and examine the packet trace. Wireshark is used for network troubleshooting analysis and Education. A packet capture includes time stamped to every packet. Wireshark provides a graphical UI that helps us to capture the sequence of packets and understand the bit operation. It color-codes packets by their type, and has an inbuilt feature to filter and analyze packets to investigate the behavior of network protocols.

Dhclient:

A dhclient provides the means for configuring one or multiple network interfaces using the Dynamic Host Configuration Protocol(DHCP), BOOTP protocol, or if these protocols fail, by statically assigning an address.

Ifconfig(linux):

In this lab we use ifconfig(linux) to check the IPv4/IPv6 address, subnet mask, Default gateway address of a computer. Overall it provides the network state of the computer. It is preinstalled into the operating system.

```
gunveet@gunveet-VirtualBox: ~  
gunveet@gunveet-VirtualBox:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:e6:22:21  
          inet addr:10.0.0.195  Bcast:10.0.0.255  Mask:255.255.  
255.0  
          inet6 addr: 2601:646:8501:5d70:a00:27ff:fee6:2221/64  
Scope:Global  
          inet6 addr: 2601:646:8501:5d70:9809:9aea:c012:2054/64  
Scope:Global  
          inet6 addr: fe80::a00:27ff:fee6:2221/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
RX packets:1070 errors:0 dropped:0 overruns:0 frame:0  
TX packets:472 errors:0 dropped:0 overruns:0 carrier:  
0  
collisions:0 txqueuelen:1000  
RX bytes:839522 (839.5 KB)  TX bytes:59562 (59.5 KB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING  MTU:65536  Metric:1  
RX packets:275 errors:0 dropped:0 overruns:0 frame:0  
TX packets:275 errors:0 dropped:0 overruns:0 carrier:  
0
```

DHCP Commands in Windows:

- To display IP configuration:

\system32> ipconfig

```
Command Prompt  
C:\Users\Gunveet>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Ethernet:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
  
Wireless LAN adapter Local Area Connection* 2:  
  
Media State . . . . . : Media disconnected  
Connection-specific DNS Suffix . :  
  
Ethernet adapter VirtualBox Host-Only Network:  
  
Connection-specific DNS Suffix . :  
Link-local IPv6 Address . . . . . : fe80::2c74:d14d:596c:51b6%13  
IPv4 Address. . . . . : 192.168.56.1  
Subnet Mask . . . . . : 255.255.255.0  
Default Gateway . . . . . :  
  
Wireless LAN adapter Wi-Fi:  
  
Connection-specific DNS Suffix . : hsd1.ca.comcast.net  
IPv6 Address. . . . . : 2601:646:8501:5d70:fd60:e9bf:5b65:1272  
Temporary IPv6 Address. . . . . : 2601:646:8501:5d70:c8b2:27dd:f41e:8a3b  
Link-local IPv6 Address . . . . . : fe80::fd60:e9bf:5b65:1272%9  
IPv4 Address. . . . . : 10.0.0.104
```

- To release IP address:

\system32> ipconfig /release

```

Command Prompt
C:\Users\Gunveet>ipconfig /release

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::2c74:d14d:596c:51b6%13
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2601:646:8501:5d70:fd60:e9bf:5b65:1272
    Temporary IPv6 Address. . . . . : 2601:646:8501:5d70:c8b2:27dd:f41e:8a3b

```

- To assign IP address

\system32> ipconfig /renew

```

Command Prompt
C:\Users\Gunveet>ipconfig /renew

Windows IP Configuration

No operation can be performed on Ethernet while it has its media disconnected.
No operation can be performed on Local Area Connection* 2 while it has its media disconnected.

Ethernet adapter Ethernet:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::2c74:d14d:596c:51b6%13
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . : hsd1.ca.comcast.net
    IPv6 Address. . . . . : 2601:646:8501:5d70:fd60:e9bf:5b65:1272
    Temporary IPv6 Address. . . . . : 2601:646:8501:5d70:c8b2:27dd:f41e:8a3b

```

Overview

We will see how Dynamic Host Configuration Protocol (DHCP) works using its various operations. Topics that we will discuss in the report are:

- What is DHCP?
- DHCP Handshake
- How DHCP works
- DHCP Protocol Components
- Standards
- DHCP Packet Format
- DHCP Packet Header
- Quality of Service (QoS) in DHCP
- Signaling
- Signaling Records
- Session
- Screenshots depicting sessions
- DHCP Snooping
- Conclusion

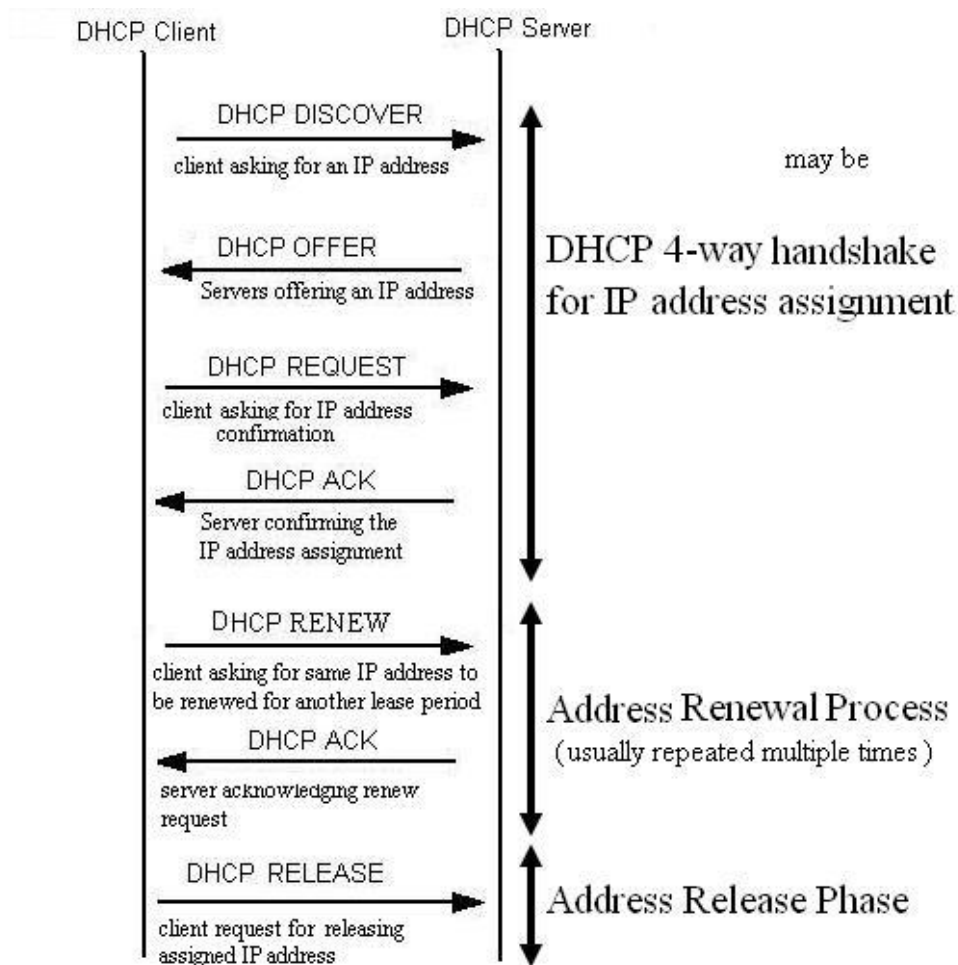
What is DHCP?

DHCP Stands for Dynamic Host Configuration Protocol. It is a client/server protocol that provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. The other main features of DHCP are:

- Controlling the network configuration of a host using a remote server.
- Providing a framework for passing configuration information to hosts on a TCP/IP network.
- Assigning IP configuration to the host connecting to the network.

It is based on a Bootstrap Protocol(BOOTP). Also, DHCP distributes the IP address, subnet mask and default gateway to a host, but can include other configuration parameters such as name servers and net bios configuration. Plus, because DHCP being a protocol it has its own set of messages that are exchanged between the client and the server.

DHCP Handshake



A complete DHCP exchange involves four types of packets.

- 1) **Discover**, for client to locate the DHCP server
 - 2) **Offer**, for the server to offer an IP address
 - 3) **Request**, for client to ask for an offered address
 - 4) **Ack**, for the server to grant the address lease.
- Whenever, the client already has an IP address and only wants to renew its lease, the initial **DHCPDISCOVER/DHCPOFFER** messages can be skipped.
 - In such a case, the protocol begins with the client requesting the address it is currently using with a **DHCPREQUEST** message.
 - Now, the protocol works as already described: the server will likely grant the request (with a DHCPACK) or deny the request by sending a **DHCPNAK**.

- In a case if the client already has an address and does not need to renew it but requires other (non-address) configuration information, it can use a **DHCPINFORM** message in place of a **DHCPREQUEST** message to indicate its use of an existing address and desire to obtain additional information.

How DHCP works?

During the DHCP process, a DHCP client goes through following six stages.

- Initializing
- Selecting
- Requesting
- Binding
- Renewing
- Rebinding

Different messages that are used in the process are:

1. DHCPDISCOVER

It marks the beginning of any DHCP interaction between a client and server. It is sent by client connected to a local subnet. It's a broadcast message that uses 255.255.255.255 as destination IP address while the source IP address is 0.0.0.0

2. DHCPOFFER

It is DHCP message sent in response to DHCPDISCOVER by a DHCP server to DHCP client. This message includes network configuration settings for the client sending the DHCPDISCOVER message.

3. DHCPREQUEST

This DHCP message is sent in response to DHCPOFFER. It indicates that the client has accepted the network configuration sent in DHCPOFFER message from the server.

4. DHCPACK

This message is sent by the DHCP server as a response to DHCPREQUEST received from the client. It marks the end of the process that started with DHCPDISCOVER. This message is an acknowledgement by the DHCP server authorizing the DHCP client to start using the network configuration it received from the DHCP server.

5. DHCPNAK

This message is the exact opposite to DHCPACK. This message is sent by the DHCP server when it is not able to satisfy the DHCPREQUEST message from the client.

6. DHCPDECLINE

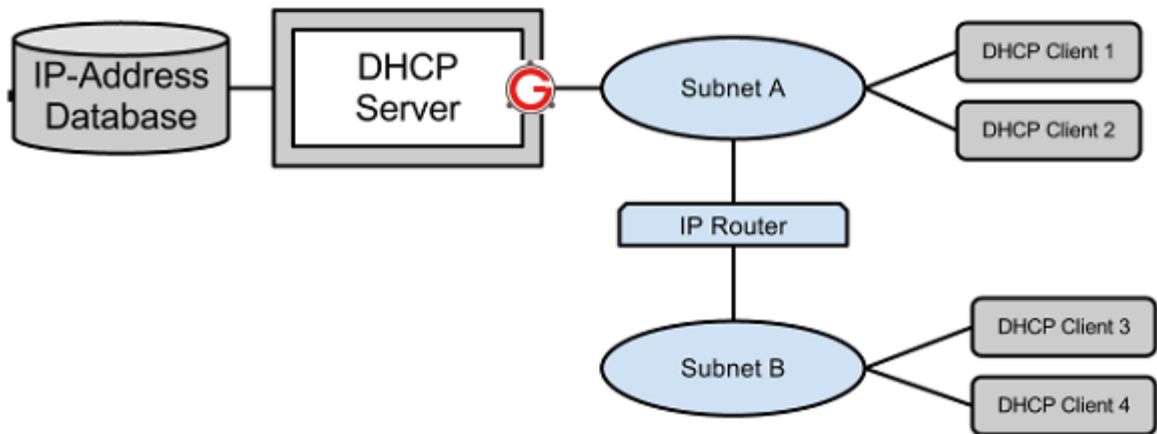
This message is sent from the DHCP client to the server when the client finds that the IP address assigned by server is already in use.

7. DHCPINFORM

This message is sent from the DHCP client in case when IP is statically configured on client and other configurations are to be dynamically acquired from DHCP server.

8. DHCPRELEASE

This message is sent by the DHCP client in case it wants to terminate the lease of network address it has been provided by DHCP server.



Here are the steps:

Step 1: When the client device boots up (connected to network), a DHCPDISCOVER message is sent from the client to the server.

The client sends a message with 0.0.0.0 as source address and 255.255.255.255 as destination address since there is no network configuration information on client.

If the DHCP server is on local subnet, it receives the message directly and if it is on different subnet, then a relay agent connected on client's subnet is used to pass request to DHCP server.

The transport protocol used is UDP and the port number used is 67. This is the initializing stage of the client.

Step 2: When the DHCP server receives the DHCPDISCOVER request message, it replies with a DHCPOFFER message.

This message contains all the network configuration settings required by the client.

The subnet mask and gateway information is filled in the options field.

The server fills in the client MAC address in the chaddr field.

This message is sent as a broadcast (255.255.255.255) message for client to receive it directly or sent to the relay agent that takes care of whether the message is to be passed as unicast or broadcast.

UDP protocol is used at the transport layer with destination port as 68. Here the client enters selecting stage.

Step 3: The client sends DHCPREQUEST message in reply to DHCPOFFER message to the server indicating it wants to accept the DHCPOFFER message.

If there were multiple DHCP servers that received DHCPDISCOVER then client could receive multiple DHCPOFFER messages.

The client replies to only one of the messages by setting the server id field with the IP address of that DHCP server.

All other DHCP server messages implicitly declined.

The DHCPREQUEST message will still contain the source address as 0.0.0.0 since the client is not allowed to use the IP address from DHCPOFFER message. This is Requesting stage.

Step 4: When the server receives DHCPREQUEST from the client, it sends the DHCPACK message allowing the client to use the IP address assigned to it. This is the Binding stage.

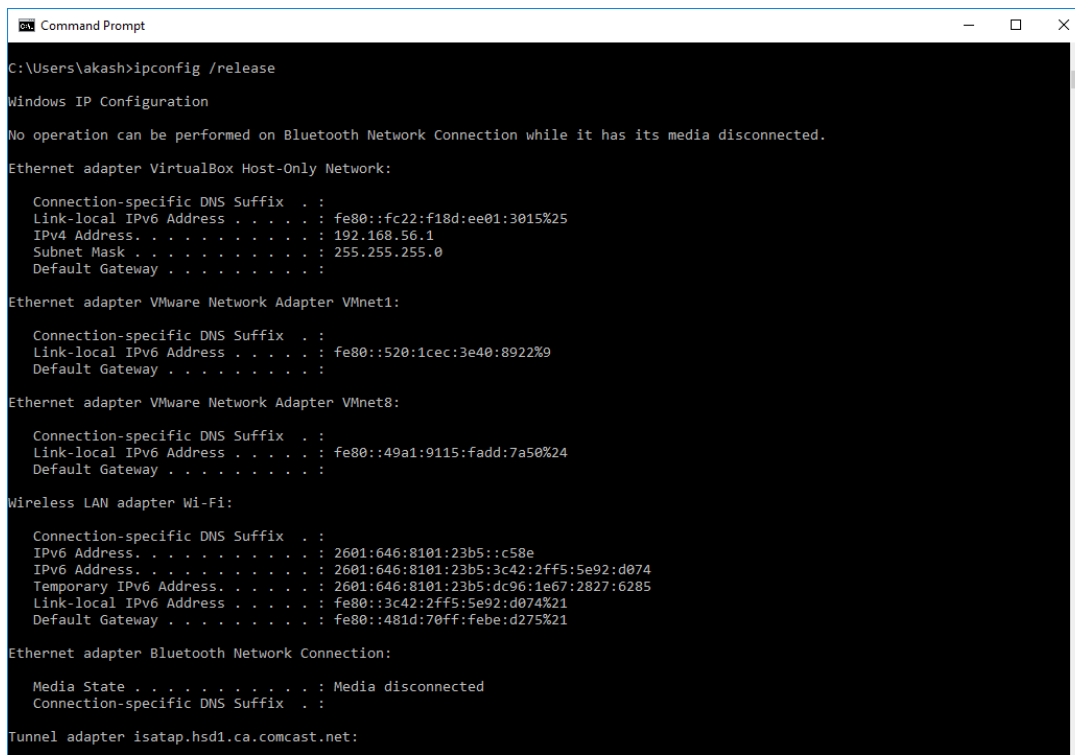
Step 5: The IP address assigned by the server to client is on a lease. When the lease expires the DHCP server can assign the same IP address to any other host requesting for it.

Lease has to be renewed time to time.

The DHCP client tries renewing the lease after half of the lease time has expired. This is done by exchanging DHCPREQUEST and DHCPACK messages. This is renewing stage.

Start the capture in Wireshark.

- Leased IP address is released.



```
Command Prompt
C:\Users\akash>ipconfig /release

Windows IP Configuration

No operation can be performed on Bluetooth Network Connection while it has its media disconnected.

Ethernet adapter VirtualBox Host-Only Network:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::fc22:f18d:ee01:3015%25
    IPv4 Address. . . . . : 192.168.56.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::520:1cec:3e40:8922%9
    Default Gateway . . . . . : 

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::49a1:9115:fadd:7a50%24
    Default Gateway . . . . . : 

Wireless LAN adapter Wi-Fi:

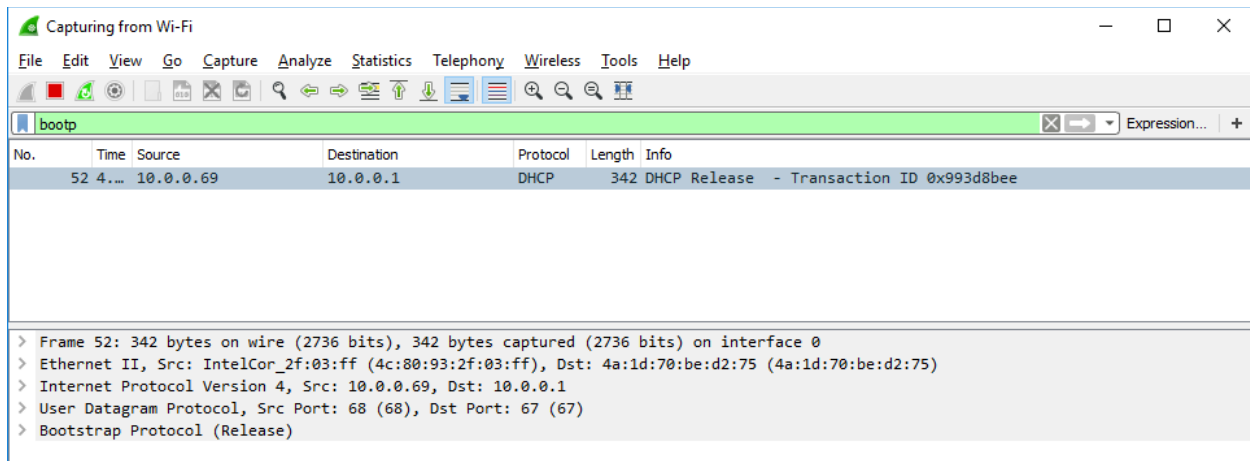
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2601:646:8101:23b5::c58e
    IPv6 Address. . . . . : 2601:646:8101:23b5:3c42:2ff5:5e92:d074
    Temporary IPv6 Address. . . . . : 2601:646:8101:23b5:dc96:1e67:2827:6285
    Link-local IPv6 Address . . . . . : fe80::3c42:2ff5:5e92:d074%21
    Default Gateway . . . . . : fe80::481d:70ff:febe:d275%21

Ethernet adapter Bluetooth Network Connection:

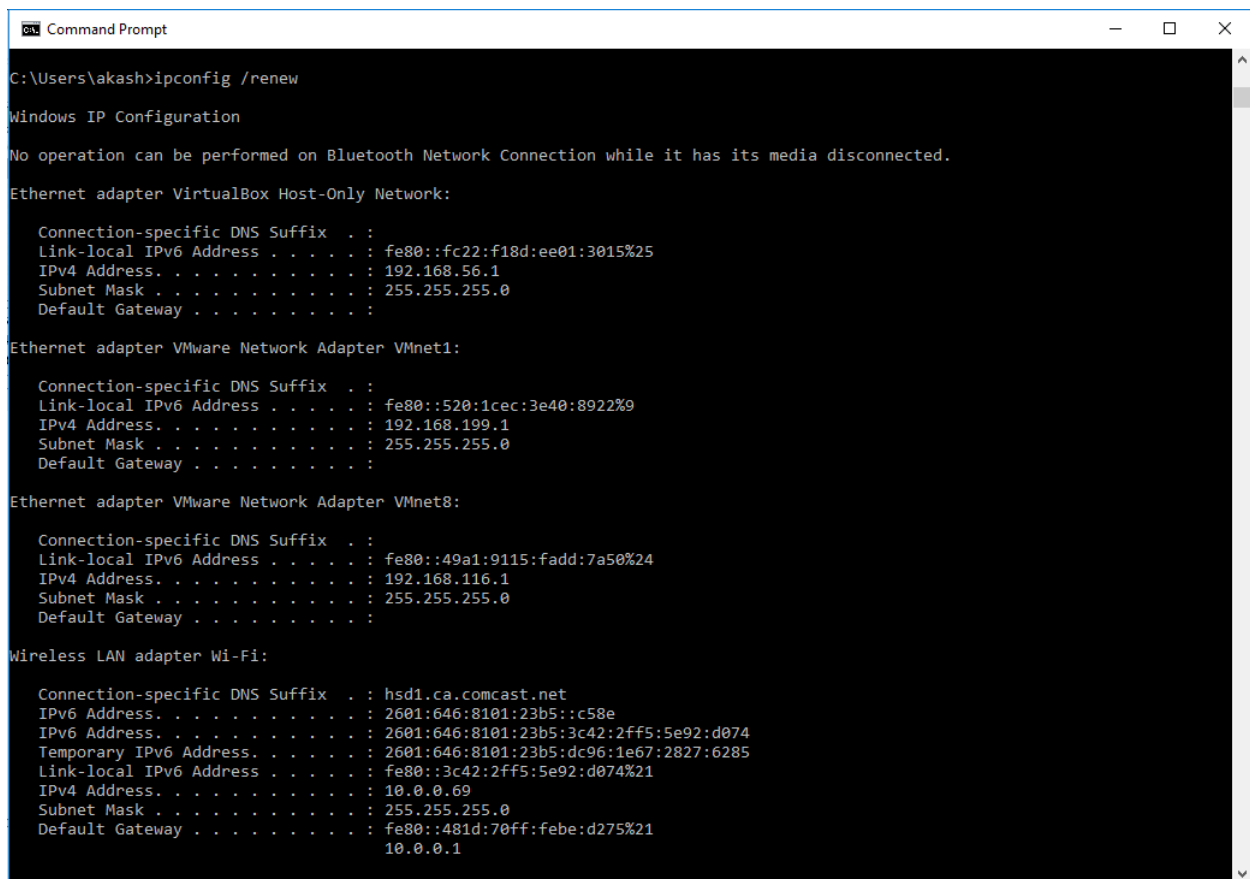
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Tunnel adapter isatap.hsd1.ca.comcast.net:
```

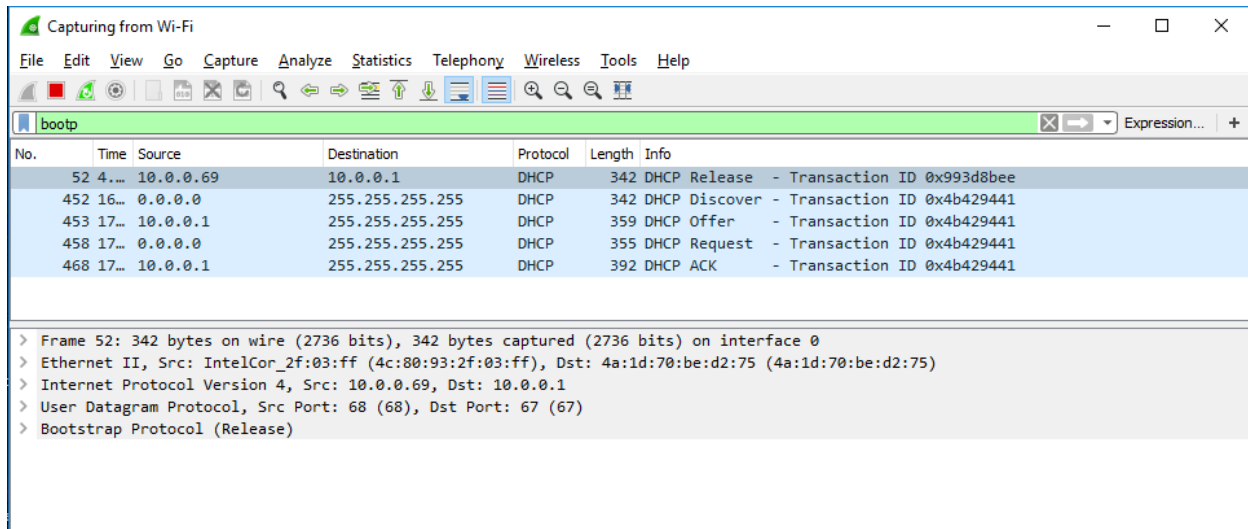
- Trace is inspected



- Lease is renewed.



- Wireshark packets corresponding to it.



No.	Time	Source	Destination	Protocol	Length	Info
52	4....	10.0.0.69	10.0.0.1	DHCP	342	DHCP Release - Transaction ID 0x993d8bee
452	16...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x4b429441
453	17...	10.0.0.1	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0x4b429441
458	17...	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0x4b429441
468	17...	10.0.0.1	255.255.255.255	DHCP	392	DHCP ACK - Transaction ID 0x4b429441

> Frame 52: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0 > Ethernet II, Src: IntelCor_2f:03:ff (4c:80:93:2f:03:ff), Dst: 4a:1d:70:be:d2:75 (4a:1d:70:be:d2:75) > Internet Protocol Version 4, Src: 10.0.0.69, Dst: 10.0.0.1 > User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67) > Bootstrap Protocol (Release)						
---	--	--	--	--	--	--

DHCP Protocol components:

DHCP is software collection that implements all aspects of the DHCP (Dynamic Host Configuration Protocol) suite. It includes:

- **DHCP server**, an Internet host that returns configuration parameters to DHCP clients.
- **DHCP client**, which can be bundled with the operating system of a client computer or other IP capable device and which sends configuration requests to the server. Most devices and operating systems already have DHCP clients included.
- **DHCP relay agent**, which passes DHCP requests from one LAN to another so that there need not be a DHCP server on every LAN.

DHCP protocol has following messages:

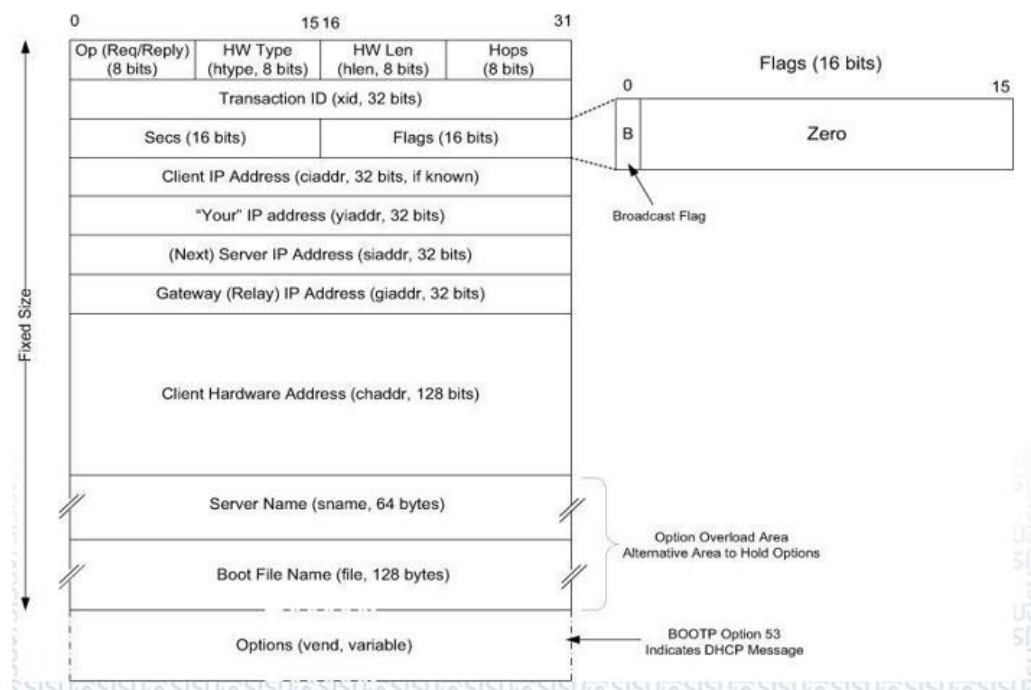
- **DHCP DISCOVER**: Client broadcast to locate available servers.
- **DHCP OFFER**: Server to client in response to DHCPDISCOVER with offer of configuration parameters.
- **DHCP REQUEST**: Client message to servers either (a) requesting offered parameters from one server and implicitly declining offers from all others, (b) confirming correctness of previously allocated address after, e.g., system reboot, or (c) extending the lease on a particular network address.
- **DHCP ACK**: Server to client with configuration parameters, including committed network address.
- **DHCP NAK**: Server to client indicating client's notion of network address is incorrect (e.g., client has moved to new subnet) or client's lease as expired

- **DHCP DECLINE:** Client to server indicating network address is already in use.
- **DHCP RELEASE:** Client to server relinquishing network address and cancelling remaining lease.
- **DHCP INFORM:** Client to server, asking only for local configuration parameters; client already has externally configured network address.

Standards:

RFC 1531	Dynamic Host Configuration Protocol
RFC 1534	Interoperation between DHCP and BOOTP
RFC 1542	Clarifications and Extensions for the Bootstrap Protocol
RFC 2131	Dynamic Host Configuration Protocol
RFC 2132	DHCP Options and BOOTP Vendor Extensions
RFC 3046	DHCP Relay Agent Information Option
RFC 3942	Reclassifying Dynamic Host Configuration Protocol Version Four (DHCPv4) Options
RFC 4242	Information Refresh Time Option for Dynamic Host Configuration Protocol for IPv6
RFC 4361	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)
RFC 4388	Dynamic Host Configuration Protocol (DHCP) Lease query
RFC 4436	Detecting Network Attachment in IPv4 (Dनाव4)

Packet Format



- **Op (Operation) field:** Identifies the message as either a request (1) or a reply (2).
- **HW Type (htype) field:** Assigned based on values used with ARP and defined in the corresponding IANA ARP parameters page [IARP], with the value 1 (Ethernet) being very common.
- **HW Len (hlen) field:** Gives the number of bytes used to hold the hardware (MAC) address and is commonly 6 for Ethernet-like networks.
- **Hops field:** It is used to store the number of relays through which the message has traveled. The sender of the message sets this value to 0, and it is incremented at each relay.
- **Transaction ID field:** It is a (random) number chosen by the client and copied into responses by the server. It is used to match replies with requests.
- **Secs field:** It is set by the client with the number of seconds that have elapsed since the first attempt to establish or renew an address.
- **Flags field:** Currently it contains only a single defined bit called the broadcast flag. Clients may set this bit in requests if they are unable or unwilling to process incoming unicast IP datagrams but can process incoming broadcast datagrams (e.g., because they do not yet have an IP address). Setting the bit informs the server and relays that broadcast addressing should be used for replies.
- **Client IP Address (ciaddr) field:** Includes current IP address of the requestor, if known, and is 0 otherwise.
- **“Your” IP Address (yiaddr) field:** It is filled in by a server when providing an address to a requesting client.
- **Next Server IP Address (siaddr) field:** It gives the IP address of the next server to use for the client’s bootstrap process (e.g., if the client needs to download an operating system image that may be accomplished from a server other than the DHCP server).
- **Gateway (or Relay) IP Address (giaddr) field:** It is filled in by a DHCP or BOOTP relay with its address when forwarding DHCP (BOOTP) messages.
- **Client Hardware Address (chaddr) field:** It holds a unique identifier of the client and can be used in various ways by the server, including arranging for the same IP address to be given each time a particular client makes an address request. This field has traditionally held the client’s MAC address, which has been used as an identifier.
- **Server Name (sname) & Boot File Name (file) fields:** These fields are not always filled in, but if they are, they contain 64 or 128 bytes, respectively, of ASCII characters indicating the name of the server or path to the boot file. Such strings are null-terminated, as in the C programming language. They can also be used instead to hold DHCP options if space is tight.
- **Options field:** It is originally known as the *Vendor Extensions* field in BOOTP and fixed in length, is now known as the *Options* field and is variable in length. As we shall see, options are used extensively with DHCP and are required to distinguish DHCP messages from legacy BOOTP messages. Given that DHCP extends BOOTP, any fields needed by DHCP that were not present when BOOTP was designed are carried as options. Options take a standard format beginning with an 8-bit tag indicating the option type. For some options, a fixed number of bytes following the tag contain the option value. All others consist of the tag followed by 1 byte containing the length of the option value (not including the tag or length), followed by a variable number of bytes containing the option value itself.

```

> Ethernet II, Src: LiteonTe_50:78:f5 (b8:86:87:50:78:f5), 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 (68), Dst Port: 67 (67)
  ▾ Bootstrap Protocol (Request)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xe11be73e
    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: LiteonTe_50:78:f5 (b8:86:87:50:78:f5)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP

```

0000	ff ff ff ff ff ff b8 86 87 50 78 f5 08 00 45 00Px...E.
0010	01 5d 12 df 00 00 80 11 26 b2 00 00 00 00 ff ff	..].D.C.I (.....
0020	ff ff 00 44 00 43 01 49 28 f7 01 01 06 00 e1 1b	...>.....
0030	e7 3e 00 00 00 00 00 00 00 00 00 00 00 00 00Px.....
0040	00 00 00 00 00 00 b8 86 87 50 78 f5 00 00 00 00
0050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Snapshot showing the message format and its content captured in Wireshark for DHCP Request.

Packet Header

There are 4 different types of packets corresponding to DHCP.

1. Discover : For the host to locate DHCP Server
2. Offer : From the server to offer IP Address
3. Request : From local host to request offered IP Address
4. ACK: From Server to grant IP Address lease.

However, if a computer is reestablishing its IP address on a network, it may perform a short exchange involving only two types of DHCP packets: Request and ACK.

Wireshark capture Inspection

Look for the DHCP exchange in the trace of packets captured with Wireshark. Select each DHCP Request packet, and observe the protocol stack to see how DHCP messages are carried. The link protocol is likely Ethernet, and the next higher protocol is IP. Then comes UDP, so each DHCP message is carried in a UDP packet. Below UDP, Wireshark is likely to say BOOTP (Bootstrap Protocol) instead of DHCP because DHCP is implemented as an extension of an older protocol called BOOTP. We can consider the BOOTP section as the DHCP header and message.

Consider any type of DHCP packet and expand the BOOTP (DHCP) section (using the “+” expander or icon) to look at the details of a DHCP Header details. There are many fields, and most of them were explained in **Packet Format** section. Let us look at each type of message and observe their corresponding values.

Discover Type Packet inspection

As discover packet is used to locate the server for attaining IP address, following type of packet header is found on the capture

Bootstrap Protocol (Discover)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xe4bd7f7c

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_e8:b0:72 (00:0c:29:e8:b0:72)

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

Option: (12) Host Name

Bootstrap Protocol (Offer)

Message type: Boot Reply (2)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xe4bd7f7c

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 192.168.59.133

Next server IP address: 192.168.59.254

Relay agent IP address: 0.0.0.0

Client MAC address: Vmware_e8:b0:72 (00:0c:29:e8:b0:72)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

Option: (53) DHCP Message Type (Offer)

Option: (54) DHCP Server Identifier

Option: (51) IP Address Lease Time

Option: (1) Subnet Mask

Option: (28) Broadcast Address

Option: (3) Router

Option: (15) Domain Name

Option: (6) Domain Name Server

Option: (44) NetBIOS over TCP/IP Name Server

Option: (255) End

Padding: 00

Message type specifically specifies that it is an offer type of message. The message is sent from server to client upon server receiving the Discover type of message. In this case, the next server IP address field and Your IP address fields were filled by server and broadcasted to offer requested client with an IP address available.

bootp						
No.	Time	Source	Destination	Protocol	Length	Info
1 0...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xbd04f108
2 0...	192.168.59.254	192.168.59.133	DHCP	342	DHCP ACK	- Transaction ID 0xbd04f108
55 21...	192.168.59.132	192.168.59.254	DHCP	342	DHCP Release	- Transaction ID 0xff6e0d13
63 23...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	- Transaction ID 0xe4bd7f7c
67 23...	192.168.59.254	192.168.59.133	DHCP	342	DHCP Offer	- Transaction ID 0xe4bd7f7c
68 23...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xe4bd7f7c
69 23...	192.168.59.254	192.168.59.133	DHCP	342	DHCP ACK	- Transaction ID 0xe4bd7f7c

▼ Bootstrap Protocol (Offer)

Message type: Boot Reply (2)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xe4bd7f7c
Seconds elapsed: 0
Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.59.133
Next server IP address: 192.168.59.254
Relay agent IP address: 0.0.0.0
Client MAC address: Vmware_e8:b0:72 (00:0c:29:e8:b0:72)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Offer)
Option: (54) DHCP Server Identifier
Option: (51) IP Address Lease Time
Option: (1) Subnet Mask
Option: (28) Broadcast Address
Option: (3) Router
Option: (15) Domain Name

0020	3b 85 00 43 00 44 01 34 7f 5f 02 01 06 00 e4 bd	...C.D.4 .
0030	7f 7c 00 00 00 00 00 00 00 00 c0 a8 3b 85 c0 a8;
0040	3b fe 00 00 00 00 00 00 0c 29 e8 b0 72 00 00 00	;.).r...
0050	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
0070	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
0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Request Type Packet inspection

As Request packet is used to ask server the IP address offered, following type of packet header is found on the capture

Bootstrap Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xe4bd7f7c

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_e8:b0:72 (00:0c:29:e8:b0:72)

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

Length: 4

DHCP Server Identifier: 192.168.59.254

ACK Type Packet inspection

As Acknowledgment packet is used grant lease of the IP address to the requested it , following type of packet header is found on the capture

Bootstrap Protocol (ACK)

Message type: Boot Reply (2)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xe4bd7f7c

Seconds elapsed: 0

Bootp flags: 0x0000 (Unicast)

Client IP address: 0.0.0.0

Your (client) IP address: 192.168.59.133

Next server IP address: 192.168.59.254

Relay agent IP address: 0.0.0.0

Client MAC address: Vmware_e8:b0:72 (00:0c:29:e8:b0:72)

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

Length: 4

DHCP Server Identifier: 192.168.59.254

Option: (51) IP Address Lease Time

Length: 4

IP Address Lease Time: (1800s) 30 minutes

Option: (1) Subnet Mask

Length: 4

Subnet Mask: 255.255.255.0

Option: (28) Broadcast Address

Length: 4

Broadcast Address: 192.168.59.255

Option: (3) Router

Length: 4

Router: 192.168.59.2

Option: (15) Domain Name

Option: (6) Domain Name Server

Length: 4

Domain Name Server: 192.168.59.2

Option: (44) NetBIOS over TCP/IP Name Server

Option: (255) End

Padding: 00

Message type specifically specifies that it is an Acknowledgement type of message. The message is sent from server to client to acknowledge requested IP Address requested previously. This corresponding data is observed in the options fields. Option **53** acknowledges the IP address. Option **51** shows the lease time which is 30 min in our case. Router and DNS information is also sent through options **3** and **6**.

bootp						
No.	Time	Source	Destination	Protocol	Length	Info
1	0...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xbd04f108
2	0...	192.168.59.254	192.168.59.133	DHCP	342	DHCP ACK - Transaction ID 0xbd04f108
55	21...	192.168.59.132	192.168.59.254	DHCP	342	DHCP Release - Transaction ID 0xff6e0d13
63	23...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe4bd7f7c
67	23...	192.168.59.254	192.168.59.133	DHCP	342	DHCP Offer - Transaction ID 0xe4bd7f7c
68	23...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xe4bd7f7c
69	23...	192.168.59.254	192.168.59.133	DHCP	342	DHCP ACK - Transaction ID 0xe4bd7f7c

▼ Bootstrap Protocol (ACK)	
Message type: Boot Reply (2)	
Hardware type: Ethernet (0x01)	
Hardware address length: 6	
Hops: 0	
Transaction ID: 0xe4bd7f7c	
Seconds elapsed: 0	
▶ Bootp flags: 0x0000 (Unicast)	
Client IP address: 0.0.0.0	
Your (client) IP address: 192.168.59.133	
Next server IP address: 192.168.59.254	
Relay agent IP address: 0.0.0.0	
Client MAC address: Vmware_e8:b0:72 (00:0c:29:e8:b0:72)	
Client hardware address padding: 00000000000000000000	
Server host name not given	
Boot file name not given	
Magic cookie: DHCP	
▶ Option: (53) DHCP Message Type (ACK)	
▶ Option: (54) DHCP Server Identifier	
▶ Option: (51) IP Address Lease Time	
▶ Option: (1) Subnet Mask	
▶ Option: (28) Broadcast Address	
▶ Option: (3) Router	
▶ Option: (15) Domain Name	

0020	3b 85 00 43 00 44 01 34 7c 5f 02 01 06 00 e4 bd	...C.D.4
0030	7f 7c 00 00 00 00 00 00 00 00 c0 a8 3b 85 c0 a8	...;...
0040	3b fe 00 00 00 00 00 00 0c 29 e8 b0 72 00 00 00	...r...
0050	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
0070	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
0090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Quality of Service (QoS) in DHCP

DHCP protocol provides Option 133 for VLAN QOS that is defined by IANA.org.

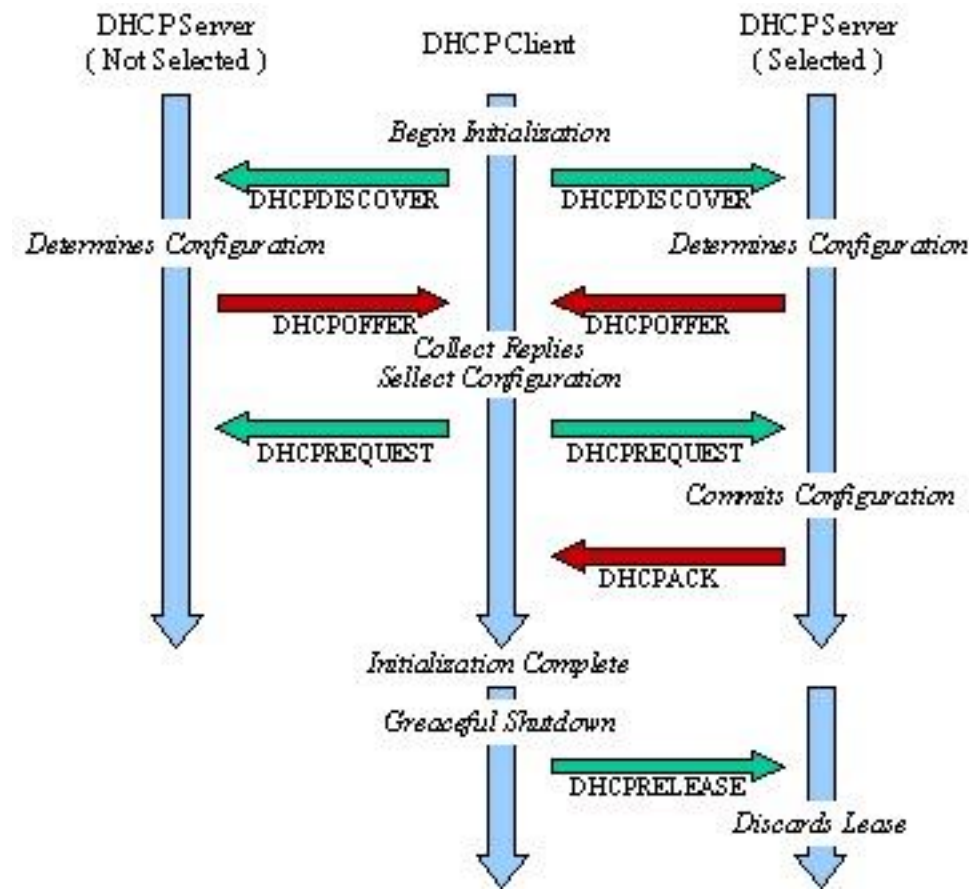
In the Lab we have observed that all the DHCP messages contains DSF as **0x10** and DSCP code as **0x04** in the IPV4 section which can be considered as default code. This gives a hint that DHCP does not use any kind of special priorities in transferring the packets.

Following are the Wireshark captures of Request and Acknowledge packets of DHCP

```
✓ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x0000 (0)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 128
    Protocol: UDP (17)
  > Header checksum: 0x3996 [validation disabled]
    Source: 0.0.0.0
    Destination: 255.255.255.255
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  > User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
  > Bootstrap Protocol (Request)
```

```
Internet Protocol Version 4, Src: 192.168.59.254, Dst: 192.168.59.133
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes
  > Differentiated Services Field: 0x10 (DSCP: Unknown, ECN: Not-ECT)
    Total Length: 328
    Identification: 0x0000 (0)
  > Flags: 0x00
    Fragment offset: 0
    Time to live: 16
    Protocol: UDP (17)
  > Header checksum: 0xb0c1 [validation disabled]
    Source: 192.168.59.254
    Destination: 192.168.59.133
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
  User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
  Bootstrap Protocol (ACK)
```


Signaling



A typical DHCP exchange. A client discovers a set of servers and addresses they are offering using broadcast messages, requests the address it desires, and receives an acknowledgment from the selected server. The transaction ID (xid) allows requests and responses to be matched up, and the server ID (an option) indicates which server is providing and committing the provided address binding with the client. If the client already knows the address it desires, the protocol can be simplified to include use of only the REQUEST and ACK messages.

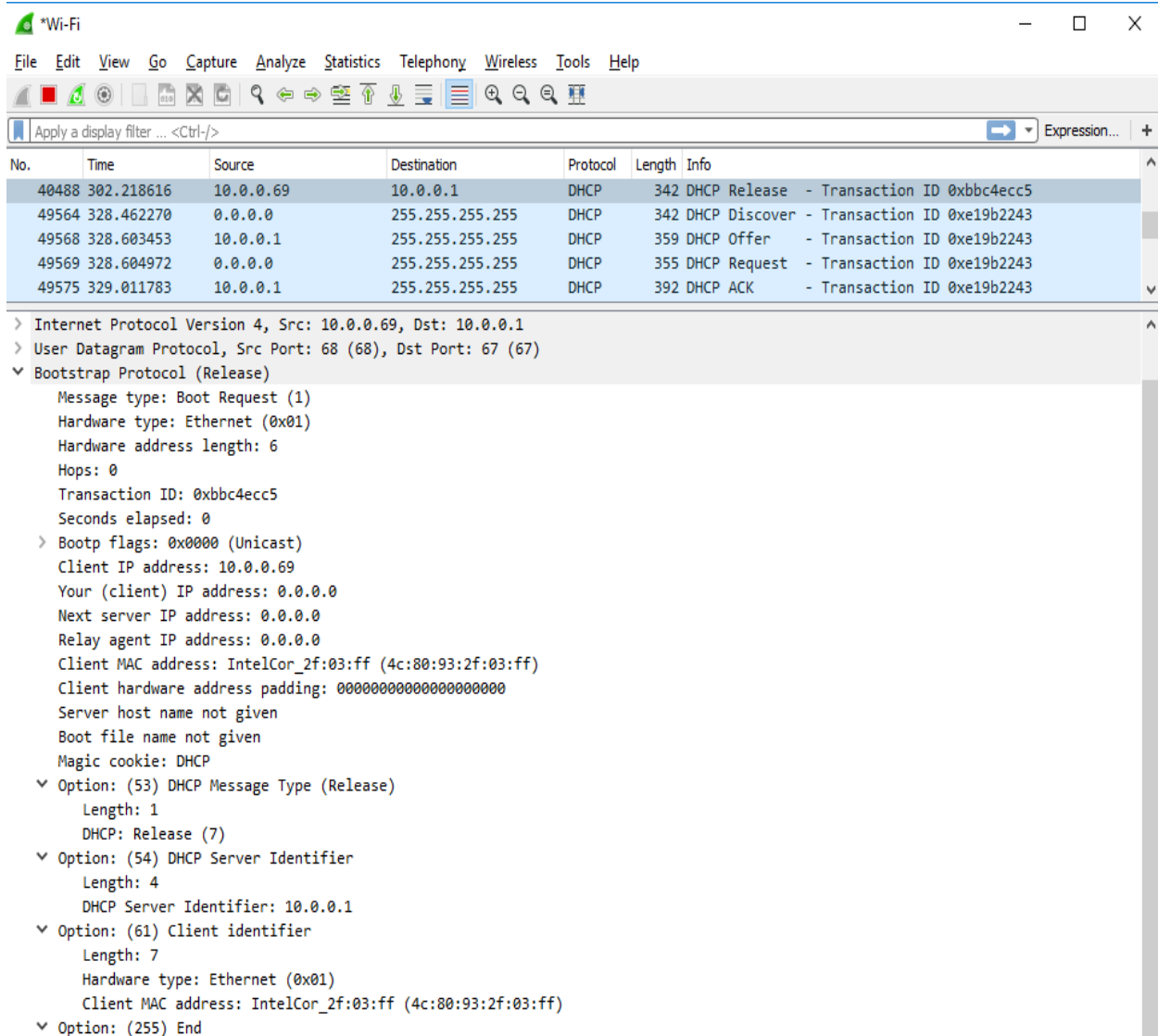
Signaling Records:

DHCP_PACKETS:

1. DHCP Release
2. DHCP Discover
3. DHCP Offer
4. DHCP Request
5. DHCP ACK

Client Port: 68 (68)
Server Port: 67 (67)
Protocol Name: DHCP
Protocol carrier: UDP/IP

DHCP Release:



The image shows a Wireshark packet capture window titled '*Wi-Fi'. The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons. A display filter is set to 'Apply a display filter ... <Ctrl-/>'. The packet list pane shows six packets, with the first five selected. The packet details pane shows the selected packet (No. 40488) as an Internet Protocol Version 4 packet from 10.0.0.69 to 10.0.0.1. The User Datagram Protocol section shows the source port as 68 (68) and the destination port as 67 (67). The Bootstrap Protocol (Release) section shows the message type as Boot Request (1), hardware type as Ethernet (0x01), and transaction ID as 0xbbc4ecc5. The DHCP section shows the DHCP Release (7) message with options (53) DHCP Message Type (Release), (54) DHCP Server Identifier, (61) Client identifier, and (255) End.

No.	Time	Source	Destination	Protocol	Length	Info
40488	302.218616	10.0.0.69	10.0.0.1	DHCP	342	DHCP Release - Transaction ID 0xbbc4ecc5
49564	328.462270	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe19b2243
49568	328.603453	10.0.0.1	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0xe19b2243
49569	328.604972	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0xe19b2243
49575	329.011783	10.0.0.1	255.255.255.255	DHCP	392	DHCP ACK - Transaction ID 0xe19b2243

> Internet Protocol Version 4, Src: 10.0.0.69, Dst: 10.0.0.1
> User Datagram Protocol, Src Port: 68 (68), Dst Port: 67 (67)
▼ Bootstrap Protocol (Release)
 Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0xbbc4ecc5
 Seconds elapsed: 0
 > Bootp flags: 0x0000 (Unicast)
 Client IP address: 10.0.0.69
 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: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)
 Client hardware address padding: 00000000000000000000
 Server host name not given
 Boot file name not given
 Magic cookie: DHCP
 ▼ Option: (53) DHCP Message Type (Release)
 Length: 1
 DHCP: Release (7)
 ▼ Option: (54) DHCP Server Identifier
 Length: 4
 DHCP Server Identifier: 10.0.0.1
 ▼ Option: (61) Client identifier
 Length: 7
 Hardware type: Ethernet (0x01)
 Client MAC address: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)
 ▼ Option: (255) End

DHCP Discover:

The screenshot shows a Wi-Fi network analyzer interface with a packet list and a detailed view of a DHCP Discover packet (No. 49564).

No.	Time	Source	Destination	Protocol	Length	Info
40488	302.218616	10.0.0.69	10.0.0.1	DHCP	342	DHCP Release - Transaction ID 0xbbc4ecc5
49564	328.462270	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe19b2243
49568	328.603453	10.0.0.1	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0xe19b2243
49569	328.604972	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0xe19b2243
49575	329.011783	10.0.0.1	255.255.255.255	DHCP	392	DHCP ACK - Transaction ID 0xe19b2243

Frame 49564: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

Ethernet II, Src: IntelCor_2f:03:ff (4c:80:93:2f:03:ff), 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 (68), Dst Port: 67 (67)

Bootstrap Protocol (Discover)

- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0xe19b2243
- Seconds elapsed: 0
- Bootp flags: 0x8000, Broadcast flag (Broadcast)
- 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: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP
- Option: (53) DHCP Message Type (Discover)
 - Length: 1
 - DHCP: Discover (1)
- Option: (61) Client Identifier
- Option: (50) Requested IP Address
- Option: (12) Host Name
- Option: (60) Vendor class identifier
- Option: (55) Parameter Request List
- Option: (255) End

DHCP Offer:

The screenshot shows the same Wi-Fi network analyzer interface, now displaying the details of a DHCP Offer packet (No. 49568).

No.	Time	Source	Destination	Protocol	Length	Info
40488	302.218616	10.0.0.69	10.0.0.1	DHCP	342	DHCP Release - Transaction ID 0xbbc4ecc5
49564	328.462270	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe19b2243
49568	328.603453	10.0.0.1	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0xe19b2243
49569	328.604972	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0xe19b2243
49575	329.011783	10.0.0.1	255.255.255.255	DHCP	392	DHCP ACK - Transaction ID 0xe19b2243

Frame 49568: 359 bytes on wire (2872 bits), 359 bytes captured (2872 bits) on interface 0

Ethernet II, Src: 4a:1d:70:be:d2:75 (4a:1d:70:be:d2:75), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 10.0.0.1, Dst: 255.255.255.255

User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)

Bootstrap Protocol (Offer)

- Message type: Boot Reply (2)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 0
- Transaction ID: 0xe19b2243
- Seconds elapsed: 0
- Bootp flags: 0x8000, Broadcast flag (Broadcast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 10.0.0.69
- Next server IP address: 10.0.0.1
- Relay agent IP address: 0.0.0.0
- Client MAC address: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)
- 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
 - Length: 4
 - DHCP Server Identifier: 10.0.0.1
- Option: (51) IP Address Lease Time
 - Length: 4
 - IP Address Lease Time: (604800s) 7 days

DHCP Request:

The screenshot shows a Wireshark packet capture window titled "*Wi-Fi". The packet list pane displays five packets. Packet 49569 is selected, showing details for a DHCP Request. The packet is an Ethernet II frame with source IntelCor_2f:03:ff (4c:80:93:2f:03:ff) and destination Broadcast (ff:ff:ff:ff:ff:ff). It is an Internet Protocol Version 4 packet with source 0.0.0.0 and destination 255.255.255.255. The User Datagram Protocol (UDP) section shows source port 68 and destination port 67. The Bootstrap Protocol (Request) section shows a Message type of Boot Request (1), Hardware type of Ethernet (0x01), Hardware address length of 6, Hops of 0, Transaction ID of 0xe19b2243, and Seconds elapsed of 0. The Bootp flags are 0x8000, indicating a Broadcast flag. The Client IP address is 0.0.0.0, and the Your (client) IP address is 0.0.0.0. The Next server IP address is 0.0.0.0, and the Relay agent IP address is 0.0.0.0. The Client MAC address is IntelCor_2f:03:ff (4c:80:93:2f:03:ff), and the Client hardware address padding is 00000000000000000000. The Server host name is not given, and the Boot file name is not given. The Magic cookie is DHCP. The Options section shows three options: Option (53) DHCP Message Type (Request) with Length 1, Option (61) Client identifier with Length 7, and Option (50) Requested IP Address with Length 4.

No.	Time	Source	Destination	Protocol	Length	Info
40488	302.218616	10.0.0.69	10.0.0.1	DHCP	342	DHCP Release - Transaction ID 0xbbc4ecc5
49564	328.462270	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe19b2243
49568	328.603453	10.0.0.1	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0xe19b2243
49569	328.604972	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0xe19b2243
49575	329.011783	10.0.0.1	255.255.255.255	DHCP	392	DHCP ACK - Transaction ID 0xe19b2243

> Frame 49569: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface 0
> Ethernet II, Src: IntelCor_2f:03:ff (4c:80:93:2f:03:ff), 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 (68), Dst Port: 67 (67)
▼ Bootstrap Protocol (Request)
 Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0xe19b2243
 Seconds elapsed: 0
 > Bootp flags: 0x8000, Broadcast flag (Broadcast)
 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: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)
 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: (61) Client identifier
 Length: 7
 Hardware type: Ethernet (0x01)
 Client MAC address: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)
 ▼ Option: (50) Requested IP Address
 Length: 4

DHCP ACK:

The screenshot shows a Wireshark packet capture window titled "*Wi-Fi". The packet list pane displays five packets. Packet 49575 is selected, showing details for a DHCP ACK. The packet is an Ethernet II frame with source 4a:1d:70:be:d2:75 (4a:1d:70:be:d2:75) and destination Broadcast (ff:ff:ff:ff:ff:ff). It is an Internet Protocol Version 4 packet with source 10.0.0.1 and destination 255.255.255.255. The User Datagram Protocol (UDP) section shows source port 67 and destination port 68. The Bootstrap Protocol (ACK) section shows a Message type of Boot Reply (2), Hardware type of Ethernet (0x01), Hardware address length of 6, Hops of 0, Transaction ID of 0xe19b2243, and Seconds elapsed of 0. The Bootp flags are 0x8000, indicating a Broadcast flag. The Client IP address is 0.0.0.0, and the Your (client) IP address is 10.0.0.69. The Next server IP address is 10.0.0.1, and the Relay agent IP address is 0.0.0.0. The Client MAC address is IntelCor_2f:03:ff (4c:80:93:2f:03:ff), and the Client hardware address padding is 00000000000000000000. The Server host name is not given, and the Boot file name is not given. The Magic cookie is DHCP. The Options section shows three options: Option (53) DHCP Message Type (ACK) with Length 1, Option (54) DHCP Server Identifier with Length 4, and Option (51) IP Address Lease Time with Length 4.

No.	Time	Source	Destination	Protocol	Length	Info
40488	302.218616	10.0.0.69	10.0.0.1	DHCP	342	DHCP Release - Transaction ID 0xbbc4ecc5
49564	328.462270	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xe19b2243
49568	328.603453	10.0.0.1	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0xe19b2243
49569	328.604972	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0xe19b2243
49575	329.011783	10.0.0.1	255.255.255.255	DHCP	392	DHCP ACK - Transaction ID 0xe19b2243

> Frame 49575: 392 bytes on wire (3136 bits), 392 bytes captured (3136 bits) on interface 0
> Ethernet II, Src: 4a:1d:70:be:d2:75 (4a:1d:70:be:d2:75), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 10.0.0.1, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 67 (67), Dst Port: 68 (68)
▼ Bootstrap Protocol (ACK)
 Message type: Boot Reply (2)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0xe19b2243
 Seconds elapsed: 0
 > Bootp flags: 0x8000, Broadcast flag (Broadcast)
 Client IP address: 0.0.0.0
 Your (client) IP address: 10.0.0.69
 Next server IP address: 10.0.0.1
 Relay agent IP address: 0.0.0.0
 Client MAC address: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)
 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
 Length: 4
 DHCP Server Identifier: 10.0.0.1
 ▼ Option: (51) IP Address Lease Time
 Length: 4
 IP Address Lease Time: (604800s) 7 days

Sessions:

Every session in DHCP involves the following:

- **DHCP client:** A DHCP client is an Internet host that uses DHCP to obtain configuration parameters such as a network address.
- **DHCP server:** A DHCP server is an Internet host that returns configuration parameters to DHCP clients.

It is observed that the number of DHCP session(Discover, Offer, Request, Ack) is equal to the number of repeated Transaction ID's. Depending on the number of Transaction ID's that are repeated, we are going to have that many number of sessions.

Here we have captured the DHCP packets for different sessions with different Transaction IDs. It can be clearly seen that the number of DHCP session (Discover, Offer, Request, Ack) is equal to the number of repeated Transaction ID's.

Screenshots depicting Sessions:

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons. A filter bar shows the expression `bootp.option.type == 53`. The packet list pane shows four captured packets:

No.	Time	Source	Destination	Protocol	Length	Info
4744	22...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x78ea5276
4747	23...	10.0.0.1	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0x78ea5276
4748	23...	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0x78ea5276
4794	23...	10.0.0.1	255.255.255.255	DHCP	392	DHCP ACK - Transaction ID 0x78ea5276

The packet details pane for the selected packet (4744) shows the following structure:

- > Frame 4744: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
- > Ethernet II, Src: IntelCor_2f:03:ff (4c:80:93:2f:03:ff), 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 (68), Dst Port: 67 (67)
- > Bootstrap Protocol (Discover)
 - Message type: Boot Request (1)
 - Hardware type: Ethernet (0x01)
 - Hardware address length: 6
 - Hops: 0
 - Transaction ID: 0x78ea5276
 - Seconds elapsed: 0
 - > Bootp flags: 0x8000, Broadcast flag (Broadcast)
 - 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: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)
 - 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: (61) Client identifier
 - > Option: (50) Requested IP Address
 - > Option: (12) Host Name
 - > Option: (60) Vendor class identifier
 - > Option: (55) Parameter Request List
 - > Option: (255) End
 - Padding: 000000000000

pcap2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

Packet list Narrow & Wide Case sensitive Display filter Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
943	24...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x4b61fada
944	24...	10.0.0.1	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0x4b61fada
945	24...	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0x4b61fada
947	25...	10.0.0.1	255.255.255.255	DHCP	392	DHCP ACK - Transaction ID 0x4b61fada

> Frame 943: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

> Ethernet II, Src: IntelCor_2f:03:ff (4c:80:93:2f:03:ff), 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 (68), Dst Port: 67 (67)

▼ Bootstrap Protocol (Discover)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0x4b61fada

Seconds elapsed: 0

> Bootp flags: 0x8000, Broadcast flag (Broadcast)

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: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)

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: (61) Client identifier

> Option: (50) Requested IP Address

> Option: (12) Host Name

> Option: (60) Vendor class identifier

> Option: (55) Parameter Request List

> Option: (255) End

Padding: 000000000000

pcap3.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

bootp

Packet list Narrow & Wide Case sensitive Display filter Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
8474	17...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb58b4595
8477	17...	10.0.0.1	255.255.255.255	DHCP	359	DHCP Offer - Transaction ID 0xb58b4595
8482	17...	0.0.0.0	255.255.255.255	DHCP	355	DHCP Request - Transaction ID 0xb58b4595
8501	18...	10.0.0.1	255.255.255.255	DHCP	392	DHCP ACK - Transaction ID 0xb58b4595

> Frame 8482: 355 bytes on wire (2840 bits), 355 bytes captured (2840 bits) on interface 0

> Ethernet II, Src: IntelCor_2f:03:ff (4c:80:93:2f:03:ff), 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 (68), Dst Port: 67 (67)

▼ Bootstrap Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xb58b4595

Seconds elapsed: 0

> Bootp flags: 0x8000, Broadcast flag (Broadcast)

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: IntelCor_2f:03:ff (4c:80:93:2f:03:ff)

Client hardware address padding: 00000000000000000000

Server host name not given

Boot file name not given

Magic cookie: DHCP

> Option: (53) DHCP Message Type (Request)

> Option: (61) Client identifier

> Option: (50) Requested IP Address

> Option: (54) DHCP Server Identifier

> Option: (12) Host Name

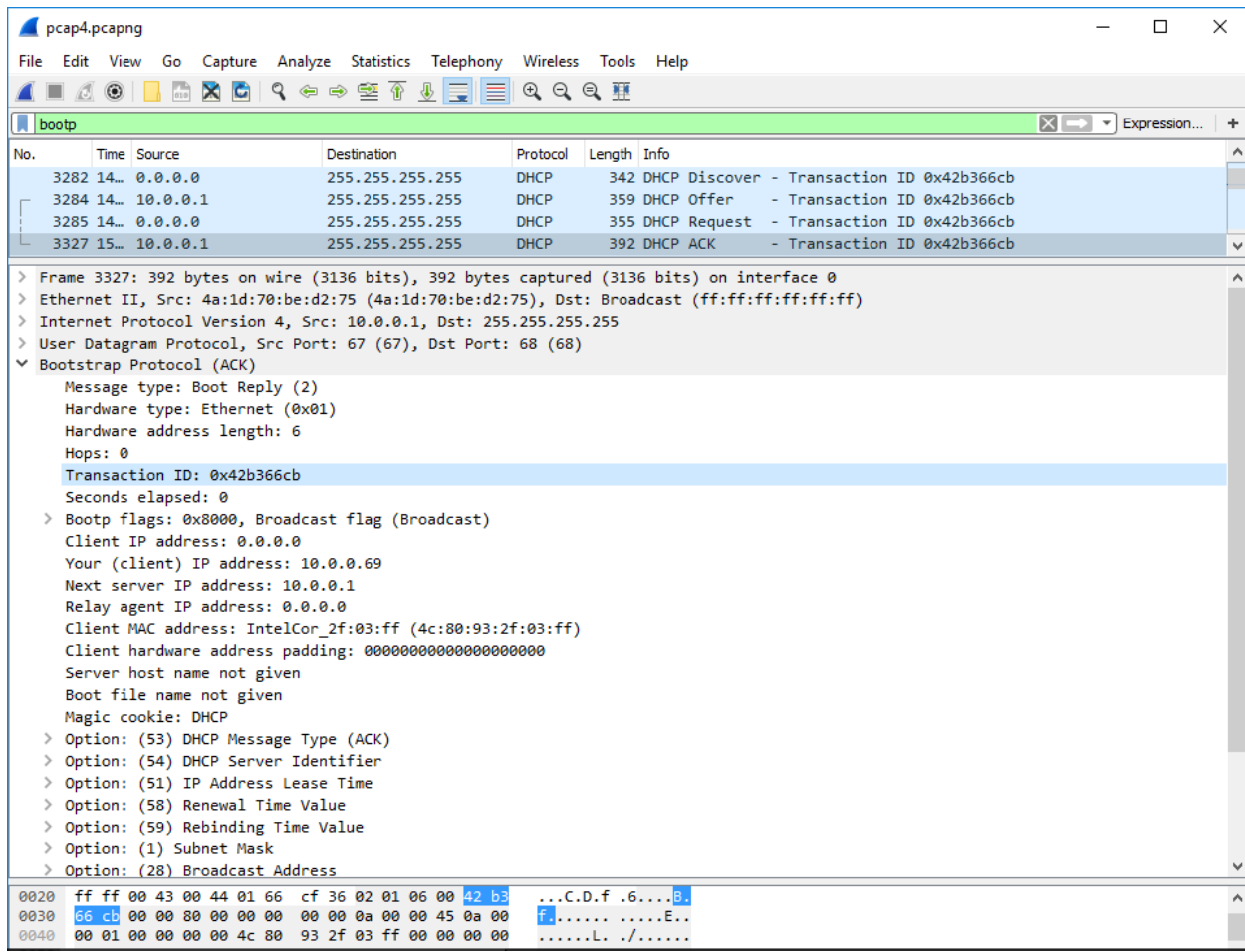
> Option: (81) Client Fully Qualified Domain Name

> Option: (60) Vendor class identifier

0020 ff ff 00 44 00 43 01 41 6e c8 01 01 06 00 b5 8b ...D.C.A n....

0030 45 95 00 00 80 00 00 00 00 00 00 00 00 00 00 00

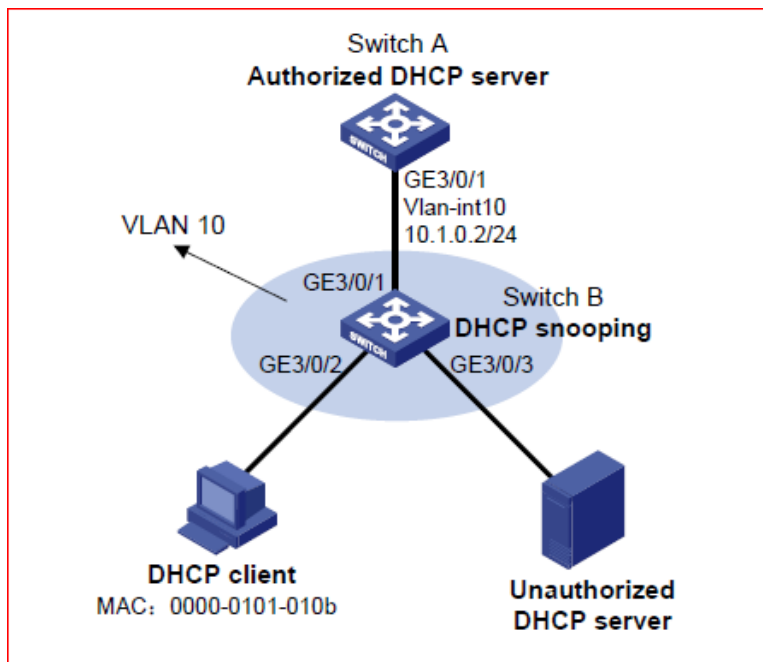
0040 00 00 00 00 00 00 4c 80 93 2f 03 ff 00 00 00 00L ./.....



DHCP Snooping

DHCP snooping is a security feature that acts like a firewall between untrusted hosts and trusted DHCP servers. The DHCP snooping feature performs the following activities:

- Validates DHCP messages received from untrusted sources and filters out invalid messages.
 - Rate-limits DHCP traffic from trusted and untrusted sources.
 - Builds and maintains the DHCP snooping binding database, which contains information about untrusted hosts with leased IP addresses.
 - Utilizes the DHCP snooping binding database to validate subsequent requests from untrusted hosts.
- Other security features, such as dynamic ARP inspection (DAI), also use information stored in the DHCP snooping binding database.



DHCP snooping is enabled on a per-VLAN basis. By default, the feature is inactive on all VLANs. You can enable the feature on a single VLAN or a range of VLANs.

The DHCP snooping feature is implemented in software on the route processor (RP). Therefore, all DHCP messages for enabled VLANs are intercepted in the PFC and directed to the RP for processing.

To enable DHCP Snooping globally, we need to perform following task:

	Command	Purpose
Step 1	Router(config)# ip dhcp snooping	Enables DHCP snooping globally.
Step 2	Router(config)# do show ip dhcp snooping include Switch	Verifies the configuration.

This example shows how to enable DHCP snooping globally:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip dhcp snooping
Router(config)# do show ip dhcp snooping | include Switch
Switch DHCP snooping is enabled
Router(config)#
```


Conclusion

Once a DHCP client has requested and established lease, it stores information about the lease in a file named `dhclient.leases`, which is stored in the `/var/lib/dhclient` directory.

This information is used to reconnect to the server using a lease when either the server or the client needs to reboot. The DHCP client configuration file, `/etc/dhclient.conf`, is required during custom configurations and is most commonly not used by the user, it's either done manually or automatically without user's consent.

DHCP as a whole does following activities

- Use IP address space optimally with periodic renewal of assigned IP addresses.
- Prevent IP address conflicts.
- Decrease time spent configuring and reconfiguring hosts on the network.