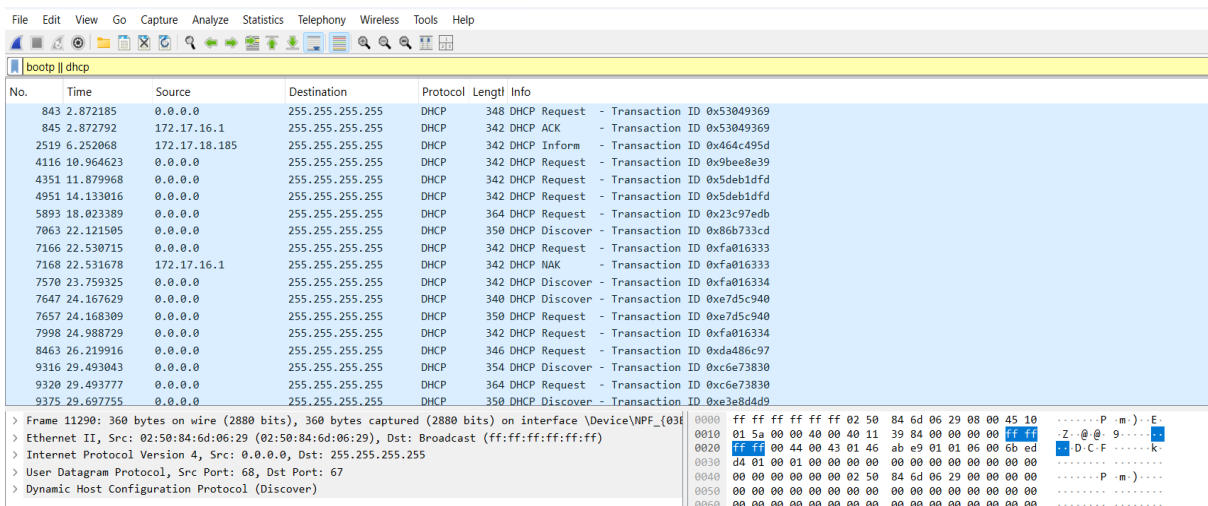


## 4) Use Wireshark to capture DHCP Discover, Offer, Request, and Acknowledge messages and explain the process.

When a device connects to a network, it follows DORA to get an IP from a DHCP server.



No.	Time	Source	Destination	Protocol	Length	Info
843	2.872185	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0x53049369
845	2.872792	172.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x53049369
2519	6.252068	172.17.18.185	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x464c495d
4116	10.964623	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x9bee8e39
4351	11.879968	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x5deb1dfd
4951	14.133016	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x5deb1dfd
5893	18.023389	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x23c97edb
7063	22.121505	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover - Transaction ID 0x86b73cd
7166	22.530715	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfa016333
7168	22.531678	172.17.16.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xfa016333
7570	23.759325	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xfa016334
7647	24.167629	0.0.0.0	255.255.255.255	DHCP	340	DHCP Discover - Transaction ID 0xe7d5c940
7657	24.168309	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0xe7d5c940
7998	24.988729	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfa016334
8463	26.219916	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0xda486c97
9316	29.493043	0.0.0.0	255.255.255.255	DHCP	354	DHCP Discover - Transaction ID 0xc6e73830
9320	29.493777	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xc6e73830
9375	29.697755	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover - Transaction ID 0xe3e8dd49

> Frame 11290: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF\_{03e...}

> Ethernet II, Src: 02:50:84:6d:06:29 (02:50:84:6d:06:29), 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)

bootp is used for DHCP messages.

```
C:\Users\brindha>ipconfig /release

Windows IP Configuration

No operation can be performed on Local Area Connection* 1 while it has its
No operation can be performed on Local Area Connection* 2 while it has its

Unknown adapter Local Area Connection*:

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

Wireless LAN adapter Local Area Connection* 1:

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

Wireless LAN adapter Local Area Connection* 2:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . : fe80::c6d3:c85d:d9bd:d131%3
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet1:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . : fe80::b902:56d5:7740:2ac3%2
    Default Gateway . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . : fe80::5684:b125:9f2:3f3e%10
    Default Gateway . . . . . :
```

No.	Time	Source	Destination	Protocol	Length	Info
843	2.872185	0.0.0.0	255.255.255.255	DHCP	348	DHCP Request - Transaction ID 0x53049369
845	2.872792	172.17.16.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x53049369
2519	6.252068	172.17.18.185	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x464c495d
4116	10.964623	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x9bee8e39
4351	11.879968	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x5deb1dfd
4951	14.133016	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x5deb1dfd
5893	18.023389	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x23c97edb
7063	22.121505	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover - Transaction ID 0x86b733cd
7166	22.530715	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfa016333
7168	22.531678	172.17.16.1	255.255.255.255	DHCP	342	DHCP NAK - Transaction ID 0xfa016333
7570	23.759325	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xfa016334
7647	24.167629	0.0.0.0	255.255.255.255	DHCP	340	DHCP Discover - Transaction ID 0xe7d5c940
7657	24.168309	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0xe7d5c940
7998	24.988729	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfa016334
8463	26.219916	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0xda486c97
9316	29.493043	0.0.0.0	255.255.255.255	DHCP	354	DHCP Discover - Transaction ID 0xc6673830
9320	29.493777	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xc6673830
9375	29.697755	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover - Transaction ID 0xe3e8d4d9
9626	30.622683	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover - Transaction ID 0xe3e8d4d9
9792	31.135308	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover - Transaction ID 0xe3e8d4d9
9980	31.949215	0.0.0.0	255.255.255.255	DHCP	346	DHCP Request - Transaction ID 0x724d5024
10516	33.488283	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x17763d60

> Frame 12900: 360 bytes on wire (2880 bits), 360 bytes captured (2880 bits) on interface \Device\NPF\_{03EF3B24-15EB-4AC0-BFD3-940B0EABDEB} (03EF3B24-15EB-4AC0-BFD3-940B0EABDEB), id 0  
 > Ethernet II, Src: 02:50:04:6d:06:29 (02:50:04:6d:06:29), 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)

Wireshark - Packet 843 - Wi-Fi

Section number: 1

- > Interface id: 0 (\Device\NPF\_{03EF3B24-15EB-4AC0-BFD3-940B0EABDEB})
- Encapsulation type: Ethernet (1)
- Arrival Time: Mar 13, 2025 14:20:45.886391000 India Standard Time
- UTC Arrival Time: Mar 13, 2025 08:50:45.886391000 UTC
- Epoch Arrival Time: 1741855845.886391000
- [Time shift for this packet: 0.000000000 seconds]
- [Time delta from previous captured frame: 0.000000000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 2.872185000 seconds]
- Frame Number: 843
- Frame Length: 348 bytes (2784 bits)
- Capture Length: 348 bytes (2784 bits)
- [Frame is marked: false]
- [Frame is ignored: false]
- [Protocols in frame: eth:ethertype:ip:udp:dhcp]
- [Coloring Rule Name: UDP]
- [Coloring Rule String: udp]

> Ethernet II, Src: AzureWaveTec\_A1:de:10 (28:08:43:41:de:10), Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
 > Destination: Broadcast (ff:ff:ff:ff:ff:ff)  
 > Source: AzureWaveTec\_A1:de:10 (28:08:43:41:de:10)  
 Type: IPv4 (0x0800)  
 [Stream index: 188]

> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255  
 > User Datagram Protocol, Src Port: 68, Dst Port: 67

0000 ff ff ff ff ff ff 28 d0 43 41 de 10 00 00 45 00 .....( CA---E  
 0010 01 de 02 dd 00 00 00 11 b6 c2 00 00 00 ff ff ..B---.....  
 0020 ff ff 00 44 00 43 01 3a a5 74 01 01 00 00 53 04 ...D.C.:t---S

No: 843 Time: 2.872185 Source: 0.0.0.0 Destination: 255.255.255.255 Protocol: DHCP Length: 348 Info: DHCP Request - Transaction ID 0x53049369

☒ Show packet bytes Layout: Vertical (Stacked)

## DHCP DORA Process

Client → DHCP Discover:

Broadcasts - Any DHCP servers out there?

Sent to 255.255.255.255

Server → DHCP Offer:

DHCP server replies: I have an IP for you

Offers an IP

Client → DHCP Request:

Client asks: I accept this IP, please assign it

Server → DHCP Acknowledge:

Server confirms: Done! You can use this IP.