

BAYANI, Femo Steven Felicisimo

2015-07104

Wireshark Lab 9: DHCP

CMSC 138

```
C:\WINDOWS\system32\cmd.exe
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* 12 while it has its media disconnected.
No operation can be performed on Local Area Connection* 14 while it has its media disconnected.
No operation can be performed on VPN64 - VPN Client while it has its media disconnected.
No operation can be performed on Ethernet 2 while it has its media disconnected.
No operation can be performed on ProtonVPN while it has its media disconnected.

Ethernet adapter Ethernet:

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

Wireless LAN adapter Local Area Connection* 12:

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

Wireless LAN adapter Local Area Connection* 14:

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

Ethernet adapter VPN64 - VPN Client:

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

Ethernet adapter Ethernet 2:

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

Ethernet adapter ProtonVPN:

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

Wireless LAN adapter Wi-Fi:

    Connection-specific DNS Suffix  . :
    Link-Local IPv6 Address . . . . : fe80::296e:1333:2c1f:6695%18
    IPv4 Address. . . . . : 192.168.1.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

1. Are DHCP messages sent over UDP or TCP?

DHCP messages are sent over **UDP**.

No.	Time	Source	Destination	Protocol	Length	Info
65	5.536464	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0xc6880447
147	9.478726	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0xc6880447
181	14.444...	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0xc6880447
187	14.450...	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0xc6880447
188	14.450...	0.0.0.0	255.255.255...	DHCP	357	DHCP Request - Transaction ID 0xc6880447
189	14.457	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK - Transaction ID 0xc6880447

> Frame 65: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0

> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), 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

Source Port: 68

Destination Port: 67

Length: 308

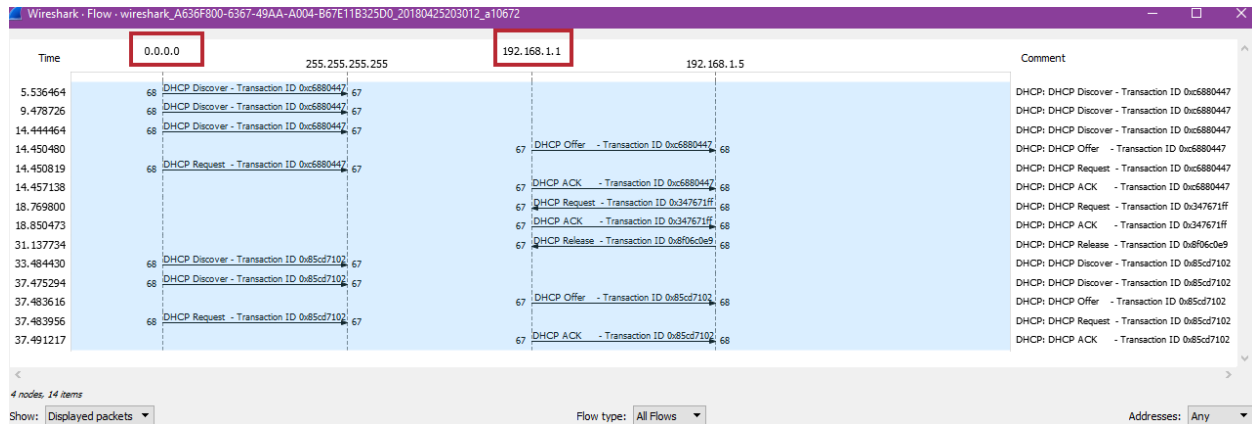
Checksum: 0x889c [unverified]

[Checksum Status: Unverified]

[Stream index: 19]

> Bootstrap Protocol (Discover)

- Draw a timing diagram illustrating the sequence of the first four-packet. Discover/Offer/Request/Ack DHCP exchange between client and server. For each packet, indicate the source and destination port numbers.



- What is the data link layer (e.g. Ethernet) address of your host?

The data link layer address of my host is **54:27:1e:15:fd:65**.

No.	Time	Source	Destination	Protocol	Length	Info
181	14.444...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc6880447
187	14.450...	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0xc6880447
188	14.450...	0.0.0.0	255.255.255.255	DHCP	357	DHCP Request - Transaction ID 0xc6880447
189	14.457...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK - Transaction ID 0xc6880447
452	18.769...	192.168.1.5	192.168.1.1	DHCP	345	DHCP Request - Transaction ID 0x347671ff
453	18.850...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK - Transaction ID 0x347671ff

>	Frame 181: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
>	Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
>	Destination: Broadcast (ff:ff:ff:ff:ff:ff)
>	Source: Azurewav_15:fd:65 (54:27:1e:15:fd:65)
>	Type: IPv4 (0x0800)
>	Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
>	User Datagram Protocol, Src Port: 68, Dst Port: 67

- What values in the DHCP Discover message differentiate this message from the DHCP Request message?
 - DHCP Message Type
 - Request has DHCP Server Identifier
 - Request has Client Fully Qualified Domain Name

Net	Time	Source	Destination	Protocol	Length	Info
181	14.444...	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0xc6880447
187	14.450...	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0xc6880447
188	14.450...	0.0.0.0	255.255.255...	DHCP	357	DHCP Request - Transaction ID 0xc6880447
189	14.457...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK - Transaction ID 0xc6880447
452	18.769...	192.168.1.5	192.168.1.1	DHCP	345	DHCP Request - Transaction ID 0x347671ff
453	18.850...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK - Transaction ID 0x347671ff

```
> User Datagram Protocol, Src Port: 68, Dst Port: 67
```

- ▼ Bootstrap Protocol (Discover)

```
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xc6880447
```

Transaction ID: 0xc6880447

```
> Seconds elapsed: 4
```

```
> 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: Azurewav_15:fd:65 (54:27:1e:15:fd:65)
```

```
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: 0000000000

188	14.450...	0.0.0.0	255.255.255...	DHCP	357	DHCP Request	- Transaction ID 0xc6880447
189	14.457...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK	- Transaction ID 0xc6880447
452	18.769...	192.168.1.5	192.168.1.1	DHCP	345	DHCP Request	- Transaction ID 0x347671ff
453	18.850...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK	- Transaction ID 0x347671ff

▼ Bootstrap Protocol (Request)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xc6880447

> Seconds elapsed: 4

> 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: Azurewav_15:fd:65 (54:27:1e:15:fd:65)

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

> Option: (55) Parameter Request List

> Option: (255) End

5. What is the value of the Transaction-ID in each of the first four (Discover/Offer/Request/ACK) DHCP messages? What are the values of the Transaction-ID in the second set of DHCP messages? What is the purpose of the Transaction-ID field?

All the four DHCP messages have the same Transaction ID: **0xc6880447**.

No.	Time	Source	Destination	Protocol	Length	Info
181	14.444...	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0xc6880447
187	14.450...	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0xc6880447
188	14.450...	0.0.0.0	255.255.255...	DHCP	357	DHCP Request - Transaction ID 0xc6880447

> Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), 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

▼ Bootstrap Protocol (Discover)

Message type: Boot Request (1)

Hardware type: Ethernet (0x01)

Hardware address length: 6

Hops: 0

Transaction ID: 0xc6880447

> Seconds elapsed: 4

> Bootp flags: 0x0000 (Unicast)

The second set of DHCP messages all have the same Transaction ID: **0x85cd7102**.

1020	37.475...	0.0.0.0	255.255.255...	DHCP	342	DHCP Discover - Transaction ID 0x85cd7102
1026	37.483...	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0x85cd7102
1027	37.483...	0.0.0.0	255.255.255...	DHCP	357	DHCP Request - Transaction ID 0x85cd7102

> Frame 1020: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
 > Ethernet II, Src: Azurewav_15:fd:65 (54:27:1e:15:fd:65), 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
 > Bootstrap Protocol (Discover)
 Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0x85cd7102
 Seconds elapsed: 0

The Transaction ID field is different from each set of messages so that the host can differentiate different requests.

- A host uses DHCP to obtain an IP address, among other things. But a host's IP address is not confirmed until the end of the four-message exchange. If the IP address is not set until the end of the four-message exchange, then what values are used in the IP datagrams in the four-message exchange? For each of the four DHCP messages (Discover/Offer/Request/ACK), indicate the source and destination IP addresses that are carried in the encapsulating IP datagram.

Discover: 0.0.0.0 -> 255.255.255.255

Offer: 192.168.1.1 -> 192.168.1.5

Request: 0.0.0.0 -> 255.255.255.255

ACK: 192.168.1.1 -> 192.168.1.5

No.	Time	Source	Destination	Protocol	Length	Info
181	14.444...	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xc6880447
187	14.450...	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0xc6880447
188	14.450...	0.0.0.0	255.255.255.255	DHCP	357	DHCP Request - Transaction ID 0xc6880447
189	14.457...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK - Transaction ID 0xc6880447

- What is the IP address of your DHCP server?

The IP address of my DHCP server is **192.168.1.1**.

No.	Time	Source	Destination	Protocol	Length	Info
187	14.450...	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0xc6880447
188	14.450...	0.0.0.0	255.255.255.255	DHCP	357	DHCP Request - Transaction ID 0xc6880447
189	14.457...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK - Transaction ID 0xc6880447

✓ Bootstrap Protocol (Request)
 Message type: Boot Request (1)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0xc6880447
 > Seconds elapsed: 4
 > 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: Azurewav_15:fd:65 (54:27:1e:15:fd:65)
 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
 Length: 4
 DHCP Server Identifier: 192.168.1.1
 > Option: (12) Host Name
 > Option: (81) Client Fully Qualified Domain Name

8. What IP address is the DHCP server offering to your host in the DHCP Offer message? Indicate which DHCP message contains the offered DHCP address.

The IP address that the DHCP server is offering to my host is **192.168.1.5**.

No.	Time	Source	Destination	Protocol	Length	Info
187	14.450...	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer - Transaction ID 0xc6880447
188	14.450...	0.0.0.0	255.255.255.255	DHCP	357	DHCP Request - Transaction ID 0xc6880447
189	14.457...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK - Transaction ID 0xc6880447

Message type: Boot Reply (2)
 Hardware type: Ethernet (0x01)
 Hardware address length: 6
 Hops: 0
 Transaction ID: 0xc6880447
 Seconds elapsed: 0
 > Bootp flags: 0x0000 (Unicast)
 Client IP address: 0.0.0.0
 Your (client) IP address: 192.168.1.5
 Next server IP address: 192.168.1.1
 Relay agent IP address: 0.0.0.0
 Client MAC address: Azurewav_15:fd:65 (54:27:1e:15:fd:65)

9. Is there a relay agent between the host and the DHCP server? If yes, what is the IP address of the relay agent? If none, how did you know there is none?

10. Explain the purpose of the router and subnet mask lines in DHCP offer message.
11. Explain the purpose of the lease time. How long is the lease time in your experiment?

The purpose of the lease time is to tell the client how long it can use the IP address until it is reassigned a new IP address.

The lease time in my experiment is **2959200 seconds or 3 days**.

187	14.450...	192.168.1.1	192.168.1.5	DHCP	342	DHCP Offer	- Transaction ID 0xc6880447
188	14.450...	0.0.0.0	255.255.255.255	DHCP	357	DHCP Request	- Transaction ID 0xc6880447
189	14.457...	192.168.1.1	192.168.1.5	DHCP	590	DHCP ACK	- Transaction ID 0xc6880447


```

Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0xc6880447
Seconds elapsed: 0
> Bootp flags: 0x0000 (Unicast)
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.1.5
Next server IP address: 192.168.1.1
Relay agent IP address: 0.0.0.0
Client MAC address: Azurewav_15:fd:65 (54:27:1e:15:fd:65)
Client hardware address padding: 00000000000000000000
Server host name: P-660HN-T1 v2
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Offer)
> Option: (1) Subnet Mask
> Option: (3) Router
> Option: (6) Domain Name Server
> Option: (15) Domain Name
> Option: (58) Renewal Time Value
> Option: (59) Rebinding Time Value
▼ Option: (51) IP Address Lease Time
  Length: 4
  IP Address Lease Time: (259200s) 3 days

```

12. What is the purpose of the DHCP release message? Does the DHCP server issue an acknowledgement of receipt of the client's DHCP request? What would happen if the client's DHCP release message is lost?

The purpose of the DHCP release message is to release the IP address back to the server.

There is no acknowledgement from the DHCP server that the DHCP request has been received.

If the message is lost, the client releases the IP address, but the server will not reassign that address until the client's lease on the address expires.

13. Clear the bootp filter from your Wireshark window. Were any ARP packets sent or received during the DHCP packet exchange period? If so, explain the purpose of those ARP packets.

Yes, there were ARP packets sent.

The purpose of these ARP packets are used to recognize and find the IP addresses of other machines in the network.

162	10.089...	169.254.1...	169.254.255.255	NBNS	92	Name query NB DPMUGUPFRWEV<00>
163	10.090...	169.254.1...	169.254.255.255	NBNS	92	Name query NB FULLTYOKL<00>
164	10.123...	ZyxelCom_...	Broadcast	ARP	60	Who has 192.168.1.5? Tell 192.168.1.1
165	10.162...	169.254.1...	169.254.255.255	NBNS	92	Name query NB HPAD<00>
166	10.145...	169.254.1...	169.254.255.255	NBNS	92	Name query NB HPAD<00>