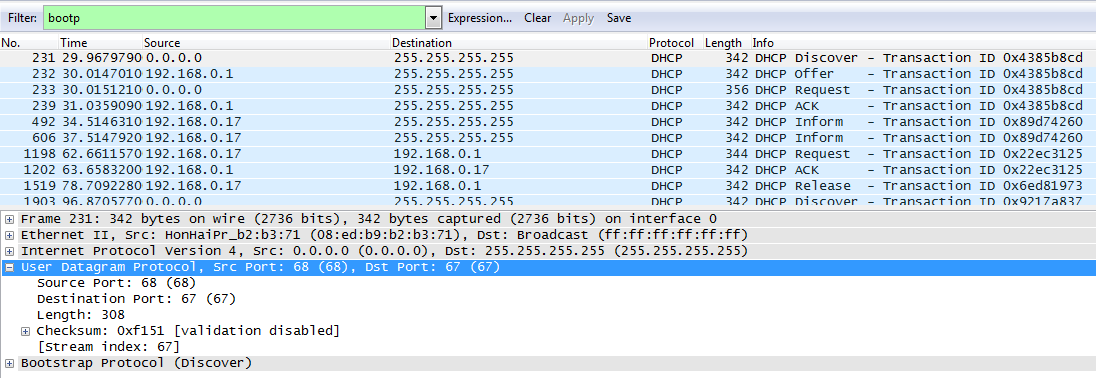
**Title of the Lab:** Wireshark / DHCP

**Name:** MITHUN MARAGIRI

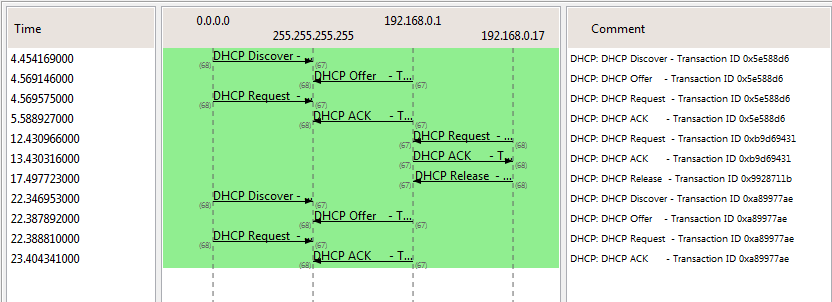
**Session #:** 2

1. DHCP packets are sent over UDP.

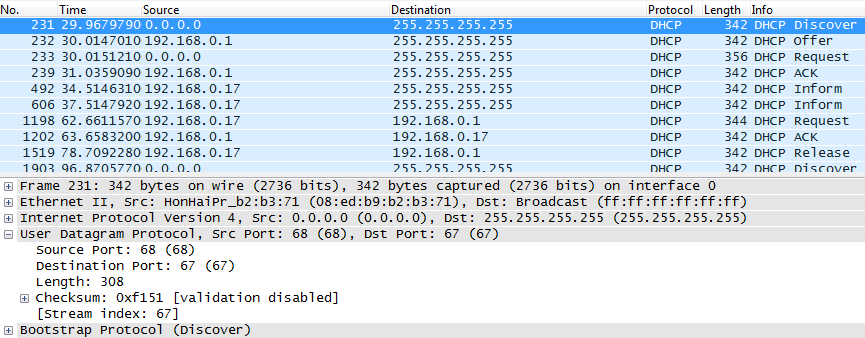


As highlighted in the above snapshot, User Datagram Protocol is used as the transport layer protocol with src port (client port) as 68 and Dst port (Server port) as 67.

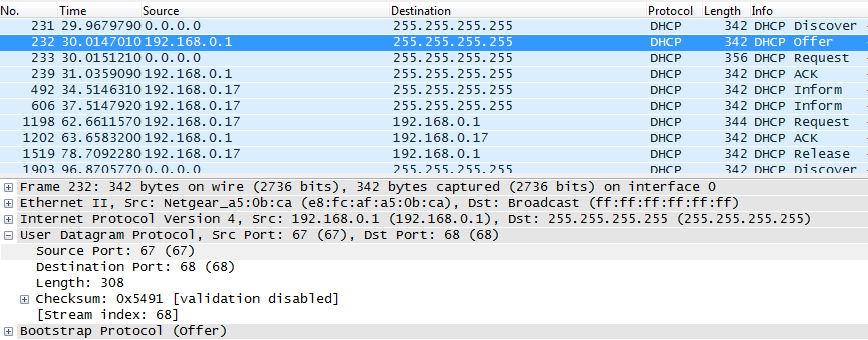
1. Timing Diagram with Port Numbers



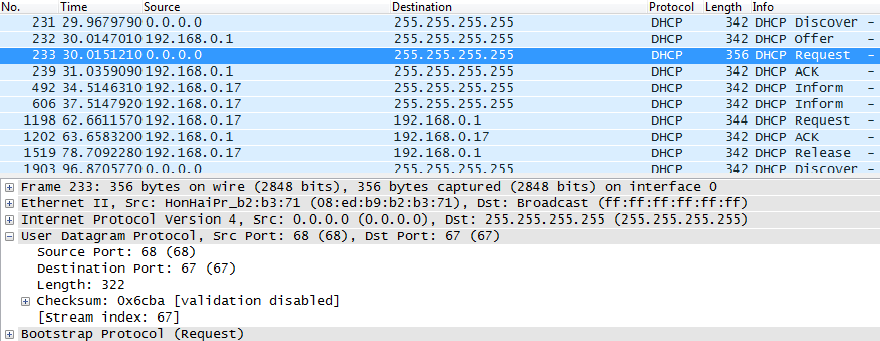
Discover Msg: Source Port : 68, Dest Port:67



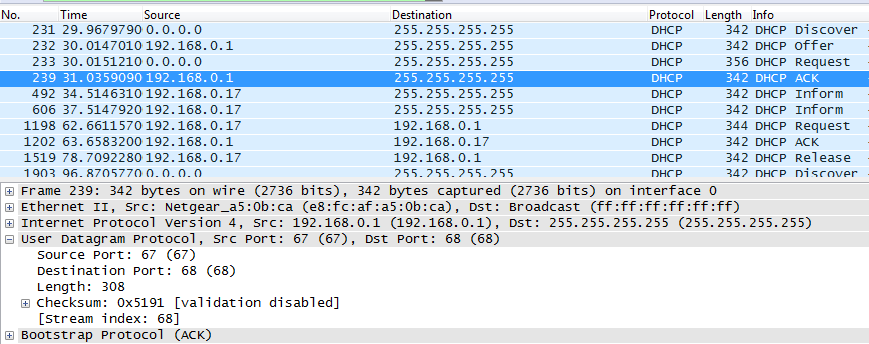
Offer Msg: Source Port :67, Dest Port: 68



Request Msg: Source Port:68 , Destination Port: 67

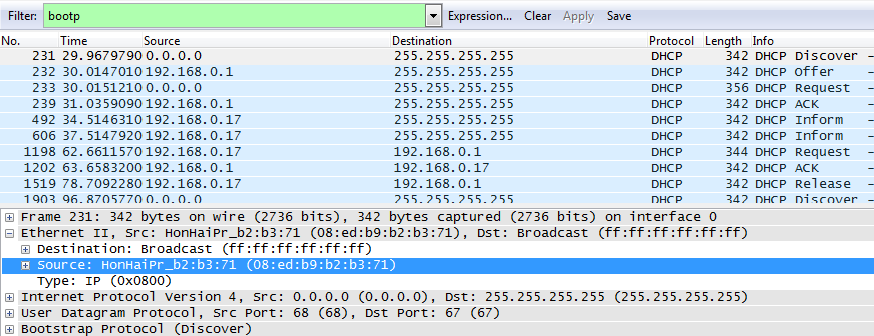


ACK msg: Source Port: 67, Dest Port: 68



Yes the port numbers are the same as given in the lab assignment. DHCP uses standard ports for both client and server. Client uses the port number 68 and server uses the port number 67. The reason for both client and server using standard port numbers is because client will not have IP address during boot, so if client uses random port number assigned by Network OS then for every client the port number will be random and DHCP server will have to reply to each of these client requests on different ports.

1. The link layer (Ethernet) address of my host is **HonHaiPr\_b2:b3:71 (08:ed:b9:b2:b3:71)**

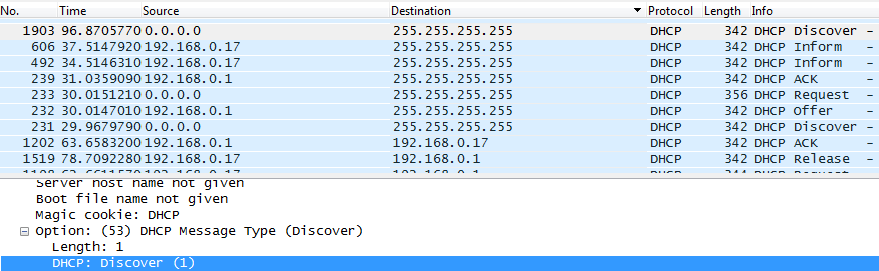


1. The optional Parameter called “DHCP Message Type” will help in differentiating the Discover message from Request message.

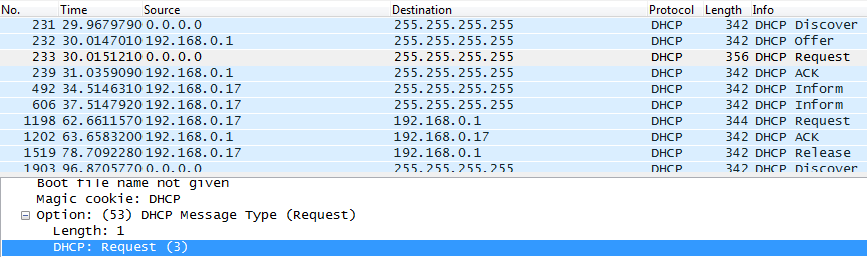
Value of DHCP Message Type for Discover Msg: 1

Value of DHCP Message Type for Request Msg: 3

Discover Message with DHCP Message Type Value as 1.

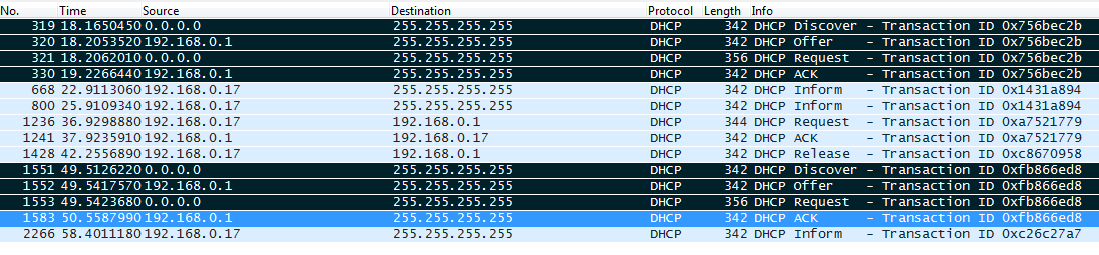


Request Message with DHCP Message Type value 3:



1. The value of Transaction ID for the first four DHCP messages (Dicover/Offer/Request/Ack)is **0x756bec2b**

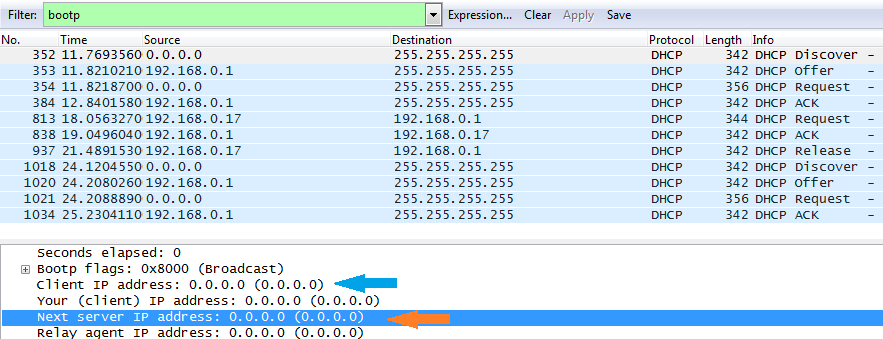
The value of Transaction ID for the second set of DHCP messages is **0xfb866ed8**



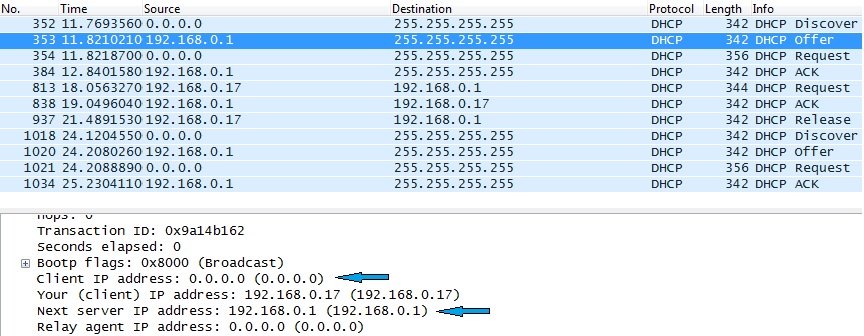
Transaction ID field is used to differentiate the different clients who send request messages to DHCP server. Since the client port and server port are the standard ports, all clients send requests from port 68 to port 67 hence for the DHCP server to distinguish the different clients Transaction ID field is used. Also the transaction ID identifies if a message is part of a set of messages related to one transaction.

1. IP address details for the 4 DHCP messages

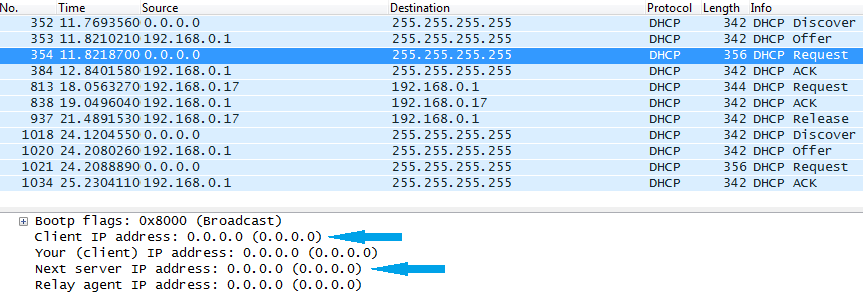
* Discover Message: Message sent as a broadcast with Dst Ip 255.255.255.255
  + Client IP address: 0.0.0.0
  + Server IP address : 0.0.0.0



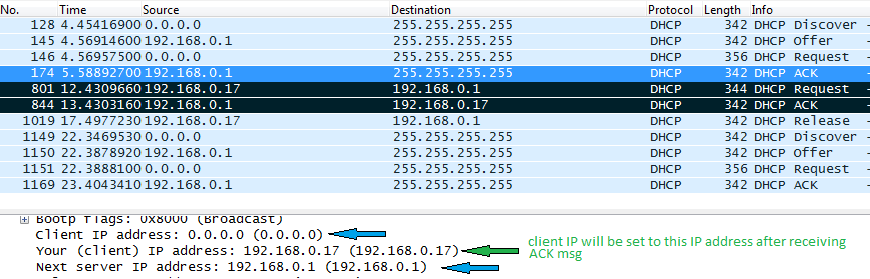
* Offer Message: Message sent as a broadcast with Dst IP 255.255.255.255
  + Client IP address: 0.0.0.0
  + Server IP address: 192.168.0.1



* Request Message: Message sent as a Broadcast with Dst IP 255.255.255.255
  + Client IP address: 0.0.0.0
  + Server IP address: 0.0.0.0



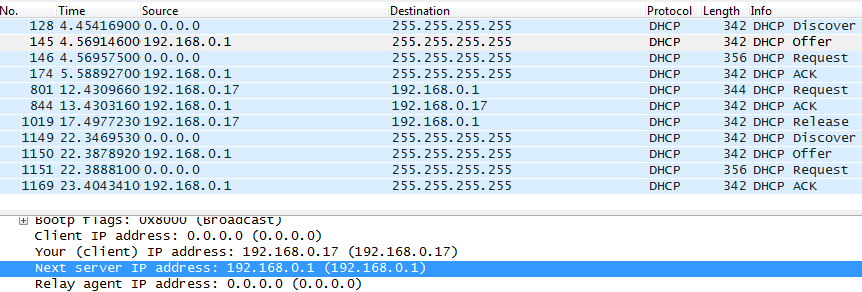
* ACK Message: Message is sent as a broadcast with Dst IP 255.255.255.255
  + Client IP Address: 0.0.0.0
  + Server IP Address: 192.168.0.1



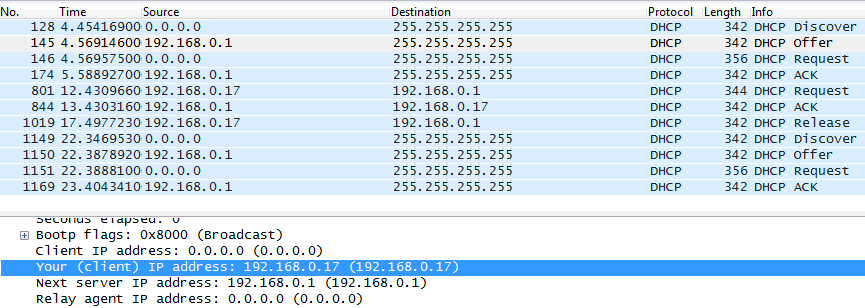
Note that the IP address of Client is still set to 0.0.0.0 during ACK message, this is because the IP address for the client will be set with “Your IP address” once the ACK is received. Until it’s received the IP address will be 0.0.0.0. As a proof of that notice the 2 messages highlighted in black which are the second renew / ACK messages. In these messages the IP address of client is updated with the IP address mentioned in Your Client IP address.

1. IP address of my DHCP server is 192.168.0.1

Since the relay agent IP address is 0.0.0.0 there is no relay agent server hence “Next Server IP” is the DHCP server.

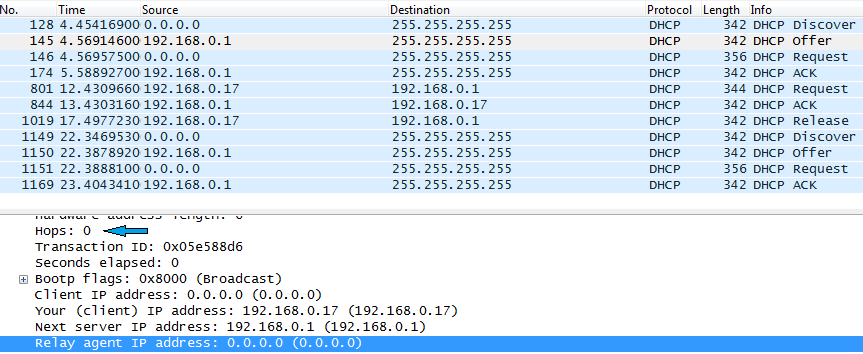


1. DHCP Server is offering my host the IP address 192.168.0.17



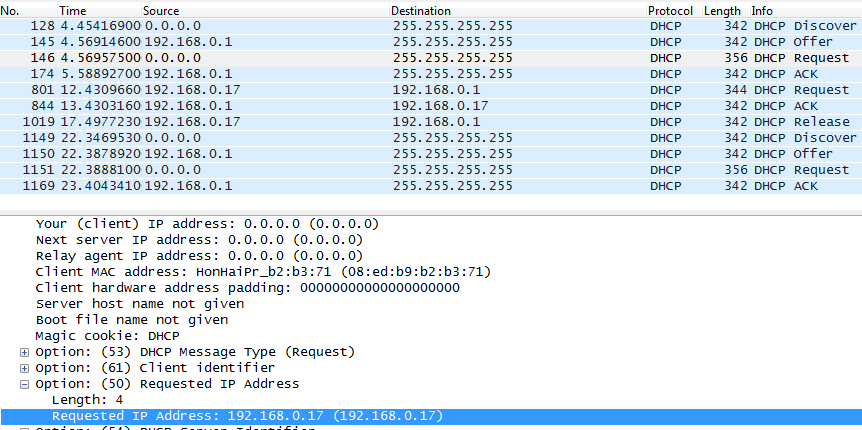
The DHCP Offer message contains the offered DHCP address. This offered address will be in the Your IP address parameter.

1. From the Trace Message we can observe that the “Relay Agent IP address” is set to 0.0.0.0. This parameter indicate the absence of relay agent.

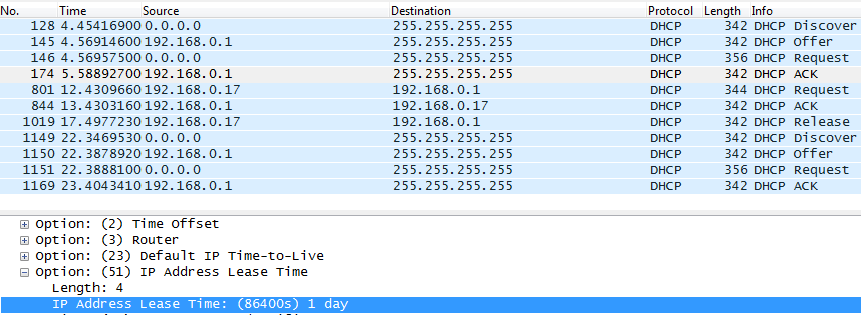


There is no relay agent in my experiment.

1. The IP address of the router identifies the default internet gateway. The subnet mask defines the subnet of the network that is available; the network part of the IP address is determined by subnet mask.
2. Usually the client will accept the IP address offered by first DHCP server. The client’s requested IP address will be in the optional parameter list of the DHCP REQUEST message.



1. Lease time is the amount of time the user can use the IP address assigned to the host. Purpose of the lease time could be to control the accessibility of network by the user. In café or airports lease time will be very effective where we cannot access internet after the lease time. The lease time in my experiment is 1 day (86400s)



1. The Release message is a request from the client to DHCP server to cancel the IP address assigned to it. NO the DHCP server will not issue any acknowledgement for the received DHCP release request message. If the Client’s Release request message is lost then the IP address will be retained till the lease period. The client will have to send the release message again if it wants to release the IP address before lease time.
2. Yes there was ARP packets sent / received during DHCP packet exchange period. When the client sends DHCP REQUEST message to DHCP server, the DHCP server before acknowledging to the requested IP address will execute ARP. This is to check if any other client is assigned the same IP address. If no client replies for the ARP of DHCP server then the IP address if free and DHCP server will acknowledge the DHCP request.

