**SAN JOSE STATE UNIVERSITY**

**Charles W. Davidson College of Engineering**

**DEPARTMENT OF COMPUTER ENGINEERING**

**CMPE-208 Network Architecture and Protocols**



**By**

**Group #1**

**Jeevan Venkataramana (011917477)**

**Pavan Haravu Ramesh(011875318)**

**Roopashree Munegowda(012235834)**

**Sai Sree Vaishnavi Chittoori (012415130)**

**Submitted to**

**Prof. Shai Silberman**

**Department of computer Engineering**

**SAN JOSE STATE UNIVERSITY**

**October 7, 2018**

1. **Contributions:**

|  |  |
| --- | --- |
| **Name** | **Task** |
| Jeevan Venkataramana | Analysis of routing information |
| Pavan Haravu Ramesh | Analysis of DHCP messages using wireshark |
| Roopashree | Lab setup and Execution |
| Sai Sree Vaishnavi Chittoori | Configure DHCP server on Mininet |

**2) Objective:**

The purpose of this lab is to observe and analyze the working of Dynamic Host Configuration Protocol. A sample topology is setup on GNS3 and wire-shark is used for packet captures.

**3) Introduction**

For initial configuration of a TCP/IP protocol suite for a host connected to a network requires some basic information about the network. Some basic info include Subnet Mask, Router info, Domain name server, Domain name so on. Dynamic Host Configuration Protocol(DHCP) is a agent that facilities basic information to the newly configured host. A server acts as an agent supporting DHCP for the network. The design of DHCP is based on Bootstrap Protocol. The bootstrap protocol carries basic information relating to the host to the DHCP server. It mainly sends Mac address and Hostname and requests a list of details required to configure the host to the network.

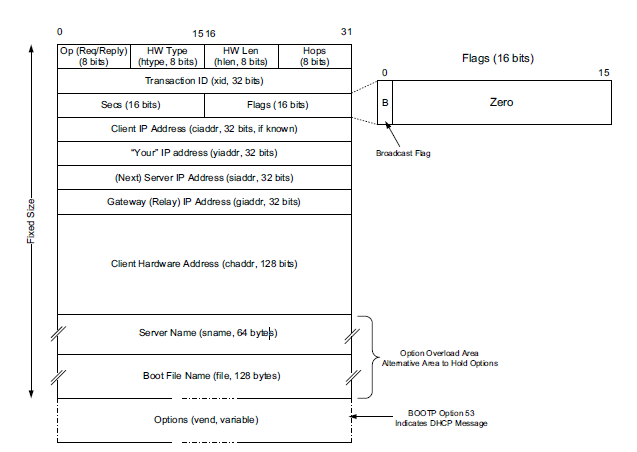
DHCP (Dynamic Host Configuration Protocol) is a protocol used to configure the components in a network. A server called DHCP server will be maintained in the network for this purpose where the network components communicate with it to get its configuration to access the network. Obtaining the configuration involves getting the IP address, network mask, router IP address, DNS server address and more.

This is the most efficient way of the configuring the hosts (dynamic allocation) compared to other type of the configurations such as manual and automatic allocation where the network administrator should manually take care of configuring the hosts in the network. In manual allocation type, the configuration of the network component will be done by the network administrator physically and in the automatic allocation, the configuration done for a network component cannot be revoked. The concept called leasing is used in the dynamic allocation which the DHCP protocol typically uses, where the assignment of configuration for the network components hold good for a specific amount time. The network components can extend or renew the lease for further access to the network. Predecessor to DHCP was BOOTP (Internet Bootstrap Protocol) in which the address allocation is permanent, i.e. Manual allocation.

Assigning the IP addresses with the help of DHCP server makes the job easy of keeping a track of the devices and configuring them properly or in a synchronized manner to make the devices communicate efficiently using the network. IN a single network there can be more than one DHCP servers to assign IP addresses to clients/devices in the network. In a single network there can be more than one DHCP servers to assign IP addresses to clients/devices in the network.

**DHCP and BOOTP message format:**

The DHCP Message packets extends most of the properties from the BOOTP message so that the DHCP can be used in the network where the BOOTP is used as well as the BOOTP can be used in the network where only DHCP is used. Typically, the all the information that is not used in the BOOTP will be considered as the options in the DHCP. The message format for the DHCP and BOOTP is as shown below.



**OP (Reply/Request):** The op (Option) is 8 bits wide which defines whether the DHCP message is a request or Reply. For the Request DHCP packet, the Op field will be set as 1 and for the Reply DHCP packet, the Op field will be set as 2.

**HW Type:** HW Type (Hardware Type) field is 8 bits wide which defines which hardware type is being used for the network component. For example, for the hosts of a network this field is set as 1 which means that the Ethernet is used to access the network. The value for the different hardware type is defined in the IANA APR parameter page.

**HW Length:** HW Length (Hardware Length) is 8 bits wide which will be used to define how much bytes will be used to define the hardware address of a component. For the mac-address this field will be set as 6.

**Hops:** This is 8 bits wide which will be used to define how many hops that the hosts need to cross the DHCP server to gets its configuration. This field helps the host to decide which DHCP server can be used to gets its configuration from the network which has the multiple DHCP networks.

**Transaction ID:** This is the 32 bits wide used to assign unique ID to each DHCP message that is being assigned from the host to get its configuration from the DHCP server. This will be used to match the different packets that is being involved in the DHCP protocol.

**Sec:** This is the 16 bits wide field used to note down the number of seconds that is being taken for the DHCP message transaction between the host and the DHCP server. This field will be set to zero by the host during broadcasting the DHCP discover message to the network.

**Flags:** It is 6 bits wide but currently only one bit is used to define whether the host can attend unicast messages also or it can attend the broadcast messages only. This helps the DHCP server whether the host is interesting in attending only broadcast message or the unicast message only.

**Client IP address (ciaddr):** This is 32 bits wide used to hold the current IP address of the host requesting the DHCP server if known. Otherwise this field will be set as 0.

**Your IP address (yaddr):** This is 32 bits wide used by the DHCP server to mention what IP address it can offer to the host which is requesting the configuration.

**(Next) server IP address:** The Next Server IP Address (siaddr) field 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)

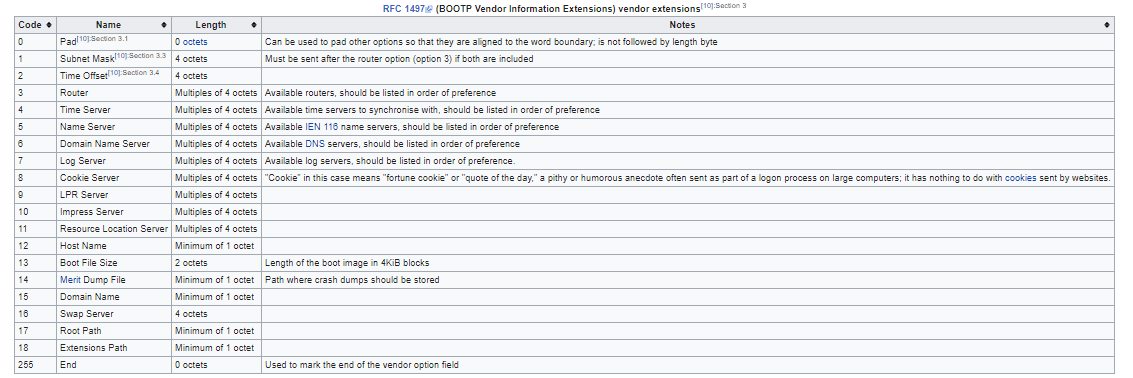
**The Gateway (or Relay) IP Address (giaddr):** This field is 32 bits wide and filled in by a DHCP or BOOTP relay with its address when forwarding DHCP (BOOTP) messages.

**The Client Hardware Address (ciaddr):** This is a 128 bits wide field which is used hold the unique identifier of the host such as the mac address. This will be used by the DHCP server to link the configuration that it has assigned to a particular host.

**Server Name (sname) and 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. This field can also be used to take some options that we define in next section.

**Option:** This is a variable length field that is used to get the extra information that the hosts and the DHCP server that exchanges in getting the configuration to access the network. All the options have a specific format where the option defined with the option tag which is unique for each option followed by the option value. Some options have the option tag followed by defined size of option value and all other have the format of having the option tag followed by option length defining the size of the option field and option value which contains the value for specific option.

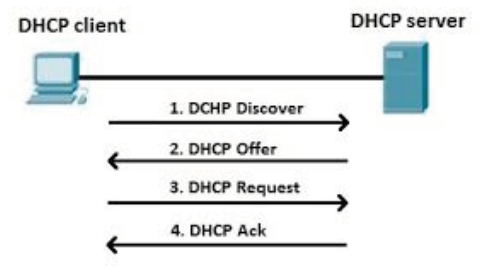
A large number options are being defined for the DHCP of which some of them are used by the BOOTP also. Example for options are given below.



**Reference:** <https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#DHCP_options>

**4) DHCP Process**

DHCP operates based on client server model. The DHCP client broadcast a discover packet requesting necessary information. The above figure describes the normal process of obtaining an IP address for a newly connected host.



The below process was observed over sjsu campus wifi

**DHCP Discover packet**:

The DHCP discover packet is a broadcast request for ip address. The DHCP server will respond for such requests.

1. Ethernet field: destination assigned ff ff ff ff ff ff and source as the client ethernet address.
2. IP field: Destination ip assigned to ff ff ff ff and source ip assigned to 00 00 00 00 initially
3. Transport field: UDP with source port 68 and destination port 67
4. Bootstrap Protocol field:

sends

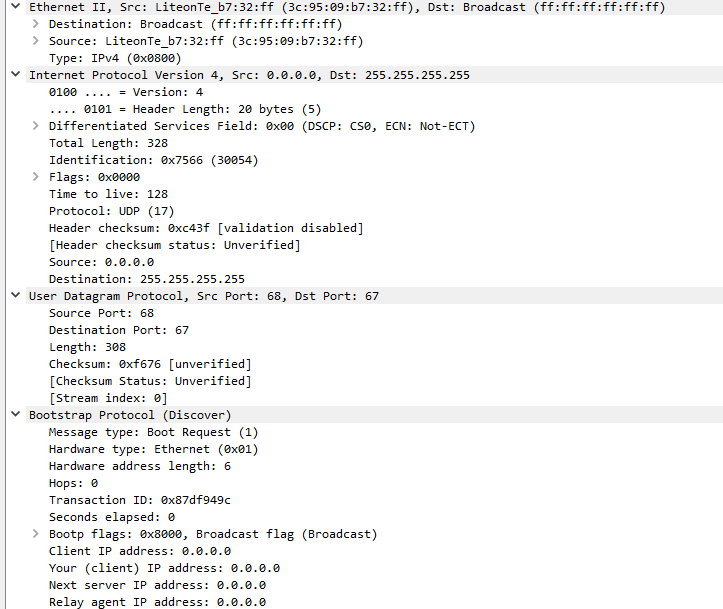
Client Mac address: Mac address of host

Message Type: DHCP Disover

Host Name: Client host name

Parameter request list:

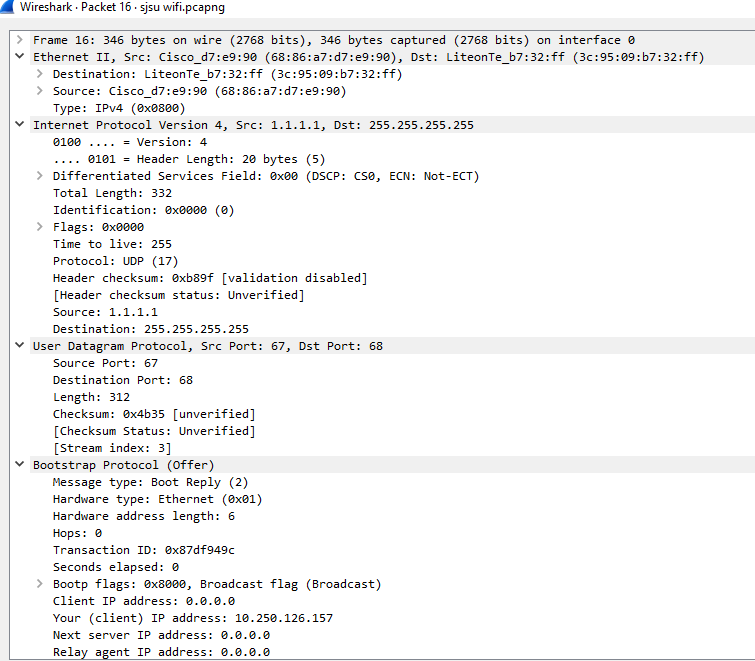
* 1. Subnet Mask
  2. Router info
  3. Domain name server
  4. Domain name
  5. Router Discover
  6. Domain search
  7. Classless static route



**DHCP Offer**:

An Offer packet broadcasted by the DHCP server configured on the network. The offer packet mainly contains the below list of information. The offer packet sends the information requested in the parameter list of discover packet.

1. DHCP server ip address 🡪 A IP address recognized by the router for DHCP server related activity
2. Assigned client IP address
3. IP lease duration
4. Message type – DHCP offer
5. DHCP server identifier
6. Subnet Mask
7. Assigned Router information
8. Domain name server ip address
9. Domain name



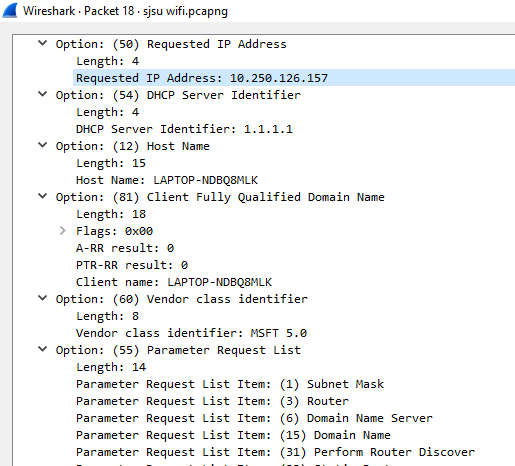
**DHCP Request**:

The DHCP request is broadcasted by the client hoping for an acknowledgement from the DHCP server. This requests is sent in response to Offer packet. However the client still not configured with the DHCP server provided IP address. The client includes some additional details in this request. It send the information sent by offer packet along with the requested IP address. This address is mostly the previous assigned ip address of the client over the same network.

Additional Information contained in DHCP request:

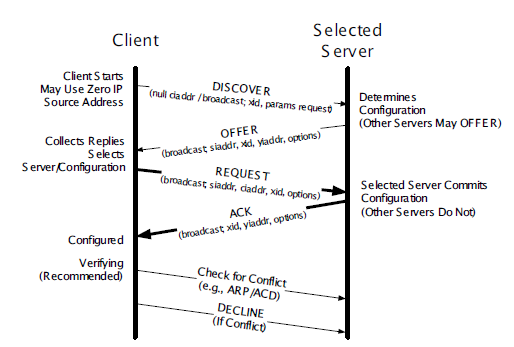
DHCP server identifier

Requested Ip address



**DHCP Acknowledgement**:

This is a packet broadcasted by the DHCP server confirming the details it sent over the offer. If any modifications required the DHCP server responds with a Negative acknowledgement requesting the whole process to be done again. The DHCP acknowledgement packet is more or less contains the same information carried by the DHCP offer packet.

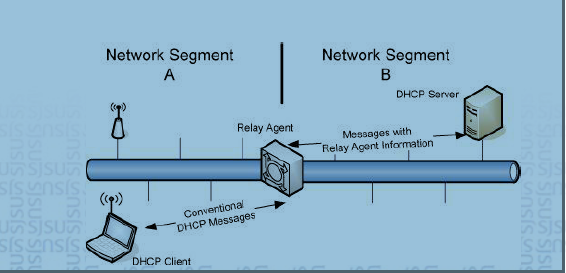


The above picture just denotes the DHCP process.

**Using relays with DHCP:**

The relays forward the messages from client to DHCP sever and it may annotate the messages by defining some extra options or by defining the empty field. The relays are often used in the network with DHCP server which blocks the broadcast messages and sends a unicast message to the DHCP server. It also sends the DHCP messages called DHCP lease query messages to the DHCP Server to get the information about the clients.

The DHCP sever responds with the DHCPLEASEUNASSIGNED, DHCPLEASEACTIVE or DHCPLEASEUNKNOWN to inform the status of the client with respect to the DHCP server.

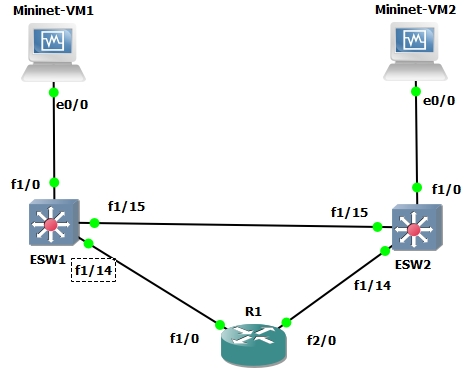


**5) Lab setup environment**

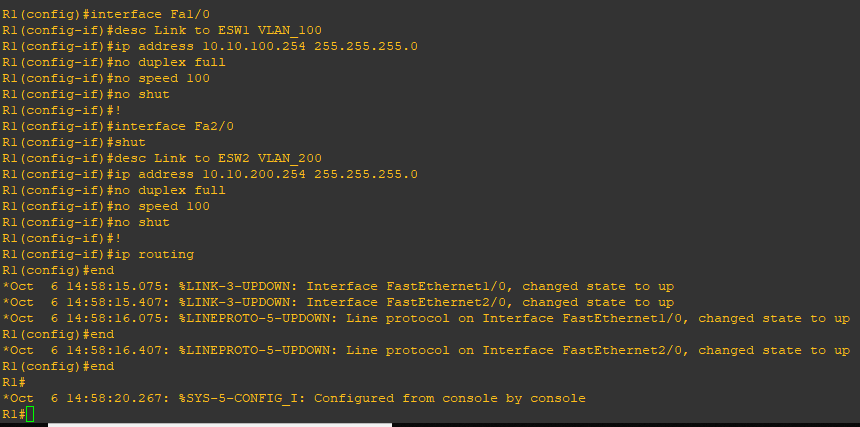
Network built using GNS3

Packet Captures done through wire-shark

**6) Topology:**

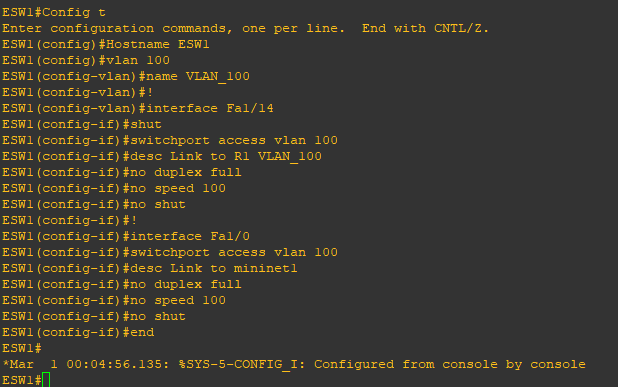


7) Configuration on R1

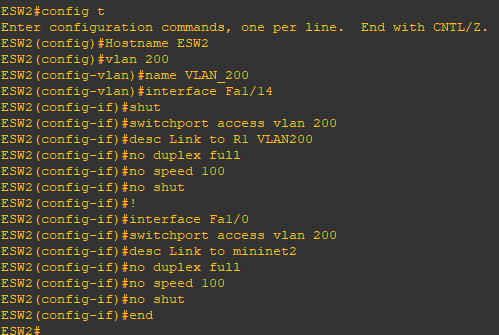


Configuring router R1. As shown in the topology the router has 2 interface f1/0 and f2/0. Each interface is configured to a VLAN and assigned separate ip address.

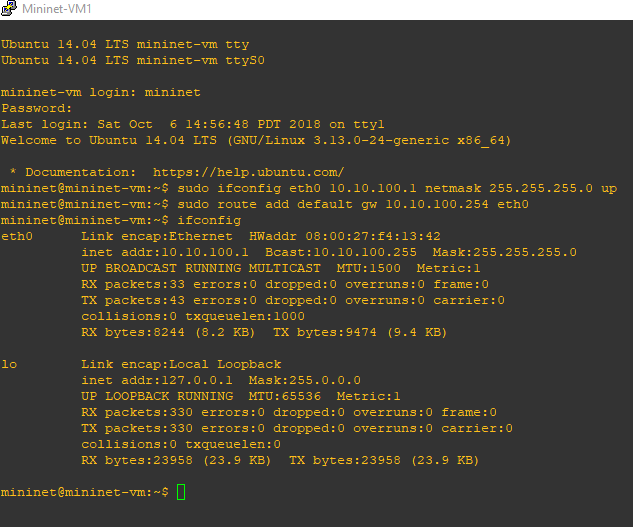
8) Configuration on ESW1



9) Configuration on ESW2

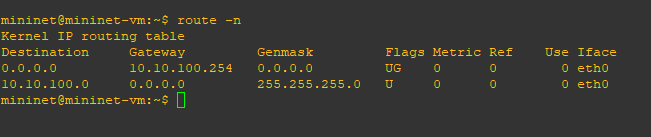


10) Assigning an IP address to Mininet 1

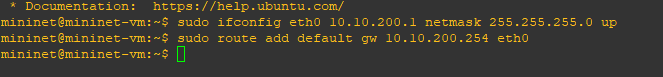


Assigns ip address 10.10.100.1 to Mininet 1 and subnet mask. Also assigned a gateway address 10.10.100.254

11) Routing table on Mininet 1

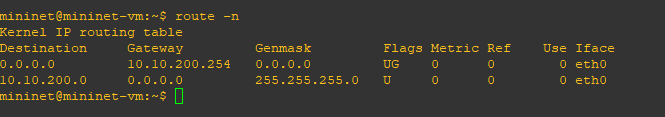


12) Assigning an IP address to Mininet 2



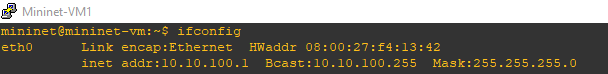
Assigns ip address 10.10.200.1 to Mininet 2 and subnet mask. Also assigned a gateway address 10.10.200.254

13) Routing table on Mininet 2

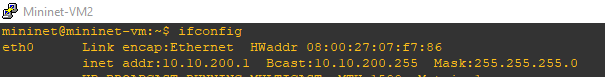


**Mac address of all devices in the network**

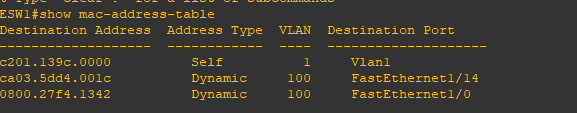
Mininet 1:



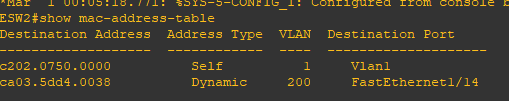
Mininet 2:



ESW1:



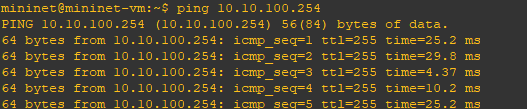
ESW2:



These mac addresses will be helpful in analyzing the message flow in steps 14 and 15.

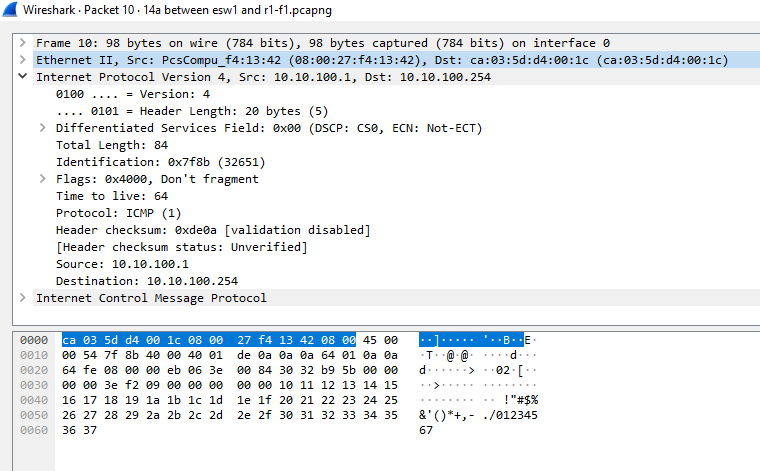
14) Pings from Mininet 1

1. ping 10.10.100.254 🡪 mininet1 to f1/0 interface of R1

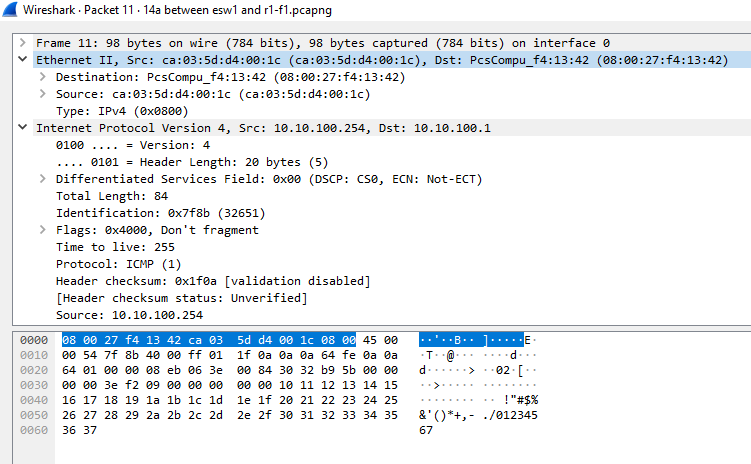


Capture between ESW1 and R1 F1/0 interface

ICMP Request

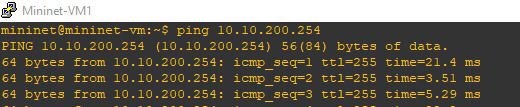


ICMP Reply

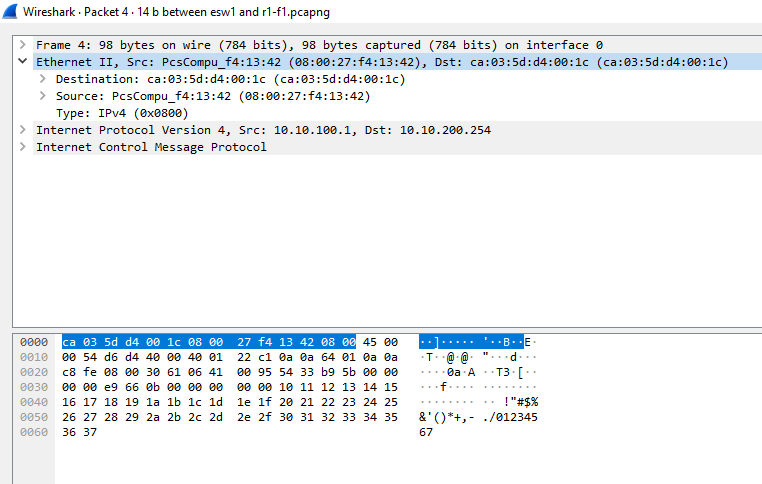


Mininet1 pings the F1/0 interface of R1. The switch ESW1 receives a packet on F1/0 interface and check the destination mac address. The switch in the mac address table has an entry of a destination mac address in its mac address table. The switch directs the packet to the respective interface.

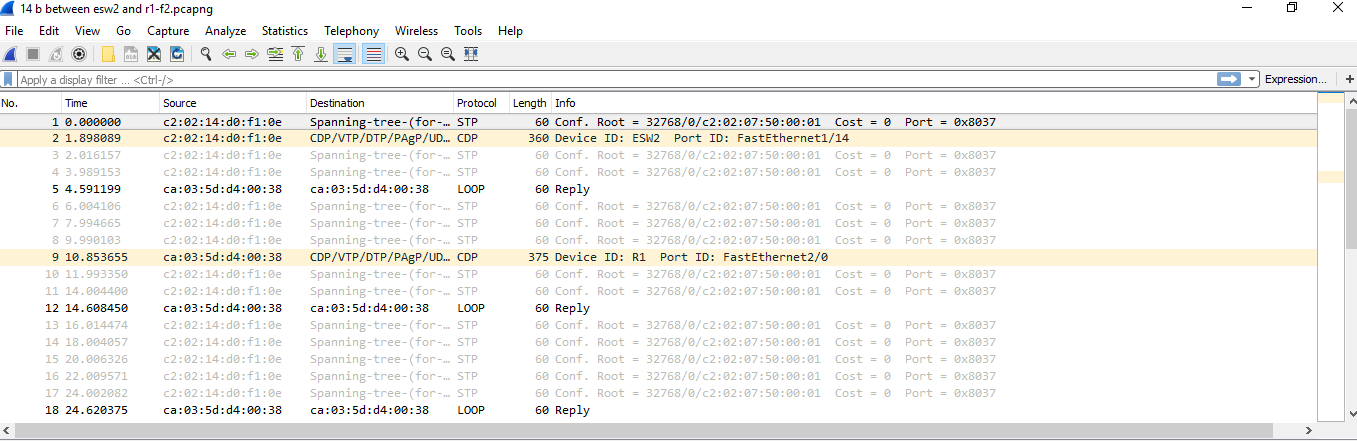
1. ping 10.10.200.254 🡪 Ping from Mininet1 to Router2 VLAN 200 Interface



Packet capture between ESW1 and R1 Vlan 100 interface



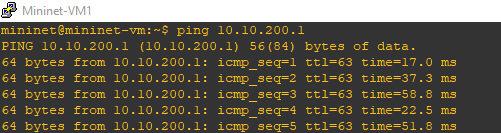
Packet capture between ESW2 and R2 Vlan 200 Interface



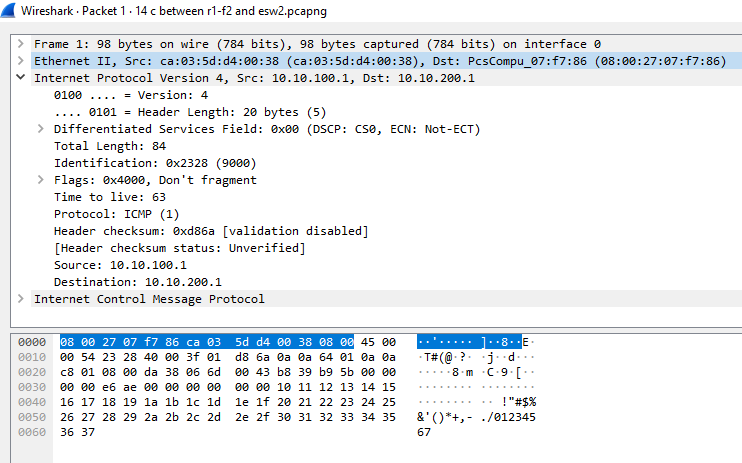
Here the mininet1 pings the other interface f2/0 of router. Though there are two paths to reach the router R1. Mininet1 arp request for the other interface would be answered by the router only with the ethernet address of the interface for which it is connected. The switch ESW1 checks the destination Mac address and learns it needs to forward to the f1/14 interface. All traffic incoming to ESW1 to reach R1 are always forwarded to F1/14 interface. The spanning tree entry for VLAN2 will not be updated since it creates a loop.

From the ICMP request it can be noted that the mac address is of router1 Vlan 100 even for the other interface ip address.

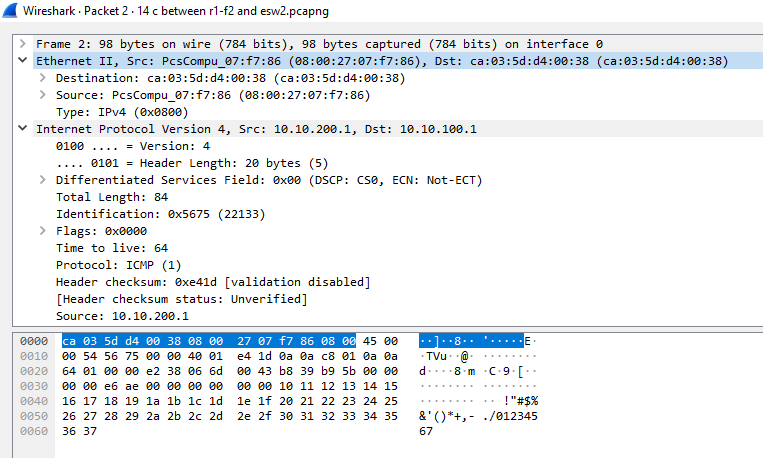
1. ping 10.10.200.1 🡪 ping mininet 2



Packet capture between R2 Vlan 200 interface and ESW2 – ICMP Request



ICMP Reply

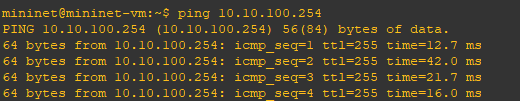


Ping from mininet1 to mininet2. Since mininet 2 is on a different VLAN network. The mininet1 learns this by the subnet mask. The mininet forward the packet by updating mac address of the router f1/0 interface.

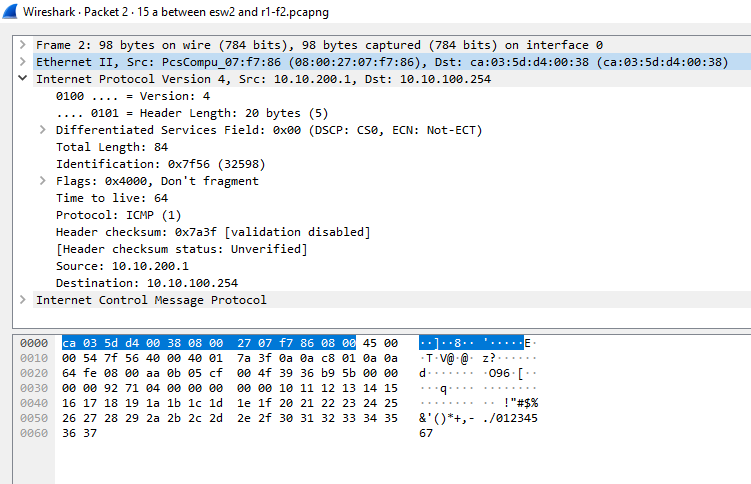
The router now learns mininet2 is on the other interface. The router now replace the src mac address field to the vlan200 interface and destination mac address to the mininet2 mac address. And forward the packet through F2/0 interface.

15) Pings from Mininet2

1. ping 10.10.100.254 🡪 Mininet 2 to R1 VLAN 100 router interface

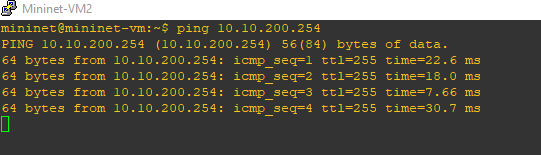


ICMP Request capture between ESW2 and R2 VLAN 100 interface



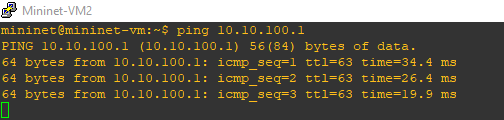
The Mininet2 arp request reaches the router and the router knowing the ip address being its own ip address for a different interface. The routers arp reply will be the ethernet address of the interface the mininet 2 is connected. The mininet2 forwards the packet to the R1 F2/0 interface.

1. ping 10.10.200.254 🡪 Mininet 2 to R2 VLAN 200 interface

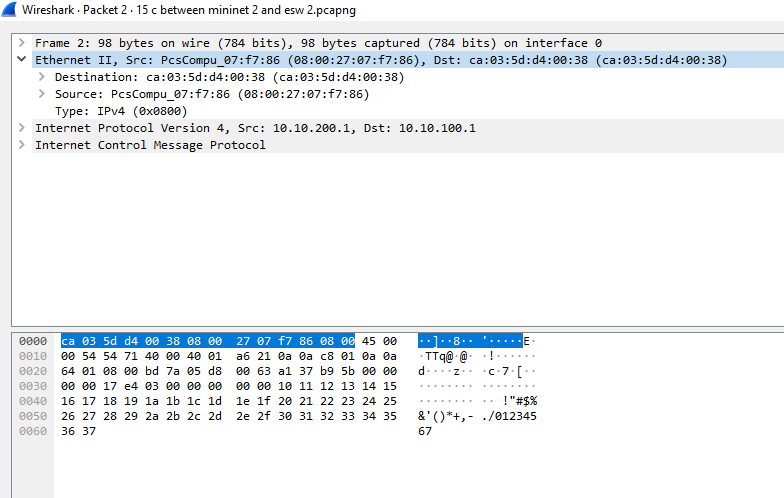


The switch ESW2 has an entry of the mac address of R1 F2/0 interface. It will forward to the respective interface.

1. ping 10.10.100.1 🡪 Mininet2 to Mininet1

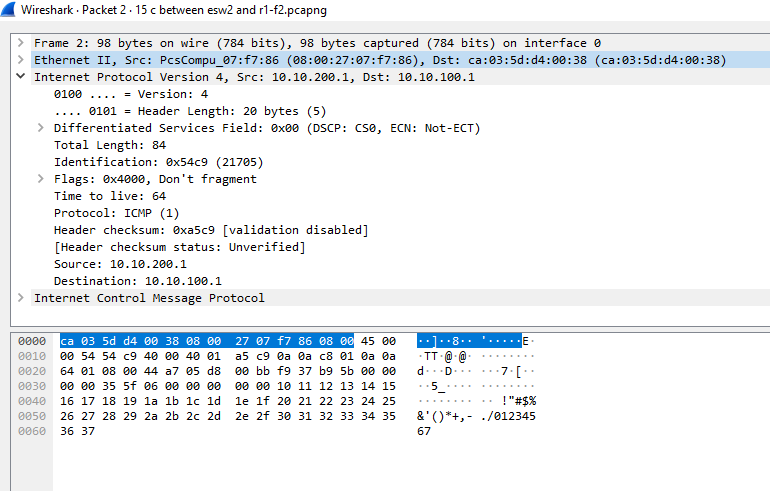


Packet capture between Mininet 2 and ESW2



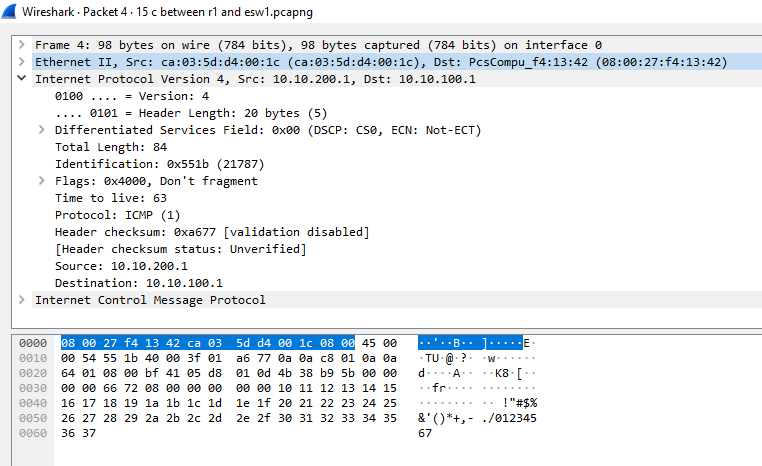
Mininet2 learns the IP address is of a different subnet through its subnet mask. The mininet sends a arp request with the mininet ip address. The router R1 F2/0 interface learning the ip address belong to a different subnet of same network will provide its mac address of R1 F2/0 interface. The mininet2 will now pass the packet with mininet 1 ip address and Router F2/0 interface mac address.

Packet capture between ESW2 and R2 VLAN 200 interface



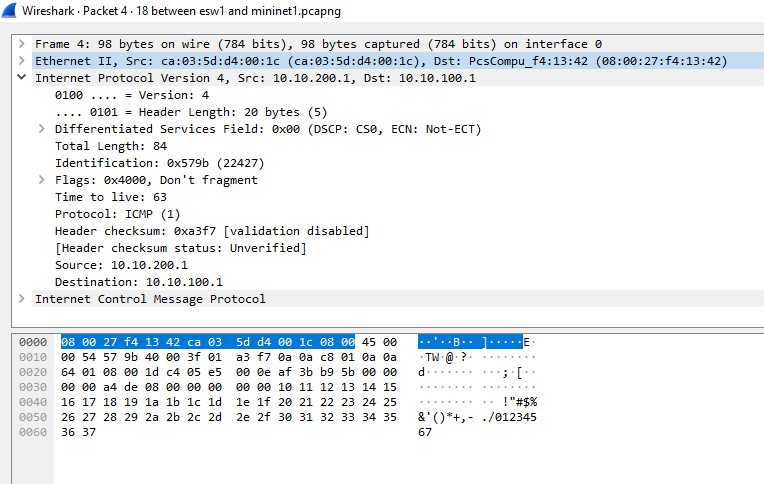
The switch ESW2 will just check the destination mac address and forward the packet to the respective interface the destination mac address is connected to.

Packet capture between R1 VLAN 100 Interface and ESW1



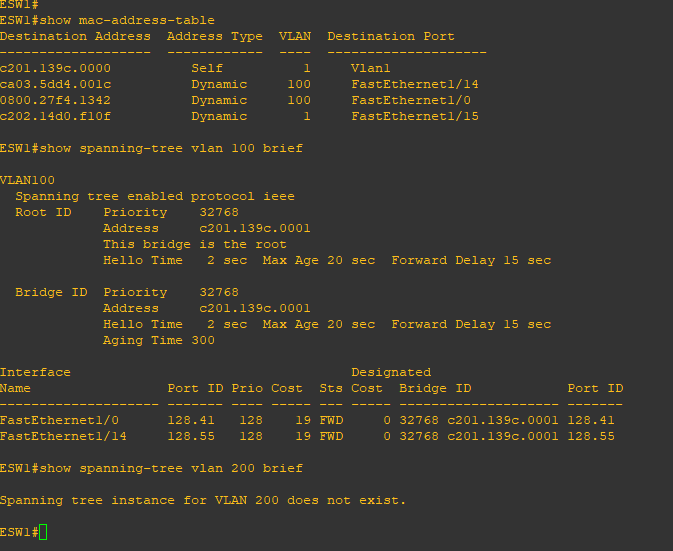
Here we can notice the destination and source ethernet address are changed. The router learns destination ip (mininet 1) is on the other interface. The router replaces the mac address field of destination to mininet1 mac address and source address to the mac address of its interface mininet1 is connected to.

Packet capture between ESW1 and Mininet 1

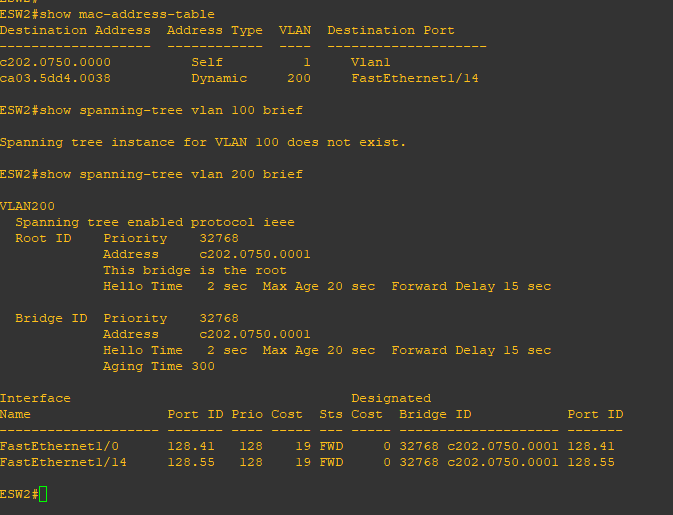


The switch just follows the normal procedure of looking the destination mac address. Since it has an entry of the destination mac address and its interface. It forwards the packet to the respective port.

16) Mac address table and spanning tree on ESW1



17) Mac address table and spanning tree on ESW2



18) Packet captures from mininet 2 to mininet 1

Discussed at 15 c step.

19) Configure Mininet 2 to works as DHCP server

sudo nano /etc/dhcp/dhcpd.conf

subnet 10.10.200.0 netmask 255.255.255.0 {

}

subnet 10.10.100.0. netmask 255.255.255.0 {

range 10.10.100.40 10.10.100.60;

option broadcast-address 10.10.100.255;

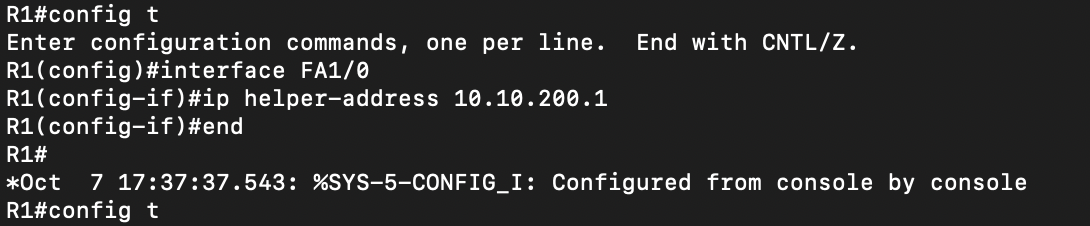
option routers 10.10.100.254;

}

20) Started the DHCP server

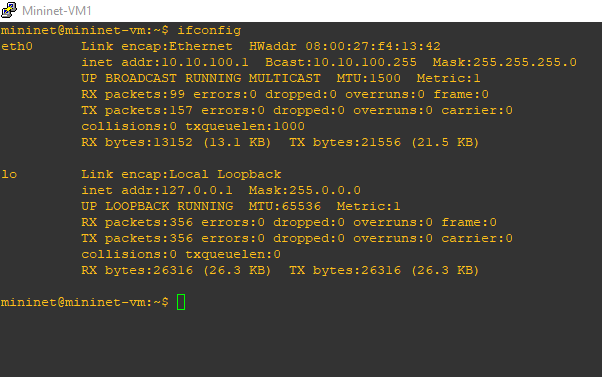


21) Configure R1 to forward DHCP request to mininet2

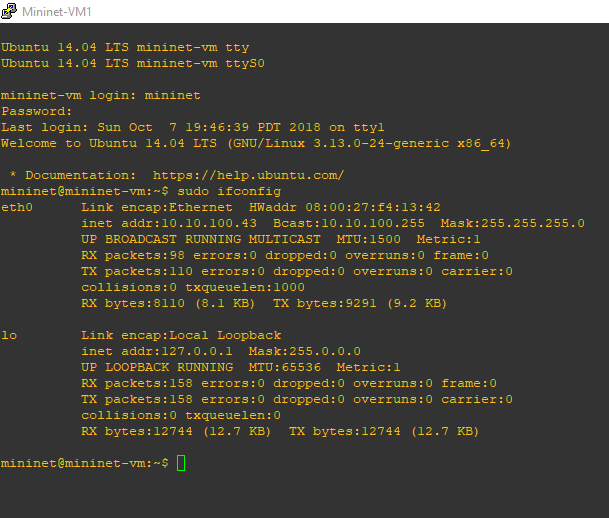


22) Configure mininet1 as DHCP client

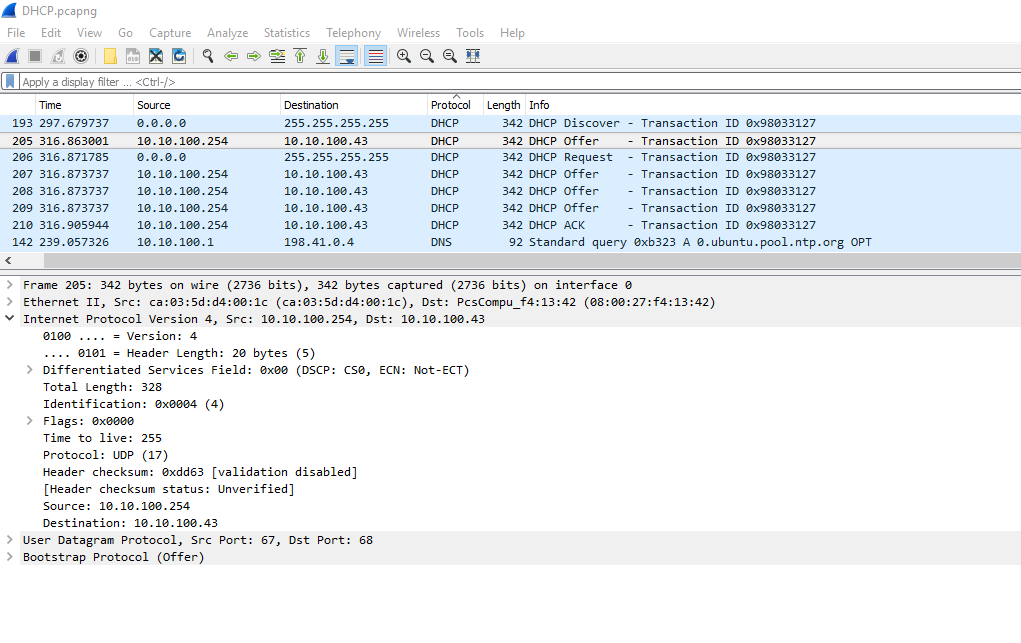
Mininet 1 before reboot



Mininet 1 is configured a new ip address after reboot.



23) Capture on ESW1 and Mininet1 interface



DHCP Offer Message:

On getting the DHCPREQUEST message from the client side the DHCP server will send the

configuration information by broadcasting the DHCPOFFER message. This is also broadcast

message since the IP address has not yet assigned for the client. The offer message contains the

IP address that it is indented to give, and the Server IP address that the client might uses in

future. The other extra information such as the network mask address and others that is being

requested from the client will be mentioned in Option part of the OFFER message.

DHCP Request Message:

On receiving the DHCPOFFER message from the DHCP server side, the client broadcasts the

DHCPOFFER message. Even though the client has the IP address, it broadcast the

DHCPREQUEST message to inform the other DHCP servers to which it was not interested to

clear any status if it is maintained. The information in the DHCPREQUEST message is almost

same as that of DHCP offer message except that the DHCP Server identifier will up updated with

the IP address of the DHCP server.

DHCPACK Message:

On receiving the DHCPREQUEST message from the client side, the DHCP server sends the

ACK message to the client. As we see in the picture, it is a unicast message since the IP address

for the client is defined.

**Protocols Used in this Lab:**

* DHCP (Dynamic Host Configuration Protocol)

**802.X standards employed in this Lab:**

* Wireless Lan (802.11)

**Conclusion:**

The Dynamic Host Configuration protocol is used to configure the network components in the

Network. We have concluded that the different types of messages will be exchanged between the

client and the DHCP server in the DHCP protocol.

**References:**

* TCP Illustrated Volume 1, Second edition, The Protocols by Kevin R. Fall and W.

Richard Steven.

* <https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol>
* <http://www.ids-sax2.com/Unicorn/Tutorials/Dynamic-Host-Configuration-Protocol.htm>
* <https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol#DHCP_options>
* <https://www.cyberciti.biz/faq/howto-linux-renew-dhcp-client-ip-address/>