

**Department of Computer Engineering**

**Spring 2018**

**CMPE-208: Net Architecture and Protocol**

**Dynamic Host Control Protocol**

**Group Lab 2 Report**

**By**

**Team 4**

**Virat Mathur**

**Shivangi Gupta**

**Tejas Chumbalkar**

**Vishal Govindraddi Yarabandi**

Table of Contents

[Overview and Purpose 3](#_Toc506737649)

[Brief Overview of Address Resolution Protocol (DHCP) 3](#_Toc506737652)

[DHCP ARCHITECTURE 4](#_Toc506737653)

[Working of Dynamic Host Configuration Protocol (DHCP) 4](#_Toc506737654)

[DHCP MESSAGE FORMAT 6](#_Toc506737655)

[ADDRESS LEASE TIME 7](#_Toc506737656)

[DHCP ATTACK 7](#_Toc506737657)

[Lab Setup 10](#_Toc506737658)

Lab Configuration.................................................................................................................................10

[Lab Execution and Observations. 15](#_Toc506737659)

[Contribution 15](#_Toc506737660)

References............................................................................................................................................22

## **Overview and Purpose**

The purpose of setting up this lab is to study the various concepts of **Dynamic Host Configuration Protocol** (**DHCP**).

The following tools were used to setup this lab:

* **GNS3**: A free graphical network simulator that allows to design, plan, configure, test, troubleshoot complex network topologies and run simulations without direct interaction with network hardware.
* **Wireshark**:A free open source network packet analyzer, which allows examining the network packet data at microscopic level.

# **Brief Overview of Dynamic Host Configuration Protocol (DHCP)**

This section provides a brief overview of the Dynamic Host Configuration Protocol (DHCP). This section provides with the better understanding of the protocol itself and provide with the path through our observations to obtain result.

## **What is Dynamic Host Configuration Protocol (DHCP)**

The Dynamic Host Configuration Protocol (DHCP) is a [network management protocol](https://en.wikipedia.org/wiki/Network_protocol) used on [TCP/IP](https://en.wikipedia.org/wiki/TCP/IP) networks where a DHCP server dynamically assigns an [IP address](https://en.wikipedia.org/wiki/IP_address) and other network configuration parameters to every device on a network so that they can communicate with other IP networks. A DHCP server enables computers to request IP addresses and networking parameters automatically, reducing the need for a [network administrator](https://en.wikipedia.org/wiki/Network_administrator) or a user to manually assign IP addresses to all network devices. In the absence of a DHCP server, a computer or other device on the network needs to be manually assigned an IP address.

DHCP can be implemented on networks ranging in size from [home networks](https://en.wikipedia.org/wiki/Home_network) to large [enterprise networks](https://en.wikipedia.org/wiki/Campus_network). A [router](https://en.wikipedia.org/wiki/Router_(computing)) or a [residential gateway](https://en.wikipedia.org/wiki/Residential_gateway) can act as a DHCP server. Most residential network routers receive a globally unique IP address within the ISP network. Within a local network, a DHCP server assigns a local IP address to each device connected to the network.

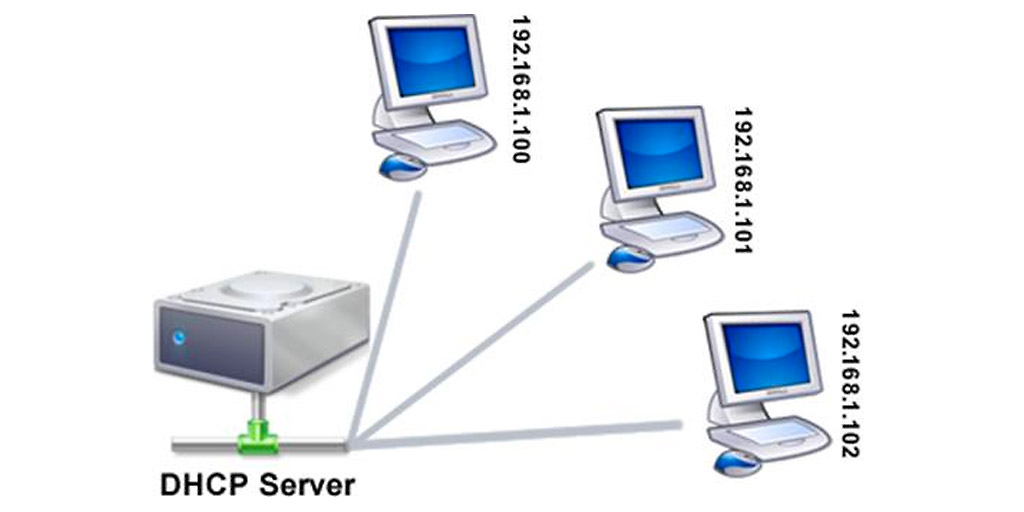


Image Reference:<https://whatismyipaddress.com/dhcp>

## **DHCP ARCHITECTURE**

The DHCP architecture consists of:

1. DHCP clients
2. DHCP servers
3. DHCP relay agents on a network.

The clients interact with servers using DHCP messages in a DHCP conversation to obtain and renew IP address leases.

* **DHCP server**: which receives client’s request and replies to them.
* **DHCP client**: which can be combined with the operating system of a computer or other IP capable device and which sends configuration requests to the server.
* **A DHCP relay agent**: which passes DHCP requests from one LAN to another network so that there need not be a DHCP server on every LAN.

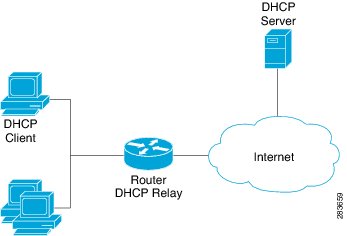


Image Reference:

<https://www.cisco.com/c/en/us/td/docs/routers/asr9000/software/asr9k_r5-1/bng/configuration/guide/b_bng_cg51xasr9k/b_bng_cg51xasr9k_chapter_0101.html>

**Working of Dynamic Host Configuration Protocol (DHCP)**

DHCP is a client-server protocol in which servers have a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools allowed. DHCP enabled clients send a request to the DHCP server whenever they connect to a network.

Clients configured with DHCP, broadcast a request to the DHCP server and request network configuration information from the local network to which they are attached. A client broadcasts a query for this information after booting up. The DHCP server responds to the client REQUEST by providing IP configuration information previously specified by a N.A. This

includes a specific IP address for the time period called a lease, for which the address is valid. When reassigning, a DHCP client requests the same parameters, but the DHCP server may assign a new IP address based on policies set by administrators.

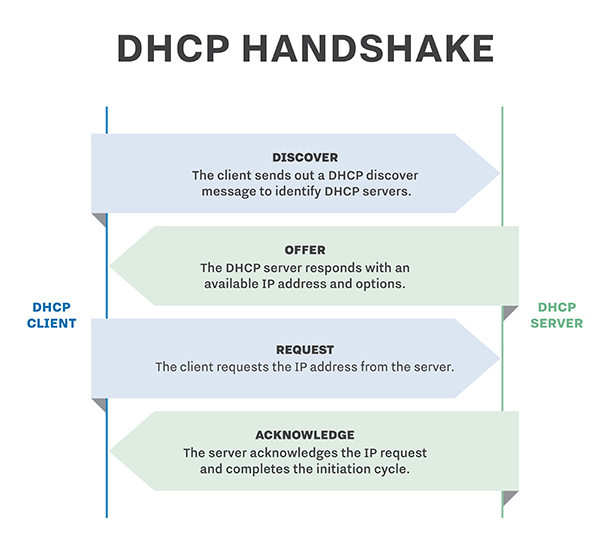
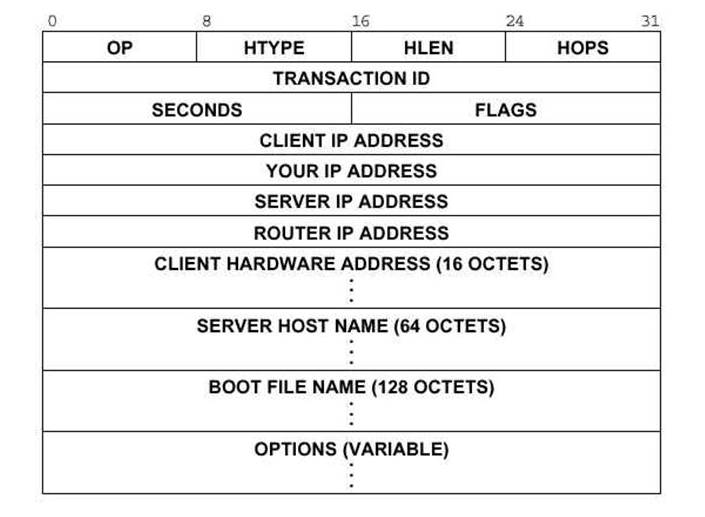
****

Image Reference: <http://searchnetworking.techtarget.com/definition/DHCP>

**DHCP MESSAGE FORMAT**

****

* **Op:** Message op code / message type.

1 = BOOTREQUEST, 2 = BOOTREPLY

* **Htype:** Hardware address type; e.g., '1' = 10mb ethernet.
* **Hlen:**  Hardware address length (e.g. '6' for 10mb ethernet).
* **Hops:**  Client sets to zero, optionally used by relay agents

when booting via a relay agent.

* **Transaction id:** Transaction ID, a random number chosen by the

client, used by the client and server to associate

messages and responses between a client and server.

* **Secs:** Filled in by client, seconds elapsed since client

began address acquisition or renewal process.

* **Flags:**  Flags
* **Ciaddr:** Client IP address; only filled in if client is in

BOUND, RENEW or REBINDING state and can respond

to ARP requests.

* **Yiaddr:** 'your' (client) IP address.
* **Siaddr:** IP address of next server to use in bootstrap;

returned in DHCPOFFER, DHCPACK by server.

* **Giaddr:** Relay agent IP address, used in booting via a relay agent.
* **Chaddr:** Client hardware address.
* **Sname:** Optional server host name, null terminated string.
* **File:** Boot file name, null terminated string; "generic"

name or null in DHCPDISCOVER, fully qualified

directory-path name in DHCPOFFER.

* **Options:** Optional parameters field.

**ADDRESS LEASE TIME**

A DHCP server manages and tracks IP address assignments on the network. When a device without a permanent assignment requests an IP address, the DHCP server assigns an address to the device for a certain period of time. If the device is using the IP address halfway through the lease period, it requests a renewal and the DHCP server extends the lease.

If the lease expires and the device have not contacted the DHCP server, the server reuse the IP address. Some DHCP servers wait for an additional grace period before reassigning an expired address in case the device is in a different time-zone, clocks are not in synchronization or the device is disconnected when the lease expires.

**DHCP ATTACK**

Since DHCP protocol do not need an authentication from the client, any user within or outside the network can obtain a lease of IP which can reveal the data like DNS server IP or server data to the unauthorized user, compromising the network’s security.

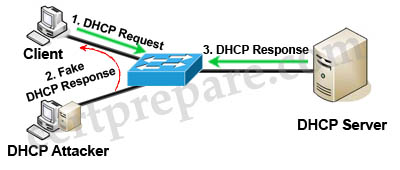


Image Reference: <https://www.certprepare.com/dhcp-spoofing-questions>

There are lot of attacks related to DHCP server. Two of them are-

* **DHCP Spoofing** – Here, attacker use the rogue DHCP server in the network to sniff the LAN traffic. It takes place through following method. As soon as the client broadcasts the DHCP DISCOVER packet, the rogue DHCP server replies before the actual genuine DHCP server consisting of IP address and other information such that one of the attacker’s machine is designated as the default gateway to the client. This directs all the packets from the client to the attacker’s machine through which attacker can open and get all the data from the packet.

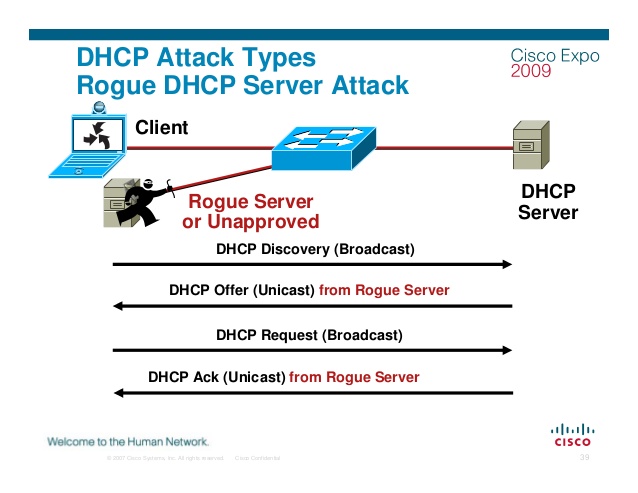
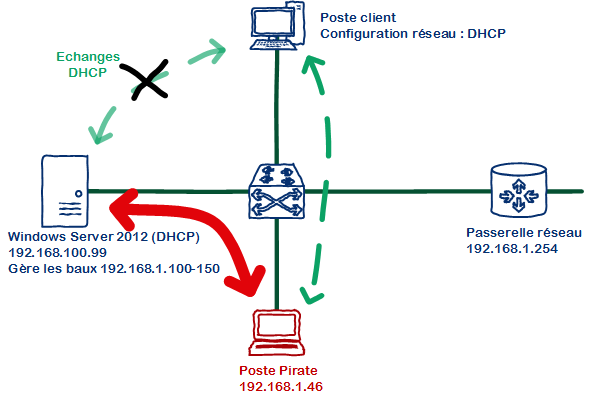


Image-Reference:<https://www.cisco.com/c/dam/global/en_ae/assets/exposaudi2009/assets/docs/layer2-attacks-and-mitigation-t.pdf>

* **DHCP Starvation** - Here, attacker keeps on requesting for the IP configurations from DHCP through different slave machines by spoofing its MAC address until DHCP server’s pool is completely exhausted. Therefore, the genuine client does not get the IP configuration from DHCP server and hence cannot connect to the network.

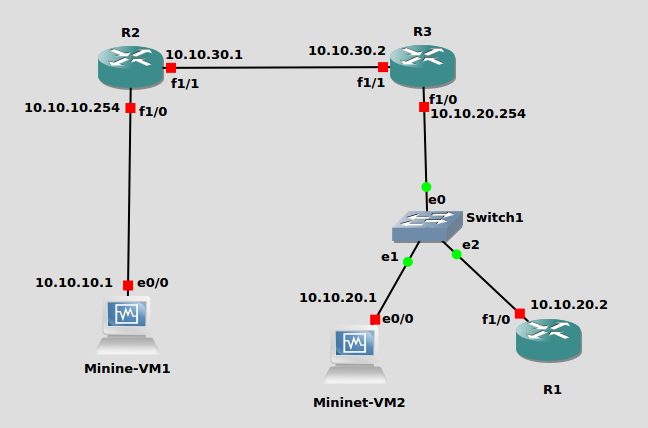


# 

# **Lab Setup**

## **Network Topology**

We created a network of various devices as shown below in the ‘Network Setup’ figure with the help of GNS3 and configured these devices using the configuration instructions mentioned in the ‘Lab Configuration’ section.



**Network setup**

### **Lab Configuration**

Commands on Router 2 –

//configuring ip address on router 2 and assigning helper -address on fa1/0 interface

R2# config t

R2(config)# int fa1/0

R2(config-if)# ip address 10.10.10.254 255.255.255.0

R1(config-if)# ip helper-address 10.10.20.1

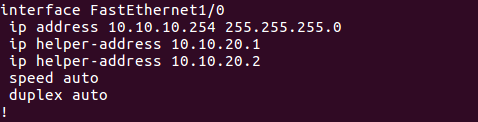
R1(config-if)# ip helper-address 10.10.20.2

R2(config-if)# no duplex full

R2(config-if)# no speed 100

R2(config-if)# no shut

R2(config-if)# ^z



R2# config t

R2(config)# int fa1/1

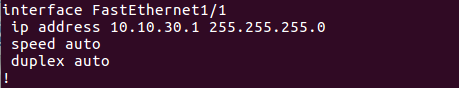
R2(config-if)# ip address 10.10.30.1 255.255.255.0

R2(config-if)# no duplex full

R2(config-if)# no speed 100

R2(config-if)# no shut

R2(config-if)# ^z



//starting rip protocol

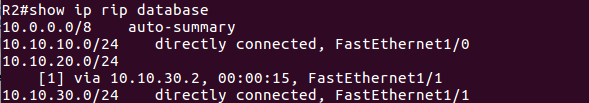
R2(config-if)# config t

R2(config)# router rip

R2(config-router)# network 10.10.30.0

R2(config-router)# network 10.10.10.0

R2(config-if)# ^z



**Router 3** is configured as gateway for network 10.10.20.0

Commands on Router 3 –

!

//setting IP address on fa1/0 interface of Router 3

R3# config t

R3(config)# int fa1/0

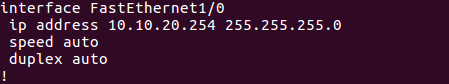
R3(config-if)# ip address 10.10.20.254 255.255.255.0

R3(config-if)# no duplex full

R3(config-if)# no speed 100

R3(config-if)# no shut

R3(config-if)# ^z



//setting IP address on fa2/0 interface of Router 2

R3#config t

R3(config)# int fa1/1

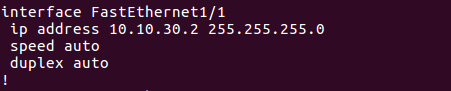
R3(config-if)# ip address 10.10.30.2 255.255.255.0

R3(config-if)# no duplex full

R3(config-if)# no speed 100

R3(config-if)# no shut

R3(config-if)# ^z



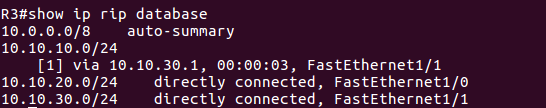
//starting rip protocol

R3(config)# router rip

R3(config-router)# network 10.10.30.0

R3(config-router)# network 10.10.20.0

!



**Router 1** is configured as a DHCP server with IP address pool range from 10.10.10.1 to 10.10.10.20

Commands on Router 1 -

R1# config t

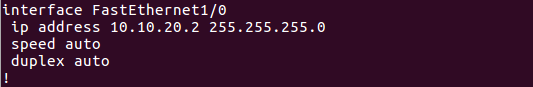
R1(config)# int fa1/0

R1(config-if)# ip address 10.10.20.2 255.255.255.0

R1(config-if)# no duplex full

R1(config-if)#no shut

R1(config-if)# ^z

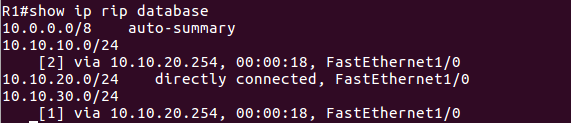


//starting rip protocol

R1(config-if)# router rip

R1(config-router)# network 10.10.20.0

R1(config-router)#^z



R1# config t

R1(dhcp-config)# ip dhcp pool DHCP // assigning name to dhcp pool: DHCP

R1(dhcp-config)# network 10.10.10.0 255.255.255.0

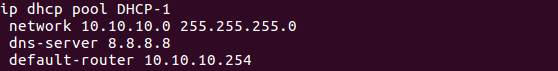
R1(dhcp-config)# dns-server 8.8.8.8

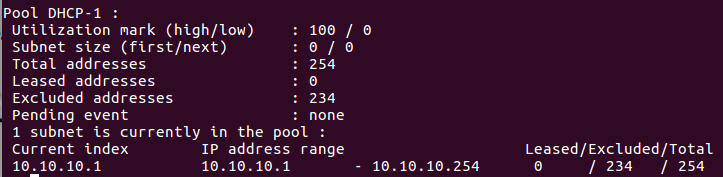
R1(dhcp-config)# default-router 10.10.10.254

R1(dhcp-config)# ip dhcp excluded-address 10.10.10.21 10.10.100.254 // exclude-range

R1(config)# service dhcp // to enable DHCP service on router

!



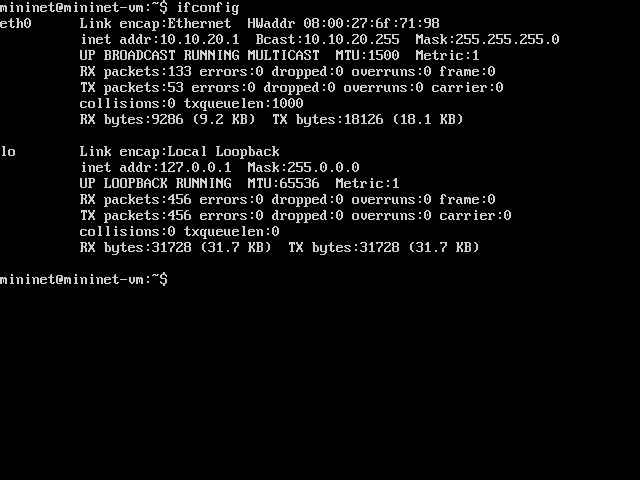
****

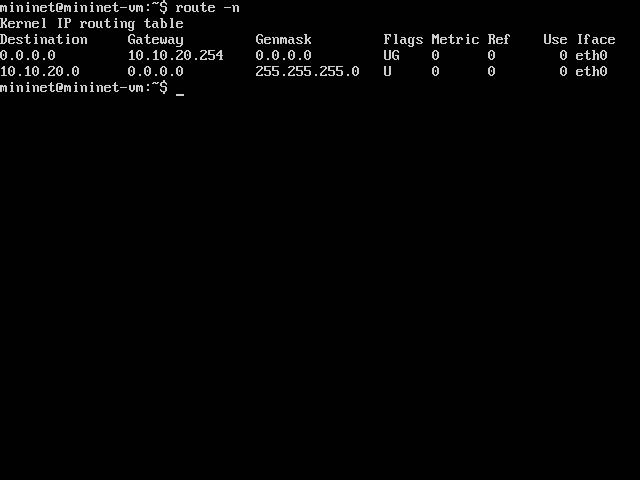
**Mininet-VM2** is also configured to act as a DHCP server

Commands on Mininet-VM2 –

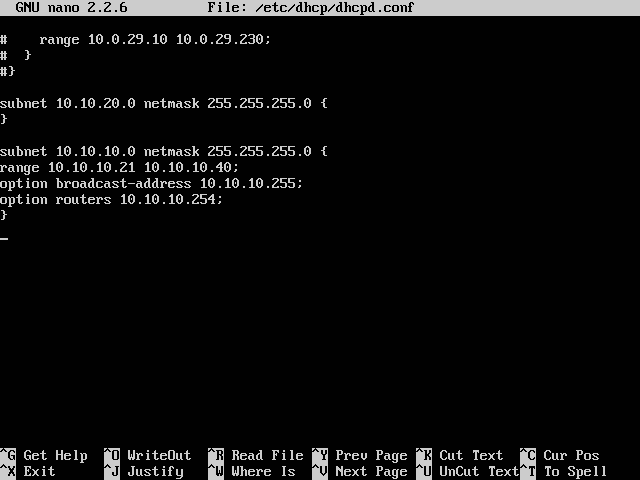
Mininet-VM2> sudo ifconfig eth0 10.10.20.1 netmask 255.255.255.0 up

Mininet-VM2> sudo route add default gw 10.10.20.254 eth0





**Mininet VM1** is configured as a DHCP server with IP address pool range from 10.10.10.21 to 10.10.10.40. Following changes are made in the file /etc/dhcp/dhcpd.conf to make Mininet-VM2 as DHCP server



Restart the DHCP service as changes are made in the configuration file:

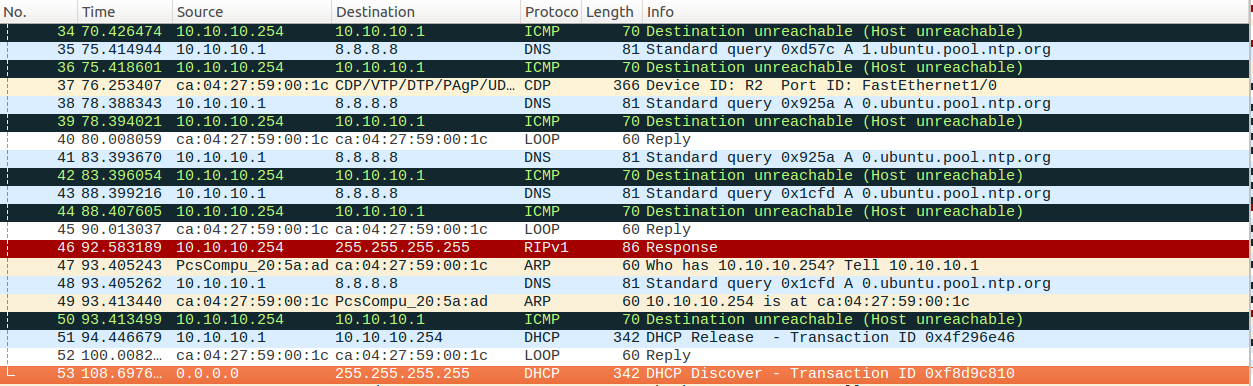
Mininet-VM2> sudo service isc-dhcp-server restart

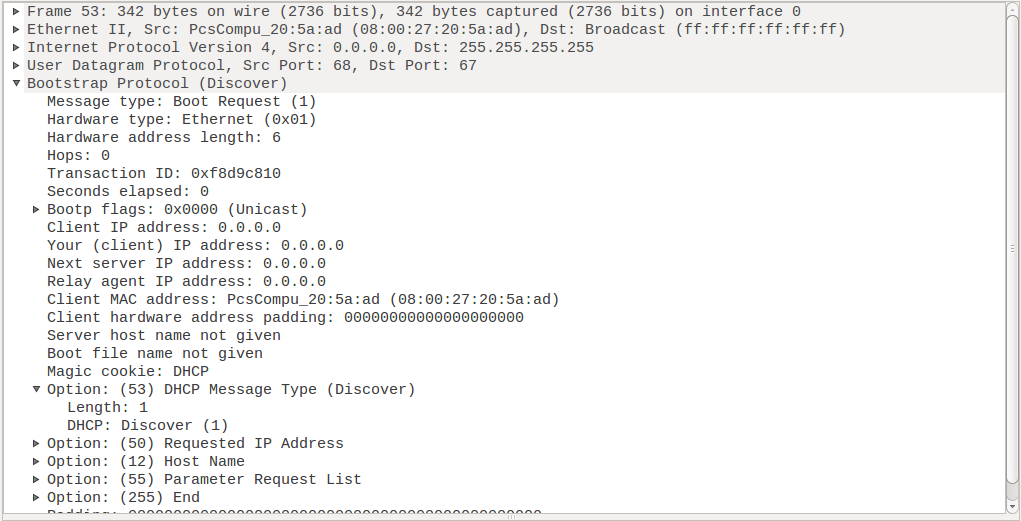
**Mininet-VM1:** Mininet-VM1 acts as a DHCP client. It will asks for the IP address and other information from the available DHCP server i.e. Router R1 and Mininet-VM2.

**Lab Execution and Observations:**

**Case 1-: Two DHCP servers Router R1 and Mininet VM2 are in the network to provide ip address to Mininet VM1**

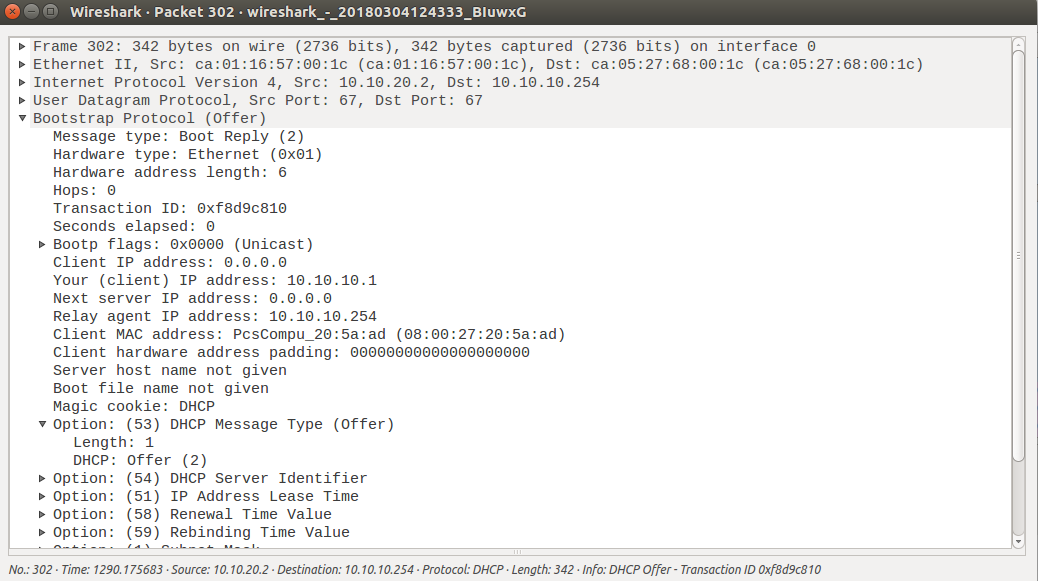
When Mininet VM1 boots up, it sends the following broadcast **DHCP discover packet** into the network.

****

****

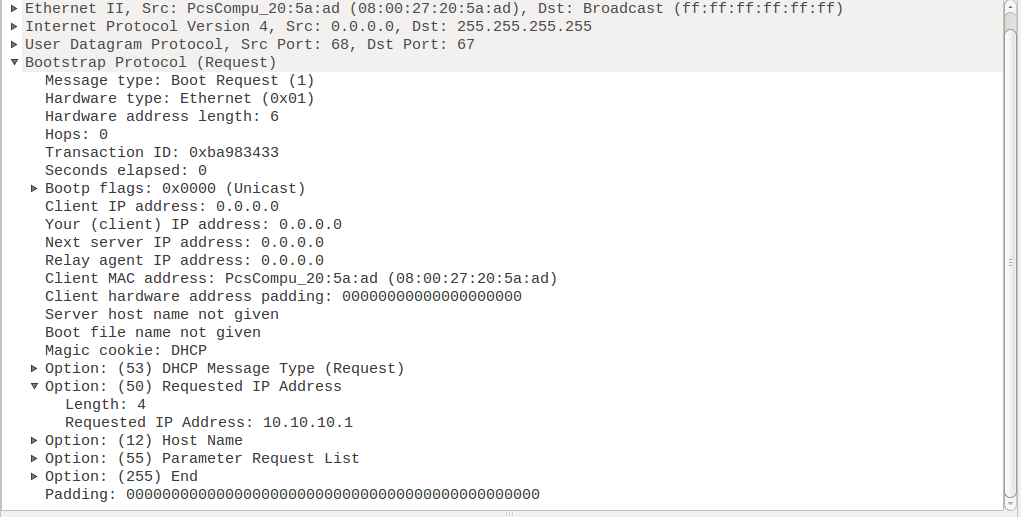
* As it is a broadcast packet, destination ip address as 255.255.255.255 and destination MAC address as FF:FF:FF:FF:FF:FF
* As it does not have IP, source IP is set as 0.0.0.0

Router1 sends a **DHCP offer packet** to Mininet VM1

****

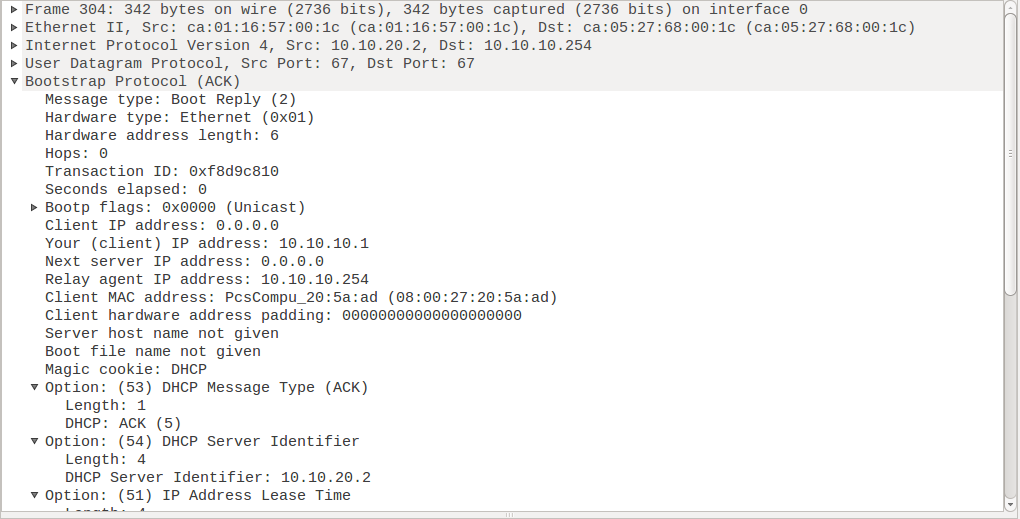
* Source IP address is 10.10.20.2: IP address of Router1. Destination IP address is 10.10.10.254: Gateway for Mininet VM1.

Mininet VM1 sends a **DHCP request packet** to Router R1 requesting for **10.10.10.1** ip address.



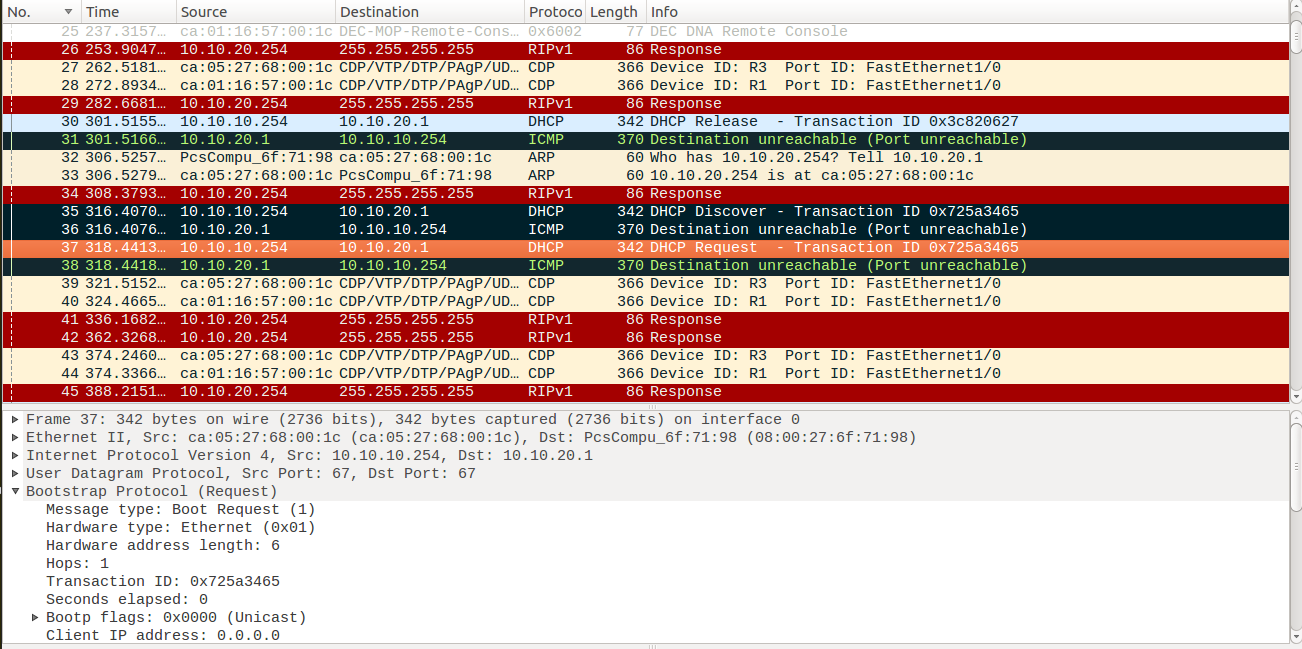
* Mininet VM1 uses source ip address 0.0.0.0 for requesting the IP address for further communication.

Router1 sends an acknowledgement to Mininet1 to confirm the use of ip address **10.10.10.1** for further communication.



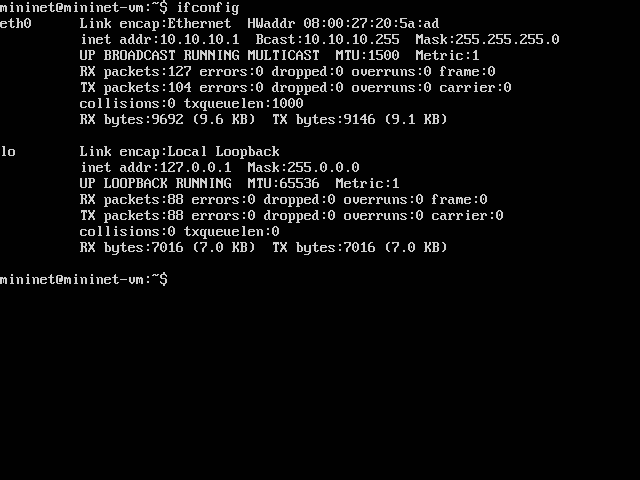
* Source IP address is 10.10.20.2: IP address of Router1. Destination IP address is 10.10.10.254: Gateway for Mininet VM1.

In the meantime, we can see the activities on the DHCP server Mininet VM2.



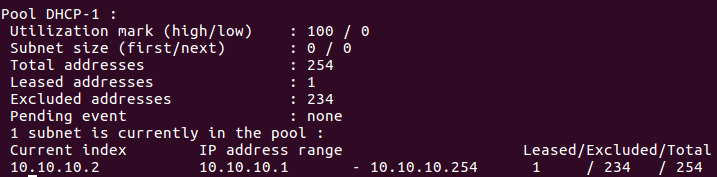
* As Mininet VM1 receives the DHCP offer of Router 1 earlier than Mininet VM2, it accepts the ip address assigned by Router1

The new assigned ip address on VM Mininet1:

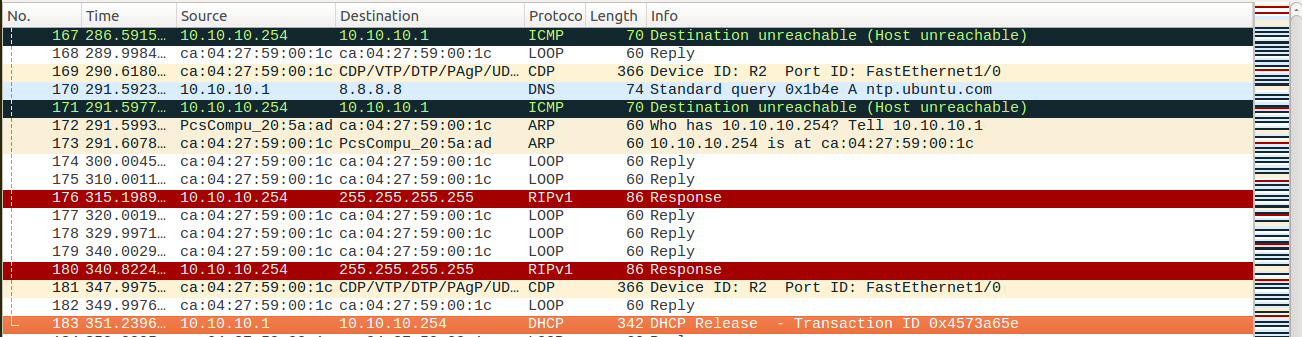


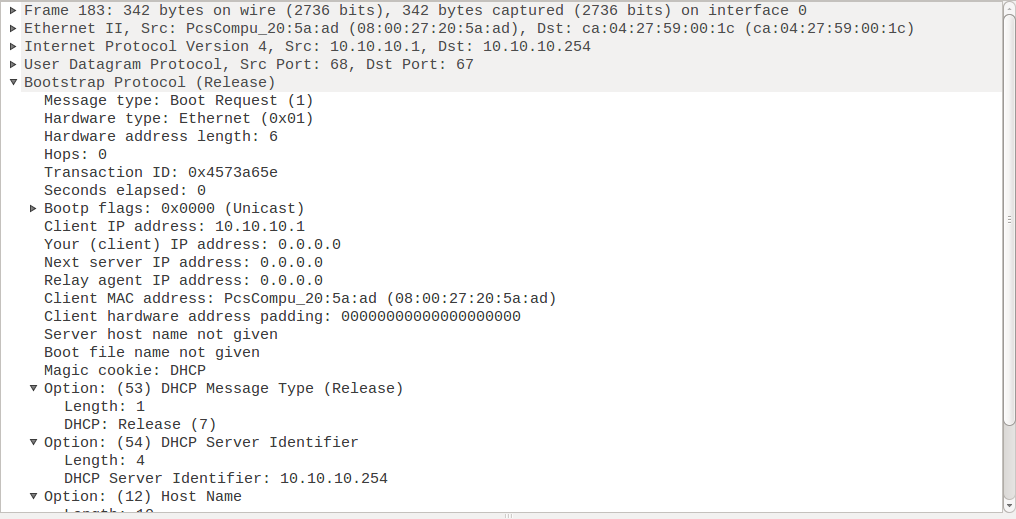
DHCP pool details on Router1:

We can see the leased ip address i.e 1 and current index as 10.10.10.2



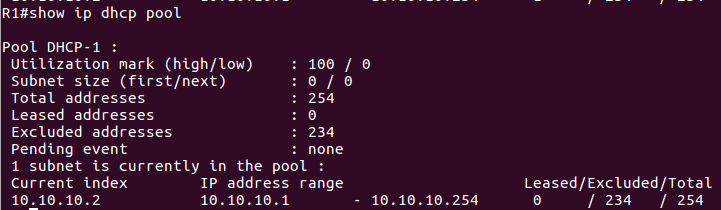
When Mininet1 is rebooted, it releases the ip address assigned by Router1





DHCP pool details on Router1:

We can see the leased ip address is 0:



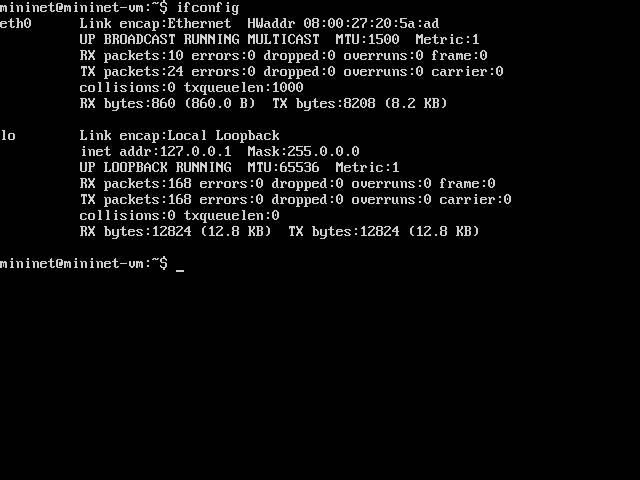
**Case 2: Only DHCP server Mininet VM2 is available in the network to provide ip address to Mininet VM1 and DHCP server Router1 is DHCP server is down.**

Router 1:

DHCP service of Router1 is down.

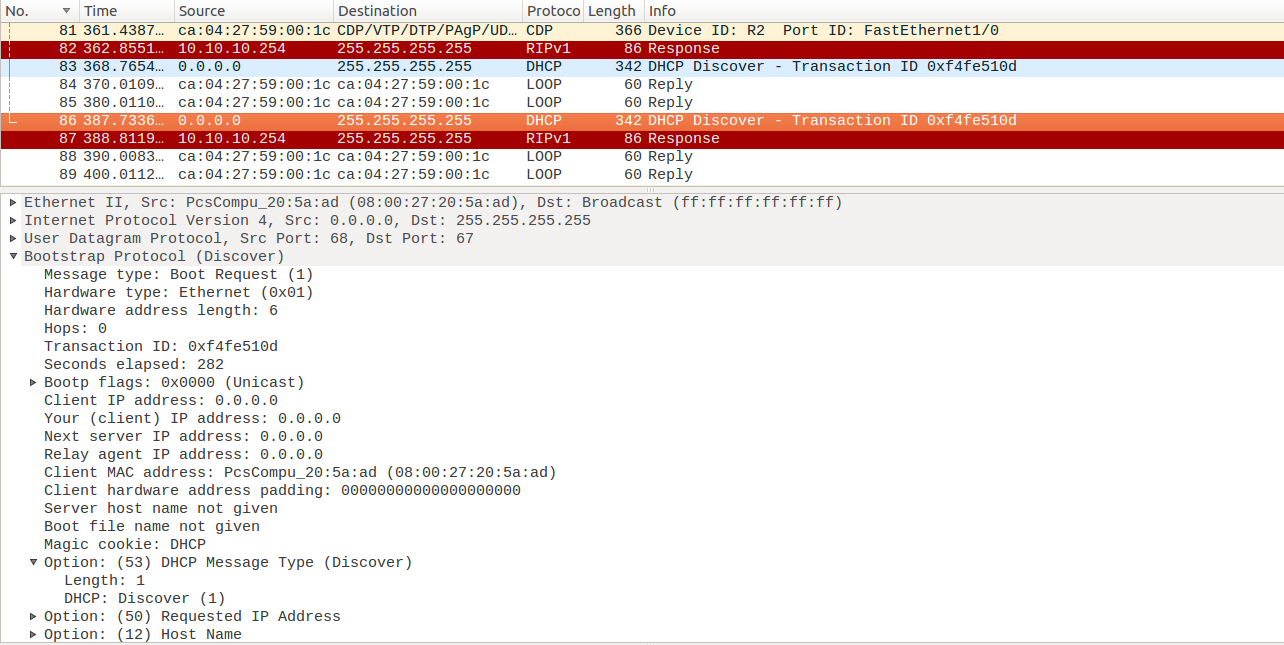
C:\Users\admin\Desktop\Screenshot\208 Group LAB 2\Case2_ip_assigned_from_VM2\r1_shutdown_dhcp_server.png

Initial Configuration of Mininet VM1:



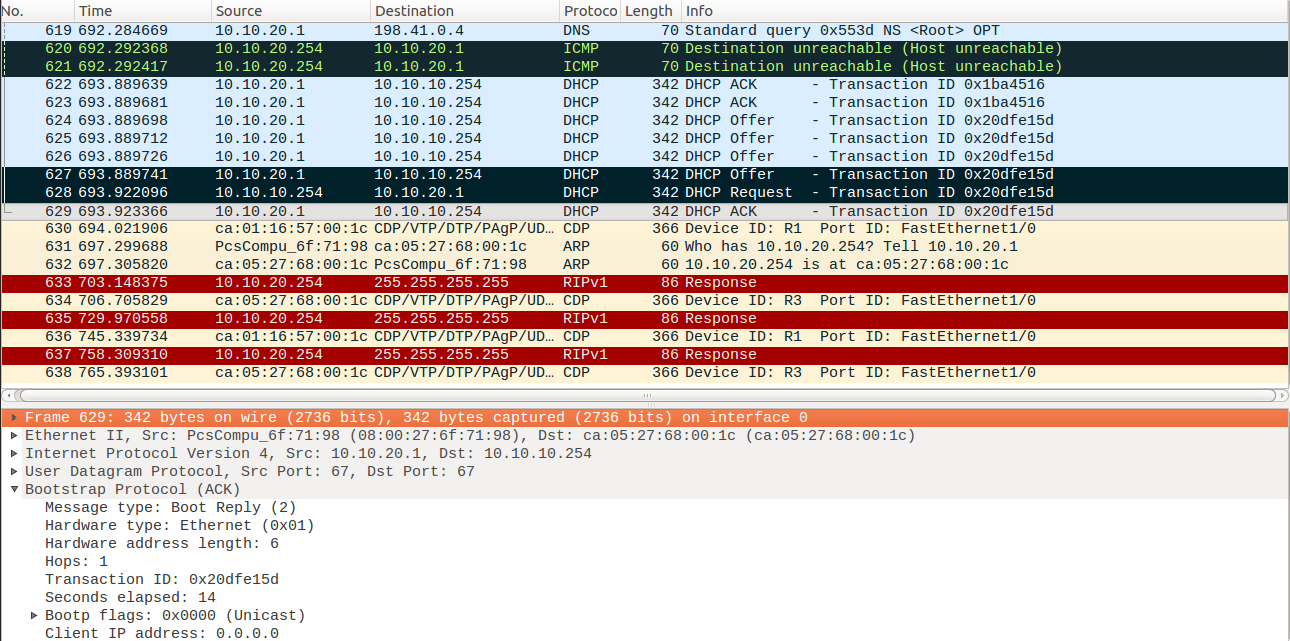
**Wireshark activity on Mininet VM1:**

Mininet VM1 sends a DHCP discover packet into the network



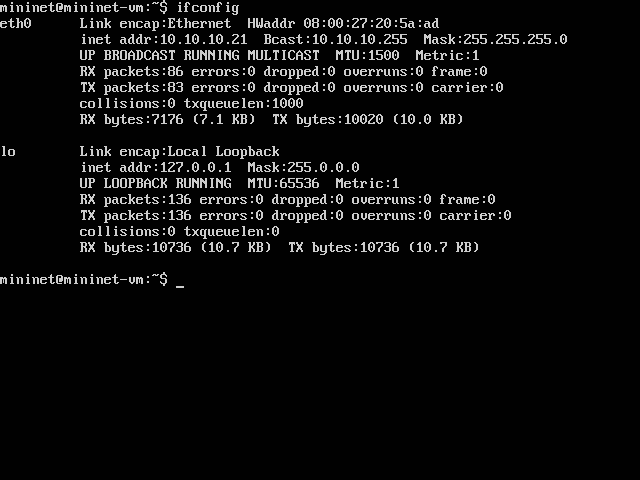
**Wireshark activity on Mininet VM2:**

DHCP Offer, Request and Acknowledgement packets can be seen.

****

**Mininet VM1:**

Mininet VM2 assigns an IP address 10.10.10.21 to Mininet VM1.

****

# **Contribution**

|  |  |
| --- | --- |
| Name | Contribution |
| Tejas Chumbalkar | * Set up lab in GNS3 * Executed lab in GNS3 * Troubleshooting network topology |
| Vishal Govindraddi Yarabandi | * Wireshark observation * DHCP message format * DHCP Architecture |
| Shivangi Gupta | * Documentation and report formatting * Observations on Wireshark * GNS3 Console observations |
| Virat Mathur | * Lab Configurations * Working of DHCP * Documentation and report formatting |

**References**

* <http://searchnetworking.techtarget.com/definition/DHCP>
* <https://technet.microsoft.com/en-us/library/cc781008(v=ws.10).aspx>
* <https://technet.microsoft.com/en-us/library/cc780760(v=ws.10).aspx>
* <https://tools.ietf.org/html/rfc2131>
* <https://www.lifewire.com/what-is-dhcp-2625848>
* <https://www.thegeekstuff.com/2013/03/dhcp-basics/>
* <http://www.omnisecu.com/tcpip/dhcp-dynamic-host-configuration-protocol-how-dhcp-works.php>
* <https://www.cisco.com/c/en/us/support/docs/ip/dynamic-address-allocation-resolution/27470-100.html>