SAN JOSÉ STATE UNIVERSITY

Department of Computer Engineering

Network Architecture and Protocol

(CMPE208)

Dynamic Host Control Protocol

GROUP LAB 2

Group 5
Charit Upadhyay
Devika Jadhav
Pradeep Patil

Table of Contents

Introduction

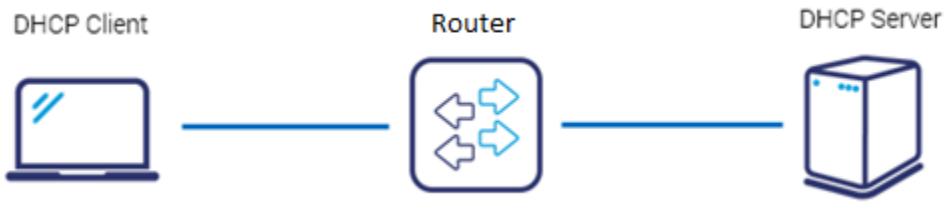


Image Reference: https://www.grandmetric.com

The purpose of setting up this lab is to study the various concepts of **Dynamic Host Configuration Protocol** (**DHCP**). DHCP provides a method for passing configuration information to hosts on a TCP/IP network. DHCP is based on a client–server model, where the server is the host that allocates network addresses and initialization parameters, and the client is the host that requests these parameters from the server. With this lab we aim to obtain practical and detail understating of DHCP with following learning objectives

- Learn to build and configure a layer 3 topology in GNS using Cisco 7200 routers
- Learn to analyze Spanning Tree Protocol (STP) on the router
- Learn to configure DHCP Relay across different VLANS/Networks
- Learn to configure DHCP on end-point/client systems (Linux VMs)

The following tools are used to setup this lab:

- **GNS3**: A graphical network simulator that allows to design, plan, configure, test, troubleshoot complex network topologies and run simulations without direct interaction with network hardware.

- **Oracle Virtual Box**: A software virtualization package that installs on an operating system as an application. VirtualBox allows additional operating systems to be installed on it, as a Guest OS, and run in a virtual environment.

- **Wireshark**: An open source network packet analyzer, which allows examining the network packet data at microscopic level.

DHCP Overview

Dynamic Host Configuration Protocol is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP. Manually configuring thousands of workstations with unique IP addresses would be a time consuming, and cumbersome experience, increasing the risk of duplicating IP address assignments, configuring the incorrect subnet masks, and incorrectly configuring other TCP/IP configuration parameters. This is where the Dynamic Host Configuration Protocol (DHCP) becomes important. DHCP is a service that does the above-mentioned tasks for administrators, thereby saving simplifying the administration of IP addressing in TCP/IP based networks.

The Dynamic Host Configuration Protocol (DHCP) is defined in RFC 1541 and provides a mechanism for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP) defined in RFC 1542, but adds automatic allocation of reusable network addresses and additional configuration options. DHCP is based on a client–server model, where the server is the host that allocates network addresses and initialization parameters, and the client is the host that requests these parameters from the server.

Functions of DHCP

- Dynamically assign IP addresses to DHCP clients.
- Allocate the following TCP/IP configuration information to DHCP clients:
    - Subnet mask information.
    - Default gateway IP addresses.
    - Domain Name System (DNS) IP addresses.
    - Windows Internet Naming Service (WINS) IP addresses.

DHCP supports three mechanisms for IP address allocation. A network will use one or more of these mechanisms, depending on the policies of the network administrator

In Automatic allocation mechanism the DHCP assigns a permanent IP address to a host. In **Dynamic allocation mechanism the** DHCP assigns an IP address to a host for a limited period of time, or until the host explicitly relinquishes the address. Allows automatic reuse of an address. In **Manual allocation mechanism** a host's IP address is assigned by the network administrator, and DHCP is used simply to convey the assigned address to the host.

DHCP has two databases.
First one has static bindings for *physical addresses* (MAC) with IP addresses. Second one has a list of available *IP addresses* that may be assigned for a period of time. Client request to DHCP server causes server to see if MAC is in static database. If so assign the static IP entry to client. If not, choose from available pool. Assigned addresses are temporary (leased). When client's lease expires, must renew or stop using. For dynamic allocation, DHCP assigns an IP address to a host for a limited period of time called the **lease time**. The minimum lease time is 3600 seconds. The maximum lease time is the largest unsigned 32-bit integer, called INFINITY and lease never expires.

DHCP Architecture

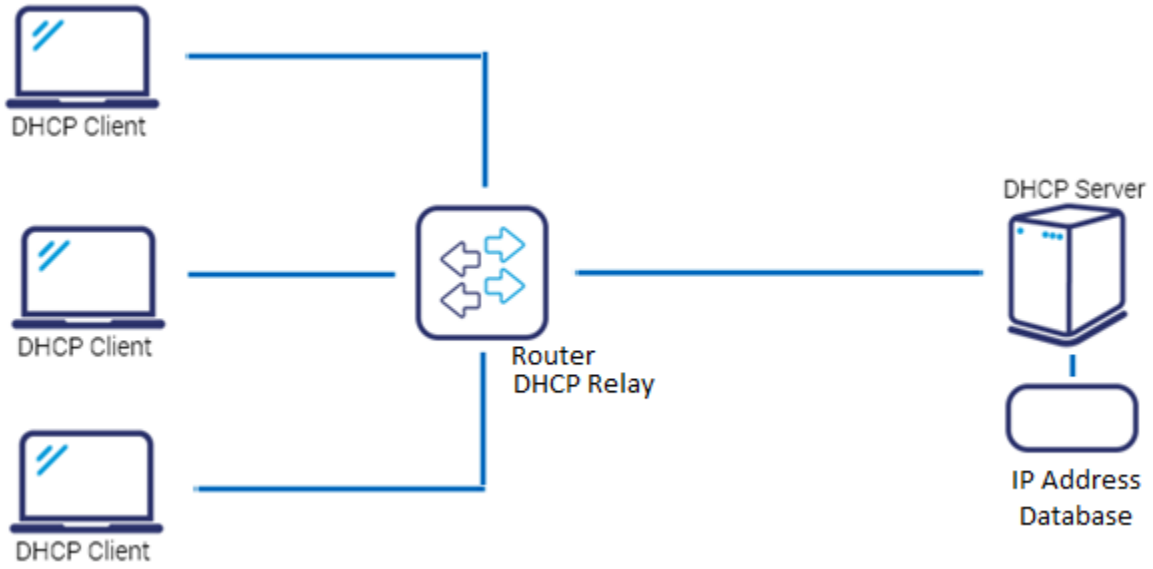


Image Reference: https://www.grandmetric.com

The DHCP architecture is made up of **DHCP clients**, **DHCP servers**, and **DHCP relay agents**. The client interacts with servers using DHCP messages in a DHCP conversation to obtain and renew IP address leases.

DHCP Client A DHCP client is any IP device connected on the network that has been configured to act as a host requesting configuration parameters such as an IP address from a DHCP server. Configuration parameters and other control information are carried in tagged data items that are stored in the Options field of the DHCP message. DHCP uses the Options to pass additional IP settings to DHCP clients such as the default gateway IP address, DNS server address, and the DNS domain name.

DHCP Server The DHCP server is a device on the network with a pool of IP addresses at its disposal to automatically assign to devices as they join the network. The DHCP server assigns the network device its, **IP address** – dynamically configured, **Subnet mask** – statically configured, **Default gateway** for the network – statically configured, **Primary DNS server** – to match a device NAME to an IP address **Secondary DNS server** – statically configured for redundancy and load balancing.

DHCP Relay Agent DHCP relay agents pass DHCP messages between servers and clients where the DHCP server does not reside on the same IP subnet as its clients. For example, on large networks consisting of multiple subnets, a single DHCP server may service the entire network when aided by DHCP relay agents located on the interconnecting routers. You can configure a maximum number of 400 DHCP relay agents (one per interface) on Allied Ware Plus devices. You can use DHCP relay agent information, Option 82, to protect your switch from spoofing attacks, where untrusted hosts send requests for IP addresses to access the network

DHCP Operation

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. Clients configured with DHCP, broadcast a request to the DHCP server. This initiates a 4 way DHCP handshake which is explained in detail below.

Image Reference: http://searchnetworking.techtarget.com/

There are four basic steps the DHCP process follows when a client connects to the network:

DHCP Discover

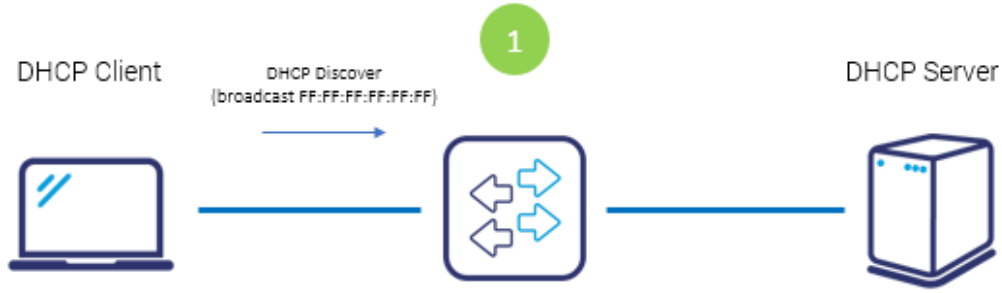


Image Reference: https://www.grandmetric.com

Host connecting to network sends DHCP discover message to all hosts in Layer 2 segment where the destination address is FF:FF:FF:FF:FF:FF. Frame with this **DISCOVER** message hits the DHCP Server.

DHCP OFFER

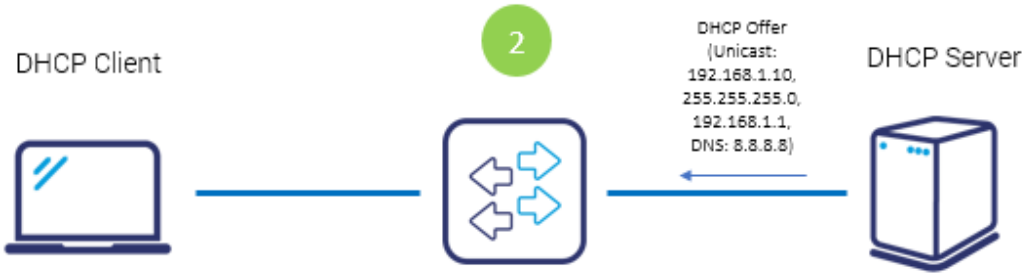


Image Reference: https://www.grandmetric.com

After the DHCP Server receives discover message it suggests the IP addressing offering to the client host by unicast. This **OFFER** message contains: proposed IP address for client (here 192.168.1.10) , subnet mask to identify the subnet space (here 255.255.255.0) IP of default gateway for subnet (here 192.168.1.1), IP of DNS server for name translations (here 8.8.8.8)

DHCP REQUEST

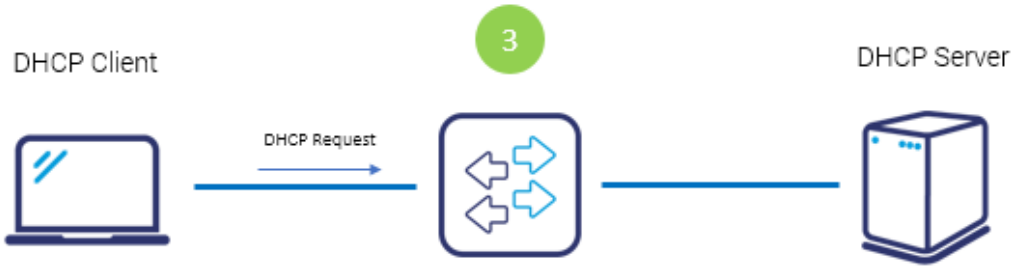


Image Reference: https://www.grandmetric.com

Now after the client receives the offer it requests the information officially sending **REQUEST** message to server this time by unicast. All servers are informed which offer the client selected.

DHCP ACKNOWDGE

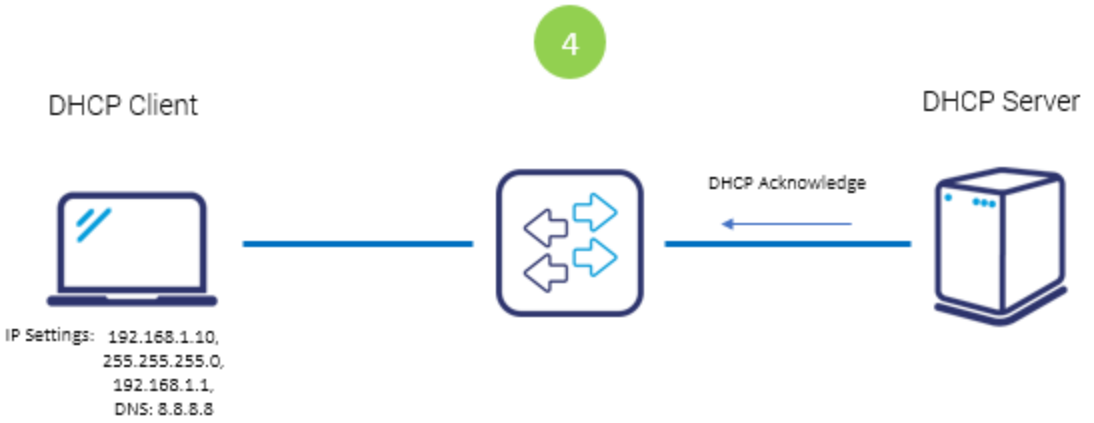


Image Reference: https://www.grandmetric.com

Server sends **ACKNOWLEDGE** message confirming the DHCP lease to client. Now client is allowed to use new IP settings.

Other DHCP Messages

DHCP NAK Server to client indicating client's notion of network address is incorrect (e.g. client has moved to new subnet) or client's lease has expired.

DHCP Decline Error message from DHCP client to server indicating network address is already in use.

DHCP Release Message from DHCP client to server releasing network address and canceling remaining lease.

DHCP Inform Client asking DHCP server only for local configuration parameters because the client already has externally configured network address.

DHCP Message format

Dynamic Host Configuration Protocol				
Bit Offset	0–15		16–31	
0	OpCode	Hardware Type	Hardware Length	Hops
32	Transaction ID			
64	Seconds Elapsed		Flags	
96	Client IP Address			
128	Your IP Address			
160	Server IP Address			
196	Gateway IP Address			
228+	Client Hardware Address (16 bytes)			
	Server Host Name (64 bytes)			
	Boot File (128 bytes)			
	Options			

The fields ae explained as follows,

- **Operation Code:** Message op code / message type.1 = BOOTREQUEST, 2 = BOOTREPLY
- **Hardware Type:** Hardware address type; e.g., '1' = 10mb ethernet.
- **Hardwar Length:** Hardware address length (e.g. '6' for 10mb ethernet).
- **Hops:** Client sets to 0, 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.
- **Seconds Elapsed:** Filled in by client, seconds elapsed since client began address acquisition or renewal process.
- **Flags:** Flags
- **Client IP Address:** Client IP address; only filled in if client is in BOUND, RENEW or REBINDING state and can respond to ARP requests.
- **Your IP Address:** 'your' (client) IP address.
- **Server IP Address:** IP address of next server to use in bootstrap; returned in DHCPOFFER, DHCPACK by server.
- **Gateway IP Address:** Relay agent IP address, used in booting via a relay agent.
- **Client Hardware Address:** Client hardware address.
- **Server Host Name:** 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.

DHCP Lease Process

The DHCP lease process, also known as the DHCP negotiation process, is a fairly straightforward process. The DHCP lease process is described below:

1. The DHCP Discover message is sent from the client to the DHCP server. This is the message used to request an IP address lease for a DHCP server. The message is sent when the client boots up. The DHCP Discover message is a broadcast packet that is sent over the network, requesting for a DHCP server to respond to it.

2. The DHCP servers that have a valid range of IP addresses, sends an offer message to the client. The DHCP Offer message is the response that the DHCP server sends to the client. The DHCP Offer message informs the client that the DHCP server has an available IP address. The DHCP Offer message includes the following information:

- o IP address of the DHCP server which is offering the IP address.
- o MAC address of the client.
- o Subnet mask. o Length of the lease.

3. The client sends the DHCP server a DHCP Request message. This message indicates that the client accepted the offer from the first DHCP server which responded to it. It also indicates that the client is requesting the particular IP address for lease. The client broadcasts the acceptance message so that all other DHCP servers who offered addresses can withdraw those addresses. The message contains the IP address of the DHCP server which it has selected.

4. The DHCP server sends the client a DHCP Acknowledge message. The DHCP Acknowledge message is actually the process of assigning the IP address lease to the client.

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 reuses 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 Advantages and Disadvantages

DHCP offers the following advantages:

- **IP address management**: Easier management of IP addresses is a primary advantage of DHCP. When DHCP is enabled, the DHCP server manages and assigns IP addresses without administrator intervention or manual configuration.

- **Centralized network client configuration:** The configuration information is stored in one place, in the DHCP data store. You can make changes for multiple clients just by changing the information in the data store.

- **Support of BOOTP clients:** Both BOOTP servers and DHCP servers listen and respond to broadcasts from clients. The DHCP server can respond to requests from BOOTP clients as well as DHCP clients.

- **Support of local clients and remote clients:** Most network routers can be configured to act as BOOTP relay agents to pass BOOTP requests to servers that are not on the client's network. DHCP requests can be relayed in the same manner because, to the router, DHCP requests are indistinguishable from BOOTP requests.

- **Network booting:** The DHCP server can give a client all the information that the client needs to function, including IP address, boot server, and network configuration information. Eliminating time needed for RARP (Reverse Address Resolution Protocol) and the boot params file.

- **Large network support:** Networks with millions of DHCP clients can use DHCP. The DHCP server uses multithreading to process many client requests simultaneously. The server also supports data stores that are optimized to handle large amounts of data.

DHCP suffers the following disadvantages:

- **Single point of Failure:** The DHCP server can well be a single point of failure in networking environments that only have one DHCP server. For this reason, it is recommended to have multiple DHCP servers on a large network

- **Error Propagation:** All incorrectly defined configuration information will automatically be propagated to your DHCP clients. Since DHCP servers inform and manage the network any wrong configuration information can propagate to other DHCP servers or nodes.

- **Segmented Network:** If your network has multiple segments, you have to perform either of the following additional configurations:
    - o Place a DHCP server on each segment
    - o Place a DHCP relay agent on each segment
    - o Configure routers to forward Bootstrap Protocol (BootP) broadcasts.

DHCP Attacks

Since DHCP protocol does 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. Few of the attacks related to DHCP are explained below

DHCP Spoofing

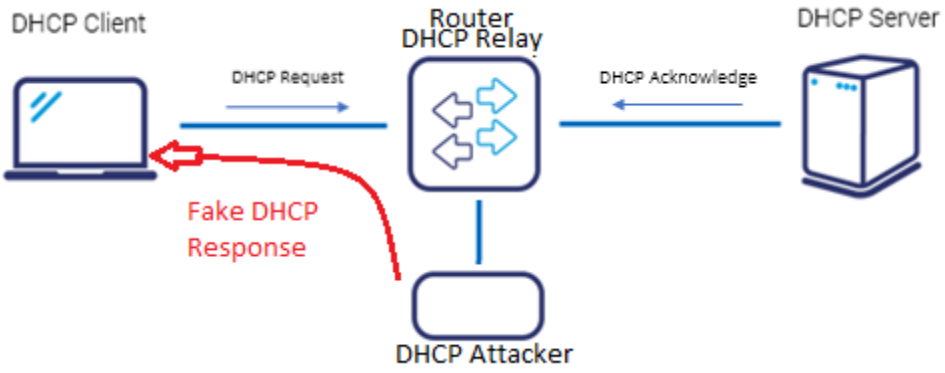


Image Reference: https://www.grandmetric.com

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.

DHCP Starvation

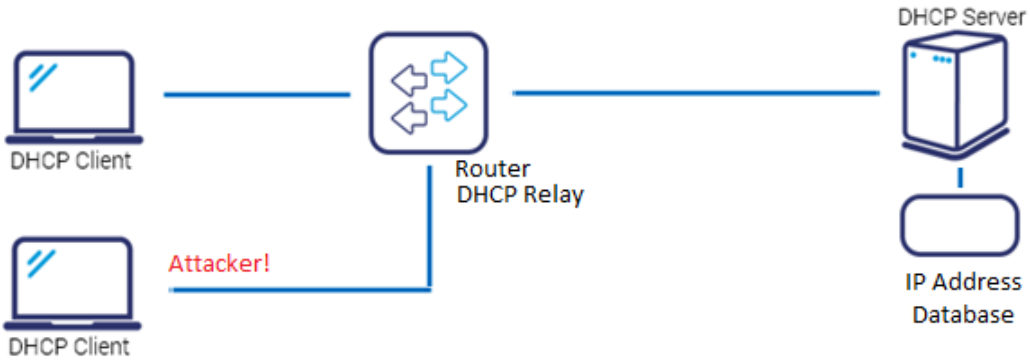
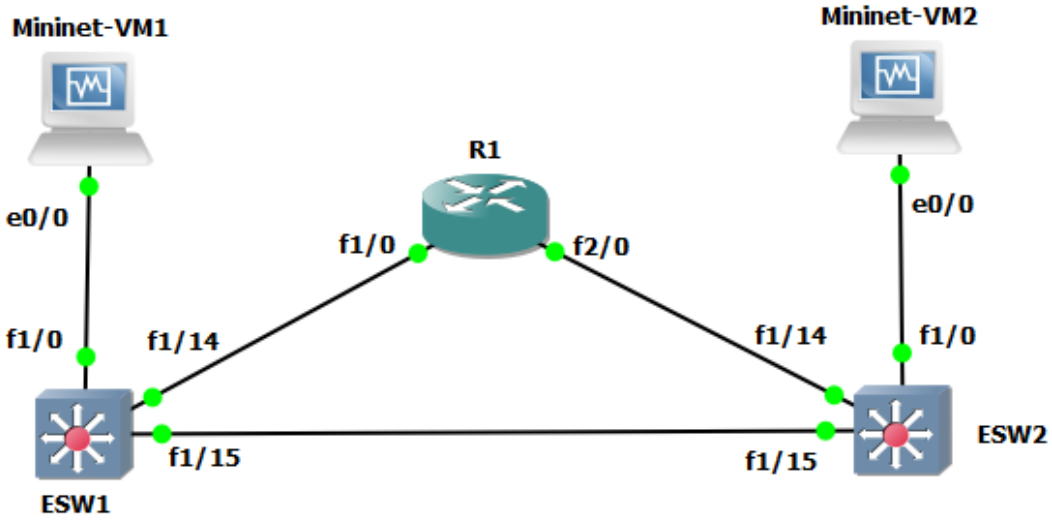


Image Reference: https://www.grandmetric.com

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.

DHCP Lab Setup



Lab2 Network Configuration Diagram.

The figure shows the network configuration used to simulate the operation of DHCP. We make of GNS3 to emulate a virtual network environment. The Network consists of the following simulated nodes.

Virtual Machines: To simulate two end points clients (VM1 and VM2), we make use of Oracle virtual box to virtualize 2 Linux client machines. Machines are added to GNS3 and are connected as shown in the figure

Ether-Switch Network Modules: Two simulate two Ether Switch (ESW1 and ESW2), we use 2 instances of Cisco 3725 ether switch. And connection is established between ESW1 and ESW2. Also each VM is connected to a ESW switch as shown in the above figure.

Router 7200: An instance of Router 7200 is created and connected to ESW1 and ESW2. Wired connection is established from ESW1 (1/14) and ESW2 (1/14) to FastEathernet 1/0 and FastEathernet 2/0 of router respectively.

Once the all the nods are created and connected the network is turned on by powering on all the nodes from GNS3.

After the network is up and running the following network configurations are made on **ESW1 ESW2** and **Router R1.**

Configurations on Router R1

```
Hostname R1
shut
interface Fa1/0
desc Link to ESW1 VLAN_100
ip address 10.10.100.254 255.255.255.0
no duplex full
no speed 100
no shut
!
```

```
Interface Fa1/0 has been added to VLAN_100
that was created in LAB1.It is assigned
IP: 10.10.100.254. Interface is set to full
duplex enabling simultaneous bidirectional
communication with 100mbps of network speed.
```

```
interface Fa2/0
shut
desc Link to ESW2 VLAN_200
ip address 10.10.200.254 255.255.255.0
no duplex full
no speed 100
no shut
!
ip routing
end
```

Interface Fa2/0 has been added to VLAN_200 that was created in LAB1.It is assigned IP: 10.10.200.254. Interface is set to full duplex enabling simultaneous bidirectional communication with 100mbps of network speed.

Layer 2 Configurations on Ether Switch 1

```
Hostname ESW1
vlan 100
name VLAN_100
!
interface Fa1/14
shut
switchport access vlan 100
desc Link to R1 VLAN_100
no duplex full
no speed 100
no shut
!
interface Fa1/0
switchport access vlan 100
desc Link to mininet1
no duplex full
no speed 100
no shut
end
```

Interface Fa1/14 is added to VLAN_100 that was created in LAB1.Switching link between R1 and VLAN_100 is established. Interface is set to full duplex enabling simultaneous bidirectional communication with 100mbps of network speed.

Interface Fa1/0 is added to VLAN_100 that was created in LAB1.Switching link between Linux Virtual Machine 1 and ESW1 (VLAN_100) is established. No IP is assigned to VM's yet. Interface is set to full duplex enabling simultaneous bidirectional communication with 100mbps of network speed.

Layer 2 Configurations on Ether Switch 2

```
Hostname ESW2
vlan 200
name VLAN_200
interface Fa1/14
shut
switchport access vlan 200
desc Link to R1 VLAN200
no duplex full
no speed 100
no shut
!
interface Fa1/0
switchport access vlan 200
desc Link to mininet2
no duplex full
no speed 100
no shut
end
```

Interface Fa1/14 is added to VLAN_200 that was created in LAB1.Switching link between R1 and VLAN_100 is established. Interface is set to full duplex enabling simultaneous bidirectional communication with 100mbps of network speed.

Interface Fa1/0 is added to VLAN_200 that was created in LAB1.Switching link between Linux Virtual Machine 2 and ESW2 (VLAN_200) is established. No IP is assigned to VM's yet. Interface is set to full duplex enabling simultaneous bidirectional communication with 100mbps of network speed.

Configurations on Mininet VM 1

```
sudo ifconfig eth0 10.10.100.1 netmask 255.255.255.0 up
sudo route add default gw 10.10.100.254 eth0
```

The above commands assign IP, Sub-netmask and default Gateway to VM1. We can see the effective configurations by *route -n*, output is as follows

```
mininet@mininet-vm:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.10.100.254   0.0.0.0         UG    0      0        0 eth0
10.10.100.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

Configurations on Mininet VM 2

```
sudo ifconfig eth0 10.10.200.1 netmask 255.255.255.0 up
sudo route add default gw 10.10.200.254 eth0
```

The above commands assign IP, Sub-netmask and default Gateway to VM1. We can see the effective configurations by *route -n*, output is as follows

```
mininet@mininet-vm:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.10.200.254   0.0.0.0         UG    0      0        0 eth0
10.10.200.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

This completes the initial Lab set up. We verified the connections by pinging all the nodes from each Virtual machine. All the pings were successful, and all the devices are behaving according to the configurations. We will now go through the mac addresses tables and spanning trees of ESW1 and ESW2

Mac-address tables and spanning tree in ESW1

Terminal O/P of Mac-address table:

```
ESW1#show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
c201.1248.0000          Self          1     Vlan1
ca03.2270.001c          Dynamic     100     FastEthernet1/14
0800.27ad.f28c          Dynamic     100     FastEthernet1/0
```

Terminal O/P of Spanning tree (VLAN_100)

```
ESW1#show spanning-tree vlan 100 brief
VLAN100
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     c201.1248.0001
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32768
             Address     c201.1248.0001
```

```
            Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
            Aging Time 300
Interface                                   Designated
Name                Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
------------------- ------- ---- ----- --- ----- -------------------- -------
FastEthernet1/0     128.41   128    19 FWD     0 32768 c201.1248.0001 128.41
FastEthernet1/14    128.55   128    19 FWD     0 32768 c201.1248.0001 128.55
```

Terminal O/P of Spanning tree (VLAN_200)

```
ESW1#show spanning-tree vlan 200 brief
Spanning tree instance for VLAN 200 does not exist.
ESW1#
```

Note that we do not see any spanning tree for VLAN 200 at ESW1 because it does not belong to VLAN_200.

Mac-address tables and spanning tree in ESW2

Terminal O/P of Mac-address table:

```
ESW2#show mac-address-table
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
c202.56f4.0000          Self          1     Vlan1
ca03.2270.0038          Dynamic     200     FastEthernet1/14
```

Terminal O/P of Spanning tree (VLAN_100)

```
ESW2#show spanning-tree vlan 100 brief
Spanning tree instance for VLAN 100 does not exist.
```

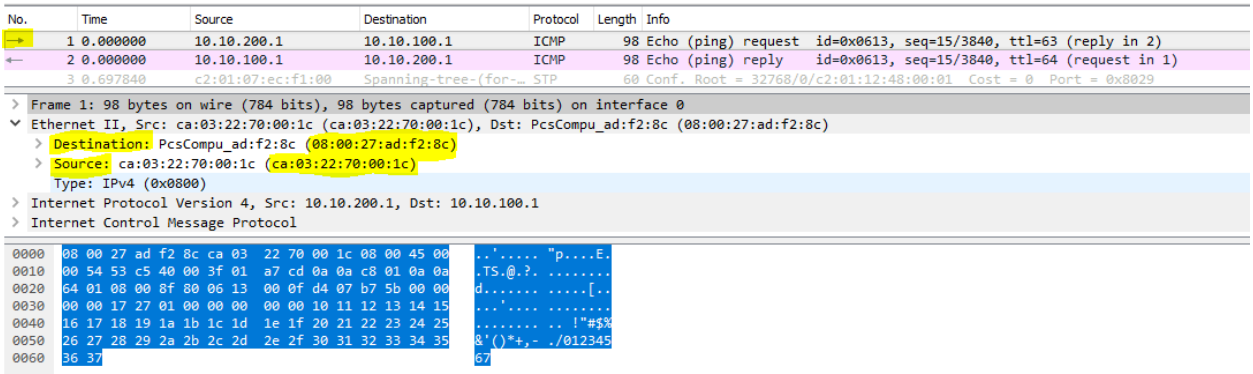
Note that we do not see any spanning tree for VLAN 200 at ESW1 because it does not belong to VLAN_200.

Terminal O/P of Spanning tree (VLAN_200)

```
ESW2#show spanning-tree vlan 200 brief
VLAN200
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     c202.56f4.0001
             This bridge is the root
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
  Bridge ID  Priority    32768
             Address     c202.56f4.0001
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
Interface                                   Designated
Name                Port ID Prio Cost  Sts Cost  Bridge ID            Port ID
------------------- ------- ---- ----- --- ----- -------------------- ------
FastEthernet1/0     128.41   128    19 FWD     0 32768 c202.56f4.0001 128.41
FastEthernet1/14    128.55   128    19 FWD     0 32768 c202.56f4.0001 128.55
```

Observations Part 1

After all the configurations of all the nodes we are ready to populate the network with packets and observe the packet path and addresses/data those packets hold. For this we start the ping from virtual machine 2 to virtual machine 1. Once the ping begins we observe the traffic on the link between ESW1 and virtual machine 1. We use Wireshark to capture the packets and the observations are as follows.



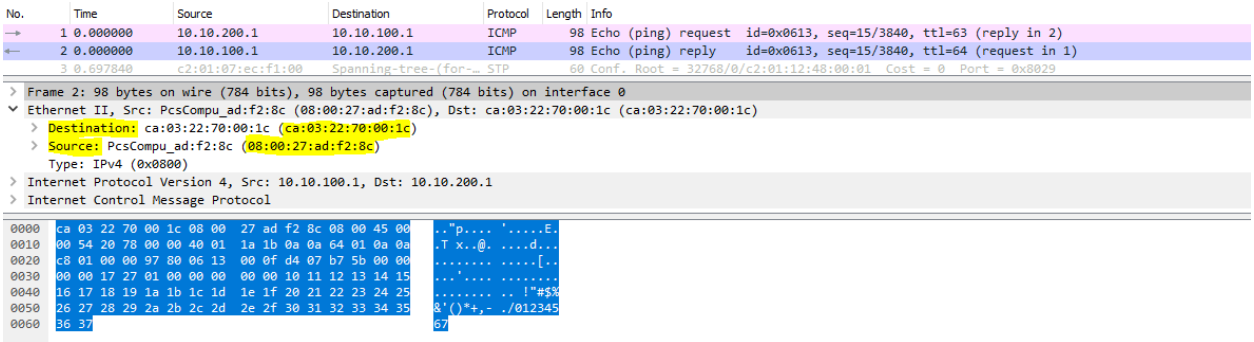
Wire shark capture of ICMP packet from Virtual machine 2 to virtual machine 1

VM1 mac Address: 08:00:27:ad:f2:8c. VM2 mac Address: **ca03.2270.001c**

Form the mac-address table of ESW1 we know the following

```
Mac address ca03.2270.001c is reachable on port/interface FastEthernet1/14
Mac address 0800.27ad.f28c is reachable on port/interface FastEthernet1/0
```

From the wireshark capture on interface f1/0 we can observe that the packets carry mac address of destination (**ca03.2270.001c**). ESW1 forwards all the packets to this destination to interface f1/0.



Wire shark capture of ICMP packet from Virtual machine 2 to virtual machine 1

When we observe the Response packet from Virtual machine 2 to virtual machine we can see that the destination mac address is ca03.2270.001c, which will be forwarded to interface f1/14 on ESW1. The packet reaches vm2 via router and ESW2.

Configurations Part 2

For this part of the lab we will configure Virtual machine 2 as our DHCP server and observe the changes and its effects on the network.

Virtual Machine 2 configuration
Commands

```
sudo nano /etc/dhcp/dhcpd.conf
```

and the following lines are added to the dhcpd.conf file

```
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;
}
```

Here we provide a pool of IP addresses to the DHCP server which it can use to allocate the IP addresses. In this case 10.10.100.0 till 10.10.100.60. other details such as broadcast address router IPS are initialized and DHCP is configured.

For the changed to take effect we restart the DHCP server.

```
sudo service isc-dhcp-server restart
```

Router configuration
We will configure router R1 to forward DHCP requests to virtual machine 2

Commands

```
config_t
interface FA1/0
ip helper-address 10.10.200.1
```

Virtual Machine 1 configuration
We will now configure VM1 as DHCP client

Commands

```
sudo ifconfig
sudo ifconfig eth0 down
sudo ifconfig eth0 up
```

This should have reset the interface on mininet1 and mininet2 should have provided an IP address. We will now take a look at the IP address again.

View IP configurations on VM1

```
mininet@mininet-vm:~$ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ad:f2:8c
          inet addr:10.10.100.40  Bcast:10.10.100.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:204 errors:0 dropped:0 overruns:0 frame:0
          TX packets:203 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15884 (15.8 KB)  TX bytes:17158 (17.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:165 errors:0 dropped:0 overruns:0 frame:0
          TX packets:165 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12756 (12.7 KB)  TX bytes:12756 (12.7 KB)
```

View Route -n after reboot

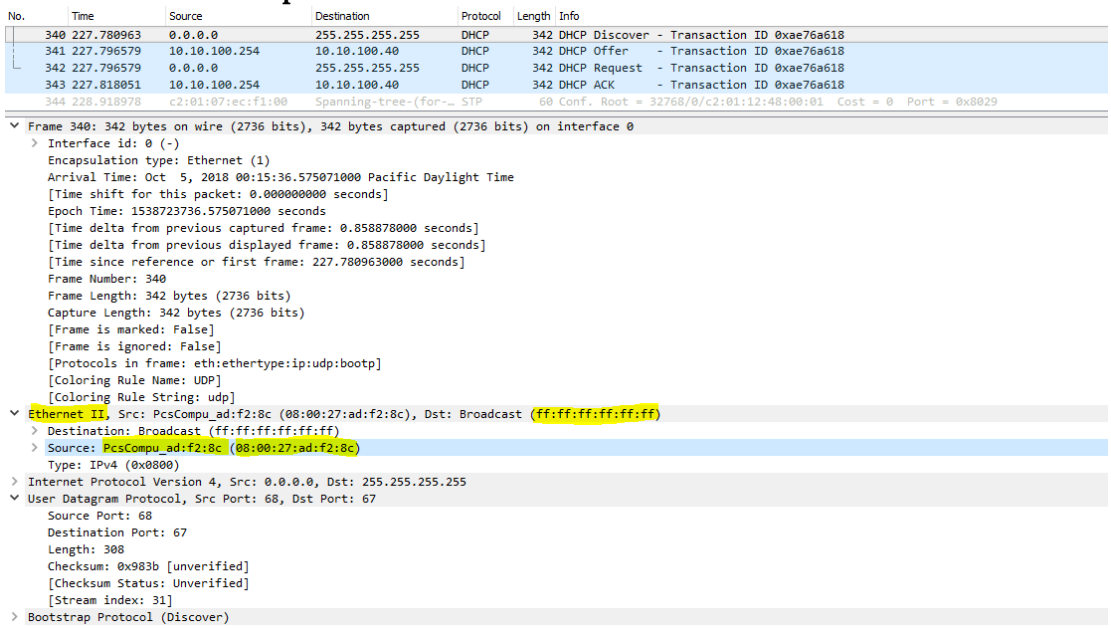
```
mininet@mininet-vm:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.10.100.254   0.0.0.0         UG    0      0        0 eth0
10.10.100.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

After the network card reset we can see that the DHCP has assigned the VM1 with IP addr:10.10.100.40 Which was the starting address of IP Pool provided during the DHCP configuration at VM2.

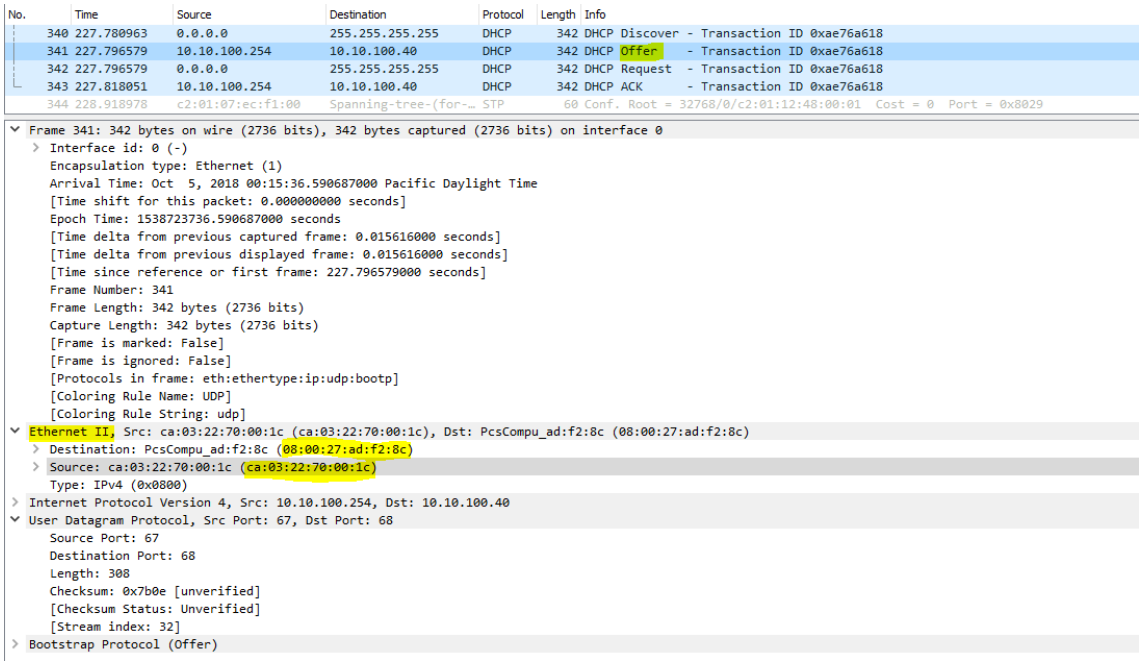
Observations Part 2

After all the configurations of all the nodes we are ready to populate the network with packets and observe the packet path and addresses/data those packets hold. For this we start the ping from virtual machine 2 to virtual machine 1. Once the ping begins we observe the traffic on the link between ESW1 and virtual machine 1. We then capture traffic on the link between ESW2 and virtual machine 2. We use Wireshark to capture the packets and the observations are as follows.

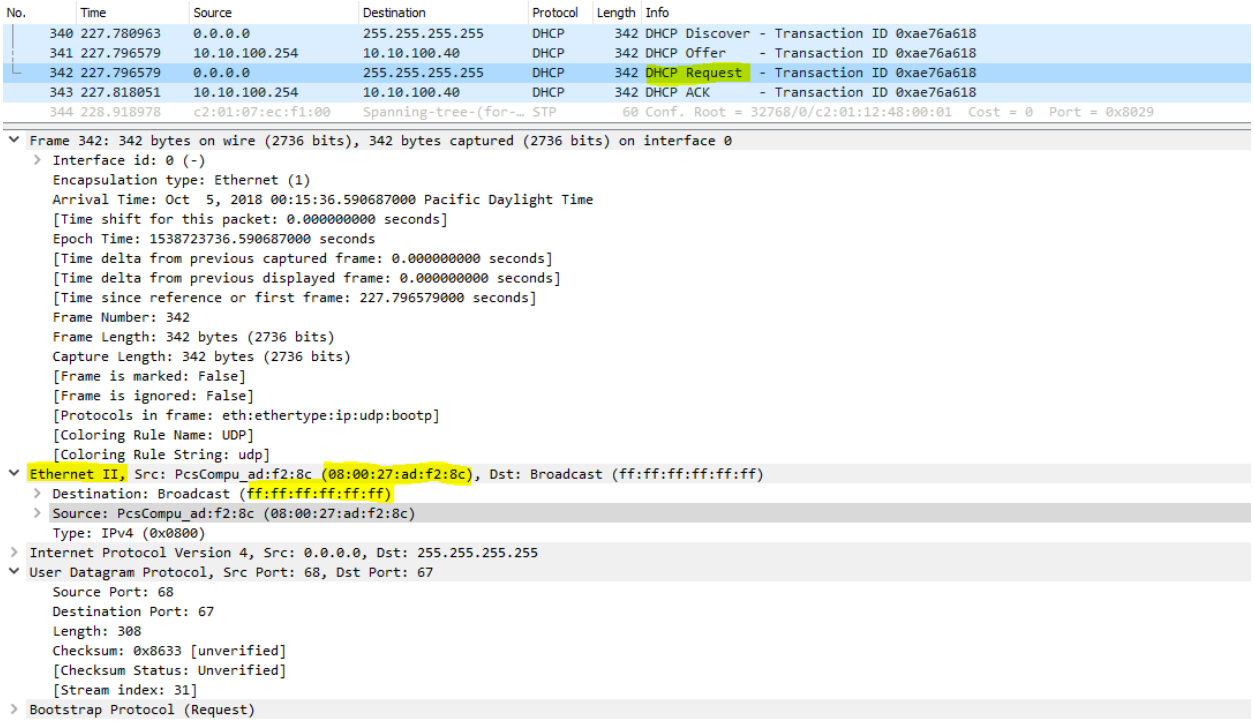
Captures on the interface between vm1 and ESW1



Wireshark Capture of DHCP Discover Message from vm1 to all the nodes.



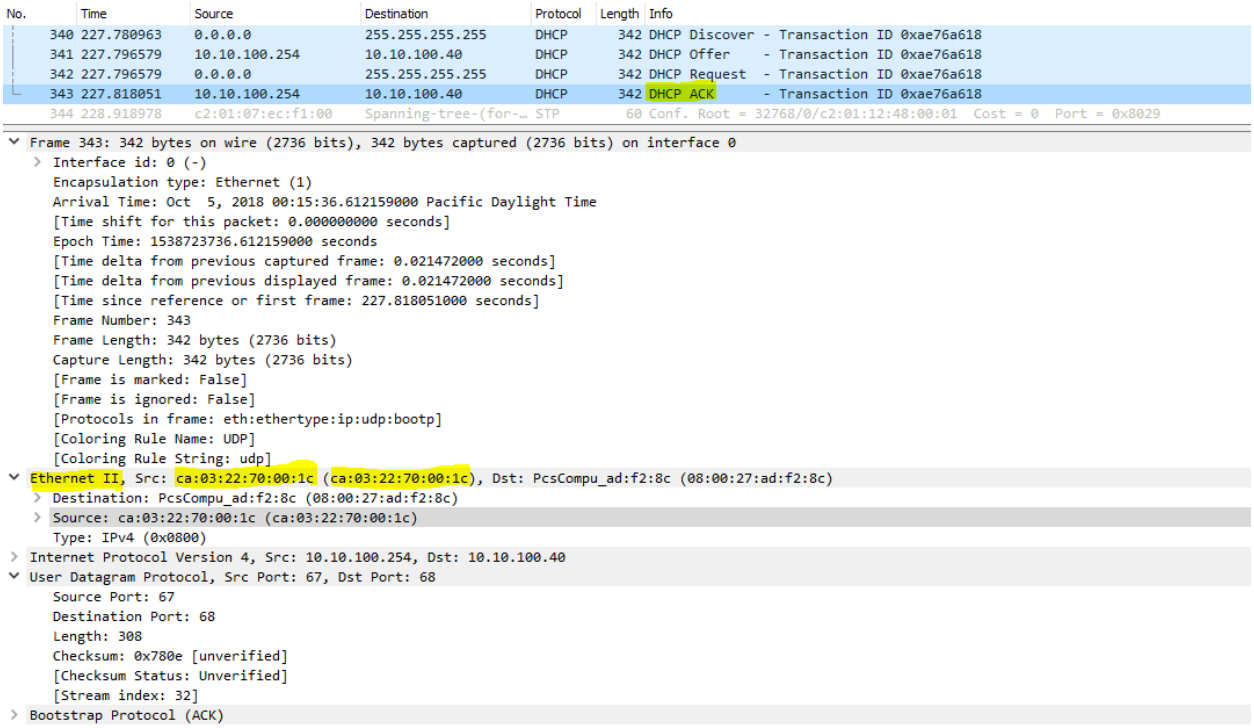
Wireshark Capture of DHCP Offer Message from DHCP server to VM1.



```
No.  Time         Source          Destination     Protocol Length Info
 340 227.780963   0.0.0.0         255.255.255.255 DHCP       342 DHCP Discover - Transaction ID 0xae76a618
 341 227.796579   10.10.100.254   10.10.100.40    DHCP       342 DHCP Offer    - Transaction ID 0xae76a618
 342 227.796579   0.0.0.0         255.255.255.255 DHCP       342 DHCP Request  - Transaction ID 0xae76a618
 343 227.818051   10.10.100.254   10.10.100.40    DHCP       342 DHCP ACK      - Transaction ID 0xae76a618
 344 228.918978   c2:01:07:ec:f1:00 Spanning-tree-(for-… STP    60 Conf. Root = 32768/0/c2:01:12:48:00:01  Cost = 0  Port = 0x8029

Frame 342: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
  Interface id: 0 (-)
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct  5, 2018 00:15:36.590687000 Pacific Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1538723736.590687000 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: 227.796579000 seconds]
  Frame Number: 342
  Frame Length: 342 bytes (2736 bits)
  Capture Length: 342 bytes (2736 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:bootp]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
Ethernet II, Src: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  Source: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c)
  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
  Source Port: 68
  Destination Port: 67
  Length: 308
  Checksum: 0x8633 [unverified]
  [Checksum Status: Unverified]
  [Stream index: 31]
Bootstrap Protocol (Request)
```

Wireshark Capture of DHCP Request Message from vm1.



```
No.  Time         Source          Destination     Protocol Length Info
 340 227.780963   0.0.0.0         255.255.255.255 DHCP       342 DHCP Discover - Transaction ID 0xae76a618
 341 227.796579   10.10.100.254   10.10.100.40    DHCP       342 DHCP Offer    - Transaction ID 0xae76a618
 342 227.796579   0.0.0.0         255.255.255.255 DHCP       342 DHCP Request  - Transaction ID 0xae76a618
 343 227.818051   10.10.100.254   10.10.100.40    DHCP       342 DHCP ACK      - Transaction ID 0xae76a618
 344 228.918978   c2:01:07:ec:f1:00 Spanning-tree-(for-… STP    60 Conf. Root = 32768/0/c2:01:12:48:00:01  Cost = 0  Port = 0x8029

Frame 343: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
  Interface id: 0 (-)
  Encapsulation type: Ethernet (1)
  Arrival Time: Oct  5, 2018 00:15:36.612159000 Pacific Daylight Time
  [Time shift for this packet: 0.000000000 seconds]
  Epoch Time: 1538723736.612159000 seconds
  [Time delta from previous captured frame: 0.021472000 seconds]
  [Time delta from previous displayed frame: 0.021472000 seconds]
  [Time since reference or first frame: 227.818051000 seconds]
  Frame Number: 343
  Frame Length: 342 bytes (2736 bits)
  Capture Length: 342 bytes (2736 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:bootp]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]
Ethernet II, Src: ca:03:22:70:00:1c (ca:03:22:70:00:1c), Dst: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c)
  Destination: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c)
  Source: ca:03:22:70:00:1c (ca:03:22:70:00:1c)
  Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.10.100.254, Dst: 10.10.100.40
User Datagram Protocol, Src Port: 67, Dst Port: 68
  Source Port: 67
  Destination Port: 68
  Length: 308
  Checksum: 0x780e [unverified]
  [Checksum Status: Unverified]
  [Stream index: 32]
Bootstrap Protocol (ACK)
```

Wireshark Capture of DHCP Acknowledge Message from vm1 to all the nodes.

Captures on interface between ESW2 and VM2

No.	Time	Source	Destination	Protocol	Length	Info
340	227.780963	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xae76a618
341	227.796579	10.10.100.254	10.10.100.40	DHCP	342	DHCP Offer - Transaction ID 0xae76a618
342	227.796579	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xae76a618
343	227.818051	10.10.100.254	10.10.100.40	DHCP	342	DHCP ACK - Transaction ID 0xae76a618
344	228.918978	c2:01:07:ec:f1:00	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/0/c2:01:12:48:00:01 Cost = 0 Port = 0x8029
345	229.257649	PcsCompu_ad:f2:8c	Broadcast	ARP	60	Who has 10.10.100.254? Tell 10.10.100.40
346	229.267410	ca:03:22:70:00:1c	PcsCompu_ad:f2:8c	ARP	60	10.10.100.254 is at ca:03:22:70:00:1c

```
> Frame 340: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
v Ethernet II, Src: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
      Source Port: 68
      Destination Port: 67
      Length: 308
      Checksum: 0x983b [unverified]
      [Checksum Status: Unverified]
      [Stream index: 31]
> Bootstrap Protocol (Discover)
```

Wireshark capture of Discover message from VM1 to DHCP server which is a broad cast.

No.	Time	Source	Destination	Protocol	Length	Info
340	227.780963	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xae76a618
341	227.796579	10.10.100.254	10.10.100.40	DHCP	342	DHCP Offer - Transaction ID 0xae76a618
342	227.796579	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xae76a618
343	227.818051	10.10.100.254	10.10.100.40	DHCP	342	DHCP ACK - Transaction ID 0xae76a618
344	228.918978	c2:01:07:ec:f1:00	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/0/c2:01:12:48:00:01 Cost = 0 Port = 0x8029
345	229.257649	PcsCompu_ad:f2:8c	Broadcast	ARP	60	Who has 10.10.100.254? Tell 10.10.100.40
346	229.267410	ca:03:22:70:00:1c	PcsCompu_ad:f2:8c	ARP	60	10.10.100.254 is at ca:03:22:70:00:1c

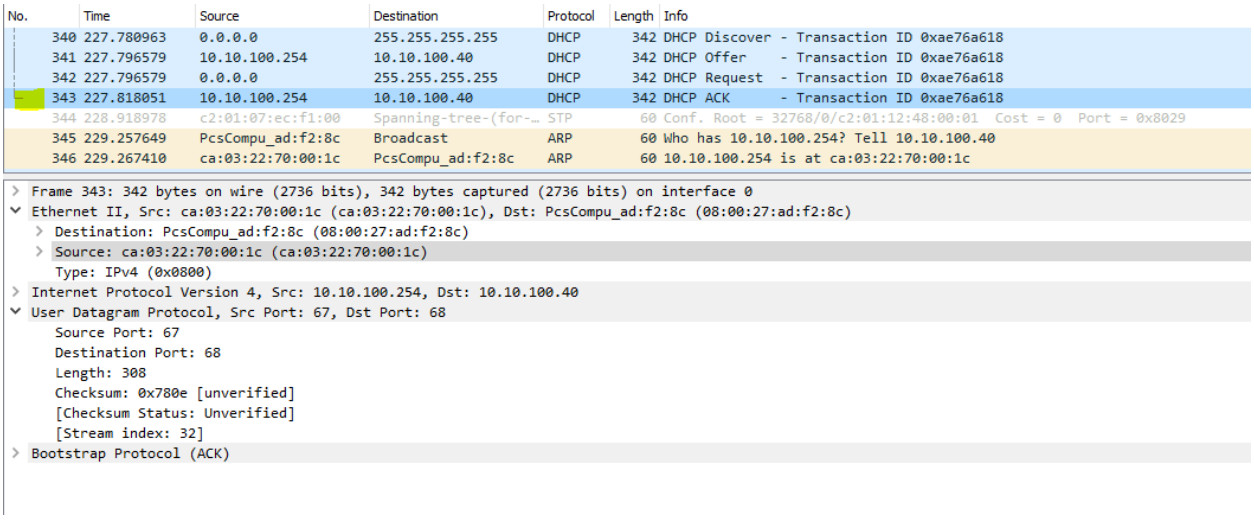
```
> Frame 341: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
v Ethernet II, Src: ca:03:22:70:00:1c (ca:03:22:70:00:1c), Dst: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c)
    > Destination: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c)
    > Source: ca:03:22:70:00:1c (ca:03:22:70:00:1c)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.10.100.254, Dst: 10.10.100.40
v User Datagram Protocol, Src Port: 67, Dst Port: 68
      Source Port: 67
      Destination Port: 68
      Length: 308
      Checksum: 0x7b0e [unverified]
      [Checksum Status: Unverified]
      [Stream index: 32]
> Bootstrap Protocol (Offer)
```

Wireshark capture of Offer message from DHCP to VM1 which is a unicast message

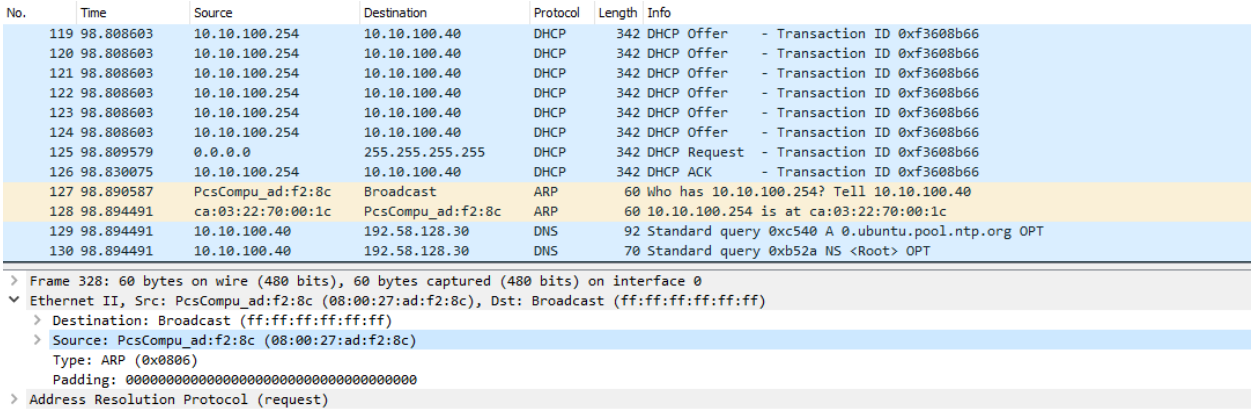
No.	Time	Source	Destination	Protocol	Length	Info
340	227.780963	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xae76a618
341	227.796579	10.10.100.254	10.10.100.40	DHCP	342	DHCP Offer - Transaction ID 0xae76a618
342	227.796579	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xae76a618
343	227.818051	10.10.100.254	10.10.100.40	DHCP	342	DHCP ACK - Transaction ID 0xae76a618
344	228.918978	c2:01:07:ec:f1:00	Spanning-tree-(for-…	STP	60	Conf. Root = 32768/0/c2:01:12:48:00:01 Cost = 0 Port = 0x8029
345	229.257649	PcsCompu_ad:f2:8c	Broadcast	ARP	60	Who has 10.10.100.254? Tell 10.10.100.40
346	229.267410	ca:03:22:70:00:1c	PcsCompu_ad:f2:8c	ARP	60	10.10.100.254 is at ca:03:22:70:00:1c

```
> Frame 342: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
v Ethernet II, Src: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    > Source: PcsCompu_ad:f2:8c (08:00:27:ad:f2:8c)
      Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
v User Datagram Protocol, Src Port: 68, Dst Port: 67
      Source Port: 68
      Destination Port: 67
      Length: 308
      Checksum: 0x8633 [unverified]
      [Checksum Status: Unverified]
      [Stream index: 31]
> Bootstrap Protocol (Request)
```

Wire shark capture if Request message from Vm1 to Vm2 again a broadcast message



Wireshark capture of DHCP Acknowledge message from DHCP server to VM1 unicast



Wireshark Capture of DHCP ARP and DNS packets on the interface used for path discovery.

Conclusion

With this lab we obtained practical and detail understating of DHCP.Discussed the operation of DHCP, Types of DHCP Messages, Message/packet format and looked at some of the Advantages and disadvantages of using DHCP. We also covered few aspects such as security threats related to DHCP. Lastly the following learning objectives were accomplished

- Learnt to build and configure a layer 3 topology in GNS using Cisco 7200 routers
- Learnt to analyze Spanning Tree Protocol (STP) on the router
- Learnt to configure DHCP Relay across different VLANS/Networks
- Learnt to configure DHCP on end-point/client systems (Linux VMs)

Contributions

Charit Upadhyay

- Set up lab in GNS3
- Executed lab in GNS
- Troubleshooting network topology
- Wireshark observation
- Equal contribution and learning on all aspects

Devika Jadhav

- DHCP message format
- DHCP Architecture
- Documentation and report formatting
- Observations on Wireshark
- Equal contribution and learning on all aspects

Pradeep Patil

- GNS3 Console observations
- Lab Configurations
- Working of DHCP
- Documentation and report formatting
- Equal contribution and learning on all aspects

References / Links

- 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
- GNS: https://www.gns3.com/
- Wireshark: https://www.wireshark.org/
- ISC DHCP Server https://help.ubuntu.com/community/isc-dhcp-server/
- Cisco Basic IOS commands: https://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r/frf001.html