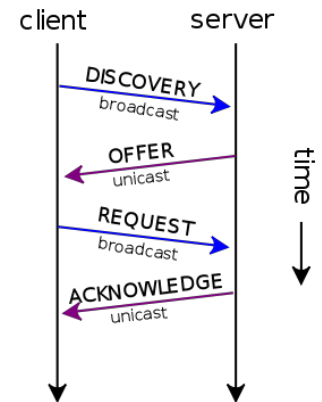


WIRESHARK LAB : DHCP

The Dynamic Host Configuration Protocol (DHCP) is a network service that enables host computers to be automatically assigned settings (including IP address and network parameters) from a server as opposed to manually configuring each network host. With DHCP, computers (hosts) can request IP addresses and networking parameters automatically from a DHCP server, without having to manually configure these settings. Recall that The DHCP protocol employs a connectionless service model, using UDP. It is implemented with two UDP port numbers for its operations which are the same as for the BOOTP protocol. UDP port number 67 is the destination port of a server, and UDP port number 68 is used by the client.



DHCP operations fall into four phases: server discovery, IP lease offer, IP request, and IP lease acknowledgment. These stages are often abbreviated as DORA for discovery, offer, request, and acknowledgment, as shown in the figure.

The purpose of this lab is to learn about the following:

- How to setup a DHCP server.
- What kind of messages are exchanged between DHCP server and DHCP client.
- What happens if two DHCP servers are present in the same network.
- What will be the IP address of a client when it is broadcasting using the DISCOVERY message.

PART 1: In this section you are expected to set up your own DHCP server.

The basic idea in this section is to setup the configuration shown in the figure below. To do so complete the following steps.

Step 1a: Boot up your computer. Log into each Linux machine with Ubuntu 12.04 (do not login as Guest). After the machines are ready, using the `ifconfig` command, determine which *eth* is connected to the Internet on each machine. Make sure you disable the *eth* interface to the Internet on each machine.

Step 1b: Check the back of your computer and see which *eth* (*eth0*, *eth1*, etc.) is connected to the patch panel. Activate one of the available *eth* interfaces connected to the patch panel.

YOUR RESPONSE:

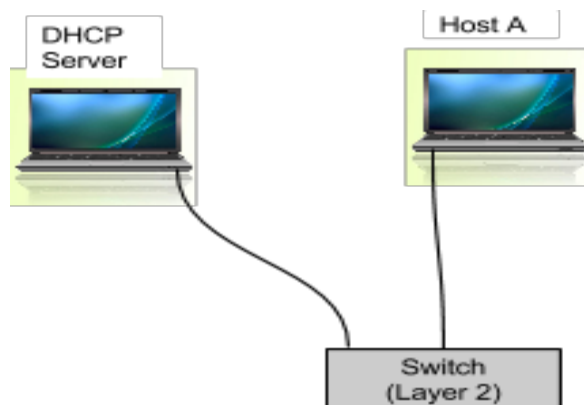
Step 2a: Turn on the layer 2 switch. Select one of the computer as your DHCP server. Using appropriate cables create the network shown in the figure below.

Step 2b: Your DHCP server must have IP address of `192.168.0.1`. Don't worry about the IP address of the host for now.

```
sudo ifconfig eth<x> 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255
```

Step 3: Check and make sure machine has the latest updates. What command you use?

YOUR RESPONSE:



SERVER INSTALLATION & CONFIGURATION:

Step 5: Install DHCP server on your machine using the following command:

```
sudo apt-get install dhcp3-server.
```

you should see something like this at the end of installation :

```
Setting up isc-dhcp-server (4.1.ESV-R4-0ubuntu5.9) ...  
Generating /etc/default/isc-dhcp-server...  
isc-dhcp-server start/running, process 4414  
isc-dhcp-server6 stop/pre-start, process 4447  
Setting up dhcp3-server (4.1.ESV-R4-0ubuntu5.9) ...
```

Step 6: Copy the `dhcpd.conf` file into `dhcpd_copy.conf`. Now open the file `dhcpd.conf` using nano or VI, or any other editor and do the following changes to the `dhcpd.conf` file in order to configure the DHCP service. Add the following lines to `dhcpd.conf`

```
/etc/dhcp/dhcpd.conf
```

```
option routers 192.168.0.1;  
  
subnet 192.168.0.0 netmask 255.255.255.0 {  
    range 192.168.0.2 192.168.0.50;  
}
```

Note that in this case *option routers 192.168.0.1* is your gateway address.

Also note that *range 192.168.0.2 - 192.168.0.50* is the range of IP address the DHCP server can provide.

Step 7: Make sure the IP address of your server is 192.168.0.1. Don't worry about IP addresses on Host A.

Step 8: Start the DHCP server using the following command:

```
sudo /etc/init.d/isc-dhcp-server start
```

Step 9: Check if the server is running or not using the following command: (Note: You need to check your IP address often to make sure it is set to 192.168.0.1)

```
sudo ps fax | grep dhcp
```

CLIENT CONFIGURATION:

Step 10: On the client machine (HOST A - as shown in the figure above) make sure you have disconnected the Internet using `ifconfig` command and make sure it is connected to the switch as shown in the figure above.

```
sudo ifconfig eth<x> down
```

Step 11: When you are ready, in the DHCP server open the wireshark program and start capturing the packets. Disable and enable the `eth` interface on HOST A.

```
sudo ifconfig eth<y> down
```

```
sudo ifconfig eth<y> up
```

In the wireshark make sure you see all the messages exchanged between DHCP server and client are captured. Stop the wireshark and save the files as `wireshark_dhcp.pcap`.

(Note: If you are not able to capture messages exchanges between DHCP server and client, delete all the lease in the client machine by using the following command.

```
sudo cd /var/lib/dhcp
```

```
sudo rm -r lease*
```

Now repeat steps 7 through 9 and start capturing again. You may also have to disable and enable the `eth` interface on HOST A.)

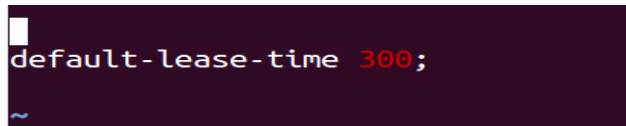
Answer the following questions:

- 1) Using the timing diagram show all the packets exchanged between DHCP server and host.
- 2) What is the IP address of the DHCP server?
- 3) What IP address did the DHCP server assign to the host?
- 4) Which transport protocol is used by DHCP server?

- 5) How can you filter all the DHCP packets? What filter is used?
- 6) Filter all the DHCP packets. Go to Statistics → flow graph → select general flow for displayed packets. Show a snapshot of the flow graph.
- 7) what is the gateway address? What command did you use to find the Gateway address?
- 8) Can you find the lease time given to the client? What is the lease time?

Step 12: Change the lease time to 5 min by editing the `default-lease-time` in the DHCP server.

`/etc/dhcp/dhcpd.conf` file.



```
default-lease-time 300;
```

Step 13: Open the Wireshark on HOST A and start capturing the packets.

Step 14a: Stop the DHCP server and restart it again:

```
sudo /etc/init.d/isc-dhcp-server stop
```

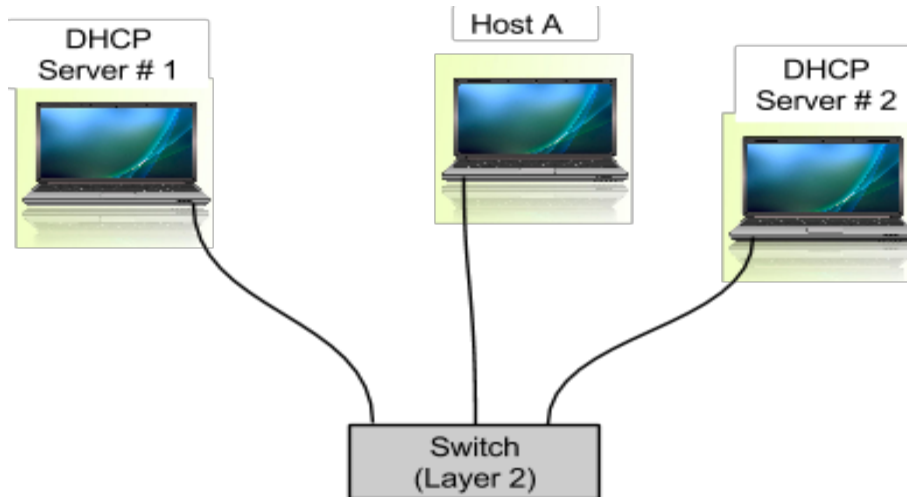
```
sudo /etc/init.d/isc-dhcp-server restart
```

Step 14b: Stop the Wireshark and save the files as `wireshark_dhcp_step14.pcap`.

Provide your answers to the following questions:

- 9) Did the host system send any DHCP messages to the DHCP server? Explain your answer
- 10) Restart the host machine. What is the IP address the host received? Did it get a new IP address or it has the same IP address as before. Explain your answer?
- 11) Wait until the lease is expired. Do you see any exchange of packets after the lease is expired? Explain your answer.
- 12) Show a snapshot of the change in lease time.

PART 2: In this section you are expected to set up two DHCP servers and observe the interaction of the host with the servers.



Step 15: Set up another DHCP server in the same network by following the steps from 5 through 8 with a different IP address (192.168.0.51) and range of IP address the DHCP server can provide. Add the following lines in the second server's dhcpd.conf file.

```
/etc/dhcp/dhcpd.conf
```

```
option routers 192.168.0.51;
subnet 192.168.0.0 netmask 255.255.255.0 {
    range 192.168.0.52 192.168.0.100;
}
```

Step 15a: Your second DHCP server must have IP address of 192.168.0.51. Set the IP address of the second dhcp server to 192.168.0.51 by using the following command.

```
sudo ifconfig eth<x> 192.168.0.1 netmask 255.255.255.0 broadcast 192.168.0.255
```

Step 16: Before starting the wireshark check your IP address of the two DHCP servers and make sure they are running. Open wireshark in one of the server and start capturing.

Restart the client machine (HOST A). Make sure HOST A received an IP address from the DHCP server. Stop the Wireshark and save the file as `wireshark_dhcp_step16.pcap`.

Provide your answers to the following questions:

- 13) What is the new IP address of HOST A?
- 14) Using the timing diagram show all the packets exchanged between the two DHCP servers and the client.
- 15) How do you know which DHCP server provided the IP address?
- 16) Is it possible to ensure that HOST A only uses the first SERVER to receive its IP address?

Show your results to the instructor before you leave the lab!

References:

1- Wikipedia: http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol