## Assignment 02 Task 02

## Understanding IP addressing: Subnetting, DHCP, NAT etc.

### Experiment Scenario

### Introduction

In this experiment I did some packet trace captures and saved outputs of some other networking commands while I used some networking applications. For you to understand the packet trace, you need to understand exactly where and when the trace was captured or where the commands were issued and output saved. Read this part carefully.

In the  [folder of data files](https://www.dropbox.com/sh/afy7lwmkfy6sgxv/AACnjensp2QSTFeCv0WSQ0gga?dl=0) collected for this experiment, you have been given the following trace files:

1. laptopConnectingToWireless.pcap
2. laptopSSHtoLoginIITB.pcap
3. loginIITB\_trace\_ssh.pcap

In addition you have

1. tracertToLoginIITB.out (traceroute from my laptop to login.iitb.ac.in)
2. tracerouteFromLoginIITB (traceroute from login.iitb.ac.in to a certain IP address)
3. Netstat\_laptop.out (Output of netstat issued on my laptop)
4. Netstat\_surya.out (Output of netstat issued on machine surya)

In the rest of this document, first, I will describe the scenario under which the trace files and other files were captured and saved, then there are questions which you need to answer and submit for evaluation. (You can download this as odt or doc, write in the answers,

**This is the file you must convert to pdf and submit at the end. Upload is on bodhitree1, so the usual “double tarring” will be required.**

### Scenario under which trace files were collected

The network scenario is as follows:

* I have a Windows laptop (hostname ProfVarshaApte) which I was using in my home wireless network (Internet Service Provider: Spectranet). Note that I do not live on campus.
* At the beginning I had turned the wireless interface off (with a hard button on my laptop). The outputs of various networking commands were as follows:

**-bash-3.2$ arp -a**

**No ARP Entries Found**

**-bash-3.2$** **ipconfig**

**Ethernet adapter Local Area Connection 5:**

**Media State . . . . . . . . . . . : Media disconnected**

**Ethernet adapter Local Area Connection:**

**Media State . . . . . . . . . . . : Media disconnected**

**Ethernet adapter Wireless Network Connection:**

**Media State . . . . . . . . . . . : Media disconnected**

**-bash-3.2$** **route PRINT**

**Interface List**

**0x1 ........................... MS TCP Loopback interface**

**0x2 ...00 22 fa 2b 4f 50 ...... Intel(R) Wireless WiFi Link 5100 - Packet Scheduler Miniport**

**0x3 ...00 1c 7e ec a5 bb ...... Intel(R) 82567V Gigabit Network Connection - Packet Scheduler Miniport**

**0x4 ...00 ff cc 93 71 1a ...... TAP-Win32 Adapter V9 - Packet Scheduler Miniport**

**===========================================================================**

**===========================================================================**

**Active Routes:**

**Network Destination Netmask Gateway Interface Metric**

**127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1**

**255.255.255.255 255.255.255.255 255.255.255.255 2 1**

**255.255.255.255 255.255.255.255 255.255.255.255 3 1**

**255.255.255.255 255.255.255.255 255.255.255.255 4 1**

**===========================================================================**

**Persistent Routes:**

**Now I first started capturing packets on the wireless interface and THEN turned the wireless interface button ON**

***This trace file is laptopConnectingtoWireless.pcap***

Outputs of various commands on my laptop after connection is established are:

**-bash-3.2$ arp -a**

**Interface: 192.168.0.2 --- 0x2**

**Internet Address Physical Address Type**

**192.168.0.1 94-d7-23-7b-e1-90 dynamic**

**-bash-3.2$ route**

**<Initial part is the same>**

**===========================================================================**

**Active Routes:**

**Network Destination Netmask Gateway Interface Metric**

**0.0.0.0 0.0.0.0 192.168.0.1 192.168.0.2 25**

**127.0.0.0 255.0.0.0 127.0.0.1 127.0.0.1 1**

**169.254.0.0 255.255.0.0 192.168.0.2 192.168.0.2 20**

**192.168.0.0 255.255.255.0 192.168.0.2 192.168.0.2 25**

**192.168.0.2 255.255.255.255 127.0.0.1 127.0.0.1 25**

**192.168.0.255 255.255.255.255 192.168.0.2 192.168.0.2 25**

**224.0.0.0 240.0.0.0 192.168.0.2 192.168.0.2 25**

**255.255.255.255 255.255.255.255 192.168.0.2 192.168.0.2 1**

**255.255.255.255 255.255.255.255 192.168.0.2 20003 1**

**255.255.255.255 255.255.255.255 192.168.0.2 4 1**

**Default Gateway: 192.168.0.1**

**===========================================================================**

**-bash-3.2$ ifconfig**

**Ethernet adapter Wireless Network Connection:**

**Connection-specific DNS Suffix . :**

**IP Address. . . . . . . . . . . . : 192.168.0.2**

**Subnet Mask . . . . . . . . . . . : 255.255.255.0**

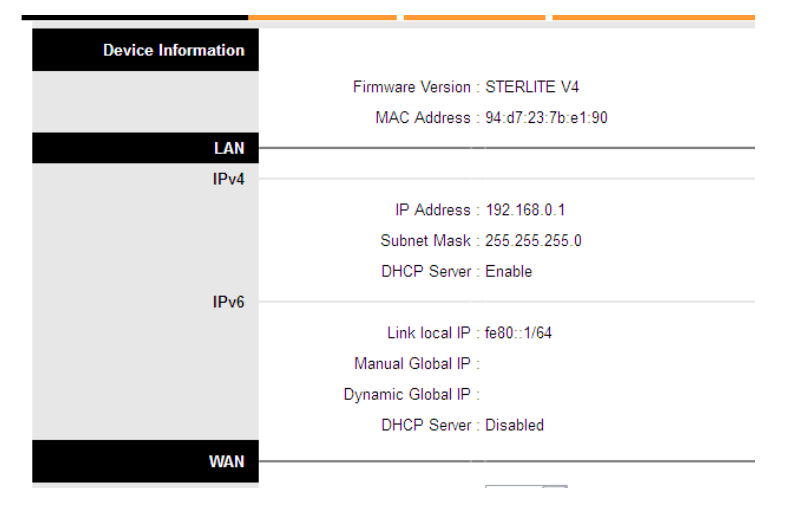
**Default Gateway . . . . . . . . . : 192.168.0.1**

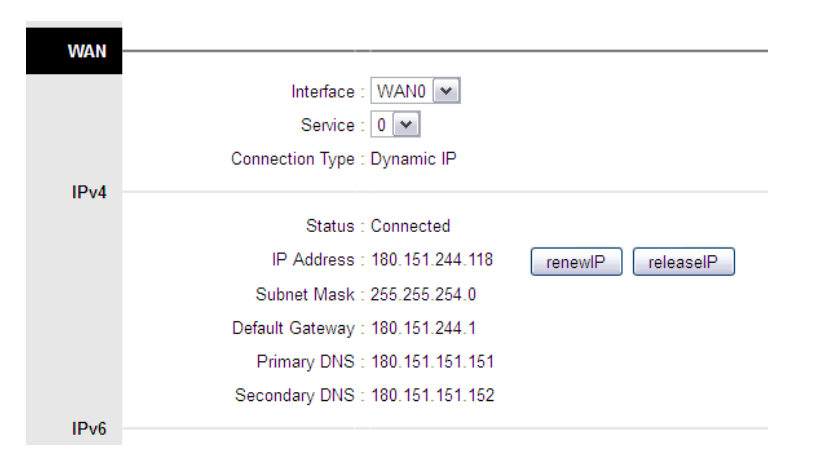
**-bash-3.2$ nslookup login.iitb.ac.in**

**Name: login.iitb.ac.in**

**Address: 103.21.126.139**

Also, these are screenshots from my WiFi router’s admin pages: (“LAN” refers to WiFi network, “WAN” refers to the side that connects to the rest of the Internet).





### Commands given at my laptop while packet capture was ongoing

**Output of this trace file is laptopSSHtoLoginIITB.pcap**

//command given at my laptop

-bash-3.2$ ssh varsha@login.iitb.ac.in -p 5022

**As soon as ssh shell opened, tcpdump\* was started on login.iitb.ac.in. Output of this trace file is loginIITB\_trace\_ssh.pcap**

(\*tcpdump is a packet capturing tool, it captures and saves all packets sent or received at a particular interface).

**Then a SECOND SSH session was started from my laptop to login.iitb.ac.in**

//my laptop

-bash-3.2$ ssh varsha@login.iitb.ac.in -p 5022

After this, both ssh sessions were closed and packet capture was stopped.

Study all the data (packet traces collected, netstat output, any other outputs provided) and answer these questions. **You can also show curiosity about any other things, ask those questions, and write those observations. Meaningful and clever observations will get credit.**

# ***Write answers in the space provided.***

1. What is the MAC address of my laptop?
2. What is the MAC address of the wireless interface of WiFi access point?
3. What do the first four packets of the laptopConnectingToWireless.pcap trace seem to be doing?
4. What is the subnet address of my home wireless network (write in a.b.c.d/x notation)?
5. My laptop is getting an IP address through DHCP. How many packets are involved in getting this address? Why does it seem to be less than the expected number of packets?
6. What is my laptop’s IP address?
7. What is the IP address of the wireless interface of the Wifi access point?
8. The access point (router) is connected to the WAN, i.e.. the “rest of the Internet” through a wired interface
   1. What is the IP address of this interface?
   2. What is the subnet number of the network that this interface connects to? (in a.b.c.d/x notation)

*Now look at the laptopSSHtoLoginIITB trace (taken on laptop) and loginIITB\_trace\_ssh trace (taken on login.iitb).*

1. What is the IP address of my laptop as seen on “login.iitb.ac.in”?
2. Where do you think the NAT is happening for my laptop’s address? Explain why you think so.
3. What is the actual port number on the laptop of the first ssh connection?
4. What is the actual port number on the laptop of the second ssh connection?
5. What must be the NAT table entry (in my ISP's NAT) corresponding to the ssh connections from my laptop? (Show both entries)
6. What is network address of the network that login.iitb is on? (a.b.c.d./x notation
   1. What is its default router address?
   2. What is the default router’s MAC address?
7. What is login.iitb.ac.in’s internal (private) IP address? What is the actual port number at which the ssh connection is made?
8. What is login.iitb's IP address & port number for the two ssh connections - AS SEEN BY my laptop?
9. What do you think is the table entry in IITB’s NAT corresponding to the two ssh connections from my laptop to login.iitb.ac.in?
10. Label the diagram on the next page with all the interface addresses that are possible to be known (write the actual addresses, not NAT translations). Some samples of how to show this are shown, you have to show this for all interfaces that can be labeled with the given data. Also, write the approximate RTTs between the hops in the space shown. You may use multiple sources of information for this purpose – which may not have been taken for the same time.
    1. Find one (or more) samples of RTT between my laptop and login.iitb.
    2. State whether you think the total RTT correlated well with the individual hop RTTs, if not why?
    3. Suppose you are forced to guess the number of hops in the “unknown” area – how many do you think there are, and what is your reasoning behind your guess?

