CS 378 Lab 06

Understanding IP addressing: Subnetting, DHCP, NAT etc.

1 September 24th, 2014

Introduction

This is a graded continuation of Lab 05. **IT IS AN INDIVIDUAL LAB. NO DISCUSSIONS.**
In your lab download tar, you have been given the following trace files:

1. laptopConnectingToWireless.pcap
2. laptopSSHtoLoginIITB.pcap
3. loginIITB_trace_ssh.pcap

In addition you have

4. tracertToLoginIITB.out (traceroute from my laptop to login.iitb.ac.in)
5. tracerouteFromLoginIITB (traceroute from login.iitb.ac.in to a certain IP address)

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 in the file:

lab06QandA.odt.
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
```

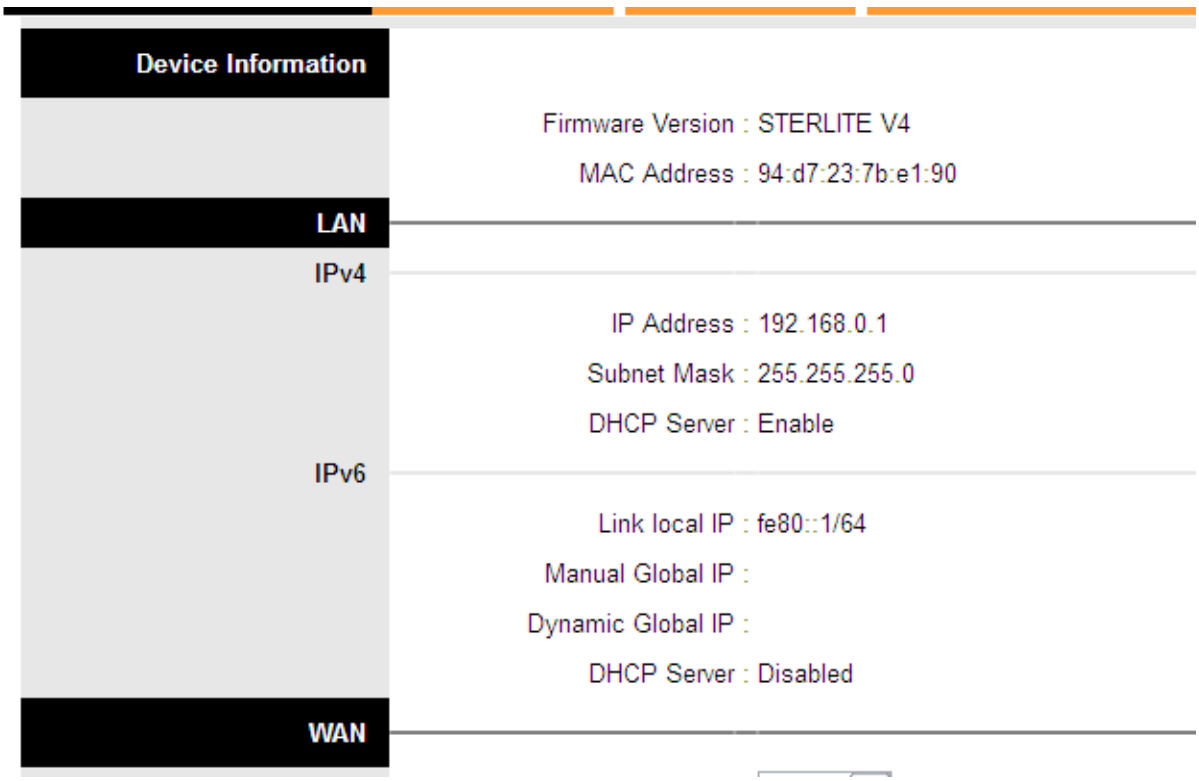
```
    192.168.0.255  255.255.255.255      192.168.0.2     192.168.0.2       25
        224.0.0.0        240.0.0.0      192.168.0.2     192.168.0.2       25
  255.255.255.255  255.255.255.255      192.168.0.2     192.168.0.2       1
  255.255.255.255  255.255.255.255      192.168.0.2           20003       1
  255.255.255.255  255.255.255.255      192.168.0.2               4       1
Default Gateway:       192.168.0.1
===========================================================================
```

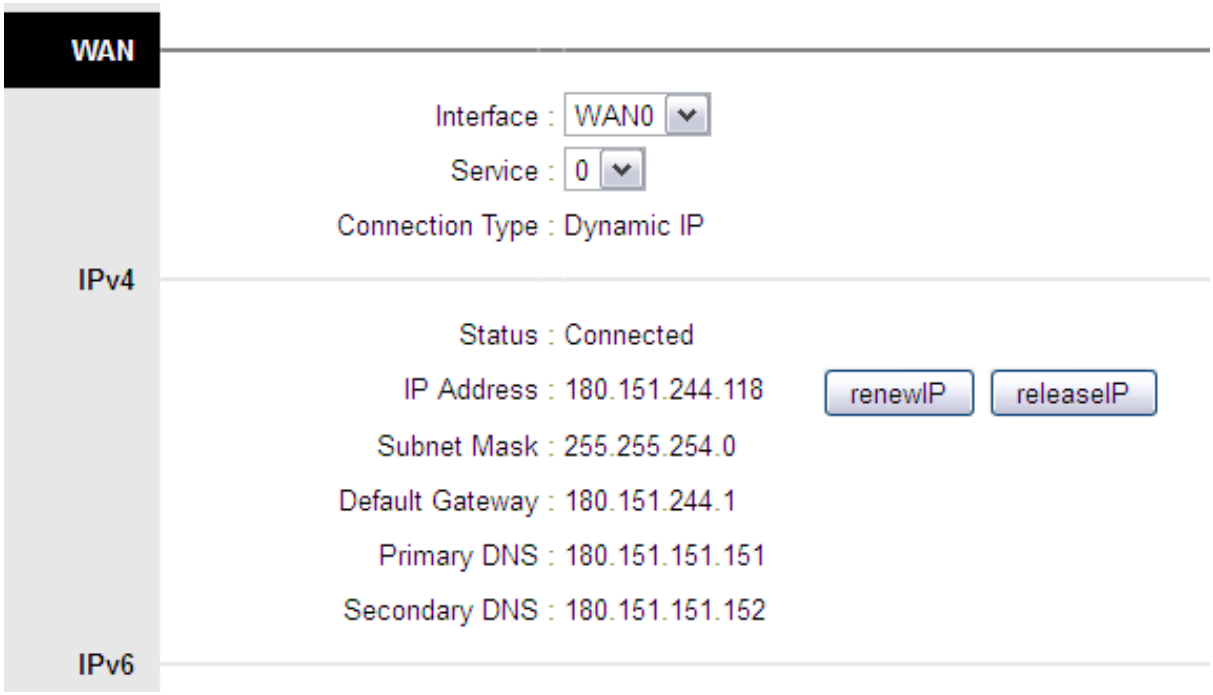
```
-bash-3.2$ ifconfig
Ethernet adapter Wireless Network Connection:

        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

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.

1. Study the trace files and the above information and make all the correlations that you can

2. Use todaysmeet.com/cs378lab06 or ask clarification questions to TAs (today's lab is grades so direct “answers” will not be provided)

3. Open lab06QandA.odt, write the answers in that file itself. **CONVERT TO PDF AND UPLOAD ON BODHITREE1**

4. Strict deadline is 5pm: Uploads after that will be penalized (penalty of: delay minutes X 1%)