Lab #9: Basic Linux Networking

Understanding Linux networks starts with understanding Linux network commands and the information they provide. We will use a number of Linux commands to analyze our network and our Linux network capabilities. View the online help (man pages) for more information on each command.

BACKGROUND INFORMATION *(Lab starts on page 3)*

ping

The **`ping`** command allows the user to test whether or not a network connection is active, the speed of that connection, and how a network behaves given specific data loads. We will use this command in its simplest form:

`ping` *`IP-address`*

When the `ping` command is finished (or you manually stop it with CTRL-C), a minimum, average, and maximum time taken to transmit and receive the request packets is calculated, as is a percentage of packets that may have been lost.

ifconfig also: ifcfg, ifup, ifdown, ethtool, nm-tool

The **`ifconfig`** command is a tool used to display and configure network interfaces. We will use this command to display information about our network interface by entering the `ifconfig` command with no options. This command will display information about the network card (typically called **`eth0`**), IP address, broadcast address, and network mask. It also shows how many packets were received and transmitted. There is also information about the *loopback* device (**`lo`**).

The loopback device is a path for your machine to network with itself. This feature is useful for testing a computer's networking capabilities without being physically connected to a network. By convention, the loopback device is given the address **`127.0.0.1`**.

On Ubuntu, the **`nmcli`** command will display a summary for each network interface. (Older versions of Ubuntu use **`nm-tool`** instead .

arp also: arping

The **`arp`** command by itself is used to view the information currently in the ARP table (Address Resolution Protocol). This table maps the IP address of machines on your network segment with their MAC address.

hostname also: domainname, dnsdomainname

The **hostname** command tells you what the hostname of your machine is set to. The hostname is determined from a number of sources, such as the **/etc/hosts** file. On Ubuntu, the **/etc/hostname** file is used to set your machine's hostname.

netstat also: route

The **netstat** command displays details about the network, including routing tables and other interface statistics. When used by itself, the `netstat` command displays a large amount of data. The information of interest to us is at the top of the list: *Active Internet Connections*. This list displays the Internet address your connected to, how you are connected to it, and how much data has been sent and received by this connection.

nslookup also: host, dig

These commands query the DNS database to determine information about network hosts. If you supply the IP address, the command gives the hostname. If you supply the hostname, the command gives you the IP address. All three commands use the **/etc/resolv.conf** file to determine the DNS server(s).

tcpdump also: iptraf, ethereal, tethereal, wireshark

This is a packet decoder that displays all traffic across the entire network due to the Ethernet card's ability to detect the incoming and outgoing transmission data (called *promiscuous* or "snoop" mode). This program is 'normally' used to analyze TCP performance.

traceroute also: tracepath

This program prints the route along which an IP packet travels from the local host to reach the destination host. It also shows each hop along the connection route from a local to remote host and gives all the intermediate routers.

Other Linux networking commands:
route, ip, ipcalc, nmap, lokkit, iptables, ...

PART A INSTRUCTIONS:

1. Read the **Lab 9 Guide** from the course web site.

2. Make sure that you are using the **L17 Open** and logged on as **Administrator**.

3. If working in L17, follow the directions in the guide to verify that the **USB 3.0 drivers** are installed on your PC.

4. Obtain an L17 USB **flash drive**.

5. Copy the files to the SSD -- **F:** drive.

6. Follow the directions in the guide to install/upgrade **Oracle VirtualBox**, including **Extensions**, if necessary.

7. **Import** the Ubuntu virtual appliance (**.ova**) file. **DO NOT FORGET** TO "Re-initialize the MAC address of all network cards".

8. **Start** the Ubuntu virtual machine.

9. **Log on** using your assigned password (to be handed out in L17; if you are not there, you can obtain it via email.)

PART B INSTRUCTIONS:

1. Click on the "Dash home" icon (closest to the top left of the screen) and type in "net" into the search box ... Network Tools should be this first application listed.

   Go through the various tabs: Devices, Ping, Netstat, Traceroute for starters.

   Answer the following questions... use LibreOffice Writer to type in or copy-and-paste your answers.

   To do a screen shot, you can type in "scr" in Dash home.

   - What does Linux call the NIC connected to the CAT5 cable?
   - What network services are active? (list the port numbers only)
   - How many hops to the Technology web server are *shown*?
   - What is the IP address of the mail exchanger for Niagara College?

     (*Hint:* look up the Mail Exchanger for one of the College domains [niagarac.on.ca or niagaracollege.ca], and then look up the Internet Address of the host that is listed.)

2. Do a Port Scan on the Windows 7 instructor station at the front of the lab (*you will be given the IP address.)*

   (If you are working on this lab in L17, make sure that the instructor PC is on and booted into L17 Open; if you are working on this lab outside of L17, use any Windows PC, find out the IP address, make sure that the Windows Firewall is OFF, and ping it.)

   What are three (3) open ports?

Part B, Procedure 2 continued...

To run a port scan from the command line, first open a Terminal window by pressing **Ctrl-Alt-T** from the desktop.

Enter a command line similar to the following (*the IP will probably be different)*:

```
sudo  nmap  -sT  192.168.2.82
```

(The `nmap` command is the port scanner; the `sudo` command is required because `nmap` requires administrator privileges.)

Leave the Terminal window open.

3. Use the **`hostname`** command to determine your hostname. Record it.

4. Use the **`ifconfig`** program to determine your IP and MAC addresses. Record them. You can use **Shift-PageUp** and **Shift-PageDown** to scroll.

5. Run **`ip a`** to display all your network interfaces. Are there the same number of entries as displayed in the previous step, or more entries? Record any additional ones their IP and MAC addresses (if applicable).

6. Run **`nmcli d show`** and record the output. What additional information is displayed over `ifconfig and ip`?

7. Use the **`arp`** command to determine if your neighbour's IP address is listed. If not, **`ping`** your neighbour's IP address and then run the **`arp`** command again. (Alternatively, you can use **`arping`**.) Does it show up now? Record your neighbour's IP and MAC addresses.

   NOTE: *If your arp table is not working, you probably forgot to reset the MAC address when you installed your Ubuntu virtual machine. Shut down, fix it, and try again.*

8. Use the **tcpdump** command to analyze network traffic. Watch the network traffic for a few minutes then summarize what you have seen.

   For example, in the Terminal window, if your Ethernet card is called **eth1**, run

   ```
   sudo tcpdump -i eth1
   ```

   (The sudo command is required because tcpdump requires administrator privileges.)

   Then, start Firefox and log on to Blackboard, for example.

   Copy or shoot one screenful of your network traffic output and paste it into your document.

9. Use the **tracepath** or **traceroute** command to find a route to various hosts on the Internet. For example,

   ```
   tracepath technology.niagarac.on.ca
   ```

   Copy or shoot your trace and paste it into your document.

10. Save your document and close LibreOffice writer. Using **ftp**, upload your document to your account on the Technology server.

    Alternately, you may install **FileZilla** from the **Ubuntu Software Center** and use it to upload.

To complete this part, upload your document to your account on the Technology server -- *you should have been already given the username and password; if not, ask.*

11. **Verify with your professor that your document has been uploaded.**

PART C INSTRUCTIONS

Set up ***two-way*** **SSH public key authentication** between your Ubuntu Linux machine and the Technology server.

Background Information

- The **ssh** and **scp** commands are useful to copy between UNIX hosts.
- By default, both will prompt you for a password each time.
- It is fairly simple to set up public key encryption between UNIX hosts (and between UNIX servers and Windows clients.)
- On each machine, run **ssh-keygen -t rsa**
  (Simply press Enter for all prompts.)
- This creates a **.ssh** directory and two key files:
  - **id_rsa** -- The private key
  - **id_rsa.pub** -- The public key
- Transfer only the public key file from each machine to the other:
  scp ~/.ssh/id_rsa.pub *host*:

  where *host* is the hostname or IP address of the other machine
- Update (or create) the authorized keys file on each machine:
  cat ~/id_rsa.pub >> ~/.ssh/authorized_keys
- SSH is very sensitive about permissions. The `cat` command may create incompatible permissions on `authorized_keys`. To fix it:

  chmod 644 ~/.ssh/authorized_keys
- On some systems, an SSH Agent is running. To notify it: **ssh-add**
- Optionally, to clean up: **rm -i ~/id_rsa.pub**
- Now **ssh** and **scp** will not prompt you for a password again.

To Log on to a Host via SSH

From a terminal window, log in to the Technology server using **ssh**. For example,

```
ssh  jblough1@192.197.62.35          (connect via Internet)
```

or

```
ssh  jblough1@192.168.2.17           (connect via CIT LAN)
```

or

```
ssh  -p  443  jblough1@192.197.62.35    (connect via Internet)
```

or

```
ssh  -p  443  jblough1@192.168.2.17     (connect via CIT LAN)
```

to log on to the Technology server, where your home directory is hosted.

NOTE: I have two SSH servers, one listening on port 22 (the standard SSH port), and the other on port 443. Hence, the **-p** switch.

To Copy Files or Directories from One Host to Another via SSH

You can use **scp** to copy a file across the network (and, like FTP and SSH, the other way, if you wish).

Examples:

1. To copy a file called "*myfile*" from my Linux PC to the Technology web server:

```
scp  -P 443  myfile  jblough1@192.168.2.17:
```

The file is copied to your home directory on Technology.

NOTE 1: *Don't forget to type in the colon (:) at the end of the line. (Otherwise,* scp *will simply make a copy of the file locally.)*

NOTE 2: *A capital* **-P** *switch is used to specify the SSH port for* **scp**, *because lowercase* **-p** *is used to preserve file permissions and timestamps when copying.*

2. To copy an entire directory called "*somedir*" (and all of its contents), and rename it at the destination (works for files, too):

```
scp -P 443 -r somedir jblough1@192.168.2.17:nameofdestdir
```

In both cases, `192.168.2.17` is the IP of the *destination* machine and `jblough1` is a user on the destination machine.

Lab Procedure for Part C

IMPORTANT! In L-17, you must be connected to the CIT network and use 192.168.2.17 as the IP address to Technology.

1. Ubuntu 16.04 Desktop normally installs only the SSH client programs. To install and enable the SSH server:

```
sudo apt-get install ssh
```

2. Run `ssh-keygen` to set up your public and private keys.

3. Run `ssh-add` to notify the **SSH Agent** software running on Ubuntu.

4. SCP your public key file to your account on the Technology web server.

5. SSH to the Technology web server and add your public key to the `authorized_keys` file there.

6. While logged in to Technology, run `ssh-keygen` there, too.

7. SCP your Technology public key file back to your Ubuntu box, using your IP address from Part A.

8. Log out of Technology and add the public key to your Ubuntu `authorized_keys` file.

9. To complete this part, ssh to Technology and then *back* to your Ubuntu box. Take a screen shot of the Terminal window showing this.

Email your screen shot to your instructor or post on Blackboard.