Linux Networking Commands and Programs

Overview

This practical session will introduce you to the fundamentals network utilities of the Linux operating system. They consist of various Linux shell commands that can be found, in some or other forms, on most networked operating systems.

To learn how to use these tools to their full extent, read the **man** page for each command. To do this, execute: **man <command>** at the shell prompt.

The Basics

To be able to use the full features of the different networking programs, it is best to run in on machines that are not within a firewall. A firewall, like the one we are using in the computer laboratory, can restrict some of the functions. Hence, we are going to run all the networking commands in the agila server. Please approach your laboratory instructor in case you don't have an agila account. Note that some of the networking programs can still be run in your laboratory computers.

ssh

This tool gives terminal access to another machine securely (i.e. you can use the machine's terminal from another location). Strong encryption is used between the intercommunicating nodes to verify identity, maintain integrity, and secure privacy. We will be using this to connect to agila in order the run our networking programs. To connect to a server with the default SSH port (22), type

```
> ssh <username>@<hostname>
```

Answer 'yes' to the question you are presented with. This tells your machine to trust the digital certificate on the destination node for this session as well as future communications. If some other node tries to pretend to be the destination you will be notified upon attempting to connect and advised not to proceed. Once this is settled, type your password when prompted.

To connect to agila from Linux, type the following in Terminal.

```
> ssh <username>@agila.upm.edu.ph
```

Let's get acquainted with the different networking tools by running them in agila.

ifconfig

ifconfig is a network interface configuration tool. It is a good source of information for the network interfaces on a computer and whether they are active or not. Execute the following command to get information about your NIC.

```
$ ifconfig
```

The Ethernet NIC (Network Interface Card) on your machine is called **eth0**. In other machines, it could be **eth1**. There is also a loopback interface called **lo**. The loopback interface is used for routing networked data to your local machine and is purely logical. The other interface is the physical NIC connected to the LAN. Here are the information that can be obtained:

- Protocol used (denoted by encap)
- IP address (denoted by inet addr)
- Broadcast address (denoted by Bcast)
- Subnet mask (denoted by Mask)
- MAC address (HWAddr)

ip

Another network interface configuration tool is ip. This is available in most Linux operating system and is the replacement for ifconfig. To list the IP addresses of the current machine, you can use either of the following:

```
$ ip a
$ ip addr
```

Since the command above displays all IP addresses, you can limit the displayed IP addresses to either IPv4 or IPv6 addresses only. To display IPv4 addresses only, use

```
$ ip -4 a
```

To display IPv6 addresses only, use

```
$ ip -6 a
```

If you want to limit the IP addresses displayed to a particular interface only, use any of the following

```
$ ip a show eth0
$ ip a list eth0
$ ip a show dev eth0
```

ping

ping is a network testing tool. It sends an echo request to a network node via an IP address, using a protocol called ICMP. If the node is present, it responds to the request. Ask your classmate for their IP address and issue the following command:

```
$ ping <IP Address>
$ ping <hostname>
```

After a while, you will see the results of the echo requests. Press Ctrl-C to stop the program about 10 lines of output. Here are the information that can be obtained:

- Average time taken for 64 bytes of data to return from the remote host
- Any ICMP packets that arrive out of sequence
- Percentage of packet loss

A host name can also be used in place of an IP address. Try pinging www.upm.edu.ph to determine the IP address of the UPM site server.

hostname

This tool is used to get and set a node in human-readable name (e.g. www.google.com).

```
$ hostname
```

What is host name of the machine where you are currently running?

host

This tool is used to query DNS servers interactively. You can use it to obtain the IP address of a given node if you have the name.

```
$ host
```

What is the IP address of berdugo.upm.edu.ph? Of vpn.upm.edu.ph?

nmap

This tool is a network exploration tool and security scanner. It can be used to determine if an IP address range contains any live nodes, what services (ports) are open, what operating system is running etc. To use nmap, simply type:

```
$ nmap <IP address>
$ nmap <hostname>
```

What are the services running on your berdugo.upm.edu.ph?

nslookup

This tool is used to query the DNS servers interactively. You can use it to obtain the name of a give node if you have the IP address. It can also be used to determine the IP address of name.

```
$ nslookup <IP address>
```

What is the name of 202.92.148.162? What is the name of the 202.92.148.168?

traceroute

This tool uses a simple algorithm to print the route packets from machine to a destination. For example, to determine the route to www.google.com, type:

```
$ traceroute www.google.com
```

The information that can be obtained are:

- The number of hops required to reach the remote host
- The address/s of routing nodes along the way

mtr

If you want to be able to continuously monitor the route to a host, you can use mtr.

```
$ mtr www.google.com
```

This prints the response percentage and response times of the route to the host. This could be used to check for bad link.

Exercises:

Connect to agila and answer the following questions. For each answer, include a screenshot and highlight the part that supports your answer. All answers is to be saved in a document file using a word processor. The document file with your answer should be converted into pdf format before uploading it to Courses.

1. How many interfaces are there in agila?
2. What protocols are being used by the interface(s)?
3. What is the IP address of the interface(s)?
4. What is the subnet mask of the interface(s)?
5. What is the MAC address of the interface(s)?

   For questions 6 – 11, use the interface that gives the maximum value for the answer.
6. How many total packets have been sent from your machine? How did you obtain this value?
7. How much total data (MB) have been sent from your machine? How did you obtain this value?
8. How many total packets have been received? How did you obtain this value?
9. How much total data (MB) have been received? How did you obtain this value?
10. How many total collisions have occurred?
11. How many packets can your NIC queue for transmission?

12. What is the average time taken for 64 bytes of data to return from www.google.com?
13. What is the IP address of sais.up.edu.ph?
14. What are the services running on timog.upm.edu.ph?
15. What is the hostname of 202.92.148.182?