Lab 01- Computer Networks Basics

Sherif Saad

January 14, 2025

Purpose

This lab aims to introduce the students to common computer networking commands and practice capturing real network traffic.

1 Lab Instructions

1.1 Unique Identifiers of End System over Network

Every host or end system could uniquely identify over the network using different identifiers.

What are the unique identifiers, and how do we find them?
The unique identifiers are Hostname, IP address, MAC address, and process socket.

We need to install the network-tools library on Linux to access many network commands and tools. To install the network-tool type and run the following command:

```
sudo apt install net-tools
```

1.1.1 Host Name

Each host or device connected to the network is associated with a unique hostname. This hostname is human-readable and unique over the same network. We can think of URI (Uniform Resource Identifier) and URL (Uniform Resource Locator) as similar to hostname on the web and over the internet. To find out your Linux machine hostname, type the following command:

```
hostname
```

or

```
hostnamectl
```

1.1.2 IP Address

The IP address (Internet Protocol) address is a numerical identifier that uniquely identifies any device connected to an Internet Protocol network. To view your machine IP address or addresses on a Linux machine, you run the following command

```
ip addr
```

The above commands will list all the network interfaces (logical/physical) and the IP address associated with each interface.

1.1.3 MAC Address

The MAC (Media Access Control) address is a numerical identifier that uniquely identifies a network interface. Each network interface has a unique MAC address (aka physical address). The MAC address exists in any network interface that uses Ethernet, WIFI, or Bluetooth technology. To show the MAC address for all attached network interfaces to your machine, use the following commands:

```
ip link
```

1.1.4 Network Socket

A socket is a logical identifier that uniquely identifies a process connected to the internet (TCP/IP) network on the same machine. The socket is a combination of an IP address and port number. To list all processes running on your machine and connected to the internet with their socket information, type the following command

```
netstat -A inet -p
```

1.2 Check Host Connectivity

We can use Ping to check connectivity between any two network devices connected to TCP/IP network. The command ping needs either the hostname or the IP address of the remote node. To test the ping command, run the following.

```
ping www.facebook.com
ping 8.8.8.8
ping 172.55.4.1
```

1.3 Finding the IP address of a Remote Host

To find the IP address of a remote host, we need the hostname or URL. Then, using the command host we can find the ip address of the host; here are a few examples:

```
host www.facebook.com
host https://www.guc.edu.eg/
host www.uvic.ca
host www.google.com
host www.notexist.ca
```

1.4 Finding the MAC addresses in Your Network

To find all the MAC addresses for all the machines/interfaces that share the same network (LAN) with your machine, use the command ARP:

```
arp -a
```

1.5 Display Routing Table

You can display or modify the machine routing table using the route command. Simply type the route as follows:

```
route
```

1.6 Query DNS record

We can query a DNS server to get a domain name, IP address mapping, or DNS records using nslookup (Name Server Lookup) command

```
nslookup https://www.uvic.ca/
```

1.7 Query Website Information

whois command is used to fetch all the information related to a website.

```
sudo apt install whois

whois uwindsor.ca
whois wasplabs.ca
```

1.8 Capturing Network Traffic With TcpDump

Another powerful network diagnosis and troubleshooting tool is tcpdump. Using tcpdump we can capture and analyze network traffic going through our network. Here we only cover the basic functions of tcpdump. To list all the available (visible) network interfaces, use the following command

```
sudo tcpdump –D
```

To start capturing network packets, type the following command:

```
sudo tcpdump -i eth0
# replace eth0  in the above by your interface name
```

Tcpdump continues to capture packets, until you stop it by pressing ***Ctrl+C***
To capture only n number of packets, you could use the count option, as follows:

```
sudo tcpdump -i eth0 -c 10
```

In the above example, tcpdump will only capture 10 packets and terminate.
TCP dump resolves the ip address to hostname and the port number to application layer protocol such as 443 to https, and 137.207.72.197 to ”https://www.guc.edu.eg/”, to show the IP address and the port number use the option -nn

```
sudo tcpdump -i eth0 -nn
```

To save packets to a file instead of displaying them on the screen, we need to use the option -w followed by the filename.

```
sudo tcpdump -i eth0 -c100 -nn –w /home/shsaad/output.pcap
```

We can also use many filtering options to filter the captured packets, such as the port number, the protocol type, the host ip address, etc

```
sudo  tcpdump -i any -nn icmp
sudo  tcpdump -i any -nn icmp or udp
sudo  tcpdump -i eth0 -nn host 147.164.8.1
suod  tcpdump -i any -nn src 192.168.0.44 and dst 8.8.8.8
```

2 Lab Questions

1. What is the difference between the commands ”hostname” and ”hostnamectl”? (Support your answer by adding a screenshot of the output of each command)

2. On your course VM, open the web browser and go to the university website `https://www.uwindsor.ca/`. Use the appropriate command(s) to find the process id for firefox and the number of ports associated with this process. (support your answer by adding a screenshot of the output of each command)

3. On your course VM execute the command ”ip addr”, explain what information this command return. For example, how many interfaces are on your VM, what are the ip addresses, and what other addresses have this command returned? (support your answer by adding a screenshot of the output of each command)

4. Write a command to capture and save 25 packets between your VM machine IP address and the university website `https://www.uwindsor.ca/`. Save the packets in a file named ”$comp8670\_lab01.pcap$”.

5. Did you test and executed successfully all the commands in the lab instruction? If your answer is yes, then simply write down ”Yes, I did” otherwise, report any command that did not work and include screenshots of error messages for the commands that did not work.