Lab 01- Computer Networks Basics

Sherif Saad

May 28, 2021

Purpose

This lab aims to introduce the students to common computer networking commands, practice capturing real network traffic, and perform basic network diagnosis operations.

1 Basic Network Commands

1.1 Unique Identifiers of End System over Network

Every host or end system could be uniquely identified 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, Network Socket.

On Linux, we need to install the network-tools library 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 interface to your machine, use the following commands:

```
ip link
```

1.1.4 Network Socket

A socket is a logical identifier that uniquely identify 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 host URL. Then, using the command host we can find the ip address of the host, here are few examples:

```
host www.facebook.com
host www.uwindsor.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/ interface that share the same network (LAN) with your machine, use the command ARP:

```
arp -a
```

1.5 Display Routing Table

Using the route command you can display or modify the machine routing table. Simply type 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 www.uwindsor.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
```

2 Basic Network Diagnosis with Traceroute

Traceroute is a command-line network diagnosis tool that we could use to perform basic diagnoses. Traceroute mainly enables you to discover the following Information:

- The route a packet takes from the source to the ultimate destination.
- The different networks and the name of the routers between on the discovered route.

- The network latency represented as the round trip time (the time taken to send and receive data to each router on the path)

Traceroute relies on IP address, ICMP (Internet Control Message Protocol), and the time to live (TTL) of IP packets. To test traceroute run the following commands:

```
# The following command will install traceroute
sudo apt install traceroute

# Now we will test traceroute
traceroute facebook.com
traceroute 8.8.8.8
traceroute msa.edu.eg
traceroute www.aast.edu
```

- How does traceroute work?
- How do we interpreted the output of traceroute?
- Any abnormal or unexpected results from the above test?

3 Capturing Network Traffic With TcpDump

Another powerful network diagnosis and troubleshooting tool is tcpdump. Using tcpdump we can capture and analyze network traffic going though our network. Here we only cover basic functions of tcpdump.
To list all the available (visible) network interface 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 then terminate. TCP dump resolve the the ip address to host name and the port number to application layer protocol such as 443 to https, and 137.207.72.197 to "www.uwindsor.ca", to show the IP address and the port number use the option -nn

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

We can also use many filtering options to filter the captured packates, 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 dst 8.8.8.8
```

We can also show the packet contents for textual application layer protocols such as HTTP or SMTP by using the ASCII option -A

```
sudo tcpdump -i eth0 -nn -A port 80
```

We can also save the catupred packates to a tcpdump file or pcap file and read the saved data from a file as follow

```
# to save packets to file mypackets.pcap
sudo tcpdump -i eth0 -nn -w mypackets.pcap

# to read packets from file mypackets.pcap
sudo tcpdump  -r mypackets.pcap

# you can also read the packets and apply filters
sudo tcpdump  -r mypackets.pcap port 80
sudo tcpdump  -r mypackets.pcap icmp
```