University of Dhaka

Department of Computer Science and Engineering

CSE-3111 : Computer Networking Lab

Lab Report 1: SELF-READING MATERIALS and PRACTICE documents related

Submitted By:

Name : Sudipto Das Sukanto

Roll No : 29

Name : Ahanaf Ahmed Shawn

Roll No : 47

Submitted On :

January 26, 2024

Submitted To :

Dr. Md. Abdur Razzaque

Dr. Md. Mamun Or Rashid

Dr. Muhammad Ibrahim

Mr. Md. Redwan Ahmed Rizvee

1 Introduction

In this first lab, we learned about some terminology and understand the working characteristic behavior of them.

1.1 Objectives

The objective of this lab is to familiarize students or participants with essential network utilities and tools. Through hands-on exploration and practical exercises, the lab aims to achieve the following objectives:

- Understanding Network Connectivity
- Tracing Network Routes
- Configuring Network Interfaces
- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP)
- Domain Name System (DNS) Queries
- Network Statistics and Connections

2 Theory

Participants in this lab interact with fundamental network utilities to obtain real-world understanding of networking concepts. In order to test connectivity and track packet routes, we use tools like ping and traceroute. We also use ifconfig to configure and display network interfaces, arp to map IP addresses to MAC addresses, rarp to resolve reverse addresses, nslookup to query DNS servers, and netstat to show network statistics.

3 Methodology

3.1 Ping

Ping determines the latency of communication between to network or device.

Ping sends echo request messages to the destination host via the Internet Control Message Protocol (ICMP) and waits for echo responses. In addition to measuring the round-trip time, the utility reports on packet loss.

```
ping <hostname or IP address>
```

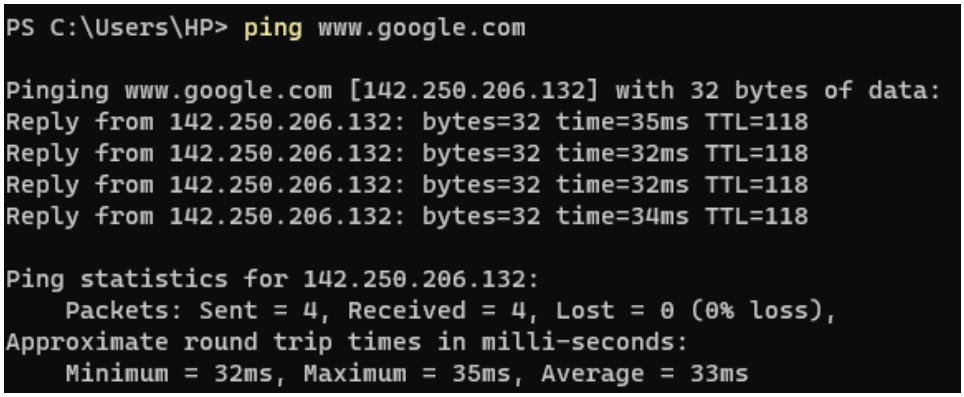

Figure 1: ping in google.com

3.2 Tracerouter

A traceroute shows the path taken by data as it moves from its source to its destination via the internet.
Traceroute is to identify and display the network hops (intermediate routers) between the source and the destination and display the taken time each hops.

Traceroute and tracert accomplish the same general function. The only significant difference is that the command is “traceroute” on Mac and Linux systems and “tracert” on a Windows system.

```
tracert <hostname or IP address>
```

Ping and traceroute differ primarily in that traceroute provides you with the exact route, router by router, along with the duration of each hop, whereas ping only indicates whether a server is reachable and the time it takes to send and receive data. I am done to tracerote two PC with each other during Lab time. For connecting to PC tracroute one PC to other PC’s IP address. After tracerouting I find one Hop by this hop two PC connecting with each other.

3.3 Ifconfig

The Unix and Unix-like operating systems, such as Linux and macOS, use the command-line network configuration tool ifconfig. ”Ifconfig” is short for

Figure 2: tracerote in google.com

"interface configuration." It enables users to set up, show, and control a system's network interfaces.

For window, we use "ipconfig". Same as "Ifconfig" .

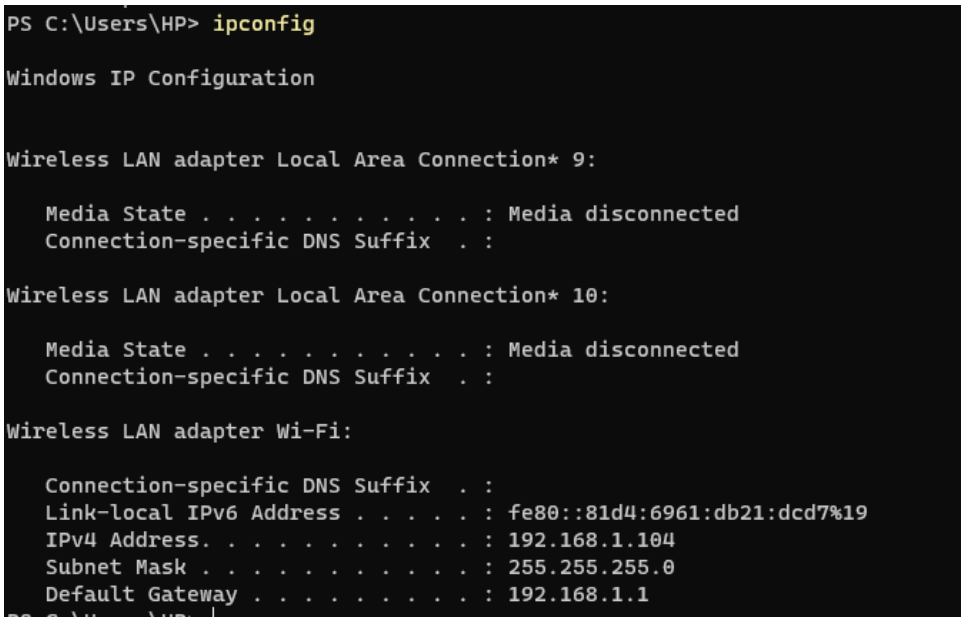

Figure 3: Interface configuration of my PC

The following ifconfig command with the -a argument will display information on all active or inactive network interfaces on the server. It displays

the results for eth0, lo, sit0, and tun0. For Windows use "ipcpnfig /all".

We can also up and down the interface by ifconfig command. I tried in the lab to up and down the lab PC interface but because of the authentication PC didn't allow to me to down or up any interface.

```
ifconfig eth0 up OR ifup eth0
```

To assign an IP address to a specific interface, use the following command with an interface name (eth0) and ip address that you want to set. For example, "ifconfig eth0 172.16.25.125" will set the IP address to interface eth0.

```
ifconfig eth0 172.16.25.125
```

```
(Those command for Linux environment)
```

3.4 ARP and RARP

ARP, or Address Resolution Protocol, is a networking protocol used to map an IP address (Layer 3) to the corresponding hardware or MAC address (Layer 2) on a local network. The primary purpose of ARP is to discover the MAC address associated with a given IP address. When a device on a local network wants to communicate with another device, it uses ARP to determine the MAC address of the destination device.

RARP, or Reverse Address Resolution Protocol, performs the opposite function of ARP. While ARP maps IP addresses to MAC addresses, RARP is used to map MAC addresses to IP addresses.

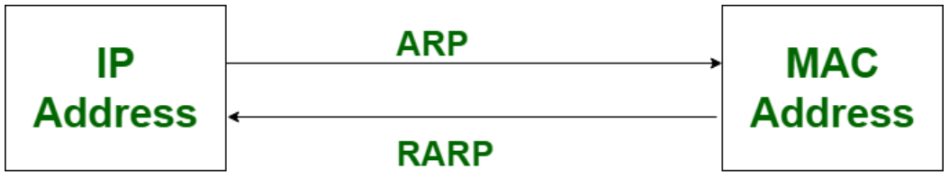

Figure 4: ARP and RARP

```
arp [-v] [-i if] [-H type] -a [hostname]
```

```
PS C:\Users\HP> arp -a

Interface: 192.168.0.103 --- 0x13
  Internet Address      Physical Address      Type
  192.168.0.1           b4-b0-24-07-f5-94     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

Figure 5: ARP and RARP

3.5 NSLOOKUP

The command-line program "nslookup," which stands for "Name Server Lookup," is used to query DNS (Domain Name System) servers in order to get IP address or domain name information. There are several operating systems that support nslookup, including Windows, Linux, and macOS. Network administrators, IT specialists, and individuals who need to investigate domain names or handle DNS-related difficulties will find it to be a useful tool.

```
nslookup [option] [hosts]
```

```
PS C:\Users\HP> nslookup google.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    google.com
Addresses:  2404:6800:4002:81d::200e
          142.250.193.238
```

Figure 6: NSLOOKUP

```
nslookup [IP Address]
```

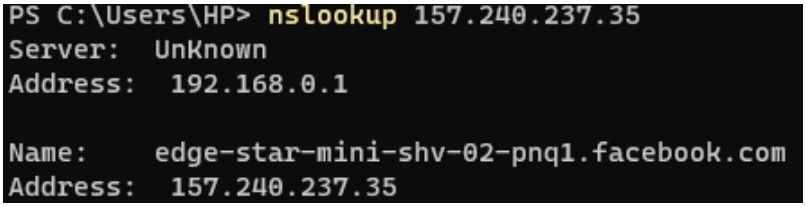

Figure 7: NSLOOKUP

3.6 `netstat` Command

The `netstat` command is a powerful utility used to display network connections, routing tables, interface statistics, masquerade connections, and much more. It provides comprehensive information about network-related activities on a system.

Basic Syntax

```
netstat [options]
```

Common Options

- `-a`: Displays all active connections and listening ports.
- `-n`: Shows numerical addresses instead of resolving hostnames.
- `-p protocol`: Displays connections for the specified protocol (e.g., `-p tcp`).
- `-r`: Displays the kernel routing table.

Examples

- Display all active connections:

  ```
  netstat -a
  ```

- Show numerical addresses and port numbers:

  ```
  netstat -n
  ```

- Display TCP connections:

```
netstat -p tcp
```

Terminal Snapshot

Some netstat command snapshots:

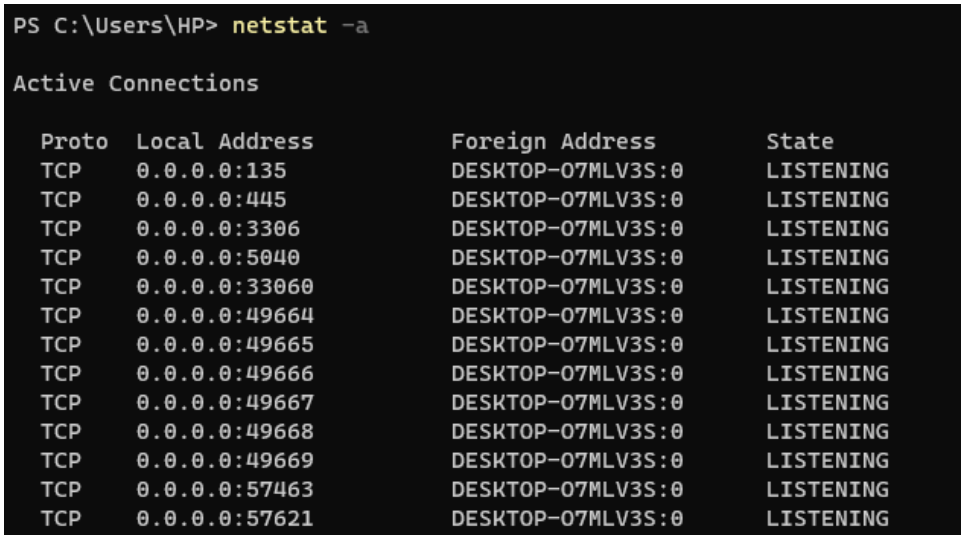

Figure 8: Netstat Command

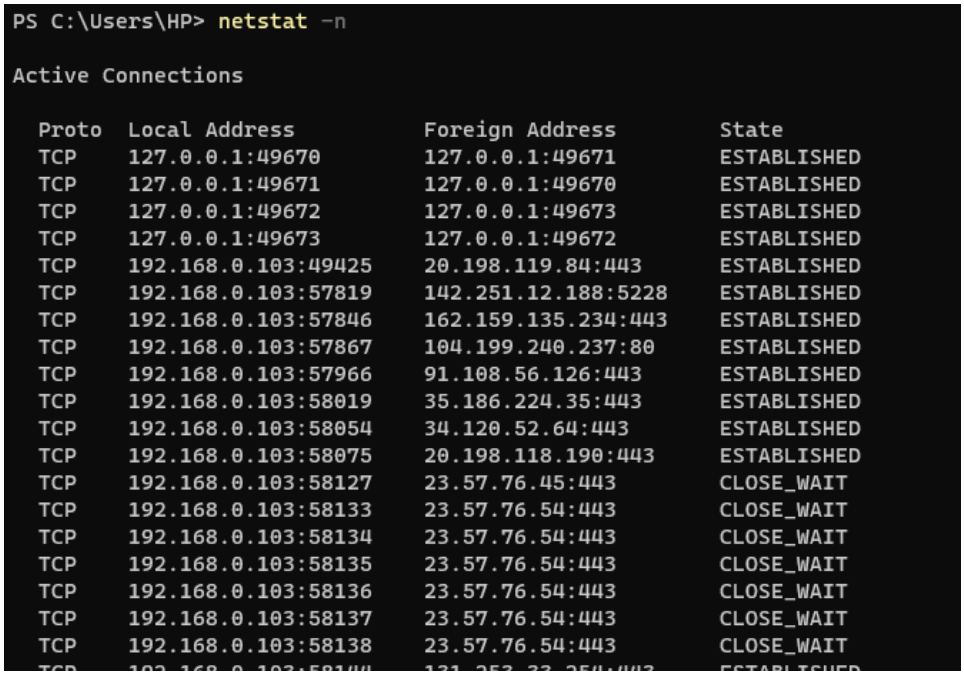

Figure 9: Netstat Command

4 Conclusion

In summary, the practical engagement with these networking commands has fortified our understanding of network troubleshooting, configuration, and information retrieval. The knowledge gained from this exploration lays a solid foundation for further studies and hands-on experiences in the dynamic field of computer networking.

References

[1] Computer networking : a top-down approach 6th ed.

[2] ping : https://pimylifeup.com/ubuntu-ping/#:~:text=Example%20of%20Limiting%20the%20Number%20of%20pings%20on%20Ubuntu&text=To%20achieve%20this%2C%20we%20use,the%20destination%20for%20our%20pings.&text=After%20running%20this%20command%2C%20your,to%20stop%20the%20process%20manually.

[3] TRACEROUTE: https://cloudinfrastructureservices.co.uk/how-to-install-traceroute-and-run-on-ubuntu-20-04/

[4] IFCONFIG: https://www.tecmint.com/ifconfig-command-examples/

[5] ARP: https://www.geeksforgeeks.org/arp-command-in-linux-with-examples/

[6] RARP: https://www.geeksforgeeks.org/what-is-rarp/

[7] NSLOOKUP: https://www.geeksforgeeks.org/nslookup-command-in-linux-with-examples/