University of Dhaka

Department of Computer Science and Engineering

CSE-3111 : Computer Networking Lab

Lab Report 1 : LAN Configuration and Troubleshooting Tools

Submitted By:

Name : Md. Imran Shorif Shuvo

Roll No : SH-56

Submitted On :

January 21, 2024

Submitted To :

Dr. Md. Abdur Razzaque

Dr. Md Mamunur Rashid

Dr. Md. Ibrahim

Mr. Md. Redwan Ahmed Rizvee

1 Introduction

The lab's main goal is to familiarize with some troubleshooting tools (Ping, Traceroute, ARP, Static Routing, Netstat, Ifconfig, nslookup, whois, etc.) and learn how to utilize them in computer networks.

1.1 Objectives

Write down two or three specific objectives of this lab experiment.

- To demonstrate LAN configuration and troubleshooting skills using a range of tools and methods for different LANs, such as Ethernet and Wi-Fi networks.

- To check the competency in using tools like ping, traceroute, network analyzers, and network monitoring tools to find and diagnose network problems.

2 Theory

A group of connected devices that may communicate with one another across a wired or wireless network is known as a local area network (LAN). LANs connect computers, servers, printers, and other devices within a limited geographic region, such as a home, business, or building. Configuring a LAN involves setting up the network infrastructure, which consists of routers, switches, and access points, as well as configuring the network settings on each connected device.

This includes assigning IP addresses, subnet masks, and default gateways to each device as well as configuring security settings to protect the network from unauthorized access. Locating and resolving any potential connectivity or performance issues are part of troubleshooting a LAN.

These techniques and technologies could entail checking the network configuration, looking at network activity, and finding and resolving network device conflicts.

The general objective of the LAN setup and troubleshooting tools lab report is to demonstrate the ability to build, manage, and troubleshoot a LAN as well as to succinctly and clearly document the lab procedures and results.

3 Methodology

3.1 PING

Ping is a command-line program used to test the network connectivity of two devices. It sends an Internet Control Message Protocol (ICMP) echo request packet to a specific host and then waits for an ICMP echo reply packet. A measurement and report of the packet's round-trip time from source to destination and return are subsequently given to the user.

The syntax for the ping command is normally "ping [hostname/IP address]." Four ICMP echo request packets will be sent by Ping at first, and it will continue to do so until the user cancels the instruction. The user can also specify the number of packets to send and the size of the packets by using the -c and -s parameters.

3.2 TRACEROUTE

Traceroute is a command-line program that is used to display the path that a packet follows from its origin to its destination. It functions by sending a series of ICMP echo request packets with a Time-to-Live (TTL) value that is rising. As each packet travels the network path, routers along the way reduce the TTL value. When the TTL value reaches zero, the router notifies the source that "time exceeded" has occurred. Traceroute uses these messages to ascertain the path that the packets took.

Traceroute is also used to identify routing issues such as network congestion or improperly setup routers. Additionally, it can be used to pinpoint a host's location and calculate how long it takes a packet to travel from its origin to its destination.

Traceroute commands often have the syntax "traceroute [hostname/IP address]." Traceroute can optionally use TCP or UDP in addition to the ICMP echo request packets it uses by default. Most OS including Windows, Linux, and macOS, support it.

3.3 IFCONFIG

On Unix-like operating systems like Linux, network interface configuration is done using the command-line tool ifconfig, which stands for "interface configuration." It can be used to change a device's IP addresses, subnet masks, and other network settings. Using ifconfig, you may view the current status of your network interfaces, including their IP address, netmask, and MAC address.

The basic syntax for ifconfig is "ifconfig [interface] [options]," where "interface" denotes the name of the network interface you desire to configure (for instance, "eth0" for the initial Ethernet interface) and "options" denotes the specific parameters you wish to employ.

For instance, you might type "ifconfig eth0" to see the "eth0" interface's current state. If you want to give the "eth0" interface an IP address, type "ifconfig eth0 192.168.1.10 netmask 255.255.255.0" on your computer's command line.

Additionally, we can use ifconfig to monitor interface statistics, assign a new MAC address to an interface, and bring up or down an interface. Other alternatives include:

- up: bring an interface up
- down: bring an interface down
- hw ether xx:xx:xx:xx:xx:xx: set the MAC address
- -a : display all interfaces, active and inactive

ifconfig is a powerful tool that can be used to configure network interfaces. However, it is not recommended to use it on modern systems because it's being deprecated in favor of iproute2, a more modern and versatile tool.

3.4 ARP

The communication method known as ARP, or Address Resolution Protocol, converts a network address, such as an IP address, into a physical (MAC) address on a local network. When the host's network layer address is the only one accessible, the hardware address of the host is determined using this address. The mapping of an IP address to a corresponding MAC address enables hosts on a network to communicate with one another. ARP runs in the Data Link Layer of the OSI Model.

3.5 RARP

Reverse Address Resolution Protocol is known as RARP. When a host's physical (MAC) address is known, it is utilized to ascertain the IP address of the host. Similar to ARP, it operates at the OSI Model's Data Link Layer.

3.6 NSLOOKUP

NSLOOKUP is an abbreviation for Name Server Lookup. It is a command-line tool for investigating DNS-related problems. It is used to query DNS servers in order to obtain details regarding host addresses, mail servers, and other domain name-related data. It can be used to discover a website's IP address, a domain's mail server, or other DNS details. When an email is not delivered or a website won't load, DNS-related problems can be identified using the results of an NSLOOKUP query. On Windows command prompts and Linux/macOS terminals, we can run NSLOOKUP. It enables us to look up data on a certain domain name or IP address by contacting a specific DNS server.

3.7 NETSTAT

Network Statistics is referred to as NETSTAT. It is a command-line tool used to show details about a computer's network connections. It can be used to check whether ports are open, the state of a connection, and the process that is currently utilizing a given connection. The routing table and the status of the IP, TCP, UDP, and ICMP protocols can also be seen using NETSTAT.

Both Windows' command prompt and Linux's/macOS' terminal allows to execute NETSTAT. You can display particular information using the NETSTAT command's many options, including:

-a : Shows all active connections and the ports they are using -b : Shows the executable involved in creating each connection or listening port -n : Displays addresses and port numbers in numerical form -o : Shows the owning process ID associated with each connection -r: Displays the routing table

NETSTAT can be a helpful tool for resolving network-related problems, such as figuring out what's causing a spike in network usage or locating open ports that could be dangerous.

We will see links to some files that the server provided. If we click any of them we can download them in our pc.

4 Experimental result

Some Snapshots of the troubleshooting tools are given below:

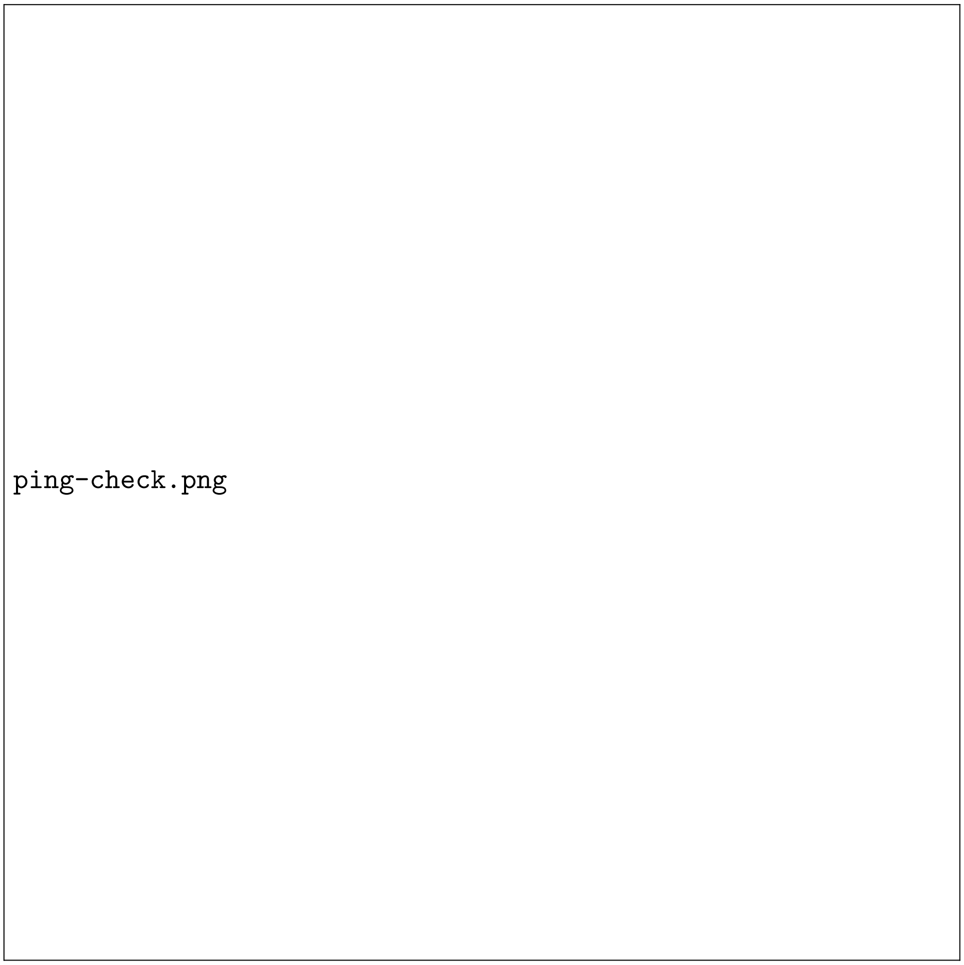

Figure 1: Use of ping command

new-ss-traceroute-check.png

Figure 2: Use of traceroute command

ss4-define-num-of-probes.png

Figure 3: Use of traceroute -N command [Defining the number of probes]

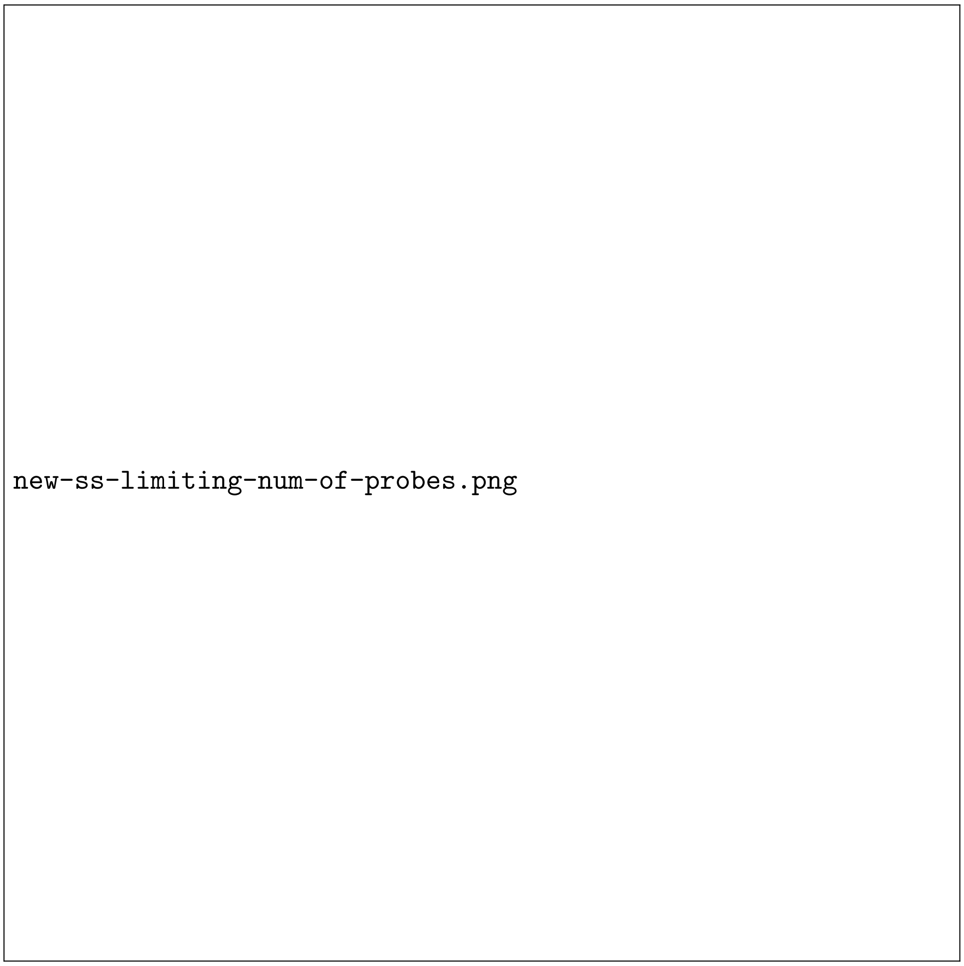

Figure 4: Use of traceroute -m command [Limiting the number of hops]

new-ss11-ifconfig-all-settings.png

Figure 5: Use of ifconfig command

ss14-enable-or-disable-network-interface.png

Figure 6: Enable or disable connection using ifconfig enp3s0 up/down command

ss18-change-all-address.png

Figure 7: Changing all address with ifconfig

ss20-enable-promisc-mode.png

ss21-disable-promisc-mode.png

ss22-add-new-alias.png

ss23-remove-alias.png

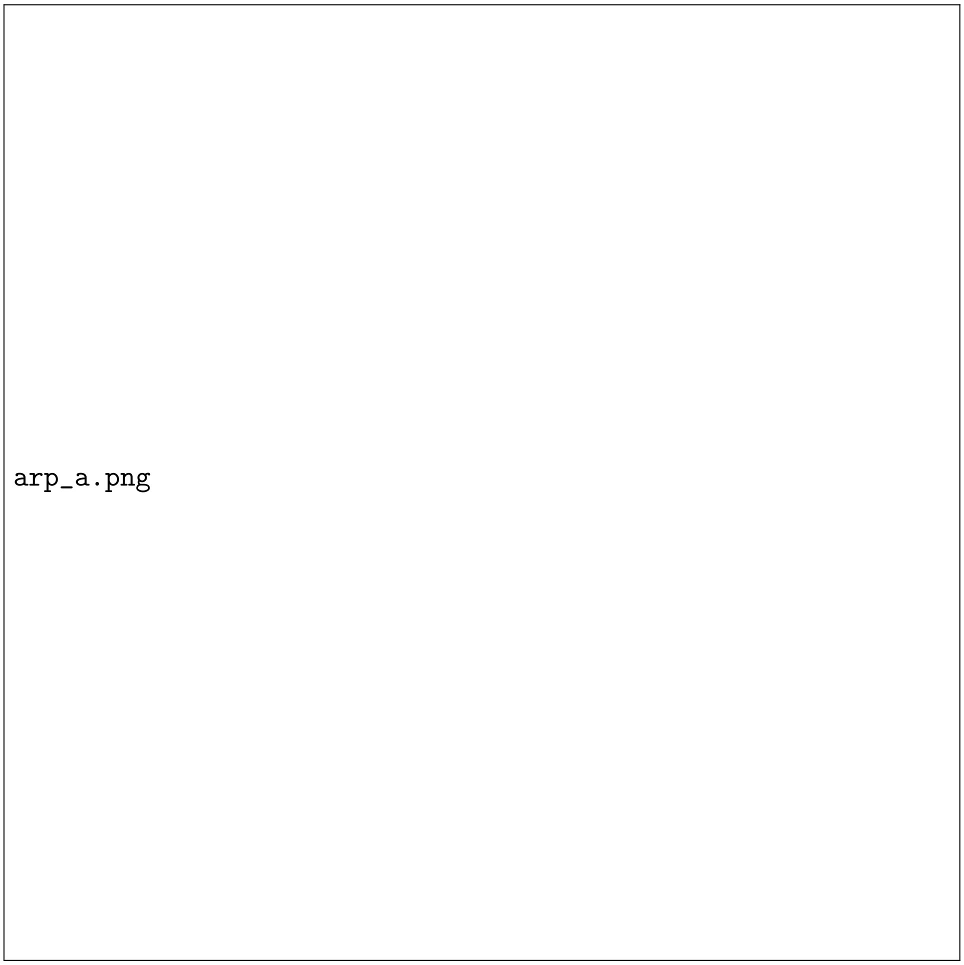

Figure 10: Use of arp -a command

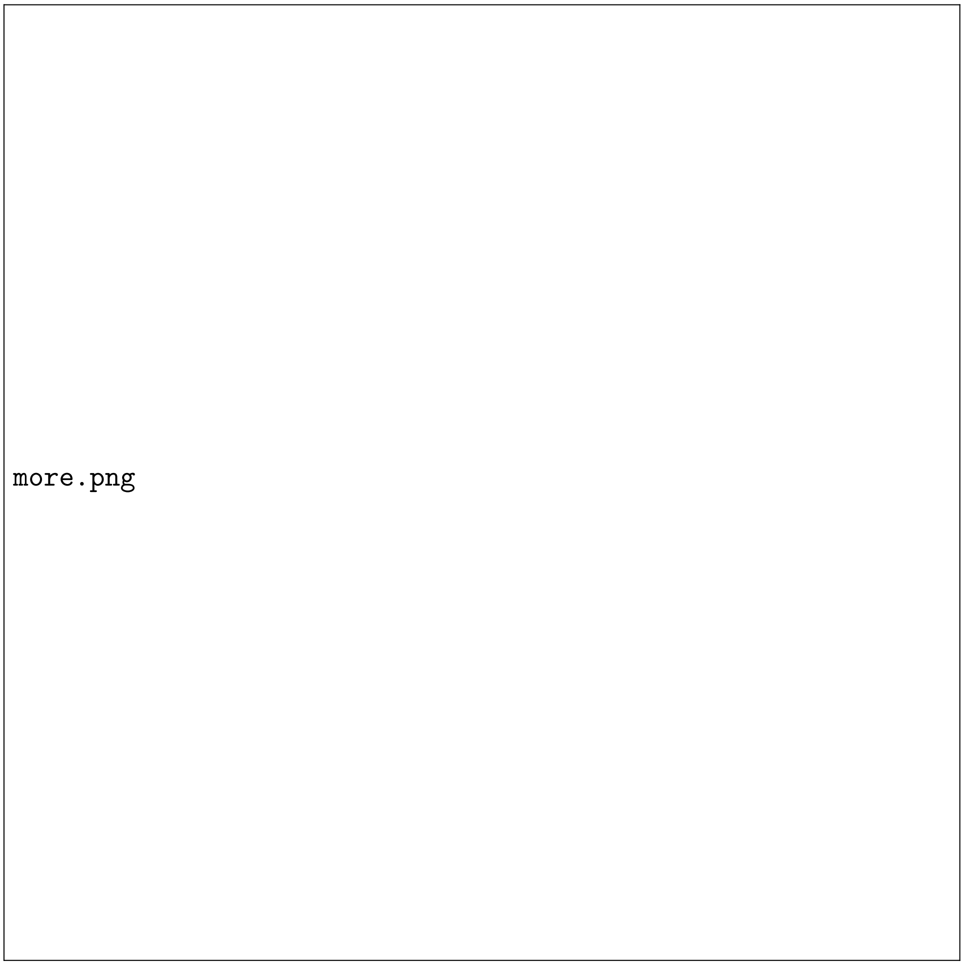

Figure 11: Use of more command

Figure 12: Use of nslookup command

netstat_a.png

Figure 13: Use of netstat -a command

netstat_st.png

Figure 14: Use of netstat -st command

netstat_su.png

Figure 15: Use of netstat -su command