University of Dhaka

Department of Computer Science and Engineering

CSE-3111 : Computer Networking Lab

Lab Report 1 : Lab exercises on LAN configuration and troubleshooting tools

Submitted By:

Name : Zisan Mahmud

Roll No : 23

Name : Abdullah Al Mahmud

Roll No : 15

Submitted On:

January 25, 2024

Submitted To:

Dr. Md. Abdur Razzaque

Dr. Md Mamunur Rashid

Dr. Muhammad Ibrahim

Mr. Md. Redwan Ahmed Rizvee

1 Introduction

In this lab, the main goal is to become acquainted with essential network troubleshooting tools such as PING, TRACEROUTE, IFCONFIG, ARP, RARP, NSLOOKUP, NETSTAT.Proficiency in utilizing these tools is crucial for network administrators to effectively manage and troubleshoot network issues.

2 Objectives

- This lab evaluates the ability to use tools like ping, traceroute, network analyzers, and monitoring tools for identifying and diagnosing network problems.
- This lab equips us with the skills needed for effective network administration, fostering competence in managing and troubleshooting LAN networks.
- This lab also introduces us to deeper concepts of data communication, package routing, LAN, Ethernet, and Wi-Fi configurations.

3 Theory

A Local Area Network or simply LAN constitutes a network of interconnected devices within a limited geographic region,facilitating communication via either wired or wireless connections. This network encompasses computers, servers, printers, and other devices, all of which necessitate systematic configuration for optimal functionality. The LAN infrastructure involves essential components such as routers, switches, and access points. Individual device settings, including IP addresses, subnet masks, and default gateways, are configured to establish seamless communication.Integral to the LAN setup and troubleshooting process is the utilization of terminal commands that empower administrators to diagnose and resolve connectivity issues. The following commands play a crucial role in this endeavor:

ping:

`ping` is employed to assess the reachability of a target device within the network. It sends packets to the target and reports the round-trip time, aiding in identifying potential communication problems.

traceroute:
`traceroute` reveals the path taken by data packets between the source and destination devices. It helps identify potential bottlenecks or issues along the route.

ifconfig:
`ifconfig` provides information about the network interfaces of a device, allowing administrators to review and configure settings such as IP addresses, subnet masks, and interface status.

arp and rarp:
`arp` resolves IP addresses to MAC addresses, while `rarp` performs the reverse, resolving MAC addresses to IP addresses. These commands are valuable for addressing issues related to address resolution.

nslookup:
`nslookup` is employed to query DNS servers for information about domain names and IP addresses, aiding in the resolution of domain-related issues.

netstat:
`netstat` provides a snapshot of a device's network connections, routing tables, and interface statistics. This command is instrumental in identifying active connections and potential issues affecting network performance.

In summary, the LAN setup and troubleshooting tools aims to showcase proficiency in employing these terminal commands. The documentation should articulate the methodologies applied, highlight the results obtained through these commands, and provide a comprehensive overview of the troubleshooting process.

4 Methodology

4.1 PING

ping:
The `ping` command is a fundamental network diagnostic tool used to assess the reachability and responsiveness of a target device within a network. It operates by sending a series of small data packets, known as "echo requests," to the target device and measuring the time it takes for the device to send back corresponding "echo replies."

Syntax: `ping [options] destination`

Usage:

- `ping example.com` - Sends ICMP echo requests to the specified domain or IP address.
- `ping -c 4 example.com` - Sends only 4 packets for the test.

Functionality:

1. **Assessing Reachability:** `ping` helps verify whether a target device is reachable over the network. A successful ping indicates that the target device is responsive and can be reached.

2. **Round-Trip Time (RTT):** `ping` measures the Round-Trip Time (RTT), which is the time taken for an echo request to travel from the source device to the target device and back. This provides insights into the latency or delay in the network.

3. **Packet Loss:** `ping` also reports on packet loss, indicating the percentage of sent packets that did not receive a reply. High packet loss can signify network congestion or connectivity issues.

Options:

`-c count:` Specifies the number of echo requests to send.
`-i interval:` Sets the time interval between sending echo requests.
`-s packetsize:` Defines the size of the data packets to send.
`-t timeout:` Sets the maximum time to wait for an echo reply.

Use Cases:

1. **Basic Connectivity Check:** `ping` is commonly used to verify the basic connectivity between devices, such as checking if a computer can communicate with a server.

2. **Troubleshooting Network Issues:** When experiencing network connectivity problems, administrators often use `ping` to diagnose issues such as high latency, packet loss, or unresponsive devices.

3. **Monitoring Network Stability:** System administrators use `ping` in network monitoring tools to continuously assess the stability and performance of network connections over time.

4.2 TRACEROUTE

traceroute:
The `traceroute` command is a network diagnostic tool used to visualize and analyze the route that data packets take from the source device to a target destination across a network. It helps identify the intermediary devices (routers) along the path and measure the time it takes for packets to traverse each hop.

Syntax: `traceroute [options] destination`

Usage:

- `traceroute example.com` - Traces the route to the specified domain or IP address.
- `traceroute -m 20 example.com` - Limits the maximum number of hops to 20.

Functionality:

1. **Visualizing Network Route:** `traceroute` displays a list of routers (hops) through which data packets traverse from the source to the destination. It helps identify the path taken by packets across the network.

2. **Measuring Hop Delays:** The tool measures the time it takes for an individual packet to travel from the source to each intermediary router, providing insights into the latency at each hop.

Options:

`-m max_hops:` Specifies the maximum number of hops to search for the target.
`-n:` Skips DNS resolution for faster results.
`-w waittime:` Defines the maximum time to wait for a response at each hop.
`-d`: Trace path without resolving each hop ip address.
`-N`: Define number of probes.

Use Cases:

1. **Network Path Analysis:** `traceroute` is used to analyze the path taken by data packets, providing a visual representation of network routes.

2. **Diagnosing Latency Issues:** Network administrators utilize `traceroute` to identify and troubleshoot latency problems at specific hops along the route.
3. **Determining Network Congestion:** By observing delays and packet loss at certain hops, administrators can infer potential network congestion points.

4.3 IFCONFIG

ifconfig:
The `ifconfig` command, short for "interface configuration," is a powerful network utility used to view and configure network interfaces on a Unix or Unix-like operating system. It provides information about the current state of network interfaces and allows administrators to modify their configuration settings.

Syntax: `ifconfig [interface] [options]`

Usage:

- `ifconfig` - Displays information for all active network interfaces.
- `ifconfig eth0 up` - Brings up the specified network interface.

Functionality:
1. **Displaying Interface Information:** `ifconfig` without any options provides a comprehensive overview of all active network interfaces, including IP addresses, MAC addresses, and operational status.
2. **Activating/Deactivating Interfaces:** The command can be used to bring up or down specific network interfaces, controlling their operational state.
3. **Configuring IP Addresses:** Administrators can use `ifconfig` to assign or change the IP address, subnet mask, and other parameters of a network interface.

Options:
`up:` Activates the specified network interface.
`down:` Deactivates the specified network interface.
`inet addr:` Specifies the IPv4 address for the interface.
`netmask:` Sets the subnet mask for the interface.
`hw ether:` Assigns a specific MAC address to the interface.

Use Cases:
1. **Interface Configuration:** `ifconfig` is commonly used to configure the network interfaces on a system, including assigning IP addresses and activating or deactivating interfaces.
2. **Troubleshooting Connectivity:** Administrators leverage `ifconfig` to diagnose and troubleshoot network connectivity issues by inspecting the status and configuration of network interfaces.
3. **Monitoring Network Traffic:** The command provides real-time information about network interfaces, enabling administrators to monitor network traffic and identify potential issues.

4.4 ARP

arp:
The `arp` command, standing for "Address Resolution Protocol," is used to display and manipulate the mapping between IP addresses and MAC addresses on a local network. It is instrumental in resolving IP addresses to their corresponding hardware addresses.

Syntax: `arp [options] [hostname]`

Usage:

- `arp -a` - Displays the ARP cache, listing the IP and MAC addresses of devices on the local network.
- `arp -d 192.168.1.1` - Deletes the ARP cache entry for the specified IP address.

Functionality:
1. **IP to MAC Resolution:** `arp` is used to map and display the IP address to MAC address resolution table, which is crucial for local network communication.
2. **ARP Cache Management:** Administrators can view, add, or remove entries from the ARP cache to control the IP-to-MAC address mappings.

Options:
`-a`: Displays the ARP cache.
`-d address`: Deletes a specific entry in the ARP cache.
`-s address MAC`: Adds a static ARP cache entry.

Use Cases:
1. **Network Troubleshooting:** `arp` is used to troubleshoot network issues by inspecting and managing ARP cache entries.
2. **MAC Address Discovery:** The command is employed to discover the MAC addresses of devices on the local network.

4.5 RARP

rarp:
The `rarp` command, or "Reverse Address Resolution Protocol," is a network protocol used to map a MAC address to an IP address. It is primarily used in legacy systems and diskless workstations.

Syntax: `rarp [options] [hardware_address]`

Usage:

- `rarp -a` - Displays the RARP table, listing MAC addresses and corresponding IP addresses.

Functionality:
1. **MAC to IP Resolution:** `rarp` is used to map and display the MAC address to IP address resolution table, allowing systems to obtain their IP addresses.

Options:
`-a`: Displays the RARP table.

Use Cases:
1. **Legacy System Support:** `rarp` is utilized in environments with diskless workstations that require IP address assignment based on MAC addresses.

4.6 NSLOOKUP

nslookup:
The `nslookup` command is a network tool used to query Domain Name System (DNS) servers to obtain information about domain names, IP addresses, and other DNS records.

Syntax: `nslookup [options] [hostname]`

Usage:

- `nslookup example.com` - Queries DNS for information about the specified domain.
- `nslookup 192.168.1.1` - Resolves the IP address to a domain name.

Functionality:
1. **Domain Name Resolution:** `nslookup` is used to translate domain names to IP addresses and vice versa.
2. **Querying DNS Records:** Administrators can use the command to query various DNS records, such as MX, CNAME, and NS records.

Options:
`-type=record_type:` Specifies the type of DNS record to query.

Use Cases:
1. **DNS Troubleshooting:** `nslookup` is employed to troubleshoot DNS-related issues by querying DNS records.
2. **IP Address Resolution:** The command is used to resolve IP addresses to domain names.

4.7 NETSTAT

netstat:
The `netstat` command is a network utility that provides information about network connections, routing tables, interface statistics, masquerade connections, and multicast memberships on a Unix-like operating system.

Syntax: `netstat [options]`

Usage:

- `netstat -a` - Displays all active connections and listening ports.
- `netstat -r` - Shows the routing table.
- `netstat -i` - Get List of Network Interfaces.

- `netstat -s` - List Statistics for All Ports.

Functionality:

1. **Connection Information:** `netstat` provides details about active network connections, including local and remote addresses, protocols, and connection states.

2. **Routing Table Display:** The command displays the routing table, showing the paths that network packets take.

Options:

`-a`: Displays all connections and listening ports.
`-r`: Shows the routing table.
`-i`: Displays a list of network interfaces.

Use Cases:

1. **Monitoring Network Connections:** `netstat` is used to monitor active network connections and identify potential issues.
2. **Routing Table Analysis:** The command is employed to analyze the routing table and diagnose routing-related problems.

5 Experimental Result

Some snapshots of the troubleshooting tools usage are given below:

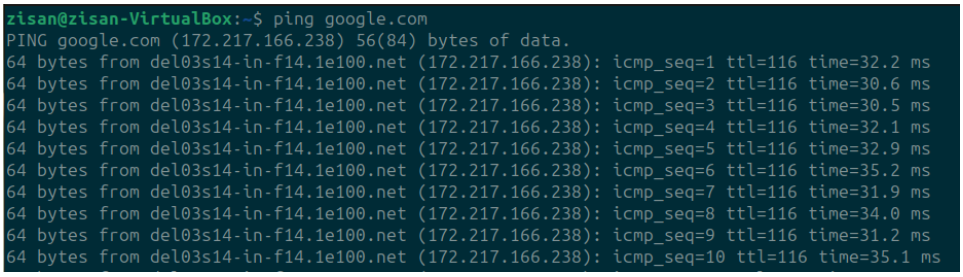

Figure 1: use of ping

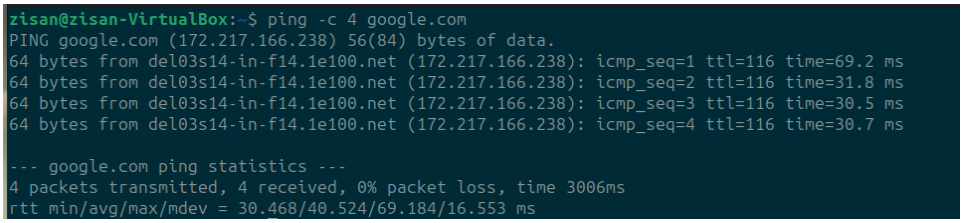

Figure 2: use of ping

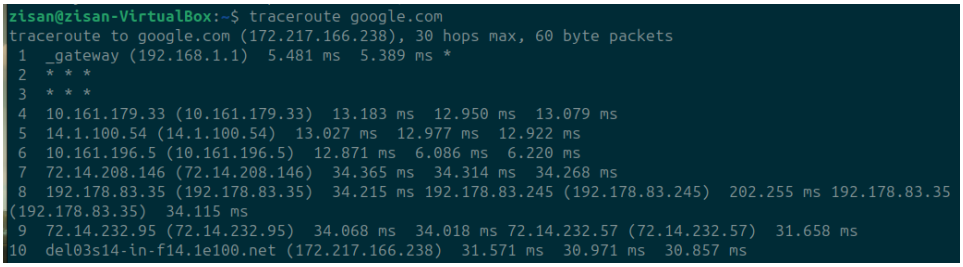

Figure 3: use of traceroute

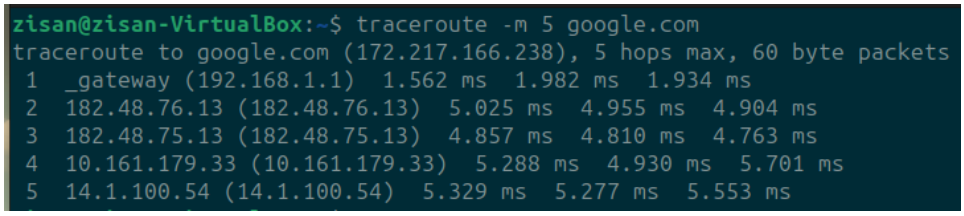

Figure 4: use of traceroute -m command to limit maximum number of hops

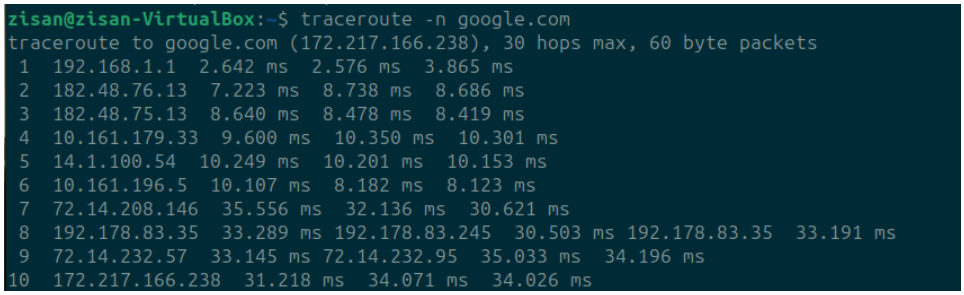

Figure 5: use of traceroute -n [Skips DNS resolution]

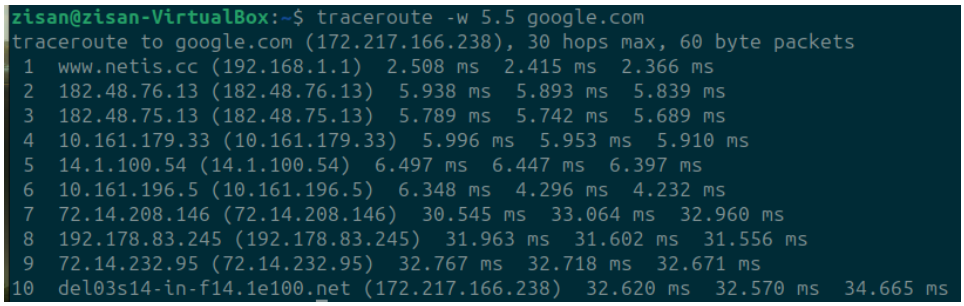

Figure 6: use of traceroute -w

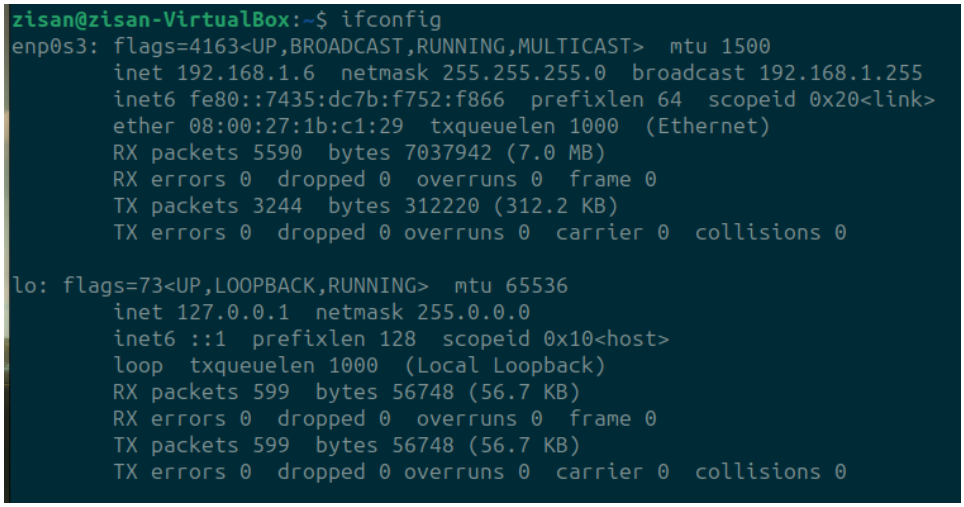

Figure 7: use of ifconfig

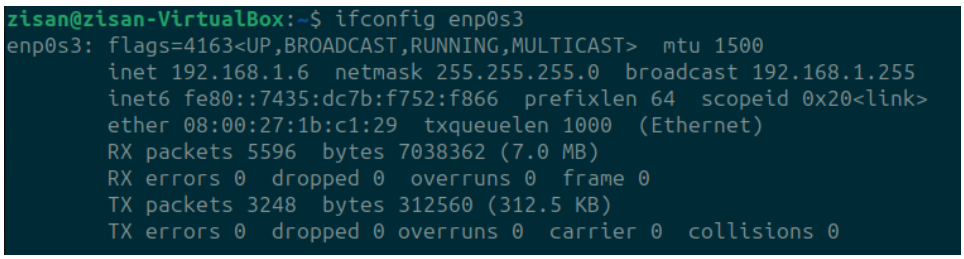

Figure 8: ifconfig with specific network interface

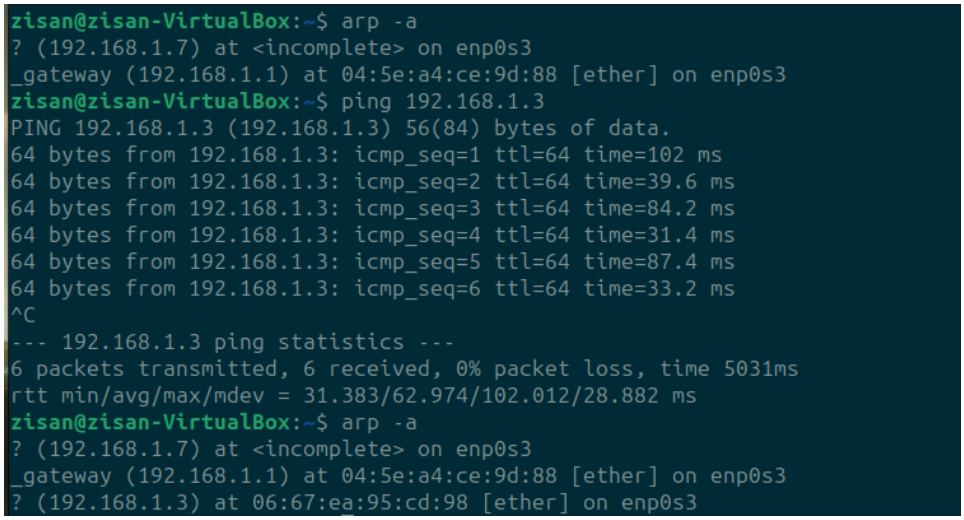

Figure 9: use of ARP command

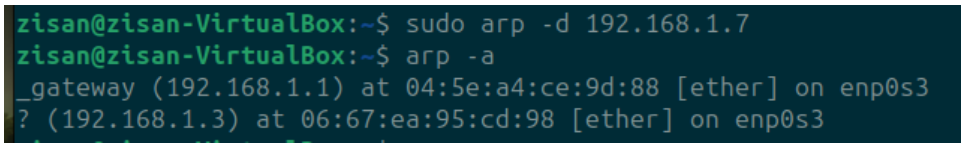

Figure 10: deleting ARP cache with specific ip

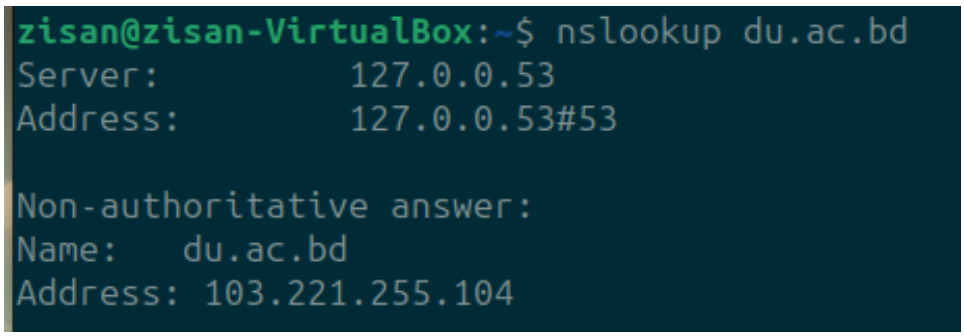

Figure 11: use of nslookup coomand tool

```
zisan@zisan-VirtualBox:~$ nslookup 127.0.0.53
53.0.0.127.in-addr.arpa name = localhost.
```

Figure 12: reverse DNS lookup using nslookup

```
zisan@zisan-VirtualBox:~$ nslookup -type=any du.ac.bd
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
du.ac.bd
        origin = dns1.du.ac.bd
        mail addr = hostmaster.du.ac.bd
        serial = 617
        refresh = 10800
        retry = 1800
        expire = 604800
        minimum = 86400
du.ac.bd        text = "google-gws-recovery-domain-verification=44766890"
du.ac.bd        text = "v=spf1 include:_spf.google.com ~all"
du.ac.bd        mail exchanger = 10 aspmx.l.google.com.
du.ac.bd        mail exchanger = 20 alt1.aspmx.l.google.com.
du.ac.bd        mail exchanger = 30 aspmx4.googlemail.com.
du.ac.bd        mail exchanger = 20 alt2.aspmx.l.google.com.
du.ac.bd        mail exchanger = 30 aspmx3.googlemail.com.
du.ac.bd        mail exchanger = 30 aspmx2.googlemail.com.
du.ac.bd        mail exchanger = 30 aspmx5.googlemail.com.
Name:   du.ac.bd
Address: 103.221.255.104
du.ac.bd        nameserver = dns1.du.ac.bd.
du.ac.bd        nameserver = dns2.du.ac.bd.

Authoritative answers can be found from:
```

Figure 13: Lookup for any record using nslookup

```
zisan@zisan-VirtualBox:~$ nslookup -type=record_type google.com
unknown query type: record_type
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 172.217.166.238
Name:   google.com
Address: 2404:6800:4002:80a::200e
```

Figure 14: `nslookup type=record_type`

```
zisan@zisan-VirtualBox:~$ netstat -a
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN
tcp        0      0 localhost:ipp           0.0.0.0:*               LISTEN
tcp6       0      0 ip6-localhost:ipp       [::]:*                  LISTEN
udp        0      0 0.0.0.0:58481           0.0.0.0:*
udp        0      0 0.0.0.0:mdns            0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 localhost:domain        0.0.0.0:*
udp        0      0 zisan-VirtualBox:bootpc _gateway:bootps         ESTABLISHED
udp6       0      0 [::]:mdns               [::]:*
udp6       0      0 [::]:52135              [::]:*
raw6       0      0 [::]:ipv6-icmp          [::]:*                  7
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  3      [ ]         STREAM     CONNECTED     28026    /run/user/1000/at-spi/bus
unix  3      [ ]         STREAM     CONNECTED     18096    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     28652    /run/user/1000/at-spi/bus
unix  3      [ ]         STREAM     CONNECTED     29881
unix  3      [ ]         STREAM     CONNECTED     28333    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     27922    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     24525
unix  3      [ ]         STREAM     CONNECTED     24411
unix  3      [ ]         STREAM     CONNECTED     22305
unix  2      [ ACC ]     STREAM     LISTENING     20701    /run/irqbalance/irqbalance643.sock
unix  3      [ ]         STREAM     CONNECTED     26046    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     25744
unix  3      [ ]         STREAM     CONNECTED     20891
unix  2      [ ]         DGRAM      CONNECTED     19196
```

Figure 15: use of netstat

```
zisan@zisan-VirtualBox:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp0s3
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
```

Figure 16: use of netstat -r [Get Kernel Routing Information]

```
zisan@zisan-VirtualBox:~$ netstat -i
Kernel Interface table
Iface             MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3           1500   129758      0      0 0          4131      0      0      0 BMPRU
lo              65536      927      0      0 0           927      0      0      0 LRU
```

Figure 17: use of netstat -i [Provide details about each interface's activity]

```
zisan@zisan-VirtualBox:~$ netstat -s
Ip:
    Forwarding: 2
    6518 total packets received
    0 forwarded
    0 incoming packets discarded
    6228 incoming packets delivered
    4870 requests sent out
Icmp:
    309 ICMP messages received
    11 input ICMP message failed
    ICMP input histogram:
        destination unreachable: 52
        timeout in transit: 176
        echo replies: 81
    124 ICMP messages sent
    0 ICMP messages failed
    ICMP output histogram:
        destination unreachable: 8
        echo requests: 116
IcmpMsg:
        InType0: 81
        InType3: 52
        InType11: 176
        OutType3: 8
        OutType8: 116
Tcp:
    62 active connection openings
    1 passive connection openings
```

Figure 18: netstat -i provides statistical information for all ports, offering insights into network activity.

6 Experience

1. We have learned how network troubleshooting tools work.
2. Used different tools to understand the network configuration and gained experience.
3. Get familiar with ip address, mac address.
4. Assigned IP addresses, subnet masks, and default gateways to devices.
5. Recorded troubleshooting steps and outcomes for future reference.

7 Reference

1. https://pimylifeup.com/ubuntu-ping
2. https://cloudinfrastructureservices.co.uk/how-to-install-traceroute-and-run-on-ubuntu-20-04/
3. https://www.tecmint.com/ifconfig-command-examples/
4. https://www.geeksforgeeks.org/arp-command-in-linux-with-examples/
5. https://www.geeksforgeeks.org/what-is-rarp/
6. https://www.geeksforgeeks.org/nslookup-command-in-linux-with-examples/
7. https://www.geeksforgeeks.org/netstat-command-linux/