CS 315 – COMPUTER NETWORKS

ASSIGNMENT – 1

210010012

TASK - 1

1. The ping command is used to test the reachability of a network host (in this case, www.google.com) by sending out echo request packets and waiting for the corresponding echo reply packets. The output typically includes information about the round-trip time (RTT) it takes for the packets to travel to the destination and back, as well as any packet loss.If the host is reachable and responsive, you will see a series of lines indicating successful pings along with the round-trip time. If there are issues with connectivity, the output may show failed attempts or display error messages indicating the nature of the problem (such as unreachable host or timeout).

2. The output of traceroute typically includes a list of IP addresses or domain names representing the routers or intermediate devices along the path. You'll also see round-trip times for each hop, which can give you an idea of the network latency between your computer and the destination. If the destination is unreachable or there are network issues, you may see asterisks (*) or timeout messages.

3. The Address Resolution Protocol (ARP) is a network protocol used to map a 32-bit IP address to the physical hardware address (MAC address) in a local network. It plays a crucial role in the communication between devices on a local area network (LAN). The ARP protocol is used when a device wants to communicate with another device on the same network. If the destination device's IP address is known, but its MAC address is not, the sending device will use ARP to discover the MAC address associated with the given IP address.

4. The ifconfig command is used to configure and display information about network interfaces on Unix and Unix-like operating systems. It allows users to view, configure, and manage network interface parameters such as IP addresses, netmasks, broadcast addresses, hardware addresses (MAC addresses), and more.

5. The hostname command is used to display or set the hostname of a system. The hostname is a label assigned to a device on a network and is used to identify it in various network communications. Additionally, the hostname is often used internally by the operating system for system identification.

6.

1) /etc/hostname:

This file typically contains the hostname of the system. The hostname is the label assigned to the machine on a network. Changes made to this file can affect the system's hostname, but it might not persist across reboots on some systems. In some Linux distributions, this file may store the hostname directly.

2)/etc/hosts:

The /etc/hosts file is used for hostname-to-IP address mapping. It allows the system to map hostnames to their corresponding IP addresses without relying on DNS (Domain Name System). This file is often used for local network configuration and can be manually edited to add custom host entries.

3)/etc/resolv.conf:

The /etc/resolv.conf file contains information about the DNS (Domain Name System) name servers and search domains. It is used by the system's resolver library to determine where to send DNS queries. This file is crucial for translating human-readable domain names to IP addresses.

4)/etc/protocols:

The /etc/protocols file lists the known protocols used in the Internet Protocol suite. It associates protocol names with their corresponding protocol numbers. This file helps applications and services identify and use specific protocols.

5)/etc/services:

The /etc/services file is a list of well-known port assignments. It associates service names with their corresponding port numbers. Applications and services use this file to determine the port numbers associated with specific services, enabling communication over a network.

TASK – 2

1.

(I) Hostname:

To find the hostname of your machine, you can use the following command in the terminal or command prompt

rahul@rahul-ubuntu:~/Desktop$ hostname

rahul-ubuntu

(II) IP Address:

To find the IP address of your machine, you can use the following command (on Linux) to display network interface information:

rahul@rahul-ubuntu:~/Desktop$ ifconfig

enp3s0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500

ether 04:42:1a:02:43:cf txqueuelen 1000 (Ethernet)

RX packets 0 bytes 0 (0.0 B)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 0 bytes 0 (0.0 B)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536

inet 127.0.0.1 netmask 255.0.0.0

inet6 ::1 prefixlen 128 scopeid 0x10<host>

loop txqueuelen 1000 (Local Loopback)

RX packets 3099 bytes 295326 (295.3 KB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 3099 bytes 295326 (295.3 KB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 10.196.12.136 netmask 255.255.0.0 broadcast 10.196.255.255

inet6 fe80::61dc:e2e7:40c0:2b9f prefixlen 64 scopeid 0x20<link>

ether 48:e7:da:0d:70:4d txqueuelen 1000 (Ethernet)

RX packets 1729212 bytes 398164094 (398.1 MB)

RX errors 0 dropped 9111 overruns 0 frame 0

TX packets 79036 bytes 10372782 (10.3 MB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

2. Task-2:

(i) To retrieve the hostname (e.g., `manikantaksn-Inspiron-14-5410`) and the IP address (e.g., `10.196.181.60`), execute the following commands:

- Hostname: `$ hostname`
- IP address: `$ ip addr` (Check the `inet` address in the wireless connection.)

(ii) For the next hop router:

- Next hop router’s IP address: `10.196.3.250`

- Next hop router’s MAC address: `02-04-96-9a-82-e8`

Obtain this information by running:

- `$ traceroute [followed by a domain name]`, e.g., `$ traceroute www.amazon.in`.

- `$ arp [IP address]` to fetch the corresponding MAC address from the ARP table.

(iii) The local DNS server's IP address is `127.0.0.53`. Retrieve it with the command:

- `$ cat /etc/resolv.conf`

(iv) In the file `/etc/protocols`, the numbers signify protocol numbers. These values identify the protocol in the layer above IP to which the data should be passed. Each entry includes the official protocol name, protocol number, and aliases.

(v) Service ports information:

- SSH (Secure Shell) - Port: `22/tcp`. Run: `$ grep ssh /etc/services`.

- FTP (File Transfer Protocol) - Port: `21/tcp`. Run: `$ grep ftp /etc/services`.

- NFS (Network File System) - Port: `2049/tcp, 2049/udp`. Run: `$ grep nfs /etc/services`.

- SMTP (email) - Port: `25/tcp`. Run: `$ grep smtp /etc/services`.

(vi) For an Android/iOS phone:

- Hostname and IP Address: Accessible in the "About Phone" section or "Status Information" in settings.

- DNS Server's IP Address: Obtain by navigating to WiFi settings and changing IP settings from DHCP to Static.

3. You can check the DNS server configuration in the /etc/resolv.conf file:

rahul@rahul-ubuntu:~/Desktop$ cat /etc/resolv.conf

This is /run/systemd/resolve/stub-resolv.conf managed by man:systemd-resolved(8).

Do not edit.

#

This file might be symlinked as /etc/resolv.conf. If you're looking at

/etc/resolv.conf and seeing this text, you have followed the symlink.

#

This is a dynamic resolv.conf file for connecting local clients to the

```
# internal DNS stub resolver of systemd-resolved. This file lists all
# configured search domains.
#
# Run "resolvectl status" to see details about the uplink DNS servers
# currently in use.
#
# Third party programs should typically not access this file directly, but only
# through the symlink at /etc/resolv.conf. To manage man:resolv.conf(5) in a
# different way, replace this symlink by a static file or a different symlink.
#
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search .
```

4. The /etc/protocols file in Unix-like operating systems contains a list of protocol names and their associated protocol numbers. Each line in the file represents a protocol entry, and the entries follow a specific format. The format generally consists of three fields:

1)Protocol Name:

The first field represents the human-readable name of the protocol (e.g., "tcp" for Transmission Control Protocol).

2)Protocol Number:

The second field is a numerical value assigned to the protocol. This number uniquely identifies the protocol in network communications.

3)Aliases:

The third field may contain aliases or alternative names for the protocol.

5. The port numbers associated with specific applications are standardized and defined by the Internet Assigned Numbers Authority (IANA). Here are the port numbers for the mentioned applications:

1)SSH (Secure Shell): Port Number: 22

SSH is a secure protocol used for remote access to systems and secure file transfer.

2)FTP (File Transfer Protocol): Port Number: 21

FTP is a standard network protocol used for transferring files between a client and a server on a computer network.

3)NFS (Network File System): Port Numbers: 2049 (TCP and UDP)

NFS is a distributed file system protocol that allows clients to access and share files over a network.

4)SMTP (Simple Mail Transfer Protocol): Port Number: 25

SMTP is a protocol used for sending email messages between servers.

The information above is based on the standard port assignments defined by IANA. You can find this information in various ways:

i) Documentation: The IANA maintains a list of registered ports on their website. You can check the Service Name and Transport Protocol Port Number Registry for the most up-to-date information.

ii) Command-Line Tools: On Unix-like systems, you can use the grep command to search the /etc/services file for specific application names and their associated port numbers:

rahul@rahul-ubuntu:~/Desktop$ grep "ssh\|ftp\|nfs\|smtp" /etc/services

```
ftp-data        20/tcp
ftp             21/tcp
ssh             22/tcp                  # SSH Remote Login Protocol
smtp            25/tcp          mail
tftp            69/udp
submissions     465/tcp         ssmtp smtps urd # Submission over TLS [RFC8314]
ftps-data       989/tcp                 # FTP over SSL (data)
ftps            990/tcp
nfs             2049/tcp                # Network File System
nfs             2049/udp                # Network File System
venus-se        2431/udp                # udp sftp side effect
codasrv-se      2433/udp                # udp sftp side effect
```

gsiftp	2811/tcp	
zope-ftp	8021/tcp	# zope management by ftp

6.

1. Hostname and IP Address:

- On both Android and iOS, you can find the device's IP address in the Wi-Fi or network settings. The hostname may not be directly accessible or set by the user in these environments.

2. Next Hop Router's IP Address and MAC Address:

- Similar to hostname and IP address, finding the next hop router's information is not a direct capability of the mobile device. The device relies on the network infrastructure, and access to router information may not be provided through standard user interfaces.

3. Local DNS Server's IP Address:

- Mobile devices typically obtain DNS server information automatically from the network they are connected to. You can check the DNS settings in the Wi-Fi or network settings, but accessing specific DNS server details might not be available without additional tools.

4. /etc/protocols File:

- Android and iOS do not expose the `/etc/protocols` file directly to users. These systems are designed to abstract lower-level networking details from regular users.

5. Port Numbers for Applications:

- The default port numbers for common applications (SSH, FTP, NFS, SMTP) are typically consistent across different platforms. However, accessing detailed networking information, such as port assignments, might require specialized apps or tools. For example, network utility apps on both Android and iOS can provide insights into open ports and network connections.

TASK - 3

1.(a) Explain the Results of the Ping:

1. www.amazon.in:

- The ping to www.amazon.in was successful. All 11 packets were transmitted and received without any packet loss.

- The round-trip time (RTT) values are displayed for each packet, indicating the time it took for the packet to travel from the source to the destination and back.

- The average RTT is calculated as the average of these values.

2. www.iitb.ac.in:

- The ping to www.iitb.ac.in was not successful. Out of 21 packets transmitted, none were received, resulting in 100% packet loss.

- This suggests that there is a network issue or the destination server (www.iitb.ac.in) may be unreachable or not responding to ICMP echo requests.

(b) Reasons for RTT Values:

- www.amazon.in:

- The RTT values represent the time it takes for the ICMP echo request packets to travel from the source to the destination (Amazon's server) and back.

- The variations in RTT can be influenced by network congestion, routing decisions, and the responsiveness of the destination server.

- Lower RTT values generally indicate a responsive and well-performing network.

- www.iitb.ac.in:

- Since all packets were lost, there is no information available about RTT for www.iitb.ac.in.

- The 100% packet loss suggests that either the destination server is not reachable or it is configured not to respond to ICMP echo requests (ping).

- Possible reasons for this could include network issues, firewall configurations, or the server not being available.

2.

rahul@rahul-ubuntu:~/Desktop$ traceroute www.amazon.in

traceroute to d1elgm1ww0d6wo.cloudfront.net (52.84.11.190), 64 hops max

1 10.196.3.250 20.733ms 2.838ms 5.604ms

2 10.240.0.1 3.155ms 3.227ms 3.542ms

3 10.240.240.1 7.609ms 4.079ms *

4 117.205.73.161 3.952ms 4.271ms 2.593ms

5 117.216.207.218 17.450ms 13.467ms 15.799ms

6 117.216.207.219 19.001ms 10.375ms 10.525ms

7 * * *

8 * * *

9 * * *

10 * * *

11 * * *

12 * * 117.216.207.122 21.056ms

13 99.83.116.180 38.608ms 26.262ms 22.864ms

14 52.93.19.120 38.082ms 50.028ms 33.155ms

15 52.93.19.83 27.880ms 46.780ms 24.867ms

16 * * *

17 150.222.219.92 24.517ms 22.850ms 22.652ms

18 15.230.133.13 32.696ms 31.657ms 49.201ms

19 * * *

20 * * *

21 * * *

22 * * *

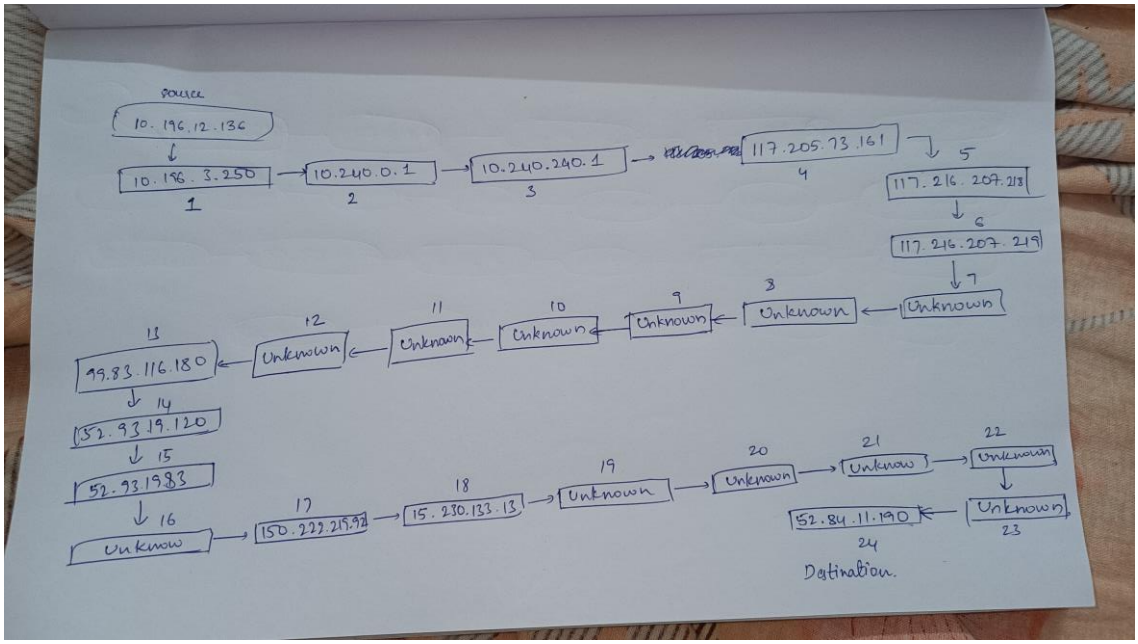
23 * * *

24 52.84.11.190 29.548ms 54.391ms 22.992ms

(a) Explanation and Network Map:

The traceroute output shows the route taken from your machine to the destination (www.amazon.in) and the response times at each hop.

Here's a simplified network map:



Each arrow represents a hop, and the IP addresses shown in the traceroute output correspond to the routers at each hop.

(b) Changing Maximum Hop Number:

The maximum hop number is the number of hops or routers that traceroute will attempt to trace before stopping.

You can change the maximum hop number using the -m or --max-hops option. For example, to set the maximum hop number to 30:

traceroute -m 30 www.amazon.in

(c) Timestamps in Traceroute:

The three timestamps in the traceroute output represent the time taken for three separate ICMP echo requests (ping) to travel from the source to the destination and back.

They indicate the round-trip time (RTT) for each packet at a particular hop.

(d) Use of TTL (Time To Live) Field in ICMP Packets:

The TTL field in ICMP packets is used to limit the lifespan or the number of hops a packet can traverse.

Each router along the path decrements the TTL value by 1. If the TTL reaches 0, the router discards the packet and sends an ICMP Time Exceeded message back to the source.

Traceroute utilizes this mechanism by sending packets with increasing TTL values. As the TTL increases, the packets are allowed to traverse more hops, revealing the path to the destination.

The TTL field is crucial for preventing packets from circulating indefinitely in the network and ensures that they eventually reach their destination or are discarded after a certain number of hops.