Text

Description automatically generated

|  |  |
| --- | --- |
| Student Name | Saurabh P Khodke |
| SRN No | 202200497 |
| Roll No | 33 |
| Program | Btech. Computer Eng. |
| Year | Third Year |
| Division | B |
| Subject | Computer Network Laboratory (BTECCE22506) |
| Assignment No | Two |

Assignment Number - 02

**Title :** Study of Linux and Windows Network commands

**Problem Statement** Studying Linux and Windows network commands. [ ping, pathping, ipconfig/ifconfig, arp, netstat, nbtstat, nslookup, route, traceroute/tracert, nmap, etc]

**Try to execute following commands on linux terminal or Windows command prompt.**

* + **Ipconfig / ifconfig**
  + **ping**
  + **Tracert/Traceroute/Tracepath**
  + **Finger**
  + **NSlookup**
  + **Netstat**
  + **Hostname**
  + **Port Scan / nmap**
  + **Arp Route**
  + **Whois**

**Theory :**

**1. ipconfig / ifconfig**

Purpose: These commands are used to view and configure the network interfaces on a system.

ipconfig (Windows):

Displays all current TCP/IP network configuration values.

Common options include:

/all: Provides detailed information about each network adapter.

/release and /renew: Release and renew the IP address assigned to the network adapter.

Example: ipconfig /all displays detailed IP configuration information.

ifconfig (Linux/Unix):

Displays or configures a network interface.

Common options include:

ifconfig eth0: Displays information about the eth0 network interface.

ifconfig eth0 up/down: Enables or disables the eth0 interface.

It has largely been replaced by the ip command in modern Linux distributions.

**2. ping**

Purpose: The ping command tests the connectivity between two devices on a network by sending ICMP Echo Request messages and waiting for a response.

Theory: Ping helps in checking if a host is reachable and measuring the round-trip time for messages sent from the originating host to a destination computer.

Example: ping google.com sends a series of packets to Google's server to check connectivity.

**3. tracert / traceroute / tracepath**

Purpose: These commands are used to trace the route packets take from one device to another across an IP network.

tracert (Windows):

Displays the path data packets take to reach a specific destination.

Lists each hop (router) along the path, showing the time taken for each hop.

traceroute (Linux/Unix):

Performs a similar function to tracert, but with additional options for customizing packet behavior.

tracepath (Linux/Unix):

A simplified version of traceroute, with less detail but easier to use without requiring root privileges.

Theory: Helps in diagnosing network routing issues and identifying where packets are delayed or dropped.

**4. finger**

Purpose: The finger command displays information about users on a system, such as their real name, login name, terminal name, idle time, and office location.

Theory: Commonly used in UNIX/Linux environments to check user information on a remote or local system.

Example: finger username shows detailed information about the specified user.

**5. nslookup**

Purpose: The nslookup command queries the Domain Name System (DNS) to obtain domain name or IP address mapping.

Theory: Useful for diagnosing DNS problems or obtaining information about a domain, such as its IP address or mail server.

Example: nslookup google.com returns the IP address associated with Google's domain.

**6. netstat**

Purpose: netstat displays network connections (both incoming and outgoing), routing tables, interface statistics, masquerade connections, and multicast memberships.

Theory: It's a powerful tool for network troubleshooting and monitoring, showing active connections and listening ports.

Example: netstat -an displays all active connections and listening ports with numeric addresses.

**7. hostname**

Purpose: The hostname command displays or sets the system's host name.

Theory: The host name is a unique name assigned to a machine within a network, used to identify the device over a network.

Example: hostname displays the current host name; hostname newname sets a new host name.

**8. Port Scan / nmap**

Purpose: Port scanning is the process of probing a server or host for open ports using a tool like nmap.

nmap:

nmap (Network Mapper) is a powerful network scanning tool used to discover hosts and services on a network.

Can identify open ports, running services, and detect the operating system of a device.

Theory: Port scanning helps in network security by identifying potential entry points for unauthorized access.

Example: nmap -sS 192.168.1.1 performs a stealth scan on the IP address 192.168.1.1.

**9. arp / route**

**arp:**

Purpose: The arp command is used to view and manipulate the ARP (Address Resolution Protocol) cache, which maps IP addresses to MAC addresses.

Theory: ARP is a protocol used to find the physical address of a device associated with an IP address in a local network.

Example: arp -a displays the current ARP cache.

**route:**

Purpose: The route command displays or modifies the IP routing table.

Theory: The routing table contains rules that determine where data packets should be directed based on their destination IP addresses.

Example: route -n displays the routing table with numeric IP addresses.

**10. whois**

Purpose: The whois command queries databases that store domain registration information, providing details about the domain's ownership, registration dates, and contact information.

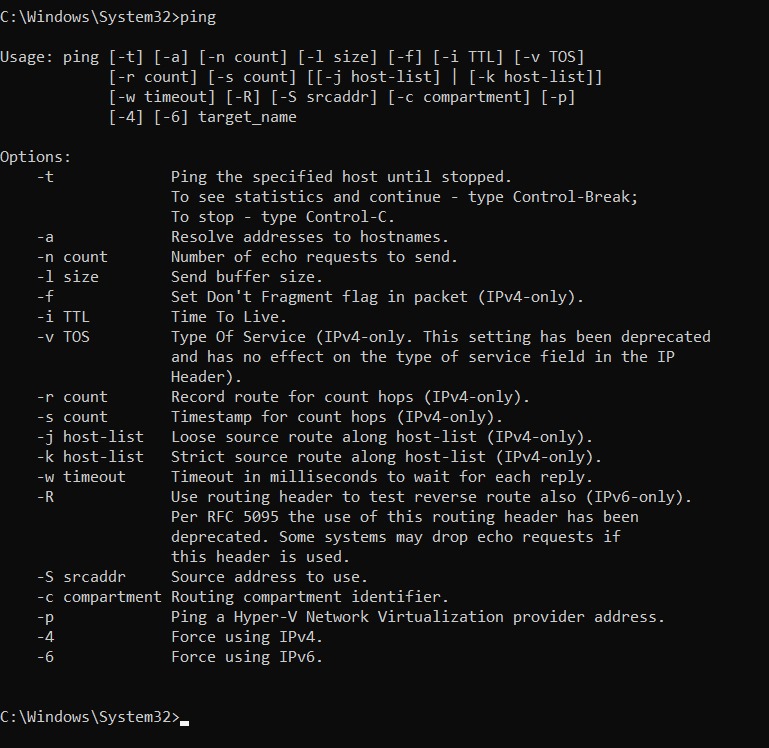
Theory: Used to check the registration and ownership details of a domain name.

Example: whois example.com returns information about the domain example.com.

These commands are essential tools in network administration, security analysis, and troubleshooting, providing detailed insights into network operations and configurations.

**Execution Of Commands:**

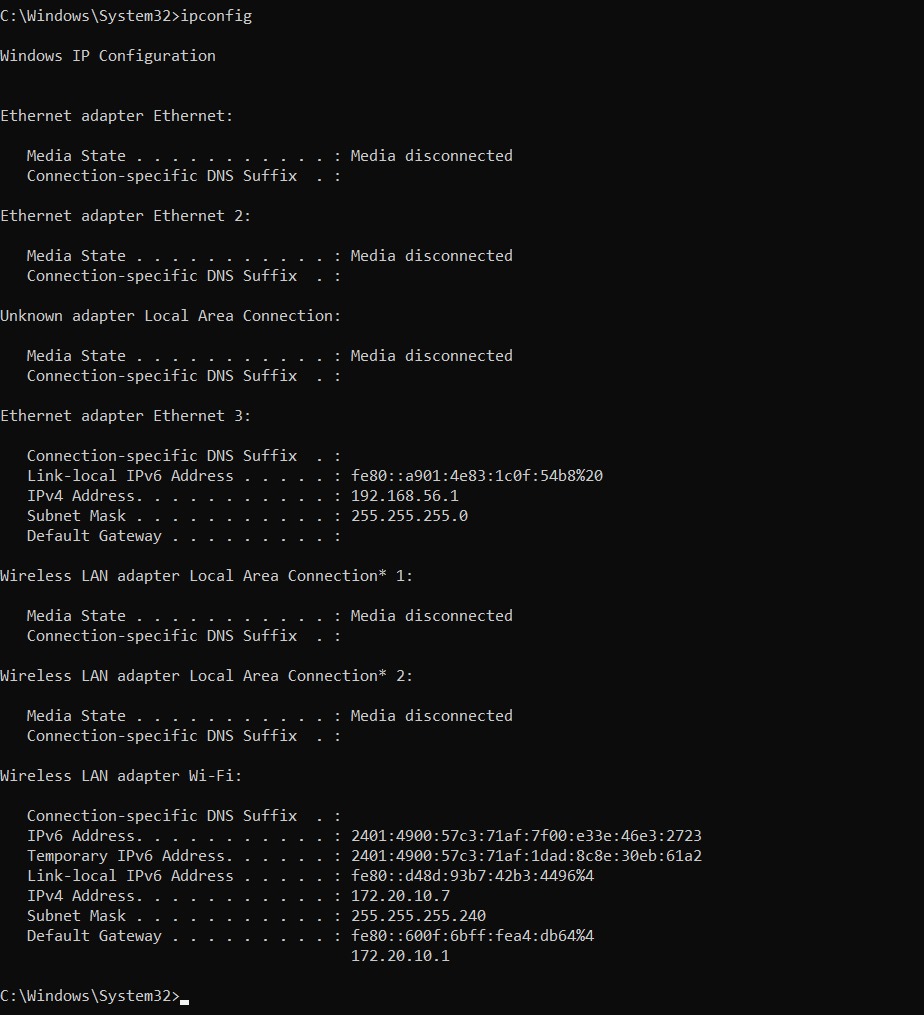
**1). ping**

****

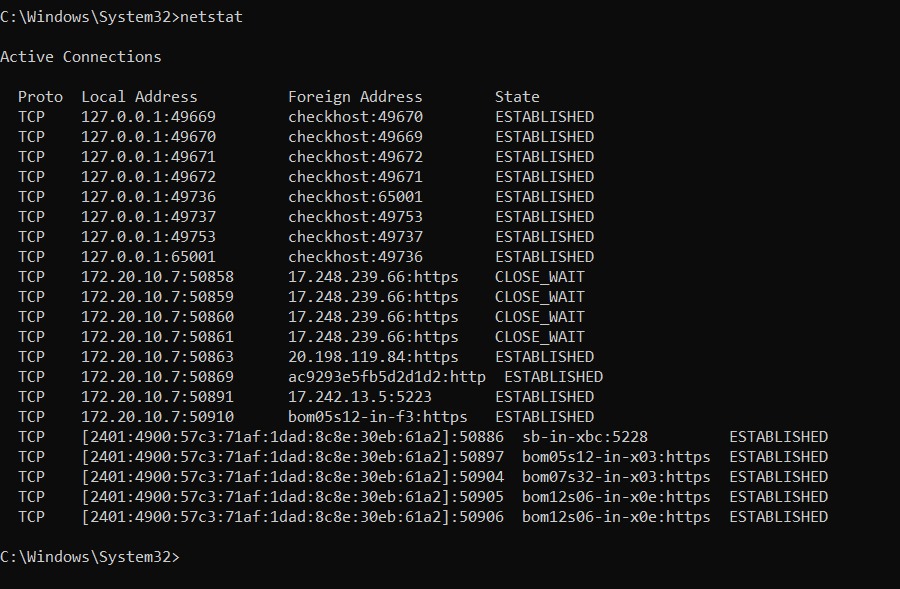
**2). pathping**

****

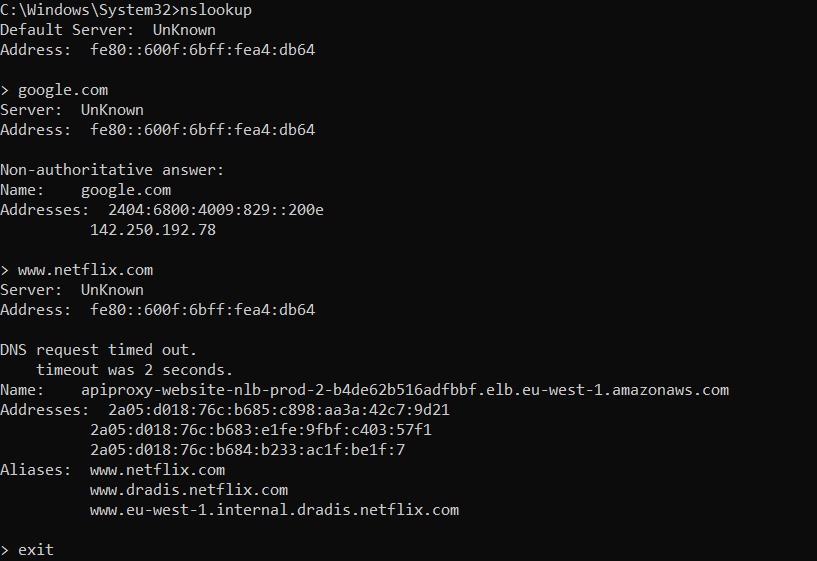
1. **. Ipconfig**

****

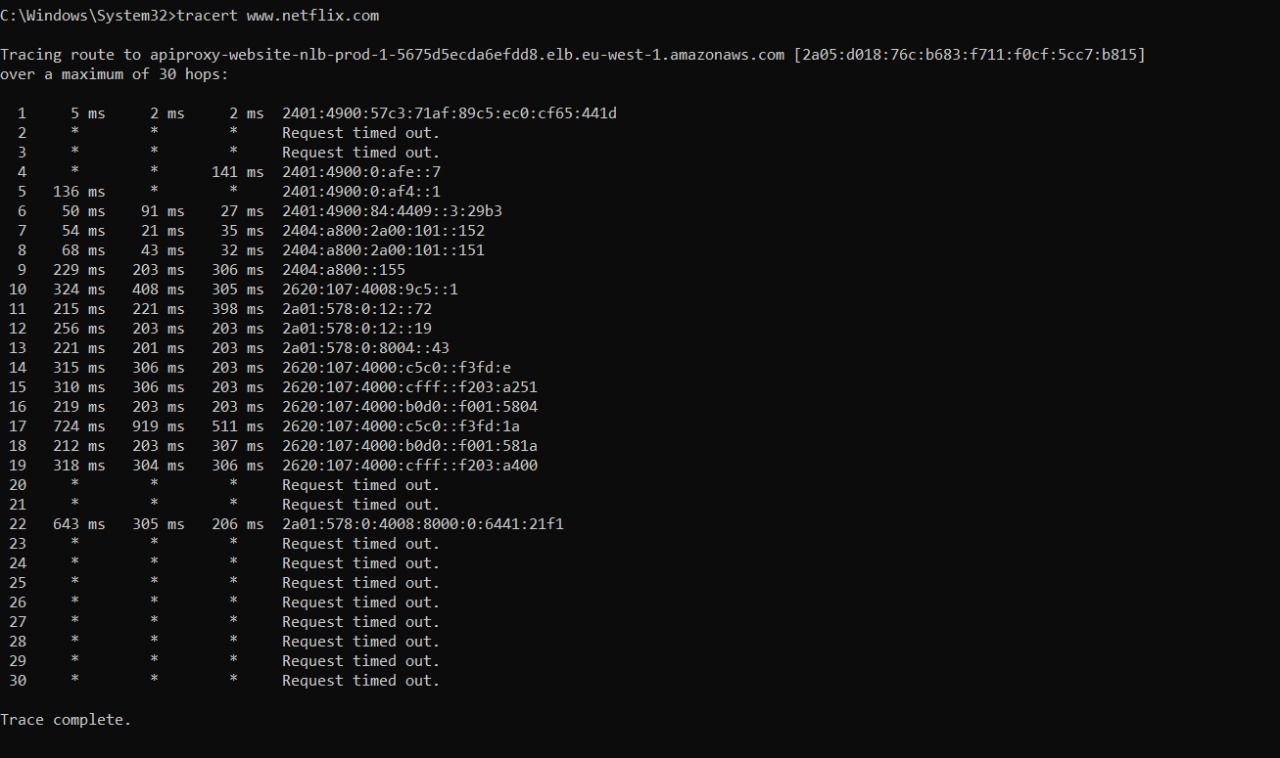
1. **. Netstat**

****

1. **. Nslookup**

****

1. **. Tracert**

****

1. **. Route**

****

**Conclusion :**

In conclusion, the commands discussed are vital tools in network management and security. They allow administrators and users to:

**1. Monitor and troubleshoot network connectivity** (`ping`, `tracert/traceroute`, `ipconfig/ifconfig`).

**2. Analyze network traffic and connections** (`netstat`, `nmap`).

**3. Manage and diagnose DNS and routing issues** (`nslookup`, `arp`, `route`).

**4. Identify and understand user and domain information** (`finger`, `whois`, `hostname`).

Mastering these commands equips individuals with the ability to efficiently manage, secure, and troubleshoot networks, ensuring smooth and reliable network operations.