Aim

To execute various networking commands for diagnostic and troubleshooting purposes on a Windows system.

1. Ping Command

The ping command is used to test network connectivity and diagnose network-related issues by sending Internet Control Message Protocol (ICMP) Echo Request packets to a target host or IP address and waiting for ICMP Echo Reply packets.

Syntax:
ping [options] destination
destination: The IP address or hostname (domain name) of the target host you want to ping.

Common Options:
-n <count>: Specify the number of ICMP Echo Request packets to send (default is 4).
-t: Ping continuously until manually stopped (press Ctrl + C to stop).
-l <size>: Set the size of the ICMP Echo Request packets in bytes.
-w <timeout>: Set the timeout in milliseconds to wait for each reply.
-4: Force the use of IPv4.

Examples:

1. Send four ICMP Echo Request packets to an IP address (e.g., 8.8.8.8):
   ping -n 4 8.8.8.8

2. Continuously ping a host and display the results until manually stopped:
   ping -t google.com

3. Set the size of the ICMP packets to 100 bytes:
   ping -l 100 example.com

4. Set a longer timeout (e.g., 3000 milliseconds) for waiting for replies:
   ping -w 3000 example.com

5. Force the use of IPv4 for the ping:
   ping -4 example.com

2. Traceroute Command:

The tracert command is used to perform the equivalent of the traceroute command in Unix-like operating systems. tracert allows you to trace the route that packets take from your computer to a destination host or IP address by sending ICMP Echo Request packets with varying Time-to-Live (TTL) values and observing the ICMP Time Exceeded replies from routers along the path.

Syntax:
tracert [options] destination

destination: The IP address or hostname (domain name) of the target host you want to trace the route to.

Common Options:
-d: Perform a trace without resolving hostnames to IP addresses (numeric output).
-h <max_hops>: Set the maximum number of hops (TTL) to search for the target.
-w <timeout>: Set the timeout in milliseconds to wait for each reply.
-4: Force the use of IPv4.

Examples:

1. Trace the route to a domain (e.g., google.com):
   tracert google.com

2. Trace the route to an IP address (e.g., 8.8.8.8) using numeric output:
   tracert -d 8.8.8.8

3. Set the maximum number of hops (TTL) to 30:
   tracert -h 30 example.com

4. Set a longer timeout (e.g., 500 milliseconds) for waiting for replies:
   tracert -w 500 example.com

5. Force the use of IPv4 for the trace:
   tracert -4 example.com

3. Netstat Command

The netstat command in Windows is a network utility that allows you to display network statistics, active network connections, routing tables, and various network-related information on a Windows operating system. It's a versatile tool for troubleshooting network issues and monitoring network activities.

Syntax:
netstat [options]

Common Options:
-a: Display all active connections and listening ports.
-n: Display addresses and port numbers in numeric format (no hostname resolution).
-b: Display the executable involved in creating each connection or listening port.
-o: Display the owning process identifier (PID) for each connection.
-r: Display the routing table.
-s: Display per-protocol statistics (e.g., TCP, UDP).
-p <protocol>: Show connections for a specific protocol (e.g., -p tcp or -p udp).
Examples:

1. Display all active connections and listening ports:
netstat -a

2. Display all active connections and listening ports with numeric addresses and ports:
netstat -an

3. Display listening ports and the associated processes:

netstat -ab

4. Display routing table information:
netstat -r

5. Display per-protocol statistics (e.g., TCP and UDP):
netstat -s

6. Display active connections for a specific protocol, such as TCP:
netstat -p tcp

4. Ipconfig

The ipconfig command in Windows is a command-line tool used to display and manage network configuration settings on a Windows computer. It provides information about the computer's IP configuration, including the IP address, subnet mask, default gateway, DNS servers, and more.

Basic Usage:

To display basic IP configuration information for all network interfaces, open Command Prompt and type:
ipconfig
This command will display information for all active network interfaces on your computer.

Common ipconfig Options:

1. /all: Displays detailed information for all network interfaces, including physical and virtual adapters.
   ipconfig /all

2. /release: Releases the DHCP lease for all network interfaces, relinquishing their IP addresses.
   ipconfig /release

3. /renew: Renews the DHCP lease for all network interfaces, obtaining new IP addresses if available.
   ipconfig /renew

4. /flushdns: Flushes the DNS resolver cache, which can be useful when troubleshooting DNS-related issues.
   ipconfig /flushdns

5. /displaydns: Displays the contents of the DNS resolver cache, showing the resolved domain names and their corresponding IP addresses.
   ipconfig /displaydns

5. Nslookup

The nslookup command is a network administration tool available in Windows for querying the Domain Name System (DNS) to obtain information about domain names, IP addresses, and other DNS-related records. It can help you troubleshoot and diagnose DNS-related issues or perform DNS lookups.

Basic options

nslookup domain_name

1. Replace domain_name with the domain or hostname you want to look up.

nslookup www.example.com

This will display the IP address(es) associated with the specified domain.

2. To perform a reverse DNS lookup (resolve an IP address to its domain name), type the following command:

nslookup IP_address

Replace IP_address with the actual IP address you want to look up. For example:

nslookup 8.8.8.8

This will display the domain name(s) associated with the specified IP address.

3. To check specific DNS record types for a domain, you can use the following format:

nslookup -type=record_type domain_name

Replace record_type with the specific DNS record type you want to query (e.g., A, MX, NS, TXT) and domain_name with the domain you want to query. For example:

nslookup -type=MX example.com

This will show the MX (Mail Exchange) records for the domain.

4. To change the DNS server used for the lookup (instead of using the default DNS server), you can specify the server using the following format:

nslookup domain_name dns_server

Replace dns_server with the IP address or hostname of the DNS server you want to use.

nslookup www.google.co.in 10.10.1.10

6. **Arp Command**

arp command displays and manages the ARP (Address Resolution Protocol) cache, which maps IP addresses to MAC addresses on your local network.

arp –a

7. **route:** route command is to display and manage the local IP routing table.

   route print

Result

Thus, various networking commands were executed successfully.