SYCS CN

PRACTICAL 1

AIM :
Using, linux-terminal or Windows-cmd, execute following networking commands and note the output: ping, traceroute, netstat, arp, ipconfig, Getmac, hostname, NSLookUp, pathping, SystemInfo

1) ping:

- This diagnostic command verifies connections to one or more remote computers.

Syntax ping [-t] [-a] [-n count] [-l length] [-f] [-i ttl] [-v tos] [-r count] [-s count] [[-j host-list] | [-k host-list]] [-w timeout] destination-list

2) tracert:

- This diagnostic utility determines the route taken to a destination by sending Internet Control Message Protocol (ICMP) echo packets with varying time-to-live (TTL) values to the destination.
- Each router along the path is required to decrement the TTL on a packet by at least 1 before forwarding it, so the TTL is effectively a hop count.
- When the TTL on a packet reaches 0, the router is supposed to send back an ICMP Time Exceeded message to the source computer. tracert determines the route by sending the first echo packet with a TTL of 1 and incrementing the TTL by 1 on each subsequent transmission until the target responds or the maximum TTL is reached.
- The route is determined by examining the ICMP Time Exceeded messages sent back by intermediate routers.
- Notice that some routers silently drop packets with expired TTLs and will be invisible to tracert.

Syntax tracert[-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

3) netstat:

This diagnostic command displays protocol statistics and current TCP/IP network connection
Syntax
netstat [-a] [-e][-n][-s] [-p protocol] [-r] [interval]

Parameters
-a Displays all connections and listening ports; server connections are usually not shown. -e Displays Ethernet statistics.
This can be combined with the -s option.
-n Displays addresses and port numbers in numerical form (rather than attempting name lookups).
-s Displays per-protocol statistics. By default, statistics are shown for TCP, UDP, ICMP, and IP; the -p option can be used to specify a subset of the default.
-p protocol Shows connections for the protocol specified.
-r Displays the contents of the routing table.
Interval Redisplays selected statistics, pausing interval seconds between each display.

4) arp : This diagnostic command displays and modifies the IP-to-Ethernet or Token Ring physical address translation tables used by the Address Resolution Protocol (ARP).

-a Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.
-g Same as -a.
-v Displays current ARP entries in verbose mode. All invalid entries and entries on the loop-back interface will be shown.
inet_addr Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified by if_addr.
-d Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all hosts.
-s Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.
eth_addr Specifies a physical address.

if_addr If present, this specifies the Internet address of the
interface whose address translation table should be modified.
If not present, the first applicable interface will be used.

5) ipconfig:

This diagnostic command displays all current TCP/IP network configuration values. This command is useful on computers running DHCP because it enables users to determine which TCP/IP configuration values have been configured by DHCP. If you enter only ipconfig without parameters, the response is a display of all of the current TCP/IP configuration values, including IP address, subnet mask, and default gateway.

Syntax ipconfig [/all | /renew [adapter] | /release [adapter]

6) GETMAC:

Returns the media access control (MAC) address and list of network protocols associated with each address for all network cards in each computer, either locally or across a network.
This command is particularly useful either when you want to enter the MAC address into a network analyzer, or when you need to know what protocols are currently in use on each network adapter on a computer.

getmac[.exe][/s <computer> [/u <domain\<user> [/p <password>]]][/fo {table | list | csv}][/nh][/v]

7) NSLookUp

nslookup is the name of a program that lets an Internet server administrator or any computer user enter a host name (for example, "whatis.com") and find out the corresponding IP address or domain name system (DNS) record.
The user can also enter a command for it to do a reverse DNS lookup and find the host name for an IP address that is specified.

Popular nslookup commands include:

- /name: queries the current name server for the specified name

- /server name: sets the current name server to the server the user specifies
- /root: sets the root server as the current server
- /set type=x: specifies the type of records to be displayed, such as A, CNAME, MX, NS, PTR or SOA. Specify ANY to display all records.
- /set debug: turns on debug mode, which displays detailed information about each query
- /set recurse: tells the DNS name server to query other servers if it does not have the information
- /exit: exits nslookup and returns the user to a command prompt

8) pathping

The pathping command is a command-line utility tool in Windows operating systems. It is commonly used to troubleshoot network issues, particularly the ones related to latency and network performance.

It is considered an alternative to tracert and it combines ping and tracert commands. This means that, like tracert, pathping traces all the intermediate hops between a source and a destination, and like ping, it gives you latency and packet loss data. However, pathping will show more detailed results as it can detect which routers are having problems and where they are located.

9) SystemInfo

Systeminfo or systeminfo.exe is a command-line utility that is capable of showing information about Windows version, CPU, BIOS, memory and network information, and many other useful items.