Ans tracert -d www.kiit.ac.in
tracert -4 www.kiit.ac.in // force IPv4.
tracert -6 www.kiit.ac.in // force IPv6.

4) How can you limit number of hops to 10 in traceroute command?

Ans traceroute -m 10 www.kiit.ac.in.

5) How can you display statistical for all protocol using netstat?

Ans netstat -s.

6) Use nslookup to find IP address of www.kiit.ac.in and www.facebook.com
nslookup www.kiit.ac.in (IPv4)
nslookup -type=AAAA www.facebook.com (IPv6)

7) how can you perform reverse DNS lookup to find domain name of IP address 8.8.8.8?

Ans nslookup 8.8.8.8

8) how can you use nslookup to query www.example.com using DNS server at 8.8.8.8?

Ans nslookup www.example.com 8.8.8.8

9) How do you use the ipconfig command to display all TCP/IP network configurations?

Ans ipconfig /all.

10) what are the ipconfig command to release & renew IP address on windows.

Ans ipconfig/release , ipconfig /renew

11) How do you use iptables to add a rule that allows all incoming HTTP traffic (Port 80)?

Ans Sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
-A append rule -p protocol --dport destination port

12) How can you block incoming traffic from IP address 192.168.1.100?

Ans Sudo iptables -A INPUT -s 192.168.1.100 -j DROP
-s source

- Netstat : network statistics provides user with basic stats on all network activity. Lets users know which TCP & UDP connections are active.

1) -r displays Kernel routing tables.
2) -w shows only raw connection.
3) -a all TCP & UDP
4) -l all open listening port.
5) -ap|grep http finds no of program listening on a port.
6) -x shows Unix socket connection.
7) -e displays info about who owns socket
8) -p shows PID & program name for each socket.
9) -M Displays network mask.

- NS lookup : used to determine IP address of a host or domain name that corresponds to an IP address. domain name & mail servers for a domain.
- ipconfig / ifconfig → interface configuration. Used to display all computers current TCP/IP network configuration settings.

1) ipconfig /all: provides systematic complete configuration.
2) ifconfig /registerdns: updates all DHCP & reregisters DNS names.
3) ipconfig /showclassid : all class ids that are permitted for the adapter.
4) ipconfig /setclassid : used to change the DHCP class id.

ASSIGNMENT

1) find IP address of your computer.
Ans ipconfig

2) How to send exactly 4 packets of size 100 bytes to www.github.com?
Ans -c packet count -s packet size
ping -c 4 -s 100 www.github.com

3) Run Traceroute for IPV4 & IPV6 force on website www.kiit.ac.in.

16) -v Verbose output
17) -V print version information.
18) -4 Use IPv4 only.
19) -6 Use IPv6.
20) -c count Stop after sending & receiving count Echo - Request packets.
21) -F flowlabel for IPv6 packets.
22) -i interval between sending each packet.
23) -I use specified network interface to send packet.
24) -l Send specified no. of packet as fast as possible before falling into normal mode of behaviour.
25) -m set the mark for packet.

Reverse DNS is the process of resolving IP address to its corresponding domain name.

- Traceroute / Tracert - diagonistic utility tool which determines the route to a destination by sending internet control message protocol to destination. Used to track real time pathways taken by a packet.

1) -F Set the dont fragment bit.
2) -f first-ttl (set initial time to live value ie start at the first-ttl hop)
3) -T use TCP SYN for probing
4) -m max-ttl - set maximum TTL.
5) -n do not resolve IP address to their domain names, providing numeric output only.
6) -p Set distination port to use.
7) -q nqueries Sets no. of probe queries per hop.
8) -z Set the time to wait between probes.
9) -i specify network interface to be used.
10) -r bypass normal routing tables.

functions

- ping - primary TCP/IP command used to troubleshoot connectivity, reachability & name resolution.
  ICMP → Internet control message protocol is used for error messages & operational information queries.
  Echo → Test connectivity between devices.
  packet inter - network groper.

1) -a audible ping when there is response.
2) -A adaptive ping determines interval between pings dynamically to avoid network congestion.
3) -b allows pinging a broadcast address.
   Broadcast refers to the transmission of message or data packet to all devices on network.
4) -B prevents socket from being bound to source address. Used for cheaking default route.
   A socket is an endpoint for sending or receiving data accross computer network. It is an abstraction provided by OS. TCP socket (reliable, ordered, error-cheacked), UDP socket (connectionless, unreliable)
5) -d set the So_debug option on the socket being used. (provides debugging information)
6) -D print timestamps before each line.
7) -f flood ping. Sends packets as fast as they come back at a rate 100 times per second.
8) -h Displays help message & exits.
9) -L Suppress loopback of multicast packet.
10) -n numeric output avoids DNS lookup.
11) -O report outstanding pings when program terminate.
12) -q quiet output. display start and end summary.
13) -r bypass normal routing & send directly to a host on attached interface.
14) -R records route.
15) -U prints user to user latency (delay btw transmission & reception)

- presentation layer - SSL/TLS (Secure Socket layers / Transport layer security) [cryptographic protocol design to provide secure communication over network, data encryption] JPEG [Joint Photographic Expert Group standard for compressing image file], GIF, ASCII (American Standard Code for Information Interchange)
- Application layer - HTTP (HyperText Transfer protocol), FTP (file transfer ~~protoo~~ protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name system).

TCP/IP Model

- Link layer - Ethernet, ARP, PPP, DSL (Digital Subscribe line provides internet over phone lines)
- Internet layer - IP, ICMP, IGMP.
- Transport layer - TCP, UDP
- application layer - HTTP, FTP, Telnet (protocol for remote terminal access), SNMP (Simple Network management protocol), DNS.

IPV4	IPV6
1) 32 bit address length	1) 128 bit address length
2) Supports Manual & DHCP address configuration.	2) Supports Auto & renumbering address configuration.
3) checksum feild available	3) checksum feild unavailable.
4) header of 20-60 bytes	4) ~~Heder~~ header of 40 bytes.
5) Encryption & authentication not available.	5) Encryption & authentication available.
6) Can be converted to IPV6	6) Not all can be converted to IPV4.
7) Supports Variable Length Subnet mask.	7) Does not support VLSM.
8) 4 feilds present	8) 8 feild present.

TCP/IP model.

- network access layer - controls hardware and media that make up network.
- internet layer - Determines best path through network.
- Transport layer - Supports communication between diverse devices across diverse network.
- application layer - Represents data to user, plus encoding and dialog control.

Different protocols At different layers

OSI Model

- physical layer - ethernet, Wifi, DSL, fibre optics. Ethernet operates at speed 10Mbps to 100Gbps defines wiring & signaling standards.
  DSL (Digital Subscriber Line) transmits digital data over telephone line.
- Data link layer - point to point protocol [direct communication between 2 nodes], HDLC (high level data link control) [Bit oriented protocol used to transfer data over serial connection], ARP (Address Resolution protocol) used to map IP address to MAC address within local network.
- Network layer - IP (internet protocol), ICMP (Internet control Message protocol sends error message, operational information), IGMP (internet Group Management Protocol).
- Transport layer - TCP (Transmission Control Protocol), UDP (User Datagram Protocol).
- Session Layer - NetBIOS (API providing service for network communication & session management), RPC (Remote Procedure call) [protocol allows a program to execute code on a remote server as it is is local & facilitates client-server communication], PPTP (point to point tunelling protocol used to create virtual private networks by tunelling data through public network)

OSI Model [Open Systems Interconnection]
primary architectural model having 7 layers.

→ layer 7 [Application Layer] → Top layer provides set of interface for sending & receiving applications & to use network services like message handling, database query. Eg → file transfer, remote login etc.

→ layer 6 [presentation layer] → manages data format information for networked communication. Responsible for data encryption/decryption.

→ layer 5 [Session layer] → enables 2 networked resources to hold ongoing communications (called session) across network (dialog session). Responsible for synchronization services, checkpoint, initiating, maintaining & terminating sessions.

→ layer 4 [Transport layer] → manages flow of data between parties by segmenting long data stream into smaller data chunks and reassembling them [jitter].

→ layer 3 [Network layer] → decides how route transmission works, handles packet switching & network congestion control - [Timeliness] Gives internet protocol address to each packet ie logical address.

→ layer 2 [Data link layer] → handles special data frames between network layer & physical layer. packets from network layer are divided into frames. [ie to provide hop delivery] increasing reader. helps in flow & error handling.

→ layer 1 [physical layer] → responsible for movement of individual bits which tells driver (software for MAU (media attachment unit) eg NIC, modem what needs to be send & converts bits to electronic signal vice versa.

CN - ASSIGNMENT - 1

NIC -> network interface card a hardware component that connects a computer to a network. Two types of NIC are there ie Wireless & USB based.

It provides:

-> Supports input / output interrupt.
-> direct memory access interface.
-> data transmission.

NIC uses open system interconnection model (OSI) to send signals at the physical layer, transmits data packets at network layer & operates an interface at TCP/IP layer.

RJ-45 -> Type of physical interface commonly used for network cabling for Ethernet networking. It is an 8 pin / 8-position plug or jack used to connect computers & other network devices to Lan. [Registered Jack - 45]

Hub -> connects multiple ethernet device in Lan. operates at physical layer (layer 1) of OSI model. A hub broadcasts data it receives to all connected devices.

Switch -> advance of Hub that connects devices on LAN based on definite Mac address operates on data link layer (layer 2) of OSI model.

Router -> connects multiple network and direct packets between them. Operates on (layer 3). finds best path to transfer data.

Modem -> modulator - demodulator converts digital data from computer into analog signal for transmission.