Bharatiya Vidya Bhavan's
SARDAR PATEL INSTITUTE OF TECHNOLOGY
(Autonomous Institute Affiliated to University of Mumbai)
Munshi Nagar, Andheri (W), Mumbai – 400 058.
Department of Master of Computer Applications

Experiment	0
Aim	To Demonstrate basics of Networking and Network configuration
Objective	1) Learn IP address communication 2) Learn TCP/IP communication 3) Understand the concept of networking.
Name	Vivek Tiwari
UCID	2023510059
Class	SYMCA
Batch	C
Date of Submission	06-08-24

Task	**Answer the questions given Below. Wherever there is command, run it and see the output and analyze the output. Take screenshot and paste in document for the same.**
Question and Answers with screenshots	a) What is IP address? who defines IP Address? What is its range (private and public) **IP address** is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two main functions: network interface identification and location addressing. IP addresses are defined by the Internet Assigned Numbers Authority (IANA). **IP Address Ranges**: • Class A: 10.0.0.0 - 10.255.255.255 • Class B: 172.16.0.0 - 172.31.255.255 • Class C: 192.168.0.0 - 192.168.255.255 b) What is DNS and DNS records? **DNS (Domain Name System)** is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. A Domain Name System (DNS) record is a set of instructions used to connect domain names with internet protocol (IP) addresses within DNS servers. The most commonly used DNS records are A (Address), AAAA (IPv6 Address), CNAME (Canonical Name), MX (Mail Exchange), and NS (Name Server) records. c) Explain is TCP Header, IP Header, and ICMP Header. **TCP Header** contains information necessary for delivering the encapsulated data to the application, such as source and destination port numbers, sequence numbers, and flags. **IP Header** contains information necessary for delivering the encapsulated data to the correct destination, such as source and destination IP addresses, protocol type, and time-to-live (TTL). **ICMP Header** is used for error reporting and diagnostic functions, such as destination unreachable, time exceeded, and echo request/reply messages. d) What is the use of port number? Give its range. **Port numbers** are used to identify specific processes or applications associated with network traffic using the TCP/IP protocol suite. Port numbers range from 0 to 65535, with well-known ports ranging from 0 to 1023.

e) Which service runs on the following port? What is the use of following port number?

- 21: FTP (File Transfer Protocol) - used for file transfers
- 22: SSH (Secure Shell) - used for secure remote access
- 23: Telnet - used for remote terminal access (unencrypted)
- 25: SMTP (Simple Mail Transfer Protocol) - used for email transmission
- 80: HTTP (Hypertext Transfer Protocol) - used for web traffic
- 5900: VNC (Virtual Network Computing) - used for remote desktop access
- 1524: ingreslock - used by the Ingres database management system
- 445: Microsoft-DS - used for Windows file and printer sharing
- 443: HTTPS (HTTP Secure) - used for secure web traffic

f) How to check IP address of a machine? What does Protocol is used for the same?

To check the IP address of a machine, you can use the following commands:

- **ipconfig** (Windows) - displays all current TCP/IP network configuration values
- **ifconfig** (Unix-like) - configures a network interface

The protocol used for IP address resolution is the Address Resolution Protocol (ARP), which maps a network layer address (IP address) to a data link layer address (MAC address).

g) Use of following command:

- **netstat** - displays active network connections and listening ports
- **iwconfig** - configures a wireless network interface
- **whois** - retrieves registration information for a domain name or IP address
- **nslookup** - queries Internet domain name servers
- **route** - manipulates the IP routing table
- **dig** - performs DNS lookups and displays the answers
- **traceroute** - determines the path taken by packets across an IP network
- **ping** - tests the reachability of a host on an IP network

What is the difference between IPv4 and IPv6 address?

IPv4 (Internet Protocol version 4) uses 32-bit addresses, allowing for a total of approximately 4.3 billion unique addresses. **IPv6 (Internet Protocol version 6)** uses 128-bit addresses, greatly expanding the available address space. IPv6 also introduces improvements such as simplified header format, better support for extensions and options, and better support for real-time data.

a) What is a router and routing table?

A **router** is a networking device that forwards data packets between computer networks. It determines the best path for forwarding the packets based on information in the IP header and its routing table. The **routing table** is a data table stored in a router or network host that lists the routes to particular network destinations, often based on the destination's IP address.

b) What is Network Interface Card?

A **Network Interface Card (NIC)** is a computer hardware component that connects a device to a computer network. It provides a physical interface for sending and receiving data over a network link.

c) What is firewall and its types?

A **firewall** is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewall types include:

- **Packet filtering firewalls** - inspect the headers of network packets to

	determine whether to allow or block them • **Circuit-level gateways** - monitor TCP handshaking to determine if a session is legitimate • **Application-level gateways (proxy firewalls)** - apply security mechanisms to specific applications, such as FTP and HTTP • **Stateful inspection firewalls** - track the state of network connections and use this information to determine if packets are allowed d) What is DMZ? A **DMZ (Demilitarized Zone)** is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, such as the Internet. It is an additional layer of security between an organization's internal network and an external network, designed to prevent unauthorized access to private data.
Conclusion	Your Learning from the session.