Data Communication and Computer Networks

Lab Assignment – 1

**Name: ANKIT GOSWAMI**

**Roll No: 120CS0156**

**Q1) Study about functionality of intermediate devices used in Internet and compare it.**

**Ans)** The functionality of intermediate devices used in Internet are:

1. **Modem:** Any electronic devices that convert digital data signals into modulated analog signals suitable for transmission over analog telecommunications circuits.
2. **Hub:** Hub is a node that broadcasts data to every computer or Ethernet-based device connected to it.
3. **Repeater:** A dynamic network device used to reproduce the signals when they transmit over a greater distance so that the signal's strength remains equal.
   * It can be used to create an Ethernet network.
   * A repeater that occurs as the first layer of the OSI layer is the physical layer.
4. **Switch:** Network switch connects devices in a network to each other, enabling them to talk by exchanging data packets.
5. **Bridge:** A bridge in a computer network is a device used to connect multiple LANs together with a larger Local Area Network (LAN).
6. **Router:** A router is a device that connects two or more packet- switched networks or subnetworks. It serves two primary functions:

managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

1. **Firewall:** Firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.
2. **Gateway:** A gateway is a network node used in telecommunications that connects two networks with different transmission protocols together.

**Q2) Study about UNIX commands used in TCP/IP. Ans)** The UNIX commands used in TCP/IP are:

1. **ftp:** ftp is the user interface to the Internet standard File Transfer Protocol. The program allows a user to transfer files to and from a remote network site.
   * ftp -a: Use active mode for data transfers. This is useful for transmissions to servers which do not support passive connections(for whatever reason).
   * ftp -p: Use passive mode for data transfers. Allows use of ftp in environments where a firewall prevents connections from the outside world back to the client machine. Requires that the ftp server support the PASV command. This is the default now for all clients (ftp and pftp) due to security concerns using the PORT transfer mode. The flag is kept for compatibility only and has no effect anymore.
   * ftp -i: Turns off interactive prompting during multiple file transfers.
   * ftp -n: Restrains ftp from attempting ''auto-login'' upon initial connection. If autologin is enabled, ftp will check the . netrc (see netrc(5)) file in the user's home directory for an entry describing an account on the remote machine. If no entry exists, ftp will prompt for the remote machine login name (default is the user identity on the local machine), and, if necessary, prompt for a password and an account with which to login.
   * ftp -e: Disables command editing and history support, if it was compiled into the ftp executable. Otherwise, does nothing.
   * ftp -g: Disables file name globbing.
   * ftp -m: The default requires that ftp explicitly binds to the same interface for the data channel as the control channel in passive mode. Useful on multi-homed clients. This option disables this behavior.
   * ftp -v: Verbose option forces ftp to show all responses from the remote server, as well as report on data transfer statistics.
   * ftp -d: Enables debugging.
2. **hostname:** with no options displays the machine's hostname.
   * hostname -d: Displays the domain name of the machine belongs to.
   * hostname -f: Displays the fully qualified host and domain.
   * hostname -i: Displays the IP address of the current machine.
3. **ifconfig:** View network configuration, it displays the current network adapter configuration. It is handy to determine if you are getting transmit (TX) or receive (RX) errors.
4. **netstat:** Most useful and very versatile for finding a connection to and from the host. You can find out all the multicast groups (network) subscribed by this host by issuing **"netstat -g"**.
5. **ip:** This command is used to show or manipulate routing, devices, and tunnels. It can perform several other tasks like configuring and modifying the default and static routing, setting up tunnel over IP, listing IP addresses and property information, modifying the status of the interface, assigning, deleting and setting up IP addresses and routes.
6. **ping:** It sends packets of information to the user-defined source. If the packets are received, the destination device sends packets back. Ping can be used for two purposes.
   * To ensure that a network connection can be established.
   * Timing information as to the speed of the connection.
7. **traceroute:** A handy utility to view the number of hops and response time to get to a remote system or website is a traceroute. Again you need an internet connection to make use of this tool.
8. **scp:** The scp command files or directories between a local and a remote system or between two remote systems.
9. **sftp:** The sftp command is an interactive file transfer program with a user interface similar to ftp. However, sftp uses the SSH file transfer protocol to create a secure connection to the server.
10. **telent:** Connects destination host via the telnet protocol, if telnet connection establishes on any port means connectivity between two hosts is working fine.
11. **nslookup:** If you know the IP address it will display the hostname. To find all the IP addresses for a given domain name, the command nslookup is used. You must have a connection to the internet for this utility to be useful.