3] Telnet and SSH

Telnet	SSH
• Telnet is the Std TCP/IP protocal for virtual terminal services. it enables you to establish a connection to a remote system in such a manner that it appears as a local system	• SSH or Secure Shell is a program to log into another computer over a network to execute command in a remote machine.
• Telnet uses port 23, which was designed specifically for local area networks	• SSH runs on port 22 by default, which you can change it.
• no privileges are provided for the user's authencation	• SSH is more secure, so it uses publickey encryption for auth
• Sutaible for privote networks	• Sutaible for public networks
• telnet transfer the data in plain text.	• The encrypted format is used to send data.
• low bandwidth usage	• High bandwidth.
• use in linux & Windows	• all OS
• vulnerable to security attacks	• over come many security issues of Telnet.

4] FTP and TFTP

FTP (File Transfer Protocol)

- FTP is a std network protocol used to transfer files between computers on a network.
- FTP is a client-server protocol, which means that a client establish a connetion to an FTP server and then initiatos file transfers
- FTP uses two channels to transfer files. control channel & Data channel
- The control channel is used to establish the connection between the client and the server & to send commands & recive responses.
- The data channel is use to transfer the actual files.
- ~~FTP has two modes of operations : active & passive mode~~

TFTP (Trivial File Transfer Protocol)

- Trivial File Transfer Protocol (TFTP) is a simple, lock-step, file transfer protocol.
- It is used to transfer files bet^n devices on a network & typically used for transferring firmware & config files to network devices
- TFTP is a connectionless, datagram-oriented protocol, which means it does not establish a dedicated connection before transfering files insted it uses UDP
- TFTP uses a very simple form of authentication, it only check the client's IP address to ensure that it is authorized to access the server.

Stands for	FTP	TFTP
size	heavier	light weight.
ports	20 & 21	69
Protocol	TCP	UDP
Complexity	more complex	less Complex
commands	lot of commond	five commond.
services	connection-oriented	connection-less.
speed	slower	faster.

5] HTTP and SMTP

HTTP	SMTP
• HTTP stands for Hypertext transfer protocol	• SMTP stands for Simple mail transfer protocol
• It is use for Data & file transfer	• SMTP is used for mail services
• HTTP uses port no 80.	• SMTP uses port no 25
• HTTP transfers files & data from web server to web client	• SMTP uses mail servers to transfer emails from one inbox to another
• HTTP uses Pull protocol	• SMTP uses push protocol
• HTTP uses both a persistent & non-persistent connection	• uses persistent connection
• place each object in it's own HTTP message	• Place all object into a single message

6] SNMP:

- SNMP (Simple Network Management Protocol) is a protocol to manage & monitor network devices such as router, switches servers.
- It is used to collect information about the device's performance, configuration, etc.
- SNMP is composed of several management components.
  1. managed devices : network device that are being managed & monitored
  2. management station :- The computer or device that is used to monge & monitor the monged devices.
  3. Agent :- Software that runs on the managed devices and communicates with management stations.
- SMI (Structure management Info) :- SMI defines the structure and Format of Info that is exchanged betn management station & agent.

- MIB (Management Info Base):- MIB is database of info about the managed device. it contains info about device performance, config etc.
- SNMP : SNMP is the protocol that is used to exchange info between the management station & agent, it is based on UDP and uses 161 port.
- UDP Port :- SNMP uses UDP port 161 for sending and receiving SNMP messages.
- Security :- v1 & v2 are not secure v3 added security features like authentication & encryption.