

6.

TFTP: stands for trivial file transfer protocol. TFTP is used to transfer a file either from client to server or from server to client without need of FTP feature. Software of TFTP is smaller than FTP. TFTP works on 69 port no. & its service is provided by UDP.

- The complexity of TFTP is less than FTP complexity.
- there are only 5 msg in TFTP. doesn't need authentication for communication.
- TFTP is mainly used for transmission of configurations to & from n/w devices.
- TFTP unreliable transfer protocol faster as compared to FTP.
- requires less programming effort.
- requires less memory & uses the simple control commands.

TELNET:

- stands for Teletype Network. it is type of protocol that enables one computer to connect to local computer. used as standard TCP/IP protocol for virtual terminal service.
- computer which starts being connected starts connection known as local computer.
- computer which being connected known as remote computer.
- During telnet operation whatever that is being performed on remote computer will be displayed by local computer.

- operates on client / server principle.
- commands of Telnet are identified by prefix character, interpret as command which is having code 255. basic format of command is.

255	command code	option code
-----	--------------	-------------

- Telnet is not a secure communication protocol because it does not use any security mechanism & transfers data over network in a plain-text form.
- There is no authentication policies & data encryption techniques used in Telnet causing huge security threat that is why telnet is no longer used for accessing network devices & servers over public network.

SSH: or Secure Shell

- is now only major protocol to access the n/w devices & servers over the internet.
- SSH was developed by SSH communication security it is a program to log into another computer over n/w, to execute command in remote machine & move files from one machine to another.
- provides strong authentication & secure communication over insecure channels.

- SSH runs on port 22 by default it can be easily changed. it is very secure protocol becoz it shares & sends the info in encrypted form which provides confidentiality & security of data over an un-secured n/w such as internet
- Once data for communication is encrypted using SSH, it is extremely difficult to decrypt & read that data.
- SSH protects a n/w from attack such as IP spoofing, IP source routing & DNS spoofing
- SSH also uses a public key for authentication for users accessing a server & it is great practice providing us extreme security

Diff betn SSH & Telnet

- SSH is more secure compared to Telnet
- SSH encrypts data while Telnet sends data in plain text.
- SSH uses public key for authentication while Telnet doesn't use any authentication
- SSH adds a bit more overhead to bandwidth compared to Telnet
- Telnet has been all but replaced by SSH in almost all uses.
- SSH & telnet commonly serves the same purpose.

HTTP:

- stands for Hyper Text transfer protocol
- used for to transfer info over a computer network & are an integral part of today's Internet
- HTTP is backbone of world wide web. It defines format of messages through which web browsers & web servers communicate, also define how a web browser should respond to a particular web browser request.
- HTTP is stateless. A stateless protocol implies that the HTTP web server doesn't maintain which request had originated from which user. Hence, to give customized service to users, HTTP uses cookies.
- HTTP encapsulates each file in a different HTTP msg.
- A client that wants to access a webpage needs the address. To facilitate the access of documents distributed throughout the world, HTTP uses locators.
- The uniform resource locator (URL) is a standard for specifying any kind of info on internet. URL defines 4 things: protocol, host computer, port & path.

SNMP: (Simple Network Management Protocol)

- SNMP is an application layer protocol that uses UDP port no. 161/162. SNMP is used to monitor the n/w, detect n/w faults & sometimes even used to configure remote devices.

There are 3 components of SNMP.

1) SNMP manager:

- centralised system used to monitor n/w. also known as Network Management Station (NMS)

2) SNMP agent

- software management software module installed on managed device. Managed device can be network devices like PC, routers, switches, servers etc.

3) Management Information Base

- MIB consists of info on resources that are to be managed. This info is organised hierarchically, consists of objects instances which are essentially variables.

- SNMP messages -

Diff. variables are:

1. GetRequest - SNMP manager sends this message to request data from SNMP agent. SNMP agent responds with requested value through response msg.

2. GetNext Request -

- This msg can be sent to discover what data is available on SNMP agent.

3. GetBulk Request -

- used to retrieve large data at once by SNMP manager from SNMP agent.

4. Set Request

5. Response.

6. Trap

7. Inform Request.

SMTP (simple mail Transfer protocol)