- Title :- Understand and Compare Telnet and SSH protocol

- Objective :- To understand the difference between Telnet and SSH protocols and stimulate their usage in Cisco packet tracer

- Mode Used :- Cisco Packet Tracer

- Theory :-

1) Telnet (Telecommunication Network) :- It is a type of protocol that enables one computer to connect to the local computer. It is used as a standard TCP/IP protocol for virtual terminal service which is provided by ISO.
   - Duming telnet operation, whatever is being performed on the remote computer will be displayed by the local computer.
   - It operates on a client server principle
   - It is an unencrypled remote management protocol used to access and manage devices remotely.
   - It operates on port 23.

Advantages of telnet :-

1. It provides remote access to someone's computer system.
2. Telnet allows user for more access with

fewer problems in data transmission.

3. Telnet saves a lot of time.

4. The oldest system ~~with~~ ~~tel~~ can be conne
to a newer system with telnet having
different operating system.

5. It is straightforward and easy to set u

Disadvantages of Telnet :

1. Data is send in plain text, making it
vulnerable to eavesdropping and attacks like
man-in-the middle.

2. It's lack of encryption poses security risks
especially on untrusted networks.

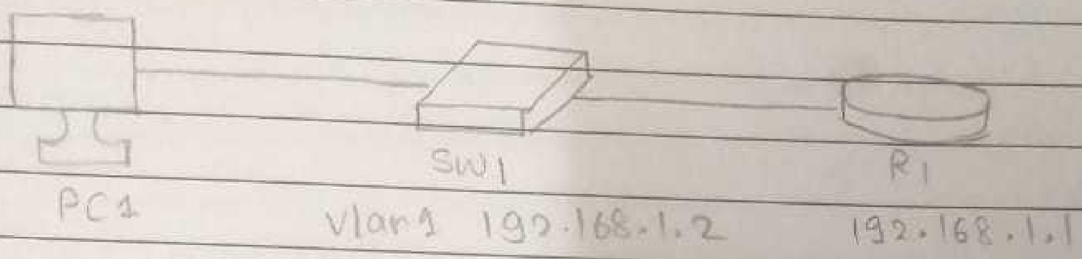
3. Some capabilities are disabled because
of not proper interlinking of the remote
and local devices

2) SSH (Secure Shell) :- It is network protocol that
provides a secure way to access and manage
devices remotely over an unsecured network.

- It provides encrypted and secure access to
remote devices such as severs routers and
switches. ~~SSH~~
- It is commonly used for remote login, file
transfer and command execution
- It ensures confidentiality and integrity of
data by encrypting the communication between
the client and server, making it resistant to
evesdropping and tampering.
- It uses port 22

- It is considered more secure alternative to protocols like Telnet.

- Procedure :
- Create a network topology in Cisco Packet Tracer as given in figure.



- Configure Telnet.

1 Click on switch 1 → CLI. Type the commands as follows.

- en
- config t
- int vlan 1
- ip address 192.168.1.2 255.255.255.0
- no shutdown

- This configure ip address for Sw1

2. Click on Router → CLI. Type the commands

- en
- config t
- int g0/0
- ip address 192.168.1.1 255.255.255.0
- no shutdown

- This configures ip address for R1

3. To configure user on R1. Type following commands.

- exit
- username cisco password lab

4. To configure user on Sw1. Use following commands
   - exit
   - username cisco password lab
5. To configure ~~vT~~ vty line on Sw1 and R1.

   ~~# vty (Virtual teldg tape)~~
   - vty stands for virtual teletype.
   - Sw1 :- (commands)
     1. line vty 0-15
     2. login local
     3. transport input telnet
   - R1 :- (commands)
     1. line vty 0 15
     2. login local
     3. transport input telnet
6. Go on PC1 > Desktop > Command prompt
   - telnet 192.168.1.2
   - provide username and password.
   - exit

   Try now for router 1
   - telnet 192.168.1.1
   - provide username and password
   - exit.

Here we get access to the command line of R1 and Sw1.

- Configure SSH :-
  1. Configur ip address
     - Sw1 >> CLI
       - en
       - config t
       - hostname sw1.
       - int vlan1
       - ip address 192.168.1.2 255.255.255.0
       - no shutdown.
     - R1 >> CLI
       - en
       - config t
       - hostname R1
       - int g0/0
       - ip address ·192.168.1.1 255.255.255.0
       - no shutdown
  2. To configure single user on switch and router
     - ~~ex~~ sw1 :-
       - exit
       - usemame cisco password lab
     - R1 :-
       - exit
       - usemame cisco password lab
  3. To configure DNS domain name on each device.
     - R1 :-
       - ip domain-name cisco.com
     - sw1
       - ip domain-name cisco.com

4. To generate keys to encrypt the packet.
   - SW1 :-
     - crypto key generate rsa.
     - 1024
   - R1 :-
     - crypto key generate rsa
     - 1024
5. To configure vty line.
   - R1 :-
     - line vty 0 15
     - login local
     - transport input SSH.
     - exact timeout 5
   - SW1 :-
     - line vty 0 15
     - login local
     - transport input SSH
     - exact timeout 5
6. For using SSH version 2 use following command in R1 and SW1.
   - exit
   - ip SSH version 2
7. To connect to command line of sw1 and R1 from PC1

(Telenet command doesn't work here)
use following command in command prompt of PC1

- ssh -l cisco .192.168.1.2
- enter password
- exit

- ssh -l cisco 192.168.1.1
- enter passwoord
- exit.

° Observation :-

1. When using Telnet, the connection is estabilished in plain text and the passwoord is transmitted as plain text.
2. When using SSH the connection is encrypted, ensuring secure communication and the passwoord is not visible durning transmission.

° Conclusion :-

- Telnet is easy to configure but lacks security due to its plain text nature
- SSH provides secure, encrypted communication making it the preferred choice for remote management, especially in sensitive environment
- It is important to use SSH over telnet for secured netwoork connection.