

COMPUTER NETWORKS ASSIGNMENT 7

Name: Diksha Katake
Roll No. 331023
GR NO: 21820112
Batch: A1

Aim: Installation and Configuration of Remote Login Service Telnet/SSH and access it through Telnet/SSH client

Objective: To understand and implement the configuration of Remote Login Service

Theory:

TelNet:

Telnet is a network protocol that allows a user to communicate with a remote device. It is a virtual terminal protocol used mostly by network administrators to remotely access and manage devices. Administrator can access the device by *telnetting* to the IP address or hostname of a remote device.

To use telnet, you must have a software (Telnet client) installed. On a remote device, a Telnet server must be installed and running. Telnet uses the TCP port 23 by default.

One of the greatest disadvantages of this protocol is that all data, including usernames and passwords, is sent in clear text, which is a potential security risk. This is the main reason why Telnet is rarely used today and is being replaced by a much secure protocol called SSH.

On Windows, you can start a Telnet session by typing the *telnet IP_ADDRESS or HOSTNAME* command:

1. It doesn't support authentication.
2. Data is sent in clear text therefore less secure.
3. No encryption mechanism is used.
4. Designed to work in local networks only.

The Telnet application protocols call the terminal emulator a *Telnet client* and the device that listens for commands and replies to them a *Telnet server*. To be able of using Telnet, the user must install Telnet client software onto computer. The switch or router runs Telnet server software by default, but the switch or router does need to have an IP address configured so that it can send and receive IP packets. (You can see this configuration in our basic network device configuration section.) In addition, the network between the computer and router needs to be set up and working correctly so that the PC and switch can exchange IP packets and make connection.

SSH:

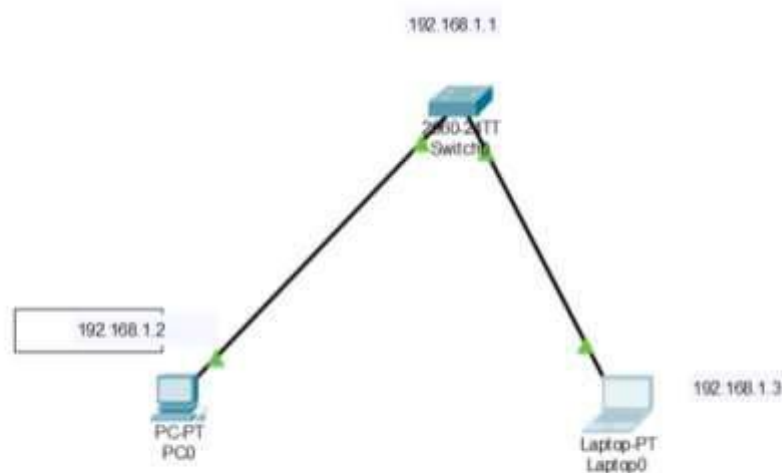
SSH is a network protocol used to remotely access and manage a device. The key difference between Telnet and SSH is that SSH uses encryption, which means that all data transmitted over a network is secure from eavesdropping. SSH uses the **public key encryption** for such purposes.

Like Telnet, a user accessing a remote device must have an SSH client installed. On a remote device, an SSH server must be installed and running. SSH uses the TCP port 22 by default.

1. Unlike telnet, it provides authentication methods.
2. The data sent is in encrypted form.
3. It is designed to work in public network.
4. It uses public key for encryption mechanism.

SSH is the most common way to remotely access and manage a Cisco device.

Network Diagram:



Commands for telnet:

Switch>enable

Switch#conf t

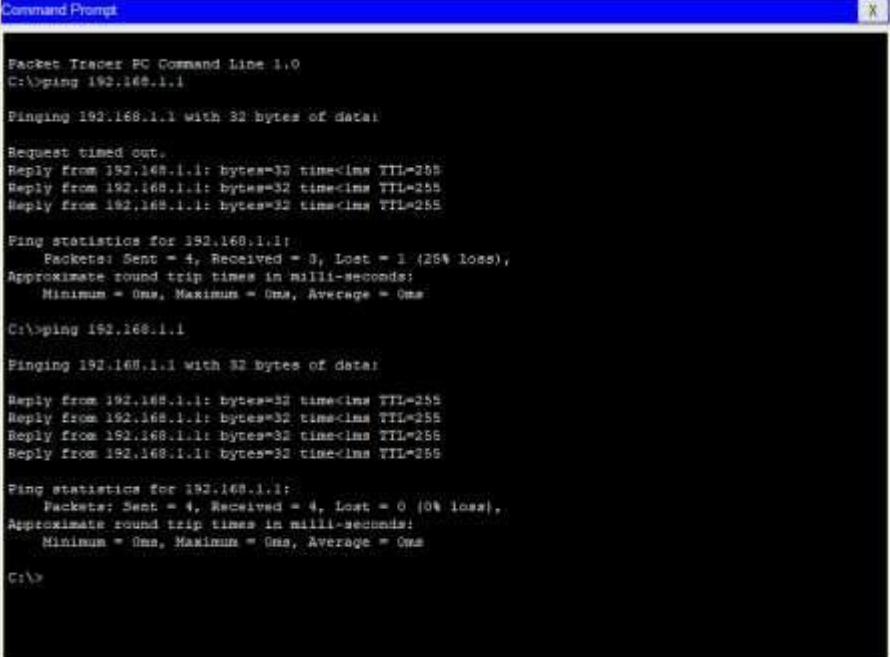
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#interface vlan 1

Switch(config-if)#ip address 192.168.1.1 255.255.255.0

Switch(config-if)#no shutdown

Switch(config-if)#%LINK-5-CHANGED: Interface Vlan1, changed state to up



```
Command Prompt
Packet Tracer PC Command Line 1.0
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
```

Switch#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#line vty 0 4

Switch(config-line)#login local

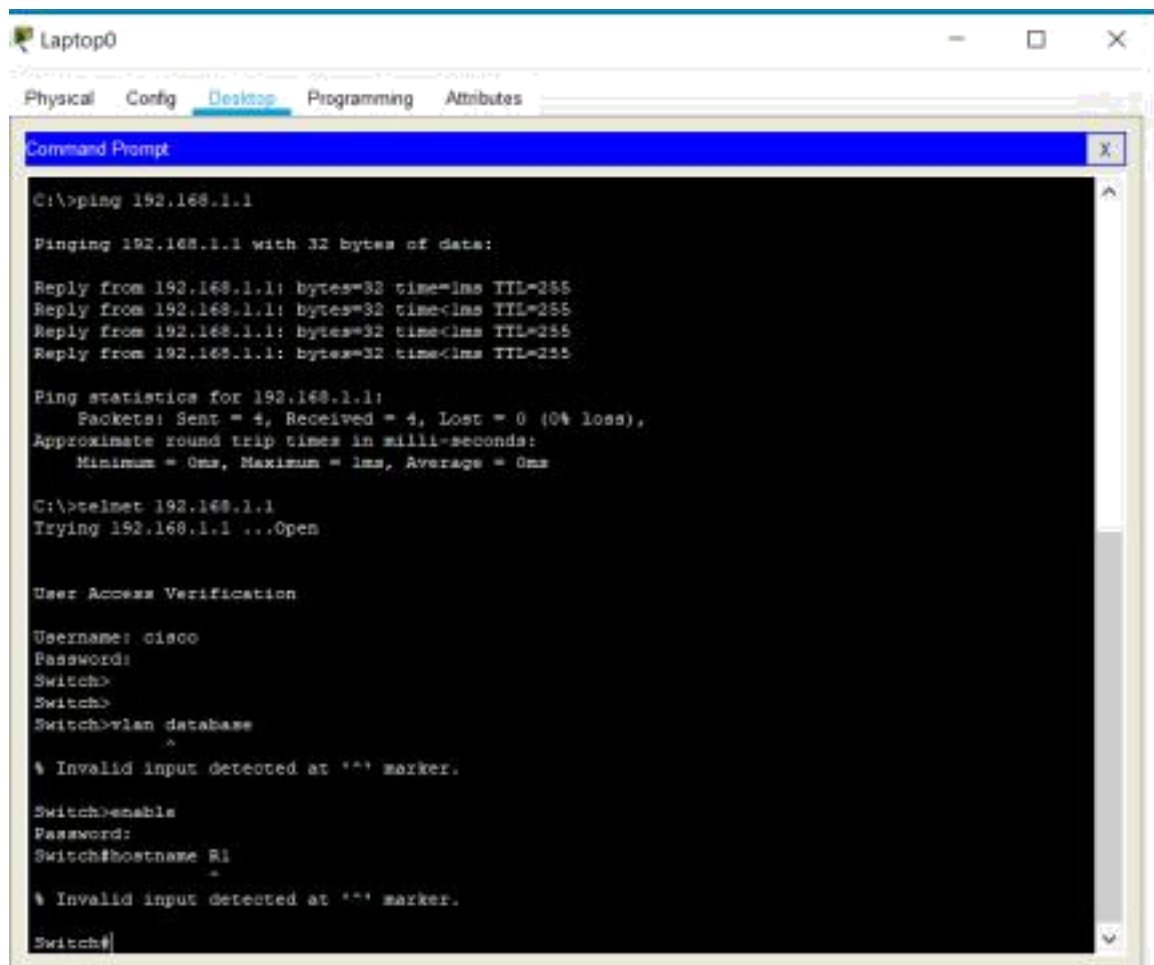
Switch(config-line)#user cisco password cisco

Switch(config)#

Switch(config)#

Switch(config)#

Switch(config)#enable password cisco1



The screenshot shows a Windows Command Prompt window titled "Laptop0" with tabs for Physical, Config, Desktop, Programming, and Attributes. The Desktop tab is active. The Command Prompt displays the following commands and output:

```
C:\>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open

User Access Verification

Username: cisco
Password:
Switch>
Switch>
Switch>vlan database
^
% Invalid input detected at '^' marker.

Switch>enable
Password:
Switch#hostname R1
^
% Invalid input detected at '^' marker.

Switch#
```

Now, we can configure the switch using a remote device

Conclusion:

Hence, we have successfully understood and implemented the remote accessing of a switch through TelNet.