Experiment No: 12

Experiment Name: Configuration and Remote Access of Network Devices Using Telnet and SSH in Cisco Packet Tracer.

Objectives:

- Understand the purpose of remote device access using Telnet and SSH.
- Configure Telnet for basic remote login on network devices.
- Configure SSH for secure encrypted remote access.
- Compare Telnet and SSH in terms of security and usage.
- Verify and test remote connectivity between devices using both protocols.

Telnet:

Telnet (Port 23) is a protocol used to access network devices remotely.

Features of Telnet:

- Works on **TCP port 23**
- Sends **username & password in clear text**
- No encryption → **Not secure**
- Used mainly for **lab experiments**, not production networks
- Requires only VTY password or local login

Telnet Advantages:

- Easy to configure
- Works on all network devices
- Fast, low overhead

Telnet Disadvantages:

- **Unsecured** (username, password, commands visible)
- Vulnerable to packet sniffing
- Not recommended for real networks

SSH:

SSH (Secure Shell) is a secure protocol used for encrypted remote device management.

Features of SSH:

- Works on **TCP port 22**
- Encrypts username, password, and all traffic
- Requires:
  ✅ Domain name
  ✅ RSA key generation
  ✅ Local username/password

SSH Advantages:

- **Secure & encrypted**
- Uses public-key cryptography
- Protected from attacks/sniffing

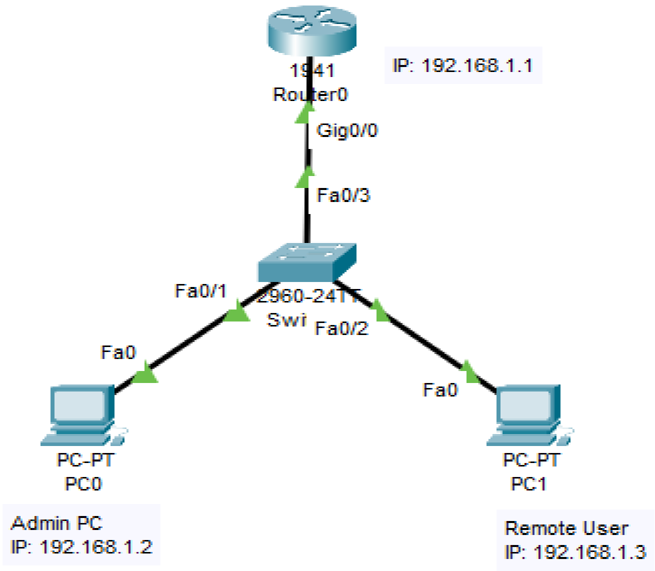
- Industry standard for remote access

SSH Disadvantages:

- Slightly more complex to configure
- Requires RSA keys

Example-1:

Basic Network Topology



IP Addressing Table

Device	Interface	IP Address	Purpose
Router0	G0/0	192.168.1.1	Gateway / Remote Access
PC0	NIC	192.168.1.2	Local Admin PC
PC1	NIC	192.168.1.3	Remote Access PC

TELNET Configuration (Only Telnet)

Step-by-Step: Telnet Setup on Router

```
Router> enable
Router# configure terminal

! Set hostname (optional)
Router(config)# hostname R1

! Set enable password
R1(config)# enable secret cisco123

! Configure interface
R1(config)# interface gig0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit
```

```
! Create local user (optional)
R1(config)# username admin privilege 15 secret admin123

! Configure Telnet on VTY lines
R1(config)# line vty 0 4
R1(config-line)# password telnet123   (if no username)
R1(config-line)# login
R1(config-line)# transport input telnet
R1(config-line)# exit
```

Telnet Testing (From PC)

```
PC> telnet 192.168.1.1

If username configured:
PC> telnet 192.168.1.1
Username: admin
Password: admin123
```

SSH Configuration (Only SSH)

Step-by-Step: SSH Setup on Router

```
Router> enable
Router# configure terminal

! Set hostname and domain name (required)
Router(config)# hostname R1
R1(config)# ip domain-name mynet.local

! Create local user for SSH login
R1(config)# username admin privilege 15 secret admin123

! Configure interface
R1(config)# interface gig0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit

! Generate RSA keys
R1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024

! Force SSH version 2
R1(config)# ip ssh version 2

! Configure VTY lines for SSH
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

SSH Testing (From PC)

```
PC> ssh -l admin 192.168.1.1
Password: admin123
```

Combined Configuration (Telnet + SSH Enabled Together)

This allows **both Telnet and SSH** on the same router.

Step-by-Step: Combined Configuration

```
Router> enable
Router# configure terminal

! Hostname and domain name
Router(config)# hostname R1
R1(config)# ip domain-name mynet.local

! Local user
R1(config)# username admin privilege 15 secret admin123

! Interface configuration
R1(config)# interface gig0/0
R1(config-if)# ip address 192.168.1.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# exit

! Generate RSA keys for SSH
R1(config)# crypto key generate rsa
How many bits in the modulus [512]: 1024

! SSH version
R1(config)# ip ssh version 2

! Enable both Telnet + SSH
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet ssh

              !#(transport input all)
R1(config-line)# exit
```

Testing Both Protocols

Test Telnet

```
PC> telnet 192.168.1.1
```

Test SSH

```
PC> ssh -l admin 192.168.1.1
```

Important Show & Troubleshooting Commands

Purpose	Command
Check SSH status	show ip ssh
Show active users	show users
Verify VTY configuration	show running-config
Check lines	show line
Debug SSH issues	debug ip ssh

Summary Table

Feature	Telnet	SSH
Port	23	22
Encryption	✗ No	✓ Yes
Security	Low	High
Recommended	✗ No	✓ Yes
Command	telnet <ip>	ssh -l user <ip>

Lab Task-1:

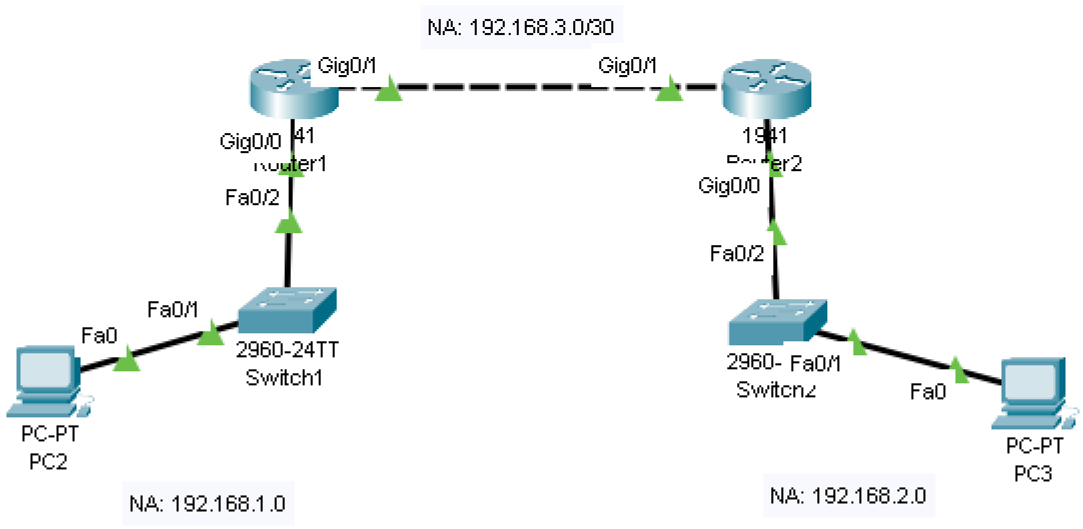
- **LAN1 (R1 side):** `192.168.1.0/24`
- **LAN2 (R2 side):** `192.168.2.0/24`
- **Router-to-Router link:** `192.168.3.0/30`

Now, you'll configure **R1** and **R2** so that:

- ✓ They can route packets between LANs
- ✓ Telnet and SSH work between networks
- ✓ You can test remote login (Telnet-only, SSH-only, or both)

Solution:

Network Topology:



Device	Interface	IP Address	Purpose
R1	G0/0	192.168.1.1	LAN1
R1	G0/1	192.168.3.1	Link to R2
R2	G0/0	192.168.2.1	LAN2
R2	G0/1	192.168.3.2	Link to R1

Step-by-Step Configuration

Router R1 Configuration:

```
enable
configure terminal

! Assign IP addresses
interface gig0/0
 ip address 192.168.1.1 255.255.255.0
 no shutdown
exit

interface gig0/1
 ip address 192.168.3.1 255.255.255.252
 no shutdown
exit

! Enable routing
ip routing

! Add static route to LAN2
ip route 192.168.2.0 255.255.255.0 192.168.3.2

! Configure Telnet access
line vty 0 4
 password cisco
 login
 transport input telnet
exit

! Configure SSH access
hostname R1
ip domain-name example.com
crypto key generate rsa
1024
username admin password admin123

line vty 0 4
 login local
 transport input ssh
exit

! Allow both SSH and Telnet
line vty 0 4
 transport input all
exit
```

```
end
wr
```

Router R2 Configuration:

```
enable
configure terminal

! Assign IP addresses
interface gig0/0
 ip address 192.168.2.1 255.255.255.0
 no shutdown
exit

interface gig0/1
 ip address 192.168.3.2 255.255.255.252
 no shutdown
exit

! Enable routing
ip routing

! Add static route to LAN1
ip route 192.168.1.0 255.255.255.0 192.168.3.1

! Configure Telnet access
line vty 0 4
 password cisco
 login
 transport input telnet
exit

! Configure SSH access
hostname R2
ip domain-name example.com
crypto key generate rsa
1024
username admin password admin123

line vty 0 4
 login local
 transport input ssh
exit

! Allow both SSH and Telnet
line vty 0 4
 transport input all
exit

end
wr
```

Testing Remote Access:

From **PC1 (LAN1)** → access **R2 (LAN2)** via R1 path:

1. **Ping Test:**
2. `ping 192.168.2.1`

   (This confirms routing is working.)

3. **Telnet Access:**
4. `telnet 192.168.2.1`
5. **SSH Access:**
6. `ssh -l admin 192.168.2.1`
7. **Combined (both Telnet + SSH enabled):**
   You can use either Telnet or SSH depending on your preference.

Summary:

Access Type	Command on Router	Line Config
Telnet only	`transport input telnet`	Uses password set under `line vty`
SSH only	`transport input ssh`	Requires local username and crypto key

Both SSH & Telnet	`transport input ssh telnet/`
	`transport input all`
		Allows both