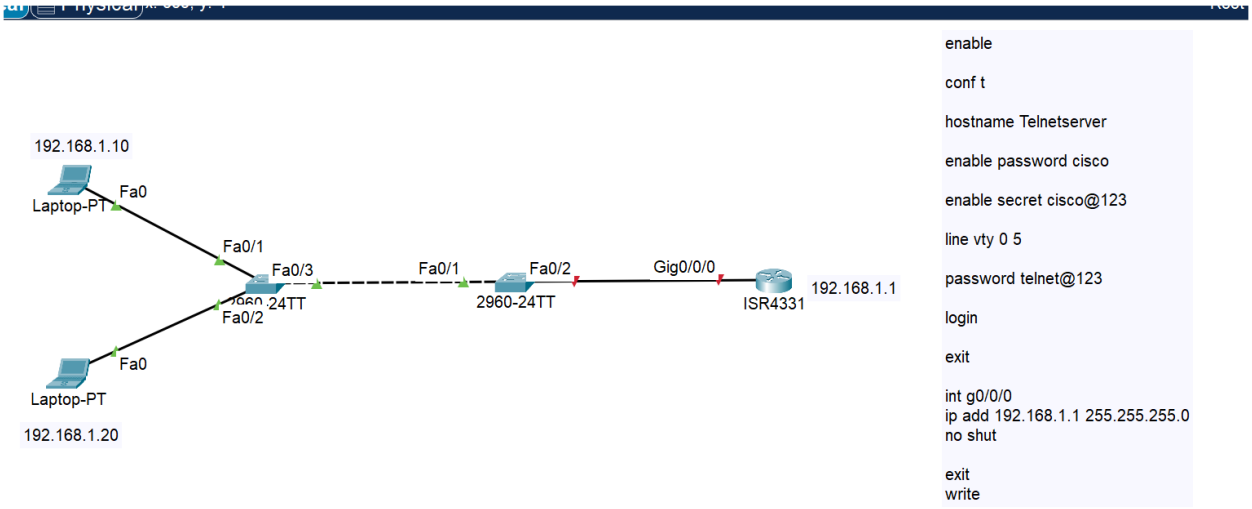
Cisco Router SSH and Telnet Configuration Guide

Prepared by: Baba shaheer

Date: March 20, 2025

Network Topology

- Router: ISR4331 (192.168.1.1)
- Switches: 2960-24TT
- Client PCs: Laptop-PT (192.168.1.10, 192.168.1.20)
- Interfaces: Router G0/0/0, Switch Fa0/1, Fa0/2, Fa0/3



1. Router Interface Configuration

```
enable
configure terminal
int g0/0/0
ip address 192.168.1.1 255.255.255.0
no shut
exit
```

2. Telnet Configuration

Basic Setup

```
enable
configure terminal
hostname TelnetServer
enable password cisco
enable secret cisco@123
line vty 0 5
password telnet@123
```

```
login
exit
write
```

Testing Telnet

From client PC (192.168.1.10 or 192.168.1.20):

```
telnet 192.168.1.1
```

Enter password: `telnet@123`

3. SSH Configuration

Basic Setup

```
enable
configure terminal
hostname TelnetServer
ip domain-name example.com
crypto key generate rsa
```

When prompted for key size, enter: `1024`

```
username admin privilege 15 secret Cisco@123
line vty 0 5
transport input ssh
login local
exit
ip ssh version 2
exit
write
```

Testing SSH

From client PC (192.168.1.10 or 192.168.1.20):

```
ssh -l admin 192.168.1.1
```

Enter password: `Cisco@123`

4. Dual Configuration (Telnet and SSH)

To enable both Telnet and SSH on the same device:

```
enable
configure terminal
hostname TelnetServer
ip domain-name example.com
enable password cisco
enable secret cisco@123
crypto key generate rsa
```

When prompted for key size, enter: `1024`

```
username admin privilege 15 secret Cisco@123
line vty 0 5
transport input telnet ssh
login local
exit
exit
write
```

5. Packet Tracer Specific Notes

- Some versions of Packet Tracer have limited SSH functionality
- The command `crypto key generate rsa modulus 2048` is not supported in all versions, use `crypto key generate rsa` instead
- If SSH doesn't work immediately, try rebooting the devices in the simulation
- Ensure proper IP connectivity before testing (ping test)

6. SSH vs. Telnet Comparison

Feature	SSH	Telnet
Data Encryption	Encrypted (secure)	Plain text (unsecure)
Authentication	Username and password	Password only (typically)
Default Port	22	23
Security	High	Low
Key Exchange	Yes	No
Public Key Authentication	Supported	Not supported
Version	Current: SSH-2	Older technology
Packet Capture Risk	Low (encrypted)	High (readable data)
Configuration Complexity	Moderate	Simple
Resource Usage	Slightly higher	Lower
Industry Standard	Current standard	Legacy protocol

Case Example: Why Choose SSH Over Telnet

Scenario: A network administrator is remotely managing a router containing sensitive network configuration from a coffee shop with public Wi-Fi.

With Telnet: An attacker on the same public Wi-Fi network runs a packet sniffer and captures the Telnet traffic. They can easily read: 1. The administrator's password: `Cisco@123` 2. All commands entered: `show run`, `conf t`, etc. 3. Sensitive configuration information including access lists, VPN settings, and routing information

Result: The attacker gains the password and detailed knowledge of the network, potentially compromising the entire infrastructure.

With SSH: The same attacker captures the SSH traffic but only sees encrypted data. They cannot determine: 1. The administrator's credentials 2. Commands being executed 3. Any configuration data

Result: The network remains secure despite the administrator working from an unsecured location.

7. Security Best Practices

- Always use SSH instead of Telnet in production environments
- Use strong passwords with a combination of letters, numbers, and special characters
- Limit access to management interfaces with ACLs
- Use SSH version 2 (more secure than version 1)
- Change default usernames and passwords
- Implement timeout values for idle sessions
- Consider using SSH key-based authentication where supported

---

Troubleshooting

If you experience issues with the configuration:

1. Verify IP connectivity between devices
2. Check interface status (show ip interface brief)
3. Verify SSH status (show ip ssh)
4. Check VTY line configuration (show run | section line vty)
5. Ensure RSA keys are generated properly (show crypto key mypubkey rsa)

For additional assistance, refer to Cisco documentation or contact your network administrator.