INTERNATIONAL JOURNAL OF LATEST TECHNOLOGY IN ENGINEERING, MANAGEMENT & APPLIED SCIENCE (IJLTEMAS)
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

Remote Router Access Protocols: Security Implications of TELNET and SSH

Renuka Kulkarni, Satyavan Kunjir*

Department of Computer Science, Dr. D. Y. Patil, Arts commerce & Science College, Pimpri Pune 18, Maharashtra, India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1413SP045

Received: 26 June 2025; Accepted: 30 June 2025; Published: 27 October 2025

Abstract - A key component in current network administration is remote access to network devices, which helps effective management and troubleshooting. TELNET and Secure Shell (SSH), two of the protocols that provide this kind of access, are widely used for their functions in router setup and upkeep. The security implications of remote router access via TELNET and SSH are critically examined in this work. Due to its early architecture and lack of encryption, TELNET makes network traffic extremely vulnerable to eavesdropping in modern settings. On the other hand, SSH improves the secrecy and integrity of data by providing secure communication channels and strong authentication.

Keywords — TELNET, SSH, Cisco Router, Encryption, Cybersecurity.

I. Introduction

Remote access to routers and other network devices is necessary for effective administration and troubleshooting in the modern network management architecture. TELNET and Secure Shell (SSH) are the two main tools that make this remote access possible. Although it offers a simple way to connect network devices, TELNET—one of the first protocols created for remote communication—transmits data, including credentials, in plaintext. Due to this basic flaw, networks are vulnerable to a number of security threats, including unauthorized access, session hijacking, and eavesdropping.

Security Problems with Routers serve as gateways for other networks, making them a popular target for many types of assaults. Here are a few examples of various security problems: Violating access control will expose network configuration details, opening a path for attacks on other network components.

II. Literature Review

TELNET uses command-line interface for creating remote access connection for devices. It uses port 23 for communication and is unencrypted, leaving private information open to prying eyes. Unsecured Data Transmission TELNET sends all data, including credentials, in plaintext. Due to this, it is susceptible to replay, sniffer, and interception attacks. Due to Absence of Authentication Integrity TELNET provides little defense against session hijacking and spoofing. Because TELNET is lightweight, it is still utilized in legacy systems and low-power devices, especially in Web of Things contexts, despite the hazards involved. Several breach reports highlight the way constant TELNET use, particularly in poorly configured or unmanaged routers, can serve as a backdoor for attackers.

SSH originated as a secure replacement for TELNET. SSH provides secure authentication, session integrity, and end-to-end encryption when running on port 22. Encryption and Confidentiality provide to protect the communication channel, SSH makes use of public-key infrastructure and symmetric encryption techniques, such as AES. Strong access control and user verification are provided by authentication mechanisms that support both password-based and key-based authentication. For Protection and Session Integrity, the Message authentication codes (MACs) and other built-in methods ensure the session data is kept intact. SSH is now the standard remote access protocol found in enterprise-class firewalls and routers. Currently, a lot of company's advice stringent SSH setups for production environments and block TELNET by default.

The performance of SSH and TELNET have been compared in multiple studies: Even when applied over untrusted networks, SSH significantly lowers the danger of unwanted access when compared to TELNET. Using TELNET in favor of SSH is specifically advised by NIST and leading network manufacturers such as Cisco and Juniper. Over 90% of companies surveyed by Nicol have switched from TELNET to SSH for remote management duties. Despite these developments; TELNET is still frequently enabled by default on consumer routers and embedded equipment, which increases its exposure in networks in houses and small offices.

III. Methodology

The research strategy, tools, methods, and procedures used to examine the security implications of SSH and TELNET protocols in remote router access are provided in this section. The study compares and evaluates the security benefits and drawbacks of both protocols using an experimental and qualitative methodology. Structure of the Research Using simulated settings and simulation tools, Demonstrate of SSH and TELNET on router. Analyze the ways they affect the integrity, confidentiality, and authenticity of data. Included in the study are: analysis of the literature to find known security threats. Using simulation-based testing to show risks and mitigations in practice

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

1. Telnet-

TELNET is a common term for Teletype Network. This is a client server-based protocol creates virtual connection for systems to be used over local area networks (LAN) or the Internet. In essence, TELNET operates on the Microsoft operating system. As it offers a command-line interface, sending data in its original form makes it less safe. It uses port number TCP 23 for remote communication. Configuration of TELNET on Cisco router shown in figure1.

Configuration of TELNET on Cisco Router

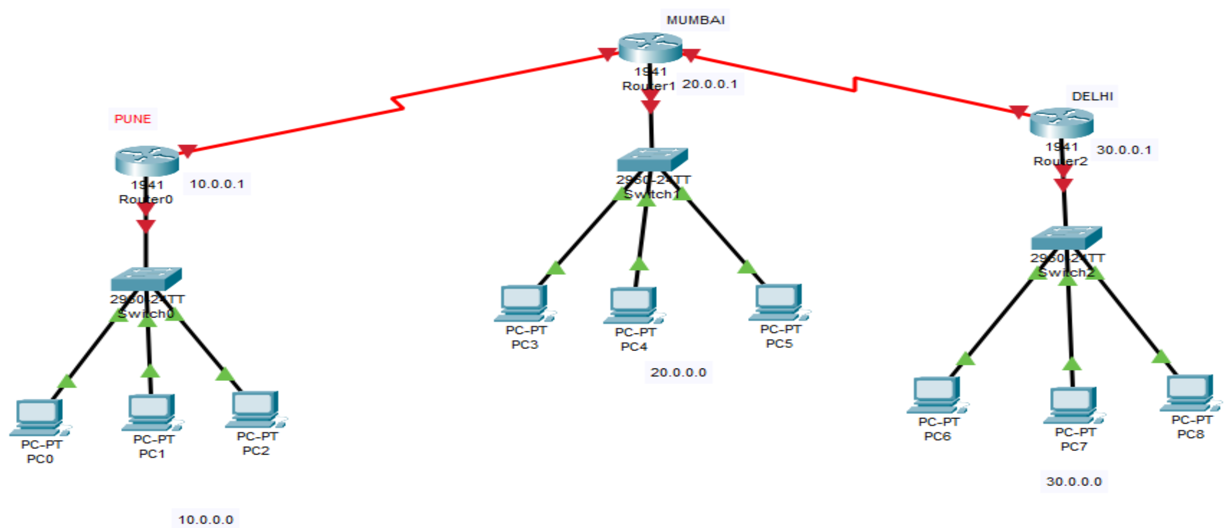

Figure 1: TELNET Implementation on Cisco router

Open the configure terminal in global configuration mode.

Configure the router's hostname to DELHI.

Router> enable

Router # Configure terminal

Router (Config)# Hostname DELHI

Assuming the gateway is on an interface, such as Gigabit Ethernet 0/0,

Configure its IP address. Enter IP address is 30.0.0.1 with subnet mask 255.0.0.0

For enabling the connection enter no shutdown command and then exit from this mode.

Create a login password

DELHI (Config)# line console 0

DELHI (Config-line)#password indiac

DELHI (Config-line)# login

DELHI (Config-line)#exit

DELHI (Config)#

Assign TELNET Password

DELHI (Config)# line vty 0   15

DELHI (Config-line)# password indiae

DELHI (Config-line)# login

DELHI (Config-line)#exit

DELHI (Config)#

Save the configuration and write the memory.

DELHI # write

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

To check

From PC located at PUNE location having IP address 10.0.0.1

Open command Prompt

First check connectivity using ping command

Ping 30.0.0.1

Now check TELNET

Telnet 30.0.0.1

SSH-

The SSH Protocol named SSH (Secure Shell). In other terms, it is a network protocol that uses cryptography to send encrypted data between networks. SSH's port number is 22. Without remembering or entering a password for every system, it enables users to access to the server.

It always arrives in pairs of keys.

1. The public key is visible to anyone and does not require protection. (for the purpose of encryption).

2. Private Key remains on the computer and needs to be secured. (for the purpose of decryption).

SSH is a security method that enables you to access a router or switch's configuration mode and privileges from a distance in order to carry out the necessary activity. The main goal of configuring SSH is to provide remote access to networked devices so that necessary settings may be made and resources can be supplied without interruption. With the help of Cisco Packet Tracer is used to execute he commands to be run the SSH on router. Configuration of SSH on router shown in figure2.

Configuration of SSH on Cisco Router

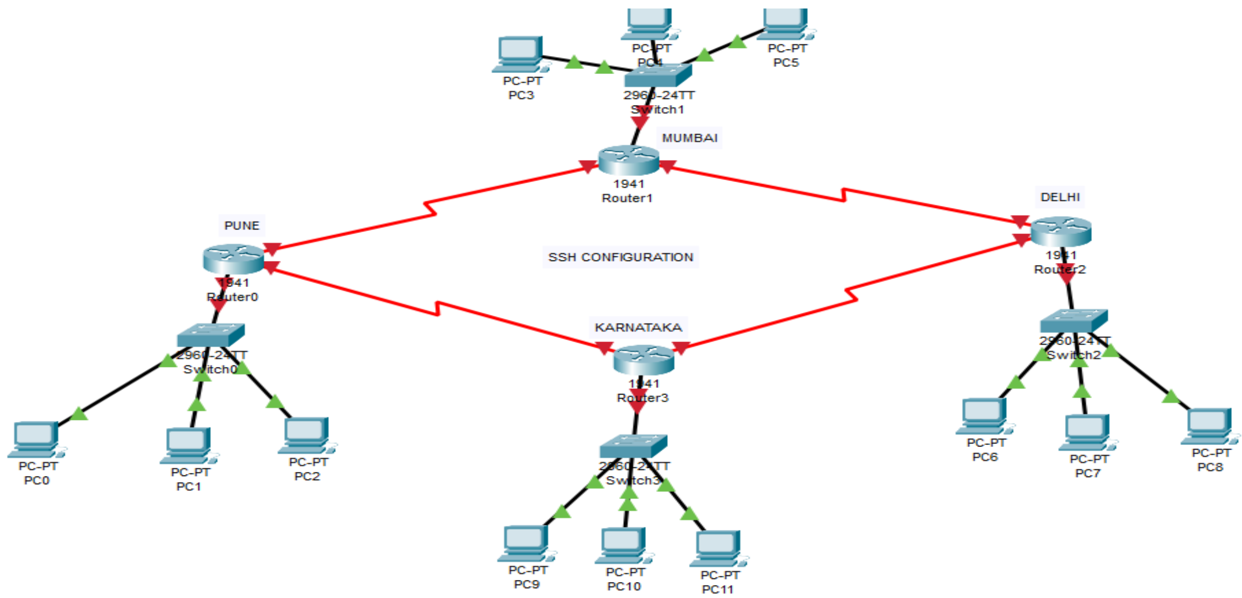

Figure 2: SSH Implementation on cisco router

Open the configure terminal in global configuration mode.

Configure the router's hostname to DELHI. Similar configuration as TELNET

Configuration of domain user and encryption

Router (config) # hostname DELHI

DELHI (config) # ip domain-name mydomain.com

DELHI (config) # username admin Password 123

DELHI (config) # crypto key generate RSA

It will ask for the size (e.g., 1024 or 2048):

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Special Issue | Volume XIV, Issue XIII, October 2025

How many bits in the modulus [512]: 1024

DELHI (config)# line vty 0 4

DELHI (config-line)# transport input SSH

DELHI (config-line)# exit

DELHI (config)# exit

Save the configuration and write the memory.

DELHI # write

To check

From PC located at PUNE location having IP address 10.0.0.1

Open command Prompt

First check connectivity using ping command

Ping 30.0.0.1

Now check SSH

ssh –l admin <IP address of router>

ssh –l admin 30.0.0.1

IV. Conclusions

In the conclusion, the contrast between TELNET and SSH makes it very clear how crucial secure communication protocols are to network administration, Despite its historical significance, TELNET is inappropriate for modern network environments because it lacks encryption and leaves sensitive data vulnerable to attacks and interception.SSH, on the other together, provides strong security via encrypted communication, authentication procedures, and integrity checks, providing secure and private remote access to routers and other network devices. Organizations must prioritize using SSH over TELNET in order to protect network infrastructure and preserve the confidentiality and integrity of transmitted data, especially in light of the growing sophistication of cyber threats. In today's cybersecurity environment, using secure protocols like SSH is not only a best practice but also necessary.

References

1. https://info.pivitglobal.com/resources/telnet-versus-ssh
2. https://www.geeksforgeeks.org/computer-networks/introduction-to-ssh-secure-shell-keys/
3. https://www.geeksforgeeks.org/computer-networks/how-to-configure-ssh-on-cisco-routers-and-switches/
4. Nicol, D. M., Sanders, W. H., & Trivedi, K. S. (2017). "Security Evaluation of Network Protocols in Critical Infrastructure."*IEEE Transactions on Secure Computing*.
5. Sivaraman, V., et al. (2016). "Security Concerns in Home Routers and IoT Devices."*IEEE SecureComm*.