ADVENTIST UNIVERSITY OF CENTRAL AFRICA

NAME: Joseph MUTANGANA

STUDENT ID: 29061

COURSE NAME: Computer Networks

INSTRUCTOR NAME: Joshua IRADUKUNDA

ASSIGNMENT TITLE: Assignment#1

DATE: Oct-12-2025

SSH & TELNET CONFIGURATION LAB

IN CISCO PACKET TRACER

HANDS-ON LAB

Prepared by: Joseph MUTANGANA

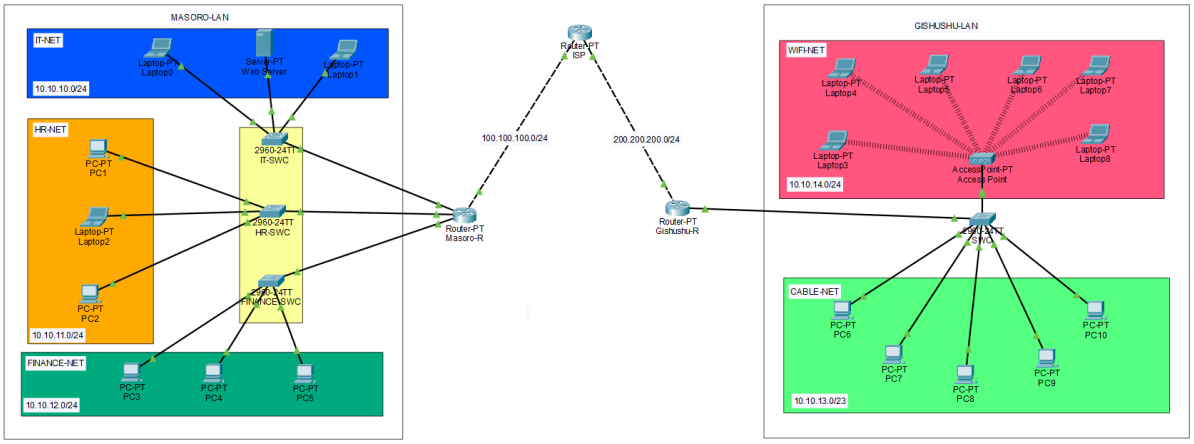
Table of Contents

1. Introduction

In this network, Secure Shell (SSH) and Telnet were configured to enable remote management of routers and switches from any device within the network. Both protocols allow administrators to access and configure network devices without being physically connected to them.

Telnet provides remote access through plaintext communication, which makes it easy to use but less secure since passwords and data are transmitted unencrypted. On the other hand, SSH (Secure Shell) performs the same function but adds data encryption and authentication, ensuring secure management sessions.

2. Network Topology Design



Routers: Used to make connect network and Acts as DHCP server

Switch: Connects multiple end devices

End Devices (Server, PCs/Laptops): Clients used in topology

3. Remote Access Configuration (SSH)

```
29061-S3(config)# ip domain-name jmutangana.rw
29061-S3(config)# username 29061 secret 29061
29061-S3(config)# crypto key generate rsa
```

```
29061-S3(config)# ip ssh version 2
29061-S3(config)# enable secret 29061
29061-S3(config)# line vty 0 4
29061-S3(config-line)# transport input ssh
29061-S3(config-line)# login local
29061-S3(config-line)# exit
```

Explanation of used Commands

ip domain-name jmutangana.rw: defines the domain name for the router because SSH requires a domain to generate RSA encryption keys.

username: Allows to set name of user who is using the device.

Secrete: Allows to set secrete for user when try log in.

crypto key generate rsa: Generates RSA key used for SSH encryption.

```
29061(config)# crypto key generate rsa
The name for the keys will be: 29061.cnet.local
How many bits in the modulus [512]: 1024
```

ip ssh version 2: Enable SSH version 2

line vty 0 4: Enters configuration for virtual terminal lines 0 to 4

transport input ssh: Restrict remote to SSH only.

login local: tells the router/switch to use local username and password

Summary:

Configuring SSH and Telnet provided an understanding of how network devices can be managed remotely and securely. Telnet served as an example of basic remote access, while SSH demonstrated a more secure and modern method using encryption and authentication.

After completing the configuration, all routers were accessible remotely using SSH with local credentials, and Telnet access was disabled to enhance security. This ensured that network management traffic

remained confidential, authenticated, and protected, strengthening the overall security posture of the topology.

END.