Name: Joseph MUTANGANA

Student ID: 29061

Course Name: Computer Networks

Instructor Name: Joshua IRADUKUNDA

Assignment Title: Assignment#1

Date: Oct-11-2025

NETWORK CONFIGURATION

IN CISCO PACKET TRACER

HANDS-ON LAB

Prepared by: Joseph MUTANGANA

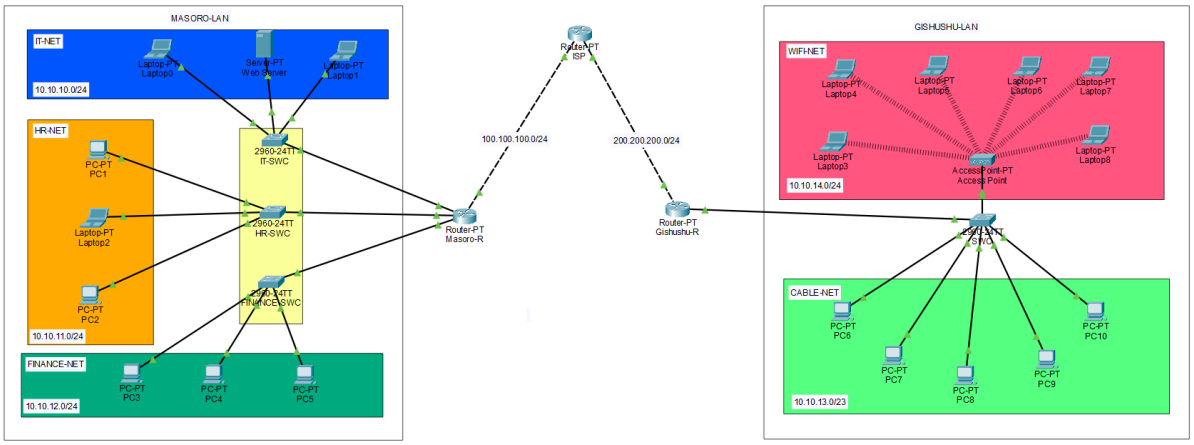
Table of Contents

1. Introduction

The purpose of the activity was to design, configure, and verify a **small-scale network** for two LANs — **Masoro** and **Gishushu** — connected through an **ISP router**, implementing core networking concepts used in real-world environments. The exercise focused on several key networking skills, including:

- **Subnetting and IP addressing**: Assigning unique IP subnets to different departments (IT, HR, Finance, CableNet, and WIFI-NET) and configuring routers and switches accordingly.
- **DHCP configuration**: Automating IP assignment for clients while excluding critical addresses such as the DNS server.
- **Routing**: Enabling communication between subnets using static routing.
- Etc..

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. IP Addressing Scheme and DHCP configuration

Step 1: Opened Router in Packet Tracer -> Opened CLI tab

Step 2: Enter Configuration global mode

```
29061> enable
29061# configure terminal
```

Step 3: Excluded IP address

```
29061(config)# ip dhcp excluded-address 10.10.10.10
```

I only had one Static IP address on server, this command ensures that this IP address exclude from DHCP pool

Step 4: Create DHCP Pool

```
29061(config)# ip dhcp pool IT-NET
29061(dhcp-config)# network 10.10.10.0 255.255.255.0
29061(dhcp-config)# default-router 10.10.10.1
29061(dhcp-config)# dns-server 10.10.10.10
```

```
29061> enable
29061# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
29061(config)# ip dhcp excluded-address 10.10.10.10
29061(config)# ip dhcp pool IT-NET
29061(dhcp-config)# network 10.10.10.0 255.255.255.0
29061(dhcp-config)# default-router 10.10.10.1
29061(dhcp-config)# dns-server 10.10.10.10
```

Explanation of commands

enable: this enable enter EXEC mode.

configure terminal: Enter global mode.

ip dhcp exclude-address 10.10.10.10: This tells dhcp pool to exclude that ip address.

ip dhcp pool IT-NET: This name of subnet you want pool address too.

network: Shows range of network and specify subnet mask

default-router: shows the gateway clients will use

dns-server: Sets domain name server

Step 5: Configure router interface

```
29061(config)# interface GigabitEthernet8/0
29061(config-if)# ip address 10.10.10.1 255.255.255.0
29061(config-if)# no shutdown
29061(config-if)# exit
```

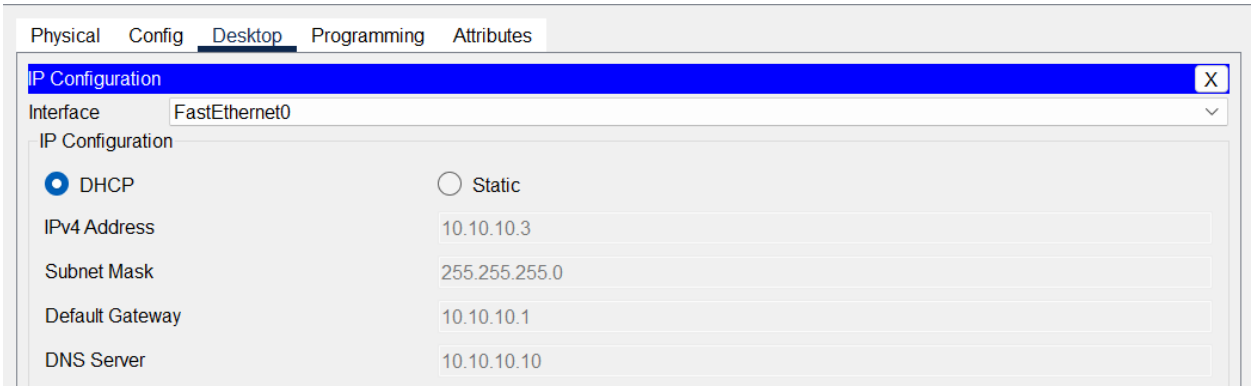
On Clients laptops to get IP address Dynamically

Step 1: Open laptop device

Step 2: Navigate to Desktop tab

Step 3: Select IP configuration

Step 4: Select DHCP



Verification by using the command prompt

Step 1: Open laptop device

Step 2: Navigate to Desktop tab

Step 3: Select command prompt

Step 4: type ipconfig or ipconfig /all

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: FE80::260:70FF:FEDB:B5A2
   IPv6 Address.....: ::
   IPv4 Address.....: 10.10.10.3
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: ::
                         10.10.10.1

Bluetooth Connection:

   Connection-specific DNS Suffix..:
   Link-local IPv6 Address.....: ::
   IPv6 Address.....: ::
   IPv4 Address.....: 0.0.0.0
   Subnet Mask.....: 0.0.0.0
   Default Gateway.....: ::
                         0.0.0.0
```

4. Routing between both LANs MASORO and GISHUSH

Step 1: Gave IP address to all subnets

Step 2: Assigned IP address on ISP

- Interface that face to MASORO-LAN

```
29061(config)# interface g9/0
29061(config-if)# ip address 100.100.100.2 255.255.255.0
29061(config-if)# no shutdown
```

- Interface that face to GISHUSHU-LAN

```
29061(config)# interface g8/0
29061(config-if)# ip address 200.200.200.2 255.255.255.0
29061(config-if)# no shutdown
29061(config-if)# exit
```

Step 3: Applied IP Route commands on GISHUSH-ROUTER

```
29061(config)# ip route 10.10.10.0 255.255.255.0 200.200.200.2
29061(config)# ip route 10.10.11.0 255.255.255.0 200.200.200.2
29061(config)# ip route 10.10.12.0 255.255.255.0 200.200.200.2
```

Step 4: Applied IP Route commands on MASORO-ROUTER

```
29061(config)# ip route 10.10.13.0 255.255.255.0 100.100.100.2
29061(config)# ip route 10.10.14.0 255.255.255.0 100.100.100.2
```

Step 3: Applied IP Route commands on ISP-ROUTER

```
29061(config)# ip route 10.10.10.0 255.255.255.0 100.100.100.1
29061(config)# ip route 10.10.11.0 255.255.255.0 100.100.100.1
29061(config)# ip route 10.10.12.0 255.255.255.0 100.100.100.1
29061(config)# ip route 10.10.13.0 255.255.255.0 200.200.200.1
29061(config)# ip route 10.10.14.0 255.255.255.0 200.200.200.1
```

ip route 10.10.10.0 255.255.255.0 200.200.200.2: This tells Gishushu router to use 200.200.200.2 port faces to ICP to send traffic to network has this IP 10.10.10.0 in Masoro LAN, and vice versa.

5. 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.

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

6. NAT (PAT & Static NAT) Configuration

Step 1: Define inside and Outside Interface

```
29061(config)# interface g9/0
29061(config-if)# ip nat outside
29061(config-if)# exit
29061(config)# interface range g8/0 - g6/0
29061(config-if-range)# ip nat inside
29061(config-if-range)# exit
```

i**p nat outside:** Marks the WAN interface as outiside

ip nat inside: Marks the LAN interfaces as inside for NAT

Step 2: Create an Access List to define inside Address

```
29061(config)# access-list 11 permit 10.10.10.0 0.0.0.255
29061(config)# access-list 11 permit 10.10.11.0 0.0.0.255
29061(config)# access-list 11 permit 10.10.12.0 0.0.0.255
29061(config)# access-list 11 deny host 10.10.10.10
```

Access-lists 11 permit 10.10.10.0 0.0.0255: Defines which private IPs are allowed to be translated (Masoro's LANs).

access-lists 11 deny 10.10.10.10 0.0.0255: Excludes the server IP from translation

Step 3: Apply NAT Overload (PAT)

```
29061(config)# ip nat inside source list 11 interface g9/0 overload
```

ip nat inside source list 11 interface g9/0 overload: Tells the router to use the public IP of the outside interface (g9/0) for all internal users

overload: Enable PAT (Port Address Translation) many private IPs share one public IP, using different port numbers

7. STP/RSTP and Port Security

```
29061-S4(config)# interface range FastEthernet0/2 - 6
29061-S4(config-if-range)# switchport mode access
29061-S4(config-if-range)# switchport access vlan 13
29061-S4(config-if-range)# switchport port-security
29061-S4(config-if-range)# switchport port-security maximum 1
29061-S4(config-if-range)# switchport port-security mac-address sticky
29061-S4(config-if-range)# switchport port-security violation shutdown
29061-S4(config-if-range)# exit
```

Explanation of used commands

Interface range FastEthernet0/2 – 6: This allows to apply configure same configuration on more than one port.

switchport mode access: forces port to work as access port.

switchport access vlan 13: Assign the port to vlan 13.

switchport port-security: Enables port security features on the port.

switchport port-security maximum 1: Limits each port to learn only one MAC addresss

switchport port-security violation shutdown: If violation occurs, the port goes into error.

switchport port-security mac-address sticky: Allows switch to store first connected MAC address in the running configuration

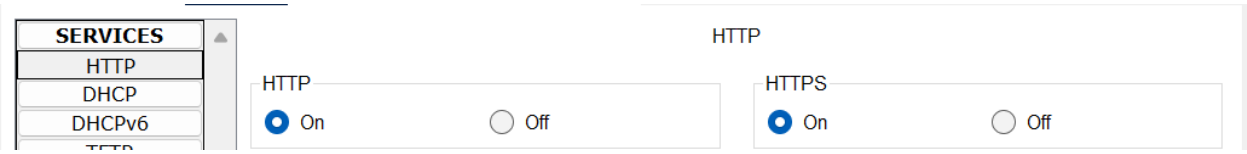
8. HTTP Web Server Setup

Step 1: Open Server

Step 2: Go to service tab

Step 3: Select HTTP on left side

Step 4: Enable on button on HTTP



9. Mail Server Configuration

Step 1: Open Server

Step 2: Go to service tab

Step 3: Select EMAIL on left side

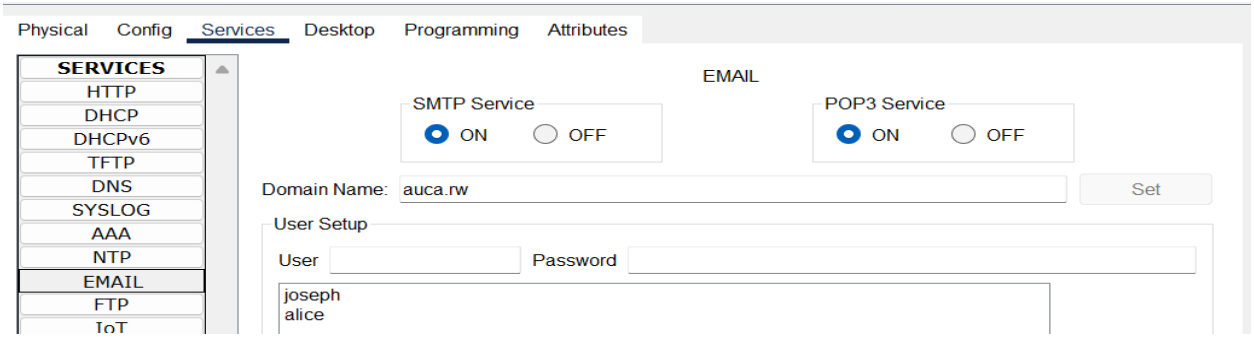
Step 4: Enable (on) button to open SMTP

Step 5: Enter Domain Name

Step 6: Click set button

Step 7: Create user by Entering username and password

Step 8: Click on Plus Button on right side



10. Verification and Troubleshooting

1.Device information

```
29061# show running-config
29061# show startup-config
```

2. Interface & IP Verification

```
29061# show ip interface brief
29061# show interfaces
```

3. Routing Verification

```
29061# show ip route
29061# show ip protocols
```

4.Nat Verification

```
29061# show ip nat translations
29061# show ip nat statistics
```

5. DHCP Verification

```
29061# show ip dhcp pool
29061# show ip dhcp binding
```

6. Access Control List (ACL) Verification

```
29061# show access-lists
29061# show running-config | include access-list
```

7.Vlan & Trunk Verification

```
29061-S4# show vlan brief
29061-S4# show interfaces trunk
29061-S4# show interfaces switchport
```

8. Port Security Verification

```
29061-S4# show port-security
29061-S4# show port-security interface f0/1
```

9.Connectivity Tests

```
29061# ping 10.10.10.1
29061# ping 10.10.13.1
29061# ping 100.100.100.2
```

10. Saving & Exiting

```
29061# copy running-config startup-config
29061# write
29061# write memory
29061# end
29061# exit
```

Explanation of used Commands

show-running-config: Displays current configuration

show startup-config: Display saved configuration

show ip interface brief: Gives summary of all interface

show interfaces: Displays detailed info about every interface

show ip route: Shows the routing table, including directly connected.

show protocols: Lists all interfaces with their assigned IPs and protocol status

show ip nat translations: Displays the active NAT translation

show ip nat statistics: Displays how many translations exist.

show ip dhcp pool: Shows all configured DHCP pools with details

show ip dhcp binding: Shows current IPs leased to clients

show access-lists: List all ACLs configure on the devices

show vlan brief: shows all vlan configure on the switch

show interface trunk: verifies interface are operating as trunks

show interfaces switchport: shows switchport mode

show port-security: This summarize port-security status for all interfaces.

chow port-security interface fa0/1: Display detailed port-security info for specific port

ping: used to test network reachability

copy running-config startup-config: Saves current configuration startup-config.

write: Saving configuration

write memory: Saving configuration

end: exiting any configuration mode.

exit: Exist the CLI

11. Achieved Outcomes

Connectivity Masoro ↔ Gishushu achieved.

Web server reachable on all clients.

Mail server operational across campuses.

Secure management via SSH.

VLANs, STP, and port security correctly configured.

12. Faced Challenges

In the **Gishushu LAN**, I initially struggled with assigning IP addresses to **WIFI-NET (10.10.14.0/24)** and **CABLE-NET (10.10.13.0/24)** because both networks were connected to the **same switch**, which in turn had only **one physical link to the router**. At first, I tried assigning only one IP address to the router port, but this did not allow both networks to communicate properly.

Later, I discovered the concept of **Router-on-a-Stick**, which allows a single physical router port to handle multiple IP subnets by creating **sub-interfaces**, each assigned to a specific VLAN. I configured the switch port connecting to the router in **trunk mode**, enabling it to carry traffic for multiple VLANs simultaneously. I then applied **NAT** on these sub-interfaces to allow the devices in both VLANs to access external networks.

Using this method, a single router port was able to serve multiple IP flows corresponding to their respective VLANs, resolving the connectivity issue and reinforcing my understanding of **inter-VLAN routing** and VLAN tagging.

I corrected by following these steps

Step 1: Configure sub-Interface

```
29061(config)# interface g8/0.13
29061(config-subif)# encapsulation dot1Q 13
29061(config-subif)# ip address 10.10.13.1 255.255.255.0
29061(config-subif)# ip nat inside
29061(config-subif)# exit
```

```
29061(config)# interface g8/0.14
29061(config-subif)# encapsulation dot1Q 14
29061(config-subif)# ip address 10.10.14.1 255.255.255.0
29061(config-subif)# ip nat inside
29061(config-subif)# exit
```

Explanation of used Commands

Interface g8/0.13: creates a sub-interface .13 on physical interface g8/0

Interface g8/0.14: creates a sub-interface .14 on physical interface g8/0

Encapsulation dot13Q: Assigns VLA 13 to this sub-interface using 802.1Q trunking.

Ip address 10.10.13.1 255.255.255.0: Assigns IP address for CABLE-NET (VLAN 13)

Ip nat inside: Marks sub-interface as inside for NAT

exit: Exit from sub-interface

Step 2: Switch port Trunking

```
29061-S4(config)# interface g0/1
29061-S4(config-if)# switchport mode trunk
29061-S4(config-if)# switchport trunk allowed vlan 13,14
```

Explanation of use commands

Interface g0/1: entering the port connected to router

switchport mode trunk: Configure the switch port connectivity to router as trunk.

switchport trunk allowed vlan 13,14: Restrict the trunk to only VLAN 13 and VLAN 14

Summary

During the activity, the following tasks were successfully completed:

1. **IP Addressing & Subnetting**:
    a. Masoro LAN: IT-NET (10.10.10.0/24), HR-NET (10.10.11.0/24), FINANCE-NET (10.10.12.0/24)
    b. Gishushu LAN: CABLE-NET (10.10.13.0/24), WIFI-NET (10.10.14.0/24)
    c. All subnets configured with mask 255.255.255.0, DNS server 10.10.10.10.

2. **DHCP Configuration**:
    a. Created pools for each subnet.
    b. Excluded critical IPs (like the DNS server).
    c. Configured default gateways and DNS settings for automated client IP assignment.

3. **Routing**: Static routing enabled on both Masoro and Gishushu routers to ensure inter-subnet communication and internet access via the ISP.

4. **VLANs & Trunking**:
    a. Configured VLANs on the S4 switch.
    b. Access ports assigned to appropriate VLANs.

   c. Trunk links set to carry multiple VLANs between switch and router.

5. **Port Security**:
   a. Applied to all access ports, limiting the number of MAC addresses per port.
   b. Sticky MAC addresses enabled and violation action set to shutdown.

6. **SSH Configuration**:
   a. Local users created and encrypted passwords configured.
   b. RSA keys generated, SSH version 2 enabled.
   c. VTY lines configured for SSH login only.

7. Used commands like show ip interface brief, show running-config, show vlan brief, show port-security, show ip nat translations, and ping to confirm network connectivity, security, and proper configuration.

END.