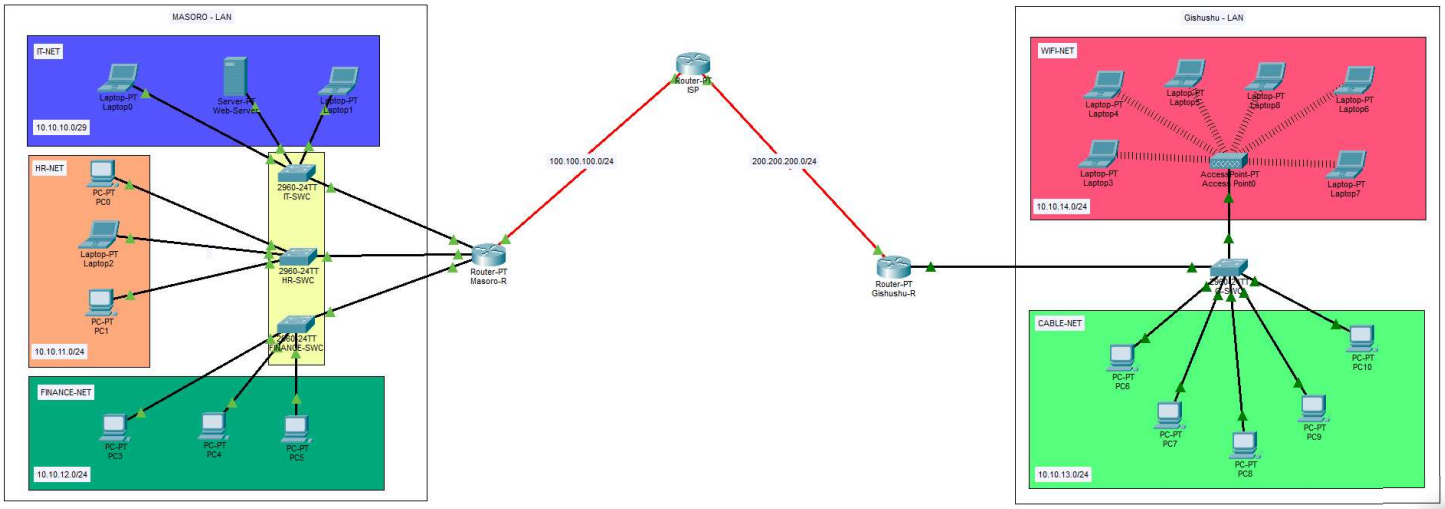
Assignment#1

Start Assignment

- Due Sep 28 by 11:59pm
- Points 100
- Submitting a file upload
- Available Sep 14 at 12am - Sep 29 at 11:59pm



NETWORK CONFIGURATION LAB

Objective

The goal of this assignment is to design, configure, and test a network topology for a simulated university environment using Cisco Packet Tracer. You will implement IP addressing, device configurations, secure remote access, DHCP services, routing protocols, NAT, security features, and server setups to enable seamless connectivity between the Masoro and Gishushu LANs at AUCA. This hands-on exercise will strengthen your skills in network setup and troubleshooting, preparing you for the in-class assessment.

Required Resources

- **Software**: Cisco Packet Tracer (latest version recommended).
- **Reference Materials**: Review the videos in the Canvas LMS Pages module: "3. Packet Tracer Labs [v1] (https://canvas.instructure.com/courses/12757746/pages/3-packet-tracer-labs-v1) ", "4. Packet Tracer Labs [v2] (https://canvas.instructure.com/courses/12757746/pages/4-packet-tracer-labs-v2) ", and "5. Packet Tracer Labs [v3] (https://canvas.instructure.com/courses/12757746/pages/5-packet-tracer-labs-v3) " for guidance on configurations.
- **Topology Diagram**: Use the provided topology file "AUCA Masoro+Gishushu LANs.png" as the base. This includes two campuses (Masoro and Gishushu) connected via routers, with switches,

PCs, laptops, servers, and other devices. Redesign it as needed to incorporate department separations and additional requirements.

Instructions

1. Network Topology Design

- Redesign the provided topology to include clear department separations (e.g., based on functions like administration, academics, or IT).
- Assign ip addresses accodingly.
- Draw or update the topology diagram clearly, labeling all devices, connections, subnets, and interfaces. Ensure it shows interconnections between Masoro and Gishushu campuses.

2. IP Addressing Scheme

- Assign appropriate subnet masks based on your subnetting design.
- Configure IP addresses for all devices, including PCs, laptops, servers, switches, and routers.
- Use the last valid IP address in each subnet as the default gateway (typically on the router interface).
- Assign static IP addresses to all servers for reliability.
- Configure PCs and laptops to obtain IP addresses dynamically via DHCP.

3. Device Connections and Interface Types

- Connect servers using FastEthernet interfaces for standard performance.
- Interconnect switches with GigabitEthernet interfaces for higher bandwidth.
- Ensure proper cabling: Use straight-through cables for unlike devices (e.g., PC to switch) and crossover cables for like devices where necessary (though Packet Tracer auto-detects in many cases).
- Test connectivity across all devices using the ping command to verify basic communication.

4. Hostname Configuration

- Set the router hostname as <StudentID>-R (e.g., if your Student ID is 12345, use "12345-R").
- Set each switch hostname as <StudentID>-S (e.g., "12345-S1" for the first switch, incrementing as needed).
- Replace <StudentID> with your actual Student ID to ensure unique identification.

5. Remote Access Configuration (Telnet and SSH)

- Enable and configure both Telnet and SSH on all switches and routers for secure management.
- Set the username and password/secret to your Student ID (e.g., username: 12345, password: 12345).
- Configure a domain name using the first letter of your first name followed by your full last name, with the .rw top-level domain (e.g., for Joshua Iradukunda, use "jiradukunda.rw").
- Generate crypto keys for SSH and enforce SSH as the preferred method over Telnet for security.

6. DHCP Configuration

- Configure DHCP pools on the routers for each campus (Masoro and Gishushu) to automatically assign IP addresses to PCs and laptops.
- Align DHCP settings with your subnet design, including network address, subnet mask, default gateway, and DNS server (use a simulated DNS if needed).
- Exclude server IP addresses from DHCP pools to ensure they remain static.

7. Additional Configuration Requirements

Based on the provided topology and videos, incorporate these advanced features to ensure full functionality:

- **NAT (PAT)**: Implement Network Address Translation (PAT) on each campus router to translate local (private) IP addresses to public ones for internet access. Define inside and outside interfaces, and create access lists if required for traffic control.
- **Routing**:
  - Set up static routes for specific networks.
  - Configure default routes for unknown destinations.
  - Enable EIGRP (Enhanced Interior Gateway Routing Protocol) as the dynamic routing protocol across routers for automatic route discovery and redundancy.
- **STP/RSTP and Port Security**:
  - Enable Spanning Tree Protocol (STP) or Rapid STP (RSTP) on switches to prevent loops and ensure network stability.
  - Configure port security on switch ports connected to end devices (e.g., limit MAC addresses, enable sticky learning, and set violation actions to shutdown).
- **HTTP Web Server**:
  - Set up an HTTP web server on the Masoro LAN with a static IP.
  - Use static NAT (one-to-one mapping) to make the web server accessible publicly from outside the network.
  - Test access by loading a simple webpage from devices on the Gishushu LAN or simulated internet.
- **Mail Server**:
  - Configure a mail server (using Packet Tracer's built-in server device) to allow all users across both LANs to send and receive emails.
  - Set up email accounts, SMTP/POP3 protocols, and test email exchange between users on different campuses.

8. Verification and Troubleshooting

- Use key show commands to confirm configurations, such as:
  - show ip interface brief (for IP assignments).
  - show running-config (for full config review).
  - show vlan brief (if VLANs are implemented).
  - show ip dhcp binding or show dhcp leases (for DHCP assignments).

  - show ip nat translations (for NAT verification).
  - show ip route (for routing tables).
  - show spanning-tree (for STP status).
  - show port-security (for port security settings).
- Interpret outputs to troubleshoot issues like connectivity failures, routing errors, or security violations.
- Ensure end-to-end communication: Ping between LANs, access the web server publicly, and send/receive emails.

9. Saving Configuration

- Save changes on all devices with the copy running-config startup-config command (or wr shortcut).
- Reload routers and switches to test if configurations persist after reboot.
- Verify post-reload using show commands to confirm no loss of settings.

Best Practices

- Take screenshots or export outputs for each major step (e.g., subnetting, configurations, verifications) to document your work.
- Note any challenges encountered (e.g., routing convergence issues) and how you resolved them—this will aid in-class discussions.
- Practice the setup multiple times to build confidence and speed.
- Simulate real-world scenarios, such as device failures, to test redundancy.

Submission

Submit your work as a well-documented PDF document. The PDF must follow this structure to ensure clarity, organization, and completeness:

- **Cover Page**: Include the assignment title, your full name, Student ID, course name, submission date, and instructor's name.
- **Table of Contents**: List all sections and subsections with page numbers for easy navigation.
- **Table of Figures**: Enumerate all screenshots, diagrams, and tables with captions and page references (e.g., Figure 1: Updated Network Topology Diagram).
- **Table of All Used Commands**: Provide a comprehensive table listing every Cisco command used in the configuration, including the device it was applied to, a brief description of its purpose, and the full command syntax.
- **Executive Summary**: A concise overview (1/2 to 1 page) summarizing the assignment objectives, key configurations implemented, and overall outcomes.
- **Achieved Outcomes**: Detail what was successfully accomplished, such as seamless inter-LAN communication, secure remote access, and server functionality. Highlight how the setup meets the requirements and any notable achievements (e.g., efficient subnetting or robust security).
- **Body**: The main content, organized by configuration steps. Include screenshots of all configurations, verifications, and tests. Each screenshot must be accompanied by a detailed description explaining

what it shows, the commands used, and why it was configured that way. Structure this section to mirror the Instructions above (e.g., subsections for Topology Design, IP Addressing, etc.).

- **Conclusion**: Summarize key learnings, challenges faced, solutions applied, and how this assignment prepares you for real-world network administration. Suggest any potential improvements to the setup.

Submit the PDF via Canvas LMS by the due date. Additionally, include the Packet Tracer file **(.pkt)** as a separate attachment for verification. Late submissions will not be accepted.