Project 1:

Problem Statement: Multi-Branch Office Network Setup

Objective:
Design and configure a network for a company with two branches in different cities, connected via a WAN link. Implement **subnetting**, **routing**, and **Port Address Translation (PAT)** to ensure efficient communication between branches and secure access to the internet.

Scenario:

A company operates from two branches: **Head Office (HO)** and **Branch Office (BO)**. Each branch has multiple departments that need to communicate internally and access the internet via a shared public IP. The following requirements must be met:

1. **Subnetting** must be used to allocate IP addresses efficiently for departments within each branch.
2. **Routing** must be configured to enable communication between the two branches over the WAN link.
3. **Port Address Translation (PAT)** must be implemented to provide internet access to all devices using a single public IP.
4. The design must ensure scalability for future department additions.

Deliverables:

1. A fully functional network topology in Cisco Packet Tracer.
2. Configuration files for HO and BO routers, including:
    - Subnetting details for each department.
    - Static routing setup.
    - PAT configuration for internet access.
3. Verification steps to test communication:
    - Ping between devices in different branches.
    - Internet access from any PC.

Project 2:

Problem Statement: Centralized File Sharing System for a Multi-Department Office

Objective:
Design a network to implement a centralized **FTP file-sharing system** between departments in a single office. The network should use **DHCP** for dynamic IP address allocation and **routing** to ensure efficient communication between departments.

Scenario:

A company has three departments: **HR**, **IT**, and **Finance**, located in separate subnets. The IT department hosts an FTP server to store and share files with other departments. DHCP is used for dynamic IP allocation, and routing is configured to enable communication between departments.

The following requirements must be met:

1. **FTP Server:** Centralized file-sharing server in the IT department, accessible by all departments.
2. **DHCP Server:** Dynamically assign IP addresses to all devices in the network.
3. **Routing:** Enable communication between departments using static routes.
4. Ensure proper network segmentation for security and scalability.

Deliverables:

1. A complete network topology in Cisco Packet Tracer.
2. Configuration files for:
    - DHCP Server: IP pool and default gateway setup.
    - FTP Server: Shared folder setup with user authentication.
    - Router: Static routes between subnets.
3. Verification Steps:
    - Test DHCP by checking dynamically assigned IPs on PCs.
    - Test FTP by transferring files between the server and PCs in each department.
    - Verify inter-department communication using ping and traceroute commands.

Project 3:

Problem Statement: Smart Office Network with Inter-VLAN Routing, STP, and Access Control

Objective:
Design and configure a smart office network using **Inter-VLAN Routing** and **Spanning Tree Protocol (STP)** to provide secure and reliable communication between VLANs. Additionally, implement **Access Control Lists (ACLs)** to restrict server access to authorized devices only.

Scenario:

The office has an automated network with IoT devices, workstations, and administrative servers. To ensure proper functionality and security:

1. **VLANs** segregate devices into logical groups.
2. **Inter-VLAN Routing** enables communication between these groups.
3. **STP** ensures redundancy and prevents loops while electing a switch connected to the administrative servers as the **root bridge**.
4. **Access Control Lists (ACLs)** restrict access to the administrative servers, allowing only authorized devices.

Deliverables:

1. **Network Topology:**
    - Visual representation of the VLANs, switches, and router.
    - Clearly indicate redundant links and the root bridge.
2. **Configuration Files:**
    - **Switches:** VLAN and STP settings.
    - **Router:** Sub-interfaces for inter-VLAN routing and ACL rules.
3. **Test Scenarios:**
    - **STP:**
        - Disable a redundant link to observe failover and verify S1 remains the root bridge.
    - **ACL:**
        - Test access to the administrative servers:
            - **PC1** and **IoT1** should successfully access the servers.
            - Other devices should be denied access.
    - **Inter-VLAN Communication:** Verify communication between VLANs using ping or traceroute.

Project 4:

Problem Statement: Dynamic Network with DNS and DHCP for a Corporate Environment

Objective:
Design and configure a corporate network with a **DNS server** for centralized domain name resolution, **DHCP server** for automatic IP allocation, and **Dynamic Routing** to ensure seamless communication across multiple branches.

Scenario:

A multinational company has two branch offices and one head office. The network should include:

1. A **DNS server** to resolve domain names for internal and external services.
2. A **DHCP server** to dynamically assign IP addresses to devices in each branch.
3. **Dynamic Routing** to ensure automatic path adjustments between branches for reliable communication.

Application Requirements:

- Employees across all branches need to access shared resources (e.g., an internal website hosted on a DNS server).
- DNS resolution is required for both internal domains (e.g., `intranet.company.com`) and external websites (e.g., `example.com`).
- IP addresses for all devices are managed dynamically via DHCP.
- Dynamic routing ensures scalability and resilience for the expanding branch network.

Deliverables:

1. **Network Topology:**
   - A comprehensive diagram in Cisco Packet Tracer showing all connections, devices, and subnet assignments.
2. **Configuration Files:**
   - DNS server: Internal domain and forwarders for external domain resolution.
   - DHCP server: IP address pool and relay configurations.
   - Routers: OSPF configuration.
3. **Test Results:**
   - Ping and resolve internal (`intranet.company.com`) and external (`example.com`) domains from all PCs.
   - Test routing failover by disabling one WAN link and observing traffic redirection.

Project 5:

Problem Statement: Implementing a Time Synchronization Network Using a Time Server

Objective:
Design and configure a network where all devices synchronize their system time using a **Network Time Protocol (NTP) Server**. This ensures accurate time settings across the network, critical for logging, scheduling, and security auditing.

Scenario:

A company requires all network devices to have synchronized time for proper log correlation, scheduled tasks, and secure communications. The company's network includes a centralized **NTP server** to provide accurate time to all devices. The configuration must also include **DHCP for automatic IP address assignment** and **Static Routing** to connect multiple subnets.

Deliverables:

1. **Network Topology:**
   - A diagram showing the placement of the NTP server, DHCP server, router, and PCs in Cisco Packet Tracer.
2. **Configuration Files:**
   - NTP Server: Time synchronization settings.
   - DHCP Server: IP address pool and scope configuration.
   - Router: Static route configuration.
3. **Verification Tests:**
   - Verify DHCP-assigned IP addresses for PCs.
   - Test time synchronization by checking the system time on all devices and comparing it to the NTP server.
   - Verify inter-subnet communication using ping and traceroute.

Project 6:

Problem Statement: Secure and Scalable Bank Network

Objective:
Design and implement a secure, scalable bank network in **Cisco Packet Tracer** with the following requirements:

1. Four branch offices connected via routers to the central head office.
2. A centralized server at the head office that hosts the **Bank Management System (BMS)** where clients can create accounts.
3. Ensure reliable communication between branches and head office using **Dynamic Routing (OSPF)**.
4. Provide **DHCP services** for client devices in each branch.
5. Secure the network using **Access Control Lists (ACLs)** to restrict access to the centralized server.

Scenario:

A bank operates four branches in different cities. Each branch has its own network with workstations for clients to access the **Bank Management System (BMS)** hosted on a centralized server at the head office.

- The branches need dynamic IP management to handle client devices efficiently.
- The routers in the network must support **dynamic routing** to adapt to changes and ensure uninterrupted communication between branches and the head office.
- Security policies must ensure only authorized devices can access the centralized server.

Deliverables:

1. **Network Topology:**
    - A diagram in Cisco Packet Tracer showing all devices, subnets, and connections.
2. **Configuration Files:**
    - Router configurations for OSPF, DHCP, and ACLs.
    - Server configuration details.
3. **Testing Logs:**
    - Successful communication between branches and head office.
    - ACL testing to confirm restricted access.

Project 7:

Problem Statement: Scalable Hotel Management Network Design

Objective:

Create a secure, scalable, and functional network for a hotel using **Cisco Packet Tracer**. The network should ensure departmental isolation, controlled data sharing, and efficient resource management while being capable of accommodating future growth. This network will simulate real-life hotel operations and address key IT challenges.

Scenario:

A large hotel with multiple departments—**Reception**, **Finance**, **Restaurant**, and **Sales**—requires a robust network design to handle its daily operations securely. Each department has distinct requirements and handles critical functions as follows:

1. **Reception**: Manages guest check-ins, reservations, and communication with the finance department for billing. Requires direct communication with the finance department while being isolated from others.
2. **Finance**: Handles sensitive financial data such as payroll, invoices, and transactions. No department except reception should have access to this data.
3. **Restaurant**: Manages food orders, inventory, and guest room service. Operates independently from finance but shares occasional data with sales for promotions.
4. **Sales**: Focuses on marketing campaigns, online bookings, and promotions. Can communicate with the restaurant but not with finance.

The network must be designed to:

- Ensure **secure inter-departmental communication** using **VLANs**, **Access Control Lists (ACLs)**, and **Inter-VLAN Routing**.
- Enable centralized control for efficient management and troubleshooting.
- Provide **redundancy** to maintain operations during device failures.
- Ensure scalability for future expansion, including adding new departments or branches.

Additional Features:

1. **Centralized Server:**
   - Deploy a centralized server for storing shared files like promotional materials, daily sales reports, and customer feedback forms.
   - Host the server in a separate VLAN (e.g., **VLAN 50**, `192.168.50.0/24`) with access controlled via ACLs.
2. **Guest Wi-Fi Network:**
   - Configure a **guest VLAN (VLAN 60)** to provide internet-only access for hotel guests.
   - Isolate this VLAN from all internal networks.

Deliverables:

1. **Network Topology Diagram:**
   - Include all devices, VLANs, IP addresses, and interconnections.
2. **Configuration Files:**
   - Provide switch and router configurations for VLANs, routing, DHCP, and ACLs.
3. **Test Results:**
   - Screenshots or logs showing successful implementation of VLANs, inter-VLAN routing, STP redundancy, and ACL enforcement.

Project 8:

Problem Statement: Inter-Campus Mail Server Network Design

Objective:
Design and implement a secure and efficient inter-campus mail server system in **Cisco Packet Tracer**. The system will use the **SMTP protocol** to send emails and **POP3/IMAP protocols** to retrieve emails. Each campus will have its local mail server connected to a centralized mail server at the head office, ensuring reliable communication between campuses.

Scenario:
An organization operates across three campuses: **Main Campus**, **North Campus**, and **South Campus**, with the following requirements:

1. **Mail Server Setup:**
   - Each campus must have a **local mail server** to handle intra-campus email communication.
   - A **centralized mail server** at the Main Campus will manage inter-campus communication.
2. **Network Infrastructure:**
   - The campuses are connected via **routers** using dynamic routing protocols (OSPF/EIGRP).
   - Each campus network is segmented into departments using **VLANs** to ensure data isolation.
3. **Email Services:**
   - Employees within a campus can send emails to one another through the local mail server.
   - Emails to other campuses will be routed through the centralized mail server.
4. **Security:**
   - Implement **Access Control Lists (ACLs)** to restrict access to the centralized mail server to only mail servers from other campuses.
   - Ensure inter-campus traffic is encrypted using **IPSec (if required)** for secure email transmission.
5. **Scalability:**
   - The network should support the addition of new campuses or departments without requiring major reconfiguration.

Features to Implement in Cisco Packet Tracer:

1. **Mail Server Configuration:**
   - Enable **SMTP** and **POP3/IMAP** services on each server.
   - Configure user accounts for each department.
2. **Routing Protocols:**
   - Use OSPF for inter-campus routing to ensure efficient path selection.
3. **VLAN Configuration:**
   - Assign VLANs for each department within a campus.
   - Use trunking to connect access switches to core switches.

4. **Inter-Campus Communication:**
    - Test email delivery between campuses by simulating user accounts sending emails.
5. **Security:**
    - Implement ACLs to permit only SMTP and POP3/IMAP traffic between mail servers.
    - Block unauthorized devices or traffic using ACLs on routers.
6. **Testing and Verification:**
    - Verify VLAN segmentation using ping between devices in different VLANs.
    - Test email functionality by sending emails within a campus and between campuses.
    - Verify ACLs by attempting unauthorized access to the centralized mail server.

Deliverables:

1. **Network Topology Diagram:**
    - Visual representation of the three campuses, their mail servers, VLANs, and interconnections.
2. **Configuration Files:**
    - Switch and router configurations for VLANs, routing, DHCP, and ACLs.
    - Mail server settings for SMTP and POP3/IMAP protocols.
3. **Test Results:**
    - Screenshots or logs showing successful email transmission within and between campuses.