Project 1: University Network Design & Implementation

Problem Statement:

Design and implement a fully functional campus-wide network for a university that spans multiple academic buildings and administrative blocks. The network should support segmentation, inter-department routing, essential services, and internet access for all authorised users.

Objectives:

- Build a real-world campus network using a hierarchical (three-tier) design.
- Implement VLAN-based segmentation for departments and labs.
- Configure inter-VLAN routing using Layer-3 switches or routers.
- Deploy DHCP, DNS, Web, FTP, and Email servers.
- Implement OSPF for internal routing and NAT for internet access.
- Provide redundancy through STP.
- Enforce access control for sensitive resources.

Scenario:

The University consists of multiple academic departments (like CSE, ECE, Mechanical, Civil etc.), Administration and Library. Requirements:

1. **Segmentation** using VLANs (departments, servers).
2. **High-speed backbone** through distribution and core layers.
3. **Server farm** with DNS, DHCP, Web (intranet), Email, FTP, and NTP services.
4. **Campus backbone routing** using OSPF.
5. **Internet access** through an edge router using NAT/PAT.
6. **Redundancy** with STP in switches.
7. **Basic ACLs** to protect administration and server VLANs.

Deliverables:

1. Network topology (along with ***.pkt*** file) of the campus network, giving a clear visibility of different segments, links and devices (both end and intermediate).
2. Configuration files for
    a) VLAN assignments.
    b) OSPF + NAT configuration for Internet access.
    c) Server configurations (DHCP, DNS, Web, Mail, FTP).
    d) Ether Channel and STP configuration for redundancy.
    e) ACLs restricting unauthorized access.
3. Testing documentation (ping test, DNS resolution, web access, mail access).

Project 2: Inter-Campus Mail Server Network Using SMTP/POP3/IMAP

Problem Statement:

Design a multi-campus email communication system utilising local mail servers at each campus, with centralised routing.

Objectives:

- Deploy SMTP + POP3/IMAP mail servers.
- Implement OSPF-based routing between campuses.
- Secure centralised server with ACLs.

Scenario:

Three campuses—Main, North, South—need internal and cross-campus email. Requirements:

1. Local mail servers per campus.
2. Centralised mail relay at the Main campus.
3. VLAN-based segmentation across each campus.
4. ACLs allowing only mail traffic between campuses.

Deliverables:

1. Network topology (along with ***.pkt*** file) of the multi-campus network, giving a clear visibility of different segments, links and devices (both end and intermediate).
2. Configuration files for
    a) VLANs
    b) OSPF routing
    c) SMTP/POP3/IMAP implementation.
    d) ACL for permitted ports.
3. Test logs for email exchange.

Project 3: Centralised File-Sharing System with DHCP & FTP Server

Problem Statement:

Develop a centralised file-sharing system using an FTP server hosted within the IT Department. All departments should receive IPs dynamically from a DHCP server, and communication must be enabled across separate subnets.

Objectives:

- Deploy FTP server for centralised file access.
- Configure DHCP to automatically assign IP addresses.
- Enable inter-department communication using static routing.
- Implement secure and organised departmental segmentation.

Scenario:

A single-office organisation has HR, IT, and Finance departments located in different subnets. The IT department runs an FTP server for document sharing. Requirements:

1. DHCP server providing IPs to all PCs.
2. Static routing between departmental subnets.
3. FTP server with authentication for file transfers.
4. Logical departmental isolation.

Deliverables:

1. Network topology (along with ***.pkt*** file) of the organisation, giving a clear visibility of different departments, connections and devices (both end and intermediate).
2. Configuration files for
    a) DHCP pool creation and assignment.
    b) FTP setup with user accounts.
3. Verification: DHCP-assigned IP, file upload/download test.

Project 4: Multi-Branch Corporate Office Network.

Problem Statement:

Design and configure a multi-branch corporate network where a Head Office (HO) and Branch Office (BO) are interconnected through a WAN link. The network must support internal communication, WAN routing, and Internet access using Port Address Translation (PAT).

Objectives:

- Implement efficient subnetting for both BO and HO networks.
- Enable branch-to-branch and branch-to-HO communication using static routing.
- Provide Internet access through PAT using a shared public IP.
- Build a scalable network that can grow with additional departments.

Scenario:

A company operates two major branches. Each branch has multiple departments requiring internal connectivity and unified communication across the WAN. The HO hosts the main Internet gateway. Requirements:

1. Subnetting based on individual BO and HO host numbers.
2. WAN routing between HO and BO.
3. PAT on HO router for shared Internet access.
4. Scalability for future departments.

Deliverables:

1. Network topology (along with ***.pkt*** file) of the organisation, giving a clear visibility of different departments, connections and devices (both end and intermediate).
2. Configuration files for
    a) Router configuration (subnetting, interfaces, and static routes).
    b) PAT configuration on HO router.
3. Connectivity testing: ping across branches + Internet simulation.

Project 5: Hotel Management Network with VLANs, ACLs & Guest Wi-Fi

Problem Statement:

Develop a network for a large hotel with multiple departments and a dedicated guest Wi-Fi VLAN.

Objectives:

- Use VLANs to isolate hotel departments.
- Implement ACL-controlled inter-department communication.
- Set up a central server for reports and shared data.
- Provide secure guest Internet-only through Wi-Fi.

Scenario:

Departments include Reception, Finance, Restaurant, and Sales. Requirements:

1. VLAN segmentation per department.
2. ACL control for Finance and Server VLANs.
3. Guest Wi-Fi with Internet-only access.
4. Central file server accessible based on department rules.

Deliverables:

1. VLAN-based network topology (along with ***.pkt*** file) of the hotel network, giving a clear visibility of different departments, connections and devices (both end and intermediate).
2. Configuration files for
   a) ACL meant for authorised/unauthorised access.
   b) DHCP and routing.
3. Test logs for department-wise communication, guest Wi-Fi internet access.

Project 6: Industrial Networking with Sensors (Manufacturing)

Problem Statement:

Design and configure a networking system that supports industrial sensors, PLCs, edge gateways, SCADA/OT services, and enterprise IT — demonstrating safe, reliable, and secure data flow from the factory floor to enterprise systems.

Objectives:

- Understand differences between IT and OT (Operational Technology) networking.
- Integrate sensors and PLCs into a simulated network using Packet Tracer's IoT features and standard network devices.
- Simulate data collection, edge processing, and forwarding for analytics and predictive maintenance.
- Demonstrate OT security measures and safe segmentation between production and enterprise networks.

Scenario:

A small-to-mid-sized manufacturing plant produces electromechanical components. The plant has:

- ❖ Production Line A (assembly) with sensors: proximity sensors, temperature sensors, vibration sensors, and actuators controlled by PLCs.
- ❖ Production Line B (testing) with higher-frequency vibration sensors and cameras for visual inspection.
- ❖ Central Control Room hosting SCADA/HMI, PLC programming workstation, and an OPC/MQTT gateway for telemetry to the enterprise.
- ❖ Quality & Analytics Team requiring access to processed telemetry and historical logs.
- ❖ Enterprise Network (finance, HR, management) separated from OT for compliance.

Requirements:

1. Subnetting for different departments based on the number of industrial sensors and computing units.
2. DHCP server-based central control room.
3. DAT configured routing between the industry and enterprise network.
4. ACL-based Quality and & Analytics team for cloud access.

Deliverables:

1 Network topology (along with ***.pkt*** file) of the industry, giving a clear visibility of different departments, connections and devices (both end and intermediate).

2 DHCP pool creation and assignment.

3 ACL list configuration.

4 DAT-based routing.

5 Test results for inside and outside industry communication.

Project 7: Smart City Traffic Surveillance Network

Problem statement:

Design and implement a centralised vehicle traffic monitoring cum controlling network for a city that comprises different traffic zones. The network should support segmentation, inter-zonal routing, and controlled traffic forwarding in different routes, along with alerting the vehicle owners through proper message communication.

Objectives:

- Deploy IP-based surveillance cameras across multiple city zones.
- Implement a centralised monitoring and storage server.
- Configure DHCP for automatic IP assignment to both end and intermediary devices.
- Enable communication between different city zones using routing.
- Ensure secure, scalable, and organised network segmentation.

Scenario:

A smart city is divided into four zones: **East Zone, West Zone, North Zone and South Zone,** each equipped with IP-based traffic surveillance cameras connected to a local network. All surveillance data is transmitted to a **Central Monitoring Centre (CMC),** where traffic authorities monitor live feeds and store recordings. Based on the traffic scenario, the appropriate message is also communicated to the vehicle owner through the public network for route modification or a penalty against traffic violation. Requirements:

1. Central monitoring server for traffic surveillance
2. DHCP server to assign IP addresses dynamically
3. Inter-zone communication via static routing
4. Smart IP-based cameras for traffic information transmission
5. Secure and logical segmentation of city zones
6. Static NAT configured router for the connection between CMC and the vehicle owner

Deliverables:

1. Network topology (along with ***.pkt*** file) of zones and CMC, giving a clear visibility of connectivity, routers, switches, IP-based cameras, and servers.
2. DHCP pool configuration for all city zones.
3. Central monitoring server configuration.
4. Verification of message communication between
    a) CMC and IP-based cameras
    b) CMC and vehicle owner

Project 8: Enterprise LAN/WAN with Subnetting, Supernetting, DNS, DHCP.

Problem Statement:

Design and implement a small enterprise network using IP subnetting (VLSM), a supernetting example for route aggregation, DHCP for host addressing, DNS for name resolution, and routing (static + OSPF) between sites. Demonstrate configuration, testing, and documentation.

Objectives:

- Design IP addressing using VLSM for multiple VLANs/departments.
- Create an aggregated (supernet) route advertisement.
- Configure DHCP server(s) to dynamically assign addresses per subnet.
- Configure authoritative DNS (BIND) and reverse DNS.
- Configure routing on routers: static and OSPF.

Scenario:

Multi-Site Organisation (Routing + Subnetting + Supernetting). Multi-VLAN Enterprise Network (Subnetting + DHCP + DNS). You are designing the network of a multi-site enterprise with headquarters and branch offices. Requirements:

At Headquarters (HQ):

- Multiple VLANs: Servers, Admin, Sales, IoT
- VLSM-based subnetting
- DHCP server for all VLANs
- DNS server for internal name resolution
- L3 switch doing inter-VLAN routing
- HQ router connecting to branches

At Branch Offices (Branch 1 & Branch 2):

Each branch has its own subnet(s)

- Routers connect back to HQ
- Routing is done using OSPF
- Branch subnets can be summarised (supernetting) toward HQ

Deliverables:

1. Network topology (along with ***.pkt*** file) of the enterprise network, giving a clear visibility of HQ and branch offices, connections and devices (both end and intermediate)
2. Device configuration files: Routers, switches, DHCP server, DNS server
3. Routing protocol configuration (OSPF, static routes).
4. Testing & Verification Report: DNS queries, OSPF routing tables, and connectivity check through ***ping*** command.