COMPUTER NETWORKS

SEMESTER PROJECT - FYP 1 REPORT

AIR UNIVERSITY

AIR UNIVERSITY

Submitted By:

MUHAMMAD HASEEB	242292
AHMED SALEEM	242348
SYED AHTESHAM	242364

Submitted To:

MISS MAILA ZAHRA

VLSM Network Design

Introduction

For our Computer Networks semester project, we aim to design and implement a complete enterprise-level network for SecureBooks Inc., a rapidly expanding company that operates a centralized Main Office, a dedicated DMZ (Demilitarized Zone) hosting the company's Web and Database Servers, and a separate Branch Office that must securely connect to the Main Office.

We will use Cisco Packet Tracer to build the full infrastructure from scratch. The entire design will operate under a strict constraint: we must use only one IP block (172.16.10.0/24) for all offices, servers, and WAN links. To achieve this, we will apply VLSM subnetting, implement mixed routing protocols (RIP v2, Static, Default Routing), and configure ACL-based traffic control to enforce strict security policies.

The core idea behind our project is to simulate a genuine corporate environment where multiple network segments must communicate effectively while ensuring the confidentiality and integrity of sensitive resources—specifically, ensuring the Branch Office can access only the Web Server, whereas the Database Server remains fully restricted to Branch users.

This report outlines the complete planning phase, including background research, methodology, proposed flow, future improvements, and expected outcomes.

2. Literature Review

Beforebeginningthe implementation, we studied several networking concepts and industry standards to support the design of our project.

VLSM & IP Address Management

Research on enterprise subnetting practices highlights the importance of **Variable Length Subnet Masking** to efficiently divide large IP blocks into optimized sub-blocks.
VLSM is widely used in organizational networks to:

- Avoid IP wastage
- Create subnets sized according to host requirements
- Enhance routing efficiency through hierarchical addressing structures

We will apply VLSM to segment the 172.16.10.0/24 block into four subnets based on host density.

Routing Protocols in Enterprise Networks

Routing is central to multi-network communication.
Literature shows three major routing approaches:

- **Dynamic Routing (RIP v2)**
  RIP is commonly used in small and medium networks for its simplicity and automatic route sharing.
- **Static Routing**
  Ideal for sensitive networks (e.g., DMZ) where traffic paths must remain predictable and controlled.
- **Default Routing**
  Allows edge routers (like Branch Office routers) to forward unknown networks to a central router.

Enterprise networks often use a combination of routing types for stability, scalability, and administrative control, which aligns directly with our project’s requirements.

DMZ-Based Security Architecture

Academic and industry literature emphasizes that a **DMZ** isolates publicly accessible services (Web Server) from critical internal systems (Database Server).
It acts as a controlled "buffer zone" between the internal network and external access points.
Access to the Database Server is normally restricted to trusted internal networks only, making it ideal for enforcing strict ACL rules in our project.

ACLs and Network Access Control

Extended ACLs (Layer 3 + Layer 4 filtering) allow organizations to:

- Specify allowed/denied sources
- Filter traffic based on protocols and ports
- Enforce least-privilege communication

Extended ACLs will help us implement the rule:

- Branch → Database = DENY
- Branch → Web Server = ALLOW

ACL-based segmentation has been identified as one of the most effective security tools in corporate environments.

Enterprise Documentation Practices

We also examined documentation standards for network design reports, focusing on:

- Network addressing schemas
- Flow diagrams
- Routing tables
- Security rule definitions
- Future scalability considerations

These standards guide the structure and depth of the report we are creating.

3. Methodology

Ourapproach isdividedinto multiple phases, each focusing on the technical design, configuration, and validation of SecureBooks Inc.'s corporate network.

Phase 1 – VLSM Subnetting

We will begin by breaking down the 172.16.10.0/24 address block using VLSM.
The host requirements are:

Segment	Hosts Needed
Main Office LAN	60
Branch Office LAN	28
DMZ Servers	14
WAN Link	2

We will calculate subnet masks, usable ranges, broadcast addresses, and assign the **first usable IP** to each router interface.

Phase 2 – Network Device Configuration

This phase includes configuring all core infrastructure:

Router Configuration

- Assign IPs to all interfaces
- Set subnet masks from VLSM
- Configure default gateways for LAN devices
- Enable RIP v2
- Add static route for DMZ
- Add default route for Branch

DHCP Configuration

DHCP will be provided only in the Main Office. We will:

- Create a DHCP pool
- Exclude the router interface IP
- Reserve at least 5 IPs for future static devices
- Verify IP allocation through PCs

Server Configuration

- Manually assign static IPs in the DMZ
- Set gateway pointing to HQ Router
- Configure DNS entries if required

Phase 3 – Mixed Routing Implementation

Routing will be implemented as follows:

Dynamic Routing – RIP v2

We will enable RIP v2 and advertise:

- Main Office LAN
- Branch Office LAN
- WAN link network

Benefits:

- Simple
- Automatic route exchange
- Suitable for small networks

Static Routing – DMZ

We will add a static route on HQ Router for the DMZ network.
This prevents unnecessary advertisements in RIP and creates a stable route to critical servers.

Default Routing – Branch Router

The Branch Router will use a default route pointing to HQ.
This allows Branch devices to reach remote networks without extra routing configuration.

Phase 4 – ACL Security Enforcement

The heart of the project: **SECURE_DMZ ACL**.

We will implement the following security rules on HQ Router:

Rule	Action	Source	Destination	Purpose
A	Permit	HQ/Branch	Web Server	Allow legitimate access
B	Permit	HQ only	Database Server	Allow internal trusted access
C	Deny	Branch	Database Server	Enforce data confidentiality

Rules will be applied *in order* to the correct interface *inbound or outbound*, depending on optimal security placement.

Phase 5 – Verification & Testing

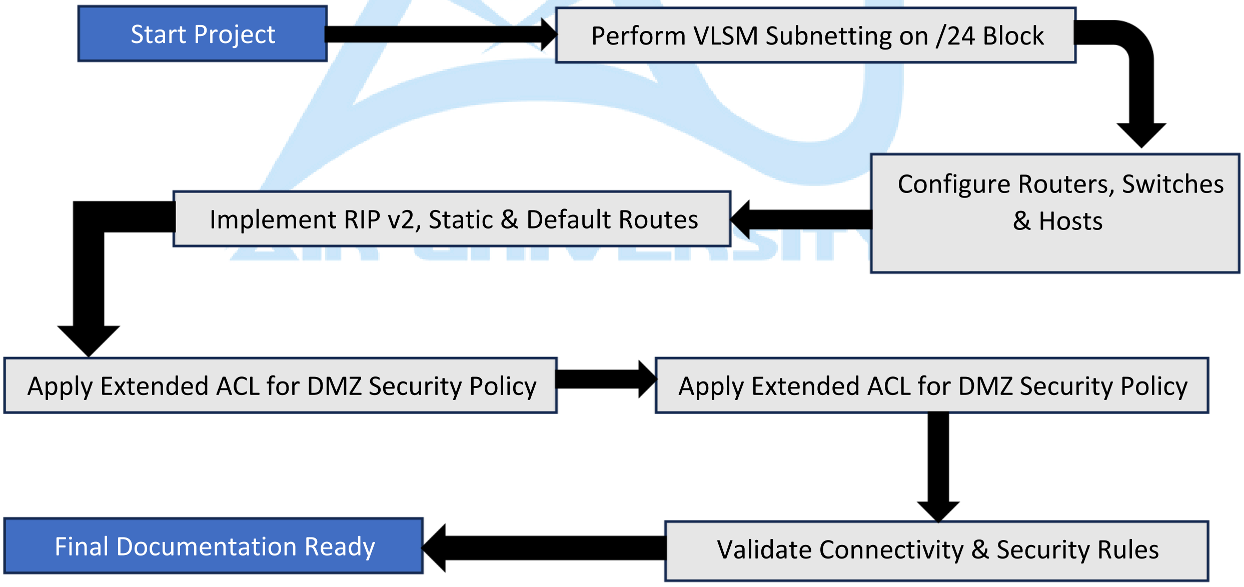
We will conduct detailed testing:

- **Ping tests** between all segments
- **Traceroutes** to validate routing paths
- Checking **show ip route** on R1 & R2
- Verifying DHCP allocation
- Confirming ACL counters increment correctly
- Testing permitted/denied traffic explicitly

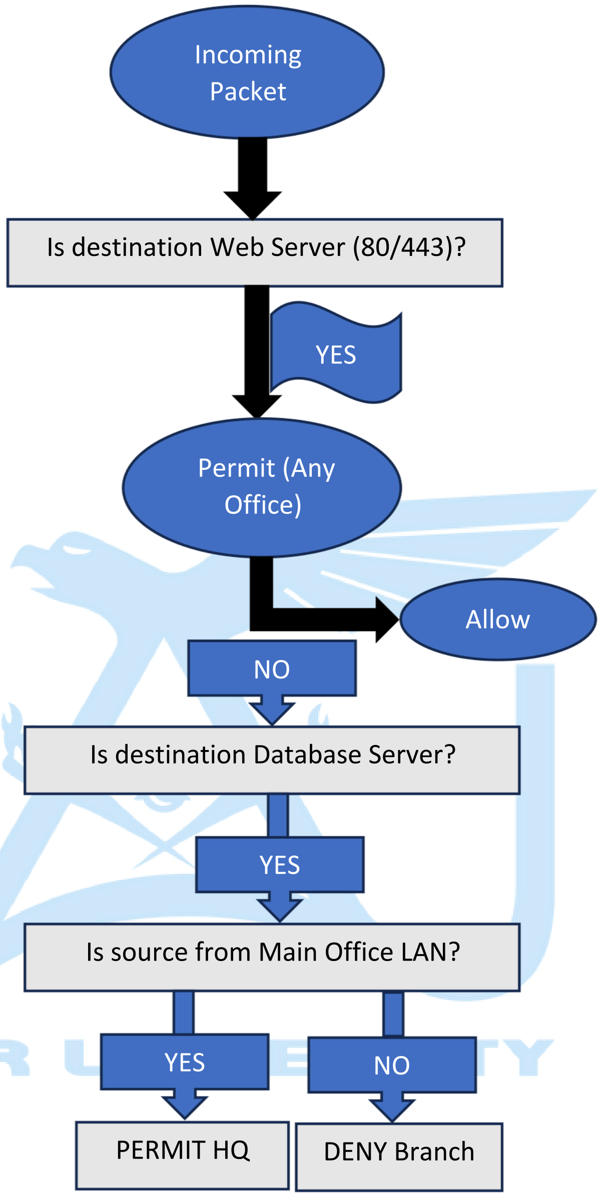
This ensures the network is functioning exactly as designed.

4. Flow Diagrams

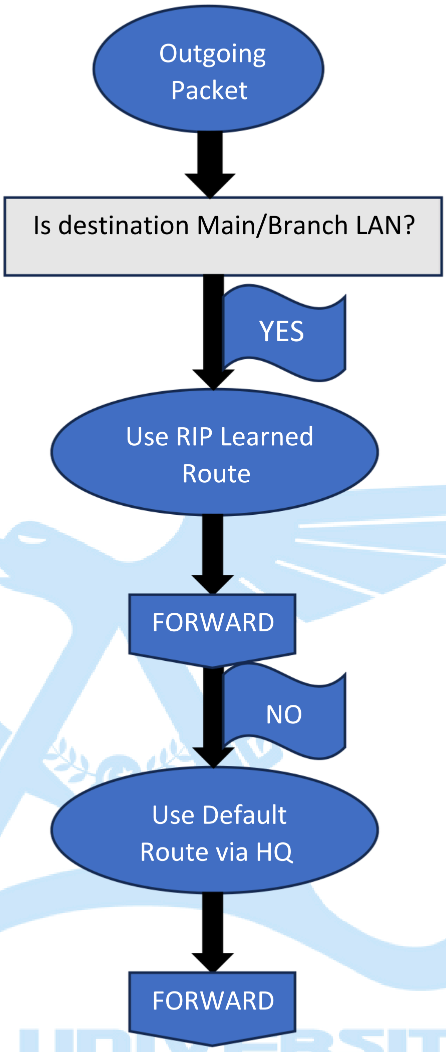
Flowchart 1 – Overall Project Workflow


Start Project
Perform VLSM Subnetting on /24 Block
Configure Routers, Switches & Hosts
Implement RIP v2, Static & Default Routes
Apply Extended ACL for DMZ Security Policy
Apply Extended ACL for DMZ Security Policy
Validate Connectivity & Security Rules
Final Documentation Ready

Flowchart 2 – ACL Decision Logic


Incoming Packet
Is destination Web Server (80/443)?
YES
Permit (Any Office)
Allow
NO
Is destination Database Server?
YES
Is source from Main Office LAN?
YES
NO
PERMIT HQ
DENY Branch

Flowchart 3 – Routing Logic (Branch Router)



5. Future Work

After completing the primary implementation, we plan to extend the project with advanced networking and security features. Potential future enhancements include:

VLAN Segmentation

Separate Main Office departments (HR, Admin, Accounts, IT) using VLANs and inter-VLAN routing.

VPN Deployment

Add encrypted site-to-site VPN tunnels to replace standard WAN links.

Server Redundancy

Implement:

- Failover Web Server
- Database replication
- Load balancing

Network Automation

Use Python or Ansible to automate:

- Router configuration backups
- ACL rule generation
- DHCP reservation updates

Intrusion Detection/Prevention

Implement a simulated IDS/IPS to detect unauthorized access attempts.

Monitoring & Logging

Introduce:

- SNMP
- Syslog server
- Real-time traffic analysis dashboards

These improvements would elevate the project from a basic design into a scalable enterprise environment.

6. Conclusion

This project aims to develop a secure, scalable, and professionally structured enterprise network for SecureBooks Inc. We will design the addressing plan with VLSM, configure routing through a combination of dynamic and static protocols, deploy a DMZ for protected server hosting, and enforce strict access control using Extended ACLs.

By the end, we expect a fully functional network where:

- Every device can communicate efficiently
- Routing paths are optimized
- IP addressing is fully structured
- Security policies are strictly enforced
- Branch office access is selectively controlled

The design reflects real industry practices and prepares us for professional networking roles.