Final Project Manual: SMB Office Migration & Security

Imagine you are a Network Engineer hired by a small but growing company called SecureBooks Inc. This company has a main office where all the staff work, and they also run two important servers (a Web Server and a Database Server) in a highly secure server area called the DMZ. They also have a small remote Branch Office that needs to connect to the main office network. Your job is to build and secure this entire network. You must design the entire addressing scheme from one single IP range, connect all the offices using different routing methods (mixing automatic and manual routes), and, most importantly, set up security rules. The critical rule is that staff at the remote Branch Office can see the Web Server, but they must be completely blocked from ever reaching the secret Database Server.

Project Goal

Imagine you are a Network Engineer hired by a small but growing company called **SecureBooks Inc.** This company has a main office where all the staff work, and they also run two important servers (a Web Server and a Database Server) in a highly secure server area called the **DMZ**. They also have a small remote **Branch Office** that needs to connect to the main office network.

Your job is to build and secure this entire network using **Cisco Packet Tracer**.

Key Constraints:

- **Total IP Block:** You must use the single address block **172.16.10.0/24** for the entire network.
- **Security Priority:** The final solution must block traffic from the Branch Office to the Database Server.

Design, configure, and secure a multi-segmented corporate network for **SecureBooks Inc.** using Cisco Packet Tracer. The project requires the application of **VLSM Subnetting, Mixed Routing (Static/RIP/Default), DHCP, and Access Control Lists (ACLs)** to enforce real-world security policies.

I. Scenario and Topology Requirements

A. IP Address Block

- **Total IP Space Allocated:** 172.16.10.0/24

B. Required Topology (To be Built in Packet Tracer)

1. **Router HQ (R1):** Central router.

2. **Router Branch (R2):** Remote router.
3. **HQ LAN:** Switch, at least **2 PCs**, and a **Printer**.
4. **DMZ:** Separate Switch, a **Web Server**, and a **Database Server**.
5. **Branch LAN:** Switch and at least **2 PCs**.

II. Task 1: VLSM Subnetting

You must use **Variable Length Subnet Masking (VLSM)** on the `172.16.10.0/24` block to create the following four subnets, prioritizing the largest host requirement first.

Segment Name	Required Hosts	Subnet Address (e.g., 172.16.10.X)	New Subnet Mask	Usable Range (First & Last Host)
1. Main Office LAN	60			
2. Branch Office LAN	28			
3. DMZ (Servers)	14			
4. WAN Link (R1-R2)	2			

Deliverable A: Complete the table above and include it as the first page of your documentation.

III. Task 2: Basic & Advanced Configuration (30 Points)

Apply your calculated IP addresses to the Packet Tracer topology.

Configuration Item	Router/Device	Detailed Requirements
Interface IPs	All Routers (R1, R2)	Configure the appropriate interface IP addresses and subnet masks based on your **VLSM Table (Task 1)**. Use the **first usable IP** in the range for the router interface.

DHCP Service	**Router HQ (R1)**	Configure a **DHCP Pool** for the **Main Office LAN** segment. Exclude the router interface IP and at least 5 additional IPs from the pool.
Server IPs	Web Server, DB Server	Assign a static IP address, subnet mask, and default gateway (R1 interface IP) from the **DMZ** segment.

IV. Task 3: Mixed Routing Implementation

Configure a robust, mixed-protocol routing solution to ensure every device can reach every other device (unless blocked by ACLs).

1. **Dynamic Routing (RIP v2):**
    - Configure **RIP v2** on **Router HQ (R1)** and **Router Branch (R2)**.
    - Advertise the **Main Office LAN** and **Branch Office LAN** networks. Use the `no auto-summary` command.
2. **Static Routing:**
    - Configure a **Static Route** on **Router HQ (R1)** to specifically advertise the **DMZ (Server) network**. Use the appropriate next-hop IP.
3. **Default Routing:**
    - Configure a **Default Route** (0.0.0.0 0.0.0.0) on **Router Branch (R2)**, pointing to the next-hop address of **Router HQ (R1)**. This ensures R2 can reach the DMZ and any future networks behind R1.

V. Task 4: Security Policy Enforcement

The final and most critical task is to enforce the firm's security policy using an **Extended Access Control List (ACL)**.

- **Location:** Apply the ACL on **Router HQ (R1)** to filter traffic moving between the networks.
- **Name:** Name the ACL `SECURE_DMZ`.

Security Policy:

Rule	Action	Source Network	Destination Host/Service
A (Web Access)	**PERMIT**	**Any Host** on the HQ LAN or Branch LAN	**Web Server** (Target: HTTP/80 or HTTPS/443)

B (DB Access)	**PERMIT**	**Only** the **Main Office LAN** (HQ)	**Database Server** (Target: ALL protocols/ports)
C (Security Block)	**DENY**	**Branch Office LAN**	**Database Server** (Target: ALL protocols/ports)

VI. Deliverables Checklist

The following items must be submitted for grading:

Item	Requirement
1. VLSM Table	Completed Task 1 table showing all calculations.
2. Packet Tracer File	Final, working .pkt file with all configurations.
3. Verification Screenshots	**a.** Successful ping from **HQ PC** to **Database Server**. **b. Failed** ping from **Branch PC** to **Database Server**. **c.** Output of show ip route from **R1** and **R2**. **d.** Output of show access-lists from **R1**.
4. Routing Explanation	Briefly explain *why* you chose RIP for one segment and a Static Route for the DMZ (50 words max).

VII. Marks Distribution

Section/Task	Detailed Component	Marks
I. VLSM & IP Planning	**VLSM Table Accuracy** (4 correct subnets calculated and applied)	**4**
II. Basic & Advanced Configuration	**Interface IPs** configured correctly on R1/R2 and all devices.	3
	DHCP Service operational on HQ LAN (correct pool/exclusion).	3
Subtotal		**6**

III. Mixed Routing Implementation	**RIP v2** (R1 & R2) configured correctly (network advertisements, no auto-summary).	3
	Static/Default Routes (DMZ Static on R1, Default on R2) configured correctly.	3
Subtotal		**6**
IV. Security & Verification	**ACL (SECURE_DMZ)** implemented correctly on the right interface/direction.	2
	Verification & Documentation (Screenshots showing successful and *blocked* pings, plus router config output).	2
Subtotal		**4**
Grand Total		**20 Marks**