Mid-Term Exam Project: Comprehensive Network Configuration Guide

Project Name: YOUR_STUDENT_ID BANK NETWORK DEPLOYMENT

Course: Computer Networks

Submission Deadline: Sunday, Oct 27, 2025, 11:59 P.M.

Lecturer: Eng. Joshua K. IRADUKUNDA.

> **CRITICAL NOTE:** After downloading the .pka file from Canvas, you MUST update your User Profile in Packet Tracer before starting any configuration:
>
> - **Name:** Your Student ID (e.g., 12345)
> - **Additional Info:** Your Full Name, Phone Number, and Starting Date
> - **Failure to update these fields will result in your work NOT being graded**

Table of Contents

1. Project Overview & Network Topology

Network Topology Overview

The network architecture follows a hierarchical design with four main functional blocks:

- **HQ-Block A:** IT-NETWORK and SERVER-ROOM
- **HQ-Block B:** FINANCE-NETWORK, ACCOUNTING-NETWORK
- **HQ-Block C:** HR-NETWORK, RISK-NETWORK, and Distribution layer connecting HQ-Block D
- **HQ-Block D:** TELLER-NETWORK, CUSTOMER NETWORK (WiFi)
- **CORE:** Central switching connecting all distribution layers

The diagram shows a segmented corporate network with departmental VLANs (IT, HR, Finance, Accounting, Risk, Teller) and service VLANs (Core-Servers, Monitoring).

Project Goals

- Build complete campus network following the provided topology diagram
- Implement VLAN segmentation and inter-VLAN routing on Main-Router
- Configure VTP modes (Server, Transparent, Client) as specified
- Deploy EtherChannels for link aggregation
- Implement comprehensive security controls
- Configure DHCP services for client networks
- Setup DNS and NTP services
- Document and demonstrate full network functionality

Network Topology Description

The provided network topology diagram, titled "YOUR-STUDENT_ID BANK", illustrates a hierarchical network design with a central **CORE-SWC** connecting to various network blocks (HQ-Block A, B, C, D) and a Main-Router.

- **Main-Router:** Connected to CORE-SWC, positioned at the top-left of the diagram.
- **CORE-SWC:** A central 2960-24TT switch, connecting the Main-Router to blocks A, B, C, and D.
- **HQ-Block A:** Contains an "IT-NETWORK" (2960-24TT IT-NET switch) and a "SERVER-ROOM" (2960-24TT SERVER-ROOM switch). Both connect to A-SWC (BLOCK A - SWC). The IT-NETWORK houses various laptops and PCs. The SERVER-ROOM contains WEB SERVER, AD/DC, CBS, EDWH, SYSLOG, NET-MONITORING, and SIEM servers.
- **HQ-Block B:** Features a "FINANCE-NETWORK" (2960-24TT FINANCE-NET switch) and an "ACCOUNTING-NETWORK" (2960-24TT ACCOUNTING-NET switch). Both connect to B-SWC (BLOCK B - SWC). These networks are populated with laptops and PCs.
- **HQ-Block C:** Includes a "HR-NETWORK" (2960-24TT HR-NET switch) and a "RISK-NETWORK" (2960-24TT RISK-NET switch). Both connect to C-SWC (BLOCK C - SWC). Laptops and PCs are present in these networks.

- **HQ-Block D:** Consists of a "TELLER-NETWORK" (2960-24TT TELLER-NET switch) and a "CUSTOMER-NETWORK" served by a HomeRouter-PT-AC wireless router. The TELLER-NETWORK has PCs and laptops, while the CUSTOMER-NETWORK has visitor and client laptops/PCs connecting wirelessly. The TELLER-NET switch connects to the HomeRouter-PT-AC, which in turn connects to C-SWC.
- **Interconnections:**
    - Main-Router to CORE-SWC (likely using multiple links for inter-VLAN routing).
    - CORE-SWC to A-SWC (BLOCK A - SWC), B-SWC (BLOCK B - SWC), C-SWC (BLOCK C - SWC) via EtherChannels (indicated by multiple dashed lines).
    - A-SWC to IT-NET and SERVER-ROOM switches.
    - B-SWC to FINANCE-NET and ACCOUNTING-NET switches.
    - C-SWC to HR-NET, RISK-NET, and HomeRouter-PT-AC.
    - HomeRouter-PT-AC to TELLER-NET switch.
- **IP Addressing:** IP subnets like 192.168.10.0/28 (IT-NET), 192.168.80.0/28 (SERVER-ROOM), 192.168.30.0/28 (FINANCE-NET), 192.168.40.0/28 (ACCOUNTING-NET), 192.168.20.0/28 (HR-NET), 192.168.50.0/28 (RISK-NET), and 192.168.60.0/28 (TELLER-NETWORK) are indicated next to their respective switches/networks.
- **Device Labels:** Switches are labeled with their names (e.g., IT-SWC, FINANCE-SWC,...) and model (2960-24TT). End devices are generically labeled Laptop-PT or PC-PT with specific identifiers (e.g., IT-L1, TELLER-P1).

2. Pre-Configuration Requirements

> **IMPORTANT:** Before starting configuration, ensure all equipment and software requirements are met.

Software & Equipment Requirements:

- Cisco Packet Tracer v8.2.2.0400 or compatible
- Download file format: YourStudentID_YourFullName_CNet-F25_MID - ID BANK.pka
- **Console Access:** Use console cable from IT computer to device console port
- **Router&Switch Terminals use Console cable:** To configure any network device (Routers, Switches), connect an IT Computer to the device using a Console cable and use its Terminal application.
- Lab notebook or digital log for command tracking

File Naming Conventions

- **Pka File:** YourStudentID_YourFullName_CNet-F25_MID.pka
- **PDF Report:** YourStudentID_YourFullName_CNet-F25_MID.pdf
- **HD Video:** YourStudentID_YourFullName_CNet-F25_MID.mp4

3. Naming and Credential Standards

> **MANDATORY:** You MUST replace "YOUR_STUDENT_ID" with your actual student ID throughout the configuration

Required Changes Across All Devices

Element	Format	Example
Network Container Name	YOUR-STUDENT_ID BANK	12345 BANK
Wireless Router Device Name	YOUR-STUDENT_ID_HQ_WIFI	12345_HQ_WIFI
Guest Network SSID	YOUR-STUDENT_ID_Guest_WIFI	12345_Guest_WIFI
Domain Names (VTP, SSH, DNS)	your_student_id.f25	12345.f25
Username	Your last name	Joshua
Password/Secret	Your student ID	12345

4. Network Device Setup & Addressing

Complete VLAN Configuration Table

VLAN ID	Name	IP Network	Subnet Mask (/28)	Gateway IP	Interfaces Used	Devices & Purpose
1	PUBLIC-NET	192.168.100.96/28	255.255.255.240	192.168.100.97	F0/1	WEB-SERVER (Public web services)
10	IT-NET	192.168.10.0/28	255.255.255.240	192.168.10.1	F0/1-3	IT Computers and admin workstations
20	HR-NET	192.168.20.0/28	255.255.255.240	192.168.20.1	F0/4-6	HR Computers
30	FIN-NET	192.168.30.0/28	255.255.255.240	192.168.30.1	F0/7-9	Finance PCs

40	ACC-NET	192.168.40.0/28	255.255.255.240	192.168.40.1	F0/10-12	Accounting PCs
50	RISK-NET	192.168.50.0/28	255.255.255.240	192.168.50.1	F0/13-15	Risk Dept PCs
60	TELLER-NET	192.168.60.0/28	255.255.255.240	192.168.60.1	F0/16-18	Teller PCs
70	VISITOR-NET	192.168.70.0/28	255.255.255.240	192.168.70.1	Wireless SSID	Visitor/Guests
80	CORE-SVR	192.168.80.0/28	255.255.255.240	192.168.80.1	F0/2-4	AD/DC, CBS, EDWH
90	MONITOR-SVR	192.168.90.0/28	255.255.255.240	192.168.90.1	F0/5-7	SYSLOG, NET-MONITORING, SIEM

Server IP Configuration Table

Server Name	Hostname	IP Address/Mask	Default Gateway	VLAN	Role & Services
WEB SERVER	web.yourID.f25	192.168.100.100/28	192.168.100.97	1	Web Server, HTTP Service
AD/DC SERVER	ad.yourID.f25	192.168.80.10/28	192.168.80.1	80	Active Directory, Domain Controller, DNS Server
CBS SERVER	cbs.yourID.f25	192.168.80.11/28	192.168.80.1	80	Core Banking System, FTP Service
EDWH SERVER	edwh.yourID.f25	192.168.80.12/28	192.168.80.1	80	Enterprise Data Warehouse, Restricted DB Server
SYSLOG SERVER	syslog.yourID.f25	192.168.90.10/28	192.168.90.1	90	Syslog Server, Monitoring/Log Collector

NET-MONITORING	mon.yourID.f25	192.168.90.11/28	192.168.90.1	90	NTP Server
SIEM	siem.yourID.f25	192.168.90.12/28	192.168.90.1	90	Security Monitoring

DHCP Pool Configuration

Network Pool	DHCP Range	Excluded Addresses	Default Gateway	DNS Server
IT-NET (VLAN 10)	192.168.10.6 to 192.168.10.14	192.168.10.1 to 192.168.10.5	192.168.10.1	192.168.80.10
HR-NET (VLAN 20)	192.168.20.6 to 192.168.20.14	192.168.20.1 to 192.168.20.5	192.168.20.1	192.168.80.10
FIN-NET (VLAN 30)	192.168.30.6 to 192.168.30.14	192.168.30.1 to 192.168.30.5	192.168.30.1	192.168.80.10
ACC-NET (VLAN 40)	192.168.40.6 to 192.168.40.14	192.168.40.1 to 192.168.40.5	192.168.40.1	192.168.80.10
RISK-NET (VLAN 50)	192.168.50.6 to 192.168.50.14	192.168.50.1 to 192.168.50.5	192.168.50.1	192.168.80.10
TELLER-NET (VLAN 60)	192.168.60.6 to 192.168.60.14	192.168.60.1 to 192.168.60.5	192.168.60.1	192.168.80.10

5. VLANs Configuration & Port Assignments

VLAN Deployment Strategy

Implement VLANs according to the hierarchical network design:

- **Core Switch:** Creates all VLANs (since VTP Server) and propagates to clients
- **Transparent Switches:** Must manually create ALL required VLANs locally
- **Client Switches:** Receive VLAN information from VTP Server

Port Configuration Requirements

Switch Type	VTP Mode	VLAN Creation
CORE-SWC	Server	Create VLANs: 1, 10, 20, 30, 40, 50, 60, 70, 80, 90
A-SWC, B-SWC, C-SWC	Transparent	MANUAL creation of all VLANs required
SVR-SWC, FIN-SWC, ACC-SWC, TELLER-SWC	Client	Learn VLANs from VTP Server

> **CONFIGURATION ORDER:** Configure core VLANs first, then access switches, then security

VLAN Interface Assignments and Security

- **Access Port Configuration:** All end-device interfaces must have:
  - switchport mode access
  - switchport access vlan XX
  - spanning-tree portfast
  - spanning-tree bpduguard enable
  - port-security with maximum 1 MAC address, violation shutdown
- **Unused Ports:** All unused switch interfaces must be shutdown
- **VTP Domain:** All devices must use your_student_ID.f25
- **VTP Password:** Use student ID as VTP password

Port Security Configuration

Required on ALL end-device access interfaces:

```
interface fastethernet 0/1
 switchport mode access
 switchport access vlan XX
 switchport port-security
 switchport port-security maximum 1
 switchport port-security violation shutdown
 spanning-tree portfast
 spanning-tree bpduguard enable
```

```
no shutdown
```

6. Trunking and EtherChannel Configuration

Comprehensive EtherChannel & Trunk Mapping

Port-Channel Group	Devices Connected	Interfaces	Allowed VLANs	Protocol
1	CORE-SWC ↔ A-SWC	Fa0/20-21	1,10-90	LACP Active
2	A-SWC ↔ SVR-SWC	Gi0/1-2	80,90	LACP Active
3	A-SWC ↔ B-SWC	Fa0/22-23	1,10-90	LACP Active
4	CORE-SWC ↔ C-SWC	Fa0/22-23	10-70	LACP Active

7. Server Configuration & Services

Complete Server Configuration Matrix

Server Name	IP Address	VLAN Assignment	Interfaces Used	Services Enabled	ACL Restrictions
WEB	192.168.100.100/28	1	F0/1 (SVR-SWC)	HTTP, static IP	VISITOR: HTTP only; Others: Full access
AD/DC	192.168.80.10/28	80	F0/2 (SVR-SWC)	DNS, AD Services	Restricted access per ACL
CBS	192.168.80.11/28	80	F0/3 (SVR-SWC)	FTP	Restricted access per ACL
EDWH	192.168.80.12/28	80	F0/4 (SVR-SWC)	DB Server	IT-NET only
SYSLOG	192.168.90.10/28	90	F0/5 (SVR-SWC)	Syslog	Full access

NET-MON	192.168.90.11/28	90	F0/6 (SVR-SWC)	NTP	Full access
SIEM	192.168.90.12/28	90	F0/7 (SVR-SWC)	SIEM	Full access

General Server Configuration Steps

- Go to Desktop > IP Configuration.
- Set IP Address, Subnet Mask, Default Gateway (VLAN Gateway IP from Main-Router), and DNS Server (192.168.80.10 for all).
- Go to Services tab to enable/configure specific services.

8. Security Implementation

Access Control Lists (ACLs) - On Main-Router

ACLs are critical for security and must be applied on the Main-Router. Name your ACLs using your Student ID for clarity **(e.g., IP access-list standard Standard_12345)**. Remember the implicit deny any at the end of every ACL, so explicitly permit necessary traffic.

ACL Application Guidelines:

- ACLs should be applied on the sub-interfaces of the Main-Router.
- Carefully consider the direction (in or out) based on the flow of traffic you want to filter.

Standard ACL (Named):

Objective: Block VISITOR/CLIENT Network (VLAN 70) from accessing any other network.

- **Name:** IP access-list standard Standard_<YourStudentID>_Visitor_Block
- **Rules:** Deny all traffic originating from 192.168.70.0/28.
- **Application:** Apply inbound on the GigabitEthernet 0/0.70 sub-interface.

Extended ACLs (Named):

Objective: Allow VISITOR/CLIENT Network (VLAN 70) to access WEB SERVER (HTTP) and AD/DC SERVER (DNS) only.

- **Name:** IP access-list extended Extended_<YourStudentID>__Visitor_Access
- **Rules:**
    - Permit TCP traffic from 192.168.70.0/28 to 192.168.100.100 (WEB SERVER) on port 80 (HTTP).

    - Permit UDP traffic from 192.168.70.0/28 to 192.168.80.10 (AD/DC) on port 53 (DNS).
    - Explicitly deny all other traffic from 192.168.70.0/28 (or rely on implicit deny).
- **Application:** Apply inbound on the GigabitEthernet 0/0.70 sub-interface (after the Standard ACL if it blocks all). Alternatively, if you want to block all, then selectively permit, make sure this extended ACL comes before any broader deny. A better approach might be to just use this extended ACL, permitting HTTP/DNS and then having an implicit deny for everything else.

Objective: Allow other networks (all except Visitors/Clients) to send only PING and DNS traffic to AD/DC SERVER. IT-NET users have Full Access.

- **Name:** IP access-list extended Extended_<YourStudentID>_ADDC_Access
- **Rules:**
    - Permit IP traffic from 192.168.10.0/28 (IT-NET) to 192.168.80.10 (AD/DC). (Full access for IT-NET).
    - Permit ICMP (ping) traffic from any (or specific subnets excluding 70) to 192.168.80.10 (AD/DC).
    - Permit UDP traffic (DNS) from any (or specific subnets excluding 70) to 192.168.80.10 (AD/DC) on port 53.
    - Deny all other traffic to 192.168.80.10.
- **Application:** Apply outbound on the GigabitEthernet 1/0.80 sub-interface (towards the AD/DC server).

Objective: Allow all networks (except Visitors/Clients) to send only FTP traffic to CBS SERVER. IT-NET has Full Access.

- **Name:** IP access-list extended Extended_<YourStudentID>__CBS_Access
- **Rules:**
    - Permit IP traffic from 192.168.10.0/28 (IT-NET) to 192.168.80.11 (CBS). (Full access for IT-NET).
    - Permit TCP traffic from any (or specific subnets excluding 70) to 192.168.80.11 (CBS) on ports 20 and 21 (FTP).
    - Deny all other traffic to 192.168.80.11.
- **Application:** Apply outbound on the GigabitEthernet 1/0.80 sub-interface.

Objective: Allow only IT-NET to access EDWH SERVER.

- **Name:** IP access-list extended Extended_<YourStudentID>__EDWH_Access
- **Rules:**
    - Permit IP traffic from 192.168.10.0/28 (IT-NET) to 192.168.80.12 (EDWH).
    - Deny IP traffic from any to 192.168.80.12.
- **Application:** Apply outbound on the GigabitEthernet 1/0.80 sub-interface.

Special Note for NET-MONITORING Systems:

The NET-MONITORING Systems (VLAN 90) are allowed to send and receive traffic from all networks/devices without any restrictions from these ACLs. This means you should ensure your ACLs do not implicitly block traffic to/from 192.168.90.0/28 for monitoring purposes. You might need to add explicit permit ip any 192.168.90.0 0.0.0.15 and permit ip 192.168.90.0 0.0.0.15 any statements in your extended ACLs if necessary, before any broad deny statements.

Mandatory Security Settings

- **Port Security:** Apply on all access ports with maximum MAC addresses: 1, violation action: shutdown
- **SSH Configuration:** Enable SSH on all devices, disable Telnet completely, username: Your last name, password: Your student ID, service password-encryption enabled
- **STP Hardening:** spanning-tree mode rapid-pvst, BPDU Guard on all PortFast enabled interfaces

9. Verification & Testing Procedures

Essential Show Commands & Expected Outputs

Router Verification Commands

Command	Expected Result
show ip interface brief	All subinterfaces show correct IPs and UP/UP status
show ip route	All VLAN networks visible as connected routes
show ip dhcp binding	Client leases shown from pools with correct IPs
show ip access-lists <ACL_NAME>	Hits increment for allowed/blocked flows

Step-by-Step Testing Procedure

1. Verify subinterfaces are operational with correct IP assignments
2. Test within same VLAN first (ping between computers in same VLAN)
3. Then test cross-VLAN routing (ping between different VLANs)
4. Test DHCP functionality across all client VLANs
5. Validate DNS resolution for instance, web.yourID.f25
6. Check inter-VLAN routing connectivity
7. Verify ACL implementations and counters
8. Finally test services (NTP, SYSLOG, FTP)

10. Troubleshooting Guide

Common Issues & Solutions

- **VLAN Mismatch:** Ensure VLAN IDs match between switches and router subinterfaces
- **Port Security Violations:** Check port-security status and clear violations
- **ACL Blocking Required Traffic:** Temporarily remove or re-order ACL rules
- **Trunk Issues:** Verify allowed VLANs on trunk interfaces
- **EtherChannel Problems:** Ensure consistent LACP mode on both sides
- **VTP Domain Mismatch:** Verify VTP domain name and password match across all switches

Critical Best Practices

> ⚠️ **IMPORTANT:** Save your Packet Tracer file frequently at each major configuration milestone

Key Screenshot Evidence Required

- VLANs and Inter-VLANs
- DHCP_Lease_Proof
- Web_Access_by_IP
- Web_Access_by_Domain
- DNS_Resolution
- NTP_Sync_Router.png
- NTP_Sync_Switch.png
- ACL_Counters
- EtherChannel_Summary
- Port_Security_Enabled

BEST PRACTICES AND FINAL TIPS

During Configuration

- ✓ **Plan Before You Configure**
  - Draw port-to-port mapping
  - Create an interface assignment table
  - Document IP assignments beforehand
- ✓ **Configure Incrementally**
  - Complete one phase before moving to next

    - Test after each major step
    - Save backup after each phase
- ✓ **Document Everything**
    - Keep detailed lab notebook
    - Record every command used
    - Note reasons for configuration choices
    - Capture timestamps of changes

- ✓ **Save Frequently**
    - **Save after each phase:** pka, Phase2_Config.pka, etc.
    - **Final PKA submission:** Your_Student_ID_FullName_CNet-F25_MID.pka (12345_FullName_CNet-F25_MID.pka)
    - **Final PDF submission:** Your_Student_ID_FullName_CNet-F25_MID.pdf (12345_FullName_CNet-F25_MID.pka)

11. Submission Requirements & Grading

Submission Package Requirements

Upload the following files to the designated Google Form:

- **Packet Tracer Activity (.pka) file:** The completed network configuration
- **PDF Document:** A detailed report outlining your configuration steps, verification outputs (screenshots of show commands, ping results, browser tests), and any challenges faced during the project
- **HD Short demo video:** 4–8 minutes showing:
    - Provide a comprehensive demonstration of the network, detailing how everything is connected and how devices interact with each other
    - Router & switch show commands outputs
    - Browser visiting the web page by DNS name
    - Ping tests and ACL evidence

Grading Rubric

Area	Points	Criteria
VLANs & IP addressing	20	Correct VLANs created; subnets assigned; DHCP pools configured correctly
Trunks & Port-Channels	15	Trunks up, allowed VLANs correct; EtherChannel stable and up
Router & inter-VLAN routing	15	Subinterfaces correct, routes visible, gateways reachable

Servers & DNS/NTP	15	Web resolvable by name, NTP sync, services running
ACLs & Security	20	ACLs implemented exactly as specified, port-security, SSH only, STP hardened
Documentation & Evidence	15	Complete report, HD Short video, show outputs, screenshots, mapping table

MOTIVATION: "Dream big and work hard to achieve your goals. Stay strong and keep fighting for your dreams. Do not let anything discourage you; the future looks bright."

Good luck!