Mid-Term Exam

Start Assignment

- Due Sunday by 11:59pm
- Points 100
- Submitting a text entry box
- Available Oct 19 at 12am - Oct 27 at 11:59pm

image.png

Faculty of Information Technology

Mid-Term Examination Academic Year: 2024-2025 (3)

Course Code & Name: INSY 8121 & Computer Maintenance

Lecturer: Joshua IRADUKUNDA **Date:** From 19th to 26th OCT, 2025

MAX/30 **Group Day: (ALL)** A, B, C, and D **DURATION:** 7 Days

Mid-Term Exam Project: Network Configuration Guidelines

Project Name: YOUR_STUDENT_ID BANK NETWORK DEPLOYMENT

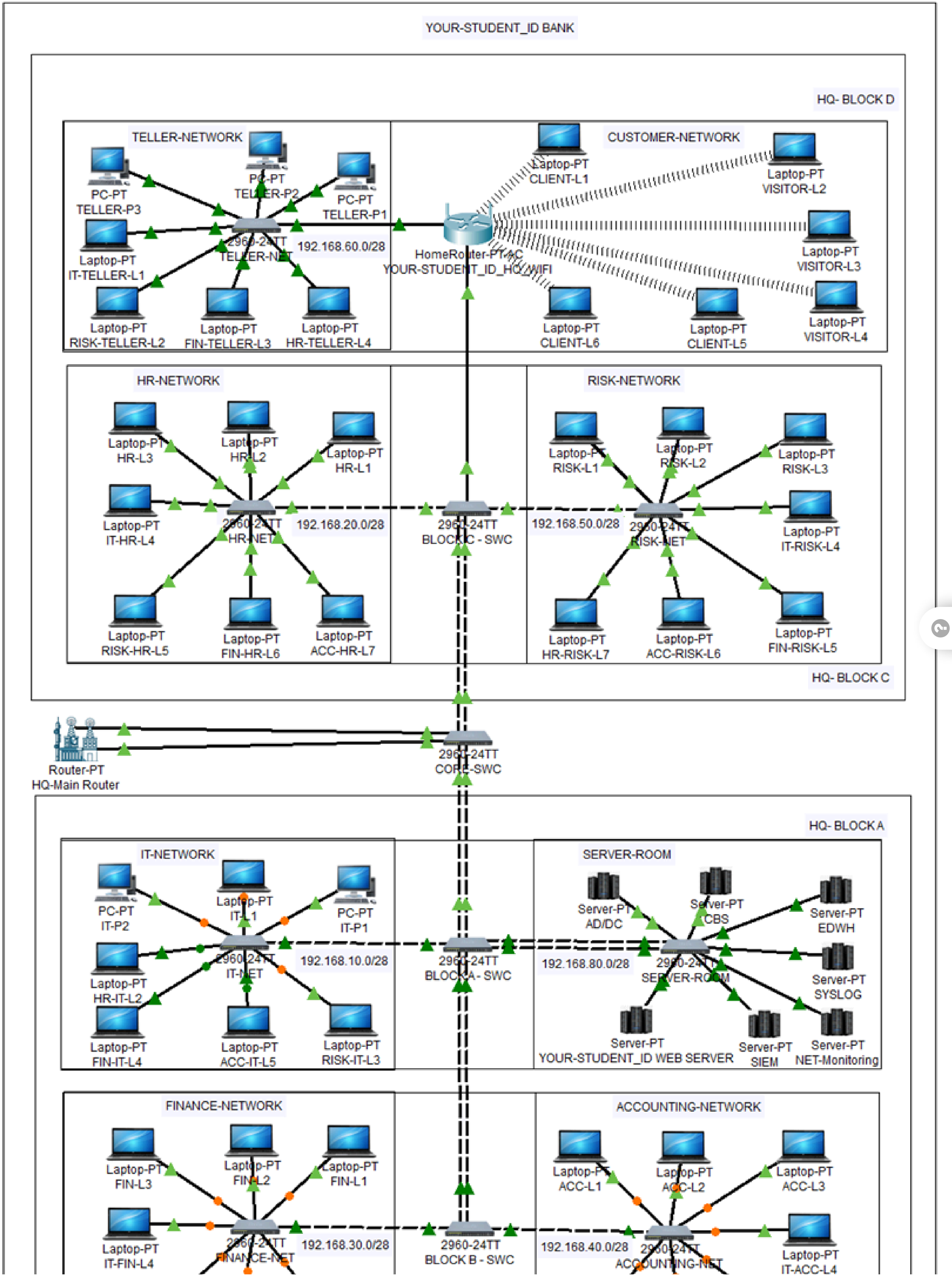
Course: Computer Networks

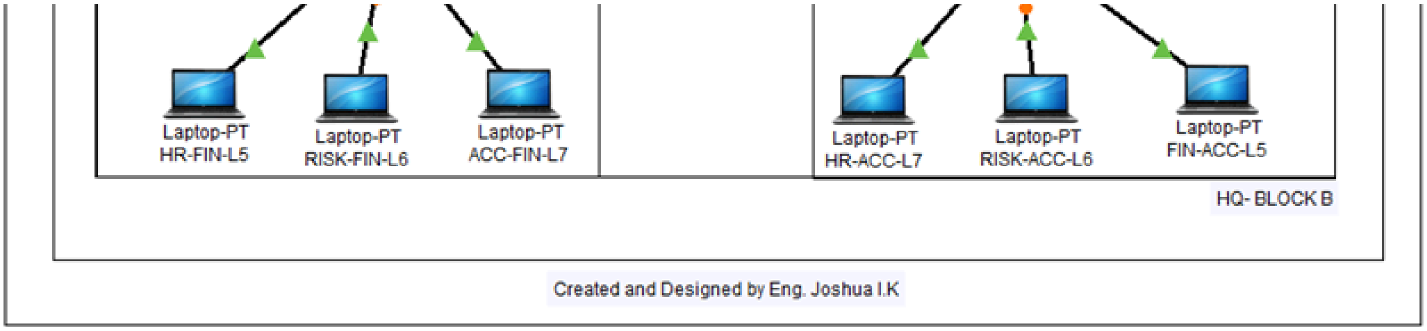
TABLE OF CONTENTS

Project Overview

This project requires you to configure a complex network topology, including routers, switches, servers, and end-devices, to meet specific functional and security requirements. You will implement inter-VLAN routing, VLAN Trunking Protocol (VTP), EtherChannels, Spanning Tree Protocol (STP) enhancements, Port Security, Access Control Lists (ACLs), and various server services like DHCP, DNS, and NTP. The goal is to build a robust and secure network infrastructure.

Network Topology:


YOUR-STUDENT_ID BANK
HQ- BLOCK D
TELLER-NETWORK
PC-PT
TELLER-P3
PC-PT
TELLER-P2
PC-PT
TELLER-P1
Laptop-PT
IT-TELLER-L1
2960-24TT
TELLER-NET
192.168.60.0/28
Laptop-PT
RISK-TELLER-L2
Laptop-PT
FIN-TELLER-L3
Laptop-PT
HR-TELLER-L4
CUSTOMER-NETWORK
Laptop-PT
CLIENT-L1
Laptop-PT
VISITOR-L2
HomeRouter-PT-AC
YOUR-STUDENT_ID_HQ_WIFI
Laptop-PT
VISITOR-L3
Laptop-PT
CLIENT-L6
Laptop-PT
CLIENT-L5
Laptop-PT
VISITOR-L4
HR-NETWORK
Laptop-PT
HR-L3
Laptop-PT
HR-L2
Laptop-PT
HR-L1
Laptop-PT
IT-HR-L4
2960-24TT
HR-NET
192.168.20.0/28
Laptop-PT
RISK-HR-L5
Laptop-PT
FIN-HR-L6
Laptop-PT
ACC-HR-L7
2960-24TT
BLOCK C - SWC
RISK-NETWORK
Laptop-PT
RISK-L1
Laptop-PT
RISK-L2
Laptop-PT
RISK-L3
192.168.50.0/28
2960-24TT
RISK-NET
Laptop-PT
IT-RISK-L4
Laptop-PT
HR-RISK-L7
Laptop-PT
ACC-RISK-L6
Laptop-PT
FIN-RISK-L5
HQ- BLOCK C
Router-PT
HQ-Main Router
2960-24TT
CORE-SWC
HQ- BLOCK A
IT-NETWORK
PC-PT
IT-P2
Laptop-PT
IT-L1
PC-PT
IT-P1
Laptop-PT
HR-IT-L2
2960-24TT
IT-NET
192.168.10.0/28
Laptop-PT
FIN-IT-L4
Laptop-PT
ACC-IT-L5
Laptop-PT
RISK-IT-L3
2960-24TT
BLOCK A - SWC
SERVER-ROOM
Server-PT
AD/DC
Server-PT
CBS
Server-PT
EDWH
192.168.80.0/28
2960-24TT
SERVER-ROOM
Server-PT
SYSLOG
Server-PT
YOUR-STUDENT_ID WEB SERVER
Server-PT
SIEM
Server-PT
NET-Monitoring
FINANCE-NETWORK
Laptop-PT
FIN-L3
Laptop-PT
FIN-L2
Laptop-PT
FIN-L1
Laptop-PT
IT-FIN-L4
2960-24TT
FINANCE-NET
192.168.30.0/28
2960-24TT
BLOCK B - SWC
ACCOUNTING-NETWORK
Laptop-PT
ACC-L1
Laptop-PT
ACC-L2
Laptop-PT
ACC-L3
192.168.40.0/28
2960-24TT
ACCOUNTING-NET
Laptop-PT
IT-ACC-L4



Network Architecture Overview

Component	**Quantity**	**Details**
Router	1	Main-Router (Inter-VLAN Routing)
Core Switches	1	CORE-SWC (VTP Server)
Distribution Switches	3	A-SWC, B-SWC, C-SWC (VTP Transparent)
Access Switches	3	SVR-SWC (VTP Client), FIN-SWC (VTP Client), ACC-SWC (VTP Client) TELLER-SWC (VTP Client)
Wireless Router	1	HomeRouter-PT-AC (for VLAN 60 & 70)
VLANs	10	Public, IT, HR, Finance, Accounting, Risk, Teller, Visitor, Core-Servers, Monitoring
Servers	7	WEB, AD/DC, CBS, EDWH, SYSLOG, NET-MONITORING, SIEM

Pre-Configuration Requirements

Software & Equipment Requirements:

- **Cisco Packet Tracer v8.2.2.0400**
- **Download: YourStudentID_YourFullName_CNet-F25_MID - ID BANK.pka (https://canvas.instructure.com/courses/12757746/files/316743625?**

wrap=1) (https://canvas.instructure.com/courses/12757746/files/316743625/dov download_frd=1)

- Open in Packet Tracer
- **Update User Profile:**
  - **Name:** Your Student ID (e.g., 12345)
  - **Additional Info:** Full Name, Phone Number, Starting Date
  - image.png
- **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 tracking commands

Naming and Credential Standards

- **Network Name:** Rename the main network container "YOUR-STUDENT_ID BANK" to your actual student ID (e.g., "**12345 BANK**"). Apply this renaming wherever the default name is mentioned to the corresponding name.
- **Wireless Router (Device Name):** YOUR-STUDENT_ID_HQ_WIFI → (e.g., **12345_HQ_WIFI**)
- **Guest Network SSID:** YOUR-STUDENT_ID_Guest_WIFI → (e.g., **12345_Guest_WIFI**)
- **Domain Names:** All domain names, including SSH domain name, web-server domain name, and VTP domain, must be Your_student_ID.f25 (e.g., 12345.f25).
- **Credentials:**
  - **Username:** Use your last name (e.g., Joshua).
  - **Password/Secret:** Use your student ID (e.g., 12345).

Enable service password-encryption in all Network Devices for security purpose

Phase 1: Network Device Setup and Access

Network Topology & Addressing

The network is divided into several VLANs, each with a specific purpose and IP address range. Servers also have static IP addresses.

VLANs Table

VLAN ID	Name	IP Network	Interfaces	Devices

1	PUBLIC-NET	192.168.100.96/28	F0/1	WEB-SERVER
10	IT-NET	192.168.10.0/28	F0/1-3	IT Computers
20	HR-NET	192.168.20.0/28	F0/4-6	HR Computers
30	FIN-NET	192.168.30.0/28	F0/7-9	FIN Computers
40	ACC-NET	192.168.40.0/28	F0/10-12	ACC Computers
50	RISK-NET	192.168.50.0/28	F0/13-15	RISK Computers
60	TELLER-NET	192.168.60.0/28	F0/16-18	TELLER Computers
70	VISITOR-NET	192.168.70.0/28	WIRELESS	VISITOR Computers
80	CORE-SVR	192.168.80.0/28	F0/2-4	AD/DC, CBS, and EDWH
90	MONITOR-SVR	192.168.90.0/28	F0/5-7	SYSLOG, NET-MONITORING, and SIEM

Server IPs Table

Server Name	**IP Address**	**Role**
WEB	192.168.100.100/28	Web Server
AD/DC	192.168.80.10/28	Active Directory/Domain Controller, DNS Server
CBS	192.168.80.11/28	(Specific Role to be determined by student, e.g., Core Banking System)
EDWH	192.168.80.12/28	(Specific Role to be determined by student, e.g., Enterprise Data Warehouse)

SYSLOG	192.168.90.10/28	Syslog Server
NET-MONITOR	192.168.90.11/28	Network Monitoring, NTP Server
SIEM	192.168.90.12/28	Security Information and Event Management

DHCP Pools

Configure DHCP pools on the Main-Router for the following networks, excluding the specified ranges for static assignments if necessary. These ranges indicate the scope of addresses to be assigned dynamically:

Network Pool	**Range**
IT	FROM: 192.168.10.1 to 192.168.10.5
HR	FROM: 192.168.20.1 to 192.168.20.5
FIN	FROM: 192.168.30.1 to 192.168.30.5
ACC	FROM: 192.168.40.1 to 192.168.40.5
RISK	FROM: 192.168.50.1 to 192.168.50.5
TELLER	FROM: 192.168.60.1 to 192.168.60.5

General Network Device Configuration Principles

Apply these principles to all relevant network devices unless specified otherwise.

- **Interface Management:**
  - Unused ports/interfaces on all switches must be shut down.
- **Port Security:**
  - Implement Port Security on all end-device access interfaces.
  - Configure interfaces to learn only one MAC address (maximum 1).

  - Configure interfaces to shut down (shutdown) if an unrecognized device is connected (violation mode).
- **Spanning Tree Protocol (STP):**
  - Implement PortFast on all end-device access interfaces to ensure immediate connection.
  - Implement BPDU Guard on all PortFast enabled interfaces to prevent rogue switches.
  - Spanning-tree mode must be rapid-pvst on all switches.
- **EtherChannel Load Balancing:**
  - Implement a suitable Port-channel load-balance method for optimal traffic distribution.
- **Remote Access (SSH):**
  - Implement secure remote access on all network devices (routers and switches).
  - Only allow SSH access. Telnet must be disabled.
  - Only IT Users (using their last name as username and student ID as password) are allowed to remotely access these devices.
  - Ensure SSH domain name is configured as your_student_ID.f25.
- **Network Time Protocol (NTP):**
  - All network devices (routers and switches) must synchronize their time with the NET-MONITORING Server.

Device Specific Configurations

Follow these detailed instructions for each network device.

Main-Router (HQ-Main Router)

This router is the core of your network, responsible for inter-VLAN routing and DHCP services.

- **Physical Connections:**
  - GigabitEthernet 0/0connects to GigabitEthernet 0/1 on the CORE-SWC.
  - GigabitEthernet 1/0connects to GigabitEthernet 0/2 on the CORE-SWC.
- **Inter-VLAN Routing (Router-on-a-Stick):**
  - Configure sub-interfaces on GigabitEthernet 0/0for VLANs 1, 10, 20, 30, 40, 50, 60, and 70.
    - For each sub-interface, assign the first usable IP address of its respective VLAN's /28subnet as the gateway address.
    - interface GigabitEthernet 0/0.10
    - encapsulation dot1Q 10
    - ip address <gateway_ip_for_VLAN10> <subnet_mask_for_/28>
    - no shutdown(on the main interface and sub-interfaces)
  - Configure sub-interfaces on GigabitEthernet 1/0for VLANs 80 and 90.
    - Assign the first usable IP address of their respective VLAN's /28subnet as the gateway address.
  - **DHCP Server Configuration:**
    - For each DHCP pool listed in section 3.3, configure:

        - ip dhcp excluded-address <start_ip> <end_ip>(Exclude server IPs and gateway IPs first).
        - ip dhcp pool <VLAN_NAME>(e.g., ip dhcp pool IT-NET)
        - network <network_address> <subnet_mask_for_/28>(e.g., network 192.168.10.0 255.255.255.240)
        - default-router <gateway_ip_for_this_VLAN>(The sub-interface IP you configured).
        - dns-server 192.168.80.10(The AD/DC server).
    - **ACL Application:**Implement and apply all ACLs as detailed in section 7 on this router. Carefully consider inbound/outbound direction and interface application.

CORE-SWC

This is the central distribution layer switch.

- **VTP Configuration:**
    - vtp version 2
    - vtp mode server
    - vtp domain your_student_ID.f25(e.g., f25)
    - vtp password your_student_ID(e.g., 12345)
    - **Create all VLANs**on this switch (VLAN 1, 10-90) so they can be propagated.
- **Trunking Interfaces:**
    - GigabitEthernet 0/1(to Main-Router G0/0): Configure as a trunk port allowing only VLANs 10, 20, 30, 40, 50, 60, and 70.
        - switchport mode trunk
        - switchport trunk allowed vlan 10-70(or list them specifically)
    - GigabitEthernet 0/2(to Main-Router G1/0): Configure as a trunk port allowing only VLANs 1, 80, and 90.
        - switchport mode trunk
        - switchport trunk allowed vlan 1,80,90
    - **EtherChannels:**
        - **EtherChannel to A-SWC (Group 1):**
            - Interfaces: FastEthernet 0/20-21.
            - Configure these as members of Port-channel Group 1 (use LACP or PAgP mode, e.g., channel-group 1 mode active).
            - Configure Port-channel 1as a trunk port allowing **all VLANs**.
        - **EtherChannel to C-SWC (Group 4):**
            - Interfaces: FastEthernet 0/22-23.
            - Configure these as members of Port-channel Group 4 (use LACP or PAgP mode, e.g., channel-group 4 mode active).
            - Configure Port-channel 4as a trunk port allowing only VLANs 10, 20, 30, 40, 50, 60, and 70.

A-SWC

- **VTP Configuration:**
  - vtp version 2
  - vtp mode transparent
  - vtp domain your_student_ID.f25
  - vtp password your_student_ID
  - **Manually create all necessary VLANs**on this switch, as it's transparent.
- **Connections & EtherChannels:**
  - FastEthernet 0/20-21(to CORE-SWC): Configure as EtherChannel Group 1 (matching CORE-SWC's mode).
    - Port-channel 1must be a trunk allowing **all VLANs**.
  - GigabitEthernet 0/1-2(to SVR-SWC): Configure as EtherChannel Group 2.
    - Port-channel 2must be a trunk allowing only VLANs 80 and 90.
  - FastEthernet 0/24(to IT-SWC): Configure as a trunk allowing VLANs 10, 20, 30, 40, and 50.
  - FastEthernet 0/22-23(to B-SWC): Configure as EtherChannel Group 3.
    - Port-channel 3must be a trunk allowing **all VLANs**.

SVR-SWC

- **VTP Configuration:**
  - vtp version 2
  - vtp mode client
  - vtp domain your_student_ID.f25
  - vtp password your_student_ID
  - VLANs will be learned from the VTP server (CORE-SWC).
- **Connections & EtherChannels:**
  - GigabitEthernet 0/1-2(to A-SWC): Configure as EtherChannel Group 2 (matching A-SWC's mode).
    - Port-channel 2must be a trunk allowing only VLANs 1, 80, and 90.
  - **Access Ports:**Connect servers to appropriate access ports (e.g., AD/DC to F0/2, CBS to F0/3, etc.). Configure these access ports for their respective VLANs (1, 80, 90) and apply Port Security, PortFast, and BPDU Guard.

B-SWC

- **VTP Configuration:**
  - vtp version 2
  - vtp mode transparent
  - vtp domain your_student_ID.f25
  - vtp password your_student_ID
  - **Manually create all necessary VLANs.**
- **Connections & EtherChannels:**
  - FastEthernet 0/22-23(to A-SWC): Configure as EtherChannel Group 3.

    - Port-channel 3must be a trunk allowing only VLANs 10, 20, 30, 40, and 50.
  - FastEthernet 0/20(to FIN-SWC): Configure as a trunk allowing only VLANs 10, 20, 30, 40, and 50.
  - FastEthernet 0/21(to ACC-SWC): Configure as a trunk allowing only VLANs 10, 20, 30, 40, and 50.

FIN-SWC

- **VTP Configuration:**
  - vtp version 2
  - vtp mode client
  - vtp domain your_student_ID.f25
  - vtp password your_student_ID
- **Connections:**
  - FastEthernet 0/20(to B-SWC): Configure as a trunk allowing only VLANs 10, 20, 30, 40, and 50.
- **Access Ports:**Connect FIN computers to access ports in VLAN 30, with Port Security, PortFast, BPDU Guard.

ACC-SWC

- **VTP Configuration:**
  - vtp version 2
  - vtp mode client
  - vtp domain your_student_ID.f25
  - vtp password your_student_ID
- **Connections:**
  - FastEthernet 0/21(to B-SWC): Configure as a trunk allowing only VLANs 10, 20, 30, 40, and 50.
- **Access Ports:**Connect ACC computers to access ports in VLAN 40, with Port Security, PortFast, BPDU Guard.

C-SWC

- **VTP Configuration:**
  - vtp version 2
  - vtp mode transparent
  - vtp domain your_student_ID.f25
  - vtp password your_student_ID
  - **Manually create all necessary VLANs.**
- **Connections & EtherChannels:**
  - FastEthernet 0/22-23(to CORE-SWC): Configure as EtherChannel Group 4.
    - Port-channel 4must be a trunk allowing only VLANs 10, 20, 30, 40, 50, 60, and 70.
  - FastEthernet 0/20(to HR-SWC): Configure as a trunk allowing only VLANs 10, 20, 30, 40, and 50.

- FastEthernet 0/21(to RISK-SWC): Configure as a trunk allowing only VLANs 10, 20, 30, 40, and 50.
- GigabitEthernet 0/1(to HomeRouter-PT-AC G1): Configure as a trunk allowing only VLANs 60 and 70.

HomeRouter-PT-AC (YOUR-STUDENT_ID_HQ_WIFI)

- **Device Renaming:**Rename this device to YOUR_STUDENT_ID_HQ_WIFI (e.g., 12345_HQ_WIFI).
- **Physical Connections:**
  - GigabitEthernet 1(to C-SWC G0/1): Configure as a trunk allowing only VLANs 60 and 70.
  - GigabitEthernet 2(to TELLER-SWC G1): Configure as a trunk allowing only VLANs 60 and 70.
- **Wireless Configuration:**
  - Configure the Wireless LAN (WLAN) to provide connectivity for the VISITOR-NET(VLAN 70).
  - **SSID:**Can be a descriptive name like YOUR_STUDENT_ID_GUEST_WIFI.
  - **Security:**Implement a strong security protocol (e.g., WPA2-PSK) with a secure passphrase.
  - Ensure devices in VISITOR-NETcan obtain IP addresses from the DHCP server (Main-Router) and connect to the network.

TELLER-SWC

- **VTP Configuration:**
  - vtp version 2
  - vtp mode client
  - vtp domain your_student_ID.f25
  - vtp password your_student_ID
- **Connections:**
  - GigabitEthernet 1(to HomeRouter-PT-AC G2): Configure as a trunk allowing only VLANs 60 and 70.
- **Access Ports:**Connect TELLER computers to access ports in VLAN 60, with Port Security, PortFast, BPDU Guard.

Server Specific Configurations

WEB SERVER (192.168.100.100/28)

- **IP Configuration:**Set static IP address, subnet mask, and default gateway.
- **DNS Server:**Set AD/DC server (168.80.10) as its DNS server.
- **HTTP Service:**
  - Enable the HTTP service.
  - Edit the htmlfile to display the following content, centrally aligned:

- **DNS Registration:**Ensure that the AD/DC server (acting as the DNS server) has an A record configured to resolve f25 to the WEB SERVER's IP address (192.168.100.100).

AD/DC SERVER (192.168.80.10/28)

- **IP Configuration:**Set static IP address, subnet mask, and default gateway.
- **DNS Service:**
  - Enable the DNS service.
  - Configure it to resolve f25to 192.168.100.100 (the WEB SERVER).
  - It will serve as the primary DNS for all clients.

NET-MONITORING SERVER (192.168.90.11/28)

- **IP Configuration:**Set static IP address, subnet mask, and default gateway.
- **NTP Service:**
  - Enable the NTP service on this server.
  - Set the correct current date and time (e.g., 2025-10-19) for this server. All network devices wil synchronize their clocks with this server.

Other Servers (CBS, EDWH, SYSLOG, SIEM)

- **IP Configuration:**Set static IP address, subnet mask, and default gateway for each as per the "Server IPs Table".
- **DNS Server:**Set AD/DC server (168.80.10) as their DNS server.
- No other specific services are required on these servers unless necessary for ACL testing (e.g., FTP on CBS).

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 12345_Standard_ACL). 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 (inor 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 <YourStudentID>_Standard_Visitor_Block

- **Rules:**Deny all traffic originating from 168.70.0/28.
- **Application:**Apply inbound on the GigabitEthernet 0/0.70 sub-interface.

- **Extended ACLs (Named):**
  1. **Objective:**Allow VISITOR/CLIENT Network (VLAN 70) to access WEB SERVER (HTTP) and AD/DC SERVER (DNS) *only*.
     - **Name:**IP access-list extended <YourStudentID>_Extended_Visitor_Access
     - **Rules:**
       - Permit TCP traffic from 168.70.0/28to 192.168.100.100 (WEB SERVER) on port 80 (HTTP).
       - Permit UDP traffic from 168.70.0/28to 192.168.80.10 (AD/DC) on port 53 (DNS).
       - Explicitly deny all other traffic from 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.* Consider using this extended ACL *instead* of a standard ACL if it's more precise. If using both, the standard ACL would block *everything*, so you'd need to permit traffic using this ACL first, and then deny. A better approach might be to just use this extended ACL, permitting HTTP/DNS and then having an implicit deny for everything else.
  2. **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 <YourStudentID>_Extended_ADDC_Access
     - **Rules:**
       - Permit IPtraffic from 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 168.80.10 (AD/DC).
       - Permit UDPtraffic (DNS) from any (or specific subnets excluding 70) to 168.80.10 (AD/DC) on port 53.
       - Deny all other traffic to 168.80.10.
     - **Application:**Apply outbound on the GigabitEthernet 1/0.80 sub-interface (towards the AD/DC server).
  3. **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 <YourStudentID>_Extended_CBS_Access
     - **Rules:**
       - Permit IPtraffic from 168.10.0/28 (IT-NET) to 192.168.80.11 (CBS). (Full access for IT-NET).
       - Permit TCPtraffic from any (or specific subnets excluding 70) to 168.80.11 (CBS) on ports 20 and 21 (FTP).
       - Deny all other traffic to 168.80.11.

    - **Application:**Apply outbound on the GigabitEthernet 1/0.80 sub-interface.
4. **Objective:**Allow **only** IT-NET to access EDWH SERVER.
    - **Name:**IP access-list extended <YourStudentID>_Extended_EDWH_Access
    - **Rules:**
        - Permit IPtraffic from 168.10.0/28 (IT-NET) to 192.168.80.12 (EDWH).
        - Deny IPtraffic from any to 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 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.

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)

Testing Strategy

1. **Test within same VLAN first**(ping between computers in same VLAN)
2. **Then test cross-VLAN routing**(ping between different VLANs)
3. **Then test DNS resolution**(ping by hostname)
4. **Then test web accessibility**(browse web page)
5. **Then test security**(verify ACL filtering)
6. **Finally test services**(NTP, SYSLOG, FTP)