التكنولوجيا التطبيقية
APPLIED TECHNOLOGY
وزارة التربية والتعليم والتعليم الفني

مدارس we للتكنولوجيا التطبيقية

شبكات و امن معلومات
الصف الثالث

IT Department
Networks & Cybersecurity

Networks and Cybersecurity
Final Project

2st

2025 - 2026

1. Hostname Configuration

Configure the **hostname** of each device according to the **network topology**

All device names **must match exactly** as specified (case-sensitive).

2. Console Password Configuration

To ensure secure local access to all network devices, **console line passwords must be configured** according to the device role as outlined below.

The login command **must be enabled** on all console lines.

Passwords **must be entered exactly as specified**, including uppercase letters, lowercase letters, numbers, and special characters.

A- Access Switches

- All **Access Switches** shall be configured with the following console password: **AC-CON@admin12026**

B- Multilayer (Distribution) Switches

- All **Multilayer Switches** shall be configured with the following console password: **ML-CON@admin22026**

C- Core Switches

- All **Core Switches** shall be configured with the following console password: **CO-CON@admin32026**

D- Routers

- All **Routers** shall be configured with the following console password: **RO-CON@admin42026**

3. Privileged EXEC Mode Security (Enable Password)

To secure access to **Privileged EXEC mode**, all network devices **must be configured with an enable password** according to their functional role.

Enable Password Requirements

A- Access Switches

- All **Access Switches** shall be configured with the following enable password: **AC-Enpr@admin12026**

B- Multilayer (Distribution) Switches

- All **Multilayer Switches** shall be configured with the following enable password: **ML-Enpr@admin22026**

C- Core Switches

- All **Core Switches** shall be configured with the following enable password: **CO-Enpr@admin32026**

D- Routers

- All **Routers** shall be configured with the following enable password: **RO-Enpr@admin42026**

4. Password Encryption

To ensure that all passwords configured on the devices (console, VTY, and enable passwords) are **not stored in plain text**, the **service password-encryption** command **must be applied to all devices**.

5. Local User Account Configuration

To allow authenticated access to network devices, **a local user account must be configured** on all devices with the following credentials.

User Account Requirements

- **Username:** NetAdmin
- **Password:** N3C@Admin!2026

6. Assign IP addresses to all network devices according to the provided IP addressing table:

DEVICE	Interface	IP address
HQ-DSW1	G1/0/1	10.20.20.33/30

HQ-DSW2	G1/0/1	10.20.20.37/30
HQ-CORE	G1/0/1	105.100.50.2/30
	G1/0/2	10.20.20.34/30
	G1/0/3	10.20.20.38/30
	G1/0/4	10.10.10.1/24
R1	G0/1	105.100.50.1/30
	G0/0	20.20.20.2/30
R2	G0/1	20.20.20.1/30
	G0/0	30.30.30.1/30
R3	G0/1	30.30.30.2/30
	G0/0	205.200.100.1/30
BR-CORE	G1/0/3	205.200.100.2/30
	G1/0/1	10.20.20.42/30
	G1/0/2	10.20.20.46/30
BR-DSW1	G1/0/6	10.20.20.45/30
BR-DSW2	G1/0/6	10.20.20.41/30

7. VLAN Trunking Protocol (VTP) Configuration

To ensure VLAN consistency across the network, all **Access and Distribution switches** must be configured with **VTP according to the following requirements**.

- All switch-to-switch links connecting VTP-enabled switches **must be configured as trunk ports**.
- The VTP password **must match exactly** on all switches within the same VTP domain as required.
- Using **VTP version 2** provides support for extended VLANs and consistency checks.

VTP Requirements

Domain and Version

- **VTP Domain Name:** Nass.com
- **VTP Version:** 2
- **VTP Password:** VTPpass@admin2026

VTP Mode

- **HQ-DSW1** shall operate in **server mode**, with all other HQ switches set to **client mode**.
- **BR-DSW1** shall operate in **server mode**, with all other BR switches set to **client mode**.

Scope

- Configuration applies to all **Access Switches** and **Distribution (Multilayer) Switches** in both HQ and BR sites.
- Core switches do **not participate** in VTP.

8. VLAN Configuration

To segment the network and organize departments, **VLANs must be created on the distribution switches** at each site according to the specifications below.

- All VLANs must be **created only on the distribution switches (HQ-DSW1 and BR-DSW1)**.
- VLAN names **must match exactly**, including capitalization.
- VLAN IDs **must be unique and correctly assigned** according to the table.
- VLAN propagation to access switches is handled automatically via **VTP** (configured in previous step).

VLAN Requirements

HQ Site – HQ-DSW1

Create the following VLANs on **HQ-DSW1**:

VLAN ID	VLAN Name
10	Engineers
20	Management
30	Finance
40	IT

BR Site – BR-DSW1

Create the following VLANs on **BR-DSW1**:

VLAN ID	VLAN Name
60	Maintenance
70	HR
80	Sales

9. Inter-VLAN Routing (SVI) Configuration

To enable communication **between VLANs within the same site**, **Switched Virtual Interfaces (SVIs)** must be configured on the distribution switches at HQ and BR sites.

Each VLAN SVI **must have a unique IP address** within its subnet.

The SVI must be **enabled with no shutdown** to allow inter-VLAN routing.

Configuration Notes

1. Each VLAN SVI **must have a unique IP address** within its subnet.
2. The SVI must be **enabled with no shutdown** to allow inter-VLAN routing.
3. Routing between these VLANs will be handled by the **Layer 3 capability** of the distribution switches (ML switches).

HQ Site – HQ-DSW1

- **VLANs:** 10, 20, 30, 40, 50
- **Purpose:** Allow connectivity between VLANs 10, 20, 30, 40,

Device	Int VLAN 10	Int VLAN 20	Int VLAN 30	Int VLAN 40
HQ-DSW1	192.168.10.1/24	192.168.20.1/24	192.168.30.1/24	192.168.40.1/24
HQ-DWS2	192.168.10.2/24	192.168.20.2/24	192.168.30.2/24	192.168.40.2/24
HQ-ASW1	192.168.10.3/24			
HQ-ASW2		192.168.20.3/24		
HQ-ASW3			192.168.30.3/24	
HQ-ASW4				192.168.40.3/24

BR Site – BR-DSW1

- **VLANs:** 60, 70, 80
- **Purpose:** Allow connectivity between VLANs 60, 70, and 80.

Device	Int VLAN 60	Int VLAN 70	Int VLAN 80
BR-DWS1	192.168.60.1/24	192.168.70.1/24	192.168.80.1/24
BR-DSW2	192.168.60.2/24	192.168.70.1/24	192.168.80.2/24
BR-ASW1	192.168.60.3/24		
BR-ASW2		192.168.70.3/24	
BR-ASW3			192.168.80.3/24

10.

EtherChannel Configuration

To provide **high-speed redundant links** between distribution switches, **EtherChannel (Port-Channel) links** must be configured at HQ and BR sites.

Purpose: Aggregate multiple physical links into a single logical link for redundancy and higher bandwidth.

All physical interfaces in the EtherChannel must have the same speed, duplex, and VLAN configuration.

Requirements

HQ Site: HQ-DSW1 to HQ-DSW2

- **Protocol:** LACP (Link Aggregation Control Protocol)

BR Site: BR-DSW1 to BR-DSW2

- **Protocol:** PAGP (Port Aggregation Protocol)

11. HSRP Redundancy Configuration

To ensure **default gateway redundancy** for client VLANs at HQ and BR sites, **HSRP must be configured between the distribution switches**.

HSRP ensures **high availability** of the default gateway for all connected VLANs.

HSRP must be configured per VLAN to ensure clients in each VLAN have a highly available default gateway.

Priority settings determine the active and standby device:

Set the **priority of the intended active device higher** than the standby.

Requirements

HQ Site – HQ-DSW1 & HQ-DSW2

- **Purpose:** Provide a redundant default gateway for all HQ VLANs (10, 20, 30, 40,).
- **Active Device:** HQ-DSW1
- **Standby Device:** HQ-DSW2
- **Virtual IP Address:** Assign a virtual gateway IP for each VLAN

VLAN ID	Network Subnet	VirtualIP (Gateway)	HSRP Group
VLAN 10	192.168.10.0/24	192.168.10.10	10
VLAN 20	192.168.20.0/24	192.168.20.10	20
VLAN 30	192.168.30.0/24	192.168.30.10	30
VLAN 40	192.168.40.0/24	192.168.40.10	40

BR Site – BR-DSW1 & BR-DSW2

- **Purpose:** Provide a redundant default gateway for all BR VLANs (60, 70, 80).
- **Active Device:** BR-DSW1
- **Standby Device:** BR-DSW2
- **Virtual IP Address:** Assign a virtual gateway IP for each VLAN

VLAN ID	Network Subnet	VirtualIP (Gateway)	HSRP Group
VLAN 60	192.168.60.0/24	192.168.60.10	60
VLAN 70	192.168.70.0/24	192.168.70.10	70
VLAN 80	192.168.80.0/24	192.168.80.10	80

12. Rapid Spanning Tree Protocol (RSTP) Configuration

To prevent **Layer 2 loops** and ensure **fast convergence** in the network, **RSTP must be enabled on all switches** in both HQ and BR sites.

RSTP should be enabled globally or per VLAN as needed.

Ensure that **all trunk and access ports participate in RSTP**

Requirements

- **Protocol:** Rapid Spanning Tree Protocol (802.1w)
- **Scope:** All switches in the topology, including:
    - Access Switches (HQ-ASW1–5, BR-ASW1–3)
    - Distribution Switches (HQ-DSW1–2, BR-DSW1–2)

13. PortFast Configuration

To **allow end devices PCs to connect immediately without waiting for STP convergence**, **PortFast must be enabled on all access ports** connected to end devices.

PortFast **should only be enabled on ports connected to end devices**, not on uplinks between switches.

14. DHCP Server Configuration-HQ-SITE

To dynamically assign IP addresses to clients in the HQ network, a DHCP server must be configured on Server 10.10.10.6 according to the following specifications.

Excluded addresses ensure static IPs or important devices are not assigned dynamically.

DHCP must provide the default gateway for each VLAN so that clients can communicate across VLANs.

DHCP pools must match VLAN subnets exactly.

DHCP Requirements

- Server Location: Server 10.10.10.6
- Purpose: Provide dynamic IP addressing to client devices in each VLAN.
- Address Pools and Exclusions:

VLAN 10 – Engineers

- **Network**: 192.168.10.0 /24
- **Default Gateway**: 192.168.10.10
- **Excluded IPs**: 192.168.10.1 – 192.168.10.50
- **WLC**: 192.168.40.100

VLAN 20 – Management

- **Network**: 192.168.20.0 /24
- **Default Gateway**: 192.168.20.10
- **Excluded IPs**: 192.168.20.1 – 192.168.20.50
- **WLC**: 192.168.40.100

VLAN 30 – Finance

- **Network**: 192.168.30.0 /24
- **Default Gateway**: 192.168.30.10
- **Excluded IPs**: 192.168.30.1 – 192.168.30.50
- **WLC**: 192.168.40.100

VLAN 40 – IT

- **Network**: 192.168.40.0 /24
- **Default Gateway**: 192.168.40.10

- **Excluded IPs**: 192.168.40.1 – 192.168.40.50
- **WLC**: 192.168.40.100

14-2. DHCP Server Configuration– BR Site

To provide **dynamic IP addressing** for client VLANs at the BR site the following requirements must be implemented on **BR-DSW1** and **BR-DWS2**

Ensure DHCP pools **match the correct VLAN subnets**.

Exclude IPs for static devices to **prevent IP conflicts**.

DHCP Requirements – BR Site

- **Server Location: BR-DSW1 ,BR-DWS2** (DHCP services are configured on both distribution switches BR-DSW1 and BR-DSW2)
- **Purpose:** Dynamically assign IP addresses to clients.

VLAN 60 – Maintenance

- **Network:** 192.168.60.0 /24
- **Default Gateway:** 192.168.60.10
- **Excluded IPs:** 192.168.60.1 – 192.168.60.50

VLAN 70 – HR

- **Network:** 192.168.70.0 /24
- **Default Gateway:** 192.168.70.10
- **Excluded IPs:** 192.168.70.1 – 192.168.70.50

VLAN 80 – Sales

- **Network:** 192.168.80.0 /24
- **Default Gateway:** 192.168.80.10
- **Excluded IPs:** 192.168.80.1 – 192.168.80.50

15-OSPF Routing Configuration – Area 0

To enable **dynamic routing between routers , distribution and core switches**, **OSPF must be configured using Area 0** as the backbone.

1. Assign **all connected networks** on routers and Layer 3 switches to OSPF Area 0.
2. Use **router IDs** for clarity (manually or automatically assigned).

Requirements

- **Routing Protocol:** OSPF (Open Shortest Path First)
- **OSPF Area:** 0 (backbone area)
- **Scope:** All routers (R1, R2, R3) and **distribution and core switches**
- **Purpose:**
    - Automatically share routing information between HQ and BR sites.
    - Ensure connectivity between all VLANs and remote networks.

16- Unused Ports Security

All switch ports that are not actively connected to an authorized device (PC, Printer, AP, or Server) must be manually disabled to minimize the attack surface and prevent unauthorized physical access to the network

17-Port Security Configuration

To enhance Layer 2 security, **Port Security must be applied on all access ports connected to end devices** on all Access Switches.

Port Security **must only be applied on end-device ports**, not uplinks.

Sticky MAC addresses allow the switch to **remember connected devices across reboots**.

- **Purpose:**
    - Prevent unauthorized devices from connecting to the network.
    - Automatically learn and secure legitimate MAC addresses.

Requirements

- **Scope:** All **access ports** on Access Switches (HQ-ASW1–5, BR-ASW1–3) connected to end devices.
- **Learning Mode:** MAC addresses **must be learned dynamically and saved as sticky** (sticky option).
- **Violation Modes:**
    - **HQ Access Switches:** Violation mode set to shutdown (port is automatically disabled if a violation occurs).
    - **BR Access Switches:** Violation mode set to restrict (traffic from violating MAC is blocked, but port remains up).

18. DHCP Snooping & Dynamic ARP Inspection Configuration

To **protect the network from DHCP spoofing and ARP poisoning attacks**, the following security features must be enabled on all Layer 2 switches.

18.1: DHCP Snooping

Purpose: Prevent unauthorized DHCP servers from issuing IP addresses (DHCP spoofing).

Requirements:

- **Enable DHCP snooping globally** on all Access and Distribution switches.
- **Enable DHCP snooping per VLAN** (all VLANs with DHCP pools).
- **Trusted Ports:**
    - **Uplink ports** toward DHCP servers (HQ-DSW1 for HQ, BR-DSW1 for BR)
- **Untrusted Ports:**
    - All other access ports (connected to end devices).

18.2: Dynamic ARP Inspection (DAI)

Purpose: Prevent ARP spoofing/poisoning attacks on the network.

Requirements:

- **Enable DAI globally** and per VLAN on all switches.
- **Trusted Ports:**
    - Ports toward DHCP servers and distribution switches
- **Untrusted Ports:**
    - All access ports connected to end devices

19. Remote Access

Secure remote access by enabling SSH only on all devices, generating keys, setting exec-timeout, and disabling Telnet.

Requirements:

- Set the device domain name to we.com.
- Generate RSA crypto keys with key size 2048 bits.
- Configure a local username and password for SSH login.
- Configure all vty lines to:
    - Allow SSH only
    - Use local login
    - Set exec-timeout 2 minutes
    - Ensure SSH service is active on the device.
    - Disable Telnet access on all vty lines

20. Access Control List (ACL) Configuration

Configure a Named Extended Access Control List **on the** HQ-Core switch **to enhance the security of the Server network.**

Requirements:

- **Create a Named Extended ACL.**
- Deny ICMP **traffic from any source to the server network.**
- Deny HTTP **traffic from any source to the server network.**
- Permit all other traffic **to ensure normal network operation.**
- **Apply the ACL on the** HQ-Core **device in the appropriate direction to control traffic destined to the servers**

21. Wireless Configuration:

21-1:WLC & Lightweight AP Configuration – HQ Site

To provide centralized wireless management and control, a Wireless LAN Controller (WLC) must be deployed at the HQ site to manage all Lightweight Access Points (LWAPs).

- Configure the WLC to manage all **Lightweight Access Points**.
- Configure SSIDs, security policies, and VLAN mapping on the WLC.
- Configure the **WLC Management Interface**:
  - IP address : 192.168.40.100
  - Default gateway = **virtual IP for vlan 40**
- Ensure all APs obtain IP addresses via **DHCP**.
- Ensure APs automatically discover and **join the WLC**.
- Verify all APs are **Joined** on the WLC.
- Verify wireless clients can connect to the configured **SSIDs**

21.2 Stand-Alone Wireless Access Point Configuration – BR Site

To provide **wireless connectivity** for users in each BR VLAN, **stand-alone Access Points (APs)** must be deployed and configured accordingly.

Configuration Requirements

- Each access point **must be connected to an access switch port** configured as:
  - **Access mode**
  - Assigned to the **corresponding VLAN**
- Each AP shall broadcast a **unique SSID** mapped to its VLAN.
- Wireless clients must receive IP addresses via **DHCP**
- AP management IP addresses **must belong to the same VLAN** as the SSID.
- Appropriate **security settings** (WPA2-PSK or WPA2-Enterprise) should be enabled.

22-Syslog Server Configuration

To centralize logging and monitor network events, **all network devices must forward logs to a dedicated Syslog server**.

Requirements

- **Syslog Server IP:** 10.10.10.7
- **Scope:** All switches (Access, Distribution, Core) and routers (R1, R2, R3)
- **Purpose:**
    - Collect device logs centrally for monitoring and troubleshooting.
    - Ensure all critical events, such as interface status changes, port security violations, and HSRP changes, are logged.

23. NTP Server Configuration

To ensure **accurate and synchronized system time** across all network devices, **an NTP server must be configured** for centralized time synchronization.

All devices **must synchronize their clocks** with the specified NTP server.

Time synchronization is critical for Syslog analysis, Security auditingNetwork troubleshooting

Requirements

- **NTP Server IP Address:** 10.10.10.8
- **Scope:**
    - All Access Switches
    - Distribution (Multilayer) Switches
    - Core Switches
    - Routers (R1, R2, R3)
- **Purpose:**
    - Maintain consistent timestamps for **Syslog messages**, **security events**, and **troubleshooting**
    - Support accurate log correlation across devices

24. Backup Configuration to TFTP Server

To ensure **network configuration safety and quick recovery**, all devices must **backup their running or startup configurations** to a TFTP server.

TFTP server must be reachable from all devices.

Save either **running-config** or **startup-config** as needed.

Use a **unique filename per device** to avoid overwriting backups.

Requirements

- **TFTP Server IP:** 10.10.10.9
- **Scope:** All switches (Access, Distribution, Core) and routers (R1, R2, R3)
- **Purpose:**
    - Store configuration files centrally for disaster recovery.
    - Allow easy restoration of device configurations in case of failure.

📦 Project Submission

1. To complete the project successfully, submit the following:
2. Network Topology File: Packet Tracer (.pkt) Fully configured and saved.
3. Device Configuration Document: All running configurations exported into one organized PDF file
4. Verification & Testing Report (Screenshots – PDF): Provide labeled screenshots proving functionality.

📊 Evaluation Criteria

- Configuration Accuracy – 40%
- Network Functionality – 25%
- Security & Redundancy – 15%
- Documentation Quality – 10%
- Troubleshooting Evidence – 10%

🗓️ Deadline [30/3/2026]

Submission Package

Submit one compressed folder containing:

- Project file (.pkt or equivalent)
- Configuration document
- Screenshot report