Case Study: Al-Nahda University in Egypt (NUB) – ICT Infrastructure Overhaul

---

Basic Knowledge

Al-Nahda University in Egypt (NUB) is a prestigious institution with two campuses located 160 kilometers apart—one in Cairo and another in Beni Suef. The university is renowned for its wide range of academic programs across four major faculties:

- Health and Sciences
- Business
- Engineering and Computing
- Arts and Design

As part of its commitment to providing state-of-the-art resources for its growing student population, the university is undergoing an ambitious ICT infrastructure overhaul. This project focuses on ensuring high-performance, secure, and scalable networking across both campuses.

Current Situation

1. **User Community**:
   NUB currently has around 35,000 students, staff, and faculty members who rely on the university's IT systems for education, communication, and research. The administration plans to double this number by 2025, placing significant demands on the university's IT infrastructure.
2. **Main Campus IT Department**:
   The main campus in Cairo houses the central IT department. This team is responsible for managing both campuses and ensuring a seamless connection between them.
3. **Technology Infrastructure**:
   The Cairo campus has a Demilitarized Zone (DMZ) that hosts several key servers, including
   - DHCP (for dynamic IP address assignment)
   - DNS (for resolving domain names)
   - FTP (for file sharing)
   - Web Server (for hosting university websites)
   - Email and SMTP (for email services)
4. **Secure Access for Branch Campus**:
   The branch campus in Beni Suef securely connects to the main campus DMZ via a dedicated network link, ensuring that students and staff can access critical resources from anywhere.

Planned ICT Upgrade

The current network setup works but is not robust enough to handle the expected increase in users and devices. The upgrade will focus on:

- Increased network capacity and segmentation using VLANs to improve security and performance.
- High availability and redundancy to ensure no downtime in communication between the campuses.
- Enhanced security to prevent unauthorized access and cyberattacks.

Infrastructure Details

1. **Internet Connectivity**:
   NUB has an agreement with Vodafone Egypt for its internet services.
2. **Core Networking Components**:
   - **Routers**: Two Cisco ISR 4000 Series routers—one at each campus to protect internal networks and manage external connections, replacing the previous firewalls.
   - **Core Switches**: Two Catalyst 3650 48-Port switches at each campus to handle the main network traffic.
   - **Access Switches**: For each department, Catalyst 2960 48-Port switches are deployed to handle local traffic.
3. **Server and Virtualization**:
   NUB runs two physical servers at each campus for virtualization. These servers host redundant DHCP and DNS services to ensure continuous operation.
4. **Wireless Access**:
   Wireless connectivity across both campuses is managed by two Cisco Wireless LAN Controllers (WLC) and multiple Lightweight Access Points (LAPs), providing strong Wi-Fi access for students and staff.
5. **IP Addressing Scheme**:
   - Main Campus (Cairo): 172.16.0.0/16 for LAN.
   - Branch Campus (Beni Suef): 172.17.0.0/16 for LAN.
   - Management in main campus : 192.168.10.0/24
   - Wireless Network (WLAN) in main campus: 10.10.0.0/16.
   - Wireless Network (WLAN) in Branch: 10.11.0.0/16.
   - DMZ Servers: 10.20.20.0/27.
   - Public Addresses: 105.100.50.0/30 (Cairo) and 205.200.100.0/30 (Beni Suef).

Project Scope

This project is carried out by a dedicated team of six IT professionals. Their goal is to implement an upgraded and secure network infrastructure for the growing university. Each team member is responsible for a specific part of the project.

Detailed Tasks for Each Week

Week 1: Network Building and Basic Configuration

1. **Basic Network Topology Setup**:
    - Create the Network Topology in Cisco Packet Tracer that includes both campuses.
    - Connect the devices (switches, routers) as per the hierarchical design: DMZ servers, core switches, and access switches.
    - ISP Connectivity: Configure the Airtel ISP router to provide internet access for both campuses, connected via routers.
2. **IP Address Assignment**:
    - **Subnet the Network**:
        - Assign IP address ranges for each department's VLAN, as outlined in the case study.
        - For LAN users:
            - Main Campus: 10.10.0.0/16
            - Branch Campus: 10.11.0.0/16
        - For WLAN users:
            - 192.168.10.0/24
        - For DMZ servers:
            - 10.20.20.0/27
        - For Voice communication (VoIP):
            - Main Campus: 172.16.0.0/16
            - Branch Campus: 172.17.0.0/16
        - For public addresses (for external connections):
            - Main Campus: 105.100.50.0/30
            - Branch Campus: 205.200.100.0/30
    - Assign IP addresses to each device, including servers, switches, and other network infrastructure, according to the subnets defined.
3. **Switch Configuration**:
    - **Assign Hostnames and Basic Settings**:
        - Configure hostnames, banners, and passwords for each network device.
        - Apply basic security settings like SSH for remote access to devices.
    - Enable IP Routing on core switches to allow routing between VLANs for inter-departmental communication.
4. **DHCP Server Configuration**:
    - Configure DHCP servers in the DMZ to dynamically assign IP addresses to LAN and WLAN users.
    - Ensure redundancy by running two DHCP servers and enabling failover.

Week 2: VLANs, Inter-VLAN Routing, and DHCP

1. **VLAN Configuration**:
    - Create VLANs in main campus:
        - VLAN 10: MANAGEMENT
        - VLAN 20: LAN USERS
        - VLAN 50: WIRELESS USERS
        - VLAN 199: BACKHOLE
    - Create VLANs in BRANCH CAMPUS:
        - VLAN 60: LAN USERS
        - VLAN 90: WIRELESS USERS
        - VLAN 199: BACKHOLE
    - Assign these VLANs to segment traffic by department and enforce security.
2. **Inter-VLAN Routing**:
    - Enable routing between VLANs on core switches at both campuses.
    - Assign IP addresses to each VLAN interface (SVI) for routing purposes, so that communication can take place between VLANs when necessary.
3. **DHCP Services**:
    - Configure DHCP on the servers to automatically assign IP addresses to devices in each VLAN. Ensure the DHCP server can assign addresses for each department and VLAN across both campuses.
    - Implement DHCP relay agents if necessary to ensure VLANs can communicate with DHCP servers.

Week 3: Security Features, VLAN ACLs, and Wireless Infrastructure

1. **Wireless LAN Configuration**:
    - Configure Cisco Wireless LAN Controllers (WLC) at both campuses to manage Lightweight Access Points (LAPs) and provide Wi-Fi access.
    - Assign the 10.10.0.0/16 IP range for WLAN users and integrate them with the wired network for seamless communication.
2. **Network Security**:
    - Apply Access Control Lists (ACLs) on switches and routers to control which VLANs can communicate with each other.
3. **Advanced Security Measures**:
    - Implement DHCP Snooping to prevent rogue DHCP servers from providing incorrect IP addresses.
4. **Documentation of Configurations**:
    - Maintain detailed records of all configurations, changes, and security policies implemented throughout the project.

Week 4: Testing, Monitoring, and Final Presentation

1. **Network Testing**:
   - Perform comprehensive testing of the network to ensure all devices are connected, VLANs are correctly configured, and inter-VLAN routing is functioning.
2. **Monitoring Tools**:
   - Implement network monitoring tools to continuously check performance and security status.
   - Set up logging and alerts for any unusual activities detected on the network.
3. **Final Presentation**:
   - Prepare a comprehensive presentation detailing the completed project, showcasing the enhanced ICT infrastructure and its benefits to the university community.

Team Members and Task Assignments

1. **Taha Abd-AlWadod Hassan**:
   - **Basic Network Setup**:
     - Created the network topology in Cisco Packet Tracer.
     - Configured basic settings on network devices (hostnames, passwords, banners).
     - Assigned IP addresses for each subnet (LAN, WLAN, DMZ, Public).
   -
2. **Mohamed Hesham Mohamed**:
   - **VLAN Configuration**:
     - Configured on all switches.
     - Assigned VLANs to interfaces on switches across both campuses.
   - **Inter-VLAN Routing**:
     - Set up routing between VLANs on core switches.
     - Assigned IP addresses to VLAN interfaces for inter-department communication.

     DHCP Server Configuration:
     - Set up DHCP servers for automatic IP addressing.
     - Ensured redundancy between DHCP servers.
3. **Ahmed Mohamed Saad El-Raggal**:
   - **Wireless LAN Infrastructure**:
     - Configured the Wireless LAN Controllers (WLC) and Lightweight Access Points (LAPs).
     - Assigned the WLAN IP range and ensured seamless connectivity between wired and wireless networks.
   - **Access point configuration**:
     - Configured the Lightweight Access Points (LAPs).
     - Configured all the wireless devices.
4. **Esmael Mamdoh Sedky Ahmed**:
   - **VLAN and ACL Security**:
     - Applied Access Control Lists (ACLs) to control communication between VLANs (e.g., blocking Guest from accessing internal resources).
   - **Public Access Configuration**:
     - Assigned public IP addresses to relevant services and ensured secure access.
5. **Momen Osama Mohamed**:
   - **subnetting and IP address:**
     Configured optimized subnetting and IP addressing scheme to ensure efficient allocation of IP resources and reduce wastage. Set up network segmentation with customized subnets, enhancing both traffic management and security across various departments.
   - **Advanced Campus Network Design:**
     Configured subnetting and IP addressing scheme for WLAN, LAN, Management, and DMZ networks across HQ and branch locations Set up default gateways and broadcast addresses to optimize network traffic flow and ensure efficient routing.

6. **Hamza Mohamed Sanad**:
   - **High Availability & Redundancy**:
     - Configured Hot Standby Router Protocol (HSRP) for redundancy on core switches.
     - Set up EtherChannel and Spanning Tree Protocol (STP) for high availability and load balancing between switches.
   - **Final Testing and Documentation**:
     - Prepared the final presentation and compiled network diagrams, security testing results, and lessons learned.

Design and Implementation: