Project Report: Securing and Scaling the Network Infrastructure for ITC University

Prepared by: Mustafa Elsayed, Nasr Salah, Mohamed Abdelhamid, Hossam Ahmed

Table of Contents

1. Introduction

ITC University operates across two campuses, providing services to approximately 25,000 users across multiple faculties. The university's growth forecast suggests a doubling of this number by 2030, necessitating a scalable, secure, and reliable network infrastructure. This project focuses on designing and implementing an optimized network architecture to address the needs of the current and future user base, ensuring high performance, security, and scalability.

2. Project Objectives

The core objectives of the project are:

- **Network Scalability**: Design a network capable of supporting a growing user base with ease of future expansion.
- **Security**: Implement security measures to protect the confidentiality, integrity, and availability (CIA) of university data.
- **Redundancy**: Ensure high availability through redundancy and failover mechanisms to minimize downtime.
- **Seamless Connectivity**: Facilitate secure communication between the two campuses.
- **Robust Management**: Provide a well-managed network with VLANs, firewalls, and access controls to ensure performance and security.

3. Network Design Overview

Topology and Hierarchical Design

The network follows a **hierarchical design model** to enhance scalability, redundancy, and ease of management. The design comprises three layers:

1. **Core Layer**: Centralized on the main campus with core multilayer switches (Catalyst 3650), handling both routing and switching functionalities.
2. **Distribution Layer**: Interconnecting various VLANs and facilitating inter-VLAN routing via multilayer switches.
3. **Access Layer**: Serving individual faculties and departments via Catalyst 2960 switches.

This hierarchical approach ensures that the network is both scalable and easy to manage, with clear separation of traffic and optimized performance.

The network employs several advanced protocols and technologies to ensure optimal performance, security, and scalability, including:

- OSPF (Open Shortest Path First) for dynamic routing
- LACP EtherChannel for link aggregation and increased bandwidth
- HSRP (Hot Standby Router Protocol) for redundancy and high availability
- STP PortFast and BPDUguard to mitigate network loops and improve port transitions
- ACL (Access Control Lists) for fine-tuned traffic management and security
- VLAN segmentation for traffic isolation and improved security
- NAT (Network Address Translation) for IP address management and external connectivity
- CAPWAP (Control And Provisioning of Wireless Access Points) for centralized control of wireless networks
- DHCP (Dynamic Host Configuration Protocol) for automated IP address allocation
- HTTP and DNS services for web and domain name resolution

VLAN Segmentation

VLANs are used to segment the network logically and increase security:

- **VLAN 10**: Management VLAN (192.168.10.0/24)
- **VLAN 20 , 60**: LAN VLAN (172.16.0.0/16 for the main campus, 172.17.0.0/16 for the branch)
- **VLAN 50 , 90**: WLAN VLAN (10.10.0.0/16 for the main campus, 10.11.0.0/16 for the branch)
- **VLAN 199**: Blackhole VLAN for unused ports

Inter-VLAN routing is achieved using the core multilayer switches.

4. Implementation Phases

Phase 1: Planning and Requirements Gathering

- **Goal**: Identify the current and future network requirements, including user base growth and security considerations.
- **Key Actions**:
    - Meeting with university IT staff to understand operational needs.
    - Assessing current network infrastructure to ensure it can scale for future needs.

Phase 2: Network Design and Scalability Considerations

- **Goal**: Design a network capable of supporting up to 50,000 users by 2030.
- **Design Highlights**:
    - **EtherChannel (LACP)** was implemented for link aggregation to improve bandwidth and redundancy.
    - **STP PortFast** and **BPDUguard** were enabled to protect against network loops and optimize port transitions.

Phase 3: Hardware and Software Configuration

- **Goal**: Configure core devices including firewalls, switches, wireless controllers, and IP addressing.
- **Hardware Setup**:
    - Cisco ASA 5506-X series firewalls for both campuses.
    - Catalyst 3650 and 2960 switches to support wired connections and facilitate VLANs.
    - Wireless LAN Controllers (WLC) to centralize the management of Lightweight Access Points (LAPs).
- **Software Setup**:
    - **OSPF** routing protocol was configured for dynamic route advertisement.
    - Basic settings such as hostnames, passwords, and SSH access control were implemented.

Phase 4: Security Enhancements

- **Goal**: Ensure secure communication and safeguard network resources.
- **Key Actions**:
    - **Cisco ASA Firewalls** were configured with security levels and access policies to define the network's security zones.
    - **Standard ACL for SSH** was established to restrict administrative access only to authorized personnel.

5. Key Technologies and Components

Firewalls and Security Zones

Each campus features a **Cisco ASA 5506-X firewall** to establish secure network segments. The DMZ (Demilitarized Zone) hosts critical servers such as DHCP, DNS, and web servers, which are secured and isolated from the rest of the network.

Routing and Switching Infrastructure

The network uses a combination of core switches for both routing and switching. Multilayer switches allow for both data forwarding and routing between VLANs. **EtherChannel** is implemented to bundle multiple physical links for increased bandwidth and redundancy.

Wireless LAN Infrastructure

The university's wireless network is managed centrally using **Wireless LAN Controllers (WLC)**, which control all **Lightweight Access Points (LAPs)**. This infrastructure ensures seamless wireless connectivity across campuses.

IP Addressing and Subnetting

The university has been allocated specific IP address ranges for each segment, with subnetting employed to optimize address allocation:

- Managemet: 192.168.10.0/24
- WLAN (Main): 10.10.0.0/16
- WLAN (Branch): 10.11.0.0/16
- DMZ: 10.20.20.0/27
- LAN: 172.16.0.0/16 (Main), 172.17.0.0/16 (Branch)
- Public: 105.100.50.0/30 (Main), 205.200.100.0/30 (Branch)

Network Components:

- 6 Servers
- 2 Firewalls
- 3 Routers (acting as Internet Service Providers, ISPs)
- 4 Multilayer Switches
- 10 Layer 2 Switches
- 1 Wireless LAN Controller
- 9 Access Points
- Up to 60,000 end-devices, including PCs, Laptops, Smartphones, Tablets, Printers…etc

6. Challenges and Solutions

- **Challenge**: Ensuring secure communication between campuses while maintaining high performance.
- **Solution**: Implemented a VLANs and access controls to ensure performance and security and used OSPF for efficient routing.
- **Challenge**: Providing a scalable solution for future growth.
- **Solution**: Designed the network with ample IP address space and modular VLAN segmentation for easy expansion.

7. Final Testing and Verification

Final testing included:

- **Inter-VLAN Routing**: Confirmed successful communication between VLANs.
- **ACL and Firewall Rules**: Tested access control lists to ensure proper restrictions and security policies.
- **Performance Testing**: Assessed network speed and reliability, verifying EtherChannel link aggregation and redundancy mechanisms.

8. Conclusion

The newly designed network for ITC is robust, scalable, and secure. It is capable of handling the anticipated growth, supports high availability through redundancy, and ensures secure communication across campuses. The system's hierarchical design, combined with modern technologies such as OSPF routing, VLAN segmentation, and EtherChannel, ensures the university is well-equipped for its future needs.