|  |
| --- |
| **Secure IT Company Network design**  **(IDS&IPS)**    **A Mini Project Report**  ***Submitted for***  **19EC651 – Computer Communication Networks Laboratory**    ***By***  **Jeyanthan GJ (Roll No.22BEC170 )**  **Selvaraj RS(Roll No.22BEC181 )**  **III Year B.E ECE C (VI Semester)**    **Department of Electronics and Communication Engineering Academic Year 2025**      **Mepco Schlenk Engineering College**  **(An Autonomous Institution Affiliated to Anna University, Chennai)**  **Mepco Engineering College (PO), Sivakasi – 626 005 Virudhunagar (District), Tamil Nadu**    **February 2025** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **TABLE OF CONTENTS**   |  |  |  | | --- | --- | --- | | **S.No.** | **CONTENTS** | **Page No.** | | 1 | Introductiom | 1 | | 2 | Case Study and Requirements | 1 | | 3 | Network Devics Description | 1 | | 4. | Technologies Implemented | 4 | | 5. | Device settings and configuration | 7 | | 6. | Implementation and progress | 9 | | 7. | Conclusion | 9 | |

Design and Implementation of a Secure Company

Network System

**Introduction**

This document outlines the design and implementation of a secure network system for Cytonn Innovation Ltd, a

forward

-

thinking company specializing in providing innovative cloud solutions globally. The project focuses on

creating a robust network infrastruc

ture to support various departments within the organization while ensuring

the security of sensitive data and resources.

**Case Study and Requirements**

Cytonn Innovation Ltd has a workforce of 600 staff and is preparing to move to a new building with three floors.

The building will host various departments, including Sales and Marketing, Human Resources, Finance, ICT, and a

Server Room. The ICT department

includes Software Developers, Cloud Engineers, Cybersecurity Engineers,

Network Engineers, System Administrators, IT Support Specialists, Business Analysts, and Project Managers.

Prior to the move, a new network service needs to be designed and implemented. The company aims to ensure

robust security against internal and external threats by implementing a multi

-

layered security approach, including

a firewall with distinct security z

ones: outside, inside, and DMZ.

**Network Devices Description**

**Cisco ASA Firewall**

Cisco Adaptive Security Appliance (ASA) is a security device that combines firewall, VPN, and other network

security services in a single platform. It provides advanced threat defense, intrusion prevention,

and protects the network from attacks by monitor

ing, controlling, and filtering traffic. Key features include:

-

Stateful packet inspection

-

Virtual Private Network (VPN) support

-

Intrusion Prevention System (IPS)



* Web filtering and malware defense
* Secure access control and user authentication

# Cisco Catalyst Switches (3850 & 2960)

Cisco Catalyst switches are enterprise-class switches designed for secure and scalable network access.

- Cisco Catalyst 3850: Stackable access switches with integrated wireless controller. Supports advanced features like high-performance Layer 3 routing and quality of service (QoS). Supports up to 480 Gbps stacking bandwidth. - Cisco Catalyst 2960: Layer 2 access switch for small to medium networks. Supports basic features like VLANs, STP (Spanning Tree Protocol), and port security. Energy-efficient and simple to deploy for cost-effective LANs.



# DHCP Server

A Dynamic Host Configuration Protocol (DHCP) server automatically assigns IP addresses and other network configuration parameters (like subnet masks and default gateways) to client devices. This reduces the need for manual IP configuration and ensures that devices in a network can communicate efficiently. Key functions include: - Automatic IP assignment

* IP address lease management
* DNS and gateway configuration

# DNS Server

A Domain Name System (DNS) server resolves human-readable domain names (like www.example.com) into machine-readable IP addresses. This process is essential for web browsing and network operations, as it allows devices to locate and communicate with others over the internet or internal networks. Key functions include: - Domain name resolution



* IP address mapping
* Caching previous lookups for faster responses

# FTP Server

A File Transfer Protocol (FTP) server enables the transfer of files between a client and a server over a network.

FTP is often used for uploading and downloading large files in business environments. Key features include:

* File sharing and storage
* Authentication and user access control
* Data encryption via secure FTP (SFTP)

# WEB Server

A web server hosts and delivers websites or web-based applications to users over the internet or

intranet. It processes incoming HTTP/HTTPS requests, interprets them, and sends the appropriate content (web pages, images, scripts). Commonly used web servers include Apache, Nginx, and Microsoft IIS. Key functions include:

* Serving static and dynamic content
* SSL/TLS encryption for secure connections - Load balancing for high-traffic sites

# Email Server

An email server handles the sending, receiving, and storage of emails. It allows users to communicate using email protocols such as SMTP (Simple Mail Transfer Protocol) for outgoing mail, and IMAP/POP3 for incoming mail.

Popular email servers include Microsoft Exchange and Postfix. Key functions include:

* Email routing and delivery
* Mailbox storage and management
* Security features like spam filtering and virus scanning

# VoIP Gateway

A Voice over IP (VoIP) gateway converts voice signals between the public switched telephone network (PSTN) and an IP network. It allows voice calls to be transmitted over IP networks, making it a critical component for enterprises that want to integrate traditional telephony with modern IP-based communication systems. Key features include: - Call routing between IP and analog phones

* Codec conversion and compression for voice data
* Fax and SMS integration

# Wireless LAN Controller (WLC)

A Wireless LAN Controller (WLC) manages and controls wireless access points in a network, ensuring secure and efficient wireless communication. It centralizes wireless network management, enabling simplified configuration, monitoring, and troubleshooting. Key functions include:

* Wireless network security and access control
* Centralized configuration for multiple access points
* Load balancing and roaming support

# NAS Storage Server

A Network-Attached Storage (NAS) server provides file storage and sharing over a network. It allows users to store and retrieve data from a centralized location, making it ideal for backups, file sharing, and media streaming.

NAS servers often come with built-in redundancy and data protection features like RAID. Key functions include:

* Centralized file storage and sharing
* User access control and permissions
* Data redundancy and backups

# Technologies Implemented

## Design Tool: Cisco Packet Tracer

Cisco Packet Tracer was used for network design and simulation before the actual deployment.It allowed for a virtual environment to test configurations, create network topologies, and simulate device behavior to ensure functionality before real-world implementation.



## Hierarchical Design

A hierarchical network design model was implemented, consisting of three layers: Core,

Distribution, and Access. This model improves scalability, redundancy, and network manageability. Redundancy is achieved through multiple links between layers to ensure high availability.

## Wireless LAN Controller (WLC)

Each department was equipped with a Wireless Access Point (WAP) managed by a Wireless LAN

Controller (WLC). This provided WiFi access for users and allowed centralized management and monitoring of wireless networks.



## VoIP: Deployment of IP Phones

VoIP (Voice over IP) technology was implemented using IP phones to enable efficient voice

communication over the IP network. This solution integrates voice services with the existing data network, reducing costs and simplifying management.



## VLAN: Maintained VLANs with Specific IDs

VLANs (Virtual Local Area Networks) were set up with unique IDs to segregate network traffic. VLANs were created for:

* Management
* LAN (General user traffic)
* WLAN (Wireless network traffic)
* VoIP (Dedicated for IP phone communication)
* Blackhole (For isolating unwanted or suspicious traffic)

## EtherChannel: LACP for Link Aggregation

Link Aggregation Control Protocol (LACP) was used to implement EtherChannel, allowing multiple physical links between switches to be combined into a single logical link. This increases bandwidth and provides redundancy in case of link failure.

## Spanning Tree Protocol (STP)

STP was configured to prevent network loops and ensure a loop-free topology. Features like PortFast were enabled on access ports to expedite the connection of end devices, and BPDUguard was applied to prevent the introduction of rogue switches.

## Subnetting: IP Address Allocation

Subnetting was used to logically divide the network into smaller sub-networks. This allows for efficient IP address allocation, improved network management, and enhances security by isolating different departments or services.

## Basic Device Settings

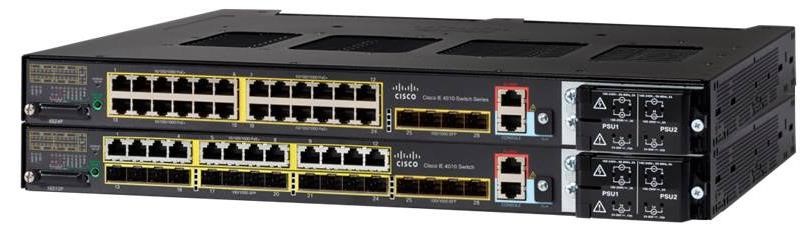
Basic configurations were applied to all network devices, including setting hostnames, enabling secure passwords for access, and configuring necessary logging and monitoring settings to enhance security and manageability.

## Inter-VLAN Routing

Inter-VLAN routing was enabled on multilayer switches to allow communication between different VLANs. This setup ensures that departments can communicate with each other while maintaining network segmentation for security purposes.

## Core Switch: IP Assignment for Multilayer Switches

Multilayer switches in the core layer were assigned IP addresses to handle both Layer 2 switching and Layer 3 routing. These switches manage both local traffic and inter-VLAN routing.



## DHCP Server: Dynamic IP Allocation

A DHCP server was configured to dynamically assign IP addresses to end devices in the network.This ensures efficient IP management and reduces the chances of IP conflicts.

## HSRP: High Availability Router Protocol

The Hot Standby Router Protocol (HSRP) was implemented to ensure high availability for routing services. In case the primary router fails, the standby router takes over, minimizing downtime.

## Static Addressing: Server Room Devices

Static IP addresses were assigned to critical devices in the server room, such as servers, storage devices, and printers. This ensures stable and predictable access to these resources.

## Routing Protocol: OSPF for Route Advertisement

OSPF (Open Shortest Path First) was selected as the routing protocol to efficiently advertise routes within the internal network. OSPF is a scalable and reliable protocol for dynamic routing, providing fast convergence and optimal path selection.

**Standard ACL for SSH**

A Standard Access Control List (ACL) was created to allow secure remote access using SSH.

This restricts remote

access to specific IP addresses, enhancing security.

**Cisco ASA Firewall**

The Cisco ASA firewall was configured to secure the network by controlling incoming and outgoing traffic based on

predefined security rules. It

provides protection against external threats and ensures internal network

segmentation

.

Intrusion Detection and Prevention Sys

tem

:

An Intrusion Detection and Prevention System (IDPS) is a security solution that monitors network

traffic for suspicious activities and policy violations. It combines the capabilities of an Intrusion

Detection System (IDS), which detects threats and generat

es alerts, with an Intrusion Prevention

System (IPS), which actively blocks or mitigates malicious activities in real time.

Device Settings and Configuration

**Device Settings and Configuration**

Device settings and configuration are critical components in

establishing a stable, secure, and efficient network

infrastructure. These settings include fundamental

configurations like assigning IP addresses, enabling password

protection, and setting up pr

otocols that ensure

communication and security across the network.

**1**

**. Basic Device Configuration**

Every network device must undergo initial configuration to ensure it can participate in the overall network. Basic

settings include:

-

Hostname Assignment: Each device is given a unique hostname for easy identification within the network.

-

Password Protection: For security, devices are configured with console, enable, and virtual terminal (VTY)

passwords. This ensures that only authorized personnel can access or manage the devices.



* Password Encryption: To safeguard the password, the service password-encryption command is applied. This encrypts the stored passwords to prevent unauthorized viewing.
* Banner Messages: A login banner, often containing legal warnings or important network information, is configured to display when users attempt to access the device.

## 2. IP Addressing and Subnetting

IP address configuration is essential for network devices to communicate. Each device, especially switches and routers, is configured with static or dynamic IP addresses:

* Static IPs: Static addresses are assigned to core devices like servers, switches, and firewalls to ensure consistent communication.
* Dynamic IPs (DHCP): For end-user devices and temporary devices like guest systems, Dynamic Host Configuration Protocol (DHCP) is used to automatically assign IP addresses.
* Subnetting: Proper subnetting ensures efficient use of the available IP address space and helps to segregate traffic for security and performance optimization.

## 3. Routing Protocols Configuration

Routing protocols are configured to enable devices to communicate across different networks. Open Shortest Path First (OSPF) is often used due to its scalability and efficiency in larger networks. OSPF helps devices learn the network's topology and route traffic efficiently.

* Inter-VLAN Routing: In multi-VLAN setups, multilayer switches are configured to route traffic between VLANs, ensuring communication between different departments or segments.
* Static Routes: Some devices may require static routes, especially in cases where security or performance requires fixed paths for certain types of traffic.

## 4. Security Features

Security settings are essential to prevent unauthorized access and to safeguard network data:

* Access Control Lists (ACLs): ACLs are configured to control which traffic is allowed or denied across different parts of the network.
* SSH Configuration: Secure Shell (SSH) is set up for secure remote access to network devices, ensuring encrypted management sessions.
* Port Security: This feature is often applied on switches to limit the number of devices that can connect to a port, preventing unauthorized device access.

5. Spanning Tree Protocol (STP) Configuration

STP is essential for preventing network loops, which can cause severe disruptions in the network. PortFast and BPDUguard are specific features configured on access ports:

-

PortFast: This feature ensures that ports move directly to the forwarding state, reducing downtime for

connected devices like computers or phones.

-

BPDUguard: This security feature shuts down a port if a bridge protocol data unit (BPDU) is detected, which

helps in protecting against rogue switches.

**6**

**. EtherChannel Configuration**

Link Aggregation Control Protocol (LACP) is used for EtherChannel configurations. This combines multiple

physical links into a single logical link, improving bandwidth and providing redundancy.

**7**

**. Testing and Verification**

After configuring devices, testing is crucial to ensure that settings are correct and that devices can communicate

as expected. This includes:

-

Ping Tests: Testing connectivity between devices using ICMP ping.

-

Traceroute: Verifying the path packets between devices.

-

Show Commands: Various show commands are used to inspect the configuration and status of interfaces,

protocols, and routing tables.

Effective device settings and configurations form the backbone of any network. They ensure smooth operation,

security, and optimal performance, allowing the organization to focus on its core business needs

.

**Implementation:**

**Conclusion**

The design and implementation of a secure network system for Cytonn

Innovation Ltd is critical to ensuring

operational efficiency and safeguarding sensitive data. By employing a structured approach with robust security

measures, the new network will support the company's growth and adaptability in the digital landscape.

