Project Phase 2 Report

Computer Networks

Table of Contents

Objective

- The primary goal of this project is to design and implement a secure and scalable network infrastructure for a cybersecurity startup.

- This network will support VLAN segmentation for departments, dynamic IP addressing through DHCP, and essential services like DNS, email, and web hosting.

- Advanced security features, including firewalls, IDS/IPS, and ACLs, will be integrated to protect against potential threats.

Scope

This project involves designing and configuring a network infrastructure for a cybersecurity startup. The network will consist of:

1: VLANs for departmental segmentation.

2: Centralized routing and DHCP configuration.

3: A Secure server environment hosting web, email, and backup services.

4: Adding firewalls, access control lists (ACLs), and simulated IDS/IPS for network security.

5: Dynamic IP address assignment to reduce administrative overhead.

6: A scalable architecture to accommodate future growth.

Deliverables

- A Cisco Packet Tracer project file with a complete network design, including VLANs and security features.
- A network topology diagram showing device connections and traffic segmentation.
- Configuration documentation for all devices and security settings.
- A testing report with results on network functionality and security.
- A final project report summarizing the design, configurations, and outcomes.

Group Members & their Responsibilities

Abeera Mehtab
232087

PROJECT DESIGNER AND PLANNING,TOPOLOGY AND PHYSICAL DESIGN, PROJECT PROPOSAL AND PRESENTATION MAKING

Mahnoor
232083

PROJECT DESIGN CONSULTANCY, FINAL CONFIGURATIONS AND TESTINNG AND FINAL REPORT MAKING

Mahnoor Ikram
232115

PROJECT DESIGN CONSULTANCY, FINAL CONFIGURATIONS AND TESTINNG AND FINAL REPORT MAKING

Eman Mansoor
232149

FINAL CONFIGURATIONS AND TESTING AND INTERMEDIATE PLAN MAKING AND SECOND PHASE REPORT MAKING

Background & Problem Statement

Current Network Infrastructure

The existing network infrastructure at CyberTech Solutions lacks proper segmentation, security measures, and scalability. This can lead to potential security vulnerabilities, inefficient communication between departments, and limited room for expansion.

Challenges & Limitations

- Lack of VLANs to segment departments and enhance security.
- Unrestricted access to external websites such as YouTube, Instagram, and TikTok, which could lead to bandwidth misuse.
- Insufficient network security measures, leaving the network vulnerable to potential threats.
- Scalability issues in expanding the network to accommodate future departments and services.

Project Necessity

This project aims to address the challenges by providing a secure, segmented, and scalable network. The implementation of VLANs, dynamic IP assignment, ACLs, firewalls, and simulated IPS will enhance security, ensure efficient communication within departments, and allow room for future growth.

Proposed Solution

Network Design:

The network will be designed using a *star topology*, with a central switch connecting all department switches. VLANs will be implemented to segment the departments, ensuring traffic segregation and increased security. Each department will have its own server for DNS, DHCP, Email, and Web services.

Cisco Technologies To be Used:

- **Cisco Catalyst 2960 Series Switches:** For VLAN implementation and departmental traffic management.
- **Cisco 2911 Router:** For routing between VLANs and providing external network connectivity.
- **Cisco ASA 5505 Firewall:** For securing internal and external communications.
- **Cisco Packet Tracer:** For network simulation and testing.

Network Protocols:

- **VLAN** for segmentation and security.
- **DHCP** for dynamic IP addressing.
- **ACL** for access control and security measures.
- **TCP/IP** for internal and external communication.

Tools To Be Used:

- Cisco Packet Tracer for simulation and configuration.
- Cisco ASA 5505 Firewall for security and IPS simulation.

Technical Requirements

Hardware Requirements:

- **Router:** Cisco 2911
- **Switches:** Cisco Catalyst 2960 Series
- **Firewall:** Cisco ASA 5505
- **Servers:** Email, DNS, DHCP, FTP, and Web Servers (Configured through their respective interfaces).
- **End Devices:** PCs, Laptops, Printers, and IoT Devices (cameras and access control).
- **Cloud:** Internet-Cloud for external access.

Software Requirements:

Cisco Packet Tracer for network simulation.

Network Topology:

The network will be designed in a star topology with:

- One Central-Switch
- Five Departmental Switches connected to the Central-Switch.
- One Main Router connecting the internal network to the external internet via the Cloud.
- One Firewall between the internal network and the router.

Protocols and Standards:

- IPv4 will be used for all addressing.
- VLANs will be used to segregate traffic within departments.
- TCP/IP for communication across the network.
- Dynamic Host Configuration Protocol (DHCP) for automatic IP addressing.
- Access Control Lists (ACLs) for internal and external traffic control.

Security measures & Scalability:

- ACLs to control access between departments and restrict external site access.
- Firewall rules to deny certain websites and control external communication (e.g., block YouTube, Instagram).
- Simulated IPS via ACLs on the router and firewall.

The design allows easy addition of new departments by assigning new VLANs and integrating additional servers and end devices.

Budget Estimation:

Cisco Hardware and Software

- Cisco Catalyst 2960 Switches: $500 each (5 units) = $2500
- Cisco 2911 Router: $1500
- Cisco ASA 5505 Firewall: $800
- Cisco Packet Tracer: Free (Educational License)

Additional Tools and Resource

- Network Cables: $100
- End Devices (PCs, Laptops, IoT Devices): Estimated cost $1500

Implementation and Training Costs

- Estimated cost for implementation: $1000
- Training for staff on managing the network: $500

- **Total Estimated Budget:**
- $6400

Team Roles and Responsibilities

Member 1:

- Responsible for configuring the Central Switch, VLANs, End Devices, and IoT devices.
- Ensuring proper IP allocation and connectivity between devices.

Member 2:

- Responsible for Router Configuration, including routing, VLAN interfaces, and dynamic IP configuration for servers.
- Server Configuration for DNS, Email, and Web servers.

Member 3:

- Responsible for ACL and Firewall Configuration, setting up security policies for internal communication, external access, and traffic filtering.

Testing and Evaluation

Functionality Testing

- Verify connectivity between end devices in the same VLAN.
- Test server accessibility from each department’s devices.
- Ensure that all devices receive dynamic IP addresses from the DHCP server.

Security Testing

- Test the ACL and Firewall rules to ensure proper segmentation.
- Verify that access to blocked websites (e.g., YouTube, Instagram) is denied.
- Confirm that no unauthorized external access is allowed via the firewall.

Performance Testing

- Evaluate network performance under normal load conditions.
- Test the scalability by adding new devices and ensuring network performance remains consistent.

Risk Assessment

Hardware Failure:

Mitigation: Use backup devices and ensure proper configuration backups

Configuration Errors:

Mitigation: Regular configuration backups and peer reviews of configurations before deployment.

Security Breaches:

Mitigation: Implement strong firewall rules and ACLs, test network security regularly.

Documentation and Reporting

Network Configuration Documentation:

- Device configurations, VLAN settings, ACLs, and firewall rules will be documented.
- Server setup procedures for DNS, Email, and Web servers will be recorded.

Testing Report:

- Document results of all functionality, security, and performance tests.
- Provide recommendations for improvements if any issues arise during testing.

Presentation:

- A comprehensive presentation will be created, covering the entire network setup, security measures, and test results.

Conclusion
&
References

Conclusion:

The implementation of the secure and scalable network for CyberTech Solutions will address current challenges in segmentation, security, and scalability. With proper VLAN configurations, server setups, and robust security measures using ACLs and firewalls, the network will be well-equipped to handle current needs and future expansions.

Refences:

Cisco IOS Configuration Guides

Cisco Packet Tracer Documentation

Cisco Security Best Practices