**Report**

Title: Design and Implementation of a Secure Campus Network

Course: CIS 192

Name: Tejas Pathange

1. Overview:

The first task is to create a design for your campus. I have created a campus network with four building connected to a LAN for each building and then connected two multilayer switches, and then connected to a firewall, and the firewall is connected to router that can be connected to other routes (in future).

1. Design:

After thinking a lot about the design. I finally decided to go with this design

A diagram of a network

Description automatically generated

Devices used:

* 1. For each department:
     1. 3 Computer
     2. 2 Laptop
     3. 1 printer
     4. 1 Switch (Model 2960)
  2. 2 Multilayer Switches (Model 3560)
  3. 1 Firewall
  4. 1 Router
  5. DMZ
     1. 1 Switch (Model 2960)
     2. 2 Servers

All the networks are connected with copper straight through and Copper cross over cables.

This network consists of 4 departments:

1. Classroom
2. Library
3. IT
4. Administration

The DMZ consists of 2 Serves:

1. DHCP
2. DNS

The core layer consists of router, firewall and multilayer switch

The distribution layer consists of switch in every department

The access layer consists of computer, laptop and printers

1. IP Addressing and VLAN

The network appears to utilize VLANs for segmentation, ensuring better performance and security:

1. **VLAN 10 - Administration**:
   * IP Range: 192.168.10.0/24.
2. **VLAN 20 - Classroom**:
   * IP Range: 192.168.20.0/24.
3. **VLAN 30 - Library**:
   * IP Range: 192.168.30.0/24.
4. **VLAN 40 - IT**:
   * IP Range: 192.168.40.0/24.

**Subnet:** 10.20.20.0/27  
**Subnet Mask:** 255.255.255.224  
DMZ - Firewall

**Subnet:** 10.20.20.32/30  
**Subnet Mask:** 255.255.255.252  
Multilayer switch - Firewall

**Subnet:** 10.20.20.36/30  
**Subnet Mask:** 255.255.255.252 Multilayer switch -Firewall

**Subnet:** 105.100.50.0/30  
**Subnet Mask:** 255.255.255.252 Firewall - Router

1. Network Features
2. **Routing and Switching**

* A **multilayer switch** is deployed to handle Layer 3 routing between VLANs.
* **Static routes** or **dynamic routing protocols** (e.g., OSPF) are used for inter-VLAN communication.
* **Access switches** manage device-level connections.

1. **Network Security**
   * Access control lists (ACLs) are used to filter traffic and secure inter-VLAN communication.
   * Port security on switches limits the number of devices per port, reducing the risk of unauthorized access.
   * Firewalls protect against external threats.
2. **Device Management**
   * Secure management protocols, such as SSH, are enabled on all network devices.
   * Unused ports and protocols are disabled to minimize the attack surface.
3. Testing for Latency

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Source | Destination | Min Latency (ms) | Avg Latency (ms) | Max Latency (ms) | Observations |
| IT- PC1 | Administration PC1 | 0 | 1 | 10 | Not much Delay |
| IT- PC1 | Classroom PC1 | 0 | 3 | 11 | Not much Delay |
| IT- PC1 | Library PC1 | 0 | 2 | 0 | Not much Delay |
| Administration PC1 | Classroom PC1 | 0 | 4 | 28 | Not much Delay |
| Administration PC1 | Library PC1 | 0 | 7 | 14 | Not much Delay |
| Administration PC1 | IT- PC1 | 0 | 8 | 14 | Not much Delay |
| Classroom PC1 | Administration PC1 | 0 | 0 | 1 | Not much Delay |
| Classroom PC1 | Library PC1 | 0 | 0 | 0 | Not much Delay |
| Classroom PC1 | IT- PC1 | 0 | 4 | 17 | Not much Delay |
| Library PC1 | Administration PC1 | 0 | 0 | 1 | Not much Delay |
| Library PC1 | IT- PC1 | 0 | 0 | 0 | Not much Delay |
| Library PC1 | Classroom PC1 | 0 | 0 | 1 | Not much Delay |

After performing multiple tests for the network there is not much latency observed as the network is small.

A computer screen shot of a black screen

Description automatically generated A computer screen shot of a black screen

Description automatically generated

1. Conclusion

* The network topology employs a **hierarchical structure** with Core, Distribution, and Access layers for improved performance and scalability.
* **VLAN segmentation** is implemented to optimize traffic management and ensure logical separation of departments.
* Advanced **security measures**, including firewalls, access control lists (ACLs), and secure device configurations, protect the network from unauthorized access and threats.
* **Redundancy** through multiple links and the use of protocols like Spanning Tree Protocol (STP) ensures high availability and minimizes downtime.
* The network is designed to support **scalability**, allowing for future growth and additional devices or departments.