اونيۏرسيتي مليسيا ڤهڠ

UNIVERSITI MALAYSIA PAHANG

BCN2093 Network Analysis and Design

Topic for Project : State Education Department

Lab Section : 1B

Lecturer's Name : Syahrizal Azmir Bin MD. Sharif

Group Name : ALPHA-1B

No.	Name	Matric ID
1	AHMAD NAZHAN HAZIQ BIN AHMAD FUAD	CA21060
2	MUHAMMAD NAZHIIM SYAKIR BIN MOHD SYAHRIZAL	CA21049
3	MUHAMMAD AFIQ BIN SHAMSUDIN	CA21083
4	MUHAMAD ASYRAF MUHAIMIN BIN MAZLAN	CA21058

Table of Content

EXECUTIVE SUMMARY

The Alpha Network Sdn. Bhd. is a partnership company with 100% local ownership, stock, and management. It was founded on May 10, 2023. It is a non-profit organization dedicated to the reliable deployment of information and communication technology for the growth of industry and culture worldwide. We offer a diverse range of value-added systems, network goods, and services aimed at advancing and expanding information technology. The utility of the company extends equally into the public and private sectors in both domestic and foreign markets.

With a vast community of technical professionals, an experienced and competent management staff, and a strong group of technical specialists, we are committed to providing value-added systems and network technologies. As a systems and network specialist, we have taken the lead, supporting a wide range of small, medium, and big organizations, with a focus on specialized and vertical industries.

PROJECT GOAL

Our project goal is to create and build a network infrastructure for the state education department's new branch. Our plan is to establish a reliable and secure internet connection provided by an Internet Service Provider (ISP) for a company occupying three floors in a building. Additionally, the project aims to set up a Virtual Private Network (VPN) to accommodate the connectivity needs of at least 30 staff members who work remotely, ensuring seamless and protected access to the company's network resources.

PROJECT SCOPE

1. To conduct a comprehensive assessment of the network infrastructure
2. To Develop a detailed network design and plan that aligns with the organization's requirements and future growth.
3. To Identify and procure the necessary network hardware.
4. To install, configure, and deploy the network infrastructure components based on the approved design and plan.
5. To configure and deploy a Virtual Private Network (VPN).
6. To create comprehensive documentation.
7. To conduct training for end users.
8. To conduct thorough testing of the network infrastructure.

DESIGN REQUIREMENT

Business Goal

- The objective is to achieve resource sharing within the State Education Department network, regardless of the physical location of the resources or the client. This includes making data and hardware easily accessible to all users.
- Another goal is to enhance the performance of the system by improving accessibility and ensuring high-speed data transmission through both wired and wireless connections.
- Furthermore, it is important to enhance network security to safeguard servers and data from unauthorized access.
- The target is to cater to a minimum of 100 employees within the State Education Department, with at least 30 of them requiring remote access through a VPN.
- Additionally, the server should securely store all employee data in a database, which should only be accessible by internal employees.

Technical Goal

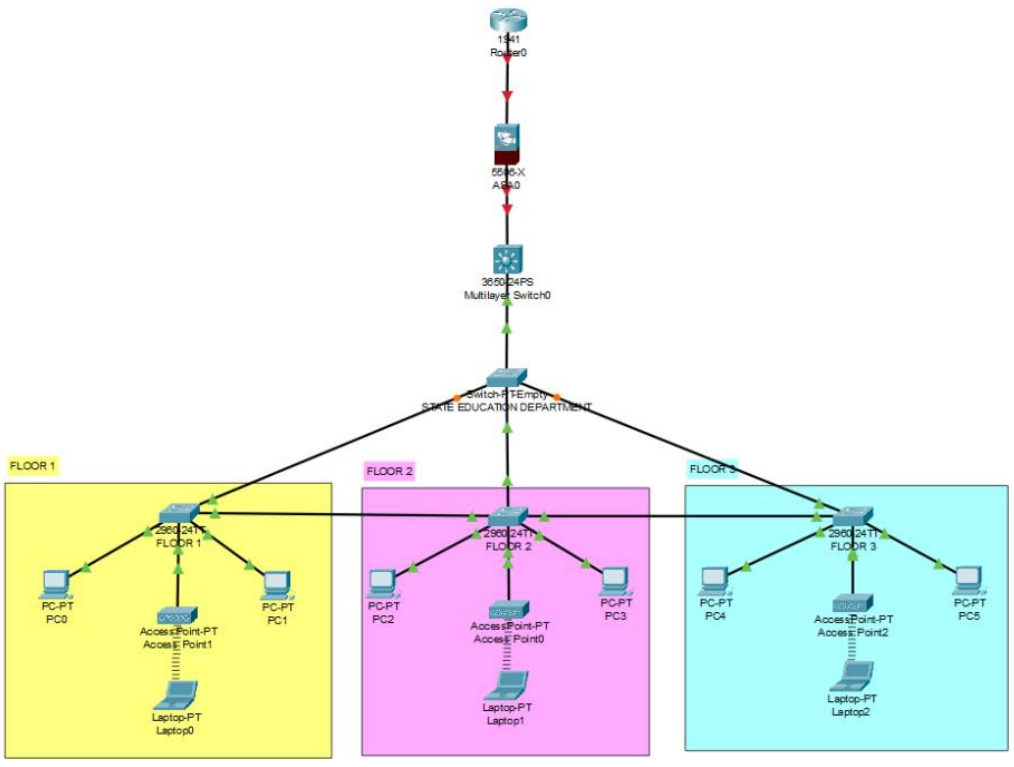
- Availability - The primary objective of this network design is to maximize network availability, enabling users to connect to the server with optimal performance and connection speed. The registration user data is more dependable, ensuring its storage and usability over an extended period. Moreover, maintenance tasks can be scheduled during periods of low registration activity, such as midnight, to minimize disruptions and preserve network efficiency.
- Security - The network design implemented by the State Education Department prioritizes data security by implementing firewalls and routers to prevent unauthorized access. These security measures effectively protect users from malicious or threatening data, which is filtered out by the security system.

- Scalability - The network's scalability can be achieved by adding additional computers and servers, thereby increasing network throughput and enhancing overall network productivity.

LOGICAL DESIGN

1. NETWORK TOPOLOGY

The suitable network topology for the new branch is Partial Mesh Hierarchical. Connection to the internet will be provided by an ISP. The state education department occupies 3 floors. The first floor contains the administrative offices of the company. The organization also requires a VPN setup for at least 30 staff who work remotely.



2. MODELS FOR ADDRESSING AND NAMING THE SEGMENTS AND DEVICES

Model utilized is a private Class A IP address, with a focused range roughly between 10.0.0.0 and 10.255.255.255. This private IP address was chosen because the local area network (LAN section) of large networks uses it.

The segments and gadgets are then given names according to where they are in Block M. It is necessary to give the router, core switch, switch, and PC new names because this topology consists of three floors, numbered floor 1, floor 2, and floor 3. This can help in reading network maps, putting route summarization into practise, and achieving usability objectives.

3. SWITCHING AND ROUTING PROTOCOLS

ROUTING

- OSPF
- Dynamic
- Supports large internetwork
- Authenticate protocol ro meet security goals
- Shorter bandwidth

SWITCHING

- Multilayer switching
- Spanning Tree Protocol
- Layer 2 transparent bridging
- VLAN technology

4. RECOMMENDED SECURITY MECHANISMS AND STRATEGIES

PHYSICAL SECURITY

During the first stages of the network design project,we need to make sure that equipment is situated in computer rooms with card key access and security guards. Uninterruptible power supply, fire alarms, fire suppression systems, and water removal systems should all be present in computer rooms. To protect it from earthquakes and strong winds during storms, equipment should be put in racks that attach to the floor or wall.

AUTHENTICATION

Two-factor authentication is used by the system, which requires the user to present two different pieces of identification. One illustration is an access control system that demands a security card and a password. When two-factor authentication is used, the system cannot be hacked if one factor is compromised. Although a password could be learned, it is useless without a security card. Without a password, the security card won't function if it is lost or stolen.

AUTHORIZATION

The least privilege principle is applied when authorizing something. This rule is founded on the idea that each user should only be given the minimal authority necessary to complete a given task. Because of this, an authorisation process should only give a user the absolute minimum access rights. Techniques are used to make the process easier because it is

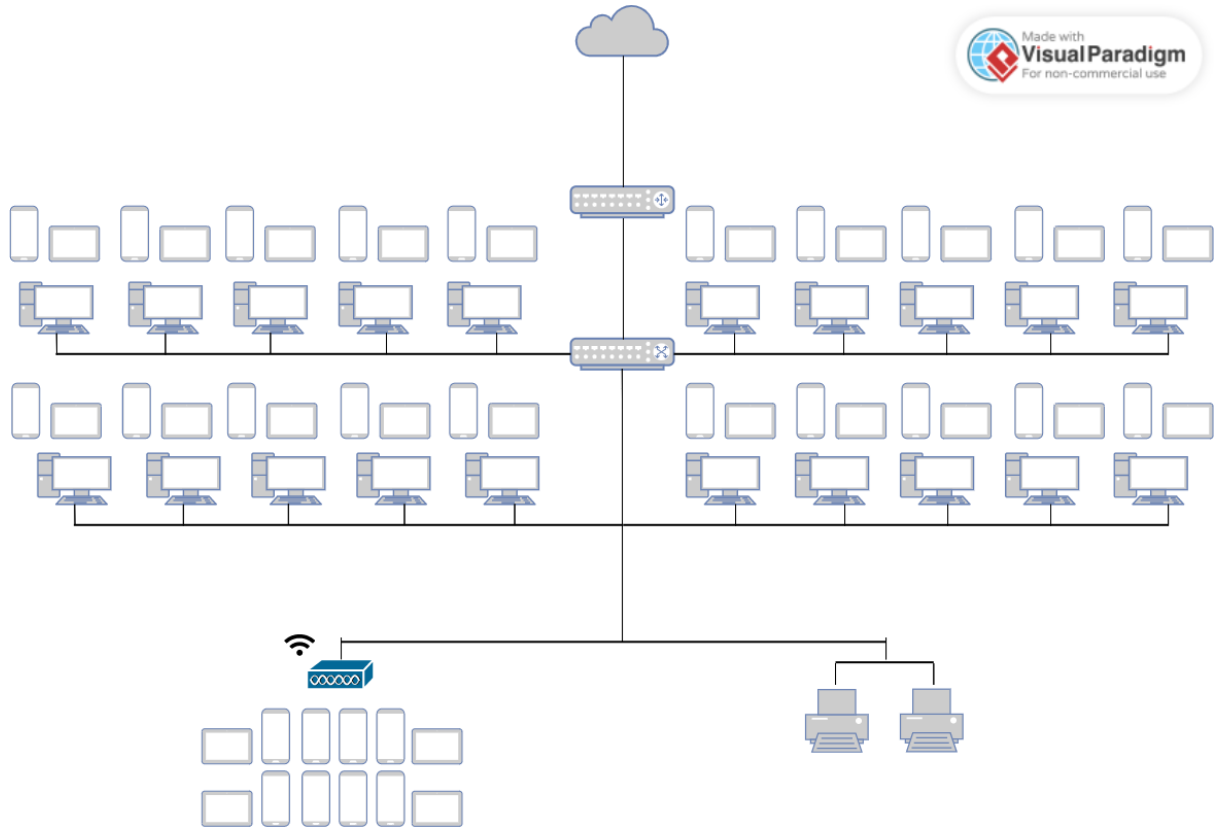
difficult to list each user's authorized actions in relation to each resource in a clear and unambiguous manner. For instance, a network administrator can make user groups for users with the same permissions.

5. RECOMMENDED NETWORK MANAGEMENT STRATEGIES

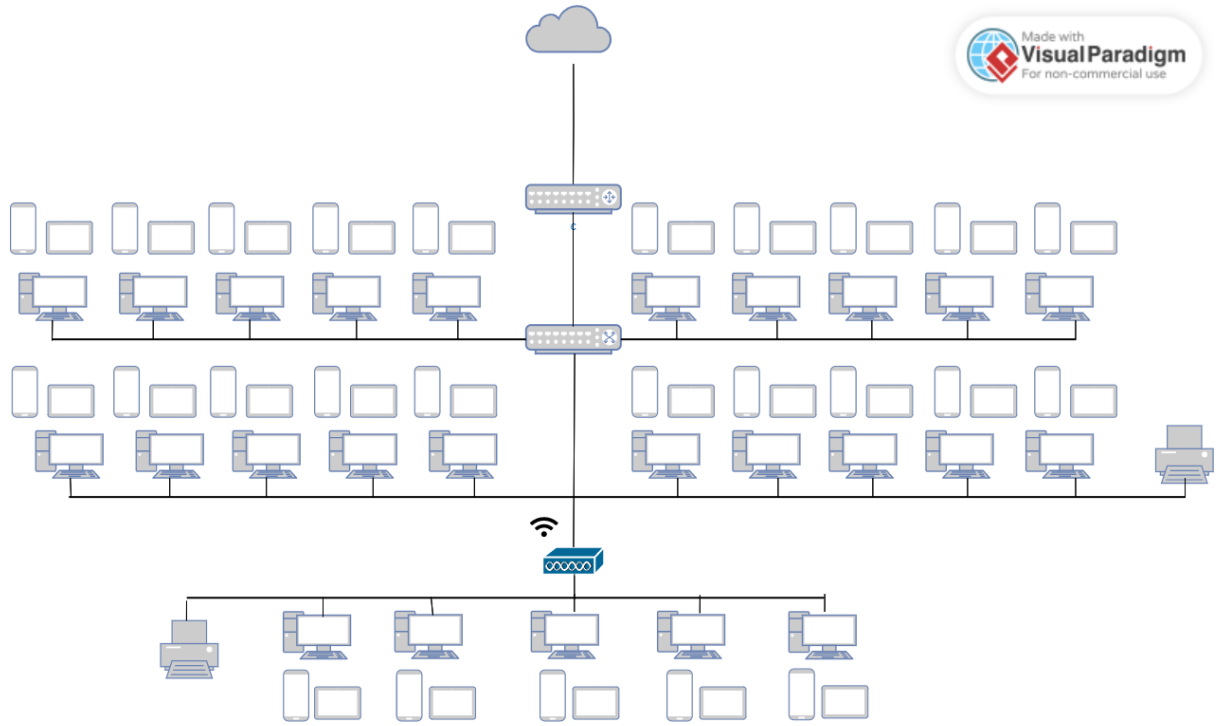
For suggested network management techniques, Simple Network Management Protocol can be used to monitor and maintain an internet. The method and tool for managing managed devices such as servers, workstations, switches, routers, and other network components locally and remotely. Remote devices in this topology can be configured using SNMP. Each networked host can get configuration information from the management system. Then, network performance is tracked. It can assist in monitoring network throughput, processing speed, and data transfer success.

PHYSICAL DESIGN

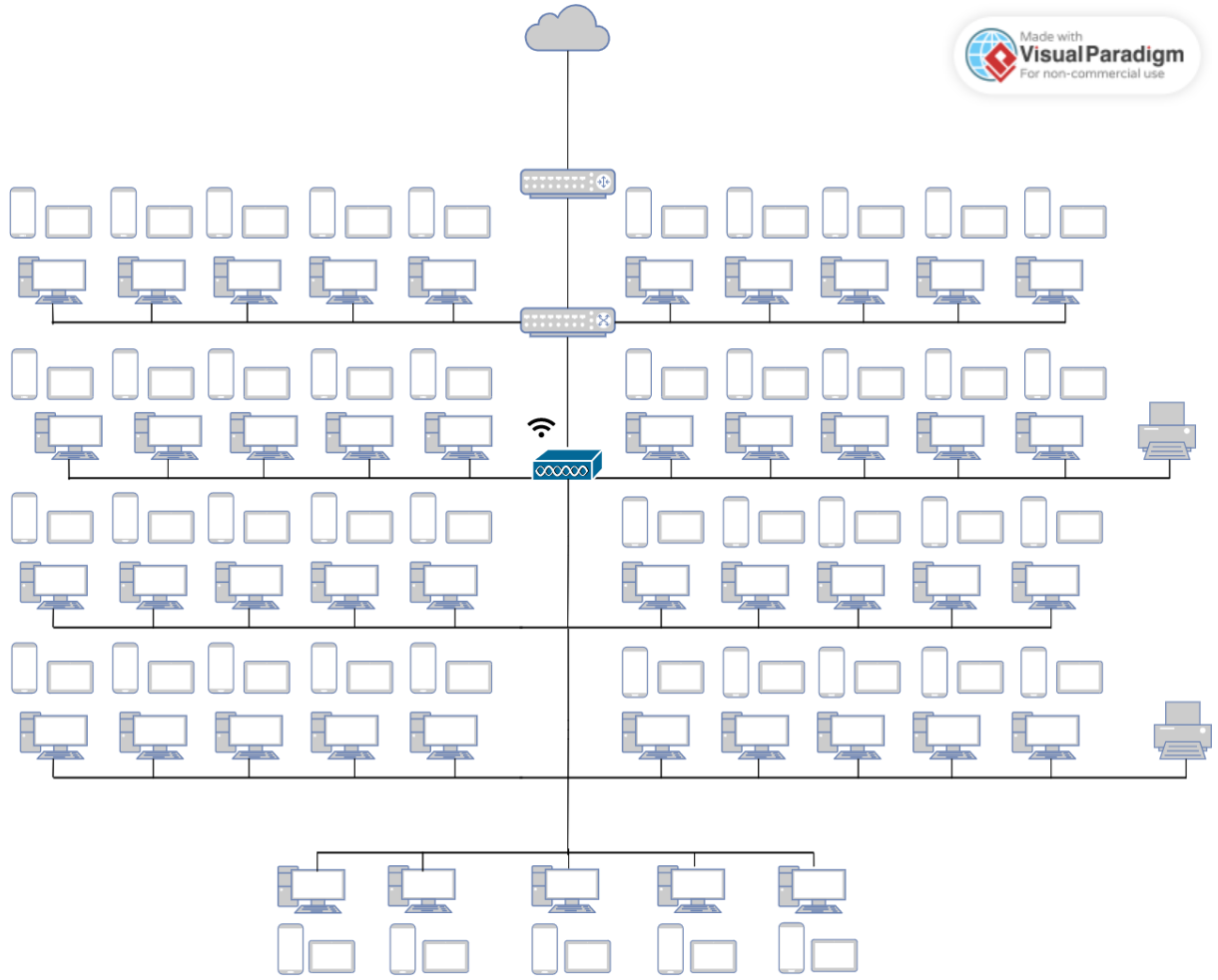
Floor 1



Floor 2



Floor 3



NETWORK TOPOLOGY DIAGRAM

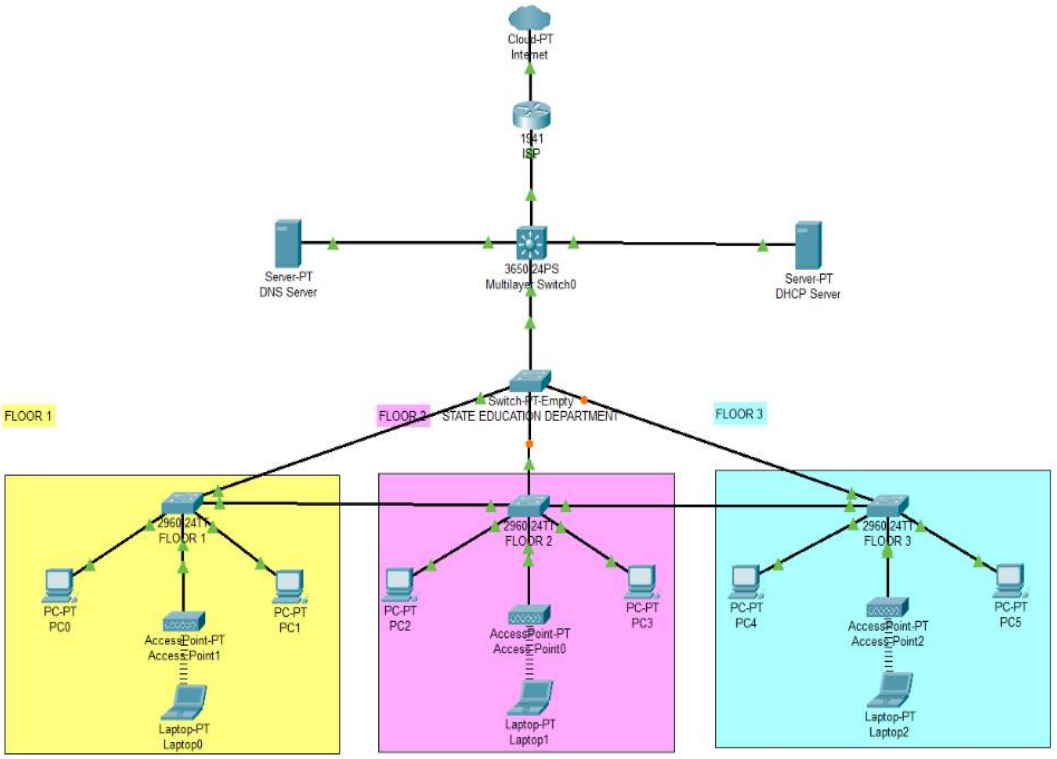
Partial Mesh Hierarchical

A mesh architecture is typically advised by network designers to satisfy availability needs. In a full-mesh topology, every router and switch is linked to every other router and switch. A full-mesh network offers total redundancy and effective performance because there is only one link delay between any two sites. A partial-mesh network has fewer connections. Reaching a different router or switch may require navigating intermediary links in a partial-mesh network.

TOP-DOWN Network Design

Top-down network design is a method of network design that works its way down from the top levels of the OSI reference model. It concentrates on applications, sessions, and data transfer before choosing routers, switches, and media that function at the lowest layers. Part of the top-down network design process involves examining divisional and group structures to identify the individuals for whom the network will deliver services and from whom you should obtain crucial information to make the design successful. Top-down iterative network design is also an option. It's important to first gain a general understanding of a customer's needs in order to avoid becoming mired down in specifics too soon. Later, more data can be acquired regarding protocol behaviour, scalability requirements, technology preferences, and so forth. Top-down network design is aware that the logical model and physical design may change as more data is gathered.

The network structure of this project has been separated into three layers: Core, Distribution, and Layers. We are using a Cisco Catalyst 3850-12XS-S on the core layers. There are 12 SPF+ optical ports on the Cisco Catalyst 3850-12XS-S. The switch offers a 420 Gbps switch capacity and 380 GB of stack bandwidth. The best switch to use as a core switch is that one. In the distribution layers, WS-C3650- 24PD-L will be used, and in the access layers, Cisco Catalyst 2960X-48TD-L.



TCP/IP NETWORK DESIGN

We are employing a classless IP address for our project. Using the VLSM technique, 10.10.0.0/8 has been partitioned into a number of subnets. On this project, there are 6 subnets, each of which corresponds to a different VLAN. The subnets for computer labs are Floors 1, 2, and 3. IP addresses will be dynamically assigned to each end user.

VLAN TABLE

Vlan Id	Name	Network Address	Subnet Mask	Remark
10	Management	10.10.10.0	255.255.255.0	
21	1stFloor	10.10.21.0	255.255.255.0	
22	2ndFloor	10.10.22.0	255.255.255.0	
23	3rdFloor	10.10.23.0	255.255.255.0	
30	Staff	10.10.30.0	255.255.255.0	
40	Guest	10.10.40.0	255.255.255.0	

IP ADDRESSING MANAGEMENT

Location	**Name**	**IP Address**	**Remark**
Router	ISP	10.10.10.1	
State Education Department	CoreSwitch	10.10.10.2	
State Education Department	StateEducationDepartment	10.10.10.3	
1stFloor	1stFloor	10.10.10.4	
2ndFloor	2ndFloor	10.10.10.5	
3rdFloor	3rdFloor	10.10.10.6	

VLAN ADDRESSING

Device	Interface	IP Address	Subnet Mask
ISP	G0/1/0.10	10.10.10.1	255.255.255.0
	G0/1/0.21	10.10.21.1	255.255.255.0
	G0/1/0.22	10.10.22.1	255.255.255.0
	G0/1/0.23	10.10.23.1	255.255.255.0
	G0/1/0.30	10.10.30.1	255.255.255.0
	G0/1/0.40	10.10.40.1	255.255.255.0
CoreSwitch	Vlan 10	10.10.10.1	255.255.255.0
	Vlan 21	10.10.21.1	255.255.255.0
	Vlan 22	10.10.22.1	255.255.255.0
	Vlan 23	10.10.23.1	255.255.255.0
	Vlan 30	10.10.30.1	255.255.255.0
	Vlan 40	10.10.40.1	255.255.255.0

ROUTER CONFIGURATION (LAN, DEFAULT ROUTE, ACCESS CONTROL LISTS, IP HELPER ADDRESS)

The VLAN name and IP DHCP pool will be configured on the CoreSwitch. We set up OSPF on the router with an ID of 10. The distribution layer's ports will all be set up as trunk ports. They will also have VLAN configurations based on their placements at the access layer.

Please refer to appendix for full configuration

ISP

- Vlan
- Trunking
- OSPF
- IP Management
- Encapsulation dot1Q
- Basic Configuration (hostname, password, telnet, console)

Please refer to appendix for full configuration

CoreSwitch

- Vlan
- Trunking
- IP Management
- DHCP Pool
- Basic Configuration (hostname, password, telnet, console)

Please refer to appendix for full configuration

StateEducationDepartment

- Vlan
- Trunking
- IP Management
- Basic Configuration (hostname, password, telnet, console)

Please refer to appendix for full configuration

1stFloor

- Vlan
- Trunking
- IP Management
- Basic Configuration (hostname, password, telnet, console)

Please refer to appendix for full configuration

2ndFloor

- Vlan
- Trunking
- IP Management
- Basic Configuration (hostname, password, telnet, console)

Please refer to appendix for full configuration

3rdFloor

- Vlan
- Trunking
- IP Management
- Basic Configuration (hostname, password, telnet, console)

Please refer to appendix for full configuration

PROPOSED NETWORK SECURITY AND NETWORK MANAGEMENT STRATEGIES

NETWORK MANAGEMENT STRATEGIES

As part of network management activities, Simple Network Management Protocol (SNMP) has been used to monitor and maintain the internet for the State Education Department. Network monitoring tasks carried out by the State Education Department in a practical organizational environment are supposed to be made simpler by SNMP. By employing the SNMP network monitoring protocol to obtain a current network topology, the State Education Department will save time and money. so that we can easily get a list of all the devices that are currently linked to the State Education Department's network, together with important details and a thorough network inventory for each item.

NETWORK SECURITY STRATEGIES

1. **VIRTUAL PRIVATE NETWORK (VPN)**

   The ability to establish a secure network connection when using public networks is known as a "Virtual Private Network," or VPN. VPNs can encrypt the State Education Department's internet traffic as well as conceal its online identity. This makes it more difficult for outsiders to spy on the State Education Department's internet usage and steal information. A VPN hides the IP address of the State Education Department by allowing the network to reroute it through a carefully configured remote server run by

a VPN host. In other words, the VPN server becomes the source of the staff data if employees utilize a VPN to surf the internet. To put it another way, neither the employee's Internet Service Provider (ISP) nor any other third parties are able to keep an eye on the websites the staff visits or the information they send and receive online. A VPN serves as a filter that scrambles all employee data. Even if someone succeeded to obtain the information from the State Education Department, it would be meaningless.

2. FIREWALL

Through a firewall, a network security device, the State Education Departments are employed to monitor and filter both incoming and outgoing network traffic. At its most basic level, a firewall is essentially the barrier that sits between a private internal network and the public Internet. A firewall's primary purpose is to allow only safe traffic, such as that from the State Education Department, while preventing malicious traffic. In order to authenticate access, it can analyze network traffic for dangerous components like hackers and malware and block any incoming network traffic that has not been requested.

3. SERVER FARM

A server farm, often referred to as a server cluster, is a collection of computer servers that are typically managed by a business to offer server functionality that is significantly greater than that of a single machine. Server farms, which frequently house thousands of computers and need a lot of electricity to run and stay cool, are widespread.

4. IEEE 802.1X EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

A wireless or wired client (Supplicant) can communicate with an authentication server (RADIUS) through an Authenticator (a wired switch or wireless access point that serves as a proxy) using the 802.1X challenge and response-based authentication protocol. Some of the authentication methods offered by EAP are secure, while others are not (although older endpoints still support them).

5. SANDBOXING

Using a host system that resembles end-user operating environments, staff employees run applications or open files in a protected, segregated environment using the cybersecurity method known as sandboxing. Sandboxing monitors opened files or code while looking for potentially harmful behaviour in order to prevent threats from

accessing the network. For instance, viruses in documents like PDFs, Word, Excel, and PowerPoint can be safely detected and stopped before they reach an unwary end user at the State Education Department.

6. INTRUSION PREVENTION SYSTEMS (IPS)

Network security risks like brute force assaults, denial-of-service attacks, and exploits of well-known flaws can be recognised or stopped by IPS technology. An exploit is an attack that makes use of a vulnerability, such as one in a software system, to seize control of the target system. After a vulnerability is made public, attackers typically have a window of opportunity before the security remedy is applied. The State Education Department's intrusion protection system can quickly block these attacks.

7. WI-FI PROTECTED ACCESS (WPA)

The Wi-Fi Alliance created the Wi-Fi Protected Access, Wi-Fi Protected Access II, and Wi-Fi Protected Access 3 security and certification systems to safeguard wireless computer networks. All access points for wireless in buildings will be configured with WPA encryption to guarantee the Wi-Fi's security.

RESULTS OF NETWORK DESIGN TESTING

PC0 to PC1

```
C:\> ping 10.10.21.4

Pinging 10.10.21.4 with 32 bytes of data:
Reply from 10.10.21.4: bytes=32 time=1ms TTL=255
Reply from 10.10.21.4: bytes=32 time=1ms TTL=255
Reply from 10.10.21.4: bytes=32 time=1ms TTL=255
Reply from 10.10.21.4: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.21.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

PC2 to PC3

```
C:\> ping 10.10.22.10

Pinging 10.10.22.10 with 32 bytes of data:
Reply from 10.10.22.10: bytes=32 time=1ms TTL=255
Reply from 10.10.22.10: bytes=32 time=1ms TTL=255
Reply from 10.10.22.10: bytes=32 time=1ms TTL=255
Reply from 10.10.22.10: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.22.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milliseconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

PC2 to PC4

```
C:\> ping 10.10.23.4

Pinging 10.10.23.4 with 32 bytes of data:
Reply from 10.10.23.4: bytes=32 time=1ms TTL=255
Reply from 10.10.23.4: bytes=32 time=2ms TTL=255
Reply from 10.10.23.4: bytes=32 time=1ms TTL=255
Reply from 10.10.23.4: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.23.4:
Packets: Sent=4, Received=4, Lost=0 (0% loss),
Approximate round trip times in milliseconds:
Minimum=1ms, Maximum=2ms, Average=1ms
```

PC2 to PC5

```
C:\> ping 10.10.23.16

Pinging 10.10.23.16 with 32 bytes of data:
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255
Reply from 10.10.23.16: bytes=32 time=2ms TTL=255

Ping statistics for 10.10.23.16:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

PC3 to PC4

```
C:\> ping 10.10.23.4

Pinging 10.10.23.4 with 32 bytes of data:
Reply from 10.10.23.4: bytes=32 time=1ms TTL=255
Reply from 10.10.23.4: bytes=32 time=2ms TTL=255
Reply from 10.10.23.4: bytes=32 time=1ms TTL=255
Reply from 10.10.23.4: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.23.4:
Packets: Sent=4, Received=4, Lost=0 (0% loss),
Approximate round trip times in milliseconds:
Minimum=1ms, Maximum=2ms, Average=1ms
```

PC3 to PC5

```
C:\> ping 10.10.23.16

Pinging 10.10.23.16 with 32 bytes of data:
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255

Ping statistics for 10.10.23.16:
Packets: Sent=4, Received=4, Lost=0 (0% loss),
Approximate round trip times in milliseconds:
Minimum=1ms, Maximum=1ms, Average=1ms
```

PC4 to PC5

```
C:\> ping 10.10.23.16

Pinging 10.10.23.16 with 32 bytes of data:
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255
Reply from 10.10.23.16: bytes=32 time=1ms TTL=255
Reply from 10.10.23.16: bytes=32 time=2ms TTL=255

Ping statistics for 10.10.23.16:
Packets: Sent=4, Received=4, Lost=0 (0% loss)
Approximate round trip times in milliseconds:
Minimum=1ms, Maximum=2ms, Average=1ms
```

HARDWARE LIST

Name	Specification	Quantity	Remarks
UTP cable	PROLINK CAT6 23AWG UTP NETWORK CABLE 305M (GREY)	7	
Transceiver	10/100/1000BASE-T SFP SGMII Copper RJ-45 100m Transceiver Module for FS Switches	12	
Access Point	TP-Link 1 Port Wireless Access Point, IEEE 802.11 ac/n/g/b/a	3	
Face Plate	CAT5E/CAT6 1 Port 2 Ports Faceplate Data Wall Socket Outlet Faceplate 1 Gang RJ45 Wall Socket Single port	100	
Rack	15U Network Cabinet Server Rack soundproof fireproof rack server cabinet Network Switch cabinet	4	
Fibre Cable	Ubiquiti Networks FC-SM-100 FiberCable Single-Mode LC Fiber	2	

	Cable (100')		
Patch Cord	5m SC TO SC FIBER OPTIC PATCH CORD FIVER OPTIC CABLE	6	
Switch	S5850-48T4Q, 48-Port Ethernet L3 Switch, 48 x 10GBASE-T	1	Core
	TP-Link TL-SX1008 8-Port 10G	3	Access
	Aruba Instant On 1930 48-Port Gigabit Managed Switch with 10Gb SFP+	1	Distribution
Patch panel	Patch Panel 48-Port (CAT6 / CAT-6) CAT6 UTP PATCH PANEL 48PORT	3	
	12 Port Fiber Patch Panel SC FC LC Pigtail ODF 1U Optical Fiber Terminal Box Optical Fiber	4	For Fibre Optic

IMPLEMENTATION PLAN

Activities	October				November				December				January			
	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4	W1	W2	W3	W4
Observe the facilities																
Develop project proposal																
Implementing new topology																
Install hardware and Software																
Testing network																
Optimize network																
Data transfer																
User training																
System testing																

PROJECT BUDGET

Hardware Budget				
Name	Specification	Quantity	Price Per Unit (RM)	Total Price (RM)
UTP cable	PROLINK CAT6 23AWG UTP NETWORK CABLE 305M (GREY)	7	400.00	2,800.00
Transceiver	10/100/1000BASE-T SFP SGMII Copper RJ-45 100m Transceiver Module for FS Switches	12	130.00	1,560.00
Access Point	TP-Link 1 Port Wireless Access Point, IEEE 802.11 ac/n/g/b/a	3	596.00	1,788.00
Face Plate	CAT5E/CAT6 1 Port 2 Ports Faceplate Data Wall Socket Outlet Faceplate 1 Gang RJ45 Wall Socket Single port	100	4.00	400.00

Rack	15U Network Cabinet Server Rack soundproof fireproof rack server cabinet Network Switch cabinet	4	569.00	2,276.00
Fibre Cable	Ubiquiti Networks FC-SM-100 FiberCable Single-Mode LC Fiber Cable (100')	2	275.91	551.82
Patch Cord	5m SC TO SC FIBER OPTIC PATCH CORD FIVER OPTIC CABLE	6	8.00	48.00
Switch	S5850-48T4Q, 48-Port Ethernet L3 Switch, 48 x 10GBASE-T	1	21,901.00	21,901.00
	TP-Link TL-SX1008 8-Port 10G	3	1,600.00	4,800.00
	Aruba Instant On 1930 48-Port Gigabit Managed Switch with 10Gb SFP+	1	1,400.15	1,400.15

Patch panel	Patch Panel 48-Port (CAT6 / CAT-6) CAT6 UTP PATCH PANEL 48PORT	3	155.00	465.00
	12 Port Fiber Patch Panel SC FC LC Pigtail ODF 1U Optical Fiber Terminal Box Optical Fiber	4	154.50	618.00
			Total for Hardware Budget	38,607.97
Support and maintenance				
	Support for 5 years (including maintenance)	1	60,000.00	60,000.00
	Training	1	Free	Free
			Total for Support And Maintenance	60,000.00
			Nett Price	98,607.97

A TRAINING PLAN

Training Plan Objective: To brief the State Education Department's staff on how to manage the new network design topology effectively. Below is the training plan that we have conducted for the staff :

Training Plans	**Durations**	**Participants**
Project information session	2 days	All staff State Education Departments
Cisco related training	1 days	10 State Education staff
Brief about the Software & Hardware	1 days	10 State Education staff
Support Training	1 days	10 State Education staff
Software Management training	1 days	10 State Education staff
Firewall training	1 days	10 State Education staff

SUPPORT AND SERVICE INFORMATION

SUPPORT

Depending on the warranty period agreed upon between the third party and the firm, the warranty granted can be used within a particular time frame if an accident or error happens within a few days of the installation of the device, hardware, or software. Any errors or accidents that occur during the trial period have no bearing on the guarantee that is established in accordance with the agreement.

SERVICE INFORMATION

If users have any queries or reservations about utilising the new system, they can seek advice or comments from experts. It can aid with problem-solving and assisting clients in understanding the new system even after providing them with training. Customers can contact us at any time as well.

APPENDICES

ISP

```
ISP#sh run

Building configuration…

Current configuration : 1694 bytes

!

version 15.1

no service timestamps log datetime msec

no service timestamps debug datetime msec service password-encryption

!

hostname ISP

!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
```

```
!

no ip cef no ipv6 cef

!

license udi pid CISCO1941/K9 sn FTX15248N6A-

!

spanning-tree mode pvst

!

Interface GigabitEthernet0/0
 no ip address

duplex auto
 speed autoshutdown

!

interface GigabitEthernet0/1 no ip address
```

```
duplex auto

speed auto shutdown

!

interface GigabitEthernet0/0/0

ip address 100.0.0.5 255.255.255.252

!

interface GigabitEthernet0/1/0 no ip address

!

interface GigabitEthernet0/1/0.1 encapsulation dot1Q 10  native

ip address 10.10.10.1 255.255.255.0

!

interface GigabitEthernet0/1/0.21 encapsulation dot1Q 21
```

```
ip address 10.10.21.1 255.255.255.0

!

interface GigabitEthernet0/1/0.22 encapsulation dot1Q 22

ip address 10.10.22.1 255.255.255.0

!

interface GigabitEthernet0/1/0.23 encapsulation dot1Q 23

ip address 10.10.23.1 255.255.255.0

!

interface GigabitEthernet0/1/0.30 encapsulation dot1Q 30

ip address 10.10.30.1 255.255.255.0

!

interface GigabitEthernet0/1/0.40 encapsulation dot1Q 40
```

```
ip address 10.10.40.1 255.255.255.0

!

interface GigabitEthernet0/1/0.50 encapsulation dot1Q 50

ip address 10.10.50.1 255.255.255.0

!

interface Vlan1 no ip address shutdown

!

router ospf 10

router-id 1.1.1.1

log-adjacency-changes network 100.0.0.5 0.0.0.0 area 0

network 10.10.10.0 0.0.255.255 area 1

!
```

```
ip classless

!

ip flow-export version 9

!

banner motd ^CUnauthorized User are now allowed^C

!

line con 0

password 7 0822455D0A16 login

!

line aux 0

!

line vty 0 4
```

```
password 7 0822455D0A16 login


!


!


end
```

CoreSwitch

```
CoreSwitch#sh run

 Building configuration...



Current configuration : 3182 bytes

!

version 16.3.2

no service timestamps log datetime msec

no service timestamps debug datetime msec service password-encryption

!

hostname CoreSwitch

!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

!
```

```
ip dhcp pool 1stFloor

network 10.10.21.0 255.255.255.0
default-router 10.10.21.1
dns-server 10.10.10.10

ip dhcp pool 2ndFloor

network 10.10.22.0 255.255.255.0
default-router 10.10.22.1
dns-server 10.10.10.10

ip dhcp pool 3rdFloor

network 10.10.23.0 255.255.255.0
default-router 10.10.23.1
dns-server 10.10.10.10

 ip dhcp pool Staff

network 10.10.30.0 255.255.255.0
default-router 10.10.30.1
dns-server 10.10.10.10
```

```
ip dhcp pool Guest

network 10.10.40.0 255.255.255.0
default-router 10.10.40.1
dns-server 10.10.10.10

!

no ip cef ip routing

!

no ipv6 cef

!

spanning-tree mode pvst

!

interface GigabitEthernet1/0/1
switchport trunk encapsulation dot1q
switchport mode trunk
```

```
!

interface GigabitEthernet1/0/2
switchport trunk encapsulation dot1q
switchport mode access

switchport nonegotiate

!

interface GigabitEthernet1/0/3
 switchport trunk encapsulation dot1q
 switchport mode access

switchport nonegotiate

!

interface GigabitEthernet1/0/4
 switchport trunk encapsulation dot1q
 switchport mode trunk

!
```

```
interface GigabitEthernet1/0/5
 switchport trunk encapsulation dot1q
switchport mode trunk

!

interface GigabitEthernet1/0/6
 switchport trunk encapsulation dot1q
switchport mode trunk

!

interface GigabitEthernet1/0/7

!

interface GigabitEthernet1/0/8

!

interface GigabitEthernet1/0/9
```

!

interface GigabitEthernet1/0/10

!

interface GigabitEthernet1/0/11

!

interface GigabitEthernet1/0/12

!

interface GigabitEthernet1/0/13

!

interface GigabitEthernet1/0/14

!

interface GigabitEthernet1/0/15

```
!

interface GigabitEthernet1/0/16

!

interface GigabitEthernet1/0/17

!

interface GigabitEthernet1/0/18

!

interface GigabitEthernet1/0/19

!

interface GigabitEthernet1/0/20

!

interface GigabitEthernet1/0/21
```

```
!

interface GigabitEthernet1/0/22

!

interface GigabitEthernet1/0/23

!

interface GigabitEthernet1/0/24

!

interface GigabitEthernet1/1/1

switchport trunk encapsulation dot1q

switchport mode trunk

!

interface GigabitEthernet1/1/2

!
```

```
interface GigabitEthernet1/1/3

!

interface GigabitEthernet1/1/4

!

interface Vlan10

ip address 10.10.10.2 255.255.255.0

shutdown

!

interface Vlan21

mac-address 0006.2a10.5701

ip address 10.10.21.2 255.255.255.0

!
```

```
interface Vlan22

mac-address 0006.2a10.5702

ip address 10.10.22.2 255.255.255.0

!

interface Vlan23

mac-address 0006.2a10.5703

ip address 10.10.23.2 255.255.255.0

!

interface Vlan30

mac-address 0006.2a10.5704

ip address 10.10.30.2 255.255.255.0

!

interface Vlan40
```

```
mac-address 0006.2a10.5705

ip address 10.10.40.2 255.255.255.0

!

!

ip classless

!

ip flow-export version 9

!

banner motd ^CUnauthorized User are now allowed^C

!

line con 0

password 7 0822455D0A16 login

!
```

```
line aux 0

!

line vty 0 4

password 7 0822455D0A16 login

line vty 5 15

password 7 0822455D0A16 login

!

!

end
```

StateEducationDepartment

StateEducationDepartment

#sh run Building configuration...

Current configuration : 1866 bytes

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

service password-encryption

!

hostname StateEducationDepartment

!

```
enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0

!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

switchport mode trunk

!

interface FastEthernet0/2

 switchport mode trunk

!
```

```
interface FastEthernet0/3

switchport mode trunk

!

interface FastEthernet0/4

 switchport mode trunk

!

interface FastEthernet0/5

switchport mode trunk

!

interface FastEthernet0/6

switchport mode trunk

!
```

```
interface FastEthernet0/7

 switchport mode trunk

!

interface FastEthernet0/8

 switchport mode trunk

!

interface FastEthernet0/9

switchport mode trunk

!

interface FastEthernet0/10

switchport mode trunk

!
```

```
interface FastEthernet0/11

switchport mode trunk

!

interface FastEthernet0/12

switchport mode trunk

!

interface FastEthernet0/13

switchport mode trunk

!

interface FastEthernet0/14

switchport mode trunk

!
```

```
interface FastEthernet0/15

switchport mode trunk

!

interface FastEthernet0/16

switchport mode trunk

!

interface FastEthernet0/17

switchport mode trunk

!

interface FastEthernet0/18

switchport mode trunk

!
```

```
interface FastEthernet0/19

switchport mode trunk

!

interface FastEthernet0/20

switchport mode trunk

!

interface FastEthernet0/21

switchport mode trunk

!

interface FastEthernet0/22

switchport mode trunk

!
```

```
interface FastEthernet0/23

switchport mode trunk

!

interface FastEthernet0/24

switchport mode trunk

!

interface GigabitEthernet0/1

switchport mode trunk

!

interface GigabitEthernet0/2

 switchport mode trunk

!
```

```
interface Vlan10

ip address 10.10.10.3 255.255.255.0

!

banner motd ^CUnauthorized User are now allowed^C

!

!

!

line con 0

password 7 0822455D0A16 login

!

line vty 0 4

password 7 0822455D0A16 login
```

```
line vty 5 15

password 7 0822455D0A16 login

!

!

end
```

1stFloor

```
1stFloor#sh run

Building configuration...

Current configuration : 2536 bytes

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec service password-encryption

!

hostname 1stFloor

!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
```

```
!

!

spanning-tree mode pvst

spanning-tree extend system-id

!

interface FastEthernet0/1

switchport mode trunk

!

interface FastEthernet0/2

 switchport mode trunk

!

interface FastEthernet0/3

 switchport access vlan 21
```

```
 switchport mode access


!


interface FastEthernet0/4
 switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/5
switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/6
 switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/7
switchport access vlan 21
```

```
 switchport mode access


!


interface FastEthernet0/8
 switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/9
 switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/10
switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/11
 switchport access vlan 21
```

```
switchport mode access


!


interface FastEthernet0/12
switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/13
 switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/14
 switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/15
 switchport access vlan 21
```

```
 switchport mode access


!


interface FastEthernet0/16
 switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/17
 switchport access vlan 21
 switchport mode access


!




interface FastEthernet0/18
 switchport access vlan 21
 switchport mode access


!


interface FastEthernet0/19
```

```
switchport access vlan 21
switchport mode access

!

interface FastEthernet0/20
 switchport access vlan 21
 switchport mode access

!

interface FastEthernet0/21
switchport access vlan 21
switchport mode access

!

interface FastEthernet0/22
 switchport access vlan 21
 switchport mode access

!

interface FastEthernet0/23
```

```
 switchport access vlan 21
 switchport mode access

!

interface FastEthernet0/24
switchport access vlan 21
switchport mode access

!

interface GigabitEthernet0/1
switchport mode trunk

!

interface GigabitEthernet0/2
 switchport mode trunk

!

interface Vlan10
ip address 10.10.10.4 255.255.255.0
```

```
!


banner motd ^CUnauthorized User are now allowed^C


!


line con 0
password 7 0822455D0A16 login


!


line vty 0 4


password 7 0822455D0A16 login


line vty 5 15
password 7 0822455D0A16 login


!


end
```

2ndFloor

```
2ndFloor#sh run

Building configuration...

Current configuration : 2515 bytes

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec service password-encryption

!

hostname 2ndFloor

!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
```

```
!

!

spanning-tree mode pvst spanning-tree extend system-id

!

interface FastEthernet0/1

 switchport mode access

!

interface FastEthernet0/2

 switchport mode trunk

!

interface FastEthernet0/3

 switchport access vlan 22

 switchport mode access
```

```
!

interface FastEthernet0/4
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/5
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/6
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/7
 switchport access vlan 22
 switchport mode access
```

```
!

interface FastEthernet0/8
 switchport access vlan22
switchport mode access

!

interface FastEthernet0/9
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/10
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/11
 switchport access vlan 22
 switchport mode access
```

```
!

interface FastEthernet0/12
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/13
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/14
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/15
 switchport access vlan 22
 switchport mode access
```

```
!

interface FastEthernet0/16
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/17
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/18
switchport access vlan 22
switchport mode access

!

interface FastEthernet0/19
 switchport access vlan 22
 switchport mode access
```

```
!

interface FastEthernet0/20
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/21
switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/22
 switchport access vlan 22
 switchport mode access

!

interface FastEthernet0/23
switchport access vlan 22
switchport mode access
```

```
!

interface FastEthernet0/24
 switchport access vlan 22
 switchport mode access

!

interface GigabitEthernet0/1
 switchport mode trunk

!

interface GigabitEthernet0/2
 switchport mode trunk

!

interface Vlan10
ip address 10.10.10.5 255.255.255.0

!
```

```
interface Vlan21

 no ip address

!

banner motd ^CUnauthorized User are now allowed^C

!

line con 0

password 7 0822455D0A16 login

!

line vty 0 4

password 7 0822455D0A16 login

line vty 5 15

password 7 0822455D0A16 login

!
```

```
!


end
```

3rdFloor

```
3rdFloor#sh run

Building configuration...

Current configuration : 2508 bytes

!

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec service password-encryption

!

hostname 3rdFloor

!

enable secret 5 $1$mERr$hx5rVt7rPNoS4wqbXKX7m0
```

```
!

spanning-tree mode pvst spanning-tree extend system-id

!

interface FastEthernet0/1

 switchport mode trunk

!

interface FastEthernet0/2
 switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/3
 switchport access vlan 23
switchport mode access

!
```

```
interface FastEthernet0/4
switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/5
 switchport access vlan 23
switchport mode access

!

interface FastEthernet0/6
switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/7
switchport access vlan 23
 switchport mode access

!
```

```
interface FastEthernet0/8
switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/9
 switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/10
 switchport access vlan 23
switchport mode access

!

interface FastEthernet0/11
 switchport access vlan 23
 switchport mode access

!
```

```
interface FastEthernet0/12
 switchport access vlan 23
switchport mode access

!

interface FastEthernet0/13
switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/14
 switchport access vlan 23
switchport mode access

!

interface FastEthernet0/15
 switchport access vlan 23
switchport mode access

!
```

```
interface FastEthernet0/16
 switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/17
 switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/18
switchport access vlan 23
switchport mode access

!

interface FastEthernet0/19
switchport access vlan 23
 switchport mode access

!
```

```
interface FastEthernet0/20
 switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/21
 switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/22
 switchport access vlan 23
 switchport mode access

!

interface FastEthernet0/23
switchport access vlan 23
switchport mode access

!
```

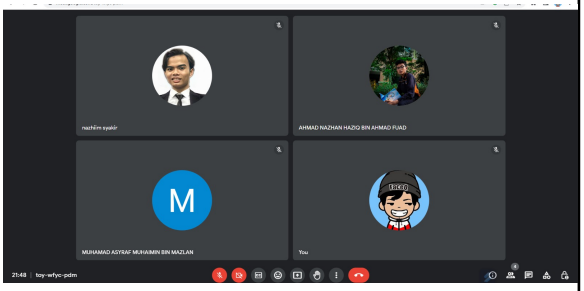
```
interface FastEthernet0/24
switchport access vlan 23
 switchport mode access

!

interface GigabitEthernet0/1
 switchport mode trunk

!

interface GigabitEthernet0/2
switchport mode trunk

!

interface Vlan10
ip address 10.10.10.6 255.255.255.0

!

banner motd ^CUnauthorized User are now allowed^C
```

```
!

line con 0

password 7 0822455D0A16 login

!

line vty 0 4

password 7 0822455D0A16 login

line vty 5 15

password 7 0822455D0A16 login

!

!

end
```

REFERENCES

1. PacketTracerNetwork. (14 April 2020). *Download cisco packet tracer 8.2.1 & GNS3*. Cisco Packet Tracer. Accessed on 27 June 2023 <https://www.packettracernetwork.com/download/download-packet-tracer.html>
2. Tech-FAQ. (6 April 2019). "*Considerations in planning a Network Infrastructure*". Tech-FAQ. Accessed on 27 June 2023 <https://www.tech-faq.com/considerations-in-planning-a-network-infrastructure.htm>
3. Admin, A. (17 October 2022). "*Ultimate Guide to Designing Your Network Infrastructure*". AxiomQ. Accessed on 27 June 2023 <https://axiomq.com/blog/ultimate-guide-to-designing-your-network-infrastructure/>
4. PCS. (n.d.). "*Infrastructure, network, and server management*". PCS. Accessed on 27 June 2023 <https://www.helpmepcs.com/server-network-management>
5. Hari Subedi, (22 November 2020). "A Guide To Network Topology". JONES IT. Accessed on 27 June 2023 <https://www.itjones.com/blogs/2020/11/22/a-guide-to-network-topology>
6. Jennifer Bridges, (10 May 2023). "How to Make a Project Budget: Project Budgeting Basics". Accessing on 27 June 2023 <https://www.projectmanager.com/training/create-and-manage-project-budget#:~:text=What%20Is%20a%20Project%20Budget,of%20the%20project%20planning%20process.>
7. Larry Ponemon. (14 September 2007). "Eight Strategies to Strengthen Network Security". Ponemon Institute. Accessed on 27 June 2023 <https://www.cio.com/article/274617/it-strategy-eight-strategies-to-strengthen-network-security.html>

MEETING MINUTE ALPHA-1B

Date	10/05/2023
Time	9:00 PM
Attendances	1. AFIQ 2. NAZHAN 3. ASYRAF 4. NAZHIM
Agenda Items	1. Team Leader starts the meet by using google meet. 2. Start discussion about progress 1. 3. The Team Leader give and divide the task
Meeting Evidences	

Date	9/06/2023
Time	12:00 PM
Attendances	5. AFIQ 6. NAZHAN 7. ASYRAF 8. NAZHIM
Agenda Items	4. Team Leader starts the meeting face to face. 5. Start discussion about progress 2. 6. The Team Leader give and divide the task
Meeting Evidences