**TABLE OF CONTENTS**

## CHAPTERS CONTENTS PAGE NO.

* + - 1. **INTRODUCTION**
      2. **DEVICE AND EQUIPMENTS USED**
      3. **NETWORK SCOPE**
      4. **OBJECTIVE**
      5. **NETWORK NEED ANALYSIS**
      6. **NETWORK DIAGRAM AND TOPOLOGIES**
      7. **IMPLEMENTATION**
      8. **CONCLUSION, LIMITATIONS**
      9. **REFERENCES**

# 

**Introduction: -**

The general aim of this project is to simulate a banking system which is secure and easy to use. Previously the system was manual, not secure, also working slowly. This proposed system overcomes the lacking of the existing manual system. All branches of the Bank situated at District level provide the Banking services to customers and had to send report to the central branch manually, which sometimes creates problem to get, up-to-date information rapidly. But now through this system whenever any transaction will be taking place it will store in the central database and authorized person can get necessary information or report when they get into the system from any branches through Wide Area Network (WAN).To implement our project we have used OSI model. This system is using Packet Tracer 5.3 for network simulation, Wamp Server, PHP Mysql, for Banking Web application Security. After implementation of all functions, the system is tested in different stages and it was successful for its purpose. Bank will have have departments of internal IT supports, ATM services, consumer banking, investment banking, loans and insurance. All their departments network is separated but able to communicate with each other using an internal chatting system using a port. AHB Bank has a budget of RM200,000 and prefer the branch to have a balance between network performance network performance, security and cost effectiveness.

## Devices & Equipment Used

IT Department

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Model | Port | IP Address | Subnet Mask | Default gateway |
| IT Admin | PC-PT | Fe0 | 192.168.10.100 | 255.255.255.0 | 192.168.10.1 |
| IT Admin2 | PC-PT | Fe0 | 192.168.10.200 | 255.255.255.0 | 192.168.10.1 |
| Server | Server-PT | Fe0 | 192.168.10.254 | 255.255.255.0 | N/A |
| SwitchIT | 2960-24TT | N/A | N/A | N/A | N/A |

Table 1: IT department

ATM

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Model | Port | IP Address | Subnet Mask | Default gateway |
| ATM | PC-PT | Fe0 | 192.168.20.101 | 255.255.255.0 | 192.168.20.1 |
| ATM2 | PC-PT | Fe0 | 192.168.20.201 | 255.255.255.0 | 192.168.20.1 |
| ATM3 | PC-PT | Fe0 | 192.168.20.301 | 255.255.255.0 | 192.168.20.1 |
| SwitchATM | 2960-24TT | N/A | N/A | N/A | N/A |

Table 2: ATM

Consumer Banking

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Model | Port | IP Address | Subnet Mask | Default gateway |
| ConsuPC | PC-PT | Fe0 | 192.168.30.101 | 255.255.255.0 | 192.168.30.1 |
| ConsuPC2 | PC-PT | Fe0 | 192.168.30.201 | 255.255.255.0 | 192.168.30.1 |
| ConsuPC3 | PC-PT | Fe0 | 192.168.30.301 | 255.255.255.0 | 192.168.30.1 |
| SwitchConsumer | 2960-24TT | N/A | N/A | N/A | N/A |

Table 3: Consumer Banking

Investment Banking

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Model | Port | IP Address | Subnet Mask | Default gateway |
| InvestPC | PC-PT | Fe0 | 192.168.40.101 | 255.255.255.0 | 192.168.40.1 |
| InvestPC2 | PC-PT | Fe0 | 192.168.40.201 | 255.255.255.0 | 192.168.40.1 |
| InvestPC3 | PC-PT | Fe0 | 192.168.40.301 | 255.255.255.0 | 192.168.40.1 |
| SwitchInvest | 2960-24TT | N/A | N/A | N/A | N/A |

Table 4: Investment Banking

Loans

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Model | Port | IP Address | Subnet Mask | Default gateway |
| LoansPC | PC-PT | Fe0 | 192.168.50.101 | 255.255.255.0 | 192.168.50.1 |
| LoansPC2 | PC-PT | Fe0 | 192.168.50.201 | 255.255.255.0 | 192.168.50.1 |
| LoansPC3 | PC-PT | Fe0 | 192.168.50.301 | 255.255.255.0 | 192.168.50.1 |
| SwitchLoans | 2960-24TT | N/A | N/A | N/A | N/A |

Table 5: Loans

Insurance

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Model | Port | IP Address | Subnet Mask | Default gateway |
| InsuPC | PC-PT | Fe0 | 192.168.60.101 | 255.255.255.0 | 192.168.60.1 |
| InsuPC2 | PC-PT | Fe0 | 192.168.60.201 | 255.255.255.0 | 192.168.60.1 |
| InsuPC3 | PC-PT | Fe0 | 192.168.60.301 | 255.255.255.0 | 192.168.60.1 |
| SwitchInsu | 2960-24TT | N/A | N/A | N/A | N/A |

Table 6: Insurance

Guest WiFi

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Model | Port | IP Address | Subnet Mask | Default gateway |
| Guest-Wifi Router | HomeRouter-PT-AC | N/A | N/A | N/A | N/A |
| GuestDevice | SMARTPHONE-PT | Wireless0 | 192.168.70.2 | 255.255.255.0 | 192.168.70.1 |

Table 7: Guest WiFi

Multilayer Switch

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Device | Model | Port | IP Address | Subnet Mask | Default gateway |
| Multi-sw 1(MAIN) | 3650-24PS | Vlan10 | 192.168.10.1 | 255.255.255.0 | N/A |
| Vlan11 | 192.168.20.1 | 255.255.255.0 |
| Vlan12 | 192.168.30.1 | 255.255.255.0 |
| Vlan13 | 192.168.40.1 | 255.255.255.0 |
| Vlan14 | 192.168.50.1 | 255.255.255.0 |
| Vlan15 | 192.168.60.1 | 255.255.255.0 |
| Vlan16 | 192.168.70.1 | 255.255.255.0 |
| Vlan17 | 192.168.80.1 | 255.255.255.0 |

Table 8: Multilayer Switch

## 

## Network Scope

This proposed network has 6 main departments for their new outlet which are:

* Internal IT support
* ATM services
* Consumer Banking
* Investment Banking
* Loans
* Insurance

## Objectives

Below are the main goals of the network being to achieve several operational objectives which are:

* Every department network is separated. All staffs can communicate through emails and an internal chatting system using port 465.
* There should be a guest Wi-Fi is provided to customers. This is an isolated network isolated with only web browsing capabilities.
* The IT department consists of a small team that the staffs are mainly performing operational tasks instead of planning and implementations. Your team is required to provide detail documentations so that the IT staffs can troubleshoot their systems with references.
* Your team are working to strike a balance between network performance, security and cost effectiveness so that your team can close this deal.

## Design Features and Coverage

One of the features that we apply is ACL (Access Control-List)

|  |  |
| --- | --- |
| Vlan/Subnet | ACL Permission |
| Vlan10: IT Department | - Remote access (SSH) to all the networking devices for troubleshooting, except ATM network.  - perform remote into the branch through VPN for troubleshooting.  - communicate throught emails and an internal chatting system using port 465. |
| Vlan11: ATM | - Isolated network and directly connect to Headquarter network through 5556 port.  - All staffs including IT support has no access to the ATM network. |
| Vlan12: Consumer Banking | - communicate throught emails and an internal chatting system using port 465. |
| Vlan13: Investment Banking | - communicate throught emails and an internal chatting system using port 465.  - Internet access (HTTP and HTTPS only) to support overseas customers. |
| Vlan14: Loans | - communicate throught emails and an internal chatting system using port 465.  - Internet access with port 9999 to check customer credit scores. |
| Vlan15: Insurance | - communicate throught emails and an internal chatting system using port 465.  - port 7772 to connect to national insurance portal.  -No internet access. |
| Vlan16: Guest Wifi | -Only can connect to WiFi |

Table 9: Access Control List Permissions

## Design Assumptions

This network design is only meant for a small scale organization where the access point could support approximately 200 users. The extra or unused port either on layer 2 or 3 switch could be reserved for further use especially when there is a need of expanding the network usage.

# Network Needs Analysis

## Data Types & Sources for Daily Operations

## Number of Users & Priority Levels

The consumer department would be the main users that occupies 60% of the network usage while the IT department would have the highest priority where they are tasked with taking care of networking devices of AHB bank and they are able to Access all the department’s network with the ability to provide VPN services to remote department and perform actions. The ATM department occupies 15% of the network usage and it is isolated network and directly connect to Headquarter network. The loans and Investment Department will also occupies 10% each of the network usage for check the customer credit score and support overseas customers. While the rest of the departments are within low priority as they do not require to use the network extensively compared to the other departments.

## Security Requirements

Here are the main objectives of our network’s security requirements which comprises of:

* Users are required to change their password every 90 days.
* The IT Department are given the privilege to access all the group’s network and they are able to conduct troubleshooting activities remotely to all the groups’ network.
* Firewalls will be implemented within the server to prevent unauthorized users from accessing the networks.
* All routers are provided with the security of radius aaa server and have their own usernames and passwords.

## Transmission Speed Requirements

We recommend a minimum connectivity speed of 100 Mbps and a target speed of 1 Gbps per 100 users by 2019. In preparing for next generation applications, it is critical to replace 100 Mbps shared-bandwidth hubs in the wiring closet with Ethernet and Fast Ethernet (100/1000 Mbps) or Gigabit Ethernet (10000 Mbps) switches. These switches dedicate 100-, 1000- or 10000-Mbps bandwidth to an individual LAN or WLAN node.

## Load Variations Estimates

Average required throughput upon LAN during work hours are 5 Mbps while expected peak traffic load would be ranging 10 Mbps - 20 Mbps. We are designing the network in such a way to accommodate the peak traffic load instead of the average required throughput.

## 4.6 Reliability Requirements

The network will be designed to be running with an expected uptime of 99.99% with an undiscovered error rate of 0.01%.

# Network Diagram and Topologies

## Site 1 – IT Department

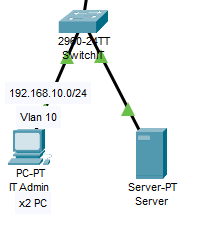


Figure 1: Site 1 - IT Dept. Design

This site consists of 2 IT administrators, and 1 server. The default gateway got IT Department is 192.168.10.1/24. IT Department is using VLAN 10 to control access between the groups.

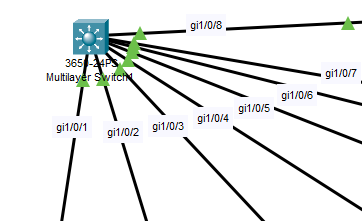


Figure 2: Main Multilayer Switch (Layer 3 Switch)

Trunk (encapsulation dot1q) is used at the Multilayer switch (layer 3 switch) as we want create VLAN traffic between the switches. A trunk connection is a normal link that is able to pass traffic from different VLANs and has a method to separate traffic between VLANs.

DHCP protocol are used on layer 3 switch so that it could enable automatic assignment of IP configurations for nodes on the network. It is efficient as we do not have to assign all the IP addresses manually. The DHCP server accepts address assignment requests and renewals from the client and assigns the addresses from predefined groups of addresses within DHCP address pools. These address pools are also be configured to supply additional information to the requesting client such as the IP address of the Domain Name System (DNS) server.

## Site 2 – ATM

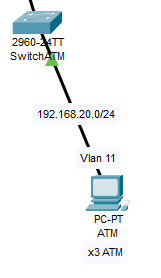


Figure 3: Site 2 -ATM. Design

As for site 2, this would be the ATM Department which consists 3 ATM and 1 Switch of ATM. ATM Department is using VLAN 11 to control access between the departments.

## Site 3 – Consumer Banking

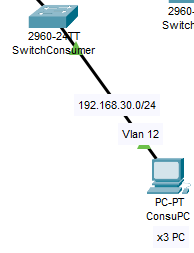


Figure 4: Site 3 - Consumer Banking. Design

The figure above is the site dedicated for the Consumer Banking department. It consists 3 Consumer PC and 1 Switch for Consumer Department, and it’s using VLAN 12 to control access between the departments.

## Site 4 – Investment Banking

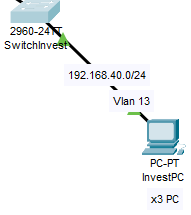


Figure 5: Site 4 - Investment Banking Design

As for Site 4, This is Investment Banking which consists 3 PC of Investment and 1 switch for using VLAN 13 to control access between the department.

## Site 5 – Loans

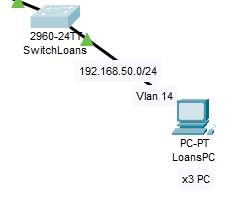


Figure 6: Site 5 - Loans Design

This Site 5 is for the Loans Department and its consists 3 Loans PC for staff and 1 switch for Loans Department. Its using VLAN 14 to control access between the departments.

## Site 6 – Insurance

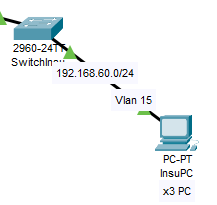


Figure 7: Site 6 - Insurance Design

The figure above is the site dedicated for the Insurance department. It consists 3 Insurance PC for staff and 1 Switch for Insurance Department, and it’s using VLAN 15 to control access between the departments.

## Site 7 – Guest Wifi

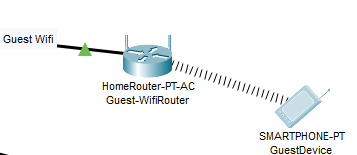


Figure 8: Guest Wifi Design

As for Site 4, This is Guest Wifi Design which only consists 1 Wireless router and 1 example device of user for access into internet. Its using VLAN 16 that only allow users to access the internet.

## Site 8 – Site-to-site VPN

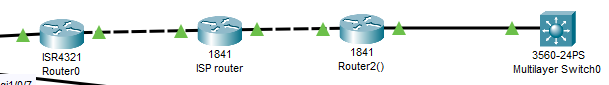
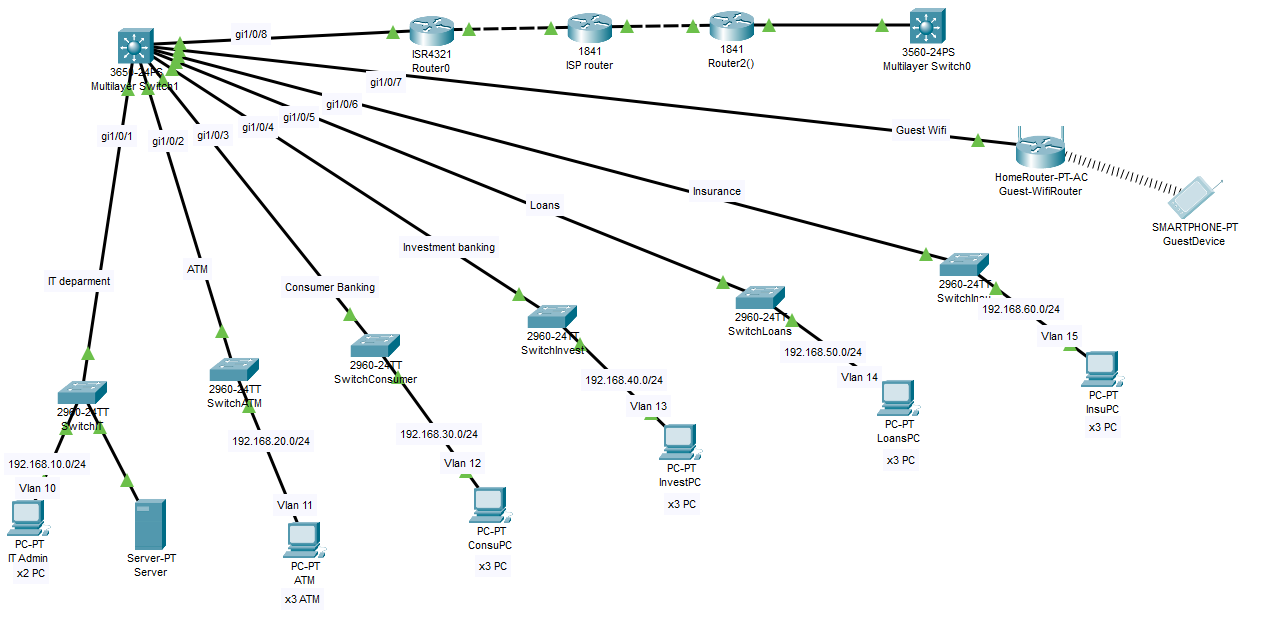


Figure 9: VPN Design

Site-to-Site IPSec VPN Tunnels are used to allow the secure transmission of data and perform remote into the branch for troubleshooting. The VPN tunnel is created over the Internet public network and encrypted using a number of advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

## Overview of entire network



# CONCLUSION: -

# Now a days, technological development, and automated system development is more essential and crying need for the expansion of banking services because They will need less employers by using automated system. On top of that Security is a major issue regarding banking issues. With this system network will be easier to handle and it will route the data in a shortest path in a vast distributed system. In future we will try to implement it in real life so that banks can use it and get benefited from this project.

**Limitations: -**

* One of the limitations of this system is that it is not applicable in real world as it was simulated using packet tracer.
* High initial cost.
* Over reliance on networks.

# References

A Short Guide to Network Disaster Recovery Planning. (2019, March 5). Retrieved from https://www.nakivo.com/blog/create-effective-network-disaster-recovery-plan/