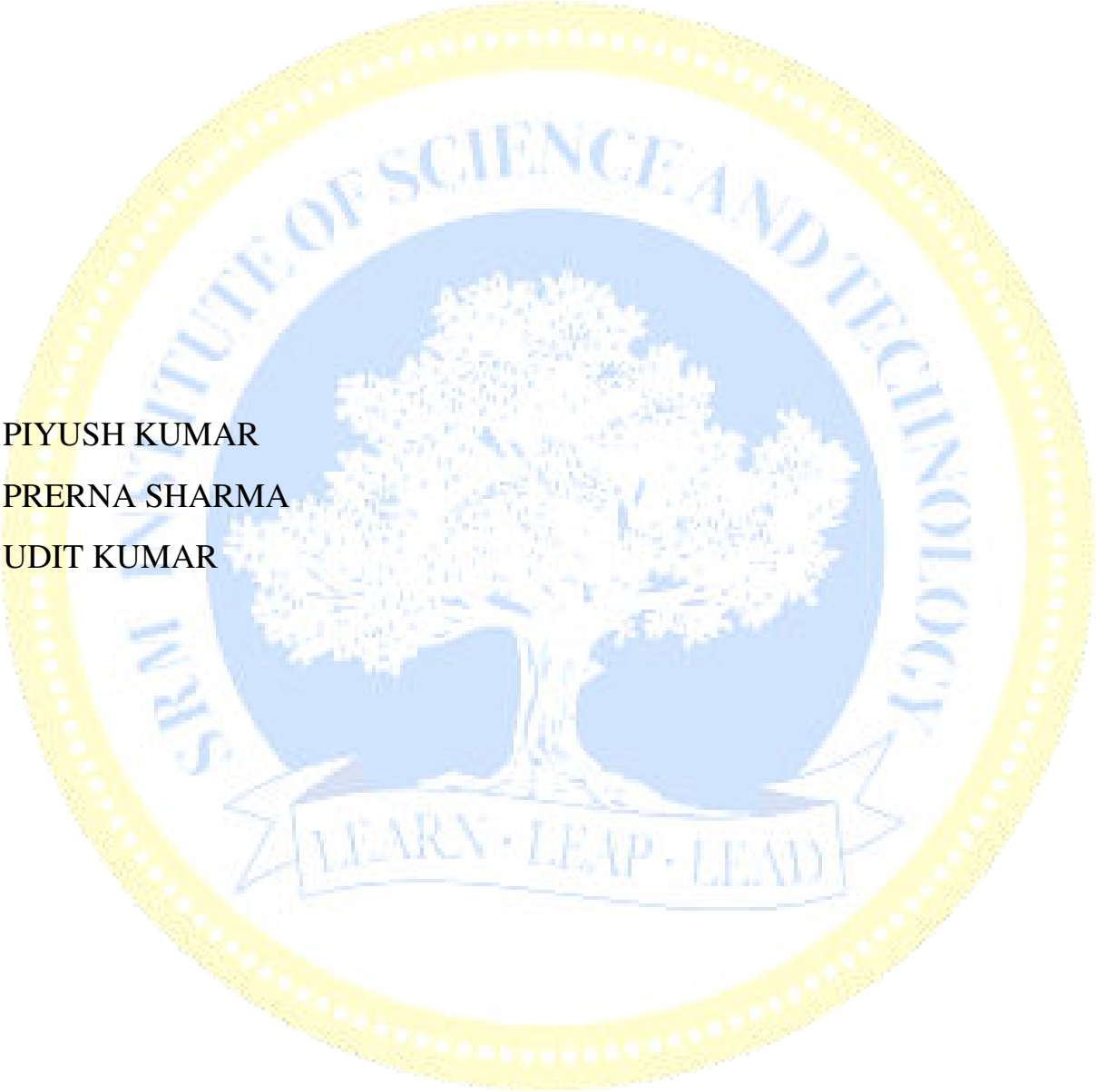
# Network Design Proposal for Banking System




PIYUSH KUMAR

PRERNA SHARMA

UDIT KUMAR

*SRM Institute of Science and Technology*

# NETWORK DESIGN PROPOSAL FOR BANKING SYSTEM REPORT


***Submitted by***

**PIYUSH KUMAR (RA2011031010078)**

**PRERNA SHARMA (RA2011031010086)**

**UDIT KUMAR (RA2011031010099)**


***Under the Guidance of***

**Ms. M. Safa**

**(Assistant Professor Department of NWC)**

***in partial fulfilment of the requirement for the IV semester for subject***

**COMPUTER COMMUNICATIONS**

of

**BACHELOR OF TECHNOLOGY**

in

**COMPUTER SCIENCE ENGINEERING**



**DEPARTMENT OF NWC**

**COLLEGE OF ENGINEERING AND TECHNOLOGY**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

**KATTANKULATHUR- 603 203**


**SESSION- 2021-22**

# ACKNOWLEDGMENTS

We sincerely thank Ms. M. Safa, Assistant Professor, Department of Networking and Communications, who have been the greatest inspiration and have provided sufficient background knowledge and understanding of this subject.

Our humble prostration goes to her, for providing all the necessary resources and environment, which have aided us to complete this project successfully.

# ABSTRACT

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 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 LAN and WAN. To implement our project, we have used Packet Tracer 5.3 for network simulation. After implementation of all functions, the system is tested in different stages and it was successful for its purpose. It provides support to various applications of banking. This Network will let various users of the bank and their employees connect to the main Server. The objective only authorized user to access Network including all servers and network devices. It provides greater speed & reduce time consumption and 99.99% of uptime of Network. It allocates bandwidth to servers accordingly. The proposed Network will be user-friendly so that even a beginner can troubleshoot any issue easily.

# Table of Contents

## 1.0 Introduction

### 1.1 Company Background

SRM Bank is setting up a new 3-storey branch in Hinduja Business Park, Noida, Uttar Pradesh. It is planning to have 6 departments allocated on their new branch in Hinduja Business Park. SRM Bank proposed to 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. SRM Bank has a budget of Rs.20,00,00,000 and prefer the branch to have a balance between network performance network performance, security and cost effectiveness.

### 1.2 People Involved

Below are the people involved when implementing the network system for SRM Bank.

- Lead Network Engineer
- Network Administrator

## 2.0 Scope of Work

### 2.1 Coverage of Work

Lead Network Engineer is responsible for implementing, maintaining, supporting, developing and, in some cases, designing communication networks within an organization. His focus is to ensure that high availability and stable network infrastructure to provide maximum performance for their users. Occasionally he will help on documents and perform analysis of all networking topologies.

Network Administrator is responsible for the day-to-day operation to maintaining computer network and solving the problems that might occur to them. Mainly focusing on installing and configuring computer networks and identifying any problems that arise with computer networks and system. He also helps on prepare research plans and documented projects for all LAN and WAN based methods. Identify and resolve all technical issues in the matter of formulation and creation of strategies.

## 2.2 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 Wi-Fi

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

*Table 7: Guest Wi-Fi*

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*

# 3.0 Feasibility Study

## 3.1 Network Scope

This proposed network is designed for SRM Bank in Hinduja Business Park, Noida, Uttar Pradesh. The client requires 6 main departments for their new outlet which are:

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

SRM Bank provided us with a budget of Rs. 20,00,00,000 to design a network for them that has high performance and cost effectiveness.

## 3.2 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. The team is required to provide detail documentations so that the IT staffs can troubleshoot their systems with references.
- The team is working to strike a balance between network performance, security and cost effectiveness so that it can close this deal.

## 3.3 Design Features and Coverage

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

| Vlan/Subnet | ACL Permission |
|---|---|
| Vlan10: IT | - Remote access (SSH) to all the networking devices for |

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

*Table 9: Access Control List Permissions*

### 3.4 Design Assumptions

This network design is only meant for a small-scale organization (SRM Bank) 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.

## 4.0 Network Needs Analysis

### 4.1 Data Types & Sources for Daily Operations

### 4.2 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 SRM 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 occupy 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.

### 4.3 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 and server and have their own usernames and passwords.

### 4.4 Transmission Speed Requirements

We recommend a minimum connectivity speed of 100 Mbps and a target speed of 1 Gbps per 100 users for SRM Bank 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.

### 4.5 Load Variations Estimates

Based on SRM Bank operating hours, the network will be mainly used during the weekdays from 9 a.m. to 5 p.m. from Monday to Friday. Peak network traffic volume is expected to experience during 10 a.m. up till 4 p.m.

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%.

## 5.0 Network Diagram and Topologies

### 5.1 Site 1 – IT Department

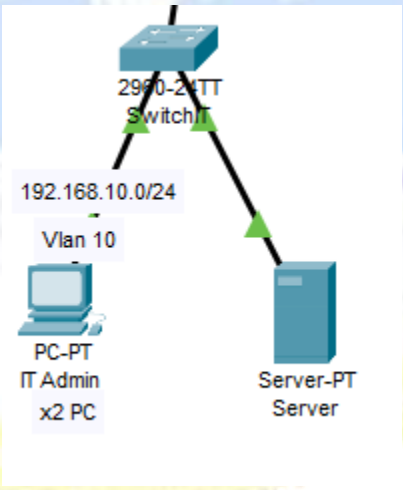



*Figure 1: Site 1 - IT Dept. Design*

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.

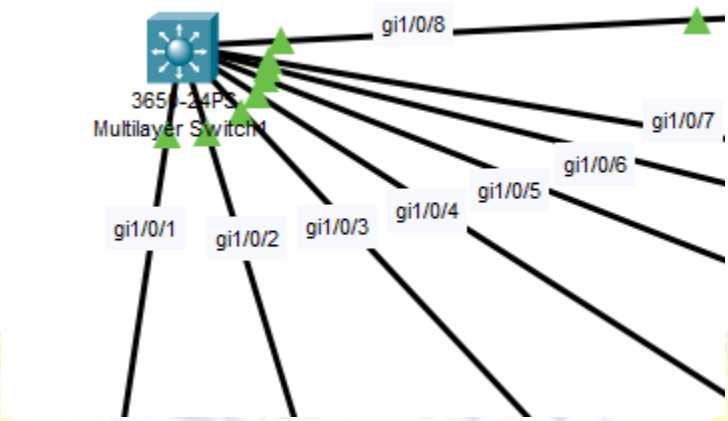



*Figure 2: Main Multilayer Switch (Layer 3 Switch)*

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.

## 5.2 Site 2 – ATM

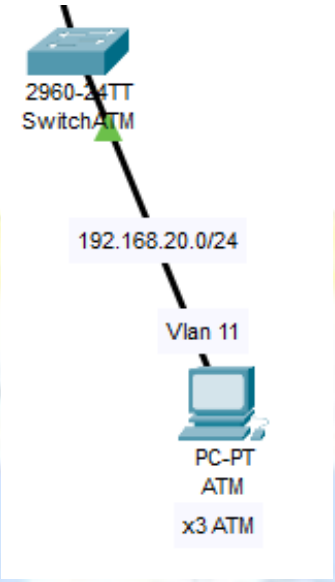



*Figure 3: Site 2 -ATM. Design*

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.

## 5.3 Site 3 – Consumer Banking

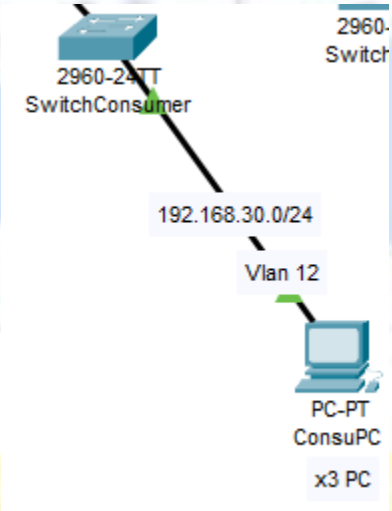



*Figure 4: Site 3 - Consumer Banking. Design*

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.

## 5.4 Site 4 – Investment Banking

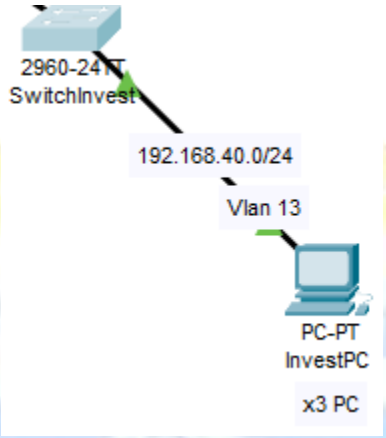



*Figure 5: Site 4 - Investment Banking Design*

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.

## 5.5 Site 5 – Loans

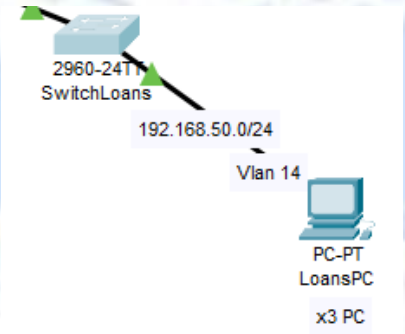



*Figure 6: Site 5 - Loans Design*

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

## 5.6 Site 6 – Insurance

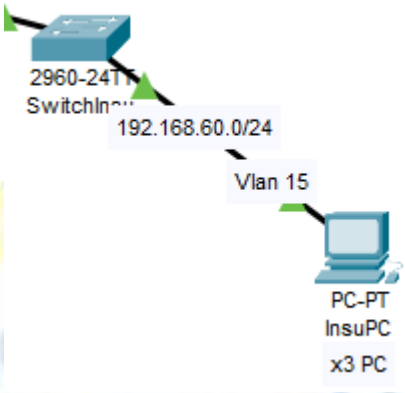



*Figure 7: Site 6 - Insurance Design*

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.

## 5.7 Site 7 – Guest Wi-Fi

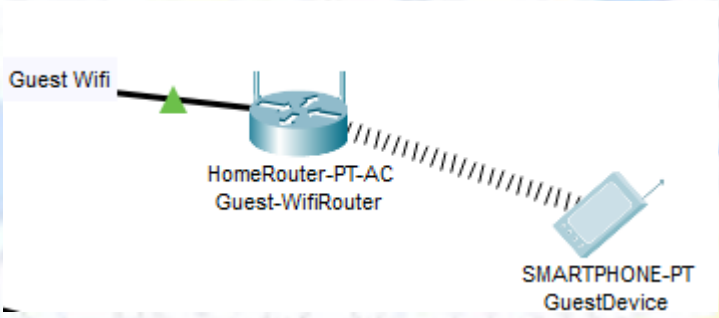



*Figure 8: Guest Wi-Fi Design*

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

### 5.8 Site 8 – Site-to-site VPN

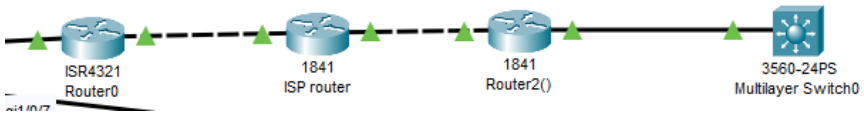
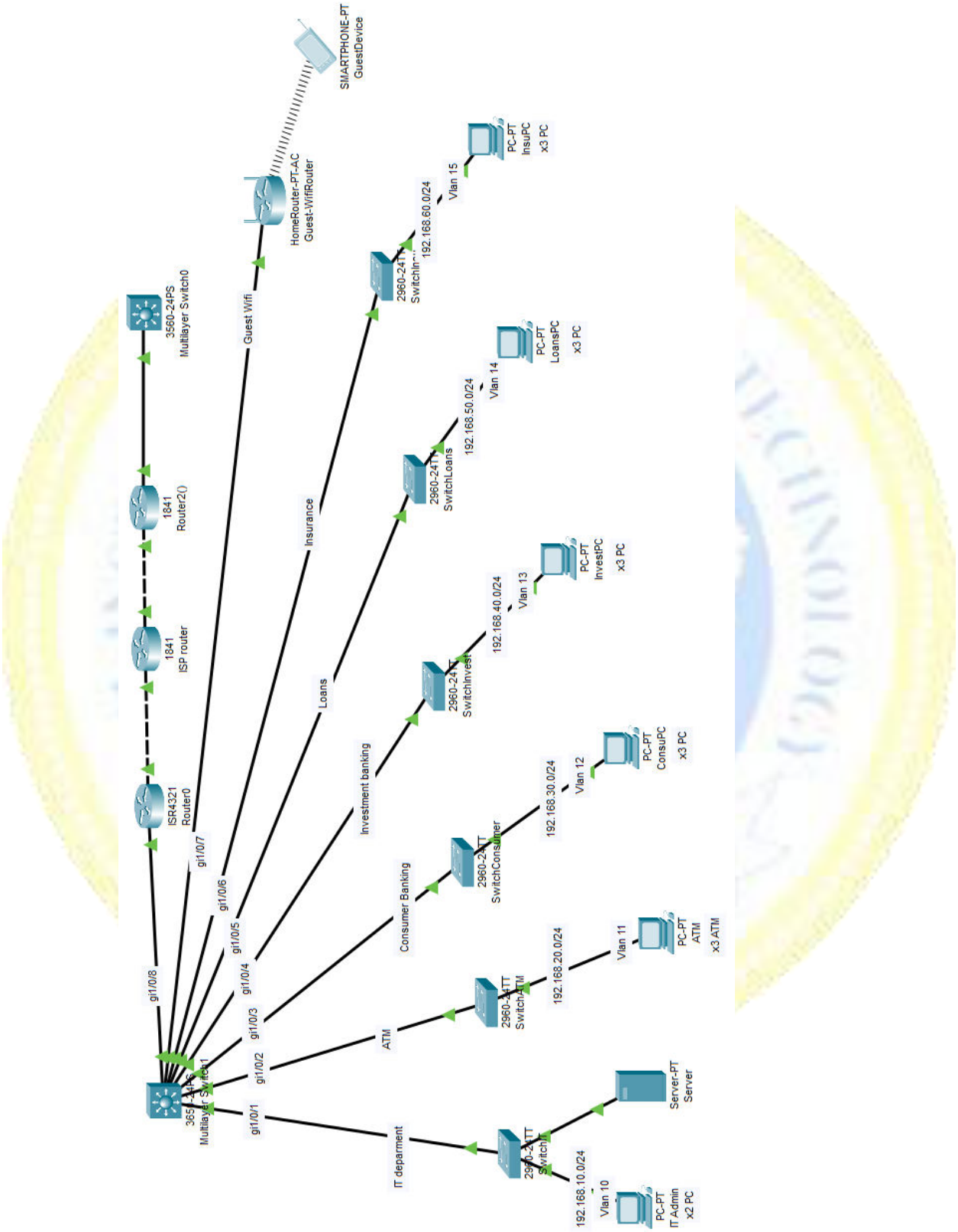



*Figure 9: VPN Design*

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.

## 5.9 Overview of entire network



## 6.0 Items and Labor cost

| Model | Quantity | Price per unit (RM) | Total (RM) |
|---|---|---|---|
| Hardware cost | | | |
| WS-C2960-24TT-L Cisco 2960 Switch | 6 | 963 | 5778 |
| CISCO1841 Cisco 1841 Router | 2 | 2445 | 4890 |
| WS-C3650-24PS-S Catalyst 3650 Switch | 1 | 5121 | 5121 |
| 100m CAT5e Ethernet Cable | 40 | 212 | 8480 |
| TP-LINK EAP115 | 1 | 179 | 179 |
| Cisco ISR4321-AX/K9 ISR 4321 | 1 | 4978 | 4978 |
| Cisco UCS C-Series Rack Servers | 1 | 6573 | 6573 |
| PC | 14 | 5000 | 70000 |
| | | | Total (Rs.) 105999 |
| Labor / intangible cost | | | |
| Unifi 100Mbps (per month | | 125 | 125 |
| Technical support (per month) | 5 | 4000 | 20000 |
| Electrician | 5 | 3000 | 15000 |
| Network design and planning (hours) | 24(hours) | 20000 | 20000 |
| | | | Total (Rs.) 161124 |

*Table 10: Items and Labor Cost*

## 7.0 Network Disaster Recovery Planning

A network disaster recovery plan includes a set of procedures required to effectively respond to a disaster that affects a network and causes its disruption. The main purpose of network disaster recovery is to ensure that services can be delivered to customers despite a disruption in network connectivity.

- **Back up network configuration files**

The main aim is to ensure that a network is restored to its normal state as rapidly as possible. That is why it is important to regularly back up network configuration files, including the initial

parameters and settings for configuring network devices. Regarding this, you are advice to install third-party data protection software, which can be used to back up and recover critical data when your infrastructure is hit by a disaster.

- **Regularly test and update the plan**

By regularly testing and updating network disaster plans, it will reduce the chances of panicking when a network disaster occurs. IT recovery team will be more ready and prepared to deal with network disasters.

- **Assess potential risks and threats**

You also need to determine risks and threats which your organization is most exposed to that can disrupt your network services. After assessing potential dangers, you can come up with preventive measures to stop them from occurring to reduce the possible impact on your infrastructure.

- **Create an IT recovery team and assign responsibilities**

It is not enough to create a network disaster recovery plan; you should also decide who will implement the plan when an actual disaster strikes. So, by having an IT team recovery team will have the organization prepared for disaster recovery. Each recovery team member should be assigned with a specific role and a unique set of responsibilities to avoid any confusion and panic during a disaster recovery event.

- **Document steps of the network disaster recovery process.**

By documenting the steps of the network disaster recovery process will avoid confusion when the actual network disaster occurs. By listing the document also helps identify the weakness of the infrastructure of the organization which indirectly reduce network disaster from occurring.

### 7.1 Objectives of Disaster Recovery Plan

- To limit the extent of disruption and damage.
- To minimize the economic impact of the interruption.
- To establish an alternative means of operation in advance.
- To train personnel with emergency procedures

### 7.2 Risk Assessments

- Identify Possible Threats A high-level risk assessment can still be done by involving the simplest network component where it can still pose a threat if it has an IP address on the network, stores any sensitive data, and/or allows users to access it over the network.

- Rate Each Risk and Impact Each risk is can be classified as low, medium or high risk. This helps to prioritize where you should focus most of your effort initially, and you work down your list to the medium and low-risk resources.

- Analyze Your Protection Firewalls and antivirus software installed on desktops. Analyze any cyber security protection in place, because it reduces risk. This step might affect your priority because you could have a high-priority item that already has the best protection. This type of resource would then be a lower priority.

### 7.3 Emergency Response Procedure

- Evaluate current plans, procedures and incident
- Identify hazards
- Emergency resources
- Review codes and regulations
- Training Programs
- Communication
- Write the plan

### 7.4 Recovery Response Procedure

Prevention

- Focuses on creating concrete plans, training, hazard response plans and exercises well ahead of a disaster to prepare your organization, through proactive planning

Preparedness

- A continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action.

Mitigation

- Effort to reduce loss property by developing structural and non-structural measures that will mitigate the effects of a disaster

## 8.0 References


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