Network implementation for banking

Submitted by

<u>Team :- CODEX :</u>

Anubhav Vats (RA2011033010062)

Hasan Kamran (RA2011033010059)

Nilay (RA2011033010056)

Vaibhav Jha(RA2011033010058)

Amit Kumar Jha (RA2011033010049)

Under the Guidance of

Dr. B.Hariharan

Assistant Professor , Department of Computational Intelligence

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING

with Specialization in Software Engineering

SCHOOL OF COMPUTING

COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR
- 603203

JUNE 2022

SRM INSTITUTION OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR-603203

BONAFIDE CERTIFICATE

Certified that this project report titled **"Network implementation for banking"** is the bonafide workdone by Anubhav Vats (062), Hasan Kamran (059), Nilay(056), Vaibhav Jha(058), Amit Kumar Jha (049) who carried out the Project under my supervision. Certified further,that to the best of my knowledge the work reported herein does not form part of any other work.

SIGNATURE

Dr. B.Hariharan

Computer Comunication – Course

FacultyAssistant Professor ,
Department of Computational Intelligence

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 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

OBJECTIVE OF THE PROJECT

This proposed network is designed for banking system, our client requires 6 main departments for their new outlet which are:

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

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.

Introduction

An ideal Bank Networking system will be fully network base and easy with friendly user interface staff task management system where any banking system manage their networking system somehow Head office , Branch Office, and other office are maintain LAN, MAN, WAN, VLAN, VLSM,VPN and some branch are maintain by manageable switch. LAN is used by Local Area Networking system for example one office and a one building. And MAN are using by the Metro Politian area Network for Example small town, and WAN are use by the WIDE AREA NETWORK. In this networking system are used by all banking users can use by shared their data very easily. So that every user use to take about Network Structure & Security of Banking System instantly this way anywhere.

1. To design and simulate a banking network system which is secure.

2. To simulate a banking network system that will easily manage any banking task.
3. To manage the banking network by a central system

1.3 Justification of study The trend of growth of Online Banking brings many security issues and increasing cost of implementing higher security system for both Online Banking users and the banks. Classers said security is all about risks and associated cost in his paper .The most critical issue of Online Banking security is to protect valuable information that is susceptible to unauthorized access by attackers. Hence, the banks must constantly increase security. At the same time, the banks must manage costs to make a profit. In contrast, increasing security is increasing the cost for attackers to break into the system, and increasing the punishment that the attackers may suffer. Hence the Internet criminals/attackers/crackers may lose motivation for hacking a high security online banking system.

1.4 Scopes of study The scope of the Network Structure & Security of Banking System includes.

1. Online based day to day transmission.

2. Save time and cost because of day to day transmission.

3. Established relation between one branch to another

4. Connect all branches to head branch in same network.

5. Online based update and maintain everyday work.

Modules Of the Project

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	Wireless 0	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

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 organisation (AHB 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.

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 for this banking system. 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.

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%.

Module Description

Network Diagram and Topologies

Site 1 – IT Department

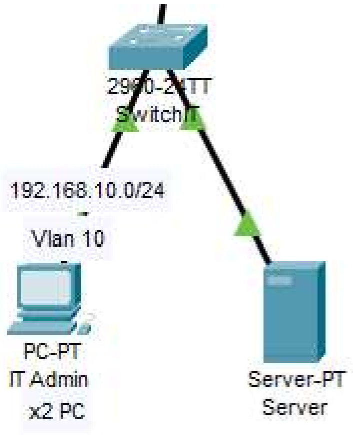


Figure 1: Site 1 - IT Dept. Design

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.

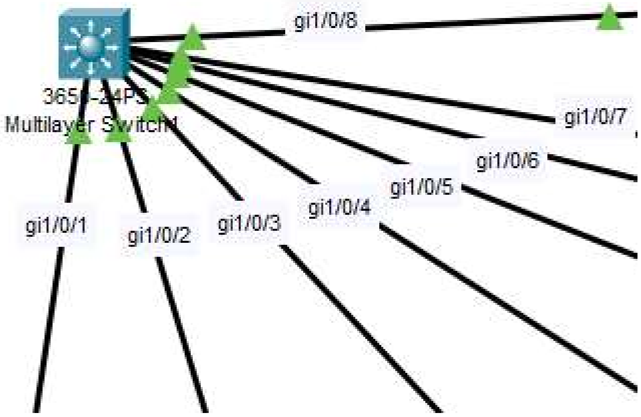


Figure 2: Main Multilayer Switch (Layer 3 Switch)

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

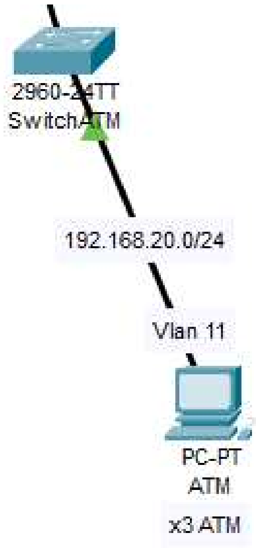


Figure 3: Site 2 -ATM. Design

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

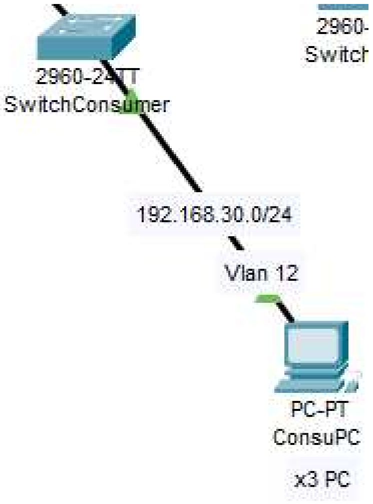


Figure 4: Site 3 - Consumer Banking. Design

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

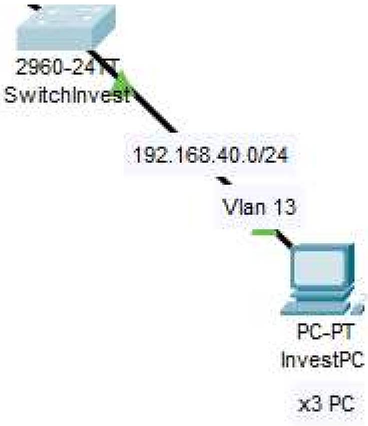


Figure 5: Site 4 - Investment Banking Design

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

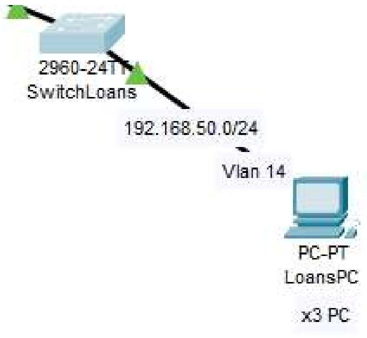


Figure 6: Site 5 - Loans Design

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

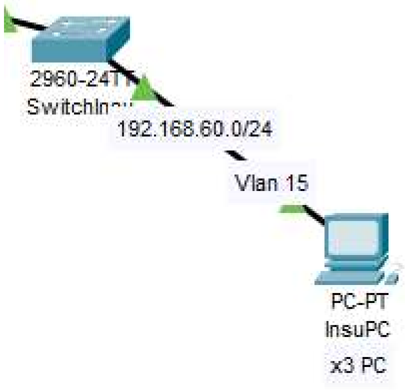


Figure 7: Site 6 - Insurance Design

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

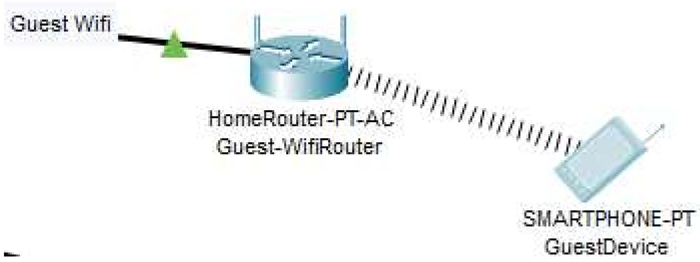


Figure 8: Guest Wifi Design

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

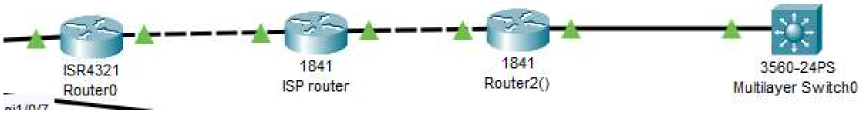
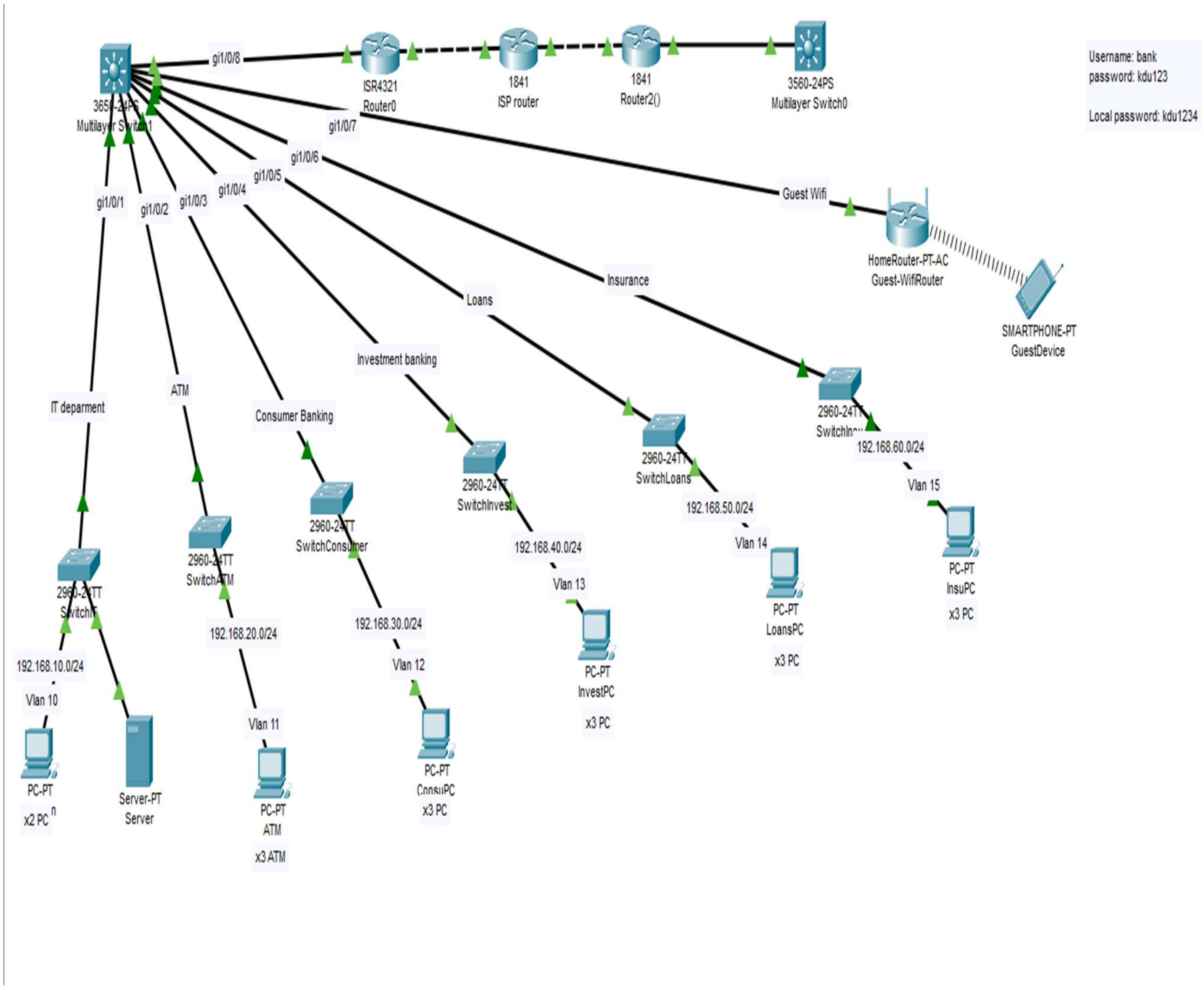


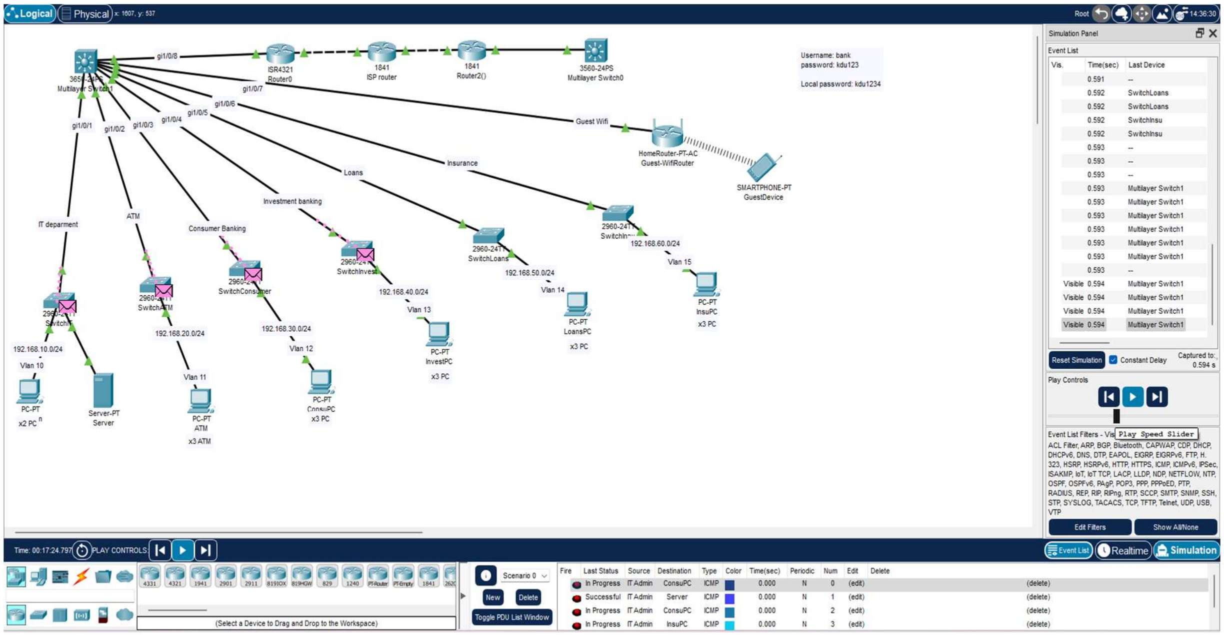
Figure 9: VPN Design

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.



Username: bank
password: kdu123

Local password: kdu1234

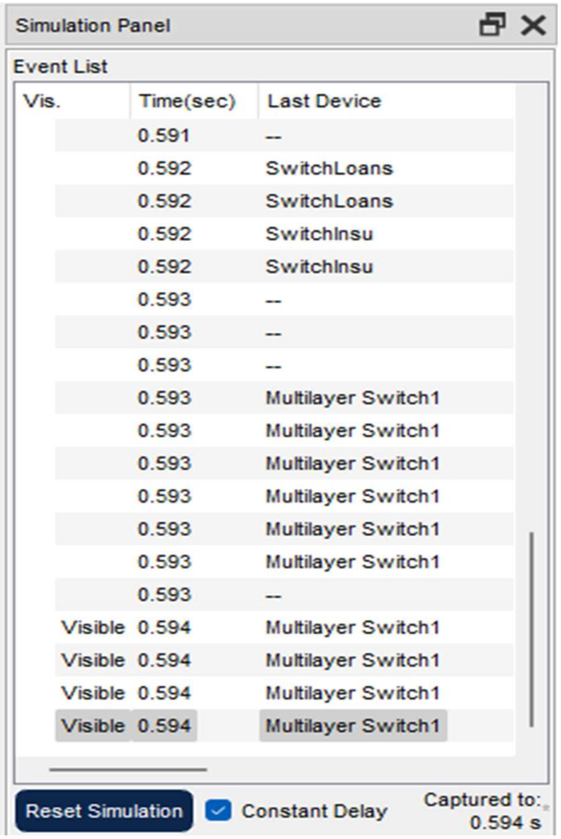


Username: bank
password: kdu123

Local password: kdu1234

Event List Filters - Visible Events: ACL Filter, ARP, BGP, Bluetooth, CAPWAP, CDP, DHCP, DHCPv6, DNS, DTP, EAPOL, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, IoT, IoT TCP, LACP, LLDP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, PPP, PPPoED, PTP, RADIUS, REP, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, USB, VTP

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
●	In Progress	IT Admin	ConsuPC	ICMP	■	0.000	N	0	(edit)	(delete)
●	Successful	IT Admin	Server	ICMP	■	0.000	N	1	(edit)	(delete)
●	In Progress	IT Admin	ConsuPC	ICMP	■	0.000	N	2	(edit)	(delete)
●	In Progress	IT Admin	InsuPC	ICMP	■	0.000	N	3	(edit)	(delete)



Event List

Vis.	Time(sec)	Last Device
	0.591	--
	0.592	SwitchLoans
	0.592	SwitchLoans
	0.592	SwitchInsu
	0.592	SwitchInsu
	0.593	--
	0.593	--
	0.593	--
	0.593	Multilayer Switch1
	0.593	Multilayer Switch1
	0.593	Multilayer Switch1
	0.593	Multilayer Switch1
	0.593	Multilayer Switch1
	0.593	Multilayer Switch1
	0.593	--
Visible	0.594	Multilayer Switch1
Visible	0.594	Multilayer Switch1
Visible	0.594	Multilayer Switch1
Visible	0.594	Multilayer Switch1

Reset Simulation ☑ Constant Delay Captured to: 0.594 s

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 (RM) 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 (RM) 161124

Inferences

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.

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

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.

Emergency Response Procedure

- Evaluate current plans, procedures and incident
- Identify hazards
- Emergency resources

- Review codes and regulations
- Training Programs
- Communication
- Write the plan

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

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 more easy 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.

Future work

1. Add time based transmission.
2. Security system will be upgraded .
3. Make the project more user friendly. ⎤
4. Real life implementation.

Limitations

1. The main Limitation is to implement the project in real world . Because we only simulate it via packet tracer.
2. Due to less time and work pressure we could not add more features which could make the project more useful.

References

Resources:-

- Data and Computer communication by William Stallings
- Computer Communication and Network technologies by Bill Hancock

Websites:-

- www.geeksforgeeks.org
- www.ibm.com
- www.javatpoint.com