Back Khoa University

Computer Network Assignment 2

Mini Project: Design for building of the Bank

Group Member:
Alexandre Rousseau

Summary

1. Introduction 2
2. Devices and Equipment Used 2
3. Network Needs Analysis 4
   a) Number of Users & Priority Levels 4
   b) Security Requirements 5
   c) Transmission Speed Requirements 5
   d) Load Variations Estimates 5
   e) Reliability Requirements 5
4. Network Diagram and Topologies 6
   a) Site 1 – IT Department 6
   b) Site 2 – ATM 7
   c) Site 3 – Consumer Banking 8
   d) Site 4 – investment Banking 8
   e) Site 5 – Loans 9
   f) Site 6 – Insurance 9
   g) Site 7 – Guest Wifi 10
   h) Site 8 – Site-to-site VPN 10
   i) Overview of Entire Network 11
5. Items and Labor Cost 12
6. Network Disaster Recovery Planning 13
   a) Objectives of Disaster Recovery Plan 14
   b) Risk Assessments 14
   c) Emergency Response Procedure 14
   d) Recovery Response Recovery 15

1. Introduction

CCC (Computer & Construction Concept) was asked to design a computer network used in the headquarters and two branches of a BBB (BB Bank) under construction. BB Bank's Computer Network is estimated for a growth rate of 20% in 5 years (in terms of the number of users, network load, branch extensions).

2. Devices and 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
Switch IT	2960-24TT	N/A	N/A	N/A	N/A

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
Switch ATM	2960-24TT	N/A	N/A	N/A	N/A

Consumer Banking:

Device	Model	Port	IP Address	Subnet Mask	Default Gateway
ConsumPC	PC-PT	Fe0	192.168.30.101	255.255.255.0	192.168.30.1
ConsumPC2	PC-PT	Fe0	192.168.30.201	255.255.255.0	192.168.30.1
ConsumPC3	PC-PT	Fe0	192.168.30.301	255.255.255.0	192.168.30.1
Switch Consumer	2960-24TT	N/A	N/A	N/A	N/A

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
Switch Invest	2960-24TT	N/A	N/A	N/A	N/A

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
Switch Loans	2960-24TT	N/A	N/A	N/A	N/A

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
Switch Insu	2960-24TT	N/A	N/A	N/A	N/A

Guest Wi-Fi:

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

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	

3. Network Needs Analysis

a) 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 the 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.

b) 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 can 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 a server and have their own usernames and passwords.

c) Transmission Speed Requirements

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

d) 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.

e) 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%.

4. Network Diagram and Topologies

a) Site 1 – IT Department

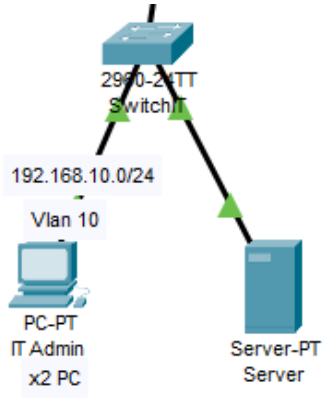


Figure 1: Site 1 - IT Dept. Design

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 to create VLAN traffic between the switches. A trunk connection is a normal link that can 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.

b) Site 2 – ATM

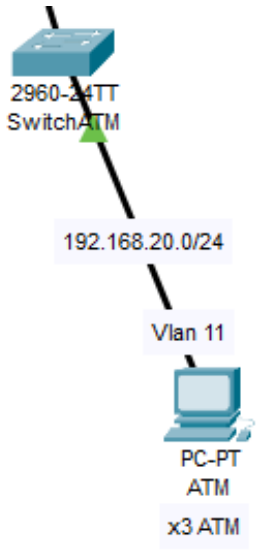


Figure 3: Site 2 -ATM. Design

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

c) Site 3 – Consumer Banking

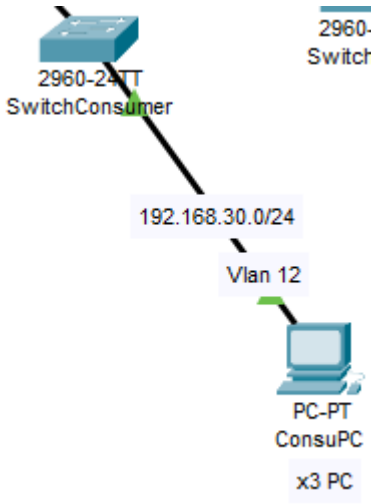


Figure 4: Site 3 - Consumer Banking. Design

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

d) Site 4 – investment Banking

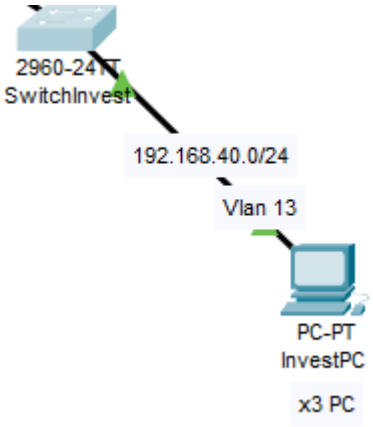


Figure 5: Site 4 - Investment Banking Design

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

e) Site 5 – Loans

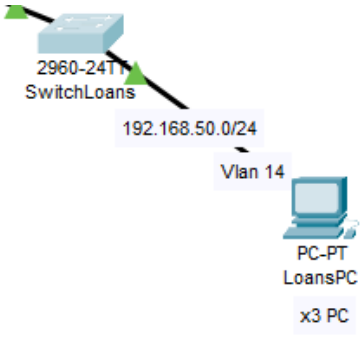


Figure 6: Site 5 - Loans Design

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

f) Site 6 – Insurance

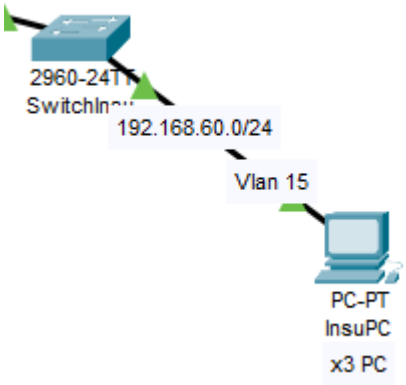


Figure 7: Site 6 - Insurance Design

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

g) Site 7 – Guest Wifi

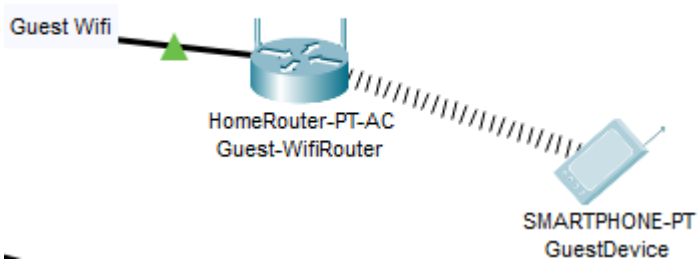


Figure 8: Guest Wifi Design

As for Site 4, This is Guest Wifi Design which only consists of 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.

h) Site 8 – Site-to-site VPN

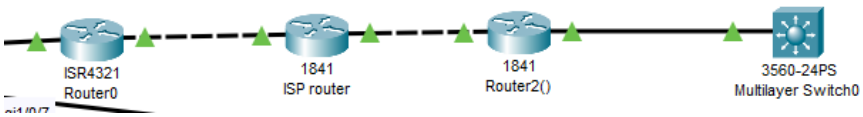
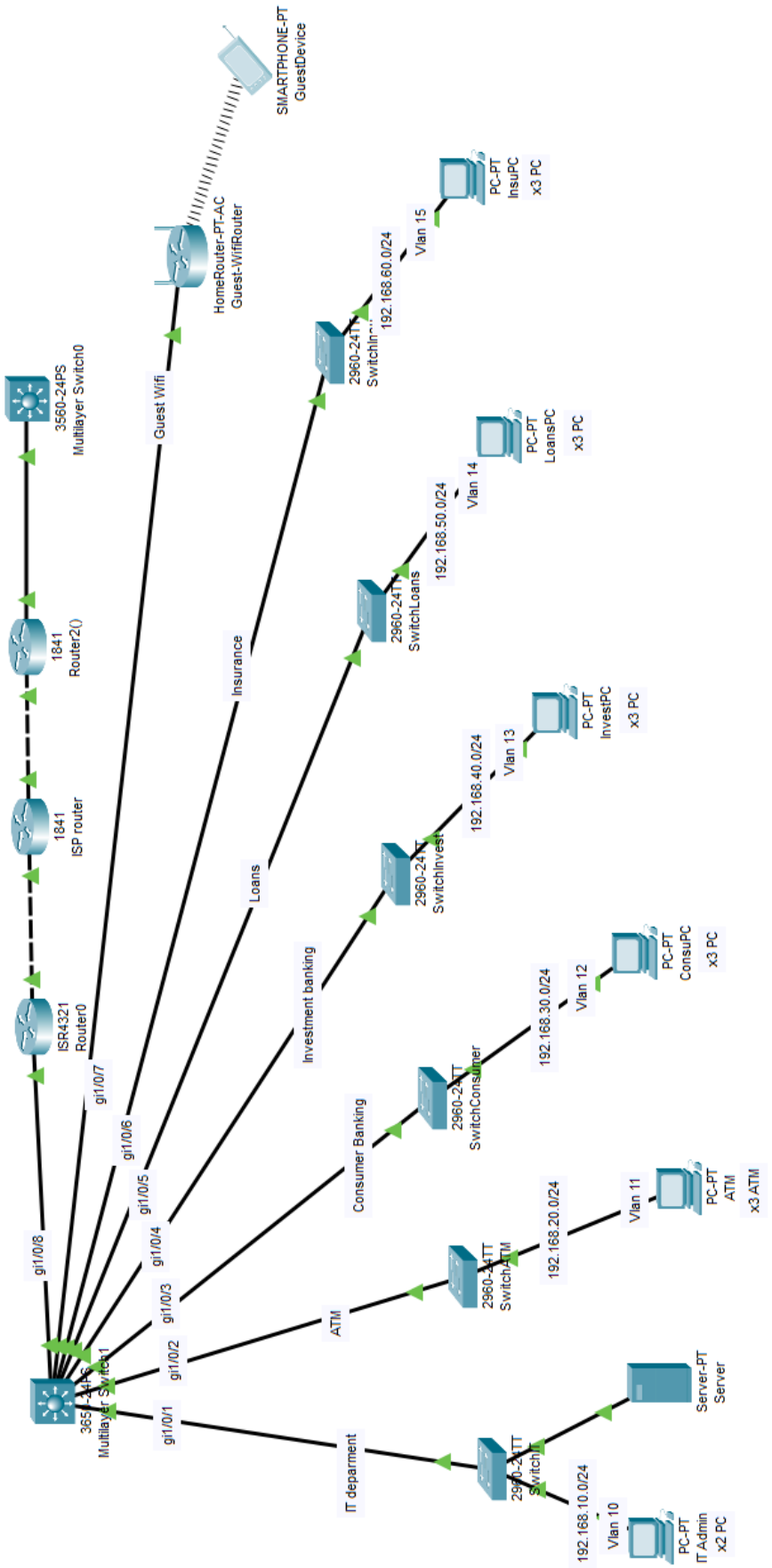


Figure 9: VPN Design

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 few advanced encryption algorithms to provide confidentiality of the data transmitted between the two sites.

i) Overview of Entire Network



5. Items and Labor Cost

Hardware Cost:

Model	Quantity	Price per unit (USD)	Total (USD)
WS-C2960-24TT-L Cisco 2960 Switch	6	232	1392
CISCO1841 Cisco 1841 Router	2	590	1180
WS-C3650-24PS-S Catalyst 3650 Switch	1	1236	1236
100m CAT5e Ethernet Cable	40	51	2040
TP-LINK EAP115	1	43	43
Cisco ISR4321-AX/K9 ISR 4321	1	1200	1200
Cisco UCS C-Series Rack Servers	1	1586	1586
PC	14	1207	48280
Total (USD) = 55371			

Labor / Intangible Cost:

Model	Quantity	Price per unit (USD)	Total (USD)
Unifi 100Mbps (per month		30	30
Technical support (per month)	5	965	4825
Electrician	5	724	3620
Network design and planning (hours)	24 (Hours)	4830	4830
Total (USD) = 13325			

6. 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.

a) 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

b) 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 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.

c) Emergency Response Procedure

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

d) Recovery Response Recovery

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