American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-4, Issue-11, pp-79-91
www.ajer.org
Research Paper Open Access

Design and Simulation of a Banking Network System

Abdul Hannan1[1], M.A.Jobayer Bin Bakkre[2], Rajib Chandra Ray[3], Md.Selim Hossain[4].

[1,2,3]*Dept. of Computer Science & Engineering, Jahangirnagar University, Dhaka, Bangladesh.*
[4]*Dept. of Computer Science & Engineering,Shahjalal University of Science and Technology,Sylet,Bangladesh.*

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.*

KEYWORD- *Relevant literature, Methodology, Analysis design &development, Limitation & Future work.*

I. 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.

1.1 Objectives

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.

II. LITERATURE REVIEW

2.1 Review of relevant literature

Networks can also be characterized in terms of spatial distance as local area networks (LANs), metropolitan area networks (MANs), and wide networks (WANs). A given network can also be characterized by the type of data transmission technology in use on it (for example, a TCP/IP or Systems Networks Architecture network); by whether it carries voice, data, or both kinds of signals; by who can use the network (public or private); by the usual nature of its connections (dial-up or swathed, dedicated or no switched, or virtual connections); and by the types of physical links (for example, optical fiber, coaxial cable, and Unshielded twisted Pair).

The flowing methods to be traditional (old) way of recurrent

- Data transfer / transition send branch office to head office by manually.
- Need extra cost for transmission because of manually transmission.
- Time based transmission.
- Low security system .Data carries or transfers by human.
- User unfriendly because of slow process.
- Very complex to maintain.

2.2 Computer Networking

A computer network is a system for combination among two or more computers. These networks are fixed (cabled, permanent) or temporary (as via modems). A computer network of computer networks that use the TCP/IP network protocols to facilitate data transmission and exchange intranet a restricted computer network; a private network created using World Wide Web software.

2.3 IP address

An IP address consists of 32 bits of information. The 32 bit IP address is a structured or hierarchical address. 32 bits are divided 4 sections. And every section is 8 bit address the 32 bits addresses are divided two parts one is Host section, and another is m section. 32 bits addresses have also 5 classes, which is,

	bits	8bits	8bits	8bits
Class A:	Network	Host	Host	Host
Class B:	Network	Network	Host	Host
Class C:	Network	Network	Network	Host
Class D:	Multicast			
Class E:	Research			

Network address of Class A: 1 to 126

Network address of Class B: 128 to 191

Network address of Class C: 192 to 223

Network address of Class D and E: The address between 224 and 255 are reserved for class D and E networks. Class D is used for multicast address, Class E is used for scientific purpose.

2.4 VLSM

Network administrators must anticipate and manage the physical growth of networks. This may require them to buy or lease another floor of a building for new network equipment such as racks, patch panels, switches, and routers, Network designers must choose address schemes that allow for growth. Variable-length subnet mask (VLSM) is used to create efficient and scalable address schemes. IPv4 offered an address strategy that was scalable for a time before it resulted in an inefficient allocation of addresses. IPv4 may soon be replaced with IP version 6 (IPv6) as the dominant protocol of the internet. IPv6 has virtually unlimited address space and implementation has begun in some networks. Over the past two decades, engineers have successfully modified IPv4 so that it can survive the exponential growth of the Internet. VLSM is one of the modifications that has helped to bridge the gap between IPv4 and IPv6.

2.4.1 Why is it used?

As IP subnets have grown, administrators have for ways to use their address space more efficiently. This page introduces a technique called VLSM. With VLSM, a network administration can use a long mask on networks with few hosts, and a short mask on subnets with many hosts.

VLSM is used for following reasons

- The ultimate solution is IPv6 with 128-bit address space.
- It allows for 340, 283, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456 address.

2.4.2 Importance of VLSM

Efficient use of organizations assigned IP address space. Route aggregation VLSM. Efficient use of the organization's assigned IP address space Assume that a network administrator has decided to configure the 130.5.0.0/16 network with a /22 extended-network prefix. This design allows for 64 subnets with 1,022 hosts each. Fine if the organization plans to deploy a number of large subnets. What about the occasional small subnet containing only 20 or 30 hosts? About 1,000 IP host addresses wasted for every small occasional subnet.

2.5 Networking devices

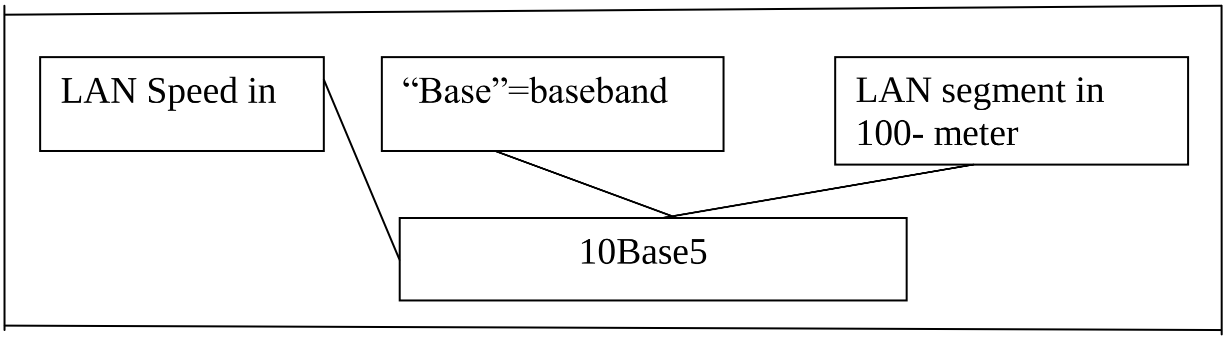
A computer network is comprised of different devices to share, transmit, and boost the signal, voice and data. Network devices or components are the physical parts connected to a network. The basic network devices, Individual computers, Hub, Switch, Bridges, Routers. The following is the Devices.
Switch, Router

2.6 ETHERENET

Ethernet was originally developed by digital, Intel and Xerox (DIX) in the early 1970's and has been designed as a 'broadcast' system, i.e. stations on the network can send messages whenever and wherever it wants. All stations may receive the messages, however only the specific station to which the message is directed will respond. The original format for Ethernet was developed in Xerox Palo Alto Research Center (PARC) California in 1972 Using Carrier Sense Multiple Access with Collusion Detection (CSMA/CD) it had a transmission rate of 2.94MBps and could support 256 devices over cable stretching for 1km. the two inventors were Robert Metcalf and David Boggs. The 'Ether' part of Ethernet denotes that the system is not meant to be restricted for use on only one medium type, copper cables, fiber cables and even radio waves van be used .

2.6.1 PHYSICAL CONNECTIONS

IEEE 802.3 specifies several different physical layers, where Ethernet is defines only one. Each IEEE 802.3 physical layer protocol has a named that summarizes its characteristics.



2.6.2 ETHERNET FRAME FORMATS

Field length,
In bytes

Ethernet

7	1	6	6	2	46-1500	4
Preamble	S O	Destination address	Source address	Type	Data	FCS

Field length:-
In bytes:

7	1	6	6	2	46-1500	4
Preamble	S O F	Destination address	Source address	Type	Data	FCS

SOF = Start of frame delimiter

Figure: Ethernet and IEEE 802.3 Frame Formats

FCS = Frame check sequence
SOF = Start of frame delimiter
FCS = Frame check sequence

Both Ethernet and IEEE 802.3 Frames begin with alternating pattern of ones and zeros called a preamble. The preamble tells receiving stations that a frame is coming. The byte before the destination address in both an Ethernet and an IEEE 802.3 frame is a state of frame delimiter. This byte ends with two consecutive one bits, which serve to synchronize the frame reception portions of all stations on the LAN. Immediately following the preamble in both Ethernet and IEEE 802.3 LANs are the destination and source address fields. Both Ethernet and IEEE 802.3 addresses are 6 bytes long.

III. METHODOLOGY

3.1 METHODOLOGY

In this project "Design and Simulation of a Banking System" discuss the total banking network structure & some security feathers. We are survey in the different bank and collect some data or information. The OSI layer was introduced by the International Organization for Standardization (ISO) in 1984 in order to provide a reference model to make sure products of different vendors would interoperate in networks. OSI is short for Open Systems Interconnection. Data transmitted between software programs passes all 7 layers. The Application, Presentation and Session layers are also known as the Upper Layers. The Data Link and Physical layers are often implement4ed together to define LAN and WAN specifications.

3.2 When to use the OSI model

One of the first things we learn when we started working in the field of computer networking is the OSI model. The OSI model is used to describe how data should pass across a network. It is broken up into 7 layers, starting with layer 1 as the lowest layer and moving up to layer 7. The 7 layers are labeled, starting with layer 1 at the bottom, 1-Physical, 2-Data Link, 3-Network, 4-Transport, 5-Session, 6-Presentation, and 7-Application.There are many things that live at each layer. Layer 1, the Physical Layer, has to do with all things that are used to provide physical connectivity. Some of them are Ethernet cables, Fiber cables, and wall jacks. The most common networking device at Layer 1 is a hub. It provides device connectivity and that is about it. Hubs have no brain, and cannot be managed at all. With hubs, the broadcast domain (which is the segment of the network where all nodes can reach each other by broadcast) and the collision domain (which is the segment of a network where data packets can collide with one another) are the same, and include every port on every hub connected together on a physical segment

3.2.1 BENEFITS OF OSI MODEL

The separating sales communications and multi-level marketing into smaller logical sections, the OSI model simplifies how networking protocols are created. The OSI model was designed to ensure different types of equipment (like adapters, routers, hubs and network adaptors) are compatible.

1. Provide a wide variety of choice. Customers have a wide variety of choice since software/ hardware from different manufactures work together in harmony. In addition, the OSI model can fit to any compatible software/hardware from different users in other parts of the world.

2. It does not rely on a specific operating system. OSI is convenient since errors are dealt with at each level, as different levels operate automatically independent of each other. This makes it easier to troubleshoot problems that may arise at each stage, by separating the networks into small manageable pieces.

3. The user can understand the common terms used in networking. OSI model also help the user to understand different networking terms and functional relationship applied on multiple networks. In addition, the user also understand how new technologies are developed in the existing networks.

4. Interprets product functionality at each stage. The OSI model simply uses different stages of functionality. For instance, each stage has specific functions to ensure all networks operate without technical hitches. Also, each layer has its own interface specifications and a well-defined connector.

5. Encrypt data for security purposes. Decryption and encryption services are also available for security purposes. Expansion and compression of messages is simplified to ensure it travels from one system to another efficiently.

6. It is easier to add multiple network models. The OSI model is designed in such a way that user further extend new protocols within the process. This means you can use additional layered architecture other than the existing one. Due to its complexity, poor performance can be obtained in day to day applications, thereby it requires great technical know-how.

3.3 TCP/IP Network Model

Although the OSI model is widely used and often cited as the standard, TCP/IP protocol has been used by most UNIX workstation vendors. TCP/IP is designed around a simple four-layer scheme. It does omit some features found under the OSI model. Also it combines the features of some adjacent OSI layers and splits other layers apart. The four network layers defined by TCP/IP model are as follows**.**

IV. ANALYSIS DESIGN AND DEVELOPMENT

4.1 Requirement Gathering Technique

Functional Requirements

Banking system in Bangladesh all banks has an IT department. IT department solution all type of IT problem and serve the core network. IT creates a core network diagram. This diagram involves all type of useable network mechanism (Switch, Router, Firewall, Server) etc. Simulation is the most important of any system.
An accurate system design, accurate performance and accurate Simulation give best performance of a system.

4.1.1 Analysis of Requirement

The description of the services and constraints are the requirements for the system and the process of finding out, analyzing, documenting and checking these services and constraints is called requirements engineering. The hardware and software requirement which we need in our project is given below.

4.2 Hardware Requirement

IBM compatible , Intel Pentium 4,Intel core-i3 based PC with a monitor ,keyboard and mouse, system must have 1 GB Ram, Hard disk 80 GB or of available memo.

4.3 Software Requirement

This following software we have used to implement our project-

- Windows XP or.
- Windows 7 or.
- Windows 8 platform.
- Packet Tracer 5.3.3
- Switch.
- Router.
- Firewall.
- Server.

4.3.1 Packet Tracer 5.3

LAN, MAN, VLAN, ACL, VPN, & Banking Network Combine diagram, Protocol, and different branch transmission simulation.

4.4 Data Flow diagram

Data Flow diagram is a way of expressing system requirements in graphical from. It defines the flow of data, the process and the area where they are store.

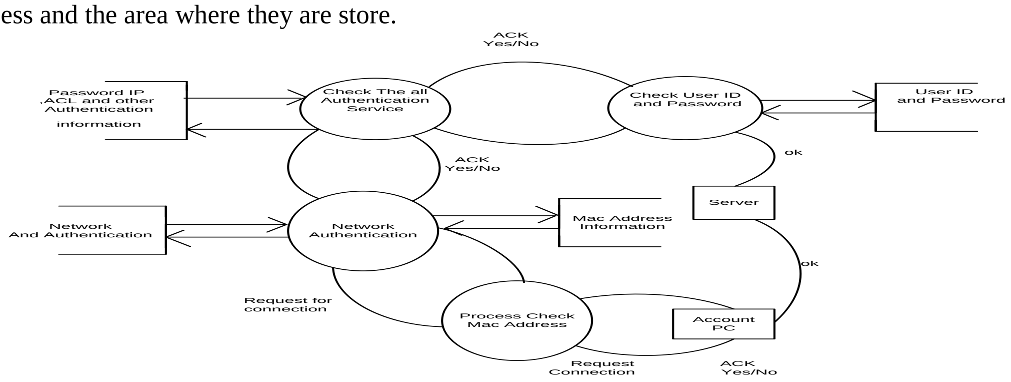

ACK
Yes/No
Password IP ,ACL and other Authentication information
Check The all Authentication Service
Check User ID and Password
User ID and Password
ACK
Yes/No
ok
Network And Authentication
Network Authentication
Mac Address Information
Server
ok
Request for connection
Process Check Mac Address
Account PC
Request Connection
ACK
Yes/No

Fig: Data Flow diagram

4.4.1 Symbol of DFD

- A square define the data source.
- Arrow defines the data flow.
- A circle represents a process that transforms incoming into outgoing data flow.
- An open rectangle is a data store – data at rest or a temporary repository of data.

4.5 ROUTER

A router is a special type of computer. It has the same basic components as a standard desktop PC. It has a CPU, memory, a system bus, and various input/output interfaces. However, routers are designed to perform some very specific functions that are not typically performed by desktop computers. For example, routers connect and allow communication between two networks and determine the best path for data to travel through the connected networks. Just as computers need operating systems to run software applications, routers need the Internet work Operating System (IOS) software to run configuration files? These configuration files contain the instructions and parameters that control the flow of traffic in and out of the routers. Routers use routing protocols to determine the best path for packets. The configuration file specifies all the information for the correct setup and use of the selected or enabled, routing and routed protocols on a router.

4.5.1 ROUTER CONFIGURATION

Here discussed about the routing configuration

Setting Hostname

A router should be given a unique name as one of the first configuration tasks. This task is accomplished in global configuration mode with the following command.

Now router configuration start

```
Router (config) #hostname JU
WUB (config) #
```

Now setting Router Password:

Console password:

```
Router(config)#line console 0
Router(config-line)#login
Router(config-line)#password<password>
```

Virtual Privileged EXEC Mode:

```
Router(config)#line console 0 4
Router(config-line)#login
Router(config-line)#password<password>
```

Secure Privileged EXEC Mode

The enable password and enable secret commands are used to restrict access to the privileged EXEC mode. The enable password is only used if the enable secret has no t been set. The enable secret command should be used because the enable secret command is encrypted. The enable passwords command is not encrypted.

```
Router (config) #enable password <password> Router(config)#enable secret <password>
```

Password

Encryption

The service password-encryption command applies a weak encryption to all unencrypted passwords. The enable secret <password> command uses a strong MD5 algorithm for encryption.

```
Router (config) #service password-encryption
```

Backup Configuration File :

A current copy of the configuration can be stored on a TFTP server. The copy running-configuration TFTP command can be used to store the current configuration on a network**.** TFTP server.

```
 Router# copy running-config tftp
```

Interface Configuration:

Serial Interface

Each connected serial interface must have an IP address and subnet mask to router IP packet. Configuration the IP address with the following commands:

```
Router:r(config)#interface serial 0/0/0
Router(config)#ip address<ip address> <subnetmask>
```

Setting Clock Rate & No Shutdown:

By default, Cisco routers are DTE devices but they can be configured as DCE devices.

By default, interfaces are turned off, or disabled. To turn on or enable an interface, the command no shutdown

is entered. If an interface needs to be administratively disabled
For maintenance or troubleshooting, the shutdown
Command used to turn off the interface.

```
Router (config) #interface serial 0/0/0
Router(config-if)#clock rate 400000
Router(config-if)#do wr
Router(config-if)#exit
```

4.6 ROUTING PROTOCOL

A routing protocol is used by routers to dynamically find all the networks in the internet work and to ensure that all routers have the routing table. Basically, a routing protocol determines the path of a packet through an internet work. Examples of routing protocols are Static, RIP, EIGRP, and OSPF.

4.7Administrative Distances

Administrative distance is the feature used by routers to select the best path when there are two or more different routers to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol.

Router source	Default Distance
Connected interface	0
Static router	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EGP	140
EIGRP external route	170
Internal BGP	200
Unknown	255

Table: default administrative distances.

4.8 CLASSIFICATION OF DYNAMIC ROUTING PROTOCOL.

Dynamic routing protocols do not change how routing is done. They just allow for dynamic altering of routing tables. There are two classifications of protocols:

4.8.1 Interior Gateway Protocols (IGPs) exchanges routing information within a single autonomous system. Common examples include.

4.8.2 Exterior Gateway Protocols (EGPs) route between separate autonomous systems. EGPs include.

- EGP (The original exterior gateway protocol used to connect to the former internet backbone network ~ now obsolete).
- BDP (Border Gateway Protocol: current version, BGPv4m, was adopted around 1995).

4.8.3 RIP Routing Updates

RIP sends routing-update messages at regular intervals and when the network lopi changes. When a router receives a routing update that includes changes to an entry, it updates its routing table to reflect the new router. The metric value for the path is increased by I, and the sender is indicated as the next hop. After updating its routing table, the router immediately beings transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates the RIP routers send.

4.8.4 RIP Configuration

The command syntax is as follows:

```
Router (config) #router rip
Router (config-router) #network network-number net-mask
```

4.9 IGRP Configuration

To configure the IGRP routing process use the router igrp configuration command. The command syntax is as follows. Router A (config) #router igrp as-number
Router A (config) #network network-number net-mask
There as number identifies the IGRP process.
To specify a list of networks for IGRP routing process, se the network router configuration command. To remove an entry, use the no form of the command.

4.9.1 EIGRP Features and Operation

EIGRP is sometimes referred to as a hybrid routing protocol because it has characteristics of both distance-vector and link-state protocols. For example, EIGRP doesn't send link-state packets as OSPF does; instead, it sends traditional distance-vector updates containing information about networks plus the cost of reaching them from the perspective of the advertising router. This makes EIGRP suitable for very large networks. EIGRP has a maximum hop count of 255.There are a number of powerful features that make EIGRP a real standout from IGRP and other protocols. The main ones are listed here.

- Support for IP , IPX, and Apple Talk via protocol-dependent modules
- Considered classless (same as RIPv2 and OSPF)
- Support for VLMS/CIDR
- Support for summaries and discontinuous networks networks
- Efficient neighbor discovery
- Communication via Reliable Transport Protocol (RTP)
- Best path selection via Diffusing Update Algorithm (DUAL)

4.9.2 EIGRP Configuration

EIGRP is an ideal choice for large, multi-protocol networks built primary on Cisco routers.
RouterA(Config)#router eigrp as-number
RouterA(Config)#network network-number net-mask.

4.10 OSPF Features and Operation

OSPF configuration requires that he OSPF routing process be enabled on the router with network addresses and area information specified. Network addresses are configured with a wildcard mask and not a subnet mask. The wildcard mask represents the links or host addresses that can be present in this segment. Area IDs can be written as a whole number or doted decimal notation.

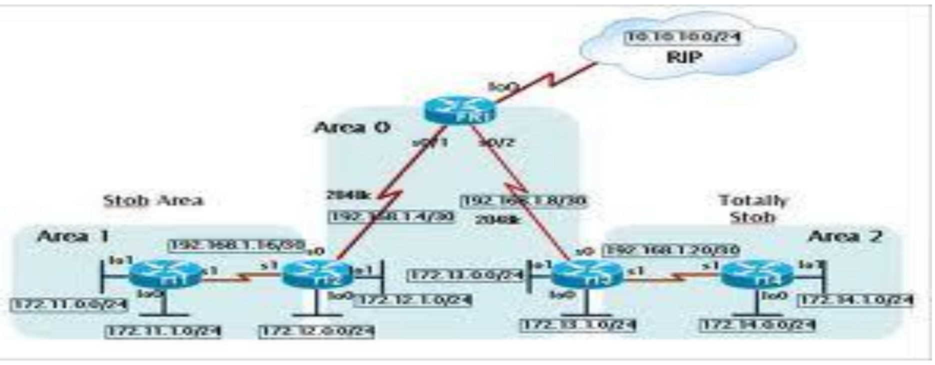


Figure: An OSPF as Consists of Multiple Areas Linked by Routers.

OSPF provides the following features [8];

- Consists of areas and autonomous systems
- Minimizes routing update traffic
- Allows scalability

Supports VLSM/CIDR

- Has unlimited hop count
- Allows multi-vendor deployment (open standard)

Is supposed to be designed in a hierarchical fashion, which basically means that you can separate the larger internetwork into smaller internetworks called areas.This is the best design for OSPF.

4.10.1 OSPF Configuration

To enable OSPF routing, use the global configuration command syntax:
Router (configure) #router ospf process-id
Router (configure-router) #network address wildcard-mask area area-id.

Now discuss and simulate the RIP Protocol.

Routing Information Protocol (RIP) is a true Distance-Vector routing protocol. It sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15, meaning that 16 is deemed unreachable.

Network structure: Banking system in Bangladesh all banks has an IT department. IT department solution all type of IT problem and serve the core network. IT creates a core network diagram. This diagram involves all type of useable network mechanism (Switch, Router, Firewall, Server) etc. Simulation is the most important of any system. An accurate system design, accurate performance and accurate Simulation give best performance of a system.

4.11 Usable Protocol:

In banking network system data transfer for router configuration using two types of routing protocol.

- RIP (Version 2)
- OSPF

OSPF protocol uses the following bank

- HSBC
- Standard Chartered

RIP (Version 2)

- NCC bank
- BRAC bank

4.12 Project Structure:

Now we discuss and simulate the OSPF protocol.

Open Shortest Path First (OSPF) is a routing protocol developed for Internet Protocol (IP) networks by the interior gateway protocol (IGP) working group of the Internet Engineering Task Force.

4.13 Now discuss and simulate the RIP Protocol.

Routing Information Protocol (RIP) is a true Distance-Vector routing protocol. It sends the complete routing table out to all active interfaces every 30 seconds. RIP only uses hop count to determine the best way to a remote network, but it has a maximum allowable hop count of 15, meaning that 16 is deemed unreachable.

4.14 What is ATM?

ATM is Automated Teller Machine. Now it's making peoples life very easy as they get their money when they need. So, they do not need to carry either big amount of money or the checque book all the time. To get rid from this burden they need to deposit money in the bank by opening an account and then the bank will be given a Card i.e. an ATM card with a PIN number to them. By using that they can withdraw money from any ATM machine of that bank. When they insert the card in the machine and the PIN number the machine will show few instructions on the screen. By that time verification (PIN Number and Account Number) will be done with the main bank computer as they are connected. If the verification is correct then the user will choose an instruction and the ATM will dispense money to the card holder.

4.15 Internal Structure of ATM

In the following pictures we have the internal structure of two different type of ATM machine.
And also it can be divided into two different parts:- Upper Unit, -Lower Unit

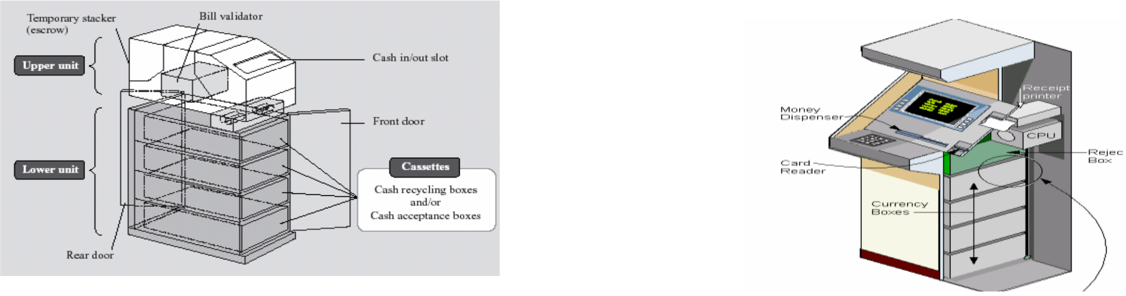


Fig: Shows the Complete Internal Structure.

4.16 Interactive components of ATM

Card Reader: Customer inserts their card in it when there is written “Please Insert Your card” on the screen.
Keypad: Use for PIN code input, choices, amount of money etc as the input to
The ATM machine.
Display Screen: This screen shows all the instructions or options for the customers ‘convenience.
Screen Buttons: When options are given on the screen one user can choose any of the options accordingly by the use of button on left or right side of the screen. These buttons select the option from the screen.
Cash Dispenser: Withdrawal money is given by this slot.
Deposit Slot: To deposit money this slot is use.
Speaker: Speaker provides the facilities to the customer by giving auditory feedback.

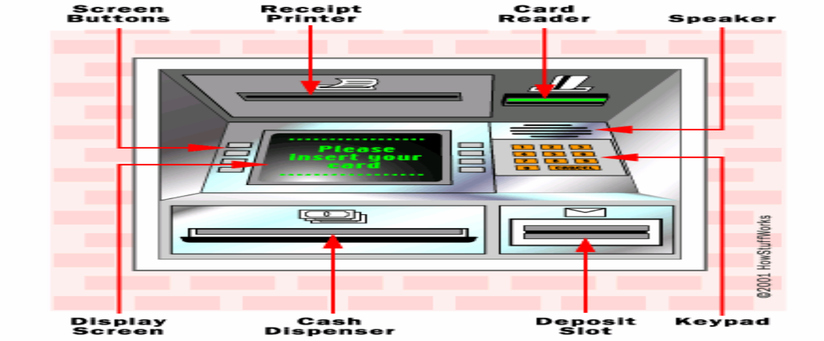


Fig: Interactive Components of ATM

4.17 Possible Type of Data stored in Magnetic Stripe Card

Mainly magnetic strip hold the following information:

- Cardholder Name
- Card Number / Account Number
- Expiration Date and
- Additional Data if needed

4.18 Algorithm use for Card Number Generation

LUHN‘s algorithm is used for card number generation and encoding. It is also called mod 10 algorithms. Card number must be 13 to 16 digits. And the last digit is the check digit. To calculate check Digit:
1. First drop the last digit from the card number (because that’s what we are trying to calculate).
2. Reverse the number.
3. Multiply all the digits in odd positions (The first digit, the third digit, etc) by 2.
4. If anyone is greater than 9 subtract 9 from it.
5. Sum those numbers up.
6. Add the even numbered digits (the second, fourth, etc) to the number you got in the previous step.
7. The check digit is the amount you need to add to that number to make a multiple of 10. So if you got 68 in the previous step the check digit would be 2. You can calculate the digit in code using check digit = ((sum / 10 + 1) * 10 – sum) % 10. For Credit Card Number Validation use 10 mod Algorithm:
- First step: number is reversed and then every second digit is doubled
Example:
378282246310005
Reverse
5 **0** 0 **0** 1 **3** 6 **4** 2 **2** 8 **2** 8 **7** 3
Second digit
0 0 6 8 4 4 14
- Second step: resulted values will be added to those of which are not multiplied.
= 5 + (0) + 0 + (0) + 1 + (6) + 6 + (8) + 2 + (4) + 8 + (4)
+ 8 + (14-9) + 3 = 60.

4.19 What is ATM Card?

ATM card is also like magnetic strip card. It is also a data carrier which electronically reads and writes data. ATM cards mainly a debit card.

4.21 Connection Type of ATM

ATM connections mainly have two types:
- Dial up Connection using Modem
- Leased Line Connection

4.22 ATM Service Providers in Bangladesh

-Standard Chartered, HSBC, BRAC Bank, Bank Asia & NCC etc.

4

30 Survey Report

Bank Asia

Bank Asia uses ETN (Electrical Transaction Network) network which is a United International ATM service provider. ETN combined nine banks to give E-Cash services. Network equipments like ATM machine, switches etc are setup by ETN.

4.23 Ways of Transaction

In Bank Asia transactions are divided into three main categories

- My bank to others bank A customer of a bank uses other banks ATM.
- Others bank to my bank other banks customer uses ATM of Bank Asia.
- My bank to my bank a customer uses its own bank ATM machine.

4.24 Connectivity Type

For ATM machines Bank Asia (provided by ETN) uses two types of connections. They use leased line for connection. Bank Asia uses two connection lines because if one line is down immediately other one will be activated within a minute. These connections are:

- DDN (under T&T)
- Metro net

4.25 No. of Digit Uses

Bank Asia uses 18 digit ATM card (provided by ETN). They divide 18 in five sections for the identification of those banks, Account number, branch etc.

1-6 digits	7-9 digits	10-12 digits	13-17 digits	18 digits
International Identification number (IIN)	Regional code	Branch code	Account number	Computer generated

Fig: Classification of 18 Digit Number

IIN

First six digits are different for those nine banks. So, ATM machine can easily identify among these banks.

Regional Code

0These 3 digits are used to distinguish between different districts Branch Code.

Branch Code

These 3 digits are used to distinguish between different districts

Account Number

These five digits are the account number which differentiate among the user and unique for each user.

4.26 Problems of ATM

Bank Asia has few problems with their ATM machines

- Do not have Bangle Interface
- ATM booths are not available in every locality.

4.27 SECURITY

Security is most important part for online banking system. We use the different method for provide strong online banking security system and use owasp top ten project provide online banking security. Ensuring comprehensive network security visibility is no easy task. Uncover expert tips on how to improve network security visibility with network flow analysis tools, cloud security monitoring solutions, and anomaly-based monitoring technology.

4.28 AUTHENTICATION MECHANISM

Authentication is the process of establishing whether a client is who or what it claims to be in a particular context. A client can be an end user, a machine, or an application. The authentication mechanism is responsible for creating a credential, which is an internal product representation of a successfully authenticated client user. The abilities of the credential are determined by the configured authentication mechanism.

4.28.1. Challenge handshake Authentication Protocol (Chap)

CHAP is an authentication scheme used by point to point servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. CHAP provides protection against playback attack by the peer through the use of an incrementally changing identifier and of a variable challenge-value. CHAP requires that the client make the secrete available in plaintext form.

CHAP Packets

Description	1 byte	1 byte	2 bytes	1 byte	Variable	Variable
Challenge	Code = 1	ID	Length	Challenge length	Challenge value	Name
Response	Cade = 2	ID	Length	Response length	Response value	Name
Success	Cade = 3	ID	Length		Message	
Failure	Cade = 4	ID	Length		Message	

4.29 ACCESS CONTROL LIST (ACL)

ACLs are lists of conditions used to test network traffic that tries to travel across a router interface. These lists tell the router what types of packets to accept or deny.

01. ACLs can be created for all routed network protocols such as IP and Internet
02. Packet Exchange (IPX).
03. ACLs can be configured at the router to control access to a network or subnet.
04. To filter network traffic, ACLs determine if routed packets are forwarded or blocked at the router interfaces.

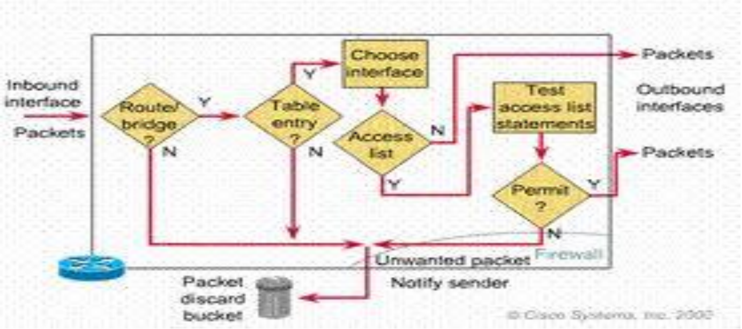


Figure: ACLs working Area

4.29.1 ACLs can be used to perform the following task

- Limited network traffic and increase network performance
- Provide traffic follow control
- Provide a basic level of security for network access.
- Decide which types of traffic are forwarded or blocked at the router interfaces.
- Control which areas a client can access on a network.
- Script hosts to permit or deny access to a network.

4.29.2 How ACLs Work:

ACL is made up of statements that define whether packets are accepted or rejected at inbound interfaces.

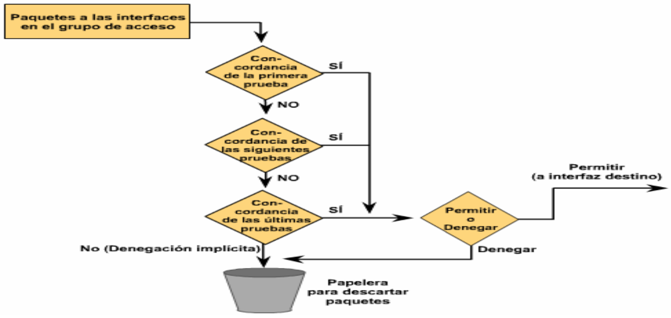

Paquetes a las interfaces en el grupo de acceso
Con-cordancia de la primera prueba
SI
NO
Con-cordancia de las siguientes pruebas
SI
NO
Con-cordancia de las últimas pruebas
SI
Permitir o Denegar
Permitir (a interfaz destino)
Denegar
No (Denegación implícita)
Papelera para descartar paquetes

Figure: ACL Working Flowchart.

4.30 Virtual Local Area Network (VLAN)

VLAN is another process of secure the network security. In the banking system using the VLAN head office to other branch office for provides the integrated security. VLAN configuration using a manageable Cisco switch. Configure the switch and separate the each department. Each department only access the own department data cannot access the other department data without permission.

4.30.1 Virtual private Network (VPN)

VPN follows a client and server approach. VPN clients authenticate users, encrypt data, and otherwise manage sessions with VPN servers utilizing a technique called **tunneling**.

V. SUMMARY STEP WORK DESCRIPTION

DESCRIPTION

The aim of this system is to overcome the lacking of the 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 create 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). Routers are generally known as intermediate systems, which operates at the network layer of the OSI reference model, routers are devices used to connect two or more networks (IP networks) or a LAN to the Internet. A router acts as a packet filter when it forwards or denies packets according to filtering rules. As a Layer 3 device, a packet-filtering router uses rules to determine whether to permit or deny traffic based on source and destination IP addresses, source port and destination port, and the protocol of the packet. These rules are defined using access control lists or ACLs. Banking system in Bangladesh all banks has an IT department. IT department solution all type of IT problem and serve the core network. IT creates a core network diagram. This diagram involves all type of useable network mechanism (Switch, Router, Firewall, Server) etc. Simulation is the most important of any system. An accurate system design, accurate performance and accurate Simulation give best performance of a system. Now we discuss and simulate the OSPF protocol.
Open Shortest Path First (OSPF) is a routing protocol developed for Internet Protocol (IP) networks by the interior gateway protocol (IGP) working group of the Internet Engineering Task Force (IETF)

VI.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 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.

6.1 Future work

- ✓ Add time based transmission.
- ✓ Security system will be upgraded .
- ✓ Make the project more user friendly.
- ✓ Real life implementation.

6.2 Limitations

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

REFERENCE

[1] J.Claessens, V. Dem, D. Cock, B. Preneel, J. Vandewalle (2002) “On the Security of Today's On-line Electronic Banking Systems”.

[2] Andrew S. Tanenbaum, (2002)“Computers network”.

[3] CCNA study Guide, Available At: https://www.google.com.bd/?source=search_app&gws_rd=cr, ssl&ei=y9b VYniG4KsuQ TuvY84#q=Todd+Lammle,+%E2%80%9CCCNA+study+Guide%E2%80%9D,BPB+Publications,+Edition:+5th.

[4] Computer Network Device, Available At: http://basic-networking.blogspot.com/2007/08/computer-network-devices-and component.hml

[5] IPv4 - Address Classes Available At: http://www.tutorialspoint.com/ipv4/ipv4_address_classes.htm

[6] Stuttgart Available At: http://www.ba-stuttgart.de/~schulte/html/55771.html#HDR3

[7] http://cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/ethernet.htm#1020850

[8] Definition Available At : www.defination.com

[9] OSPF Available At: http://www.answers.com/topic/open-shortest-path-first

[10] Understanding of ATM in Bangladesh Available At: http://www1.searchresults.com/web?l=dis&q=understanding+ ATM+in+bangladesh&o=APN10645&apn_dtid=^BND406^YY^BD&shad=s_0042&apn_uid =9734054855124.

[11] Access Control List (ACL) Available At: http://en.wikipedia.org/wiki/access_control_list.

[12] standard-access-control-list Available At: http://www.answers.com/topic/standard-access-control-list.

[13] Computer networking Available At: http://compnetworking.about.com/od/vpn/g/bldef_vpn.htm.

[14] OWASP Available At: https://www.owasp.org/index.php/Category: OWASP_Top_Ten_2013_Project.