A Case Study: VLAN to Optimize the Network Solution to Enhance the Customized Service

Farzana Nawrin, Syed Jamaluddin Ahmad, Roksana Khandoker

***Abstract*— VLANs provide for logical groupings of stations or switch ports, allowing communications as if all stations or ports were on the same physical LAN segment. This includes stations or ports that are physically located on different 802.1D bridged LANs. Technically, each VLAN is simply a broadcast domain. VLAN broadcast domains are configured through software rather than hardware, so even if a machine is moved to another location, it can stay on the same VLAN broadcast domain without hardware reconfiguration.**

***Index Terms*— VLANs, switch ports.**

I. Introduction

VLAN is Virtual Local Area Network used widely in computer network technology. VLAN is a technology through which LAN devices are divided into network segments based on logical instead of physical what? It is the logical segmentation of network users that connect to the second layer on the switch port. The network segmentation does not limit the physical location of network users. It is according to the user needs, for example, a VLAN could be based on the location of network users, roles, departments, users of the network applications and protocols used for grouping.

VLAN technology allows network managers of a VLAN to physically divide it into different broadcast domains logically. Each VLAN contains the same properties of a group. However, it is logically, not physically divided. Although some workstations belong to the same VLAN,

there is no need to place them in the physical VLAN segment.

VLAN solves the Ethernet issue which is about broadcasting and security. It increases the VLAN ID base on the Ethernet. The VLAN ID could be for users divided into smaller working groups to limit the second layer of user exchange visits from different working groups. Each working group is a VLAN. The advantage of VLAN limits broadcast range and forms virtual working groups to a dynamic manage network.

II. TYPES OF VLAN

To overcome the broadcasting problem of Ethernet, the network uses VLAN (Virtual LAN) technology to change Ethernet into point-to-point communication to prevent interception. Currently there are four kinds of VLAN:

➢ ¤ Port-Based VLAN Tagging based on switch ports. For example, you might group switch ports 1 to 2 into VLAN 101 for the HR department and ports 6 to 12 into VLAN 102 for the IT department. This kind of configuration is the simplest to deploy and maintain. However, it is inflexible as moving a workstation may require changing the switch configuration.

➢ ¤ MAC-Based VLAN Tagging based on layer 2 MAC address. This requires signifi¬cant initial configuration of the switches,. However, automatic tracking is possible thereafter.

➢ ¤ Protocol Based VLAN Tagging based on layer 3 IP address, layer 4 transport protocol information, or even higher-layer protocol information.

➢ ¤ Policy Based VLAN Tagging based on certain policies or user configuration. This may involve classifying network traffic into groups and assign¬ing QoS priority bits and VLAN ID to each group.

III. REASON FOR VLAN

The management through that the VLAN deliver unprecedented levels of security, performance and reliability such as the following;

¤ Flexible Network Partition and Configuration Using VLANs, a network can be partitioned based on the logical grouping (Figure), not based on the physical topology. For instance, you can move a user from the sales floor to the accounting floor and maintain the same logical grouping even though the physical topology has changed.

Farzana Nawrin, Lecturer and Coordinator, Department of Computer Science & Engineering, Shanto-Mariam University of Creative Technology, City: Dhaka, Country: Bangladesh

Syed Jamaluddin Ahmad, Assistant Professor and Head, Department of Computer Science & Engineering, Shanto-Mariam University of Creative Technology, City: Dhaka, Country: Bangladesh

Roksana Khandoker: Senior Lecturer, Department of Computer Science & Engineering, University of South Asia, City: Dhaka, Country: Bangladesh

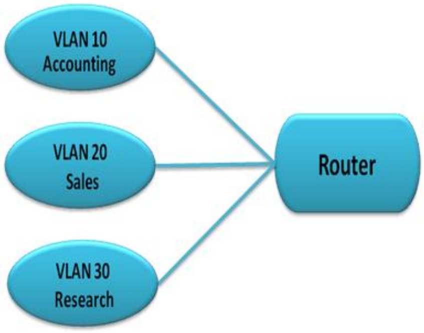


Fig 1: Flexible Network Partition

¤ Performance Improvement TCP/IP network protocols and most other protocols broadcast frames periodically to advertise or discover network resources. On a traditional flat network, frames reach all hosts on a network. This can have a significant impact on the network performance when you have a large number of end users. Confining broadcast traffic to a subset of the switch ports or end users saves significant amounts of network bandwidth and processor time.

¤ Cost Savings Without VLANs, network administrators partition LANs into multiple broadcast domains by using routers between those segments. However, routers are expensive and may introduce more delay.

IV. VLAN DIVISION

A port divided-VLAN is divided according to the several number of switch ports of the VLAN in the network. Computers belonging to the same VLAN have same network address, but different communication between VLAN needs to go through layer 3 routing protocols. VLAN uses this approach in work process when the network node migrates. If the old and the new port are not within the same VLAN, then the user must reset the port. For accessing each different network unit, VLAN uses the router and the filtering port of the MAC address to prevent illegal access and stealing IP address.

MAC address divided-VLAN: regardless of whether the node is moved in the network or not, the administrator does not have to re-configure VLAN when this way is used to divide VLAN. Because MAC address is not changed.

IP address divided-VLAN: The VLAN does not need not complicated configurations when a new node is added to the network. The switch will automatically allocate the node into different VLAN according to its IP address. This is best intelligent method to divide VLAN, but it is also complicated. The IP address will be unavailable when the VLAN is deleted, thus preventing unauthorized users use of resources on network through modifying the IP address.

Protocol divided-VLAN: This method divided VLAN according to the protocol fields of layer 2 data frames. Determining the upper layer run of the network protocol is through the protocol fields of layer 2(such as IP protocol or IPX protocol). If there are IP, IPX and others protocols running in a physical network, this method is best way.

V. VLAN COMMUNICATION

Designing a VLAN is a requisite in a current network structure. Considering the security performance and transmission speed of network, the VLAN communication problem is also very important aspect because the network product of development and application is very fast and inter-VLAN communication has no uniform standard. Each network equipment manufacturer ha their own strong point for inter-VLAN communication technologies. Therefore, the specific network planning should be based on characteristics of network devices and applications of network to decide which method to use.

VI. ESX Server VLAN Solutions

In order to support VLANs for ESX Server users, one of the elements on the virtual or physical network has to tag the Ethernet frames with 802.1Q tag. There are three different configuration modes to tag (and untag) the packets for virtual machine frames.

VII. Virtual Machine Guest Tagging (VGT Mode)

One may install an 802.1Q VLAN trunking driver inside the virtual machine, and tags will be preserved between the virtual machine networking stack and external switch when frames are passed from/to virtual switches. (Figure)

The advantages of using this mechanism are:

¤ The number of VLANs per virtual machine is not limited to the number of virtual adapters, which means your virtual machines can be on any number of VLANs on your network.

¤ If a physical server is already running VLAN driver, then it will be natural to use P2V Assistant to convert this server and keep running the existing VLAN tagging.

The disadvantage of using this mechanism is that it is not always possible or easy for the user to find and configure 802.1Q drivers for the guest operating system.

Without VLAN hardware acceleration, it takes additional CPU cycles to tag the outbound frames and remove the tag for inbound frames.

One may have to use this solution if a single virtual machine must be on five or more different VLANs in the network. This method could also be appropriate when existing physical servers running 802.1Q trunking drivers are being virtualized. Such servers can be virtualized simply by using P2V Assistant and no additional network configuration is required. The new virtual machine will automatically inherit all VLAN settings from the physical machine.

Some operating systems, including some Linux distributions, support 802.1Q trunking well.

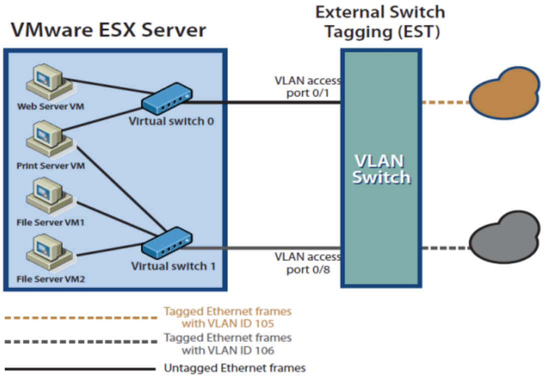


Fig 2: Virtual Machine Guest Tagging

VIII. External Switch Tagging (EST Mode)

The user may use the external switches for VLAN tagging. This is similar to a physical network, and VLAN configuration is normally transparent to each individual physical server. The tag is appended when a packet arrives at a switch port and stripped away when a packet leaves a switch port toward the server. (Figure)

ESX Server users can set up the VLAN configuration just as they would for any physical server. One drawback of this approach is that if port-based VLAN tagging is used (common in enterprise VLAN deployments) the total number of virtual LANs supported would be limited to the number of NICs installed on a given ESX Server system. This limitation is removed using VGT or VST modes as described in this white paper.

IX. ESX Virtual Switch Tagging (VST Mode)

In this mode, you provision one port group on a virtual switch for each VLAN, and then attach the virtual machine's virtual adapter to the port group instead of the virtual switch directly. The virtual switch port group tags all outbound frames and removes tags for all inbound frames. It also ensures that frames on one VLAN do not leak into a different VLAN. (Figure)

ESX Server virtual switch tagging has the following benefits:

¤ Different VLAN frames can be multiplexed onto a single physical NIC, so you can consolidate all traffic regardless of VLAN into a single physical NIC. There is no need for multiple NICs to service multiple VLAN’s.

¤ It eliminates the need to run a guest operating system specific VLAN driver inside the virtual machine.

¤ Since all modern high-speed network cards support VLAN acceleration, there is little performance impact by supporting VLAN tagging in the virtual switches.

¤ Once the switch trunk mode is appropriately set up, no additional switch configuration is needed when provisioning additional VLANs. External switch configuration becomes easy.

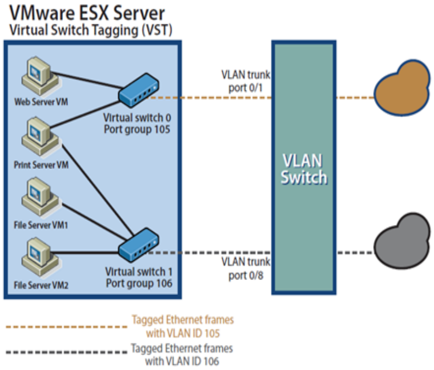
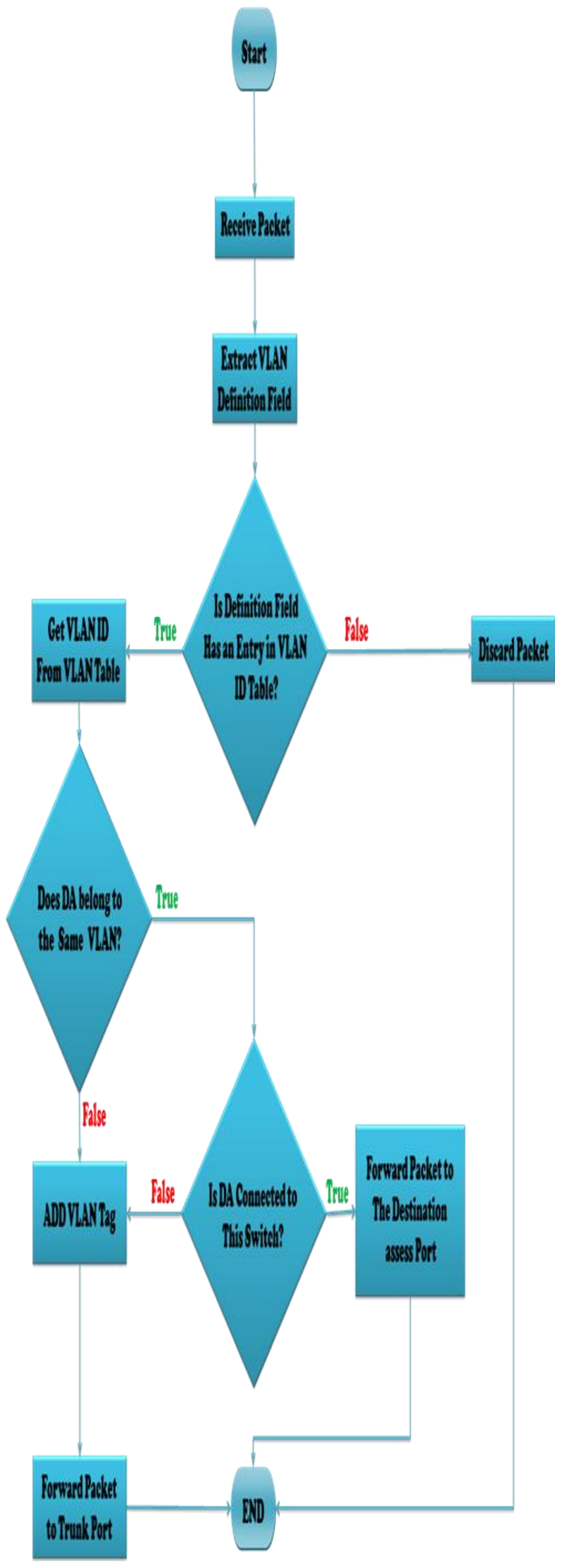


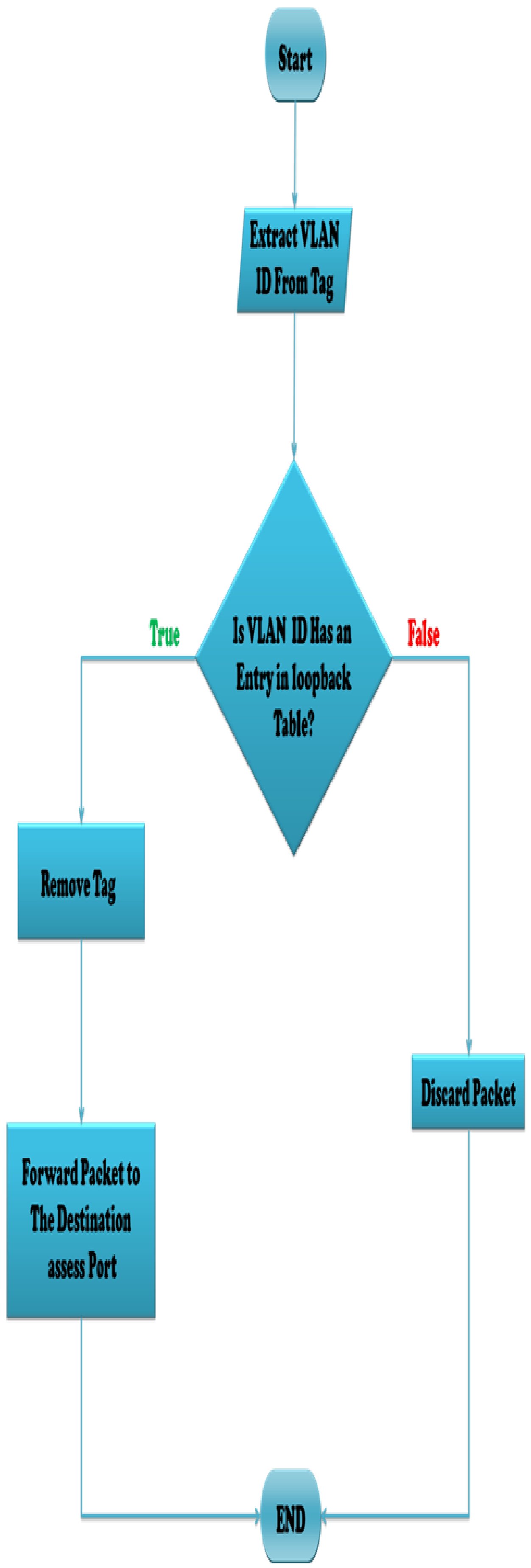
Fig 3: External Switch Tagging

IX. Flowchart of VLAN

Flowchart of a VLAN switch action to a packet receive from an access link is given below;


Start
Receive Packet
Extract VLAN Definition Field
Is Definition Field Has an Entry in VLAN ID Table?
True
False
Get VLAN ID From VLAN Table
Discard Packet
Does DA belong to the Same VLAN?
True
False
False
ADD VLAN Tag
Is DA Connected to This Switch?
True
Forward Packet to The Destination assess Port
Forward Packet to Trunk Port
END

Flowchart of a VLAN switch action to a packet receive from trunk link is given below;


Start
Extract VLAN ID From Tag
True
Is VLAN ID Has an Entry in loopback Table?
False
Remove Tag
Discard Packet
Forward Packet to The Destination assess Port
END

X. A CASE STUDY

There are 100 computers in a company network, mainly used by the following departments: Accounting (30), Research (20) and Sales (50).

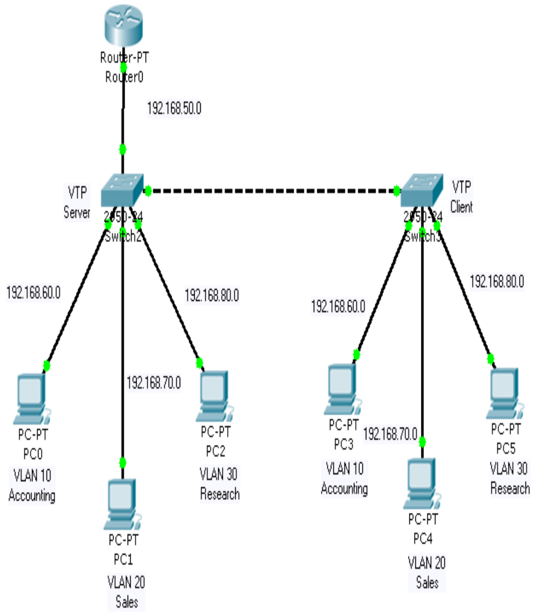


Fig 4 : A company network

XI. DESIGNING VLAN DIVISION AND CONFIGURATION

The basic structure of network is as follows: The network required resources use 3 switches (Cisco 2950-24, named as: Switch2, Switch3). One router (Router-PT), the network would connect to the Internet through the router.

The connected users are mainly distributed in four parts: Accounting, Research and Sales. VLAN is divided for the user of the four departments to ensure the network resources of appropriate department are not stolen or destroyed. Network resource security requires sensitive company departments such as the accounting are not easily accessed by other users. So the company used the VLAN method to solve the problem. Divided by VLAN, the network can be mainly divided into: Accounting, Research and Sales, corresponding to VLAN group name: Accounting, Research and Sales. The segment of each VLAN group is as follows:

VLAN	VLAN Name	Number of port
10	Accounting	4 to 10
20	Research	11to 15
30	Sales	16 to 23

Also VTP Server is applying in Switch 1 and VTP client is apply in switch 2.

XII. PRIVILEGED MODE

Router or Switch use “>” prompt to enter privilege mode command “enable”, the command is entered as “>enable”. Then we enter switch privilege mode.

```
Switch>enable
Switch#
```

XIII. CONFIGURE MODE

The next step is to enter the configuration mode for changing the system configurations. To enter the config mode, enter the following command:

```
Switch#configure terminal
Switch(config)#
```

XIV. TRUNK MODE

Trunk the port connected with the other Switch or router. It must be configure after enter the interface. To give the Trunk Mode, enter the following command:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
```

XV. IP ADDRESS SETING

Switch must need an IP address. To set the IP Address in the Switch enter the following command:

```
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.60.1 255.255.255.1
Switch(config-if)#no shutdown
Switch(config-if)#exit
```

XVI. VLAN NAME

Set the VLAN name. Because 3 VLAN belongs to different switch and configure a name and same VLAN number on Switch2 and Switch2. To give the VLAN Name, enter the following command:

```
Switch(config)#interface fastEthernet 0/1
Switch(config-if)#vlan 10
Switch(config-if)#name  Accounting
Switch(config-if)#exit
```

XVII. ACCESS MODE

Each port of Switch must be Access. So To give the Access mode, enter the following command:

```
Switch(config)#interface fastEthernet 0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 10
Switch(config-if)#exit
```

XVIII. VTP MODE

To easy the work one can do VTP in the Switch. One switch would be server and other would be client. If any command would be written in server switch then client switch copy this command. So To give the VTP mode in server Switch, enter the following command:

```
Switch(config)#VTP mode server
Switch(config)#VTP Domain Name
Switch(config)#VTP password password
Switch(config)#end
```

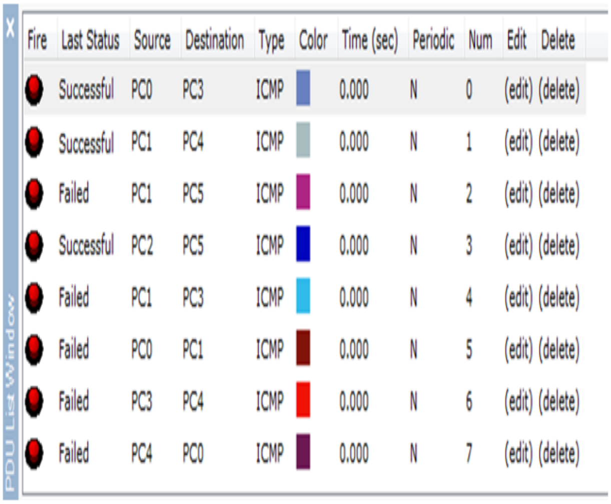
To give the VTP mode in Client switch, enter the following command:

```
Switch(config)#VTP mode client
Switch(config)#VTP password password
Switch(config)#end
```

The configuration commands can be seen in Appendix 2.

XIX. Simulation

After doing the configuration using **Packet Tracer** Software we get the simulation output which given bellow;



Fire	Last Status	Source	Destination	Type	Color	Time (sec)	Periodic	Num	Edit	Delete
●	Successful	PC0	PC3	ICMP	■	0.000	N	0	(edit)	(delete)
●	Successful	PC1	PC4	ICMP	■	0.000	N	1	(edit)	(delete)
●	Failed	PC1	PC5	ICMP	■	0.000	N	2	(edit)	(delete)
●	Successful	PC2	PC5	ICMP	■	0.000	N	3	(edit)	(delete)
●	Failed	PC1	PC3	ICMP	■	0.000	N	4	(edit)	(delete)
●	Failed	PC0	PC1	ICMP	■	0.000	N	5	(edit)	(delete)
●	Failed	PC3	PC4	ICMP	■	0.000	N	6	(edit)	(delete)
●	Failed	PC4	PC0	ICMP	■	0.000	N	7	(edit)	(delete)

From the simulation output we see that PC0 and PC3 are on same VLAN. So that when PC0 send an ICPM packet to the destination PC3 the Last Status is Successful. That means the packet is successfully sent form PC0 to PC3. Again PC1 and PC4 are on same VLAN. PC1 send an ICPM packet to the destination PC4 the Last Status is Successful. That means the packet is successfully sent form PC1 to PC4. The same process is done for PC2 andPC5.

PC1 and PC5 are on different VLAN. So that when PC1 send an ICPM packet to the destination PC5 the Last Status is Failed. That means the packet is not reach to PC5. Again PC1 and PC3 are on same VLAN. PC1 send an ICPM packet to the destination PC3 the Last Status is Successful. That means the packet is successfully sent form PC1 to PC3. The same process is done for PC2 andPC3. The same process is done for PC0 andPC1, PC3 andPC4, PC4 andPC0.

XX. Conclusion

The thesis mainly introduces an analysis of network security technology applied in LAN. It is also introduces how to establish a preliminary LAN Protection System using VLAN technology to protect and design a LAN structure from the internal network.

Network information security is a very important and extensive topic, which contains a large amount of information. It can be greatly helpful for our society's development and play a crucial role in people's lives. We need to research and master more and more technologies that can be used to guarantee network information security. Some technologies, such as firewall technology, anti-virus technology, against external technology and VLAN technology, are useful for every LAN. Based on methods that the thesis mentioned, we are capable of initially establishing a LAN security protection system. It makes great improvement on a network's security. If all the methods are applied in the same network, the effect of security protection is obvious.

References

[1] https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security
[2] https://digitalguardian.com/blog/what-cyber-security
[3] https://www.csoonline.com/article/3242690/data-protection/what-is-cyber-security-how-to-build-a-cyber-security-strategy.html
[4] https://www.csoonline.com/article/2616316/data-protection/the-5-types-of-cyber-attack-youre-most-likely-to-face.html
[5] https://www.csoonline.com/article/3227065/security/cyber-attacks-cost-us-enterprises-13-million-on-average-in-2017.html
[6] https://www.mwrinfosecurity.com/our-thinking/targeted-attack-case-studies/
[7] https://www.alertlogic.com/customers/case-studies/
[8] https://www.acorn.gov.au/learn-about-cybercrime
[9] cyber Law
[10] https://www.fireeye.com/current-threats/what-is-cyber-security.html
[11] [11] https://www.fireeye.com/current-threats/detect-and-prevent.html
[12] https://www.fireeye.com/current-threats/what-a-ceo-needs-to-know-about-cyber-security.html
[13] https://www.fireeye.com/current-threats/best-defense-against-spear-phishing-attacks.html
[14] https://www.fireeye.com/current-threats/tco.html
[15] https://www.fireeye.com/current-threats/stopping-todays-cyber-attacks.html

Farzana Nawrin achieved Bachelor of Science in Computer Science and Engineering (BCSE) from Dhaka City College under National University, Masters of Science in Computer Science from Jahangirnagar University. She achieved 1st class 1st both B.Sc. and M.Sc. degree. Presently working as a lecturer & Coordinator, Computer Science and Engineering department, Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh. Formerly, was also a lecturer of Computer Science and Engineering department of Dhaka City College under National University. She has done two thesis about network security in her B.Sc. and M.Sc. level. She has two international journal.She was also attended many national workshop. She has got special training from Bangladesh Institute of Design and Development(BIDD). She has special certification in CCNA and CompTIA A+. Her areas of interest include Network Security, Telecommunication, System analysis, Automata Design, Routing and Switching, Design and Analysis Compiler, Wifi,Wimax,3g and 4g Network.

Syed Jamaluddin Ahmad, achieved Bachelor of Science in Computer Science and Engineering (BCSE) from Dhaka International University, Masters of Science in Computing Science Associates with research: Telecommunication Engineering from Athabasca University, Alberta, Canada and IT-Pro of Diploma from Global Business College, Munich, Germany. Presently Working as an Assistant Professor and Head, Computer Science and Engineering, Shanto-Mariam University of Creative Technology, Dhaka, Bangladesh. Formerly, was head of the Department of Computer Science & Engineering, University of South Asia from 2012-2014, also Lecturer and Assistant Professor at Dhaka International University from 2005-2007 and 2011-2012 respectively and was a lecturer at Loyalist College, Canada, was Assistant Professor at American International University, Fareast International University, Royal University, Southeast University and Many more. He has already 15th international publications, 12th seminar papers, and conference articles. He is also a founder member of a famous IT institute named Arcadia IT (www.arcadia-it.com). Achieved Chancellor's Gold Crest in 2010 for M.Sc. in Canada and Outstanding result in the year of 2005. and obtained "President Gold Medal" for B.Sc.(Hon's). Best conductor award in Germany for IT relevant works. Membership of "The NewYork International Thesis Justification Institute, USA, British Council Language Club, National Debate Club, Dhaka, English Language Club and DIU . Developed projects: Mail Server, Web Server, Proxy Server, DNS(Primary, Secondary, Sub, Virtual DNS), FTP Server, Samba Server, Virtual Web Server, Web mail Server, DHCP Server, Dial in Server, Simulation on GAMBLING GAME Using C/C++, Inventory System Project, Single Server Queuing System Project, Multi Server Queuing System Project, Random walk Simulation Project, Pure Pursuit Project (Air Scheduling), Cricket Management Project, Daily Life Management Project, Many Little Projects Using Graphics on C/C++, Corporate Network With Firewall Configure OS:LINUX (REDHAT) Library Management Project Using Visual Basic, Cyber View Network System:Tools:Php OS: Windows Xp Back-end: My SQL Server, Online Shopping: Tools: Php, HTML, XML. OS:Windows Xp, Back-end: My SQL and Cyber Security" Activities-'Nirapad Cyber Jogat, Atai hok ajker shapoth'-To increase the awareness about the laws, 2006 (2013 amendment) of Information and Communication and attended Workshop on LINUX Authentication"-Lead by- Prof. Andrew Hall, Dean, Sorbon University, France, Organized By-Athabasca University, CANADA, April, 2009. His areas of interest include Data Mining, Big Data Management, Telecommunications, Network Security, WiFi, Wimax, 3g, 4g network, UNIX, LINUX Network Security,Programming Language(C/C++ or JAVA), Database (Oracle), Algorithm Design, Graphics Design & Image Processing and Algorithm Design.

Roksana Khandoker, achieved Bachelor of Science in Computer Science and Engineering (BCSE) from United International University, Masters of Science in Computer Science and Engineering from University of South Asia. Presently Working as a Senior Lecturer, Computer Science and Engineering, University of South Asia, Dhaka, Bangladesh. Formerly, was also a lecturer at different poly-technique institutes. She has 4th international journals and attended different international and national conferences. She is the Chairman of the famous IT institute named Arcadia IT and Chairman of Brighton International Alliance. Her areas of interest include Data Mining, Big Data Management, Telecommunications, Network Security, WiFi, Wimax, 3g and 4g network.