World Journal of Engineering Research and Technology
WJERT
www.wjert.org
SJIF Impact Factor: 5.924

DESIGN AND IMPLEMENTATION OF A NETWORK SECURITY MODEL FOR DEPARTMENTS USING TELNET

[1]*Nisarga Patil, [2]Shambhavi Hiremath and [3]Dr. S. V. Viraktamath

[1,2]Student and [3]Assistant Professor

Article Received on 08/04/2020 **Article Revised on 28/04/2020** **Article Accepted on 18/05/2020**

***Corresponding Author**
Nisarga Patil
Student

ABSTRACT

Nowadays, network is becoming more and more complex but has become extremely important in present day society. VLANs are widely used in many enterprises, data collection and campus networks. It analyses in detail about the application of VLAN and in addition it proposes a strategy on how to divide different department networks.An active security mechanisms ie; Secure VLAN architecture which is used for switched LAN; is connected to Internet. This paper proposes implementing the method of LAN-Switching using VLAN to break up broadcast domains into segments, so as to improve network performance. It includes implementation of Telnet protocol.

Index Terms – *Simulation, Switch, Packet Tracer, VLAN and TELNET.*

I. INTRODUCTION

Network traffic trends vary from time to time. Advancement in the development and co-existence of various types of network applications results in more dynamic traffic trends. So the statistics of the network traffic need to be refreshed frequently to get an accurate picture of the underlying traffic trends. In such type of dynamic network usage, any system that takes decision on the basis of various properties of the network traffic should also be intelligent enough to respond to these varying trends. A VLAN can be defined as a logical group of devices or users, associated using any function, department or application etc which is not dependent on physical location on the LAN (Local Area Network). VLAN is used to minimize local traffic existing outside the logical group.

For the purpose of more security the remotely control transport functions by using a Telnet-based user interface provided in network equipment. We separate a control function as an external entity from a transport control function and get separated functions to intercommunicate through a Telnet protocol. It is utilized to deploy new services or protocols to the existing networks without difficulties to embed them in the networks equipment or without risks to replace the existing network equipment with the newly developed ones.

This paper aims at design and simulation of an enterprise network using Packet Tracer to provide VLAN security. A Virtual Work Group is created which introduces network design concepts, principles, models and architectures. Typically, network design consists of the entire logical map network to be designed and the location of the networking devices like switches routers etc. This technique enables to forecast project duration more accurately.

1.1 Security in Departments

Virtual local area network is a local area network configured by software, not by physical wiring. The whole idea of VLAN technology is to divide a LAN into logical, instead of physical, segments. A LAN can be divided into several logical LANs called VLANs. Each VLAN is a work group in the organization. VLAN technology even allows the grouping of stations connected to different switches in a VLAN. VLANs group stations belonging to one or more physical LANs into broadcast domains. The stations in a VLAN communicate with one another as though they belonged to a physical segment. VLAN use different characteristics such as port numbers, MAC addresses, IP addresses, IP multicast addresses, or a combination of two or more of these. Advantages of using VLANs are Cost and Time Reduction VLANs can reduce the migration cost of stations going from one group to another. Physical reconfiguration takes time and is costly. Instead of physically moving one station to another segment or even to another switch, it is much easier and quicker to move it by using software. For example, in a campus environment, professors working on the same project can send broadcast messages to one another without the necessity of belonging to the same department. This can reduce traffic if the multicasting capability of IP was previously used. Security VLANs provide an extra measure of security. People belonging to the same group can send broadcast messages with the guaranteed assurance that users in other groups will not receive these messages.

II. LITRATURE SURVEY

2.1 Related work

In the year 2017, Prof. Mrs. Jaya N. Ingole, Kshama S. Bhise purposed "Study on Virtual LAN Usage in Campus Networks". The author mainly targeted towards campus networks which deliver required security. IT indicates that VLANs are used for many objectives that they were not originally intended for and are often ill-suited for the tasks further, the use of VLANs complicates network configuration management.

In the year 2009, Kang Woon Hong, Won Ryu, Jun Kyun Choi purposed "Telnet-based Transport Control" which aimed at remote transport control scheme for a packet forwarding network equipment using a Telnet user interface.

By using the proposed scheme, it is possible to easily deploy new services and protocols to the network without efforts to develop a new transport control function for the existing network equipment as well as without concern about performance degradation for the network.

In the year 2010, Sun Litan, purposed "The Application of VLAN in College Library Network" which aims in the application of VLAN can effectively control broadcasting storm, ensure the performance of network and is very flexible and extendable. VLAN improves the efficiency and security of network and strengthen the secrecy and cooperation among different departments in college library and thus enables the library network to serve both the library and readers much better.

III. PROPOSED WORK

Implementation of virtual local area network for security mechanism in different department network. Security can be obtained by using security mechanism like IP configuration and TELNET. Specifically the aim of research is:

Implementation of Star Topology

A network topology is the arrangement of a network, including its nodes and connecting lines. In computer networking, topology refers to the layout of connected devices. Network topologies are categorized into the following basic types: Star, ring, bus line, tree, mesh. In this project we basically consider a star topology shown in Fig 3.1. It is one of the most common network setups. In this configuration, every node connects to a central network

device, like a hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients. Depending on the type of network card used in each computer of the star topology, a coaxial cable or an RJ-45 network cable is used to connect computers together.

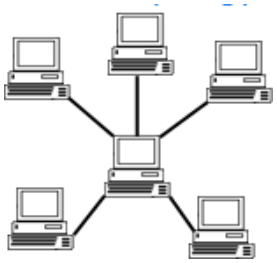

Fig 3.1: Star Topology.

Implementation of TELNET

Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator or another user can access someone else's computer remotely. The Web, HTTP and FTP protocols allows us to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, we log on as a regular user with whatever privileges we may have been granted to the specific application and data on that computer. Telnet's true value is not the abstraction of how-to-wire-terminals-to-hosts instead; it's the abstraction of terminals Telnet's application-level semantics are captured in its external interface, the Network Virtual Terminal. Its internal interfaces have close ties to TCP transport facilities, an option negotiation scheme, and symmetric treatment of client and server roles. Simple as Telnet may seem to use, its internal implementation depends on understanding TCP, a careful ballet of option-negotiation steps, and symmetry as a design principle. There's only one category of Telnet client programs: login tools. But Telnet itself can be used by many applications. It may seem odd to have dissected Telnet at such length without once mentioning logins, passwords, and all the other details of establishing a terminal connection. Telnet, though, connects arbitrary processes, raises the specter of deadlock if information backs up.

IV. METHODOLOGY

In order to design and implement a Hierarchical Model of an Enterprise Network between various departments the following methodology was used:

a) Conceptualizing the Ideas.

b) Designing the Network Architecture.

c) Use of TELNET for more security purpose.

V. DESIGN AND IMPLEMENTATION

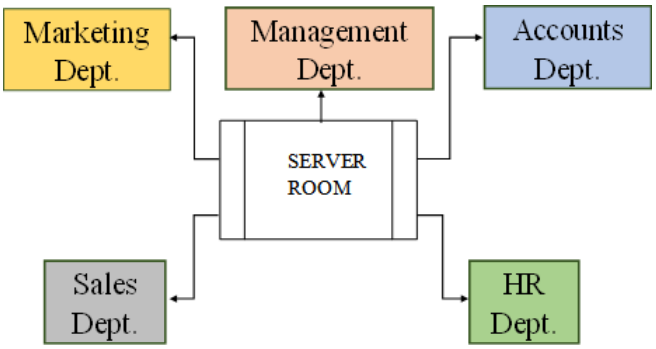

Fig 5.1: Block Diagram.

A network is created consisting of PCs, Laptops, switch (acting as VLAN) constituting a department; say 'Marketing Dept'. Several such departments like 'Management', 'Accounts', 'Sales' and 'Human Resources' are created forming a Local Area Network as shown in Fig 5.1. Thus, a network is created through which secure communication can be done.

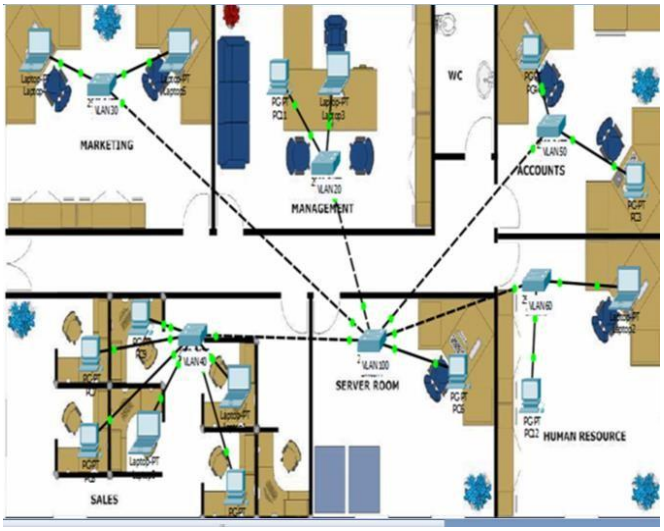

Fig 5.2: VLAN implemented LAN window.

Cisco packet tracer tool designs, builds and configures network with drag-and-drop devices providing valuable hands-on experience that can be applied in the classroom and on the job. It supports the majority of protocols and technologies taught in several networking academy courses.

We begin with logging into packet tracer. Using drag and drop tool, we obtain required number of PCs, Switches and connect them and setup the LAN as shown in Fig 5.2. We

configure IP addresses for all PC's and Switches, a snapshot of ranges of different PCs of different department is shown in Fig 5.3(a) and Fig 5.3(b).

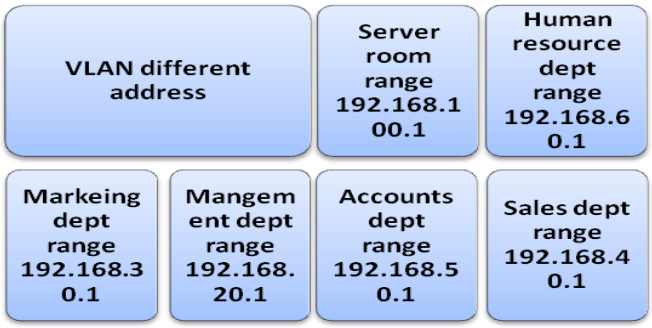

Fig 5.3(a): IP address of VLAN.

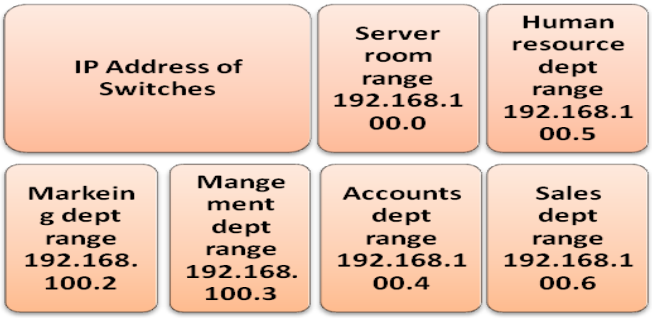

Fig 5.3(b): IP address of Switches.

Thus an infrastructure has been setup.

The IP address of one of PC of Marketing Dept. is 192.168.30.1, and IP address of another PC in same department is 192.168.30.2. The IP address of Management Dept. is 192.168.20.1; the connectivity status among the PC's of same department and of different department.

The IP address of Accounts Dept. is 192.168.50.1; the IP address of HR Dept. is 192.168.60.1; the connectivity status among the PC of Marketing department and of different department. The IP address of Server room is 192.168.100.1; and the IP address of Sales Dept. is 192.168.40.1; the connectivity status among the PC of Marketing department and of different department.

The IP address given to Marketing Dept. Switch is 192.168.100.2; Even though switch is in same department, the PC of marketing department will not be able to form connection with the switch because of security purpose; this type of configuration has been setup. There will be fail in connectivity. This type of connectivity is not only limited to marketing department

the same state is done for rest of the department also. The PCs connected in the same department can communicate with each other but fails to communicate with PCs of other department and even cannot ping with the switches.

To provide security, only PC in the server room has the accessibility to switches of all the departments, the switch IP addresses are shown in Fig 5.3 and the connectivity from server room PC to switches of other department. The PC in server room has accessibility to different switches; telnet is remotely accessing the switches, telnet into switch of marketing department, management department, accounts department and human sales department.

Commands

switch > en

To go from user exec mode to privileged exec mode, en=enable

switch > configure terminal

For configuration of switches we need to go from user exec mode to global configuration mod and the command is as shown below

1. Hostname

switch < config >#hostname

switch < config > exit //to come out of the terminal

2. Logon banner

switch < config > #Banner motd& Welcome to____Department *switch < config > exit*

3. Console Password

switch < config > #line con 0 switch < config_line> #password switch < config_line> login

switch < config_line> exit

// Passwords for all the Departments are taken as follows: Marketing Department market Management Department management Accounts Department accounts Human Resources Department hr

Sales Department sales

4. Telnet

switch < config > # line vty 0 switch < config_line> #login

switch < config_line> password ABHI switch < config_line> exit

5. Management IP address for switch

switch < config > #int vlan 100

switch < config_if> #ip address 192.168.100.2 switch < config_if> #no shutdown

switch < config_if> exit

// IP Addresses

192.168.100.2 Marketing Dept.

192.168.100.3 Management Dept.

192.168.100.4 Accounts Dept.

192.168.100.5 HR Dept.

192.168.100.6 Sales Dept.

6. Enable Password

switch < config > #enable password allow switch < config > exit.

VI. RESULTS

The command line interface of marketing switch is shown in Fig 6.1. Now using telnet we can make any changes in the marketing department switch and the same changes will be seen in switch for example we have changed the hostname from server room PC and change is seen in switch as shown in Fig 6.2. The changes is not only limited to hostname we can change the console, telnet and enable password, logon banner etc. from the switch.

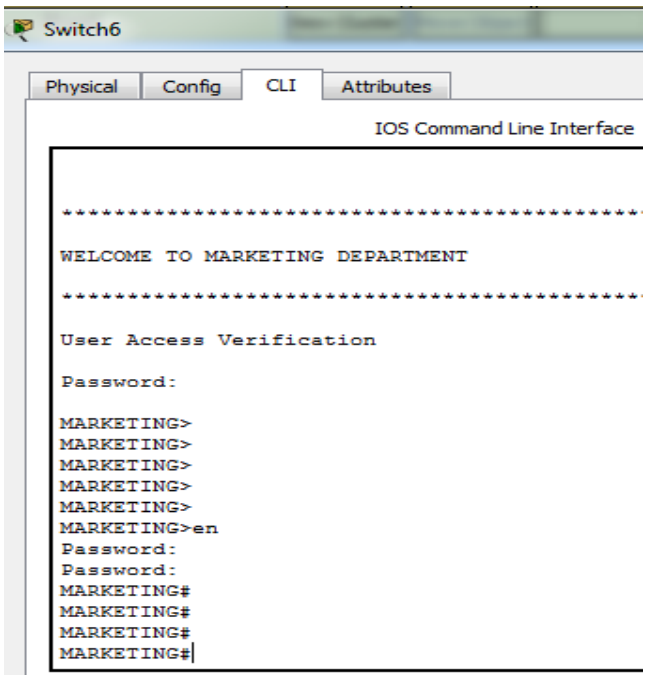

Fig 6.1: Command line interface of marketing switch.

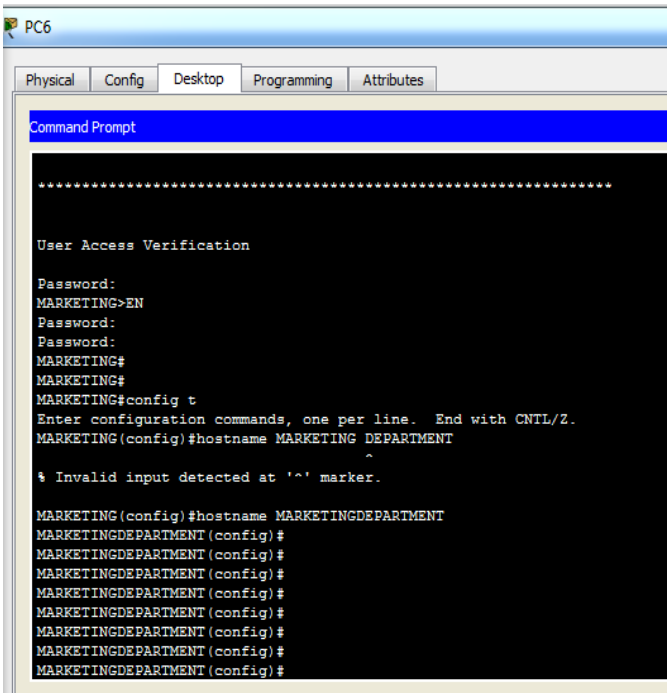

Fig 6.2: Change in hostname using TELNET.

CONCLUSION

There is a lack of security mechanism which makes the department network vulnerable to different kinds of threats and attacks. For providing better security to department network we can use security mechanism by setting up a network between users through which they can communicate with each other. Department networks provide better understanding and illustrate working of VLANs. VLANs enable administrators to limit the scope of broadcast traffic and network-wide flooding, to reduce network overhead and enhance both privacy and security. They provide an extra measure of security. People belonging to the same group can send broadcast message with the guaranteed assurance that users in other groups will not receive these messages through Telnet command which is an underlying TCP/IP protocol for accessing remote computers.

REFERENCES

1. Kartik Pandya (2013), "Network Structure or Topology", Volume 1, Issue 2, July 2013 in International Journal of Research in Computer Science and Management Studies.
2. Honni and Johanes Fernades Andry (2016), "Design and Simulation VLAN Using Cisco Packet Tracer: A case study.
3. Abdul Hameed, Adnan Noor Mian "Finding efficient VLAN topology for better broadcast containment".

4. Garima Jain Pai, Nasreen, Noorani, Nisha, Kiran, Sourabh Sharma (2015),"Designing and Simulation of Topology Network is using Packet Tracer", Volume 2, Issue 2, May 2015 in International Research of Engineering and Technology.
5. Chan Wai Kok, M. Salim Beg "Simple IP Subnet VLAN Implementation".
6. G. P. Pal and S. Pal, "Virtual Local Area Network (VLAN)", volume 1, Issue 10 in International Journal of Scientific Research Engineering and Technology.
7. Janitor, Jakab, F. Kniewald, K., "Visual Learning Tools for Teaching/Learning Computer Networks: Cisco Networking Academy and Packet Tracer," Networking and Services (ICNS), 2010 Sixth International Conference on, vol., no., pp.351,355, 7-13 March 2010.
8. Li Xinzhan and Cheng Chuanqing "Discuss on VLAN stacking in Packet Network". International Symposium on Intelligent Ubiquitous Computing and Education 2009.