Project Title: LAN Switching and Security

Group ID: 17

Group Members and Student IDs:

Arushi Talwar (300103561)
Chandana Gowragondanahalli Partha (300134265)
Kavitha Ashwathnarayan (300140526)
Sneh Sneh (300120108)

GitHub Link: https://github.com/ccnproject/LAN.git

CONTENT

ABSTRACT

The pervasiveness of wireless communications introduces new security challenges. It is imperative that the security of wireless connections is intact so that no information is leaked to anyone but the intended receiver. Our project demonstrates the design of the routing for networking using LAN. It also illustrates how the protection of the confidential data transferred is done. Furthermore, it deploys the knowledge of Switching VLAN's, VLAN Trucking Protocol, Switch Port securities and secure Shell (SSH) protocol (whatever technologies are used) various protocols, various interfaces and their serial communication and how they are communicating with each other.

1.INTRODUCTION

This chapter gives the brief introduction about the LAN and interprets the goals and main objective of the project.

1.1 Overview

LAN switching is a form of packet switching in which the data packets are transferred from one computer to another over a network. Switching technologies are vital to network design, as these technologies permit the traffic to be sent only where it is required; in most of the cases, making use of fast, hardware-based methods. LAN switching technology helps to improve the overall efficiency of local area networks and address the existing bandwidth issues. LAN's are easy to establish, but complex to maintain [1]. For LAN's, different networking techniques are used to implement and maintain.

LAN switching includes mainly 4 types of switching [2-4]. They are as follows:

1. **Layer 2 Switching**: It is a hardware-based switching which makes use of the (media access control (MAC) addresses.

2. **Layer 3 switching:** Provides the functionality as router. Offers highly efficient packet switching High speed data transmission with low latency.

3. Layer 4 switching: An enhanced version of layer 3 switching, switching uses hardware-based switching which implies that a quality of service (QoS) may be defined for every user.

4. Multi-Layer Switching: Multi-layer switching (MLS) provides low latency and high performance. All three-layer switching (2, 3 and 4) are combined in MLS.

1.2 OBJECTIVE AND GOAL

1.2.1 OBJECTIVE

The problems that we come across in the recent wireless communication networking accounts for the following:

1. Slow network
2. Insecure network
3. Increased traffic
4. Wastage of IP address

These are the few predominant issues that outlines the purpose of our project. These above-mentioned extremities are kept in mind in designing our prototype network.

1.2.2 GOAL OF THE PROJECT

Switching technologies are vital for network design. This technology permits the traffic to be sent only where it is required by making use of the fastest hardware-based methods.

The essence of the amateur design is to provide:

- Efficient and high-speed data transmission with low latency.
- Secured network with higher performance.
- Time reduction.
- Accurate tracking and monitoring.
- Secure remote access to network devices
- Improves overall efficiency of LAN's and address the existing bandwidth issues.
- Encrypted network.

1.2.3 TOOL USED FOR THE IMPLEMENTATION

CISCO Packet Tracer: It is a cross platform visual simulation tool which is designed by CISCO systems. This allows user to create the network topologies and imitates the modern computer networks and protocols. Our design is developed, tested and simulated on the same software.

2. TECHNOLOGIES USED

This chapter gives the brief introduction about technologies used to implement

2.1 VIRTUAL LOCAL AREA NETWORK (VLAN)

A Local Area Network (LAN) is defined as an interconnection of network computers within a limited area. LAN are broadcast domain that means if a user broadcasts an information on one LAN, the broadcast will be received by every other user on the LAN. The main disadvantage is routers, it takes more time to process incoming data compared to a bridge or a switch. A solution was developed to using routers to contain broadcast traffic called Virtual Local Area Networks (VLAN's).[5]

How VLAN's work

VLAN uses explicit tagging to tag the data with a VLAN identifier indicating the VLAN from which the data came, and it also uses implicit tagging to identify the port to which VLAN the data received. Tagging is done based on the port, Media Access Control (MAC) field, source network address or combination of fields. The tagging can be done using the bridge which has an updated database containing a mapping between VLAN’s and the field used for tagging. This type of database is called as filtering database. Bridges maintain the database also make sure that all the bridges have same information in each of their databases. The bridge identifies where the data is to go next. Once it is identified where the data must be sent, then it determines whether the VLAN identifier should be added to the data and sent. If data sent to a device that knows about VLAN implementation, then VLAN identifier is added to the data. If data sent to a device that has no knowledge of VLAN implementation, then data is sent without VLAN identifier. [5]

Advantages of VLAN:

- Security
- Higher Performance
- Cost reduction
- Formation of virtual workgroups
- Simplified administration

2.2VLAN TRUNKING PROTOCOL(VTP)

VLAN trunking protocol (VTP) is a protocol used to carry VLAN information to all switches in a VTP domain. VTP helps to maintain VLAN configuration consistency across the entire network. VTP synchronises VLAN information, there is no necessity to configure VLAN information on each switch within a VTP domain. When there are configuration changes there is some inconsistency arises, which can be minimized by VTP. VTP provides three modes namely, VTP server, VTP client and VTP transparent.[6]

- VTP server provides VTP domain VLAN information to VTP-enabled switches in the same VTP domain and stores the VLAN information for the entire domain and it is responsible for creation, deletion and renaming of the domain.
- VTP client stores the VLAN information when the switch is on and deletes the information when it is switch is reset.
- VTP transparent delivers the VTP advertisements to VTP server and VTP client.[6]

VTP benefits:

- Monitoring and accurate tracking of VLANs
- Maintains configuration consistency across the network.
- VLAN mapping scheme allows the VLAN to be trunked over mixed media
- When new LAN's are added it helps in dynamic reporting

2.3 SWITCH PORT SECURITY

In order to limit the traffic to certain or configured MAC addresses, switch port security feature is used, and it enable configuration to switch ports that helps to monitor and hence limit the traffic.

Why there arises the need to secure the network and the aspects that are taken into consideration in order to provide a reliable communication:

As these days cyber threats are prevailing in the society therefore while dealing with transmission of data switch port security plays paramount role and various aspects that are taken into consideration in this project to provide access only to the authorized users are as follows:

1) The first and foremost is acceptable user policy, this policy broadly categories the kind activities to which the authorization need not be provided for accessing the network and the type of activities for which it is mandatory to provide access.
2) In order to curb the problems of unreliable access to E-mails and attachments, security features are provided to E-mails and attachments via encryption and decryption.
3) In order to prevent the network against threats like worms, Trojan horses and threats security is provided through antivirus policy.
4) To prevent the network from unauthorized user's system is configured with identity policy.
5) To help the employees to safely access the network while they are working outside the office.
6) Password policy is provided to select strong passwords so that the access of unauthorized users can be prevented.[7]

Type of switch port security used in this project:

The software we used for this project is CISCO packet tracer therefore CISCO catalyst switches are used that are basically layer 2 switches. These switches permit administrator configure individual switch ports to provide access to already defined number of source MAC addresses entering the port.

How switch ports are enabled:

In order to enable switch port security single command is used during interfacing that will enable default parameters (the one which are already registered in the router installed in this project).

The commands that are used to provide switch port security are:

Switch (configure) #interface F0/13

Switch (configure-if) #Switch port –security

2.4 SSH PROTOCOL

SSH Stands for secure shell security protocol which is basically a cryptographic network protocol and its purpose is to provide secure remote access connection to network devices over an unsecured network. In this project SSH protocol is used in a client-server architecture that provide a reliable connection between SSH client and SSH server. In order to encrypt the information with SSH protocols two different versions are used that is SSH version 1 and SSH version 2.[8]

SSH version 1: This version was designed with the goal of protecting the network from password sniffing attacks. This version of SSH protocol was the replacement of the earlier used unauthenticated protocols like FTP and TELNET.

SSH version 2: It use more enhanced security encryption algorithm. The benefit of version 2 over first version is that it provides flexibility to the network as it has the ability to run multifarious shell sessions on the one SSH connection.[8]

Benefits of SSH Protocol:

1) SSH provides encryption for data transfer thereby prevents attackers from accessing authentic user information like passwords.
2) With the assistance of SSH, dedicated servers can be managed remotely**.** In addition to that monitor logs, start and stop services can be managed meticulously.
3) It is far better platform as compare to the web-based control panel as it is the most secure method to manage the server.

Working of switch port security by using SSH protocol:

The routers act as the central and main entity to provide switch port security. Routers already have the IP address of all the authorized devices. Authorized devices are the one that have the access to the network. The functioning of the router can be broadly categorized in to two different ways based on the type of the device accessing the network. When any device try to connect to the network first of all the routers through the multilayer sub switches will check the identity of the device by running the sticky command and in case the IP address of the device matches with the IP address already stored in the router then the access will be provided to device for establishing connection to the particular device. In case the device is unauthorized that is the one whose IP address is not stored in the router then the connection will not be provided to that device and the device of that user will automatically be shut down within the already defined time duration. [9-10]

3. PROJECT DESCRIPTION

This chapter describe about the implentation of the project.

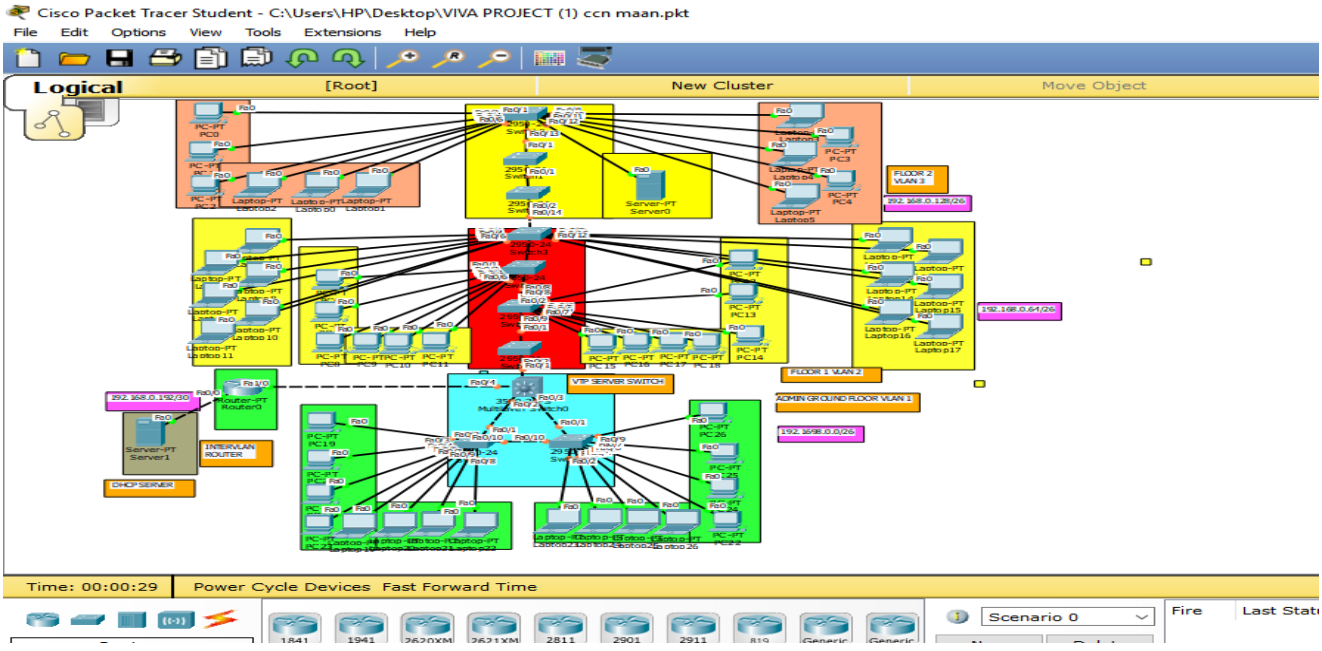

Figure 1: Design of the routing network

First, the server has been put up in which we have created 3 pools for the 3 floors. Server is assigning IP addresses to 3 different VLAN devices by DHCP (Dynamic Host Configuration Protocol). Domain name server resolves domain names to IP addresses.

We can see that there are three pools as shown in Figure 1, so we need at least 3 different range of IP addresses, thereby we have done subnetting starting from 192.168.0.0/26, which creates a space for 256 devices. Starting IP address is from 192.168.0.1 up till 192.168.0.254.

Next comes the function of router in which we have created 3 sub interfaces. IP addresses provided to these interfaces act as gateways. Encapsulation applied in the coding of router acts as an intermediate between 2 VLANs.

Multilayer switches are the main switch in which we have created 3 VLANs so that we do not have to create VLANs in each of the switches manually. This is possible through VTP (Virtual Trunking Protocol). In multilayer switch, we have performed trunking that allows communication to take place between devices enclosed in a network. Multilayer switch acts as VTP server whereas all other switches act as VP clients.

For this reason, only we have made 3 VLANs in a multilayer switch which automatically creates 3 VLANs in rest of the switches.

For security concerns, we have enabled switch port security which does not let any unauthorised PC to access the network and hack it.

In our project, we have configured telnet as well that allows remote access to the all the devices present in the network. We can see that there are three pools, so we need at least 3 different range of IP addresses thereby we have done subnetting starting from 192.168.0.0/26 which creates a space for 256 devices. Starting IP address is from 192.168.0.1 up till 192.168.0.254[6].

4.CONCLUSION

Winding up the whole project following were the main aspects that were taken into consideration in order to meticulously mange and integrate multifarious platforms and entities involved in the project.

1) In order to main connectivity throughout the time duration when the connection is maintained in the network to achieve the target of end to end delivery without any loss of data all the routers and switches are configured properly with a basic router configuration.
2) Based on the design requirements all the routing features are configured correctly.
3) Switches are configured appropriately with a security configuration.
4) In order to be sure about the connectivity troubleshooting is provided between all the devices.

5.FUTURE SCOPE

- Acceptable use policy, to specify what types of network activities are allowed and which ones are prohibited
- E-mail and communications activities, to help minimize problems from e-mails and attachments
- Antivirus policy, to help protect the network against threats like viruses, worms, and Trojan horses
- Identity policy, to help safeguard the network from unauthorized users
- Password policy, to help employees select strong passwords and protect them
- Encryption policy, to provide guidance on using encryption technology to protect network data
- Remote access policy, to help employees safely access the network when working outside the office

6.REFERENCES

[1] IEEE 802 LAN/MAN Standards Committee. (2009). Wireless LAN media access control (MAC) and physical layer (PHY) specifications. *http://standards. ieee. org/getieee802/*.

[2] Kim, Y. J., & Suh, Y. J. (2005, May). An efficient rate switching scheme for IEEE 802.11 wireless LANs. In *2005 IEEE 61st Vehicular Technology Conference* (Vol. 4, pp. 2364-2368). IEEE.

[3] Sahin, C., Katz, B., & Dandekar, K. R. (2016, January). Secure and robust symmetric key generation using physical layer techniques under various wireless environments. In *2016 IEEE Radio and Wireless Symposium (RWS)* (pp. 211-214). IEEE.

[4] Furukawa, H., Wada, N., Harai, H., Naruse, M., Otsuki, H., Katsumoto, M., ... & Shimizu, H. (2007, May). Novel layer-3 IP packet switching between 10 Gbps Ethernet and 80 Gbps optical packet-switched networks. In *2007 Workshop on High Performance Switching and Routing* (pp. 1-6). IEEE.

[5] Hein, M., & Griffiths, D. (1997). *Switching technology in the local network: from LAN to switched LAN to virtual LAN*. Thomson Executive Pr.

[6]https://www.researchgate.net/institution/NIIT_University/department/PhD_Program_in_Electronics_and_Communication_Engineering_ECE. NIIT Research-gate ECE.

[7] Buerger, D. J. (1995). ``Virtual LAN cost savings will stay virtual until networking's next era,". *Network World, March*.

[8] Metagar, S. M., Hiregouder, R. G., & Sing, H. R. (2013). Virtual Local Area Network Technology.

[9] Mahajan, U., Mellacheruvu, R., & Jain, P. (2009). *U.S. Patent No. 7,606,177*. Washington, DC: U.S. Patent and Trademark Office.

[10] Mittal, A., & Chen, H. P. (2016). *U.S. Patent No. 9,363,207*. Washington, DC: U.S. Patent and Trademark Office.