

**YEAR: 2018-19**

COMPUTER NETWORKS

(CS435P)

**MINI PROJECT REPORT**

On

**ENTERPRISE NETWORK DESIGN**

By

**TANISHA MANOJ (1760440)**

**BHAVYA (1760436)**

Of

**4-BTCS-C**

Under the Guidance of

**Mr. Praveen Kulkarni**

**Department of Computer Science and Engineering**

**DECLARATION**

We certify that this project is entirely our own work, except where we have given fully documented references to the work of others, and that the material in this assignment has not previously been submitted for assessment in any formal course of study.

We assert the statements made and conclusions drawn are an outcome of our project work. We further certify that

* The work contained in the report is original and has been done by us under the general supervision of our supervisor.
* The work has not been submitted to any other Institution for any other degree/diploma/certificate in this university or any other University of India or abroad.
* We have followed the guidelines provided by the university in writing the report.
* Whenever we have used materials (data, theoretical analysis, and text) from other sources, we have given due credit to them in the text of the report and giving their details in the references.

NAME: TANISHA MANOJ NAME: BHAVYA

SIGNATURE: SIGNATURE:

COURSE CODE: CS 435P

COURSE TITLE: COMPUTER NETWORKS

DATE: 7th March 2019

**ACKNOWLEDGEMENT**

We are grateful to our university, which helped us in many ways. Our sincere thanks to **FATHER Dr BENNY THOMAS** the director of our university and to **FATHER ANTONY PUTHUSSERY the campus coordinator** for permitting us to develop this project. We shall thank our head of department

**Dr BALACHANDRAN K**, who has been a source of inspiration throughout our project work. We are highly thankful and indebted to our project guide

**Mr. PRAVEEN KULKARNI**, Asst.Professor, computer science department.

We are also thankful to everyone who all supported us, for that we have completed our assignment effectively and moreover on time. They gave us many helpful comments which helped us a lot in preparing this project.

Last but not the least we also thank to all non-teaching staff of the university for their support in successful completion of our project.

BHAVYA

TANISHA MANOJ

**ABSTRACT**

Network security is one of the most important requirements today. Networks are extremely vulnerable and face the major issue of security threat and misuse of information. In order to secure the network, many mechanisms are used in networking. In this project, virtual LAN, port security of the switches, inter VLAN routing and the access control list in router have been used. We used cisco packet tracer to implement the above simulation. This technique which combines the above-mentioned concepts is seen to significantly enhance the security of the network.

**INDEX**

1. INTRODUCTION

Overview

Advantage

Disadvantage

1. DESIGN

Protocols Used

Servers Used

1. IMPLEMENTATION

Topology

Description

1. CONCLUSION
2. BIBLIOGRAPHY

**INTRODUCTION**

Unauthorized access is one of the major threats in a network. Information and data can be misused and manipulated by the unauthorized user causing disruption and chaos in the maintenance and smooth functioning of the existing network.

We have used the concepts of Virtual Network, Port Security and Access Control List in order to try and prevent such unauthenticated and unauthorized access.

The advantages include:

1. Number of networks can be created on switch using VLAN
2. If any unauthorized PC or laptop try to connect with the switch, then the port will be turn off and hence no further communication can take place for this unauthorized PC, laptop.
3. Unauthorized user will not be able to communicate with other laptops as its MAC address has not been included in the switch.
4. Router works as a firewall.

The disadvantages include:

1. If you fake the MAC address to the host, you are in
2. Insider/outsider threat is great since physical security to equipment is not well controlled in many organizations
3. Have to take into account failover scenarios or you can DoS yourself
4. Hard to manage large number of switch ports to ensure they are configured correctly at all times

**DESIGN**

Protocols Used: HTTPS (Hyper Text Transfer Protocol Secure)

It is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or, formerly, its predecessor, Secure Sockets Layer (SSL). The protocol is therefore also often referred to as HTTP over TLS, or HTTP over SSL. It protects against man-in-the-middle attacks. The bidirectional encryption of communications between a client and server protects against eavesdropping and tampering of the communication.

Servers Used: 1. DNS (Domain Name System/Server)

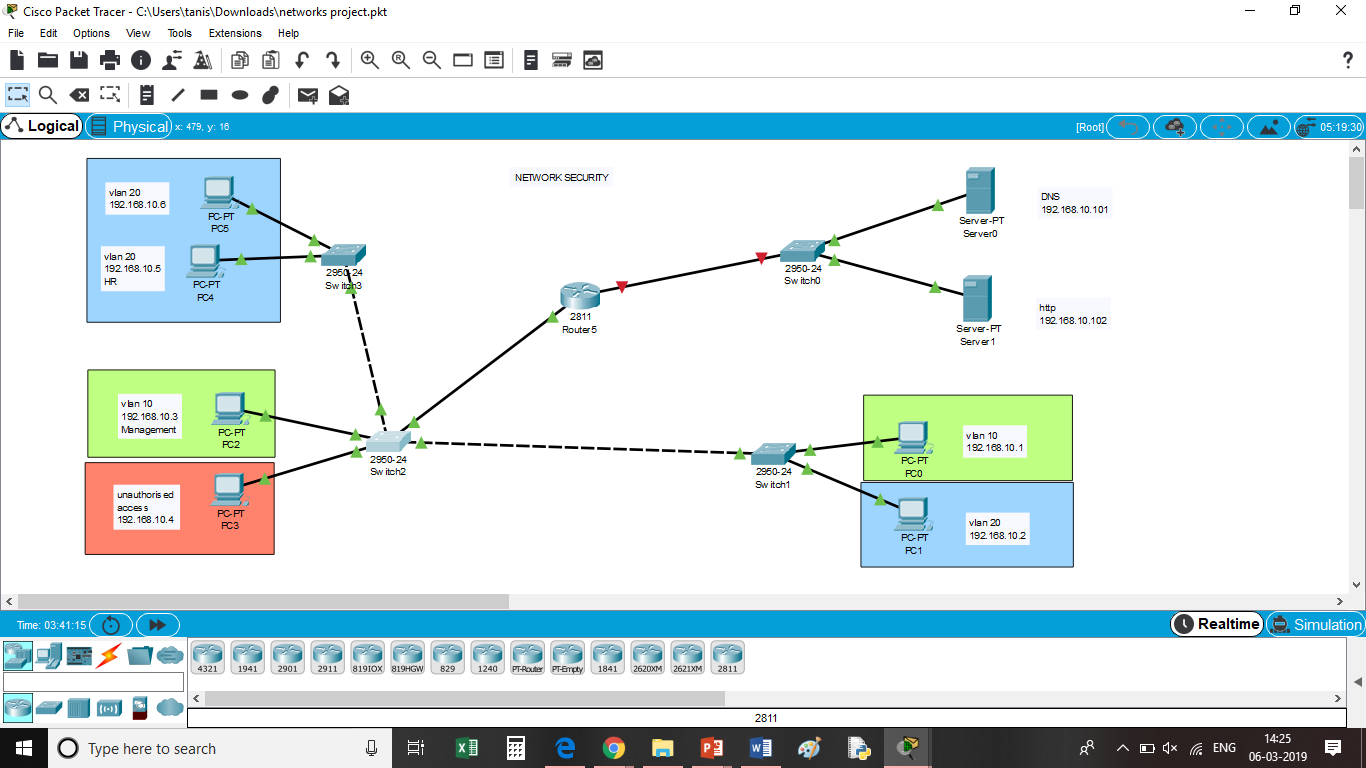
DNS server is a computer server that contains a database of public IP addresses and their associated hostnames.DNS servers run special software and communicate with each other using special protocols.

2. HTTP Server (Hypertext Transfer Protocol Server)

The primary function of a web server is to store, process and deliver web pages to clients. The communication between client and server takes place using the Hypertext Transfer Protocol (HTTP). Pages delivered are most frequently HTML documents, which may include images, style sheets and scripts in addition to the text content.

**IMPLEMENTATION**

Topology:



|  |  |
| --- | --- |
| **Device** | **Quantity** |
| PCs | 6 |
| Switch | 3 |
| Router | 1 |
| DNS | 1 |
| HTTP Server | 1 |

Description:

1. Drag and drop the devices as shown in fig 1.1. Connect them using Copper Straight-Through wires.
2. Configure their IP Addresses as shown against each PC.
3. Configure the Router using the code given in fig 1.2.
4. Create VLANs and assign to respective switches as shown in fig 1.3.
5. Configure the DNS Server and turn the DNS Service on.
6. Configure the Web Server and turn http and https on.
7. Enter the commands in CLI for port security for the switch as shown in fig 1.4.
8. Configure ACL on the router.

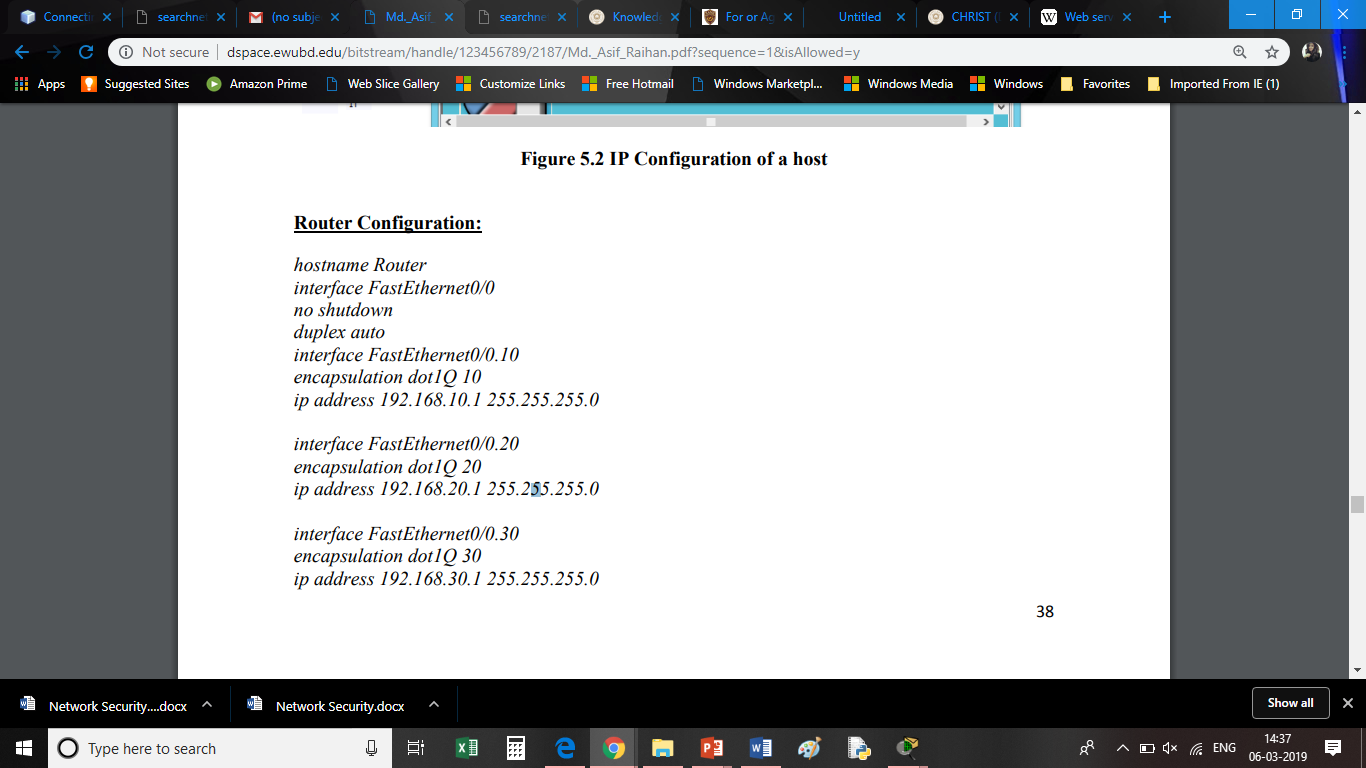


Fig 1.1



Fig 1.2

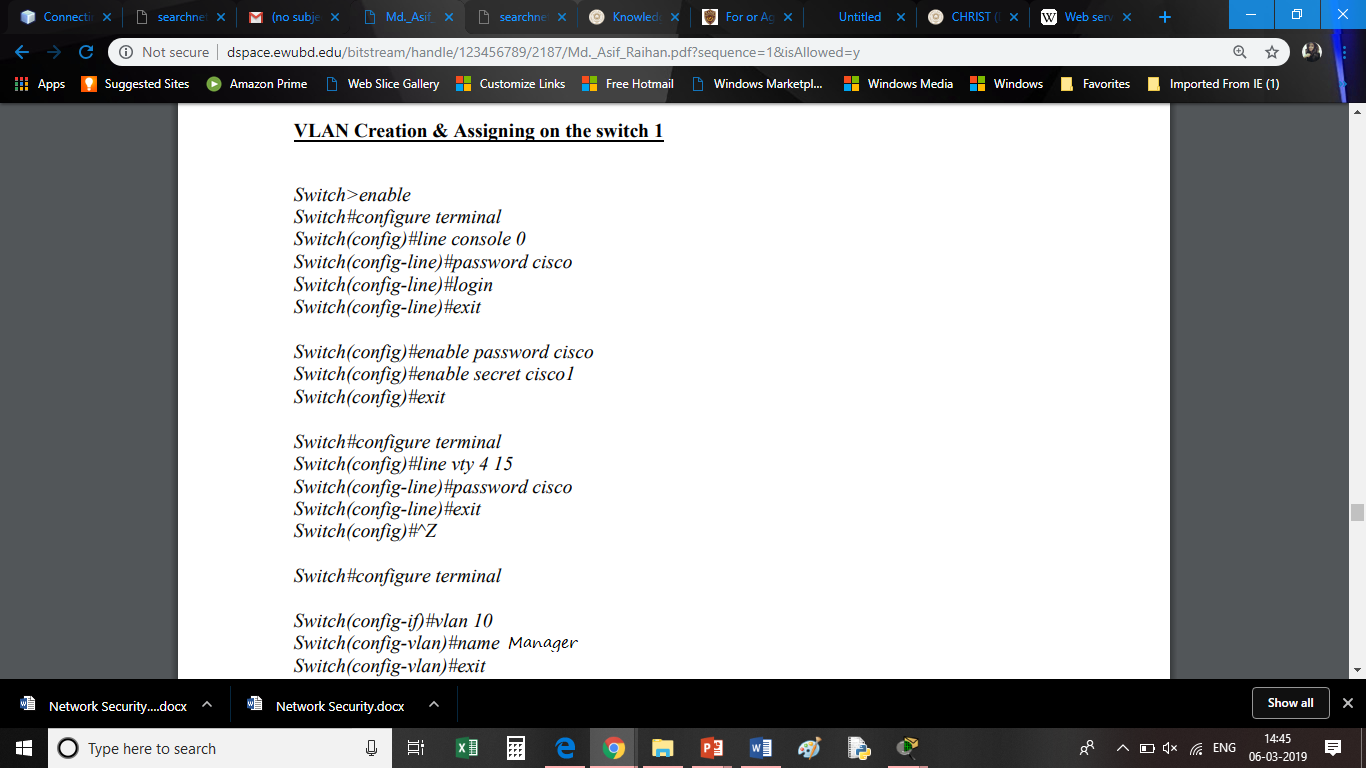


Fig 1.3

**CONCLUSION**

In this project, we see that the use of virtual networks, port security and access control lists helps in reducing if not fully eliminating the threats faced by networks due to unauthorized access. Asking of password and terminating the process of sending data if the sender is found to be an unauthenticated user has shown significant reduction in the risk of misuse and manipulation of information. The idea is to try and curb such unauthorized access and build on working towards a better and more secure model for networks in the future. This mini project is just a primitive model to show the concept and working and may be applied to big time networks and agencies with an improvised version.