

CHAPTER 1
INTRODUCTION

1.1 INTRODUCTION:

With the increasing reliance on technology and the internet in today's world, network security has become a critical aspect for colleges and universities. The sensitive and confidential information that these institutions handle requires maximum protection from cyber threats. This project aims to implement VLAN and port security measures to enhance the security of the college network.

The VLAN implementation involves the segregation of the network into logical sub-networks, where users with similar security requirements can be grouped together. This limits unauthorized access to data and reduces the attack surface available to hackers. Port security, on the other hand, involves the control of access to network ports by specific devices. Only authorized devices are allowed to access the network ports, thereby reducing the likelihood of a malicious attack or unauthorized access.

This project will involve the implementation of VLANs and port security measures across the college network, from the core switches to the end-user devices. The implementation will be done using appropriate network devices and protocols, while ensuring that the network performance is not adversely affected. The project will also involve training and awareness programs for the college staff and students, to ensure that they understand the importance of network security and adhere to the established policies and procedures.

The overall goal of this project is to provide a secure and resilient network infrastructure to the college, which will enable the efficient and effective utilization of technology and the internet for teaching, learning, and research. By the end of the project, the college network will be better prepared to handle cyber threats and attacks, minimizing the risks of data breaches and other security incidents.

1.2 OBJECTIVE OF OUR PROJECT:

1. To create VLANs for different departments within the college.
2. To ensure that only authorized devices connect to a particular VLAN.
3. To configure port security to restrict access to a particular port.
4. To segment the college network into multiple VLANs for different user groups, departments, and services.
5. To implement VLAN access control policies to control network traffic, prevent unauthorized access, and minimize the risk of attacks.

1.3 SYSTEM STUDY

As an AI language model, I can provide a general overview of how VLANs and port security can be used to improve network security in college settings, along with a suggestion on how to simulate this setup using Cisco Packet Tracer.

VLANs (Virtual LANs) and port security are widely used in college network environments to segregate network traffic and secure network access. VLANs allow administrators to partition their network into separate broadcast domains, which limits the ability of attackers to intercept sensitive data flowing between devices. On the other hand, port security settings can prevent unauthorized devices from connecting to the network, ensuring that only authorized devices can access the resources available on the network.

To simulate VLAN and port security settings using Cisco Packet Tracer, you can create a network topology in the software that reflects a typical college setting. The network will consist of multiple devices such as switches, routers, servers, and workstations. Devices will be connected to switches using Ethernet cables, and switches connected to one another to form a network. The following steps can be taken to implement VLANs and port security:

1. Create VLANs – create separate VLANs for different departments and user groups. For example, you can create a VLAN for finance, another for students, another for faculty, etc.

2. Assign Ports to VLANs – assign ports on switches to the appropriate VLANs. Configure the switch ports to access or trunk mode, depending on the needs of the device connected to the port.
3. Enable Port Security – configure port security settings such as static MAC addresses, violation actions, and maximum number of allowed MAC addresses per port. This will prevent unauthorized access to the network.
4. Test the Network – Once the configuration is complete, test the network by connecting authorized devices to the ports and verifying connectivity. Attempt to connect unauthorized devices to the network and ensure that port security settings prevent access.

In conclusion, VLANs and port security are powerful tools that can improve the security of a college network. Cisco Packet Tracer is an excellent tool for simulating VLAN and port security settings in a safe and controlled environment. With this setup, network administrators can protect their network from unauthorized access and ensure that only authorized devices have access to network resources.

1.4 LITERATURE SURVEY

There are different types of VLANs: Static VLANs and Dynamic VLANs. Static VLANs are configured by network administrators, and devices are placed into specific VLANs manually. Dynamic VLANs, on the other hand, are created dynamically by software without the need for manual configuration.

Cisco Packet Tracer is a simulation tool designed by Cisco Systems that enables network administrators to design, configure, and troubleshoot networking solutions without the need for physical hardware. Cisco Packet Tracer is a valuable tool for students and network administrators to learn, implement and test networks, and prepare for Cisco certification exams. With Cisco Packet Tracer, network administrators can create and test different network topologies, including VLAN and Port Security.

CHAPTER 2

SYSTEM ANALYSIS

2.1 SYSTEM ANALYSIS

SYSTEM REQUIREMENTS:

To implement VLAN and port security, our system should meet the following requirements:

1. Network devices - We need routers, switches, and computers to create the network topology.
2. Software - We will use Cisco Packet Tracer software to simulate the network.
3. VLAN configuration - We will need to configure VLANs to segment the network and prevent unauthorized access.
4. Port security - We will need to set up port security rules to restrict access to the network based on the MAC address of the device.

2.1.1 Design of Network Topology:

The network topology for college network security using VLAN and port security will consist of the following components:

1. Core Switch - This will be the central switch that connects all the other switches and devices in the network. It will be configured with VLANs to segment the network.
2. Distribution Switches - These switches will be located in different parts of the college campus, and they will connect to the core switch via trunk links. Each distribution switch will also have its own VLANs to segregate the network.
3. Access Switches - These switches will be connected to the distribution switches and will provide network access to the end devices like computers, printers, and servers.
4. End Devices - These are the devices that will be connected to the access switches, including student and faculty computers, servers, printers, etc.

2.1.2 Configuration of VLAN:

To configure VLAN, we will follow the steps below:

1. Log in to the Cisco Packet Tracer software and create the network topology as per the design.
2. Create VLANs on the core switch using the command 'vlan [vlan number]' in the global configuration mode.
3. Assign the ports to different VLANs using the command 'switchport access vlan [vlan number]' in the interface configuration mode.
4. Configure trunk links between the core switch and distribution switches using the command 'switch port mode trunk' in the interface configuration mode.
5. Create VLANs on the distribution switches and assign the ports to different VLANs using the commands mentioned earlier.
6. Finally, configure access switches and end devices to connect to the VLANs on the distribution switches.

2.1.3 Configuration of Port Security:

Port security is an essential component of network security, which allows only authorized devices to connect to the network. To configure port security, we will use the following steps:

1. Identify the MAC addresses of authorized devices that need access to the network.
2. Configure the port security settings on the access switches using the command 'switchport port-security'.
3. Set the maximum number of MAC addresses allowed on the port using the command 'switchport port-security maximum [number]'.
4. Configure the MAC addresses on the port using the command 'switchport port-security mac-address [mac address]'.

5. Set the violation mode using the command 'switchport port-security violation [mode]'.
6. Finally, test the configuration by connecting unauthorized devices to the network and check if they are denied access.

2.2 SYSTEM SPECIFICATION:

2.2.1 HARDWARE REQUIREMENTS:

- Computer with Cisco packet tracer software installed
- Router and switch equipment

2.2.2 SOFTWARE REQUIREMENTS:

- Cisco packet tracer software
- Windows operating system

2.2.3 SYSTEM FEATURES:

- VLAN configuration to secure college network
- Port security implementation to prevent unauthorized access
- Switch configuration for port security
- Router configuration for VLAN

System Design: The network system will consist of a router and multiple switches. The router will connect to the campus network and the switches will be connected to the router. The switches will connect to the end devices such as computers, printers, and servers.

VLAN Configuration: The network administrator will configure VLANs to limit the amount of traffic that can flow between departments or groups. VLANs can help prevent security threats such as unauthorized access or network attacks.

Port Security: To prevent unauthorized access to the network, the system will implement port security. Port security enables the network administrator to limit

the number of MAC addresses that can access the network through a particular port.

Switch Configuration: The switches will be configured with port security enabled. This will ensure that only authorized devices can connect to the network. The switch ports will be configured to shut down in case of a security breach or unauthorized access.

Router Configuration: The router will be configured with VLANs enabled to allow communication between departments or groups. The router will also be configured to connect to the Internet, allowing access to the outside world.

CHAPTER 3
PROJECT DESCRIPTION

3.1 PROJECT DESCRIPTION:

The objective of this project is to design and implement a secure network infrastructure for a college campus using VLAN and port security features in Cisco Packet Tracer.

Step 1: Network Design

First, create a network topology in Cisco Packet Tracer that consists of multiple buildings, each with several floors or rooms. The topology will include a core switch and several distribution switches, which will connect to access switches in each building. The access switches will connect to end devices such as computers, printers, and servers.

Step 2: VLAN Configuration

Next, configure VLANs on the switches. Create separate VLANs for students, faculty, and staff with appropriate IP address ranges. Implement VLAN tagging to ensure that network traffic flows only through the designated VLANs.

Step 3: Port Security

Configure port security on the access switches to prevent unauthorized access to the network. Configure the switches to allow only authorized MAC addresses to connect to each port. Also, limit the number of MAC addresses that can connect to each port to prevent MAC address spoofing.

Step 4: Access Control

Implement access control lists (ACLs) on the core switch to restrict access to network resources. Configure ACLs to permit only authorized traffic and block any unauthorized traffic attempting to access the network.

Step 5: Testing and Verification

Finally, test and verify the network infrastructure to ensure that it is functioning properly. Use tools such as ping and trace route to test connectivity between end devices and verify that traffic is flowing only through the designated VLANs.

By following these steps, you can design and implement a secure network infrastructure for a college campus using VLANs and port security features in Cisco Packet Tracer. This project will not only enhance the security of the college network but also provide valuable experience in configuring and managing complex network environments.

3.2 OVERVIEW OF THE PROJECT:

The College Network Security project involves designing and implementing a secure network infrastructure for a college campus using VLAN and port security mechanisms using Cisco Packet Tracer. The project emphasizes the importance of network security in educational institutions and focuses on creating a secure environment to protect sensitive data, personal information, and intellectual property from unauthorized access, theft, and cyber-attacks.

The network infrastructure consists of multiple VLANs, each representing a different department or function of the college (such as student services, faculty, finance, etc.). The VLANs are segregated from each other to prevent unauthorized access and data leakage. Each VLAN has its own subnet and IP address range, ensuring that network traffic is isolated and secure.

Port security is also implemented to prevent unauthorized access to the network devices. This is done by configuring the switch ports to allow only specific MAC addresses to connect to the network. Any unauthorized device attempting to connect to the network is automatically denied access.

In addition, the project includes the implementation of firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to protect the network from external threats, such as malware, viruses, and hacking attempts.

Overall, the College Network Security project provides a comprehensive solution to securing the college network infrastructure using VLAN and port security mechanisms, ensuring a safe and secure educational environment for students and faculty.

3.2.1 CONFIGURATION:

1. VLAN Configuration: VLANs can be used to separate different departments or groups within a college network. By creating separate VLANs, you can ensure that users within each department cannot access resources or data belonging to other departments. This helps keep sensitive information secure.

To configure VLANs in Cisco Packet Tracer, you would need to:

- a. Create VLANs for each department.
 - b. Assign switch ports to VLANs.
 - c. Configure switch VLAN interfaces for inter-VLAN routing.
2. Port Security: Port security can be used to restrict access to the network by limiting the number of MAC addresses that can be learned on each switch port. This prevents unauthorized devices from connecting to the network and accessing sensitive information.

To configure port security in Cisco Packet Tracer, you would need to:

- a. Enable port security on each switch port.
- b. Set the maximum number of MAC addresses that can be learned on each port.
- c. Configure the port security violation action (e.g., shutdown port, restrict access, etc.)

Overall, using a VL

CHAPTER 4
DESIGN AND DEVELOPMENT PROCESS

4.1 DESIGN AND DEVELOPMENT PROCESS:

VLANs (Virtual Local Area Networks) and port security are two essential components in college network security. VLANs allow for network segmentation, which can help prevent cyber attacks from spreading, while port security can prevent unauthorized devices from accessing the network.

To design a college network with VLANs and port security, we would first divide the network into different departments such as administration, academics, library, and dorms. We would then create VLANs for each department, which would be isolated from each other.

For example, the admin VLAN would be assigned to ports that are only accessible to the employees of the administration department. Similarly, the academic VLAN would be assigned to ports that only academic staff and students can access.

Next, we would configure port security on each port in the network. Port security allows us to determine which devices are authorized to access the network, and we can do this by assigning a maximum number of MAC addresses per port.

For example, we could set a limit of one MAC address per port, which would allow only the authorized device to access the network. We could also enable the “sticky” option, which would dynamically learn the MAC address of the first device that connects to the port and allow only that device to access the network in the future.

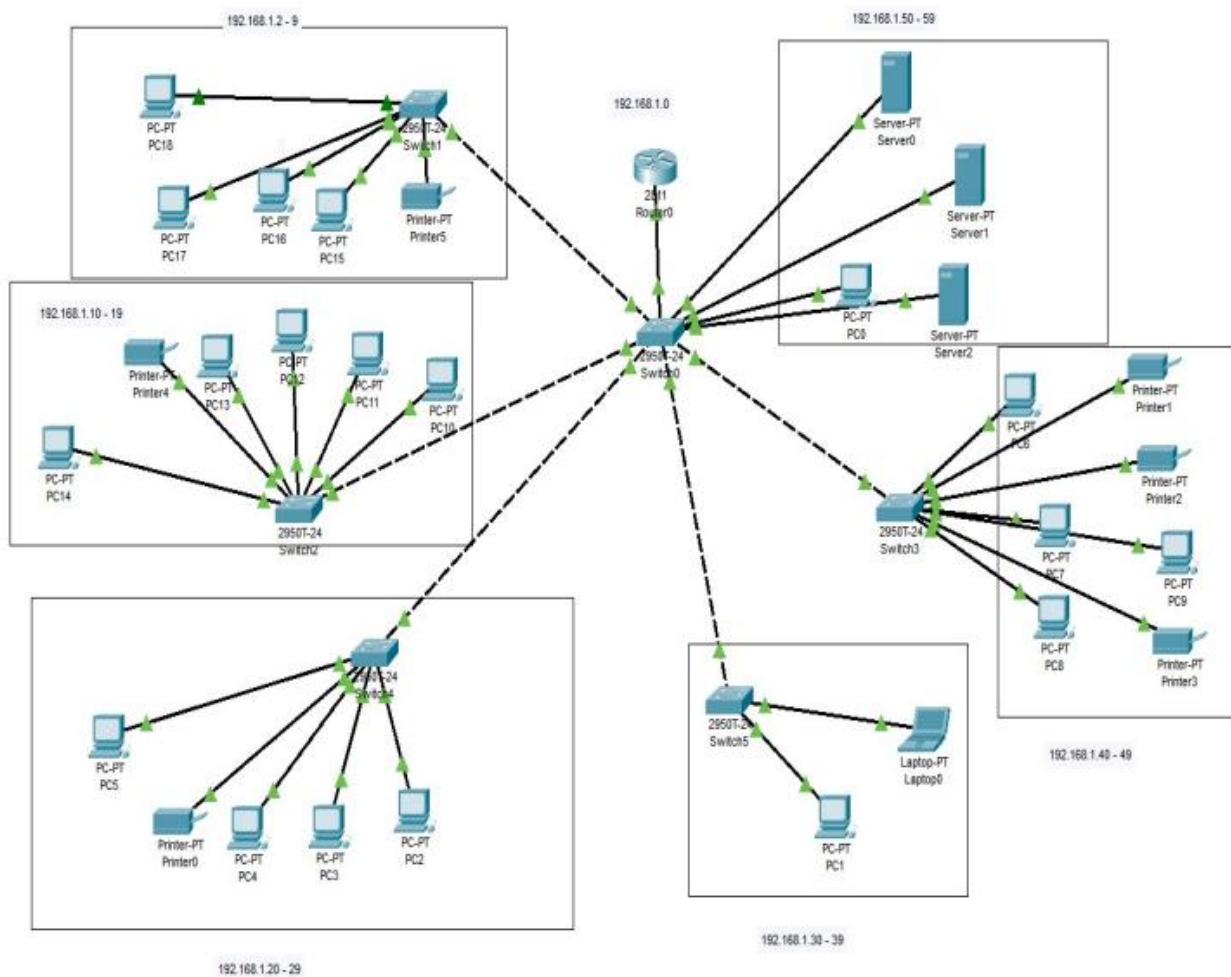
Additionally, we could configure other security features like DHCP snooping to prevent rogue DHCP servers, IP source guard to prevent IP spoofing, and access control lists (ACLs) to restrict network traffic.

To implement this design using Cisco Packet Tracer, we would start by creating VLANs for each department and assigning ports to the VLAN. We would then configure port security on each port by setting a maximum number of MAC addresses and enabling the sticky option.

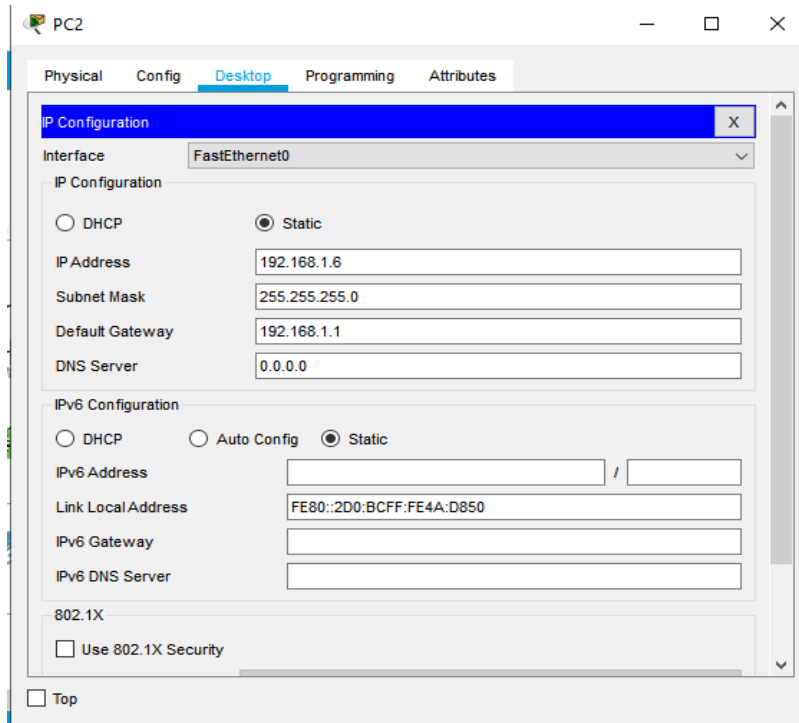
Finally, we would test the network by connecting authorized devices to each port and attempting to connect unauthorized devices to see if they are blocked from accessing the network.

Overall, designing a college network with VLANs and port security can go a long way in ensuring network security and preventing cyber attacks.

4.2 NETWORK TOPOLOGY :



PC CONFIGURATION



PC2

Physical Config **Desktop** Programming Attributes

IP Configuration [X]

Interface: FastEthernet0

IP Configuration

☐ DHCP ☒ Static

IP Address: 192.168.1.6

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.1.1

DNS Server: 0.0.0.0

IPv6 Configuration

☐ DHCP ☐ Auto Config ☒ Static

IPv6 Address: /

Link Local Address: FE80::2D0:BCFF:FE4A:D850

IPv6 Gateway:

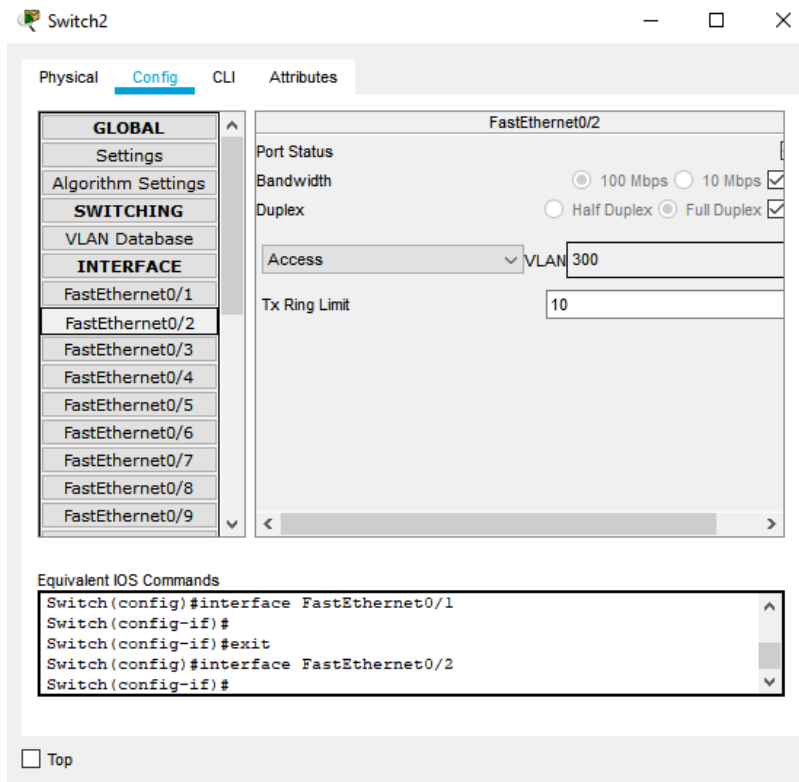
IPv6 DNS Server:

802.1X

☐ Use 802.1X Security

☐ Top

SWITCH CONFIGURATION



Switch2

Physical **Config** CLI Attributes

GLOBAL

Settings

Algorithm Settings

SWITCHING

VLAN Database

INTERFACE

FastEthernet0/1

FastEthernet0/2

FastEthernet0/3

FastEthernet0/4

FastEthernet0/5

FastEthernet0/6

FastEthernet0/7

FastEthernet0/8

FastEthernet0/9

FastEthernet0/2

Port Status

Bandwidth: ☒ 100 Mbps ☐ 10 Mbps

Duplex: ☐ Half Duplex ☒ Full Duplex

Access VLAN: 300

Tx Ring Limit: 10

Equivalent IOS Commands

```
Switch(config)#interface FastEthernet0/1
Switch(config-if)#
Switch(config-if)#exit
Switch(config)#interface FastEthernet0/2
Switch(config-if)#
```

☐ Top

SERVER CONFIGURATION

Server0

Physical Config **Services** Desktop Programming Attributes

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

HTTP

HTTP ☒ On ☐ Off HTTPS ☒ On ☐ Off

File Manager

	File Name	Edit	Delete
1	copyrights.html	(edit)	(delete)
2	cscoplogo177x111.jpg		(delete)
3	helloworld.html	(edit)	(delete)
4	image.html	(edit)	(delete)
5	index.html	(edit)	(delete)

New File Import

☐ Top

ROUTER CONFIGURATION

Router0

Physical **Config** CLI Attributes

GLOBAL

- Settings
- Algorithm Settings

ROUTING

- Static
- RIP

SWITCHING

- VLAN Database

INTERFACE

- FastEthernet0/0
- FastEthernet0/1

FastEthernet0/0

Port Status ☒ On

Bandwidth ☒ 100 Mbps ☐ 10 Mbps ☒ Auto

Duplex ☐ Half Duplex ☒ Full Duplex ☒ Auto

MAC Address 0050.0FA3.B001

IP Configuration

IP Address 192.168.1.1

Subnet Mask 255.255.255.0

Tx Ring Limit 10

Equivalent IOS Commands

```
Router(config)#interface FastEthernet0/0
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface FastEthernet0/0
Router(config-if)#
```

☐ Top

CHAPTER 5

PLANNING

5.1 PLANNING

The purpose of this project is to plan and implement a secure network infrastructure for a college network using VLAN and port security. The network will consist of multiple departments with different levels of access and security needs. The college network will have a core switch and multiple access switches. Cisco Packet Tracer will be used to simulate the network environment.

5.1.2 PROJECT GOALS:

- Create VLANs for different departments of the college
- Configure port security for each switch port
- Implement security policies for each department
- Enforce 802.1X authentication for network access
- Create a secure management network for administrators

5.2 PLAN:

1. Create VLANs for each department- Department A, B, and C will have their own VLANs. The Management VLAN will be created for the administrators.
2. Configure port security on each switch port- MAC address filtering will be used to restrict access to each port. Only authorized devices will be able to connect to the network.
3. Implement security policies for each department- Each department will have different security needs based on their function. Department A, which deals with sensitive data, will require the highest level of security. Department C, which is more public-facing, will require less stringent security policies.
4. Enforce 802.1X authentication for network access- This will further increase the security by requiring users to authenticate themselves before being granted network access.
5. Create a secure management network for administrators- The Management VLAN will be used for administrative tasks. This VLAN will be completely

separate from the rest of the network, and only authorized administrators will be able to access it.

5.3 IMPLEMENTATION:

1. Create VLANs: Using Cisco Packet Tracer, create VLANs for each department, and the Management VLAN.
2. Configure port security: Configure MAC address filtering on each switch port. Use the Cisco IOS command "switchport port-security mac-address [MAC address]" to add MAC addresses to the whitelist. Use "switchport port-security maximum [number]" to limit the number of devices that can connect to each port.
3. Implement security policies: Define security policies based on each department's function. For example, Department A might require encryption for all data transmitted on the network, while Department C might not.
4. Enforce 802.1X authentication: Configure the network to require 802.1X authentication using the Cisco IOS command "authentication port-control auto".
5. Create a secure management network: Create a separate VLAN for the Management network. Use access control lists (ACLs) to limit access to authorized administrators only.

CHAPTER 6
CONCLUSION

CONCLUSION:

After completing the College Network Security project using VLAN and port security in Cisco Packet Tracer, the effectiveness of implementing these security measures is clearly evident. The VLAN segregates the network into separate virtual LANs, which can only be accessed by authorized users. This ensures that only the intended target audience can access the relevant resources and information, resulting in enhanced confidentiality and privacy protection.

Moreover, port security secures the physical ports connecting network devices to prevent unauthorized access. By limiting the number of MAC addresses that can be assigned to a port and allowing only authorized devices to access, this measure prevents rogue devices from gaining access to the network. Additionally, assigning unique VLANs to specific ports improves network management and aids in troubleshooting network issues.

Overall, the implementation of VLAN and port security measures in a college network security system helps in safeguarding critical resources and prevents data breaches. Therefore, implementing these security measures is vital in securing college network infrastructure and maintaining the integrity of sensitive data.

ANNEXURE:

VLAN SECURITY

LABS

show ?

switch > en

switch # configuration terminal

switch (config) # vlan 100

switch (config - vlan) # name labs

switch (config - vlan) # exit

switch (config) # exit

switch #

switch # configuration terminal

switch (config) # interface range fastethernet 0/2 – 0/20

switch (config - if) # switchport mode access

switch (config - if) # switchport access vlan 100

switch (config - if) # exit

switch (config) # exit

switch #

LIBRARY

show ?

switch > en

switch # configuration terminal

switch (config) # vlan 200

switch (config - vlan) # name library


```
switch (config - vlan) # exit
switch (config) # exit
switch #
switch # configuration terminal
switch (config) # interface range fastethernet 0/2 – 0/20
switch (config - if) # switchport mode access
switch (config - if) # switchport access vlan 200
switch (config - if) # exit
switch (config) # exit
switch #
```

HOSTELS

```
show ?
switch > en
switch # configuration terminal
switch (config) # vlan 300
switch (config - vlan) # name hostels
switch (config - vlan) # exit
switch (config) # exit
switch #
switch # configuration terminal
switch (config) # interface range fastethernet 0/2 – 0/20
switch (config - if) # switchport mode access
switch (config - if) # switchport access vlan 300
switch (config - if) # exit
```

switch (config) # exit

switch #

OFFICES

show ?

switch > en

switch # configuration terminal

switch (config) # vlan 400

switch (config - vlan) # name offices

switch (config - vlan) # exit

switch (config) # exit

switch #

switch # configuration terminal

switch (config) # interface range fastethernet 0/2 – 0/20

switch (config - if) # switchport mode access

switch (config - if) # switchport access vlan 400

switch (config - if) # exit

switch (config) # exit

switch #

PORT SECURITY

show ?

switch > en

switch #

switch # configuration terminal

```
switch (config) # interface fastethernet 0/2
switch (config - if) # switchport mode access
switch (config - if) # switchport port-security
switch (config - if) # switchport port-security maximum
switch (config - if) # switchport port-security mac-address sticky
switch (config - if) # switchport port-security violation shutdown
switch (config - if) # exit
switch (config) # exit
switch #
```

BIBLIOGRAPHY:

References:

1. Lammle, T. (2016). CCNA Routing and Switching Complete Study Guide: Exam 100-105, Exam 200-105, Exam 200-125. John Wiley & Sons.
2. Cisco Packet Tracer. (n.d.). Retrieved from <https://www.netacad.com/courses/packet-tracer>
3. Cisco. (2008). VLAN Trunking Protocol (VTP) Version 3. Retrieved from <https://www.cisco.com/c/en/us/support/docs/lan-switching/vtp/118977-configure-vtp-00.html>
4. Cisco. (2018). Configuring VLANs. Retrieved from <https://www.cisco.com/c/en/us/support/docs/lan-switching/vlans/40981-configure-vlan-00.html>
5. Cisco. (2018). Understanding and Configuring VLANs. Retrieved from https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_55_se/configuration/guide/scg_2960/swvlan.html
6. Cisco. (2018). Configuring Port Security. Retrieved from <https://www.cisco.com/c/en/us/support/docs/lan-switching/port-security/21063-configure-port-security-00.html>
7. Cisco. (2018). PPPoE Configuration. Retrieved from <https://www.cisco.com/c/en/us/support/docs/lan-switching/pppoe/29260-pppoeconf-00.html>
8. Cisco. (2018). SNMP Configuration Guide, Cisco IOS Release 15M&T. Retrieved from <https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-mt/snmp-15-mt-book/snmp-config.html>
9. Cisco. (2018). Security Configuration Guide: Access Control Lists, Cisco IOS Release 15M&T. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_acl/configuration/15-mt/sec-data-acl-15-mt-book/sec-access-cntrl-list.html