

**University of Mumbai**

**Design and Implementation of End to End  
Secured Campus Area Network**

Submitted in partial fulfillment of requirements

For the degree of

**Bachelor of Technology**

by

**Harsh Panchal**  
**Roll No: 1813033**

**Kaushal Patil**  
**Roll No: 1813038**

**Shubh Dedhia**  
**Roll No: 1813040**

**Rohit Shah**  
**Roll No: 1813042**

Guide

**Dr. Kiran Ajetroa**



**Department of Electronics and Telecommunication Engineering**  
**K. J. Somaiya College of Engineering, Mumbai-77**  
(Autonomous College Affiliated to University of Mumbai)

**Batch 2018 -2022**

# **K. J. Somaiya College of Engineering, Mumbai-77**

(Autonomous College Affiliated to University of Mumbai)

## **Certificate**

This is to certify that the dissertation report entitled **Design and Implementation of End to End Secured Campus Area Network** is bona fide record of the dissertation work done by Harsh Panchal, Kaushal Patil, Shubh Dedhia, Rohit Shah in the year 2021-22 under the guidance of Dr. Kiran Ajetroa of Department of Electronics and Telecommunication Engineering in partial fulfillment of requirement for the Bachelor of Technology degree in Electronics and Telecommunication Engineering of University of Mumbai.

---

Guide

---

Head of the Department

---

Principal

Date:

Place: Mumbai-77

# **K. J. Somaiya College of Engineering, Mumbai-77**

(Autonomous College Affiliated to University of Mumbai)

## **Certificate of Approval of Examiners**

We certify that this dissertation report entitled **Design and Implementation of End to End Secured Campus Area Network** is bona fide record of project work done by Harsh Panchal, Kaushal Patil, Shubh Dedhia, Rohit Shah.

This project is approved for the award of Bachelor of Technology Degree in Electronics and Telecommunication Engineering of University of Mumbai.

---

Internal Examiner

---

External Examiner

Date:

Place: Mumbai-77

# **K. J. Somaiya College of Engineering, Mumbai-77**

(Autonomous College Affiliated to University of Mumbai)

## **DECLARATION**

We declare that this written thesis submission represents the work done based on our and / or others' ideas with adequately cited and referenced the original source. We also declare that we have adhered to all principles of intellectual property, academic honesty and integrity as we have not misinterpreted or fabricated or falsified any idea/data/fact/source/original work/matter in my submission.

We understand that any violation of the above will be cause for disciplinary action by the college and may evoke the penal action from the sources which have not been properly cited or from whom proper permission is not sought.

<hr/> <b>Signature of the Student</b> <hr/> <hr/> <b>Roll No.</b> <hr/>	<hr/> <b>Signature of the Student</b> <hr/> <hr/> <b>Roll No.</b> <hr/>
<hr/> <b>Signature of the Student</b> <hr/> <hr/> <b>Roll No.</b> <hr/>	<hr/> <b>Signature of the Student</b> <hr/> <hr/> <b>Roll No.</b> <hr/>

**Date:**

**Place: Mumbai-77**

*Dedicated to*  
*My family and friends*

## Abstract

In today's digital world, network security is becoming increasingly important. As a result, having an authorization and authentication system in place is critical for protecting data and systems from cyber threats, identifying new users, monitoring traffic, and approving or blocking unwanted access. It relates to the network system's dependability, as well as the confidentiality, integrity, and availability of data information in the system. The challenge of network security exists at all tiers of the computer network. It is necessary to have a secured network design to protect the campus network from various threats and attacks in order to assure its safety, reliability, and smooth operation.

In our Project we propose campus network design with the help of BUS topology model to explore concepts like VLANs, InterVLANs, OSPFs, ACLs and implementing ASA firewall for internal security of network with the help of Cisco Packet Tracer and GNS3 to make the network more secured. Using this approach, we prevented common internal attacks such as ARP Spoofing, DHCP Snooping, VLAN Hopping, DDOS Attack. Also we measured network performance parameters such as Bandwidth, Throughput, Latency using network monitoring tool i.e. Solarwinds, PRTG.

In future, the scope of the project could be expanded by creating service prevention tool for all common attacks. Also we can create intrusion detection system to protect the campus network.

**Key words:** ACLs (Access Control Lists), Addressing Table (AT), Domain name System (DNS), File Transfer Protocol (FTP), Hypertext Transfer Language (HTTP) Open Shortest Path First (OSPF), Simple Mail Transfer Protocol (SMTP), SSH (Secure Shell), Virtual LAN (VLAN)

# Contents

<b>List of Figures.....</b>	<b>Viii</b>
<b>List of Tables.....</b>	<b>xi</b>
<b>1 Introduction.....</b>	<b>1</b>
1.1 Background.....	1
1.2 Motivation .....	2
1.3 Scope of the project .....	2
1.4 Brief description of project undertaken.....	3
1.5 Organization of the report.....	3
<b>2 Literature Survey.....</b>	<b>4</b>
<b>3 Project design .....</b>	<b>8</b>
3.1 Introduction.....	8
3.2 Problem statement.....	8
3.3 Network Topology.....	9
3.4 Flow Chart.....	10
3.5 Network Description.....	11
<b>4 Methodology.....</b>	<b>18</b>
4.1 Software Requirements.....	18
4.2 Methodology.....	19
<b>5 Implementation.....</b>	<b>29</b>
5.1 Model Working.....	29
5.2 Results.....	41
<b>6 Conclusions and scope for further work.....</b>	<b>51</b>
6.1 Conclusions.....	51
6.2 Scope for further work.....	51
<b>References .....</b>	<b>52</b>
<b>Acknowledgements.....</b>	<b>53</b>

## List of Figures

3.1	Network Topology 1 of campus area network .....	9
3.2	Network Topology 2 of campus area network .....	9
3.3	Flowchart of Campus area network .....	10
3.4	Data-Centre.....	11
3.5	Network-admin.....	11
3.6	Reception.....	12
3.7	Boys Hostel.....	12
3.8	Girls Hostel .....	13
3.9	Library.....	14
3.10	Departments.....	14
3.11	ARP Spoofing dig.....	16
3.12	DHCP Snooping dig.....	17
3.13	GNS3 Network Topology.....	17
4.1	VLANS.....	19
4.2	InterVLAN Routing.....	20
4.3	SSH.....	21
4.4	ARP Spoofing.....	22
4.5	DHCP Snooping 1.....	23
4.6	DHCP Snooping 2.....	24
4.8	VLAN Hopping.....	25
5.1	COMP-1 (Switch).....	29



5.2	COMP-2 (Switch).....	30
5.3	COMP-2 (Switch).....	30
5.4	COMP-2 Switch (VLAN Configuration).....	31
5.5	Department Switch.....	31
5.6	Router R4 (InterVLAN Routing).....	31
5.7	Hostel-A Switch.....	32
5.8	Boys Hostel Switch.....	32
5.9	Hostel-A (VLAN Configuration).....	33
5.10	Router Hostel-A,B (InterVLAN Routing) .....	33
5.11	SSH Configuration .....	34
5.12	ARP Spoofing Configuration .....	35
5.13	DHCP Snooping Configuration .....	35
5.14	DHCP Show Configuration .....	35
5.15	VLAN Hopping Configuration.....	36
5.16	OSPF Configuration .....	36
5.17	Access-List Configuration.....	37
5.18	Network Topology of GNS3.....	38
5.19	Importing GNS3 VM.....	38
5.20	GNS3 Specifications.....	39
5.21	PRTG 1.....	39
5.22	PRTG 2.....	40
5.23	R1 SNMP Server.....	40

5.24	Dept. head PC.....	41
5.25	Dept. head PC.....	42
5.26	Dept. head PC.....	42
5.27	Professors PC.....	43
5.28	Hostel-A Warden's PC.....	44
5.29	Hostel-C Warden's PC.....	45
5.30	SSH Configuration (Router) .....	46
5.31	SSH Configuration (Switch ).....	46
5.32	ARP Spoofing result.....	47
5.33	DHCP Server0.....	48
5.34	DHCP Server-PC trusted .....	48
5.35	DHCP Server-PC untrusted.....	48
5.36	VLAN Hopping Result .....	48
5.37	OSPF Result.....	49
5.38	Access-list Show configuration Result .....	49
5.39	Access-list Result .....	49
5.40	R1 Discovery.....	50
5.41	PRTG Dashboard Result 1.....	50
5.42	PRTG Dashboard Result 2.....	50

## List of Tables:

2.1	Data Centre Survey.....	7
3.1	Data-Centre AT .....	11
3.2	Network-Admin AT .....	12
3.3	Reception AT.....	12
3.4	Boys Hostel AT.....	13
3.5	Girls Hostel AT.....	13
3.6	Library AT.....	14
3.7	Comp Department AT.....	15
3.8	IT Department AT.....	15
3.9	ETRX Department AT.....	15
3.10	EXTC Department AT.....	16
3.11	MECH Department AT.....	16
4.1	DHCP Snooping Table.....	24
5.1	COMP VLANs .....	29
5.2	Boys-Hostel VLANs .....	32
5.3	Girls-Hostel VLANs .....	33

# Chapter 1

## Introduction

*This chapter presents the introduction of the Design and Implementation of End to End Secured Campus Area Network. It contains the background of the technology utilized in the project topic, the motivation behind choosing this project and also the scope and overview of the developed project.*

### 1.1 Background:

Network is important for a society from very ancient age. A good network plays vital role in establishment of any government, research organization, or business establishment. In the age of Information Technology, ancient information network converted into computer network which is very fast and easily manageable. Similar to ancient era computer network security threat is always a serious issue and is very crucial. A campus network is an autonomous network under the management of university campus or within a local geographic area such as a business park, a government institution, a Research Centre or a Medical Centre. While the network may be managed by a single entity, it may be used by different organizations. The campus network has matured and grown more complex than ever. Often, a campus network provides an access path into a larger network, such as a metropolitan area network or the Internet. To build a stable, safe, efficient, convenient wireless campus network has become the inevitable trend of development and construction of campus network.

Campus network faces challenges to address core issues of security. Network security will prevent the college network from different types of threats and attacks. In this project, a tested and secured network design is implemented based on the practical requirements and this proposed network infrastructure is realizable with adaptable infrastructure.

## 1.2 Motivation:

The main goal for creating this project is to improve campus security in the age of ever-increasing data and the many threats and attacks that come with it. Because college data is so important at every level of the campus network, a secure network is essential to prevent any privacy breaches of any entity. Also, to avoid harmful attacks that could risk the lives of students or faculty. With the Pandemic, things are going virtual, and studying/working from home has become the new normal, the network security is crucial thing to consider in campus network

## 1.3 Scope of the Project:

This project aims to build a secured robust campus area network and we also researched various attacks that can happen in campus area network and specific methods to prevent common attacks. The two important factors while evaluating the scope of CAN are security and speed which are discussed below in detail:

- **Much Secured:** Campus Area Networks are maintained and administered by a single entity, which is usually the campus Data Centre. Network administrators can simply monitor, control, and grant network access. To prevent unwanted access, the team also installs firewalls between CAN and internet providers. They may also employ proxy servers to restrict access to specific internet ports or websites.
- **High Speed:** Data transfer speeds within the network remain stable and faster than average internet speeds. Users can swiftly share huge files using this method. When connected to the internet, for example, uploading a large film can take several hours. Transferring similar videos over CAN, on the other hand, takes a few minutes.

## **1.4 Brief Description of project undertaken:**

The project is implemented on a platform called Cisco Packet tracer. This project aims to design Campus network using Bus Topology. Campus consists of Data centre, Network Admin office, Boy's & Girls Hostel, Reception area, 5 Departments and Library. As every entity is in different network we created virtual LANs in which with the help of inter-VLAN routing we can communicate with different networks.

The server consists of 4 servers viz. DNS, HTTP, SMTP, FTP. The DNS is used to create domain of the campus. HTTP is for webpage access to end users, SMTP is for Email service. FTP is a way to download, upload, and transfer files from one location to another on the internet and between computer systems. We used SSH on network admin's Switch & Router to take access remotely.

We implemented OSPFs, ACLs to restrict, permit, or deny traffic which is essential for security of Network. We prevented common attacks such as ARP Spoofing, DHCP Snooping, VLAN Hopping in campus network. Also measured network performance parameters by integrating GNS3 with PRTG. In future we can create a service prevention tool to prevent this common attacks that can happen in campus network. We have done comparative analysis with existing college network with data centre to identify the gaps between our project.

## **1.5 Organization of the Report:**

The report is structured in 5 chapters where, chapter 1 consists of existing campus security problems and we believe creating a network model for campus. Chapter 2 i.e., literature review consists of a brief summary of study of different secured campus area networks, problems and their use cases. Chapter 3 consisting of Problem Statement, Network Topology, Network Devices used, Flowchart, Addressing table of developed network. Chapter 4 comprises of methodology used for project. Chapter 5 consists of implementation and results of campus area network. Chapter 6 consists of Conclusions and future work that can be implemented to the project.

## **Chapter 2**

### **Literature Review**

*This chapter presents a brief about the literature review of the project implemented and overview of the references from which the literature review has been composed.*

In “Design and Implementation of University Network” [1] This paper focuses on network design using bus topology which will be used for an entire university and every user of the network will be interlinked with each other. It proposes a novel approach to communicate among various users that are present at different sites at the same time. Departments will share information among faculty members and students where the whole university works on a single network. Thus it explores various concepts like network design, creating dynamic host configuration protocol, sub net masking, DNS and VLAN within a single network with the help of Cisco Packet Tracer.

In “Campus Network Security and Management” [2] This paper focuses on the designing of the campus area network using star topology. It discusses about Switches: VTP and VLANs, STP, Routers: Router-on-a-stick, Gateway Router/DHCP, Routing protocol i.e. EIGRP, NAT and ACLs. Further it focuses on network security applications such as Authentication Applications i.e. Kerberos which is a trusted third-party. In end it discusses about various types attacks that can happen in campus network such as Passive attacks, Active attacks.

In “Security Problems in Campus Problems and its solutions” [3] This paper focuses on the current security status of the campus network and analyze security threats to campus network and describe the strategies to maintain network. Users and institutions are demanding more and more network services and the exchange of potentially sensitive information within these services. Therefore, the issue of network security has become a priority to campus network management. Obviously, the current Internet is convenient but at the same time it is unsafe. Thus network services in campus area network can be more easily attacked.

In “Design and Implementation of a Secure Campus Network” [4] This paper focuses on network attacks. There are various types of attacks such as Passive Attack, Active Attack, Distributed Attack, Insider Attack, Close-in Attack, Phishing Attack, Hijack attack, Spoof attack, Buffer overflow, exploit attack, Password attack. Mainly 2 attacks are prevented in this research paper. ARP spoofing is an attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over Local Area Network (LAN). DHCP snooping is done on switches that connects end devices to prevent DHCP based attack. Basically DHCP snooping divides interfaces of switch into two parts i.e. trusted port and untrusted port. Thus in this research several attacks are demonstrated.

In “Detection and Prevention of ARP Spoofing using Centralized Server” [5] This paper tells about the ARP Spoofing attack and it aims to detect and mitigate the attack. The “ARP spoofing” attack is based on impersonating a system in the network, making the two ends of a communication believe that the other end is the attacker’s system, tracking the traffic interchanged. S-ARP model is encryption based security model in which every host has own public/private key it will sent it to the Authoritive Key Distribution(AKD) through which the encryption and decryption of data occurs. Local Area Network (LAN) based attacks are caused by compromised hosts in the LAN and mainly involve spoofing with falsified IP-MAC pairs. Thus in this paper several solutions are discussed to mitigate the ARP spoofing attacks

In “Mitigating DHCP starvation attack using snooping technique” [6] The aim of the paper is to solve the issue of DHCP starvation attack caused in DHCP sever. Dynamic Host Configuration Protocol (DHCP) is network management protocol used to automatically allocate IP addresses There are techniques which have been developed over the years to mitigate attacks to the DHCP server. This research used DHCP snooping to mitigate the attack to achieve a more secured network. The experiment was done in a virtual environment using GNS3. The experiment demonstrated how easy it was to attack and exhaust DHCP pool of address thereby prohibited the legitimate client from getting IP address. Thus the research demonstrated the mitigation of DHCP starvation attack by using DHCP snooping



In “VLAN hopping, ARP poisoning and Man-In-The-Middle Attacks in Virtualized Environments” [7] This paper aims to demonstrate VLAN hopping, ARP poisoning and Man-in-the Middle attacks across every major hypervisor platform and also tries to mitigate the attack by proposing solution. It evaluates layer 2 network security, include testing of network configurations including VLANs and mixed physical/virtual environments. Thus in this paper it presents detailed descriptions of the attack methodology used for each of our VLAN hopping and ARP poisoning scenarios and provide mitigation strategies that could help to prevent the attacks.

In “The Research and Analysis of Security of Campus Network” [8] This paper focuses on methods to provide security in campus network such as Guard Against Virus, Allocation of Firewall, Adoption of Intrusion Detection System, Web, Email, BBS Monitoring System, Scanner of Hole, Solving to embezzlement of IP, Using Network Monitoring to Maintain Security Thus we must preserve and renew the system constantly according to change of situation and some problems in current system so that ensure efficiency, advancement and positive development of network security defensive system.

In “Network Architecture and Security Issues in Campus Networks” [9] This paper represents Hierarchical Campus Network Design as it is broken up into three layers: Access Layer, Distribution Layer, and Core Layer network. Each layer provides specific functions that define its role within the overall network. Also several techniques are discussed for mitigating network attacks such as configuring port security, DHCP snooping, IP Source Guard, Dynamic ARP Inspection, and ACLs, Encrypt and password-protect sensitive data. Also Implement security hardware and software such as firewalls, IPSs, virtual private network (VPN) devices, anti-virus software, and content filtering.

In “Design and Implementation of the Campus Network Monitoring System” [10] This paper focuses on technical analysis of network monitoring. Network monitoring is the basic measure to ensure network stability and monitor the flow of information online. The proper control of network information can also be used to monitor the network information, eliminate unhealthy Internet information, maintain the network environment. Thus Network monitoring system can satisfy the needs of our campus network management and security management.

- **Data Center Survey:**

<b>Existing College Network</b>	<b>Our College Network</b>
Fortigate Firewall	ASA Firewall
Layer 2 Device – 2960 Switch (Cisco Nexus 9000)	Layer 2 Device – 2960 Switch
Core Switch (L3 Switch)	L3 Switch is not used
Router is not used	2911 Router
Bus Topology is used	Bus Topology is used
Static Routing is used	OSPF Routing is used
Intervlan Communication is blocked for segregation of college networks	Intervlan Communication is used
Network performance parameters (Bandwidth, Port Bandwidth, Latency)	Network performance parameters (Bandwidth, Port Bandwidth, Latency)
Fortigate Firewall is used to monitor network performance parameters	PRTG, Solar winds network monitoring tool

Table no. 2.1 Data Centre Survey

- **Objectives of the Project:**

- Literature Survey of Project.
- To create design of Secured Campus Area Network.
- Creation of VLANs, OSPFs, ACLs and implementing ASA firewall for internal security of network.
- For security of the network, we will identify the internal threats which are common in a campus area network and prevent them.
- Measure network performance parameters of Campus Network using network monitoring tool i.e. Solarwinds, PRTG

## Chapter 3

### Project Design

*This chapter presents the details about the design of the project. A basic introduction is given which is followed by the problem statement. It also provides the Network topology, flowchart, addressing table of network, and diagram of ARP Spoofing, DHCP Snooping, VLAN Hopping.*

#### 3.1 Introduction:

In this project we created campus area network topology using cisco packet tracer. We used bus topology to design the campus network. Campus Network consists of Data centre, Network Admin office, Boys & Girls hostel, Reception area, 5 departments and library. As every entity is in different network we created virtual LANs in which with the help of inter VLAN routing we can communicate with different networks. The server consists of 4 servers viz. DNS, HTTP, SMTP, and FTP. We configured multiple services such as DNS, HTTP, SMTP, FTP in one server. Also common attacks such as ARP Spoofing, DHCP Snooping, VLAN Hopping are demonstrated and prevented in campus network.

#### 3.2 Problem Statement:

The security concerns that the campus network encounters are determined by network infrastructure. To safeguard data privacy and the integrity of the campus network from many sorts of assaults, a secure network design is required. The goal of this project is to create a secure campus network design that includes ACLs and a Firewall to protect against internal attacks as well as common attacks like ARP Spoofing, DHCP Snooping, VLAN Hopping, and DDOS attacks. The most fundamental measure to ensure network stability and monitor the flow is network monitoring. Network monitoring tool can be used to monitor network.

### 3.3 Network Topology:

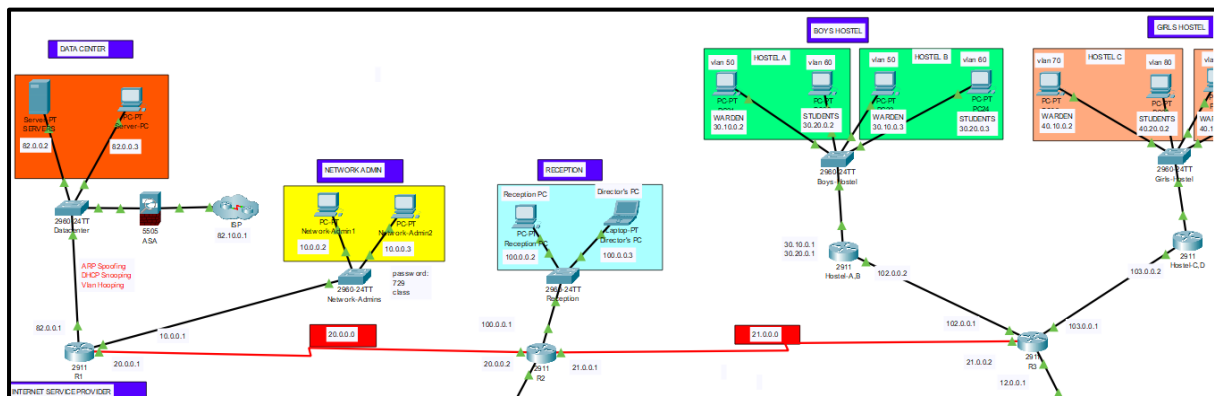


Figure no. 3.1 Network Topology 1 of campus area network (1<sup>st</sup> half part)

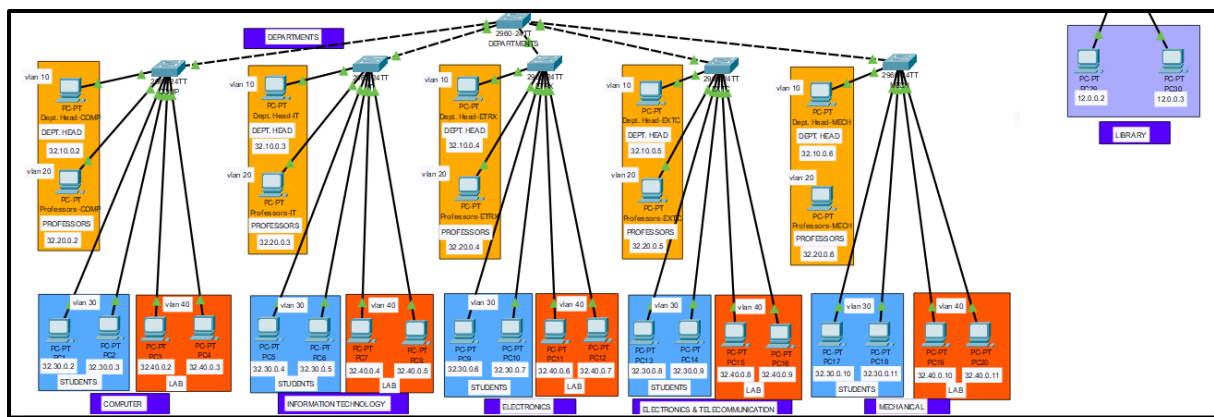


Figure no. 3.2 Network Topology 2 of campus area network (2<sup>nd</sup> half part)

### 3.4 Flow Chart:

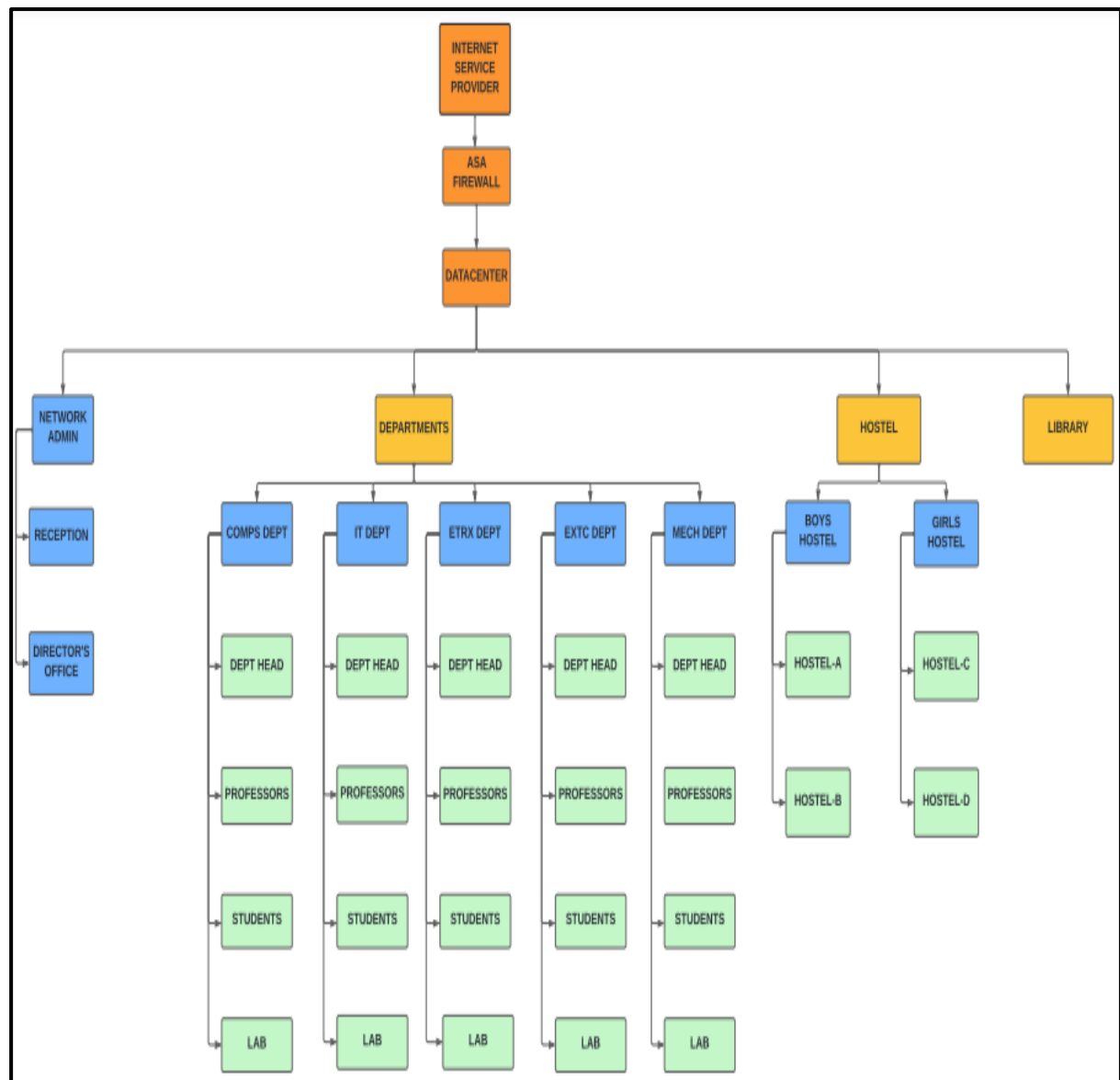


Figure no. 3.3 Flowchart of campus area network

### 3.5 Network Description:

#### 1. Data Centre / Server Room

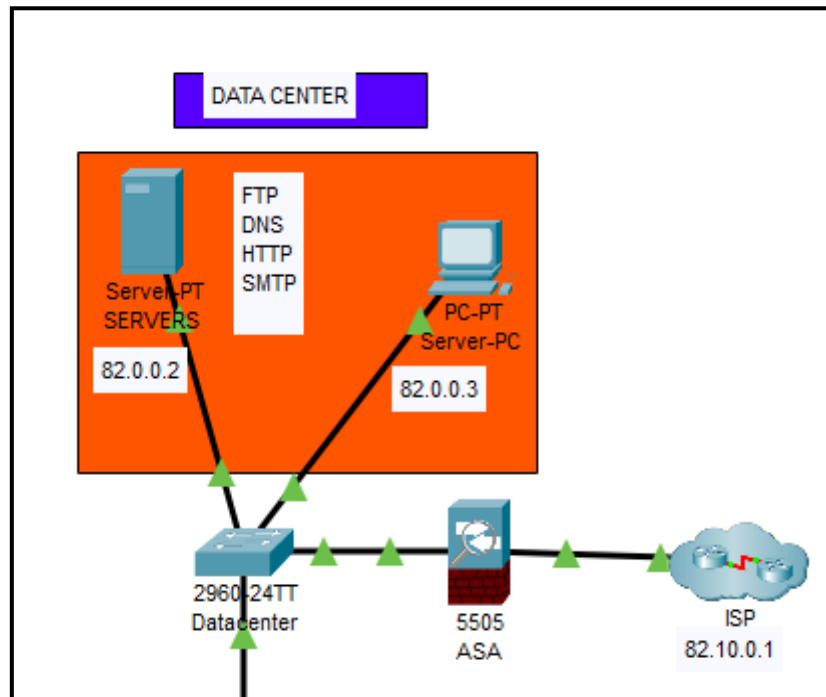


Figure no. 3.4 Data Centre

The server room has 4 servers. i.e. DNS, HTTP, SMTP, FTP. It also has a PC to access the servers. All the data of the entire campus is stored in server room.

Addressing Table:

Hostname	IP address	Subnet Mask	Default gateway
Servers	82.0.0.2	255.0.0.0	82.0.0.1
Server-PC	82.0.0.3	255.0.0.0	82.0.0.1
ISP Router	82.10.0.1	255.0.0.0	82.10.0.1

Table no. 3.1 Data Centre AT

#### 2. Network Admin

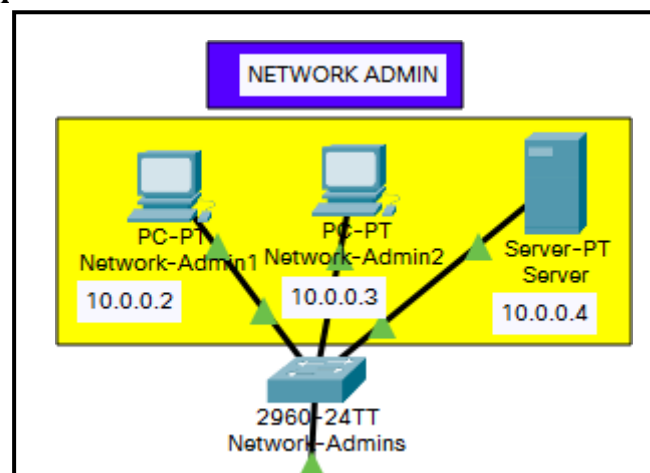


Figure no. 3.5 Network Admin

The role of the network administrator is to monitor and troubleshoot the network.

Addressing Table:

Hostname	IP address	Subnet Mask	Default gateway
Network-Admin1	10.0.0.2	255.0.0.0	10.0.0.1
Network-Admin2	10.0.0.3	255.0.0.0	10.0.0.1
Server	10.0.0.4	255.0.0.0	10.0.0.1

Table no. 3.2 Network Admin AT

### 3. Reception:

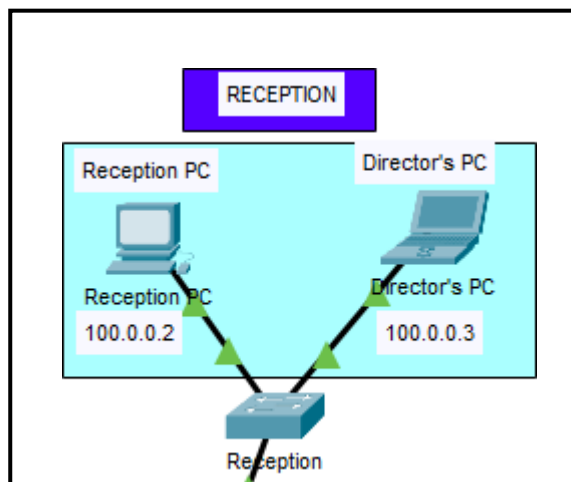


Figure no. 3.6 Reception

The reception has a PC of itself and a director's Laptop

Addressing Table

Hostname	IP address	Subnet Mask	Default gateway
Reception PC	100.0.0.2	255.0.0.0	100.0.0.1
Director_s PC	100.0.0.3	255.0.0.0	100.0.0.1

Table no. 3.3 Reception AT

### 4. Boys Hostel

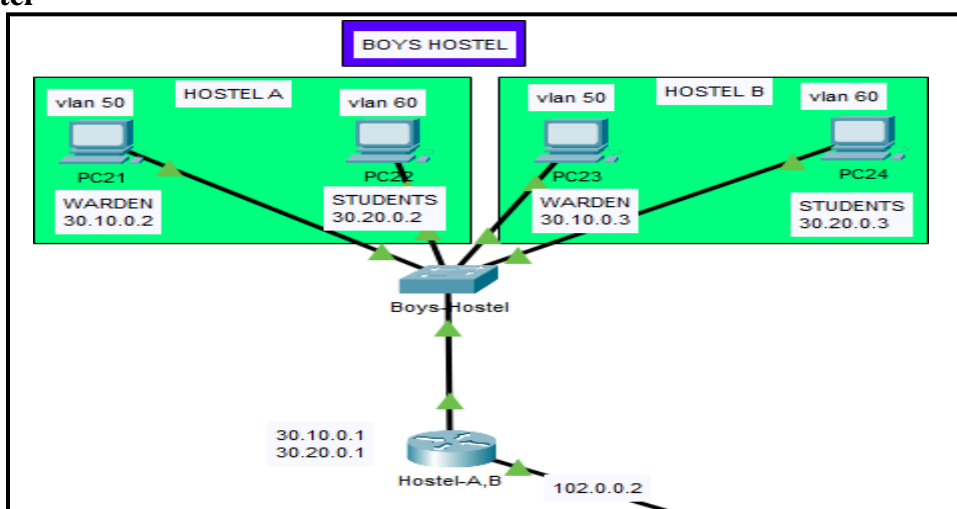


Figure no. 3.7 Boys Hostel

The whole Hostel consists of 4 buildings. 2 for boy's hostel and 2 for Girl's hostel. Each Building has a warden and End devices for students.

### Addressing Table

Hostname	IP address	Subnet Mask	Default gateway
PC21	30.10.0.2	255.255.0.0	30.10.0.1
PC22	30.20.0.2	255.255.0.0	30.20.0.1
PC23	30.10.0.3	255.255.0.0	30.10.0.1
PC24	30.20.0.3	255.255.0.0	30.20.0.1

Table no.3.4 Boys Hostel AT

### 5. Girls Hostel

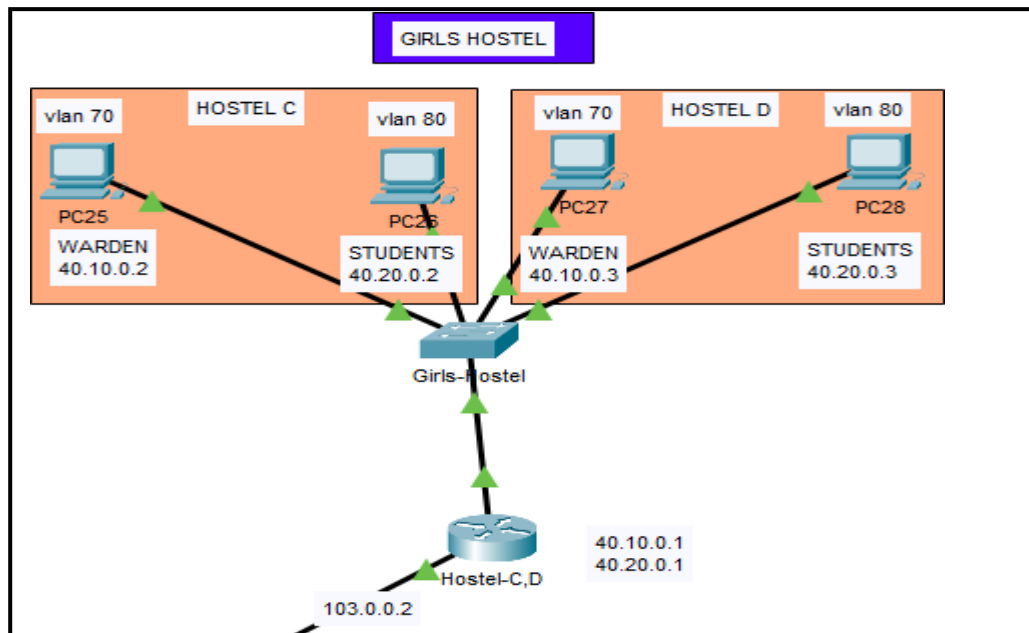


Figure no. 3.8 Girls Hostel

### Addressing Table

Hostname	IP address	Subnet Mask	Default gateway
PC25	40.10.0.2	255.255.0.0	40.10.0.1
PC26	40.20.0.2	255.255.0.0	40.20.0.1
PC27	40.10.0.3	255.255.0.0	40.10.0.1
PC28	40.20.0.3	255.255.0.0	40.20.0.1

Table no. 3.5 Girls Hostel AT



## 6. Library

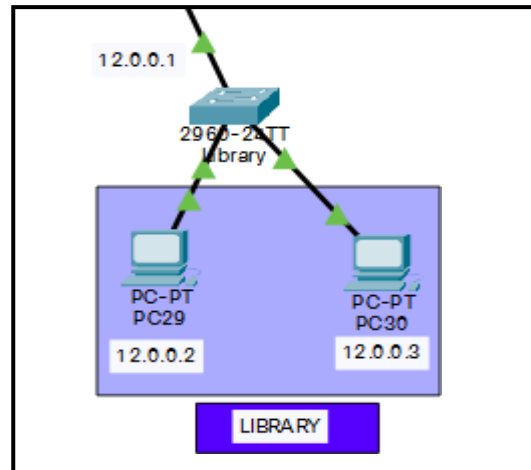


Figure no. 3.9 Library

### Addressing Table

Hostname	IP address	Subnet Mask	Default gateway
PC29	12.0.0.2	255.0.0.0	12.0.0.1
PC30	12.0.0.3	255.0.0.0	12.0.0.1

Table no. 3.6 Library AT Specifications

## 7. Departments

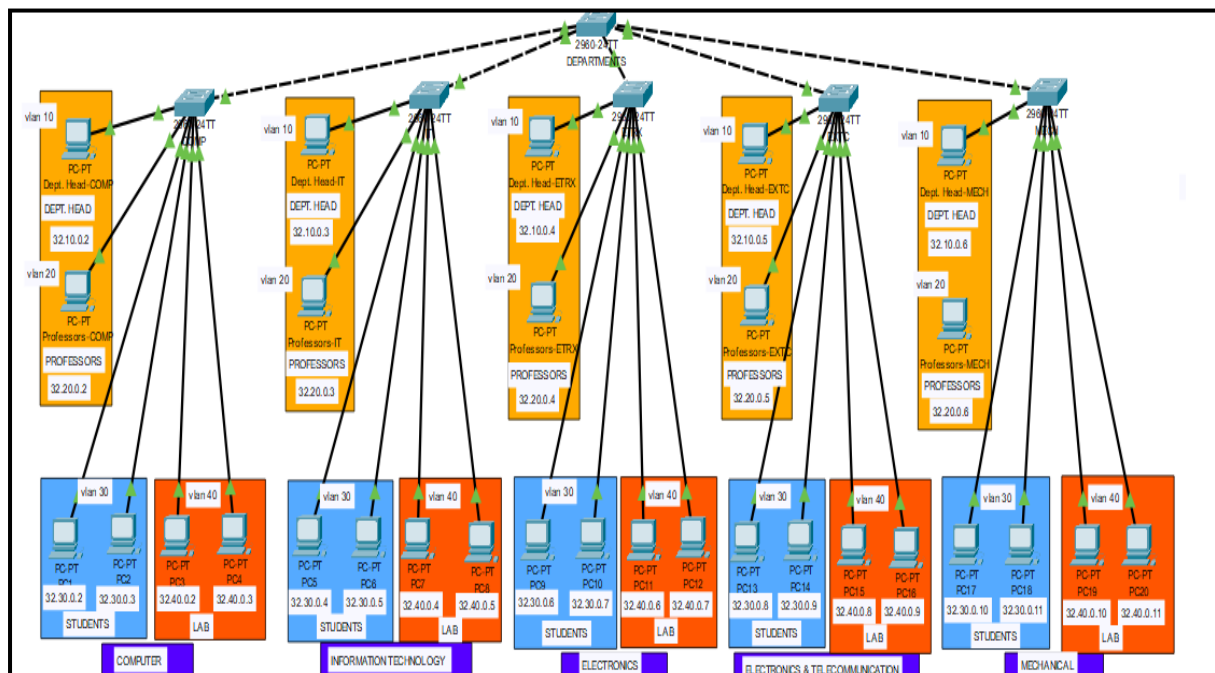


Figure no. 3.10 Departments

## 7.1 Computer Department

Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head COMP	32.10.0.2	255.255.0.0	32.10.0.1
Professors- COMP	32.20.0.2	255.255.0.0	32.20.0.1
PC1	32.30.0.2	255.255.0.0	32.30.0.1
PC2	32.30.0.3	255.255.0.0	32.30.0.1
PC3	32.40.0.2	255.255.0.0	32.40.0.1
PC4	32.40.0.3	255.255.0.0	32.40.0.1

Table no. 3.7 Comp Department AT

## 7.2 IT Department

Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head IT	32.10.0.3	255.255.0.0	32.10.0.1
Professors- IT	32.20.0.3	255.255.0.0	32.20.0.1
PC5	32.30.0.4	255.255.0.0	32.30.0.1
PC6	32.30.0.5	255.255.0.0	32.30.0.1
PC7	32.40.0.4	255.255.0.0	32.40.0.1
PC8	32.40.0.5	255.255.0.0	32.40.0.1

Table no. 3.8 IT Department AT

## 7.3 ETRX Department

Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head ETRX	32.10.0.4	255.255.0.0	32.10.0.1
Professors- ETRX	32.20.0.4	255.255.0.0	32.20.0.1
PC9	32.30.0.6	255.255.0.0	32.30.0.1
PC10	32.30.0.7	255.255.0.0	32.30.0.1
PC11	32.40.0.6	255.255.0.0	32.40.0.1
PC12	32.40.0.7	255.255.0.0	32.40.0.1

Table no. 3.9 ETRX Department AT

## 7.4 EXTC Department

### Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head EXTC	32.10.0.5	255.255.0.0	32.10.0.1
Professors-EXTC	32.20.0.5	255.255.0.0	32.20.0.1
PC13	32.30.0.8	255.255.0.0	32.30.0.1
PC14	32.30.0.9	255.255.0.0	32.30.0.1
PC15	32.40.0.8	255.255.0.0	32.40.0.1
PC16	32.40.0.9	255.255.0.0	32.40.0.1

Table no. 3.10 EXTC Department AT

## 7.5 MECH Department

### Addressing Table

Hostname	IP address	Subnet mask	Default gateway
Dept. head MECH	32.10.0.6	255.255.0.0	32.10.0.1
Professors-MECH	32.20.0.6	255.255.0.0	32.20.0.1
PC17	32.30.0.10	255.255.0.0	32.30.0.1
PC18	32.30.0.11	255.255.0.0	32.30.0.1
PC19	32.40.0.10	255.255.0.0	32.40.0.1
PC20	32.40.0.11	255.255.0.0	32.40.0.1

Table no. 3.11 MECH Department AT

## 8) ARP Spoofing:

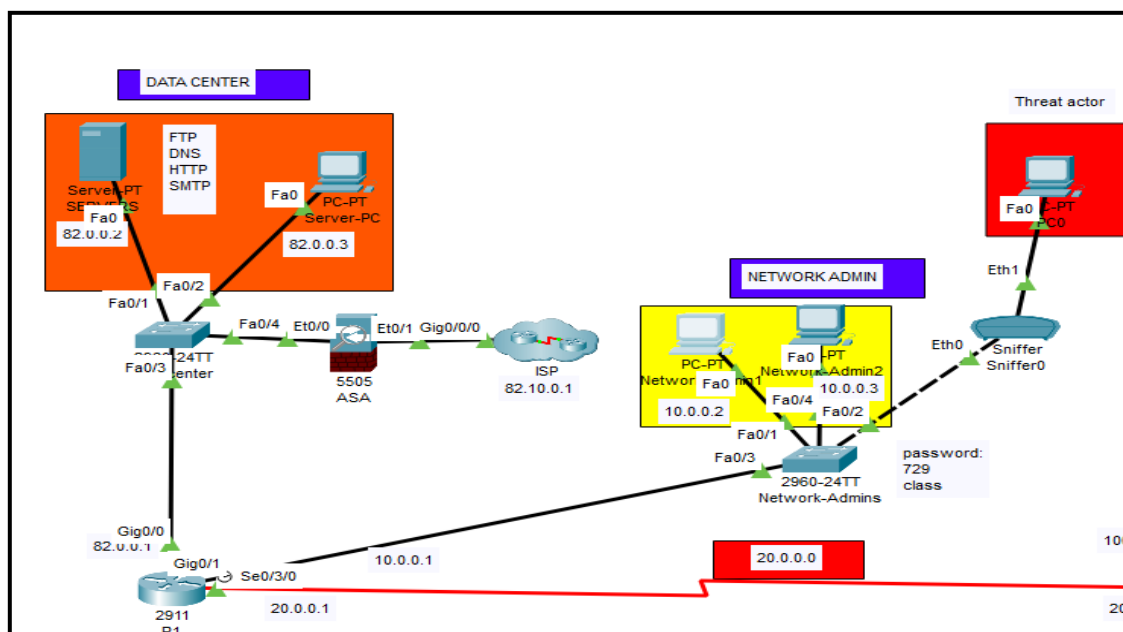


Figure no. 3.11 ARP Spoofing dig

- The threat actor tries to snoop the information exchanged between the network admins and the datacenter.
- The Threat actor is the man in the middle because it has acquired the mac address of the default gateway so ARP spoofing is also called Man in the middle attack

### 9) DHCP Snooping & VLAN Hopping:

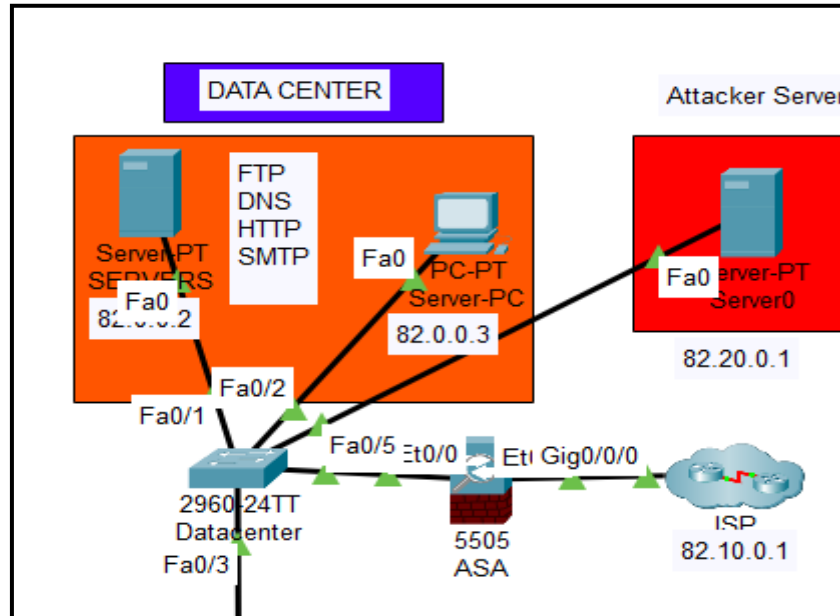


Figure no.3.12 DHCP Snooping dig

- The threat Server tries to snoop the information exchanged between the datacenter by creating DHCP Serverpool
- We created 3 vlans vlan 10 for Servers, vlan 20 for data center and vlan 30 for unused ports
- We used switchport nonegotiate command to disable dtp server.

### 10) GNS Topology:

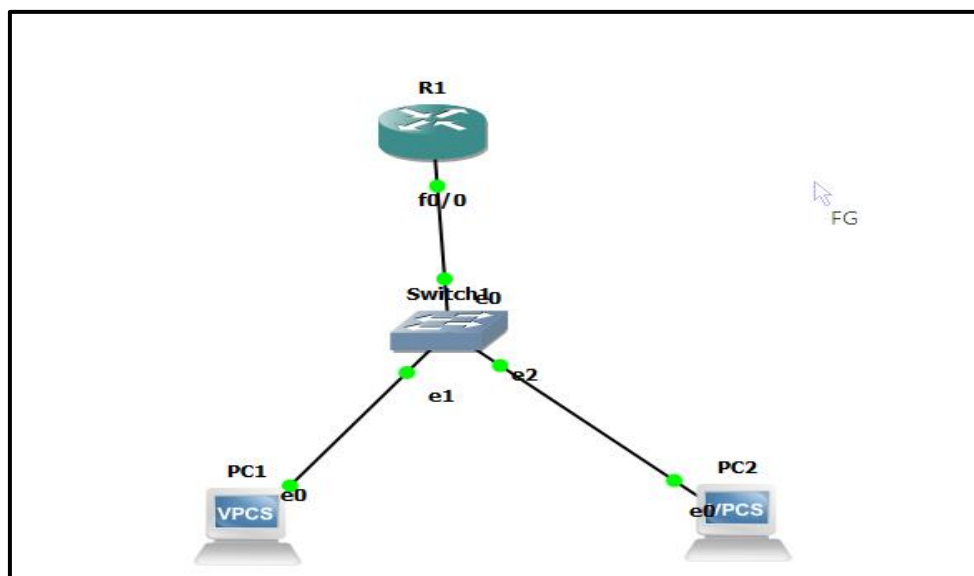


Figure no.3.13 GNS3 Topology

# Chapter 4

## Methodology

*This chapter presents the details about the Software requirements and methodology of VLANs, InterVLAN Routing (Router-on-stick), SSH, OSPF, Access-lists, common internal attacks such as ARP Spoofing, DHCP Snooping, VLAN Hopping, and important network performance parameters.*

### 4.1 Software Requirements:

#### 1. Cisco Packet Tracer:

Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks.

##### Features:

- Unlimited devices
- Visualizing Networks
- Real-time mode and Simulation mode
- Supports majority of networking protocols

#### 2. GNS3:

Graphical Network Simulator-3 (shortened to GNS3) is a network software emulator. It allows the combination of virtual and real devices, used to simulate complex networks. It uses Dynamips emulation software to simulate Cisco IOS.

##### Features:

- Design of high quality and complex network topologies
- Emulation of many Cisco router platforms and PIX firewalls
- Simulation of simple Ethernet, ATM and Frame Relay switches
- Connection of the simulated network to the real world
- Packet capture using Wireshark

#### 3. PRTG:

PRTG Network Performance Monitor (NPM) is a powerful and affordable network monitoring software enabling you to quickly detect, diagnose, and resolve network performance problems and outages.

##### Features:

- Bandwidth Monitor.
- Website Monitoring.
- Uptime Monitoring.
- Network Traffic Analyzer.
- Ping Monitoring.
- SQL Server Monitoring.

## 4.2 Methodology:

### 4.2.1 VLANs:

- A virtual LAN (VLAN) is a notion that allows us to logically segregate devices on layer 2. (data link layer). Layer 3 devices typically split broadcast domains, although switches can use the idea of VLAN to divide broadcast domains.
- A broadcast domain is a network segment in which all devices in the same broadcast domain will receive a packet broadcast by one device.
- All broadcast packets are received by devices in the same broadcast domain, but this is limited to switches because routers do not forward out broadcast packets.
- InterVLAN routing is required to forward packets to different VLANs (from one VLAN to another) or the broadcast domain. VLAN allows you to construct different little sub-networks that are comparatively easy to handle.

#### Types of connections in VLAN:

##### 1. Trunk Link:

VLAN awareness is required for all devices connected to a trunk link. A specific header called tagged frames should be appended to all frames on this page.

##### 2. Access link:

It connects devices that aren't aware of VLANs to a VLAN-aware bridge. The access link's frames must all be untagged.

##### 3. Hybrid link:

It combines the Trunk and Access links into one. Both VLAN-unaware and VLAN-aware devices are connected here, and transmissions can be tagged or untagged.

#### Example:

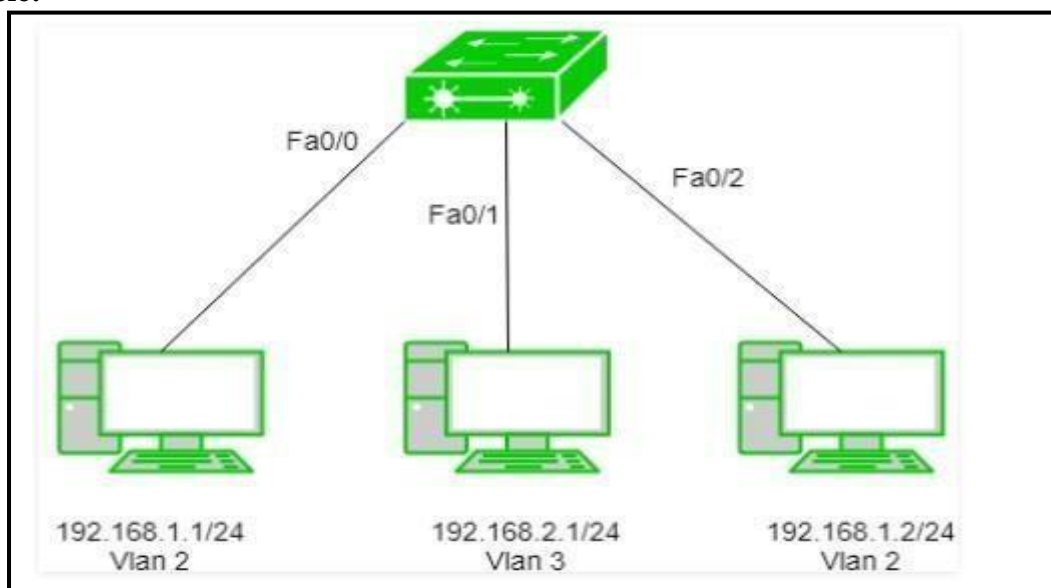


Figure no. 4.1 VLANs

### 4.2.2 InterVLAN Routing (Router on a stick Method):

- Inter VLAN routing is a process which allows different virtual LANs to interact with one another regardless of where they are located (on same switch or different switch).
- A layer-3 device, such as a router or a layer-3 switch, can accomplish this. Inter VLAN Routing is known as Router on a Stick when it is done using a router.

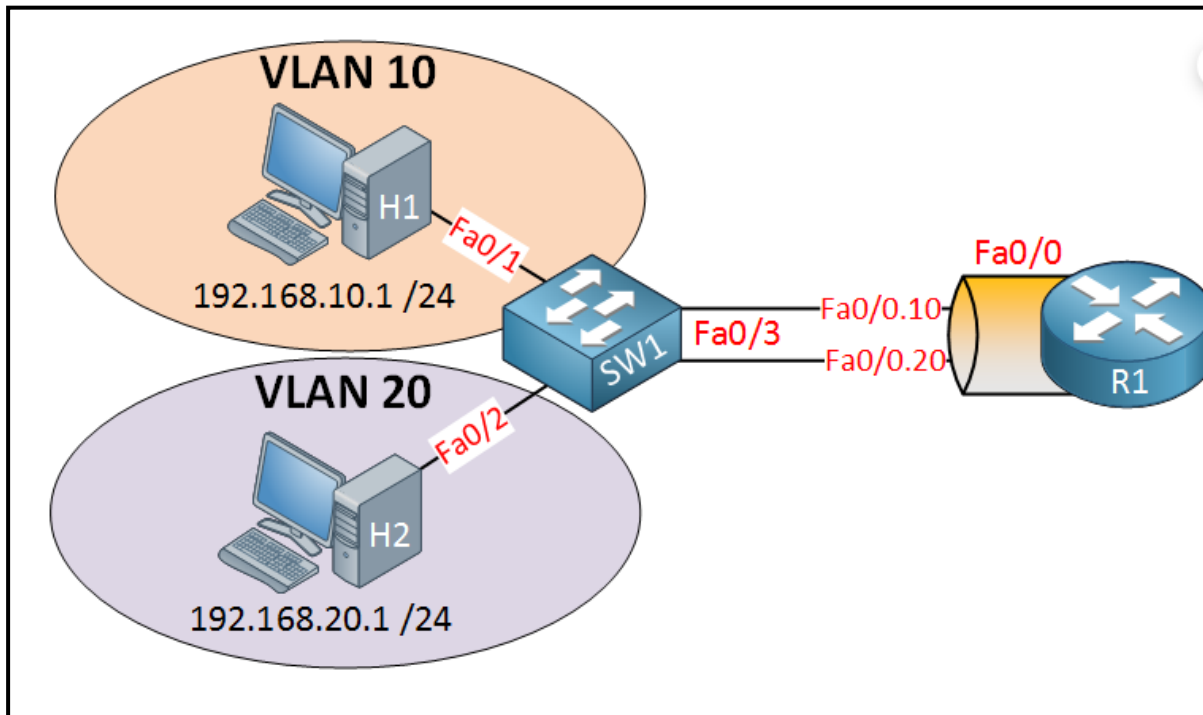


Figure no. 4.2 InterVLAN Routing

### 4.2.3 SSH:

- It's a cryptographic network protocol for sending encrypted data over the internet.
- It enables you to connect to a server, or numerous servers, without having to remember or input your password for each system that you want to login to remotely.
- It's always in a critical pair:
- Public key - No need to protect it because anybody may view it. (for the encryption feature)
- Private key - Must be kept safe in the computer. (to perform decryption)
- The following are examples of key pairs:
- User Key - If the user retains both the public and private keys.
- Host Key – If the public and private keys are on a different computer.
- Session key - This is used when a big amount of data needs to be sent.
- We used RSA Encryption method in our topology

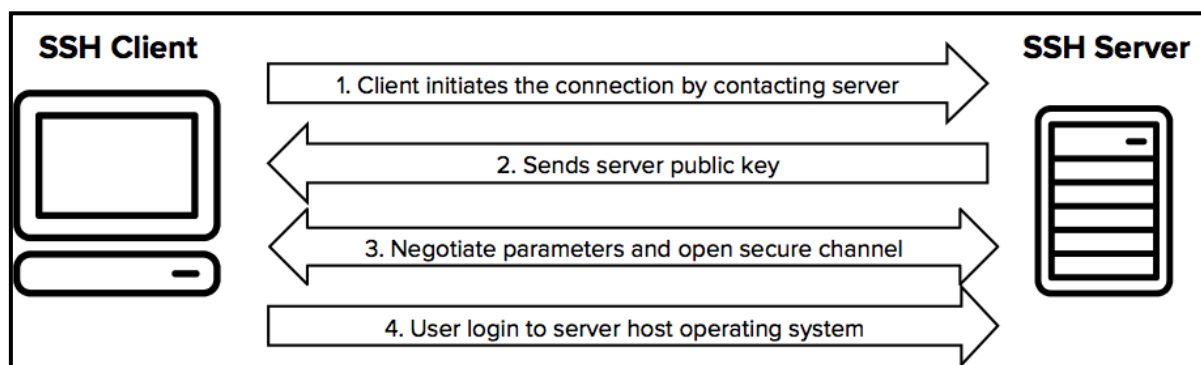


Figure no. 4.3 SSH



## 4.2.4 Internal Attacks:

### 4.2.4.1 ARP Spoofing:

- ARP spoofing is a type of attack in which a malicious actor sends forged ARP (Address Resolution Protocol) messages over a local area network, causing an attacker's MAC address to be linked to the IP address of a legitimate computer or server on the network.
- Malicious actors can intercept, change, and even stop transmitted data through ARP spoofing. Only local area networks using the Address Resolution Protocol are vulnerable to ARP spoofing attacks.

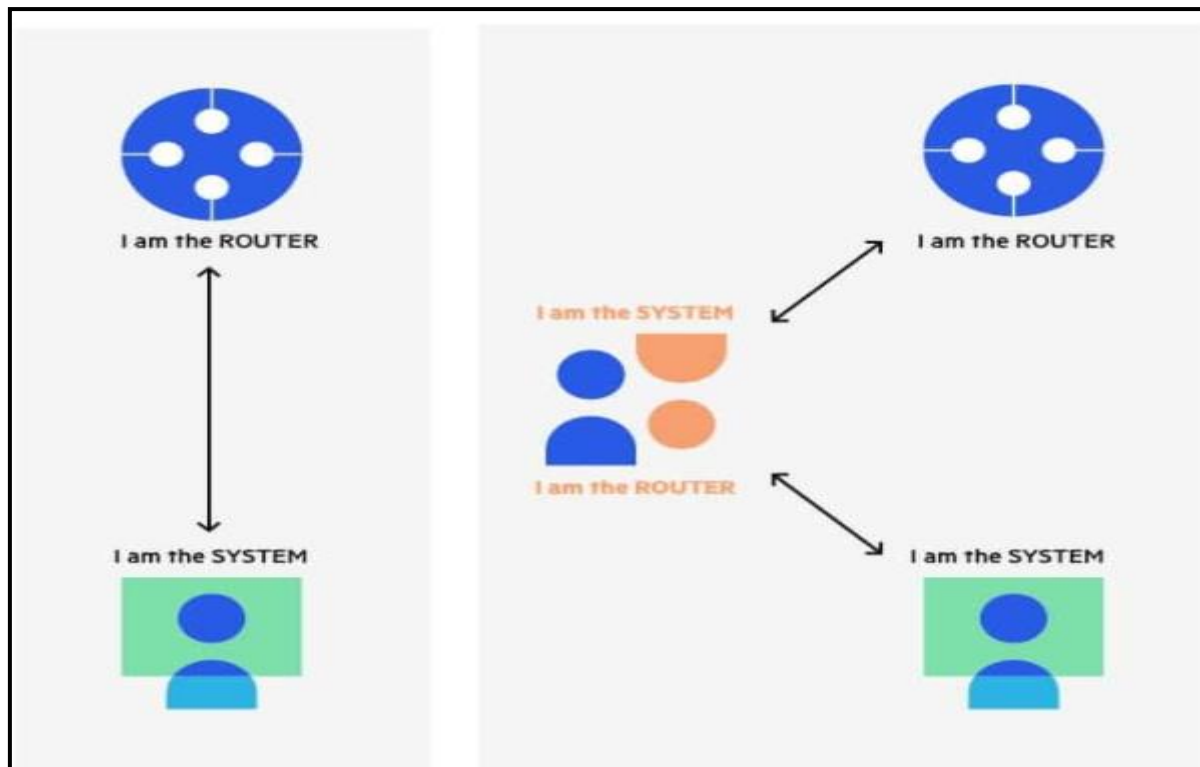


Figure no. 4.4 ARP Spoofing

The attack works as follows:

1. The attacker must have network access. They monitor the network for the IP addresses of at least two devices—say let's a workstation and a router.
2. The attacker sends out faked ARP answers using a spoofing tool like Arpspoof or Driftnet.
3. False answers claim that the attacker's MAC address is the correct MAC address for both IP addresses belonging to the router and workstation. Both the router and the workstation are tricked into connecting to the attacker's system rather than each other.
4. The two devices change their ARP cache entries and, from then on, interact with the attacker rather than each other directly.
5. The attacker is now in the middle of all communications.

#### 4.2.4.2 DHCP Snooping:

DHCP Snooping is a layer 2 security feature built into the operating system of a capable network switch that filters out DHCP communication that is deemed inappropriate. Unauthorized (rogue) DHCP servers providing IP addresses to DHCP clients are prevented by DHCP Snooping. The DHCP Snooping functionality does the following tasks:

- Validates and filters DHCP messages received from untrusted sources.
- Creates and maintains the DHCP Snooping binding database, which contains data about untrusted hosts with leased IP addresses.
- Validates subsequent requests from untrusted hosts using the DHCP Snooping binding database.

#### How DHCP Snooping Works:

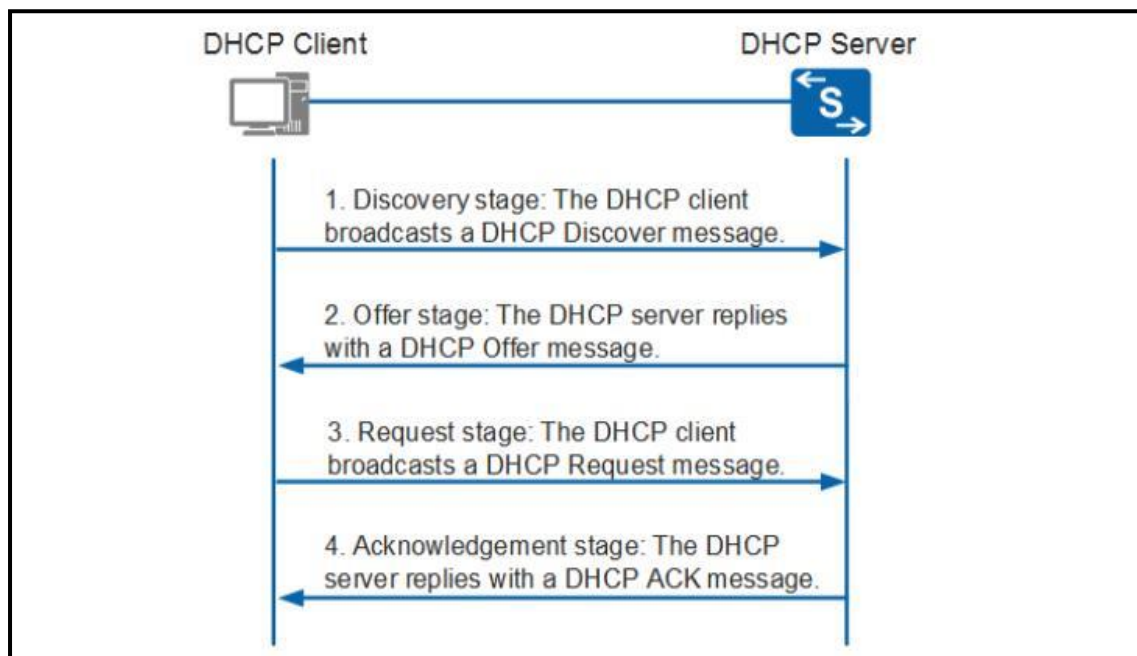


Figure no. 4.5 DHCP Snooping 1

To figure out how DHCP Snooping works, the operating mechanism of DHCP (dynamic host configuration protocol) must be understood. A network device without an IP address will "interact" with the DHCP server in four stages if DHCP is enabled.

As shown in Figure 2, DHCP Snooping divides switch interfaces into two categories: trusted and untrusted ports. A trusted port or source is one that trusts DHCP server messages. A port from which DHCP server transmissions are not trusted is known as an untrusted port. The DHCP offer message can only be transmitted through the trusted port if DHCP Snooping is enabled. It will be dropped otherwise.

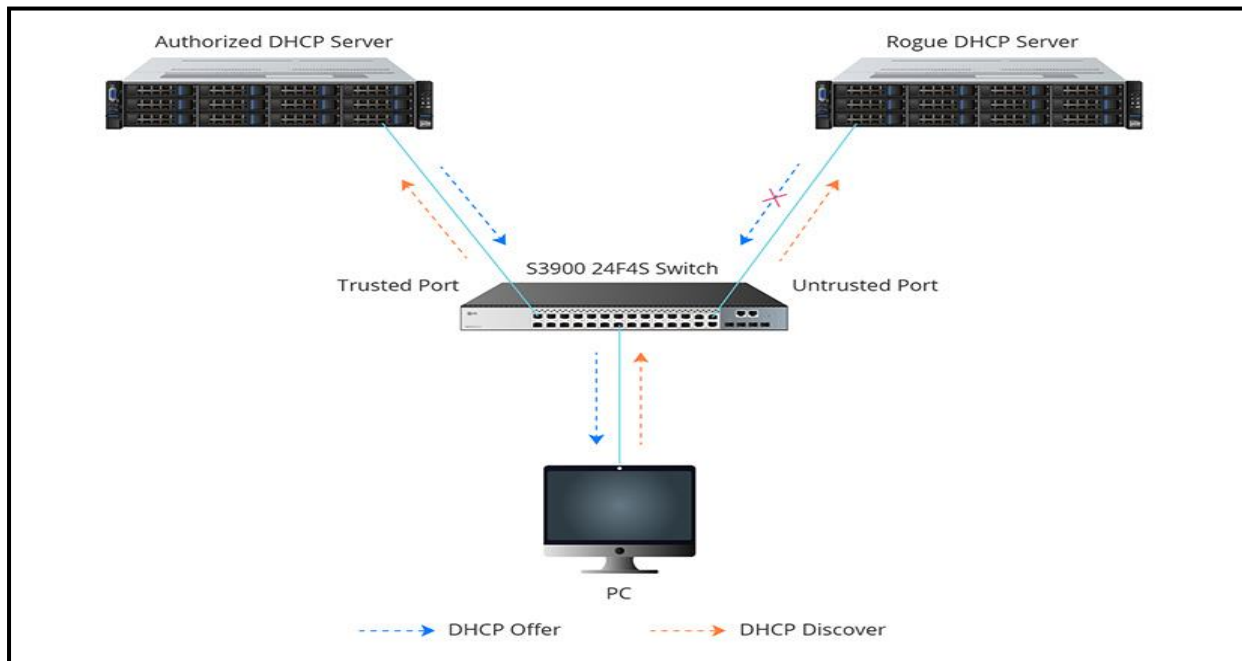


Figure no. 4.6 DHCP Snooping 2

A DHCP binding table will be constructed based on the DHCP ACK message during the acknowledgment stage. As illustrated in Figure 3, it records the host's MAC address, the leased IP address, the lease time, the binding type, and the VLAN number and interface information connected with the host. The next DHCP packet received from an untrusted host will be dropped if it does not match the information.

	MAC Address	IP Address	Lease(sec)	Type	VLAN	Interface
Entry 1	e4-54-e8-9d-ab-42	10.32.96.19	2673	dhcp-snooping	10	Eth 1/23
Entry 2						
...						

Table no. 4.1 DHCP Snooping Table

#### 4.2.4.3 VLAN Hooping:

VLAN hopping is a type of attack in which the attacker can send data from one VLAN to another. There are two options for accomplishing this:

- Double tags: the attack relies on the attacker being connected to an interface in access mode with the same VLAN as the trunk's native untagged VLAN. The attacker sends a packet with two 802.1Q tags: the "inner" VLAN tag represents the VLAN we want to connect to, while the "outer" VLAN tag represents the native VLAN. When the switch gets the frame, it removes the first (native VLAN) 802.1Q tag and passes the frame on its trunk interface with the second 802.1Q tag (s). The attacker has "jumped" from the native VLAN to the VLAN of the victim. Although it is a one-way travel, it could be utilised for a DOS assault.
- Switch spoofing: when you employ the default "dynamic auto" or "dynamic desired" switchport mode, the attacker will send DTP packets and try to negotiate a trunk with the switch. You will have access to all VLANs once you have a trunk connected to your computer. This is a misconfiguration since you should never utilise the dynamic switchport modes on your interfaces.

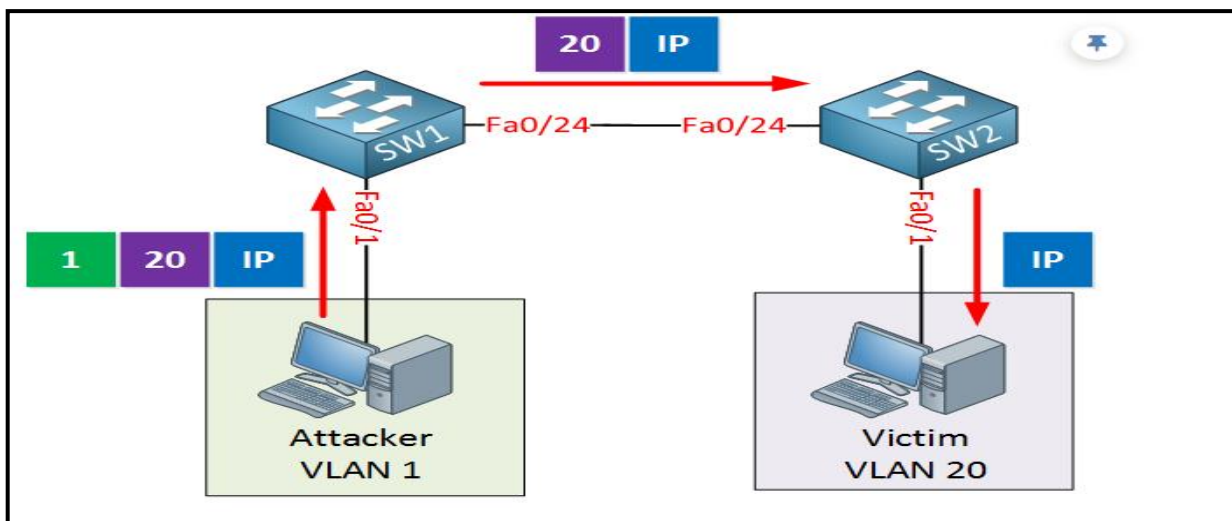


Table no. 4.7 VLAN Hopping

#### How to prevent VLAN hopping:

- Use switchport mode access instead of DTP (auto trunking) negotiations on non-trunk ports.
- Using switchport mode trunk, manually enable trunk links.
- Using switchport nonegotiate, disable DTP (auto trunking) negotiations on trunking and non-trunking ports.
- Change the native VLAN from VLAN 1.
- Unused ports should be disabled and assigned to an unused VLAN.

### 4.2.5 OSPF:

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) that uses its own shortest path first (SPF) algorithm to help discover the best routing path between the source and destination router. It's a Link-state routing technique for distributing data packet routing information inside a big Autonomous System.

- **Backbone Area:** The backbone area, also known as area0 or area 0.0.0.0, is at the heart of an OSPF network, with all other areas of the network connected to it. It's in charge of disseminating routing information between regions that aren't backbone area types.
- **Stub Area:** The area's routing is solely based on a default route in the case of Stub Area. It's a section of the autonomous system that doesn't get any outside advertising (AS)

#### How OSPF Works?

When it is configured, it listens to its network neighbours and collects all accessible connection state data. This information is then utilised to create a topology map that shows all of the network's accessible pathways. We call this database Link State Database because it is saved for future use.

OSPF generates three tables:

- **Routing Table:** This table holds the current best pathways for forwarding traffic between two neighbours.
- **Neighbour Table:** This table contains all Open Short Path First neighbours that have been discovered.
- **Topology Table:** This one contains the whole network's road map. This road map shows all of the Open Short Path First routers that are available, as well as estimated statistics on the optimal and alternate routes.

#### Types of Routers in OSPF

- **Internal Router:** This router contains all interfaces in the same area that belong to each other.
- **Area Border Router (ABR):** ABR is a backbone network that connects one or more regions. An ABR is a member of all the regions to which it is linked. In memory, it retains numerous Link State databases, one for each area.
- **Backbone Router:** A backbone router is a router with an interface to a backbone area.
- **ASBR (Autonomous System Boundary Router)** is a router with several routing protocols connected to the network. ASBR communicates with router autonomous systems to exchange routing information. These use an external routing protocol, state routes, or a combination of the two.

## 4.2.6 Access-Lists

ACL stands for access control list, and it is a set of rules for regulating network traffic and mitigating network threats. ACLs are used to filter traffic using a set of rules for incoming and outgoing network traffic.

- **Inbound access lists:** When an access list is applied to an interface's inbound packets, the packets are first processed according to the access list before being routed to the outward interface.
- **Outbound access lists** — When an access list is applied to an interface's outgoing packets, the packet is first routed before being processed at the outbound interface.

### Types of ACL :

There are two main different types of Access-list namely:

- **Standard Access-list:**  
These are the Access-list that are made using the source IP address only. These ACLs permit or deny the entire protocol suite. They don't distinguish between the IP traffic such as TCP, UDP, HTTPS, etc. By using numbers 1-99 or 1300-1999, the router will understand it as a standard ACL and the specified address as the source IP address.
- **Extended Access-list:**  
These are the ACL that uses source IP, Destination IP, source port, and Destination port. These types of ACL, we can also mention which IP traffic should be allowed or denied. These use range 100-199 and 2000-2699.

### Rules for ACL:

- The standard Access-list is generally applied close to the destination (but not always).
- The extended Access-list is generally applied close to the source (but not always).
- We can assign only one ACL per interface per protocol per direction, i.e., only one inbound and outbound ACL is permitted per interface.
- We can't remove a rule from an Access-list if we are using numbered Access-list. If we try to remove a rule, then the whole ACL will be removed. If we are using named access lists, then we can delete a specific rule.
- Every new rule which is added to the access list will be placed at the bottom of the access list therefore before implementing the access lists, analyses the whole scenario carefully.
- As there is an implicit deny at the end of every access list, we should have at least a permit statement in our Access-list otherwise all traffic will be denied.

## **4.2.7 Network Performance Parameters:**

### **4.2.7.1 Throughput:**

- Throughput is defined as the amount of data transported between various sites in a certain amount of time, usually in bits per second (bps), but also in bytes per second (Bps), kilobytes per second (KBps), megabytes per second (MBps), and gigabytes per second (GBps) (GBps).
- A variety of factors can affect throughput, including the underlying analogue physical medium's impediment, the system components' available processing capacity, and end-user behaviour. When several protocol costs are included in, the utilization rate of sent data can be much lower than the highest throughput possible.

### **4.2.7.2 Bandwidth:**

- The quantity of bandwidth allocated to the network is one of the most important aspects of a website's performance. The webserver's bandwidth controls how quickly it can upload the requested data. While there are many aspects to consider when it comes to a site's performance, bandwidth is frequently the limiting factor.
- Bandwidth is defined as the amount of data or information that can be delivered in a given amount of time. The phrase can be applied in two ways, with two different estimation values. The bandwidth of digital devices is measured in bits per second (bps) or bytes per second (Bps). The bandwidth of analogue equipment is measured in cycles per second, or Hertz (Hz).

### **4.2.7.3 Jitter:**

- Jitter is a term that describes the delay in packet flow from one client to the next. Jitter is measured in milliseconds and has the greatest impact on audio and video streaming services.
- Jitter can occur when VoIP calls lose quality for an extended period of time or cut in and out. If your favourite video streaming service has ever sat and buffered or frozen up on you, network jitter could be to reason.

### **4.2.7.4 Latency:**

- Latency is a term that describes the time it takes for data to transmit from one endpoint to another. This is measured in milliseconds, and many administrators assess latency by the time it takes a packet to travel from point A to point B.
- When testing for latency with ping or another ICMP tool, latency is sometimes referred to as "high ping times." Latency, like jitter, can cause delays and is particularly visible with streaming video, live audio, and online video games.

## Chapter 5

### Implementation

*This chapter presents the details about the project implementation in which configuration of Intervlan Routing, SSH, OSPF, Access-lists, internal attacks such as ARP Spoofing, DHCP Snooping, VLAN Hopping and network performance parameters and results for the same*

#### 5.1 Model working:

##### 5.1.1 Department Configuration:

Created VLANs for Dept. Head, Professors, Students and lab for 5 Departments.

Hostname	Ports	Assignment	Network
COMP-1	fa0/2	VLAN 10	32.10.0.0
COMP-1	fa0/3	VLAN 20	32.20.0.0
COMP-2	fa0/1-2	VLAN 30	32.30.0.0
COMP-2	fa0/3-4	VLAN 40	32.40.0.0

Table no. 5.1 COMP VLANs

Created trunking ports on Department switch and same process is done for other departments.

Example of Computer Department:

1) COMP-1 Switch:

```
COMP-1>en
COMP-1#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gig0/1, Gig0/2
10	Dept.Head	active	Fa0/2
20	Professors	active	Fa0/3
30	Students	active	
40	Lab	active	

Figure no. 5.1 COMP-1 Switch

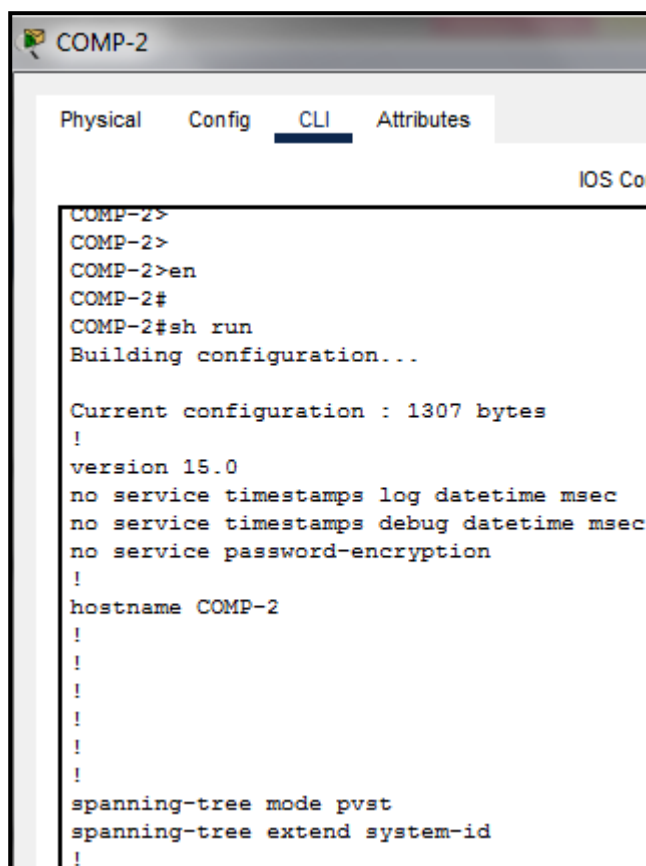


## 2) COMP-2 Switch:

```
COMP-2>
COMP-2>en
COMP-2#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gig0/1 Gig0/2
10	Dept.Head	active	
20	Professors	active	
30	Students	active	Fa0/1, Fa0/2
40	Lab	active	Fa0/3, Fa0/4

Figure no. 5.2 COMP-2 Switch



```
COMP-2>
COMP-2>
COMP-2>en
COMP-2#
COMP-2#sh run
Building configuration...

Current configuration : 1307 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname COMP-2
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
```

Figure no. 5.3 COMP-2 Switch

### 3) COMP-2 Switch (VLAN Configuration):

```
!
interface FastEthernet0/1
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/4
 switchport access vlan 40
 switchport mode access
!
interface FastEthernet0/5
 switchport mode trunk
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
```

Figure no. 5.4 COMP-2 Switch

### 4) Departments Switch:

```
DEPARTMENTS>en
DEPARTMENTS#sh int trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     auto      n-802.1q       trunking    1
Fa0/2     auto      n-802.1q       trunking    1
Fa0/3     auto      n-802.1q       trunking    1
Fa0/4     auto      n-802.1q       trunking    1
Fa0/5     auto      n-802.1q       trunking    1
Fa0/6     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005
Fa0/3     1-1005
Fa0/4     1-1005
Fa0/5     1-1005
Fa0/6     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1,10,20,30,40
Fa0/2     1,10,20,30,40
Fa0/3     1,10,20,30,40
Fa0/4     1,10,20,30,40
Fa0/5     1,10,20,30,40
Fa0/6     1,10,20,30,40
```

Figure no. 5.5 Department Switch

### 5) Router R4: (InterVLAN Routing)

```
R4
Physical  Config  CLI  Attributes
IOS Command Line Interface

interface GigabitEthernet0/0/1.10
 encapsulation dot1Q 10
 ip address 32.10.0.1 255.255.0.0
!
interface GigabitEthernet0/0/1.20
 encapsulation dot1Q 20
 ip address 32.20.0.1 255.255.0.0
!
interface GigabitEthernet0/0/1.30
 encapsulation dot1Q 30
 ip address 32.30.0.1 255.255.0.0
!
interface GigabitEthernet0/0/1.40
 encapsulation dot1Q 40
 ip address 32.40.0.1 255.255.0.0
!
```

Figure no. 5.6 Router R4 (InterVLAN Routing)

## 5.1.2 Hostels (Boys Hostel) & (Girls Hostel) Configuration

### 1. Boys Hostel (Hostel-A,B)

Created VLANs for Warden and students for Hostel A, B

Hostname	Ports	Assignment	Network
PC-21(Warden)	fa0/1	VLAN 50	30.10.0.0
PC-22 (Students)	fa0/2	VLAN 60	30.20.0.0

Table no. 5.2 Boys Hostel VLANs

Created trunking ports on Hostel-A,B switch and Same process is done for Hostel-B

Example of Hostel-A:

#### 1) Hostel-A Switch

```
Hostel-A>
Hostel-A>
Hostel-A>en
Hostel-A#sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9, Fa0/10, Fa0/11 Fa0/12, Fa0/13, Fa0/14, Fa0/15 Fa0/16, Fa0/17, Fa0/18, Fa0/19 Fa0/20, Fa0/21, Fa0/22, Fa0/23 Fa0/24, Gig0/1, Gig0/2
50	Warden	active	Fa0/1
60	Students	active	Fa0/2

Figure no. 5.7 Hostel-A Switch

#### 2) Boys-Hostel Switch

```
Boys-Hostel>en
Boys-Hostel#sh int trunk
Port      Mode      Encapsulation  Status      Native vlan
Fa0/1     on        802.1q         trunking    1
Fa0/2     on        802.1q         trunking    1
Fa0/3     on        802.1q         trunking    1

Port      Vlans allowed on trunk
Fa0/1     1-1005
Fa0/2     1-1005
Fa0/3     1-1005

Port      Vlans allowed and active in management domain
Fa0/1     1, 50, 60
Fa0/2     1, 50, 60
Fa0/3     1, 50, 60
```

Figure no. 5.8 Boys-Hostel Switch

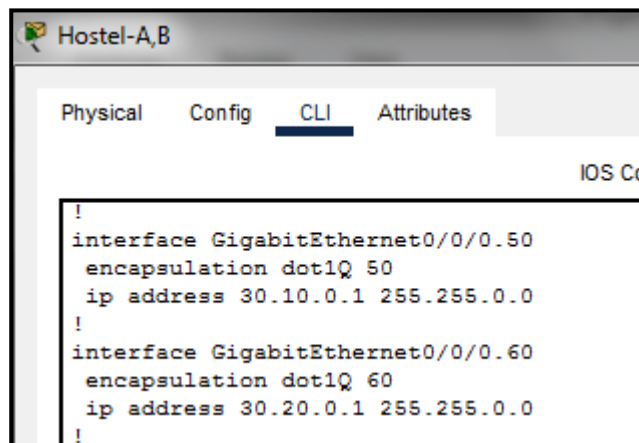
### 3) Hostel-A Switch

```
Hostel-A#sh run
Building configuration...

Current configuration : 1184 bytes
!
version 15.0
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname Hostel-A
!
!
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 50
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 60
 switchport mode access
```

Figure no. 5.9 Hostel-A (VLAN Configuration)

### 4) Router Hostel-A,B



```
Hostel-A,B
Physical Config CLI Attributes
IOS Co

!
interface GigabitEthernet0/0/0.50
 encapsulation dot1Q 50
 ip address 30.10.0.1 255.255.0.0
!
interface GigabitEthernet0/0/0.60
 encapsulation dot1Q 60
 ip address 30.20.0.1 255.255.0.0
!
```

Figure no. 5.10 Router Hostel-A,B (Intervlan Routing)

## 2. Girls Hostel (Hostel-C,D)

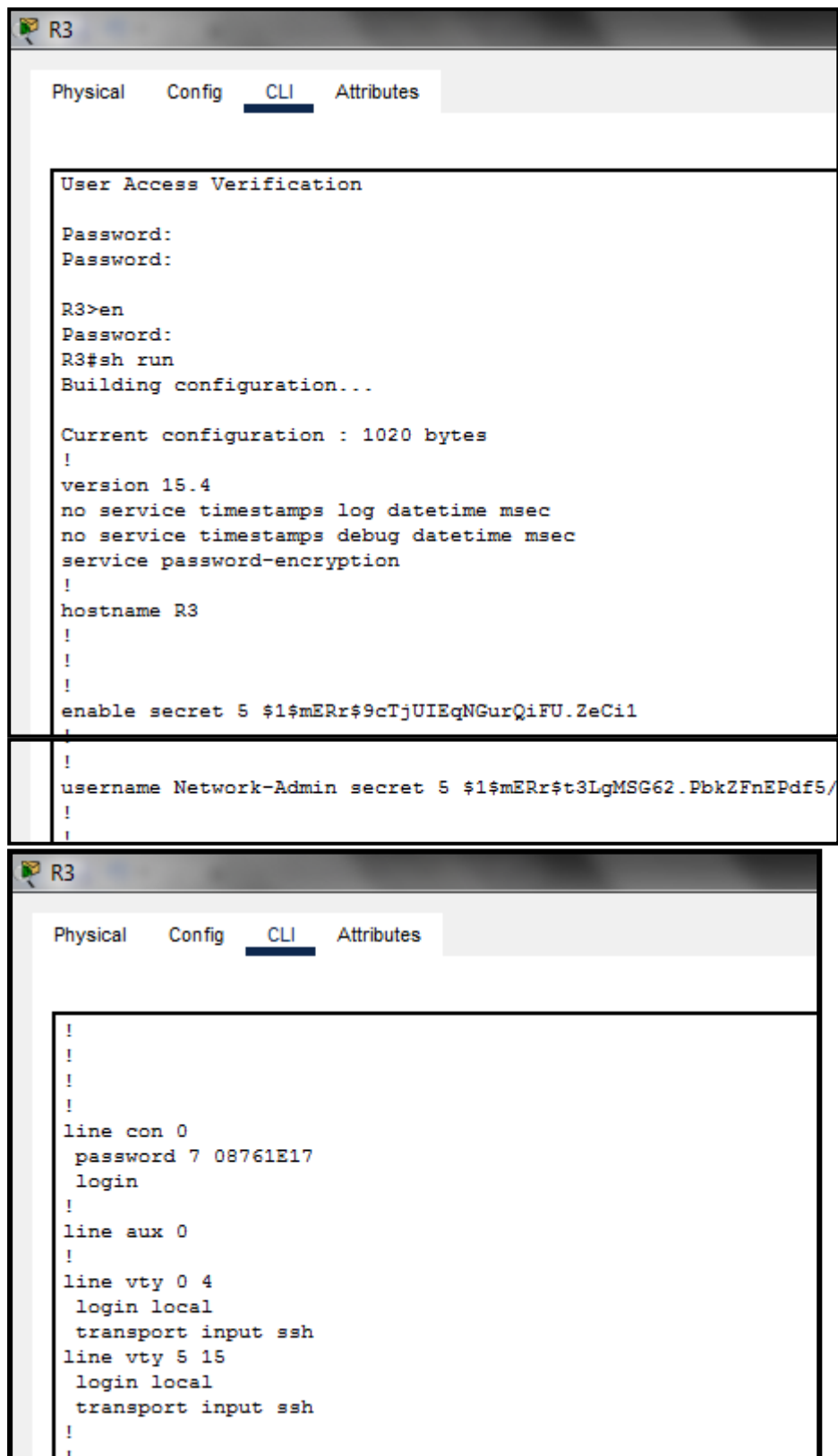
Created VLANs for Warden and students for Hostel C, D

Hostname	Ports	Assignment	Network
PC-25(Warden)	fa0/1	VLAN 70	40.10.0.0
PC-26 (Students)	fa0/2	VLAN 80	40.20.0.0

Table no. 5.3 Girls Hostel VLANs

Same process is done for Hostel-C,D as done for Hostel-A

### 5.1.3 SSH Configuration:



The figure consists of two screenshots of a Cisco R3 router's CLI interface. The top screenshot shows the 'User Access Verification' section with the following text:

```
Physical  Config  CLI  Attributes

User Access Verification

Password:
Password:

R3>en
Password:
R3#sh run
Building configuration...

Current configuration : 1020 bytes
!
version 15.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
service password-encryption
!
hostname R3
!
!
!
enable secret 5 $1$mERr$9cTjUIEqNGurQiFU.ZeCi1
!
!
username Network-Admin secret 5 $1$mERr$t3LgMSG62.PbkZFnEPdf5/
!
!
```

The bottom screenshot shows the configuration for the console, auxiliary, and VTY lines:

```
Physical  Config  CLI  Attributes

!
!
!
!
line con 0
 password 7 08761E17
 login
!
line aux 0
!
line vty 0 4
 login local
 transport input ssh
line vty 5 15
 login local
 transport input ssh
!
!
```

Figure no. 5.11 SSH Configuration

### 5.1.4 ARP Spoofing Configuration:

```
ip arp inspection vlan 10
ip arp inspection validate src-mac dst-mac ip
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/2
  switchport access vlan 10
  switchport mode access
!
interface FastEthernet0/3
  ip arp inspection trust
```

Figure no.5.12 ARP Spoofing Configuration

- Fast ethernet port 0/3 is a trusted port. Traffic from that port will have authorization
- VLAN 10 has also undergone dynamic arp inspection VLAN
- Similarly the source and destination mac address are inspected

### 5.1.5 DHCP Snooping Configuration:

```
Datacenter#
Datacenter#sh ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
1
Insertion of option 82 is enabled
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Interface                Trusted      Rate limit (pps)
-----
FastEthernet0/5          no          unlimited
FastEthernet0/2          no          unlimited
FastEthernet0/4          no          unlimited
FastEthernet0/1          yes         unlimited
Datacenter#
```

Figure no. 5.13 DHCP Snooping Configuration

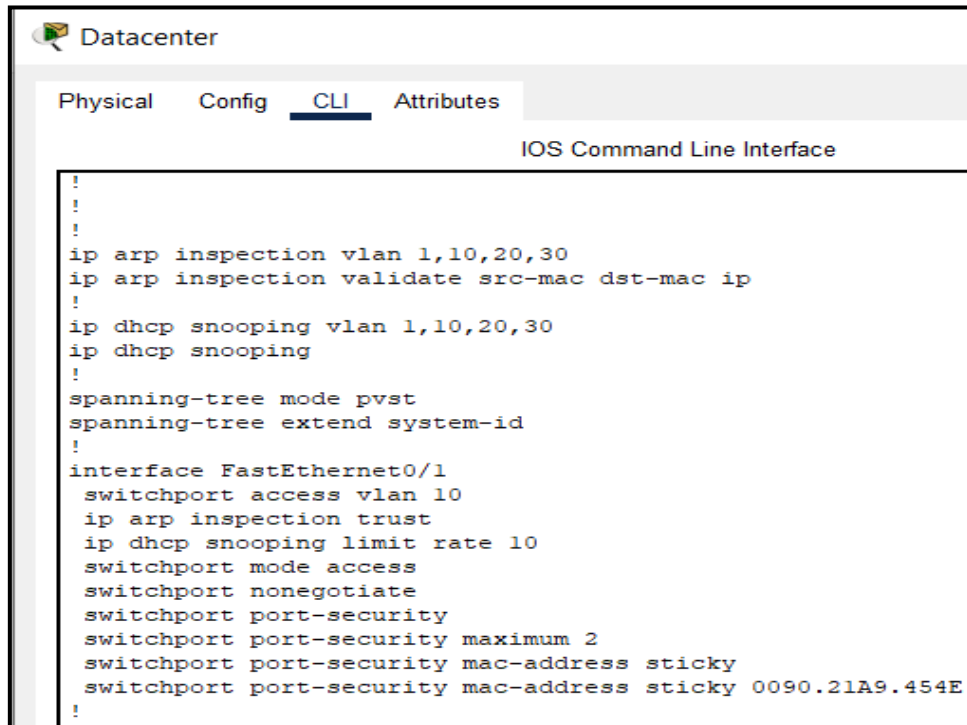
- Fast ethernet 0/1 is set as trusted port and traffic from that port will have authorization

```
Datacenter#
Datacenter#sh ip dhcp snooping binding
MacAddress      IpAddress      Lease(sec)  Type           VLAN
Interface|
-----
00:05:5E:9C:79:89  82.0.0.6      86400       dhcp-snooping  1
FastEthernet0/2
```

Figure no. 5.14 DHCP Show Configuration

- From binding table we can see ip address of our PC

### 5.1.6 VLAN Hopping Configuration:



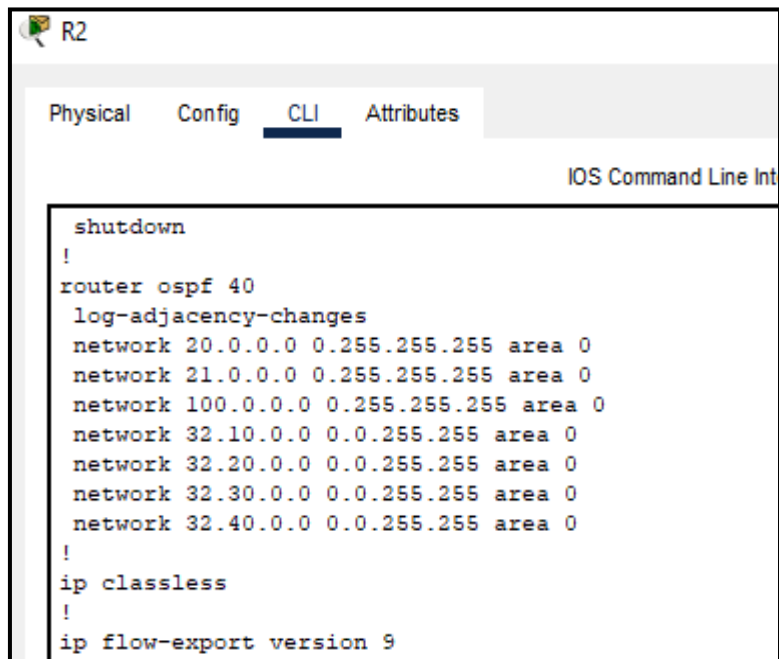
The screenshot shows the CLI interface for a device named 'Datacenter'. The 'CLI' tab is selected. The configuration commands entered are as follows:

```
!
!
!
ip arp inspection vlan 1,10,20,30
ip arp inspection validate src-mac dst-mac ip
!
ip dhcp snooping vlan 1,10,20,30
ip dhcp snooping
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport access vlan 10
 ip arp inspection trust
 ip dhcp snooping limit rate 10
 switchport mode access
 switchport nonegotiate
 switchport port-security
 switchport port-security maximum 2
 switchport port-security mac-address sticky
 switchport port-security mac-address sticky 0090.21A9.454E
!
```

Figure no. 5.15 VLAN Hopping Configuration

- Created 3 VLANs: VLAN 10 for Servers, VLAN 20 for Datacenter, VLAN 30 for Blackhole

### 5.1.7 OSPF Configuration:

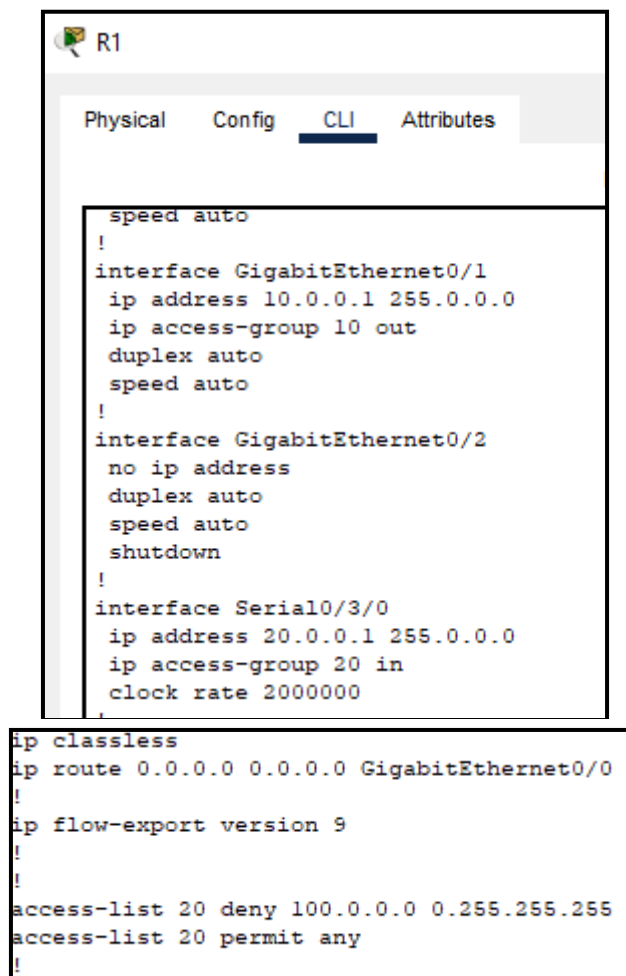


The screenshot shows the CLI interface for a device named 'R2'. The 'CLI' tab is selected. The configuration commands entered are as follows:

```
shutdown
!
router ospf 40
 log-adjacency-changes
 network 20.0.0.0 0.255.255.255 area 0
 network 21.0.0.0 0.255.255.255 area 0
 network 100.0.0.0 0.255.255.255 area 0
 network 32.10.0.0 0.0.255.255 area 0
 network 32.20.0.0 0.0.255.255 area 0
 network 32.30.0.0 0.0.255.255 area 0
 network 32.40.0.0 0.0.255.255 area 0
!
ip classless
!
ip flow-export version 9
```

Figure no. 5.16 OSPF Configuration

### 5.1.8 Access-List Configuration:



```

R1
Physical  Config  CLI  Attributes
!
speed auto
!
interface GigabitEthernet0/1
ip address 10.0.0.1 255.0.0.0
ip access-group 10 out
duplex auto
speed auto
!
interface GigabitEthernet0/2
no ip address
duplex auto
speed auto
shutdown
!
interface Serial0/3/0
ip address 20.0.0.1 255.0.0.0
ip access-group 20 in
clock rate 2000000
!
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0
!
ip flow-export version 9
!
!
access-list 20 deny 100.0.0.0 0.255.255.255
access-list 20 permit any
!
```

Figure no. 5.17 Access-List Configuration



### 5.1.9 Network Performance Parameters Configuration:

#### Step 1: Creating Network Topology

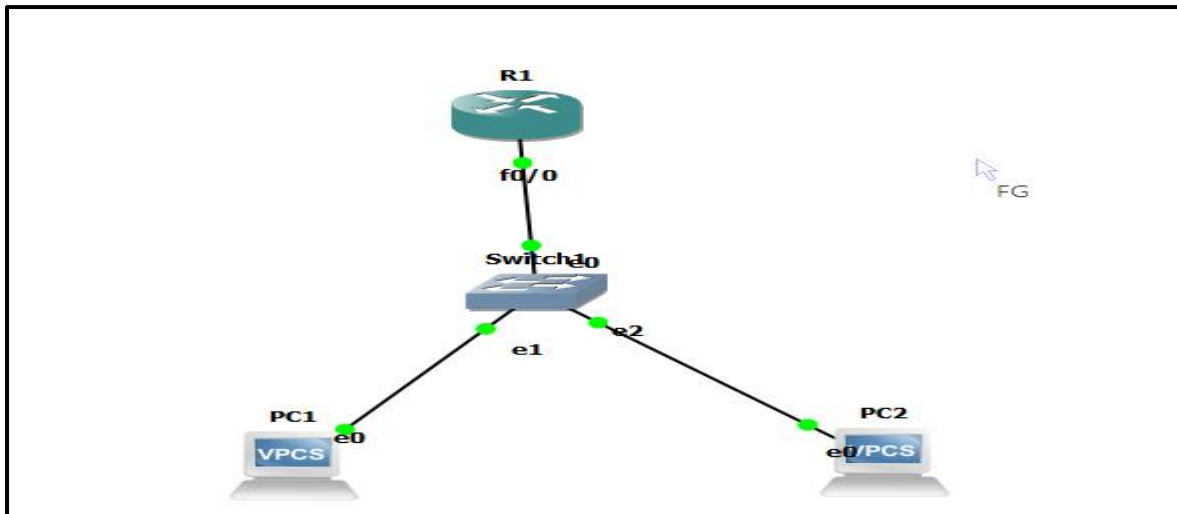


Figure no. 5.18 Network Topology of GNS3

#### Step 2: Importing GNS3 VM

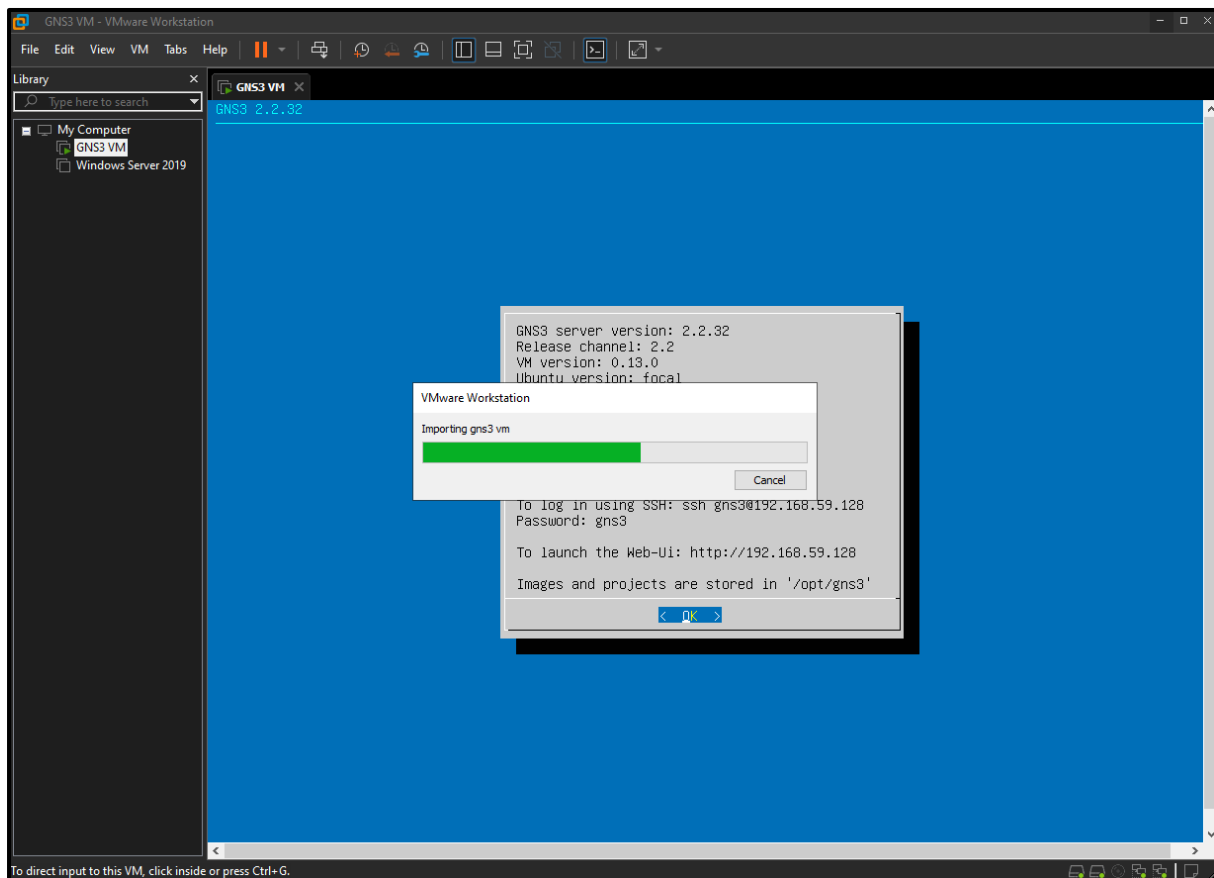


Figure no. 5.19 Importing GNS3 VM

Specifications:

```
GNS3 server version: 2.2.32
Release channel: 2.2
VM version: 0.13.0
Ubuntu version: focal
Qemu version: 4.2.1
Virtualization: vmware
KVM support available: True
Uptime: up 0 minutes

IP: 192.168.59.129 PORT: 80

To log in using SSH: ssh gns3@192.168.59.129
Password: gns3

To launch the Web-Ui: http://192.168.59.129

Images and projects are stored in '/opt/gns3'
```

Figure no. 5.20 GNS3 Specifications

Step 3: Integrating GNS3 VM with PRTG:

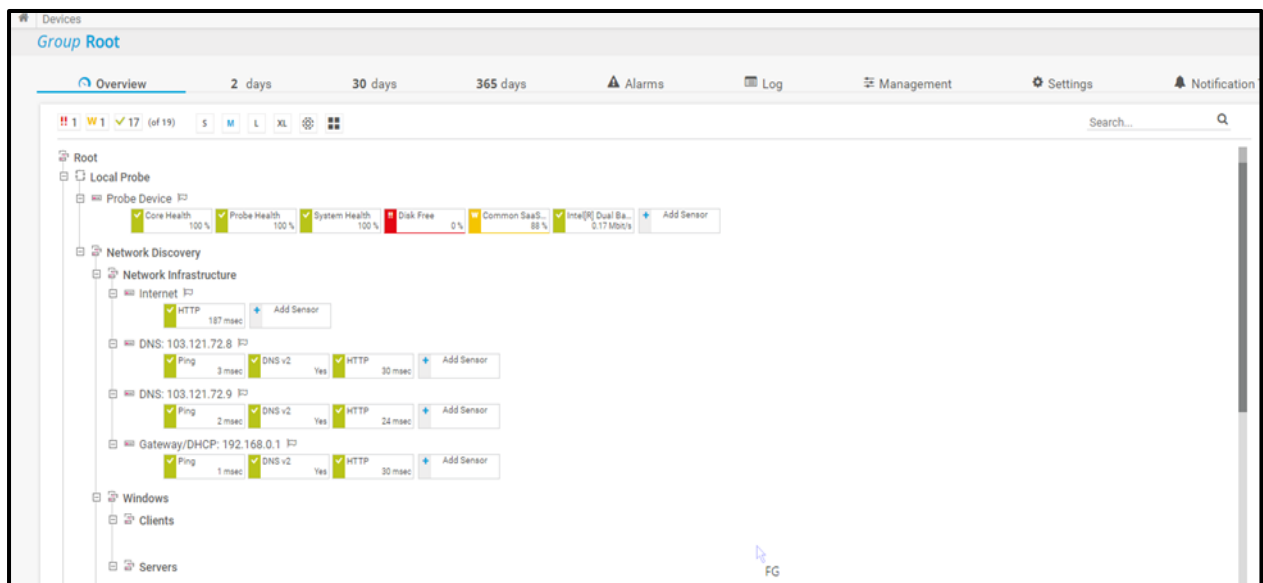


Figure no. 5.21 PRTG 1

## Dashboard of PRTG network layout overview before connecting R1



Figure no. 5.22 PRTG 2

## Step 4: Configuring R1 SNMP Server

```
Compiled Thu 20-Feb-14 06:51 by prod_rel_team
*May 8 22:17:19.863: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
et0/0, changed state to down
*May 8 22:17:19.903: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
et0/1, changed state to down
*May 8 22:17:19.911: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
et1/0, changed state to down
*May 8 22:17:19.923: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
et1/1, changed state to down
*May 8 22:17:20.971: %LINK-5-CHANGED: Interface FastEthernet0/0, changed state
to administratively down
*May 8 22:17:20.979: %LINK-5-CHANGED: Interface FastEthernet0/1, changed state
to administratively down
*May 8 22:17:20.991: %LINK-5-CHANGED: Interface FastEthernet1/0, changed state
to administratively down
*May 8 22:17:20.999: %LINK-5-CHANGED: Interface FastEthernet1/1, changed state
to administratively down
Router>
Router>
Router>
Router>conf t
^
% Invalid input detected at '^' marker.

Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#snmp-
Router(config)#snmp-server com
Router(config)#snmp-server community pu
Router(config)#snmp-server community public RO
Router(config)#do wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
Router(config)#
```

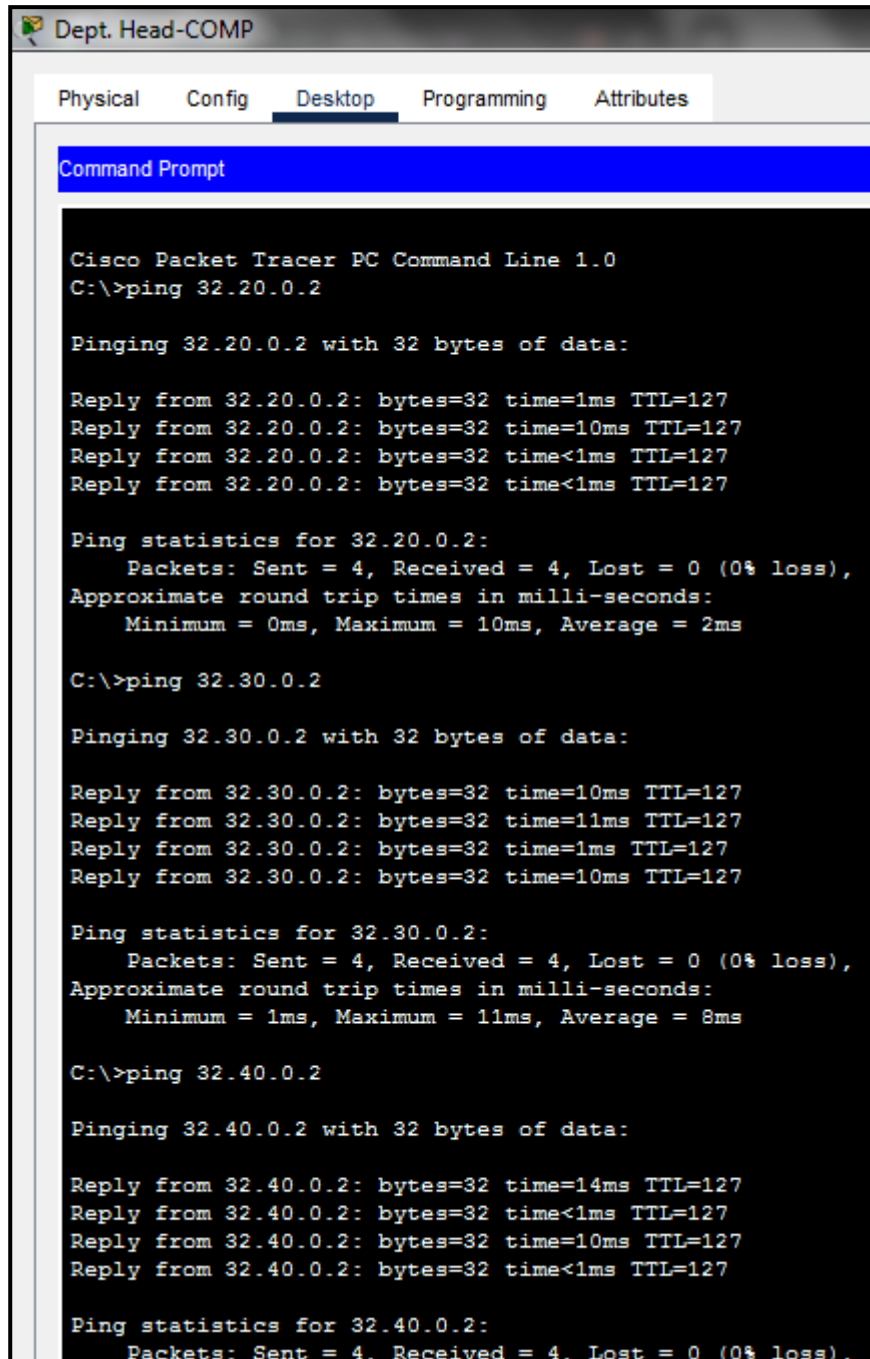
solarwinds | Solar-PuTTY free tool © 2019 SolarWinds Worldwide, LLC. All

Figure no. 5.23 R1 SNMP Server

## 5.2 Results:

### 1) InterVLAN Communication within Departments:

**From Computer Department:** Dept. Head can communicate with professors, students, lab of ComputerDepartment and can also communicate with other department\_s Dept. head, professors, students and lab



```
Dept. Head-COMP
Physical  Config  Desktop  Programming  Attributes

Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 32.20.0.2

Pinging 32.20.0.2 with 32 bytes of data:

Reply from 32.20.0.2: bytes=32 time=1ms TTL=127
Reply from 32.20.0.2: bytes=32 time=10ms TTL=127
Reply from 32.20.0.2: bytes=32 time<1ms TTL=127
Reply from 32.20.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 32.20.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 10ms, Average = 2ms

C:\>ping 32.30.0.2

Pinging 32.30.0.2 with 32 bytes of data:

Reply from 32.30.0.2: bytes=32 time=10ms TTL=127
Reply from 32.30.0.2: bytes=32 time=11ms TTL=127
Reply from 32.30.0.2: bytes=32 time=1ms TTL=127
Reply from 32.30.0.2: bytes=32 time=10ms TTL=127

Ping statistics for 32.30.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 11ms, Average = 8ms

C:\>ping 32.40.0.2

Pinging 32.40.0.2 with 32 bytes of data:

Reply from 32.40.0.2: bytes=32 time=14ms TTL=127
Reply from 32.40.0.2: bytes=32 time<1ms TTL=127
Reply from 32.40.0.2: bytes=32 time=10ms TTL=127
Reply from 32.40.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 32.40.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure no. 5.24 Dept. head PC

```
C:\>ping 32.10.0.3

Pinging 32.10.0.3 with 32 bytes of data:

Reply from 32.10.0.3: bytes=32 time<1ms TTL=128
Reply from 32.10.0.3: bytes=32 time<1ms TTL=128
Reply from 32.10.0.3: bytes=32 time<1ms TTL=128
Reply from 32.10.0.3: bytes=32 time<1ms TTL=128

Ping statistics for 32.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

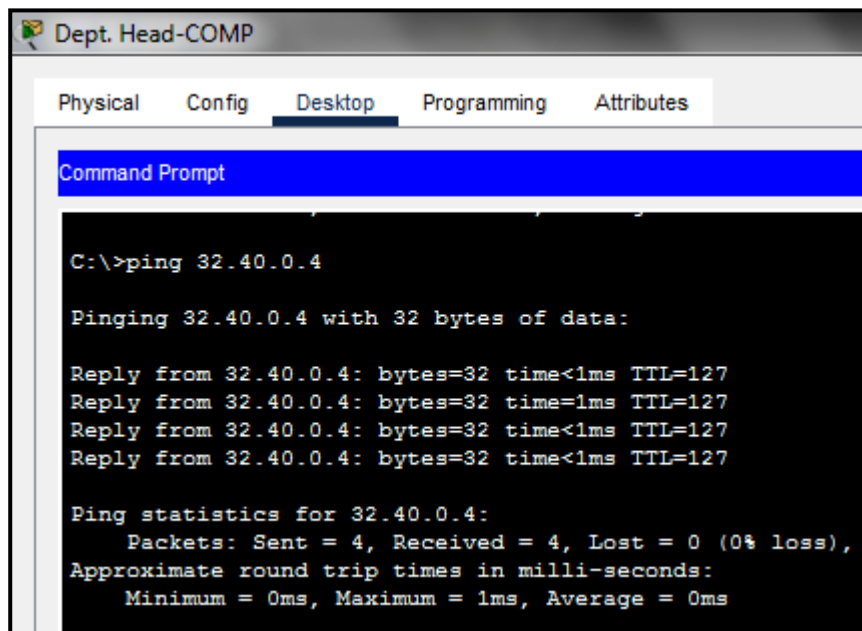
C:\>ping 32.20.0.3

Pinging 32.20.0.3 with 32 bytes of data:

Reply from 32.20.0.3: bytes=32 time<1ms TTL=127
Reply from 32.20.0.3: bytes=32 time<1ms TTL=127
Reply from 32.20.0.3: bytes=32 time<1ms TTL=127
Reply from 32.20.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 32.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Figure no. 5.25 Dept. head PC



The screenshot shows a Windows desktop environment with a window titled "Dept. Head-COMP". The window has several tabs: "Physical", "Config", "Desktop" (which is selected), "Programming", and "Attributes". Inside the "Desktop" tab, there is a "Command Prompt" window. The Command Prompt displays the following text:

```
C:\>ping 32.40.0.4

Pinging 32.40.0.4 with 32 bytes of data:

Reply from 32.40.0.4: bytes=32 time<1ms TTL=127
Reply from 32.40.0.4: bytes=32 time<1ms TTL=127
Reply from 32.40.0.4: bytes=32 time<1ms TTL=127
Reply from 32.40.0.4: bytes=32 time<1ms TTL=127

Ping statistics for 32.40.0.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Figure no. 5.26 Dept. head PC

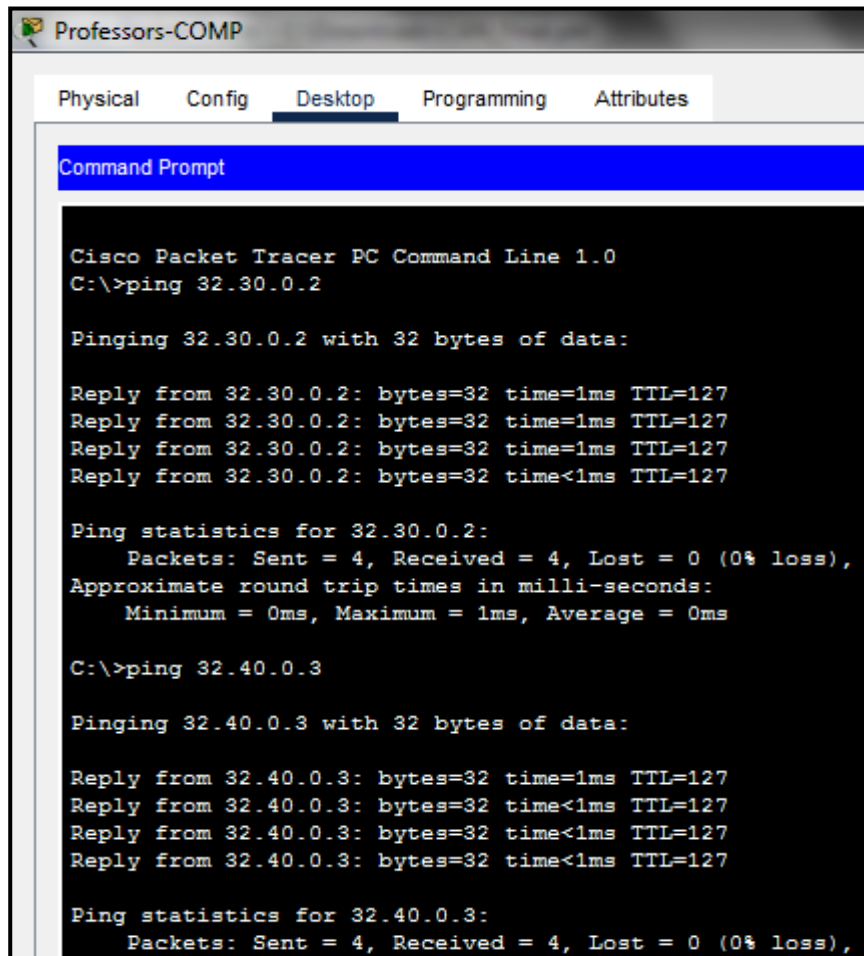
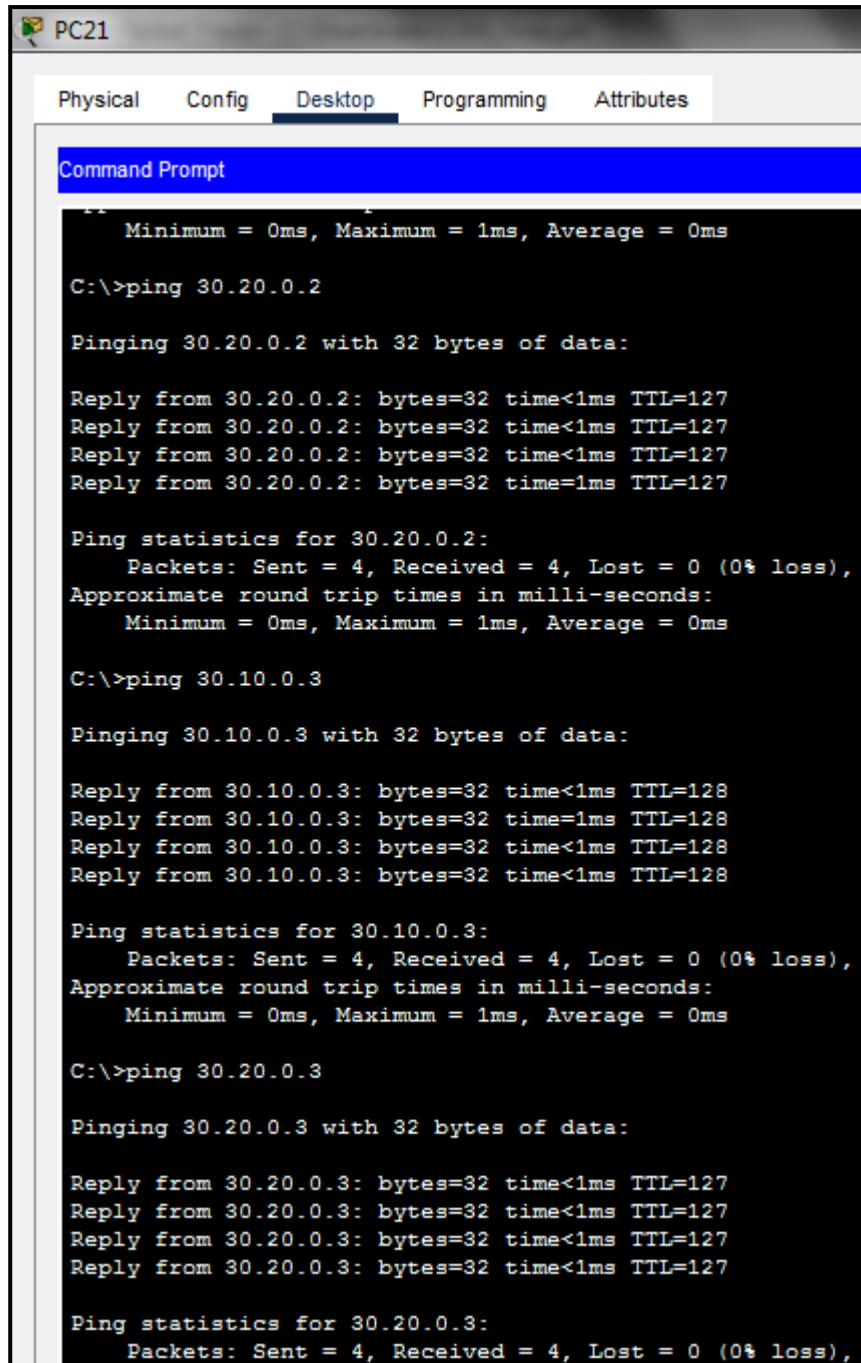


Figure no.5.27 Professors PC

**Note:** Anyone in department can communicate with any other department's Dept. head, professors, students and lab.

## 2) InterVLAN Communication within Hostel-A: (Boys-Hostel)

**From Hostel-A:** Warden from Hostel-A can communicate with students of Hostel-A and also warden, students of Hostel-B

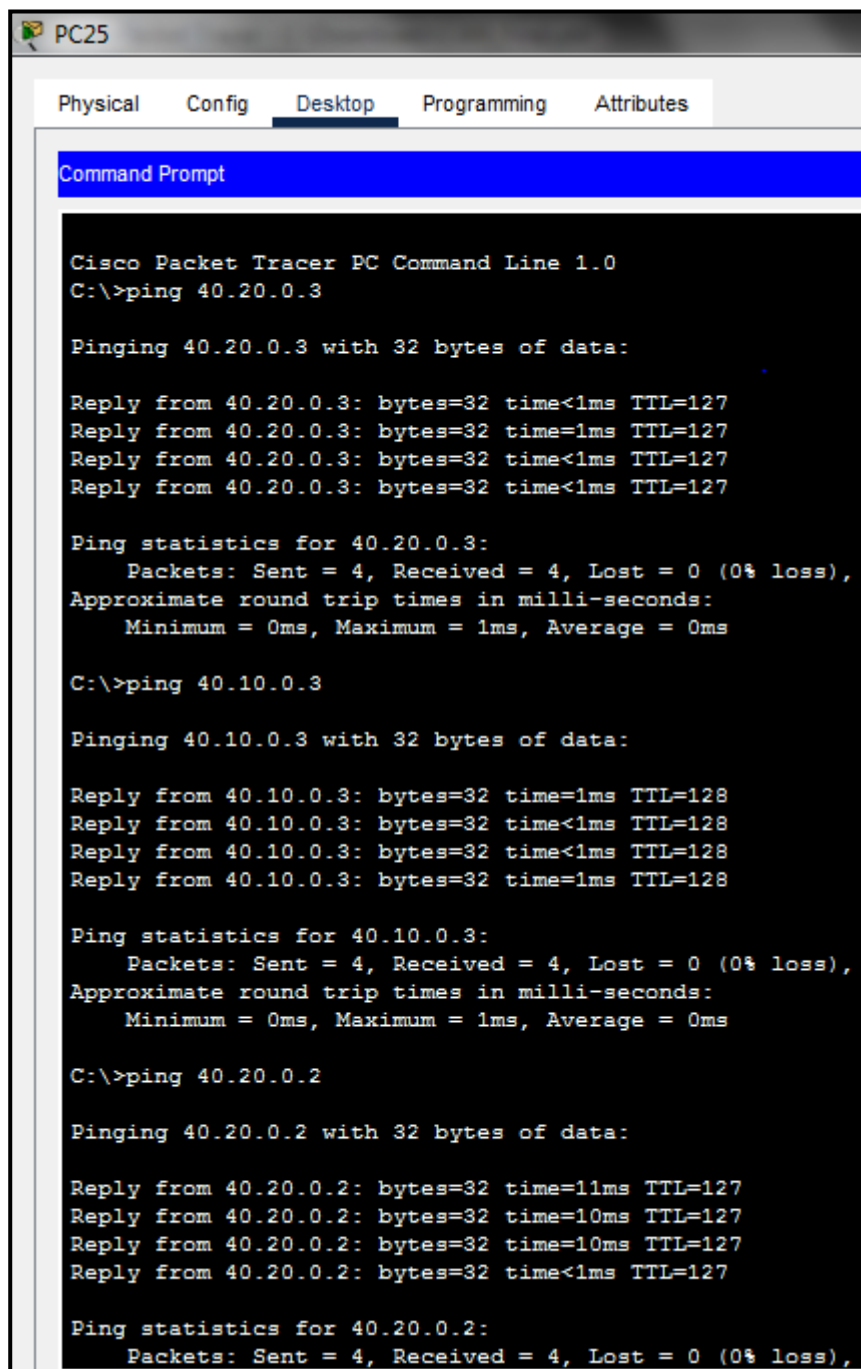


The screenshot shows a PC21 desktop environment with a Command Prompt window open. The window displays the results of three ping commands. The first command is 'ping 30.20.0.2', which shows four successful replies with a time of less than 1ms and a TTL of 127. The second command is 'ping 30.10.0.3', which shows four successful replies with a time of less than 1ms and a TTL of 128. The third command is 'ping 30.20.0.3', which shows four successful replies with a time of less than 1ms and a TTL of 127. All three ping statistics show 0% loss.

```
PC21
Physical Config Desktop Programming Attributes
Command Prompt
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 30.20.0.2
Pinging 30.20.0.2 with 32 bytes of data:
Reply from 30.20.0.2: bytes=32 time<1ms TTL=127
Reply from 30.20.0.2: bytes=32 time<1ms TTL=127
Reply from 30.20.0.2: bytes=32 time<1ms TTL=127
Reply from 30.20.0.2: bytes=32 time=1ms TTL=127
Ping statistics for 30.20.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 30.10.0.3
Pinging 30.10.0.3 with 32 bytes of data:
Reply from 30.10.0.3: bytes=32 time<1ms TTL=128
Reply from 30.10.0.3: bytes=32 time=1ms TTL=128
Reply from 30.10.0.3: bytes=32 time<1ms TTL=128
Reply from 30.10.0.3: bytes=32 time<1ms TTL=128
Ping statistics for 30.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\>ping 30.20.0.3
Pinging 30.20.0.3 with 32 bytes of data:
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Reply from 30.20.0.3: bytes=32 time<1ms TTL=127
Ping statistics for 30.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure no. 5.28 Hostel-A Warden's PC

### 3) InterVLAN Communication within Hostel-C: (Girls-Hostel)



```
PC25
Physical Config Desktop Programming Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ping 40.20.0.3

Pinging 40.20.0.3 with 32 bytes of data:

Reply from 40.20.0.3: bytes=32 time<1ms TTL=127
Reply from 40.20.0.3: bytes=32 time=1ms TTL=127
Reply from 40.20.0.3: bytes=32 time<1ms TTL=127
Reply from 40.20.0.3: bytes=32 time<1ms TTL=127

Ping statistics for 40.20.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 40.10.0.3

Pinging 40.10.0.3 with 32 bytes of data:

Reply from 40.10.0.3: bytes=32 time=1ms TTL=128
Reply from 40.10.0.3: bytes=32 time<1ms TTL=128
Reply from 40.10.0.3: bytes=32 time<1ms TTL=128
Reply from 40.10.0.3: bytes=32 time=1ms TTL=128

Ping statistics for 40.10.0.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ping 40.20.0.2

Pinging 40.20.0.2 with 32 bytes of data:

Reply from 40.20.0.2: bytes=32 time=11ms TTL=127
Reply from 40.20.0.2: bytes=32 time=10ms TTL=127
Reply from 40.20.0.2: bytes=32 time=10ms TTL=127
Reply from 40.20.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 40.20.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Figure no. 5.29 Hostel-C Warden's PC

**From Hostel-A:** Warden from Hostel-C can communicate with students of Hostel-C and also warden, students of Hostel-D



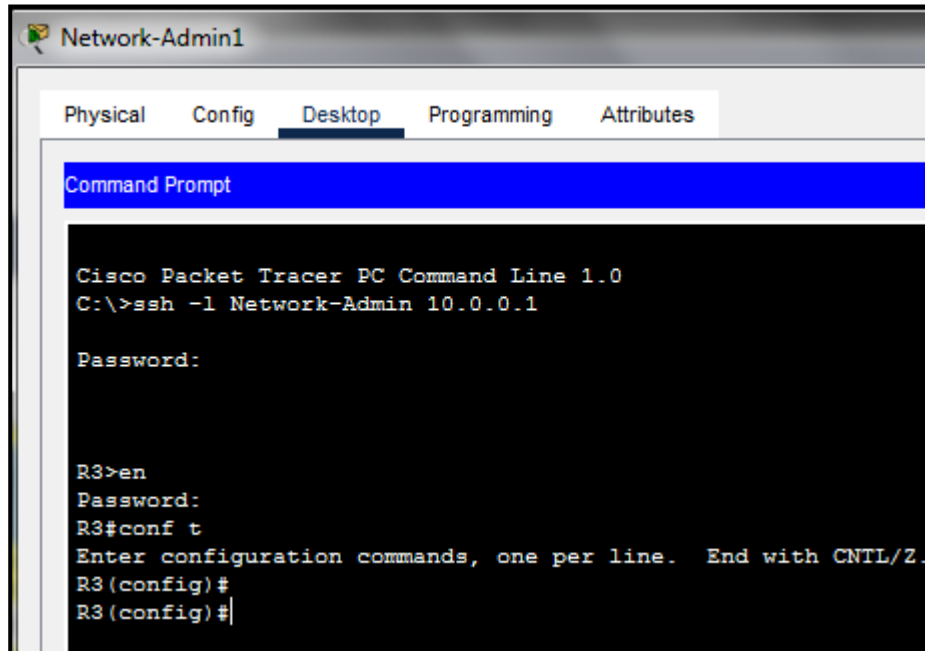
#### 4) SSH:

##### 1) Network-Admin1:

Using SSH, network-admin can remotely access Network- admins

Router and Switch  
Username - Network-Admin Password – network-admin

Password - class



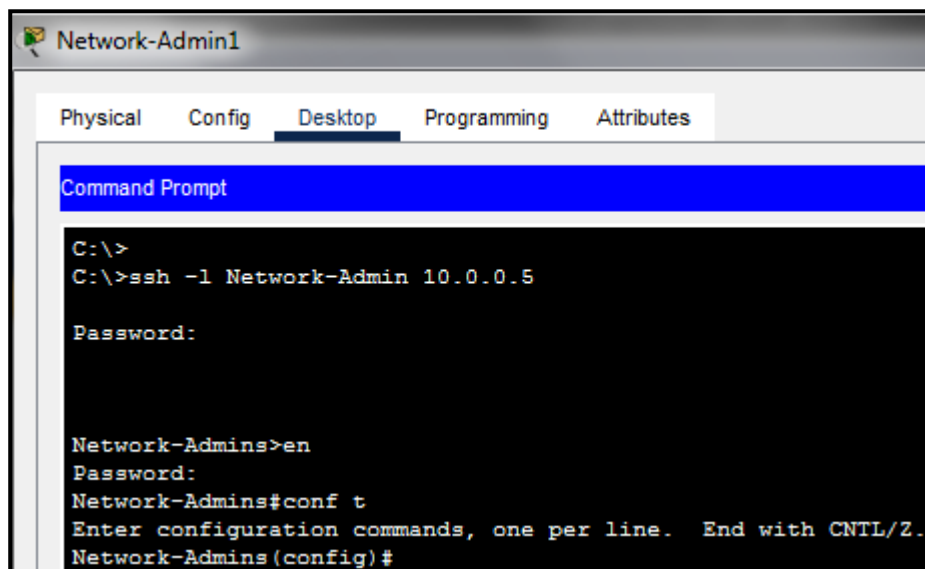
```
Network-Admin1
Physical  Config  Desktop  Programming  Attributes
Command Prompt

Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l Network-Admin 10.0.0.1

Password:

R3>en
Password:
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#
R3(config)#
```

Figure no. 5.30 SSH Configuration (Router)



```
Network-Admin1
Physical  Config  Desktop  Programming  Attributes
Command Prompt

C:\>
C:\>ssh -l Network-Admin 10.0.0.5

Password:

Network-Admins>en
Password:
Network-Admins#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Network-Admins(config)#
```

Figure no. 5.31 SSH Configuration (Switch)

## 5) ARP Spoofing:

```
Network-Admin1
Physical Config Desktop Programming Attributes
Command Prompt
Reply from 82.0.0.2: bytes=32 time=9ms TTL=127
Reply from 82.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 82.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 2ms

C:\>arp -a
    Internet Address      Physical Address        Type
    10.0.0.1              00d0.fff1c.7402        dynamic

C:\>arp -a
    Internet Address      Physical Address        Type
    10.0.0.4              00d0.fff1c.7402        dynamic

C:\>ping 82.0.0.2

Pinging 82.0.0.2 with 32 bytes of data:

Request timed out.
Reply from 82.0.0.2: bytes=32 time<1ms TTL=127
Reply from 82.0.0.2: bytes=32 time<1ms TTL=127
Reply from 82.0.0.2: bytes=32 time<1ms TTL=127

Ping statistics for 82.0.0.2:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>
C:\>arp -a
    Internet Address      Physical Address        Type
    10.0.0.1              00d0.fff1c.7402        dynamic
    10.0.0.4              00d0.fff1c.7402        dynamic

C:\>
```

Figure no. 5.32 ARP Spoofing result

## 6) DHCP Snooping:

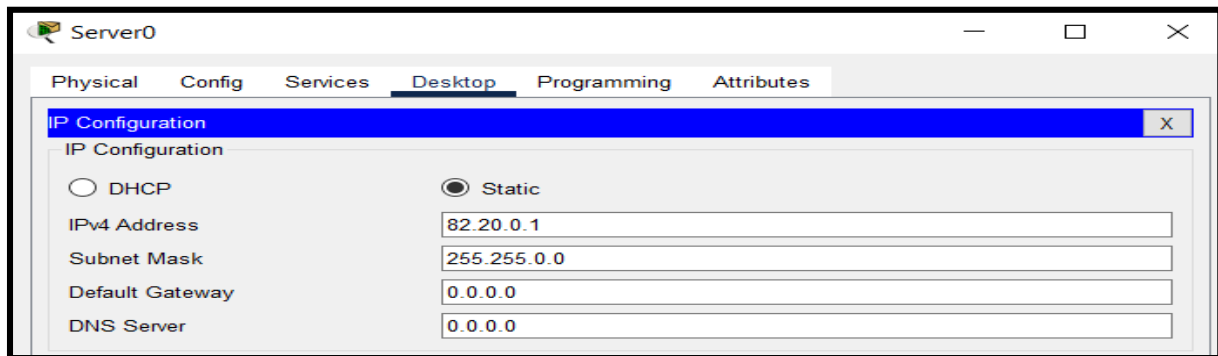


Figure no. 5.33 DHCP Server0

This is Threat Server's IP Address

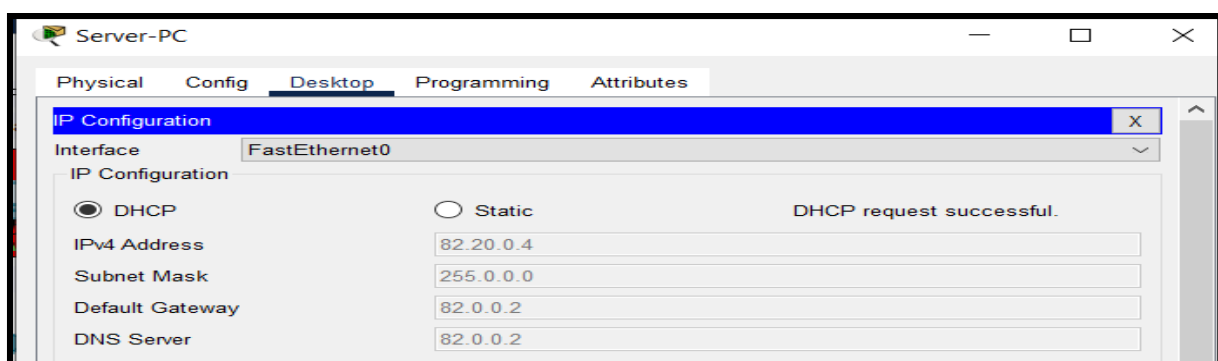


Figure no. 5.34 DHCP Server-PC trusted

Our PC has dynamically accessed Threat Server IP Address

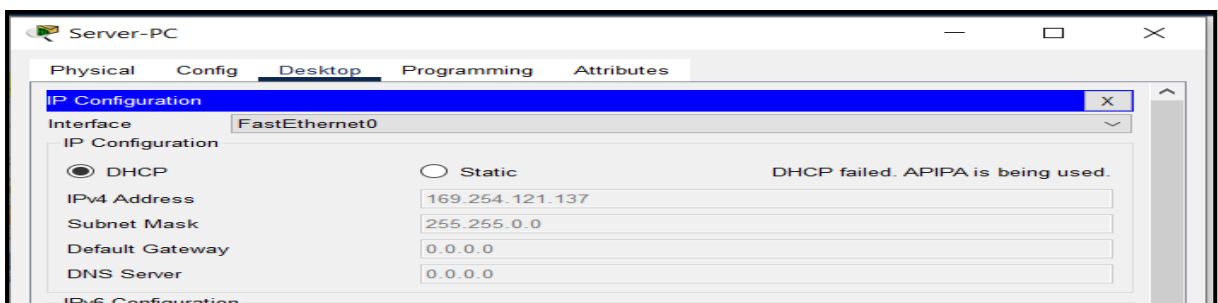


Figure no. 5.35 DHCP Server-PC untrusted

From this image we can see attack is prevented as our pc is unable to access ip address

## 7) VLAN Hopping:

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit	Delete
	Failed	Netw...	Server-PC	ICMP		0.000	N	0	(edit)	
	Failed	Netw...	Server-PC	ICMP		0.000	N	1	(edit)	

Figure no. 5.36 VLAN Hopping Result

We can see traffic from outside network is unable to communicate with datacenter

## 8) OSPF:





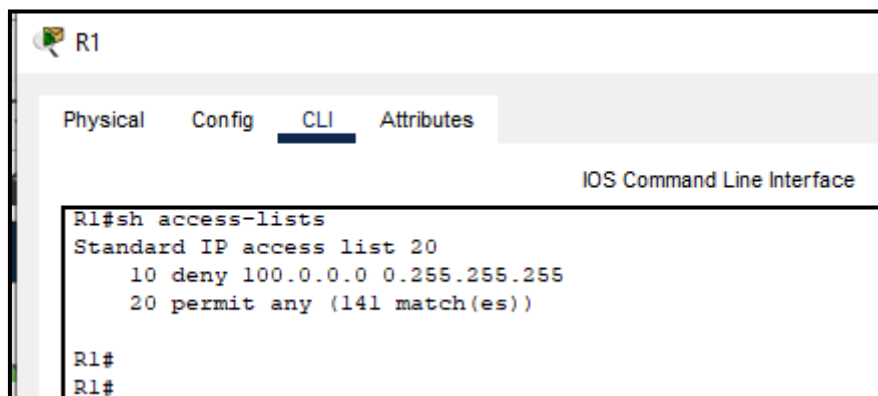
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Ed
	Successful	R1	R3	ICMP		0.000	N	0	(e
	Successful	R2	R3	ICMP		0.000	N	1	(e

Figure no. 5.37 OSPF Result

Router 1, Router 2 and Router 3 can communicate with each other as we configured ospf on these routers

## 9) Access-Lists:



```
R1#sh access-lists
Standard IP access list 20
 10 deny 100.0.0.0 0.255.255.255
 20 permit any (141 match(es))

R1#
R1#
```

Figure no. 5.38 Access-list Show Config Result







Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic	Num	Edit
	Successful	R1	Server-PC	ICMP		0.000	N	0	(ec
	Successful	Netw...	Server-PC	ICMP		0.000	N	1	(ec
	Failed	Rece...	Server-PC	ICMP		0.000	N	2	(ec

Figure no. 5.39 Access-list Result

As network admin has only access to data-center they can communicate with each other but rest of end devices can't communicate with data center

## 10) Network Performance Parameters:

R1 being discovered by PRTG:

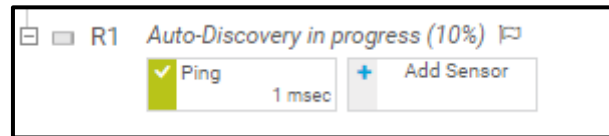


Figure no. 5.40 R1 Discovery

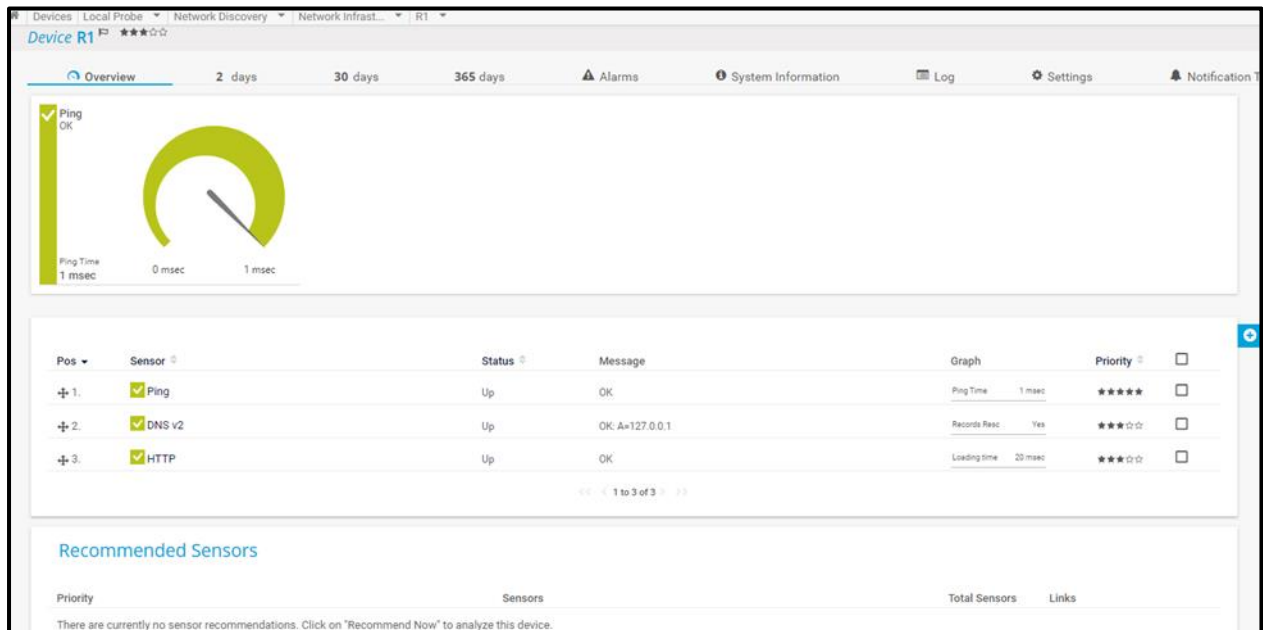


Figure no. 5.41 PRTG Dashboard Result 1

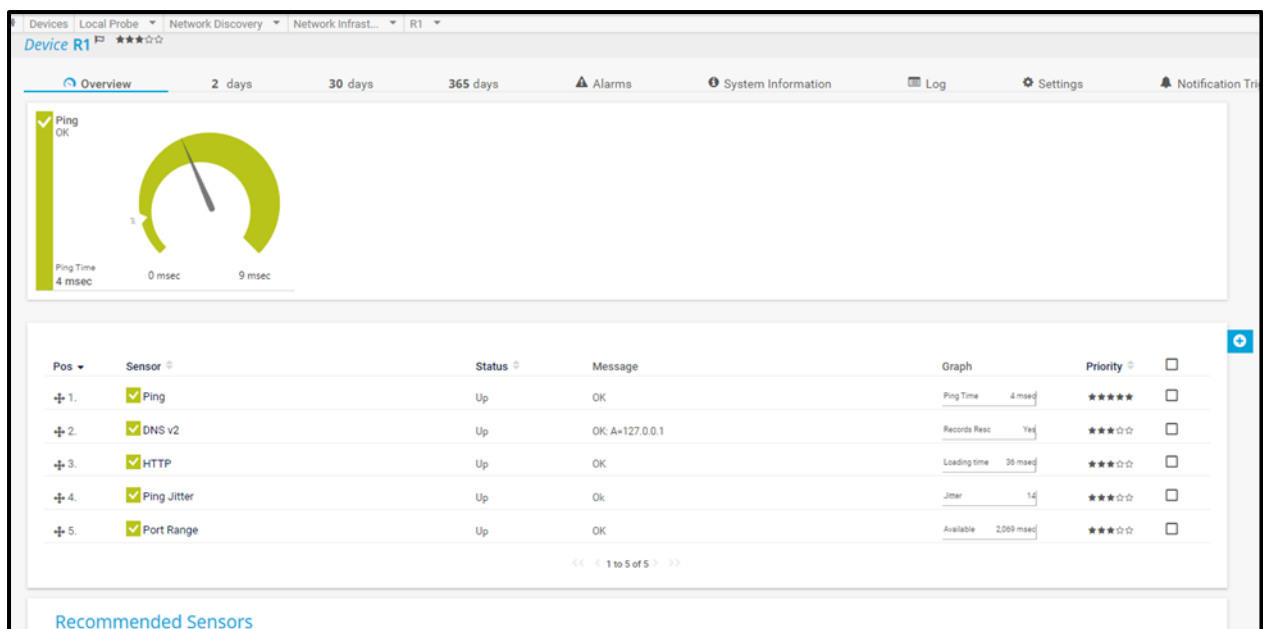


Figure no. 5.42 PRTG Dashboard Result 2

## Chapter 5

### Conclusion and Future Scope

*This chapter presents the conclusions which we have drawn based on the results and how useful will this project be in the future and what other things could be added in this project to make it more viable and advanced.*

#### 5.1 Conclusion:

- Network security is a growing concern in today's digital phenomenon. Hence, it is imperative to have an authorization and authentication system in place to protect the data and system from cyber threats, identify new users, monitor traffic, approve or block unauthorized access.
- We created design of Campus Area Network using Cisco Packet Tracer.
- We learned and implemented VLANS for segregation (Dept. Head, Professors, Students & Labs), InterVlan Routing (Router on Stick Method) for InterVlan communication between different departments, OSPF Routing Protocol for finding best routing path, Access-Control Lists to permit & deny traffic.
- We learned about different servers such as (DNS, HTTP, SMTP, FTP, DHCP) and added these multiple services in one server.
- We have done data center survey to know about existing college network for comparative analysis with our design of campus network.
- We learned and prevented common attacks that are possible in campus network such as (ARP Spoofing, DHCP Snooping, VLAN Hopping).
- We measured network performance parameters by integrating GNS3 with PRTG

#### 5.2 Future Work:

- Creating Service prevention tool to prevent internal and external attacks.
- we can also manage network traffic, enhance network performance in our project.
- Also we can create intrusion detection system to protect the campus network.

## References:

1. Ali, Md. Nadir, "Design and Implementation of a Secure Campus Network", Journal of Surface Engineered Materials and Advanced Technology, 2015
2. L. Huang, "Research on Campus Network Security Management Technology Based on Big Data," 2019 International Conference on Smart Grid and Electrical Automation (ICSGEA), 2019, pp. 571-575, doi: 10.1109/ICSGEA.2019.00133.
3. Kumari, Lalita & Debbarma, Swapan & Shyam, Radhey, "Security Problems in Campus Network and Its Solutions", International Journal of Advanced Engineering & Applications (IJAEA), 2011, Volume-1. pp 98-101.
4. G.Michael, "Design and Implementation of a Secure Campus Network" 2017 International Journal of Pure and Applied Mathematics(IJPAM), Volume 116 No. 8 2017, 303-307
5. Doss, Srinath & S.Panimalar, S.Panimalar & Simla, A.Jerrin & J.Deepa, J.Deepa, (2015). "Detection and Prevention of ARP spoofing using Centralized Server", International Journal of Computer Applications. 113. 26-30. 10.5120/19935-1931.
6. Nuhu, Abdulhafiz, "Mitigating DHCP starvation attack using snooping technique" FUDMA Journal of Sciences, 2020, 4. 560.
7. Bull, Ronny & Matthews, Jeanna & Trumbull, Kaitlin, "VLAN hopping, ARP poisoning and Man-In-The-Middle Attacks in Virtualized Environments", 2016
8. H. Ning and X. Bing, "The research and analysis of security of campus network," 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference, 2011, pp. 25-27, doi: 10.1109/ITAIC.2011.6030268.
9. M. N. B. Ali, M. L. Rahman and S. A. Hossain, "Network architecture and security issues in campus networks," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2013, pp. 1-9, doi: 10.1109/ICCCNT.2013.6726595.
10. X. Li and T. Jiang, "Design and implementation of the campus network monitoring system," 2014 IEEE Workshop on Electronics, Computer and Applications, 2014, pp. 117-119, doi: 10.1109/IWECA.2014.6845571.
11. Mohammed Nadir Bin Ali, Mohamed Emran Hossain, Md. Masud Parvez<sup>3</sup>, "Design and Implementation of a Secure Campus Network" July 2015 International Journal of Emerging Technology and Advanced Engineering
12. Joysankar Bhattacharjee, "Design and Implementation of a Cost-effective and Secured Private Area Network for smooth as well as hassle-free Computing in the University Campus" Jan - Feb 2016 IOSR Journal of Electronics and Communication Engineering
13. J. Lu, "Research and Implementation of Security Technology in Campus Network Construction," 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA), 2019, pp. 219-224, doi: 10.1109/ICCNEA.2019.00050.
14. F. Yan, Y. Jian-Wen and C. Lin, "Computer Network Security and Technology Research," 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015, pp. 293-296, doi: 10.1109/ICMTMA.2015.77

## **Acknowledgements**

We would like to express our gratitude to our guide, Dr. Kiran Ajetroa as well as our principal Dr. Shubha Pandit who gave us the golden opportunity to do this wonderful project. We are immensely thankful for their constant mentoring, reviewing, and support during our implementation. His advice and support helped us to move in the right direction towards completion of the project. We would like to thank him for his time, help and efforts towards this project. This also helped us in doing a lot of research and exploring our technical knowledge.

Thank you very much.