

SAVEETHA SCHOOL OF ENGINEERING
SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL
SCIENCES

CHENNAI 602105



INDUSTRY INTERNSHIP REPORT

ON

**“TELECOM INDUSTRY PRACTICES IN BROADBAND DATA
COMMUNICATION”**

at



**(BSNL-Advanced Level Telecom Training Centre (ALTTC), Ghaziabad,
Hyderabad)**

SUBMITTED BY

NAME: A.PRAVEEN

REG.NO: 191712256

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING**

JUNE 2021

SAVEETHA SCHOOL OF ENGINEERING
SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL
SCIENCES
CHENNAI 602105



INDUSTRY INTERNSHIP REPORT

ON

**“TELECOM INDUSTRY PRACTICES IN BROADBAND DATA
COMMUNICATION”**

at



**(BSNL-Advanced Level Telecom Training Centre (ALTTC), Ghaziabad,
Hyderabad)**

NAME: A.PRAVEEN

REG.NO: 191712256

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION
ENGINEERING**

JUNE 2021

ACKNOWLEDGEMENT

The Industrial Exposure that I have experienced in (**RTTC Hyderabad**) has helped me a lot not only in improving my theoretical knowledge but also to understand the working of a large industry. I am grateful to the company for giving me an opportunity to undergo internship in their organization. I would like to express my gratitude towards **Mr.M.Prasad** for associating me in this training.

I take this opportunity to extend our heartfelt thanks to our beloved Principal, **Dr.B.Ramesh**, for providing me the opportunity to undergo this internship.

I express my sincere thanks to our Program Director, **Dr. Kirupa Ganapathy**, for being a constant source of inspiration and also providing permission to undergo my internship.

I would also like to thank our placement coordinator **Mr. P.Jagadeesh** and our internship coordinator **Ms.Priyanka** for helping me in completing this internship successfully.

TABLE OF CONTENTS

1. Introduction on internship project	5
2. About the Company.....	6
(I)Introduction of the Company.....	6
(II)Mission of the Company.....	6
(III)Vision of the Company.....	7
(IV)Profile of the Company.....	8
(V) Profile of the company mentor	9
3. Day-by-day Work Details.....	10
[1] Day 1: “Topics of the day”.....	10
[2] Day 2: “Topics of the day”.....	11
[3] Day 3: “Topics of the day”.....	11
.	
.	
....	
[21] Day 21 “Topics of the day”.....	21
4. Internship project details	22
[I] Introduction	
[II] Methodology	
[III] Project work	
[IV] Outcome	
5. Conclusion.....	27
Outcome of the Internship program	
6. Certificate of the internship	29

1. INTRODUCTION

Designing a campus area network with a Virtual Local Area Network (VLAN) and Physical Network Security Implementation, as well as Internet connection via wired and wireless access.

This project involves the creation of a college campus area network with VLANs for various hosts and departments in order to meet the following requirements.

1. The college campus is a five-story building with (Ground + 4) floors.
2. A CISCO 2811 Router with a single LAN port provides 100Mbps Internet access to the ISP on the ground floor.
3. There are elevators on the first, second, third, and fourth levels. Hosts are from the CSC/IT/ECE/EEE departments and work in the classrooms of first-year, second-year, third-year, and fourth-year students. A switch connects these hosts on each floor.
4. The top-floor switch is linked directly to the next-floor switch, and then a cable is run from the first-floor switch to the LAN port of the CISCO Router 2811.
5. The administrator has been ordered to configure the departments in distinct VLAN domains and to ensure that they communicate with one another.
6. On a case-by-case basis, the administrator has been asked to instal a wireless access point with a security password from the fourth floor.
7. The administrator has been requested to generate security credentials for the Router and Switches, so that only authorised users may log in.
8. The administrator has been instructed to ensure that no one connects a host to any of the switch's empty ports on any level.
9. For Internet access, the administrator has been instructed to provide 40 Mbps bandwidth to CSC, 30 Mbps bandwidth to IT, 20 Mbps bandwidth to ECE, and 10 Mbps bandwidth to EEE departments.
10. The ISP assigned the college the 10.10.10.0/30 subnet and instructed the administrator to setup the WAN connection IP 10.10.10.1 at the College's WAN interface on the Router. The college's Internet IP pool is 117.117.117.0/29.
11. Administrator has been instructed to make sure that all computers available in the campus should be connected with Internet (except 192.168.2.3).
12. Administrator has been asked put college website IP as 117.117.117.3 and this website has to be accessed from Internet.

2. ABOUT THE COMPANY

I) Introduction of the Company:

The Department of Telecommunications created the Regional Telecom Training Centre in Hyderabad in 1975 to provide training to their employees. This training institution is located on 42 acres of land in Ghaziabadi, Hyderabad's I.T. hub. This includes the administrative and academic blocks, as well as the Hostel Block. With the increasing expansion in the telecom sector, labour is needed to plan, construct, operate, and maintain telecom networks. Fixed access landline phone and broadband, GSM and CDMA wireless, 3G, data networks, and optical fibre networks are all examples of telecom networks. For each of these areas and activities, certain talents are necessary.

II) Mission of the Company:

To improve human resource confidence, competence, and commitment via training in telecom technology, information technology, and behavioural science in order to fulfil BSNL's objectives.

III) Vision of the Company:

To attain world-class training in telecommunications and information technology.

IV) Profile of the Company:

Bharat Sanchar Nigam Limited (BSNL), (A Government of India Enterprise), An ISO 9001:2008 Certified Institute, Regional Telecom Training Centre(RTTC) Hyderabad is a fully standards-compliant Training Center, established by BSNL to impart training in Latest Telecom Technologies and Information Technology to its employees all over India. It also offers value-added Certification Courses and Major/Mini projects to B.Tech/B.E/MCA students in ECE and CSE/IT from various Engineering Colleges in Telangana/Andhra Pradesh and beyond.

Mail:bsnlrttchyd@gmail.com.

IV) Profile of the Company Mentor:

Name: Mr.M. Devi Prasad.

Designation in the company: Division Engineer(DE).

Contact no: 9176757408

Mail id : deviprasadmadiraju@gmail.com

3. DAY-BY-DAY WORK DETAILS

DAY 1:-

Wireless Communication Technologies

3 hrs (10AM-1PM)

DAY 2:-

Assessment over topics covered (Viva Voce)

3 hrs (10AM-1PM)

DAY 3:-

Antennas

3 hrs (10AM-1PM)

DAY 4:-

Optical Fiber in Communication

3 hrs (10AM-1PM)

DAY 5:-

Multiplexing and Multiple Access Technologies

3 hrs (10AM-1PM)

DAY 6:-

Digital Communication

3 hrs (10AM-1PM)

DAY 7:-

LAN, WAN, MAN technologies.

3 hrs (10AM-1PM)

DAY 8:-

Topologies in Networking.

3 hrs (10AM-1PM)

DAY 9,10:-

Introduction to CISCO PACKET TRACER and IP Addresses for project work.

3 hrs (10AM-1PM)

DAY 11:-

Connection of End devices with Switch in a VLAN.

3 hrs (2PM-5PM)

DAY 12:-

Implementation of Network Topologies in CISCO PACKET TRACER.

3 hrs (2PM-5PM)

DAY 13:-

Designing of VLAN in CISCO PACKET TRACER.

3 hrs (2PM-5PM)

DAY 14:-

Introduction to ISP Router

3 hrs (2PM-5PM)

DAY 15:-

Interconnection of VLAN in CISCO PACKET TRACER

3 hrs (2PM-5PM)

DAY 16:-

Wireless End devices to the LAN using Access Point.

3 hrs (2PM-5PM)

DAY 17:-

Security password implementation for Switch and Routers to avoid connecting unknown devices to VLAN.

3 hrs (2PM-5PM)

DAY 18:-

Connecting the VLAN to ISP routers and servers.

3 hrs (2PM-5PM)

DAY 19:-

WAN and IP pool allocation to the Network created in CISCO PACKET TRACER.

3 hrs (2PM-5PM)

DAY 20:-

Accessing the Website with the WAN.

3 hrs (2PM-5PM)

DAY 21:-

Final Assessment (Viva Voce).

3 hrs (2PM-5PM)

4. INTERNSHIP PROJECT DETAILS

(I) Introduction

All user devices, servers, switches, routers, cables, and wireless access points are all housed in a LAN. A LAN is made up of all devices that are part of the same broadcast domain. A broadcast domain is made up of all LAN-connected devices, and when one of them transmits a broadcast frame, all the other devices receive a copy of it. A LAN and a broadcast domain are practically the same thing from one perspective. A switch considers all of its interfaces to be in the same broadcast domain if it doesn't have VLANs. That is, when a broadcast frame reached one of the switch's ports, the switch sent the frame to all other ports. According to this logic, two distinct Ethernet LAN switches are required to generate two different LAN broadcast domains. With VLAN support, a single switch may achieve the same design goals of creating two broadcast domains with a single switch. A switch can use VLANs to assign certain interfaces to one broadcast domain and others to another, resulting in numerous broadcast domains. Virtual LANs are the separate broadcast domains generated by the switch (VLAN). Using additional VLANs, each with a lower number of devices, while designing campus LANs can benefit the LAN in a variety of ways. A broadcast transmitted by one host in a VLAN, for example, will be received and processed by all other hosts in the VLAN, but not by hosts in another VLAN. The number of hosts that receive a single broadcast frame is limited, which minimises the number of hosts that waste time processing unnecessary broadcasts. Because fewer hosts view frames delivered by a single host, security threats are reduced. These are only a few of the reasons why hosts should be divided into distinct VLANs.

The reasons for creating smaller broadcast domains (VLANs) are summarised in the following list:

- Decrease the number of devices that receive each broadcast frame to reduce CPU overhead on each device.
- To lower security concerns by limiting the number of hosts that get copies of frames flooded by switches (broadcasts, multicasts, and unknown unicasts)
- By putting hosts that transfer critical data on a different VLAN, you may increase security.
- To develop more adaptable designs that organise users by department or by collaborative groups rather than by physical location.

Packet Tracer is a Cisco Systems cross-platform visual simulation application for creating network topologies and simulating contemporary computer networks. Users may use the programme to mimic Cisco router and switch configurations using a simulated command line interface. Packet Tracer's user interface is drag-and-drop, enabling users to add and delete simulated network devices as needed. The programme is primarily designed as an instructional tool for Certified Cisco Network Associate Academy students to help them understand essential CCNA principles.

Packet Tracer enables students to construct sophisticated and massive networks, which is frequently not possible with actual hardware owing to cost considerations. Because Packet Tracer is accessible for free, CCNA Academy students frequently utilise it. By animating these pieces in a visual manner, Packet Tracer may help you comprehend abstract networking concepts like the Enhanced Interior Gateway Routing Protocol. Packet Tracer may also be used in education since it includes features such as a writing system, network protocol simulation, and a knowledge evaluation system.

Cisco Packet Tracer's major goal is to assist students understand networking fundamentals via hands-on experience while also developing Cisco-specific abilities. This programme cannot replace hardware routers or switches because the protocols are implemented solely in software. Surprisingly, this utility includes not only Cisco equipment, but also a wide range of other networking devices. Before implementing any protocol, engineers want to test it using Cisco Packet Tracer. Engineers that want to deploy any modification in the production network prefer to utilise Cisco Packet Tracer to test the changes first and then deploy if and only if everything works as planned.

Key Features:

- Unlimited devices
- E-learning
- Interactive Environment
- Visualizing Networks
- Real-time mode and Simulation mode
- Self-paced
- Supports majority of networking protocols
- International language support

(II) Methodology

Step 1: Domain connection for VLANs. In a five-story college, the first step is to construct VLAN domains for various departments, such as CSE/IT/EEE/ECE. To accomplish so, initially computers are placed on each level from the first to the fourth, and a switch with the appropriate number of ports is placed on each floor. Using the fast Ethernet cable of copper straight through switch-pc connections are given and using fast Ethernet cable of copper cross over cable switches are connected. Next, each pc is assigned with a static IP address with the suitable subnet masking and gateway. Now, in order to achieve communication between the pcs of same vlan domains the switches should be configured according to the fast Ethernet interfaces, vlan domain numbers and department names. The switch-pc interfaces are given with access mode and switch-switch interfaces are given with trunk mode. In order to check the connectivity between pcs of same domain, is given. The following figure shows the connectivity within the vlan domain.

Step2: Inter VLAN communication. It is required to connect the computers in different departments within a college. So, we need to use a Router to connect different VLAN domains. Router receives the traffic from each switch and then with its protocol communication can be achieved for different networks. The router used is CISCO2811 which is placed in the ground floor of the college and connected to switch of first floor. Just like the switches router should also be configured and it is set to trunk mode in the interface. Within an interface we can also create the sub interfaces with suitable encapsulation codes as required for each network as router consists of minimum no. of interface ports. Finally, the router configuration is saved using write command. By this step, we can achieve the communication between various departments of different networks within the college. The following figure shows the inter VLAN communication in the college.

Step3: Allocation of wireless connectivity for particular devices. There are a lot of wireless devices used inside a building and they need wireless connectivity. For, that purpose we need to connect an Access point to the switch and configure the access point with the switch and set an SSID and password to access the wireless connectivity. Let us take a laptop and put the NIC card to it and give an IP address to the laptop and thus we can access the wireless connection by connecting with the use of SSID and password set to Access point. A line is shown in the software after connectivity is

achieved. The following figure shows the connection between laptop and Access Point.

Step4:

Security for Router and Switches. The routers and switches should not be accessed by any intruders and they should not get the access as it may lead to malfunctioning of the college equipment. For that purpose, we have to give suitable encryptions to the router for telnet access, console access and configuration access. So, we use the suitable commands and write them to the router. An encryption code is given so that the password cannot be seen while typing it. For the switch, it is sufficient to give console security command so that except for the administrator any other person cannot access the switch ports and configure them on their own. As we have used a 24 port switch, it is necessary to shutdown the unused ports so that intruders cannot connect their devices to those ports. The figures shows the shutdown of the ports that are unused in the switch and also the intruder PC unable to connect to college network.

(III) Project work

Connecting to WAN-ISP:

The ISP has given a subnet of 10.10.10.0/30 to connect to the WAN. For this network the college side router is connected to ISP router using a fast Ethernet cable and with the IP address to college is 10.10.10.1 and to ISP 10.10.10.2. After giving the configurations a green colour link is established between college side and ISP side.

Internet Connection:

ISP has given a pool of IPs to the college with subnet 117.117.117.3 for the internet and let us have 117.117.117.1 to connect all the PCs to Internet. For internet connection a server should be placed at the college and it should be interfaced with the college switch port. Using the GUI we give the IP address to college server and also we edit the HTML document for purpose of college need. We can verify the server connectivity by pinging it with the gateway and also checking with the PCs of the departments in the college using browser GUI in the software. Thus the college website can be accessed using any of the PCs present in the college. Once we connect to the Internet the PCs in the college can be able to access all the websites present in the internet. We can verify it by using a test server present at the ISP side. Let the test server be given with the IP address 2.2.2.2 and the figure shows the website accessed by PC present in the college.

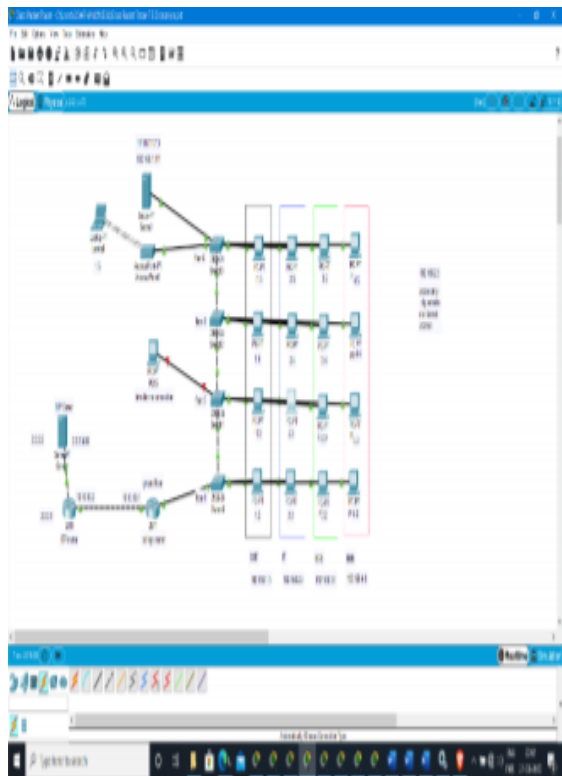
Restriction of particular PC to access Internet:

We can make the PC 192.168.2.3 not to access the internet by configuring in the college side router. The following figures shows the outputs.

Allocation of Bandwidth:

It is not necessary to allocate same bandwidth to each department in the college. So, the bandwidth can be allocated to each department in the college side router. In the configuration terminal of the router, we need to go to the sub interface of the fast Ethernet 0/0 and allocate the bandwidth to each department according to the requirement.

(IV) Outcome



```

# Configuration for the network

# Core Routers
R1: 10.0.0.1, 10.0.0.2, 10.0.0.3, 10.0.0.4
R2: 10.0.0.5, 10.0.0.6, 10.0.0.7, 10.0.0.8
R3: 10.0.0.9, 10.0.0.10, 10.0.0.11, 10.0.0.12
R4: 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.16

# Edge Routers
E1: 10.0.1.1, 10.0.1.2, 10.0.1.3, 10.0.1.4
E2: 10.0.1.5, 10.0.1.6, 10.0.1.7, 10.0.1.8
E3: 10.0.1.9, 10.0.1.10, 10.0.1.11, 10.0.1.12
E4: 10.0.1.13, 10.0.1.14, 10.0.1.15, 10.0.1.16

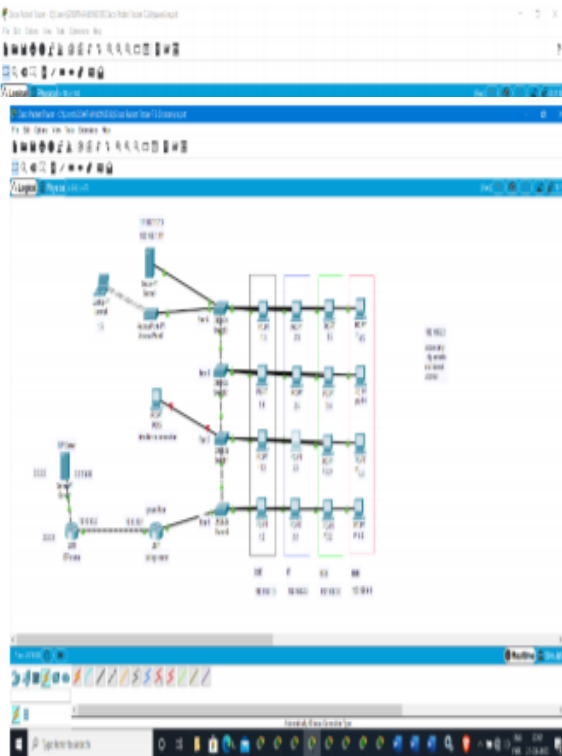
# Servers
S1: 10.0.2.1, 10.0.2.2, 10.0.2.3, 10.0.2.4
S2: 10.0.2.5, 10.0.2.6, 10.0.2.7, 10.0.2.8
S3: 10.0.2.9, 10.0.2.10, 10.0.2.11, 10.0.2.12
S4: 10.0.2.13, 10.0.2.14, 10.0.2.15, 10.0.2.16

# Configuration for the network
# Core Routers
R1: 10.0.0.1, 10.0.0.2, 10.0.0.3, 10.0.0.4
R2: 10.0.0.5, 10.0.0.6, 10.0.0.7, 10.0.0.8
R3: 10.0.0.9, 10.0.0.10, 10.0.0.11, 10.0.0.12
R4: 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.16

# Edge Routers
E1: 10.0.1.1, 10.0.1.2, 10.0.1.3, 10.0.1.4
E2: 10.0.1.5, 10.0.1.6, 10.0.1.7, 10.0.1.8
E3: 10.0.1.9, 10.0.1.10, 10.0.1.11, 10.0.1.12
E4: 10.0.1.13, 10.0.1.14, 10.0.1.15, 10.0.1.16

# Servers
S1: 10.0.2.1, 10.0.2.2, 10.0.2.3, 10.0.2.4
S2: 10.0.2.5, 10.0.2.6, 10.0.2.7, 10.0.2.8
S3: 10.0.2.9, 10.0.2.10, 10.0.2.11, 10.0.2.12
S4: 10.0.2.13, 10.0.2.14, 10.0.2.15, 10.0.2.16

```



```

# Configuration for the network

# Core Routers
R1: 10.0.0.1, 10.0.0.2, 10.0.0.3, 10.0.0.4
R2: 10.0.0.5, 10.0.0.6, 10.0.0.7, 10.0.0.8
R3: 10.0.0.9, 10.0.0.10, 10.0.0.11, 10.0.0.12
R4: 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.16

# Edge Routers
E1: 10.0.1.1, 10.0.1.2, 10.0.1.3, 10.0.1.4
E2: 10.0.1.5, 10.0.1.6, 10.0.1.7, 10.0.1.8
E3: 10.0.1.9, 10.0.1.10, 10.0.1.11, 10.0.1.12
E4: 10.0.1.13, 10.0.1.14, 10.0.1.15, 10.0.1.16

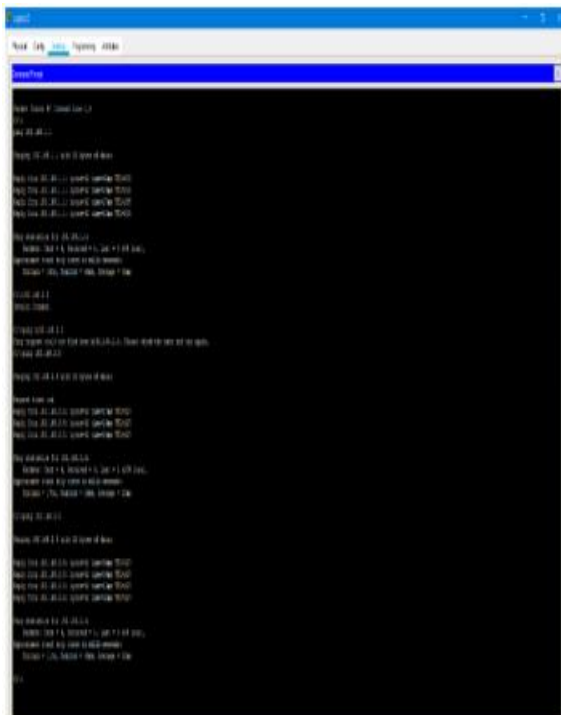
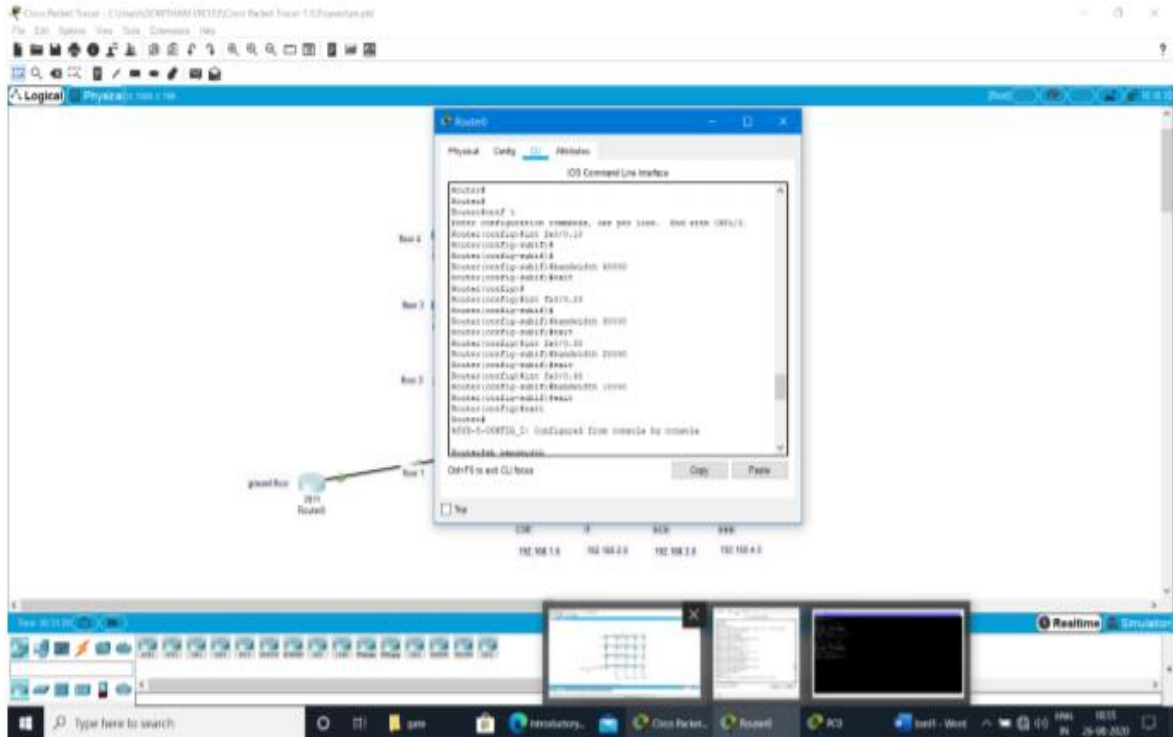
# Servers
S1: 10.0.2.1, 10.0.2.2, 10.0.2.3, 10.0.2.4
S2: 10.0.2.5, 10.0.2.6, 10.0.2.7, 10.0.2.8
S3: 10.0.2.9, 10.0.2.10, 10.0.2.11, 10.0.2.12
S4: 10.0.2.13, 10.0.2.14, 10.0.2.15, 10.0.2.16

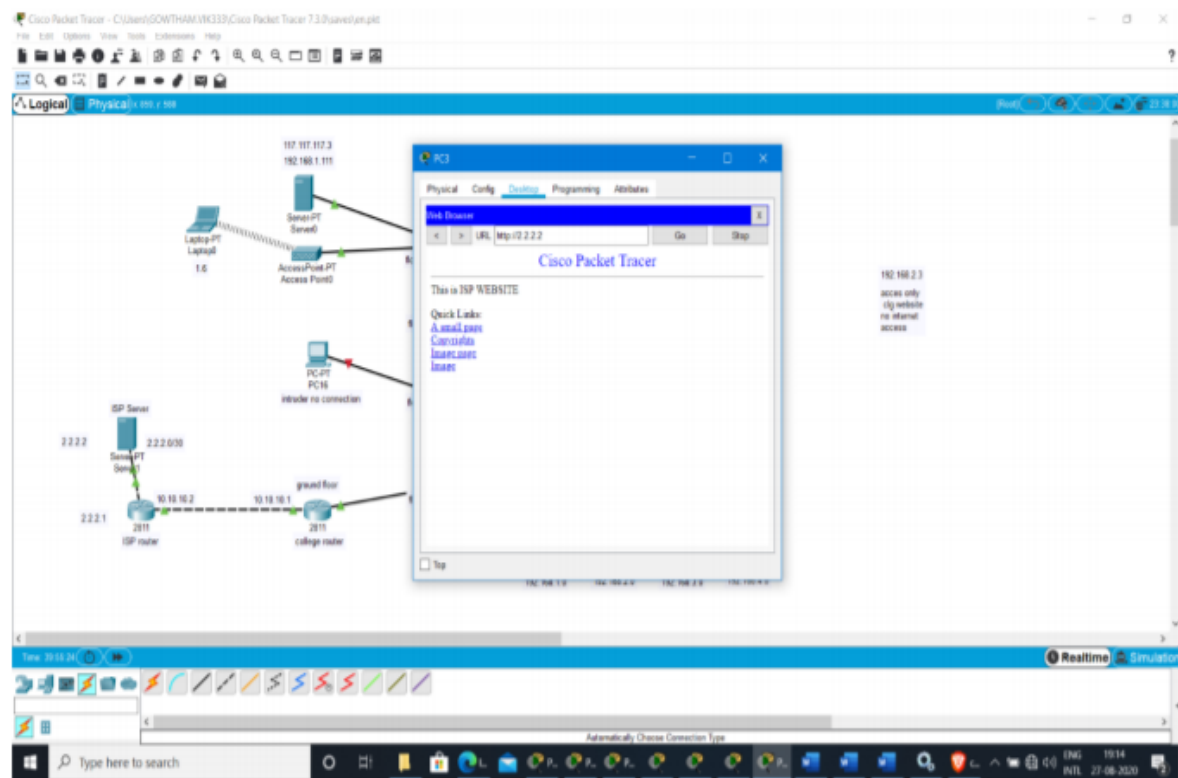
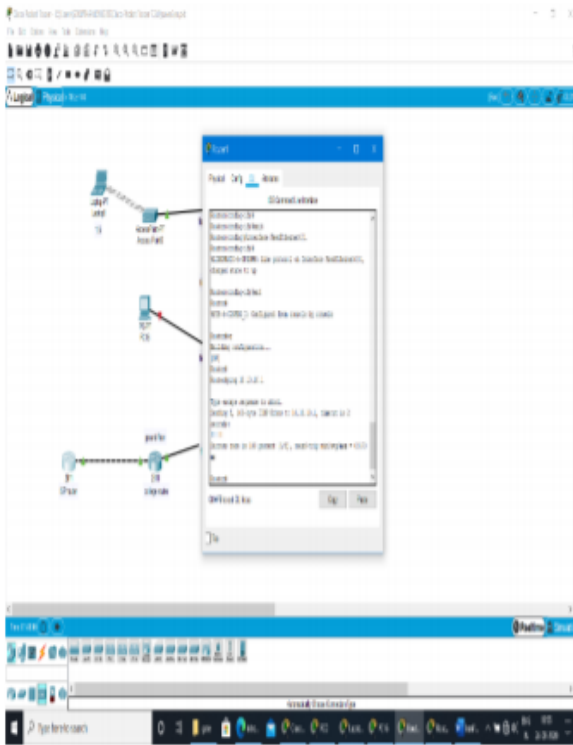
# Configuration for the network
# Core Routers
R1: 10.0.0.1, 10.0.0.2, 10.0.0.3, 10.0.0.4
R2: 10.0.0.5, 10.0.0.6, 10.0.0.7, 10.0.0.8
R3: 10.0.0.9, 10.0.0.10, 10.0.0.11, 10.0.0.12
R4: 10.0.0.13, 10.0.0.14, 10.0.0.15, 10.0.0.16

# Edge Routers
E1: 10.0.1.1, 10.0.1.2, 10.0.1.3, 10.0.1.4
E2: 10.0.1.5, 10.0.1.6, 10.0.1.7, 10.0.1.8
E3: 10.0.1.9, 10.0.1.10, 10.0.1.11, 10.0.1.12
E4: 10.0.1.13, 10.0.1.14, 10.0.1.15, 10.0.1.16

# Servers
S1: 10.0.2.1, 10.0.2.2, 10.0.2.3, 10.0.2.4
S2: 10.0.2.5, 10.0.2.6, 10.0.2.7, 10.0.2.8
S3: 10.0.2.9, 10.0.2.10, 10.0.2.11, 10.0.2.12
S4: 10.0.2.13, 10.0.2.14, 10.0.2.15, 10.0.2.16

```





In the network, VLAN offers Virtual Segmentation of the Broadcast Domain. Devices that are part of the same VLAN can communicate with one another. Routing allows devices from different VLANs to communicate with one another. As a result, the network addresses of various VLAN devices will be different. Any broadcast domain is a virtual LAN (VLAN).

6. CERTIFICATE

RHYTMNB1743-2020-7454123



ADVANCED LEVEL TELECOM TRAINING CENTRE (ALTTC), GHAZIABAD
(UNO'S ITU CENTRE OF EXCELLENCE)
APEX TRAINING INSTITUTE OF BSNL (A GOVT. OF INDIA ENTERPRISE)
A Joint Venture Of International Telecommunication Union, Geneva, UNDP And The Government Of India In 1975

CERTIFICATE

This is to Certify that Mr./Ms.
ALURU PRAVEEN

has successfully completed live interactive online training
ONLINE INTERNSHIP TRAINING WITH PROJECT-ECE-4WEEKS

with effect from 05/08/2020 TO 01/09/2020

at RTTC HYDERABAD

We wish him/her all the best for a bright future.

01/09/2020
DATE


Chief General Manager
(ALTTC)