Build New World

DADI INSTITUTE OF ENGINEERING & TECHNOLOGY

Diet

(Approved by A.I.C.T.E., New Delhi & Permanently Affiliated to JNTUK, Kakinada)
NAAC Accredited Institute and Inclusion under Section 2(f) & 12(B) of UGC Act
An ISO 9001:2008; ISO 14001:2004 & OHSAS 18001:2007 Certified Institution
NH-16, Anakapalle – 531002, Visakhapatnam, A.P.
Mobile: +91 9963981111, Website: www.diet.edu.in, E-mail: info@diet.edu.in

Anakapalle,
Dt: 5-05-2019

From,
Mr.K Joginaidu
HOD - ECE,
Dadi Institute of Engineering & Technology.

(Through Proper Channel)

To,

The Principal,
Dadi Institute of Engineering & Technology.

Sub: Request to approve and permit III B.Tech. and IV B.Tech. ECE students to take up Two weeks internship training at BSNL – Reg

Sir,

With due respect, hereby stating that, I, on behalf of the ECE Department request you for sending III B.Tech. and IV B.Tech. ECE students for a two weeks internship training at BSNL from 13-05-2019.

We, therefore, hope that you would be kind enough to grant us the permission. Waiting anxiously for your reply.

Thanking you

Yours Sincerely,

HOD-ECE, DIET

Naidu

Head of the Department
Electronics & Communication Engg
Dadi Institute of Engg. & Tech.
Anakapalle – 531 002

DADI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Approved by A.I.C.T.E., New Delhi & Permanently Affiliated to JNTUK, Kakinada)
NAAC Accredited Institute and Inclusion under Section 2(f) & 12(B) of UGC Act
An ISO 9001:2008; ISO 14001:2004 & OHSAS 18001:2007 Certified Institution
NH-16, Anakapalle – 531002, Visakhapatnam, A.P.
Mobile: +91 9963981111, Website: www.diet.edu.in, E-mail: info@diet.edu.in

CIRCULAR

DATE: 7-05-2019

This is to inform all the Students, Teaching & Technical Staff of Dadi Institute of Engineering and Technology that the Department of Electronics & Communication Engineering is arranging a two weeks internship training at BSNL for III and IV ECE B.Tech. students from 13-05-2019.

HOD ECE

Naidu

Head of the Department
Electronics & Communication Engg
Dadi Institute of Engg. & Tech
Anakapalle 531 002

REPORT ON TWO WEEKS INTERNSHIP AT BHARAT SANCHAR NIGAM LIMITED

Students of III B.Tech. ECE and IV B.Tech. completed an internship for two weeks in Networking at BSNL from 13/05/2019 to 27/05/2019.

TELECOM NETWORK:

A **telephone network** is a telecommunications network that connects telephones, which allows telephone calls between two or more parties, as well as newer features such as fax and internet.

There are a number of different types of telephone network:

- A landline network where the telephones must be directly wired into a single telephone exchange. This is known as the public switched telephone network or PSTN.
- A wireless network where the telephones are mobile and can move around anywhere within the coverage area.
- A private network where a closed group of telephones are connected primarily to each other and use a gateway to reach the outside world. This is usually used inside companies and call centres and is called a private branch exchange (PBX).
- Integrated Services Digital Network (ISDN)

Public telephone operators (PTOs) own and build networks of the first two types and provide services to the public under license from the national government. Virtual Network Operators (VNOs) lease capacity wholesale from the PTOs and sell on telephony service to the public directly.

Public Switched Telephone Network (PSTN) is an agglomeration of an interconnected network of telephone lines owned by both governments as well as commercial organizations.

Properties of PSTN

- It is also known as Plain Old Telephone Service (POTS)
- It has evolved from the invention of the telephone by Alexander Graham Bell.

- The individual networks can be owned by national government, regional government or private telephone operators.
- Its main objective is to transmit human voice in a recognizable form.
- It is an aggregation of circuit-switched networks of the world.
- Originally, it was an entirely analog network laid with copper cables and switches.
- Presently, most part of PSTN networks is digitized and comprises a wide variety of communicating devices.
- The present PSTNs comprises copper telephone lines, fibre optic cables, communication satellites, microwave transmission links and undersea telephone lines. It is also linked to cellular networks.
- The interconnection between the different parts of the telephone system is done by switching centres. This allows multiple telephone and cellular networks to communicate with each other.

Benefits Of Wi-Fi

It offers the following productivity, conveniences, and cost advantages over traditional wired networks:

Mobile: Wi-Fi systems can provide LAN users with access to real-time information anywhere in their organization

·Installation Speed and Simplicity: Installing a Wi-Fi system can be fast and easy and can eliminate the need to pull cable through walls and ceilings.

·Installation Flexibility: Wireless technology allows the network to go where wire cannot go.

·Reduced Cost-of-Ownership: While the initial investment required for Wi- Fi Hardware can be higher than the cost of wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower.

·Scalability: Wi-Fi systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to full infrastructure networks of thousands of users that allow roaming over a broad area.

Types of Network Topology:

a) Mesh Topology:

In a mesh topology, every device is connected to another device via a particular channel.

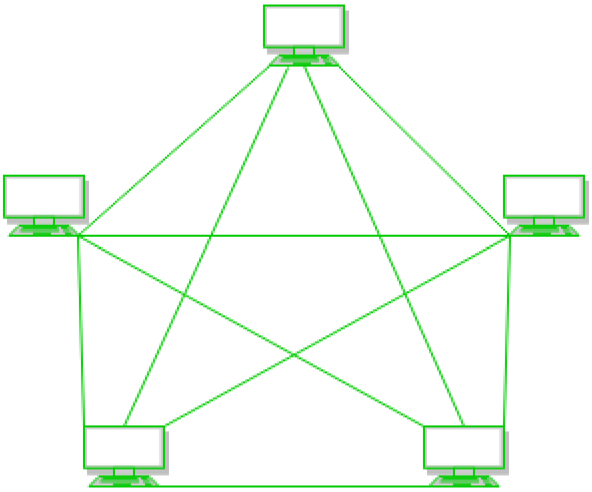


Figure 1: Every device is connected with another via dedicated channels. These channels are known as links.

- Suppose, N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. Total number of ports required=N*(N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is ${}^{N}C_2$ i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of this topology:

- It is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Problems with this topology:

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

b) Star Topology :

In star topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them.

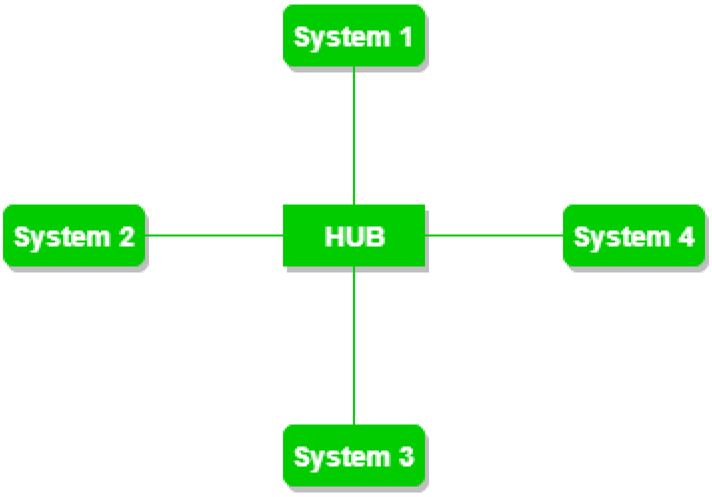


Figure 2: A star topology having four systems connected to a single point of connection i.e., hub.

Advantages of this topology:

If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.

Each device requires only 1 port i.e., to connect to the hub, therefore the total number of ports required is N.

Problems with this topology:

If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.

The cost of installation is high.

Performance is based on the single concentrator i.e., hub.

c) Bus Topology:

Bus topology is a network type in which every computer and network device is connected to a single cable. It transmits the data from one end to another in a single direction. No bi-directional feature is in bus topology. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

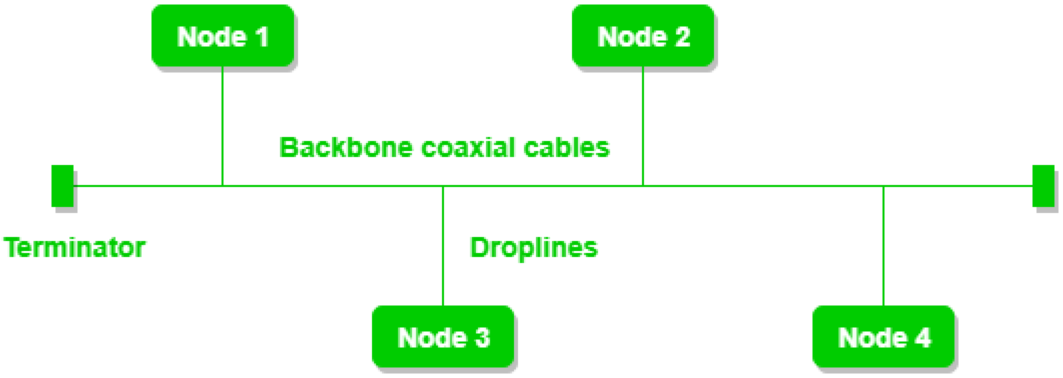


Figure 3: A bus topology with shared backbone cable. The nodes are connected to the channel via drop lines.

Advantages of this topology:

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, which is known as backbone cable, and N drop lines are required.
- The cost of the cable is less as compared to other topologies, but it is used to build small networks.

Problems with this topology:

- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.

d) Ring Topology:

In this topology, it forms a ring connecting devices with its exactly two neighbouring devices.

A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.

The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.

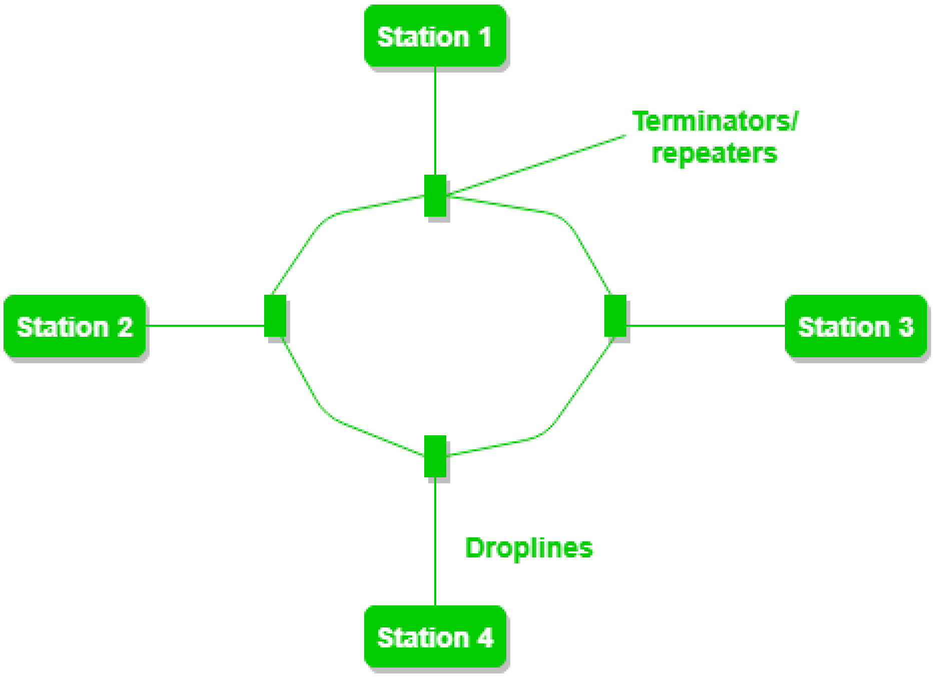


Figure 4: A ring topology comprises 4 stations connected with each forming a ring.

The following operations take place in ring topology are :

1. One station is known as a **monitor** station which takes all the responsibility to perform the operations.
2. To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
3. When no station is transmitting the data, then the token will circulate in the ring.
4. There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delay token release** releases the token after the acknowledgment is received from the receiver.

Advantages of this topology:

- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.

Problems with this topology:

- Troubleshooting is difficult in this topology.

- The addition of stations in between or removal of stations can disturb the whole topology.
- Less secure.

e) Tree Topology:

This topology is the variation of Star topology. This topology has a hierarchical flow of data.

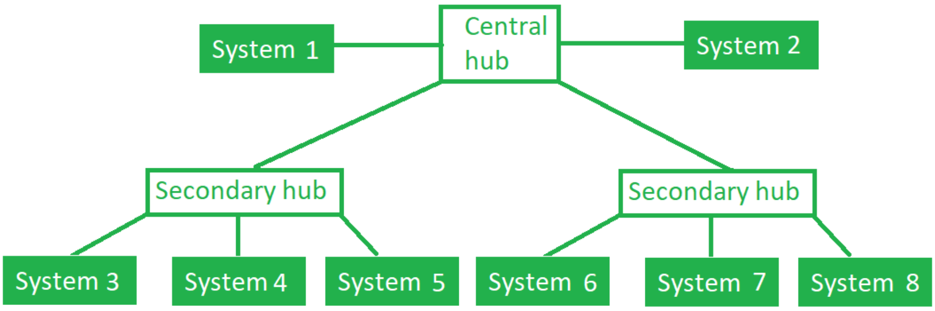


Figure 5: In this, the various secondary hubs are connected to the central hub which contains the repeater. In this data flow from top to bottom i.e., from the central hub to secondary and then to the devices or from bottom to top i.e., devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of this topology:

- It allows more devices to be attached to a single central hub thus it decreases the distance that is travelled by the signal to come to the devices.
- It allows the network to isolate and also prioritize different computers.

Problems with this topology:

- If the central hub fails the entire system fails.

- The cost is high because of cabling.

DIFFERENCE BETWEEN IPV4 AND IPV6 PROTOCOLS

IPv4	**IPv6**
IPv4 has a 32-bit address length	IPv6 has a 128-bit address length
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end, connection integrity is Unachievable	In IPv6 end to end, connection integrity is Achievable
It can generate 4.29×10^{9} address space	Address space of IPv6 is quite large it can produce 3.4×10^{38} address space
The Security feature is dependent on application	IPSEC is an inbuilt security feature in the IPv6 protocol
Address representation of IPv4 is in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by the sender
In IPv4 Packet flow identification is not available	In IPv6 packet flow identification are Available and uses the flow label field in the header
In IPv4 checksum field is available	In IPv6 checksum field is not available

It has broadcast Message Transmission Scheme	In IPv6 multicast and anycast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided

What is a Router?

The router is a physical or virtual internetworking device that is designed to receive, analyse, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets. There are some popular companies that develop routers; such are **Cisco**, **3Com**, **HP**, **Juniper**, **D-Link**, **Nortel**, etc. Some important points of routers are given below:

- A router is used in **LAN** (Local Area Network) and **WAN** (Wide Area Network) environments. For example, it is used in **offices** for connectivity, and you can also establish the connection between distant networks such as from **Bhopal** to
- It shares information with other routers in networking.
- It uses the routing protocol to transfer the data across a network.
- Furthermore, it is more **expensive** than other networking devices like switches and hubs.
- A router works on the **third layer** of the OSI model, and it is based on the IP address of a computer. It uses protocols such as ICMP to communicate between two or more networks.

Day 3 Report

OSI stands for(**Open Systems Interconnection)**

It was developed by ISO – '**International Organization for Standardization** ', in 1984. It is a 7-layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.

1. Physical Layer (Layer 1)
2. Data Link Layer (DLL) (Layer 2)
3. Network Layer (Layer 3)
4. Transport Layer (Layer 4)
5. Session Layer (Layer 5)
6. Presentation Layer (Layer 6)
7. Application Layer (Layer 7)

1. Physical Layer (Layer 1):

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

The functions of the physical layer are as follows:

1.Bit synchronization

2.Bit rate control

3. Transmission mode

4. Physical topologies

2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.
Data Link Layer is divided into two sublayers:

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The functions of the Data Link layer are :

1. Framing.
2. Physical addressing
3. Error control
4. Flow Control
5. Access control

3. Network Layer (Layer 3):

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver’s IP addresses are placed in the header by the network layer.

The functions of the Network layer are:

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
2. **Logical Addressing:** In order to identify each device on internetwork uniquely, the network layer defines an addressing scheme. The sender & receiver’s IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

4. Transport Layer (Layer 4):

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End-to-End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

At sender's side: Transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

5. Session Layer (Layer 5):

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security.
The functions of the session layer are:

1. **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered synchronization points into the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

6. Presentation Layer (Layer 6):

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The functions of the presentation layer are:

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

7. Application Layer (Layer 7):

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

Day 5 report

A **media access control address** (**MAC address**) is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment. This use is common in most IEEE 802 networking technologies, including Ethernet, Wi-Fi, and Bluetooth. Within the Open Systems Interconnection (OSI) network model, MAC addresses are used in the medium access control protocol sublayer of the data link layer. As typically represented, MAC addresses are recognizable as six groups of two hexadecimal digits, separated by hyphens, colons, or without a separator.

MAC addresses are primarily assigned by device manufacturers, and are therefore often referred to as the **burned-in address**, or as an **Ethernet hardware address**, **hardware address**, or **physical address**. Each address can be stored in hardware, such as the card's read-only memory, or by a firmware mechanism. Many network interfaces, however, support changing their MAC address. The address typically includes a manufacturer's organizationally unique identifier (OUI).

LOGICAL GATEWAY ADDRESS:

The gateway operates at the network layer (Layer 3) of the OSI Model. The gateway is used when transmitting packets. When packets are sent over a network, the destination IP address is examined. If the destination IP is outside of the network, then the packet goes to the gateway for transmission outside of the network. The gateway is on the same network as end devices. The gateway address must have the same subnet mask as host devices. Each host on the network uses the same gateway.

The gateway should have a static address, as changing the address would cause packets not to be delivered. The gateway is typically assigned either the highest or lowest network address. This is not a requirement, but many organizations use a consistent addressing scheme to facilitate network planning.

PHYSICAL GATEWAY ADDRESS:

The gateway also operates at the data link layer (Layer 2) of the OSI network model. The physical gateway address is called the *media access control(MAC)* address or *burned in address (BIA)*. The physical address is assigned when the device is manufactured, and cannot be changed. When a frame is sent to a device not on the local network, the gateway's MAC address is used in the frame header.

The gateway address must be configured on each host. The network host IP interface binds the gateway address to the MAC address of the physical gateway by broadcasting IP datagrams and caching the MAC address of the reply from the gateway in an ARP table stored on the host. The gateway address may be added manually. On Windows computers, the gateway address is configured using the TCP/IP Properties.

The gateway address can be automatically determined using Dynamic Host Configuration Protocol (DHCP). DHCP allows a host to obtain network information from a server. The host contacts the server to obtain an IP address and Default Gateway address. DHCP Servers are normally provided by Internet ServiceProviders (ISPs).

Types of cable:

1.straight cable

2.cross cable

3.roll over cable is connected to console cable

CISCO ROUTER COMMANDS:

CLI Configuration Modes

The basic CLI modes that we will be referring below are as following:

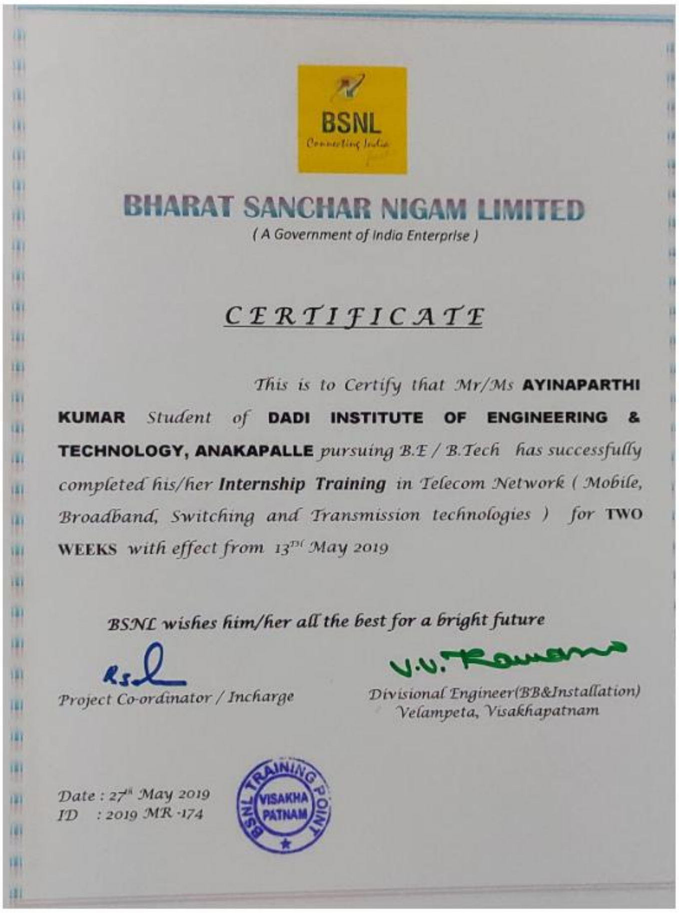
Router> <– User EXEC Mode

Router# <– Privileged EXEC mode

Router(config)# <– Global Configuration Mode

Router(config-if) # <– Interface Configuration Mode

Router(config-line) # <– Line Configuration Mode



BSNL
Connecting India

BHARAT SANCHAR NIGAM LIMITED
(A Government of India Enterprise)

CERTIFICATE

This is to Certify that Mr/Ms **AYINAPARTHI KUMAR** Student of **DADI INSTITUTE OF ENGINEERING & TECHNOLOGY, ANAKAPALLE** pursuing B.E / B.Tech has successfully completed his/her **Internship Training** in Telecom Network (Mobile, Broadband, Switching and Transmission technologies) for **TWO WEEKS** with effect from 13TH May 2019

BSNL wishes him/her all the best for a bright future

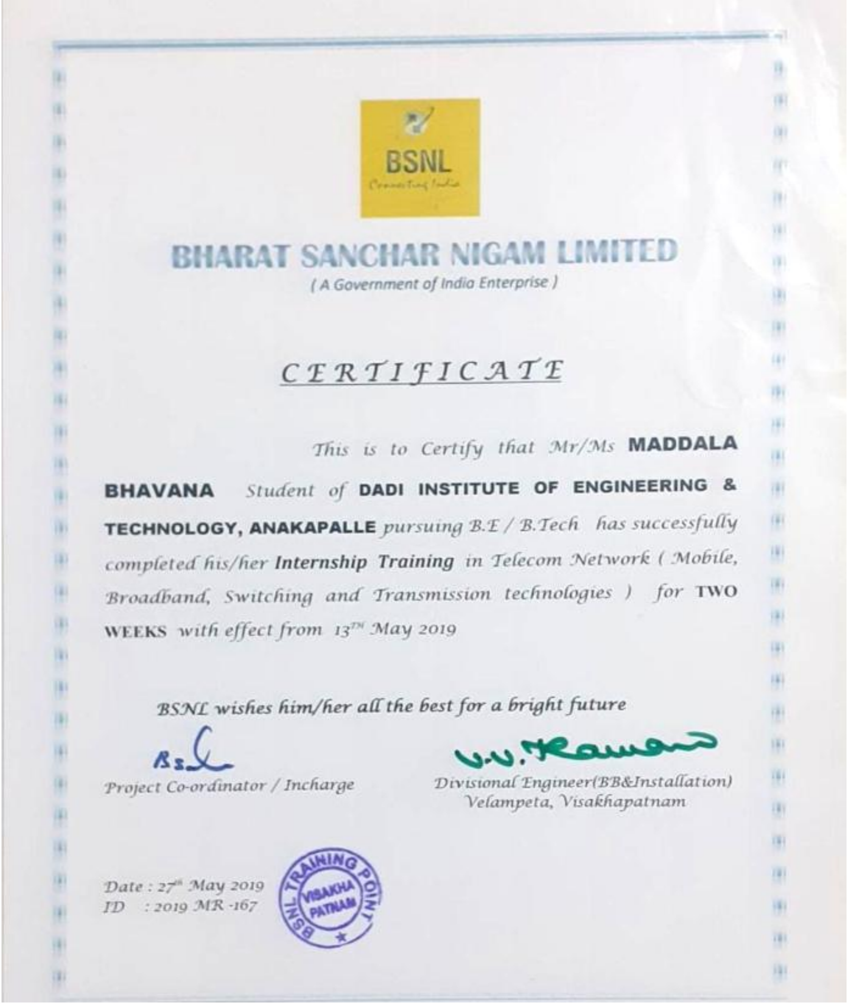
Project Co-ordinator / Incharge

V.V. Ramana
Divisional Engineer(BB&Installation)
Velampeta, Visakhapatnam

Date : 27th May 2019
ID : 2019 MR-174

BSNL TRAINING POINT VISAKHA PATNAM

Figure 6: Students undergoing training at BSNL Certificate



BSNL
Connecting India

BHARAT SANCHAR NIGAM LIMITED
(A Government of India Enterprise)

CERTIFICATE

This is to Certify that Mr/Ms **MADDALA BHAVANA** Student of **DADI INSTITUTE OF ENGINEERING & TECHNOLOGY, ANAKAPALLE** pursuing B.E / B.Tech has successfully completed his/her **Internship Training** in Telecom Network (Mobile, Broadband, Switching and Transmission technologies) for **TWO WEEKS** with effect from 13TH May 2019

BSNL wishes him/her all the best for a bright future

Project Co-ordinator / Incharge

V.V.Ramana
Divisional Engineer(BB&Installation)
Velampeta, Visakhapatnam

Date : 27th May 2019
ID : 2019 MR -167

BSNL TRAINING POINT
VISAKHA PATNAM

Figure 7: Completion certificate

Participants list

Sl.No	NAME
1	Ayinaparthi Kumar
2	Maddla Bhavana
3	Sunkara Ganesh
4	Buddha Prathyusha
5	Vallampati Rama Lakshmi
6	Kunukulaguntala Reshma
7	Bomma Sandeep
8	Vajrapu Sai Srujana

Department of ECE

FEEDBACK FORM ON INTERNSHIP TRAININNG

1. Has the Internship attained its objectives

□ Yes
□ No

2. Internship was relevant to my needs

□ Strongly agree
□ Agree
□ Neutral
□ Disagree
□ Strongly disagree

3. Instructions were clear and understandable

□ Strongly agree
□ Agree
□ Neutral
□ Disagree
□ Strongly disagree

4. Classes was well organised

□ Strongly agree

□ Agree
□ Neutral
□ Disagree
□ Strongly disagree

5. Was the Duration of the training sufficient.
□ Yes
□ No

6.Resource persons were effective.
□ Strongly agree
□ Agree
□ Neutral
□ Disagree
□ Strongly disagree

7. Queries were encouraged
□ Strongly agree
□ Agree
□ Neutral
□ Disagree
□ Strongly disagree

8. Any additional remarks

9. Overall how would you rate this event
□ Excellent
□ Very good
□ Good
□ Fair
□ Poor

10.Propose the name of the training program you will be interested in participating in future.