A REPORT OF SIX WEEKS INDUSTRIAL TRAINING

At

SUN INFOSYSTEM Pvt. Ltd.

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD

OF THE DEGREE OF

BACHELOR OF ENGINEERING

(Computer Science & Engineering)

JUNE-JULY, 2018

SUBMITTED BY:

HARSH SOMANI (16BCS3054)

ANURAG GUPTA (16BCS3042)

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CHANDIGARH UNIVERSITY GHARUAN, MOHALI

CANDIDATE'S DECLARATION

We HARSH SOMANI and ANURAG GUPTA hereby declare that we have undertaken six weeks industrial training at "**Sun Infosystem Pvt Ltd**" during a period from 12th May, 2018 to 25th June, 2018 in partial fulfillment of requirements for the award of degree of B.E (COMPUTER SCIENCE & ENGINEERING) Hons. at CHANDIGARH UNIVERSITY GHARUAN, MOHALI. The work which is being presented in the training report submitted to Department of Computer Science & Engineering at CHANDIGARH UNIVERSITY GHARUAN, MOHALI is an authentic record of training work.

Signature of the Students

The six weeks industrial training Viva–Voce Examination of CCNA has been held on _____ and accepted.

Signature of Internal Examiner

Signature of External Examiner

ACKNOWLEDGEMENT

“If practical knowledge carves and sharps the career of a person, practical experience polishes it and adds brilliance to it.”

Here, I found this golden chance to acknowledge all those people who had blessed, encouraged and supported me technically and morally through all the phases of my project. I thank almighty God for giving me this opportunity to e7ress gratitude to all those who helped me in my training. The report of “**Company Network**” this was a learning experience for me.

TABLE OF CONTENTS

CONTENTS **Page no:**

CHAPTER1: INTRODUCTION

1.1 Network

A computer network is an interconnected group of computers. , a network is any method of sharing information between two systems (human or mechanical). Networks may be classified by the network layer at which they operate according to basic reference models such as the five-layer Internet Protocol Suite model. While the seven-layer Open Systems Interconnection (OSI) reference model is better known in academia, the majority of networks use the Internet Protocol Suite (IP).

Networks in various fields:

In broadcasting: A communication system consisting of a group of broadcasting stations that all transmit the same programs; "the networks compete to broadcast important sports events"

- **In electronics:** A system of interconnected electronic components or circuits
- **In functional relationship i.e. (Network Architectures):** Computer networks may be classified according to the functional relationships which exist between the elements of the network, e.g., Active Networking, Client-server and Peer-to-peer.
- **In network topology:** Computer networks may be classified according to the network topology upon which the network is based, such as Bus network, Star network, Ring network, Mesh network, Star-bus network, Tree or Hierarchical topology network, etc.

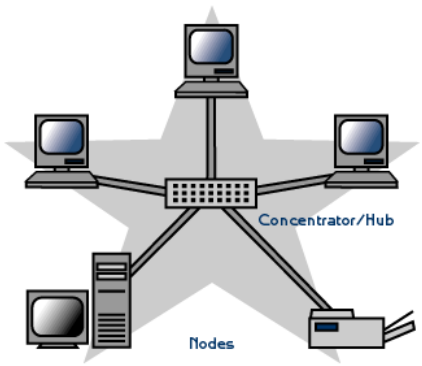
1.2 Network Topologies

Network topology is the study of the arrangement or mapping of the elements of a network, especially the physical (real) and logical (virtual) interconnections between nodes. A local area network (LAN) is one example of a network that exhibits both a physical topology and a logical

topology. Any given node in the LAN will have one or more links to one or more other nodes in the network and the mapping of these links and nodes onto a graph results in a geometrical shape that determines the physical topology of the network. Likewise, the mapping of the flow of data between the nodes in the network determines the logical topology of the network.

CLASSIFICATION OF NETWORK TOPOLOGIES:

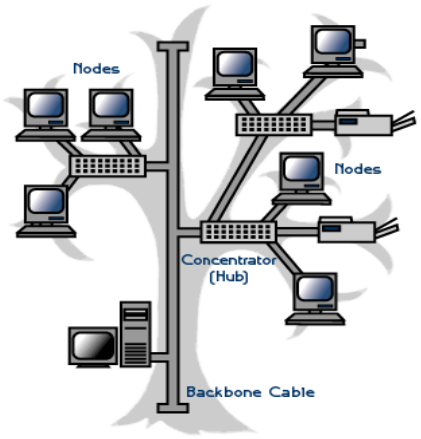
1) **Linear bus:** topology in which all the nodes of the network are connected to a common transmission medium which has exactly two endpoints. All data that is transmitted between nodes in the network is transmitted over this common transmission medium and is able to be received by all nodes in the network virtually simultaneously.
2) **Star:** it connects all cables to a central point of concentration. This point is usually a hub or switch. Nodes communicate across the network by passing data through the hub. The main disadvantage of this kind of topology is that if central hub stops working then there will be no transmission at any node.



3) **Ring:** It is the type of network topology in which each of the nodes of the network is connected to two other nodes in the network and with the first and last nodes being connected to each other, forming a ring. All the data that is transmitted between nodes in

the network travels from one node to the next node in a circular manner and the data generally flows in a single direction only.

4) **Tree:** The type of network topology in which a central 'root' node (the top level of the hierarchy) is connected to one or more other nodes that are one level lower in the hierarchy (i.e., the second level) with a point-to-point link between each of the second level nodes and the top level central 'root' node, while each of the second level nodes that are connected to the top level central 'root' node will also have one or more other nodes that are one level lower in the hierarchy (i.e., the third level) connected to it, also with a point-to-point link. The top level central 'root' node being the only node that has no other node above it in the hierarchy.



5) **Mesh:** The value of fully meshed networks is proportional to the e7onent of the number of subscribers, assuming that communicating groups of any two endpoints, up to and including all the endpoints. It is the type of network topology in which each of the nodes of the network is connected to each of the other nodes in the network with a point-to-

point link – this makes it possible for data to be simultaneously transmitted from any single node to all of the other nodes.

1.3 Types of Network

Computers connected over a network can make that information exchange easier and faster. The information moves directly from computer to computer rather than through a human intermediary. The most elementary network consists of two computers communicating over a cable. When we link computers together, we can more swiftly and efficiently move information between them. The computers can also share resources, such as printers and fax modems, allowing us to better use our hardware. A group of computers and other devices connected together is called a *network,* and the concept of connected computers sharing resources is called *networking.*

1) **Local Area Network (LAN):** A network covering a small geographic area, like a home, office, or building. Current LANs are most likely to be based on Ethernet technology. For example, a library will have a wired or wireless LAN for users to interconnect local devices (e.g., printers and servers) and to connect to the internet. All of the PCs in the library are connected by category 5 (Cat5) cable, running the IEEE 802.3 protocol through a system of interconnection devices and eventually connect to the internet
2) **Metropolitan Area Network (MAN):** It is a network that connects two or more Local Area Networks or Campus Area Networks together but does not extend beyond the boundaries of the immediate town, city, or metropolitan area. Multiple routers, switches & hubs are connected to create a MAN.
3) **Wide Area Network (WAN):** A WAN is a data communications network that covers a relatively broad geographic area (i.e. one city to another and one country to another

country) and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

4) **Personal Area Network (PAN):** A personal area network (PAN) is a computer network used for communication among computer devices close to one person. Some examples of devices that may be used in a PAN are printers, fax machines, telephones, PDAs or scanners. The reach of a PAN is typically within about 20-30 feet (approximately 6-9 meters).

5) **Internetwork :** Two or more networks or network segments connected using devices that operate at layer 3 (the 'network' layer) of the OSI Basic Reference Model, such as a router. Any interconnection among or between public, private, commercial, industrial, or governmental networks may also be defined as an internetwork. It use the Internet Protocol. There are at least three variants of internetwork, depending on who administers and who participates in them:

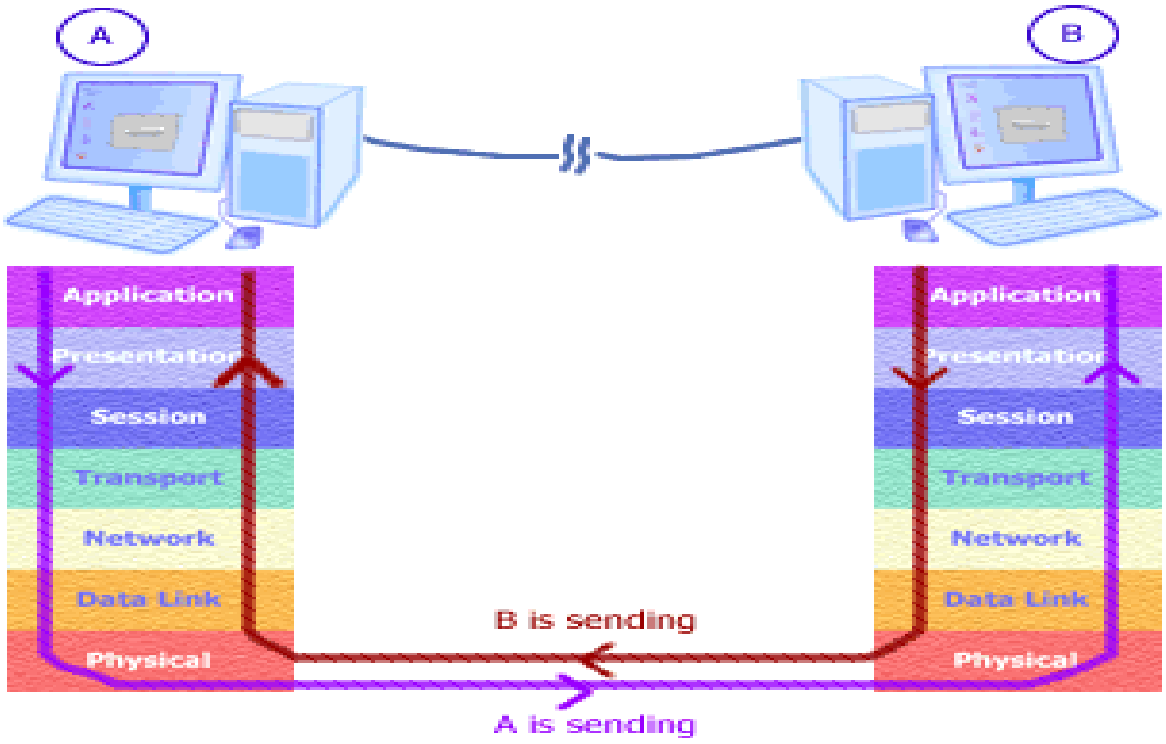
a. Intranet: An intranet is a set of interconnected networks, using the Internet Protocol and uses IP-based tools such as web browsers and ftp tools, that is under the control of a single administrative entity. An intranet is the internal network of a company or other enterprise.

b. Extranet: An extranet is a network or internetwork that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities. Technically, an extranet may also be categorized as a CAN, MAN, WAN, or other type of network,

although, by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

c. **Internet:** A specific internetwork, consisting of a worldwide interconnection of governmental, academic, public, and private networks based upon the Advanced Research Projects Agency Network (ARPANET) developed by ARPA of the U.S. Department of Defense – also home to the World Wide Web (WWW) and referred to as the 'Internet' with a capital 'I' to distinguish it from other generic internetworks.

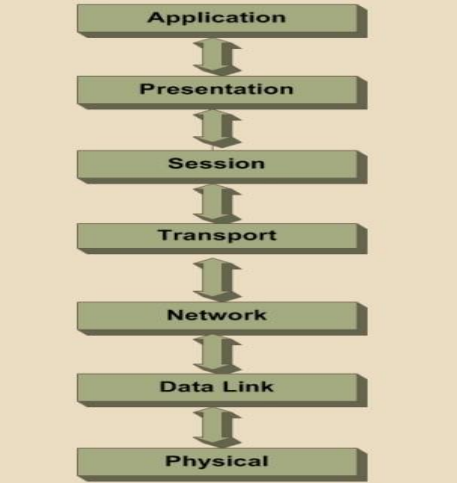
1.4 Open System Intercommunication (OSI)



Definition: The OSI model defines internetworking in terms of a vertical stack of seven layers. The upper layers of the OSI model represent software that implements network services like encryption and connection management. The OSI model was specifically made for connecting

open systems. These systems are designed to be open for communication with almost any other system. The model was made to break down each functional layer so that overall design complexity could be lessened. The model was constructed with seven layers for the flow of information.

These are 7 layers:



1) **Application layer:** It provides a means for the user to access information on the network through an application. Examples Telnet, FTP, and Protocol SMTP.
2) **Presentation layer:** It manages the presentation of the information in an ordered and meaningful manner.. Some well-known standards for video include QuickTime and MPEG, GIF and JPEG.
3) **Session layer:** The session layer establishes, manages, and terminates communication sessions. Example: token management and network time synchronization, ZIP, the AppleTalk protocoland SCP.

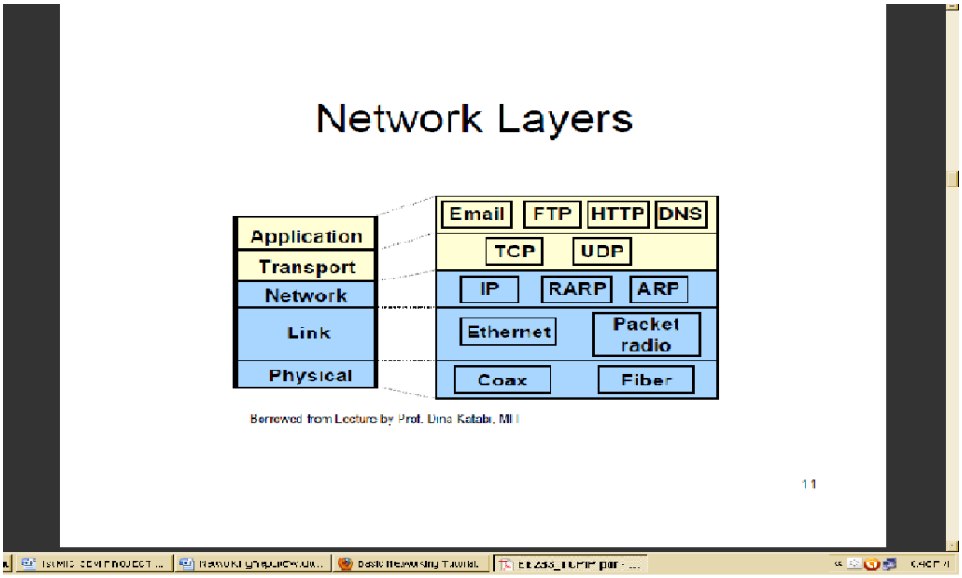
4) **Transport layer:** Responsible for reliable transmission of data and service specification between hosts. Two transport protocols are the TCP (Transmission Control Protocol) connection protocol and the UDP (User Data gram Protocol) connectionless protocol.
5) **Network layer:** Responsible for the routing of data (packets) through the network; handles the addressing and delivery of data. EG: IP
6) **Data link layer:** Provides for the reliable delivery of data across a physical network. The network data frame.
7) **Physical layer:** Handles the bit-level electrical/light communication across the network channel.

   Data travels from the application layer of the sender, down through the levels, across the nodes of the network service, and up through the levels of the receive

1.5 TCP/IP Model

Transport Control Protocol/Internet Protocol is made up of 5 layers ---------

- Physical Layer
- Data Link Layer
- Network Layer
- Transport Layer
- Application Layer



TCP PROTOCOLS

• FTP - File Transport Protocol at the application layer.

• Telnet - Remote session at the application layer.

• SMTP - Simple Mail Transport Protocol at the application layer.

• DHCP - Dynamic host configuration protocol is used to assign IP addresses dynamically to network cards. It works at the application layer.

• TCP - Transport Control protocol is a connection oriented reliable protocol working at the transport layer.

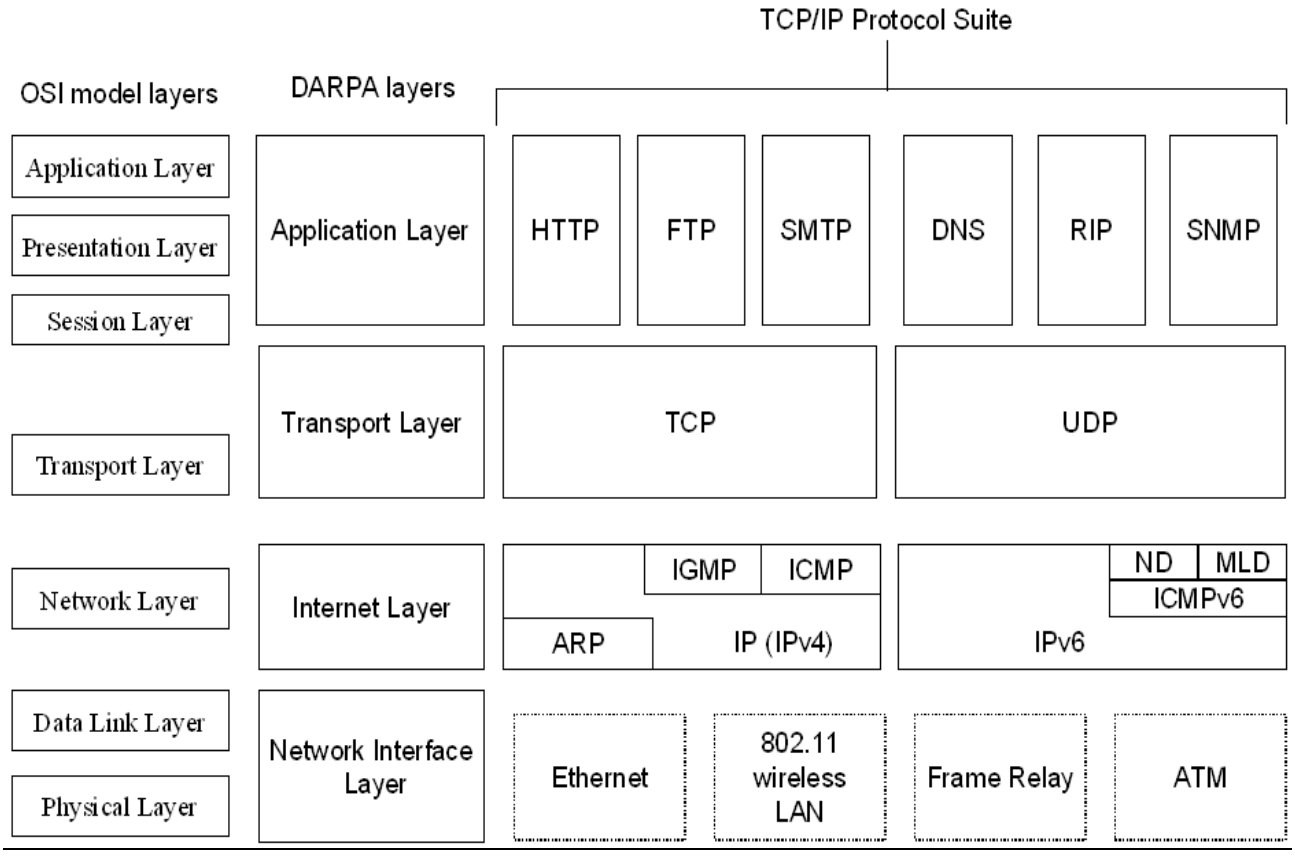
• UDP - User Datagram Protocol is a connection less unreliable protocol working at the transport layer.

• ICMP - Internet Control Message Protocol is used to perform network error reporting and status. It works at the transport layer.

• IGMP - Internet Group Management Protocol is used to manage multicast groups and it works at the transport layer.

• IP - Internet Protocol is used for software addressing of computers and works at the network layer.

• ARP - Address Resolution Protocol is used to resolve the hardware address of a card to package the Ethernet data. It works at the network Layer.



1.6 Classes of Networking

All networks in practical use have different sizes. For example, a company that will have 50 computers, will not need a network of 5000 computers, And on the contrary, a company that needs 5000 computers does not need a network that can only hold 50 computers. This is the main reason that engineers decided that IP address space should be divided in different classes in order to meet different requirements. The following classes were created:

1) **Class A:** Starts with a number between 1 and 126. Only 126 of these networks are available, however each class A network can handle 16,777,214 IP addresses or computers. Its addresses are assigned to networks with a very large number of hosts. This allows for 126 networks and approximately 17 million hosts per network.
2) **Class B:** IP addresses of this type starts with a number between 128 and 191. Class B addresses are used for small local area networks (LANs). The three high order bits in a class C address are always set to binary 110. This allows for 16, 384 networks and approximately 65,000 hosts per network.
3) **Class C:** This is the most widely used class by small businesses. When you look at the IP address, you'll notice that class C networks start with a first number that's between 192 and 223 (205.161.74.x for example). Class C address are used for small local area networks (LANs). This allows for approximately 2 million networks.
4) **Class D:** It has its highest bit order set to 1-1-1-0 it is used to support multicasting. A multicast group may contain one or more hosts. The remaining bits designated the specific group in which the client participates. Microsoft uses class D addresses for applications to multicast data to hosts on an internet work, including Windows Internet Name Service (WINS) and Microsoft NetShow.

5) **Class E:** It has its highest bit order set to 1-1-1-1 which is reserved for experimental use. Class E is an experimental address that is not available for general use; It is reserved for future use.

Network ID: Each IP address defines the network ID and host ID. The network ID identifies the systems that are located on the same physical segment. All systems on the same physical segment must have the same network ID. The network ID must be unique to the internet work.

Host ID: The host ID identifies a workstation, server, router, or other TCP/IP host within a segment. The address for each host must be unique to the network ID. Each IP address is 32 bits long and is composed of four OS-bit fields, called *octets.* Octets are separated by periods. The octet represents a decimal number in the range 0-255. This format is called *dotted decimal notation.* The following is an example of an IP address in binary and dotted decimal formats.

Binary format	Dotted decimal notation
10000011.01101011.00000011.00011000	131.107.3.24

Class	IP address	Network ID	Host ID
A	*w.x.y.z*	*W*	*x.y.z*
B	*w.x.y.z*	*w.x*	*y.z*
C	*w.x.y.z*	*w.x.y*	z

Follow this guideline when assigning network IDs and host IDs:

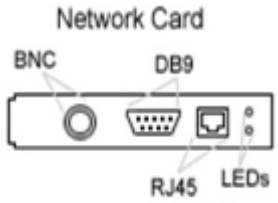
- The network ID cannot be 127. This ID is reserved for loopback functions.
- The network ID and host ID cannot be 255 (all bits set 1). If all bits are set to 1, the address is interpreted as a broadcast rather than a host ID.

- The network ID and host ID bits cannot all be set to 0. If all bits are set to 0, the address is interpreted to mean " this network only".
- The host ID must be unique to the local network ID.

1.7 Network Hardware

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers. In addition, some method of connecting these building blocks is required, in the Category 5 cable or Less common are microwave links (as in IEEE 802.11) or optical cable ("optical fiber").Some of the practically used network hardware are:

1) **Network card:** A NIC or Network Interface Card is a circuit board or chip, which allows the computer to communicate to other computers on a Network. This board when connected to a cable or other method of transferring data such as infrared can share resources, information and computer hardware. Local or Wide area networks are generally used for large businesses as well as are beginning to be found in homes as home users begin to have more than one computer.



2) **Ethernet:** Ethernet cards are usually purchased separately from a computer, although many computers (such as the Macintosh) now include an option for a pre-installed

Ethernet card. Ethernet cards contain connections for either coaxial or twisted pair cables .If it is designed for coaxial cable, the connection will be BNC. If it is designed for twisted pair, it will have a RJ-45 connection.

3) **Networking Cables:** CROSS CABLES (Unshielded Twisted Pair-8 columns) UTP cable is a medium that is composed of pairs of wires. UTP cable is used in a variety of networks.
4) **Shielded twisted-pair (STP)** cable combines the techniques of shielding, cancellation, and wire twisting. The four pairs of wires then are wrapped in an overall metallic braid or foil, usually 150-ohm cable. As specified for use in Ethernet network installations, STP reduces electrical noise both within the cable (pair-to-pair coupling, or crosstalk) and from outside the cable (EMI and RFI). STP usually is installed with STP data connector, which is created especially for the STP cable. However, STP cabling also can use the same RJ connectors that UTP uses.
5) **RJ 45 CONNECTORS:** UTP cable often is installed using a Registered Jack 45 (RJ-45) connector. The RJ-45 is an eight-wire connector used commonly to connect computers onto a local-area network .After connecting the RJ-45 to the cable, it is used to connect the client and the server. Instead one server can be connected to various clients using a switch. Then "PING" both the client and server with their static IPs. The reply indicates that the PCs are now connected.

Commonly used types of UTP cabling are as follows:

Category 1—Used for telephone communications. Not suitable for transmitting data.

Category 2—Capable of transmitting data at speeds up to 4 megabits per second (Mbps).

Category 3—Used in 10BASE-T networks. Can transmit data at speeds up to 10 Mbps.

Category 4—Used in Token Ring networks. Can transmit data at speeds up to 16 Mbps.

Category 5—Can transmit data at speeds up to 100 Mbps.

Category 5e—Used in networks running at speeds up to 1000 Mbps (1 gigabit per second [Gbps]).

Category 6—Typically, Category 6 cable consists of four pairs of 24 American Wire Gauge (AWG) copper wires. Category 6 cables is currently the fastest standard for UTP.

6) **Network Hub:** A network hub or concentrator is a device for connecting multiple twisted pair or fiber optic Ethernet devices together, making them act as a single network segment. Hubs work at the physical layer of the OSI model. The device is thus a form of multiport repeater. Network hubs are also responsible for forwarding a jam signal to all ports if it detects a collision. The main reason for purchasing hubs rather than switches was its price. This has largely been eliminated by reductions in the price of switches, but hubs can still be useful in special circumstances.

7) **Repeaters:** As signals travel along a network cable they degrade and become distorted in a process that is called attenuation. If a cable is long enough, the attenuation will finally make a signal unrecognizable by the receiver. A Repeater enables signals to travel longer distances over a network. Repeaters work at the OSI's Physical layer.

8) **Bridges:** Like a repeater, a bridge can join segments or workgroup LANs. However, a bridge can also divide a network to isolate traffic or problems. For example, if the volume of

traffic from one or two computers or a single department is flooding the network with data and slowing down entire operation, a bridge can isolate those computers or that department.

9) Routers: In an environment consisting of several network segments with different protocols and architecture, a bridge may not be adequate for ensuring fast communication among all of the segments. A complex network needs a device, which not only knows the address of each segment, but also can determine the best path for sending data and filtering broadcast traffic to the local segment. Such device is called a Router. Routers work at the Network layer of the OSI model meaning that the Routers can switch and route packets across multiple networks.Access routers, including SOHO, are located at customer sites such as branch offices that do not need hierarchical routing of their own. Typically, they are optimized for low cost.

10) Gateways: Gateways make communication possible between different architectures and environments. They repackage and convert data going from one environment to another so that each environment can understand the other's environment data. A gateway repackages information to match the requirements of the destination system. Gateways can change the format of a message so that it will conform to the application program at the receiving end of the transfer.

CHAPTER2: TRAINING WORK UNDERTAKEN

2.1 Hardware Requirements

1) CPU Speed: 2GHz recommended or higher
2) Processor: Pentium Processor or above
3) RAM: 1GB minimum, 2GB or higher recommended
4) Display Properties: Greater than 256 color depth
5) Hard disk Size: 60GB or higher recommended
6) Video adapter and monitor with Super VGA (800 x 600)or higher resolution

2.2 Software Requirements

1) Software Used: GNS3 (Graphical Network Stimulator)
2) Operating System: Windows XP, Vista , 7, 10

2.3 About the software and its installation

GNS-3 (Graphical Network Stimulator)

GNS3 is used by hundreds of thousands of network engineers worldwide to emulate, configure, test and troubleshoot virtual and real networks. GNS3 allows you to run a small topology consisting of only a few devices on your laptop, to those that have many devices hosted on multiple servers or even hosted in the cloud.

Features

The current version of GNS-3 supports an array of simulated Application Layer protocols, as well as basic routing with RIP, OSPF, and EIGRP, BGP to the extent required by the current CCNA curriculum. While GNS-3 aims to provide a realistic simulation of functional

networks, the application itself utilizes only a small number of features found within the actual hardware running a current Cisco IOS version. Thus, GNS-3 is unsuitable for modeling production networks.

Installation

Steps:

1) Double click on GNS3-0.8.4-all-in-one.exe setup wizard.
2) Once the wizard opens, click on next.

Fig 1-Installation Wizard

3) A License agreement window will open, click on 'I Agree'.

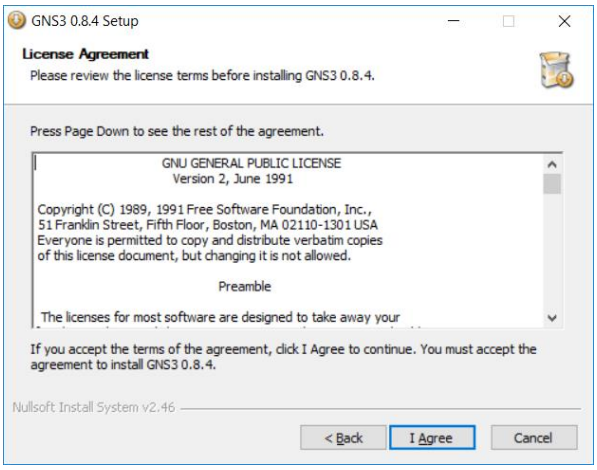


Fig 2- Agreement

4) It will ask you to choose a start menu folder, choose and press next.

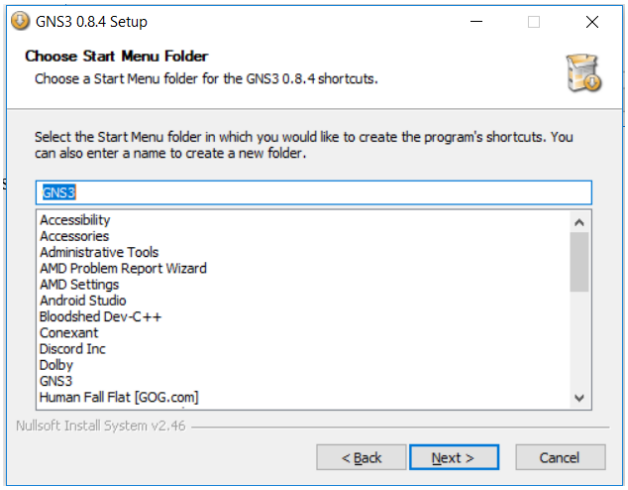


Fig 3- Agreement

5) It will then ask you to choose components. By default 'SuperPutty' would be unchecked. Check it and press next. (This will allow you to access multiple consoles in a single window.)

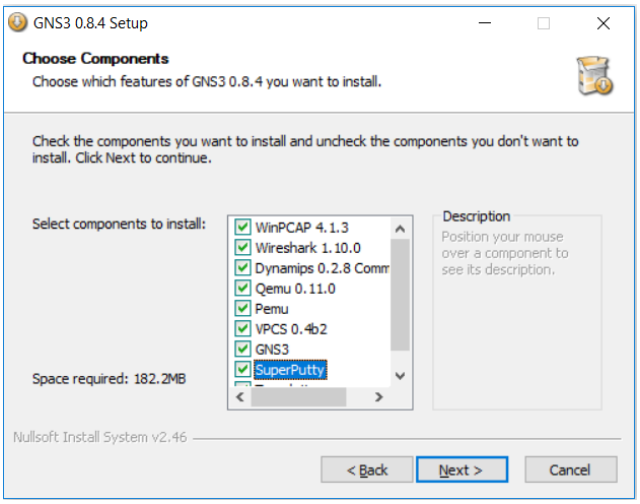


Fig 4-Choose Components

6) Choose the path to store the installation and press Install.

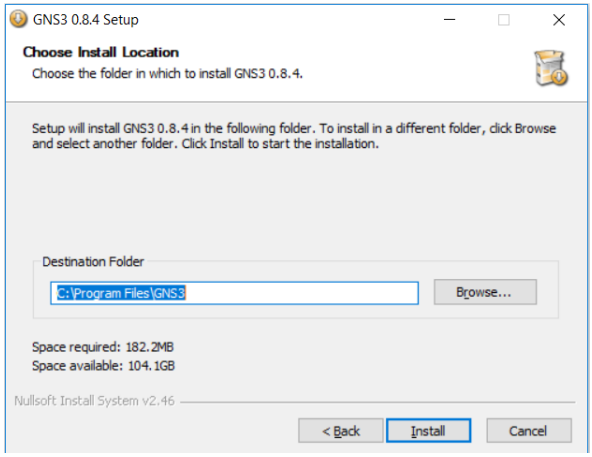


Fig 5-Choose Location

7) Finally press finish and the Installation is complete.

2.4 PROJECT DETAIL

2.4.1Description:

Here we have 5 departments in an Office building, they are accessing internet through ISPs.

2.4.2 Devices Used

1. 3 Serial Cables
2. 5 Routers
3. 4 Switches of 16 port each(LAYER 2)
4. 16 PCs
5. 28 Fast Ethernet Cables.

2.4.3 PROTOCOLS USED

1. EIGRP
2. Flat network in the switching
3. DHCP mechanism
4. Inter vlan in the switching portion
5. Subnet masking
6. Wild card masking
7. STP(Spanning Tree Protocol)

CHAPTER 3: RESULTS AND DISCUSSION

3.1 Making the Stimulated Structure

Steps:

1) Open GNS-3 and Install ‘Router c3600’ Image file by clicking on Edit->IOS image and hypervisors, then browse the ISO file and click on ‘Test Settings’ and then ‘Save’.

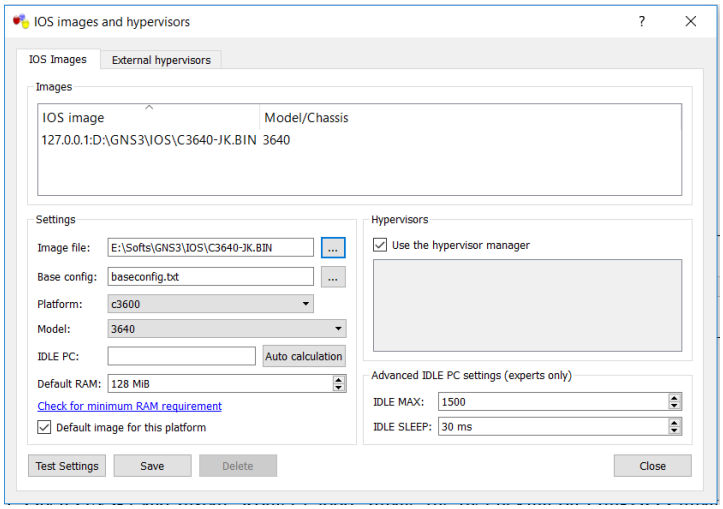


Fig 6-Intalling Router c3600

2) Draw the following Structure:

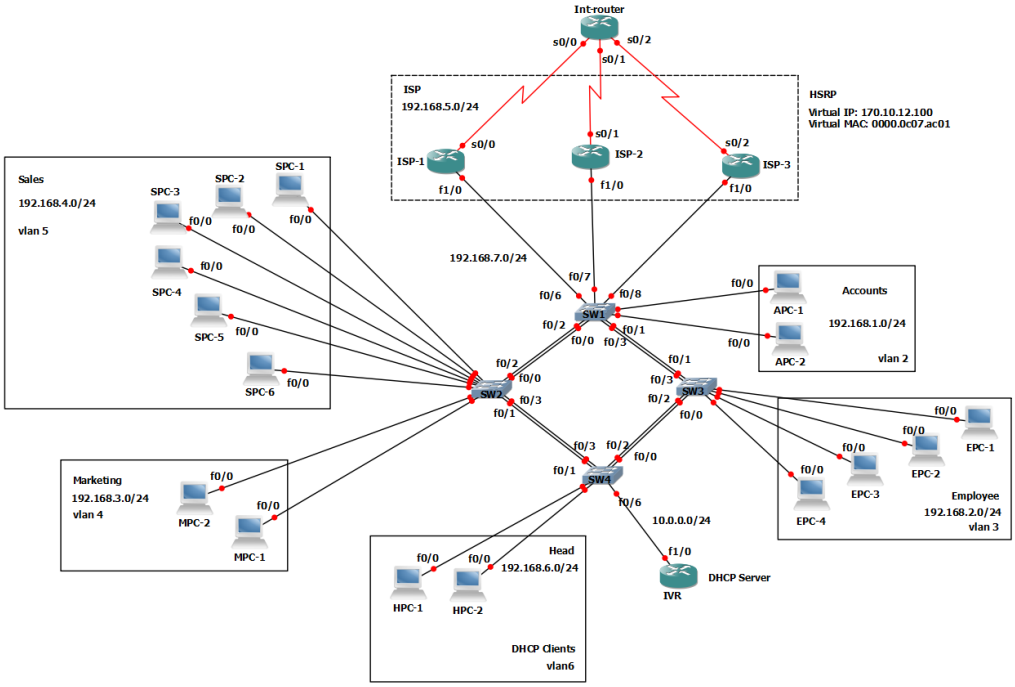


Fig 7-Company Network

3) Take Consoles of the PCs and Routers and Switches and code the following according to labels. The codes are written below.

Step 1: Configure IP Address

On ISP-1:

```
conf t
int s0/0
ip add 192.168.5.1 255.255.255.0
no shut
int f1/0
ip add 192.168.7.1 255.255.255.0
no shut
end
```

On ISP-2:

```
conf t
int s0/1
ip add 192.168.5.2 255.255.255.0
no shut
int f1/0
ip add 192.168.7.2 255.255.255.0
no shut
end
```

On ISP-3:

```
conf t
int s0/2
ip add 192.168.5.3 255.255.255.0
no shut
int f1/0
ip add 192.168.7.3 255.255.255.0
no shut
end
```

On IVR:

```
conf t
int f1/0
ip add 10.0.0.1 255.255.255.0
no shut
exit
ip dhcp pool xyz
network 192.168.6.0 255.255.255.0
default router 10.0.0.1
lease 1 1 1
dns 8.8.8.8
exit
ip dhcp excluded-address 192.168.6.10
end
```

On APC-1:

```
conf t
no ip routing
int f0/0
ip add 192.168.1.1 255.255.255.0
no shut
end
```

On APC-2:

```
conf t
no ip routing
int f0/0
ip add 192.168.1.2 255.255.255.0
no shut
end
```

On EPC-1:

```
conf t
no ip routing
int f0/0
ip add 192.168.2.1 255.255.255.0
```

no shut
end

On EPC-2:
conf t
no ip routing
int f0/0
ip add 192.168.2.2 255.255.255.0
no shut
end

On EPC-3:
conf t
no ip routing
int f0/0
ip add 192.168.2.3 255.255.255.0
no shut
end

On EPC-4:
conf t
no ip routing
int f0/0
ip add 192.168.2.4 255.255.255.0
no shut
end

On HPC-1:
conf t
no ip routing
int f0/0
ip add dhcp
no shut
end

On HPC-2:
conf t
no ip routing
int f0/0
ip add dhcp
no shut
end

On MPC-1:
conf t
int f0/0

ip add 192.168.3.1 255.255.255.0
no shut
end

On MPC-2:
conf t
no ip routing
int f0/0
ip add 192.168.3.2 255.255.255.0
no shut
end

On SPC-1:
conf t
no ip routing
int f0/0
ip add 192.168.4.1 255.255.255.0
no shut
end

On SPC-2:
conf t
no ip routing
int f0/0
ip add 192.168.4.2 255.255.255.0
no shut
end

On SPC-3:
conf t
no ip routing
int f0/0
ip add 192.168.4.3 255.255.255.0
no shut
end

On SPC-4:
conf t
no ip routing
int f0/0
ip add 192.168.4.4 255.255.255.0
no shut
end

On SPC-5:
conf t

no ip routing
int f0/0
ip add 192.168.4.5 255.255.255.0
no shut
end

On SPC-6:
conf t
no ip routing
int f0/0
ip add 192.168.4.6 255.255.255.0
no shut
end

On Int-router:
conf t
int s0/0
ip add 192.168.5.4 255.255.255.0
no shut
int s0/1
ip add 192.168.5.5 255.255.255.0
no shut
int s0/2
ip add 192.168.5.6 255.255.255.0
no shut
end

Step 2: Configure EIGRP Routing

On ISP-1:
conf t
router eigrp 123
network 192.168.5.1 0.0.0.255
network 192.168.7.1 0.0.0.255
end

On ISP-2:
conf t
router eigrp 123
network 192.168.5.2 0.0.0.255
network 192.168.7.2 0.0.0.255
end

On ISP-3:
conf t

router eigrp 123
network 192.168.5.3 0.0.0.255
network 192.168.7.3 0.0.0.255
end

On Int-router:
conf t
router eigrp 123
network 192.168.5.0
end

Step 3: Make HSRP group of all ISPs.

On ISP-1:
Conf t
Int f1/0
Standby 1 ip 170.10.12.100
Standby 1 priority 150
Standby 1 preempt delay minimum 10
Standby 1 track s0/0 60

On ISP-2:
conf t
int f1/0
Standby 1 ip 170.10.12.100
Standby 1 priority 120
Standby 1 preempt delay minimum 10
Standby 1 track s0/0 60

On ISP-3:
conf t
int f1/0
Standby 1 ip 170.10.12.100
Standby 1 priority 100
Standby 1 preempt delay minimum 10
Standby 1 track s0/0 60

Step 4: Create vlans

On SW4:
conf t
vlan database
vtp domain cisco.com
vtp version 2
vtp password cisco123
exit

vlan database
vlan 6
vlan 6 name head
end

On SW1:
conf t
vtp mode client
vlan database
vlan 2
vlan 2 name accounts
end

On SW2:
conf t
vtp mode client
vlan database
vlan 5
vlan 5 name sales
vlan 4
vlan 4 name marketing
end

On SW3:
conf t
vtp mode client
vlan database
vlan 3
vlan 3 name employee
end

Step 5: Configure trunking and encapsulation

On all Switches:
conf t
switchport trunk encapsulation dot1q
switchport mode trunk
end

Step 6: Add members to vlans

On SW1:
conf t
int range f0/4-5
switchport mode access
switchport access vlan 2

end

On SW2:
conf t
int range f0/4-9
switchport mode access
switchport access vlan 5
exit
int range f0/10-11
switchport mode access
swtichport access vlan 4
end

On SW3:
conf t
int range f0/4-7
switchport mode access
switchport access vlan3
end

On SW4:
conf t
int range f0/4-5
switchport mode access
switchport access vlan6
end

Step 7: Connect vlans

On IVR:
conf t
int f0/0.1
encapsulate dot1q 2
ip add 192.168.1.7 255.255.255.0
exit
int f0/0.2
encapsulate dot1q 3
ip add 192.168.2.7 255.255.255.0
exit
int f0/0.3
encapsulate dot1q 4
ip add 192.168.3.7 255.255.255.0
exit
int f0/0.4
encapsulate dot1q 5
ip add 192.168.4.7 255.255.255.0

exit
int f0/0.5
encapsulate dot1q 6
ip add 192.168.6.7 255.255.255.0
end

Step 8: Configure default-gateway for all hosts

On APC-1:
conf t
ip default-gateway 192.168.1.7
end

On APC-2:
conf t
ip default-gateway 192.168.1.7
end

On EPC-1:
conf t
ip default-gateway 192.168.2.7
end

n EPC-2:
conf t
ip default-gateway 192.168.2.7
end

On EPC-3:
conf t
ip default-gateway 192.168.2.7
end

On EPC-4:
conf t
ip default-gateway 192.168.2.7
end

On HPC-1:
conf t
ip default-gateway 192.168.6.7
end

On HPC-2:
conf t
ip default-gateway 192.168.6.7

end

On MPC-1:
conf t
ip default-gateway 192.168.3.7
end

On MPC-2:
conf t
ip default-gateway 192.168.3.7
end

On SPC-1:
conf t
ip default-gateway 192.168.4.7
end

On SPC-2:
conf t
ip default-gateway 192.168.4.7
end

On SPC-3:
conf t
ip default-gateway 192.168.4.7
end

On SPC-4:
conf t
ip default-gateway 192.168.4.7
end

On SPC-5:
conf t
ip default-gateway 192.168.4.7
end

On SPC-6:
conf t
ip default-gateway 192.168.4.7
end

CHAPTER4: CONCLUSION AND FUTURE SCOPE

4.1 RESULT

All the branches communicating with each other and access the internet via ISP using internet and network protocols. The internet-router provides the internet access to the Internet Service Provider via EIGRP configuration. ISP-1, 2 and 3 are 3 different ISPs that provide internet connectivity to organization such that if ISP-1 is down then ISP-2 takes the load and if both of them are down then ISP-3 takes the load. The IVR is also configured as DHCP server and both the Head department nodes have a DHCP client configuration. The Switches have a circular dual loop connection for free switching of packet communication. Each department is a member of a different vlan and vtp server is SW1.

4.2 FUTURE SCOPE:

Perhaps the greatest concern companies have in doing business over the Internet is the security risk. Hackers, denial-of-service (DoS) attacks, identity theft, and even Cyber-terrorism are very real dangers. In addition, you may wonder how to guarantee the performance and reliability of your Internet-based services. Or, you may not be certain that you have the resources and support needed to deploy and manage e-commerce services and processes.

The good news is that a sound network infrastructure can address all these issues. At the foundation of a robust e-commerce infrastructure are the routers and switches.

An integrated approach to routing and switching let’s all workers—even those at different sites—have the same access to business applications, unified communications, and video conferencing as their colleagues at headquarters. Cisco lets you grow your network over time, adding features and functionality as you need them while ensuring complete investment

protection. An added benefit of this integrated approach is that your IT personnel can centrally manage the network from headquarters, which keeps staffing counts low.

4.3 REFERENCES:

1. www.google.com

2. www.cbtnuggets.com