

# **INTRODUCTION TO COMPUTER NETWORK**



**DR. BABASAHEB AMBEDKAR OPEN UNIVERSITY  
AHMEDABAD**

## **Editorial Panel**

**Author : Maulik U. Patel**  
**Assistant Professor,**  
**Navgujarat College of Computer Application,**  
**Ahmedabad**

**&**

**Dr. Ajay Patel**  
**Associate Professor,**  
**Faculties of Computer Application,**  
**Ganpat University, Gujarat**

**Editor : Prof. (Dr.) Nilesh K. Modi**  
**Professor & Director,**  
**School of Computer Science,**  
**Dr. Babasaheb Ambedkar Open University,**  
**Ahmedabad**

**Language Editor : Jagdish Vinayakrao Anerao,**  
**Associate Professor of English at**  
**Smt AP Patel Arts & NP Patel Commerce**  
**College Naroda, Ahmedabad.**

**ISBN 978-93-91071-02-8**

**Edition : 2021**

**Copyright © 2020 Knowledge Management and Research Organisation.**

All rights reserved. No part of this book may be reproduced, transmitted or utilized in any form or by a means, electronic or mechanical, including photocopying, recording or by any information storage or retrieval system without written permission from us.

## **Acknowledgment**

Every attempt has been made to trace the copyright holders of material reproduced in this book. Should an infringement have occurred, we apologize for the same and will be pleased to make necessary correction/amendment in future edition of this book.

## **ROLE OF SELF-INSTRUCTIONAL MATERIAL IN DISTANCE LEARNING**

The need to plan effective instruction is imperative for a successful distance teaching repertoire. This is due to the fact that the instructional designer, the tutor, the author (s) and the student are often separated by distance and may never meet in person. This is an increasingly common scenario in distance education instruction. As much as possible, teaching by distance should stimulate the student's intellectual involvement and contain all the necessary learning instructional activities that are capable of guiding the student through the course objectives. Therefore, the course / self-instructional material is completely equipped with everything that the syllabus prescribes.

To ensure effective instruction, a number of instructional design ideas are used and these help students to acquire knowledge, intellectual skills, motor skills and necessary attitudinal changes. In this respect, students' assessment and course evaluation are incorporated in the text.

The nature of instructional activities used in distance education self-instructional materials depends on the domain of learning that they reinforce in the text, that is, the cognitive, psychomotor and affective. These are further interpreted in the acquisition of knowledge, intellectual skills and motor skills. Students may be encouraged to gain, apply and communicate (orally or in writing) the knowledge acquired. Intellectual-skills objectives may be met by designing instructions that make use of students' prior knowledge and experiences in the discourse as the foundation on which newly acquired knowledge is built.

The provision of exercises in the form of assignments, projects and tutorial feedback is necessary. Instructional activities that teach motor skills need to be graphically demonstrated and the correct practices provided during tutorials. Instructional activities for inculcating change in attitude and behaviour should create interest and demonstrate need and benefits gained by adopting the required change. Information on the adoption and procedures for practice of new attitudes may then be introduced.

Teaching and learning at a distance eliminate interactive communication cues, such as pauses, intonation and gestures, associated with the face-to-face method of teaching. This is

particularly so with the exclusive use of print media. Instructional activities built into the instructional repertoire provide this missing interaction between the student and the teacher. Therefore, the use of instructional activities to affect better distance teaching is not optional, but mandatory.

Our team of successful writers and authors has tried to reduce this.

Divide and to bring this Self-Instructional Material as the best teaching and communication tool. Instructional activities are varied in order to assess the different facets of the domains of learning.

Distance education teaching repertoire involves extensive use of self-instructional materials, be they print or otherwise. These materials are designed to achieve certain pre-determined learning outcomes, namely goals and objectives that are contained in an instructional plan. Since the teaching process is affected over a distance, there is need to ensure that students actively participate in their learning by performing specific tasks that help them to understand the relevant concepts. Therefore, a set of exercises is built into the teaching repertoire in order to link what students and tutors do in the framework of the course outline. These could be in the form of students' assignments, a research project or a science practical exercise. Examples of instructional activities in distance education are too numerous to list. Instructional activities, when used in this context, help to motivate students, guide and measure students' performance (continuous assessment)

## **PREFACE**

We have put in lots of hard work to make this book as user-friendly as possible, but we have not sacrificed quality. Experts were involved in preparing the materials. However, concepts are explained in easy language for you. We have included many tables and examples for easy understanding.

We sincerely hope this book will help you in every way you expect.

All the best for your studies from our team!

# INTRODUCTION TO COMPUTER NETWORK

## Contents

---

### **BLOCK 1 : NETWORK ESSENTIALS, STANDARDS AND NETWORK LAYERING AND ADDRESSING**

---

#### **Unit 1      NETWORKING ESSENTIALS**

Introduction, Brief History of Networking, Networking, Types of Networking, Network Fundamentals, Fundamentals of Network Characteristics, Market Leaders, The Future of Networking, Advantages of Network, Disadvantages of Networking, Networks Terminologies, Data Communication, Protocol, Internet, Intranet, Local Area Network (LAN), Metropolitan Area Network (MAN), Wide Area Network (WAN), World Wide Web, Analog Signals, Digital Signals, Bandwidth of Signals, Amplitude of Signals, Frequency of Signals

#### **Unit 2      STANDARDS**

Introduction, LAN Components, Ethernet, Definition : 802.11, IEEE Standards 802.11, IEEE 802.11 Working Group Standards, Bluetooth, Is 5 GHz Wireless Network Hardware better than 2.4 GHz ?, GHz and Network Speed, GHz and Network Interface

#### **Unit 3      NETWORK LAYERING AND ADDRESSING**

Introduction, OSI Reference Model, TCP/IP Model, Addressing in Network, IP Address, IPV-4 Address, IPV-6, MAC Address, IP Address Class, IP Headers, Static Addressing, Dynamic Addressing, Subnetting, Handshaking

---

### **BLOCK 2 : LAN, WAN, TCP/IP AND NETWORK PROTOCOLS**

---

#### **Unit 4      LAN AND WAN - I**

Introduction, LAN Protocols, LAN, LAN Protocols and OSI Reference Model, LAN Media Access Methods, LAN Transmission Methods, LAN Topologies, LAN Devices, WAN Protocols, HDLC, PPP, Frame Relay, WAN, Protocol Structure, Wide Area Network and WAN Protocols, Point to Point Links, Circuit Switching, Packet Switching, WAN Virtual Circuits, WAN Dialup Services, WAN Devices, WAN Switch

**Unit 5 LAN AND WAN – II**

Introduction, Origin and Evolution of Network Operating System, Functional Separation and Process Scheduling, Virtual Memory/Preemptive Scheduling Programming Model, WAN Interface Information

**Unit 6 TCP/IP**

Introduction, Network Function, TCP Protocol Operation, Connection Establishment, Features of SPP-over-IP, Repeater Operation, SPP-over-IP over GPRS, Opening Connection from Access Server, SPP-over-IP and COM Ports, Maintaining and Forwarding Outgoing Connections, Some TCP/IP Suite Members and their Functions, IP Address

**Unit 7 TCP/IP PROTOCOLS-I**

Introduction, ARP, RARP, IPv4, IPv4 Header, IPv6, IPv 6 Address Type, ICMP, TCP, TCP Header, UDP

**Unit 8 TCP/IP PROTOCOLS-II**

Introduction, Remote Access Protocol, Serial Line Internet Protocol (SLIP), Point-to-Point Protocol (PPP) and PPPoE (Point-to-Point Protocol over Ethernet), Point-to-Point Tunnelling Protocol (PPTP), Windows Remote Access Services (RAS), Remote Desktop Protocol (RDP), FTP, Hypertext Transfer Protocol, Hypertext Transfer Protocol Secure, Mailing Protocols, POP3, IMAP, SMTP, Exchange Account (EAS – Exchange ActiveSync)

---

**BLOCK 3 : NETWORK OS AND NETWORK MANAGEMENT**

---

**Unit 9 NETWORK OPERATING SYSTEMS**

Introduction, Windows NT Workstation, Browsing, NetBIOS Interface to Application Programs, WINS/NBNS (Windows Internet Name Service/NetBIOS Name Service), NetBIOS Over TCP/IP, Workgroup, Multiple Master Domain Model, Multiple Trust Models, Windows Server Application

**Unit 10      NETWORK MANAGEMENT**

Introduction, Function and Characteristics, Routers, Network Management, Fault Management, Network Management Platform, Troubleshooting Infrastructure, Fault Detection and Notification, Proactive Fault Monitoring and Notification, Configuration Management, Configuration Standards, Configuration File Management

**Unit 11      HIGH SPEED NETWORKING**

Introduction, The Need for Speed Tests, Network Latency, Latency vs Bandwidth, Latency of Satellite Internet Service, Measuring Network Latency, Benchmarking the Testing Services, Methodology, Text File Download, Image Download, DSL and Cable Speeds, Cable Speed : How fast is Cable Modem Internet ?, DSL Speed of Downloading and Uploading

---

**BLOCK 4 : NETWORK COMMUNICATION AND SOCKET PROGRAMMING**

---

**Unit 12      NETWORKING DEVICES**

Introduction, Network Interface Card, HUB, Switches, Wireless Access Point, Router, Firewall, DHCP Servers, SOHO Networks

**Unit 13      SOFTWARE CONSIDERATIONS IN NETWORKING AND COMMUNICATION**

Introduction, HP-UX IO Cards, Types of Communication Services, Communication Media, Terminal Emulator, Network Cards, Wireless Router

**Unit 14      SOCKET PROGRAMMING**

Introduction, Connections Oriented with Server Side Program, Connections Oriented with Client Side Program, Connectionless Server Side Programs, Connectionless Client Side Programs, How to Listen for Socket Connections ?, How to Talk between Sockets ?, What to do when you're done with A Socket ?





**BAOU**  
Education  
for All

Dr. Babasaheb Ambedkar  
Open University Ahmedabad

BCAR-301

# **INTRODUCTION TO** **COMPUTER NETWORK**

---

**BLOCK 1 : NETWORK ESSENTIALS, STANDARDS AND  
NETWORK LAYERING AND ADDRESSING**

---

UNIT 1 NETWORKING ESSENTIALS

UNIT 2 STANDARDS

UNIT 3 NETWORK LAYERING AND ADDRESSING

# ***NETWORK ESSENTIALS, STANDARDS AND NETWORK LAYERING AND ADDRESSING***

## **Block Introduction :**

In this block the whole content has been divided into Three units .The first unit covers the topic networking essentials and has been discussed in detail, the second unit covers the topic standards which have even been discussed in detail, whereas the the third unit covers the Layering of Computer Network communication and addressing technic in detail. The writer in the book has tried his best to explain the topics he has kept the language of the book very simple in order to make it more understandable.

This block will be giving you an introduction to the essentials of networking along with its history. Here you will be detailed about the fundamentals of networking its various layers, various models and architecture of networking.

Apart from this in the second unit you will be detailed about the various components of LAN, Ethernet and you will also be given a brief introduction about the Bluetooth and about 5 GHz wireless.

In the Third unit you will be detailed about the OSI Reference model and TCP/IP model which acknowledge you the role of different layer in Network, also while we connect machine in network it also follow some protocols and their architecture it is also detailed in well manner. You will also get the different types of Unique Addressing numbers which are used to identify a machine uniquely in network.

Through this block the readers will get a detailed overview of the topics under essentials and standards under networking.

## **Block Objectives :**

**After learning this block, you will be able to understand :**

- Networking and its types
- Various layer and architecture of Networking
- various Protocols of networking
- Advantages and disadvantages of Networking
- Lan components
- IEEE Standards
- Addressing Technic
- TCP/IP Header

**Block Structure :**

**Unit 1 : Networking Essentials**

**Unit 2 : Standards**

**Unit 3 : Network Layering and Addressing**

**UNIT STRUCTURE**

- 1.0 Learning Objectives**
  - 1.1 Introduction**
  - 1.2 Brief History of Networking**
  - 1.3 Networking**
    - 1.3.1 Types of Networking**
  - 1.4 Network Fundamentals**
    - 1.4.1 Fundamentals of Network Characteristics**
  - 1.5 Market Leaders.**
    - 1.5.1 The Future of Networking**
  - 1.6 Advantages of Network**
  - 1.7 Disadvantages of Networking**
  - 1.8 Networks Terminologies**
    - 1.8.1 Data Communication**
    - 1.8.2 Protocol**
    - 1.8.3 Internet**
    - 1.8.4 Intranet**
    - 1.8.5 Local Area Network (LAN)**
    - 1.8.6 Metropolitan Area Network (MAN)**
    - 1.8.7 Wide Area Network (WAN)**
    - 1.8.8 World Wide Web**
    - 1.8.9 Analog Signals**
    - 1.8.10 Digital Signals**
    - 1.8.11 Bandwidth of Signals**
    - 1.8.12 Amplitude of Signals**
    - 1.8.13 Frequency of Signals**
  - 1.9 Lets Sum UP**
  - 1.10 Answers for Check Your Progress**
  - 1.11 Glossary**
  - 1.12 Assignment**
  - 1.13 Activities**
  - 1.14 Case Study**
  - 1.15 Further Readings**
-

## **1.0 Learning Objectives :**

**After learning this unit, you will be able to understand :**

- Networking characteristics
- Future of networking
- Networking layers
- Protocol and its meaning
- Advantages and disadvantages of networking

## **1.1 Introduction :**

Now-a-days, networks are everywhere. The internet has revolutionized not only the computer world, but also the lives of millions in a variety of ways in the "real world".

Given the ubiquitous quality of networking, it is hard to believe that the field is still a relatively young one, especially when it comes to connecting small computers like PCs. In approaching any discussion of networking, it is very useful to take a step back and look at networking from a high level. What exactly is it and why is it now considered so important that it is assumed that most PCs and other devices should be networked?

In this section, a quick introduction to networking is provided, wherein general terms related to it are discussed. Thereafter, pros and cons of networking are described, along with costs incurred.

## **1.2 Brief History of Networking :**

Having made devices converse with each other to serve the purposes of communication is not very new. Early forays into telephony such as the telegraph and telephone have since evolved into more complicated devices and now a computer can be networked to the Internet, another PC or even a home stereo. In the early 1960s, individual computers had to be shared on the physical basis, thereby making the sharing of data and other information tough. Seeing this was impractical, researchers developed a way to "connect" the computers so they could share their resources more efficiently. This led to the birth of early computer network.

Through the then novel communication protocol termed as packet switching, numerous applications like secure voice transmission in military channels became possible. These new circuits provided the basis for the communication technologies of the rest of the 20th century and with further refinement, these were applied to computer networks.

Such networks provided the bases for the early ARPANET, which was found to be the forerunner of the modern Internet. The Advanced Research Projects Agency (ARPA) submitted the proposal for the project on June 3, 1968, which was approved a few weeks later. The proposal entitled "Resource Sharing Computer Networks" would let ARPA not just promote sharing of their data, but would let them further their research in abroad variety of military as well as scientific fields. After being tested in four locations, the network spread and the new protocols created for its use evolved into today's World Wide Network.

In 1977, the early PC-based Local Area Networks, better known as LANs (Local Area Networks), were spreading and while initially restricted to hobbyists and academics, they eventually found their way into the workplace and in homes, even though the explosion into the latter 2 arenas is a comparatively recent phenomenon. LAN variants also developed, including Metropolitan Area Networks (MANs) to cover large areas such as a college campus and Wide Area Networks (WANs) for university-to-university communication. With the widespread usage on the part of computers in the corporate world, the speed and convenience to use them to communicate and transfer data has forever altered the landscape of the way people conduct businesses.

❑ **Check Your Progress – 1 :**

1. LAN variants also developed, including \_\_\_\_\_ to cover large areas such as
  - a. college campus
  - b. MAN
  - c. WAN (Size Bullets)

<b>1.3 Networking :</b>
-------------------------

For such an extensive and involved subject, which includes so many different technologies, hardware devices and protocols, the definition of networking is actually quite simple. A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

Networks are used for an incredible array of different purposes. While most people learning about networking focus on the interconnection of PCs and other "true" computers, you use various types of networks every day. Each time you pick up a phone, use a credit card at a store, get cash from an ATM machine or even plug in an electrical appliance, you are using some type of network.

In fact, the definition can even be expanded beyond the world of technology altogether : you must have heard the term "networking" used to describe the process of finding an employer or employee by talking to friends and associates. In this case too, the idea is that independent units are connected together to share information and cooperate.

The widespread networking of personal computers is a relatively new phenomenon. For the first decade or so of their existence, PCs were very much "islands unto themselves" and were rarely connected together. In the early 1990s, PC networking began to grow in popularity as businesses realized the advantages that networking could provide. By the late 1990s, networking in homes with two or more PCs started to really take off as well.

This interconnection of small devices represents, in a way, a return to the "good old days" of mainframe computers. Before computers were small and personal, they were large and centralized machines that were shared by many users operating remote terminals. While having the entire computer power in one place had many disadvantages, one benefit was that all users were connected because they shared the central computer.

Individualized PCs took away that advantage, in favour of the benefits of independence. Networking attempts to move computing into the middle ground, providing PC users with the best of both worlds: the independence and flexibility of personal computers and the connectivity and resource sharing of mainframes.

### **1.3.1 Types of Networking :**

In the world of computers, networking is the practice of linking two or more computing devices together for sharing data. Networks are built with a mix of computer hardware and computer software.

#### **➤ Area Networks :**

Networks can be categorized in several different ways. One approach defines the type of network according to the geographic area it spans. Local area networks (LANs), for example, typically reach across a single home, whereas wide area networks (WANs) reach across cities, states or even across the world. The internet is the world's largest public WAN.

#### **➤ Network Design :**

Computer networks also differ in their design. The two types of high-level network design are called client-server and peer-to-peer. Client-server networks feature centralized server computers that store email, web pages, files and or applications. On a peer-to-peer network, conversely, all computers tend to support the same functions. Client-server networks are much more common in business and peer-to-peer networks much more common in homes.

A network topology represents its layout or structure from the point of view of data flow. In so-called bus networks, for example, all of the computers share and communicate across one common conduit, whereas in a star network, all data flows through one centralized device. Common types of network topologies include bus, star, and ring and mesh.

#### **➤ Network Protocols :**

In networking, the communication language used by computer devices is called protocol. Yet another way to classify computer networks is by the set of protocols they support. Networks often implement multiple protocols to support specific applications. Popular protocols include TCP/IP, the most common protocol found on the internet and in-home networks.

#### **➤ Wired vs Wireless Networking :**

Many of the same network protocols like TCP/IP work are present in both wired and wireless networks. Networks with Ethernet cables predominated businesses, schools and homes for several decades. Recently, however, wireless networking alternatives have emerged as the premier technology for building new computer networks.

#### **☐ Check Your Progress – 2 :**

1. A \_\_\_\_\_ is simply a collection of computers or other hardware devices that are connected together.

- a. Network      b. Lan      c. Wan      d. MAN



## 1.4 Network Fundamentals :

In order to get the most of The TCP/IP Guide, a certain level of knowledge regarding the basics of networking is very helpful. Thus, this section provides an overview of some of the basic issues related to networking. Here you will find discussions of some of the most fundamental networking concepts and ideas. It serves not only to provide you with useful background material, but also as a repository for "general" information. This in turn allows those who already know about these basics to avoid having to skip over them in many other locations.

### 1.4.1 Fundamentals of Network Characteristics :

There are many different kinds of networks and network technologies used to create them. The proliferation of networking methods has generally occurred for a very good reason : different needs require different solutions. The drawback of this is that there are so many different types of protocols and technologies for the networking student to understand. Before you can really compare these approaches, you need to understand some of the basic characteristics that make networks what they are. While network types may be quite dissimilar, they are often described and even contrasted on the basis of a number of common attributes.

In this section, a number of key networking concepts that describe and differentiate different types of networks and networking technologies are introduced and discussed. A number of terms and "buzzwords" that you cannot avoid if you are going to learn about networks are explained. The topics here include explanations of protocols, switching methods, types of network messages, and message formatting apart from ways of addressing messages. Discussion of differences between client–server and peer–to–peer networking is also included.

#### □ Check Your Progress – 3 :

1. The drawback of proliferation of networking methods is that there are so many different types of \_\_\_\_\_ and technologies for the networking student to understand.
  - a. Protocols
  - b. Format
  - c. buzzwords

## 1.5 Market Leaders :

Much of the technological advances in networking come from a wide variety of sources, but a number of companies continue to innovate and lead by providing the infrastructure and necessary hardware. While Microsoft dominates the field of operating systems on workstations and on many servers with Windows, the open source Apache Web server provides the foundation for more Web servers than any competing product by a tremendous margin. Numerous companies continue to develop and invent new technologies, such as hardware from Cisco Systems. Known for their routers and countless other products, they also provide diverse wireless networking solutions through their Linksys brand. Other networking market leaders include: Nortel Networks, Novell, Lucent Technologies and Juniper Networks.

### 1.5.1 The Future of Networking :

While the initial concept behind computer networking was to see each and every person on the planet being "wired," the evolution of technology aims to do just the opposite. Wireless technologies are emerging as a popular, cable–

free alternative to traditional wired networks. By the year 2009, it was predicted that wearable computers – which would replace the personal digital assistant or PDA – would be fully integrated in the workplace, with the ability of connecting to both wired and wireless networks. Other emerging technologies range from smart appliances– products which have enhanced capabilities and/or the ability of accessing the internet, to completely automated homes which have all appliances, heating and cooling systems, entertainment and the other home needs connected through a LAN. Voice–Over Internet Protocol (VoIP) and convergence are also considered in the recent developments.

❑ **Check Your Progress – 4 :**

1. \_\_\_\_\_ server provides the foundation for more Web servers than any competing product by a tremendous margin.
  - a. Apache Web
  - b. Microsoft
  - c. Apple

**1.6 Advantages of Network :**

You have undoubtedly heard the "the whole is greater than the sum of its parts." This phrase describes networking very well and explains why it has become so popular. A network is not just a bunch of computers with wires running between them. Properly implemented, a network is a system that provides its users with unique capabilities, above and beyond what the individual machines and their software applications can provide.

Most of the benefits of networking can be divided into two generic categories : connectivity and sharing. Networks allow computers and hence their users to be connected together. They also allow for the easy sharing of information and resources and cooperation between the devices in other ways. Since modern business depends so much on the intelligent flow and management of information, this tells you a lot about why networking is so valuable.

Here are some of the specific advantages generally associated with networking :

**Connectivity and Communication** – Networks connect computers and the users of those computers. Individuals within a building or work group can be connected into local area networks (LANs); LANs in distant locations can be interconnected into larger wide area networks (WANs). Once connected, it is possible for network users to communicate with each other using technologies such as electronic mail. This makes the transmission of business (or non–business) information easier, more efficient and less expensive than it would be without the network.

**Data Sharing** – One of the most important uses of networking is to allow the sharing of data. Before networking was common, an accounting employee who wanted to prepare a report for his manager would have to produce it on his PC, put it on a floppy disk and then walk it over to the manager, who would transfer the data to his PC's hard disk. True networking allows thousands of employees to share data much more easily and quickly than this. More so, it makes possible applications that rely on the ability of many people to access and share the same data, such as databases, group software development and much more. Intranets and extranets can be used to distribute corporate information between sites and to business partners.

**Hardware Sharing** – Networks facilitate the sharing of hardware devices. For example, instead of giving each of 10 employees in a department an expensive color printer, one printer can be placed on the network for everyone to share.

**Internet Access** – The internet is itself an enormous network, so whenever you access the Internet, you are using a network. The significance of the internet on modern society is hard to exaggerate, especially for those of us in technical fields.

**Internet Access Sharing** – Small computer networks allow multiple users to share a single Internet connection. Special hardware devices allow the bandwidth of the connection to be easily allocated to various individuals as they need it and permit an organization to purchase one high-speed connection instead of many slower ones.

**Data Security and Management** – In a business environment, a network allows the administrators to manage the company's critical data in a better manner. Instead of having this data spread over dozens or even hundreds of small computers in a haphazard fashion as their users create it, data can be centralized on shared servers. This makes it easy for everyone to find the data, and possible for the administrators to ensure that the data is regularly backed up and allows for the implementation of security measures to control who can read or change various pieces of critical information.

**Performance Enhancement and Balancing** – Under some circumstances, a network can be used to enhance the overall performance of some applications by distributing the computation tasks to various computers on the network.

**Entertainment** – Networks facilitate many types of games and entertainment. The internet itself offers many sources of entertainment, of course. In addition, many multi-player games that operate over a local area network exist. Many home networks are set up for this reason and gaming across wide area networks (including the internet) has become quite popular, too.

❑ **Check Your Progress – 5 :**

1. The \_\_\_\_\_ is itself an enormous network, so whenever you access it, you are using a network.
  - a. Internet
  - b. LAN
  - c. MAN

<b>1.7 Disadvantages of Networking :</b>
--

We have seen the value and many useful benefits of networking up to this point. Networking really does represent a "whole that is greater than the sum of its parts"; however, it does have some real and significant demerits and drawbacks associated with it.

**Network Hardware, Software and Setup Costs** – Computers obviously do not just magically network themselves. Setting up a network requires an investment in hardware and software, as well as funds for planning, designing and implementing the network.

**Hardware and Software Management and Administration Costs** – In all but the smallest of implementations, ongoing maintenance and management of the network requires the care and attention of an IT professional. In a smaller organization that already has a system administrator, a network may fall within

this person's job responsibilities but it will take time away from other tasks. In more substantial organizations, a network administrator may need to be hired and in large companies, an entire department may be necessary.

**Undesirable Sharing** – While networking allows easy sharing of useful information, it also allows the sharing of undesirable data. One significant "sharing problem" in this regard has to do with viruses, which are easily spread over networks and the Internet. Mitigating these effects costs more time, money and administrative effort.

**Illegal or Undesirable Behaviour** – Similar to the point above, networking facilitates useful connectivity and communication, but also brings difficulties with it. Typical problems include abuse of company resources, distractions that reduce productivity, downloading of illegal or illicit materials and even software piracy. In larger organizations, these issues must be managed through explicit policies and monitoring, which again, further increases management costs.

**Data Security Concerns** – If a network is implemented properly, it is possible to greatly improve the security of important data. In contrast, a poorly secured network puts critical data at risk, exposing it to the potential problems associated with hackers, unauthorized access and even sabotage.

Most of these costs and potential problems can be managed; that occupies a big part of the job of those who set up and run networks. In the end, as with any other decision, whether to network or not is a matter of weighing the advantages against the disadvantages.

❑ **Check Your Progress – 6 :**

1. If a \_\_\_\_\_ is implemented properly, it is possible to greatly improve the security of important data.
  - a. Network
  - b. Internet
  - c. Protocol

**1.8 Networks Terminologies :**

**1.8.1 Data Communication :**

When we communicate, we are sharing information. This sharing can be local or remote. between individuals, local communication usually occurs face to face, while remote communication takes place over distance. But in Terms of Computer Data Communication means exchange information or data between two computers or source and destination. In Computer data are in binary format so it is transferring data in 1 and 0 formats. Source transmits the data and receivers receive the data. Data Communication is interested in the transfer of data, the method of transfer and the preservation of the data during the transfer process. Data communication is take place under some protocols. These protocols are defined rules and regulations.

**1.8.2 Protocol :**

Protocol means "set of rules". In Communication there must be some rules that rules are define in protocols. For different types of communication there are different types of protocols are design. These protocols are implementing on same types of communication medium, hardware and software which are used in network. For example, if one person can speak only French language then he cannot communicate with other persons in Other Language. Same as, two devices must communicate with each other if it can follow and understand same protocols. It is also compulsory sending device and receiving device both

understand same protocols and ready to conversations. Then and only then sender and receiver device communicate. Otherwise, sender is ready to send but receiver is not understood the protocol so it will not full fill complete communication and there must be error occur in communication. There are many protocols are design in Data Communications. Each Protocol is start their own task based on Communication and Data which is send and receive. Some protocols are very popular but some are use very less. Protocols are work on three basic characteristic.

**Syntax :** It is focused on Data. What kind of Data is send ,the structure of Data also define in syntax. Same structure of Data Sender and Receiver machine can understand, It is a role of protocol to convert data in same syntax so communication can take place.

**Semantics :** IT Focused on Interpretation of Data which is sent. How data is understand and how it is interpreted by receiver, IT is also defined how it is communicated.

**Timing :** IT is focused on Agreement between Sender and receiver, when to start a communication and when communication is end. It defines the duration of Communication. In duration the communication must complete, it is role of protocol to set a time as much as data with sender. It also defines the transmission rate, what speed sender will send and what speed receiver will receive data. Speed management between sender and receiver also done by protocol.

### **1.8.3 Internet :**

Internet is worldwide/public network. Internet has unlimited traffic. Internet is not owned by any one. Internet is manage by Internet Service Provider (ISP). there are billions of servers are operated by internet. Internet is not a part of Intranet. Internet has various LANs, MANs and WANs

### **1.8.4 Intranet :**

Intranet is develop for privet netwrok.it is own by privet organizations.In intranet each Computers are connected with each other for local (internal) communication .Computer in intranet are not communicate with out side world. Intranet has limitd traffic mins limited users are communicate. Intranet is owned by specific organization. Intranet is manage by network administrator who is woking in organization. More then one intranet can be a part of Internet

For example our college lab. In lab each machines are communicate with each other intenal only some machines have permission to work in internet.same as shoos, compny, organization, hospital etc. develop their own application which accessibel within their network only.

### **1.8.5 Local Area Network (LAN) :**

LAN Usually private/owned network. It established Network in single Building or Campus up to a few kilometers. LAN can span UP to 1mete to 100 meter but now days LAN can span up to 1 kilometer. LAN is widely used to connect personal computer and workstation in company, college to share resources and exchange data. Most common LAN Topology is Bus, Ring and Star. Traditional LAN Data Rate is 4 to 6 Mbps. Today speed is increasing and Data rate is up to 100 Mbps.

### **1.8.6 Metropolitan Area Network (MAN) :**

MAN is designed to extend over an entire city or town. This kind of network spread across city. MAN can connect large network through Fiber optic or Coaxial cable now a days it can be connected wireless. It may be a single network such as a cable television network (GTPL).It may be connecting a number of LANs in to a large network.

### **1.8.7 Wide Area Network (WAN) :**

WAN spans a large geographical area .It often connected with country or continent. It provide long distance transmission of data. Communication in WAN is done by telephone, satellite dishes and Radio waves.Every MAN and LAN are connected with WAN.

### **1.8.8 World Wide Web :**

WWW is a collection of different web documents which are access on web browser. WWW is a help full to browsing a hypertext document on internet. Web browser are used to view such pages that may contain image, video and other multimedia document with the help of HTTP. Its Inventor Tim Berners-Lee in 1980 was investigating how computer could store information with random links. In 1989 at the European Particle Physics Laboratory, he proposed the idea of Global Hypertext space in which any network accessible information could be referred by a single 'Universal Document Identifier'.in 1990 this idea is expanded with a program called 'World Wide Web'.

### **1.8.9 Analog Signals :**

Analog waves are in continuous so it is transmit in wave form. Example of Analog signal is Human voice, or any other voice. Analog signals are visualize as a simple curve. It is call oscillations. This signals are transmit on medium by generating smooth cycles in rolling flow. An analog signal can be defined by using amplitude frequency, & phase. This can be captured by microphone. An analog signal is not resistant toward the noise, therefore; it faces distortion as well as reduces the transmission quality. Anlaog signal passes from one destination to another with infinite waves. For long distance transmission Analog signals are regenerated by Amplifier. Analog signal is not encrypted, Analog signals bandwidth is low.

### **1.8.10 Digital Signals :**

Digital data transmit in form of value like on and off or 1 and 0 so it is represented with square waves. Digital Signals are generated through voltage so it is store in memory and transmit in form of 1 and 0. Digital signal can be defined by bit interval as well as bit rate. It is in binary forate .Digital signals are more resistant toward the noise; therefore, it barely faces some distortion. Digital Signals transmit in limited value so there is fixed number of digits is transmit and that number of waves are generate in this signal. For long distance transmission Digital signals are regenerated by Repeater. Digital signal is encrypted. Digital signals bandwidth is high.

### **1.8.11 Bandwidth of Signals :**

As we know any data can transmit in medium, we major the capacity of medium to transfer data. To major Capacity of medium is consider as major bandwidth. For example There is one Tank in Tenement and there is one Water pipe is passing from Tank to each house that pipe is large enough to flow

a water to each house but at the end each house has smaller pipe then main tank pipe so each house can get enough water in equal quantity. In above example main pipe is large so its capacity to transmit water is high flow. But each house has smaller pipe so the capacity of water flow will decrees. Bandwidth means maximum capacity to transmit data thorough medium. We are using different bandwidth to pass data in different types of transmission. Analog signal are transmit different types of voice in different bandwidth, same digital signals are transmit different data on different bandwidth.

### **1.8.12 Amplitude of Signals :**

Each signals are traverse in horizontal line, it traverse with some value this value is called its voltage .Voltages are measure in vertical line on T time period as the signal traverse. To measure a voltage on vertical line is also called amplitude of signals in other word it is called signals amplitude. It refers Height of the signals. The maximum amplitude of signal means highest value signal reaches on vertical axis. Amplitude is measured in volts or watts.

### **1.8.13 Frequency of Signals :**

Signals traverse in form of waves are called its cycle. Frequency is used measure how many cycles (oscillations) of signal is completed in 1 second. Means if there is only one cycle complete in one second then the frequency of signal is 1, if there are 3 cycles completed in one second then the frequency of signal is 3.Frequency is measured in Hz. We can say that 3Hz frequency. Frequency and Force are work to gather, as the Force is increase number of Frequency also increase. If the force is decrease number of Frequency also decreases.

## **1.9 Lets Sum Up :**

In this unit, we have learned :

- Initially LANs was restricted to hobbyists and academics, they eventually found their way into the workplace and in homes.
- LAN variants also developed, including Metropolitan Area Networks (MANs) to cover large areas such as a college campus and Wide Area Networks (WANs) for university-to-university communication.
- A network can be explained as a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate.
- Networks can be categorized in several different ways: Area Networks, Network Design, Network Protocols, Wired vs. Wireless Networking.
- There are many different kinds of networks and network technologies used to create them. The proliferation of networking methods has generally occurred for a very good reason: different needs require different solutions.
- So after a detailed discussion the conclusion can be drawn that here an introduction about the essentials of networking was given event the history of networking was also discussed in detail. Readers were also briefed about the fundamentals of networking its various layers, various models and architecture of networking. Apart from this in the second unit you will be detailed about the various componenets of LAN, ethernet

and you will also be given a brief introduction about the bluetooth and about 5 GHz wireless.

**1.10 Answer for Check Your Progress :**

- Check Your Progress 1 :**  
1 : a
- Check Your Progress 2 :**  
1 : a
- Check Your Progress 3 :**  
1 : a
- Check Your Progress 4 :**  
1 : a
- Check Your Progress 5 :**  
1 : a
- Check Your Progress 6 :**  
1 : a

**1.11 Glossary :**

1. **Network Layer :** The third lowest layer in the OSI seven layer model. The network layer determines routing of packets of data from sender to receiver via the data link layer and is used by the transport layer. The most common network layer protocol is IP.
2. **Repeater :** A network or communications device which propagates electrical signals from one cable to another, amplifying them to restore them to full strength in the process. Repeaters are used to counter the attenuation which occurs when signals travel long distances
3. **Router :** A device which forwards packets between networks. The forwarding decision is based on network layer information and routing tables, often constructed by routing protocols.
4. **Virtual Circuit :** A connection-oriented network service which is implemented on top of a network which may be either connection-oriented or connectionless (packet switching).
5. **Virtual Memory :** a system whereby addressable memory is extended beyond main storage through the use of secondary storage managed by system software in such a way that programs can treat all of the designated storage as addressable main storage.

**1.12 Assignment :**

What are the fundamental characteristics of networking ?

**1.13 Activities :**

Explain Terminology of Network.

**1.14 Case Study :**

Draw the Architecture of LAN MAN and WAN.



**1.15 Further Readings :**

1. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001 Digital Networking.
2. Sams Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002.

**UNIT STRUCTURE**

- 2.0 Learning Objectives
- 2.1 Introduction
- 2.2 LAN Components
- 2.3 Ethernet
- 2.4 Definition : 802.11
- 2.5 IEEE Standards 802.11
- 2.6 IEEE 802.11 Working Group Standards
- 2.7 Bluetooth
- 2.8 Is 5 GHz Wireless Network Hardware better than 2.4 GHz ?
  - 2.8.1 GHz and Network Speed
  - 2.8.2 GHz and Network Interface
- 2.9 Let Us Sum Up
- 2.10 Answers for Check Your Progress
- 2.11 Glossary
- 2.12 Assignment
- 2.13 Activities
- 2.14 Case Study
- 2.15 Further Readings

**2.0 Learning Objectives :**

After learning this unit, you will be able to understand :

- LAN components
- Ethernet
- IEEE Standards
- Work group standards
- Pros and cons of standards

**2.1 Introduction :**

In this unit, you will learn about local area network, or LAN terminology, basic Ethernet networking, a general introduction to LAN, introduction to IEEE, LAN topologies, WAN standards.

The Institute of Electrical and Electronic Engineers (IEEE) in 1985 produced a series of standards for the Local Area Networks, which are called IEEE 802 standards. The IEEE standards have been developed by the International Standards Organisation (ISO).

These standards have been accepted widely throughout the world of information technology. One of the IEEE 802 standards, the IEEE 802.3 is

known as "Ethernet". Ethernet is the most widely used LAN technology. Ethernet was developed by Xerox Corporation in the year 1972. This was the first LAN.

Ethernet, in its simplest form, uses a passive bus, which operates at 10 Mbps. The bus is formed from the co-axial cable, which connects all the PCs in the LAN.

One or more segments of the co-axial cable are attached end to end to create the Ethernet cable segment. Each segment is terminated by 50-ohm resistors. A single LAN may have 1024 attached computers, although in real practice most LANS have fewer computers than this number.

Today, reliable and timely access to the information has become vital. The present scenario is such that co-workers- thousands of miles apart from each other- can share data, voice, video, etc., within fractions of a second. On the similar lines, a larger number of the co-workers can review research data simultaneously. Ethernet is a communication protocol that is embedded in software and hardware devices that intend to be embedded. Ethernet has become the standard computer networking protocol with the help of the Xerox, Intel and Digital

## **2.2 LAN Components :**

LAN components are as follows :

- Two or more computers
- Network Interface card or LAN Card in each PC
- Ethernet cable (Cat 5, UTP/SPT) cable to connect the two computers
- A hub, switch or router to route or direct the network traffic
- Software for the communication/computer networking

A network interface card (NIC) is attached and installed in each PC and is assigned a unique address. An Ethernet cable is used to connect two computers; Ethernet cable has RJ45 connectors at both its ends. There can be two scenarios:

1. Two computers can directly connect with each other
2. Each computer is directly connected with the hub/switch and hence communication occurs in the network. The hub or switch acts as relay.

Computer network can be wireless. Despite using Ethernet cable for communication, wireless network interface cards use radio waves to communicate with wireless switch or hub. A small antenna is used in the wireless NICs, switches and hubs. Although the wireless networks are easier to use as compared to the cabled networks, more configurations and extra care is required to setup and run a wireless network.

The alternate technology to Ethernet is "token ring", which is used in the ring topologies networks. In ATM (Asynchronous Transfer Mode) networking, devices are connected with each other over a very large distance (thus forming a WAN) and behave like LANs.

Ethernet is a well-established and widely used network standard for small to medium sized Ethernet networks as well as for other networks. Ethernet has been used for over 3 decades. It forms an excellent networking/communication environment.

❑ **Check Your Progress – 1 :**

1. A \_\_\_\_\_ is attached and installed in each PC and is assigned a unique address.
  - a. Network interface card
  - b. CPU
  - c. UPS

**2.3 Ethernet :**

Ethernet is a physical "data link layer technology" for local area networks (LANs). It was invented by engineer Robert Metcalfe. When first widely deployed in the 1980s, Ethernet supported a maximum theoretical data rate of 10 megabits per second (Mbps). Later, so-called "fast Ethernet" standards increased this maximum data rate to 100 Mbps. Today, Gigabit Ethernet technology further extends peak performance up to 1000 Mbps. Higher level network protocols like Internet Protocol (IP) use Ethernet as their transmission medium. Data travels over Ethernet inside protocol units called "frames".

The run length of individual Ethernet "cables" is limited to roughly 100 meters, but Ethernet networks can be easily extended to link entire schools or office buildings using network bridge devices. Ethernet is a protocol, which controls the way data is transmitted over a local area network (LAN). It uses wires (meaning it is not a wireless technology). The wires used for a LAN are mostly those headed by an RJ-45 jack, which is similar to the jack plugged into your telephone set, but twice as big. Some Ethernet networks use coaxial cables, but that is rarer and present in rather large LANs, which span over areas between buildings. An example of a coaxial cable is the thick cable that links your TV antenna to your TV set.

Ethernet is, by far, the most popular LAN protocol used today. It is so popular that if you buy a network card to install on your machine, you will get an Ethernet card, unless you ask for something different, if of course that different protocol is available. Ethernet has evolved for over the years. Today, you can get cheap Ethernet LAN cards with speeds up to 100 Mbps; while the fastest Ethernet reaches Gbps (1 Gbps = 1000 Mbps) in speed.

Ethernet follows a simple set of rules. To understand these rules it is important to understand the following terminology.

- **Node** – Devices that are attached to segments are nodes.
- **Frame** – Nodes (computers or network devices) communicate in the form of short messages that are known as frames. Frames are chunks of information with variable size.
- **Segment** – A single shared medium is known as an Ethernet segment.
- **Medium** – Ethernet devices are attached to a common medium. The frames of the data travel along with that medium. This medium can be coaxial cable.

Most commonly used communication mediums are UTP/STP cable, fibre optic cables.

Frames are analogous in human language. There are some rules for constructing sentences. The Ethernet protocol specifies a set of rules for constructing frames. The frame's length varies. Each frame must contain source and destination address for the identification of the recipient and sending of the message. Nodes can be identified uniquely and easily. Each Ethernet devices must have a single unique address.

❑ **Check Your Progress – 2 :**

1. Ethernet was invented by engineer \_\_\_\_\_.
- a. Robert Metcalfe
  - b. Bill gates

**2.4 Definition – 802.11 :**

802.11 is the generic name of a family of standards for wireless networking. The numbering system for 802.11 comes from the IEEE, that uses "802" for many networking standards like Ethernet (802.3). 802.11 standards define rules for communication on wireless local area networks (WLANs). Popular 802.11 standards include 802.11a, 802.11b and 802.11g. 802.11 was the original standard in this family, ratified in the year 1997. 802.11 defined WLANs that operate at 1–2 Mbps. This standard is obsolete today. Each extension to the original 802.11 appends a unique letter to the name. While 802.11a, 802.11b and 802.11g are found to be the most interesting as far as the average consumer is concerned, many other extensions exist or are under development.

❑ **Check Your Progress – 3 :**

1. 802.11 is the generic name of a family of standards for \_\_\_\_\_.
- a. wireless networking
  - b. Wired networking
  - c. Networking

**2.5 IEEE Standards 802.11 :**

The following IEEE 802.11 standards exist or are under development to support the creation of technologies for wireless local area networking:

- 802.11a – 54 Mbps standard, 5 GHz signalling (ratified 1999).
- 802.11b – 11 Mbps standard, 2.4 GHz signalling (1999).
- 802.11c – operation of bridge connections (moved to 802.1D).
- 802.11d – worldwide compliance with regulations for use of wireless signal spectrum (2001).
- 802.11e – Quality of Service (QoS) support (not yet ratified).
- 802.11F – Inter-Access point protocol recommendation for communication between access points to support roaming clients (2003).
- 802.11g – 54 Mbps standard, 2.4 GHz signaling (2003).
- 802.11h – enhanced version of 802.11a to support European regulatory requirements (2003).
- 802.11i – security improvements for the 802.11 family (2004).
- 802.11j – enhancements to 5 ghz signaling to support Japan regulatory requirements (2004).
- 802.11k – WLAN system management (in progress).
- 802.11l – skipped to avoid confusion with 802.11i.
- 802.11m – maintenance of 802.11 family documentation.
- 802.11n – 100+ Mbps standard improvements over 802.11g (in progress).
- 802.11o – skipped.
- 802.11p – Wireless access for the vehicular environment.
- 802.11q – skipped.

## Introduction to Computer Network

- 802.11r – fast roaming support via basic service set transitions.
- 802.11s – ESS mesh networking for access points.
- 802.11T – Wireless performance prediction – recommendation for testing standards and metrics.
- 802.11u – internetworking with 3G / cellular and other forms of external networks.
- 802.11v – wireless network management / device configuration.
- 802.11w – Protected management frames security enhancement.
- 802.11x – skipped (generic name for the 802.11 family).
- 802.11y – Contention based protocol for interference avoidance.
- 802.11a – WLAN communication standard, 802.11a is one of the wireless Ethernet standards in the 802.11 series.

### □ Check Your Progress – 4 :

1. Worldwide compliance with regulations for use of wireless signal spectrum  
\_\_\_\_\_
- a. 802.11d            b. 802.11y            c. 802.11v

## 2.6 IEEE 802.11 Working Group Standards :

802.11a wireless networks supports a maximum theoretical bandwidth of 54 Mbps. 802.11a's principal advantages over 802.11b is that it supports 11 Mbps, and shows improved performance. However, 802.11a access points (APs) and adapters cost significantly more than their 802.11b counterparts did.

802.11a transmits radio signals in the frequency range above 5 GHz. This range is "regulated", meaning that 802.11a gear utilises frequencies not used by other commercial wireless products like cordless phones. In contrast, 802.11b utilises frequencies in the unregulated 2.4 GHz range and encounters much more radio interference from other devices.

**Examples :** Though it helps improve network performance and reduces interference, the range of an 802.11a signal is limited by use of the high 5 GHz frequency. An 802.11a AP transmitter may cover less than one-fourth the area of a comparable.

802.11b AP. Brick walls and other obstructions affect 802.11a wireless networks to a greater degree than they do comparable 802.11b.

Home and business networkers looking to buy wireless local area network (WLAN) gear have an array of choices. Many products conform to the 802.11a, 802.11b, 802.11g or 802.11n wireless standards collectively known as Wi-Fi technologies. Additionally, Bluetooth and various other non Wi-Fi technologies also exist, each designed for specific networking applications.

### 802.11

In the year 1997, the Institute of Electrical and Electronics Engineers (IEEE) created the first WLAN standard. They called it 802.11 after the name of the group formed to oversee its development. Unfortunately, 802.11 only supported a maximum network bandwidth of 2 Mbps – too slow for most applications. For this reason, ordinary 802.11 wireless products are no longer manufactured.

**802.11b**

IEEE expanded on the original 802.11 standard in July 1999, creating the 802.11b specification. 802.11b supports bandwidth up to 11 Mbps, comparable to traditional Ethernet.

802.11b uses the same unregulated radio signaling frequency (2.4 GHz) as the original 802.11 standard. Vendors often prefer using these frequencies to lower their production costs. Being unregulated, 802.11b gear can incur interference from microwave ovens, cordless phones and other appliances using the same 2.4 GHz range. However, by installing 802.11b gear a reasonable distance from other appliances, interference can easily be avoided.

- **Pros of 802.11b:** Lowest cost; signal range is good and not easily obstructed
- **Cons of 802.11b:** Slowest maximum speed; home appliances may interfere on the unregulated frequency band

**802.11a**

While 802.11b was in development, IEEE created a second extension to the original 802.11 standard called 802.11a. As 802.11b gained popularity faster than 802.11a, certain folks believe that 802.11a was created after 802.11b. In fact,

802.11a was created at the same time. Due to its higher cost, 802.11a is usually found on business networks, whereas 802.11b better serves the home market.

802.11a supports bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz. This higher frequency compared to 802.11b shortens the range of 802.11a networks. The higher frequency also means 802.11a signals have more difficulty penetrating walls and other obstructions. As 802.11a and 802.11b utilise different frequencies, the two technologies are incompatible with each other. Some vendors offer hybrid 802.11a/b network gear but these products merely implement two standards side by side (each connected device must use one or the other).

- **Pros of 802.11a :** Fast maximum speed; regulated frequencies prevent signal interference from other devices
- **Cons of 802.11a :** Highest cost; shorter range signal that is more easily obstructed

**802.11g**

In 2002 and 2003, WLAN products supporting a newer standard called 802.11g emerged in the market. 802.11g attempts to combine the best of both

802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps and it uses the 2.4 GHz frequency for greater range. 802.11g is backwards compatible with 802.11b, meaning that 802.11g access points will work with 802.11b wireless network adapters and vice versa.

- **Pros of 802.11g :** Fast maximum speed; signal range is good and not easily obstructed
- **Cons of 802.11g :** Costs more than 802.11b; appliances may interfere on the unregulated signal frequency

### **802.11n**

The newest IEEE standard in the Wi-Fi category is 802.11n. It was designed to improve 802.11g supported by utilising multiple wireless signals and antennas (called MIMO technology) instead of one.

When this standard was finalised, 802.11n connections could support data rates of over 100 Mbps. 802.11n also offers a little better range over earlier Wi-Fi standards owing to its increased signal intensity. 802.11n equipment would be backward compatible with 802.11g gear.

- **Pros of 802.11n :** Fastest maximum speed and best signal range; more resistant to signal interference from outside sources.
- **Cons of 802.11n :** Standard is not yet finalised; costs more than 802.11g; the use of multiple signals may greatly interfere with nearby 802.11 b/g based networks.

#### **☐ Check Your Progress – 5 :**

1. 802.11a transmits radio signals in the frequency range above \_\_\_\_\_ GHz.  
a. 5                      b. 2.4                      c. 2.7

### **2.7 Bluetooth :**

Apart from these four general-purpose Wi-Fi standards, several other related wireless network technologies exist.

Other IEEE 802.11 working group standards like 802.11h and 802.11j are extensions or offshoots of Wi-Fi technology that serve a very specific purpose.

Bluetooth is an alternative wireless network technology, which followed a different development path than the 802.11 family. Bluetooth supports a very short range (approximately 10 meters) and relatively low bandwidth (1–3 Mbps in practice) designed for low-power network devices like handhelds. The low manufacturing cost of Bluetooth hardware also appeals to industry vendors. You can readily find Bluetooth in the networking of PDAs or cell phones with PCs, but it is rarely used for general-purpose WLAN networking due to the range and speed considerations.

WiMax also was developed separately from Wi-Fi. WiMax is designed for long-range networking (spanning miles or kilometers). The following IEEE 802.11 standards exist or are under development to support creation of technologies concerning wireless local area networking:

- 802.11a – 54 Mbps standard, 5 GHz signaling (ratified 1999)
- 802.11b – 11 Mbps standard, 2.4 GHz signaling (1999)
- 802.11c – operation of bridge connections (moved to 802.1D)
- 802.11d – worldwide compliance with regulations for use of wireless signal spectrum (2001)
- 802.11e – Quality of Service (QoS) support (not yet ratified)
- 802.11F – Inter-Access point protocol recommendation for communication between access points to support roaming clients (2003)
- 802.11g – 54 Mbps standard, 2.4 GHz signaling (2003)



- 802.11h – enhanced version of 802.11a to support European regulatory requirements (2003)
- 802.11i – security improvements for the 802.11 family (2004)
- 802.11j – enhancements to 5 GHz signaling to support Japan regulatory requirements (2004)
- 802.11k – WLAN system management (in progress)
- 802.11l – skipped to avoid confusion with 802.11i
- 802.11m – maintenance of 802.11 family documentation
- 802.11n – 100+ Mbps standard improvements over 802.11g (in progress)
- 802.11o – skipped
- 802.11p – Wireless access for the vehicular environment
- 802.11q – skipped
- 802.11r – fast roaming support viabasic service set transitions
- 802.11s – ESS mesh networking for access points
- 802.11T – Wireless performance prediction – recommendation for testing standards and metrics
- 802.11u – internetworking with 3G / cellular and other forms of external networks
- 802.11v – wireless network management / device configuration
- 802.11w – Protected management frames security enhancement
- 802.11x – skipped (generic name for the 802.11 family)
- 802.11y – Contention based protocol for interference avoidance and local area wireless networking.

❑ **Check Your Progress – 6 :**

1. \_\_\_\_\_ is an alternative wireless network technology, which followed a different development path than the 802.11 family.
  - a. Bluetooth
  - b. Wifi
  - c. wimax

**2.8 5 GHz Wireless Network hardware better than 2.4 GHz :**

Wireless computer network equipment typically uses radio signals in either a 2.4 GHz range or a 5 GHz range. These numbers are advertised prominently on product packaging but their meaning is often misunderstood. Is 5 GHz network hardware better than 2.4 GHz hardware just because it carries a bigger number ?

**Answer :** No. 5 GHz hardware offers a few advantages over 2.4 GHz hardware but in practice, 2.4 GHz is usually the better choice for home and other wireless local networks.

**2.8.1 GHz and Network Speed :**

The GHz range of a wireless radio only partially relates to the speed of a wireless network. For example, 802.11a Wi-Fi hardware runs at 5 GHz but supports the same maximum data rate of 54 Mbps as standard 802.11g network that runs at 2.4 GHz. 5 GHz network can carry more data than 2.4 GHz network assuming that the electric power to the higher frequency radios is maintained at a higher level. However, some 802.11g network products match

and even exceed this potential speed advantage of 5 GHz 802.11a by utilising a pair of radios instead of one, increasing capacity up to 108 Mbps under the right conditions.

➤ **Advantage :**

Both GHz and network range

The higher is the frequency of a wireless signal, the shorter is its range. Thus, 2.4 GHz networks cover a substantially larger range than 5 GHz wireless networks. In particular, the higher frequency wireless signals of 5 GHz networks

Do not penetrate solid objects nearly as well as do 2.4 GHz signals, limiting their reach inside homes.

**2.8.2 GHz and Network Interference :**

You may notice your cordless phone, automatic garage door opener or other home appliances, which also advertises 2.4 GHz signals on its packaging. As this frequency range is commonly used in consumer products, it is more likely that 2.4 GHz home network will pick up interference from appliances than will a 5 GHz home network.

➤ **GHz and Cost :**

Some people mistakenly believe 5 GHz network technology is newer or somehow more innovative than 2.4 GHz. In fact, both types of signalling have existed for many years and are both proven technologies. 802.11g Wi-Fi products that run at 2.4 GHz tend to cost less than 802.11a Wi-Fi products not as 802.11g is obsolete or less capable but as 802.11g is much more popular and thus economical for manufacturers to support.

➤ **Advantage :**

2.4 GHz

5 GHz vs 2.4 GHz – The Bottom Line

5 GHz and 2.4 GHz are different wireless signalling frequencies; each of which have advantages for computer networking. Higher frequency networks are not necessarily superior to lower frequency ones, however. So-called dual band hardware combines the best of both types of hardware by integrating both types of radios into the product.

☐ **Check Your Progress – 7 :**

1. The \_\_\_\_\_ range of a wireless radio only partially relates to the speed of a wireless network.
  - a. GHz
  - b. MHz
  - c. Khz

**2.9 Let Us Sum Up :**

"Introduction to Networking", a topology defines the structure of a network and network standards define how it works. As early 1970s, it was apparent that networks were going to play a large role in future corporate environment. Many manufacturers saw computing, network trends as potential opportunities, and became increasingly active in network component development. These companies realised that for their products to work together, standards would be necessary to ensure compatibility. The task of producing the standards fell to an international body called the Institute of Electrical and Electronics Engineers (IEEE).

The IEEE developed a set of standards called the 802 project. These standards are still used today, although there have been many changes and additions along the way. By using the standards defined by the IEEE, manufacturers can be sure that their products will work with products from other companies that adhere to the standards. Some of the IEEE 802 standards define only certain technologies, whereas others, such as the 802.3 standard, define entire networking systems.

The following are some of the most important IEEE 802 standards :

**802.1, bridging and management** : Defines the systems for managing networks. 802.1 specifies technologies for making sure that the network is available to users and responding to requests. It defines internetwork communications standards between devices and includes specifications for routing and bridging.

**802.2, the LLC sub layer** : Defines specifications for the Logical Link Control (LLC) sub layer in the 802 standard series.

**802.3, CSMA/CD** : Defines the carrier-sense multiple-access with collision detection (CSMA/CD) media access method used in Ethernet networks. This is the most popular networking standard used today.

**802.4, a token passing bus (rarely used)** : Defines the use of a token-passing system on a linear bus topology.

**802.5, token ring networks** : Defines token ring networking, also known as token ring access.

**802.6, metropolitan area network (MAN)** : Defines a data transmission method called distributed queue dual bus (DQDB), which is designed to carry voice and data on a single link.

**802.7, Broadband Technical Advisory** : Defines the standards and specifications of broadband communications methods.

**802.8, Fibre-Optic Technical Advisory** : Provides assistance to other IEEE

802 committees on subjects related to the use of fibre optics.

**802.9, integrated voice and data networks** : Defines the advancement of integrated voice and data networks.

**802.10, network security** : Defines security standards that make it possible to safely and securely transmit and exchange data.

**802.11, wireless networks** : Defines standards for wireless LAN communication.

**802.12, 100 Base VG-Any LAN** : Defines standards for high-speed LAN technologies. This chapter primarily focuses on the 802.3 Ethernet standards and their characteristics, such as access methods (CSMA/CD), signalling type (baseband/broadband), their speeds and the distances they support.

So here a brief discussion was made on network structure. Some very important IEEE standards have also been discussed in the above content which will be of great help to the students of computers in understanding the concepts of computer.

**2.10 Answers for Check Your Progress :**

- ❑ **Check Your Progress 1 :**  
1 : a
- ❑ **Check Your Progress 2 :**  
1 : a
- ❑ **Check Your Progress 3 :**  
1 : a
- ❑ **Check Your Progress 4 :**  
1 : a
- ❑ **Check Your Progress 5 :**  
1 : a
- ❑ **Check Your Progress 6 :**  
1 : a
- ❑ **Check Your Progress 7 :**  
1 : a

**2.11 Glossary :**

1. **Bluetooth** – a short-range radio technology that allows wireless communication between a computer and a keyboard, between mobile phones, etc.
2. **Circuit Switching** – Communication via single dedicated path between the sender and receiver. The telephone system is an example of a circuit switched network.
3. **Emulator** – to imitate (a particular computer system) by using a software system, often including a micro program or another computer that enables it to do the same work, run the same programs, etc., as the first.
4. **NetBIOS** – An applications programming interface (API) which activates network operations on IBM PC compatibles running under Microsoft's DOS. It is a set of network commands that the application program issues in order to transmit and receive data to another host on the network. The commands are interpreted by a network control program or network operating system that is NetBIOS compatible.
5. **Modem** – (Modulator/demodulator) an electronic device for converting between serial data (typically EIA-232) from a computer and an audio signal suitable for transmission over a telephone line connected to another modem. In one scheme the audio signal is composed of silence (no data) or one of two frequencies representing zero and one.
6. **Network** – a system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables: used to transmit or receive information.

**2.12 Assignment :**

1. What are the components of LAN ?
2. What are the terms are there in Ethernet ?
3. Explain 802.11a and 802.11b

**2.13 Activities :**

Explain the pros and cons of IEEE Standards.

**2.14 Case Study :**

1. Draw the cables : Twisted pair and fibre optic cables ?
2. Write the functions and explain the pros and cons ?

**2.15 Further Readings :**

1. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001.
2. Sams Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002.

**UNIT STRUCTURE**

- 3.0 Learning Objectives
- 3.1 Introduction
- 3.2 OSI Reference Model
- 3.3 TCP/IP Model
- 3.4 Addressing in Network
- 3.5 IP Address
  - 3.5.1 IPV-4 Address
  - 3.5.2 IPV-6
- 3.6 MAC Address
- 3.7 IP Address Class
- 3.8 IP Headers
- 3.9 Static Addressing
- 3.10 Dynamic Addressing
- 3.11 Subnetting
- 3.12 Handshaking
- 3.13 Let's sum up
- 3.14 Answers for Check Your Progress
- 3.15 Glossary
- 3.16 Assignment
- 3.17 Activities
- 3.18 Case Study
- 3.19 Further Readings

**3.0 Learning Objectives :**

After learning this unit, you will be able to understand :

- Network Layers
- Addressing Technics.
- Classes of IP Addressing.
- IP Headers
- Subnetting.
- Handshaking

**3.1 Introduction :**

As we understood data communication or exchange of data in computer network is done through various protocols but this protocols are suite under different layers by their role and type of functionality which is provided by

protocol. It is also require unique identification of Sender and receiver machine in network so both sender and receiver can full fill accurate, correct ant timely delivery of data. For that it require IP addresses. IP address is given in some specific range and structure, it is also follow by Network to give unique IP address to each machine. In network Data is also passed in some specific Protocol Headers, this headers are design to bring exact size of data and also used for data security for verify data is receive with error or error free. In this section we will learn Network Layers and how it handle different protocols under this layers also we learn the header of protocol and how it will carry data under different parameters of header.

### **3.2 OSI Reference Model :**

Networking technologies are most often compartmentalized by dividing their functions into layers, each of which contains hardware and/or software elements. Each layer is responsible for performing a particular type of task, as well as interacting with the layers above it and below it. Layers are conceptually arranged into a vertical stack. Lower layers are charged with more concrete tasks such as hardware signalling and low-level communication; they provide services to the higher layers. The higher layers in turn use these services to implement more abstract functions such as implementing user applications.

Dividing networks into layers this way is somewhat like the division of labor in a manufacturing facility and yields similar benefits. Each hardware device or software program can be specialized to perform the function needed by that layer, like a well-trained specialist on an assembly line. The different modules can be combined in different ways as needed. Understanding how a network functions overall is also made much easier this way.

The OSI or Open System Interconnection model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.

#### ➤ **Application (Layer 7) :**

This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered and any constraints on data syntaxes are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

#### ➤ **Presentation (Layer 6) :**

This is a layer, usually part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). This layer also manages security issues by providing services such as data encryption and compression. It's sometimes called the syntax layer. This layer provides independence from differences in data representation(e.g. encryption) by translating from application to network format and vice versa. The presentation

layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

➤ **Session (Layer 5) :**

This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates and terminates conversations, exchanges and dialogues between the applications at each end. It deals with session and connection coordination.

This layer allows applications on different computers to establish, use, and end a session/connection. This layer establishes dialog control between the two computers in a session, regulating which side transmits, and when and how long it transmits.

➤ **Transport (Layer 4) :**

This layer handles error recognition and recovery, manages the end-to-end control (for example, determining whether all packets have arrived) and error-checking. It ensures complete data transfer. IT is also perform flow control between two parties.

➤ **Network (Layer 3) :**

This layer handles the routing of the data, addresses messages and translates logical addresses and names into physical addresses. It also determines the route from the source to the destination computer and manages traffic problems (flow control), such as switching, routing, and controlling the congestion of data packets.

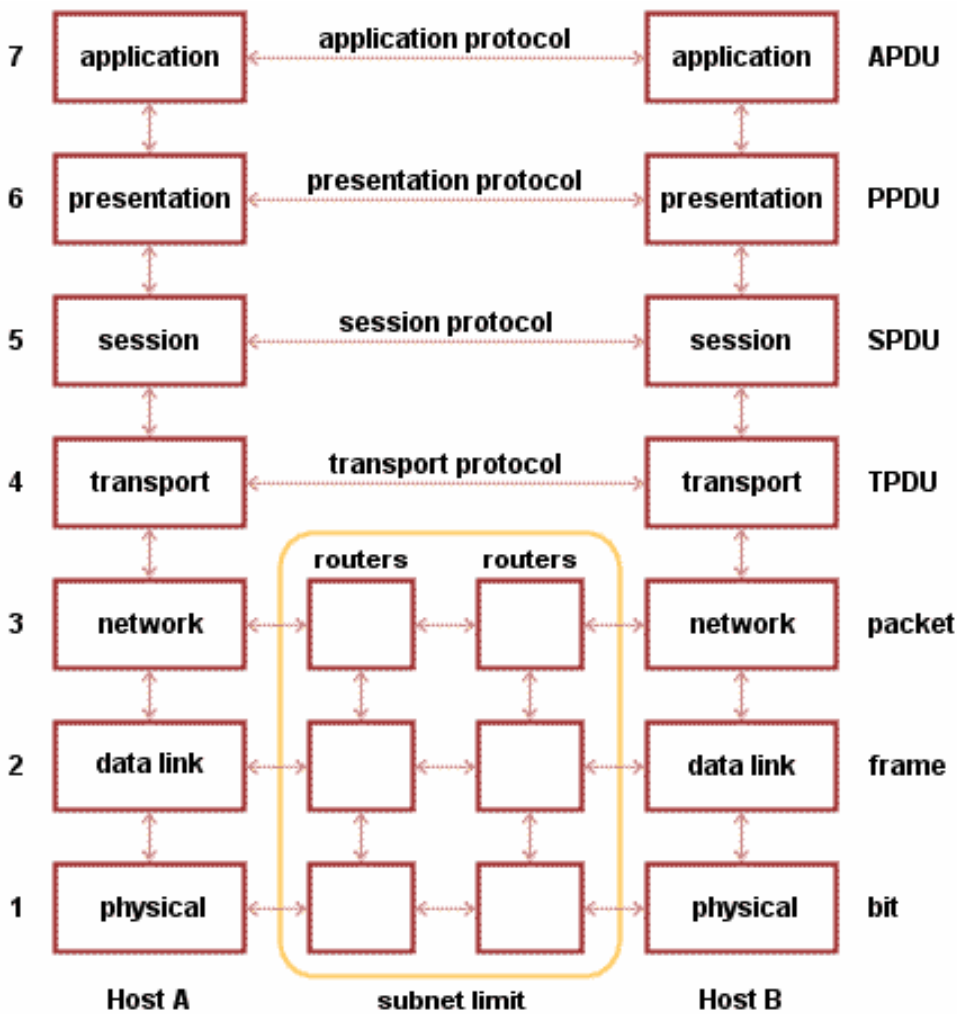
➤ **Data link (Layer 2) :**

This layer package raw bit from the Physical layer into frames (logical, structures packets for data). It is responsible for transferring frames from one computer to another, without errors. After sending a frame, it waits for an acknowledgment from the receiving computer. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer

➤ **Physical (Layer 1) :**

This layer transmits bits from one computer to another and regulates the transmission of a stream of bits over a physical medium. This layer defines how the cable is attached to the network adapter and what transmission technique is used to send data over the cable. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232 and ATM are protocols with physical layer components.





**□ Check Your Progress – 1 :**

1. \_\_\_\_\_ Layer in OSI is responsible for transmit bits from one mahchine to anathore.
  - a. Network
  - b. Physical
  - c. datalink

**3.3 TCP/IP Model :**

Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite is the engine for the Internet and networks worldwide. Its simplicity and power has led to its becoming the single network protocol of choice in the world today. TCP/IP is a set of protocols developed to allow cooperating computers to share resources across the network.

This model was initially developed & used by ARPANET (Advanced Research Project Agency Network). ARPAnet is the best- known TCP/IP network.

The most accurate name for the set of protocols is the "Internet protocol suite". TCP and IP are two of the protocols in this suite. The Internet is a collection of networks. Term "Internet" applies to this entire set of networks. Like most networking software, TCP/IP is modeled in layers.

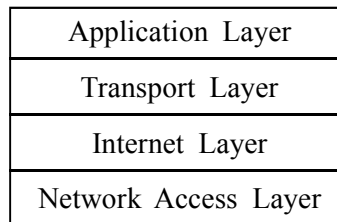
This layered representation leads to the term protocol stack, which refers to the stack of layers in the protocol suite. It can be used for positioning the TCP/IP protocol suite against others network software like Open System Interconnection (OSI) model. Layers communicate with those above and below via concise interfaces.

**Introduction to  
Computer Network**

TCP/IP is a family of protocols. A few provide "low-level" functions needed for many applications. These include IP, TCP, and UDP. Others are protocols for doing specific tasks, e.g. transferring files between computers, sending mail, or finding out who is logged in on another computer. Initially TCP/IP was used mostly between minicomputers or mainframes. These machines had their own disks, and generally were self-contained.

The layers are defined in TCP/IP Model.

1. Network Access Layer
2. Internet Layer
3. Transport Layer
4. Application Layer



1. **Network Access Layer** : A network layer is the lowest layer of the TCP/IP model. A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model. It defines how the data should be sent physically through the network. This layer is mainly responsible for the transmission of the data between two devices on the same network. The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses. The protocols used by this layer are Ethernet, token ring, FDDI, X.25, frame relay.
2. **Internet Layer** : An internet layer is the second layer of the TCP/IP model. An internet layer is also known as the network layer. The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination. The protocols used by this layer are **IP** (Internet Protocol), **ARP** (Address Resolution Protocol), **ICMP** (Internet Control Message Protocol) etc.
3. **Transport Layer** : The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network. The protocols used in the transport layer are **TCP** (Transmission control protocol) and **UDP** (User Datagram protocol User Datagram Protocol)
4. **Application Layer** : It is responsible for handling high-level protocols. This layer allows the user to interact with the application. When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer. The protocols used in this layer are HTTP/S, SMTP, DNS (Domain Name System), TELNET etc.

**☐ Check Your Progress – 2 :**

1. \_\_\_\_\_ layer is responsible for data flow control in TCP.  
a. Transport      b. Internet      c. Application

### **3.4 Addressing in Network :**

In computer network there are three different types of Addressing are used. One is Port Number, second is IP Address and MAC Address. This addresses are used to identify unique application is working on unique Computer. We will discuss all one by one for brief understanding. A network address always points to host / node / server or it can represent a whole network. Network address is always configured on network interface card and is generally mapped by system with the MAC address (hardware address) of the machine.

➤ **Port Number :**

Port number is assign by TCP and UDP. Both TCP and UDP Port numbers are assigning for different applications or Protocols which are running on internet. For example in computer we have open email application and File transfer application so computer will recognize both application by their own Port numbers. While Email application is sending or receiving mail it will define its own port number on internet so sender machine and receiver machine or server will identify the application type and identify the protocol under this application. Same while FTP application is sending request to the server at that time server machine will recognise the Port number and based on port number it will provide service.

A port number is a unique identifier used with an IP address. A port is a 16-bit unsigned integer, and the total number of ports available in the TCP/IP model is 65,535 ports. Therefore, the range of port numbers is 0 to 65535. In the case of TCP, the zero-port number is reserved and cannot be used, whereas, in UDP, the zero port is not available. IANA (Internet Assigned Numbers Authority) is a standard body that assigns the port numbers.

For example **192.168.1.20: 25**

In the above case, **192.168.1.20** is an IP address, and **25** is a port number.

To access a particular service, the port number is used with an IP address. The range from 0 to 1023 port numbers are reserved for the standard protocols, and the other port numbers are user-defined.

➤ **IP Address :**

Internet connects many networks and make possible to communicate among many people and computer or other devices. For getting connected with computer in individual network there must be require one unique identification. This unique identification is provided by IP (internet Protocol) address. Each computer has given two types of IP address to identify on internet. Static IP address and Dynamic IP address one of this IP address allotted by network to computer. There are two categories in IP address IPV4 and IPV6. We will later discuss in brief.

➤ **MAC Address :**

Both MAC Address and IP Address are used to uniquely identify a machine on the internet. MAC address is provided by the chip maker while IP Address is provided by the Internet Service Provider. MAC Address stands for Media Access Control Address. MAC Address ensure that physical address of the computer is unique. MAC Address is of six byte hexadecimal address. Total length of MAC Address is 48 byte. MAC Address are very from network to network also it is assign as a default gateway of your networks nearest Router. This address is access by Data link layer.

❑ **Check Your Progress – 3 :**

1. MAC address is assign by \_\_\_\_\_.
  - a. Manufacturer
  - b. Internet Service Provider
  - c. network administrator

**3.5 IP Address :**

IP addressing provides mechanism to differentiate between hosts and network. Because only IP addresses are assigned in hierarchical manner, a host always connect under a specific network. The host which needs to communicate outside its subnet, needs to know destination network address, where the packet/ data is to be sent. Network Addressing is one of the major responsibilities of the network layer. It also called as a Logical Address because this address is assign by Network software and it is define in two different way Static and Dynamic IP address. IP Address are Categories in two format IPV-4 and IPV-6 where IPV is consider as Internet Protocol Version.

**3.5.1 IPV-4 Address :**

When Internet Protocol is introduced there is only IPV4 address is design. IPV4 address length is 32 bit. The range of 32 bit IP address is between 0 to 255. IP address is known by "octet" which is of size 8 bit there are 4 octet in one IP address so length of IP address Is  $4 \times 8 = 32$  bits. IP address is valid IP address if and only if each octet of IP address must fullfil the range. Starting from 000.000.000.000 to 255.255.255.255 in between any range is allotted to computer.

For example 192.168.12.1 is a valid ip address because it fullfill the range of IP address each octet between 0-255 while 192.259.11.11 is invalid ip address because it do not fullfill the range of IP address one of octet is greater then 255. IPV4 address has capacity to provide 4.3 billion different IP addresses.

As the internet communication growing fast the ipv 4 address running out and new version has been introduce is IPV6.

**3.5.2 IPV-6 :**

In 1994 Internet Engineering Task Force (IETF) introduce IPV6. This address length is 128 bit. 128 bits are divide into eight blocks so each block contain 16 bits. Each 16 bit block is converted in to 4 bit Hexadecimal number separated by colon (:). As described in RFC 4291, the preferred form is x:x:x:x:x:x:x:x. Each x is a 16-bit section that can be represented using up to four hexadecimal digits, with the sections separated by colons. same like IPV-4 it is also between 0 to 255 or 0000 to FFFF range.

For example fe80:0db9:ac10:fe01:0000:0000:0000:0000 is a valid IPV-6 Address.

**3.6 MAC Addressing :**

The meaning of MAC is Media Access Control. Every node/ or device connected with LAN network is identify by MAC Address. For better understanding we assume one analogy IP address is like a city name and MAC address is like Person name. Suppose person is in Mumbai then we said he is in Mumbai. If person is in Delhi then we said he is in Delhi, means person travel in different city the location is change with city name, IP address is

change based on network in which network it is connected. But person name is not change means if he travels any city name remains same, MAC address will not change if it connects with different network it remains as it is. We can also say that MAC address and Physical address are same it is assign by Hardware Manufacturer. While NIC Card is design the MAC Address is assign to the NIC card which is installing as a Hardware part in our Computer. So it is considered as a Physical Address of Machine. Physical addressing/MAC addresses work on Layer 2. MAC Address is read by Switch. While IP Address is read by Router or gateway. Switch maintains Table of MAC Address so it can manage which sender or Receiver is sending and receiving correct data. Like IP Address MAC address is also unique which not repeated by any Hardware Manufacturer. MAC address is define in Hexadecimal value. MAC address is also 48 bit. IT is separated by hyphen (-), period (.) and colon (:). manufacture will decide which separator will used in mac address. For example 70-E4-20-ED-FC-A1 is a mac Address.

### **3.7 IP Address Class :**

As we Know IP address is numerical label which is assign by network while device is connected with network. Through that IP address devices are communicate in Internet. IP address act as an identifier for a specific machine on a particular network. Ip address is device in major 3 part Class Type, net id and host id. Each IP address is classify by its Class. Different class are design as per needs of different organizations. Classes are derive in A,B,C,D and E each has different range.

**Class A** IP address is lowest range of Address. It has 1 byte for netid and rest of 3 bytes are host id. In Class A, an IP address is assigned to those networks that contain a large number of hosts. The range of Class A address is 0 to 126 . In Class A, the first bit in higher order bits of the first octet is always set to 0 and the remaining 7 bits determine the network ID. The 24 bits determine the host ID in any network. The total number of networks in Class A =  $2^7 = 128$  network address and the total number of hosts in Class A =  $2^{24} - 2 = 16,777,214$  host address. An example of a Class A address is 102.138.122.226. Here, "102" helps you identify the network and 138.122.226 identifies the host.

IP address 127.0.0.0 to 127.255.255.255 is not assign for Class A and Class B because this address is assign for loopback address. Which is used for internal testing on the local machine.

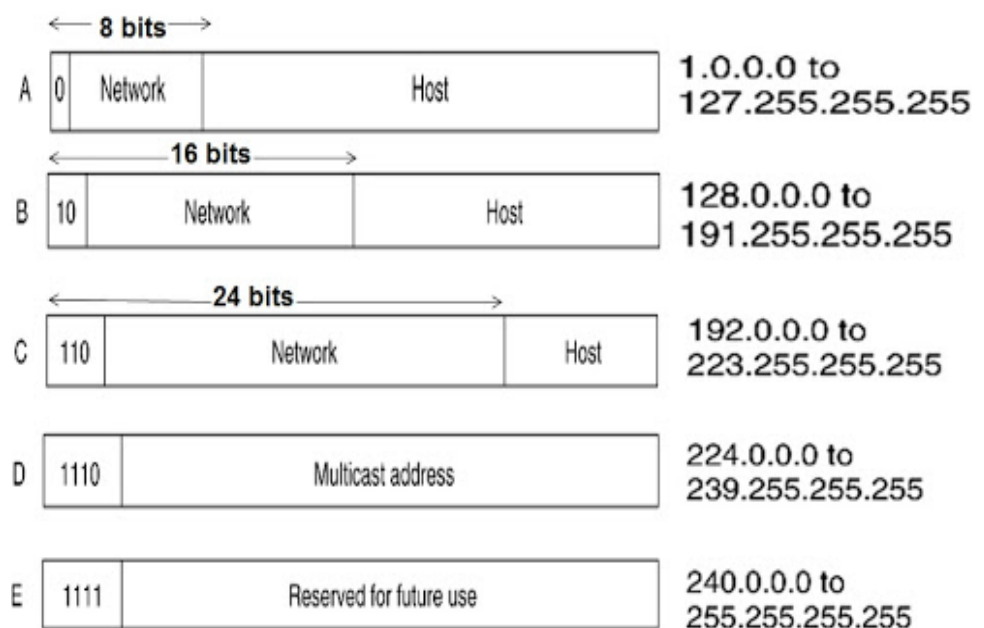
**Class B** IP address is assigned to those networks that range from small-sized to large-sized networks. Class B address has equal bytes of netid and hostid, 2 bytes for netid and 2 bytes of Host id. Range of Class B is 128 to 191. n Class B, the higher order bits of the first octet is always set to 10, and the remaining 14 bits determine the network ID. The other 16 bits determine the Host ID. The total number of networks in Class B =  $2^{14} = 16384$  network address. The total number of hosts in Class B =  $2^{16} - 2 = 65534$  host address. An example of Class B IP address is 168.212.226.204, where "168.212" identifies the network and "226.204" helps you identify the host.

**Class C** IP address is assigned to only small-sized networks. Class C address 3 bytes are used for netid and 1 byte is used for host id. Range of Class C address is 192 to 223. In Class C, the higher order bits of the first octet are always set to 110, and the remaining 21 bits determine the network

ID. The 8 bits of the host ID determine the host in a network. The total number of networks =  $2^{21} = 2097152$  network address The total number of hosts =  $2^8 - 2 = 254$  host address. An example of a Class C IP address: 192.168.178.101 where "192.168.178" is identify as net id and "101" is identify as host id.

**Class D** IP address is assign for Multicast address. This Address is allow to transfer data in group of host rather than to an individual host. Class D is never used for regular networking operations. It does not hold subnetting. Range of Class D address is 224 to 239. The higher order bits of the first octet are always set to 1110, and the remaining bits determine the host ID in any network. Example for a Class D IP address is 227.21.6.173.

**Class E** IP address Reserved for future use. These addresses are not used currently for any purpose in especially case it is used for the research and development purposes. Range of Class E address is 240 to 255. It does not possess any subnetting. The higher order bits of the first octet is always set to 1111, and the remaining bits determines the host ID in any network.



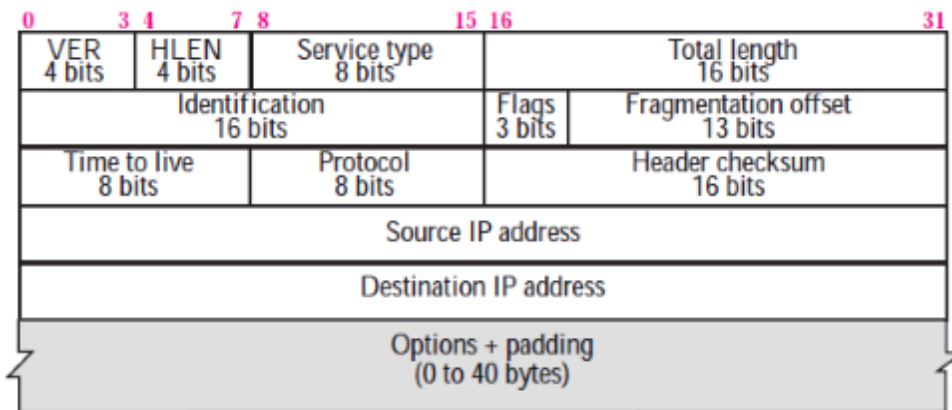
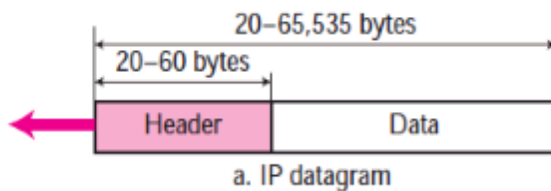
☐ **Check Your Progress – 4 :**

1. Range of Class B Address is \_\_\_\_\_.  
a 192 to 223    b 224 to 239    c. 128 to 191

**3.8 IP Headers :**

When you send data from sender to receiver there is addition layer is added it is IP Header. An **IP header** is a prefix to an IP packet that contains information about the IP version, length of the packet, source and destination IP addresses, etc. Basically this IP Header is added for accurate and correct delivery of Data on internet. It is also called as IP datagram. IT provide connection less service also helpful to identify Errors or something goes wrong in network it will fire relevant message to the host machine. The IP Header overall length is 32 bits it is a 4 group of 8 bits. We will discuss how all the Header fields are helpful in communication and how many bits they require to store information of hole data gram.

You will see the exact configuration of the IP headers in the IP headers image.



In above figure there is 32 bits IP header. There are different parts which contain size of data.

**Version :** This field is the first field (only 4 bits or one nibble wide). It contains the version number of the IP datagram: 4 for IPv4 and 6 for IPv6.

**HLEN :** this field is only 4 bits. used length of the header in 32-bit words. The minimum value is 20 bytes, and the maximum value is 60 bytes.

**Service Type :** This field is 8 bit where first 6 bits are used for Differentiated services field and 2 bits are for ECN Explicit Congestion Notification. It specifies how the datagram should be handled. IT is managing Quality of Service on IP Network. ECN provide end-to-end notification of network congestion without dropping packets.

**Total Length :** this field is 16 bits which is define total length of IP Datagram in bytes. Using this field and the IHL field can indicate where the data portion of the datagram starts, and its length. IT contains Length of Header and Data. As we know HLEN field has maximum 60 bytes so rest of bytes are actual Data size of your Data gram. We can find length of data by following question Length of data = total length – header length.

**Identification :** if the IP packet is fragmented then each fragmented packet will use the same 16 bit identification number to identify to which IP packet they belong to.IT is used for Packet tracking which packet is routing in network.

**Flag :** It is 3 bit field which is used to identify fragmentation. The first bit is always 0 and it is reserved. Second bit is for Don't Fragment bit. It is indicating doesn't fragment this Packet. If DF is set and Fragment is require in packet then packet will destroy from network. Third bit is for More Fragment, it is set while Packet require fragmentation for routing.

**Fragment Offset :** It is 13 bit field specify offset of a particular fragment relative to the beginning of the original unfragmented IP datagram. Used for fragmentation and reassembly if the packet is too large to put in a frame.

**TTL Time to Leave :** IT is 8 bit field. It is tells us how long packet may live in network. Packet is routing from one network to another at that time packet passes from many routers the time to live field value is decremented

by 1 while it pass from router. if the TTL reaches zero, the whole packet must be destroyed and discarded. ICMP message is generated Time Exceeded. This field is for safety purpose so that packet is not goes in uncontrollable loop at time of routing.

**Protocol :** This 8 bit field tells us which protocol is encapsulated in the IP packet, for example TCP has value 6 and UDP has value 17.

**Header Checksum :** This 16 bit field is used Error checking of the datagram. Whil packet reach at router it will calculate checksum for verify packet. If value of check sum is not match then it will discard the packet send Error message. Both TCP and UDP have checksum verifilaction.

**Source IP address :** This 32 bit field store the IP address of the host that sent the packet.

**Destination IP address :** This 32 bit field store the IP address of the host that should receive the packet.

**Options :** This 32 bit field is use for storing some optional settings within the datagram. used for network testing, debugging, security, and more. This field is not often used.

❑ **Check Your Progress – 5 :**

1. in TCP header \_\_\_\_\_ field is used to notify that how much packet will alive in network.
  - a. Checksum
  - b. TTL
  - c. Identification

**3.9 Static Addressing :**

Static IP Address is assign by Internet Service provider or Network Administrative. This address assign manually, person who provide static address has to allocate unique IP address to each device take care of duplication of IP address. Static IP addresses are fixed by network it will not change, once you allocate to the machine it will fixed until the device is decommissioned or your network architecture changes. Static IP addresses generally are used by servers or other important equipment. A static IP address may be IPv4 or IPv6. Static IP Address is less secured, device which use static IP address can easily track.

**3.10 Dynamic Addressing :**

Dynamic IP Address is not assigning By Internet Service Provider but it configure with host using DHCP (Dynamic Host Configuration Protocol). DHCP Automatic allocate IP Address to the host while it connect to the network. Dynamic IP address can be changed any time. Means if host is connecting with same network the dynamic IP address is different than previous one. Server itself track which IP address is used and which is free to allocate, all record is maintain by server. It is more secure then static address.IT easy to assign and mange by network. Device using dynamic IP address is more secure it is difficult to trace. Dynamic IP address is less stable than static IP address.

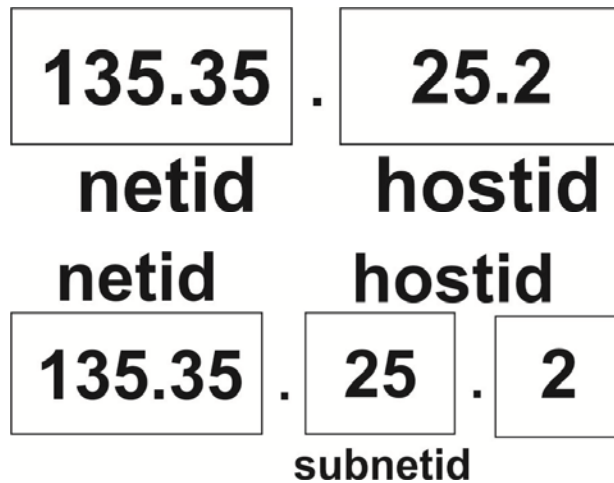
**3.11 Subnetting :**

As we know IP address is 32 bit long. It is a 4 bunch of b bits.in IP address there are two part netid and hosted. While you send any request to the machine or send any data to the other user, network will follow the hierarchy first it identify the netid and then it reach to the host with hostid. In some



case there is also possible in organization has more than one physical network. All are not organize in different group they all are at same level. Such kind of network is known as one network has many host.IT is difficult to manage each host so there is one solution to bifurcate each host in group it is known as subnetting. Network is divided in to sub network is called subnetting. This division is done through subnetid it is part of hostid in IP address third bunch of 8bit is known as subnetid.

For Example this is a class B address where two parts are define first 16 bits are netid and second 16 bits are hosted. In this address second part is define subnet id for creating sub network.



Here in above example if we want to create more number of subnet of network id 135.35 then we have to change the subnetid, then it will create up to limit of 255.255 sub network.

**□ Check Your Progress – 6 :**

1. \_\_\_\_\_ is indicate subnetwork of parent network.  
a. Subnetit      b. Subnet Mask   c. netid

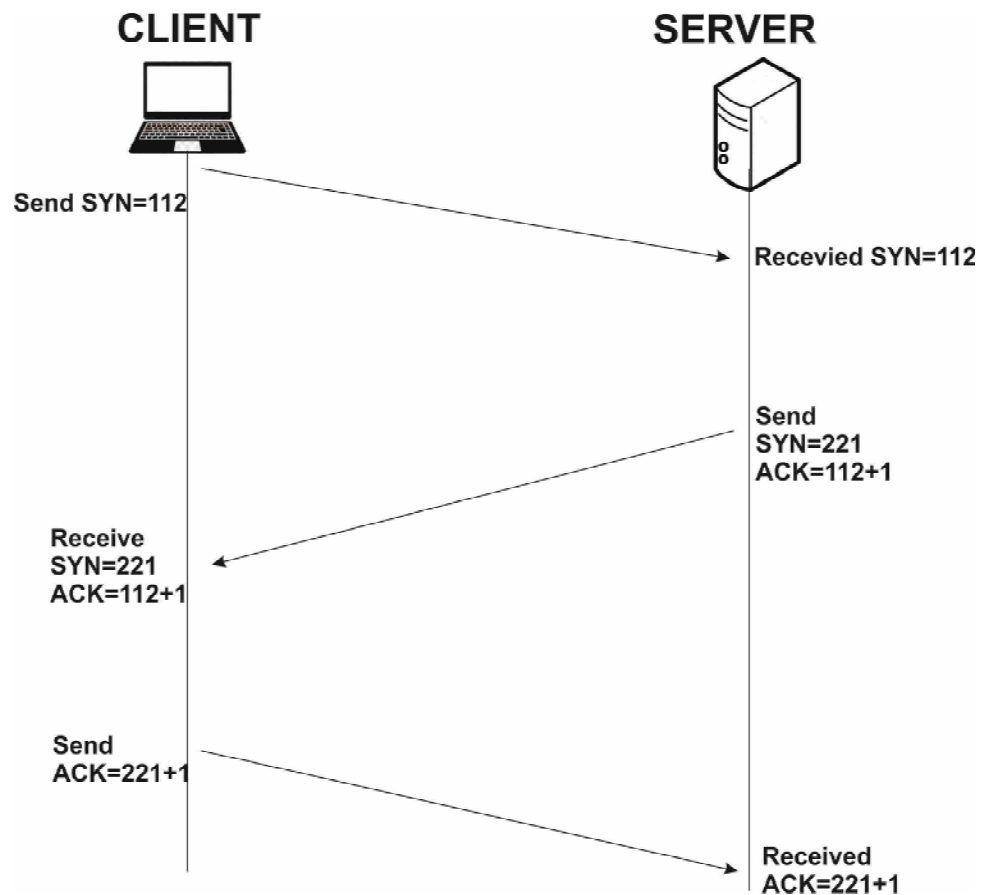
**3.12 Handshaking :**

Handshaking is Transport layer protocol procedure. In TCP handshaking means to establish the connection between client and server machine. It is take part in 3 steps it is also called as Tree Way Handshaking. IT is a process of Synchronisation and Acknowledgment of packets to establish a connection for real data transmission. This process is design to get connection at both sides using TCP socket.IT transfer multiple TCP socket at both side to establish connection. Following three steps are perform in Handshaking

**Step 1 :** In this step client send a request to the server machine to establish connection. It send a segment of (SYN) Synchronize Sequence Number to infer server that client want to establish connection. It defines the Sequence Number from which it start communication.

**Step 2 :** In this step Server will respond to the client with SYN –ACK (Acknowledgement) of requested SYN number. ACK is helpful to client that server has received segment of SYN and server is ready to establish connection.

**Step3 :** In this step client send ACK in response of server, and they both establish reliable connection. After ACK they will start actual data transfer.



### 3.13 Lets Sum Up :

In this unit, we have learned :

- OSI reference Model which is developed based on Application which will work on different Layers. It is 7 layer structures.
- TCP IP is a new structure of network communication it define different protocol first then suite each protocol according to their work. It is 4 layer structures.
- Addressing of Network which define different kinds of Addresses are available for communication also is used for correct and accurate delivery of packets in network.
- Internet Address a32-bit or 128-bit network-layer address used to uniquely define a host on an internet using the TCP/IP protocol.
- MAC address a 48 bit address which is assign to the NIC card at time of Manufacturing is not change in network configuration.
- Static address which is assign by Internet Service provider in Network it is fixed IP address. Dynamic IP address which is assign automatic by network using DHCP protocol which is not fixed in network it will change every time.
- TCP Header is used to transfer a packet in network with some specific format with some length of Packet.
- Subnetting a method to derive large parent network into subnetwork for load sharing.
- Handshaking is a technic to connect Client machine to server machine before transmission of actual data. It is used to confirm both the party are ready to transfer data in network.

**3.14 Answers for Check Your Progress :**

- Check Your Progress 1 :**  
1 : b
- Check Your Progress 2 :**  
1 : a
- Check Your Progress 3 :**  
1 : a
- Check Your Progress 4 :**  
1 : c
- Check Your Progress 5 :**  
1 : b
- Check Your Progress 6 :**  
1 : a

**3.15 Glossary :**

1. **Addressing** : a technic in network to identify network and host uniquely.
2. **Datagram** : is a TCP Header which is show the length of packet.IT is 20 to 60 byte long. It holds the information of Packet Routing and Delivery.
3. **Handshaking** : is a sequence of events to establish a connection between client and server or two party in network.
4. **IP Address** : is a logical Address provide by Network.
5. **MAC Address** : is a physical address provide by Manufacturer to the Machine Hardware or NIC Card.
6. **Subnet** : subnetwork of parent network.
7. **TTL** : Lifetime of Packet.

**3.16 Assignment :**

1. Explain OSI Reference Model In detail.
2. Explain TCP/IP Model in detail
3. Explain TCP Header.

**3.17 Activity :**

Explain Different types of Addressing with Diagram.

**3.18 Case Study :**

Draw IP Address Classes and Explain Range of Each Class Address.

**3.19 Further Readings :**

1. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001 Digital Networking.
2. TCP/IP Protocol Suite, Edition 4, Behrouz A. Forouzan.

**BLOCK SUMMARY :**

At last the gist of our detailed discussion is that networking has been discussed in very dept, right from its origin i.e the history of networking was explained in detail. Even the essentials of networking was discussed in. Here much emphasis was laid on explaining the foundation of networking i.e. the fundamentals of networking was explained in very detail to the studetns, not only this the various layers of networking and the various architecure was discussed in very detail. Along with this the various protocols, advantages and disadvantages of networking has been discussed in detail. Apart from this the last unit discussed the LAN components, ethernet and about 802.11 along with IEEE Standards 802.11

Through this block the readers will get a detailed overview of the topics under essentials and standards under networking.

## **BLOCK ASSIGNMENT :**

### ❖ **Short Questions :**

**Define the following terms :**

1. Protocol
2. Networking types
3. Layer
4. Architecture of networking
5. Future of networking
6. 802.7
7. 802. 10
8. 802.10
9. Basenet
10. Frame
11. Relay
12. IP Address
13. Static Address
14. Dynamic Address
15. Bandwidth of Signal
16. Amplitude of Signal

### ❖ **Long Questions :**

1. What do you mean by the term protocol ?
2. What is wireless networking ?
3. What are the advantages and disadvantages of networking ?
4. How is 802.11g different from 802.11e ?
5. Is 5 GHz Wireless Network Hardware better than 2.4 GHz ?
6. Explain LAN MAN and WAN in detail.
7. Explain Subnetting in detail.
8. Explain Handshaking process.

**Introduction to  
Computer Network**

❖ **Enrolment No. :**

1. How many hours did you need for studying the units ?

Unit No.	1	2	3
No. of Hrs.			

2. Please give your reactions to the following items based on your reading of the block :

Items	Excellent	Very Good	Good	Poor	Give specific example if any
Presentation Quality	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Language and Style	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Illustration used (Diagram, tables etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Conceptual Clarity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Check your progress Quest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Feed back to CYP Question	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____

3. Any other Comments

.....

.....

.....

.....

.....

.....

.....

.....



**BAOU**  
Education  
for All

Dr. Babasaheb Ambedkar  
Open University Ahmedabad

BCAR-301

# **INTRODUCTION TO** **COMPUTER NETWORK**

---

## **BLOCK 2 : LAN, WAN, TCP/IP AND NETWORK PROTOCOLS**

---

UNIT 4 LAN AND WAN – I

UNIT 5 LAN AND WAN – II

UNIT 6 TCP/IP

UNIT 7 TCP/IP PROTOCOLS – I

UNIT 8 TCP/IP PROTOCOLS – II

# ***LAN, WAN, TCP/IP AND NETWORK PROTOCOLS***

## **Block Introduction :**

In this block the whole content has been divided into four units. The first unit covers the topic LAN and WAN – I, whereas the second unit covers the topic LAN and WAN – II, under both first and second unit the whole content under LAN and WAN has been divided under two units and has been discussed in very detail. The succeeding units cover the details about TCP/IP. whereas the third unit covers the topic TCP/IP which has even been discussed in very detail. The fourth unit focuses on Network protocol related discussions.

This block provides details about the most common types of area networks. The TCP/IP standard protocols which used for communication are also discussed.

It is possible to read this block of the book like any other book (from beginning to end). Each chapter begins with an introduction about the block and further discussion of the contents it contains. As you get further into a chapter you will learn more about LAN, WAN and TCP/IP their role and capabilities, but often you will be able to head directly to the topic you wish to learn about.

## **Block Objectives :**

**After learning this block, you will be able to understand :**

- The various LAN protocols and LAN topologies
- Structure and protocol of WAN
- Installation and components of WAN
- TCP/IP Protocols
- The TCP/IP Protocol Operations
- SPP over IP over GPRS and IP address

## **Block Structure :**

**Unit 4 : LAN and WAN – I**

**Unit 5 : LAN and WAN – II**

**Unit 6 : TCP/IP**

**Unit 7 : TCP/IP Protocols – I**

**Unit 8 : TCP/IP Protocols – II**



**UNIT STRUCTURE**

- 4.0 Learning Objectives**
  - 4.1 Introduction**
  - 4.2 LAN Protocols**
    - 4.2.1 LAN**
    - 4.2.2 LAN Protocols and OSI Reference Model**
  - 4.3 LAN Media Access Methods**
    - 4.3.1 LAN Transmission Methods**
  - 4.4 LAN Topologies**
    - 4.4.1 LAN Devices**
  - 4.5 WAN Protocols**
    - 4.5.1 HDLC**
    - 4.5.2 PPP**
  - 4.6 Frame Relay**
    - 4.6.1 WAN**
    - 4.6.2 Protocol Structure**
    - 4.6.3 Wide Area Network and WAN Protocols**
    - 4.6.4 Point to Point Links**
  - 4.7 Circuit Switching**
    - 4.7.1 Packet Switching**
  - 4.8 WAN Virtual Circuits**
    - 4.8.1 WAN Dialup Services**
    - 4.8.2 WAN Devices**
    - 4.8.3 WAN Switch**
  - 4.9 Let Us Sum Up**
  - 4.10 Answers for Check Your Progress**
  - 4.11 Glossary**
  - 4.12 Assignment**
  - 4.13 Activities**
  - 4.14 Case Study**
  - 4.15 Further Readings**
-

**4.0 Learning Objectives :**

After leaning this unit, you will be able to understand :

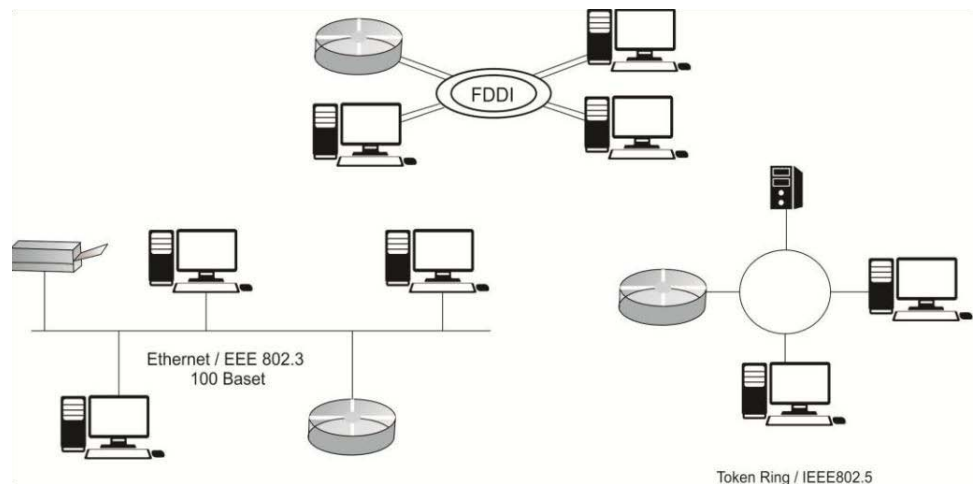
- Different LAN protocols
- Different methods used to deal with media contention
- Different LAN topologies
- LAN devices
- WAN protocol and its structure

**4.1 Introduction :**

Network types depend on how large they are and how much of an area they cover geographically. When it is discussed about a network types LAN and WAN are very familiar terms. LAN stands for local area network. A local area network is a group of devices such as computers, servers, switches, and printers which are located in the same building, such as in an office or in a home. In other words, in close proximity to each other. The most common type of LAN is an Ethernet LAN, where two or more computers are connected to Ethernet cables using a switch. The wide area network or WAN. A WAN is the largest type of network. A WAN includes multiple LANs, CANs, and MANs. It's a network that spans over a large geographical area such as a country continent or even the entire globe. A good example of a wide area network is the internet. Therefore, it is obvious that in order to function, all WANs use protocols. WANs connect LANs and other types of networks together, using protocols on a specific level. Network protocols such as TCP/IP deliver the transport and addressing portions of the link. However, protocols like Packet over SONET/SDH, MPLS, ATM and Frame relay can be used often by service providers to bring about the links used by WANs. An important early WAN was X.25 which is often considered to be the initial Frame Relay protocol. Many of its underlying protocols and functions are still used today in Frame Relay networks.

**4.2 LAN Protocols :**

The figure given below displays the implementation of basic layout of Ethernet/IEEE 802.3, Token Ring/IEEE 802.5 and Fiber Distributed Data Interface (FDDI).



**Fig. 4.1 : Three Most Commonly used LAN Implementations**

4.2.1 LAN :

A LAN is a high-speed data network that covers a relatively small geographic area. It typically connects workstations, personal computers, printers, servers and other devices. LANs offer computer users many advantages, including shared access to devices and applications, file exchange between connected user and communication between users' via electronic mail and other applications.

1.2.2 LAN Protocols and OSI Reference Model :

LAN protocols function at the lowest two layers of the OSI reference model between the physical layer and the data link layer. Figure 4.2 illustrates how several popular LAN protocols map to the OSI reference model.

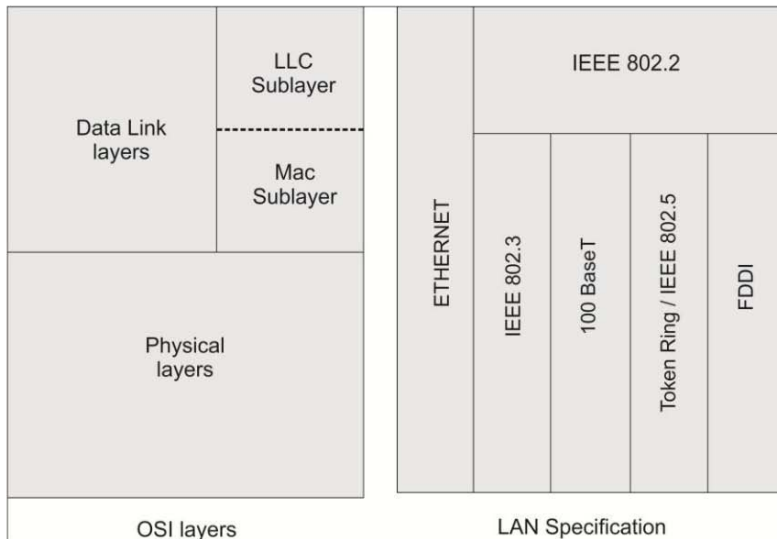


Fig. 4.2 : Popular LAN Protocols Mapped to the OSI Reference Model

□ Check Your Progress – 1 :

1. A \_\_\_\_\_ is a high-speed data network that covers a relatively small geographic area.
  - a. LAN
  - b. WAN
  - c. MAN
  - d. SAN

4.3 LAN Media Access Methods :

Media contention occurs when two or more network devices have data to send at the same time. Because multiple devices cannot talk on the network simultaneously, some type of methods must be used to allow access to one device to the network media time. This is done in two main ways: carrier sense multiple access collision detects (CSMA/CD) and token passing.

In networks using CSMA/CD technology such as Ethernet, network devices contend for the network media. When a device has data to send, it first listens to see if any other device is currently using the network. If not, it starts sending its data. After finishing its transmission, it listens again to see if a collision occurred.

A collision occurs when two devices send data simultaneously. When a collision happens, each device waits a random length of time before resending its data. In most cases, a collision between the two devices will not repeat. Because of this type of network contention, the busier a network becomes, the more collisions occur. This is why performance of Ethernet degrades rapidly as the number of devices on a single network increases.

In token-passing networks such as Token Ring and FDDI, a special network frame called a token is passed around the network from device to device. When a device has data to send, it must wait until it has the token and then sends its data. When the data transmission is complete, the token is released so that other devices may use the network media. The main advantage of token-passing networks is that they are deterministic.

In other words, it is easy to calculate the maximum time that will pass before a device has the opportunity to send data. This explains the popularity of token-passing networks in some real-time environments such as factories, where machinery must be capable of communicating at a determinable interval.

For CSMA/CD networks, switches segment the network into multiple collision domains. This reduces the number of devices per network segment that must contend for the media. By creating smaller collision domains, the performance of a network can be increased significantly without requiring addressing changes.

Normally CSMA/CD networks are half-duplex, meaning that while a device sends information, it cannot receive any at that time. While that device is talking, it is incapable of also listening for other traffic. This is much like a walkie-talkie. When one person wants to talk, he presses the transmit button and begins speaking. While he is talking, no one else on the same frequency can talk. When the sending person finishes talking, he releases the transmit button and the frequency is available to others.

When switches are introduced, full-duplex operation is possible. Full-duplex works much like a telephone— you can listen as well as talk at the same time. When a network device is attached directly to the port of a network switch, the two devices may be capable of operating in full-duplex mode. In full-duplex mode, performance can be increased, but not greatly. A 100-Mbps Ethernet segment is capable of transmitting 200 Mbps of data, but only 100 Mbps can travel in one direction at a time. Because most data connections are asymmetric (with more data travelling in one direction than the other), the gain is not as great as sometimes claimed.

However, full-duplex operation does increase the throughput of most applications because the network media is no longer shared. Two devices on a full-duplex connection can send data as soon as it is ready.

Token-passing networks such as Token Ring can also benefit from network switches. In large networks, the delay between turns to transmit may be significant because the token is passed around the network.

### **4.3.1 LAN Transmission Methods :**

LAN data transmissions fall into three classifications: unicast, multicast and broadcast. In each type of transmission, a single packet is sent to one or more nodes.

In a unicast transmission, a single packet is sent from the source to a destination on a network. First, the source node addresses the packet by using the address of the destination node. The package is then sent onto the network and finally, the network passes the packet to its destination.

A multicast transmission consists of a single data packet that is copied and sent to a specific subset of nodes on the network. First, the source node addresses the packet by using a multicast address. The packet is then sent into

the network, which makes copies of the packet and sends a copy to each node that is part of the multicast address.

A broadcast transmission consists of a single data packet that is copied and sent to all nodes on the network. In these types of transmissions, the source node addresses the packet by using the broadcast address. The packet is then sent on to the network, which makes copies of the packet and sends a copy to every node on the network.

#### ❑ Check Your Progress – 2 :

1. A \_\_\_\_\_ occurs when two devices send data simultaneously.
  - a. Collision
  - b. Accident
  - c. LAN

### 4.4 LAN Topologies :

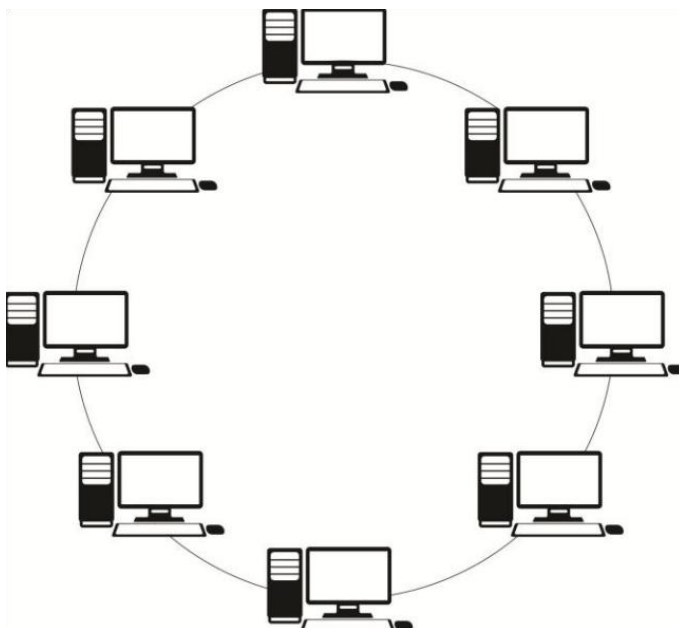
LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star and tree. These topologies are logical architectures, but the actual devices need not be physically organized in these configurations. Logical bus and ring topologies, for example, are commonly organized physically as a star.

A bus topology is a linear LAN architecture, in which transmissions from network stations propagate the length of the medium and are received by all other stations. Of the three most widely used LAN implementations, Ethernet/IEEE 802.3 networks– including 100BaseT– implement abus topology, which is illustrated in Figure 4.3



**Fig. 4.3 : Some Networks Implement a Local Bus Topology**

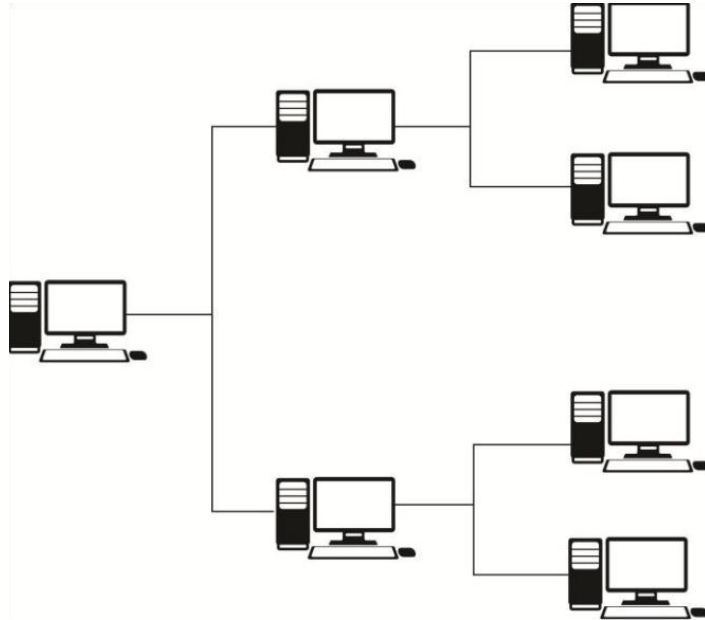
A ring topology is a LAN architecture that consists of a series of devices connected to one another by unidirectional transmission links to form a single closed loop. Both Token Ring/IEEE 802.5 and FDDI networks implement a ring topology. Figure 4.4 depicts a logical ring topology.



**Fig. 4.4 : Logical Ring Topology**

A star topology is a LAN architecture in which the endpoints on a network are connected to a common central hub or switch by dedicated links. Logical bus and ring topologies are often implemented physically in a star topology.

A tree topology is a LAN architecture that is identical to the bus topology, except that branches with multiple nodes are possible in this case. Figure 4.5 illustrates a logical tree topology.



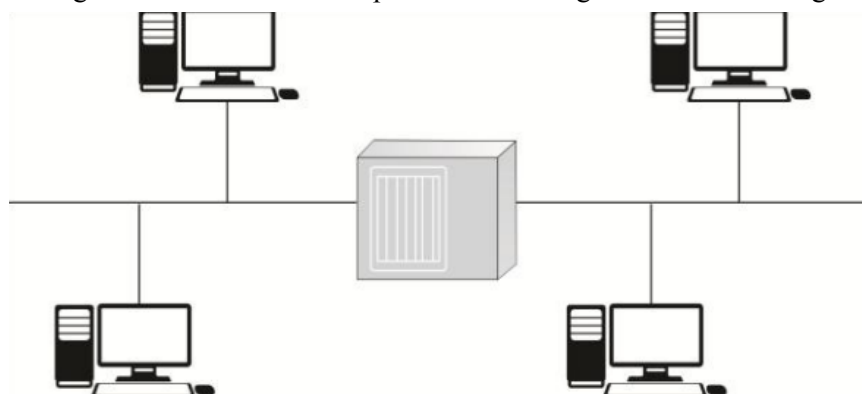
**Fig. 4.5 : A Logical Tree Topology Can Contain Multiple Nodes**

**4.4.1 LAN Devices :**

Devices commonly used in LANs include repeaters, hubs, LAN extenders, bridges, LAN switches and routers.

A repeater is a physical layer device used to interconnect the media segments of an extended network. A repeater essentially enables a series of cable segments to be treated as a single cable. Repeaters receive signals from one network segment and amplify, retime and retransmit those signals to another network segment. These actions prevent signal deterioration caused by long cable lengths and large numbers of connected devices.

Repeaters are incapable of performing complex filtering and other traffic processing. In addition, all electrical signals, including electrical disturbances and other errors, are repeated and amplified. The total number of repeaters and network segments that can be connected is limited due to timing and other issues. Figure 4.6 illustrates a repeater connecting two networks segments.

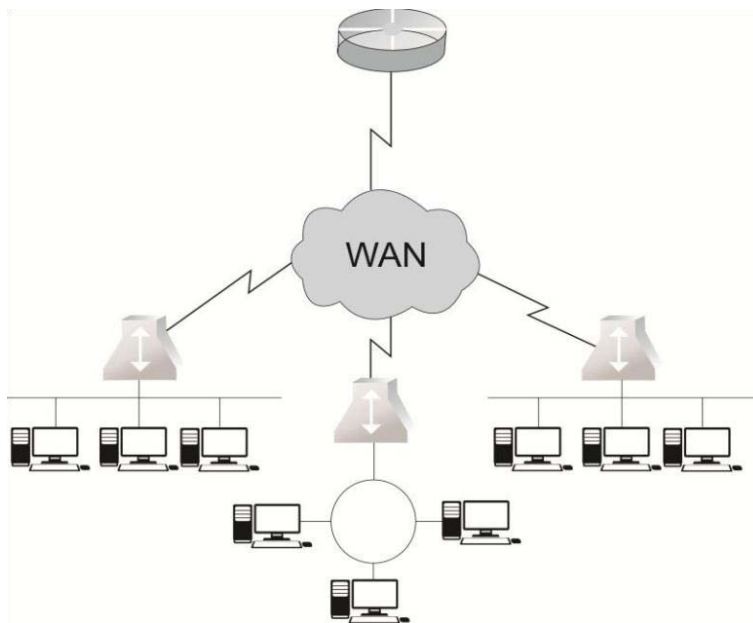


**Fig. 4.6 : A Repeater Connects Two Network Segments**

A hub is a physical layer device that connects multiple user stations, each via dedicated cable. Electrical interconnections are established inside the hub. Hubs are used to create a physical star network while maintaining the logical bus or ring configuration of the LAN. In some respects, a hub functions as a multiport repeater.

A LAN extender is a remote-access multilayer switch that connects to a host router. LAN extenders forward traffic from all the standard network layer protocols (such as IP, IPX and AppleTalk) and filter traffic based on the MAC address or network layer protocol type. LAN extenders scale well because the host router filters out unwanted broadcasts and multicasts.

However, LAN extenders are not capable of segmenting traffic or creating security firewalls. Figure 4.7 illustrates multiple LAN extenders connected to the host router through a WAN.



**Fig. 4.7 : Multiple LAN Extenders**

#### ❑ Check Your Progress – 2 :

1. LAN \_\_\_\_\_ define the manner in which network devices are organized.
  - a. Topologies      c. Design      b. Architecture      d. Method

### 4.5 WAN Protocols :

Mainly three types of WAN Protocols are used: HDLC, PPP or Frame-relay. Let us explore the differences and similarities of these protocols.

#### 4.5.1 HDLC :

HDLC stands for High-Level Data Link Control protocol. Like the two other WAN protocols mentioned in this article, HDLC is a Layer 2 protocol. HDLC is a simple protocol used to connect serial devices point-to-point. For example, you have point-to-point leased line connecting two locations, in two different cities.

HDLC would be the protocol with the least amount of configuration required to connect these two locations. HDLC would be running over the WAN, between the two locations. Each router would be de-encapsulating HDLC and turning it off on the LAN.

HDLC performs error correction, just like Ethernet. Cisco's version of HDLC is actually proprietary because they added a protocol type field. Thus, Cisco HDLC can only work with other Cisco devices. HDLC is actually the default protocol on all Cisco serial interfaces. If you do a show running-configuration on a Cisco router, your serial interfaces (by default) will not have any encapsulation. This is because they are configured to the default of HDLC. If you do a show interface serial 0/0, you will see that you are running HDLC. Here is an example:

#### **4.5.2 PPP :**

You may have heard of the Point to Point Protocol (PPP) because it is used for most every dial up connection to the Internet. PPP is documented in RFC 1661. PPP is based on HDLC and is very similar. Both work well to connect point-to-point leased lines.

The differences between PPP and HDLC are:

- PPP is not proprietary when used on a Cisco router.
- PPP has several sub-protocols that make it function.
- PPP is feature-rich with dial up networking features.

Because PPP has so many dial-up networking features, it has become the most popular dial up networking protocol in use today. Here are some of the dial-up networking features it offers:

- Link quality management monitors the quality of the dial-up link and the number of errors taken. It can bring the link down if the link is receiving too many errors.
- Multilink can bring up multiple PPP dialup links and bond them together to function as one.
- Authentication is supported with PAP and CHAP. These protocols take your username and password to ensure that you are allowed access to the network into which you are dialling.
- To change from HDLC to PPP, on a Cisco router, use the encapsulation ppp command.

#### **☐ Check Your Progress – 4 :**

1. PPP stands for \_\_\_\_\_.
  - a. Point to Point Protocol
  - b. Person to person protocol

#### **4.6 Frame-Relay :**

Frame Relay is a Layer 2 protocol and commonly known as a service from carriers. Frame relay creates a private network through a carrier's network. This is done with permanent virtual circuits (PVC). PVC is a connection from one site to another site through the carrier's network. This is really just a configuration entry that a carrier makes on their frame relay switches.

Obtaining a frame-relay circuit is done by ordering a T1 or fractional T1 from the carrier. On top of that, you order a frame-relay port, matching the size of the circuit you ordered. Finally, you order the PVC that connects your frame relay port to another of your ports inside the network.



**The benefits of frame-relay are :**

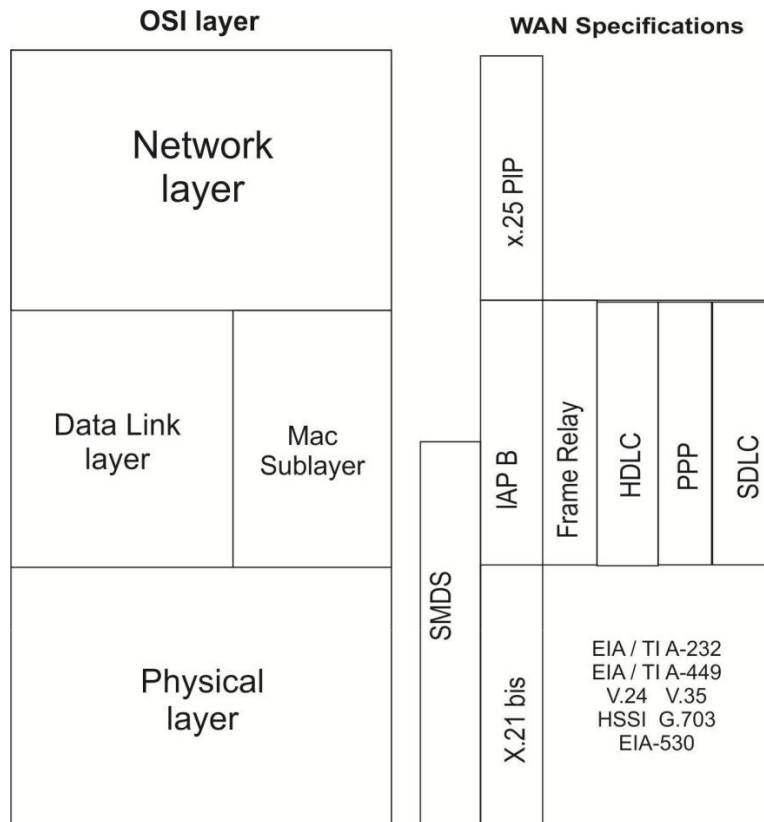
- It has the ability to have a single circuit that connects to the frame-relay cloud and gain access to all other sites (as long as you have PVCs). As the number of locations increases, you would save more and more money because you do not need as many circuits as you would if you were trying to fully-mesh your network with point-to-point leased lines.
- It offers improved disaster recovery because all you have to do is to order a single circuit to the cloud and PVC's to gain access to all remote sites.
- By using the PVCs, you can design your WAN whichever way you want. This means that, you define what sites have direct connections to other sites and you only pay the small monthly PVC fee for each connection.

**Some other terms concerning frame relay that you should know :**

- **LMI – Local Management Interface :** LMI is the management protocol of frame relay. LMI is sent between the frame relay switches and routers to communicate what DLCI's are available and if there is congestion in the network.
- **DLCI – Data Link Connection Identifier :** This is a number used to identify each PVC in the frame relay network.
- **CIR – Committed Information Rate :** This is the amount bandwidth you pay to guarantee which you receive, on each PVC. Generally, you have much less CIR than you have port speed.
- **DE – Discard Eligible :** Traffic marked DE (that was above your CIR) can be discarded by the frame-relay network if there is congestion.
- **FECN & BECN – Forward Explicit Congestion Notification and Backward Explicit Congestion Notification :** These are bits set inside LMI packets to alert the frame-relay devices that there is congestion in the network.

**4.6.1 WAN :**

A WAN is a data communications network that covers a relatively broad geographic area 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. Figure 4.8 illustrates the relationship between the common WAN technologies and the OSI model.



**Fig. 4.8 : WAN Technologies Operate at The Lowest Levels of the OSI Model**

**4.6.2 Protocol Structure :**

**The Key WAN Protocols are Listed as follows :**

<b>ATM</b>	ATM : Asynchronous Transfer Mode
	AAL : ATM Adaptation Layer
	AAL0 – AAL5 : ATM Adaptation Layer Type 0–5 reserved for variable bit rate video transfer
	LANE–NNI : LAN Emulation – Network to Network Interface
	LANE–UNI : LAN Emulation – User to Network Interface
	MPOA : Multi Protocol Over ATM
	PNNI : Private Network–to–Network Interface
	Q.2931 : Signalling for ATM
	UNI : User Network Interface
<b>SONET</b>	SONET: Synchronous Optical Network
	EoS : Ethernet over SONET/SDH
<b>Broadband Access</b>	DOCSIS : Data Over Cable Service Interface Specification
	ISDN : Integrated Services Digital Network
	Q.931 : ISDN network layer interface protocol

	LAPD : ISDN Link Access Protocol Channel D (Q.921)
	xDSL : Digital Subscriber Line Technologies (DSL, IDSL, ADSL, HDSL, SDSL, VDSL, G.Lite)
<b>Frame Relay</b>	Frame Relay : WAN protocol for internetworking at layer 2
	LAPF : Link Access Procedure/Protocol (ITU Q.922)
<b>PPP</b>	PPP : Point to Point Protocol
	BAP : PPP Bandwidth Allocation Protocol
	BACP : PPP Bandwidth Allocation Control Protocol
	BCP : PPP Bridging Control Protocol
	CHAP : Challenge Handshake Authentication Protocol
	EAP : PPP Extensible Authentication Protocol
	LCP : PPP Link Control Protocol
	MultiPPP : Multilink PPP (MP)
	PoS : Packet over SONET/SDH
	PPPoE : PPP over Ethernet
	PPPoA : PPP over ATM AAL5
<b>X.25</b>	HDLC : High Level Data Link Control protocol
	LAPB : Link Access Procedure Balanced for x.25
	X.25 : ITU-T WAN communication protocol
	X.75 : Signalling system used to connect packet switched networks (X.25).
	SDLC : Synchronous Data Link Control protocol

#### 4.6.3 Wide Area Network and WAN Protocols :

A wide area network (WAN) is a computer network covering multiple distance areas, which may spread across the entire world. WANs often connect multiple smaller networks, such as local area networks (LANs) or metro area networks (MANs). World's most popular WAN is the Internet. Some segments of the internet are also WANs in themselves. A wide area network may be privately owned or rented from service providers, but the term usually connotes the inclusion of public (shared user) networks.

- A virtual private network (VPN) riding on the public switched data network (PSDN) is often used by organizations for their private and secured communications. VPN uses encryption and other techniques to make it appear that the organisation has a dedicated network while making use of the shared infrastructure of the WAN.
- WANs generally utilize different networking technologies and equipment than LANs. Key technologies often found in WANs include SONET, Frame Relay, X.25, ATM and PPP.

- WAN technologies and protocols are mostly data link layer (layer 2) protocols, which are defined by many organizations over time. The key organizations in this space are IETF for PPP, ITU-T for ATM, Frame Relay, ISO for X.25 and SONET etc.

#### **4.6.4 Point-To-Point Links :**

A point-to-point link provides a single, pre-established WAN communications path from the customer premises through a carrier network such as a telephone company to a remote network. Point-to-point lines are usually leased from a carrier and thus are often called leased lines. For a point-to-point line, the carrier allocates pairs of wire and facility hardware to your line only.

These circuits are generally priced based on bandwidth required and distance between the two connected points.

Point-to-point links are generally more expensive than shared services such as Frame Relay. Figure 3-9 illustrates a typical point-to-point link through a WAN.



**Fig. 4.9 : A Typical Point-to-Point Link Operates through a WAN to a Remote Network**

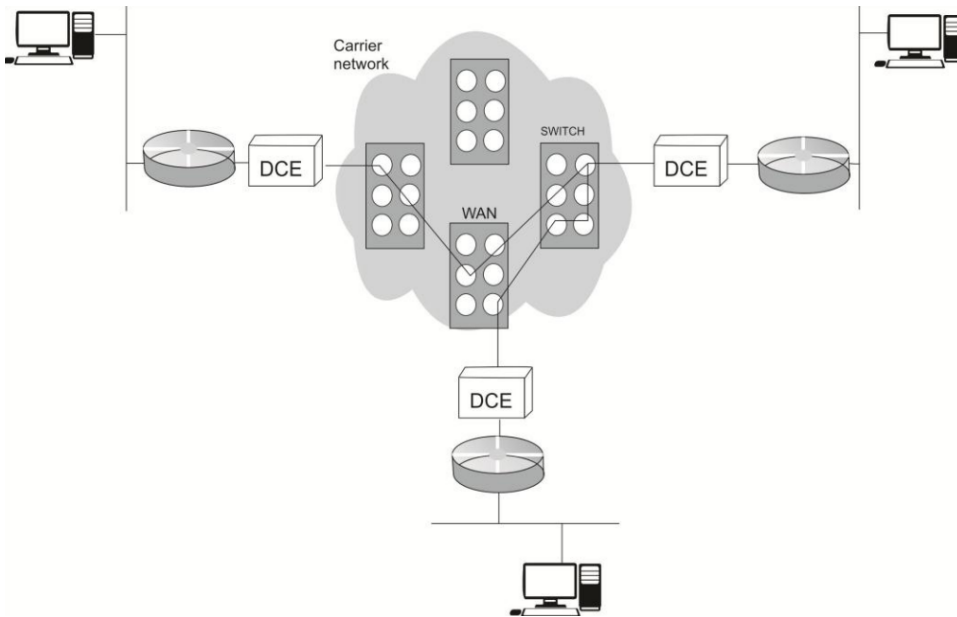
#### **❑ Check Your Progress – 5 :**

1. \_\_\_\_\_ is a connection from one site to another site through the carrier's network.  
a. PVC                      b. LAN                      c. WAN

#### **4.7 Circuit Switching :**

Switched circuits allow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication. Integrated Services Digital Network (ISDN) is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network. In the case of ISDN circuits, the device actually places a call to the telephone number of the remote ISDN circuit.

When the two networks are connected and authenticated, they can transfer data. When the data transmission is complete, the call can be terminated. Figure 4.10 illustrates an example of this type of circuit.



**Fig. 4.10 : A Circuit-Switched WAN Undergoes a Process Dimilar to that used for a Telephone Call**

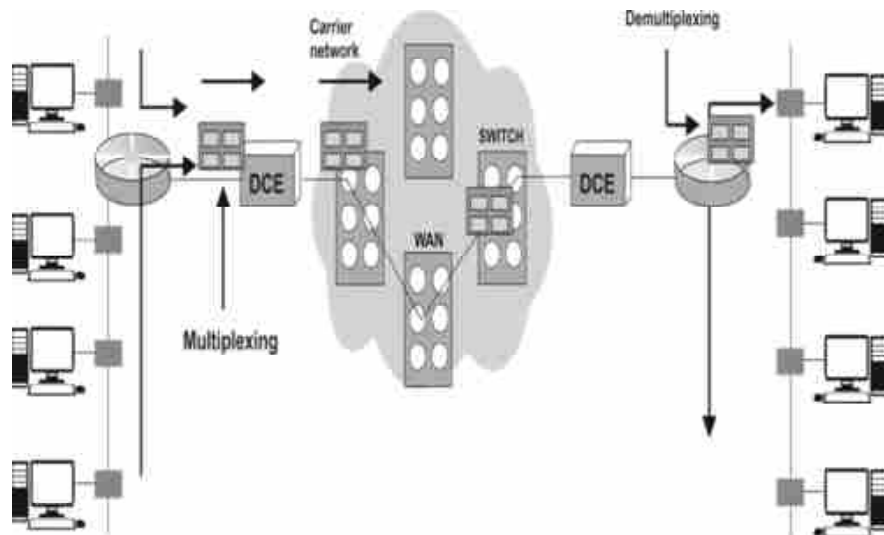
**4.7.1 Packet Switching :**

Packet switching is a WAN technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much better than with point-to-point lines. In a packet switching setup, networks have connections into the carrier's network and many customers share the carrier's network.

The carrier can then create virtual circuits between customers' sites by which packets of data are delivered from one to the other through the network. The section of the carrier's network that is shared is often referred to as a cloud.

Some examples of packet-switching networks include Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Services (SMDS) and X.25. Figure 4.11 shows an example of packet-switched circuit.

The virtual connections between customer sites are often referred to as a virtual circuit.



**Fig. 4.11 : Packet Switching Transfers Packets Across a Carrier Network**

❑ **Check Your Progress – 6 :**

1. \_\_\_\_\_ allow data connections that can be initiated when needed and terminated when communication is complete.
  - a. Switched circuits
  - b. LAN
  - c. WAN

**4.8 WAN Virtual Circuits :**

A virtual circuit is a logical circuit created within a shared network between two network devices. Two types of virtual circuits exist: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

SVCs are virtual circuits that are dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer and circuit termination. The establishment phase involves creating the virtual circuit between the source and destination devices.

Data transfer involves transmitting data between the devices over the virtual circuit and the circuit termination phase involves tearing down the virtual circuit between the source and destination devices. SVCs are used in situations in which data transmission between devices is sporadic, largely because SVCs increase bandwidth used due to the circuit establishment and termination phases, but they decrease the cost associated with constant virtual circuit availability.

PVC is a permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with the establishment and termination of virtual circuits, but they increase costs due to constant virtual circuit availability. PVCs are generally configured by the service provider when an order is placed for service.

**4.8.1 WAN Dialup Services :**

Dialup services offer cost-effective methods for connectivity across WANs. Two popular dialup implementations are dial-on-demand routing (DDR) and dial backup.

DDR is a technique whereby a router can dynamically initiate a call on a switched circuit when it needs to send data. In a DDR setup, the router is configured to initiate the call when certain criteria are met, such as a particular type of network traffic needing to be transmitted. When the connection is made, traffic passes over the line. The router configuration specifies an idle timer that tells the router to drop the connection if the circuit has remained idle for a certain period.

Dial backup is another way of configuring DDR. However, in dial backup, the switched circuit is used to provide backup service for another type of circuit, such as point-to-point or packet switching. The router is configured so that when a failure is detected on the primary circuit, the dial backup line is initiated. The dial backup line then supports the WAN connection until the primary circuit is restored. When this occurs, the dial backup connection is terminated.

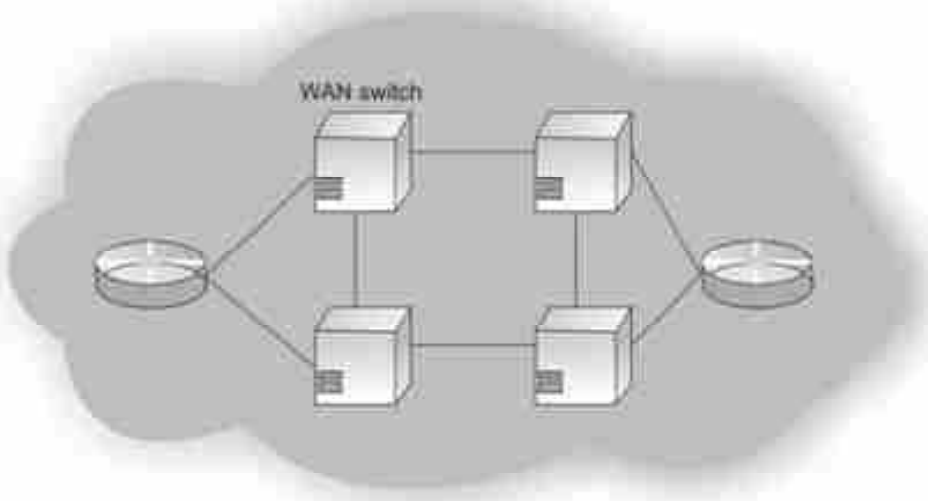
**4.8.2 WAN Devices :**

WANs use numerous types of devices that are specific to WAN environments. WAN switches, access servers, modems, CSU/DSUs and ISDN terminal adapters are discussed in the following sections. Other devices found

in WAN environments that are used in WAN implementations include routers, ATM switches and multiplexers.

#### 4.8.3 WAN Switch :

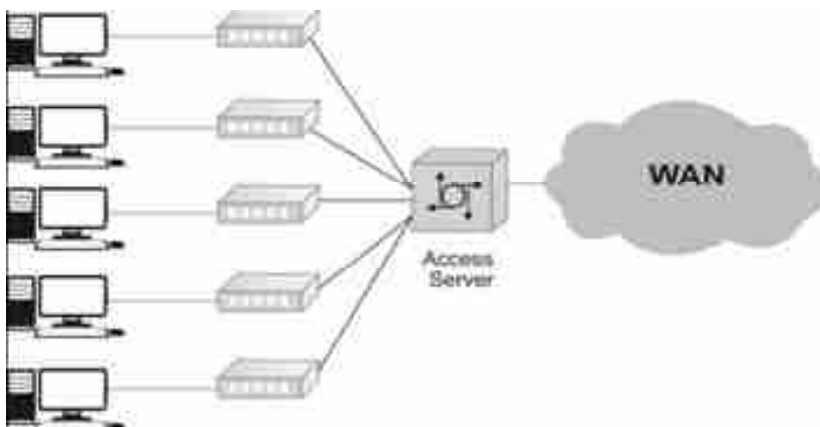
A WAN switch is a multiport internetworking device used in carrier networks. These devices typically switch such traffic as Frame Relay, X.25 and SMDS and operate at the data link layer of the OSI reference model. Figure 4.12 illustrates two routers at remote ends of a WAN that are connected by WAN switches.



**Fig. 4.12 : Two Routers at Remote Ends of a WAN can be Connected by WAN Switches**

#### Access Server :

An access server acts as a concentration point for dial-in and dial-out connections. Figure 4.13 illustrates an access server concentrating dial-out connections into a WAN.



**Fig. 4.13 : An Access Server Concentrates Dial-Out Connections Into a WAN**

#### Modem :

A modem is a device that interprets digital and analog signals, enabling data to be transmitted over voice-grade telephone lines. At the source, digital signals are converted to a form suitable for transmission over analog communication facilities. At the destination, these analog signals are returned

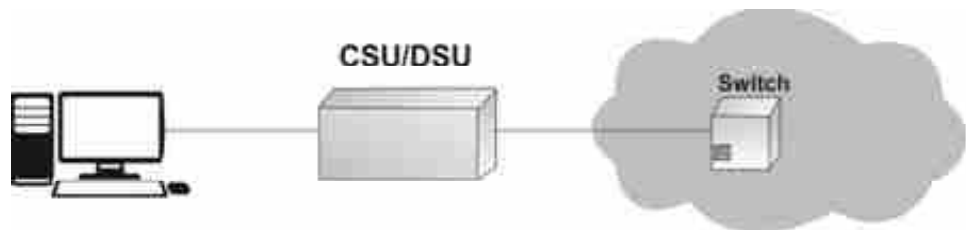
to their digital form. Figure 4.14 illustrates a simple modem-to-modem connection through a WAN.



**Fig. 4.14 : A Modem Connection through a WAN Handles Analog and Digital Signals**

**CSU/DSU :**

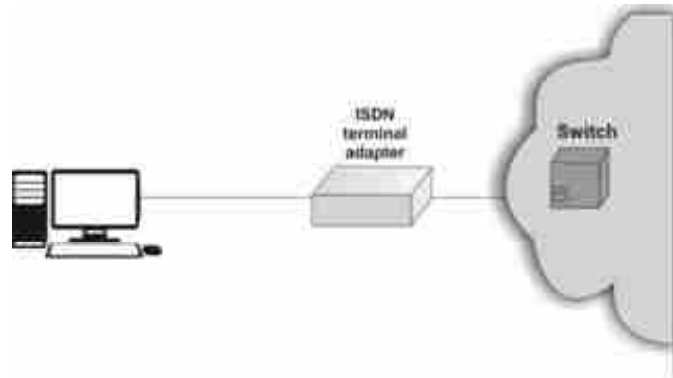
A channel service unit/digital service unit (CSU/DSU) is a digital-interface device used to connect a router to a digital circuit like a T1. The CSU/DSU also provides signal timing for communication between these devices. Figure 4.15 illustrates the placement of the CSU/DSU in a WAN implementation.



**Fig. 4.15 : The CSU/DSU Stands between the Switch and the Terminal ISDN Terminal Adapter :**

**ISDN Terminal Adapter :**

An ISDN terminal adapter is a device used to connect ISDN Basic Rate Interface (BRI) connections to other interfaces, such as EIA/TIA-232 on a router. A terminal adapter is essentially an ISDN modem; it is called a terminal adapter because it does not actually convert analog to digital signals. Figure 4.16 illustrates the placement of the terminal adapter in an ISDN environment.



**Fig. 4.16 : The Terminal Adapter Connects the ISDN Terminal Adapter to Other Interfaces**

**Check Your Progress – 7 :**

1. \_\_\_\_\_ services offer cost-effective methods for connectivity across WANs.
  - a. Dialup
  - b. ISDN
  - c. LAN

**4.9 Let Us Sum Up :**

**In this unit, we have learned :**

- A LAN is a high-speed data network that covers a relatively small geographic area which connects workstations, personal computers, printers, servers and other devices.



- LAN protocols function at the lowest two layers of the OSI reference model between the physical layer and the data link layer.
- LAN data transmissions fall into three classifications: unicast, multicast and broadcast. In each type of transmission, a single packet is sent to one or more nodes.
- LAN topologies define the manner in which network devices are organized. Four common LAN topologies exist: bus, ring, star and tree.
- Devices commonly used in LANs include repeaters, hubs, LAN extenders, bridges, LAN switches and routers.
- Mainly three types of WAN Protocols are used: HDLC, PPP or Frame-relay.
- Integrated Services Digital Network (ISDN) is a good example of circuit switching.
- In a packet switching setup, networks have connections into the carrier's network and many customers share the carrier's network.
- A virtual circuit is a logical circuit created within a shared network between two network devices. Two types of virtual circuits exist: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).
- SVCs are virtual circuits that are dynamically established on demand and terminated when transmission is complete.
- Communication over an SVC consists of three phases: circuit establishment, data transfer and circuit termination.
- WANs use numerous types of devices that are specific to WAN environments. WAN switches, access servers, modems, CSU/DSUs and ISDN terminal adapters are discussed in the following sections. Other devices found in WAN environments that are used in WAN implementations include routers, ATM switches and multiplexers.
- A WAN switch is a multiport internetworking device used in carrier networks. These devices typically switch such traffic as Frame Relay, X.25 and SMDS and operate at the data link layer of the OSI reference model.

So here a detailed discussion was done on the LAN and WAN

#### **4.10 Answers for Check Your Progress :**

- Check Your Progress 1 :**  
1 : a
- Check Your Progress 2 :**  
1 : a
- Check Your Progress 3 :**  
1 : a
- Check Your Progress 4 :**  
1 : a
- Check Your Progress 5 :**  
1 : a

❑ **Check Your Progress 6 :**

1 : a

❑ **Check Your Progress 7 :**

1 : a

**4.11 Glossary :**

1. **Circuit Switching :** Communication via a single dedicated path between the sender and receiver. The telephone system is an example of a circuit switched network.
2. **Emulator :** to imitate (a particular computer system) by using a software system, often including a microprogram or another computer that enables it to do the same work, run the same programs, etc., as the first.
3. **Network :** a system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables: used to transmit or receive information.
4. **Network Layer :** The third lowest layer in the OSI seven-layer model. The network layer determines routing of packets of data from sender to receiver via the data link layer and is used by the transport layer. The most common network layer protocol is IP.
5. **Repeater :** A network or communications device which propagates electrical signals from one cable to another, amplifying them to restore them to full strength in the process. Repeaters are used to counter the attenuation which occurs when signals travel long distances
6. **Router :** A device which forwards packets between networks. The forwarding decision is based on network layer information and routing tables, often constructed by routing protocols.
7. **Socket :** The Berkeley Unix mechanism for creating a virtual connection between processes. Sockets interface UNIX's standard I/O with its network communication facilities. They can be of two types, stream (bi-directional) or datagram (fixed length destination-addressed messages). The socket library function socket () creates a communications end-point or socket and returns a file descriptor with which to access that socket. The socket has associated with it a socket address, consisting of a port number and the local host's network address.

**4.12 Assignment :**

1. What are some types of WAN circuits ?
2. What is DDR and how is it different from dial backup ?
3. Describe the type of media access used by Ethernet.

**4.13 Activities :**

1. What is a CSU/DSU used for ?
2. What is the difference between a modem and an ISDN terminal adapter ?

**4.14 Case Study :**

Draw the LAN and WAN topology. Write your observations on the cable wires, how it is connected and significance of various colours of wires.

**4.15 Further Readings :**

1. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001
2. Sams Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002

**UNIT STRUCTURE**

- 5.0 Learning Objectives
- 5.1 Introduction
- 5.2 Origin and Evolution of Network Operating System
- 5.3 Functional Separation and Process Scheduling
- 5.4 Virtual Memory/Preemptive Scheduling Programming Model
- 5.5 WAN Interface Information
- 5.6 Let Us Sum Up
- 5.7 Answers for Check Your Progress
- 5.8 Glossary
- 5.9 Assignment
- 5.10 Activities
- 5.11 Case Study
- 5.12 Further Readings

**5.0 Learning Objectives :**

After learning this unit, you will be able to understand:

- Wide Area Network (WAN)
- Installation and components of WAN
- Digital phone service is and use of WANs in it
- Using the Internet to assemble WAN

**5.1 Introduction :**

Modern network devices can be described as complex entities comprising both– silicon and software. Thus, designing an efficient hardware platform is not by itself, sufficient to achieve an effective, cost–efficient and operationally tenable product. The control plane plays a vital role in the development of features and in ensuring device usability.

Even though progress from the development of quicker CPU boards and forwarding planes is visible, structural changes made in software are generally hidden. Though vendor collateral often offers a list of features in a carrier–class package, operational experiences might differ considerably.

Products, which have been through several generations of software releases, provide the finest instances of the difference made by the choice of OS. It is still usual to find routers or switches that started life under older, monolithic software and later migrated to designs that are more contemporary. The positive effect about stability and operational efficiency is simple to notice as well as appreciate.

However, migration from a network operating system to the other is likely to pose challenges from non-overlapping feature sets, non-contiguous operational experiences and inconsistent software quality. These potential challenges make it is very desirable to build a control plane that can power hardware products and features supported in both current and future markets.

Having developed a flexible, long-lasting and high-quality network the operating system makes provision for a foundation, which can gracefully evolve to support novel needs in its height for up as well as down scaling, width for adoption across many platforms and depth for rich integration of new features and functions. It takes time, significant investment and in-depth expertise.

Majority of the engineers writing the early releases of JUNOS Software came from the other companies where they had built network software before. They had first hand knowledge of what worked well and what could be improved. Such engineers found new-fangled ways to solve the limitations that they had experienced in having built the older operating systems. Resulting innovations in JUNOS are significant and rooted in its earliest design stages. Still, to ensure that our products anticipate and fulfil the next generation of market requirements, JUNOS is periodically re-evaluated to determine whether any changes are needed to ensure that it continues to provide the reliability, performance and resilience for which it is known.

## **5.2 Origin and Evolution of Network Operating System :**

Modern network operating systems are mostly advanced and specialised branches of POSIX-compliant software platforms and are rarely developed from scratch. The main reason behind this situation is the high cost of developing an excellent operating system all the way from concept to finished product. By adopting a general-purpose OS architecture, network vendors can focus on routing-specific code, decrease time to market and benefit from years of technology and research that went into the design of the original (donor) products.

### **First-Generation OS : Monolithic Architecture**

Typically, first-generation network operating systems for routers and switches were proprietary images running in a flat memory space, often directly from flash memory or ROM. While supporting multiple processes for protocols, packet handling and management, they operated using a co-operative, multitasking model wherein each process would run to completion or until it voluntarily relinquished the CPU.

All first-generation network operating systems shared one trait. They eliminated the risks of running full-size commercial operating systems on embedded hardware. Memory management, protection and context switching were either rudimentary or nonexistent, with the primary goals being a small footprint and speed of operation. Nevertheless, first-generation network operating systems made networking commercially viable. They were deployed on a wide range of products. The downside was that these systems were plagued with a host of problems associated with resource management and fault isolation; a single runaway process could easily consume the processor or cause the entire system to fail. Such failures were common in the data networks controlled by older software. They could be triggered by software errors, rogue traffic and operator errors.

Legacy platforms of the first generation are still seen in networks worldwide, although they are gradually being pushed into the lowest end of the telecom product lines.

### **Second-Generation OS : Control Plane Modularity**

The mid-1990s were marked by a significant increase in the use of data networks worldwide, which quickly challenged the capacity of existing networks and routers. By this time, it had become evident that embedded platforms could run full-size commercial operating systems, at least on high-end hardware, but with one catch. They could not sustain packet forwarding with satisfactory data rates. A breakthrough solution was needed. It came in the concept of a hard separation between the control and forwarding plane—an approach that became widely accepted after the success of the industry's first application-specific integrated circuit (ASIC)-driven routing platform, the Juniper Networks M40. Forwarding packets entirely in silicon was proven viable, clearing the path for next-generation network operating systems, led by Juniper with its JUNOS Software.

Today, the original M40 routers are mostly retired, but their legacy lives in many similar designs and their blueprints are widely recognized in the industry as the second-generation reference architecture.

Second-generation network operating systems are free from packet switching and thus are focused on control plane functions. Unlike its first-generation counterparts, a second-generation OS can fully use the potential of multitasking, multithreading, memory management and context manipulation, and all making system-wide failures less common. Most core and edge routers installed in the past few years are running second-generation operating systems and these systems are currently responsible for moving the bulk of traffic on the Internet and in corporate networks.

### **Third - Generation OS : Flexibility, Scalability and Continuous Operation**

Although second-generation designs were very successful, the past 10 years have brought novel challenges. Increased competition led to the need to lower operating expenses and a coherent case for network software flexible enough to be redeployed in network devices across the larger part of the end-to-end packet path. From multiple-terabit routers to Layer 2 switches and security appliances, the 'best-in-class' catchphrase can no longer justify a splintered operational experience—true 'network operating systems' are clearly needed. Such systems must also achieve continuous operation, so that software failures in the routing code, as well as system upgrades, do not affect the state of the network. Meeting this challenge requires availability and convergence characteristics that go far beyond the hardware redundancy available in second-generation routers.

Another key goal of third-generation operating systems is to run with zero downtime (planned and unplanned). Drawing on the lesson learned from previous designs regarding the difficulty of moving from one OS to another, third-generation operating systems also should make the migration path completely transparent to customers. They must offer an evolutionary, rather than revolutionary approach; upgrade experience typical to the retirement process of legacy software designs.

❑ **Check Your Progress – 1 :**

1. \_\_\_\_\_ eliminated the risks of running full-size commercial operating systems on embedded hardware.
  - a. first-generation network operating systems
  - b. second generation network operating systems

**5.3 Functional Separation and Process Scheduling :**

Multiprocessing, functional separation and scheduling are fundamental for almost any software design, including network software. As CPU and memory are shared resources, all running threads and processes have to access them in a serial and controlled fashion. Several design choices are available to achieve this goal, but the two most important ones are the memory model and the scheduling discipline. The next section briefly explains the intricate relation between memory, CPU cycles, system performance and stability.

**Memory Model**

The memory model defines whether processes (threads) run in a common memory space. If they do, the overhead for switching the threads is minimal and the code in different threads can share data via direct memory pointers. The downside is that a runaway process can cause damage in memory that does not belong to it.

In a more complex memory model, threads can run in their own virtual machines and the operating system switches the context every time the next thread needs to run. Due to this context switching, direct communication between threads is no longer possible and requires special interprocess communication (IPC) structures like pipes, files and shared memory pools.

**Scheduling Discipline**

Scheduling choices are primarily between cooperative and pre-emptive models, which define whether thread switching happens voluntarily. A cooperative multitasking model allows the thread to run to completion and a pre-emptive design ensures that every thread gets access to the CPU regardless of the state of the other threads.

❑ **Check Your Progress – 2 :**

1. The \_\_\_\_\_ defines whether processes (threads) run in a common memory space.
  - a. memory model
  - b. scheduling discipline

**5.4 Virtual Memory/Pre-emptive Scheduling Programming Model :**

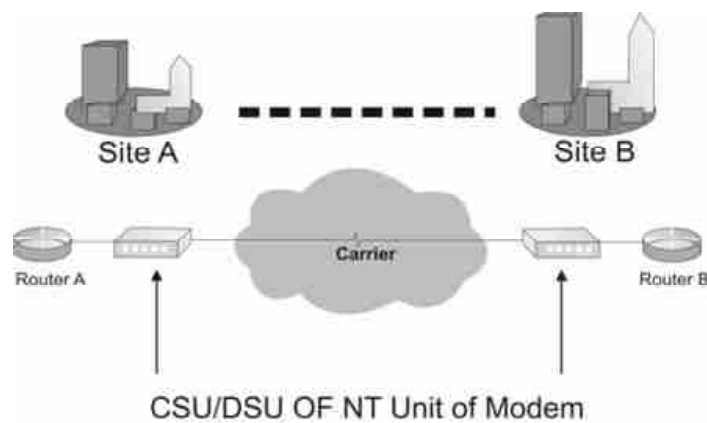
Virtual memory with pre-emptive scheduling is a great design choice for properly constructed functional blocks, where interaction between different modules is limited and well defined. This technique is one amongst the main benefits of the second-generation OS designs and under pins the stability and robustness of contemporary network operating systems. However, it has its own drawbacks. Not with standing the overhead associated with context switching, consider the interaction between two threads, A and B, both relying on the common resource R. As threads do not detect their relative scheduling in the pre-emptive model, they can actually access R in a different order and with differing intensity. For instance, R can be accessed by A, then B, then A, then

A and then B again. If thread B modifies resource R, thread A may get different results at different times—and without any predictability.

A modern O/S contains much built-in software designed to simplify networking of a computer. Typical O/S software is inclusive of an implementation of TCP/IP protocol stack and related utility programs like ping and trace route. This includes the necessary device drivers and the other software to enable a device's Ethernet interface automatically. Mobile devices also normally provide the programs needed to enable Wi-Fi, Bluetooth or other wireless connectivity.

The early versions of Microsoft Windows did not provide any computer networking support. Microsoft added basic networking capability to its operating system, starting with Windows 95 and Windows for Workgroups. Microsoft also introduced its Internet Connection Sharing (ICS) feature in Windows 98 Second Edition (Win98 SE). This can be contrasted with UNIX, which was designed from the beginning with networking in view. Nearly any consumer O/S today qualifies as a network operating system due to the popularity of the Internet.

Some security devices allow you to define the properties of a WAN data link by configuring the WAN interface. The following topic allows you to configure the properties for the physical line and the encapsulation method to be used to transfer data across the WAN.



**Fig 5.1 Transfer of Data**

**❑ Check Your Progress – 3 :**

1. Microsoft added basic networking capability to its operating system, starting with \_\_\_\_\_.
  - a. Windows 95
  - b. Windows 98
  - c. Windows 2000
  - d. Windows Me
2. Microsoft introduced \_\_\_\_\_ feature in Windows 98 Second Edition.
  - a. LAN
  - b. ICS
  - c. SMTP
  - d. Topology

**5.5 WAN Interface Information :**

**Interface Name (read-only)**

The name of a physical interface comprises the media type, slot number (for some devices) and port number, for instance, serial 1/0 or serial 6/0.



**WAN Configuration**

- **Member Link** : Select this option if the interface is to be added to a multilink interface (also called a bundle).
- **Multilink Interface** : Select the multilink interface to which the WAN interface is added.
- **Main Link** : Select this option if the WAN interface is not part of a multilink interface.
- **BRI Mode** : Select Leased Line Mode or Dial Using BRI to configure the device for ISDN support.
- **Leased Line Mode** : The interface in this mode is a Layer 3 interface. It is predefined for a data rate of 128 Kbps. There is no signalling on the D-channel and the leased line is used to deliver data only. Leased line mode supports PPP encapsulation only.

**Dial Using BRI**

Check this option to use the ISDN BRI to dial out. Click 'Apply' and edit the Dialer Enable Options Edit the following to configure the dialer for Basic Rate Interface (BRI):

- **Primary and Alternative Number** : Enter the remote destination to call. If the primary number is not connected, alternative-number is used. The primary-number and alternative-number is a string of characters 1–15.
- **Load Threshold** : Enter the threshold (in percent) to set up the second B-channel. For bandwidth on demand, if traffic is greater than the defined load-threshold, the second B-channel is setup. The range for this B-channel is 1 to 100. The default is 80.
- **Idle Time** : If there is no traffic before the idle-time expires (in seconds), the connection is lost. The range for idle time is 0 to 60000, where 0 = never idle. The default is 180.
- **Retry Times** : Enter the number of times to redial if the dial number fails. The range is 1–6 and the default is 3.
- **Interval** : The dial interval (in seconds) between retries. The range is from 1 to 60 and the default is 30.

**WAN Encapsulation**

- **None** : Sets no encapsulation method
- **PPP** : Sets the WAN interface to use Point-to-Point Protocol as the encapsulation method
- **Frame Relay** : Sets the WAN interface to use Frame Relay as the encapsulation method
- **Cisco HDLC** : Sets the WAN interface to use Cisco HDLC as the encapsulation method
- **Binding a PPP Profile (appears after you select PPP or MLPPP encapsulation and click Apply)** : Select the PPP access profile.
- **Zone Name** : Select the zone to which the interface is bound.

**Fixed IP option**

- **IP Address/Net mask** : Enter the IP Address and netmask of the interface.

## Introduction to Computer Network

- **Manageable** : Select this option to enable management of the device using the interface IP address.
- **Manage IP** : The logical IP address through which you can manage the device. You can set a different Manage IP address on each available interface. The Manage IP address must be on the same subnet as the physical IP address.
  - Unnumbered : Sets the WAN interface to use a unnumbered interface
  - Interface : Selects the unnumbered interface.

### Management Services

- **WebUI** : Select this option to enable management through the Web user interface (WebUI).
- **SNMP** : Select this option to enable the use of SNMP. The device supports the SNMPv1 protocol (described in RFC–1157) and all relevant MIB II (Management Information Base II) groups defined in RFC–1213.
- **Telnet** : Select this option to allow management through a terminal emulation program for TCP/IP networks such as the Internet. Telnet is a common way to control a network device remotely.
- **SSL** : Select this option to allow the interface to receive HTTPS traffic for secure management of the device via the WebUI.
- **SSH** : Select this option to enable management using a secure command shell (SSH). You can administer the device from an Ethernet connection or a dial-in modem using SSH.

### Other Services

- **Ping** : Select this option to allow the device to respond to ICMP echo requests or '\_pings'. Ping is a utility that determines whether a specific IP address is accessible or not.
- **Path MTU (IPV4)** : Sets the device to use the smallest MTU for all the links in a path.
- **Ident–reset** : Services like Mail and FTP send identification requests. If they receive no acknowledgment, they send the request again. While the request is processing, there is no user access. An ident–reset restores access that has been blocked by an unacknowledged identification request.
- **Maximum Transfer Unit (MTU)** : The default protocol MTU is 1500 bytes for serial, T1, E1, ISDN BRI and multilink interfaces and 4470 bytes for T3 interfaces. If the MTU of the network to which the interface connects is different, enter that value here. You can specify a value between 800 and 8192 bytes.
- **DNS Proxy** : Select this option if you want the device to proxy (forward) DNS queries received on this interface to the appropriate DNS server as configured on the DNS Proxy Configuration page.
- **WebAuth checkbox** : (Appears only when an IP address/net mask is entered and applied). Select this option to enable WebAuth authentication for this interface.
- **IP** : Enter the IP address that receives authentication requests for the WebAuth server. The WebAuth IP address must be in the same subnet as the interface IP address.

- **SSL Only checkbox** : Select this option to require that all Web Authentication requests use SSL. The URL that a Web Authentication user enters in his or her webbrowser must be https://ip\_addr, in which ip\_addr the IP address is that receives authentication requests for the WebAuth server.

Following the configuration of basic WAN interface parameters, specific WAN interface options can be configured. To configure WAN interface specific features, click WANat the top of the interface properties. Based on the interface you are configuring, you will see one amongst the following options:

- Serial Interface Options
- T1 Interface Options
- E1 Interface Options
- T3 Interface Options
- ISDN Options
- Dialer Pool Options

#### **Check Your Progress – 4 :**

1. \_\_\_\_\_ the WAN interface to use Point-to-Point Protocol as the encapsulation method.
  - a. PPP
  - b. Frame Relay
  - c. Cisco HDLC

### **5.6 Let Us Sum Up :**

**In this unit, we have learned :**

- Virtual memory with pre-emptive scheduling is a great design choice for properly constructed functional blocks, where interaction between different modules is limited and well defined.
- A CPU and memory are shared resources, all running threads and processes have to access them in a serial and controlled fashion.
- A number of design choices are available to achieve this goal, but the two most important are the memory model and the scheduling discipline.

So in this unit a detailed discussion was made on CPU and Virtual memory.

### **5.7 Answers for Check Your Progress :**

#### **Check Your Progress 1 :**

1 : a

#### **Check Your Progress 2 :**

1 : a

#### **Check Your Progress 3 :**

1 : a                      2 : b

#### **Check Your Progress 4 :**

1 : a

### **5.8 Glossary :**

1. **Socket :** The Berkeley Unix mechanism for creating a virtual connection between processes. Sockets interface Unix's standard I/O with its network communication facilities. They can be of two types, stream (bi-directional) or datagram (fixed length destination-addressed messages). The socket library function `socket ()` creates a communications end-point or socket and returns a file descriptor with which to access that socket. The socket has associated with it a socket address, consisting of a port number and the local host's network address.
2. **Virtual Circuit :** A connection-oriented network service which is implemented on top of a network which may be either connection-oriented or connectionless (packet switching).
3. **Virtual Memory :** a system whereby addressable memory is extended beyond main storage through the use of secondary storage managed by system software in such a way that programs can treat all of the designated storage as addressable main storage.

### **5.9 Assignment :**

What is WAN ?

### **5.10 Activities :**

What kind of phone lines can WAN use ?

### **5.11 Case Study :**

Based on LAN and WAN models, make a working model in Lab

### **5.12 Further Readings :**

1. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001
2. Sams Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002

**UNIT STRUCTURE**

- 6.0 Learning Objectives
- 6.1 Introduction
- 6.2 Network Function
- 6.3 TCP Protocol Operation
- 6.4 Connection Establishment
- 6.5 Features of SPP-over-IP
- 6.6 Repeater Operation
  - 6.6.1 SPP-over-IP over GPRS
  - 6.6.2 Opening Connection from Access Server
  - 6.6.3 SPP-over-IP and COM Ports
- 6.7 Maintaining and Forwarding Outgoing Connections
- 6.8 Some TCP/IP Suite Members and their Functions
- 6.9 IP Address
- 6.10 Let Us Sum Up
- 6.11 Answers for Check Your Progress
- 6.12 Glossary
- 6.13 Assignment
- 6.14 Activities
- 6.15 Case Study
- 6.16 Further Readings

**6.0 Learning Objectives :**

After learning this unit, you will be able to understand :

- TCP/IP Protocol Operation
- Features of SPP over IP
- Repeater Operation
- SPP over IP over GPRS
- IP address

**6.1 Introduction :**

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite, complementing the Internet Protocol (IP) and therefore the entire suite is commonly referred to as TCP/IP. TCP provides the service of exchanging data reliably directly between two network hosts, whereas IP handles addressing and routing message across one or more networks.

In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. TCP is the protocol that major Internet applications rely on, such as the World Wide Web, e-mail and file transfer. Other applications, which do not require reliable data stream service, may use the User Datagram Protocol (UDP), which provides a datagram service, which emphasises reduced latency over reliability.

## **6.2 Network Function :**

TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP). That is, when an application program desires to send a large chunk of data across the Internet using IP, instead of breaking the data into IP-sized pieces and issuing a series of IP requests, the software can issue a single request to TCP and let TCP handle the IP details.

IP works by exchanging pieces of information called packets. A packet is a sequence of bytes and consists of a header followed by a body. The header describes the packet's destination and optionally, the routers to use for forwarding until it arrives at its destination. The body contains the data IP is transmitting.

Due to network congestion, traffic load balancing or other unpredictable network behaviour, IP packets can be lost, duplicated, or delivered out of order. TCP detects these problems, requests retransmission of lost packets, rearranges out-of-order packets and even helps minimise network congestion to reduce the occurrence of the other problems.

Once the TCP receiver has finally reassembled a perfect copy of the data originally transmitted, it passes that datagram to the application program. Thus, TCP abstracts the application's communication from the underlying networking details.

TCP is used extensively by many of the Internet's most popular applications, including the World Wide Web (WWW), E-mail, File Transfer Protocol, Secure Shell, peer-to-peer file sharing and some streaming media applications.

TCP is optimised for accurate delivery rather than timely delivery and therefore, TCP sometimes incurs relatively long delays (in the order of seconds) while waiting for out-of-order messages or retransmissions of lost messages.

It is not particularly suitable for real-time applications such as voice over IP. For such applications, protocols like the Real-time Transport Protocol (RTP) running over the User Datagram Protocol (UDP) are usually recommended instead.

TCP is a reliable stream delivery service that guarantees delivery of a data stream sent from one host to another without duplication or losing data. Since packet transfer is not reliable, a technique known as positive acknowledgment with retransmission is used to guarantee reliability of packet transfers. This fundamental technique requires the receiver to respond with an acknowledgment message as it receives the data.

The sender keeps a record of each packet it sends and waits for acknowledgment before sending the next packet. The sender also keeps a timer from when the packet was sent. It retransmits a packet if the timer expires. The timer is needed in case a packet is lost or corrupted.

TCP consists of a set of rules: for the protocol, that are used with the Internet Protocol and for the IP, to send data in a form of message units' between computers over the Internet. At the same time that IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data transmission, called segments that a message is divided into for efficient routing through the network.

For example, when an HTML file is sent from a Web server, the TCP software layer of that server divides the sequence of bytes of the file into segments and forwards them individually to the IP software layer (Internet Layer). The Internet layer encapsulates each TCP segment into an IP packet by adding a header that includes (among other data) the destination IP address.

Even though every packet has the same destination address, they can be routed on different paths through the network. When the client program on the destination computer receives them, the TCP layer (Transport Layer) reassembles the individual segments and ensures they are correctly ordered and error free as it streams them to an application.

A TCP segment consists of a segment header and a data section. The TCP header contains 10 mandatory fields and an optional extension field.

The data section follows the header. Its contents are the payload data carried for the application. The length of the data section is not specified in the TCP segment header. It can be calculated by subtracting the combined length of the TCP header and encapsulating IP segment header from the total IP segment length (specified in the IP segment header).

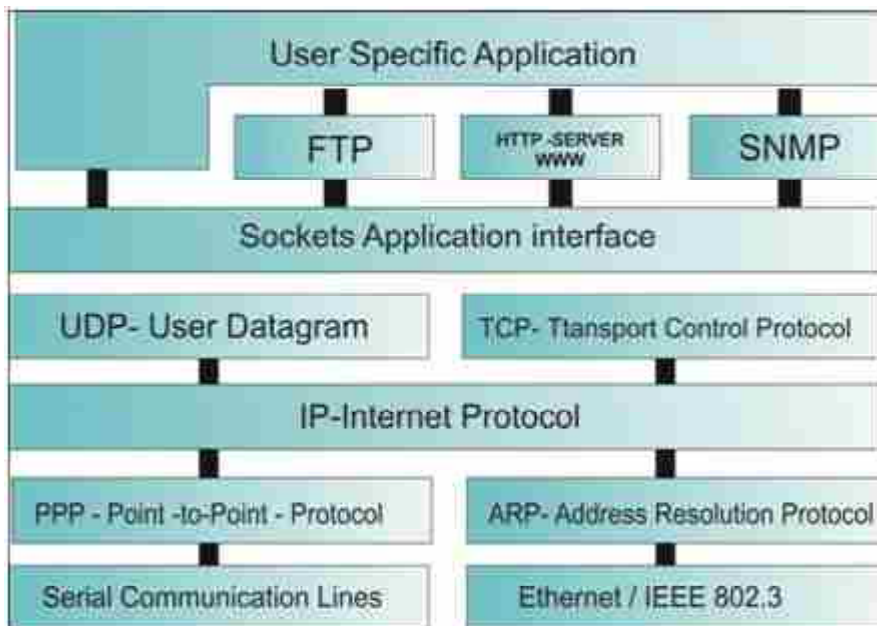
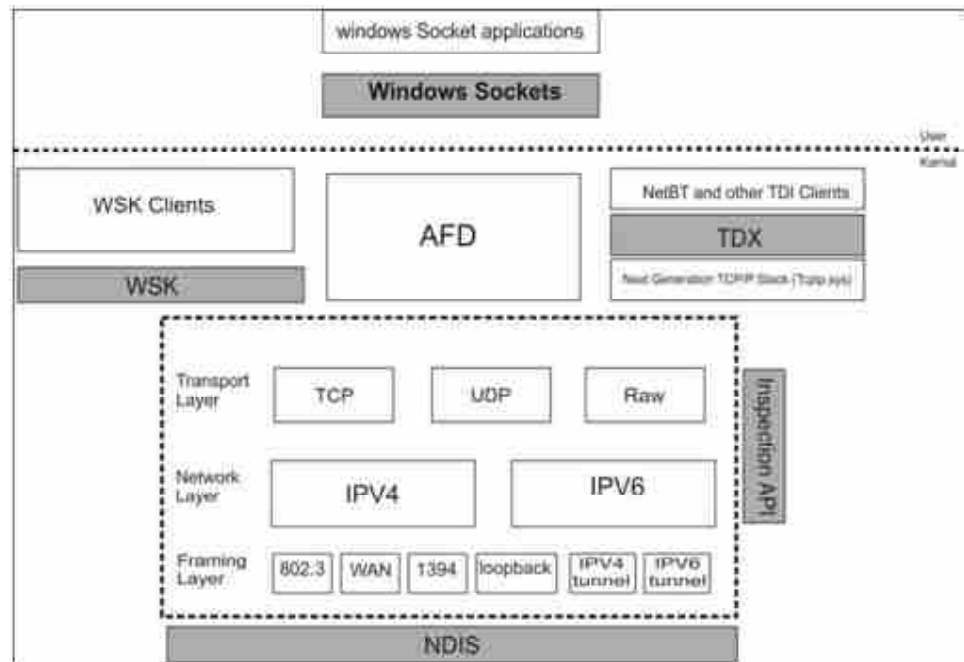


Fig. 6.1 : Protocols

- **Source port (16 bits)** : Identifies the sending port
- **Destination port (16 bits)** : Identifies the receiving port
- **Sequence number (32 bits)** : Has a dual role

If the SYN flag is set, then this is the initial sequence number. The sequence number of the actual first data byte (and the acknowledged number in the corresponding ACK) is then this sequence number plus 1.

If the SYN flag is clear, then this is the accumulated sequence number of the first databyte of this packet for the current session.



**Fig. 6.2 : Windows Socket Applications**

Acknowledgment number (32 bits) – If the ACK flag is set then the value of this field is the next sequence number that the receiver is expecting. This acknowledges receipt of all prior bytes (if any). The first ACK sent by each end acknowledges the other end's initial sequence number itself, but no data.

Data off set (4 bits) specifies the size of the TCP header in 32-bit words. The minimum size header is 5 words and the maximum is 15 words thus giving the minimum size of 20 bytes and maximum of 60 bytes, allowing for up to 40 bytes of options in the header. This field gets its name from the fact that it is also the off set from the start of the TCP segment to the actual data.

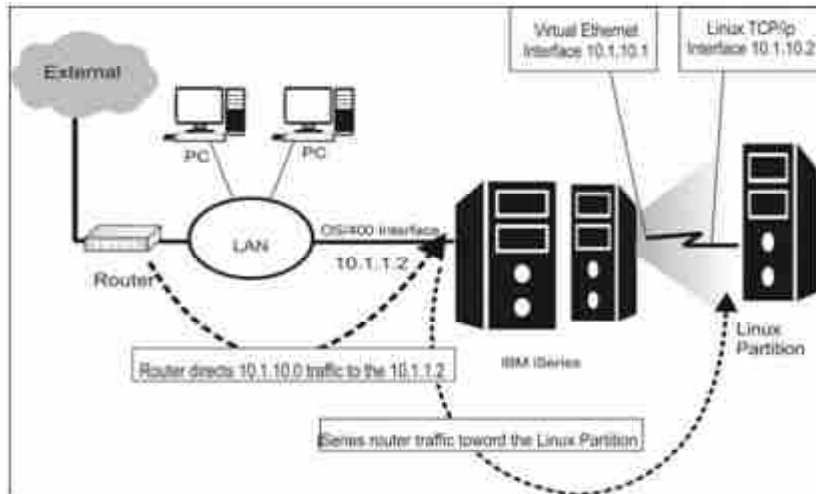
- **Reserved (4 bits) :** For future use and should be set to zero
- **Flags (8 bits) (Control bits) :** Contains 8 1-bit flags
- **CWR (1 bit) :** Congestion Window Reduced (CWR) flag is set by the sending host to indicate that it received a TCP segment with the ECE flag set and had responded in congestion control mechanism (added to header by RFC 3168).
- **ECE (1 bit) :** ECN-Echo indicates

If the SYN flag is set, then the TCP peer is ECN capable. If the SYN flag is clear, then a packet with Congestion Experienced flag in IP header set is received during normal transmission (added to header by RFC 3168).

- **URG (1 bit) :** Indicates that the urgent pointer field is significant
- **ACK (1 bit) :** Indicates that the acknowledgment field is significant. All packets after the initial SYN packet sent by the client should have this flag set.
- **PSH (1 bit) :** Push function asks to push the buffered data to the receiving application.



- **RST (1 bit)** : Reset the connection
- **SYN (1 bit)** : Synchronise sequence numbers. Only the first packet sent from each end should have this flag set. Some other flags change meaning based on this flag and some are only valid when it is set and others when it is clear.
- **FIN (1 bit)** : No more data from sender



**Fig. 6.3 : Network Connection**

- **Window (16 bits)** : The size of the 'receive window' which specifies the number of bytes (beyond the sequence number in the acknowledgment field) that the receiver is currently willing to receive.
- **Checksum (16 bits)** : The 16-bit checksum field is used for error-checking of the header and data.
- **Urgent pointer (16 bits)** : If the URG flag is set, then this 16-bit field is an offset from the sequence number indicating the last urgent data byte.
- **Options (Variable 0–320 bits, divisible by 32)** : The length of this field is determined by the data offset field. Options 0 and 1 are a single byte (8 bits) in length. The remaining options indicate the total length of the option (expressed in bytes) in the second byte. Some options may only be sent when SYN is set; they are indicated below as SYN.
- **0 (8 bits)** : End of options list
- **1 (8 bits)** : No operation (NOP, Padding). This may be used to align option fields on 32-bit boundaries for better performance.
- **2, 4, SS (32 bits)** : Maximum segment size
- **3, 3, S (24 bits)** : Window scale
- **4, 2 (16 bits)** : Selective Acknowledgement permitted. 5, N, BBBB, EEEE, ... (variable bits, N is either 10, 18, 26, or 34)– Selective Acknowledgement (SACK) these first two bytes are followed by a list of 1–4 blocks being selectively acknowledged, specified as 32-bit begin/end pointers.
- **8, 10, TTTT, EEEE (80 bits)** : Timestamp and echo of previous timestamp 14, 3, S (24 bits) – TCP Alternate Checksum Request
- **15, N, ... (variable bits)** : TCP Alternate Checksum Data

(The remaining options are obsolete, experimental, not yet standardised, or unassigned)

❑ **Check Your Progress – 1 :**

1. TCP is used extensively by many of the Internet's most popular applications.
  - a. WWW
  - b. Chat applications

**6.3 TCP Protocol Operation :**

TCP protocol operations may be divided into three phases. Connections must be properly established in a multi-step handshake process (connection establishment) before entering the data transfer phase. After data transmission is completed, the connection termination closes establishes virtual circuits and releases all allocated resources.

A TCP connection is managed by an operating system through a programming interface that represents the local end-point for communications, the Internet socket. During the lifetime of a TCP connection, it undergoes a series of state changes:

- **LISTEN** : In case of a server, waiting for a connection request from any remote client.
- **SYN-SENT** : Waiting for the remote peer to send back a TCP segment with the SYN and ACK flags set (usually set by TCP clients).
- **SYN-RECEIVED** : Waiting for the remote peer to send back an acknowledgment after having sent back a connection acknowledgment to the remote peer (usually set by TCP servers).
- **ESTABLISHED**: The port is ready to receive/send data from/to the remote peer.
  - FIN-WAIT-1
  - FIN-WAIT-2
  - CLOSE-WAIT
  - CLOSING
  - LAST-ACK
- **TIME-WAIT** : represents waiting for enough time to pass to be sure the remote peer received the acknowledgment of its connection termination request. According to RFC 793, a connection can stay in TIME-WAIT for a maximum of four minutes.
  - CLOSED

❑ **Check Your Progress – 2 :**

1. In case of a server, waiting for a connection request from any remote client.
  - a. LISTEN
  - b. SYN-SENT
  - c. SYN-RECEIVED

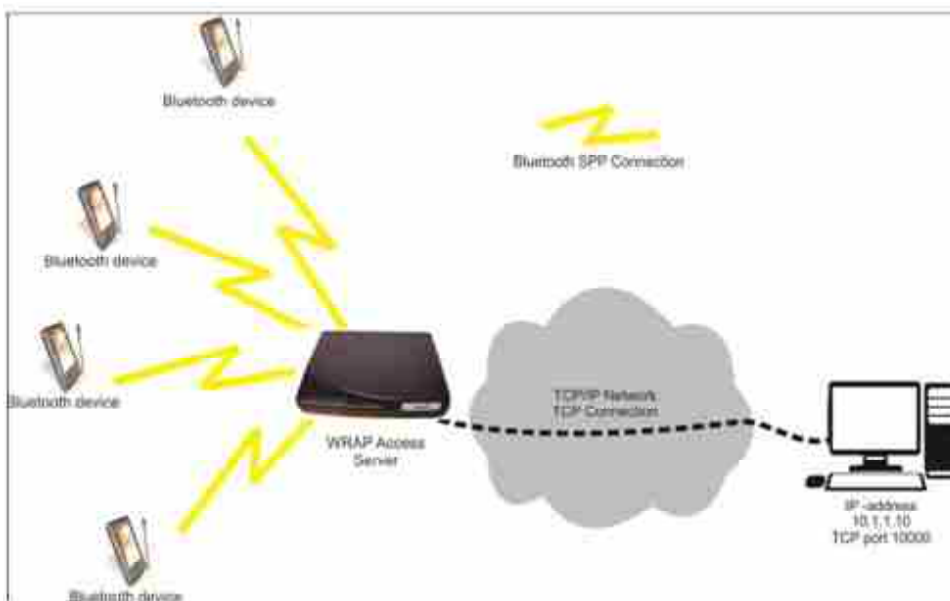
**6.4 Connection Establishment :**

To establish a connection, TCP uses a three-way handshake. Before a client attempts to connect with a server, the server must first bind to a port to open it up for connections: this is called a passive open. Once the passive open is established, a client may initiate an active open.

To establish a connection, the three-way (or 3-step) handshake occurs :

- The active open is performed by the client sending a SYN to the server. It sets the segment's sequence number to a random value A.
- In response, the server replies with a SYN-ACK. The acknowledgment number is set to one more than the received sequence number (A + 1) and the sequence number that the server chooses for the packet is another random number, B.
- Finally, the client sends an ACK back to the server. The sequence number is set to the received acknowledgement value i.e. A + 1 and the acknowledgement number is set to one more than the received sequence number i.e. B + 1.

At this point, both the client and server have received an acknowledgment of the connection.



**Fig. 6.4 : TCP PORTS**

**SPP-over-IP**

SPP-over-IP is a special functionality of iWRAP Bluetooth servers running in Access Servers. It offers a transparent way to transmit data from Bluetooth Serial Port Profile (SPP) enabled devices to server computers or PCs. Several transport medium are supported, such as Ethernet, Wi-Fi or and GPRS.

**How SPP-over-IP Works**

The SPP-over-IP application enables transparent data transfer between any Bluetooth Serial Port Profile (SPP) complaint device and a server, laptop or desktop connected to the same network. This enables plug and play connectivity from a Bluetooth network to any standard TCP/IP based network.

**☐ Check Your Progress – 3 :**

1. To establish a connection, TCP uses a \_\_\_\_\_ hand shake.
  - a. three-way
  - b. oneway
  - c. two way

**6.5 Features of SPP-Over-IP :**

- Access Server 2291 supports 7 incoming SPP connections.
- Access Server 2293 supports 21 incoming SPP connections.

## Introduction to Computer Network

- SPP-over-IP can be used over Ethernet, Wi-Fi or GRPS networks.
- SPP-over-IP also works over Bluetooth Personal Area Networking (PAN) connections, so not all Access Servers need to be physically (cable) connected to the TCP/IP network, but some Access Servers can be linked using the Bluetooth PAN connection. This is referred to as repeater operation.
- If SPP-over-IP application cannot open the TCP connection to defined IP address and port, the SPP connection will not be accepted.
- If the TCP server on PC is closed, all SPP connections will be closed as well.
- When access server is in its default configuration, it tries to enable sniff power saving mode on all idle Bluetooth connections to minimise power consumption.
- SPP-over-IP can also be used to opposite direction, i.e. access server opens the Bluetooth connections to dedicated Bluetooth devices.
- SPP-over-IP can also be combined with the Tactical Software's Serial/IP® software. Serial/IP software converts automatically TCP connections to virtual COM ports on the host PC, so legacy applications utilising COM-ports instead of TCP/IP can also be used.

### Standard operation

With the standard configuration, SPP-over-IP works as described below:

- Listens for incoming Serial Port Profile (SPP) connections
- Takes control of all incoming connections
- Opens a TCP connection to the defined IP address and TCP port
- Forwards all incoming data from the SPP device to the established TCP connection and vice versa

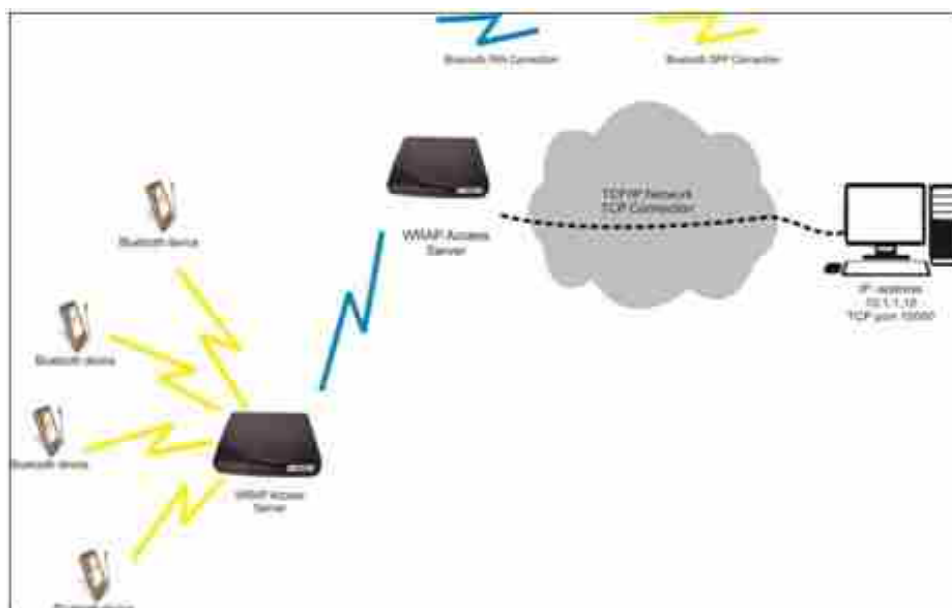
All the server computer needs to do is to listen for incoming TCP connections from access server to a specified TCP port and receive/send the application data.

### ❑ Check Your Progress – 4 :

1. Access Server 2293 supports \_\_\_\_\_ incoming SPP connections.  
a. 21                      b. 7                      c. 42

## 6.6 Repeater Operation :

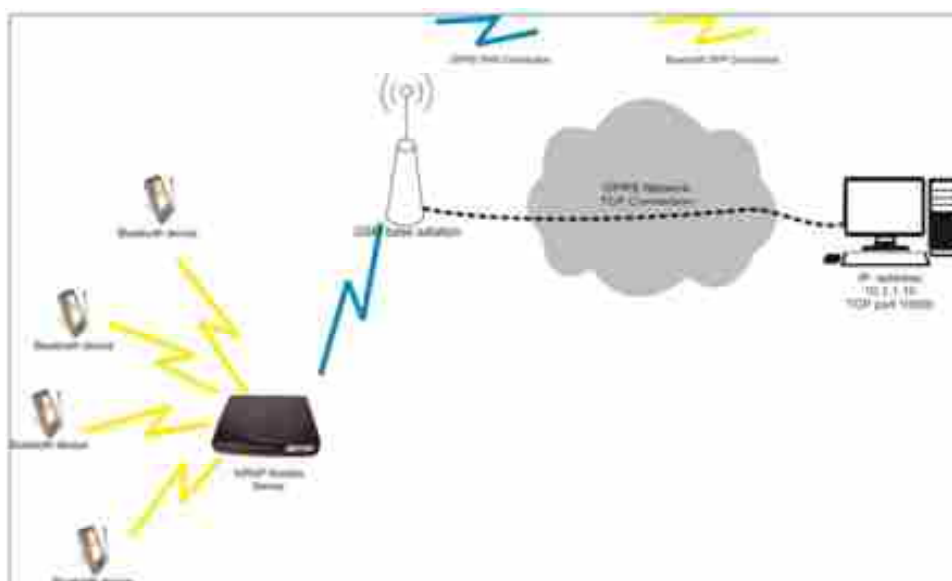
The SPP-over-IP application can also be used in a so-called repeater mode. This feature is useful when not all access servers can be directly connected to the TCP/IP network, but they can be connected to other access servers by using Bluetooth PAN-connection. PAN enables transmitting TCP/IP packets wirelessly over Bluetooth. The figure below illustrates this configuration :



**Fig. 6.5 : Repeater Mode in SPP-over-IP**

### 6.6.1 SPP-over-IP over GPRS :

SPP-over-IP software can also be used over GPRS instead of wired Ethernet connection. This requires that access server is equipped with a working GSM/GPRS compact flash card.



**Fig. 6.6 : SPP-over-IP over GPRS**

#### Notice when using GPRS :

Data upload rate is around 8–12kbps (depending on GPRS card).

Data download rate is around 32–48kbps (depending on GPRS card).

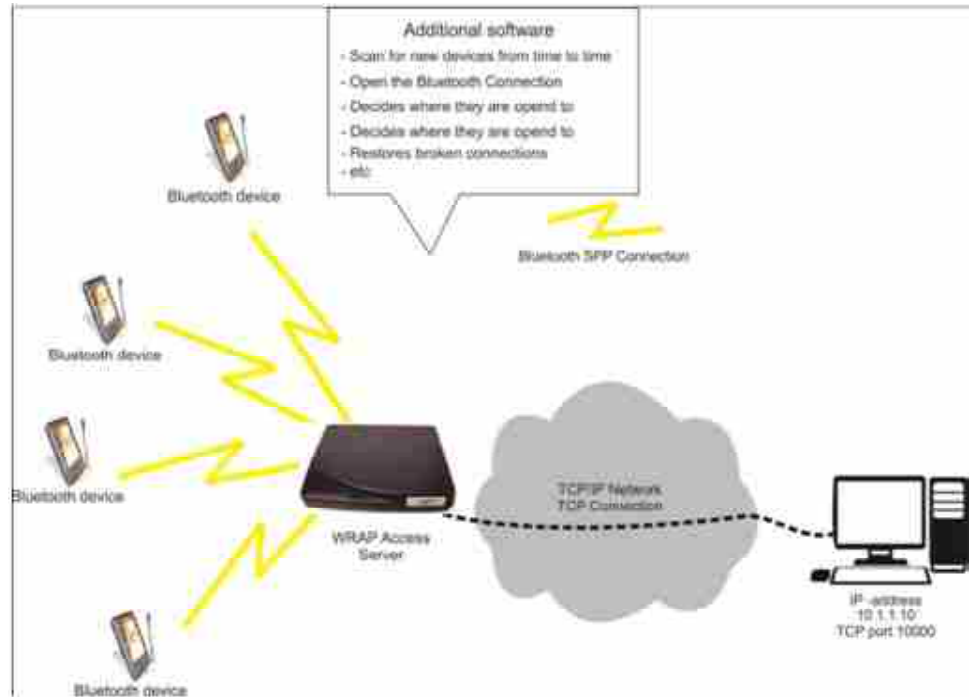
Data transmission delays can be very high, sometimes even seconds.

GPRS connection may be unreliable and break easily. This should be taken account when designing the system. If GPRS connection breaks, all the TCP and Bluetooth connections will also be closed.

### 6.6.2 Opening Connections from Access Server :

In the basic SPP-over-IP use case, Access server is in passive mode and only accepts incoming connections. Using connector service, Access server

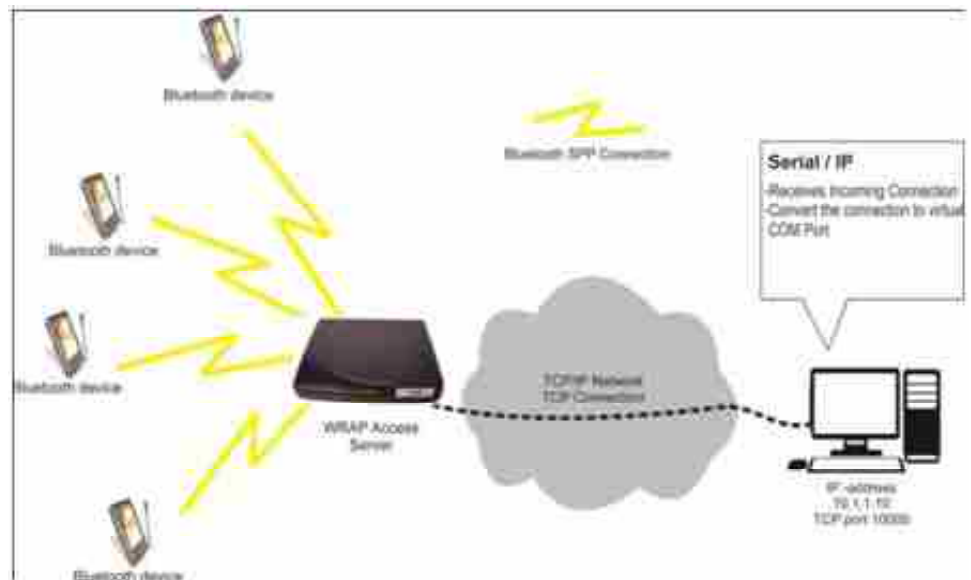
can open and maintain outgoing Bluetooth connections to defined Bluetooth devices.



**Fig. 6.7 : Access Server Opening the Connections**

**6.6.3 SPP-OVER-IP and Com Ports :**

SPP-over-IP can also be used together with Tactical Software's Serial/IP® software. Serial/IP software simply converts the TCP connections into virtual COM ports on the host computer. This is very useful in applications, which do not have support for TCP/IP but support COM ports instead.



**Fig. 6.8 : SPP-over-IP with Serial/IP**

**Configuring SPP-over-IP**

This briefly instructs you to configure SPP-over-IP to work in different network setups or use cases. SPP-over-IP is easiest to configure through WWW setup, which allows you to access all the necessary configurations.

## Forwarding Incoming Connections

The basic SPP-over-IP operation, listening to incoming Bluetooth connections and forwarding them to a TCP/IP socket on a remote host (or a local application), is configured at Setup → iWRAP settings → Bluetooth profiles → Connection forwarding.

### ❑ Check Your Progress – 5 :

1. SPP-over-IP software can also be used over GPRS instead of \_\_\_\_\_ Ethernet connection.
  - a. Wired
  - b. Wifi
  - c. Bluetooth

## 6.7 Maintaining and Forwarding Outgoing Connections :

The SPP-over-IP connector, which opens and maintains outgoing Bluetooth connections and forwards them to a TCP/IP socket on a remote host (or a local application), is configured as follows :

Setup → Applications → Connector

### Repeater configuration

If you want to configure access server also to act as a repeater, you must make some additional configurations. Add the line below to your Bluetooth startup script, editable at Setup → iWRAP settings → Edit startup script. Line starting with # is comment, which can be left out :

```
# Automatically connect to Access Server with PAN-NAP enabled using baseband 1
```

```
10101 SET CONTROL AUTOEXEC CALL 00:07:80:bf:01 PAN-NAP
```

You must replace the Bluetooth address used in the example (00:07:80:80:bf:01) with the Bluetooth address of the access server, on which you want to receive the PAN connection.

**Note :** The server receiving the PAN connection must have the PAN-NAP profile enabled. This is by default is not the case, so in setup or its WWW interface, ensure that the setting at → Bluetooth settings → Bluetooth profiles → Enable PAN network access point profile says yes. No other configuration is needed.

### ❑ Check Your Progress – 6 :

1. The server receiving the PAN connection must have the PAN-NAP profile \_\_\_\_\_ .
  - a. enabled
  - b. disabled

## 6.8 Some TCP/IP Suite Members and Their Functions :

**Table 6.1 : TCP/IP Suite Members and Their Functions**

Name	Function
TCP	Transmission control protocol Ensures that connections are made and maintained between computers
IP	Internet protocol–handles software computer addresses
RIP	Address resolution protocol– it relates IP address with hardware (MAC)

<b>OSPF</b>	Open shortest path first – A descendant of RIP that increases its speed and reliability
<b>ICMP</b>	Internet control message protocol Handles errors and sends error messages for TCP/IP
<b>BGP/EGP</b>	Border gateway protocol/ exterior gateway protocol handles how data is passed between networks.
<b>SNMP</b>	Simple network management allows network administration to connect to and manage network devices.
<b>PPP</b>	Point to point protocol : It provides for dial up networked connections to networks.PPP is commonly used by internet service providers to allow customers to connect to their services.
<b>SMTP</b>	Simple mail transport protocol– How email is passed between servers on a TCP/IP network.
<b>POP3/IMAP4</b>	Post office protocol version 3/Internet message advertising protocol version 4–Both set up ways for clients to connect to the servers and collect email.

**❑ Check Your Progress – 7 :**

1. \_\_\_\_\_ Ensures that connections are made and maintained between computers.
  - a. TCP
  - b. SMTP
  - c. PPP

**6.9 IP Address :**

3.9

An Internet Protocol address (IP address) is a numerical label that is assigned to any device participating in a computer network that uses the Internet Protocol for communication between its nodes. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterised as follows : –A name indicates what we seek. An address indicates where it is. A route indicates how to get there|.

The designers of TCP/IP defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new addressing system (IPv6), using 128 bits for the address, was developed in 1995, standardised by RFC 2460 in 1998 and is in worldwide production deployment.

Although IP addresses are stored as binary numbers, they are usually displayed in human-readable notations, such as 208.77.188.166 (for IPv4) and 2001:db8:0:1234:0:567:1:1 (for IPv6).

The Internet Protocol is used to route data packets between networks; IP addresses specify the locations of the source and destination nodes in the topology of the routing system. For this purpose, some of the bits in an IP address are used to designate a sub network. The number of these bits is indicated in CIDR notation, appended to the IP address. E.g. 208.77.188.166/24.



As the development of private networks raised the threat of IPv4 address exhaustion, RFC 1918 set aside a group of private address spaces that may be used by anyone on private networks. Such networks require 'network address translator gateways' to connect to the global Internet.

The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and cooperates with five regional Internet registries (RIRs) to allocate IP address blocks to local Internet registries (Internet service providers) and other entities.

**Check Your Progress – 8 :**

1. The designers of \_\_\_\_\_ defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today.
  - a. TCP/IP
  - b. LAN
  - c. PPP

**6.10 Let Us Sum Up :**

**In this unit, we have learned :**

- A TCP segment consists of a segment header and a data section. The TCP header contains 10 mandatory fields and an optional extension field. The data section follows the header.
- Its contents are the payload data carried for the application. The length of the data section is not specified in the TCP segment header. An Internet Protocol address (IP address) is a numerical label that is assigned to any device participating in a computer network that uses the Internet Protocol for communication between its nodes.
- An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterised as follows: –A name indicates what we seek. An address indicates where it is||.
- Acknowledgment number (32 bits) – If the ACK flag is set then the value of this field is the next sequence number that the receiver is expecting. This acknowledges receipt of all prior bytes (if any).
- Data offset (4 bits) – This specifies the size of the TCP header in 32-bit words. The minimum size header is 5 words and the maximum is 15 words.

**6.11 Answers for Check Your Progress :**

**Check Your Progress 1 :**

1 : a

**Check Your Progress 2 :**

1 : a

**Check Your Progress 3 :**

1 : a

**Check Your Progress 4 :**

1 : a

- ❑ **Check Your Progress 5 :**  
1 : a
- ❑ **Check Your Progress 6 :**  
1 : a
- ❑ **Check Your Progress 7 :**  
1 : a
- ❑ **Check Your Progress 8 :**  
1 : a

### **6.12 Glossary :**

1. **Modem (Modulator/Demodulator) :** An electronic device for converting between serial data (typically EIA-232) from a computer and an audio signal suitable for transmission over a telephone line connected to another modem. In one scheme the audio signal is composed of silence (no data) or one of two frequencies representing zero and one.
2. **Network :** a system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables: used to transmit or receive information.
3. **Network Layer :** The third lowest layer in the OSI seven layer model. The network layer determines routing of packets of data from sender to receiver via the data link layer and is used by the transport layer. The most common network layer protocol is IP.
4. **Repeater :** A network or communications device which propagates electrical signals from one cable to another, amplifying them to restore them to full strength in the process. Repeaters are used to counter the attenuation which occurs when signals travel long distances
5. **Router :** A device which forwards packets between networks. The forwarding decision is based on network layer information and routing tables, often constructed by routing protocols.
6. **Socket :** The Berkeley Unix mechanism for creating a virtual connection between processes. Sockets interface Unix's standard I/O with its network communication facilities. They can be of two types, stream (bi-directional) or datagram (fixed length destination-addressed messages). The socket library function socket() creates a communications end-point or socket and returns a file descriptor with which to access that socket. The socket has associated with it a socket address, consisting of a port number and the local host's network address.

### **6.13 Assignment :**

1. Explain TCP protocol operation.
2. What are the features of SPP over IP ?

### **6.14 Activities :**

1. Explain the repeater operation.
2. Explain SPP over IP over COM ports.

**6.15 Case Study :**

Obtain more information of TCP/IP and prepare a report on the same.

**6.16 Further Readings :**

1. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001
2. Sams Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002

**UNIT STRUCTURE**

- 7.0 Learning Objective
- 7.1 Introduction
- 7.2 ARP
- 7.3 RARP
- 7.4 IPv4
  - 7.4.1 IPv4 Header
- 7.5 IPv6
  - 7.5.1 IPv 6 Address Type
- 7.6 ICMP
- 7.7 TCP
  - 7.7.1 TCP Header
- 7.8 UDP
- 7.9 Let's Sum Up
- 7.10 Answers Chek your Progress
- 7.11 Glossary
- 7.12 Assignment
- 7.13 Activities
- 7.14 Case Study
- 7.15 Further Readings

**7.0 Learning Objectives :**

After learning this unit, you will be able to understand network protocols :

- Address resolution protocol
- Reverse address resolution protocol
- IPv4, IPv6
- Internet Control Management Protocol
- TCP,UDP

**7.1 Introduction :**

The network protocols are the rules under which two machines are communication with each other and exchanging information. The ARP protocol is responsible to get IP address related details of destination. IPv4 and IPv6 are used for addressing devices. The transport layer protocols TCP and UDP.

## 7.2 ARP :

ARP stands for address resolution protocol. Now this is a protocol that is used to resolve IP addresses to MAC addresses. The MAC address is a physical address of a device. It's a globally unique number that is assigned to every network interface card. It is a 12 digit Hexadecimal representation. A sample MAC address is like 00-04-5A-63-AI-66. Whenever a device needs to communicate with another device on a local area network, it needs the MAC address for that device and devices use ARP to acquire the MAC address for that device. So as an example let's say that computer A wants to communicate with computer B. Now computer A already knows the IP address for computer B. But in order to communicate with computer B, it still needs its MAC address. Now an IP address is used to locate a device on a network and the MAC address is what identifies the actual device.

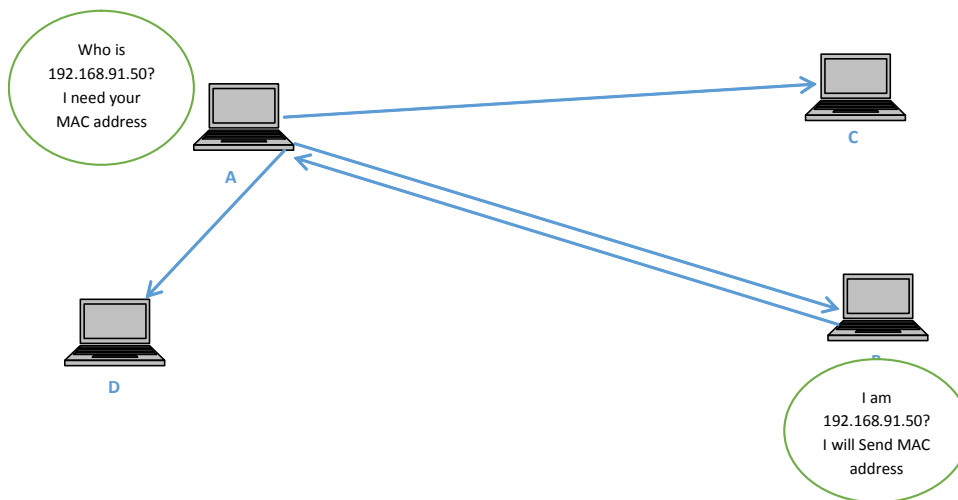


Fig. 7.1 ARP Explained

So in order to find the MAC address, computer A will first look at its internal list, called an ARP cache, to see if computer B's IP address already has a matching MAC address. In fact we can check this ourselves at a Windows command prompt by using the ARP utility. And by typing 'arp -a' and as you can see in the output there might be some entries or initially it has no entries at all, 'arp -a' displays current ARP entries in ARP cache. If computer B's entry is not found in computer A's ARP table then computer A will send out a broadcast message out on the network asking every device, which computer has the specific IP address and will ask for their MAC address. Then the computer that has the matching IP address will then respond back and tell computer A its MAC address. Then once it receives the MAC address, the communication can now take place between the two. Now once computer A has the MAC address, it'll store this information in the ARP cache. So now let's do the same commands as before and now you can see that the IP address and matching MAC address have been added to the ARP cache. The ARP cache is used to make a network more efficient. It stores IP address to MAC address associations, so that the next time it needs to communicate with a device on the network, it doesn't have to broadcast a message out on the entire network. It can just look in the ARP cache. And there are also two different types of ARP entries, dynamic and static. A dynamic entry is created automatically when a device sends out a broadcast message out on the network requesting a MAC address just like in the example we just did. Dynamic entries are not permanent, they are flushed out periodically so that the cache doesn't get filled up with

too many entries that are not being used. And a static entry is where someone manually enters an IP address to MAC address association using the ARP command-line utility. So for example let's check the ARP table. So at a command prompt you would type 'arp -a' .

```
C:\Users\ACER>arp -a

Interface: 192.168.91.159 --- 0xe
Internet Address      Physical Address      Type
192.168.91.161       7c-b0-c2-df-8a-45    dynamic
192.168.91.169       c0-b5-d7-9b-b2-2d    dynamic
192.168.91.215       c8-d9-d2-83-96-2d    dynamic
192.168.91.251       00-e0-4c-68-2f-e9    dynamic
192.168.91.255       ff-ff-ff-ff-ff-ff    static
224.0.0.22           01-00-5e-00-00-16    static
224.0.0.251          01-00-5e-00-00-fb    static
224.0.0.252          01-00-5e-00-00-fc    static
239.255.255.250     01-00-5e-7f-ff-fa    static
255.255.255.255     ff-ff-ff-ff-ff-ff    static
```

**Fig. 7.2 ARP Example in Command Prompt**

So now if we look at the ARP cache again, we would see our static ARP entry as well as dynamic entries also. Network administrators would use static entries to reduce any unnecessary ARP broadcast traffic on a network. For example, static entries are ideal if you know that two devices are constantly going to be communicating with each other.

**❑ Check Your Progress – 1 :**

1. ARP is used to resolve \_\_\_\_\_ to MAC address.
  - a IP address
  - b ARP cache
  - c TCP
  - d UDP

**7.3 RARP :**

The Reverse Address Resolution Mechanism (RARP) is a protocol that determining addresses inside a network. RFC 903 explains it in detail. When a network host, such as a diskless workstation, is booted, it does not know its own IP address. They use a process similar to ARP to identify their own IP address, but the hardware address of the host is now the known parameter, while the IP address is the queried parameter.

The reverse address resolution process is similar to the ARP address resolution process. For the ARP, the same packet format is used.

RARP request is broadcast, While RARP response is unicast in nature. With an Ethernet broadcast address and its own physical address, the client sends out a RARP request. The server then informs the client of its IP address. It is available for the LAN technologies like FDDI, token ring LANs, etc.

**RARP Vs ARP**

RARP is to determine IP address of own Machine (Self IP address)	ARP is to determine IP address of a remote machine
In RARP, the MAC address is available and the equivalent IP address for the same is requested	In ARP, the IP address is available, and the equivalent MAC address for the same is requested
It uses the value 3 for requests and 4 for responses	It uses the value 1 for requests and 2 for responses

**Limitations of RARP**

- The RARP server must be on the same physical network as the RARP client
- The computer sends the RARP request through a very low-cost network layer. As a result, a router is unable to forward the packet because the computer transmits the RARP request on the network's lowest layer.
- Because no subnet masks are sent, the RARP is unable to conduct the subnetting operation.
- Because it functions at such a low level, RARP has become outdated. It necessitates a direct network address, making it difficult to construct a server.

**❑ Check Your Progress – 2 :**

1. RARP uses the value 3 for \_\_\_\_\_ and 4 for responses
  - a. requests
  - b. IP address
  - c. MAC address
  - d. UDP

**7.4 Internet Protocol Version 4 :**

An IP address is a numeric address. It's an identifier for a computer or device on a network. Every device has to have an IP address for communication purposes. The IP address consists of two parts. The first part is the network address and the second part is the host address. There are also two types of IP addresses. The first one is the most common one, it's called IP version 4 and a second type is IP version 6.

IP version 4 is the current version of IP addresses. It's a 32-bit numeric address written as four numbers separated by periods. Each group of numbers that are separated by periods is called an octet. The number range in each octet is 0 to 255. This address version can produce over 4 billion unique addresses. In the world of computers and networks this IP address in this format here is meaningless. Computers and networks don't read IP addresses in this standard numeric format and that's because they only understand numbers in a binary format. A binary format is a number that only uses 1s and 0s. For ex. the IP address is 66.94.29.13 the computer will interpret it as 01000010.01011110.00011101.00001101. This binary number format representation what computers and networking devices actually read. So the question is, how do we get this binary number from this IP address? IP address 4 is made up of four sets of eight binary bits. And these sets are called octets. The bits in each octet are represented by a number. So starting from the left, the first bit has a value of 128 then 64 then 32 and so on. All the way down to 1. Each bit on the octet can be either a 1 or a 0. If the number is a 1 then the number that it represents counts. If the number is a 0 then the number that it represents does not count. So by manipulating the 1s and the 0s in the octet, you can come up with a range from 0 to 255. So for example the first octet in this IP address is 66. So how do we get a binary number out of 66? First you look at the octet chart and you would put 1s under the numbers that would add up to the total of 66.

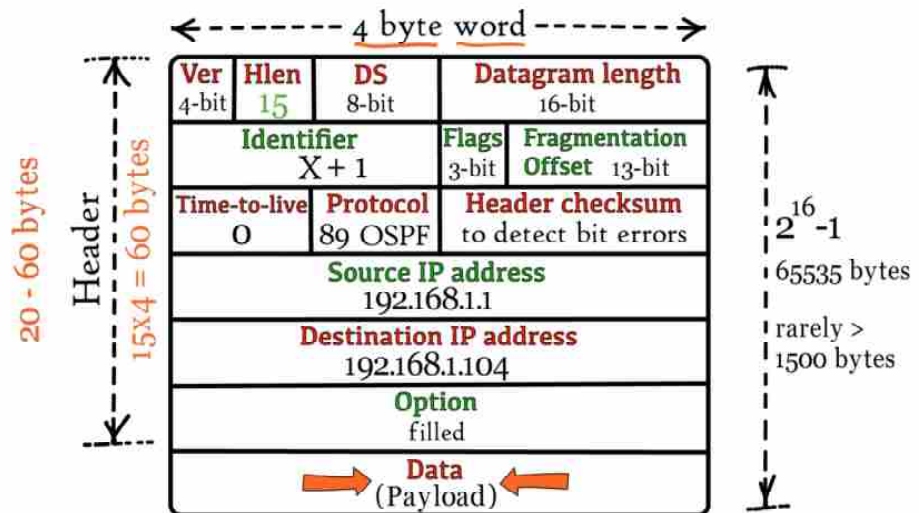
8 bit octet chart

$2^7=128$	$2^6=64$	$2^5=32$	$2^4=16$	$2^3=8$	$2^2=4$	$2^1=2$	$2^0=1$
-----------	----------	----------	----------	---------	---------	---------	---------

So you would put a 1 in the 64 slot. So now you already have 64, so we need 2 more. So let's put in number 1 in the two slot. So now if we count

all the numbers that we have 1s underneath them, you will get a total of 66. All of the other bits would be 0s because we don't need to count them since we already have our number. So this number here is the binary bit version of 66. So we'll put that number down here. So let's do the next number which is 94. So let's put a 1 under 64, 16, 8, 4, & 2. So if we were to add all the numbers that we have 1s underneath them, we would get a total of 94. And since we don't want to count any of the other numbers we just put 0s under the rest. So the next number is 29. So let's put a 1 under 16, 8, 4, & 1. And when you add all the numbers up you get 29. And our last number is 13. So let's select 8, 4, and 1. And when you add those up you get 13.

**7.4.1 IPv 4 Header :**



**Fig. 7.3 IPv 4 Header Format**

**The IPv4 header format is simplified here.**

**Version number**

It is 4-bit in length and specifies whether the datagram is of version 4 or version 6. Different versions use different datagram formats. So, this field helps the Internet Protocol software running on a machine to decide how to process the received datagram.

**Header length**

It is 4-bit in length, and it tells the total length of the IPv4 datagram header in terms of the 4-byte word. These words (in terms of the 4-byte word) mean that if I say, "The value in this field is 5", it refers that the length of IPv4 header is five words. One word in IPv4 is 4-byte in length. Therefore, the total length of the IPv4 header will be 5\*4, i.e. 20-bytes.

The 'OPTION' field is variable in length. It makes the IPv4 header vary in length too, and it ranges from 20-bytes to 60-bytes. If 'OPTION' field is empty, the value in Header length field is 5 or 0101 which makes IPv4 header 20-bytes in length. If the 'OPTION' field is filled, the value in this field will be 1111 in binary or 15 in decimal format. It increases the header length to 15\*4, i.e. 60-bytes where 1-byte is equal to 8-bits. Therefore, the IPv4 header length varies from 20-bytes to 60-bytes.

Next to the datagram header is the datagram payload or data. So, the value in the Header length field indicates where the payload begins in the datagram. The payload in the IPv4 datagram is the transport layer's segment.



### Differentiated Services

This field is 8-bit in length, out of which the first 6 bits are called code point or Differentiated Services Code Point (DSCP), and the last two bits are used for Explicit Congestion Notification. Since DSCP is 6-bit in length, so there can be  $2^6$  or 64 possible bit combinations. These bit combinations are used to classify IP packets so that one class of IP packet can receive precedence over the other in a network. For example, the IP packet used for network management must get precedence for transmission over any other type of IP packet.

### Datagram length

It tells the total length of the IP datagram, i.e. 'header' plus 'data'. Since it is 16-bit in length, so theoretically the maximum length of the datagram is  $2^{16}-1$  or 65,535 bytes. However, it is rarely larger than 1500 bytes which allow the IP datagram to fit in the payload section of the Ethernet frame. The size of the payload field in the Ethernet frame varies from 46 – 1500 bytes.

### Identifier, flags, and fragmentation offset

They are used in case of IP fragmentation. Suppose the router receives a datagram of 4000 bytes. It has a 20-byte header. So the data is 3980-bytes. This data should be encapsulated in an Ethernet frame which supports a maximum of 1500-bytes. In such a case, 3980-bytes are divided into small units and packed into separate IP datagrams so that the whole data can be transmitted. This is called IP fragmentation.

In the case of fragmented data, the receiver should :

1. Be able to identify that these are IP fragments, and they should be
2. Combined in correct order to form the original data unit

Fragmented IP packets are identified with the help of the Identifier field. When an IP datagram is created, a value is written in the Identifier field. For the next IP datagram, the value is incremented by 1. However, if the IP datagram is fragmented, the same Identifier value is written in all the fragments.

Flags are 3-bit in length out of which only two bits are used, called **do not fragment (D)** and **more fragment (M)**. If **D** is set to 0, the IP datagram can be fragmented. If not, it should not be fragmented. The value of 1 in the **M** field indicates that the datagram is not the last fragment. If the datagram has 0 in this field, it means either it is the last fragment, or it is the only fragment.

Now, the receiver has identified the IP fragments with the help of flags and identifier. These fragments should be arranged in proper order so as to form the original IP datagram. Here, 13-bit fragmentation offset solves the issue. Fragmentation offset tells the relative position of the fragments w.r.t. to the whole datagram (3980-bytes). For the first fragment, the relative position is zero. Dividing the length of the first fragment by 8 gives the offset value for the second fragment. Adding the length of first and second fragment, dividing the sum by 8 gives the offset value for the third fragment and so on. In this way, the receiver finds the correct order of the received fragments to form the original IP datagram.

IPv6 does not allow fragmentation.

### **Time-to-live**

This field is used to limit the lifetime of an IP datagram as it travels through the Internet. While transmitting a datagram, the source host sets a number in this field. When a router receives the datagram, it decrements this field by 1. If it reduces to 0, the router discards the datagram. Hence, limiting its lifetime. It is useful in cases where the routing tables become corrupted and cause the datagram to circulate among routers for a long time. Since, time-to-live field decrements with each hop, so such datagrams will be dropped by the routers at last. This field is also used to limit the journey of the datagrams. In order to limit datagrams within the local network, the source keeps value 1 in this field. When the router receives the packet, the value is decremented to 0 and hence, drops the packet preventing the packet from moving out of the local network.

### **Protocol**

When the IP datagram reaches its final destination, the value in this field indicates to which transport layer protocol the data portion of the IP datagram should be passed. For example,

- A value of 6 indicates that the data portion is passed to TCP.
- A value of 17 indicates that the data portion is passed to UDP.
- Moreover, a value of 1 indicates that the data portion belongs to ICMP, 2 for IGMP, and 89 for OSPF.

The protocol number is a glue that binds the network layer and the transport layer. Port number is a glue that binds the transport and application layer.

### **Header checksum**

It is 16-bit in length and helps in detecting the bit errors in the received IP datagram's header.

### **Source and destination IP address**

It represents the IPv4 address of the source host and the destination host, respectively. When a source host creates an IP datagram, it inserts its IP address in this field and also inserts the IP address of the destination. Source knows the IP address of the destination with the help of DNS lookup.

### **Options**

This field is optional and rarely used. It has a variable length with a maximum size of 40-bytes. When OPTION is used, it makes the length of IPv4 header vary from 20-bytes to 60-bytes. One such OPTION is 'source route' where the sender requests a certain routing path.

### **Data (Payload)**

It contains the segment of the transport layer, which has to be delivered to the destination. It can carry other types of data as well, for example, ICMP messages.

### **☐ Check Your Progress – 3 :**

- 1 IPv4 is \_\_\_\_\_ numeric address written as four numbers separated by periods
  - a. 8-bit
  - b. 16-bit
  - c. 32-bit
  - d. 64-bit

## 7.5 Internet Protocol Version 6 :

When the internet was first developed, programmers didn't realize how big it would become. They thought that IP version 4, which produced over 4 billion addresses, would be enough. But they were wrong. IP version 6 is the next generation of IP addresses. The main difference between IP version 4 and IP version 6 is the length of the address. The IP version 4 address is a 32-bit numeric address. Whereas IP version 6 is a 128-bit hexadecimal address. Hexadecimal uses both numbers and alphabets in the address. So with this type of address, IP version 6 can produce an unbelievable 340 undecillion IP addresses. That's the number 340 with 36 digits after it. So as you might have guessed, IP version 6 is more than enough for the foreseeable future. So as stated before, IP version 6 is a 128 bit hexadecimal address. It's made up of 8 sets of 16 bits with the 8 sets separated by colons as you can see here. So in a similar way that we converted an IP version 4 address to a binary number; this is how we convert a binary number to a hexadecimal address. In an IP version 6 IP address each hexadecimal character represents 4 bits. So we have to convert 4 bits at a time to get one hexadecimal character. So starting from the beginning, we convert the first 4 bits and put those bits up there against our 4-bit chart which includes an 8, 4, 2, and a 1. So if we count the numbers that we have 1s underneath them, you wind up with a 2. So a '2' is the first hexadecimal character in this IP version 6 address. So let's do the next four bits and put those under our four bit chart. So if we count all the numbers that we have 1s underneath them, we have a '4' and a '2' and if we add those up we get 6. So a '6' is the second hexadecimal character in this IP address. So let's do our next set of 4 bits. And if we add all the numbers that we have 1s underneath them, we get a total of 13. But the problem is since 13 is a double-digit number; we cannot use a double-digit number to represent 4 bits. And that's because in a hexadecimal format, double-digit numbers have to be represented with a single alphabet which is 'A' through 'F'.

IP version 4 has four sections called octets. IP version 6 has eight sections but these are commonly called hexets IP version 4 uses dots to separate octet but IP version 6 uses colons to separate hexets. Let's take a look at how IP version 6 works when it comes to binary. This is especially important when it comes to subnetting. Each hexadecimal character is made up of four binary bits. Just like IP version 4, IP version 6 has a network section and a host section. The way ipv4 does this is by using a subnet mask. However, IP version 6 has gotten rid of the subnet mask and instead it just uses a forward slash and the number of network bits which you should be familiar with from IP version 4. So in our example /64 is half of our 128 bit address. / 64 addresses are common when it comes to IP version 6 it splits a nicely down the middle and ensures we have plenty of networks and plenty of hosts but be prepared to see different numbers. Remember each character is 4 bits long and each hexet is 16 bits. Just like IP version 4 there are different types of IP version 6 addresses and they serve different purposes.

### 7.5.1 IPv6 Address Types :

There are three major categories of IPv6 addresses :

- Unicast—For a single interface.

- Multicast—For a set of interfaces on the same physical medium. A packet is sent to all interfaces associated with the address.
- Anycast—For a set of interfaces on different physical media. A packet is sent to only one of the interfaces associated with this address, not to all the interfaces.

### **Unicast Addresses**

A unicast address identifies a single interface. When a network device sends a packet to a unicast address, the packet goes only to the specific interface identified by that address. Unicast addresses support a global address scope and two types of local address scopes.

A unicast address consists of  $n$  bits for the prefix, and  $128 - n$  bits for the interface ID.

In the IPv6 implementation for a subscriber access network, the following types of unicast addresses can be used:

- **Global unicast address** – A unique IPv6 address assigned to a host interface. These addresses have a global scope and essentially the same purposes as IPv4 public addresses. Global unicast addresses are routable on the Internet.
- **Link-local IPv6 address** – An IPv6 address that allows communication between neighbouring hosts that reside on the same link. Link-local addresses have a local scope, and cannot be used outside the link. They always have the prefix FE80::/10.
- **Loopback IPv6 address** – An IPv6 address used on a loopback interfaces. The IPv6 loopback address is 0:0:0:0:0:0:0:1, which can be notated as ::1/128.
- **Unspecified address** – An IPv6 unspecified address is 0:0:0:0:0:0:0:0, which can be notated as ::/128.

### **Multicast Addresses**

A multicast address identifies a set of interfaces that typically belong to different nodes. When a network device sends a packet to a multicast address, the device broadcasts the packet to all interfaces identified by that address. IPv6 does not support broadcast addresses, but instead uses multicast addresses in this role.

Multicast addresses support 16 different types of address scope, including node, link, site, organization, and global scope. A 4-bit field in the prefix identifies the address scope.

The following types of multicast addresses can be used in an IPv6 subscriber access network:

- Solicited-node multicast address—Neighbour Solicitation (NS) messages are sent to this address.
- All-nodes multicast address—Router Advertisement (RA) messages are sent to this address.
- All-routers multicast address—Router Solicitation (RS) messages are sent to this address.

Multicast addresses use the prefix FF00::/8.

### Any Cast Addresses

An anycast address identifies a set of interfaces that typically belong to different nodes. Anycast addresses are similar to multicast addresses, except those packets are sent only to one interface, not to all interfaces. The routing protocol used in the network usually determines which interface is physically closest within the set of anycast addresses and routes the packet along the shortest path to its destination.

There is no difference between anycast addresses and unicast addresses except for the subnet router address. For an anycast subnet–router address, the low–order bits, typically 64 or more, are zero. Anycast addresses are taken from the unicast address space.

For more information about anycast addresses, see *RFC 2526, Reserved IPv6 Subnet Anycast Addresses*.

#### ❑ Check Your Progress – 4 :

1. IP version 6 has eight sections but these are commonly called \_\_\_\_\_
  - a. hexets
  - b. octets
  - c. binary
  - d. decimal

### 7.6 Internet Control Message Protocol (ICMP) :

ICMP is utilized by a gadget, similar to a switch, to speak with the wellspring of an information parcel about transmission issues. For instance, if a datagram isn't conveyed, ICMP may report this back to the host with subtleties to help perceive where the transmission turned out badly. Numerous generally utilized organization utilities depend on ICMP messages. The traceroute command can be implemented by transmitting IP datagrams with specially set IP TTL header fields, and looking for ICMP time exceeded in transit and Destination unreachable messages generated in response. The related ping utility is implemented using the ICMP echo request and echo reply messages.

ICMP utilizes the fundamental help of IP as though it were a more significant level convention; in any case, ICMP is really an indispensable piece of IP. In spite of the fact that ICMP messages are contained inside standard IP bundles, ICMP messages are typically prepared as an uncommon case, recognized from ordinary IP handling. By and large, it is important to investigate the substance of the ICMP message and convey the fitting mistake message to the application liable for communicating the IP bundle that incited the ICMP message to be sent. ICMP is a network–layer protocol. The ICMP packet is encapsulated in an IPv4 packet.

#### What is ICMP used for ?

The basic role of ICMP is for error reporting. At the point when two gadgets associate over the network, the ICMP produces errors to impart to the sending gadget if any of the information didn't get to its planned objective. For instance, if a packet of data is excessively enormous for a router, the router will drop the packet and send an ICMP message back to the first originating source for the data. An optional utilization of ICMP is to perform network diagnostics; the usually utilized terminal utilities *traceroute* and *ping* both work utilizing ICMP. The *traceroute* utility is utilized to show the routing way between two Internet gadgets. The routing way is the genuine actual way of associated switches that a solicitation should go through before it arrives at its objective. The excursion between one switch and another is known as a

'hop,' and a *traceroute* likewise reports the time needed for each hop en route. This can be helpful for deciding sources of network delay.

**How does ICMP work ?**

Not at all like the Internet Protocol (IP), ICMP isn't related with a transport layer protocol, for example, TCP or UDP. This makes ICMP a connectionless protocol: one device doesn't have to open an association with another device prior to sending an ICMP message. Typical IP traffic is sent utilizing TCP, which implies any two devices that exchange information, will initially complete a TCP handshake to guarantee the two devices are well prepared to get information. ICMP doesn't open an association thusly. The ICMP protocol likewise doesn't take into account focusing on a particular port on a device.

**❑ Check Your Progress – 5 :**

1. \_\_\_\_\_ works utilizing ICMP
  - a. traceroute
  - b. TCP
  - c. UDP
  - d. Mail

**7.7 TCP :**

TCP is one of the most important protocols of Internet Protocols suite. It is most widely used protocol for data transmission in communication network such as internet. TCP is connection oriented protocol. TCP provides full duplex communication. That is, the receiver always sends feedback about the data packet to the sender, so that the sender always has acknowledgement about whether the data packet is reached the destination or it needs to resend it. TCP guarantees that the data arrives at proposed destination in a similar order it was sent. TCP is reliable. TCP ensures that connection between two remote points be established before the actual communication happens. It supports error-checking, recovery mechanism, flow control, quality of service and end-to-end communication.

**7.7.1 TCP Header :**

The length of TCP header is minimum 20 bytes and maximum 60 bytes.

0-7	0-7	0-7	0-7
Source Port		Designation Port	
Sequence Number			
Acknowledge Number			
Data Offset	Reserved	Flags	Window Size
Options			

Source Port (16-bits) : It identifies source port of the application process on the sending device.

Destination Port (16-bits) : It identifies destination port of the application process on the receiving device.

Sequence Number (32-bits) : Sequence number of data bytes of a segment in a session.

Acknowledgement Number (32-bits) : When ACK flag is set, this number contains the next sequence number of the data byte expected and works as acknowledgement of the previous data received.

Data Offset (4–bits) : This field implies both, the size of TCP header (32–bit words) and the offset of data in current packet in the whole TCP segment.

Reserved (3–bits) : Reserved for future use and all are set zero by default.

Flags (1–bit each):

NS : Nonce Sum bit is used by Explicit Congestion Notification signalling process.

CWR : When a host receives packet with ECE bit set, it sets Congestion Windows Reduced to acknowledge that ECE received.

ECE : It has two meanings:

If SYN bit is clear to 0, then ECE means that the IP packet has its CE (congestion experience) bit set

If SYN bit is set to 1, ECE means that the device is ECT capable.

URG : It indicates that Urgent Pointer field has significant data and should be processed.

ACK : It indicates that Acknowledgement field has significance. If ACK is cleared to 0, it indicates that packet does not contain any acknowledgement.

PSH : When set, it is a request to the receiving station to PUSH data as soon as it comes to the receiving application without buffering it.

RST : Reset flag is used to refuse an incoming connection. It is used to reject a segment and restart a connection also.

SYN : This flag is used to set up a connection between hosts.

FIN : This flag is used to release a connection and no more data is exchanged thereafter. Because packets with SYN and FIN flags have sequence numbers, they are processed in correct order.

Windows Size : This field is used for flow control between two stations and indicates the amount of buffer (in bytes) the receiver has allocated for a segment, i.e. how much data is the receiver expecting.

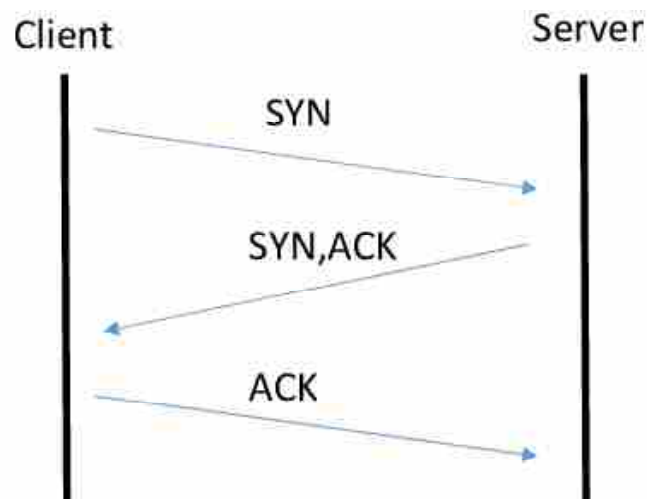
Checksum : This field contains the checksum of Header, Data, and Pseudo Headers.

Urgent Pointer : It points to the urgent data byte if URG flag is set to 1.

Options : It facilitates additional options which are not covered by the regular header. Option field is always described in 32–bit words. If this field contains data less than 32–bit, padding is used to cover the remaining bits to reach 32–bit boundary.

### **Connection Management**

TCP communication works in Server/Client model. The client initiates the connection and the server either accepts or rejects it. Three–way handshaking is used for connection management.



### **Establishment**

Client starts the association and sends the segment with a Sequence number. Server acknowledges it back with its own Sequence number and ACK of client's segment which is one more than client's Sequence number. Client in the wake of accepting ACK of its segment sends an acknowledgment of Server's response.

### **Release**

Both of server and client can send TCP segment with FIN flag set to 1. At the point when the less than desirable end reacts it back by Acknowledging FIN, that heading of TCP correspondence is shut and association is delivered.

### **Bandwidth Management**

TCP utilizes the idea of window size to oblige the need of Bandwidth management. Window size tells the sender at the remote end the number of data byte segments the receiver at this end can get. TCP utilizes moderate beginning stage by utilizing window size 1 and expands the window size dramatically after each effective correspondence. For instance, the client utilizes windows size 2 and sends 2 bytes of data. At the point when the acknowledgment of this segment got the windows size is multiplied to 4 and next the segment sent will be 4 information bytes long. At the point when the acknowledgment of 4-byte information segment is received, the client sets windows size to 8, etc. In the event that an acknowledgment is missed, for example data lost on the way network or it got NACK, at that point the window size is decreased to half and moderate beginning stage begins once more.

### **Error Control and Flow Control**

TCP utilizes port numbers to understand what application measure it needs to handover the data segment. Alongside that, it utilizes sequence numbers to synchronize itself with the remote host. All data segments are sent and received with sequence numbers. The Sender knows which last data segment was received by the receiver when it gets ACK. The receiver thinks about the last segment sent by the sender by alluding to the sequence number of as of late got packet. On the off chance that the sequence number of a segment as of late got doesn't coordinate with the sequence number the receiver was expecting, at that point it is disposed of and NACK is sent back. On the off chance that two segments show up with a similar sequence number, the TCP timestamp esteem is contrasted with settle on a choice.



## Multiplexing

The strategy to consolidate at least two data streams in a single session is called Multiplexing. At the point when a TCP client introduces a connection with Server, it always alludes to a very much characterized port number which demonstrates the application cycle. The actual client utilizes an arbitrarily created port number from private port number pools. Utilizing TCP Multiplexing, a client can speak with a number of various application measures in a solitary session. For instance, a client demands a page which thus contains various kinds of data (HTTP, SMTP, FTP and so on) the TCP session break is expanded and the session is saved open for longer time with the goal that the three-way handshake overhead can be stayed away from. This empowers the client framework to get different connection over single virtual connection. These virtual connections are bad for Servers if the break is excessively long.

## Congestion Control

When large amount of data is fed to network which is not capable of handling it, congestion occurs. TCP controls congestion by means of Window mechanism. TCP sets a window size telling the other end how much data segment to send. TCP may use three algorithms for congestion control:

Additive increase, Multiplicative Decrease

Slow Start

Timeout React

85

## Timer Management

TCP uses different types of timers to control and management various tasks :

### Keep-alive timer :

- This timer is used to check the integrity and validity of a connection.
- When keep-alive time expires, the host sends a probe to check if the connection still exists.

### Retransmission timer :

- This timer maintains stateful session of data sent.
- If the acknowledgement of sent data does not receive within the Retransmission time, the data segment is sent again.

### Persist timer :

- TCP session can be paused by either host by sending Window Size 0.
- To resume the session a host needs to send Window Size with some larger value.
- If this segment never reaches the other end, both ends may wait for each other for infinite time.
- When the Persist timer expires, the host resends its window size to let the other end know.
- Persist Timer helps avoid deadlocks in communication.

**Timed–Wait :**

- After releasing a connection, either of the hosts waits for a Timed–Wait time to terminate the connection completely.
- This is in order to make sure that the other end has received the acknowledgement of its connection termination request.
- Timed–out can be a maximum of 240 seconds (4 minutes).

**Crash Recovery**

TCP is reliable protocol. It gives sequence number to every one of byte sent in segment. It gives the input component for example at the point when a host gets a packet, it is bound to ACK that packet having the following sequence number expected (on the off chance that it isn't the last segment). At the point when a TCP Server crashes mid–way communication and re–begins its cycle, it sends TPDU broadcast to every one of its hosts. The hosts would then be able to send the last data segment which was rarely unacknowledged and convey onwards.

**❑ Check Your Progress – 6 :**

1. TCP provides \_\_\_\_\_ communication.
  - a. united
  - b. full duplex
  - c. half duplex
  - d. Single
  - e. Mail

<b>7.8 UDP :</b>
------------------

The User Datagram Protocol (UDP) is simplest Transport Layer communication protocol available of the TCP/IP protocol suite. It involves minimum amount of communication mechanism. UDP is said to be an unreliable transport protocol but it uses IP services which provides best effort delivery mechanism. In UDP, the receiver does not generate an acknowledgement of packet received and in turn, the sender does not wait for any acknowledgement of packet sent. This shortcoming makes this protocol unreliable as well as easier on processing.

Why UDP ? A question may arise, for what reason do we need an untrustworthy protocol to ship the information? We convey UDP where the affirmation packets share critical measure of bandwidth alongside the real information. For instance, if there should arise an occurrence of video web based, a huge number of packets are sent towards its clients. Acknowledging all the packets is inconvenient and may contain colossal measure of bandwidth wastage. The best conveyance instrument of hidden IP protocol guarantees best endeavours to convey its packets, yet regardless of whether a few packets in video real time get lost, the effect isn't cataclysmic and can be disregarded without any problem. Loss of few packets in video and voice traffic now and again goes unnoticed.

**UDP Header**

UDP header is as simple as its function.

0–15	16–31
Source Port	Designation Port
Length	Checksum

UDP header contains four main parameters :

1. **Source Port** : This 16 bits information is used to identify the source port of the packet.
2. **Destination Port** : This 16 bits information is used identify application level service on destination machine.
3. **Length** : Length field specifies the entire length of UDP packet (including header). It is 16–bits field and minimum value is 8–byte, i.e. the size of UDP header itself.
4. **Checksum** : This field stores the checksum value generated by the sender before sending. IPv4 has this field as optional so when checksum field does not contain any value, it is made 0 and all its bits are set to zero.

**Check Your Progress – 7 :**

1. UDP is \_\_\_\_\_ protocol.
 

a. reliable	b. bidirectional
c. connection less	d. data link layer

**7.9 Let's Sum Up :**

This unit provides details about the common protocols. The ARP protocol which is used to resolve a MAC address of destination. Transport layers protocols UDP and TCP are responsible for data transfer. TCP flags are used for network analysis also.

**7.10 Answers for Check Your Progress :**

- Check Your Progress 1 :**  
1 : a
- Check Your Progress 2 :**  
1 : a
- Check Your Progress 3 :**  
1 : c
- Check Your Progress 4 :**  
1 : a
- Check Your Progress 5 :**  
1 : a
- Check Your Progress 6 :**  
1 : b
- Check Your Progress 7 :**  
1 : c

**7.11 Glossary :**

- **TCP** : TCP (Transmission Control Protocol) is a standard that defines how to establish and maintain a network conversation through which application programs can exchange data.

## **Introduction to Computer Network**

- **UDP** : UDP (User Datagram Protocol) is a communications protocol that is primarily used for establishing low–latency and loss–tolerating connections between applications on the internet. It speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party.
- **ICMP** : ICMP is part of the Internet protocol suite as defined in RFC 792. ICMP messages are typically used for diagnostic or control purposes or generated in response to errors in IP operations (as specified in RFC 1122). ICMP errors are directed to the source IP address of the originating packet.
- **IPv4** : Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards–based internetworking methods in the Internet and other packet–switched networks. IPv4 was the first version deployed for production on SATNET in 1982 and on the ARPANET in January 1983.

### **7.12 Assignments :**

1. Discuss the Connectionless protocol
2. Explain the address resolution protocols

### **7.13 Activities :**

1. Assign static IP address to device
2. Find out the port number and protocol which is used by your email provider.

### **7.14 Case Study :**

List out the IP address and associated MAC of devices connected in LAN

### **7.15 Further Reading :**

1. Behrouz A Forouzan, Data Communications and Networking, McGraw Hill, (FourthEdition), 2007.
2. Tananbaum A.S., "Computer Networks", 3rd Ed, PHI, 199

**UNIT STRUCTURE**

- 8.0 Learning Objective
- 8.1 Introduction
- 8.2 Remote Access Protocol
  - 8.2.1 Serial Line Internet Protocol (SLIP)
  - 8.2.2 Point-to-Point Protocol (PPP) and PPPoE (Point-to-Point Protocol over Ethernet)
  - 8.2.3 Point-to-Point Tunnelling Protocol (PPTP)
  - 8.2.4 Windows Remote Access Services (RAS)
  - 8.2.5 Remote Desktop Protocol (RDP)
- 8.3 FTP
- 8.4 Hypertext Transfer Protocol
- 8.5 Hypertext Transfer Protocol Secure
- 8.6 Mailing Protocols
  - 8.6.1 POP3
  - 8.6.2 IMAP
  - 8.6.3 SMTP
  - 8.6.4 Exchange Account (EAS – Exchange ActiveSync)
- 8.7 Let's Sumup
- 8.8 Answers for check your progress
- 8.9 Glossary
- 8.10 Assignment
- 8.11 Activities
- 8.12 Case Study
- 8.13 Further Readings

**8.0 Learning Objectives :**

This unit focuses on the various network protocols. These are the protocols used for

- Remote access
- File Transfer
- Hypertext Transfer
- Mailing

**8.1 Introduction :**

This unit covers the discussion regarding the basic protocol of computer network. Remote access protocols are discussed, A remote access protocol is

a communications standard that allows your computer to talk to the remote network. If you ever intend to work from home, you will appreciate this service. After all, it enables telecommuting. **FTP** refers to a group of rules that govern how computers transfer files between systems over the internet. Hypertext Transfer Protocol (**HTTP**) is an application-layer protocol for transmitting hypermedia documents, such as HTML. Hypertext Transfer Protocol Secure (**HTTPS**) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network. Email protocol is a standard method for exchanging information between email clients. These are the major protocols discussed in this unit.

## **8.2 Remote Access Protocol :**

A remote access protocol is providing the connection facility between a remote access server and a remote computer. It's necessary for desktop sharing and remote access for help desk activities. The major remote access protocols are the

- Serial Line Internet Protocol (SLIP)
- Point-to-Point Protocol (PPP)
- Point-to-Point Protocol over Ethernet (PPPoE)
- Point-to-Point Tunneling Protocol (PPTP)
- Remote Access Services (RAS)
- Remote Desktop Protocol (RDP)

### **8.2.1 Serial Line Internet Protocol (SLIP) :**

UNIX developed SLIP as a way of transmitting TCP/IP over serial connections. SLIP available at both the data link and physical layers of the OSI model. Apart from UNIX it is also supported by other operating systems also.

SLIP is associated with a low overhead and can be used to transport TCP/IP over serial connections. You can only use it on serial connections, which is a notable restriction. The limitations of SLIP are unavailability packet addressing or error checking capabilities.

To set up SLIP for a remote connection, SLIP account is required on the host machine, as well as a batch file or script on the workstation. When you use SLIP to log in to a remote machine, you must configure a terminal mode after you've logged into the remote site. This ensures the script can enter each parameter. If you don't use a script, you'll need to establish the connection and then open a terminal window so you can manually log in to the remote access server.

### **8.2.2 Point-to-Point Protocol (PPP) and PPPoE (Point-to-Point Protocol over Ethernet) :**

PPP is a remote access protocol facilitates to implement TCP/IP. It establishes a connection via point-to-point links (i.e., dedicated leased lines and dial-up). PPP is generally used for remote connections to LANs and ISPs.

PPP utilizes the Link Control Protocol (LCP), which tests the link between client and PPP host and specifies PPP client configuration, to communicate between host and PPP client. LCP allows PPP to support authentication negotiation, in addition to compression and encryption negotiation

between the client and the server, using encryption control protocols (ECPs) and compression control protocols (CCPs). PPP can support multiple network protocols by using protocol-specific network control protocols (NPCs). Because it can run over numerous physical media types and features error-checking functionalities, PPP has almost entirely replaced SLIP.

PPP can also automatically configure TCP/IP and alternative protocol parameters via IP control protocol (IPCP) NCP. Unfortunately, one of PPP's disadvantages is it attracts a high overhead and isn't compatible with certain older configurations.

For technicians, PPP is generally considered easily configurable. Once you connect the router via PPP, it assigns all other TCP/IP parameters for you. This is usually performed with the Dynamic Host Configuration Protocol (DHCP). DHCP is a protocol within TCP/IP protocol stack that is responsible for assigning TCP/IP addressing information. This includes subnet mask, DNS configuration, and host IP address. This information can be assigned via a LAN connection or a dial-up connection. Once you connect to an ISP, the DHCP server will likely provide your IP address.

### 8.2.3 Point-to-Point Tunnelling Protocol (PPTP) :

PPTP is a remote access protocol, based on PPP, created by Microsoft. It's used to establish virtual connections across the internet via PPP and TCP/IP, enabling two networks to use the internet as their WAN link while retaining the security benefits of a private network. PPTP is a great option because it's simple and secure.

To use PPTP, It is required to set up a PPP session between the server and the client, usually over the internet. Once the session is established, you'll create a second dial-up session. This dial-up session will use PPTP to dial through the existing PPP session.

A PPTP session tunnels through an existing PPP connection, facilitating the creation of a secure session. This means you can use the internet to create a secure session between the server and the client. This type of connection is also called a virtual private network (VPN) and is less expensive than a direct connection.

PPTP is a good choice for network administrators who want to connect multiple LANs but don't want to pay for dedicated leased lines. There are, however, a few disadvantages including:

- It's not a fully accepted standard
- It's harder to set up than PPP
- It isn't available on all server types

PPTP can be implemented in two ways. You can set up a server so it acts as the gateway to the internet and is responsible for all the tunneling. This means the workstations will run normally without the need for any extra configuration. You might use this method if the aim is to connect entire networks.

The second way to use PPTP is to configure a single, remote workstation to make a connection with a corporate network via the internet. You should configure the workstation to connect via ISP, while configuring the VPN client with the VPN remote access server.

### **8.2.4 Windows Remote Access Services (RAS) :**

Windows 2000 and Windows NT let users dial up a server and connect to both the server and the server's host network. This is referred to as RAS, which is used in smaller networks where a dedicated dial-up router would not be possible or practical. With a RAS setup, you can connect a modem to a Windows 2000 or Windows NT server and configure the modem as dial-out only, dial-up only, or a combination of the two.

RAS can only provide LAN access to remote users. It doesn't let LAN users use the modem to, for example, dial their AOL account. If you want to achieve this, you'll need Microsoft's Shared Modem Services.

### **8.2.5 Remote Desktop Protocol (RDP) :**

Finally, there is the RDP, which is very similar to the Independent Computing Architecture (ICA) protocol used by Citrix products. RDP is utilized to access Windows Terminal Services, which is a close relative of the product line provided by Citrix WinFrame.

#### **❑ Check Your Progress – 1 :**

1. PPP is a remote access protocol facilitates to implement \_\_\_\_\_  
a. TCP/IP      b. UDP      c. IP      d. FTP

### **8.3 FTP :**

The File Transfer Protocol (FTP) is a common network protocol used to transfer computer files from one host to another, as would be the case when transferring data over a TCP-based network, such as the Internet. In this model, FTP is built on a client-server architecture, and separate control and data connections are set up between the client and the server.

FTP users may authenticate themselves using a clear-text sign-in protocol, which is normally done through the use of a username and password, but they can connect anonymously if the server is configured to allow it. With the increasing use of encryption in web applications, it is also increasingly important to protect FTP connections over Secure Sockets Layer (SSL/TLS) for transmission that protects the username and password, and encrypts the content (FTPS). SSH File Transfer Protocol (SFTP) is commonly used in addition to it, but it is distinctly different.

Because graphical user interfaces (GUIs) had not yet been introduced, the first FTP client applications were command-line applications developed before operating systems had GUIs, and these are still commonly shipped with most Windows, Unix, and Linux operating systems. Due to many applications having been developed since FTP has been incorporated into productivity applications, such as Web page editors, more FTP clients and automation utilities have since been developed for desktops, servers, mobile devices, and hardware.

The FTPS protocol—an extension of the commonly used File Transfer Protocol (FTP) that includes support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols—is known as FTP Secure.

FTPS should not be confused with the SSH File Transfer Protocol (SFTP), an incompatible secure file transfer subsystem for the Secure Shell (SSH)



protocol. It is also different from FTP over SSH, the practice of tunneling FTP through an SSH connection.

❑ **Check Your Progress – 2 :**

1. \_\_\_\_\_ adds support for the Transport layer security and the SSL.
  - a. FTP
  - b. TCP
  - c. FTPS
  - d. TFTP

#### 8.4 Hypertext Transfer Protocol :

The Hypertext Transfer Protocol (HTTP) is an application layer protocol for hypermedia information systems that are dispersed and collaborative. HTTP is the standard for data exchange on the World Wide Web, where hypertext texts contain links to other resources that the user can access with a mouse click or by tapping the screen in a web browser.

In the client–server computing model, HTTP is a request–response protocol. A client could be a web browser, while the server might be an application running on a machine hosting a website. The client sends the server an HTTP request message. A response message is sent to the client by the server, which offers resources such as HTML files and other content or performs other activities on the client's behalf. The message body of the answer may contain requested content as well as information about the request's completion status. A user agent is something like a web browser (UA). Indexing software used by search providers (web crawlers), voice browsers, mobile apps, and other software that accesses, consumes, or displays web material are all examples of user agents. HTTP is intended to enable or improve communication between clients and servers by allowing intermediary network nodes to participate. Web cache servers, which deliver material on behalf of upstream servers to enhance response time, are frequently used by high–traffic websites. To decrease network traffic, web browsers cache previously viewed online pages and reuse them wherever possible. By relaying messages with external servers, HTTP proxy servers at private network boundaries can make communication easier for clients without a globally routable address. The HTTP protocol is an application layer protocol that is part of the Internet protocol suite. Its definition presupposes the usage of a reliable transport layer protocol, which is usually Transmission Control Protocol (TCP). HTTPU and the Simple Service Discovery Protocol, for example, can be extended to use unreliable protocols like the User Datagram Protocol (UDP) (SSDP). Uniform Resource Locators (URLs) use the Uniform Resource Identifiers (URI's) schemes http and https to identify and locate HTTP resources on the network. URIs are encoded as hyperlinks in HTML texts, as defined by RFC 3986, to create connected hypertext documents. The original HTTP (HTTP/1.0) has been updated to HTTP/1.1. Every resource request in HTTP/1.0 requires a separate connection to the same server. After the page has been sent, HTTP/1.1 can reuse a connection to download images, scripts, stylesheets, and other data. As a result, HTTP/1.1 communications have a lower latency than TCP connections since TCP connections include a lot of overhead. Tim Berners–Lee started the development of HTTP at CERN in 1989. The Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) collaborated on the early HTTP Requests for Comments (RFCs), with work eventually passing to the IETF.

❑ **Check Your Progress – 3 :**

1. Tim Berners-Lee started the development of HTTP at \_\_\_\_\_ in 1989
  - a. Bell
  - b. MIT
  - c. CERN
  - d. ISRO

---

<b>8.5 Hypertext Transfer Protocol Secure :</b>
---

Hypertext Transfer Protocol Secure (HTTPS) is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS) or, formerly, Secure Sockets Layer (SSL). The protocol is therefore also referred to as HTTP over TLS, or HTTP over SSL.

The authentication of the accessed website, as well as the privacy and integrity of the exchanged data while in transit, are the primary objectives for HTTPS. It defends against man-in-the-middle attacks, and bidirectional encryption protects communications between a client and a server from eavesdropping and alteration. HTTPS authentication necessitates the signing of server-side digital certificates by a trustworthy third party. Due to the high cost of this operation, fully authenticated HTTPS connections were previously exclusively found on secure financial transaction services and other secure corporate information systems on the Internet. The protocol gained traction in 2016 because to a campaign coordinated by the Electronic Frontier Foundation and supported by web browser developers. HTTPS is increasingly more commonly used by web users than HTTP, principally to ensure page authenticity on all types of websites, secure accounts, and keep user communications, identity, and web browsing secret.

Over an unsecured network, HTTPS creates a secure channel. If appropriate encryption suites are used and the server certificate is validated and trusted, this provides reasonable security against eavesdroppers and man-in-the-middle attacks. Because HTTPS encrypts the entire HTTP protocol by piggybacking it on top of TLS, the entire HTTP protocol can be encrypted. The request URL (which web page was requested), query parameters, headers, and cookies are all part of this (which often contain identifying information about the user). HTTPS, on the other hand, cannot protect the publication of website addresses and port numbers because they are required to be part of the underlying TCP/IP protocols. In reality, this means that eavesdroppers can infer a user's IP address and port number, as well as the amount of data sent and the length of the communication, even from a properly configured web server. HTTPS is extremely critical when using insecure networks or networks that could be tampered with. Insecure networks, such as public Wi-Fi access points, enable anyone on the same local network to sniff packets and uncover sensitive data that isn't protected by HTTPS. Furthermore, some free and paid WLAN networks have been spotted meddling with webpages by using packet injection to broadcast their own advertisements on other websites. This approach can be used maliciously in a variety of ways, including putting malware onto websites and stealing users' personal data.

Malicious Tor nodes could otherwise destroy or alter the information travelling through them in an insecure manner, and introduce malware into the connection, hence HTTPS is especially important for communications using

the Tor anonymity network. One of the reasons the Electronic Frontier Foundation and the Tor project developed HTTPS Everywhere, which is included in the Tor Browser Bundle, is to address this issue. As more information regarding worldwide mass monitoring and criminals stealing personal information becomes available, the usage of HTTPS security on all websites, regardless of the type of Internet connection utilised, is becoming increasingly crucial. Even if metadata on individual websites visited by a user isn't considered sensitive, when aggregated, it can reveal a lot about the user and endanger their privacy. HTTP/2 (or its precursor, the now-deprecated protocol SPDY) is a new generation of HTTP meant to reduce page load times, size, and latency. It can be used with HTTPS. To protect consumers from man-in-the-middle attacks, such as SSL stripping, it is advised to employ HTTP Strict Transport Security (HSTS) with HTTPS. HTTPS should not be confused with the RFC 2660-specified Secure HTTP (S-HTTP), which is rarely used.

### Difference from HTTP

HTTPS URLs begin with "https://" and use port 443 by default, whereas, HTTP URLs begin with "http://" and use port 80 by default. Because HTTP isn't encrypted, it's subject to man-in-the-middle and eavesdropping attacks, which can give hackers access to website accounts and sensitive data, as well as modify webpages to inject malware or adverts. HTTPS is built to withstand such attacks and is deemed secure in this regard (with the exception of HTTPS implementations that use deprecated versions of SSL).

### ☐ Check Your Progress – 4 :

1. \_\_\_\_\_ is an extension of the Hypertext Transfer Protocol (HTTP).
  - a. HTTPS
  - b. SHHTTP
  - c. TCP
  - d. UDP

## 8.6 Mailing Protocols :

There are multiple protocols which are involved in mail transfer and management. It could be extremely confusing if one is not familiar of what protocols exist for emails. Also, each of this protocol performs slightly different functionality. The commonly used protocols are– IMAP, POP3, SMTP, and Exchange. These are not many protocol types one would go over while getting to an email client. The protocol subtleties can be gotten to through the server settings dependent on the email client being utilized.

### 8.6.1 POP3 :

POP3 stands for Post Office 3 protocol. POP simply reaches out to the mail server and brings back the mail contents. This is a straightforward yet normalized way which permits clients to get to mailboxes and rapidly download messages to their gadget.

With POP3, users can configure the server settings. This can be used to allow mail copies to be left on the server or move all emails without leaving any copy on the server. This is usually configurable in most cases. The main advantage of POP3 is the low dependency over the Internet. Users can download all emails and read them at leisure even if they are accessing this offline.

The way these emails are stored in local depends on the email client. For instance, Outlook utilizes .pst, while Thunderbird uses .mbox. This is a good option in case you choose to read emails offline. Apart from this, this helps you reduce the server space by storing messages locally.

The default ports for POP3 are :

- Port 110 – This is the default non–encrypted port.
- Port 995 – This is the default port for secure connections.

### **8.6.2 IMAP :**

This stands for Internet Message Access Protocol. This again is a standard protocol for accessing emails and is a client/server protocol. Unlike POP, this does not move the emails. The biggest difference between POP3 and IMAP is the mail sync up. POP3 assumes that a user will be connected to a single device. However, IMAP is suitable for different devices simultaneously.

Internet connectivity is required while using IMAP. When a user accesses the mailbox, the user is actually connected to an external server. In case of multiple user it is more beneficial IMAP can work over a relatively low internet connection since it only downloads email messages from the server when a user has requested to read a specific email.

The default ports for IMAP are :

- Port 143 – This is the default non–encrypted port.
- Port 993 – This is default port for secure connections.

### **8.6.3 SMTP :**

This stands for Simple Mail Transfer Protocol. This is a standard protocol for sending emails over the Internet. This is a protocol which is used by a Mail Transfer Agent to deliver emails to a recipient's email server. This is a protocol which defines mail sending and cannot be used for mail receiving.

SMTP is the most commonly used protocol for mail transfer between two servers. It does not require no authentication to function, unlike POP3 and IMAP. Certain Internet Service Providers block the default port 25 of SMTP. In such cases, the mail server also provides an alternate secondary port.

The default port for SMTP are :

- Port 25 – This is the default non–encrypted port.
- Port 465/ 587 – This is default port for secure connections.

### **8.6.4 Exchange Account (EAS – Exchange ActiveSync) :**

This is used by Exchange servers like Microsoft Exchange. This not only syncs mail but also syncs contacts, calendars, notes and everything in the outlook. The advantage is that users can have a synced copy of the calendar, contacts over multiple device.

#### **❑ Check Your Progress – 5 :**

1. \_\_\_\_\_ is the most commonly used protocol for mail transfer between two servers  
a. SMTP                      b. POP3                      c. IAMP                      d. EAS
2. In IMAP, \_\_\_\_\_ is default port for secure connections  
a. 143                      b. 993                      c. 25                      d. 465

### 8.7 Lets Sum Up :

#### In this unit we have learned

- Remote access protocols
  - Serial Line Internet Protocol (SLIP)
  - Point-to-Point Protocol (PPP)
  - Point-to-Point Protocol over Ethernet (PPPoE)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Remote Access Services (RAS)
  - Remote Desktop Protocol (RDP)
  - File transfer protocols, the discussion is regarding FTP and SFTP
- To transfer the text, image, audio over internet the HTTP and HTTP Secure is also discussed
- The different mailing protocols like SMTP, POP3 IMAP and EAS have also covered in this unit.

### 8.8 Answers for Check Your Progress :

#### Check Your Progress 1 :

1 : a

#### Check Your Progress 2 :

1 : c

#### Check Your Progress 3 :

1 : c

#### Check Your Progress 4 :

1 : a

#### Check Your Progress 5 :

1 : a                      2 : b

### 8.9 Glossary :

- **Remote Access Protocols :** The Remote Desktop Protocol (RDP) is a protocol, or technical standard, for using a desktop computer remotely.
  - Serial Line Internet Protocol (SLIP)
  - Point-to-Point Protocol (PPP)
  - Point-to-Point Protocol over Ethernet (PPPoE)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Remote Access Services (RAS)
  - Remote Desktop Protocol (RDP)
- **FTP :** The File Transfer Protocol (FTP) is a common network protocol used to transfer computer files from one host to another
- **The Hypertext Transfer Protocol (HTTP)** is an application layer protocol for hypermedia information systems that are dispersed and collaborative. HTTP is the standard for data exchange on the World Wide Web, where hypertext texts contain links to other resources.

## **Introduction to Computer Network**

- **Hypertext Transfer Protocol Secure (HTTPS)** is an extension of the Hypertext Transfer Protocol (HTTP). It is used for secure communication over a computer network, and is widely used on the Internet.
- **Mailing protocols** are the protocols which are involved in mail transfer and management.
- **POP3** stands for Post Office 3 protocol. POP simply reaches out to the mail server and brings back the mail contents
- **IMAP** stands for Internet Message Access Protocol
- **SMTP** is a standard protocol for sending emails over the Internet.

### **8.10 Assignment :**

1. Compare the various remote access protocols
2. List out the reserve ports for various mailing protocols

### **8.11 Activities :**

1. Access your friend's computer from your computer using remote desktop tool
2. Set up an FTP server and allow remote user to download resources available on FTP server

### **8.12 Case Study :**

1. Find out the limitations of HTTPS

### **8.13 Further Reading :**

1. Computer Networks | Fifth Edition | By Pearson Author: Andrew S. Tanenbaum
2. Data Communications and Networking | Fifth Edition | By McGraw Hill Education Author: Behrouz A. Forouzan
3. TCP/IP Protocol Suite | Fourth Edition | By McGraw Hill Education Author: Behrouz A. Forouzan

## **BLOCK SUMMARY :**

This block was written so that those readers who need information quickly are able to find it instantly, and those who wish to learn more advanced topics can even read deeper into each unit and further into the chapters. Books reference list was also provided at the end of each unit in order to help those students who wish to learn more more due to their interest in that very line.

The book begins with an overview of writer, discussing about the LAN AND WAN.

Efforts were made by the writer as you get further into a chapter you will learn more about LAN AND WAN, their role and capabilities, but often you will be able to head directly to the topic you wish to learn about.

Sufficient diagrams were even used wherever it was felt appropriate by the writer, and where according to him readers may find it helpful related to the theory, including reference to certain documents that you will be able to get from the books incase you need to study more about the topics.

<b>BLOCK ASSIGNMENT :</b>
---------------------------

❖ **Short Questions :**

**Define the following terms :**

1. Point-to-point protocol
2. Wan devices
3. HDLC
4. Circuit switching
5. Packet switching
6. Frame relay
7. WAN configuration
8. Ping
9. DNS proxy
10. SNMP
11. SSL
12. IP address
13. SPP
14. IP
15. Repeater
16. TCP/IP



❖ **Long Questions :**

1. Describe the type of mediaaccess used by Token Ring.
2. Describe unicast, multicast and broadcast transmissions.
3. How do you maintain forwarding and outgoing connection ?

**Introduction to  
Computer Network**

❖ **Enrolment No. :**

1. How many hours did you need for studying the units ?

Unit No.	4	5	6	7	8
No. of Hrs.					

2. Please give your reactions to the following items based on your reading of the block :

Items	Excellent	Very Good	Good	Poor	Give specific example if any
Presentation Quality	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Language and Style	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Illustration used (Diagram, tables etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Conceptual Clarity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Check your progress Quest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Feed back to CYP Question	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____

3. Any other Comments

.....

.....

.....

.....

.....

.....

.....

.....



**BAOU**  
Education  
for All

**Dr. Babasaheb Ambedkar  
Open University Ahmedabad**

**BCAR-301**

# **INTRODUCTION TO** **COMPUTER NETWORK**

---

## **BLOCK 3 : NETWORK OS AND NETWORK MANAGEMENT**

---

UNIT 9 NETWORK OPERATING SYSTEMS

UNIT 10 NETWORK MANAGEMENT

UNIT 11 HIGH SPEED NETWORKING

# ***NETWORK OS AND NETWORK MANAGEMENT***

## **Block Introduction :**

In this block the whole content has been divided into three units. The first unit covers the topic Network Operating Systems and has been discussed in very detail, whereas the second unit covers the topic Network Management which has even been discussed in detail. The writer in the book has tried his best to explain the topics and the third unit covers the topic High Speed Networking. The writer has kept the language of the book very simple in order to make it more understandable.

As already discussed in earlier blocks that the writer has written the content such that those who need information quickly are able to find what they need, and those who wish to learn more advanced topics can read deeper into each units and further into the chapters.

The book begins with an overview of writer, discussing about the Network OS and network management.

It is possible to read this block of the book like any other book (from beginning to end). Each chapter begins with an introduction about the block and further discussion of the contents it contains. As you get further into a chapter you will learn more about Networking OS and about the management of network and also about their role and capabilities, but often you will be able to head directly to the topic you wish to learn about.

We will also use diagrams where appropriate, and where we believe readers may find it helpful we will discuss some related theory, including reference to certain documents that you will be able to get from the books in case you need to study more about the topics.

## **Block Objectives :**

**After learning this block, you will be able to understand :**

- About the networking OS and concepts of Networking.
- WINS/NBNS, Work group and domains.
- What are multiple trust models?
- Routers and also its function.
- Network management platform and its function.
- Network latency.
- Bandwidth and cables, DSL and cable speed.
- Downloading and uploading.

## **Block Structure :**

**Unit 9 : Network Operating Systems**

**Unit 10 : Network Management**

**Unit 11 : High Speed Networking**

# *NETWORK OPERATING SYSTEMS*

## **UNIT STRUCTURE**

- 9.0 Learning Objectives
- 9.1 Introduction
- 9.2 Windows NT Workstation
- 9.3 Browsing
- 9.4 NetBIOS Interface to Application Programs
- 9.5 WINS/NBNS (Windows Internet Name Service/NetBIOS Name Service)
- 9.6 NetBIOS Over TCP/IP
- 9.7 Workgroup
- 9.8 Multiple Master Domain Model
- 9.9 Multiple Trust Models
- 9.10 Windows Server Application
- 9.11 Let Us Sum Up
- 9.12 Answers for Check Your Progress
- 9.13 Glossary
- 9.14 Assignment
- 9.15 Activities
- 9.16 Case Study
- 9.17 Further Readings

### **9.0 Learning Objectives :**

After learning this unit, you will be able to understand :

- Networking operating system
- Networking concepts
- WINS/NBNS
- Work group and domains
- Multiple trust model

### **9.1 Introduction :**

Windows for workgroups was superseded in late 1995 by windows 95–Microsoft's first attempt at a 32-bit consumer operating system. Windows 95's networking components were a great deal more comprehensive than those of windows for workgroups.

Windows 95 included NetBEUI, the flat namespace non-routable protocol that Microsoft used for very small networks, an IPX compatible protocol that Microsoft used for very small networks, an IPX compatible protocol for use with Novell Netware networks and a surprisingly capable IP stack.

## **9.2 Windows NT Workstation :**

Windows NT is a family of operating systems developed by Microsoft, the first version of which was released in July 1993. It was originally designed to be a powerful high-level-language-based, processor-independent, multiprocessing, multiuser operating system with features comparable to UNIX. It was intended to complement consumer versions of Windows that were based on MS-DOS.

NT was the first fully 32-bit version of Windows, whereas its consumer-oriented counterparts, Windows 3.1x and Windows 9x, were 16-bit/32-bit hybrids. Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Home Server, Windows Server 2008 and Windows 7 are based on Windows NT, although they are not branded as Windows NT.

Although various Microsoft publications, including a 1998 question-and-answer session with Bill Gates, reveal that the letters "NT" were expanded to "New Technology" for marketing purposes, they originally stood for "N-Ten," the codename of the Intel i860 XR processor, for which NT was initially developed. However, they no longer carry any specific meaning.

### **❑ Check Your Progress – 1 :**

1. \_\_\_\_\_ was the first fully 32-bit version of Windows.
  - a. NT
  - b. 98
  - c. 2000

## **9.3 Browsing :**

Browsing is the method of viewing the resources available on a network. The browse list on a Windows network is the list of other hosts and domains available on a network. Windows maintains the browse list to present other hosts offering network services through a point-and-click user interface rather than asking users to remember the names of remote hosts and services.

Windows clients use the browse list to construct the view of the network shown in the Network Neighborhood (renamed My Network Places in Windows XP and Windows 2000) and Windows Explorer. The browse list is also accessible from the command line using the NET VIEW command.

Windows NT® domains maintain the browse list on a computer called the Master Browser. Whenever a computer offers a network service for the first time, it broadcasts a server announcement packet. The Master Browser receives this packet and adds the computer's name to its browse list. In response, the Master Browser transmits a list of backup browsers to the new computer.

Each domain or workgroup contains at least one backup browser. A copy of the browse list is maintained on the backup browser to eliminate the need to rebuild the browse list if the Master Browser goes down.

### **CIFS**

Common Internet File System protocol (CIFS) provides an open cross-platform mechanism for client systems to request file services from server systems over a network. It is based on the SMB (Server Message Block) protocol widely used by PCs and workstations running a wide variety of operating systems.

## **NetBIOS**

NetBIOS or Network Basic Input/output System, is a vendor-independent network interface originally designed for IBM® PC computer systems running PC-DOS or MS-DOS.

NetBIOS is a software interface, not an actual networking protocol. It specifies the services that should be available without putting any restrictions on the protocol used to implement those services.

No officially defined NetBIOS standard exists. The original version, as described by IBM in 1984 in the IBM PC Network Technical Reference Manual, is treated as the de facto standard. Since its introduction, the following versions of NetBIOS have emerged, each using its own transport protocol: NetBEUI, NetBIOS over IPX and NetBIOS over TCP/IP.

### **❑ Check Your Progress – 2 :**

1. \_\_\_\_\_ is the method of viewing the resources available on a network.
  - a. Browsing
  - b. CIFS
  - c. Internet

## **9.4 NETBIOS Interface to Application Programs :**

On PCs, NetBIOS includes both– a set of services and an exact program interface to those services. The following types of NetBIOS services exist:

### **Name Service**

NetBIOS resources are referenced by name. Lower-level addresses are not available to NetBIOS applications. An application representing a resource registers one or more names that it wants to use.

The name space is flat and not hierarchically organized. It uses 15 alphanumeric characters, plus a 16th "subcode" byte. Names cannot start with an asterisk (\*).

Registration implies bidding for use of a name. The bid may be for exclusive (unique) or shared (group) ownership. Each application contends with other applications in real time. No two applications on the NetBIOS network can use the same unique name until the originating application requests that its name be deleted or the host is powered off or reset.

Name Service provides the Add Name, Add Group Name and Delete Name primitive operations.

### **Session Service**

A session is a full-duplex, sequenced and reliable message exchange conducted between a pair of NetBIOS applications. Data is organized into messages.

Multiple sessions can exist between any two applications. Both applications participating in the session have access to the name of the remote application. No specification is given for resolving session requests to a group name into a data connection. A service is provided for the detection of a session failure by an application.

The Session Service provides the Call, Listen, Hang Up, Send, Receive and Session Status primitive operations.

### **Datagram Service**

The Datagram Service is an unreliable, non-sequenced and connectionless communication between two NetBIOS applications. It is analogous to UDP service under TCP/IP.

Datagrams are sent under cover of a name properly registered to the sender.

Datagrams can be sent to a specific name or be explicitly broadcast.

Datagrams sent to an exclusive name are received, if at all, by the holder of that name. Datagrams sent to a group name are multicast to all holders of that name. The sending application cannot distinguish between group and unique names and thus must act as if all non-broadcast datagrams are multicast.

As with the Session Service, the receiver of the datagram is provided with the sending and receiving names.

The Datagram Service provides the Send Datagram, Send Broadcast Datagram, Receive Datagram and Receive Broadcast Datagram primitive operations.

### **NetBIOS Name Resolution**

Mapping a NetBIOS name to its corresponding IP address: The techniques commonly used for name resolution are the Windows Internet Name Service (WINS), the LMHOSTS file and the domain name system (DNS).

#### **❑ Check Your Progress – 3 :**

1. \_\_\_\_\_ includes both– a set of services and an exact program interface to those services.
  - a. NetBIOS
  - b. Session service
  - c. Name service

<b>9.5 WINS/NBNS (Windows Internet Name Service/NetBIOS Name Service) :</b>
---

When a new service is made available on the network, such as when a Windows machine boots or when AIX® Fast Connect is started, the service must be registered with a WINS (Windows Internet Name Service) server before it can be available to clients located on other subnets.

The WINS server records the name of the host, the NT domain the host is part of and the IP address of the host. Whenever a machine attempts to resolve a host name, it first checks with the WINS server. If the host is not registered there, it attempts to find the host using a broadcast. If the host is still not found, the system returns the message: "A computer or share name could not be found." AIX® Fast Connect registers itself with any WINS server.

WINS also includes a method for replicating its database of host names with other WINS servers to create a backup WINS server that can host queries if the primary WINS server is unavailable. It also allows large networks that are encumbered by slow links to distribute WINS servers closer to clients and provide faster name resolution. (WINS is a proprietary Microsoft protocol.)

AIX® Fast Connect can be configured to act as an NBNS (NetBIOS Name Service) server, providing most WINS functionality. AIX® Fast Connect can also be configured to act as a WINS proxy to other WINS or NBNS servers.



## **LMHOSTS**

LMHOSTS (Lan Manager Hosts) is analogous to the UNIX® / etc. / hosts file. The LMHOSTS file allows specific NetBIOS server names to be mapped to IP addresses. It also provides syntax for defining the domain in which a NetBIOS server resides, as well as loading an LMHOSTS file from a shared directory on a server.

### **Broadcast**

NetBIOS names may be resolved using broadcast on the local subnet. It is analogous to address resolution protocol (ARP) in TCP/IP. The requesting machine broadcasts a NetBIOS Name Query. If the requested host receives the broadcast, it replies with its IP address. Because broadcasts are not forwarded, only hosts on local subnets may be resolved in this manner.

### **❑ Check Your Progress – 4 :**

1. Whenever a machine attempts to resolve a host name, it first checks with the \_\_\_\_\_.  
a. WINS server    b. LAN                    c. Internet

## **9.6 NetBIOS Over TCP/IP :**

NetBIOS over TCP/IP was first proposed in RFCs 1001 and 1002. These RFCs describe an implementation of NetBIOS using Transmission Control Protocol (TCP) for connection-oriented session services and User Datagram Protocol (UDP) for datagram services.

This design has some significant advantages over NetBEUI and NetBIOS over IPX, as follows:

- NetBIOS uses the existing TCP/IP protocols, so it can be routed across the global Internet and any other wide area networks.
- Software implementing the NetBIOS interface can be built using existing TCP/IP implementation without requiring any new network drivers. As most operating systems already support TCP/IP, most are capable of supporting NetBIOS with minimal additional effort.

### **NetBIOS Scope**

NetBIOS scope means population of computers across which a registered NetBIOS name is known. NetBIOS broadcast and multicast datagram operations must reach the entire extent of the NetBIOS scope.

### **Net Command**

The net command and its subcommands can be used to configure and administer the AIX® Fast Connect Server from the command line. Alternatively, the Web-based System Manager and SMIT offer menu-driven interfaces for the same tasks.

### **Pass through Authentication**

This is a mechanism employed by the AIX® Fast Connect server to validate user credentials with a domain controller and, if validated, to grant the user access to a resource on the AIX® Fast Connect server.

### **SMB**

Server Message Block protocol is used to run on NetBIOS to implement Windows file sharing and print services.

With this protocol, clients exchange messages (called server message blocks) with a server to access resources on that server. Every SMB message has a common format, consisting of a fixed-sized header followed by a variable-sized parameter and data component.

**SMB messages are of the following types :**

- Session control messages start, authenticate and terminate sessions. File and printer messages control file and printer access respectively. Message commands allow an application to send or receive messages to or from another host.
- When an SMB client negotiates a connection with an SMB server, the two parties determine a common protocol to use for communication. This capability allows protocol extensions but can make SMB quite complex.

**Shares**

This refers to resources exported to the network by the AIX® Fast Connect server. AIX® Fast Connect supports AIX® file shares and printer shares.

**Check Your Progress – 5 :**

1. \_\_\_\_\_ protocol is used to run on NetBIOS to implement Windows file sharing and print services.
  - a. Server Message Block
  - b. SMS
  - c. MMS

**9.7 Workgroups :**

Workgroups can be referred to as logical collection of workstations and servers that do not belong to a domain. In a workgroup, every computer stores its own copy of user- and group-account information. Therefore, in workgroups, users can merely log directly in to machines on which they have accounts. Workgroup members are able to view and use resources on the other systems. To do this, resources are shared in the workgroup and network users are validated by the machine owning the resource.

**A Workgroup might refer to :**

- A peer-to-peer computer network (computer networking)
- A group of people working together towards a common goal, also known as a working group
- A courtroom workgroup, an informal arrangement between a criminal prosecutor, criminal defence attorney and the judicial officer

**Deciding between Workgroups and Domains**

This section contains information that will help you decide whether to place your servers in a workgroup or a domain. It also contains other information that will help with basic planning of the roles of servers within the domain, if you create a domain.

For information about upgrading servers in a domain where all domain controllers run Windows NT 4.0, see Upgrades in a Windows NT 4.0 Domain. For information about upgrading servers in a domain containing one or more Windows 2000 domain controllers, see Upgrades in a domain containing Windows 2000 domain controllers. For information about networks larger than five servers, see the Windows Server 2003 Deployment Kit at the Microsoft Windows Server System Web site.

### **Workgroups Compared with Domains**

A domain is a group of accounts and network resources that share a common directory database and set of security policies and might have security relationships with other domains. A workgroup is a more basic grouping, intended only to help users find objects such as printers and shared folders within that group. Domains are the recommended choice for all networks except very small ones with few users.

In a workgroup, users might have to remember multiple passwords, one for each network resource. (In addition, different users can use different passwords for each resource.) In a domain, passwords and permissions are simpler to keep track of, because a domain has a single, centralized database of user accounts, permissions and other network details.

The information in this database is replicated automatically among domain controllers. You determine which servers are domain controllers and which are simply members of the domain. You can determine these roles not only during Setup but afterward as well.

Windows 2000 is a line of operating systems produced by Microsoft for use on personal computers, business desktops, laptops and servers. It was released on 17 February 2000. It was the successor to Windows NT 4.0 and is the final release of Microsoft Windows to display the "Windows NT?" designation. It was succeeded by Windows XP for desktop systems in October 2001 and Windows Server 2003 for servers in April 2003. Windows Me was released seven months after Windows 2000 and one year before Windows XP, but Windows Me was not intended to be, nor did it serve as the successor to Windows 2000.

Windows Me was designed for home use, while Windows 2000 was designed for business.

Four editions of Windows 2000 were released: Professional, Server, Advanced Server and Datacenter Server. Additionally, Microsoft sold Windows 2000 Advanced Server Limited Edition and Windows 2000 Datacenter Server Limited Edition, which were released in 2001 and run on 64-bit Intel Itanium microprocessors.

While each edition of Windows 2000 was targeted towards a different market, they share a core set of features, including many system utilities such as the Microsoft Management Console and standard system administration applications.

All versions of the operating system support the Windows NT file system, NTFS 3.0, the Encrypting File System, as well as basic and dynamic disk storage. The Windows 2000 Server family has additional features including the ability to provide Active Directory services (a hierarchical framework of resources), Distributed File System (a file system that supports sharing of files) and fault-redundant storage volumes.

Windows 2000 can be installed through either a manual or an unattended installation. Unattended installations rely on the use of answer files to fill in installation information and can be performed through a bootable CD using Microsoft Systems Management Server by the System Preparation Tool.

Microsoft marketed Windows 2000 as the most secure Windows version ever, but it became the target of a number of high-profile virus attacks such

as Code Red and Nimda. For ten years after its release, it continued to receive patches for security vulnerabilities nearly every month until reaching the end of its lifecycle on 13 July 2010.

❑ **Check Your Progress – 6 :**

1. \_\_\_\_\_ can be referred to as logical collection of workstations and servers that do not belong to a domain.
  - a. WORKGROUPs
  - b. Work stations
  - c. Nodes

**9.8 Multiple Master Domain Model :**

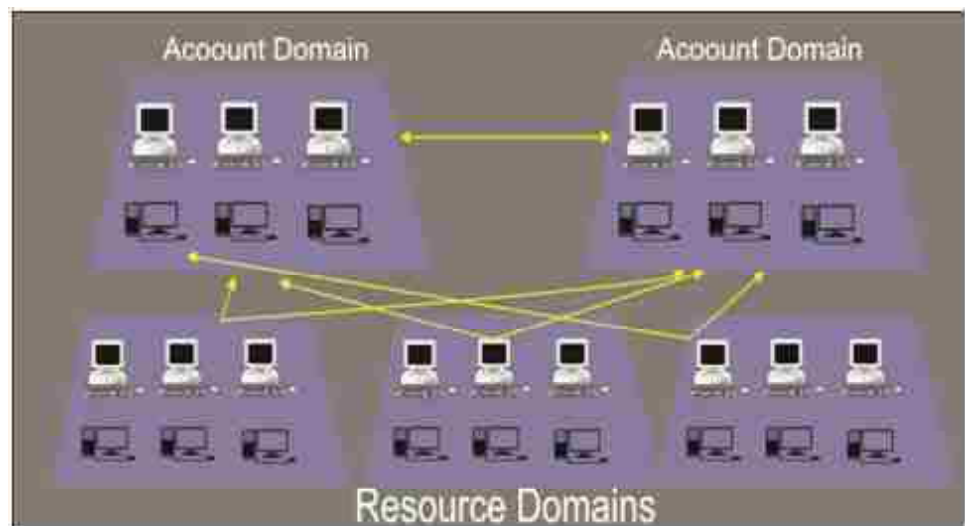
This model combines two or more master domain models. Each master domain handles user accounts, with a user having an account on one of the master domains. Two-way trusts are established between each master domain, so that all master domains trust each other.

Resource domains provide the resources for the users in the master domains. By creating global groups in the master domains, these are then imported in the local groups in the resource domains to allow master domain users access.

A user will logon to the master domain where his account resides. Due to the trust relations established between the master domains, this can occur anywhere on the network. Each master domain should contain two or more BDCs to provide redundancy and validate user logon requests [one BDC per 2000 users]. Each master domain can contain as many as 26,000 user accounts.

**The multiple master domain is suited for :**

- Organizations with 40,000 or more users
- Users who need to logon at different parts of the network [mobile users]
- Scalable networks
- Centralized user accounts via mis yet decentralized resource administration on a local level



**Fig. 9.1 : Multiple Master Domain**

❑ **Check Your Progress – 7 :**

1. \_\_\_\_\_ domains provide the resources for the users in the master domains.
  - a. Resource
  - b. Multi master

## 9.9 Multiple Trust Models :

In multiple trust models, all domains trust all other domains to create a web of trust relationships. This model rapidly becomes unmanageable as it grows larger because of its essentially peer to peer relationship among domains. It also completely decentralizes administration, which undercuts the purpose of domain hierarchies.

Another reason why the multiple trust models are not recommended is their relative lack of security. It is a great network if you can trust all your users all the time and closely control access to the network.

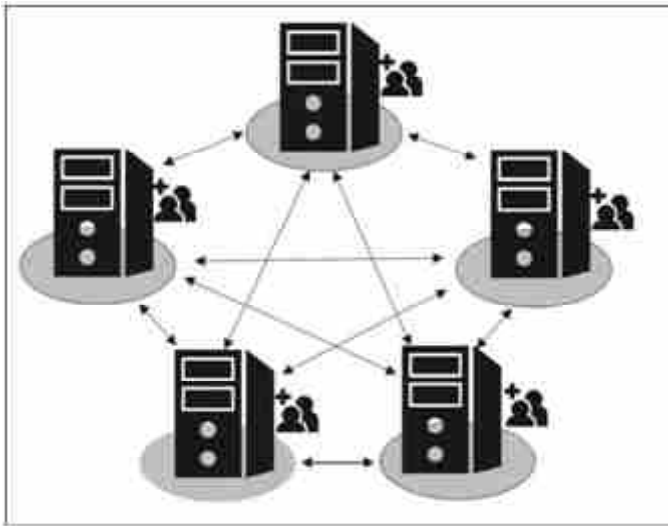


Fig. 9.2 : Data Transfer

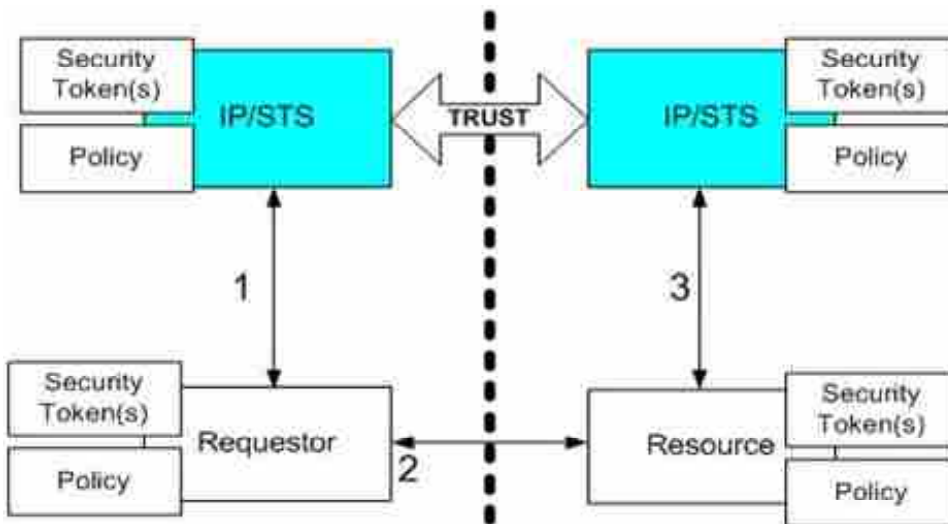


Fig. 9.3 : Security System

### Security

Microsoft stopped providing security updates for Windows NT 4.0 Workstation on 30 June 2004 and Windows NT 4.0 Server on 31 December 2004 due to major security flaws, including Microsoft Security Bulletin MS03-010, which, according to Microsoft, could not be patched without significant changes to the core operating system.

Between June 2003 and June 2007, 127 security flaws were identified and patched in Windows 2000 Server, many of which might also affect Windows NT 4.0 Server; however, Microsoft does not test security bulletins against unsupported software

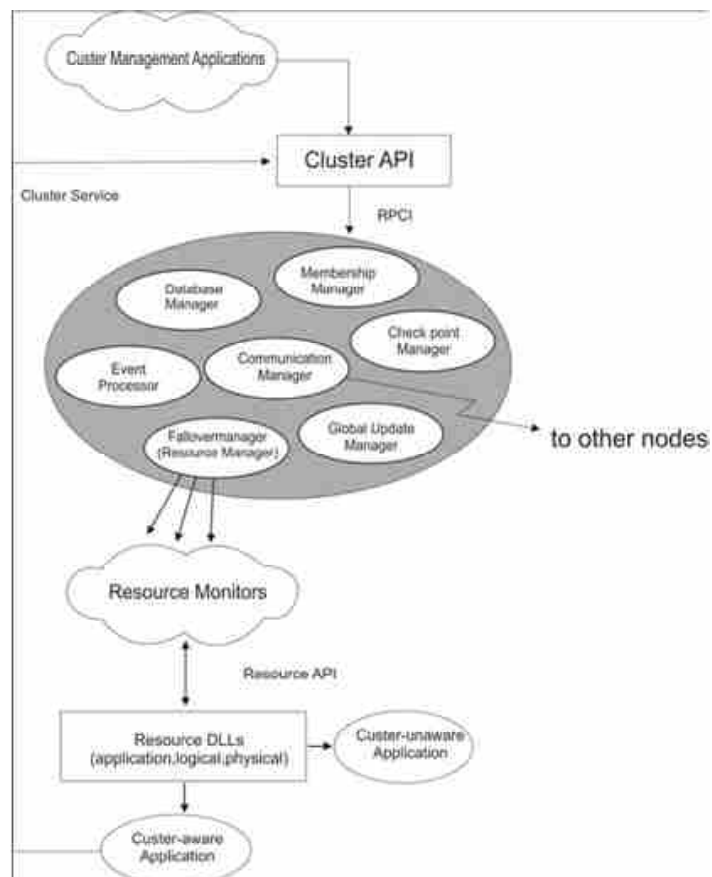
❑ **Check Your Progress – 8 :**

1. In \_\_\_\_\_, all domains trust all other domains to create a web of trust relationships.
  - a. multiple trust models
  - b. resource

**9.10 Windows Server Application :**

Microsoft has created an all in one server package called back-office that provides most of the administrative functions a network requires. It consists of the following :

- **Exchange Server :** a group ware and messaging server that can handle internet complaint emails
- **SQL Server :** a database management system that is quite robust
- **Systems Management Server (SMS) :** a network management package that enables administrators to install software and provide remote technical support to users
- **Systems Network Architecture Server (SNA Server) :** which enables windows 2000 to connect to IBM midrange and mainframe computers
- **Internet Information Server :** which turns an NT server into an Internet server for the World Wide Web, FTP, Gopher and other services NT server also comes with a complete set of TCP/IP tools. Windows 2000 server, right out of the box without any third party software, can be domain name server for the internet– a dynamic host configuration protocol server that assigns client work stations their IP addresses or a PPP dial in server through the use of remote access services. NT has built in remote dial up networking services.



**Fig. 9.4 : Client Management Applications**

**Advantages of Domains over Workgroups**

1. Centralized administration of user accounts.
2. Centralized management of domain resources (drivers, printers and so on).
3. Strong increase in security.
4. A great deal of control over the amount of access to shared resources.

**❑ Check Your Progress – 9 :**

1. A database management system that is quite robust.
  - a. SQL server
  - b. Exchange server

**9.11 Let Us Sum Up :**

To meet the needs of different users, Microsoft has designed two different PC desktop operating systems. Users and MIS managers want to know details about how these operating systems differ and how the differences will affect them in the short and long term. Microsoft's Desktop Operating System Strategy compares Windows 95 to Windows NT Workstation version 3.5 in key functional areas, helping organizations choose the right operating system for their needs.

Windows 95 is designed for office workers and home PC users and runs on PCs with minimal resources, such as a 386 machine with 4 megabytes of RAM. To run applications like spreadsheets and word processors, this system is simple to use and hides underlying complexities when possible.

Windows NT Workstation is a powerful and secure operating system, designed for software developers, scientists, statisticians and financial professionals. This operating system implements a number of security measures to protect data and supports high-end hardware systems as well.

Many organizations find the security available with Windows 95 to be more than adequate for their needs. Users can protect data using share-level security for peer-to-peer network configurations, while user-level security is available when server-based networks are used.

With Windows NT Workstation, local files are protected by secure logon, a secure file system and user rights. Users must have both a valid user name and logon password to access the machine and its resources. Windows NT Workstation protects its resources with user-level security and can specify access permissions all the way to the file level.

In addition, Windows NT Workstation can force users to change their passwords periodically and a system administrator can grant or deny a user's ability to load specific files or access other computers. It also conforms to stringent C2-level security specifications, providing protection for organizations with exacting security needs.

**9.12 Answers for Check Your Progress :**

**❑ Check Your Progress 1 :**

1 : a

**❑ Check Your Progress 2 :**

1 : a

- ❑ **Check Your Progress 3 :**  
1 : a
- ❑ **Check Your Progress 4 :**  
1 : a
- ❑ **Check Your Progress 5 :**  
1 : a
- ❑ **Check Your Progress 6 :**  
1 : a
- ❑ **Check Your Progress 7 :**  
1 : a
- ❑ **Check Your Progress 8 :**  
1 : a
- ❑ **Check Your Progress 9 :**  
1 : a

### **9.13 Glossary :**

1. **Network :** A system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables: used to transmit or receive information.

### **9.14 Assignment :**

1. What are the advantages of domains over workgroups ?
2. Explain the multiple trust model.

### **9.15 Activities :**

1. Explain multiple master domain model.
2. What are windows server applications ?

### **9.16 Case Study :**

Discuss the features of a network operating system

### **9.17 Further Readings :**

1. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001
2. Sams Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002



**UNIT STRUCTURE**

- 10.0 Learning Objectives**
- 10.1 Introduction**
- 10.2 Function and Characteristics**
- 10.3 Routers**
- 10.4 Network Management**
- 10.5 Fault Management**
- 10.6 Network Management Platform**
- 10.7 Troubleshooting Infrastructure**
- 10.8 Fault Detection and Notification**
- 10.9 Proactive Fault Monitoring and Notification**
- 10.10 Configuration Management**
  - 10.10.1 Configuration Standards**
  - 10.10.2 Configuration File Management**
- 10.11 Let Us Sum Up**
- 10.12 Answers for Check Your Progress**
- 10.13 Glossary**
- 10.14 Assignment**
- 10.15 Activities**
- 10.16 Case Study**
- 10.17 Further Readings**

**10.0 Learning Objectives :**

**After learning this unit, you will be able to understand :**

- Routers and its function
- Network management
- Network management platform and its function
- Trouble shooting and fault detection
- Configuration management
- Configuration file management

**10.1 Introduction :**

A web-based integrated network management system is applicable to management of both large-scale and small-scale business networks. The system provides a full range of network management functions as well as a friendly graphical user interface. It is capable of managing multi-vendor network devices in the IP networks simultaneously and efficiently. It has been proven that the

Rinpoche system is a perfect solution to managing heterogeneous networks that consist of diverse devices.



**Fig. 10.1 : Network Management System**

## **10.2 Functions and Characteristics :**

The various functions of network management system are discussed below :

### **Secure Network Administration :**

1. Supports user authentication.
2. Supports SSL communication between client and server.
3. Supports user authorisation with several privileges and read/write access control.
4. Audits the events of user log in and configuration change.

### **Event and Alarm Management :**

1. Supports tools for querying, tracking, and handling network events.
2. Supports various ways of alarm notifications, alarms can be notified by mobile short message, pager message, email, colour change, text display, and audible sounds.
3. Supports personalised alarm notification scheduling.

### **Abundant network management functions and friendly Graphical User Interface :**

1. Conforms to SNMP.
2. Discovers network devices and elements automatically.
3. Detects network events in real time.
4. Collects a variety of network data, such as circuit performance, traffic usage, bandwidth utilization, operational status...etc. periodically.
5. Supports real-time monitoring.
6. Provides a simple and user-friendly web graphical user interface.
7. Provides a unified working style of managing diverse devices.
8. Displays the overall network status and network health on a single window.

**Ample Network Management Reports :**

1. Provides plentiful summary reports including reports of traffic usage, and width utilisation, circuit performance, network availability and network events.
2. Is able to send reports to users by email immediately or on a daily, weekly or monthly schedule.

**Advanced Management Functions for Customisation and Extension (Professional Edition) :**

1. Supports SNMP MIB browser.
2. Provides advanced functions that can be used to monitor any SNMP managed objects, detect the corresponding events and generate the summary reports.
3. Can be customised to apply to many specific network management applications rapidly.

**Management Functions for Monitoring Application Services**

1. Provides monitoring and management functions for Internet services, including HTTP, FTP, SMTP, POP3, DNS, LDAP, TCP, and UDP.
2. Supports Microsoft SQL Server monitoring capabilities.

**Distributed Hierarchical Management Architecture**

1. It can be applied in the management of large-scale networks by adopting a single global-NMS and a set of subordinate NMSs.
2. Each individual NMS can operate independently and take the responsibility of managing a specific network domain.
3. The Global-NMS keeps a global view of the whole network. It collects and summarises network information from all subordinate NMSs.
4. Devices and elements in the network can be managed by several NMSs at the same time to enhance the fault tolerance.
5. Detail management information stored in subordinate NMSs can be accessed via the Global-NMS directly.

**❑ Check Your Progress – 1 :**

1. \_\_\_\_\_ can be applied in the management of large-scale networks by adopting a single global-NMS and a set of subordinate NMSs.
  - a. Distributed Hierarchical Management Architecture
  - b. LAN
  - c. WAN

**10.3 Routers :**

A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network or if the data packet must be transferred from one network to another. When multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

A router is a networking device whose software and hardware are customized to the tasks of routing and forwarding information. A router has two or more network interfaces, which may be two different physical types of network (such as copper cables, fiber, or wireless) or different network standards. Each network interface is a specialized device that converts electric signals from one form to another.

Routers connect two or more logical subnets, each having a different network address. The subnets in the router do not necessarily map one-to-one to the physical interfaces of the router. The term "layer 3 switching" is often used interchangeably with the term "routing". The term switching is generally used to refer to data forwarding between two network devices with the same network address. This is also called layer 2 switching or LAN switching.

**Conceptually, a router operates in two operational planes (or sub-systems) :**

1. **Control Plane :** Where a router builds a table (called routing table) as how a packet should be forwarded through which interface, by using either statically configured statements (called static routes) or by exchanging information with other routers in the network through a dynamic routing protocol.
2. **Forwarding Plane :** Where the router actually forwards traffic (called packets in IP) from ingress (incoming) interfaces to an egress (outgoing) interface that is appropriate for the destination address that the packet carries with it, by following rules derived from the routing table that has been built in the control plane.

**□ Check Your Progress – 2 :**

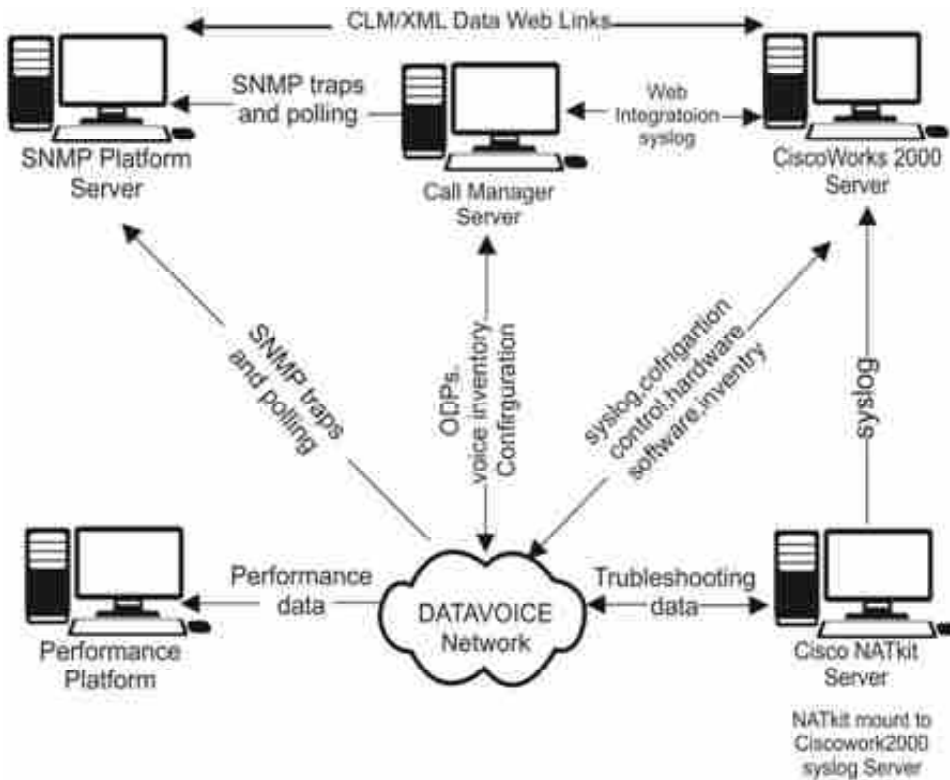
1. A \_\_\_\_\_ is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them.  
a. ROUTER      b. LAN      c. WAN

**10.4 Network Management :**

The ISO network management model's five functional areas are listed below.

- **Fault Management :** Detect, isolate, notify, and correct faults encountered in the network.
- **Configuration Management :** Configuration aspects of network devices such as configuration file management, inventory management, and software management.
- **Performance Management :** Monitor and measure various aspects of performance so that overall performance can be maintained at an acceptable level.
- **Security Management :** Provide access to network devices and corporate resources to authorised individuals.
- **Accounting Management :** Usage information of network resources.

The following diagram shows a reference architecture that Cisco Systems believes should be the minimal solution for managing a data network. This architecture includes a Cisco Call Manager server for those who plan to manage Voice over Internet Protocol (VoIP) : The diagram shows how you would integrate the Call Manager server into the NMS topology.



**Fig. 10.2 : Network Management System Topology**

**The network management architecture includes the following :**

- Simple Network Management Protocol (SNMP) platform for fault management.
- Performance monitoring platform for long term performance management and trending.
- CiscoWorks2000 server for configuration management, syslog collection, and hardware and software inventory management.

Some SNMP platforms can directly share data with the CiscoWorks2000 server using Common Information Model/eXtensible Markup Language (CIM/XML) methods. CIM is a common data model of an implementation-neutral schema for describing overall management information in a network/enterprise environment. CIM is comprised of a specification and a schema.

The specification defines the details for integration with other management models such as SNMP MIBs or Desktop Management Task Force Management Information Files (DMTF MIFs), while the schema provides the actual model descriptions.

**❑ Check Your Progress – 3 :**

1. \_\_\_\_\_ Detect, isolate, notify, and correct faults encountered in the network.
  - a. Fault Management
  - b. Configuration management

## **10.5 Fault Management :**

In network management, fault management is the set of functions that detect, isolate, and correct malfunctions in a telecommunications network. These functions compensate for environmental changes and include maintaining and examining error logs, accepting and acting on error detection notifications, tracing and identifying faults, carrying out sequences of diagnostics tests, correcting faults, reporting error conditions. They also localize and trace faults by examining and manipulating all database information.

When a fault or event occurs, a network component will often send a notification to the network operator using a protocol such as SNMP. An alarm is a persistent indication of a fault that clears only when the triggering condition has been resolved. A current list of problems occurring on the network component is often kept in the form of an active alarm list such as is defined in RFC 3877, the Alarm MIB. A list of cleared faults is also maintained by most network management systems.

A fault management console allows a network administrator or system operator to monitor events from multiple systems and perform actions based on this information.

There are two primary ways to perform fault management – active and passive. Passive fault management is done by collecting alarms from devices (normally via SNMP) when something happens in the devices. In this mode, the fault management system only knows if a device it is monitoring is intelligent enough to generate an error and report it to the management tool. However, if the device being monitored fails completely or locks up, it will not raise an alarm and the problem will not be detected. Active fault management addresses this issue by actively monitoring devices via tools such as PING to determine if the device is active and responding. If the device stops responding, active monitoring will throw an alarm showing the device as unavailable and allows for the proactive correction of the problem.

### **❑ Check Your Progress – 4 :**

1. \_\_\_\_\_, the fault management system only knows if a device is monitoring is intelligent enough to generate an error and report it to the management tool.
  - a. Active
  - b. Passive

## **10.6 Network Management Platform :**

A network management platform deployed in the enterprise manages an infrastructure that consists of multivendor network elements. The platform receives and processes events from network elements in the network. Events from servers and other critical resources can also be forwarded to a management platform. The following commonly available functions are included in a standard management platform :

- Network discovery
- Topology mapping of network elements
- Event handler
- Performance data collector and grapher
- Management data browser

Network management platforms can be viewed as the main console for network operations in detecting faults in the infrastructure. The ability to detect problems quickly in any network is critical. Network operations personnel can rely on a graphical network map to display the operational states of critical network elements such as routers and switches.

Network management platforms such HP Open View, Computer Associates Unicenter, and SUN Solstice can perform a discovery of network devices. Each network device is represented by a graphical element on the management platform's console. Different colours on the graphical elements represent the current operational status of network devices.

Network devices can be configured to send notifications, called SNMP traps, to network management platforms. Upon receiving the notifications, the graphical element representing the network device changes to a different color depending on the severity of the notification received. The notification, usually called an event, is placed in a log file.

A number of network management platforms are capable of managing multiple geographically distributed sites. This is accomplished by exchanging management data between management consoles at remote sites with a management station at the main site.

The main advantage of a distributed architecture is that it reduces management traffic, thus, providing a more effective usage of bandwidth. A distributed architecture also allows personnel to manage their networks from remote sites with systems locally.

A recent enhancement to management platforms is the ability to manage network elements using a web interface remotely. This enhancement eliminates the need for special client software on individual user stations to access a management platform.

A typical enterprise consists of different network elements. However, each device normally requires vendor-specific element management systems in order to manage the network elements effectively. Therefore, duplicate management stations might be polling network elements for the same information.

The data collected by different systems is stored in separate databases, creating administration overhead for users. This limitation has prompted networking and software vendors to adopt standards such as Common Object Request Broker Architecture (CORBA) and Computer-Integrated Manufacturing (CIM) to facilitate the exchange of management data between management platforms and element management systems.

With vendors adopting standards in management system development, users can expect interoperability and cost savings in deploying and managing the infrastructure.

CORBA specifies a system that provides interoperability between objects in a heterogeneous, distributed environment and in a manner that is transparent to the programmer. Its design is based on the Object Management Group (OMG) object model.

❑ **Check Your Progress – 5 :**

1. \_\_\_\_\_ design is based on the Object Management Group (OMG) object model.
  - a. CORBA
  - b. TFTP

## **10.7 Troubleshooting Infrastructure :**

Trivial File Transfer Protocol (TFTP) and system log (syslog) servers are crucial components of a troubleshooting infrastructure in network operations. The TFTP server is used primarily for storing configuration files and software images for network devices. Routers and switches are capable of sending system log messages to a syslog server. The messages facilitate the troubleshooting function when problems are encountered. Occasionally, Cisco support personnel need the syslog messages to perform root cause analysis.

The CiscoWorks2000 Resource Management Essentials (Essentials) distributed syslog collection function allows for the deployment of several UNIX or NT collection stations at remote sites to perform message collection and filtering. The filters can specify which syslog messages will be forwarded to the main essentials server. A major benefit of implementing distributed collection is the reduction of messages forwarded to the main syslog servers.

### **❑ Check Your Progress – 6 :**

1. Occasionally, \_\_\_\_\_ support personnel need the syslog messages to perform root cause analysis.
  - a. CISCO
  - b. TFTP

## **10.8 Fault Detection and Notification :**

The purpose of fault management is to detect, isolate, notify, and correct faults encountered in the network. Network devices are capable of alerting management stations when a fault occurs on the systems. An effective fault management system consists of several subsystems.

Fault detection is accomplished when the devices send SNMP trap messages, SNMP polling, remote monitoring (RMON) thresholds, and syslog messages. A management system alerts the end user when a fault is reported and corrective actions can be taken.

Fault detection and monitoring of network elements can be expanded from the device level to the protocol and interface levels. For a network environment, fault monitoring can include Virtual Local Area Network (VLAN), asynchronous transfer mode (ATM), fault indications on physical interfaces, and so forth. Protocol-level fault management implementation is available using an element management system such as the CiscoWorks2000 Campus Manager. The Traffic Director application in Campus Manager focuses on switch management utilizing mini-RMON support on Catalyst switches.

With an increasing number of network elements and complexity of network issues, an event management system that is capable of correlating different network events (syslog, trap, log files) may be considered. This architecture behind an event management system is comparable to a Manager of Managers (MOM) system.

A well-designed event management system allows personnel in the network operations center (NOC) to be proactive and effective in detecting and diagnosing network issues. Event prioritisation and suppression allow network operation personnel to focus on critical network events, investigate several event management systems including the Cisco Info Centre, and conduct a feasibility analysis to fully explore the capabilities of such systems.



**❑ Check Your Progress – 7 :**

1. The purpose of \_\_\_\_\_ is to detect, isolate, notify, and correct faults encountered in the network.
  - a. fault management
  - b. traffic director

**10.9 Proactive Fault Monitoring and Notification :**

RMON (Remote Monitoring) alarm and event are two groups defined in the RMON specification. Normally, a management station performs polling on network devices to determine the status or value of certain variables. For example, a management station polls a router to find out the central processing unit (CPU) utilization and generates an event when the value reaches a configured threshold. This wastes network bandwidth and can miss the actual threshold depending on the polling interval.

With RMON alarm and events, a network device is configured to monitor itself for rising and falling thresholds. At a predefined time interval, the network device will take a sample of a variable and compare it against the thresholds. An SNMP trap can be sent to a management station if the actual value exceeds or falls below the configured thresholds. RMON alarm and event groups provide a proactive method of managing critical network devices.

**❑ Check Your Progress – 8 :**

1. With \_\_\_\_\_, a network device is configured to monitor itself for rising and falling thresholds.
  - a. RMON alarm and events
  - b. CPU

**10.10 Configuration Management :**

The goal of configuration management is to monitor network and system configuration information so that the effects on network operation of various versions of hardware and software elements can be tracked and managed.

**10.10.1 Configuration Standards :**

With an increasing number of network devices deployed, it is critical to be able to identify the location of a network device accurately. This location information should provide a detailed description meaningful to those tasked with dispatching resources when a network problem occurs.

To expedite a resolution if a network problem occurs, make certain to have available contact information of the person or department responsible for the devices. Contact information should include telephone number and the name of the person or department.

Naming conventions for network devices, starting from device name to individual interface, should be planned and implemented as part of the configuration standard. A well-defined naming convention provides personnel with the ability to provide accurate information when troubleshooting network problems.

The naming convention for devices can use geographical location, building name, floor, and so forth. For the interface naming convention, it can include the segment to which a port is connected, name of connecting hub, and so forth. On serial interfaces, it should include actual bandwidth, local data link connection identifier (DLCI) number (if frame relay), destination, and the circuit ID or information provided by the carrier.

### **10.10.2 Configuration File Management :**

When you add new configuration commands on existing network device needs, you must verify the commands for integrity before actual implementation takes place. An improperly configured network device can have a disastrous effect on network connectivity and performance. Configuration command parameters must be checked to avoid mismatches or incompatibility issues. It is advisable to schedule a thorough review of configurations with Cisco engineers on a regular basis.

A fully functional CiscoWorks2000 Essentials allows for backing up configuration files on routers and Cisco Catalyst switches automatically. The security feature of essentials can be used to perform authentication on configuration changes.

A change audit log is available to track changes and the user name of individuals issuing changes. For configuration changes on multiple devices, two options are available: the web-based NetConfig in the current version of CiscoWorks2000 Essentials or the cwconfig script.

These functions can be accomplished with the configuration management tools in CiscoWorks2000 Essentials:

- Push configuration files from the Essentials configuration archive to a device or multiple devices.
- Pull the configuration from the device to the Essentials archive.
- Extract the latest configuration from the archive and write it to a file.
- Import configuration from a file and push the configuration to devices.
- Compare the last two configurations in the Essentials archive.
- Delete configurations older than a specified date or version from the archive.
- Copy the startup configuration to the running configuration.

#### **❑ Check Your Progress – 9 :**

1. A fully functional \_\_\_\_\_ Essentials allows for backing up configuration files on routers and Cisco Catalyst switches automatically.
  - a. Windows 2000
  - b. CiscoWorks2000

### **10.11 Let Us Sum Up :**

A web-based integrated network management system is applicable to management of both large-scale and small-scale business networks.

The system provides a full range of network management functions as well as a friendly graphical user interface.

It is capable of managing multi-vendor network devices in the IP networks simultaneously and efficiently.

It has been proven that the Rinpoche system is a perfect solution to managing heterogeneous networks that consist of diverse devices.

A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them.

Some SNMP platforms can directly share data with the CiscoWorks2000 server using Common Information Model/eXtensible Markup Language (CIM/XML) methods.

CIM is a common data model of an implementation-neutral schema for describing overall management information in a network/enterprise environment.

In network management, fault management is the set of functions that detect, isolate, and correct malfunctions in a telecommunications network.

These functions compensate for environmental changes and include maintaining and examining error logs, accepting and acting on error detection notifications, tracing and identifying faults, carrying out sequences of diagnostics tests, correcting faults, reporting error conditions.

They also localize and trace faults by examining and manipulating database information.

A fault management console allows a network administrator or system operator to monitor events from multiple systems and perform actions based on this information.

There are two primary ways to perform fault management – active and passive.

The purpose of fault management is to detect, isolate, notify, and correct faults encountered in the network.

RMON(Remote Monitoring) alarm and event are two groups defined in the RMON specification.

Normally, a management station performs polling on network devices to determine the status or value of certain variables.

### **10.12 Answers for Check Your Progress :**

- Check Your Progress 1 :**  
1 : a
- Check Your Progress 2 :**  
1 : a
- Check Your Progress 3 :**  
1 : a
- Check Your Progress 4 :**  
1 : b
- Check Your Progress 5 :**  
1 : a
- Check Your Progress 6 :**  
1 : a
- Check Your Progress 7 :**  
1 : a
- Check Your Progress 8 :**  
1 : a
- Check Your Progress 9 :**  
1 : a

### **10.13 Glossary :**

1. **Repeater** : A network or communications device which propagates electrical signals from one cable to another, amplifying them to restore them to full strength in the process. Repeaters are used to counter the attenuation which occurs when signals travel long distances.
2. **Router** : A device which forwards packets between networks. The forwarding decision is based on network layer information and routing tables, often constructed by routing protocols.
3. **Socket** : The Berkeley Unix mechanism for creating a virtual connection between processes. Sockets interface Unix's standard I/O with its network communication facilities. They can be of two types, stream (bi-directional) or datagram (fixed length destination-addressed messages). The socket library function socket() creates a communications end-point or socket and returns a file descriptor with which to access that socket. The socket has associated with it a socket address, consisting of a port number and the local host's network address.

### **10.14 Assignment :**

1. Explain configuration management.
2. Explain how configuration management differs from configuration file management.

### **10.15 Activities :**

1. Explain fault detection mechanism
2. How is fault management different from fault monitoring ?

### **10.16 Case Study :**

Discuss fault detection and troubleshooting mechanisms

### **10.17 Further Readings :**

1. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001
2. Sams Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002

**UNIT STRUCTURE**

- 11.0 Learning Objectives
- 11.1 Introduction
- 11.2 The Need for Speed Tests
  - 11.2.1 Network Latency
  - 11.2.2 Latency vs Bandwidth
  - 11.2.3 Latency of Satellite Internet Service
  - 11.2.4 Measuring Network Latency
- 11.3 Benchmarking the Testing Services
- 11.4 Methodology
- 11.5 Text File Download
- 11.6 Image Download
- 11.7 DSL and Cable Speeds
- 11.8 Cable Speed : How fast is Cable Modem Internet ?
- 11.9 DSL Speed of Downloading and Uploading
- 11.10 Let Us Sum Up
- 11.11 Answers for Check Your Progress
- 11.12 Glossary
- 11.13 Assignment
- 11.14 Activities
- 11.15 Case Study
- 11.16 Further Readings

**11.0 Learning Objectives :**

After learning this unit, you will be able to understand :

- Network latency
- Bandwidth and cables
- DSL and cable speed
- Downloading and uploading
- Latency of satellite internet service

**11.1 Introduction :**

In computer networking, the term bandwidth refers to the rate of data transfer. Very often the bandwidth numbers one sees and hears represent theoretical or peak performance of a device. A 100 Mbps Ethernet adapter installed in a computer with a slow processor, for example, rarely exceeds 10 Mbps in actual performance. Traditional dial-up modems, advertised as capable of 56 Kbps, never actually perform at that rate in practice.

The term speed is often used synonymously with data rate in networking. Technically speaking, speed refers to the user-perceived performance of the network application. Speed correlates positively with bandwidth in many cases, but not always.

Web browsers, for example, may perform "slowly" on a high-bandwidth network for several reasons, such as a bottleneck at the Web server or at one's ISP. Those who have upgraded from traditional dial-up to broadband may already be familiar with the phenomenon. It is common to attribute performance problems to a "low network" even though the local area data transfer rates (when transfers occur) remain high.

## **11.2 The Need for Speed Tests :**

Network performance depends on many factors. To help a person understand the state of their network, modern operating systems support various performance monitoring mechanisms. Though useful, these features tend to drastically oversimplify or "dumb down" the analysis of network performance.

### **11.2.1 Network Latency :**

Bandwidth is just one element of what a person perceives as the speed of a network. Latency is another element that contributes to network speed. The term latency refers to any of the several kinds of delays typically incurred in processing network data. A so-called low latency network connection is one that generally experiences small delay times, while a high latency connection generally suffers from long delays.

### **11.2.2 Latency Vs Bandwidth :**

Although the theoretical peak bandwidth of a network connection is fixed according to the technology used, the actual bandwidth you will obtain varies over time. The bandwidth is affected by high latencies. Excessive latency creates bottlenecks that prevent data from filling the network pipe, thus decreasing effective bandwidth. The impact of latency on network bandwidth can be temporary (lasting a few seconds) or persistent (constant) depending on the source of the delays.

### **11.2.3 Latency of Satellite Internet Service :**

Satellite Internet service illustrates the difference between latency and bandwidth on computer networks. Satellite Internet connections possess both high bandwidth and high latency. When loading a Web page, for example, most satellite users can observe a noticeable delay from the time they enter a Web address to the time the page begins loading. This high latency is primarily due to propagation delay as the request message travels at the speed of light to the distant satellite station and back to the home network. Once the messages arrive on Earth, however, the page loads quickly like on other high-bandwidth Internet connections (DSL or cable).

Besides propagation delays, latency may involve transmission delays (properties of the physical medium) and processing delays (such as passing through proxy servers or making network hops on the Internet).





### **11.2.4 Measuring Network Latency :**

Network tools like ping tests and trace route measure latency by determining the time it takes a given network packet to travel from source to destination

and back, the so-called round-trip time. Round-trip time is not the only way to specify latency, but it is the most common.

On DSL or cable Internet connections, latencies of less than 100 milliseconds (ms) are typical and less than 25 ms desired. Satellite Internet connections, on the other hand, average 500 ms or higher latency.

**Dial-Up Networking (DUN) Traffic States**

NONE	SEND	RECEIVE	SEND AND RECEIVE
			

The dynamic icon appears again on the DUN status page, shown below. This page reveals more session parameters, including connection state and duration, total bytes sent and received, errors and compression ratios.

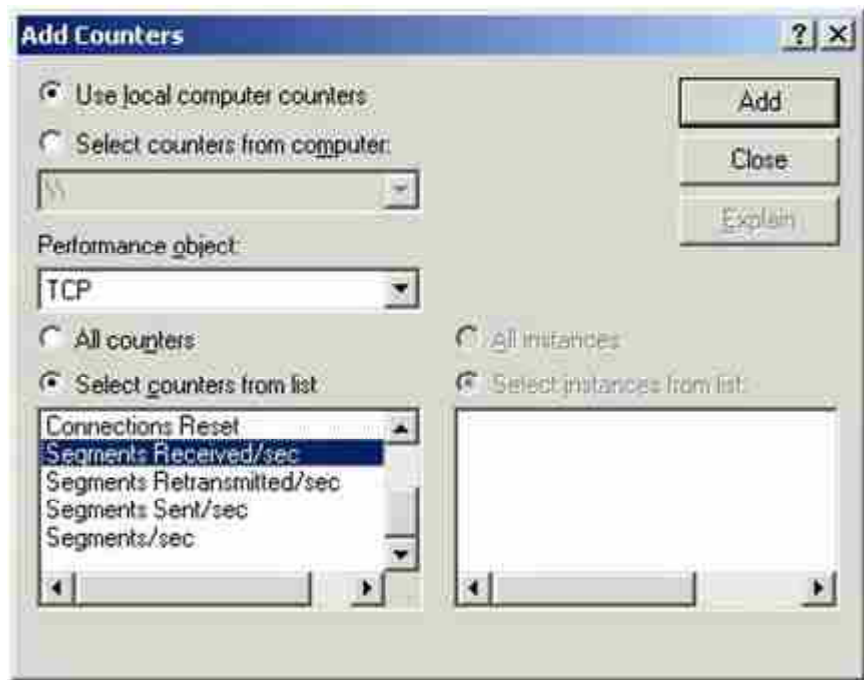
**Dial-Up Networking Status Window**



Marked in red for illustrative purposes, the speed entry in the status window displays a data rate of 21.6 Kbps. This same statistic also appears in the DUN tooltips displayed at connect time (left) and throughout the life of the connection (right).

Windows receives this statistic from the modem at the time the modem protocol establishes the connection. The number represents the expected performance of the connection, not based on any data transfer history but rather on the design of the protocol in use. On the positive side, data compression can result in much higher speeds than reported by Windows DUN. Compression works especially well with large amounts of text, such as HTML pages, though it handles images and other binary data much less effectively. Compressed data obviously cannot magically increase one's bandwidth but it can utilise the same bandwidth more intelligently, resulting in higher user-perceived speed.

**Windows Performance Monitor**

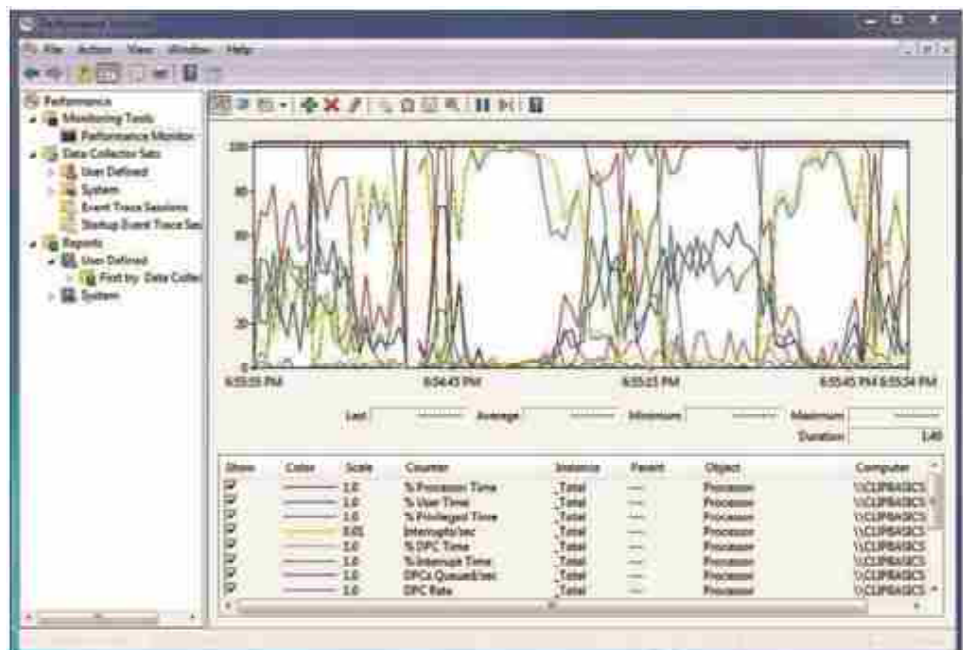


**Network groups contain counters such as the following :**

- Datagrams, segments, packets or bytes sent and/or received
- Number of active/established/passive/reset connections
- Error/failure counts

Compared to Dial-Up Networking, where statistics are displayed and are updated automatically, performance monitors display no data automatically and require a fair amount of configuration time and effort to extract data in the form of strip charts.

**Windows Performance Monitor Chart**





### The Speed Test Alternative

Tools such as Dial-Up Networking and Performance Monitor offer good insight into a computer's network performance. However, these tools generally lack two key features :

- Measure of performance at the application level rather than the network protocol level
- Ability to create a synthetic (artificially controlled) workload

Online speed testers generally offer both these features. A typical speed testing service allows one to specify their connection type (traditional dial-up, broadband and so on) and a workload, usually represented by a file download of a fixed size.

To the extent speed testers actually "work", they serve as a useful complement to other network monitoring tools.

#### □ Check Your Progress – 1 :

1. The term \_\_\_\_\_ refers to any of the several kinds of delays typically incurred in processing network data.
  - a. Latency
  - b. bandwidth

### 11.3 Benchmarking the Testing Services :

Almost all computers these days have a network connection of some description. Whether it is a modem connection to an ISP or an Ethernet connection to a corporate intranet, sending and receiving data to and from other computers is an essential part of day to day operations. A myriad of applications use TCP/IP networking technology – Email, Web browsers and games to name a few popular applications. In most cases, there is one performance factor the user is most concerned with – the speed or transfer rate.

The PassMark Advanced Network Test (which is part of Performance Test) is designed to test the data transfer rate between two computers both of which must be running Performance Test. One of the computers must act as the server and will sit waiting for a connection. The other computer acts as a client. It connects to the server machine and sends data to it for the duration of the test.

The network benchmark test will work with any type of TCP/IP connection. Including ethernet, dial up modems, ADSL, cable modems, local area networks (LAN), Wide area networks (WAN) and wireless networking (WiFi). The software has been optimized to use a minimum amount of CPU time, allowing even high speed gigabit ethernet connections to be benchmarked.

#### **Users have the ability to change the following test parameters.**

- The IP address of the machine acting as the server and the port number used for the test to help with firewall issues.
- The size of the data block used for each send request. It is also possible to select variable sized blocks to measure performance deltas as block size increases or decreases.
- The duration of the test.
- The protocol, either TCP or UDP. The TCP protocol is when data integrity is important (Errors are corrected using data re-transmission). UDP is

used with applications that are tolerant to data loss such as video streaming.

❑ **Check Your Progress – 2 :**

1. The \_\_\_\_\_ Advanced Network Test is designed to test the data transfer rate between two computers.
  - a. PassMark
  - b. ADSL
  - c. TCP

**11.4 Methodology :**

The evaluation employed a V.90 standard 56Kbps modem and Internet access via EarthLink, a reliable ISP in the USA. Tests were conducted at off-peak hours (between 1:00 AM and 2:00 AM EDT) on a week-day (Wednesday 9 May 2001). These parameters were chosen because they represent a common configuration with minimal Internet service disruptions.

**Toast.net Configuration**

Toast.net presents several configuration options on its main page as shown below. First, a person may enter the name of their ISP in the text field. Toast.net apparently uses this data for tracking purposes only; the field may be left blank or any nonsense value can be entered without affecting the results of the test.

**Toast.Net Configuration – ISP/Connection Type**

**Enter Your ISP:**

**Connection Type:**

Next, a person selects their connection type from the list as shown below. These choices represent the variety of connections that Toast.net should be able to analyse. As with the ISP setting, Toast.net provides this option for tracking purposes only.

**Toast.Net Configuration – Supported Connection Types**

Select Connection Type

- 33.6K Modem
- 56K Modem**
- 64K ISDN
- 128K ISDN
- Satellite
- Cable Modem
- ADSL
- T1 or Faster

Finally, a person must specify the Web server to be used in the test. As shown below, Toast.net offers several choices optimised for their customers. As a non-customer, the choice of Web server can still affect test results, due to geographic location or server load, as is true with all speed tests of this type. For benchmark purposes, these tests used the Toast.net Basic Hosting option.

<b>Web Server</b>
TOAST.net (Deluxe Hosting)
TOAST.net (Basic Hosting)
Interland (Atlanta, GA)
Buckeye Express (Toledo, OH)
WebJump (Staten Island, NY)
CISP (Toledo, OH)

**Test Runs**

For dial-up connections, Toast.net provides two workloads – a single large text file and a single large image. Toast.net also provides two additional workloads suited to high-speed broadband connections – a very large text file and a streaming video. A series of trials were run for each of the two dial-up workloads.

**Toast.Net Configuration – Test Workloads**

<b>TOAST.net</b> (Basic Web Hosting)	<a href="#">Text (340K)</a>
	<a href="#">Broadband Text (1,000K)</a>
	<a href="#">Image (225K)</a>
	HTTP Streaming Video <a href="#">100Kb/s</a> <a href="#">250Kb/s</a> <a href="#">700Kb/s</a> (Is your connection fast enough to play the clip?)

**Check Your Progress – 3 :**

1. For dial-up connections, Toast.net provides two workloads – a single large text file and a \_\_\_\_\_.
  - a. single large image
  - b. single small image
  - c. single small text file

**11.5 Text File Download :**

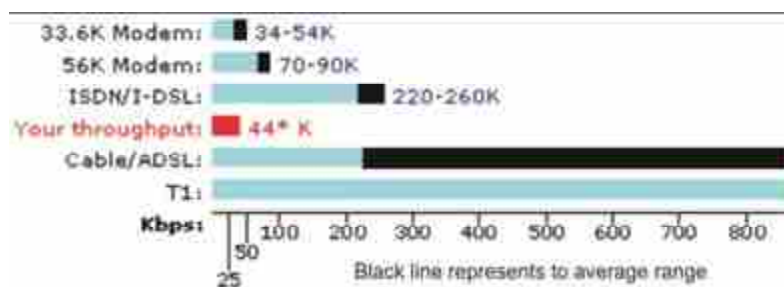
The text file test is meant to simulate downloads of HTML pages to a Web browser. The test utilises a single file of size 340,646 bytes. In the initial trial, the file download completed in 62.25 seconds, yielding an average connection speed of 44 Kbps. Five additional trials were run, with 30-second waits between each, with the results shown below.

**Toast.Net Text Download Performance**

Trial	Time (Seconds)	Speed
1	62.25	44 Kbps
2	73.586	37 Kbps
3	72.965	37 Kbps
4	70.892	38 Kbps
5	62.791	43 Kbps
6	67.567	40 Kbps

To aid interpretation of results, Toast.net provides a chart that compares the performance achieved in the trial against typical results.

**Toast.Net Expected Performance**



**Test Analysis**

Toast.net claims that modems with an optimal 56K connection can achieve speeds of 70–90 Kbps in this benchmark. These results are possible with compression features in the modem protocol. Compression works especially well for text files like HTML pages and usual to see a doubling of effective speed due to compression alone.

The V.90 modem used in this test connected to EarthLink at 21.6 Kbps. The results from Toast.net accurately point out that connection speed alone does not tell the whole performance story. Not only can much better performance be attained but also the actual speed a person sees on the Internet can vary significantly (up to 20% in these trials) from one minute to the next, even at a relatively low-traffic time of day.

Internet users typically download multiple small HTML pages rather than a single large file as done in the Toast.net benchmark. Multiple small downloads generally result in lower aggregate data rates, as the connection management overhead (messages to establish and teardown connections) take bandwidth away from the actual data transfer. For this reason, this Toast.net benchmark will likely report higher speeds than Internet users will see in practice.

**❑ Check Your Progress – 4 :**

1. The \_\_\_\_\_ test is meant to simulate downloads of HTML pages to a Web browser.
  - a. text file
  - b. image file

**11.6 Image Download :**

The image file test is meant to simulate downloads of graphics (GIF or JPEG images) contained in Web pages. The test utilises a single JPEG file of size 225,455 bytes. The snapshot below illustrates the page as it is loading.

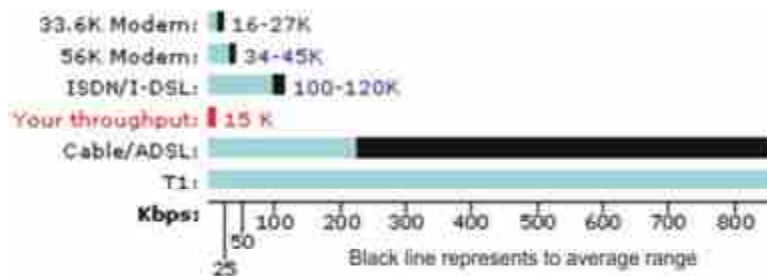
In the initial trial, the file download completed in 118.651 seconds, yielding an average connection speed of 15 Kbps. Nine additional trials were run, with 30-second waits between each, with the results shown below.

**Toast.Net Graphic Download Performance**

Trial	Time (seconds)	Speed
1	118.651	15 Kbps
2	111.831	16 Kbps
3	123.738	15 Kbps
4	123.998	15 Kbps
5	138.679	13 Kbps
6	101.186	18 Kbps
7	137.688	13 Kbps
8	98.101	18 Kbps
9	102.908	18 Kbps
10	110.379	16 Kbps

The Toast.net summary chart suggests these results are typical for modems connecting at 28.8 Kbps or lower.

**Toast.Net Expected Performance**



**Test Analysis**

Typical Web pages incorporate a mix of text and graphics; users rarely download a single image in isolation. However, the Toast.net graphic test demonstrates the network-intensive nature of large images such as maps and diagrams. As compression works very poorly with large and complex graphics, the effective network speed often drops to one-half or lower the performance of text downloads. Image download performance consistently fails to reach the rating advertised by the modem connection.

In these trials, image download performance attained only 40% of text download performance. The image trials yielded an effective speed 25% slower than the rated connection speed (21.6 Kbps in these trials). As in the text download trials, performance from run to run varied by roughly +/- 20%.

**Toast.net Summary**

Overall, Toast.net offers a useful performance measurement service. By providing both text and image download tests, users can accurately gauge the effective speed of their connection on the two most basic forms of Internet workloads. The dramatic difference in performance between the two also serves to educate users on the importance of compression in networking and the wide variation to expect in Web "surfing" performance depending on the content of a given page. Comparison charts allow one to compare their performance against other users with that their same type of connection.

**Computer Networking Ratings for Toast.net**

Accuracy / Reliability	A-
Features	B-
Informative	B
Overall	B

Toast.net offers download testing of single files only. The service would benefit from adding additional workloads that more closely simulate typical usage patterns. For example, a mixed workload of multiple small test file and images would more accurately represent Web page downloads. Upload tests would benefit Website publishers and would also greatly educate the general user on the difference between upstream and downstream performance (particularly for broadband connections).

**❑ Check Your Progress – 5 :**

1. The \_\_\_\_\_ test is meant to simulate downloads of graphics (GIF or JPEG images) contained in Web pages
  - a. image file
  - b. text file

**11.7 DSL and Cable Speeds :**

Both DSL and cable speeds exceed those of competing Internet services. Is DSL faster than cable or vice-versa ?

**DSL and Cable Speed – Bottom Line**

Cable modem Internet services on average promise higher levels of bandwidth than DSL Internet services and this bandwidth roughly translates to raw speed. However, while cable Internet will theoretically run faster than DSL, several technical and business reasons can reduce or even eliminate this advantage.

**DSL v/s Cable Raw Speed – Advantage Cable**

In terms of theoretical peak performance, cable modem runs faster than DSL. Cable technology supports approximately 30 Mbps of bandwidth, whereas most forms of DSL cannot reach 10 Mbps.

One type of DSL technology, VDSL, can match cable's performance, also supporting 30 Mbps. However, Internet service providers generally do not offer VDSL, but rather the cheaper and slower ADSL or SDSL services.

### **DSL vs Cable – Real-World Speed**

In practice, cable's speed advantage over DSL is much less than the theoretical numbers suggest. Why?

- Cable modem services can slow down significantly if many people in your neighbourhood access the Internet simultaneously.
- Both cable modem and DSL performance vary from one minute to the next depending on the pattern of use and traffic congestion on the Internet.
- DSL and cable Internet providers often implement so-called "speed caps" that limit the bandwidth of their services.
- Some home networks cannot match the speed of the Internet connection, which lowers your performance

### **DSL and Cable Speed Caps**

Both cable and DSL service providers commonly employ bandwidth/speed caps for residential customers. Bandwidth caps place an artificial limit on the maximum speed a customer can achieve by monitoring their individual traffic flow and throttling network packets if necessary. Bandwidth caps can reduce a 30 Mbps service down to 3 Mbps or even lower.

Service providers may have several motivations for imposing speed caps including the following:

Providers concerned about the capacity limits of their network may implement a cap so that they can accommodate more customers. Providers may believe that the vast majority of customers do not actually need any more bandwidth than that allowed under the cap. Providers may want to create a fair-and-equal distribution of bandwidth of customers. Without a cap, for example, some DSL subscribers would enjoy much higher bandwidth levels than others in the same neighbourhood. Providers may want to charge higher or lower rates depending on greater or lesser bandwidth levels.

### **□ Check Your Progress – 6 :**

1. Internet services on average promise higher levels of bandwidth than DSL Internet services.
  - a. Cable modem
  - b. Wifi modem

## **11.8 Cable Speed : How fast is Cable Modem Internet ?**

Cable modem has long been recognised for its superior speed compared to other forms of Internet service. Is speed offered by cable modems really that much better than the alternatives? If so, how much faster is it? Cable modem speeds vary widely. While cable modem technology can theoretically support up to about 30 Mbps, most providers offer service with between 1 Mbps and 6 Mbps bandwidth for downloads and bandwidth between 128 Kbps and 768 Kbps for uploads.

### **Cable Speed Considerations**

Did you know your cable speed will vary depending on the usage pattern of your neighbours ? Cable modem services share bandwidth among subscribers

in a locality. The same cable line connects many households. If many of your neighbours access the Internet simultaneously, it is a distinct possibility that cable speeds for you (and them) will decrease significantly during those times.

The causes of cable modem speed problems are similar to those of DSL or other high-speed Internet services:

- **Service glitches** : Cable speed can suddenly drop if the service provider has technical difficulty with their network. Speeds should return to normal after a few minutes or hours.
- **Spyware on computer(s)** : Even when your network may be functioning at full speed, spyware programs may be consuming the modem bandwidth, lowering your cable speed.
- **Mis-configured wired or wireless router** : Routers sit between your computers and the internet connection. If not functioning properly, a router can greatly limit the cable speed achievable on all computers.
- **Slow wireless network connection** : In some cases, a very slow Wi-Fi connection between a computer and a wireless home network will not keep pace with the speed of the cable Internet connection.
- **Old computer(s)** : Very old computers lacking sufficient processing power or memory cannot keep pace with a high-speed Internet connection.

As with DSL services, some cable modem services are symmetric (providing equal bandwidth for both uploading and downloading) but most offer much higher download bandwidth to match the typical needs of residential customers. Check with your service provider to determine the typical bandwidth levels associated with your subscription.

❑ **Check Your Progress – 7 :**

1. Cable speed can suddenly drop if the service provider has technical difficulty with their network. Speeds should return to normal after a few minutes or hours.
  - a. Service glitches
  - b. Spyware on computer

<b>11.9 DSL Speed of Downloading and Uploading :</b>
--

Your DSL speed can change depending on how you use the network.

DSL providers often advertise speed of their service using a combination of two bandwidth numbers; for example, "1.5 Mbps / 128 Kbps"

- The first number, 1.5 Mbps in this case, refers to the maximum bandwidth available for downloads. Examples of network download activities include browsing websites, receiving files from P2P networks and receiving emails.
- The second number, 128 Kbps in this case, corresponds to the bandwidth available for uploads. Examples of network upload activities include publishing on Web sites, sending files over a P2P network and sending emails.

Residential DSL services often provide higher bandwidth for downloads than for uploads, as most customers spend more time in network downloading activities. These are sometimes called asymmetric DSL (ADSL) services. In ADSL, the first bandwidth number will be much higher than the second as in the example above. With symmetric DSL (SDSL), both numbers will be



the same. Many business-class DSL services utilise SDSL, as business customers often spend significant time uploading over their networks.

**❑ Check Your Progress – 8 :**

1. Residential DSL services often provide \_\_\_\_\_ bandwidth for downloads than for uploads.
  - a. Higher
  - b. Lower
  - c. Equal

**11.10 Let Us Sum Up :**

Two key elements of network performance are bandwidth and latency.

However, latency matters equally to the end user experience as the behaviour of satellite internet connections illustrates. Businesses use the term Quality of Service (QoS) to refer to measuring and maintaining consistent performance on a network by managing both bandwidth and latency in a coordinated fashion.

In terms of theoretical peak performance, cable modem runs faster than DSL. Cable technology supports approximately 30 Mbps of bandwidth, whereas most forms of DSL cannot reach 10 Mbps.

One type of DSL technology, VDSL, can match cable's performance, also supporting 30 Mbps. However, internet service providers generally do not offer VDSL, but rather the cheaper and slower ADSL or SDSL services.

**11.11 Answers for Check Your Progress :**

**❑ Check Your Progress 1 :**

1 : a

**❑ Check Your Progress 2 :**

1 : a

**❑ Check Your Progress 3 :**

1 : a

**❑ Check Your Progress 4 :**

1 : a

**❑ Check Your Progress 5 :**

1 : a

**❑ Check Your Progress 6 :**

1 : a

**❑ Check Your Progress 7 :**

1 : a

**❑ Check Your Progress 8 :**

1 : a

**11.12 Glossary :**

1. **Circuit Switching :** Communication via a single dedicated path between the sender and receiver. The telephone system is an example of a circuit switched network.

## Introduction to Computer Network

2. **Emulator** : To imitate (a particular computer system) by using a software system, often including a micro program or another computer that enables it to do the same work, run the same programs, etc., as the first.
3. **NetBIOS** : An applications programming interface (API) which activates network operations on IBM PC compatibles running under Microsoft's DOS. It is a set of network commands that the application program issues in order to transmit and receive data to another host on the network. The commands are interpreted by a network control program or network operating system that is NetBIOS compatible.
4. **Modem** : (Modulator/demodulator) An electronic device for converting between serial data (typically EIA-232) from a computer and an audio signal suitable for transmission over a telephone line connected to another modem. In one scheme the audio signal is composed of silence (no data) or one of two frequencies representing zero and one.
5. **Network** : a system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables: used to transmit or receive information.
6. **Network Layer** : The third lowest layer in the OSI seven layer model. The network layer determines routing of packets of data from sender to receiver via the data link layer and is used by the transport layer. The most common network layer protocol is IP.
7. **Repeater** : A network or communications device which propagates electrical signals from one cable to another, amplifying them to restore them to full strength in the process. Repeaters are used to counter the attenuation which occurs when signals travel long distances
8. **Router** : A device which forwards packets between networks. The forwarding decision is based on network layer information and routing tables, often constructed by routing protocols.
9. **Socket** : The Berkeley Unix mechanism for creating a virtual connection between processes. Sockets interface Unix's standard I/O with its network communication facilities. They can be of two types, stream (bi-directional) or datagram (fixed length destination-addressed messages). The socket library function socket() creates a communications end-point or socket and returns a file descriptor with which to access that socket. The socket has associated with it a socket address, consisting of a port number and the local host's network address.

### 11.13 Assignment :

Discuss a DSL Cable.

### 11.14 Activities :

Explain in detail Network latency.

### 11.15 Case Study :

Write your observation on

- a. How fast the text file is downloaded ?
- b. How is the image file downloaded? Write the procedure.

### **11.16 Further Reading :**

### **High Speed Networking**

1. Sams Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002
2. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001

<b>BLOCK SUMMARY :</b>
------------------------

The block has been written by the writer such that those who need information quickly are able to find what they need, and those who wish to learn more advanced topics can read deeper into each units and further into the chapters.

The book begins with an overview of writer, discussing about the Network OS and network management.

It is possible to read this block of the book like any other book (from beginning to end). Each chapter begins with an introduction about the block and further discussion of the contents it contains. As you get further into a chapter you will learn more about Networking OS and about the management of network and also about their role and capabilities, but often you will be able to head directly to the topic you wish to learn about.

We will also use diagrams, pictures and flowcharts where appropriate, and where we believe readers may find it helpful we will discuss some related theory, including reference to certain documents that you will be able to get from the books in case you need to study more about the topics.

In our whole discussion we have discussed thoroughly on network operating Systems, where topics such as Windows NT workstation, WINS/NBNS, NetBIOS Over TCP/IP, Workgroup, Multiple Master Domain Model, Multiple Trust Models, Windows Server Application have been discussed in detail to its readers. The second unit covered the basically on network management and was also discussed in very detail. The last unit discussed on high speed networking and everything related to the topics was discussed in very detail to its readers.

## **BLOCK ASSIGNMENT :**

### ❖ **Short Questions :**

**Define the following terms :**

1. Windows NT workstation
2. Browsing
3. NetBIOS over TCP /IP
4. Windows networking concepts
5. Workstation
6. Configuration Management
7. Network Management Platform
8. Routers
9. Proactive Fault Monitoring
10. Proactive Fault Notification
11. Latency
12. Speed of the internet modem
13. Speed of the DSL cable
14. Speed test
15. Speed analysis

### ❖ **Long Questions :**

1. Explain NetBIOS System in detail.
2. Explain trouble shooting infrastructure.
3. Differentiate between latency and bandwidth.

**Introduction to  
Computer Network**

❖ **Enrolment No. :**

1. How many hours did you need for studying the units ?

Unit No.	9	10	11
No. of Hrs.			

2. Please give your reactions to the following items based on your reading of the block :

Items	Excellent	Very Good	Good	Poor	Give specific example if any
Presentation Quality	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Language and Style	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Illustration used (Diagram, tables etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Conceptual Clarity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Check your progress Quest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Feed back to CYP Question	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____

3. Any other Comments

.....

.....

.....

.....

.....

.....

.....

.....

.....



**BAOU**  
Education  
for All

**Dr. Babasaheb Ambedkar  
Open University Ahmedabad**

**BCAR-301**

# **INTRODUCTION TO** **COMPUTER NETWORK**

---

## **BLOCK 4 : NETWORK COMMUNICATION AND SOCKET PROGRAMMING**

---

UNIT 12 NETWORKING DEVICES

UNIT 13 SOFTWARE CONSIDERATIONS IN NETWORKING AND  
COMMUNICATION

UNIT 14 SOCKET PROGRAMMING

# **NETWORK COMMUNICATION AND SOCKET PROGRAMMING**

## **Block Introduction :**

In this block the whole content has been divided into Three units. The First Unit covers the Detail of Networking Device which are physically connected in network. The second unit covers the topic Software Considerations, within which Networking and Communication and has been discussed in very detail, whereas the third unit covers the topic Socket Programming which has even been discussed in detail. The writer has tried his best to explain the topics, and has even kept the language of the book very simple in order to make it more understandable.

This block was written so that those who need information quickly are able to find what they need, and those who wish to learn more advanced topics can read deeper into each unit and further into the chapters.

It is possible to read this block of the book like any other book (from beginning to end). Each chapter begins with an introduction about the block and further discussion of the contents it contains. As you get further into a chapter you will learn more about network communication as well as socket programming, their role and capabilities, but often you will be able to head directly to the topic you wish to learn about.

We will also use diagrams where appropriate, and where we believe readers may find it helpful we will discuss some related theory, including reference to certain documents that you will be able to get from the books in case you need to study more about the topics.

## **Block Objectives :**

**After learning this block, you will be able to understand :**

- Networking devices NIC Card, Fire Wall, Router, Switch etc.
- DHCP Server
- SOHO server
- Types of Communication Services
- Terminal emulator
- Socket Programming

## **Block Structure :**

**Unit 12 : Networking Devices**

**Unit 13 : Software Considerations in Networking and Communication**

**Unit 14 : Socket Programming**



**UNIT STRUCTURE**

- 12.0 Learning Objectives**
- 12.1 Introduction**
- 12.2 Network Interface Card**
- 12.3 HUB**
- 12.4 Switches**
- 12.5 Wireless Access Point**
- 12.6 Router**
- 12.7 Firewall**
- 12.8 DHCP Servers**
- 12.9 SOHO Networks**
- 12.10 Lets Sum Up**
- 12.11 Answers for Check Your Progress**
- 12.12 Glossary**
- 12.13 Assignment**
- 12.14 Activities**
- 12.15 Case Study**
- 12.16 Further Readings**

**12.0 Learning Objectives :**

**After learning this unit, you will be able to understand :**

- Network Interface Card or NIC Card
- HUB Device
- Switch Device
- Wireless Access Point
- Router
- Firewall
- What is DHCP Server ?
- SOHO Network

**12.1 Introduction :**

As we know our computer is connected with Different network for communication. For connecting any machine in network different devices are used, collaborating this device we can connect on internet. For that we need NIC card or we can say LAN Port for connecting a LAN wire with computer. Through this LAN port we connect many more network devices like switch, hub router etc. Using this device we manage our network and establish connection on internet. Also this all devices can establish connection using some protocol.

This protocol provide services for configure a device in network. In this unit we learn about such devices in detail, also will cover a DHCP Protocol.

## **12.2 Network Interface Card :**

Network Interface Card(NIC) card is a hardware cheap with port to connect a computer in LAN Network. This card also known as LAN Port. This card is work on ETHERNET LAN so IT is also call ETHERNET CARD. This card is developed by Manufacture, at the time of manufacturing it has allotted a 32 bit Physical Address same like IP Adders. This physical address is also an unique address for identify a Device in network. NIC allows both wired and wireless communications. It allows communication of Device in LAN Network or any large scale networks. NIC card is both a physical layer and a data link layer device, it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it. Each network interface card is assigned an Ethernet source address by the manufacturer of the network interface card. This card is helpful in Medium Access Control(MAC). It has Two type Wired NIC card or Wireless NIC Card. In wire NIC card we can connect Wire or LAN Cable. In Wireless NIC card we can connect a computer with wireless devices which provide Wireless LAN connection. NIC card is connected with Ethernet cable using Transceiver; it is a small hole is made in the outer layer of the coaxial cable. Transceiver is attached with medium for transfer data. Transceiver is hearing the voltage on the cable for interpreting the signals. NIC card has ROM for storing packets for communication in Network it will store the data in memory for some sort period. NIC includes a piece of Software and Hardware for reliable communication.



**Fig. 12.1 : NIC Card a Hardware Chip to Connect Device in Network**

## **12.3 HUB :**

Hub is a Hardware device which works on Physical Layer. This device is used to establish LAN Network.IT has multiple ports to connect more than one computer. Hub is responsible to manage whole network. Hub works on Broadcast network, means any device in network want to pass its data to other device first of all it pass data on hub and hub will forward its data to it's connected devices on same time every device get data. Only Indented device will receive the message and rest of device will ignore the data. This device has less security, because it broadcast packets on network. Hub is work as Repeater also; it will pass data by amplifying the signal and forward it for long-distance. Hubs do not perform packet filtering or addressing functions; they just send data packets to all connected devices. It follow Star Topology for establish Network connection.



**Fig. 13.2 : Hub Device Connected with n Number of Device**

❑ **Check Your Progress – 1 :**

1. HUB work on \_\_\_\_\_ type of network
  - a. Broad Cast    b. Unicast        c. multicast
2. HUB works on \_\_\_\_\_ kind of network
  - a. LAN                b. MAN                c. WAN

**12.4 Switch :**

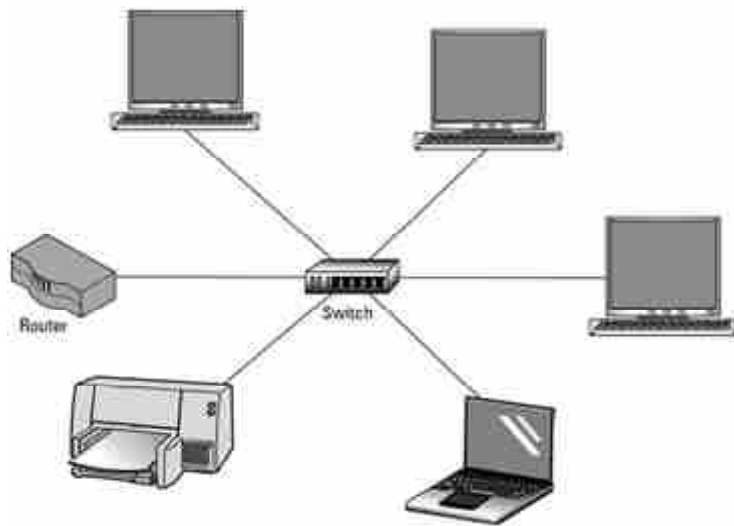
Switch is also a network device which works in Intranet. This device is work at Data Link Layer. It is used to connect one or more device in same network. It is a central device of whole network. Switch manage data transmission using star topology also it maintain the network. It is full-duplex device, any device which wants to start communication on network first of all it will send packets on switch and then switch will identify the physical address of that device and forward it to that device only. Switch works on store and forward technique. Switch store Mack address of connected device and identify that address at the time of sending and receiving frame or packets. It is supports unicast (one-to-one), multicast (one-to-many) and broadcast (one-to-all) communications. Switch is power full device because it has software to manage network also will provide security to accessing device.Switch is more powerful than Hub but less powerful then Router.

**Types of Switches**

**Unmanaged Switch** – These switch is used in small networks like home network or small business network.IT is used to connect computer to computer ,printer to computer in same network.IT is very simple to plug and connect any device in such switch. This kind of switches are less expensive.IT is based on HUB device.

**Managed Switch** – This kind of switch can provide security in network. This kind of switches are used in Organization or Large Business to create or expand large network.IT is more expensive then unmanaged because of it has a functionality of multicast. They are work on Simple Network Management Protocol (SNMP).

**LAN Switch** – This kind of switch also work on large organization, they are work on Ethernet network so it called as Ethernet Switches. These switches are work on Full Duplex mode so it can manage individual machine in network. It reduce network congestion. IT work on more bandwidth compare to other one so, it communicate fast enough and perform smooth functionality in network. It can store and forward packets in network.



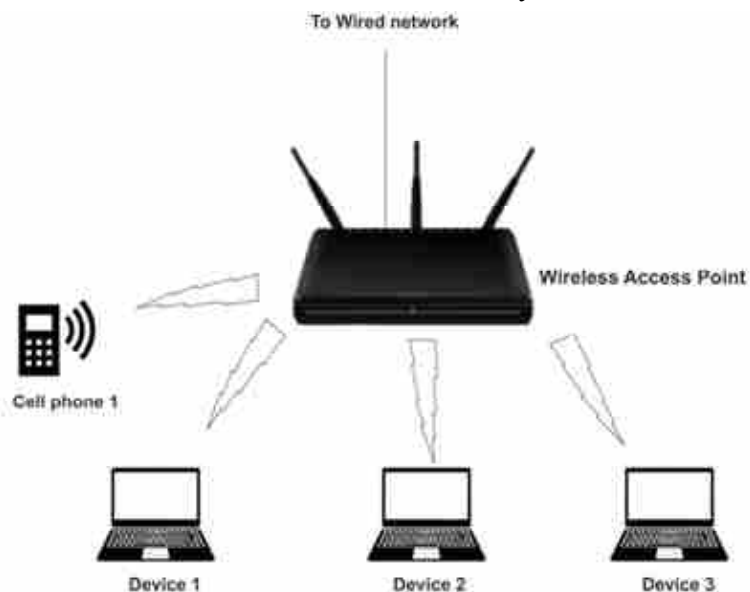
**Fig. 12.3 : Switch Network**

**□ Check Your Progress – 2 :**

1. Switch work on \_\_\_\_\_ technic.
  - a. Store and Reject
  - b. Store and Forward
  - c. Store and Delete

**12.5 Wireless Access Point :**

While Wireless technology is become popular, we need to connect such device in network full time. For such a connection Wireless LAN different standards are develop and they access by different hardware's. A wireless LAN has develop Access Point which is a central control device for mange a Network and connect n number of devices in network. This Hardware is configuring with Local Area Network. This device is constructing a wireless network or ad-hoc-network or point-to-point network. This access point is nothing but it is wireless router. It can connect with wired network also, for that it has installed transceiver. It is connect with modem or ADSL modem to get connection with internet. A device which connect with WAP must has install Wireless LAN Card. Wireless access points are most commonly thought of in the context of the 802 series of wireless standards, commonly known as Wi-Fi.



**Fig. 12.4 : Wireless Access Point**

❑ **Check Your Progress – 3 :**

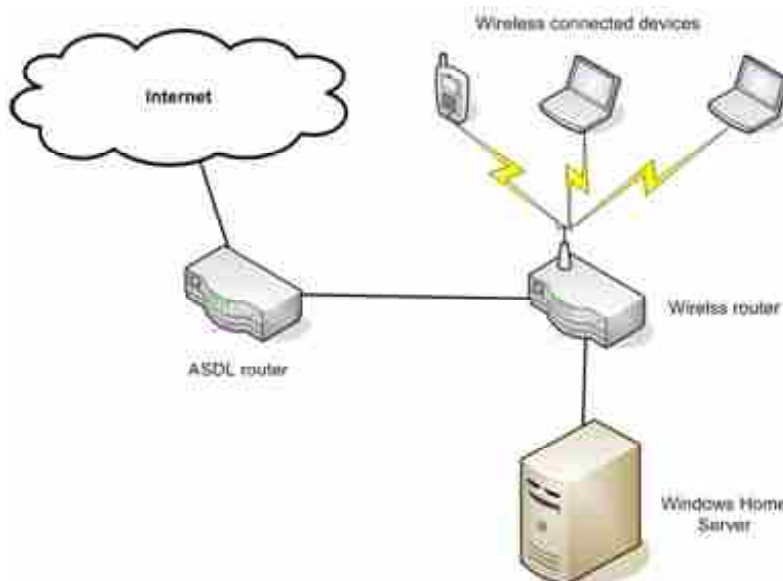
1. Wireless Access point is also known as \_\_\_\_\_
  - a. Ad-hoc-device
  - b. Ad-hoc-server
  - c. ad-hoc-network

**12.6 Router :**

Router is a Network Device. Router helps to pass data in one or more networks. Router Connect two or more networks but it works only in similar network. Main task of Router is to identify a route/path between two network devices. Router works on network layer. It sends data in Packet format. It can connect multiple Pcs in network via Ethernet cable or Wi-Fi. It Provide security to protect network. Router has a capacity to store routing details so it is both Hardware and Software Device. Router cannot work in Broadcast Network. There are two types of Routing perform by router. (1) Static Routing (2) Dynamic Routing.

**Static Routing :** This Routing is work on fixed routing, means it will not update the path of routing automatically. Once router has define any path then it will follow only that path. The path is manually updated. If the changes occur at the network side, we need to update the path in the routing table. Static routing is easy to design and implement as there is not a complex path. We can set security option manually so it is provide higher security then dynamic routing. IT works on small network like only up to MAN network.

**Dynamic Routing :** This routing is not fixed, means it will update path of routing automatically. If the changes occur at the network, there is no need to update path in routing table. It will manage routing table automatically based on sending and receiving a packets from different devices. It will follow Routing Algorithms to update routing table and manage routing service. We cannot set any security option manually, so it is less secure then static routing. Dynamic routing is implemented in large networks like WAN network.



**Fig. 12.5 : Home Network with Router Device**

❑ **Check Your Progress – 4 :**

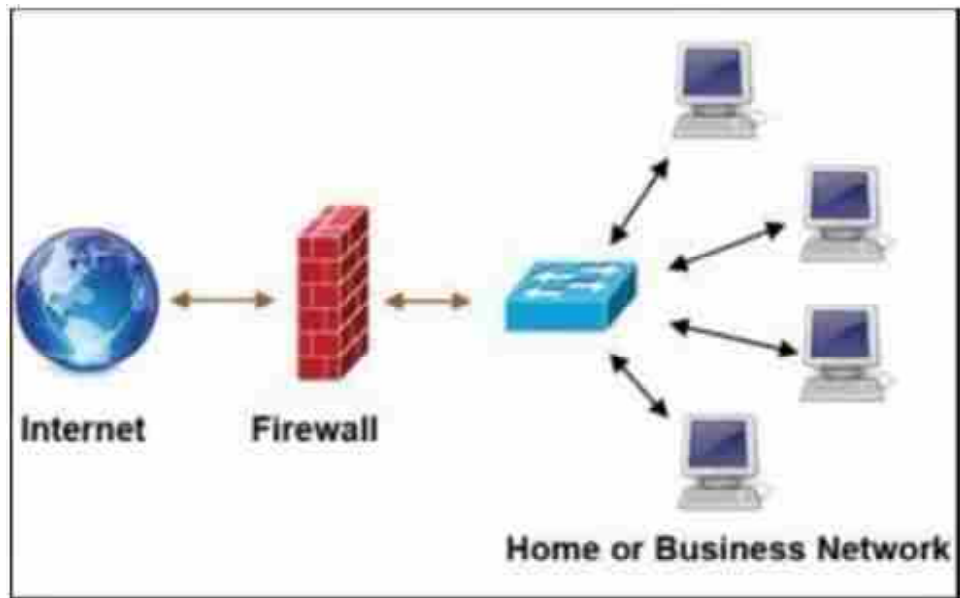
1. Router is work on \_\_\_\_\_ layer
  - a. network
  - b. datalink
  - c. Application

**12.7 Firewall :**

In terms of Computer Technology a firewall is a piece of software. Firewall will manage network traffic. It monitors the traffic arrives on computer. It has inbuilt protocols design which is apply on each packets comes inside network. The protocol will define which packet has to allow enter in computer network or discard before enter. Firewall role is like watchman in your Home or Organization. Usually firewall is placed between a network and Internet or outside the world. Firewall is a specialize version of Router. It perform normal routing function as well as firewall functionality. Fire wall will protect network against unauthorized access. Basic two types of Firewall are designed.

**Packet Filters :** Data which converted into part of Packet by network layer. Packet has some Meta data which contain some senders and receivers information. Based on reading meta data of packet firewall will decide to allow such packet in network or discarded it. It is also call screening router. In such firewall packets are pass out from some protocols. That protocol will verify the packet is collecting proper data as per rules, if not then it will reject the packet otherwise allow that packet in network.

**Application Gateway :** This fire wall will inspect the packet on TCP/IP or OSI Layer's up to the Application layer. It has the ability to block specific content, also recognize when certain application and protocols (like HTTP, FTP) are being misused. In other words, Application layer firewalls are hosts that run proxy servers.



**❑ Check Your Progress – 5 :**

1. Firewall is place between \_\_\_\_\_ and \_\_\_\_\_
  - a. network, server
  - b. Internet, network
  - c. Internet, Computer

**12.8 DHCP Servers :**

DHCP server is a network server that automatically connects IP address, other network parameters to client machine. DHCP server will connect the client using Dynamic Host Configuration Protocol (DHCP). This protocol will send

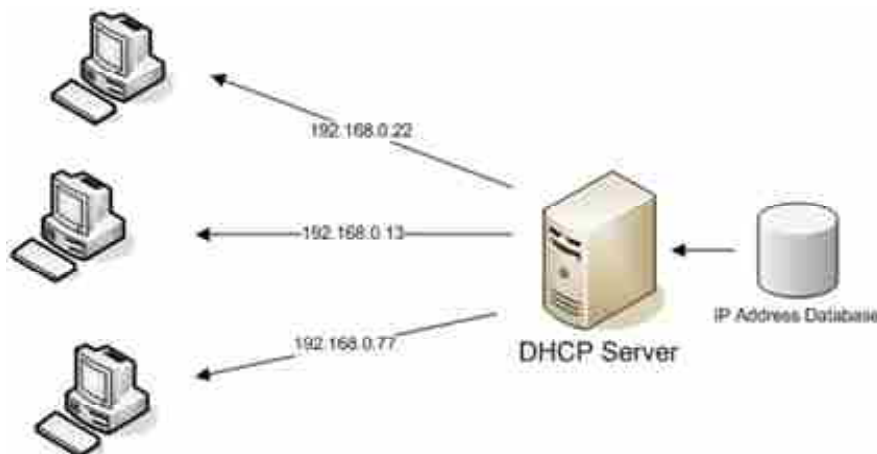
broadcast request to the clients who connect to the server and configure the machine with its physical IP to Logical IP or network IP. By using a client-server model, a DHCP server becomes the host, while the device connected to the network is the client. It is a fastest network to establish or configure a device with network. This network is easier to manage. The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer. The DHCP server stores the configuration information in a database.

**Advantages of DHCP server**

- It manages IP Addresses automatically without allotting duplicate IP address.
- It supports BOOTP clients.
- It also allow administrator to manage manual allocation of IP address.
- It set the limitation on MAC address to configure dynamic IP address.

**Disadvantages of DHCP server**

- If your DHCP server is fail then your client won't request or unable to get dynamic IP address.
- If DHCP server contains incorrect information then network administrator has to manage all clients manually and reconfigure them.



**12.9 SOHO Networks :**

SOHO is an abbreviation Small Office/Home Office Network. In SOHO network we can configure 1 to 10 computers. SOHO networks are configured for privately owned business or individuals who are self-employed. It is like LAN network for small office or Home. It is also work on both wired and wireless devices. Network services likes DNS, Email server, Webserver etc. are allow outside of SOHO network This network is easy to setup and manage. It is also known as virtual office. SOHO network is mainly used for connecting several machines to share information in organization. In SOHO network it require Routers to establish connection through wire or wireless devices. Some SOHO routers have install firewall to preventing malicious attacks which generally comes from the files or data coming from the web. It is also use ADSL modem to receiving and sending a signals out side of network using Internet service. Major two types of cables are used to connect devices in SOHO 10 base T and 100 base T.

## Introduction to Computer Network



### 12.10 Lets Sum Up :

#### In this unit we have learned :

- NIC card a hardware chip which used to connect computer in any network. It has unique physical address allotted by manufacturer of NIC card.
- Hub is a Hardware device which works on Physical Layer. This device is used to establish LAN Network. It is a broadcast network which broadcast message among all the device.
- Switch is also a network device which works in Intranet. This device is work at Data Link Layer. Switch is work on unicast, broadcast and multicast networks. It is provide more security in communication compare to HUB. It apply store and forward technic for communication.
- A wireless LAN has develop Access Point which is a central control device for mange a Network and connect n number of devices in network. This Hardware is configuring with Local Area Network.IT is also known as a Wi-Fi network.
- Router is Hardware as well as Software device which is work on network layer, is used for routing in network.IT manage both Static and Dynamic Routing with the help of Routing table. It also use Firewall for receiving packet more securely.
- Firewall is software which is installed in Router. Firewall add more security in router to allow only authenticate packets in network.
- DHCP Server allot IP Addresses automatically without allotting duplicate IP address to clients. DHCP server will connect the client using Dynamic Host Configuration Protocol (DHCP). By using a client-server model, a DHCP server becomes the host, while the device connected to the network is the client.
- SOHO is an abbreviation Small Office/Home Office Network. It is a like a small LAN network for office or home. It is also work on both wired and wireless devices. It is mainly used to share information among the devices connected in SOHO network.



### 12.11 Answers for Check Your Progress : :

- ❑ **Check Your Progress 1 :**  
1 : b                    2 : a
- ❑ **Check Your Progress 2 :**  
1 : b
- ❑ **Check Your Progress 3 :**  
1 : c
- ❑ **Check Your Progress 4 :**  
1 : a
- ❑ **Check Your Progress 5 :**  
1 : b

### 12.12 Glossary :

**Dynamic Host Configuration Protocol (DHCP) :** Is a protocol which allocates dynamic IP address in network to Computer.

**HUB :** A central device which work on star topology network.

**IP Address :** is a logical Address providing by Network.

**LAN :** Local Area Network a small network range of up to 100meters.

**MAC Address :** is a physical address provide by Manufacturer to the Machine Hardware or NIC Card.

**Network Interface Card :** The interface between a host and network.

**Router :** A network layer device which store and forward packets from one network to another network.

**Routing Table :** A table which maintain by router to decide which incoming packet will forward to it's destination.

**Transceiver :** Is a device which hearing a signal on medium.

### 12.13 Assignment :

1. Explain NIC Card in detail.
2. Write difference between HUB and Switch.
3. Explain Router in detail.

### 12.14 Activity :

Draw DHCP server and Explain All the Elements in Detail

### 12.15 Case Study :

Draw SOHO network and explain it's working model.

### 12.16 Further Readings :

1. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001 Digital Networking.
2. TCP/IP Protocol Suite, Edition 4, Behrouz A. Forouzan.

**UNIT STRUCTURE**

- 13.0 Learning Objectives
- 13.1 Introduction
- 13.2 HP-UX IO Cards
- 13.3 Types of communication services
- 13.4 Communication Media
- 13.5 Terminal emulator
- 13.6 Network Cards
- 13.7 Wireless Router
- 13.8 Let Us Sum Up
- 13.9 Answers for Check Your Progress
- 13.10 Glossary
- 13.11 Assignment
- 13.12 Activities
- 13.13 Case Study
- 13.14 Further Readings

**13.0 Learning Objectives :**

After learning this unit, you will be able to understand :

- Terminal emulator
- Network card
- Wireless router
- HP UX IO cards
- Typical services and the models

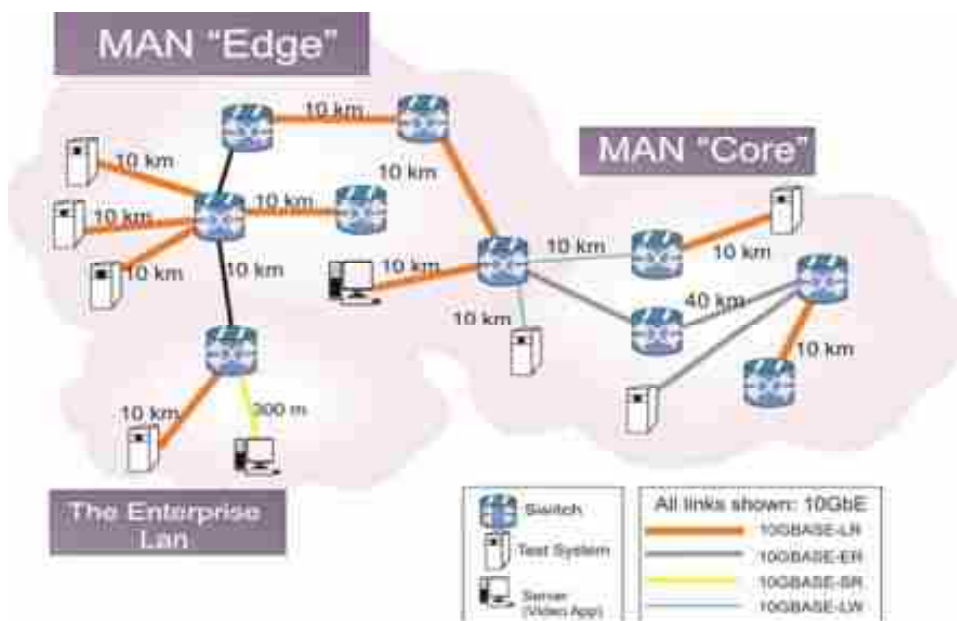
**13.1 Introduction :**

You all are acquainted with some sorts of communication in your day to day life. For communication of information and messages we use telephone and postal communication systems. Similarly data and information from one computer system can be transmitted to other systems across geographical areas. Thus, data transmission is the movement of information using some standard methods. These methods include electrical signals carried along a conductor and optical signals along optical fibers and electromagnetic areas. Suppose a manager has to write several letters to various clients. First he has to use his PC and Word Processing package to prepare the letter, if the PC is connected to all the clients' PC's through networking, he can send the letters to all the clients within minutes. Thus, irrespective of geographical area, if PCs are connected through communication channel, the data and information, computer files and any other programs can be transmitted to other computer systems

within seconds. The modern form of communication like e-mail and internet is possible only because of computer networking.

**13.2 HP-UX I/O Cards :**

**10 Gigabit Ethernet**



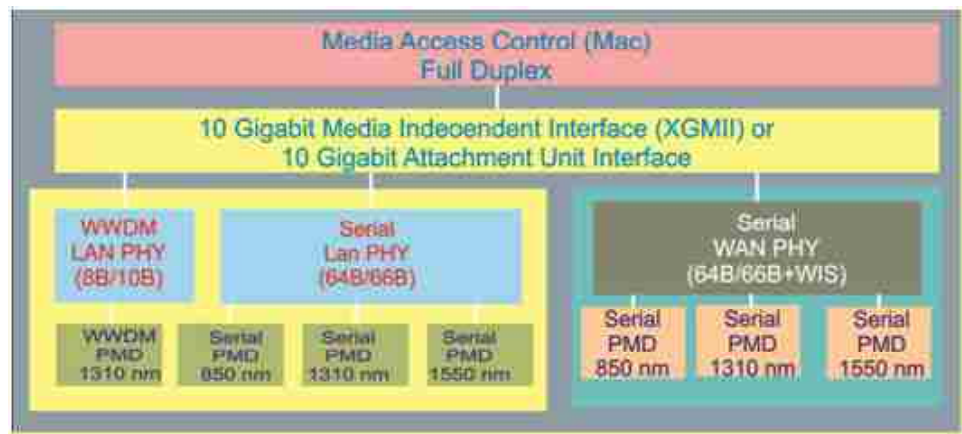
**Fig 13.1 : The 10 Gigabit Ethernet Standard**

Under the International Standards Organisation's Open Systems Interconnection (OSI) model, Ethernet is fundamentally a Layer 2 protocol. 10 Gigabit Ethernet uses the IEEE 802.3 Ethernet Media Access Control (MAC) protocol, the IEEE 802.3 Ethernet frame format and the minimum and maximum IEEE 802.3 frame size.

Just as 1000BASE-X and 1000BASE-T (Gigabit Ethernet) remained true to the Ethernet model, 10 Gigabit Ethernet continues the natural evolution of Ethernet in speed and distance. Since, it is a full-duplex only and fiber-only technology, it does not need the carrier-sensing multiple-access with collision detection (CSMA/CD) protocol that defines slower, half-duplex Ethernet technologies. In every other respect, 10 Gigabit Ethernet remains true to the original Ethernet model.

An Ethernet Physical layer device (PHY), which corresponds to Layer 1 of the OSI model, connects the media (optical or copper) to the MAC layer, which corresponds to OSI Layer 2. Ethernet architecture further divides the PHY (Layer 1) into a Physical Media Dependent (PMD) and a Physical Coding Sublayer (PCS). Optical transceivers, for example, are PMDs. The PCS is made up of coding (e.g., 64/66b) and a serializer or multiplexing functions.

The 802.3ae specification defines two PHY types: the LAN PHY and the WAN PHY (discussed below). The WAN PHY has an extended feature set added onto the functions of a LAN PHY. These PHYs are solely distinguished by the PCS.



**Fig 13.2 : 1000Base-T and 1000Base-SX (Gigabit Ethernet)**

There will also be a number of PMD types.

- Advanced Communications Controller
- Advanced Server/9000
- ATM
- Combination Cards
- CommonIO
- Datakit
- Fabric Clustering System for InfiniBand
- FDDI/9000
- Fibre Channel
- HyperFabric
- IO Cards
- Multiplexers
- NetWare
- PCI Error Handling and Recovery
- Remote Manageability & Graphics/USB Cards
- SAS Host Bus Adapters
- SCSI Host Bus Adapters
- Smart Array (RAID)
- X.25.

**☐ Check Your Progress – 1 :**

1. An \_\_\_\_\_, which corresponds to Layer 1 of the OSI model, connects the media (optical or copper) to the MAC layer, which corresponds to OSI Layer 2.
  - a. Ethernet Physical layer device
  - b. Multiplexers
  - c. Remote Manageability and Graphics/USB Cards

**13.3 Types of Communication Services :**

The term used to describe the data-handling capacity of a communication service is bandwidth. Bandwidth is the range of frequencies that is available

for the transmission of data. A narrow range of frequencies in a communication system is analogous to a garden hose with a small diameter. The flow of information in such a system is restricted, just as is the flow of water in the narrow hose. Wider bandwidths permit more rapid information flow. The communication data transfer rate is measured in a unit called baud. Baud is identical to bits per second. Therefore, a rate of 300 baud is 300 bits per second.

Communication companies such as American Telephone and Telegraph (AT&T) and Western Union are called common carriers and they provide three general classes of service for both voice and data communication:

1. Narrowband handles low data volumes. Data transmission rates are from 45 to 300 baud. The low-speed devices might use narrow band communications.
2. Voice band handles moderate data transmission volumes between 300 and 9600 baud. They are used for applications ranging from operating a CRT to running a line printer. Their major application is for telephone voice communication hence, the term voice band.
3. Broadband handles very large volumes of data. These systems provide data transmission rates of 1 million baud or more. High-speed data analysis and satellite communications are examples of broadband communication systems.

□ **Check Your Progress – 2 :**

1. \_\_\_\_\_ is the range of frequencies that is available for the transmission of data.
  - a. Bandwidth
  - b. broadband

<b>13.4 Communication Media :</b>
-----------------------------------

Following are the major communication devices which are frequently used :

1. **Wire Pairs :** Wire pairs are commonly used in local telephone communication and for short distance digital data communication. They are usually made of copper and the pair of wires is twisted together. Data transmission speed is normally 9600 bits per second in a distance of 100 meter.
2. **Coaxial Cables :** Coaxial cable is a group of specially wrapped and insulated wires that are able to transfer data at higher rate. They consist of a central copper wire surrounded by an insulation over which copper mesh is placed. They are used for long distance telephone lines and local area network for their noise immunity and faster data transfer.
3. **Microwave :** Microwave system uses very high frequency radio signals to transmit data through space. The transmitter and receiver of a microwave system should be in line-of-sight because the radio signal cannot bend. With microwave very long distance transmission is not possible. In order to overcome the problems of line of sight and power amplification of weak signal, repeaters are used at intervals of 25 to 30 kilometres between the transmitting and receiving end.
4. **Communication Satellite :** The problem of line-sight and repeaters are overcome by using satellites which are the most widely used data transmission media in modern days. A communication satellite is a

microwave relay station placed in outer space. INSAT-1 B is such a satellite that can be accessible from anywhere in India. In satellite communication, microwave signal is transmitted from a transmitter on earth to the satellite at space. The satellite amplifies the weak signal and transmits it back to the receiver. The main advantage of satellite communication is that it is a single microwave relay station visible from any point of a very large area. In microwave the data transmission rate is 16 gigabits per second. They are mostly used to link big metropolitan cities.

❑ **Check Your Progress – 3 :**

1. \_\_\_\_\_ are commonly used in local telephone communication and for short distance digital data communication.
  - a. Wire pairs
  - b. Coaxial Cables

**13.5 Terminal Emulator :**

A terminal emulator, terminal application, term or TTY for short, is a program that emulates a video terminal within some other display architecture. Though typically synonymous with a command line shell or text terminal, the term terminal covers all remote terminals, including graphical interfaces. A terminal emulator inside a graphical user interface is often called a terminal window.

A terminal window allows the user access to a text terminal and all its applications such as command line interfaces (CLI) and text user interface applications. These may be running either on the same machine or on a different one via telnet, SH or dial-up. On Unix-like operating systems it is common to have one or more terminal windows connected to the local machine.

❑ **Check Your Progress – 4 :**

1. A \_\_\_\_\_, terminal application, term or TTY for short, is a program that emulates a video terminal within some other display architecture.
  - a. terminal emulator
  - b. Network cards.

**13.6 Network Cards :**

In the vast world of computers and technology, internet acts as a lifeline. The World Wide Web connects everyone together, allowing users to chat with each other, to buy things instantly through websites and to find almost any information. If the internet is the spinal cord of the technological world, network cards are the vertebrae allowing computers to communicate with each other.



**Fig. 13.3 : Network Card**

A network interface card, network adapter, network interface controller (NIC) or LAN adapter is a computer hardware component designed to allow computers to communicate over a computer network. It is both an OSI layer 1 (physical layer) and layer 2 (data link layer) device, as it provides physical access to a networking medium and provides a low-level addressing system through the use of MAC addresses. It allows users to connect with each other either by using cables or wirelessly.

Although other network technologies exist (e.g. Token Ring), Ethernet has achieved near-ubiquity since the mid-1990s. Every Ethernet network card has a unique 48-bit serial number called a MAC address, which is stored in ROM carried on the card. Every computer on an Ethernet network must have a card with a unique MAC address. Normally, it is safe to assume that no two-network cards will share the same address, because card vendors purchase blocks of addresses from the Institute of Electrical and Electronics Engineers (IEEE) and assign a unique address to each card at the time of manufacture.

Madge 4/16Mbps TokenRing ISA NIC

Ethernet 10Base-5/2 ISA NIC

Network cards earlier were expansion cards that could be plug into a computer bus. However, the low cost and ubiquity of the Ethernet standard means that most new computers have a network interface built into the motherboard.

These either have Ethernet capabilities integrated in the motherboard chipset or implemented via low cost dedicated Ethernet chip, connected through the PCI (or the newer PCI express) bus. A separate network card is not required unless multiple interfaces are needed or some other type of network is used. Newer motherboards may even have dual network (Ethernet) interfaces built-in.

**Check Your Progress – 5 :**

1. The most new computers have a network interface built into the \_\_\_\_\_
  - a. Motherboard
  - b. Cpu
  - c. Memory

<b>13.7 Wireless Router :</b>
-------------------------------

A wireless router is a device that performs the functions of a router but also includes the functions of a wireless access point. It is commonly used to allow access to the Internet or a computer network without the need for a cabled connection. It can function in a wired LAN (local area network), a wireless only LAN or a mixed wired/wireless network. Most current wireless routers have the following characteristics:

- **LAN port :** It functions in the same manner as the ports of a network switch
- **WAN port :** It connects to a wide area network, typically one with Internet access. External destinations are accessed using this port. If it is not used, many functions of the router will be bypassed.
- **Wireless Antennae :** These allow connections from other wireless devices (NICs (network interface cards), wireless repeaters, wireless access points and wireless bridges, for example), usually using the Wi-Fi standard.



**Fig 13.4 : Wireless Router**

**❑ Check Your Progress – 6 :**

1. A \_\_\_\_\_ is a device that performs the functions of a router but also includes the functions of a wireless access point.
  - a. wireless router
  - b. modem
  - c. motherboard

**13.8 Let Us Sum Up :**

The modern forms of communication like e-mail and Internet is possible only because of computer networking.

Under the International Standards Organisation's Open Systems Interconnection (OSI) model, Ethernet is fundamentally a Layer 2 protocol.

The term used to describe the data-handling capacity of a communication service is bandwidth.

Bandwidth is the range of frequencies that is available for the transmission of data.

A narrow range of frequencies in a communication system is analogous to a garden hose with a small diameter.

The communication data transfer rate is measured in a unit called baud. Baud is identical to bits per second.

Communication companies such as American Telephone and Telegraph (AT&T) and Western Union are called common carriers and they provide three general classes of service for both voice and data communication.

A terminal emulator, terminal application, term or TTY for short, is a program that emulates a video terminal within some other display architecture.



A network interface card, network adapter, network interface controller (NIC) or LAN adapter is a computer hardware component designed to allow computers to communicate over a computer network.

A wireless router is a device that performs the functions of a router but also includes the functions of a wireless access point.

### **13.9 Answers for Check Your Progress :**

**Check Your Progress 1 :**

1 : a

**Check Your Progress 2 :**

1 : a

**Check Your Progress 3 :**

1 : a

**Check Your Progress 4 :**

1 : a

**Check Your Progress 5 :**

1 : a

**Check Your Progress 6 :**

1 : a

### **13.1 Glossary :**

1. **Network :** a system containing any combination of computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables: used to transmit or receive information.
2. **Network Layer :** The third lowest layer in the OSI seven layer model. The network layer determines routing of packets of data from sender to receiver via the data link layer and is used by the transport layer. The most common network layer protocol is IP.

### **13.11 Assignment :**

Explain the various communication devices.

### **13.12 Activities :**

Discuss the significance of WAN port.

### **13.13 Case Study :**

Discuss the use of various software's used in network management.

### **13.14 Further Readings :**

1. Sam's Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002
2. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001

**UNIT STRUCTURE**

- 14.0 Learning Objectives
- 14.1 Introduction
- 14.2 Connections Oriented with Server Side Program
- 14.3 Connections Oriented with Client Side Program
- 14.4 Connectionless Server Side Programs
- 14.5 Connectionless Client Side Programs
- 14.6 How to Listen for Socket Connections ?
- 14.7 How to Talk between Sockets ?
- 14.8 What to do when you're done with A Socket ?
- 14.9 Let Us Sum Up
- 14.10 Answers for Check Your Progress
- 14.11 Glossary
- 14.12 Assignment
- 14.13 Activities
- 14.14 Case Study
- 14.15 Further Readings

**14.0 Learning Objectives :**

After learning this unit, you will be able to understand :

- Socket methods
- Socket programming
- How to listen for socket connections
- Establish connection between Sockets

**14.1 Introduction :**

A socket is a software endpoint that establishes bidirectional communication between a server program and one or more client programs. The socket associates the server program with a specific hardware port on the machine where it runs, so any client program anywhere in the network with a socket associated with that same port can communicate with the server program.

A server program typically provides resources to a network of client programs. Client programs send requests to the server program and the server program responds to the request.

Using threads, a multi-threaded server program can accept a connection from a client, start a thread for that communication and continue listening for requests from other clients.

**Example 1 :** Sets up a client and server communication between one server program and one client program. The server program is not multi-threaded and cannot handle requests from more than one client.

**Example 2 :** Converts the server program to a multi-threaded version so it can handle requests.

The client program presents a simple user interface and prompts for text input. When you click the Click Me button, the text is sent to the server program. The client program expects an echo from the server and prints the echo it receives on its standard output.



The server program presents a simple user interface and when you click the 'Click Me' button, the text received from the client is displayed. The server echoes the text it receives whether or not you click the 'Click Me' button.



To run the example programs, start the server program first. If you do not, the client program cannot establish the socket connection. Here are the compiler and interpreter commands to compile and run the example.

The server program establishes a socket connection on Port 4321 in its listen Socket method. It reads data sent to it and sends that same data back to the server in its action Performed method.

**14.2 Connection Oriented with Server Side Program :**

When you are writing code that implements the server side of a connection oriented protocol, your code typically follows this pattern:

- Create a Server Socket object to accept connections.
- When the Server Socket accepts a connection, it creates a Socket object that encapsulates the connection.
- The Socket is asked to create InputStream and OutputStream objects that read and write bytes to and from the connection,

The Server Socket can optionally create a new thread for each connection, so that the server can listen for new connections while it is communicating with clients.

## Introduction to Computer Network

```
/* tcpserver.c */
#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <errno.h>
#include <string.h>
int main()
{
    int sock, connected, bytes_recieved, true = 1; charsend_data [1024],
    recv_data[1024]; structsockaddr_inserver_addr,client_addr; intsin_size;
    if ((sock = socket(AF_INET, SOCK_STREAM, 0)) == -1) {
        perror("Socket");
        exit(1);
    }
    if (setsockopt(sock,SOL_SOCKET,SO_REUSEADDR,&true,sizeof(int)) ==
-1) {
        perror("Setsockopt");
        exit(1);
    }
    server_addr.sin_family = AF_INET;
    server_addr.sin_port = htons(5000);
    server_addr.sin_addr.s_addr = INADDR_ANY;
    bzero(&(server_addr.sin_zero),8);
    if (bind(sock, (structsockaddr *)&server_addr, sizeof(structsockaddr))
== -1) {
        perror("Unable to bind");
        exit(1);
    }
    if (listen(sock, 5) == -1) {
        perror("Listen");
        exit(1);
    }
    printf("\nTCPServer Waiting for client on port 5000");
    fflush(stdout);
    while(1)
    {
```

```

sin_size = sizeof(structsockaddr_in);
connected = accept(sock, (structsockaddr *)&client_addr,&sin_size);
printf("\n I got a connection from (%s , %d)",
inet_ntoa(client_addr.sin_addr),ntohs(client_addr.sin_port)); while (1)
{
printf("\n SEND (q or Q to quit) : ");
gets(send_data);
if (strcmp(send_data , "q") == 0 || strcmp(send_data , "Q") == 0)
{
send(connected, send_data,strlen(send_data), 0);
close(connected);
break;
}
else
send(connected, send_data,strlen(send_data), 0); bytes_recieved =
recv(connected,recv_data,1024,0); recv_data[bytes_recieved] = '\0';
if (strcmp(recv_data , "q") == 0 || strcmp(recv_data , "Q") == 0)
{
close(connected);
break;
}
else
printf("\n RECIEVED DATA = %s " , recv_data);
fflush(stdout);
}
}
close(sock);
return 0;
}

```

**❑ Check Your Progress – 1 :**

1. When the Server Socket accepts a connection, it creates a \_\_\_\_\_ that encapsulates the connection.
  - a. Socket object
  - b. Socket
  - c. Main socket

**14.3 Connection Oriented with Client Side Program :**

Client–side sessions use cookies and cryptographic techniques to maintain state without storing as much data on the server. When presenting a dynamic web page, the server sends the current state data to the client (webbrowser) in the form of a cookie. The client saves the cookie in memory or on disk. With each successive request, the client sends the cookie back to the server, and the server uses the data to "remember" the state of the application for that specific client and generate an appropriate response.

This mechanism may work well in some contexts; however, data stored on the client is vulnerable to tampering by the user or by software that has access to the client computer. To use client-side sessions where confidentiality and integrity are required, the following must be guaranteed:

1. **Confidentiality** : Nothing apart from the server should be able to interpret session data.
2. **Data integrity** : Nothing apart from the server should manipulate session data (accidentally or maliciously).
3. **Authenticity** : Nothing apart from the server should be able to initiate valid sessions.

To accomplish this, the server needs to encrypt the session data before sending it to the client, and modification of such information by any other party should be prevented via cryptographic means.

Transmitting state back and forth with every request is only practical when the size of the cookie is small. In essence, client-side sessions trade server disk space for the extrabandwidth that each web request will require. Moreover, web browsers limit the number and size of cookies that may be stored by a web site. To improve efficiency and allow for more session data, the server may compress the data before creating the cookie, decompressing it later when the cookie is returned by the client.

```
#tcpclient.pl
use IO::Socket;

$socket = new IO::Socket::INET (
PeerAddr => '127.0.0.1',
PeerPort => 5000,
Proto => 'tcp',
)
or die "Couldn't connect to Server\n";
while (1)
{
$socket->recv($recv_data,1024);
if ($recv_data eq 'q' or $recv_data eq 'Q')
{
close $socket;
last;
}
else
{
print "RECIEVED: $recv_data";
print "\nSEND( TYPE q or Q to Quit):";
$send_data = <STDIN>;
chop($send_data);
if ($send_data ne 'q' and $send_data ne 'Q')
```

```

{
$socket->send($send_data);
}
else
{
$socket->send($send_data);
close $socket;
last;
}
}
}

```

❑ **Check Your Progress – 2 :**

1. Transmitting state back and forth with every request is only practical when the size of the cookie is \_\_\_\_\_.
  - a. Small
  - b. big

#### 14.4 Connectionless Server Side Program :

Communicating with a connectionless protocol is simpler than using a connection-oriented protocol, as both the client and the server use DatagramSocket objects. The code for the server-side program has the following pattern:

- Create a Datagram Socket object associated with a specified port number.
- Create a Datagram Packet object and ask the DatagramSocket to put the next piece of data it receives in the DatagramPacket.

On the client-side, the order is simply reversed :

- Create a Datagram Packet object associated with a piece of data, a destination network address, and a port number
- Ask a Datagram Socket object to send the data associated with the Datagram Packet to the destination associated with the Datagram Socket.

Let's look at an example that shows how this pattern can be coded into a server that provides the current time and a client that requests the current time. Here's the code for the server class :

```

public class TimeServer {
staticDatagramSocket socket;
public static void main(String[] argv) {
try {
socket = new DatagramSocket(7654);
}catch (SocketException e) {
System.err.println("Unable to create socket");
e.printStackTrace();
System.exit(1);
}
DatagramPacket datagram;

```

```
datagram = new DatagramPacket(new byte[1], 1);
while (true) {
    try {
        socket.receive(datagram);
        respond(datagram);
    } catch (IOException e) {
        e.printStackTrace();
    }
}

static void respond(DatagramPacket request) {
    ByteArrayOutputStream bs = new ByteArrayOutputStream();
    DataOutputStream ds = new DataOutputStream(bs);
    try {
        ds.writeLong(System.currentTimeMillis());
    } catch (IOException e) {
    }

    DatagramPacket response;
    byte[] data = bs.toByteArray();
    response = new DatagramPacket(data, data.length, request.getAddress(),
    request.getPort());
    try {
        socket.send(response);
    } catch (IOException e) {
        // Give up, we've done our best.
    }
}
}
```

❑ **Check Your Progress – 3 :**

1. \_\_\_\_\_ with a connectionless protocol is simpler than using a connection-oriented protocol.
  - a. Communicating
  - b. programming

<b>14.5 Connectionless Client Side Program :</b>
--

Connection-oriented transmission is like the telephone system in which you dial and are given a connection to the telephone of the person with whom you wish to communicate. The connection is maintained for the duration of your phone call, even when you are not talking.

Connectionless transmission with datagrams is more like the way mail is carried via the postal service. If a large message will not fit in one envelope, you break it into separate message pieces that you place in separate, sequentially numbered envelopes. Each of the letters is then mailed at the same time. The letters could arrive in order, out of order or not at all (the last case is rare,



but it does happen). The person at the receiving end reassembles the message pieces into sequential order before attempting to make sense of the message. If your message is small enough to fit in one envelope, you need not worry about the "out-of-sequence" problem, but it is still possible that your message might not arrive. One difference between datagrams and postal mail is that duplicates of datagrams can arrive at the receiving computer.

Connectionless communication is supported by DatagramSocket and DatagramPacket classes in java.net package. DatagramSocket class provides communication with connectionless socket and DatagramPacket provides datagram abstraction. These classes use the Unreliable Datagram Protocol (UDP) that makes no guarantees about delivery of packets or the order of delivered packets. The sender transmits UDP packets either and either it makes to receiver or it doesn't. UDP sockets are typically used in bandwidth-limited applications, where the overhead associated with resending packets is not tolerable.

**Java's java.net.DatagramSocket class**

```

Public class DatagramSocket extends Object {
public DatagramSocket()
throws SocketException;
public DatagramSocket(int port) throws SocketException;
public DatagramSocket(int port, InetAddress laddr) throws SocketException;
public void send(DatagramPacket p) throws IOException;

public synchronized void receive(DatagramPacket p) throws IOException;
public InetAddress getLocalAddress();
public int getLocalPort();

public synchronized void setSoTimeout(int timeout) throws
SocketException;
public synchronized int getSoTimeout() throws SocketException;
public void close();
}

```

**❑ Check Your Progress – 4 :**

1. Connectionless communication is supported by DatagramSocket and \_\_\_\_\_ .
  - a. DatagramPacket
  - b. Data less packet

**14.6 How to Listen to Socket Connections ?**

In order for a person to receive telephone calls, he must first have a telephone installed. Like wise you must create a socket to listen for connections. This process involves several steps. First you must make a new socket, which is similar to having a telephone line installed. The socket() command is used to do this.

Since sockets can have several types, you must specify what type of socket you want when you create one. One option that you have is the addressing format of a socket. Just as the mail service uses a different scheme to deliver mail as compared to a telephone company that uses a different approach to deliver calls, so can sockets differ. Sockets are used for IPC between processes on the same machine. Socket addressing, uses Internet addresses that are four-byte numbers usually written as four decimal numbers separated by periods (such as 192.9.200.10). In addition to the machine address, there is also a port number which allows more than one socket on each machine.

Another option which you must supply when creating a socket is the type of socket. The type that we will use here is the Datagram type. Datagram indicates that data will come in bunches (called datagrams). Streaming is another type.

**We create a socket as follows :**

```
DatagramSockets = new DatagramSocket();
```

After creating a socket, Client part of the code (only) must give the socket an address to listen to, just as you get a telephone number so that you can receive calls.

Sockets have the ability to queue incoming connection requests, which is a lot like having 'call-waiting' for your telephone. If you are busy handling a connection, the connection request will wait until you can deal with it.

After you create a socket to get calls, you must wait for calls to that socket. The receive() function is used to do this. Calling receive() is analogous to picking up the telephone if it's ringing. receive() returns a new socket that is connected to the caller.

The following function can be used to accept a connection on a socket that has been created using the Datagram Socket code above :

```
s.receive (dp);
```

Unlike the telephone, you may still accept calls while processing previous connections. For this reason you usually fork off jobs to handle each connection. You would use threads for this.

**❑ Check Your Progress – 5 :**

1. \_\_\_\_\_ have the ability to queue incoming connection requests, which is a lot like having 'call-waiting' for your telephone.
  - a. Sockets
  - b. datagram

**14.7 How to Talk Between Sockets ?**

Now that you have a connection between sockets you want to send data between them. The receive() and send() functions are used to do this, just as they are for normal files.

The code to send in Java is as follows: s.send(dp);

There is only one major difference between socket reading and writing and file reading and writing: you don't usually get back the same number of characters that you asked for, so you must loop until you have read the number of characters that you want.

**❑ Check Your Progress – 6 :**

1. The code to send in Java is \_\_\_\_\_.
  - a. s.send(dp);
  - b. send(dp);

**14.8 What to do when you're done with a socket ?**

Just as you hang up when you're through speaking to someone over the telephone, so you should close a connection between sockets. The normal close() function is used to close each end of a socket connection. If one end of a socket is closed and the other tries to write to its end, the write will return an error. The code to close a socket in Java is :

s.close());

socket programming with tcp

Client must contact server

server process must first be running

server must have created socket (door) that welcomes client's contact

Client contacts server by:

creating client–local TCP socket

specifying IP address, port number of server process

**❑ Check Your Progress – 7 :**

1. The code to close a socket in Java is
  - a. s.close()
  - b. s.exit()

**14.9 Let Us Sum Up :**

**In this unit, we have learned :**

A socket is a software endpoint that establishes bidirectional communication between a server program and one or more client programs.

The socket associates the server program with a specific hardware port on the machine where it runs so any client program anywhere in the network with a socket associated with that same port can communicate with the server program.

A server program typically provides resources to a network of client programs. Client programs send requests to the server program and the server program responds to the request.

There is only one major difference between socket reading and writing and file reading and writing: you don't usually get back the same number of characters that you asked for, so you must loop until you have read the number of characters that you want.

**14.10 Answers for Check Your Progress :**

**❑ Check Your Progress 1 :**

1 : a

**❑ Check Your Progress 2 :**

1 : a

**❑ Check Your Progress 3 :**

1 : a

**❑ Check Your Progress 4 :**

1 : a

**❑ Check Your Progress 5 :**

1 : a

**❑ Check Your Progress 6 :**

1 : a

**❑ Check Your Progress 7 :**

1 : a

#### **14.11 Glossary :**

1. **Repeater** : A network or communications device which propagates electrical signals from one cable to another, amplifying them to restore them to full strength in the process. Repeaters are used to counter the attenuation which occurs when signals travel long distances
2. **Router** : A device which forwards packets between networks. The forwarding decision is based on network layer information and routing tables, often constructed by routing protocols.
3. **Socket** : The Berkeley Unix mechanism for creating a virtual connection between processes. Sockets interface Unix's standard I/O with its network communication facilities. They can be of two types, stream (bi-directional) or datagram (fixed length destination-addressed messages). The socket library function `socket()` creates a communications end-point or socket and returns a file descriptor with which to access that socket. The socket has associated with it a socket address, consisting of a port number and the local host's network address.
4. **Virtual Circuit** : A connection-oriented network service which is implemented on top of a network which may be either connection-oriented or connectionless (packet switching).
5. **Virtual Memory** : a system whereby addressable memory is extended beyond main storage through the use of secondary storage managed by system software in such a way that programs can treat all of the designated storage as addressable main storage

#### **14.12 Assignment :**

Discuss the importance of socket.

#### **14.13 Activities :**

Explain the method of establishing socket connection.

#### **14.14 Case Study :**

Explain difference between UDP and TCP.

#### **14.15 Further Reading :**

1. Sams Teach Yourself Network Troubleshooting in 24 Hours, Jonathan Feldman, Sams Publishing, 2002.
2. Computer Networking Essentials, Debra Littlejohn Shinder, Cisco Press, 2001.

## **BLOCK SUMMARY :**

At last the gist of our detailed discussion is that networking Devices has been discussed in very dept, right from its origin i.e the networking Device like Switch, Hub, and Router etc. was explained in detail. Also different types of network like LAN network, SOHO, DHCP also explain in detail. Even the types of communication were discussed in. Here much emphasis was laid on explaining the foundation of networking i.e. the fundamentals of networking was explained in very detail to the students, Even it discuss the client and server communication Programming in well manner,socket programming is the way to communicate in client server network. In this block we also discuss coddng structure of client and server communication. How to listen socket ?, how to do connectionless and connection oriented programming in socket communication also discuss with programming. Through this block the readers will get a detailed overview of the topics under essentials and standards under network.

<b>BLOCK ASSIGNMENT :</b>
---------------------------

❖ **Short Questions :**

**Write a Short Note On :**

1. Router
2. DHCP Server
3. Terminal emulator
4. Network cards
5. Wireless router
6. 10 Gigabit ethernet standard
7. Broadband
8. s.close( )
9. receive( )
10. send( )
11. socket( )
12. datagrams

❖ **Long Questions :**

1. Write a note on HP-UX I/O Cards
2. Explain Firewall and its type in detail.
3. Difference between a synchronous and asynchronous sockets

**Introduction to  
Computer Network**

❖ **Enrolment No. :**

1. How many hours did you need for studying the units ?

Unit No.	1	2	3
No. of Hrs.			

2. Please give your reactions to the following items based on your reading of the block :

Items	Excellent	Very Good	Good	Poor	Give specific example if any
Presentation Quality	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Language and Style	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Illustration used (Diagram, tables etc)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Conceptual Clarity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Check your progress Quest	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____
Feed back to CYP Question	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	_____

3. Any other Comments

.....

.....

.....

.....

.....

.....

.....

.....