



Jawaharlal Nehru Engineering College

Laboratory Manual

COMPUTER NETWORK

For

Third Year Students CSE
Dept: Computer Science & Engineering (NBA Accredited)

FOREWORD

It is my great pleasure to present this laboratory manual for Third year engineering students for the subject of **Computer Networks** keeping in view the vast coverage required for visualization of concepts of *Computer Networks* with simple language.

As a student, many of you may be wondering with some of the questions in your mind regarding the subject and exactly what has been tried is to answer through this manual.

As you may be aware that MGM has already been awarded with ISO 9000 certification and it is our endure to technically equip our students taking the advantage of the procedural aspects of ISO 9000 Certification.

Faculty members are also advised that covering these aspects in initial stage itself, will greatly relived them in future as much of the load will be taken care by the enthusiasm energies of the students once they are conceptually clear.

Dr. S. D. Deshmukh
Principal

LABORATORY MANUAL CONTENTS

This manual is intended for the Third year students of IT & CSE branches in the subject of Computer Networks. This manual typically contains practical/Lab Sessions related Computer Network covering various aspects related the subject to enhanced understanding.

Although, as per the syllabus, only programs for simulation of various protocols on first layer, and installation of Operating Systems are prescribed. We have made the efforts to cover various aspects of the subject covering computer hardware components, software components networking aspects, Operating System concepts and programming aspects will be complete in itself to make it meaningful, elaborative understandable concepts and conceptual visualization.

Students are advised to thoroughly go through this manual rather than only topics mentioned in the syllabus as practical aspects are the key to understanding and conceptual visualization of theoretical aspects covered in the books.

Good Luck for your Enjoyable Laboratory Sessions

Prof. D.S.Deshpande
HOD, CSE

Mrs. P.V.Bidwai
Lecturer, CSE Dept.

DOs and DON'Ts in Laboratory:

1. Do not handle any equipment before reading the instructions/Instruction manuals
3. Observe type of sockets of equipment power to avoid mechanical damage
4. Do not forcefully place connectors to avoid the damage
5. Strictly observe the instructions given by the teacher/Lab Instructor

Instructions for Laboratory Teachers:

1. Submission related to whatever lab work has been completed should be done during the next lab session. The immediate arrangements for printouts related to submission on the day of practical assignments.
2. Students should be taught for taking the printouts under the observation of lab teacher.
3. The promptness of submission should be encouraged by way of marking and evaluation patterns that will benefit the sincere students.

WARM UP EXERCISES:

Define Single user operating system, multi-user operating system, real time operating system, Client Server, Master Slave and Peer to Peer Technologies, Different Operating Systems available. Difference between Windows Client Server, Linux Client Server and Novell Netware

Objectives of Computer Network. Definition of Protocol, Different Application layer protocols.

SUBJECT INDEX

1. Program to set up a dialup connection for Internet access.
2. Study of ISO-OSI reference model.
3. Program to set up a Broadband connection.
4. Details of switches, its configuration, specifications and various product and different manufacturers
5. Design of a network for a computer lab.
6. Study of wireless networks
7. Study of various internet providers along with the present plans available for different type of customers.
8. Creating network cable using crimping tool
- 9 Program to simulate OSI model
- 10 Study of TCP/IP
- 11 Program for compression and decompression of data.
- 12 Conduction of Viva-Voce Examinations
12. Submission
13. Evaluation and marking system

1. Program to setup a dialup connection for internet access

AIM: Program to set up a dialup connection for Internet access.

H/w, S/w Requirement: IBM-compatible 486 System, a hard drive, modem , telephone line, Min 8Mb memory, Win 98 S/w.

Theory:

Dialup connection:

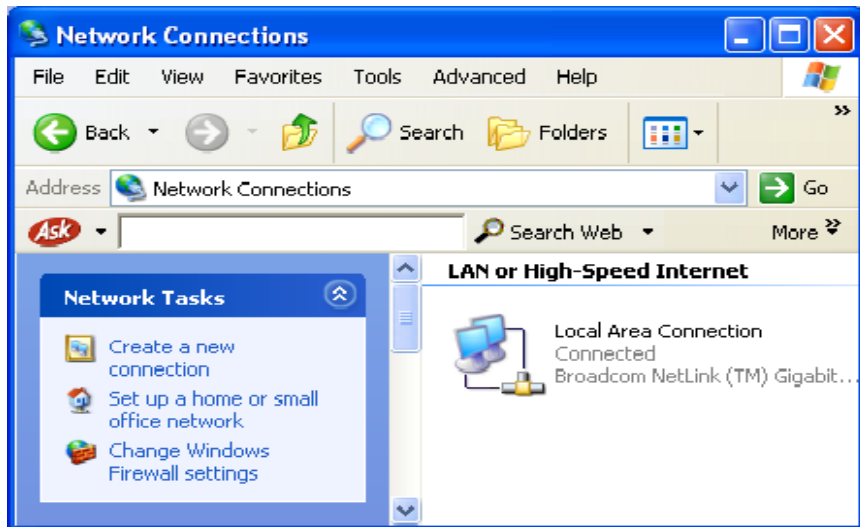
- It is a data communication link that is established when the communication equipment dials a phone number and negotiates a connection with the equipment on the other end of the link.
- It is the most popular form of Net connection for the home user, this is a connection from your computer to a host computer over standard telephone lines, and also it is a temporary connection between two computers via a telephone line normally using a modem.
- This is the most common method used to access the Internet. Setting up a dialup connection to the Internet is a common task. To set a dialup connection we require an Internet service provider and an telephone line

Steps to set up a dialup connection are as follows:

Step 1: Go to control panel

Step 2: Click on network connections

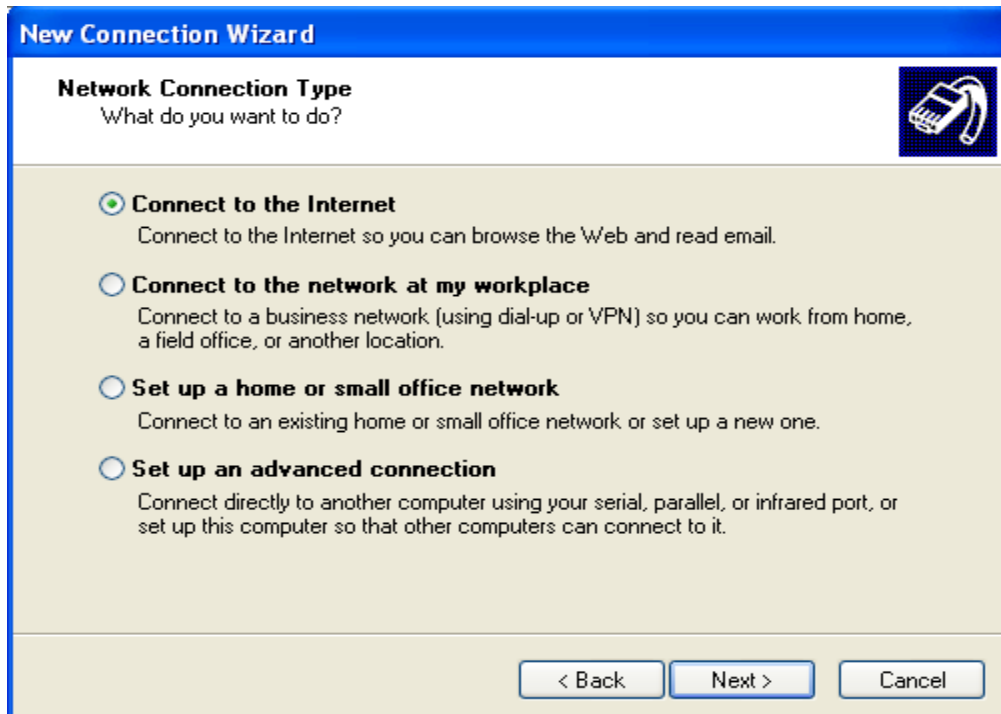
Step3: Click on create new connection



Step 4: The above window will appear



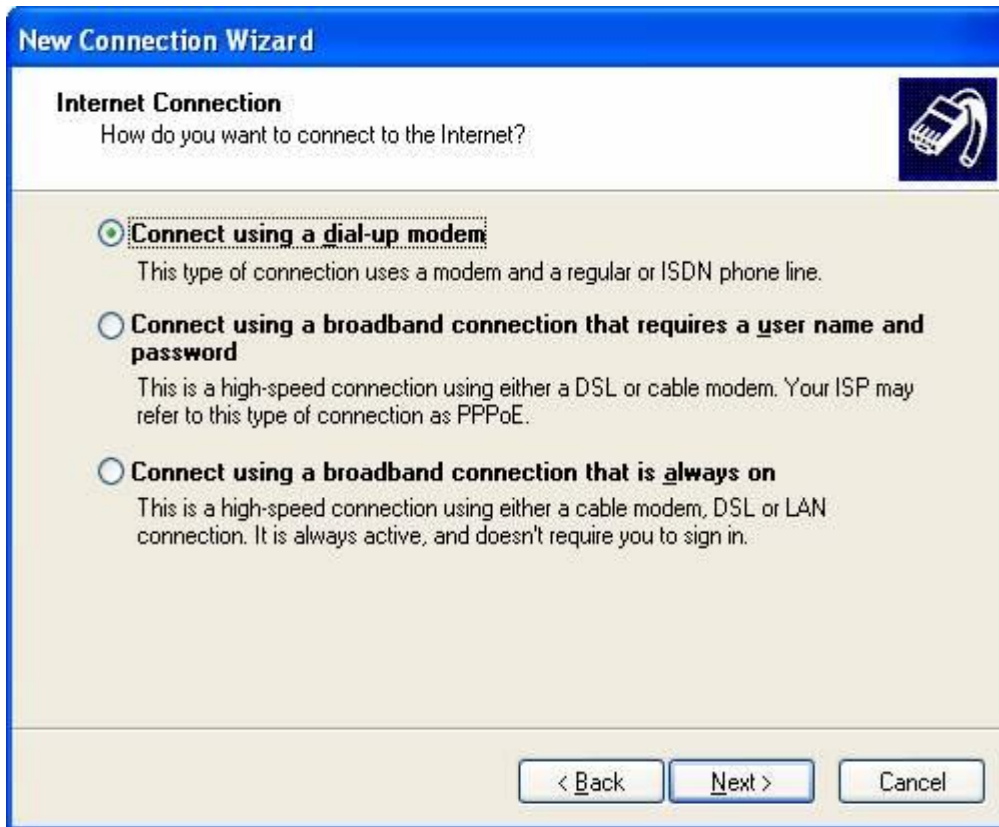
Step 5: Then Open up Network Connections in the Control Panel and choose the **Create a new network connection** button on the left-hand side. Click **Next**. Choose Connect to the Internet and click



Step 6: We are going to setup our connection manually. Choose this option and click **Next**.



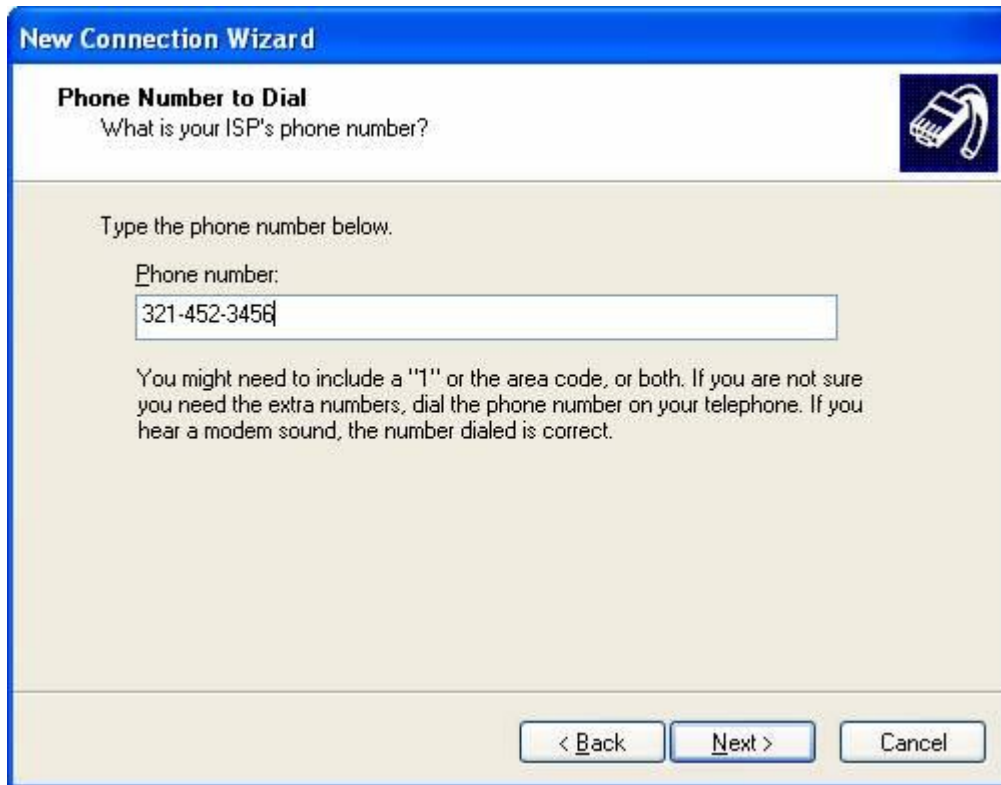
Step 7: Choose "Connect using a dial-up modem" and click **Next**



Step 8: Name your ISP and click **Next**.



Step 9: Enter the phone number you would like to dial and click **Next**.



New Connection Wizard

Phone Number to Dial
What is your ISP's phone number?

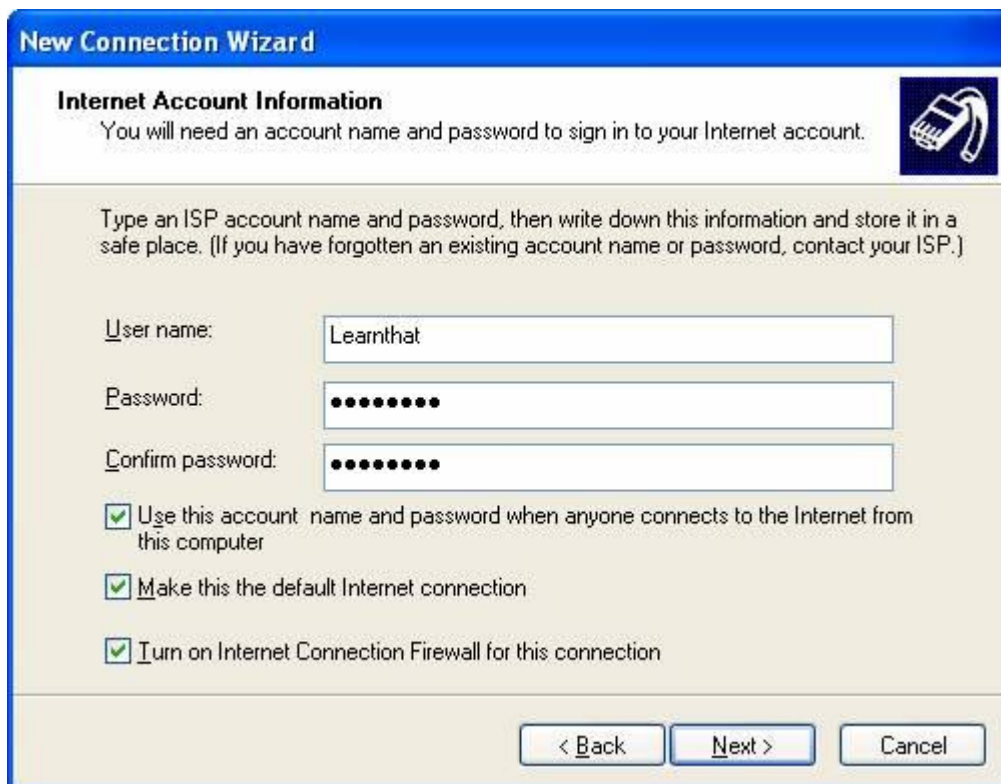
Type the phone number below.

Phone number:
321-452-3456

You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.

< Back Next > Cancel

Step 10: Enter your username and password for this connection and click **Next**



New Connection Wizard

Internet Account Information
You will need an account name and password to sign in to your Internet account.

Type an ISP account name and password, then write down this information and store it in a safe place. (If you have forgotten an existing account name or password, contact your ISP.)

User name: Learnthat

Password: ●●●●●●

Confirm password: ●●●●●●

Use this account name and password when anyone connects to the Internet from this computer

Make this the default Internet connection

Turn on Internet Connection Firewall for this connection

< Back Next > Cancel

Click **Finish**



It will automatically launch the connection dialog box. If you would like to connect, you can do so now, otherwise, you have this new icon in your Network Connections:



Congratulations! You have completed your setup of your new dialup connection.

Conclusion: Hence, we have set up a dialup connection.

2. Program to setup a Broadband connection for internet access

AIM: Setting up of broadband connection

H/w, S/w Requirement: IBM-compatible 486 System, a hard drive, modem , telephone line, Min 8Mb memory, Win 98 S/w.

Theory:

Broadband connection

- It is a high-speed Internet connection using DSL, cable, wireless, fiber optic or satellite means of transmitting data. This technology can transmit data, audio, and video all at once over long distances, it is a communication operating at a bandwidth greater than 2 Mbps.
- A communications network in which the bandwidth can be divided and shared by multiple simultaneous signals. A type of data transmission in which a single medium (wire) can carry several channels at once. Cable TV, for example, uses broadband transmission..
- A data-transmission scheme in which multiple signals share the bandwidth of a medium such as fiber-optic cable, it allows the transmission of voice, data and video signals over a single medium
- The term is commonly used to refer to communications lines or services at T1 rates (1.544 Mbps) and above. The speed threshold of broadband is subjective and can be above or below T1. Some claim 45 Mbps is the starting point of broadband. ...
- A high-speed, high-capacity transmission medium that can carry signals from multiple independent network carriers. This is done on a single coaxial or fiber-optic cable by establishing different bandwidth channels. Broadband technology can support a wide range of frequencies. ...

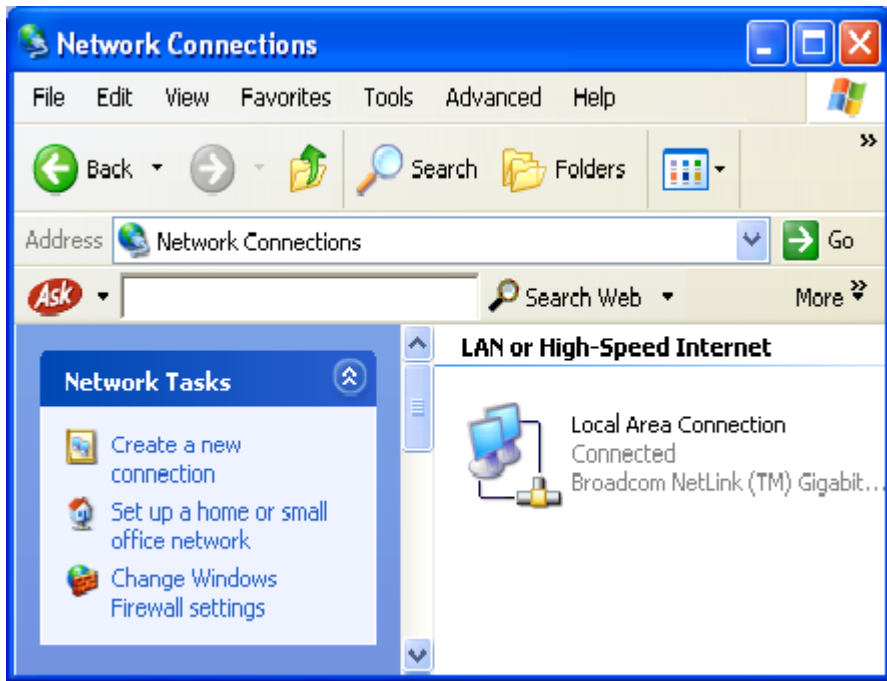
- Sometimes referred to as a high-speed internet, broadband is an ‘always on’ fast connection to the internet.
- Today there is a wide variety of broadband technologies available in most areas; two of the more commonly found and used technologies are cable and DSL broadband.

Following are the steps to set up an broadband connection:

Once you have subscribed to a broadband internet service provider, the next thing you have to do is set up the internet connection on your computer. You just have to follow the provider’s instructions in installing the network equipment that came from them. After which, you will need to set up your computer with the broadband internet connection.

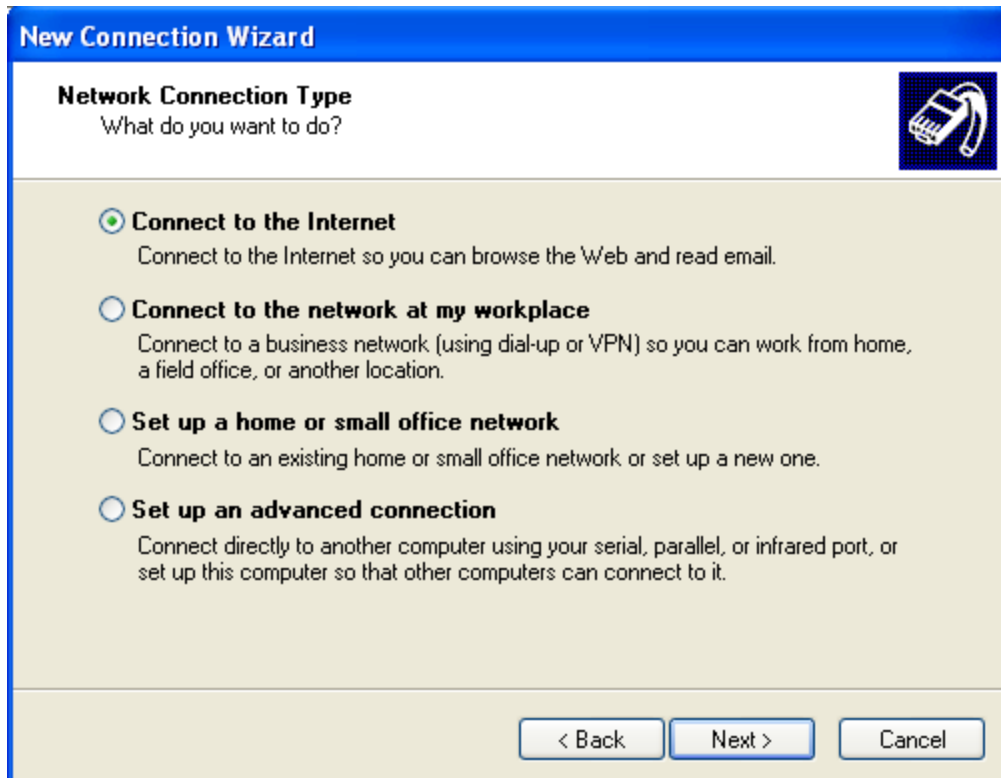
If you are using Windows XP, the steps are relatively easy as there is already a wizard that you just have to follow. The detailed instructions in setting up Windows XP for your broadband internet connection are as follows: (corresponding images are in the Images gallery)

1. Click *Start > Control Panel > Network and Internet Connections > Network Connections*. This path is true if Control Panel is in the Category View. If Control Panel is currently in the Classic View, just find *Network Connections* then click on it.
2. In the **Network Connections** window, there are several category options on the left panel. Click *Create a new connection* under **Network Tasks**.



3. The **New Connection Wizard** window will come up. Click *Next*. Under **Network Connection Type**, choose *Connect to the Internet* then click *Next*.



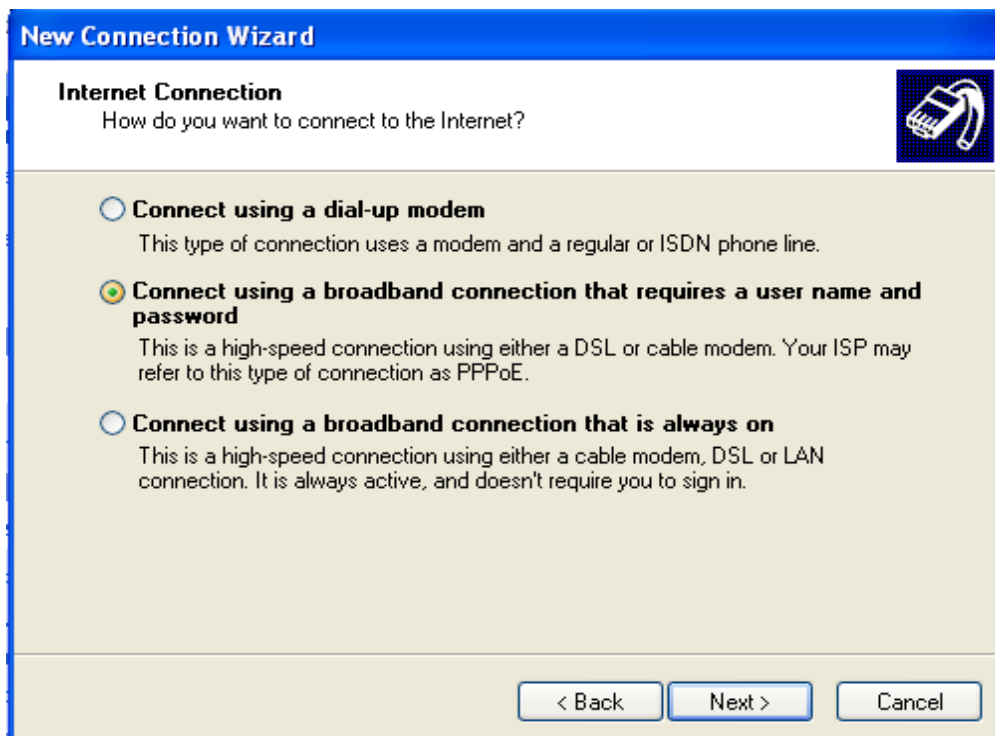


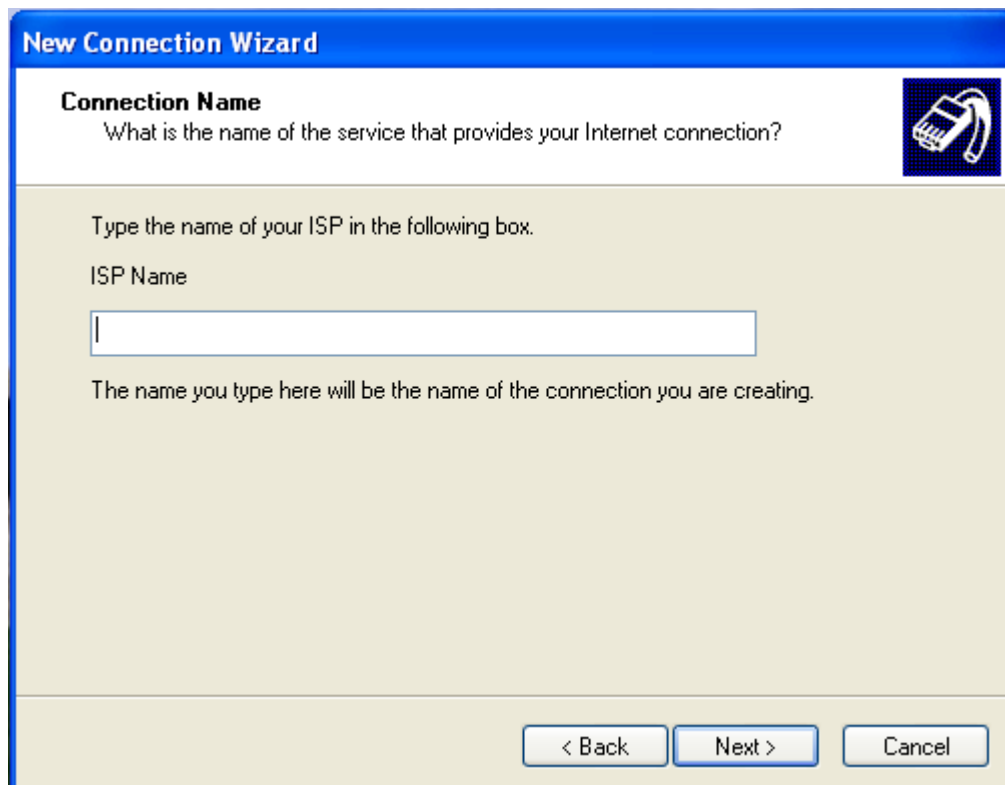
4. Select *Set up my connection manually*. Click *Next*.



5. Under **Internet Connection**, there are two options for broadband.

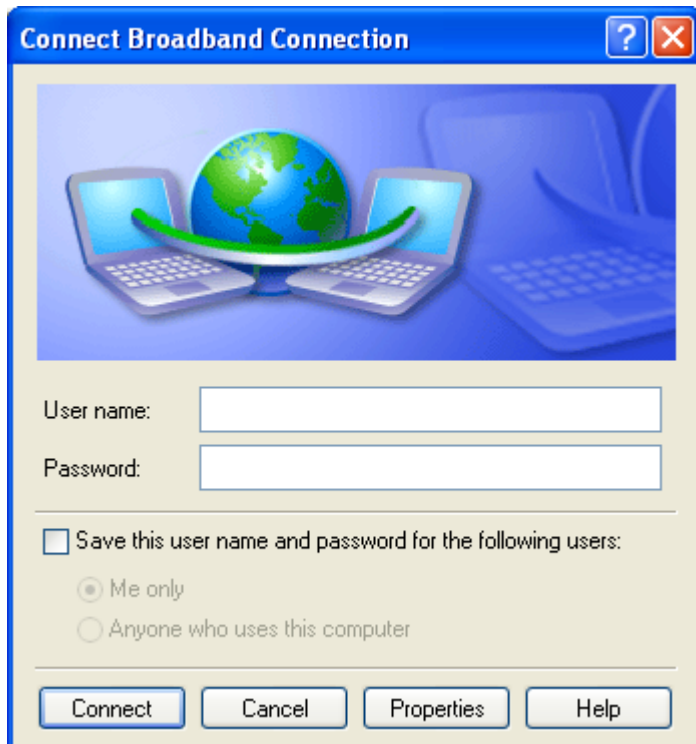
- If you are using **DSL connection**, choose the second option (*Connect using a broadband connection that requires a user name and password*). Click *Next*.
 - On the **ISP Name** field, type your preferred name for your Internet connection. Click *Next*.
 - On the **Connection Availability** window, choose *My use only*. Click *Next*.
 - Enter your account *Username* and *Password* on the **Internet Account Information** window. Click *Next*.
 - Click *Finish*.





- If you are using [Cable modem connection](#), choose the third option (**Connect using a broadband connection that is always on**). Click **Next**. Click **Finish**.





Once the wizard is finished, you are now ready to use the Internet. If you set up using DSL connection, you just need to click on the new icon added on your desktop then login. For Cable modem connection, you should be ready to browse websites now without the need to login

Conclusion: Hence, we have set up a broadband connection

3. Study of ISO-OSI Reference Model

AIM: Study of ISO-OSI Reference Model

H/w, S/w Requirement: IBM-compatible 486 System, a hard drive, Min 8Mb memory, Win 98 S/w.

Theory:

The *Open Systems Interconnect (OSI) reference model* is commonly used to describe in an abstract manner the functions involved in data communication. This model, originally conceived in the International Organization for Standardization (ISO), defines data communications functions in terms of layers.

In the OSI reference model, each *layer* is responsible for certain basic functions, such as getting data from one device to another or from one application on a computer to another. The functions at each layer both depend and build on the functions-called *services*- provided by the layers below it. Communication between peer entities at a given layer is done via one or more protocols; this communication is invoked via the *interface* with the layer below.

The OSI reference model is depicted in Table 0.1. Successful communication between two applications depends on successful functions at all seven layers. In terms of implementation, it is possible for some layers to be trivial; in the end what is required depends on the needs of the applications (and people) engaged in communication.

Table 0.1: OSI Reference Model

	Layer	Title
	7	Application
Higher Layers	6	Presentation
	5	Session
	4	Transport
	3	Network
Lower Layers	2	Data Link
	1	Physical

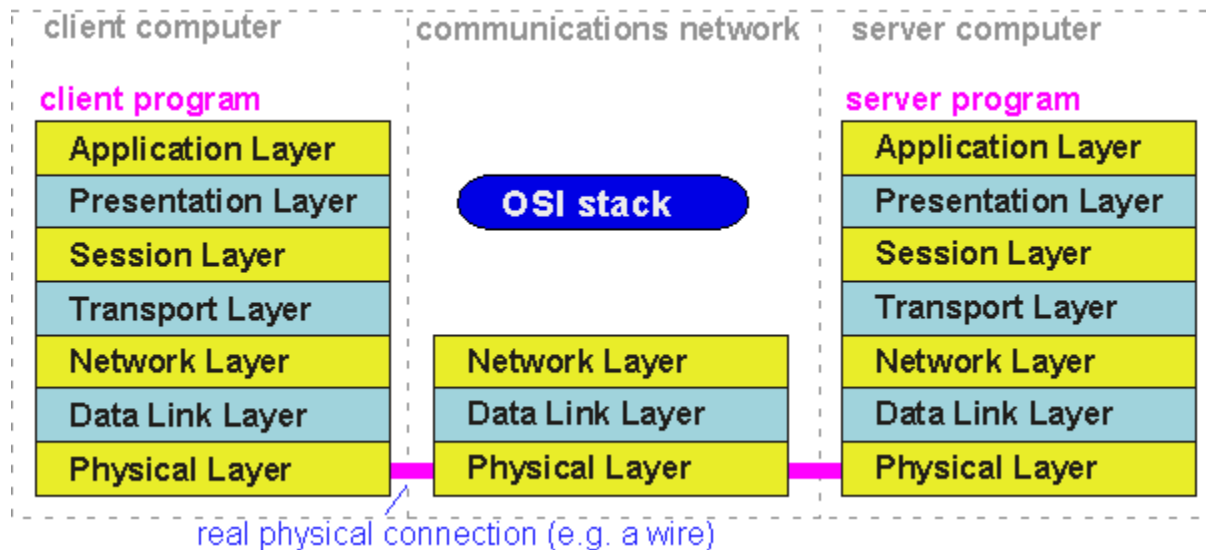


Figure 12: The OSI reference model applied to a communications network

Various companies and standards bodies have created different layered communications models, the OSI reference model remains the universally-accepted common denominator for abstract definition. Other models define the layer functions somewhat differently and often have fewer than seven layers. In some cases constituent protocols were specified before the abstract models defining the end-to-end communication.

Layer 1 - The Physical Layer

The *physical layer* functions include all physical aspects of communicating between two directly-connected physical entities. Typically these physical properties include electromechanical characteristics of the medium or link between the communicating physical entities such as connectors, voltages, transmission frequencies, etc. This layer summarizes the physics which underlie the communication path.

The essential service provided by the physical layer consists of an unstructured *bit stream*, which can be used by higher layers to provide the basis for higher layer communication services. An example of a physical layer is the ink on paper used by this book to convey information. Another example is the radio frequencies used in a wireless communications system.

Layer 2 - The Data Link Layer

The *data link layer* accepts the unstructured bit stream provided by the physical layer and provides reliable transfer of data between two directly-connected Layer 2 entities. "Directly-connected" means that the Layer 2 entities' communication path does not require another Layer 2 entity. However, this does not imply a dedicated path; in the case of Ethernet, many Layer 2 entities can be sharing a common (physical) medium such as a coaxial cable or a 10BASE-T hub.

Layer 2 functionality is limited in scope-delivery of messages over a local area. It could be likened to an intra-office correspondence between co-workers; there is a need for reliability but addressing is relatively simple. *Local area networks (LANs)* operate at Layer 2.

The data link layer is itself conceptually subdivided into two sublayers-medium access control and logical link control-which more specifically define the primary aspects of

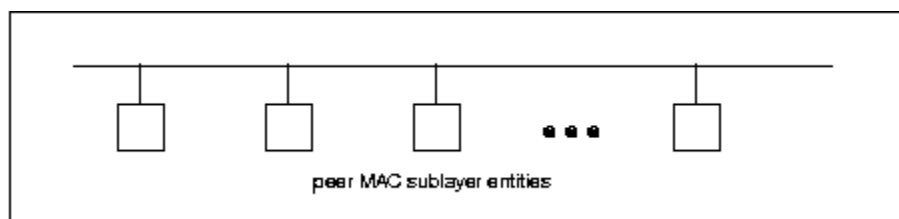
data link layer functionality. However, this conceptual partitioning by the IEEE 802 committee is somewhat arbitrary and subject to debate.

The MAC Sublayer

The *medium access control (MAC) sublayer* is closely associated with the physical layer and defines the means by which the physical channel (medium) may be accessed. It coordinates the attempts to seize a shared channel by multiple MAC entities, much as a school teacher must arbitrate between pupils' conflicting desires to speak. The MAC layer commonly provides a limited form of error control, especially for any header information which defines the MAC-level destination and higher-layer access mechanism.

Ethernet (IEEE 802.3) is a prime example of a shared medium with a defined MAC sublayer functionality. The shared medium in Ethernet has traditionally consisted of a coaxial cable into which multiple entities were "tapped," as depicted in Figure 0.5. Although this topology still applies conceptually, a hub and spoke medium is now typically used, in which the earlier coaxial cable has been physically collapsed into a *hub* device.

Figure 0.5: Ethernet MAC System

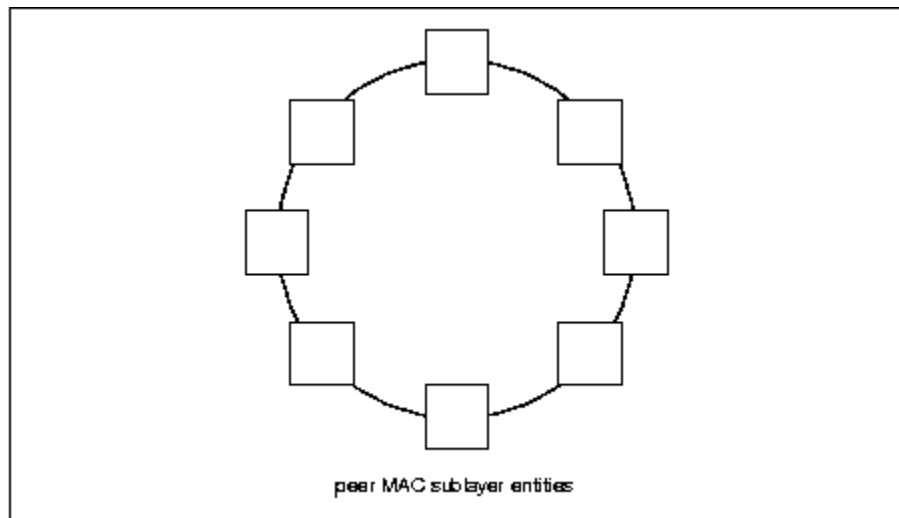


As a *contention* medium, Ethernet defines how devices *sense* a channel for its availability, wait when it is busy, *seize* the channel when it becomes available and *back-off* for a random length of time following a *collision* with another simultaneously transmitting device. On a shared channel, such as Ethernet, only a single entity can transmit at a time or messages will be garbled.

Not all shared channels involve contention. A prime example of a *contentionless* shared medium is *token ring (IEEE 802.5)*, in which control of the channel is rotated between the devices sharing the channel in a deterministic round-robin manner. Conceptually, control of the channel is given to the entity currently possessing a "token." If the device has nothing to transmit, it passes the token to the next device attached to the topological "ring," depicted in Figure 0.6.

Figure 0.6: Token Ring MAC System

1#1



IEEE-defined MAC sublayer addresses are six bytes long and permanently assigned to each device, typically called a *network interface card* or *NIC*. The IEEE administers the assignment of these addresses in blocks to manufacturers to assure the global

uniqueness that the MAC sublayer protocols rely on for "plug & play" network setup. Each manufacturer must assure individual device identifier uniqueness within their assigned block.

The LLC Sublayer

The *logical link control (LLC) sublayer* is responsible for reliable transfer of messages-called *frames* or, more formally, *link protocol data units (LPDUs)*-between two directly-connected Layer 2 entities. Functions needed to support this reliable transfer include *framing* (indicating where a Layer 2 message begins and ends), sequence control, error control and flow control.

The degree to which sequence, error and flow control are provided by the LLC sublayer is determined by whether the link protocol is connection-oriented or connectionless. A connectionless link protocol provides little if any support for these functions. A connection-oriented link might use a windowing technique for these functions, in which frames are individually numbered and acknowledged by their sequence number, with only a few such frames outstanding at any time.

The connection-oriented functions of sequencing, error and flow control provide a foundation for services provided by higher layers. As mentioned earlier, not all layer or sublayer functions are explicitly designed or implemented in any given system. Provision of these functions depends on the services required by higher layers.

If the connection-oriented functions of the LLC sublayer are not implemented, they must be performed by higher layers for reliable end-to-end communication. If these functions are provided by several layers, they might be somewhat redundant and add unnecessary overhead (inefficiency) to the system. In the worst case, redundant provision of these functions at multiple layers could serve cross purposes and actually degrade overall system performance.

An example of a connectionless LLC protocol is *frame relay (T1.617, 618)*, which defines point-to-point links with *switches* connecting individual links in a mesh topology. In a frame relay network, endpoints are connected by a series of links and switches. Because frame relay is defined in terms of the links between frame relay access devices (FRADs) and switches, and between switches themselves, it is an LLC protocol.

Connectionless Layer 2 protocols are best suited for high quality transmission media. With high quality transmission media, errors are rarely introduced in the transmission between network layer entities and discovery of and recovery from errors is most efficiently handled by the communicating hosts. In this case, it is better to move the packets quickly across the traversed subnetworks from source to destination rather than checking for errors at Layer 2.

Frame relay is derived from the *X.25 (ISO 8208)* protocol which spans Layers 2 and 3. *X.25* is a connection-oriented packet-switching technology which defines how neighboring *packet switches* exchange data with one another in a reliable manner from end-to-end. Frame relay simply removes the connection-oriented functions of error and sequence control; however, *congestion control* functions are provided in frame relay, to prevent the total traffic seen at any point in the network from overwhelming it.

Connection-oriented Layer 2 protocols are best suited for low quality transmission media where it is more efficient and cost-effective to discover and recover from errors as they occur on each hop than to rely on the communicating hosts to perform error recovery functions. With ever-increasing quality of transmission facilities and decreasing costs of computation capability at hosts, the need for connection-oriented network layer protocols is diminishing. However, *X.25* remains popular outside of North America, where it has been tariffed at levels which encourage its use.

End-to-end communications may be via shared or dedicated facilities or *circuits*. Shared facilities involve the use of *packet switching* technology to carry messages from end-to-end; messages are subdivided as necessary into packets, which share physical and logical channels with packets from various sources to various destinations. Packet switching is almost universally used in data communications because it is more efficient for the bursty nature of data traffic.

On the other hand, some applications require dedicated facilities from end-to-end because they are isochronous (e.g., voice) or bandwidth-intensive (e.g., large file transfer). This mode of end-to-end circuit dedication is called *circuit switched* communication. Because the facilities are dedicated to a single user, this tends to be much more expensive than the packet switched mode of communication. But some applications need it-it is an economic trade-off.

Dedicated circuits are a rather extreme form of connection-oriented protocol, requiring the same setup and tear-down phases prior to and following communication. If the circuit setup and tear-down is statically arranged (i.e., out-of-band), it is referred to as a *permanent virtual circuit* or *PVC*. If the circuit is dynamically setup and torn-down in-band, it is referred to as a *switched virtual circuit* or *SVC*.

Layer 3 - The Network Layer

The *network layer* defines the functions necessary to support data communication between indirectly-connected entities. It provides the capability of forwarding messages from one Layer 3 entity to another until the final destination is reached.

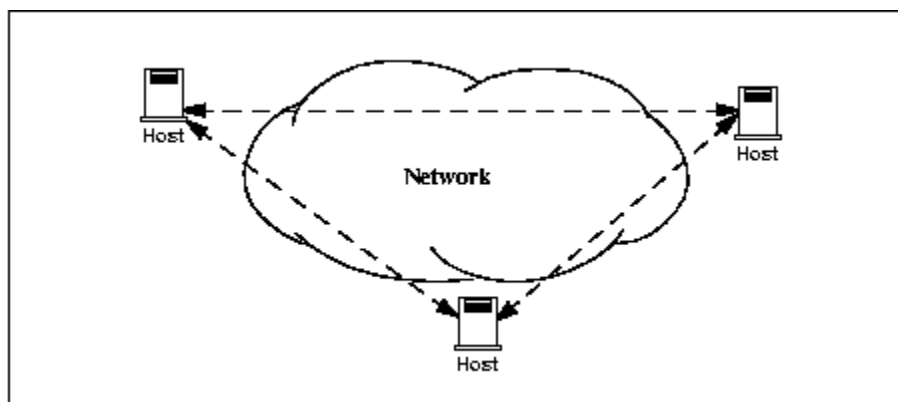
The network layer introduces another layer of abstraction to the data communications model. It moves messages-called *packets* or, more formally, *network protocol data units (NPDUs)*-between communicating Layer 3 entities-called *end systems, nodes* or

hosts. Network layer functions include route determination or *routing* and *forwarding* of packets to their final destinations.

In order to forward a packet to its destination host, routing information must be provided to the *intermediate systems (ISs)* or *routers* responsible for forwarding packets to their respective destinations. This routing information includes the *address* of the destination, which is contained in each packet. The next *hop* to be traversed by the packet is determined primarily by this destination address. We will talk more about addressing and routing in Chapter 1.

This packet forwarding and routing is accomplished independent of both the media and transmission types used at any step along the way. The unimportance of local topology to the network layer is demonstrated by the common use of "cloud diagrams" to depict networks, as in Figure 0.7. Since the network layer is concerned with getting packets across many local networks, called *subnetworks*, its title would be more accurate if it were the "Internetwork Layer."

Figure 0.7: Network Layer "Cloud" Diagram
1#1



The network layer functionality is global in scope-delivery of messages over a wide area. It could be likened to the postal system, in which correspondence is passed from location to location until it eventually reaches the destination address on the envelope. The network layer is the domain of *wide area networks (WANs)*.

In order for routers to know how (i.e., on which link) to forward packets, they must have some knowledge of network topology. This knowledge may be complete or partial, and is dynamically created and maintained via *routing protocols*, used by routers to share their knowledge of network topology with each other. Routing is essentially the reduction of global internetwork topology to local "hop-by-hop" routing decisions made independently by each router.

As with Layer 2, Layer 3 protocols may be connection-oriented or connectionless. A connection-oriented Layer 3 protocol, such as *X.25 (ISO 8208)*, operates more statically. The basic idea is that an end-to-end route (X.25 virtual connection) is established from the originating *data terminal equipment (DTE)* to *data communications equipment (DCE)*, from DCE to DCE through the network, then from the last DCE to the terminating DTE; this is the call setup. Packets are then transmitted via this prearranged route, with all packets following the same path through the network. Finally the route is torn down (release) and packets cease flowing.

X.25 operation is like a phone call because it *is* a phone call. X.25 Layer 3 operation assumes that a reliable connection-oriented service is provided by Layer 2 (also defined by the X.25 standard), although it does provide flow control via sequence numbers.

Connectionless Layer 3 protocols, such as the ever popular *internet protocol (IP)(RFC 791 and 792)* and its *ISO counterpart connectionless network protocol (CLNP) (ISO 8473)*, route packets dynamically. There is no prearranged path which is followed by subsequent packets flowing from one host to another. Instead each packet is

individually routed through a routing mesh; there is no reason to believe that sequential packets flowing between hosts will follow the same path. So sequence errors may be introduced at Layer 3, which must be corrected by a higher layer entity.

Connectionless data packets are commonly referred to as *datagrams* and the service provided by connectionless Layer 3 protocols is referred to as *datagram service*. Stateless datagram service is simpler for Layer 3 entities than connection-oriented network layer services. Because there is no state information to maintain, dynamic routing protocols can be used. If a router fails during the dialogue between two communicating hosts, neighboring routers will discover this via the routing protocols and find alternate routes which bypass the failed router.

There seems to be a fair amount of ambiguity between the network layer and the LLC sublayer. Both can provide connection-oriented or connectionless services to higher layers. To a large extent, if Layer 3 is explicitly implemented, there is no need for an LLC sublayer. The primary difference is in scope-LLC addresses and protocols are oriented toward a more local environment whereas network layer addresses and protocols are global in scope.

Excellent references to routing and forwarding of data packets can be found in [PERL92] and [STEN95].

Layer 4 - The Transport Layer

The *transport layer* is concerned with getting Layer 4 messages-called *segments* or, more formally, *transport protocol data units (TPDUs)* -from source to destination in a reliable manner. The perspective of Layer 4 is of end-to-end communications rather than the hop-by-hop perspective of Layer 3. Layer 4 assumes that packets can be moved from network entity to network entity, eventually getting to the final destination host. How this is accomplished is of no concern to Layer 4 functionality.

Like other layers, transport layer protocols can be either connection-oriented or connectionless, depending on the services required by higher layers. A common implementation of Layers 3 and 4 involves a connection-oriented transport layer protocol running over a connectionless network layer protocol, such as the ubiquitous TCP/IP protocol suite. In this instance, the communicating hosts maintain state information on communications with each other to determine when and what to send. This state information defines the connection between the communicating Layer 4 entities.

The general idea here is that two communicating hosts need not be concerned with the topology of the internetwork which lies between them. They only need to know the state of their pairwise communication. If part of the intervening internetwork "cloud" suffers a failure, the Layer 3 entities (routers) will deal with it and recover dynamically. Aside from potential retransmission of any lost segments, the hosts' Layer 4 entities do not have to be at all concerned with routing and recovery activities at Layer 3.

In the IP protocol suite, the primary connectionless Layer 4 protocol is the User Datagram Protocol (UDP)(RFC 768), which is carried by IP; the primary connection-oriented protocol is the Transmission Control Protocol (TCP)(RFC 793). The ISO world defines five classes of transport layer protocol, beginning with Class 0 (TP-0) for connectionless operation and range up to Class 4 (TP-4)(ISO 8073) for connection-oriented operation.

Layer 5 - The Session Layer

The *session layer* provides a control structure for communication between applications on hosts. The communication at layer 5 is called a *session*, which defines the relative timing of communications between the hosts' applications. Synchronization of

communicating applications comes into play when coordinated timing of corresponding events at the endpoints is imperative, such as in financial transactions.

Remember, layers define communication functions, not implementations. It is unlikely that a session layer would be explicitly implemented as a stand-alone program, although its functions would be implemented somewhere. Session layer functions depend on the reliability of communications between the endpoints, and session layer functions must therefore be implemented above Layer 4.

Layer 6 - The Presentation Layer

The *presentation layer* performs any necessary data transformations or formatting required by the end applications. Functions provided by the presentation layer include data compression, file formatting and encryption. Common data formatting is important because it allows the same application file to be accessed by the application running on different computer platforms. This book is itself the product of an application running on different platforms, with common files being modified via these different platforms.

Abstract Syntax Notation (ASN.1) is commonly used to specify data values in a way which allows processors to communicate independent of their varying native integer sizes, bit orderings (big or little endian), character sets, etc. ASN.1 is a transfer syntax, a presentation layer formatting, which appears frequently in the CDPD specification for unambiguous definition of network management, accounting, limited size messaging and other functions.

An example of ASN.1 encoding from an accounting Traffic Matrix Segment in the CDPD specification is the following:

TrafficType:= INTEGER {

registration (0),

deregistration (1),

ip(2),

clnp(3)

}

Layer 7 - The Application Layer

The *application layer* provides the services which directly support an application running on a host. These services are directly accessible by an application via common well-known *application program interfaces (APIs)*, which can actually occur at many layers. Examples of layer 7 services include *FTP (file transfer protocol)*, Telnet and *SNMP (simple network management protocol)*. Most network management activities are based on the services provided by layer 7 application entities, which in turn rely on lower layer services to be able to perform their functions

Conclusion: Hence ISO Model is studied.

4. Study of switches, configuration, specification, various products & manufacturers

Aim: Details of switches, its configuration, specifications and various products and different manufacturers

H/w, S/w Requirement: IBM-compatible 486 System, a hard drive, Min 8Mb memory, Win 98 S/w.

Theory:

Switch:

A **network switch** is a small hardware device that joins multiple computers together within one local area network (LAN). Technically, network switches operate at layer two (Data Link Layer) of the OSI model. Network switches appear nearly identical to network hubs, but a switch generally contains more intelligence (and a slightly higher price tag) than a hub. Unlike hubs, network switches are capable of inspecting data packets as they are received, determining the source and destination device of each packet, and forwarding them appropriately. By delivering messages only to the connected device intended, a network switch conserves network bandwidth and offers generally better performance than a hub.

As with hubs, Ethernet implementations of network switches are the most common. Mainstream Ethernet network switches support either 10/100 Mbps Fast Ethernet or Gigabit Ethernet (10/100/1000) standards.

Different models of network switches support differing numbers of connected devices. Most consumer-grade network switches provide either four or eight connections for Ethernet devices. Switches can be connected to each other, a so-called *daisy chaining* method to add progressively larger number of devices to a LAN.

LAN switches are used to connect a common broadcast domain (a hub). They are also used to provide frame-level filtering as well as dedicated port speed to specific end users. Some switches have limited routing capabilities and can provide Layer 3 routing functions at the most basic level. Some of the major benefits of using switches in a network are higher bandwidth to the desktop and ease of configuration. Switches are being deployed more often to replace hubs and bridges as more bandwidth-intensive applications are being implemented at all levels of an organization.

Types of switches

Form factor

Desktop, not mounted in an enclosure, typically intended to be used in a home or office environment outside of a wiring closet

- Rack mounted
- Chassis — with swappable "switch module" cards. E.g. Alcatel's Omni Switch 7000; Cisco Catalyst switch 4500 and 6500; 3Com 7700, 7900E, 8800.

Configuration options

- *Unmanaged* switches — These switches have no configuration interface or options. They are plug_and_play. They are typically the least expensive switches, found in home, SOHO, or small businesses. They can be desktop or rack mounted.
- *Managed* switches — These switches have one or more methods to modify the operation of the switch. Common management methods include: a serial console or command line interface accessed via telnet or Secure Shell, an embedded Simple Network Management Protocol (SNMP) agent allowing management from a remote console or management station, or a web interface for

management from a web browser. Examples of configuration changes that one can do from a managed switch include: enable features such as Spanning Tree Protocol, set port speed, create or modify Virtual LANs (VLANs), etc. Two subclasses of managed switches are marketed today:

- *Smart* (or intelligent) switches — These are managed switches with a limited set of management features. Likewise "web-managed" switches are switches which fall in a market niche between unmanaged and managed. For a price much lower than a fully managed switch they provide a web interface (and usually no CLI access) and allow configuration of basic settings, such as VLANs, port-speed and duplex.^[10]
- *Enterprise Managed* (or fully managed) switches — These have a full set of management features, including Command Line Interface, SNMP agent, and web interface. They may have additional features to manipulate configurations, such as the ability to display, modify, backup and restore configurations. Compared with smart switches, enterprise switches have more features that can be customized or optimized, and are generally more expensive than "smart" switches. Enterprise switches are typically found in networks with larger number of switches and connections, where centralized management is a significant savings in administrative time and effort. A stackable switch is a version of enterprise-managed switch.

Traffic monitoring on a switched network

Unless port mirroring or other methods such as RMON or SMON are implemented in a switch, it is difficult to monitor traffic that is bridged using a switch because all ports are isolated until one transmits data, and even then only the sending and receiving ports can see the traffic. These monitoring features rarely are present on consumer-grade switches.

Two popular methods that are specifically designed to allow a network analyst to monitor traffic are:

- Port mirroring — the switch sends a copy of network packets to a monitoring network connection.
- SMON — "Switch Monitoring" is described by RFC 2613 and is a protocol for controlling facilities such as port mirroring.

Another method to monitor may be to connect a Layer-1 hub between the monitored device and its switch port. This will induce minor delay, but will provide multiple interfaces that can be used to monitor the individual switch port.

Typical switch management features



[Linksys](#) 48-port switch



A rack-mounted switch with network cables

- Turn some particular port range on or off

- Link speed and duplex settings
- Priority settings for ports
- MAC filtering and other types of "port security" features which prevent MAC flooding
- Use of Spanning Tree Protocol
- SNMP monitoring of device and link health
- Port mirroring (also known as: port monitoring, spanning port, SPAN port, roving analysis port or link mode port)
- Link aggregation (also known as *bonding*, *trunking* or *teaming*)
- VLAN settings
- 802.1X network access control
- IGMP snooping

Link aggregation allows the use of multiple ports for the same connection achieving higher data transfer speeds. Creating VLANs can serve security and performance goals by reducing the size of the broadcast domain.

Manufacturers:

Many companies from countries like China, Hongkong, Taiwan, South Korea are the manufacturer of switch.

Conclusion:

Hence we have studied switches

5. Design a Network for a computer lab

Aim: Design a network for a computer lab

H/w, S/w Requirement: IBM-compatible 486 System, a hard drive, Min 8Mb memory, Win 98 S/w.

Theory:

Performance:

Perform the following steps as directed

Step 1: To make a Direct Cable connection

1. Click **Start**, click **Control Panel**, and then double-click **Network Connections**.
2. Under **Network Tasks**, click **Create a new connection**, and then click **Next**.
3. Click **Set up an advanced connection**, and then click **Next**.
4. Click **Connect directly to another computer**, and click **Next**.
5. Choose the role this machine will play in the communication. If this computer has the information to which you need to gain access, click **Host**. If this computer will access information from the other computer, click **Guest**.

Step 2: To Set Up the Host Computer

1. Click the connection device that you want to use for this connection (a parallel or serial port, or an infrared port), and then click **Next**.
2. Grant access to the users who are allowed to connect by selecting the appropriate check boxes, and then click **Next**.
3. Click **Finish** to end the configuration process.

Step 3 To Set Up the Guest Computer

1. Type a name to identify this connection, and then click **Next**.
2. Click the connection device that you want to use for this connection (a parallel or serial port, or an infrared port), and then click **Next**.
3. Decide whether this connection will be available for all users (click **Anyone's use**), or only for you (click **My use only**), and then click **Next**.
4. Click **Finish** to end the setup process

Step 4: To create Windows Workgroup

1. In Windows XP, right-click on **My Computer**, select **System Properties**.
2. Select the **Computer Name** tab, click on **Change**.
3. Enter the appropriate **Computer name** and **Workgroup**.
4. Make sure that every computer on your home network references the same workgroup.

Step 5:

- To configure TCP/IP
- To assign IP address, gateway, subnet mask, DNS

Step 6:

- To create domain
- Bring all the PC of Lab under a network using workgroup or domain.
- Create client and server

Conclusion:

Windows workgroup is established and used for sharing and transferring data between physically connected PCs.

6. Study of Wireless Networks

AIM: Study of wireless networks.

Theory:

Wireless network refers to any type of computer network that is wireless, and is commonly associated with a telecommunications network whose interconnections between nodes is implemented without the use of wires. Wireless telecommunications networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier and this implementation usually takes place at the physical level or "layer" of the network.

Although we use the term wireless network loosely, there are in fact three different types of network.

- Wide area networks that the cellular carriers create,
- Wireless local area networks, that you create, and
- Personal area networks, that create themselves.

They all have a part to play in developing wireless solutions, separately or in various combinations. This article describes these different types of network, and explains where each can add value.

Wide Area Networks

Wide Area Networks include the networks provided by the cell phone carriers such as Bell Mobility, Telus Mobility and Rogers Wireless. Originally providing cellular voice services, the carriers added data services as well, at first by overlaying digital data services on top of the early analogue voice services, and later by building out brand new generation voice-plus-data networks. Suffice it to say, wireless data services are

available just about everywhere you can use a voice cell phone (Another article describes the types of service that are available).

The carriers determine where to provide coverage based on their business strategy, and they also control Quality of Service (QoS). If you are a very large, powerful organization, the carriers may add additional network resources in your corporate tower, especially if you buy a large number of cell phones from them.

Where would you use WANs? You would use WANs when reach is the most important aspect of your solution, and speed is less important. Reach is important if you are providing wireless solutions to the public at large, for example, or you want to give your employees wireless access to your corporate data, whether they are in the office, across town, out of town, or (in some cases) in other countries.

You can't get too far in your study of wireless without running into technical terms. Here are some to start with:

- GSM/GPRS - the voice plus data network technology offered by Rogers Wireless, updated to EDGE in 2004
- 1XRTT (usually called 1X) - the latest voice plus data network technology offered by Bell Mobility and Telus Mobility

Both of these networks are completely incompatible with one another.

Wireless Local Area Networks

Wireless LANs are networks are set up to provide wireless connectivity within a finite coverage area. Typical coverage areas might be a hospital (for patient care systems), a university, the airport, or a gas plant. They usually have a well-known audience in mind, for example health care providers, students, or field maintenance staff. You would use WLANS when high data-transfer rate is the most important aspect of your

solution, and reach is restricted. For example, in a hospital setting, you would require a high data rate to send patient X-rays wirelessly to a doctor, provided he is on the hospital premises.

Wireless LANs work in an unregulated part of the spectrum, so anyone can create their own wireless LAN, say in their home or office. In principle, you have complete control over where coverage is provided. In practice, coverage spills over into the street outside exposing you to a particular range of vulnerabilities. Deliberately seeking WLAN vulnerabilities is called wardriving. Our region has its share of wardrivers, and a later article will describe our adventures during an International Wardriving Day.

Wireless LANs have their own share of terminology, including:

- 802.11 - this is the network technology used in wireless LANs. In fact, it is a family of technologies such as 802.11a, 802.11b, etc., differing in speed and other attributes
- WiFi - a common name for the early 802.11b standard.

In addition to creating your own private WLAN, some organizations (Starbucks) and some carriers (Telus Mobility) are providing high speed WLAN internet access to the public at certain locations. These locations are called hotspots, and for a price you can browse the internet at speeds about 20 times greater than you could get over your cell phone.

Personal Area Networks

These are networks that provide wireless connectivity over distances of up to 10m or so. At first this seems ridiculously small, but this range allows a computer to be connected wirelessly to a nearby printer, or a cell phone's hands-free headset to be

connected wirelessly to the cell phone. The most talked about (and most hyped) technology is called Bluetooth.

Personal Area Networks are a bit different than WANs and WLANs in one important respect. In the WAN and WLAN cases, networks are set up first, which devices then use. In the Personal Area Network case, there is no independent pre-existing network. The participating devices establish an ad-hoc network when they are within range, and the network is dissolved when the devices pass out of range. If you ever use Infrared (IR) to exchange data between laptops, you will be doing something similar. This idea of wireless devices discovering each other is a very important one, and appears in many guises in the evolving wireless world.

PAN technologies add value to other wireless technologies, although they wouldn't be the primary driver for a wireless business solution. For example, a wireless LAN in a hospital may allow a doctor to see a patient's chart on a handheld device. If the doctor's handheld was also Bluetooth enabled, he could walk to within range of the nearest Bluetooth enabled printer and print the chart.

Mobile devices networks

With the development of smart phones, cellular telephone networks routinely carry data in addition to telephone conversations:

- **Global System for Mobile Communications (GSM):** The GSM network is divided into three major systems: the switching system, the base station system, and the operation and support system. The cell phone connects to the base system station which then connects to the operation and support station; it then connects to the switching station where the call is transferred to where it needs to go. GSM is the **most common standard and is used for a majority of cell phones.**

- Personal Communications Service (PCS): PCS is a radio band that can be used by mobile phones in North America and South Asia. Sprint happened to be the first service to set up a PCS.
- D-AMPS: Digital Advanced Mobile Phone Service, an upgraded version of AMPS, is being phased out due to advancement in technology. The newer GSM networks are replacing the older system.

Uses:

Wireless networks have had a significant impact on the world as far back as World War II. Through the use of wireless networks, information could be sent overseas or behind enemy lines easily, efficiently and more reliably. Since then, wireless networks have continued to develop and their uses have grown significantly. Cellular phones are part of huge wireless network systems. People use these phones daily to communicate with one another. Sending information overseas is possible through wireless network systems using satellites and other signals to communicate across the world. Emergency services such as the police department utilize wireless networks to communicate important information quickly. People and businesses use wireless networks to send and share data quickly whether it be in a small office building or across the world.

Another important use for wireless networks is as an inexpensive and rapid way to be connected to the Internet in countries and regions where the telecom infrastructure is poor or there is a lack of resources, as in most developing countries. Compatibility issues also arise when dealing with wireless networks. Different components not made by the same company may not work together, or might require extra work to fix these issues. Wireless networks are typically slower than those that are directly connected through an Ethernet cable. A wireless network is more vulnerable, because anyone can try to break into a network broadcasting a signal. Many networks offer WEP - Wired Equivalent Privacy - security systems which have been found to be vulnerable to

intrusion. Though WEP does block some intruders, the security problems have caused some businesses to stick with wired networks until security can be improved. Another type of security for wireless networks is WPA - Wi-Fi Protected Access. WPA provides more security to wireless networks than a WEP security set up. The use of firewalls will help with security breaches which can help to fix security problems in some wireless networks that are more vulnerable.

Conclusion: Hence we have studied various wireless networks.

7. Study of Wireless Networks

AIM: Study of wireless networks.

Theory:

Study of various internet providers along with the present plans available for different type of customers

Theory:

An Internet Service Provider (ISP), sometimes called an Internet Access Provider, is a company that supplies individuals and businesses with access to the Internet. An ISP acts as an intermediary between a small business's computer system and the Internet. The ISP feeds the small business's outbound information to the Internet, and also feeds inbound Internet traffic into the small business's Internet connection. ISPs take several forms and offer a wide variety of services. They generally charge their customers for Internet access depending on their usage needs and the level of service provided.

Types of ISPs

Internet access is available from a wide range of companies, including telephone and cable companies, online services, large national ISPs, and small independent ISPs. In fact, an article in the *Philadelphia Business Journal* estimated that there were more than 7, 000 firms providing Internet access in the United States by mid-2000. The number of choices available makes selecting an ISP more difficult and time-consuming for small business owners. But the variety of providers also gives small businesses more options and keeps the price of Internet service competitive.

Online services—such as America Online (AOL) and Microsoft Network (MSN)—are probably the easiest way for beginners to gain access to the Internet. It is usually very easy to set up an account with one of the major online services. In fact, many of these companies include access programs on new computers or offer free setup software in

the mail. Computer users can establish an account and begin surfing the Internet with just a few clicks of a mouse. Unlike many other ISPs, the online services also offer a number of additional services to members, like discussion forums on various topics.

In some ways, online services may be a good way for small businesses owners to introduce themselves to the Internet. They provide a reliable connection and a safe environment. Subscribers to online services also tend to be more tolerant of promotional activities undertaken by fellow subscribers who also happen to be business owners. But as far as conducting business on the World Wide Web, online services have some disadvantages. For example, access to a small business's web site and promotional information may be limited to members of the online service. In addition, many online services charge high advertising fees—or collect a percentage of sales—when they are used to conduct Internet commerce. Finally, some online services monitor and restrict the content of information sent via e-mail or posted to newsgroups.

National ISPs—such as Earthlink and Mind Spring—are large companies that offer Internet access in a broad geographical area. Compared to local ISPs, these companies tend to offer higher-speed connections and greater long-term stability. Many national providers also offer a broad range of services, including long-distance telephone service, web site hosting, and secure electronic transactions. They are generally a good choice for small businesses that want employees to be able to access the Internet while traveling. They may also be convenient for businesses that operate in several locations and wish to use the ISP for all locations. The main disadvantages of the larger ISPs are that they rarely offer the level of personalized service available from smaller providers, and they may have so many customers that a small business's employees could have trouble gaining access during prime business hours.

Small, independent ISPs operate in many local or regional markets. These companies vary widely in size, stability, and quality of service. On the plus side, their access lines may be less busy than national ISPs. In addition, many smaller providers specialize in offering services to small businesses. Some of these ISPs may visit a small business customer's work site, evaluate the company's Internet access needs, and present different service packages. They may even assign a personal account representative to handle the small business's growing electronic needs.

Various Internet Plans

BSNL provides the following types of connections to access Internet to customer.

PSTN dial up access	BSNL internet service offers flexible options of access plans for PSTN dial-up in various slabs of 25,50,100, 200, 500 and 1,000 hours. With Sancharnet dialup account you get all India roaming advantage which is not available with any other ISP because you can access sancharnet internet by dialing '172233' from any city in India.
----------------------------	--

The following plans are available:

Limited access with 4MB email space

- Plans available in slabs of 25,50,100,200, 500 and 1000 hrs.
- one e-mail ID **and** one user ID per account(two in corporate account)

- Simultaneous logins per user ID shall be 2.
- 4 Mb E-mail space
- 1 MB web space

Limited access with 10MB email space

- Plans available in slabs of 500 and 1000 hrs.
- one e-mail ID and one user ID per account(two in corporate account)
- Simultaneous logins per user ID shall be 2.
- 10 MB e-mail space
- 1 MB webspace

Unlimited access with 10MB email space

- No limit of hours
- One User ID and one e-mail ID per package.
- Simultaneous logins restricted to one.
- Access restricted from two specified telephone numbers(CLIP restriction).
- 10 MB e-mail space
- 1 MB webspace

ISDN dial up access Enjoy blazing fast Internet surfing and download speeds in 64 and 128 Kbps ISDN dial up connections. **The uniform all India access no. for ISDN access is '172225'.**

64 and 128 Kbps-Limited access with 4MB email space

- Plans available in slabs of 25,50,100,200, 500 and 1000 hrs.
- one e-mail ID **and** one user ID per account(two in corporate account)
- Simultaneous logins per user ID shall be 2.
- 4 Mb E-mail space
- 1 MB web space

64 and 128 Kbps-Limited access with 10MB email space

- Plans available in slabs of 500 and 1000 hrs.
- one e-mail ID and one user ID per account(two in corporate account)
- Simultaneous logins per user ID shall be 2.
- 10 MB e-mail space
- 1 MB webspace

64 and 128 Kbps-Unlimited access with 10MB email space

- No limit of hours
- One User ID and one e-mail ID per package.
- Simultaneous logins restricted to one.
- Access restricted from two specified telephone numbers(CLIP restriction).
- 10 MB e-mail space
- 1 MB webspace

64 and 128 Kbps-Unlimited access with FIXED IP & 10MB email space

- No limit of hours
- One User ID and one e-mail ID per package.
- Simultaneous logins restricted to one.
- Access restricted from two specified telephone numbers(CLIP restriction)
- Fixed IP address assigned on access (customer has to apply for IP address separately)
- 10 MB e-mail space
- 1 MB webspace

Fixed monthly rental scheme

- No Call charges and Internet Access charges for accessing Sancharnet
- For calls other than Sancharnet,usual tariff applicable(addl to fixed rental)
- Applicable only for areas where DIAS is not available.
- No volume discounts etc
- Existing ISDN BRI connections can be converted.
- The rental shall be Rs 5500/- [Rs 5000/- plan charges and Rs 500/- rent]
- Initially launched only upto 30.04.2005

Leased access

line Enjoy round the clock internet connectivity at speeds varying from 64 Kbps to 45 Mbps. various plans are available to suit different needs. ISDN dial backup packages for Internet Leased Line Customers are also available.

- Tariff- leased Line Access Port Charges
- Tariff-ISDN dial backup packages for Internet Leased Line Customers

<p>Direct Internet Access (DIAS)</p>	<p>BSNL also provides DIAS in selected cities of the Country. The DIAS offers a wire-line solution for high speed symmetrical Internet access on the existing telephone lines. It provides an "always on" internet access that is permanently available at customer's premises. DIAS combines voice and internet data packets on a single twisted pair wire at subscriber premises that means you can use telephone and surf internet at the same time.</p> <ul style="list-style-type: none"> • More about DIAS technology>> • Cities where DIAS is available>> • DIAS Tariff
<p>Account free Internet dial up access based on CLI</p>	<p>Duration based Dialup Internet Service(CLI based) is a unique method providing Internet service in which the Customer can access the Internet service from any telephone through dial up. The service allows automatic registration on first LOGIN. The authentication will be based on CLI of the telephone with the password supplied by the caller. The charging is totally usage based and the service is a post paid service like normal PSTN.The billing will be separate based on the duration of use and will be charged to telephone bill(CLI based) as Internet access charge at the prescribed rate. The service is available in selected cities.The access no. of this service is '172222' in all cities.</p> <p>CLI based dial up internet service is also available for ISDN customers now.The access no. of this service is '172223'. This service is presently available in selected cities.</p>
<p>BROADBAND connection</p>	<p>Broadband service is based on DSL technology (on the same copper cable that is used for connecting telephone). This provides high speed internet connectivity up to 8Mbps. This is always - on internet access service with speed ranging from 256Kbps to 8 Mbps.</p>
<p>Wi-Fi</p>	<p>Wi-Fi Services have been introduced for providing high speed internet access at convenient public locations hereunder called as Hot Spots. Installation of Hot Spots is already under process at various cities/ locations. Hot Spot Type-A is applicable for public utility services like Airports, Railway Stations, Universities and their campus etc.</p>
<p>SANCHARNET CARD</p>	<p>BSNL has also launched "SANCHARNET CARD" recently. The Sancharnet Card" is a prepaid Internet Access Card with following features for customers:</p> <ul style="list-style-type: none"> • Self-register for internet access with your choice of userid • Renew your existing Sancharnet Account • Wide Range of Internet Access Packages • Sancharnet Cards are available in the following cities <p>Your browser does not support inline frames or is currently configured not to display inline frames.</p>

Conclusion: Hence we have seen various internet providers along with present internet plans available

6. Study of Wireless Networks

AIM: Study of wireless networks.

Theory:

Creating network cable using crimping tool

Theory:

Following are the steps to create Network cable using crimping tool



The steps below are general Ethernet Category 5 (commonly known as Cat 5) cable construction guidelines. For our example, we will be making a Category 5e patch cable, but the same general method will work for making any category of network cables.

Step 1:

Unroll the required length of network cable and add a little extra wire, just in case.

If a boot is to be fitted, do so before stripping away the sleeve and ensure the boot faces the correct way.

Step 2:

Carefully remove the outer jacket of the cable. Be careful when stripping the jacket as to not nick or cut the internal wiring. One good way to do this is to cut lengthwise with snips or a knife along the side of the cable, away from yourself, about an inch toward the open end. This reduces the risk of nicking the wires' insulation. Locate the string inside with the wires, or if no string is found, use the wires themselves to unzip the sheath of the cable by holding the sheath in one hand and pulling sideways with the string or wire. Cut away the unzipped sheath and cut the twisted pairs about 1 1/4" (30 mm). You will notice 8 wires twisted in 4 pairs. Each pair will have one wire of a certain color and another wire that is white with a colored stripe matching its partner



Step 3: **Inspect the newly revealed wires for any cuts or scrapes that expose the copper wire inside.** If you have breached the protective sheath of any wire, you will need to cut the entire segment of wires off and start over at step one. Exposed copper wire will lead to cross-talk, poor performance or no connectivity at all. It is important that the jacket for all network cables remains intact.



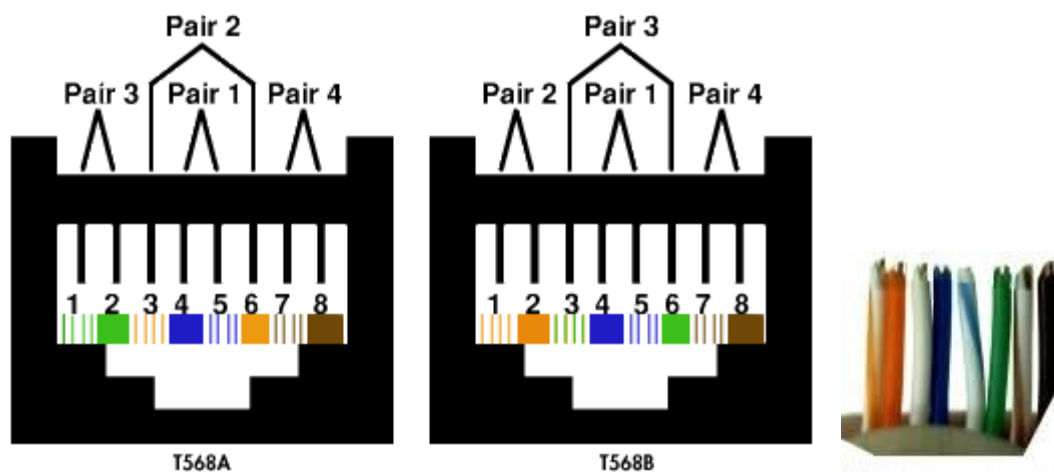
Step 4: **Untwist the pairs so they will lay flat between your fingers.** The white piece of thread can be cut off even with the jacket and disposed (see Warnings). For easier

handling, cut the wires so that they are 3/4" (19 mm) long from the base of the jacket and even in length.



Step 5: **Arrange the wires based on the wiring specifications you are following.** There are two methods set by the TIA, 568A and 568B. Which one you use will depend on what is being connected. A straight-through cable is used to connect two different-layer devices (e.g. a hub and a PC). Two **like** devices normally require a cross-over cable. The difference between the two is that a straight-through cable has both ends wired identically with 568A, while a cross-over cable has one end wired 568A and the other end wired 568B.^[1] For our demonstration in the following steps, we will use 568B, but the instructions can easily be adapted to 568A.

-
- 568B - Put the wires in the following order, from left to right:
 - white orange
 - orange
 - white green
 - blue
 - white blue
 - green
 - white brown
 - brown
 - 568A - from left to right: white/green, green, white/orange, blue, white/blue, orange, white/brown, brown. You can also use the mnemonic 1-2-3-6/3-6-1-2 to remember which wires are switched.



Step 6: **Press all the wires flat and parallel between your thumb and forefinger.** Verify the colors have remained in the correct order. Cut the top of the wires even with one another so that they are 1/2" (12.5 mm) long from the base of the jacket, as the jacket needs to go into the 8P8C connector by about 1/8", meaning that you only have a 1/2" of room for the individual cables. Leaving more than 1/2" untwisted can jeopardize connectivity and quality. Ensure that the cut leaves the wires even and clean; failure to do so may cause the wire not to make contact inside the jack and could lead to wrongly guided cores inside the plug.

Step 7:

Keep the wires flat and in order as you push them into the RJ-45 plug with the flat surface of the plug on top. The white/orange wire should be on the left if you're looking down at the jack. You can tell if all the wires made it into the jack and maintain their positions by looking head-on at the plug. You should be able to see a wire located in each hole, as seen at the bottom right. You may have to use a little effort to push the pairs firmly into the plug. The cabling jacket should also enter the rear of the jack about 1/4" (6 mm) to help secure the cable once the plug is crimped. You may need to stretch the sleeve to the proper length. Verify that the sequence is still correct before crimping.



Step 8:



Place the wired plug into the crimping tool. Give the handle a firm squeeze. You should hear a ratcheting noise as you continue. Once you have completed the crimp, the handle will reset to the open position. To ensure all pins are set, some prefer to double-crimp by repeating this step.

Step 9:

Repeat all of the above steps with the other end of the cable. The way you wire the other end (568A or 568B) will depend on whether you're making a straight-through, rollover, or cross-over cable

Step 10:



Test the cable to ensure that it will function in the field. Mis-wired and incomplete network cables could lead to headaches down the road. In addition, with power-over-Ethernet (PoE) making its way into the market place, crossed wire pairs could lead to physical damage of computers or phone system equipment, making it even more crucial that the pairs are in the correct order. A simple cable tester can quickly verify that information for you. Should you not have a network cable tester on hand, simply test connectivity pin to pin.

Conclusion: Hence we have created network cable using crimping tool.

8. Study of Wireless Networks

AIM: Study of wireless networks.

Theory:

Program for simulation of OSI Reference model. Sender and receiver side

Theory:

Simulation consist of two parts

- Sender side
- Receiver side

Sender side:

At the sender side, program the message that is to be sent to receiver to read from text. The message is then converted into ASCII by using toascii function .The ASCII form of message is then written into a new file using input() function. This new file is formed which contains ASCII form of original text message. The ASCII file is then opened in read mode, so that ASCII file can then be easily converted into binary form. Thus the original text is converted into binary form and then sent to the receiver side. Thus in short in sender side the text to be transmitted is first converted into binary form and then it is sent to receiver.

Receiver side:

At receiver side the binary form which was transmitted by sender is opened in read mode. The binary form stored in it is then converted into binary format. Thus we get original txt as it is without any error. Hence we can try that the text has transmitted easily.

Explanation of program

In this program we are converting contents of file into its binary form for transmission. In sender side contents of file are read one character at a time. This character is converted into its ASCII value using inbuilt C++ functions toascii() which gives ASCII values of particular character.

The ASCII value of a character is then converted into binary form by performing some mathematical calculations on it.And

finally this binary value is stored in separate file. This value procedure is performed for all characters in file and their respective values are stored in another file. At the receiver side the procedure is just the opposite of the above.

First and foremost the binary file produced is used and read character wise.

Then this char (binary values) ASCII values is computed and character associated with that value is printed.

Output:

Sender side

```
1. Enter File Name
2. Generate ASCII file
3. Generate Binary File
4. Exit
1
Enter File Name: plaintext.txt
```

```
The content of files are:
JNEC
```

```
1. Enter File Name
2. Generate ASCII file
3. Generate Binary File
4. Exit
2
```

```
The content of files is:
7478696710
```

```
1. Enter File Name
2. Generate ASCII file
3. Generate Binary File
4. Exit
3
```

```
The content of file is:
```

```
0000011100000100000001110000100000000110000010010000011000
0001110000000100000000
```

```
1. Enter File Name
2. Generate ASCII file
3. Generate Binary File
4. Exit
4
```

Receiver side:

1. Enter Binary File Name
2. Generate ASCII file
3. Generate Text File
4. Exit
1
Enter File Name: binary.txt
The content of files is:

0000011100000100000001110000100000000110000010010000011000
0001110000000100000000

1. Enter Binary File Name
2. Generate ASCII file
3. Generate Text File
4. Exit
2

The content of files is:
7478696710

1. Enter Binary File Name
2. Generate ASCII file
3. Generate Text File
4. Exit
3

The content of files is:
JNEC

1. Enter Binary File Name
2. Generate ASCII file
3. Generate Text File
4. Exit
4

Conclusion: Hence we have implemented the program for simulation of ISO_OSI model.

10. Study of Wireless Networks

AIM: Study of wireless networks.

Theory:

Study of DNS

Theory:

The **Domain Name System (DNS)** is a hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide. An often used analogy to explain the Domain Name System is that it serves as the "phone book" for the Internet by translating human-friendly computer hostnames into IP addresses. For example, *www.example.com* translates to *208.77.188.166*.

The Domain Name System makes it possible to assign domain names to groups of Internet users in a meaningful way, independent of each user's physical location. Because of this, World-Wide Web (WWW) hyperlinks and Internet contact information can remain consistent and constant even if the current Internet routing arrangements change or the participant uses a mobile device. Internet domain names are easier to remember than IP addresses such as 208.77.188.166 (IPv4) or 2001:db8:1f70::999:de8:7648:6e8 (IPv6). People take advantage of this when they recite meaningful URLs and e-mail addresses without having to know how the machine will actually locate them.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their particular domains, and in turn can assign other authoritative name servers for their sub-domains. This mechanism has made the DNS distributed, fault tolerant, and helped avoid the need for a single central register to be continually consulted and updated.

In general, the Domain Name System also stores other types of information, such as the list of mail servers that accept email for a given Internet domain. By providing a

worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

Other identifiers such as RFID tags, UPC codes, International characters in email addresses and host names, and a variety of other identifiers could all potentially utilize DNS.

The Domain Name System also defines the technical underpinnings of the functionality of this database service. For this purpose it defines the DNS protocol, a detailed specification of the data structures and communication exchanges used in DNS, as part of the Internet Protocol Suite (TCP/IP). The DNS protocol was developed and defined in the early 1980s and published by the Internet Engineering Task Force (cf. History).

The hierarchical domain name system, organized into zones, each served by a name server. The domain name space consists of a tree of domain names. Each node or leaf in the tree has zero or more *resource records*, which hold information associated with the domain name. The tree sub-divides into *zones* beginning at the root zone. A DNS zone consists of a collection of connected nodes authoritatively served by an *authoritative nameserver*. (Note that a single nameserver can host several zones.)

Administrative responsibility over any zone may be divided, thereby creating additional zones. Authority is said to be *delegated* for a portion of the old space, usually in form of sub-domains, to another nameserver and administrative entity. The old zone ceases to be authoritative for the new zone.

Parts of a domain name

A domain name usually consists of two or more parts (technically *labels*), which are conventionally written separated by dots, such as example.com.

- The rightmost label conveys the top-level domain (for example, the address www.example.com has the top-level domain com).
- Each label to the left specifies a subdivision, or subdomain of the domain above it. Note: “subdomain” expresses relative dependence, not absolute dependence. For example: example.com is a subdomain of the com domain, and www.example.com is a subdomain of the domain example.com. In theory, this subdivision can go down 127 levels. Each label can contain up to 63 octets. The whole domain name may not

exceed a total length of 253 octets. [8] In practice, some [domain registries](#) may have shorter limits.

- A hostname refers to a domain name that has one or more associated IP addresses (e.g., the 'www.example.com' and 'example.com' domains are both hostnames, whereas the 'com' domain is not).

DNS Organization and Structure

The Internet's DNS exactly maps the 'Domain Name' delegation structure described above. There is a DNS server running at each level in the delegated hierarchy and the responsibility for running the DNS lies with the AUTHORITATIVE control at that level.

Figure 1-2 shows this diagrammatically.

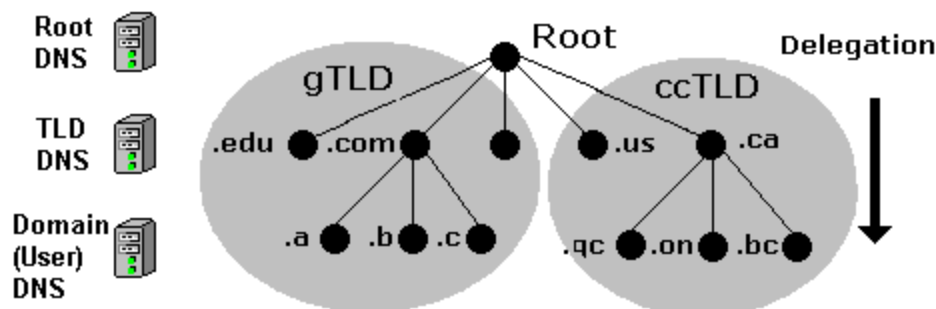


Figure 1-2 DNS mapped to Domain Delegation

The Root Servers (Root DNS) are the responsibility of ICANN but operated by a consortium under a delegation agreement. ICANN created the Root Servers Systems Advisory Committee (RSSAC) to provide advice and guidance as to the operation and development of this critical resource. The IETF was requested by the RSSAC to develop the engineering standards for operation of the Root-Servers. This request resulted in the publication of RFC 2870.

There are currently (mid 2003) 13 root-servers world-wide. The Root-Servers are known to every public DNS server in the world and are the starting point for every name lookup operation (or query). To create additional resilience each root-server typically has multiple **instances** (copies) spread throughout the world. Each instance has the same IP address but data is sent to the closest instance using a process called **anycasting**.

The TLD servers (ccTLD and gTLD) are operated by a variety of agencies and organizations (under a fairly complex set of agreements) called **Registry Operators**.

The Authority and therefore the responsibility for the User (or **Domain Name**) DNS servers lies with the owner of the domain. In many cases this responsibility is delegated by the owner of the Domain to an ISP, Web Hosting company or increasingly a registrar. Many companies, however, elect to run their own DNS servers and even delegate the Authority and responsibility for sub-domain DNS servers to separate parts of their organization.

When any DNS cannot answer (resolve) a request (a **query**) for a domain name from a client, for instance, example.com, the query is passed to a **root-server** which will direct (**refer**) the query to the appropriate TLD DNS server (for .com) which will in turn direct (**refer**) it to the appropriate Domain (User) DNS server.



2.2.4 DNS System Components

A Domain Name System (DNS) as defined by RFC 1034 includes three parts:

1. Data which describes the domain(s)
2. One or more Name Server programs.
3. A resolver program or library.

A single DNS server may support many domains. The data for each domain describes global properties of the domain and its hosts (or services). This data is defined in the form of textual Resource Records organized in Zone Files. The format of Zone files is defined in RFC 1035 and is supported by most DNS software.

The Name Server program typically does three things:

1. It will read a configuration file which defines the zones for which it is responsible.
2. Depending on the Name Servers functionality a configuration file may describe various behaviours, for instance, to cache or not. Some DNS servers are very specialized and do not provide this level of control.
3. Respond to questions (**queries**) from local or remote hosts.

The resolver program or library is located on each host and provides a means of translating a users request for, say, www.thing.com into one or more queries to DNS servers using UDP (or TCP) protocols.

Note: The resolver on all Windows systems and the majority of *nix systems is actually a **stub** resolver - a minimal resolver that can only work with a DNS that supports recursive queries. The caching resolver on MS Windows 2K and XP is a **stub** resolver with a cache to speed up responses and reduce network usage.

While BIND is the best known of the DNS servers and much of this guide documents BIND features, it is by no means the only solution or for that matter the only Open Source solution.. The zone file formats which constitute the majority of the work (depending on how many sites you operate) is standard (defined by RFC 1035) and is typically supported by all DNS suppliers. Where a feature is unique to BIND we indicate it clearly in the text so you can keep your options **open**

Conclusion: Hence we have studied DNS.

Quiz on the subject:

Quiz should be conducted on tips in the laboratory, recent trends and subject knowledge of the subject. The quiz questions should be formulated such that questions are normally is from the scope outside of the books. However twisted questions and self formulated questions by the faculty can be asked but correctness of it is necessarily to be thoroughly checked before the conduction of the quiz.

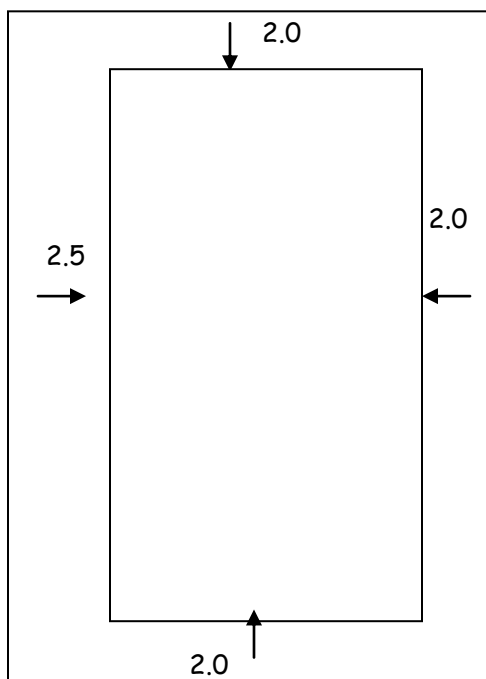
9. Conduction of Viva-Voce Examinations:

Teacher should oral exams of the students with full preparation. Normally, the objective questions with guess are to be avoided. To make it meaningful, the questions should be such that depth of the students in the subject is tested Oral examinations are to be conducted in co-cordial environment amongst the teachers taking the examination. Teachers taking such examinations should not have ill thoughts about each other and courtesies should be offered to each other in case of difference of opinion, which should be critically suppressed in front of the students.

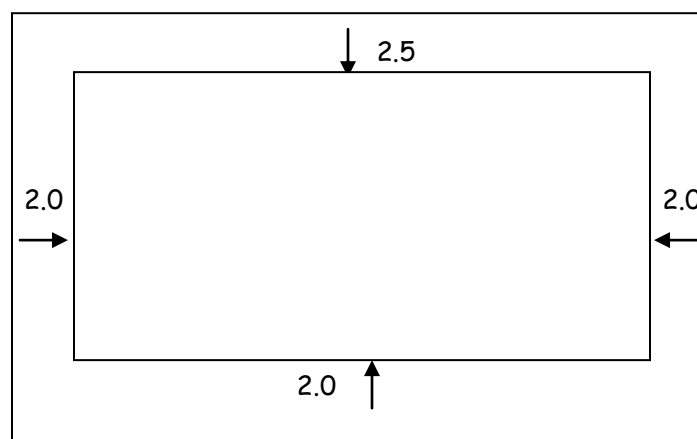
10. Submission:

Document Standard:

- | | |
|--|----------------|
| A] Page Size | A4 Size |
| B] Running text | Justified text |
| C] Spacing | 1 Line |
| D] Page Layout and Margins (Dimensions in Cms) | |
- Normal Page



Horizontal



Description	Font	Size	Boldness	Italics	Underline	Capitalize
College Name	Arial	24	-----	-----	Yes	-----
Document Title	Tahoma	22	-----	-----	-----	-----
Document Subject	Century Gothic	14	-----	-----	-----	Capital
Class	Bookman old Style	12	-----	-----	-----	-----
Document No	Bookman old Style	10	-----	-----	-----	-----
Copy write inf	Bookman old Style	9	-----	-----	-----	-----
Forward heading	Bookman old Style	12	-----	-----	Yes	Capital
Forward matter	Bookman old Style	12	-----	-----	-----	-----
Lab man Contents title	Bookman old Style	12	-----	-----	Yes	Capital
Index title	Bookman old Style	12	Yes	-----	Yes	Capital
Index contents	Bookman old Style	12	-----	-----	-----	-----
Heading	Tahoma	14	Yes	Yes	Yes	-----
Running Matter	Comic Sans MS	10	-----	-----	-----	-----

11. Evaluation and marking system:

Basic honesty in the evaluation and marking system is absolutely essential and in the process impartial nature of the evaluator is required in the examination system to become popular amongst the students. It is a wrong approach or concept to award the students by way of easy marking to get cheap popularity among the students to which they do not deserve. It is a primary responsibility of the teacher that right students who are really putting up lot of hard work with right kind of intelligence are correctly awarded.

The marking patterns should be justifiable to the students without any ambiguity and teacher should see that students are faced with unjust circumstances..