COMPUTER COURSE FOR DATABASE MANAGERS

ROORKEE

JULY 30 - AUG 9 1996

(UNDER WORLD BANK AIDED HYDROLOGY PROJECT)

MODULE - 9

COMPUTER NETWORKS

by

Dr.S.K.JAIN
SONIA BAKSHI

NATIONAL INSTITUTE OF HYDROLOGY
ROORKEE - 247 667 (U.P.)

COMPUTER NETWORKS

1. INTRODUCTION TO NETWORKS

Computer network means interconnection of autonomous (stand-alone) computers for information exchange. The connecting media could be a copper wire, optical fibre, micro-wave or satellite. The physical location of a network could be a single or multi-storeyed building or a building complex covering an area as wide as the world itself.

The term, a 'local area network' (LAN) is used to describe a network covering an area ranging from a room to a small complex such as a university campus. The physical distance covered varies from 1 m. to 1 km. The term 'wide area network' (WAN) is used when the physical distance covered is more than 10 kms. WAN could be spread over a city, a district, or a country. It may also include the whole globe. Sometimes the term long haul network is also need to mean a wide area network.

In particular LANs used in engineering environment consist of mainframes as well as engineering workstations. In a manufacturing environment they support a broad variety of applications including manufacturing, resource planning, real time process control, inventory control, maintenance management etc. Devices in this type of network include powerful mini-computers with monitoring and logic controllers. In this real environment, errors as well as down time can cause unacceptable delays and cost overruns. Network performance and reliability are very critical.

The wide area networks consist of medium/large mainframes with a variety of peripheral devices. WAN also includes a variety of switching, equipment and communication software to facilitate easy access by users. In this environment user accesses the network through a variety of computer interfaces. The applications that can be performed on a network are unlimited.

2. DEFINITION OF A LOCAL AREA NETWORK

Local Area Network is a transmission system that allows a large number and variety of computing equipment to exchange information at high speeds, over limited distances. The computing equipment may range from large mainframe system to personal computers and peripherals.

Resource Sharing is perhaps the greatest advantage of local area networks. LAN allows a large number of intelligent devices to share resources, such as storage devices, program files and even data files.

Area Covered by the LANs are normally restricted to moderate size, such as an office building, a factory, or a campus. The limiting factors are usually the overall length of the cable used and any interdevice restrictions imposed. In practice, the distances involved range from a few meters to a few kilometers.

Low Cost per Connection is also an important characteristic of LANs. Many applications for LANS involve low-cost microprocessor systems, so that the connection of these systems to a LAN should also be inexpensive.

High Channel Speed is another quality of LANs. Most LANs transfer data at rates between 1-10 million bits per second. This is equivalent to 200 pages of the book you are presently reading. This is especially beneficial for applications with high resolution, movable colour graphics and for. bulk data transfer between mainframe computers.

The block schematic of a typical local area network is shown in Fig. 1. It consists of several workstations and servers. The workstations can be a personal computer or a workstation with multi-user and multi-tasking capability. A server on the network, as the name implies, provides a specific service for all workstations. The example shown in the figure are the File Server, Print Server and Communication Server. They provide file storage and access facility, printing facility and external communication facility respectively to all the workstations connected to the local area network.

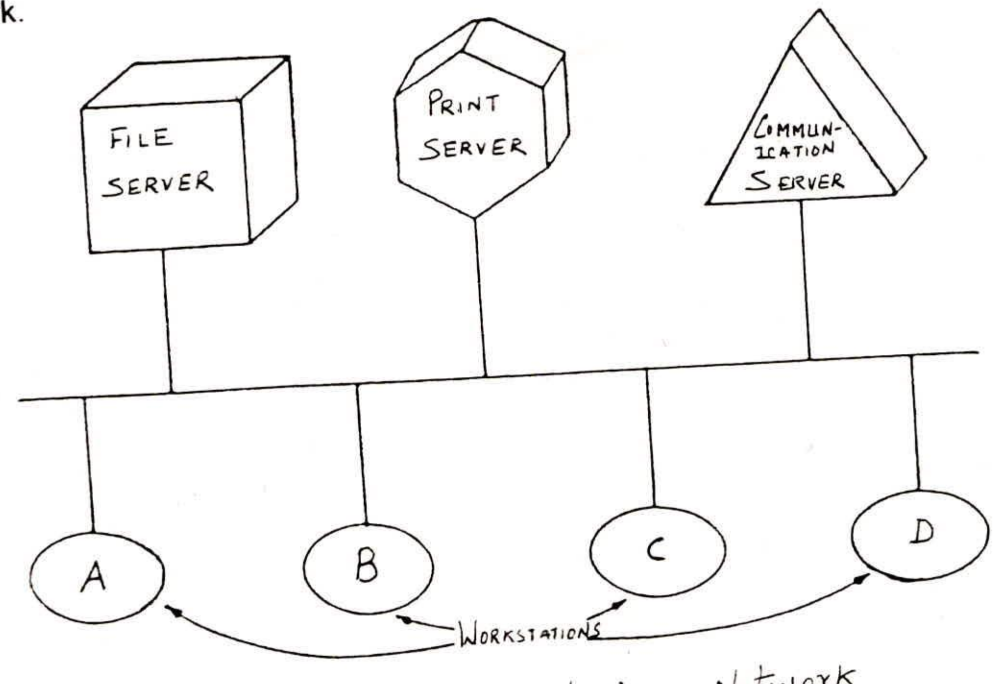

Fig. 1 A Typical Local Area Network

3. CHARACTERISTICS OF LOCAL AREA NETWORKS

A LAN is best described by the following characteristics :

- LAN is wholly contained within a limited geographical area.
- LAN provides a high degree of interconnection between devices which are otherwise independent.
- LAN uses inexpensive transmission media and interface to devices.
- Every device has the potential to communicate with any other device on the LAN.
- LANs facilitate sharing of information and Hardware.

The LANs can be compared by considering the following factors :

- The type of cabling used.
- The topology.
- Method used to control access to the shared medium.
- The nature of the interface unit which connects a device to the network.
- The rate at which digital data can be transmitted across the common shared line.
- The application services that are provided on the LAN.
- The facilities that are available to configure and manage the LAN.

Some examples of LAN are Ethernet, IEEE 802.3, Token Ring and Token Bus.

4. COMPUTER NETWORK TOPOLOGY

It is a different way of interconnections of computers. Network topology is the basic outlay or design of a computer network. Think of topology as the architectural drawing of the network components, which is much like the architectural drawing of a home or building (some are simple, some are very complex). This design can be varied in accordance with the company's needs, but certain base elements to configure the topology of a network still apply. Any system on a network is called a node. Nodes are connected to each other by links. Links can be phone lines, private lines, satellite channels, etc. When user draw a road map of the communication links between nodes, then he gets a network topology.

The main considerations in selecting a particular topology are :

(1) The availability and cost of physical communication lines between nodes and line bandwidth.
(2) The capability of a node to route information to other nodes.
(3) Delays due to routing of information.
(4) Reliability of communication between nodes when there is a breakdown of a line or a node.
(5) Strategy of controlling communication between nodes in the network centralised or distributed.

Following are the different topologies :

4.1 Ring Topology :

Five computers A, B, C, D, E are to be interconnected by physical links between A-C, A-E, D-C, B-E and B-D as shown in Fig. 2. Assuming half duplex links, A can communicate with C & E, B with E & D, C with A & D, D with B & C and E with A & B. Direct communication between A and B & A and D is not possible. If, however, C can root a message from A to D then there would be a logical connection between A and D. Similarly E can communicate with D via B and C with B via D. Each computer in the network will be called a node. The ring topology is not centrally controlled. Each node must have simple communication capability. A node will receive data from one of its two neighbours. The only decision the node has to take is whether the data is for its use or not. If data is not addressed to it, it merely passes it on to its other neighbour. Thus if E receives data from B it examines whether it is addressed to self. If it is, then it uses the data, else it passes the data to A.

The main disadvantage of a ring is larger communication delays if the number of nodes increase. It is, however, more reliable than a star network because communication is not dependent on a single computer. If one line between any two computers breaks down, if one of the computers breaks down, alternate routing is possible.

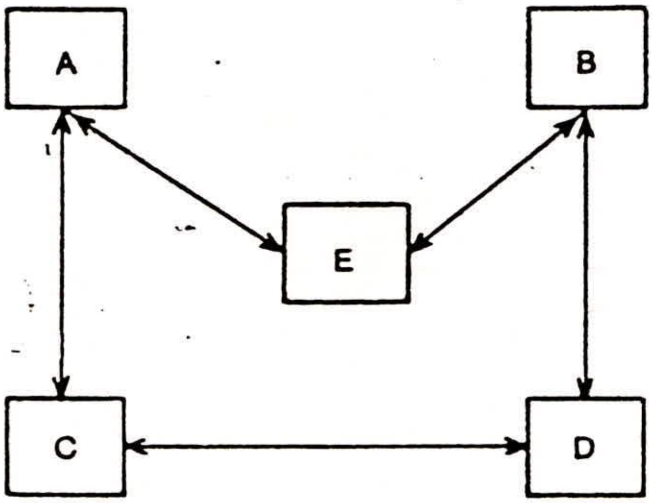

Fig. 2 A ring connection of computers

4.2 Star Topology :

The star topology has minimum line cost. As an example to connect 5 nodes only four links are required. The routing function is performed by E which centrally controls communication between any two nodes by establishing a logical path between them. Thus A wants to communicate with D, E would receive this request from A and set up the logical path A-E-D based on line availability. Delay would not increase when new nodes are added as any two nodes may be connected via two links only. The system however crucially depends on E. If E breaks down the whole network shuts. Star network is shown in Fig. 3.

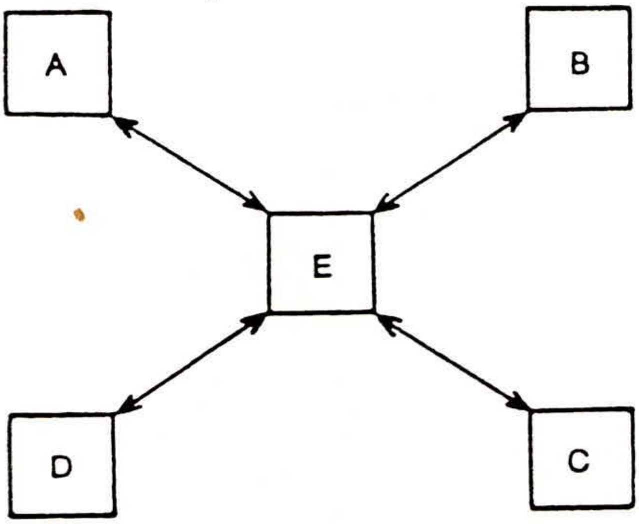

Fig. 3 A star connection of computers

4.3 Fully interconnected topology :

The fully connected topology of Fig.4 has a separate physical connection for connecting each node to any other node. It is the most expensive system from the point of view of line costs, as there are 10 separate point-to-point lines. It is, however, very reliable as any line breakdown will affect only communication between the connected machines. Each node need not have individual routing capability. Communication is very fast between any two nodes. The control is distributed, with each computer deciding its communication priorities.

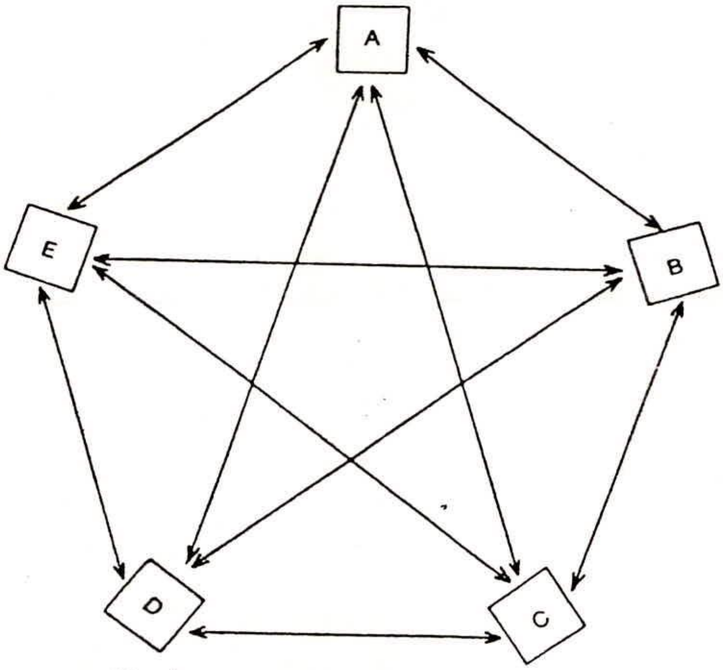

Fig. 4 A fully interconnected network

4.4 Multidrop linkage

Multidrop linkage of computers shown in Fig.5. The main advantage of this method is the reduction in physical lines. One line is shared by all nodes. If computer A wants to communicate with E then it first checks whether the communication line is free. When the line becomes free it transmits the message addressed to E on it. As the message travels on the line, each computer checks whether it is addressed to it. In this case when E finds its "address" in the message it accepts it, sends an acknowledgement to A and frees the line. Thus each computer connected to the line must have good communication and decision making capability.

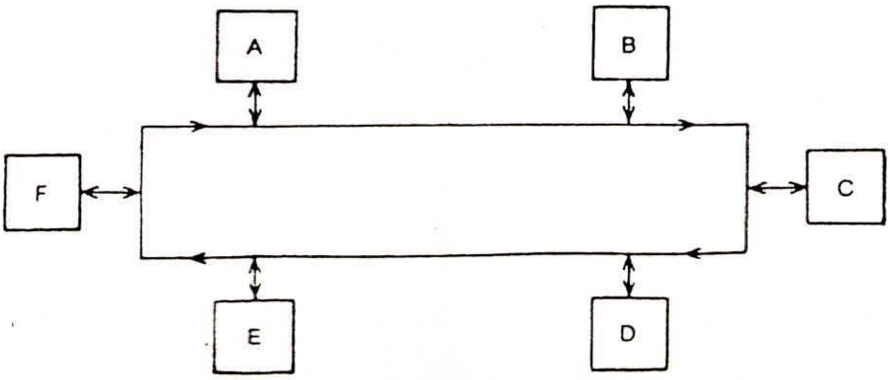

Fig. 5 A multidrop configuration

5. COMMUNICATION PROTOCOLS

When a number of computers and terminal equipment are to be connected together to form an integrated system, a well understood standard method of communication and physical interconnection should be established. This becomes particularly critical when equipment supplied by different vendors are to be connected since each vendor would have his own standards. If computers in different countries are to be connected together, yet another problem arises due to the need to use communication systems belonging to different nations which would have their own telecommunication regulations. Common agreed rules followed to interconnect and communicate between computers are known as protocols.

A universally used standard method of interconnecting user terminals to computers is the one proposed by Electronic Industries Association (USA) standard RS 232-C. This standard has been endorsed by CCITT (Commite' Consultatif International Telegraphique et Telephonique) recommendation V24. It completely specifies the interface between data communication devices (for example, modems), computers, and terminals. The RS 232-C interface consists of 25 connection points which specify the physical pin connections, voltage levels, signal transmission rates, timing information and control information such as ready and send.

The interconnection protocol for computer to computer communication is much more complex. It should define, besides the physical characteristics such as voltage levels, speeds, etc. the following :

1. How to begin and terminate a session between two computers?
2. How the messages in a session are to be framed ?
3. How errors in transmission of messages are detected ?
4. How messages are to be retransmitted when errors are detected ?
5. How to find out which message block was sent by which terminal/computer and to whom ?
6. How the dialog on the communication line proceeds ?

The most common method of sharing communication lines in a network is for a central communication controller to allocate unique addresses to computers and terminals in the network and allocate resources by polling. In polling, the communications controller asks a terminal or computer, using its address, whether a message block is to be sent. If the answer is 'yes' it accepts the message and routes it to the computer or terminal specified, if it is free to receive it.

Although no manufacturer supports another's data communications protocols, several protocols are available. One popular protocol is International Business Machines (IBM) System Data Link Control (SDLC). The other telecommunication protocols are National Cash Register Coys (NCR) BISYNC, Burrough's Data Link Control, Honewell data Link Control and DECNET.

An interconnection protocol for computer to computer communication as recommended by International Standards Organisation (ISO) is gaining wide acceptance. It is an approach based on defining a number of distinct layers each addressing itself to one aspect of linking. This is known as the ISO model for open systems interconnection. The ISO model is made up of seven layers as shown in Fig. 6. Each layer has a specific independent function. The standardisation achieved by each of the layers is explained below :

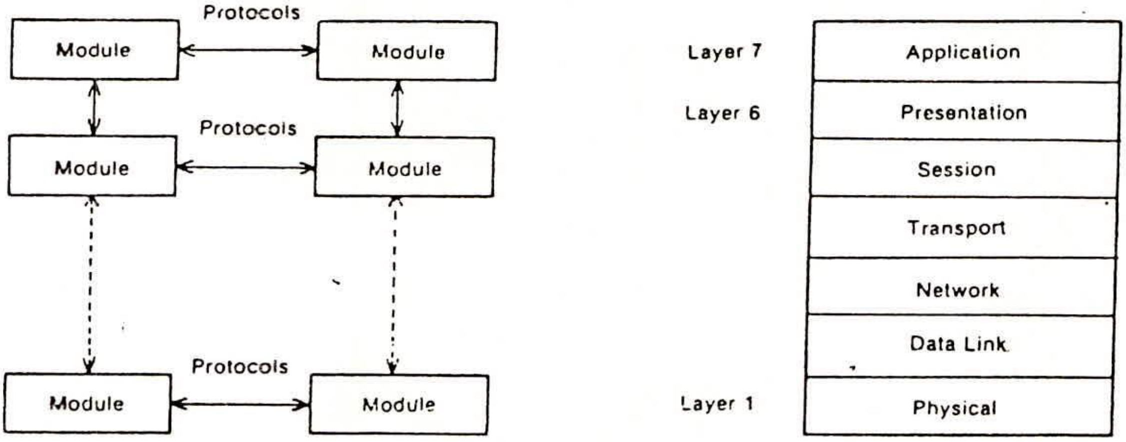

Fig. 6 ISO seven-layer model for open system interconnection

Physical link layer : This layer defines the electrical and mechanical aspects of interfacing to a physical medium for transmitting data. It also defines how physical links are set up, maintained and disconnected.

Data link layer : This layer establishes an error-free communications path between computers over the physical channel. It gives the standard for framing messages, checking integrity of received messages, accessing and using channels and sequencing of transmitted data.

Network control layer : This determines the setting up of a logical path between computers in a network, message addressing to computers, and controlling message flow between computer nodes.

Transport layer : Once a path is established between computers it provides control standards for a communication session for enabling processes to exchange data reliably and sequentially independent of which systems are communicating or their location in the network.

Session control layer : This establishes and controls system dependent aspects of communications session between specific computers in the network and bridges the gap between the services provided by the transport layer and the logical functions running under the operating system of a particular computer in the network.

6. NETWORK STRUCTURES

Networks can be classified into switching and non-switching.

A switching network has three components. These are the computer systems (Host), transmission media and the switching nodes. See fig. 7.

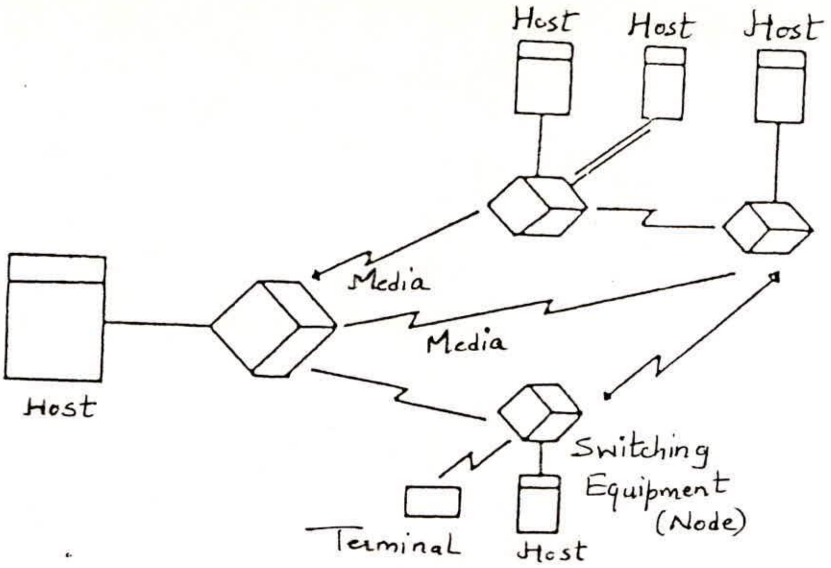

Fig. 7 A Switching Network

The computer systems are mainly used for processing and storing information. The transmission media are used to transport information between these computer systems. The switching nodes are specialised computers which are connected via the transmission media to hosts.

In the early stages of networks, host computers were directly connected to each other via the transmission lines and were responsible for performing both the switching and processing functions. But with the growth of network usage valuable host resources were used for the switching functions. To improve response times, specialised computers have been evolved to perform the switching functions. These functions mainly involve setting up a link between two hosts, and monitoring it, and disconnecting it when no longer needed.

Let us consider the following analogy. Consider the telephone network at Delhi. It has several exchanges. Each telephone is connected to its local exchange. Any individual who wishes to make a call has to connect via one or more of the exchange till the local telephone of the called party is reached. In our analogy there are three important components namely telephone sets, exchanges, and lines connecting exchanges. Here the telephone sets relate to the computer systems, the lines relate to the transmission media and the exchanges play the role of switching nodes. The computer network handles calls from computers to transfer data to each other, just as the telephone network allows people to send voice signals to each other systems.

7. What is TCP/IP?

Transmission Control Protocol and Internet Protocol are two of the primary protocols in the TCP/IP family. TCP/IP is an open networking protocol, which simply means that the technical description of all aspects of the protocol have been published. They are available for anyone to implement on their hardware and software. This open nature has helped make TCP/IP very popular. Versions of TCP/IP are now available for practically every hardware and software platform in existence, which has helped make TCP/IP the most widely used networking protocol in the world. The advantage of TCP/IP for a network operating system is simple: Interconnectivity is possible for any type of operating system and hardware platform that user might want to add.

TCP/IP family is dedicated to a different task. All the protocols that make up TCP/IP use the primary components of TCP/IP to send packets of data. The different protocols and services that make up the TCP/IP family can be grouped according to their purposes. The groups and some of their protocols are the following:

Transport: These protocols control the movement of data between two machines.

TCP (Transmission Control Protocol): A connection-based service, meaning that the sending and receiving machines communicate with each other at all times.
UDP (User Datagram Protocol): A connectionless service, meaning that the two machines don't communicate with each other.

Routing: These protocols handle the addressing of the data and determine the best routing to the destination. They also handle the way large messages are broken up and reassembled at the destination.

- **IP** (Internet Protocol): Handles the actual transmission of data.
- **ICMP** (Internet Control Message Protocol): Handles status messages for IP, such as errors and network changes that can affect routing.
- **RIP** (Routing Information Protocol): One of several protocols that determine the best routing method.

Network Addresses: These services handle the way machines are addressed, both by a unique number and a more common symbolic name.

- **ARP** (Address Resolution Protocol): Determines the unique numeric addresses of machines on the network.
- **DNS** (Domain Name System): Determines numeric addresses from machine names.
- **RARP** (Reverse Address Resolution Protocol): Determines addresses of machines on the network, but in a manner opposite of ARP.
- **BOOTP** (Boot Protocol): This starts up a network machine by reading the boot information from a server. BOOTP is commonly used for diskless workstations.

User Services: These are applications users have access to.

- **FTP** (File Transfer Protocol): This transfers files from one machine to another without excessive overhead. FTP uses TCP as the transport.
- **TELNET:** Allows remote logins so that a user on one machine can connect to another machine and behave as though they are sitting at the remote machine's keyboard.

Others: These are services that don't fall into the categories just mentioned but that provide important services over a network.

- **NFS** (Network File System): Allows directories on one machine to be mounted on another, then accessed by users as though the directories were on the local machine.

- **NIS** (Network Information Service): Maintains user accounts across networks, simplifying logins and password maintenance.

- **SMTP** (Simple Mail Transfer Protocol): A protocol for transferring electronic mail between machines.

All the TCP/IP protocol definitions are maintained by a standards body that is part of the Internet organization. Although changes to the protocols occasionally occur when new features or better methods of performing older functions are developed, the new versions are almost always backward-compatible.

7.1 IP Address

All the computers are given an IP address, a unique number for the machine. Every machine on the network has to be identified uniquely to allow proper routing. TCP/IP-based networks use 32-bit addresses to uniquely identify networks and all the devices that reside within that network. These addresses are called Internet addresses or IP addresses.

The 32 bits of the IP address are broken into four 8-bit parts. Each 8-bit part can then have valid numbers ranging from 0 to 255. In IP addresses, the four 8-bit numbers are separated by a period, a notation called dotted quad. Examples of dotted quad IP addresses are 255.255.255.255 and 147.14.123.8.

For convenience, IP addresses are divided into two parts: the network number and the device number within that network. This separation into two components allows devices on different networks to have the same host number. However, since the network number is different, the devices are still uniquely identified.

For connection to the Internet, IP addresses are assigned by the Internet Network Information Center (NIC) based on the size of the network. Anyone who wants to connect to the Internet must register with the NIC to avoid duplication of network addresses. If you don't plan to connect to the Internet, you are free to create you own numbering scheme, although future expansion and integration with Internet-using networks can cause serious problems.

For maximum flexibility, IP addresses are assigned according to network size. Networks are divided into three categories: Class A, Class B. and Class C. The three network classes break the 32-bit IP addresses into different sizes for the network and host identifiers.

A Class A address uses one byte for the network address and three bytes for the device address, allowing over 16 million different host addresses. Class B networks use two bytes for the network and two bytes for the host. Since 16 bits allows over 65,000 hosts, only a few large companies will be limited by this type of class. Class C addresses have three bytes for the network and one for the number of hosts. This provides for a maximum of 254 hosts (the numbers 0 and 255 are reserved) but many different network IDs. The majority of networks are Class B and Class C.

There is a limitation as to the first value. A Class A network's first number must be between 0 and 127, Class B addresses are between 128 and 191, and Class C addresses are between 192 and 223. This is because of the way the first byte is broken up, with a few of the bits at the front saved to identify the class of the network. Also, one can't use the values 0 and 255 for any part, because they are reserved for special purposes.

Messages sent using TCP/IP use the IP address to identify sending and receiving devices, as well as any routing information put within the message headers. If user wants to connect to an existing network, he should find out what their IP addresses are and what numbers he can use. If he is setting up a network for his own use but plan to connect to the Internet at some point, he should contact the Network Information Center for an IP Address. On the other hand, if he is setting up a network for his own use and don't plan to have more than a telephone connection to other networks (including the Internet), he can make up his own IP addresses.

If user is only setting up a loopback driver, he don't even need an IP address. The default value for a loopback driver is 127.0.0.1.

7.2 Network Mask

Next, a network mask is needed. The network mask is the network portion of the IP address set to the value 255, and it's used to blank out the network portion to determine routing. For a Class C IP address (three bytes for network and one for devices), the network mask is 255.255.255.0. A Class B network has a network mask of 255.255.0.0, and a Class A network mask is 255.0.0.0. For a loopback driver, your network mask is 255.0.0.0 (Class A).

7.3 Network Address

The network address is, strictly speaking, the IP address bitwise-ANDed to the netmask. In English, what this means is that it's the network portion of the IP address. So if the IP address is 147.120.46.7 and it's a Class B network, the network address is 147.120.0.0.

To get the network address, just drop the device-specific part of the IP address and set it to zero. A Class C network with an IP address of 201.12.5.23 has a network address of 201.12.5.0. A network mask is not needed if one is only working with a loopback address.

7.4 Broadcast Address

The broadcast address is used when a machine wants to send the same packet to all devices on the network. To get broadcast address, set the device portion of the IP address to 255. Therefore, the IP address is 129.23.123.2, the broadcast address will be 129.23.123.255 and the network address will be 129.23.123.0. To configure only a loopback driver, one needn't worry about the broadcast address.

7.5 Gateway Address

The gateway address is the IP address of the machine that is the network's gateway out to other networks (such as the Internet). User need a gateway address only if he has a network that has a dedicated gateway out. If user wants to configure a small network for his own use and don't have a dedicated Internet connection, user don't need a gateway address.

Normally, gateways have the same IP address as user machines, but they have the digit 1 as the device number. For example, if user IP address is 129.23.123.36, chances are that the gateway address is 129.23.123.1. This convention has been used since the early days of TCP/IP.

Loopback drivers do not require a gateway address, so if user want to configure his system only for loopback, ignore this address.

8. UUCP

UUCP, which stands for Unix to Unix Copy, is one of the easiest methods of connecting several UNIX machines together. UUCP enables Unix machines to send mail messages and files between themselves quite easily. In fact, UUCP was one of the first intermachine communications systems developed for UNIX, and subsequently led to Usenet newsgroups!

Under UUCP, one Linux system dials another using an asynchronous modem. A special protocol is used between the two machines to transfer information, and then the session terminates. Through UUCP user can access the Internet using a UUCP supplier for E-mail, news, and file access. Linza: for System Administrators

Configuring UUCP to enable machines to talk to one another is not difficult, but it does require patience to get all the files and settings correctly completed. Bear in mind that UUCP is somewhat of a dinosaur in today's modern network sense, using simple configurations for machine-to-machine connections and limited utility for users.

9. INTERNET

Internet is a global network made up of linked computers and could be a possible solution to users E-mail needs. Along with E-mail functions, the Internet provides a vast range of on-line databases of research material, text and libraries. To connect Internet it requires modem and communications software.

An Internet server is normally a Unix machine; Unix comes with mail and networking built in so it was the natural evolution to produce the Internet. Within Internet there is no directory synchronization-user need to know who he wants to mail and their mailing address.

This lack of directory synchronization solves one of the great problems of up-sizing a PC based E-mail system, such as Lotus CC: Mail or Microsoft Mail, both of which require directory synchronization. On a network with hundreds of servers, this would take, literally, forever.

Each user has an address in the form :

USER @ domain_1. domain_2. domain_3

domain 3 - is called the top-level domain and normally defines the type of company with a three letter acronym. The domain 1 & 2 - are sub domains that name the server. This addressing method (called RFC-822) is a hierarchial system that can easily adapt to global installations within the address.

In some cases, the Internet will not be suitable. If user has a small workgroup within a self contained LAN and are concerned about security, then the PC-based E-mail packages are perfect. However, if user wants to provide a global wide area network to link the offices within his company, the Internet becomes very appealing. To add Internet access to a LAN user can use TCP/IP or Internet gateway for mail software. Internet providers charge user by connect time.

As an alternative, there is no need to connect LAN to the Internet, nor have LAN-based E-mail system running, instead use a specialist package that run under windows and give users a direct access to the Internet. In this way, the Internet is doing the work of the back-end messaging engine that would otherwise have been Microsoft Mail or Lotus CC:Mail.

An alternative is to subscribe to one of the commercial on-line services that offers Internet access such as CompuServe that offers E-mail capability, but little else; or an alternative is CIX which gives user good access to mail and file functions.

9.1 Limitation of Internet

The only problem has been its limitations when delivering non-text attachments. If user wants to send binary attachments, user need to manually run a uuencode utility that converts the binary into a text-like format that can be transmitted over a Unix network.

To overcome this limitation many sites have now adopted MIME (Multipurpose Internet mail extensions) which allow binary attachments to be seen.

10. E-Mail

E-mail can be defined as leaving messages on a bulletin board system or a commercial on-line system such as CompuServe, CIX or MCI. Majority of E-mail users are connected to a local area network and run softwares that lets them send messages, files and notes to any other user on the network.

Requirement

Apart from the e-mail account it requires a PC with a modem, and a phone line. It also requires a communication software.

The PC: Any PC will do, though a 386 is better. Some e-mail services give windows- based front-end software and these demand a 386 with at least 4 MB of RAM.

The Modem: It requires error-correcting 2,400 bps modem, or higher speed external fax modem, and prevents E-mail getting garbled and the user gets clear, pure text.

10.1 Benifits of E-Mail

1) **Increased productivity** - No more trying to get hold of colleague on the phone or leaving yellow sticky notes on their screens.

2) **Minimal training** - By setting up software correctly, user send mail from their existing applications so minimal training is required.

3) **Cheap to run** - E-mail is one of the cheapest methods of inter office communic ations.

4) **Flexible** - User can use E-mail to transfer data between users and to query a data base.

5) **Cuts out arguments** - A track record is kept of where and when messages were sent together with proof of the time and date a message was read.

6) **Improves Communications** - E-mail makes it easy to have instant on-line meetings or brain-storming sessions.

7) **Users talk back** - Once used to E-mail, user finds it easier to say what they really feel in an E-mail than in face-to-face confrontation, which could help to cut office politics.

10.2 How E-Mail is used

E-mail works in a simple elegant manner. It's much like the old post office box system, where user mail, say, user credit card payments to a post office box. The company picks up the mail from that box, once a day.

In e-mail, user leaves a message addressed to his friend on his service provider's computers, by dialling in through a modem. It goes automatically into the directory assigned to his friend : his mail box. When he next dials in, he picks up that mail, and uploads other mail that he wants to send out. He may also read the mail right then, and reply to it quickly, on line.

It doesn't matter where the recipient is, or in what time zone. He could be travelling halfway across the world- as long as he looks in to check his mail, it's there. He reads the mail as soon as he checks his mail box.

***