They have a single communication channel, which is shared by all the computers on the network and therefore, any message transmitted by a computer on the network is received by all the computers connected to the channel. However, that message may be intended for only one computer over the channel.

In computer networks, any message to be transmitted is first broken in several packets. The packets are, then, transmitted one after another. These packets at the receiving ends are assembled to recreate the message. Each packet contains the address of the source and destination computer so that the intended receiver may receive them. In broadcast networks, all computers connected to the common channel receive packets transmitted by a computer on the same channel. The address field within the packet indicates the address of the intended receiver. All the computers after receiving the packets check the address field. Only the intended computer process the packet, other computers discard it. In this manner, the transmission and reception of the packets in broadcast networks take place.

An example of such network is Ethernet. Figure 7.3 shows the broadcast network.

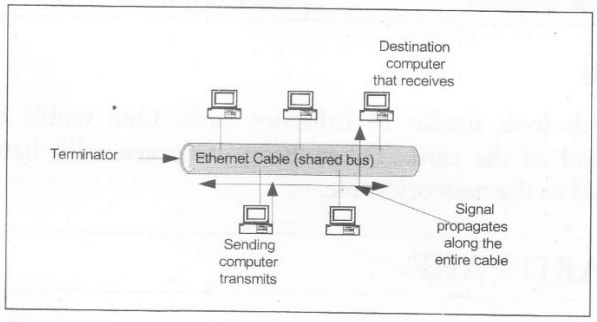


Figure 7.3: Ethernet

Broadcast network are also used to transmit same message to all computers or selected computers. It could be possible by reserving some addresses for such purposes. When same message is intended to transmit to all computers, it is called broadcasting. When it is intended for selected computers, it is termed as multicasting.

7.3.2 Point-to-point networks

It consist of many connections between individual pairs of machines.

Multiple routes and intermediate machines may exist between a pair of machines; so routing algorithms play an important role here.

A general rule (with many exceptions): smaller and localized networks tend to use broadcasting, whereas larger networks usually are point-to-point.

They provide separate communication channels for each pair of computers, which means that computers are connected together in point-to point manner consisting of many connections between individual pairs of computers. It provides multiple routes and intermediate computers between a pair of machines. Multiple routes and intermediate computers provide an opportunity to the packets traveling on network to opt different routes to reach at destination based on the easiest route. This calls for the necessity for routers as an intelligence device and routing algorithms.

The number of connections grows very quickly as number of computer increases. Figure 7.4 illustrates that two-computers need only one connection, three computers need three connections and four computers need six connections.

Figure 7.4 also illustrates that the total number of connections grow more rapidly than the total number of computers. Mathematically, the number of connections needed for N computers is proportional to the square of N:

$$\text{Point-to-point connections required} = (N^2-N)/2$$

Figure 7.5 shows a point-to-point connection for five computers located at two different locations, say, ground and first floor of a building.

As there are five PCs, therefore, a total number of ten connections will be required for point-to-point connection. Out of these ten connections six are passing through the same location and thereby making point-to-point connections an expensive one. By increasing the computer by one in the above configuration at location 2 as shown in Figure 7.5 will increase the total number of connections to fifteen. Out of these connections eight connections will pass through the same area.

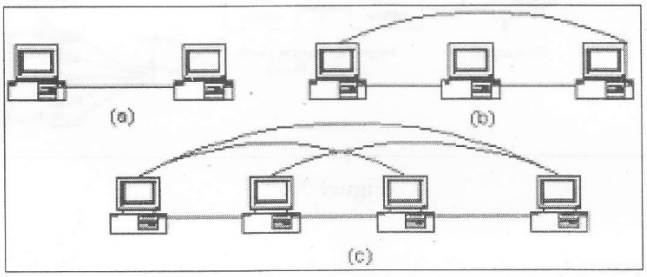


Figure 7.4: (a), (b), (c): Number of Connections for 2, 3, 4 Computers Respectively

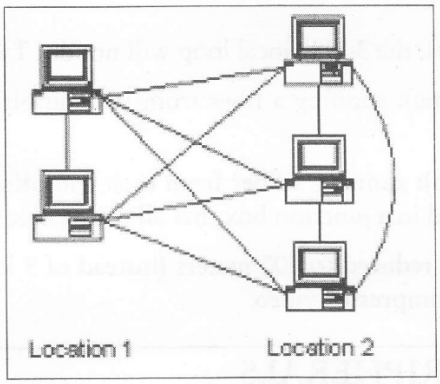


Figure 7.5: Five Computers at two Different Locations

In order to reduce the number of connections, some intermediate computer (routers) is introduced where connections from different groups of computers (network) terminate. The router routes those connections to the possible route of the destination computer.

In most of the cases, smaller and localized networks are broadcasting, whereas larger networks tend to use point-to-point connection.

7.4 TOPOLOGY PARADOX AND OTHER NETWORK TECHNOLOGIES

LAN topology and network technologies have been discussed in lesson 6.

7.5 FIBER MODEMS

The Local Loop

The use of both analog and digital transmission for a computer to computer call. Conversion is done by the modems and codes (Figure 7.6).

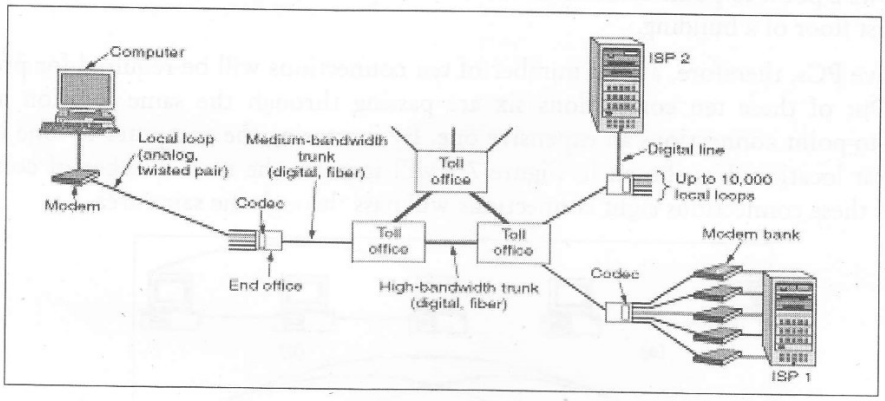


Figure 7.6

Modems

It has been discussed in lesson 4.

Fiber in the local loop

For video on demand applications, the 3-kHz local loop will not do. Two possible solutions:

1. **FTTH (Fiber To The Home):** running a fiber from the end office into everyone's house. Too expensive.
2. **FTTC (Fiber To The Curb):** running a fiber from each end office into each neighborhood (the curb). The fiber is terminated in a junction box that all the local loops enter.

The length of local loops can be reduced to 100 meters (instead of 3 km), they can be run at about 1 Mbps, which is just enough for compressed video.

7.6 NETWORKING PERIPHERALS

7.6.1 Switch

A concentrator is a device that provides a central connection point for cables from workstations, servers and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central switch/hub. Most switches are active, i.e., they electrically amplify the signal as it moves from one device to another. Switches no longer broadcast network packets as hubs did in the past, they memorize addressing of computers and send the information to the correct location directly.

7.6.2 Repeaters

Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a **repeater**. The repeater electrically amplifies the signal it receives and rebroadcasts it.

Repeaters can be separated devices or incorporated into a concentrator. They are used when the total length of your network cable exceeds the standards set for the type of cable being used.

A good example of the use of repeaters would be in a local area network using a star topology with unshielded twisted-pair cabling. The length limit for unshielded twisted-pair cable is 100 meters. The most common configuration is for each workstation to be connected by twisted-pair cable to a multi-port active concentrator. The concentrator amplifies all the signals that pass through it allowing for the total length of cable on the network to exceed the 100-meter limit.

7.6.3 Bridges

A bridge is a device that allows you to segment a large network into two smaller, more efficient networks. If you are adding to an older wiring scheme and want the new network to be up-to-date, a bridge can connect the two.

A bridge monitors the information traffic on both sides of the network so that it can pass packets of information to the correct location. Most bridges can **listen** to the network and automatically figure out the address of each computer on both sides of the bridge. The bridge can inspect each message and, if necessary, broadcast it on the other side of the network.

The bridge manages the traffic to maintain optimum performance on both sides of the network. You might say that the bridge is like a traffic cop at a busy intersection during rush hour. It keeps information flowing on both sides of the network, but it does not allow unnecessary traffic through. Bridges can be used to connect different types of cabling or physical topologies. They must, however, be used between networks with the same protocol.

7.6.4 Routers

A router translates information from one network to another; it is similar to a super intelligent bridge. Routers select the best path to route a message, based on the destination address and origin. The router can direct traffic to prevent head-on collisions, and is smart enough to know when to direct traffic along back roads and shortcuts.

While bridges know the addresses of all computers on each side of the network, routers know the addresses of computers, bridges, and other routers on the network. Routers can even **listen** to the entire network to determine which sections are busiest — they can then redirect data around those sections until they clear up. It also determines the best route to send the data over the Internet.

Check Your Progress

1. What is point to point network?
2. What are Ethernet cards?

7.7 LET US SUM UP

We have learnt and understood network hardware which is classified into transmission technology and scale. *Transmission technology can be classified into two types that is Broadcast networks and Point-to-point networks.* A LAN is a form of local (limited distance), shared packet network for computer communications. LANs interconnect computers and peripherals over a common medium in order that users might share access to host computers, databases, files, applications, and peripherals.

The Network Interface Card (NIC) provides the physical connection between the network and the computer workstation. It includes Ethernet cards, local card connectors, and token ring cards.

7.8 KEYWORDS

Local Area Network: A LAN is a form of local (limited distance), shared packet network for computer communications.

Repeaters: Since a signal loses strength as it passes along a cable, it is often necessary to boost the signal with a device called a repeater.

Bridge: Device that allows you to segment a large network into two smaller, more efficient networks.

Switches: Provides a central connection point for cables from workstations, servers and peripherals.

FTTC: Running a fiber from each end office into each neighborhood.

FTTH: Running a fiber from the end office into everyone's house.

Modem: A device which accepts a serial stream of bits as input and produces a modulated signal as output (or vice versa).

7.9 QUESTIONS FOR DISCUSSIONS

1. Discuss network hardware. What are the important dimensions for classifying networks?
2. Discuss LAN wiring and its physical topology.
3. Discuss network interface cards.
4. How is modem used as a fiber in the local loop?
5. Discuss Repeaters. How is it used in LAN?
6. Differentiate between broadcast networks and point-to-point network.

Check Your Progress: Model Answers

1. They provide separate communication channels for each pair of computers, which means that computers are connected together in point-to point manner consisting of many connections between individual pairs of computers.
2. Cards contain connections for either coaxial or twisted pair cables (or both).

7.10 SUGGESTED READING

Anuranjan Misra, *Computer Networks*, Acme Learning Pvt. Ltd. Publications

Rajneesh Agrawal and Bhata Bhushan Tiwari, *Computer Networks and Internet*, Vikas Publication

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill Osborne Media

Behrouz A. Forouzan, Sophia Chung Fegan, *Data Communications and Networking*, McGraw-Hill Companies

Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall

LESSON

8

LONG DISTANCE DIGITAL CONNECTION TECHNOLOGIES

CONTENTS

8.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Discuss various WAN technologies like ISDN, X.25, frame relay, cell relay, etc.
- Understand DSL technology
- Understand cable modem technology
- Discuss routing algorithms used for selecting the shortest and most reliable path.

8.1 INTRODUCTION

We will discuss in this lesson, Wan technologies such as ISDN, ATM, SMDS, etc. Also DSL Technology is discussed which supports the concept and the standards based upon the historical standards of the integrated service digital network in 1984. DSL Technology includes ADL. SDSL, etc. We have also discussed Routing which includes Link State routing, Hierarchical routing, etc. Routing refers to the process of selecting the shortest and most reliable path intelligently over which to send data to its ultimate destination.

8.2 DSL TECHNOLOGY

Digital subscriber line technology is not the new technology but basically the concept and the standards are based upon the historical standards of the integrated service digital network in 1984. Nowadays it has become a good and the secure form of networking, as these standards were improved with the help of latest and the modern researches. So now we can enjoy the communication and the voice data between two places without any hesitation thrpugh dsl technology.

Basically the DSL technology is the type of the broadband technology that allows the users to access the internet and do the transmission of data through digital telephone lines. In the working of the DSL, copper wires are used for that are the typical telephony lines. First of all the parts that are required for the connection of the internet such as the modem or the LAN card are checked through the configuration of the system. Then the telephone line is attached to the device and other end of the device in the system then, make a connection and use this wired and the typical broadband service for the sake of searching and using an internet technology.

8.2.1 ADSL

ADSL (Asymmetric Digital Subscriber Line) was the telephone industry's first invention which make use of existing copper twisted pairs. ADSL is regarded more as a quick-and-dirty hack than a long-term solution, but it is being located in various cities. This type of DSL is known as the ADSL. It is having high bandwidth and it provides high downloading speed to the users. Also it is having a good uploading rate. Downloading speed of this type is more then 4 Mbps and at least 1 Mbps uploading speed. It is further divided into different types such as RADSL and VDSL.

8.2.2 SDSL

Another important type of DSL is the SDSL; it is defined as the type of DSL in which the speed of the bandwidth of the downloading and the uploading is the same and it is commonly used in the business World.

It is referred to as the symmetric digital subscriber line SDSL. Commonly it provides the speed of 1.5 Mbps for all the users for all the purposes. It is also divided into sub types i.e. HDSL, UDSL, and SHDSL etc.

Advantages of DSL

Some advantages of the digital subscriber line (DSL) technology are as follows that really play a beneficial role for the users:

- As compared to the modem net, Digital subscriber line has a faster speed of broadband.
- No installment need for the configuration of the DSL as it is configured in the old telephony lines.
- While using the internet facility, you can also use the telephone lines for the voice calls.
- Easy downloading and uploading is available and easy installation on the network.

8.3 CABLE MODEM TECHNOLOGY

Television is the key source of news, entertainment and educational programs for millions of homes across the world. Cable Television (CATV) has become main transmission media for receiving television programmes in home. This has certain advantage of providing clearer picture and more channels. The CATV providers also providing high-speed connection to the Internet to their subscribers. The CATV uses cable modems that are considered high-speed Internet connections and are used to boost the speed of Internet to get access to valuable online resources. The coaxial cable that provides television signal to the home television has capability to handle enormous bandwidth in the range of hundreds of megahertz. The television signal requires only 6 MHz channel bandwidth on the cable. Fibre optic cables are also used to distribute TV signals to home television. In such a case, the fiber is terminated at an appropriate place and then the television signal is distributed to home television through coaxial cable. To utilize the extra space available on the coaxial cable for downloading and uploading Internet data, cable modems are used. Thus a CATV network is used for distributing broadband, multi-channel CATV signals from a service providers to subscribers. Cable television or CATV uses coaxial cable or optical fiber as the transmission media to transmit television programs to televisions at home or office. Conventional television uses over-the-air broadcasting of signal using radio waves to transmit television programs to television receivers. This system requires a television antenna. On the other hand, cable television system uses radio frequency signals over fixed optical fibers or coaxial cables to transmit television programs to the consumers. Other applications of cable television are FM radio programming, high-speed Internet, telephony, etc.

Using coaxial cables provide several advantages because of its huge bandwidth; transmission of bi-directional signal and large amounts of data is possible. Cable television signals require small bandwidth of coaxial lines. Hence, remaining bandwidth may be used for other digital services such as broadband Internet and cable telephony. Broadband Internet over coaxial cable is possible because of cable modems that convert the internet data into digital signal that can be transferred over coaxial cable.

Optical fiber provides boradband services for CATV. This is done with frequency multiplexing of individual TV channel signals into broadband electrical signals. Light wave communication over optical fiber networks is used for the distribution of broadband, multiple channel CATV (Cable Television) signals. This uses fibers which carry amplitude modulated broadband signals over a considerable distance in the range of 6-30 km. Electrical to optical transmitters at the sending end and optical to electrical signal at receiving end facilitates the reception of the broadband CATV electrical

signals. Distribution to CATV signal subscribers is obtained by transmitting the electrical signals from the receivers through a limited cascade of amplifiers along a coaxial cable.

CATV services uses a special telephone interface is installed at the customer's premises to convert the analog signals from the customer's in-home wiring into a digital signal. The analog signal is then sent on the local loop to the switching center. Its advantages include need of less bandwidth, better voice quality and integration to a VoIP network.

Cable Modem

Cable modem works on the principle of modems and provides access to data signal sent through the cable television infrastructure. Cable modems delivers broadband Internet access in the form of cable Internet, taking advantage of unused bandwidth on a cable television network using coaxial cable or optical fiber cable. A cable modem works like a bridge in accordance with IEEE 802.1D for Ethernet networking. The cable modem forwards Ethernet frames between a customer LAN and the coaxial cable network. The cable modem is an electronics device used to connect computers to Internet through a local CATV line. The cable modem provides a data speed of 1.5 MHz for download which is greater than dial up, DSL and ISDN circuits. The cable modem is provided with two connections. On connection of cable modem goes to the cable wall outlet and the other to a computer or to a set-top box for a TV set. Like telephone line cable modem also performs modulation and demodulation function bit in more complex ways. On the cable, the downstream data is treated like a TV channel and therefore it also occupies the same amount of cable space as any single channel of programming. The upstream data transmitted from a computer to the Internet requires only 2 MHz of cable bandwidth. The CATV system uses two types of devices for sending upstream data and receiving downstream data. They are cable modem on the subscriber's end and a Cable Modem Termination System (CMTS) at the cable provider's end. In addition to this, tools related to computer networking, security and management of Internet access over cable television is also required. Thus, the cable modems attached to a cable provider's coaxial cable communicate with a Cable Modem Termination System (CMTS) at the local cable provider's office. Hence, the cable modems are used to receive from and send signals only to the CMTS but not to other cable modems on the line. Theoretically a bandwidth for Internet service over a cable TV line is possible up to 27 Mbps for download to the subscriber with about 2.5 Mbps of bandwidth for interactive responses in the other direction. However, since the cable provider may not be connected to the Internet on a line faster than a T-Carrier circuits at 1.5 Mpbs, therefore a data rate more than 1.5 Mpbs will not be possible. The cable modem also provides continuous connection for Internet access.

The cable modems are either internal or external to the computer. They may also be part of a set-top cable box and requires only a keyboard and mouse for Internet access. The cable modems are consisted of the components like tuner, demodulator, modulator, Media Access Control (MAC) device and microprocessor. Figure 8.1 shows the internal configuration of a cable modem. The tuner connects to the wall outlet where the cable of the cable operator terminates to provide connection to the home TV. Sometimes, splitters are also provided to separate the Internet data channel from normal CATV programming. The tuner thus received unmodulated data from cable operators to pass it to the demodulator. The tuner may also contain a diplexer to allow the use of one set of frequencies for downstream traffic and another set of frequencies for the upstream data. Generally, the cable modem uses cable modem tuner for downstream data and a dial up telephone modem for upstream traffic.

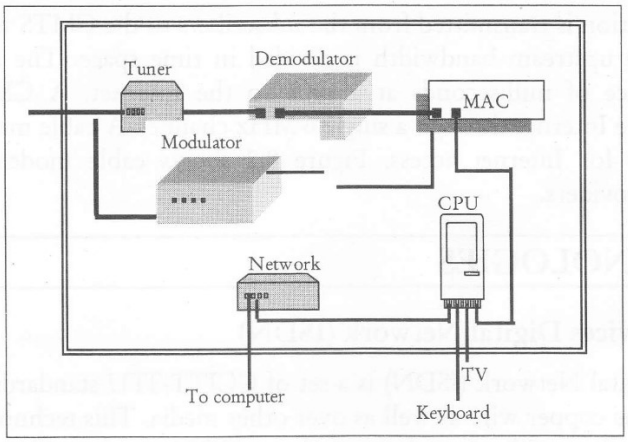


Figure 8.1: Cable Modem Configuration

The demodulators perform four functions. They are QAM, A/D converter, error correction and MPEG synchronizer. A QAM module of demodulator encodes analog signal to a simple signal that can be processed by the Analog-to-Digital (A/D) converter. The A/D converter converts the signal into a digital signal. An error correction module is provided to check the received information against a known standard. The MPEG synchronizer ensures the data groups that are in MPEG format stay in line and in order. A modulator referred to burst modulator, is used to convert the digital computer network data into radio-frequency signals for upload to Internet. This is referred to burst modulator because of the irregular nature of most traffic between a subscriber and the Internet. Thus the burst modulator comprises of a section to insert information used for error correction on the receiving end, a QAM modulator and a Digital-to-Analog (D/A) converter. A MAC card is an interface between the upstream and downstream parts of the cable modem. The MAC provides an interface between the hardware and software portions of the various network protocols. Some of the MAC functions are performed by CPU.

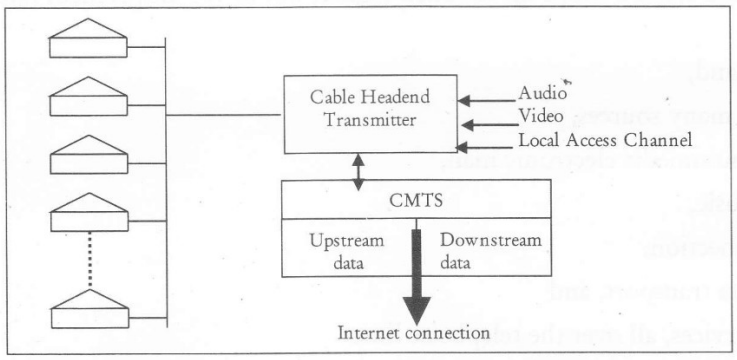


Figure 8.2: Cable Modem Arrangement

The CMTS at cable provider's end provides many of the same functions as provided by the DSLAM in a DSL system. The CMTS collects traffic from different subscribers on a single channel and routes it to an Internet Service Provider (ISP) for connection to the Internet. At the head end of the cable provider's cable, the ISP maintain servers for accounting and logging, Dynamic Host Configuration Protocol (DHCP) for assigning and administering the IP addresses of all the cable subscribers. The downstream information flows to all connected subscribers like in an Ethernet network. On the

upstream side, information is transmitted from the subscribers to the CMTS without the knowledge of other subscribers. The upstream bandwidth is divided in time space. The subscribers transmit one "burst" of a time space of milliseconds at a time to the Internet. A CMTS enable about 1,000 subscribers to access the Internet through a single 6-MHz channel. A cable modem is considered better than DSL technology for Internet access. Figure 8.2 shows cable modem arrangement between subscriber and cable providers.

8.4 WAN TECHNOLOGIES

8.4.1 Integrated Services Digital Network (ISDN)

Integrated Services Digital Network (ISDN) is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media. This technology uses ISDN adapters in place of modems and provides very fast speed up. ISDN requires adapters at both ends of the transmission. It provides a single integrated digital network for all kinds of information transfer services. In the real world, the delivery of multimedia requires a widespread network capable of delivering at high data rates. The current implementation of ISDN in the narrow band form is the best access and delivery medium available. Many in the industry see ISDN as the ramp through which multimedia networking will gain acceptance. The installed base of ISDN is growing rapidly throughout the world to provide connections among different countries. The governments of various countries are coming out with plans and policies to implement ISDN as soon as possible.

Integrated Services Digital Network in concept is the integration of both analog or voice data together with digital data over the same network. Although the ISDN integrates these on a medium designed for analog transmission, broadband ISDN (BISDN) will extend the integration of both services throughout the rest of the end-to-end path using fiber optic and radio media. Broadband ISDN will encompass frame relay service for high-speed data that can be sent in large bursts, the Fiber Distributed-Data Interface (FDDI), and the Synchronous Optical Network (SONET). BISDN will support transmission from 2 Mbps up to much higher, but as yet unspecified, rates. The new B-ISDN service will offer:

- Video on demand,
- Live TV from many sources,
- Full motion multimedia electronic mail,
- CD-quality music,
- LAN interconnection,
- High-speed data transport, and
- Many other services, all over the telephone line.

Definition of ISDN

ISDN is a network architecture in which digital technology is used to convey information from multiple networks to the end user. This information is end-to-end digital.

Features

- Offers point to point delivery
- Network access and network interconnection for multimedia

- Different data rates from 64 kbps up to 2 Mbps are commercially available which can meet many needs for transporting multimedia and is four to many times more than today's analog modems
- Call set-up times are under one second. ISDN can dramatically speed up transfer of information over the Internet or over a remote LAN connection, especially rich media like graphics, audio or video or applications that normally run at LAN speeds
- ISDN will be the feeder network for broadband ISDN based on ATM standards.

Figure 8.3 illustrates ISDN connections. The ISDN interfaces are designed in such a way that they support ordinary telephone copper wires. ISDN allows digital transmission of voice and data over ordinary telephone copper wires enabling the users to simultaneous access to Internet, telephony video teleconferencing equipment, bridge/routers, terminal adapters and fax. Some of the devices, which are designed to directly, interface with ISDN designated as Terminal Equipment 1 (TE1). The devices which are not ISDN capable interface but have a POTS telephone interface including ordinary analog telephones, FAX machines and modems, are designated as Terminal Equipment 2 (TE2). The interface is usually two-wire (single pair) interface from the phone switch and supports full-duplex data transfer over a single pair of wires. Sometimes devices like network termination (NT) are used to convert the 2-wire interface into the 4-wire interface. The 4-wire interface is capable of supporting multiple devices. A Terminal Adapters (TA) is used to connect a TE2 to an ISDN bus. The phone switch that provides connection to a pair of wires to connect customer premises equipment has Line Termination (LT) function and Exchange Termination (ET) function.

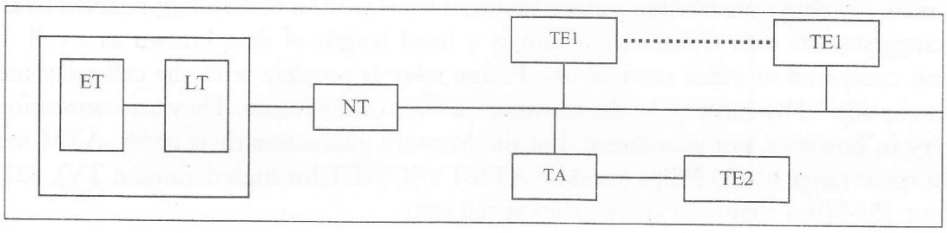


Figure 8.3: ISDN Connections

There are two forms of ISDN service:

Narrow band ISDN

Narrow band ISDN is a digital service where the transport speeds are 1.544Mbps (T1) or less. Narrow band ISDN provides for the following services:

- *Circuit Switched Voice:* Circuit switched voice service is a digital voice service that offers many of the capabilities of a business. It is centered over a 4-wire ISDN Digital Subscriber Line (DSL).
- *Circuit Switched Data:* Circuit switched data service provides end-to-end digital service to pass data or video information over the public network. ISDN uses out-of-band signaling to establish and maintain data connections, which require special processing.
- *Low Speed Packet:* ISDN lines are equipped with a packet connection that is used to manage ISDN connections. This monitoring capability is provided by using the D channel on a DSL. The D channel is a 16kbps X.25 connection that is also capable of passing low speed packet while also relaying call processing information.

- *High Speed Packet:* ISDN lines are also equipped with two B channels. Each B channel is a 64kbps channel that can be used for circuit switched voice, circuit switched data, or high-speed packet service. To provision high-speed packet service one or two of the 64kbps B channels are connected (permanent virtual circuit) to the packet network thus providing a 64kbps X.25 connection.

Broadband ISDN Service

Broadband ISDN Service is a digital service in excess of 1.544Mbs. This digital service can be in the form of Frame Relay, SMDS, or ATM. Broadband ISDN is the service of the future. The higher speeds offered are required to support the many applications of the Information Super Highway. The range of speeds for the Broadband ISDN services usually range from 25Mbs up to the Gigabit range. The two speeds that are most often discussed are OC 1 that is 155Mbs and OC 3 that is 622Mbs. The speeds in the Broadband are made possible by the high quality of the digital facilities in place on the network. The early data protocols such as X.25 required extensive overhead to insure the delivery of data. Error correction and flow control were performed at a number of intermittent points along the way of a data connection. The new digital facilities and the introduction of fiber optics have eliminated this need up to a maximum extent. High-speed broadband services rely for the most part on the upper layer protocols to perform these functions on an end-to-end basis.

8.4.2 Asynchronous Transfer Mode (ATM)

ATM makes B-ISDN possible because it transmits all information in small, fixed-size packets called cells. Cell relay is a data transmission service that uses transmission technology referred to as ATM. As the name suggests, the data transmission unit is a fixed length of data known as a cell. High-speed transmission compared to other services like Frame relay is possible with the cell relay method. The cell relay is considered by most to be the transport service of the future. They are connection-oriented. Cell delivery is, however, not guaranteed, but the network guarantees their order. ATM networks are available in speed range of 155 Mbps (used by AT&T's SONET for high definition TV), 622 Mbps (for carrying four 155-Mbps channels) and gigabits speed later.

Advantages

- *High-speed Transmission:* The purpose of ATM is to provide high speed and low-delay switching networks to support any type of user traffic such as constant rate traffic (audio, video) and variable rate traffic (data).
- *Multiplexing Transmission:* As in X.25 networks and Frame relay, multiple channels can be set within one physical line and communication is possible with multiple parties simultaneously. ATM segments and multiplexes use traffic into small, fixed length units called cells to reduce and control delay. ATM can support different speeds, traffic types and quality of service matched to applications by providing digital switching of cells.

Disadvantages

- *Cell discarding occurs with congestion:* When congestion occurs in the network, the cells (data) within the network are discarded and retransmission control can not be carried out within the network. The user must be responsible for carrying out retransmission control with the other party. ATM provides no error detection operations on user's payload inside the cell. It provides no retransmission services, and few operations are performed on the small header. The purpose of this approach is to implement a network fast enough to support multi megabit transfer rates.

- *High cost:* As the technology is new and not commercially available standards are still in the development stage.

8.4.3 X.25 Network

X.25 is considered as an early international standard for public network as connection-oriented networking from ITU-T. Earlier, it was developed for computer connections, used for terminal/ timesharing connection. This is a very popular protocol. The packet switched network and its characteristics are virtually the same as those for X.25. They allow remote devices to communicate with each other across high speed digital links without the expense of individual leased lines as shown in Figure 8.4.

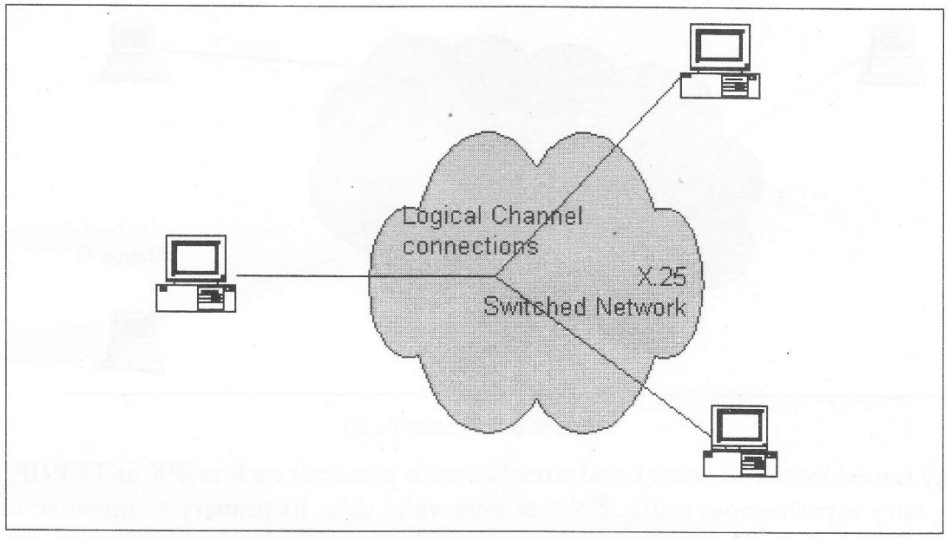


Figure 8.4: Communication among Multiple DTEs using X.25 Network

There were several networks that use the OSI model and the standard CCITT or ISO protocols for all the layers. X.25 defines the protocols from layer 1 (physical layer) to layer 3 (network layer) of OSI reference model and provides a reliable and connection-oriented packet (up to 128 bytes) delivery service, running at speeds up to 64 kbps.

Characteristics of X.25

In addition to those of the packet switched network, X.25 has the following characteristics:

- Multiple logical channels can be set on a single physical line
- Terminals of different communication speeds can communicate
- The procedure for transmission controls can be changed

8.4.4 Frame Relay

Frame relay has evolved from X.25 packet switching and the objective is to reduce network delays, protocol overheads and equipment costs. Error correction is done on an end-to-end basis rather than a link-to-link basis as in X.25 switching. Frame relay can support multiple users over the same line and can establish a permanent virtual circuit or a switched virtual circuit. Frame relay is considered to be a

protocol, which must be carried over a physical link. While useful for connection of LANs, the combination of low throughput, delay variation and frame discard when the link is congested will limit its usefulness to multimedia.

Frame relay may be looked upon as the simplified form of packet switching (each frame is addressed individually), similar in principle to X.25 in which synchronous frames of data are routed to different destinations depending on header information. It offers high-speed transmission. It is so called because a frame (a data packet) is relayed successively between transmission devices. Figure 8.5 shows the frame relay communication between different nodes.

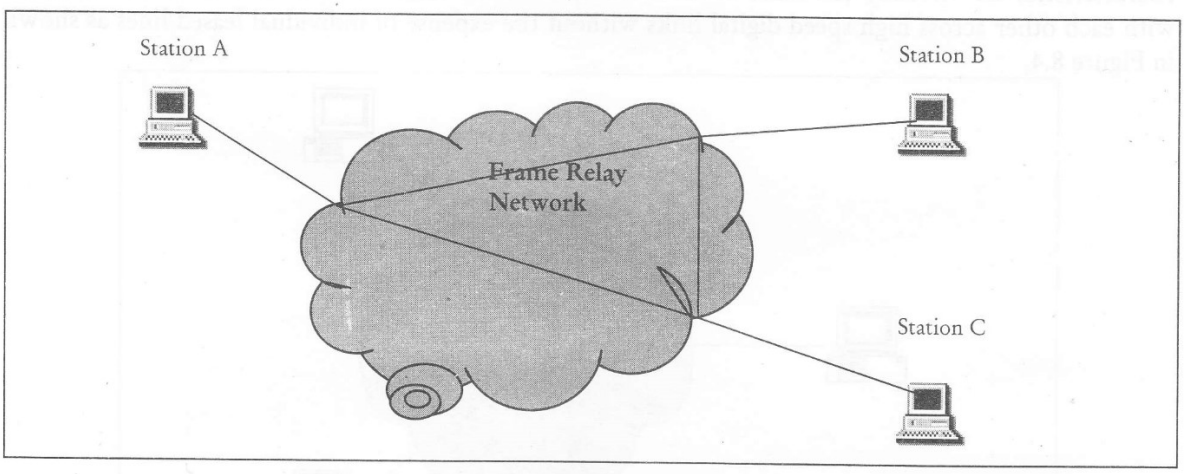


Figure 8.5: Frame Relay

Frame relay is used mostly to route Local Area Network protocols such as IPX or TCP/IP. It can also be used to carry asynchronous traffic, SNA or even voice data. Its primary competitive feature is its low cost. In North America it is fast taking on the role that X.25 has had in Europe: the most cost effective way to hook up multiple stations with high speed digital links.

Frame relay networks do not yet have the reliability of X.25 networks. Problems can be expected with new installations and none of the features can be taken for granted. At the time of writing, some public networks do not even support Status Polling properly. This makes it difficult to find out whether remote links are up or not.

The biggest difference between Frame relay and X.25 is that X.25 guarantees data integrity and network managed flow control at the cost of some network delays. Frame relay switches packets end to end much faster, but there is no guarantee of data integrity at all.

Characteristics of Frame Relay

- Frame relay service is one that supports the transportation of data.
- Frame relay is a connectionless service, meaning that each data packet passing through the network contains address information.
- Frame relay is a service that is provided with a variety of speeds from 56kbs up to 25Mbs. Even though the most used speeds for the service are currently 56kbs and 1.544Mbs
- Frames are variable in length and goes up to 4,096 bytes.

- Frame relay is considered to be a Broadband ISDN service.
- One of the unique facets of frame relay service is that the service supports variable size data packets.

8.4.5 Cell Relay

The cell relay protocol corresponds to first two layers of OSI reference model. The part that corresponds to the second layer i.e. data link layer is referred as ATM layer. However ATM layer does not have all functions of data link layer. Therefore, a protocol referred as the ATM Adaptation Layer (AAL) is prescribed above the data link layer as shown in Figure 8.6. AAL is user defined and is not mandatory for cell relay usage. It is responsible for the layout of a cell, establishment and release of virtual circuits and congestion control. It also facilitates an interface to allow users to send packets larger than a cell.

At the physical layer, ATM is independent of the transmission medium. The ATM cells may either be sent on a wire or fiber by themselves or they may be packaged inside the payload of other carrier systems.

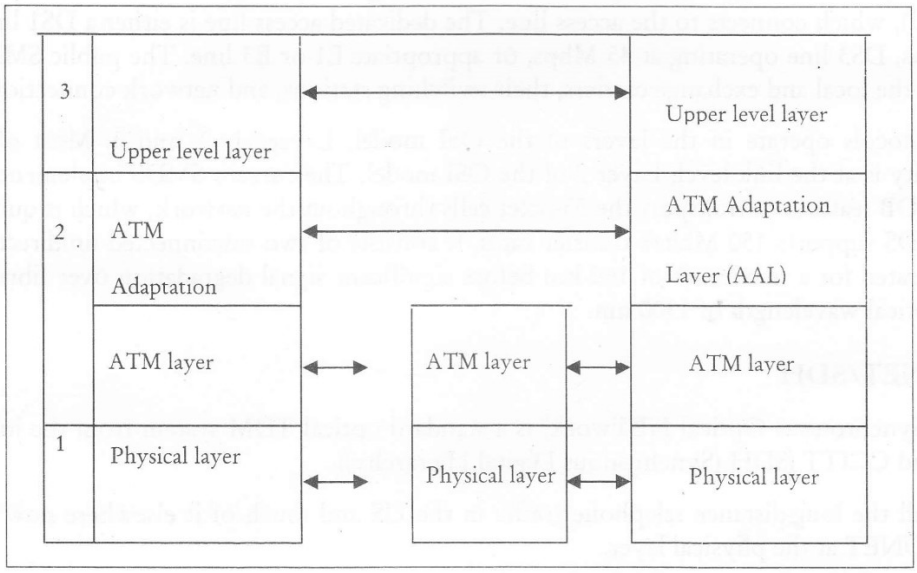


Figure 8.6: Cell Relay and the OSI Reference Model

Characteristics of ATM

- The transport speeds of most ATM applications are most often 155Mbps and 622 Mbps.
- ATM is a flexible service made possible by the size of the packets (cells). The cell size for all applications is 53 bytes.
- The small cell size allows a variety of applications to run on ATM networks including voice, video, and data. The appeal of the service has to do with the ability to pass voice and video information. These two services are time sensitive or otherwise known as isochronous data. This means that voice and video are susceptible to time delays. The small cell size of ATM and the service options such as Continuous Bit Rate Service allow such traffic to flow over the network where others such as Frame Relay and SMDS cannot guarantee this level of service.

8.4.6 Switched Multimegabit Data Service (SMDS)

Switched Multimegabit Data Service (SMDS) is a telecommunications service that provides connectionless, high-performance, packet-switched data transport. It is used to connect LANs, MANs and WANs to exchange data. SMDS is based on the IEEE 802.6 DQDB standard. SMDS fragments its datagrams into smaller "cells" for transport, and can be viewed as a technological precursor of ATM.

The IEEE 802.6 Metropolitan Area Network (MAN) standard defines SMDS, which has been implemented by Bellcore. It can use a variety of technologies, including Broadband ISDN (B-ISDN) and Distributed Queue Dual Bus (DQDB). Like Asynchronous Transfer Mode (ATM), SMDS uses cell relay transport.

SMDS Service Path

The SMDS service provides a connectionless network between Customer Premises Equipment (CPE) such as single unit or Local Area Networks (LANs) or both. These may be nationwide at various sites. It consists of customer premises; dedicated access lines and public SMDS networks. The customer premises may include single unit or LAN or both along with a router and the SMDS Data Service Unit (DSU), which connects to the access line. The dedicated access line is either a DS1 line operating at 1.5 Mbps, DS3 line operating at 45 Mbps, or appropriate E1 or E3 line. The public SMDS network consists of the local and exchange carriers, their switching stations, and network connections.

SMDS protocols operate in the layers of the OSI model, Layers 1, 2, and 3. Most of the SMDS functionality is at the link level, Layer 2 of the OSI model. The current SMDS implementation makes use of DQDB features to transport the 53-octet cells throughout the network, which is quite similar to ATM. SMDS supports 150 Mbit/s transfer rates. It consists of two unconnected unidirectional buses. DQDB is rated for a maximum of 160 km before significant signal degradation over fibre optic cable with an optical wavelength of 1300 nm.

8.4.7 SONET/SDH

SONET (Synchronous Optical NETwork) is a standard optical TDM system from the joint effort of Bellcore and CCITT (SDH (Synchronous Digital Hierarchy)).

Virtually all the long-distance telephone traffic in the US and much of it elsewhere now uses trunks running SONET at the physical layer.

Four major design goals of SONET:

1. To make it possible for different carriers to interwork, which requires defining a common signaling standard with respect to wavelength, timing, framing structure, and other issues.
2. To unify all digital systems in U.S, Europe and Japan, all of which were based on 64-kbps PCM channels, but combined in different ways.
3. To provide a standard way to multiplex multiple digital channels together.
4. To provide support for Operations, Administration, and Maintenance (OAM).

An early decision was to make SONET a traditional TDM system, with the entire bandwidth of the fiber devoted to one channel containing time slots for the various subchannels. Therefore, SONET is a

synchronous system in the sense that bits on a SONET line are sent out at extremely precise intervals controlled by a master clock.

- A SONET system consists of switches, multiplexers, and repeaters, all connected by fiber.
- The SONET topology can be a mesh, but is often a dual ring.
- The basic SONET frame is a block of 810 bytes.
- The basic SONET channel, called STS-1 (Synchronous Transport Signal-1), transmits a SONET frame every sec.

The basic SONET frame is best described as a rectangle of bytes, 90 columns wide by 9 rows high, as shown in Fig. .

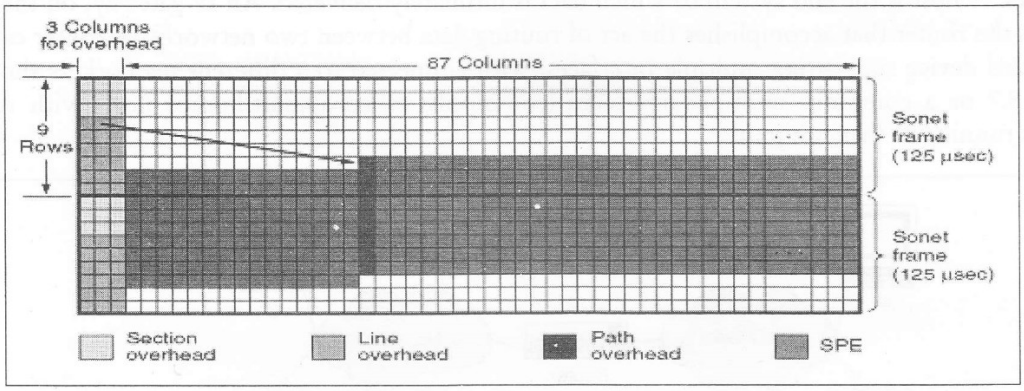


Figure 8.7: Two Back-to-back SONET Frames

The first three columns of each frame are reserved for system management information:

- The first three rows contains the section overhead.
- The next six contain the line overhead (generated and checked at the start and end of each line).
- The first row of the line overhead contains the pointer to the first byte of the user data, called **SPE (Synchronous Payload Envelope)**, which may begin anywhere within the remaining 87 columns of each frame (in total) and may span two frames.
- The first column of the SPE is the path overhead, i.e., the header for the end-to-end path sublayer protocol.

The SONET multiplexing hierarchy is shown in Figure 8.8.

SONET		SDH	Data rate (Mbps)		
Electrical	Optical	Optical	Gross	SPE	User
STS-1	OC-1		51.84	50.112	49.536
STS-3	OC-3	STM-1	155.52	150.336	148.608
STS-9	OC-9	STM-3	466.56	451.008	445.824
STS-12	OC-12	STM-4	622.08	601.344	594.432
STS-18	OC-18	STM-6	933.12	902.016	891.648
STS-24	OC-24	STM-8	1244.16	1202.688	1188.864
STS-36	OC-36	STM-12	1866.24	1804.032	1783.296
STS-48	OC-48	STM-16	2488.32	2405.376	2377.728
STS-192	OC-192	STM-64	9953.28	9621.504	9510.912

Figure 8.8: SONET and SDH Multiplex Rates

When a carrier, such as OC-3, is not multiplexed, but carries the data from only a single source, the letter is appended, so OC-3c indicate a data stream from a single source.

The reason why ATM runs at 155 Mbps is the intention to carry ATM cells over SONET OC-3c.

Example of Wan - SPF: SPF that is Sender Policy Framework is an extension of SMTP which stops e-mail spammers. SPF provides the authority that which computer can send e-mail.

8.5 ROUTING

Routing refers to the process of selecting the shortest and most reliable path intelligently over which to send data to its ultimate destination. IP routing protocol makes the distinction between hosts and gateways. A host is the end system to which data is ultimately delivered. An IP gateway, on the other hand, is the router that accomplishes the act of routing data between two networks. A router can be a specialized device supporting multiple interfaces, with connected to a different network as shown in Figure 8.7 or a computer multiple interfaces (commonly called a multihomed host) with routing services running in that computer.

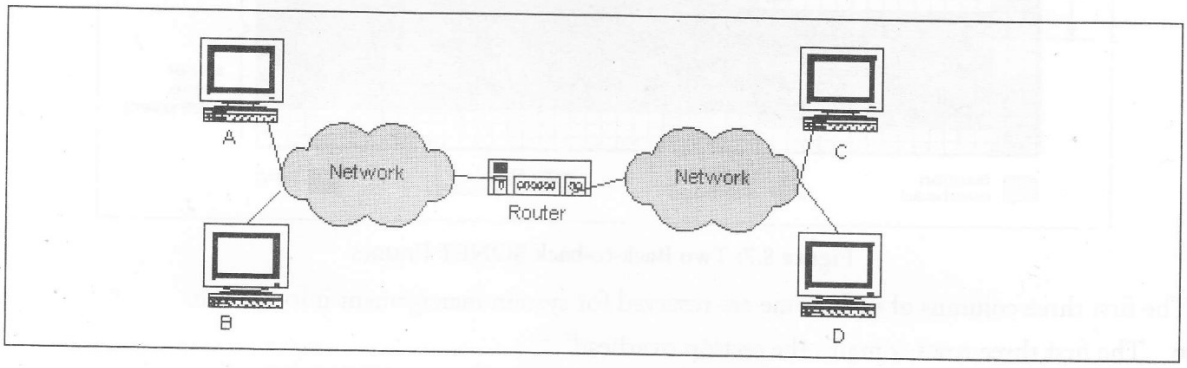


Figure 8.7: IP Router Providing Services between two Networks

By OSI norms and standards, a gateway is not only a router but also a connectivity device that provides translation services between two completely hybrid networks. For example, a gateway (not a router) is needed to connect a TCP/IP network to an AppleTalk network.

It is important to know that both hosts and IP routers (gateway) perform routing functions and therefore, compatible implementations of the IP protocol are necessary at both ends. In other words, datagrams are submitted either to a host that shares the same physical network with the originating host or to a default gateway for further routing across the network. As such, IP on a host is responsible for routing packets that originate on this host only, fulfilling local needs for routing. A gateway, on the other hand, is responsible for routing all traffic regardless of its originator (as long as the TTL field is valid).

A default gateway is a router that a host is configured to trust for routing traffic to remote systems across the network. However, the trusted router must be attached to the same network as the trusting host. A router on a remote network cannot be used for providing the functionality of the default gateway.

Routing Algorithms

The routing algorithm that runs on the network layer decides which output line an incoming packet should be transmitted on. A routing table that is built in every router tells which outgoing line should be used for each possible destination router. A router looks up the outgoing communication line to use in the routing table after receiving a datagram that contains the destination address. Thereafter, it sends the packet on its way to the destination. Thus, the major role of the network layer is to routing the packets from source to destination machine. The algorithms that enable to choose the possible routes and the data structures that they use are a major area of routing algorithm. The desirable properties of the routing algorithms are correctness, simplicity, robustness, stability, fairness and optimality.

Hence, the routing algorithm is defined as the part of the network layer software deciding which output line an incoming packet should be transmitted on. It all depends upon if the subnet uses datagrams internally, this decision is made a new for every arriving data packet since the best route may have changed since last time. If the subnet using virtual circuits such decision is made ones per session.

Figure shows the routing table for router A (address 138.25.10.1). This table lists destination addresses for each local network, and not for each destination host. This table also includes as the next hop (the address of next router) to which the packet must be transferred. If no hops are included, this means that the destination network is directly connected to the router.

When router A receives a packet, it tracks this table to perform routing. For example, if the packets addressed to the host of network 138.25.40.0, then router A sends the packet to router C (138.25.30.1). Router C has a similar routing table so that it can perform routing.

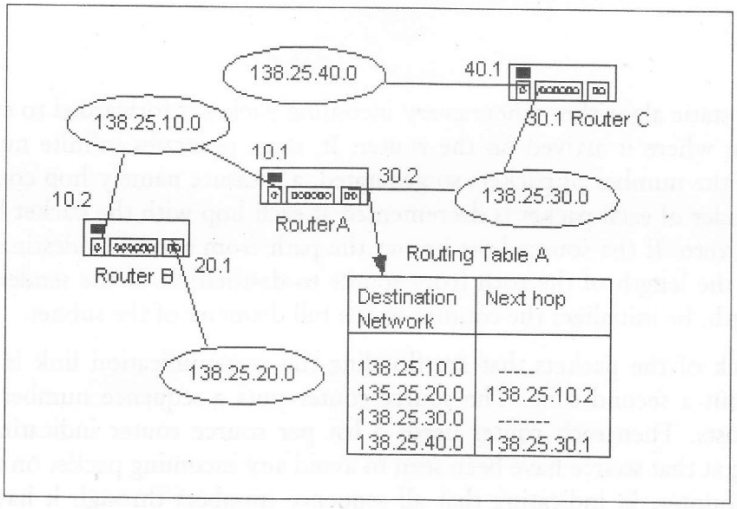


Figure 8.8: Routing Table

Routing plays a major role in the forwarding function. Routing algorithms are grouped into two classes. They are non-adaptive and adaptive algorithms.

Non-adaptive algorithms are independent of the volume of the current traffic and topology. They decide the route to which a datagram is to sent offline. The route is computed in advance and downloaded to the routers when the network is booted. Thus, routing information is manually

specified. It provides fixed route information to each router. If there is no change in route, it is made manually. This procedure is also called static routing.

Adaptive algorithms are capable of changing their routing decisions to reflect changes in the topology and the traffic. Routers automatically update routing information when changes are made to the network configuration. It is convenient, as it does not involve human intervention in case of changes to the network configuration. Its disadvantage, however, is that the overhead required to send configuration change information can be a heavy burden. They are also known as dynamic routing.

8.5.1 Optimality Principle

The optimality principle defines that if router A is on the optimal path from router B to router C, then the optimal path from A to C also falls along the same route. Consequently, the set of optimal routes from all sources to a given destination form a tree rooted at the destination. Such tree is called a sink tree.

8.5.2 Shortest Path Routing

The shortest path routing is simple and easy to understand. In this method, a graph of the subnet is built where each node of the graph represents a router and each arc represents a communication link. The shortest path algorithm chooses a shortest route between a given pair of routers on the graph. The shortest path method intends to measure path length for which number of hops; geographical distance, the mean queuing and transmission delay of router are used. The labels on the arcs are computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, etc. A number of algorithms exist for computing shortest path between two nodes of a graph.

8.5.3 Flooding

Flooding is another static algorithm where every incoming packet is forwarded to every outgoing line except the one from where it arrived on the router. It, thus, generates infinite number of duplicate packets. To control the number of packets so generated, a measure namely hop counter is applied. In this method, the header of each packet is decremented at each hop with the packet being discarded till the counter reaches zero. If the source host knows the path from source to destination, he initializes the hop counter to the length of the path from source to destination. If the sender does not have an idea of the path length, he initializes the counter to the full diameter of the subnet.

Alternatively, a track of the packets that are flooding the communication link is kept so that they could not be sent out a second time. The source router puts a sequence number in each packet it receives from its hosts. Then each router needs a list per source router indicating which sequence numbers originating at that source have been seen to avoid any incoming packet on the list. Each list is incremented by a counter, k, indicating that all sequence numbers through k have been seen. This prevents list from growing unnecessarily.

Selective Flooding

Selective flooding, which slightly more practical is a variation of flooding. Every incoming packet is not forwarded to each line. Instead, incoming packets are forwarded only to those going approximately in the right direction.

8.5.4 Flow-based Routing

Unlike the algorithms discussed above based on topology only, the flow based routing takes into account the topologic and the load. The networks, which have the mean data flow between each pair of nodes is relatively stable and predictable offers to analyze the flows mathematically to optimize the routing. The flow analysis makes it possible to compute the mean packet delay on the line from queuing theory, for which the capacity and average flow are known. This, in turn, calculates a flow-weighted average to obtain the mean packet delay for the whole subnet. However, this technology demands certain information such as the subnet topology, traffic matrix, capacity matrix, etc.

8.5.5 Distance Vector Routing

Distance Vector Routing comes under the category of dynamic routing. Modern computer networks believe in dynamic routing algorithms as compared to static routing algorithms. This routing algorithm along with link state routing is the popular. Distance vector protocols are RIP, Interior Gateway Routing Protocol (IGPR).

In distance vector algorithm each router maintains a routing table and exchanges its routing table with each of its neighbors so that their routing tables get updated. Each router will then merge the received routing tables with its own table, and then transmit the merged table to its neighbors. This is shown in Figure 8.9. This occurs dynamically after a fixed time interval by default, thus requiring significant link overhead.

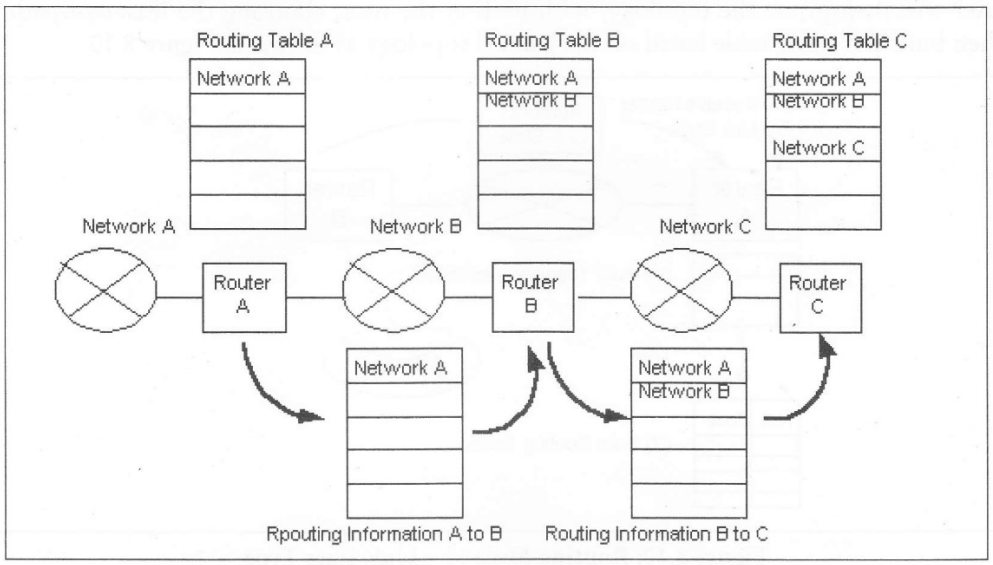


Figure 8.9: Routing Method - Distance Vector Type

There are problems, however, such as

- If exchanging data among routers every 90 seconds, for example, it takes 90 x 10 seconds that a router detects a problem in a router 10 routers ahead and the route cannot be changed during this period.
- Traffic increases since routing information is continually exchanged.

- There is a limit to the maximum amount of routing information (15 for RIP), and routing is not possible on networks where the number of hops exceeds this maximum.
- Cost data is only the number of hops, and so selecting the best path is difficult.

However, routing processing is simple, and it is used in small-scale networks in which the points mentioned above are not a problem. Distance vector routing was used in the ARPANET routing algorithm and was also used in the Internet under the name RIP. It also found its uses in early versions of DECnet and Novell's IPX. AppleTalk and CISCO routers use improved version of distance vector protocols. In the improved version, each router has a routing table indexed by and containing one entry for each router in the subnet. This entry has two parts. They are the preferred outgoing line to use for destination and an estimate of the time or distance to destination. The metric used is number of hops, time delay in milliseconds and total number of packets queued along the path or something similar.

8.5.6 Link State Routing

The link state routing is simple. These are OSPF, IS-IS (Intermediate System to Intermediate System Intra-Domain Routing Exchange Protocol). Link state routing algorithm where each router in the network learns the network topology then creates a routing table based on this topology. Each router will send information of its links (Link-State) to its neighbor who will in turn propagate the information to its neighbors, etc. This occurs until all routers have built a topology of the network. Each router will then prune the topology, with itself as the root, choosing the least-cost-path to each router, then build a routing table based on the pruned topology as shown in Figure 8.10.

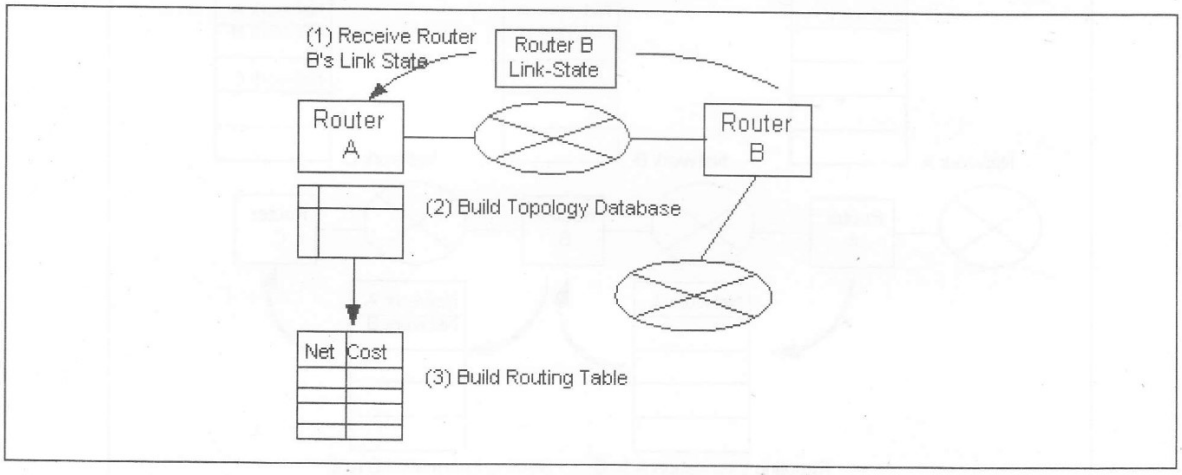


Figure 8.10: Routing Method - Link State Type

The entire topology and delays are measured and distributed to every router. Then Dijkstra's algorithm is used to find the shortest path to every other router. In link-state protocols, there are no restrictions in number of hops as in distance-vector protocols, and these are aimed at relatively large networks such as Internet backbones. The load on routers will be large however, since processing is complex.

Briefly, the link state routing deals with:

- Discovering its neighbor and learn their network addresses,
- Measuring the delay or cost to each of its neighbors,

- Constructing a packet indicating all it has just learned,
- Sending this packet to all other routers for their learning, and
- Computing the shortest path to every other router.

8.5.7 Hierarchical Routing

Because of the global nature of Internet system and ever growing networks in size, it becomes more difficult to centralize the system management and operation. For this reason, the system must be hierarchical such that it is organized into multiple levels, with several group loops connected with one another at each level. The routers are divided into regions with each router knowing all the details about how to route packets within its own region but knowing nothing about the internal structure of other regions. Therefore, hierarchical routing is commonly used for such a system as shown in the Figure 8.11.

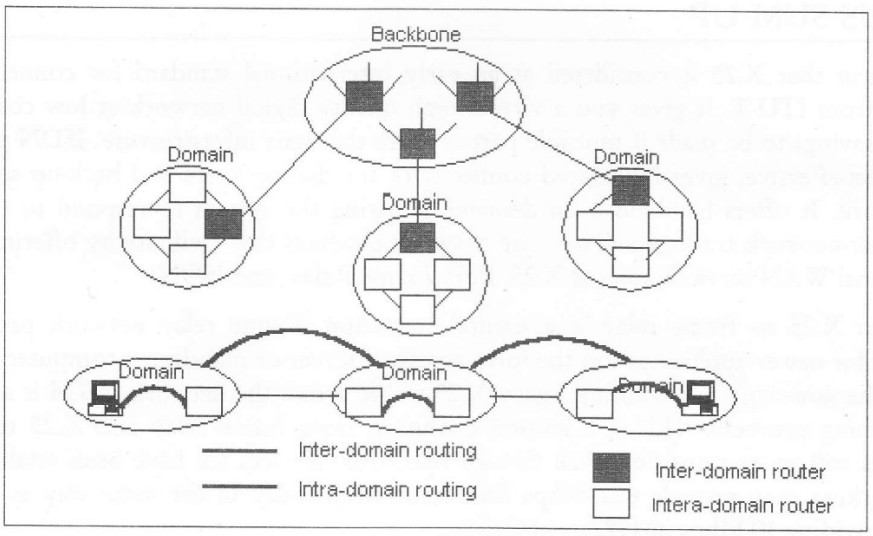


Figure 8.11: Hierarchical Routing

- A set of networks interconnected by routers within a specific area using the same routing protocol is called domain.
- Two or more domains may be further combined to form a higher-order domain.
- A router within a specific domain is called intra-domain router. A router connecting domains is called inter-domain router.
- A network composed of inter-domain routers is called backbone.
- Each domain, which is also called operation domain, is a point where the system operation is divided into plural organizations in charge of operation. Domains are determined according to the territory occupied by each organization.

Routing protocol in such an Internet system can be broadly divided into two types:

1. Intra-domain routing
2. Inter-domain routing.

Each of these protocols is hierarchically organized. For communication within a domain, only the former routing is used. However, both of them are used for communication between two or more domains.

Two algorithms, Distance-Vector Protocol and Link-State Protocol, are available to update contents of routing tables.

For Broadcast and Multicast routings, refer to lesson 6.

Check Your Progress

1. What is cell relay?
2. What is SMDS service path?

8.6 LET US SUM UP

We have learnt that X.25 is considered as an early international standard for connection-oriented networking from ITU-T. It gives you a virtual high quality digital network at low cost as there are tremendous savings to be made if multiple parties share the same infrastructure. ISDN provides high-quality, is cost-effective, gives high-speed connectivity for dial up users and back-up services on the public network. It offers bandwidth on demand, allowing the system to respond to the data burst nature of inter-network traffic etc. There are network products that facilitate by offering support for both traditional WAN services, such as X.25, PPP, Frame Relay, and ISDN.

Moving from X.25 to frame relay is a natural transition. Frame relay network provides greater performance for newer applications in the form accessing server or mainframe computer through their PCs and at the same time maintaining legacy X.25 traffic across the network. ATM is a cell-oriented, packet switching protocol. This is a natural evolution from frame relay and X.25 to ATM. This technology is still in its transition even though standards, services etc have been established. ATM-based networking may provide 622 Mbps link connection today in the same way as Ethernet was capable of providing 10 Mbps in 1982.

SMDS protocol, which is the FDDI-based standard, failed due to its expensive implementation and lack of compatibility with current LAN standards. The IEEE 802.6 standard uses the Distributed Queue Dual Bus (DQDB) network form. This form supports 150 Mbit/s transfer rates. It consists of two unconnected unidirectional buses. DQDB is rated for a maximum of 160 km before significant signal degradation over fibre-optic cable with an optical wavelength of 1300 nm. Most MANs now use Synchronous Optical Network (SONET) or Asynchronous Transfer Mode (ATM) network designs, with recent designs using native Ethernet or MPLS.

The routing algorithms that require selecting a path or route from many possible routes in the network are part of the router software. They are of two basic types namely non-adaptive or static and dynamic or adaptive. Selection of routing algorithms depends on the minimum mean delay for the packets and number of hop before reaching to the destination machine. Flooding algorithms have very limited use mostly with distributed systems or systems with tremendous robustness requirements at any instance. The distance vector algorithms require the router to know the "distance" to each of its neighbors. The distance here has a broader meaning. It can be some complex function of number of hops, delay, length of the queue along the path, etc. Link State Routing attempts to discover its neighbor and learn their network addresses and enable the router to choose a shortest path. The

hierarchal routing uses multiple groups to route the packets. Broadcast and multicast routings are used to forward a single packet to several recipients depending on whether they belong to broadcast or multicast group.

8.7 KEYWORDS

Cable Modem: works on the principle of modems and provides access to data signal sent through the cable television infrastructure

Internet Control Message Protocol (ICMP): The Internet Control Message Protocol (ICMP), an error reporting protocol that is an integral part of the IP protocol.

IP Protocol: It is a connectionless type service and operates at third layer of OSI reference model.

Link State Routing: It enables each router in the network learns the network topology to creates a routing table based on this topology.

Multicast: It is used for one or more network interfaces located on various subnets. It allows one-to-many communication.

Routers: Routers are used to connect both similar and dissimilar networks and operate on the network layer of OSI model using the physical layer, data link layer and network layer to provide connectivity, addressing and switching.

Routing Algorithms: They are software part of the router and decide which output line an incoming packet should be transmitted on.

Shortest Path Routing: It constructs a graph of the subnet where each node of the graph represents a router and each arc represents a communication link.

Asynchronous Transfer Mode (ATM): ATM transmits all information in small, fixed-size packets called cells in connection-oriented mode.

Cell Relay: It is a data transmission service that uses transmission technology referred to as ATM.

Frame Relay: Frame relay is a protocol over a physical link and can support multiple users over the same line and can establish a permanent virtual circuit or a switched virtual circuit.

Integrated Services Digital Network (ISDN): ISDN is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media.

Internet: Internetworking is a scheme for interconnecting multiple networks of dissimilar technologies.

Switched Multimegabit Data Service (SMDS): Switched Multimegabit Data Service (SMDS) is a telecommunications service that provides connectionless, high- performance, packet-switched data transport.

X.25: It is a connection oriented network and allows remote devices to communicate with each other across high-speed digital links without the expense of individual leased lines.

8.8 QUESTIONS FOR DISCUSION

1. On which layers of OSI model does X.25 work? X.25 networks are defined based on packet switched network, then why is it required to call it X.25?

2. Discuss ISDN and its forms.
3. What is frame relay? How it is evolved from X.25 packet?
4. What is cell relay? How it is connected with OSI reference model?
5. Discuss Switched Multimegabit Data Service (SMDS).
6. What is SONET/SDH? Discuss its various goals.
7. Discuss various routing algorithms used for selecting the shortest and most reliable path.
8. Discuss cable modem technology in detail.

Check Your Progress: Model Answers

1. The cell relay protocol corresponds to first two layers of OSI reference model. The part that corresponds to the second layer i.e. data link layer is referred as ATM layer.
2. The SMDS service provides a connectionless network between Customer Premises Equipment (CPE) such as single unit or Local Area Networks (LANs) or both

8.8 SUGGESTED READINGS

Rajneesh Agrawal and Bhata Bhushan Tiwari, *Computer Networks and Internet,* Vikas Publication

Burton, Bill, *Remote Access for Cisco Networks*, McGraw-Hill Osborne Media

Behrouz A. Forouzan, Sophia Chung Fegan, *Data Communications and Networking,* McGraw-Hill Companies

Andrew S. Tanenbaum, *Computer Networks,* Prentice Hall

Achyut S Godbole and Atul Kahate, *Web Technologies,* Tata McGraw Hill

J. D. Spragins, *Telecommunications protocols and design*, Addison-Wesley, Reading MA

Ferguson P., Huston G., *Quality of Service: Delivering* QoS on the *Internet and in Corporate Networks*, John Wiley & Sons, Inc., 1998

Spurgeon, Charles E., *Ethernet, The Definitive Guide*. O'Reilly & Associates, 2000.

Nassar, Daniel J. *Ethernet and Token Ring Optimization*. iUniverse.com, 2000. ISBN: 1583482199.

McDysan, David E. and Darren L. Spohn. *ATM Theory and Applications*, McGraw-Hill Osborne Media, 1998.

William A Shay, *Understanding Communication and Networks* 3rd Edition, Thomson Press

LESSON

9

PROTOCOLS AND LAYERS

CONTENTS

9.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Discuss network protocols such as TCP/IP, ATM, and ISO with protocol design issues
- Discuss techniques protocols use
- Know need for multiple protocols
- Discuss ATM AAL layer protocols
- Discuss network performance issues

9.1 INTRODUCTION

Protocols includes TCP/IP, ATM, and ISO which have been discussed in this lesson. TCP was specifically designed to provide a reliable end-to-end byte stream over an unreliable internetwork. AAL Layer in ATM and the seven ISO layers of OSI model have been discussed.

9.2 NETWORK OWNERSHIP, SERVICE PARADIGM AND PERFORMANCE ISSUES

9.2.1 Network Ownership

Network can be of two types:

- *Public:* Public network, as name suggests, is the one that can be accessed by everyone to which individuals or many companies can subscribe.
- *Private:* Private network is the one that can be used only by the owner or an individual.

9.2.2 Service Paradigm

There are some properties of network. Networks are understood by hardware and they are visible to the applications. Networks are:

- *Connection-less:* Each packet has attached with it, the destination sddress and each frame is handled independently.
- *Connection-oriented:* Here packets are send through the connection and it is terminated, when no longer needed.

9.2.3 Performance Issues

We have discussed below various performance issues:

1. *Performance problems in computer networks:* Congestion is the one example of such types of problems when more traffic suddenly arrives at a router than the router can handle, it creates problem of overloads and leads to congestion to force the performance deteriorate. The performance also degrades when there is a resource imbalance. For example, when a high speed line is connected to a low end computer, the performance will certainly degrades. Other factors of computer networks responsible for degradation of the performance are broadcast storm of error messages due to some bad parameters in TPDU, collapsing of RARP server when several machines try to learn their true identity from a RARP server in case of power restoration and booting of all machines together, setting of time-outs incorrectly, bandwidth-delay product, etc.
2. *Measuring network performance:* It includes measuring of the relevant network parameters and performance, understanding the bottleneck and reasons for it and changing of some parameters. The most basic kind of measurement is to start a timer at the beginning of some activity to see how long it takes, e.g. round trip time. Other measurements are made with counters to record how often some event has happened, e.g. number of lost TPDU's. Finally, one is often interested in knowing the amount of something, e.g. the number of bytes processed in a given time interval. To carry out the measuring of network performance, it should be ensured that the sample size is

large enough; samples are representative that is there are no congestions at lunch time; nothing unexpected is going on during the tests, etc.

3. ***System design for better performance:*** The network performance could be improved considerably with the help of measuring and tuning. However, they are not substitute for good design. System design is dependent not just on network design that includes routers, interface boards, etc, but also on the software and operating system. Improved CPU speed is one of the factors that enable getting the bits from the user's buffer out on the transmission media fast enough and having the receiving CPU process them as fast as they come in. Reduced packet count to reduce software overhead to improve processor's performance, minimized context switches, minimized copying for an incoming packet, etc are also important factors for design.
4. ***Fast TPDU processing:*** It separates out the normal case (data transfer in the ESTABLISHED state, no PSH or URG, enough window space) and handles it separately. Timer management is also optimized for the case of timers rarely expiring.
5. ***Protocols for gigabit networks:*** Some of the problems associated with it are mentioned. The communication speeds have been improving much faster than computing speeds and at a rate of 1 Gbps, use of 16 or 32 bit sequence numbers takes only 32 sec to send 2^{32} bytes and in the Internet packets live for 120 sec. The go back n protocol works poorly on lines with a large bandwidth-delay product. The gigabit lines are different from megabit lines. In the multimedia applications jitter in packet arrival time is as important as the mean delay itself. However, old protocols were often designed to minimize the number of bits on in the transmission media, frequently by using small fields and packing them together into bytes and words. Therefore, with gigabit networks, the protocol processing is the problem instead of the bandwidth. Hence, protocols need to be designed to minimize it.

9.3 PROTOCOL STACKS

- TCP/IP
- ATM
- ISO

These protocol stacks are discussed in the below section.

9.4 TCP PROTOCOL

TCP was specifically designed to provide a reliable end-to-end byte stream over an unreliable internetwork. Each machine supporting TCP has a TCP transport entity either a user process or part of the kernel that manages TCP streams and interface to IP layer. A TCP entity accepts user data streams from local processes, breaks them up into pieces not exceeding 64KB and sends each piece as a separate IP datagram. Client Server mechanism is not necessary for TCP to behave properly.

The IP layer gives no guarantee that datagram will be delivered properly, so it is up to TCP to timeout and retransmit, if needed. Duplicate, lost and out of sequence packets are handled using the sequence number, acknowledgements, retransmission, timers, etc to provide a reliable service. Connection is a must for this service. Bit errors are taken care of by the CRC checksum. One difference from usual sequence numbering is that each byte is given a number instead of each packet. This is done so that at

the time of transmission in case of loss, data of many small packets can be combined together to get a larger packet, and hence smaller overhead.

TCP connection is a *duplex connection*. That means there is no difference between two sides once the connection is established.

9.4.1 TCP Connection Establishment

The "three-way handshake" is the procedure used to establish a connection. This procedure normally is initiated by one TCP and responded to by another TCP. The procedure also works if two TCP simultaneously initiate the procedure. When simultaneous attempt occurs, each TCP receives a "SYN" segment which carries no acknowledgment after it has sent a "SYN". Of course, the arrival of an old duplicate "SYN" segment can potentially make it appear, to the recipient, that a simultaneous connection initiation is in progress. Proper use of "reset" segments can disambiguate these cases.

The three-way handshake reduces the possibility of false connections. It is the implementation of a trade-off between memory and messages to provide information for this checking.

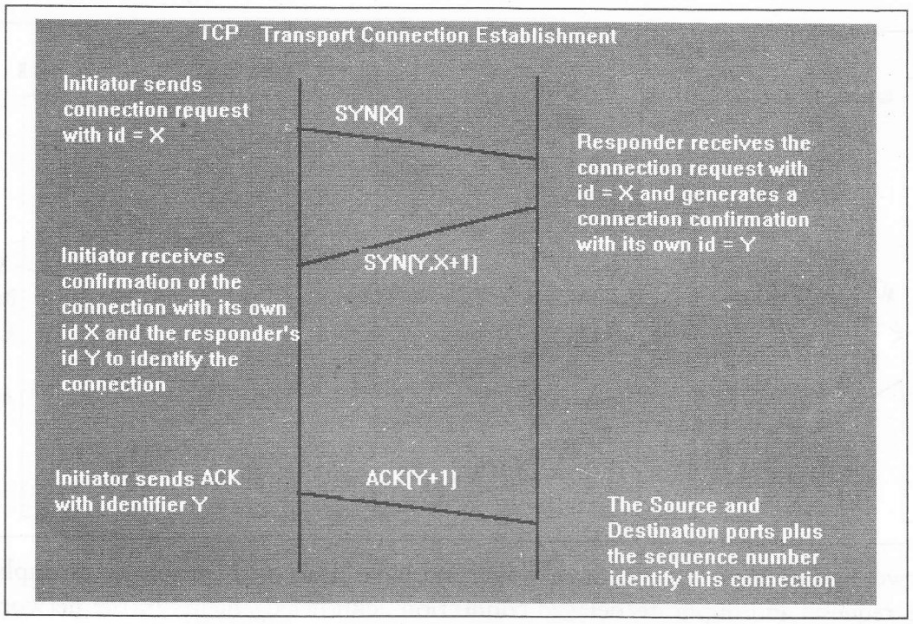
The simplest three-way handshake is shown in figure below. The figures should be interpreted in the following way. Each line is numbered for reference purposes. Right arrows (→) indicate departure of a TCP segment from TCP A to TCP B, or arrival of a segment at B from A. Left arrows (←), indicate the reverse. Ellipsis (...) indicates a segment which is still in the network (delayed). TCP states represent the state AFTER the departure or arrival of the segment (whose contents are shown in the center of each line). Segment contents are shown in abbreviated form, with sequence number, control flags, and ACK field. Other fields such as window, addresses, lengths, and text have been left out in the interest of clarity.

Basic 3-Way Handshake for Connection Synchronisation

TCP A				TCP B
1. CLOSED				LISTEN
2. SYN-SENT	→	<SEQ=100><CTL=SYN>	→	SYN-RECEIVED
3. ESTABLISHED	←	<SEQ=300><ACK=101><CTL=SYN,ACK>	←	SYN-RECEIVED
4. ESTABLISHED	→	<SEQ=101><ACK=301><CTL=ACK>	→	ESTABLISHED
5. ESTABLISHED	→	<SEQ=101><ACK=301><CTL=ACK><DATA>	→	ESTABLISHED

In line 2 of above figure, TCP A begins by sending a SYN segment indicating that it will use sequence numbers starting with sequence number 100. In line 3, TCP B sends a SYN and acknowledges the SYN it received from TCP A. Note that the acknowledgment field indicates TCP B is now expecting to hear sequence 101, acknowledging the SYN which occupied sequence 100.

At line 4, TCP A responds with an empty segment containing an ACK for TCP B's SYN; and in line 5, TCP A sends some data. Note that the sequence number of the segment in line 5 is the same as in line 4 because the ACK does not occupy sequence number space (if it did, we would wind up ACKing ACK's!).



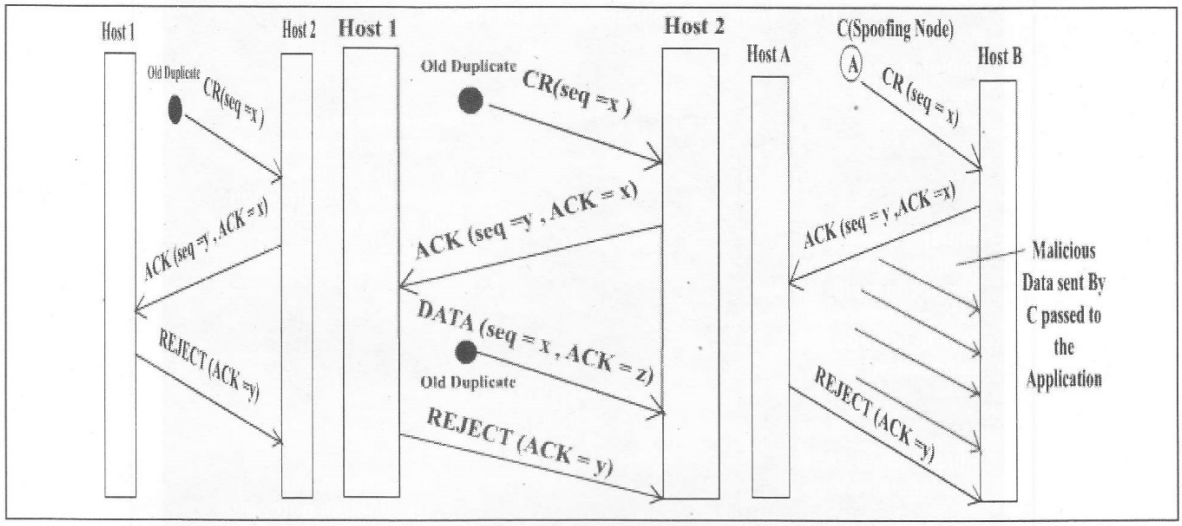
Simultaneous initiation is only slightly more complex, as is shown in figure below. Each TCP cycles from CLOSED to SYN-SENT to SYN-RECEIVED to ESTABLISHED.

Simultaneous Connection Synchronisation

	TCP A				TCP B
1.	CLOSED				CLOSED
2.	SYN-SENT	→	<SEQ=100><CTL=SYN>	...	
3.	SYN-RECEIVED	←	<SEQ=300><CTL=SYN>	←	SYN-SENT
4.		...	<SEQ=100><CTL=SYN>	→	SYN-RECEIVED
5.	SYN-RECEIVED	→	<SEQ=100><ACK=301><CTL=SYN,ACK>	...	
6.	ESTABLISHED	←	<SEQ=300><ACK=101><CTL=SYN,ACK>	←	SYN-RECEIVED
7.		...	<SEQ=101><ACK=301><CTL=ACK>	→	ESTABLISHED

Problem: Why is three-way handshake needed? What is the problem if we send only two packets and consider the connection established? What will be the problem from application's point of view? Will the packets be delivered to the wrong application?

Problem regarding 2-way handshake: The only real problem with a 2-way handshake is that duplicate packets from a previous connection (which has been closed) between the two nodes might still be floating on the network. After a SYN has been sent to the responder, it might receive a duplicate packet of a previous connection and it would regard it as a packet from the current connection which would be undesirable. Again spoofing is another issue of concern if a two way handshake is used. Suppose there is a node C which sends connection request to B saying that it is A. Now B sends an ACK to A which it rejects & asks B to close connection. Between these two events C can send a lot of packets which will be delievered to the application.

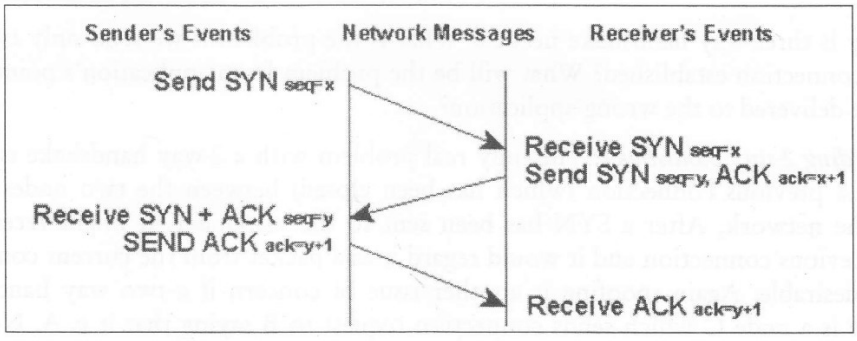


The first two figures show how a three way handshake deals with problems of duplicate/delayed connection requests and duplicate/delayed connection acknowledgements in the network. The third figure highlights the problem of spoofing associated with a two way handshake.

Some Conventions are:

1. The ACK contains 'x+1' if the sequence number received is 'x'.
2. f 'ISN' is the sequence number of the connection packet then 1st data packet has the seq number 'ISN+1'
3. Seq numbers are 32 bit.They are byte seq number (every byte has a seq number).With a packet 1st seq number and length of the packet is sent.
4. Acknowlegements are cummulative.
5. Acknowledgements have a seq number of their own but with a length 0.So the next data packet have the seq number same as ACK.

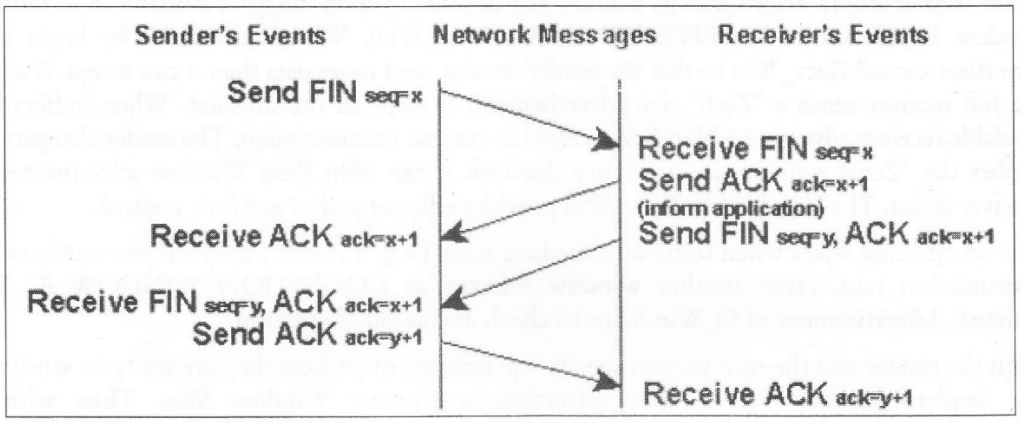
Connection Establish



- The sender sends a SYN packet with sequence number say 'x'.
- The receiver on receiving SYN packet responds with SYN packet with sequence number 'y' and ACK with seq number 'x+1'

- On receiving both SYN and ACK packet, the sender responds with ACK packet with seq number 'y+1'
- The receiver when receives ACK packet, initiates the connection.

Connection Release



- The initiator sends a FIN with the current sequence and acknowledgement number.
- The responder on receiving this informs the application program that it will receive no more data and sends an acknowledgement of the packet. The connection is now closed from one side.
- Now the responder will follow similar steps to close the connection from its side. Once this is done the connection will be fully closed.

9.4.2 TCP Design Issues

TCP connection is a duplex connection. That means there is no difference between two sides once the connection is established.

9.4.3 Multiple Nested Header

As we want to know that from which TCP connection this packet belongs. So for each new packet we have to match the header of each packet to the database that will take a lot of time so what we do is we first compare this header with the header of last received packet and on an average this will reduce the work. Assuming that this packet is from the same TCP connection from where we have got the last one (locality principal).

9.4.4 Techniques Protocols Use

1. *Sequencing:* Initial sequence number used in the TCP communication will be initialized at boot time randomly, rather than to 0. This is to ensure that packets from old connection should not interfere with a new connection. So the recommended method is to:
   (a) Initialize the ISN at boot time by a random number
   (b) For every 500 ms, increment ISN by 64K
   (c) With every SYN received, increment ISN by 64K.

2. *Flow control:* TCP uses Sliding Window mechanism at octet level. The window size can be variable over time. This is achieved by utilizing the concept of "Window Advertisement" based on:

   (a) Buffer availability at the receiver

   (b) Network conditions (traffic load etc.)

   In the former case receiver varies its window size depending upon the space available in its buffers The window is referred as RECEIVE WINDOW (Recv_Win). When receiver buffer begin to fill it advertises a small Recv_Win so that the sender does'nt send more data than it can accept. If all buffers are full receiver sends a "Zero" size advertisement. It stops all transmission. When buffers become available receiver advertises a Non Zero widow to resume retransmission. The sender also periodically probes the "Zero" window to avoid any deadlock if the Non Zero Window advertisement from receiver is lost. The Variable size Recv_Win provides efficient end to end flow control.

   The second case arises when some intermediate node (e.g. a router) controls the source to reduce transmission rate. Here another window referred as COGESTION WINDOW (C_Win) is utilized. Advertisement of C_Win helps to check and avoid congestion.

   Both the sender and the receiver can specify the number of packets they are ready to send/receive. To implement this, the receiver advertises a Receive Window Size. Thus with every acknowledgment, the receiver sends the number of packets that it is willing to accept.

   Note that the size of the window depends on the available space in the buffer on the receiver side. Thus, as the application keeps consuming the data, window size is incremented.

   On the sender size, it can use the acknowledgment and the receiver's window size to calculate the sequence number up to which it is allowed to transmit. For ex. If the acknowledgment is for packet 3 and the window size is 7, the sender knows that the recipient has received data up to packet 3 and it can send packets of sequence number up to (7+3=10).

   The problem with the above scheme is that it is too fast. Suppose, in the above example, the sender sends 7 packets together and the network is congested. So, some packets may be lost. The timer on the sender side goes off and now it again sends 7 packets together, thus increasing the congestion further more. It only escalates the magnitude of the problem.

3. *Congestion Avoidance:* This procedure is used at the onset of congestion to minimize its effect on the network. When transmission is to be scaled up it should be done in such a way that it does'nt lead to congestion again. Following algorithm is used.

   (a) At loss of a segment SET C_Win=1

   (b) Set Slow Start Threshold (SST) = Send_Win / 2

   (c) Send segment

   (d) If ACK Received, C_Win++ till C_Win <= SST

   (e) else for each ACK C_Win += 1 / C_Win

Time out and Retransmission

Following two schemes are used:

- Fast Retransmit
- Fast Recovery

When a source sends a segment TCP sets a timer. If this value is set too low it will result in many unnecessary retransmissions. If set too high it results in wastage of bandwidth and hence lower throughput. In Fast Retransmit scheme the timer value is set fairly higher than the RTT. The sender can therefore detect segment loss before the timer expires. This scheme presumes that the sender will get repeated ACK for a lost packet.

As we want to know that from which TCP connection this packet belongs. So for each new packet we have to match the header of each packet to the database that will take a lot of time so what we do is we first compare this header with the header of last received packet and on an average this will reduce the work. Assuming that this packet is from the same TCP connection from where we have ot the last one (locality principal).

9.5 THE ATM ADAPTATION LAYER PROTOCOLS

It is not really clear whether or not ATM has a transport layer.

The AAL (ATM Adaptation Layer) in ATM networks is radically different from TCP, largely because the designers were primarily interested in transmitting voice and video streams, in which rapid delivery is more important than accurate delivery.

The goal of AAL is to provide useful services to application programs and to shield them from the mechanics of chopping data up into cells at the source and reassembling them at the destination.

The AAL service space is organized along three axes:

1. Real-time service versus non-real-time service.
2. Constant bit rate service versus variable bit rate service.
3. Connection-oriented service versus connectionless service.

Eight distinct services can be defined, but only four of them were of any use and named as classes A, B, C, and D. To handle these four classes of service, four protocols, AAL 1 through AAL 4 were defined, respectively.

Later, it discovered that the technical requirements for classes C and D were so similar that AAL 3 and AAL 4 were combined into AAL 3/4.

Then the computer industry, which had been asleep at the switch, realized that none of them were any good. It solved this problem by defining another protocol, AAL 5.

9.5.1 Structure of the ATM Adaptation Layer

The ATM adaptation layer is divided into major parts. The upper part of the ATM adaptation layer is called the Convergence sub layer. It again subdivided into two parts: Service specific part and Common part. Its job is to provide the interface to the application. The functions of each of these subparts are protocol dependent but can include message framing and error detection.

The lower part of the AAL is called SAR(Segmentation and reassembly) sublayer. It can add header and trailer to the data units given to it by the convergence sublayer to from cell payloads. These payloads are given to the ATM layer for transmission.

AAL 1

AAL 1 is used for transmitting class A traffic, i.e., real-time, constant bit rate, connection-oriented traffic, such as uncompressed audio and video.

The convergence sublayer in AAL 1 detects lost and misinserted cells, smoothes out incoming traffic to provide delivery of cells at a constant rate, and breaks up the input messages or stream into 46- or 47-byte units that are given to SAR sublayer for transmission, and at the other end extracts these and reconstructs the original input.

The AAL 1 convergence sublayer does not have any protocol headers of its own. The AAL 1 SAR sublayer has defined formats of its cells. The 3-bit *SN* (Sequence Number) is used to detect missing or misinserted cells. The 3-bit *SNP* (Sequence Number Protection) is the checksum over the sequence number to allow correction of single errors and detection of double errors in the *SN* field. It uses a CRC with the polynomial. An *even parity* bit covering the header byte further reduces the likelihood of a bad sequence number sneaking in unnoticed. AAL 1 cells need not be filled with a full 47 bytes, but the number of actual data bytes per cell is the same for all cells and agreed on in advance. The cells are used when message boundaries must be preserved. *Pointer* is used to give the offset of the start of the next message.

AAL 2

For compressed audio or video, the data rate can vary strongly in time. E.g., many compression schemes transmit a full video frame periodically and then send only the differences between the subsequent frames and the last full frame. Also, message boundaries must be preserved so that the start of the next full frame can be recognized. AAL 2 is designed for this purpose. As in AAL1, the CS sublayer does not have a protocol but the SAR sublayer does.

AAL 3/4

AAL 3/4 is designed for both connection-oriented and connectionless-service for data transport that is sensitive to loss or errors but is not time dependent. AAL 3/4 can operate in two modes: stream or message.

A feature of AAL 3/4 not present in any of the other protocols is multiplexing. AAL 3/4 has both a convergence sublayer protocol and a SAR sublayer protocol. Messages as large as 64KB come into the convergence sublayer from the application. These are first padded out to a multiple of 4 bytes. Then a header and a trailer are attached.

The *CPI (Common Part Indicator)* field gives the message type and the counting unit for the *BA size* and *Length* fields. The *Btag* and *Etag* fields are used to frame messages. The *BA size* field tells the receiver how much buffer space to allocate for the message in advance of its arrival.

The *Length* field gives the payload length again. To support multiplexing, the convergence sublayer may have several messages constructed internally at once and may pass 44-byte chunks from different messages in any order to the SAR sublayer, which adds a header and trailer to make a AAL 3/4 cell.

AAL 5

The complexity and inefficiency generated by two layers of protocol, coupled with the surprisingly short checksum, caused some researchers to invent a new adaptation protocol, called SEAL (Simple Efficient Adaptation Layer).

AAL 5 offers several kinds of service to its applications:

- Reliable service, i.e., guaranteed delivery with flow control to prevent overrun.
- Unreliable service, i.e., no guaranteed delivery, with options to have cells with checksum errors either discarded or passed to the application any way (but reported as bad).
- Both unicast and multicast are supported, but multicast does not provide guaranteed delivery.
- AAL 5 supports both message mode and stream mode. Upon arrival in the convergence sublayer, a message (of up to 64KB) is padded out and a trailer added. The *UU (User to User)* filed is available for a higher layer for its own purposes, e.g., sequencing or multiplexing. The *Length* field tells how long the true payload is, in bytes. The *CRC* field is the standard 32-bit checksum over the entire message. The message is transmitted by passing it to the SAR sublayer, which does not add any headers or trailers. Instead, it breaks the message into 48-byte units and passes each of these to the ATM layer for transmission. Within the Internet community, it is expected that the normal way of interfacing to ATM networks will be to transport IP packets with the AAL 5 payload field.

9.5.2 Comparison of AAL Protocols

The overall impression that AAL gives is of too many variants with too many minor differences and a job half done. The future lies with AAL 5.

SSCOP - Service Specific Connection-Oriented Protocol

SSCOP is another AAL protocol which provides end-to-end reliable transport connections. (read the text).

9.6 ISO LAYERS

The seven layers of OSI model are defined as below:

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

These seven layers are explained in lesson 10 in detail.

Check Your Progress

1. What is Sequencing?
2. Define Congestion Avoidance.

9.7 LET US SUM UP

Protocols and layers includes three protocols stacks. They are termed as TCP/IP, ATM and ISO. TCP was specifically designed to provide a reliable end-to-end byte stream over an unreliable internetwork.

TCP connection is a duplex connection. That means there is no difference between two sides once the connection is established. We have discussed techniques protocols use that involves sequencing, flow control, and congestion avoidance. The AAL (ATM Adaptation Layer) in ATM networks is radically different from TCP. The goal of AAL is to provide useful services to application programs and to shield them from the mechanics of chopping data up into cells at the source and reassembling them at the destination. Structure of the ATM adaptation layer includes AAL1, AAL2, AAL 3/4, AAL 5.

In case of performance issues of the network, it is difficult to propound any scientific method to measure network performance. It is not only the transport layer where performance issues arise but it also includes network layer related to routing and congestion control.

9.8 KEYWORDS

TCP/IP: Designed to provide a reliable end-to-end byte stream over an unreliable internetwork.

ACK: This bit is set to indicate the ACK number field in this packet is valid.

PSH: This bit indicates PUSHed data. The receiver is requested to deliver the data to the application upon arrival and not buffer it until a full buffer has been received.

RST: This flag is used to reset a connection that has become confused due to a host crash or some other reason.

SYN: This bit is used to establish connections.

FIN: This bit is used to release a connection. It specifies that the sender has no more fresh data to transmit.

AAL: Provide useful services to application programs and to shield them from the mechanics of chopping data up into cells at the source and reassembling them at the destination.

9.9 QUESTIONS FOR DISCUSSION

1. Discuss TCP protocol. How is TCP connection evolved?
2. Discuss TCP related design issues and its features.
3. What are different techniques that protocol use?
4. What is ATM Adaptation Layer? Discuss its structure.

Check Your Progress: Model Answers

1. Initial sequence number used in the TCP communication will be initialized at boot time randomly, rather than to 0. This is to ensure that packets from old connection should not interfere with a new connection.
2. This procedure is used at the onset of congestion to minimize its effect on the network. When transmission is to be scaled up it should be done in such a way that it does'nt lead to congestion again.

9.10 SUGGESTED READING

Anuranjan Misra, *Computer Networks*, Acme Learning Pvt. Ltd. Publications.

UNIT V

LESSON

10

INTERNETWORKING

CONTENTS

10.0 AIMS AND OBJECTIVES

After studying this lesson, you will be able to:

- Discuss internetworking concepts like internet, routing in internetwork
- Understand virtual circuits

- Discuss internetwork Architecture i.e., OSI, TCP/IP, and 3 layer model
- Discuss various protocols that are being used in internetworking
- Know the concept of ARP and ICMP

10.1 INTRODUCTION

During late 60s and 70s, organizations were inundated with many different LAN and WAN technologies such as packet switching technology, collision-detection local area networks, hierarchical enterprise networks, and many other excellent technologies. The major drawbacks of all these technologies were that they could not communicate with each other without expensive deployment of communications devices. These were not only expensive but also put users at the mercy of the monopoly of the vendor they were dealing with. Consequently, multiple networking models were available as a result of the research and development efforts made by many interest groups. This paved the way for development of another aspect of networking known as protocol layering. This allows applications to communicate with each other. A complete range of architectural models were proposed and implemented by various research teams and computer manufacturers. The result of this know-how is that today any group of users can find a physical network and an architectural model suitable for their specific needs. This includes cheap asynchronous lines with no other error recovery than a bit-per-bit parity function through full-function wide area networks (public or private) with reliable protocols such as public packet switching networks or private SNA networks to high-speed but limited-distance local area networks.

It is now evident that organizations or users are using different network technologies to connect computers over the network. The desire of sharing more and more information among homogeneous or heterogeneous interest groups motivated the researcher to device a technology whereby one group of users could extend its information system to another group who had a different network technology and different network protocols. This necessity was recognized in early 70s by a group of researchers in the United States of America (USA) who hit upon a new principle popularly known as internetworking. Other organizations also became involved in this area of interconnecting networks, such as ITU-T (formerly CCITT) and ISO. All were trying to define a set of protocols, layered in a well-defined suite, so that applications would be able to communicate with each other, regardless of the underlying network technology and the operating systems where those applications run.

10.2 INTERNETWORKING CONCEPTS

The availability of different operating systems, hardware platforms and the geographical dispersion of computing resources necessitated the need of networking in such a manner that computers of all sizes could communicate with each other, regardless of the vendor, the operating system, the hardware platform, or geographical proximity. Therefore, we may say that internetworking is a scheme for interconnecting multiple networks of dissimilar technologies. Need of additional hardware and software is required to interconnect multiple networks of dissimilar technologies. This additional hardware is positioned between networks and software on each attached computer. This system of interconnected networks is called an internetwork or an Internet.

An example internetwork:

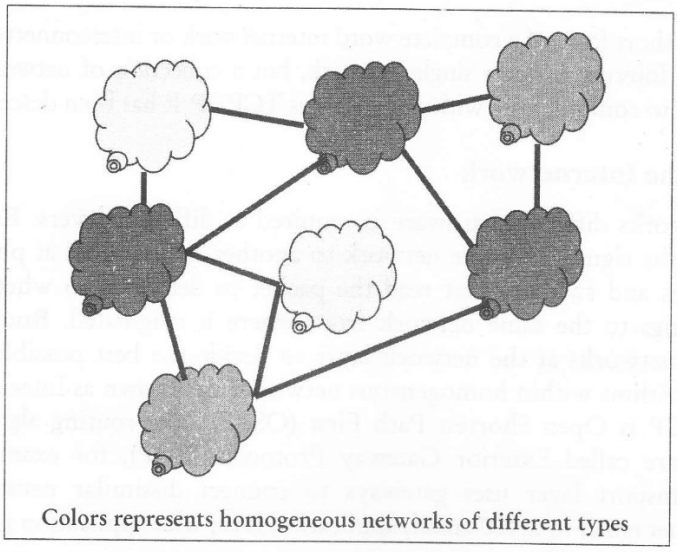


Figure 10.1: Internetworking of Different Homogeneous Networks

To develop standards for internetworking, ARPAnet, a project of DARPA introduced the world of networking with protocol suite concepts such as layering, well before ISO's initiative. This is NCP (Network Control Program) host-to-host protocol to the TCP/IP protocol suite. ARPAnet was basically a network based on leased lines connected by special switching nodes, known as Internet Message Processors (IMP). Many researchers were involved in TCP/IP research by 1979. This motivated DARPA to form an informal committee to coordinate and guide the design of the communication protocols and architecture. The committee was called the Internet Control and Configuration Board (ICCB).

The first real implementation of the Internet was when DARPA converted the machines of its research network ARPAnet to use the new TCP/IP protocols. After this transition, DARPA demanded that all computers willing to connect to its ARPAnet must use TCP/IP. The success of ARPAnet was more than the expectations of its own founders and TCP/IP internetworking became widespread. As a result, new Wide Area Networks (WAN) were created in the USA and connected to ARPAnet using TCP/IP protocol. In turn, other networks in the rest of the world, not necessarily based on the TCP/IP protocols, were added to the set of interconnected networks. Computing facilities all over North America, Europe, Japan, and other parts of the world are currently connected to the Internet via their own sub-networks, constituting the world's largest network. In 1990, ARPAnet was eliminated, and the Internet was declared as the formal global network.

DARPA also funded a project to develop TCP/IP protocols for Berkeley UNIX on the VAX and to distribute the developed codes free of charge with their UNIX operating system. The first release of the Berkeley Software Distribution (BSD) to include the TCP/IP protocol set was made available in 1983 (4.2BSD). This led to the spread of TCP/IP among universities and research centers and has become the standard communications subsystem for all UNIX connectivity. There are many updated versions of BSD code available. These are 4.3BSD (1986), 4.3BSD Tahoe (1988), 4.3BSD Reno (1990) and 4.4BSD (1993).

10.2.1 Internet

The word Internet is a short form of a complete word internetwork or interconnected network. Therefore, it can be said that the Internet is not a single network, but a collection of networks. The commonality between them in order to communicate with each other is TCP/IP. It has been described in lesson 2.

10.2.2 Routing in the Internetwork

To interconnect networks different hardware is required at different layers. Repeaters or hubs that amplify and forward the signal from one network to another are required at physical layer. The data link layer uses bridges and switches that read the packet to decide as to whether the data is to be forwarded or it belongs to the same network from where it originated. Routers or multiprotocol routers connect two networks at the network layer to decide the best possible path for delivery of packets. Routing algorithms within homogeneous networks are known as Interior Gateway Protocols (IGP). Example of IGP is Open Shortest Path First (OSPF). The routing algorithms used between dissimilar networks are called Exterior Gateway Protocols (EGP), for example, Border Gateway Protocol (BGP). Transport layer uses gateways to connect dissimilar networks. The change of application like Internet email to x.400 email, application layer uses application gateways.

10.2.3 Virtual Circuits

Connecting a number of dissimilar computer networks presents a seamless communication channel to which many systems are attached. The internal details of the large number interconnecting networks are hidden from the users. The user understands this internetwork of large computers as a single seamless large computer networks. This creates an illusion of virtual network comprising of virtual circuits. The basic idea behind the virtual circuit is to building up an internetwork connection by concatenating a series of intranetworks and gateway to gateway virtual circuits. The gateways are different from routers. Figure 10.2 shows internetworking using concatenated virtual circuits. The source machine requests to the subnet to set up a virtual circuit connection to a destination machine. When the subnet finds that the destination is remote, it builds a virtual circuit to the router nearest the destination machine network. That router creates a virtual circuit to an external gateway. An external gateway is a multiprotocol router. Multi-protocol routers connect networks of different types, which use different routing protocols. Figure 10.2 shows a multiprotocol router connecting networks of dissimilar network protocols.

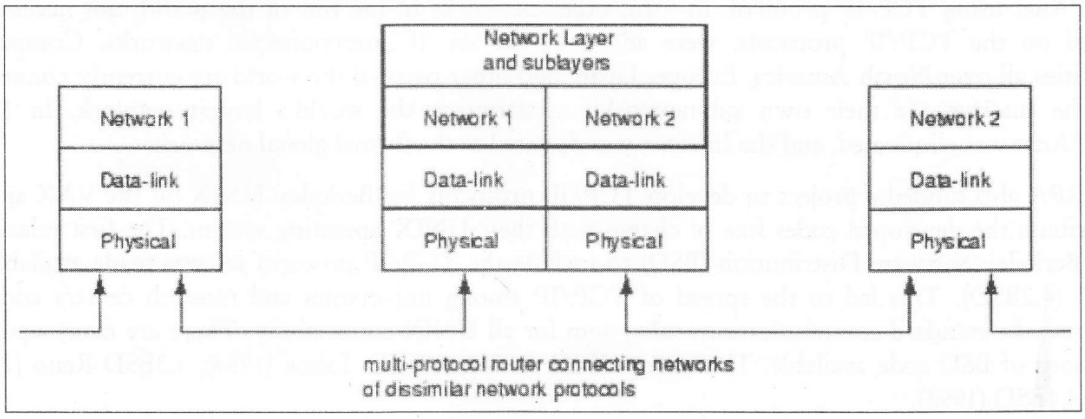


Figure 10.2: Multiprotocol Routers

Like routers, the gateway registers the existence of the virtual circuit in its table and proceeds to build another virtual circuit to a router in the next subnet till the destination host has been reached.

10.2.4 Fragmentation

Each autonomous system places limits on the maximum size of a packet. These limits are dependent on the hardware like the width of a TDM transmission slot, operating system, for example, all buffers are 512 bytes, protocols such as the number of bits in the packet length field, compliance with international standards, retransmissions, congestion, etc. If the size of the IP datagram becomes greater than the maximum size allowed by a networking technology for a hardware frame, the original IP datagram is fragmented into more than one IP datagram fragment. Each of these fragments contains their own header.

Hence, routing through an internetwork must consider the size of a packet as to whether that packet will be acceptable to every autonomous system of networks along the path. A packet entering into a new network needs to be fragmented into acceptable size packets. Thereafter, it requires to be reassembled when it reaches the next gateway. This is known as transparent fragmentation. In another case, a packet is fragmented at the first gateway and then reassembled only at the destination host. This is known as non-transparent fragmentation. ATM networks hardware provides transparent fragmentation of packets into cells and then reassembly of cells into packets. If a packet is fragmented, the fragments must be numbered in such a way that the original data stream may be reproduced.

10.3 INTERNETWORKING ARCHITECTURE

It involves:

- OSI Model
- 3-layer model
- TCP/IP Model

10.3.1 Open Systems Interconnection (OSI) Reference Model

The International Standardization Organization (ISO) developed the OSI model of data communications in 1984. OSI specifies a seven-layer model as shown in Figure 10.3. In addition to forming the basis of the ongoing development of OSI's own protocols, it is used by the industry as the frame of reference when describing protocol architectures and functional characteristics. The OSI is the most popular packet-based structure of layers or protocol stack that defines 7 layers. The Application Layer that is the top layer is user interface and the users work directly with applications. The user works way down from layer 7 to layer 1 where each successive layer adds their own header to the packet that was handed down to it from the layer above.

The ISO, in an effort to encourage open networks, developed an open systems interconnect reference model. The model logically groups the functions and sets rules, called protocols, necessary to establish and conduct communication between two or more parties. The model consists of seven functions, often referred to as layers as shown in Figure 10.3.

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

Figure 10.3: OSI Model

The last three layers are mainly concerned with the organization of terminal software and are not directly the concern of communications engineers. The transport layer is the one, which links the communication processes to this software oriented protocols. The transmitting device uses the top layer, at which point the data is placed into a packet, prepended by a header. The data and header, known collectively as a Protocol Data Unit (PDU), are handled by each successively lower layer as the data works its way across the network to the receiving node. At the receiving node, the data works its way up the layered model, successively higher layers strip off the header information.

The basic header of OSI layer is shown in Figure 10.4 PDU (Protocol Data Unit) is the units of data passed between respective layers at sending and receiving ends.

PDU	
Header	Data

Figure 10.4: OSI Header

The basic philosophy of the 7-layer model is that each layer may be defined independently of every other layer. Thus from the user point of view, interchange takes effect across each operation passes down through the layers of the model until data interchange is affected through the physical connection. The underlying principles and guidelines that were applied to arrive at the seven layers are given below:

- A layer is created at different level of abstraction.
- Each layer is assigned to perform well-defined functions.
- The function of each layer is based on internationally standardized protocols.
- The layer boundaries are chosen to minimize the information flow across the interfaces.
- The number of layers is kept large enough that distinct functions have different layers. They are also kept small enough that the architecture does not become unwieldy.

Physical Layer (Layer 1)

This layer describes the physical media or communication channel over which the bit stream is to be transmitted with the objective that when sending side sends a 1 bit, it is received by the receiving side as a 1 bit, not as a 0 bit. Hence, it defines the electrical and mechanical aspects of interfacing to a physical medium for transmitting data, as well as setting up, maintaining, and disconnecting physical links. It is primarily concerned with moving bits from one node to next over the physical link. The issues concerning with the physical layer involve amplitude of the pulses to define 1 and 0 level, width

of the pulse in microseconds, types and mode of communications, establishment and breaking of connections at the time of communications, types of connectors, etc.

It accepts data from the Data Link layer in bit streams for the subsequent transmission over the physical medium. At this layer, the mechanical (connector type), electrical (voltage levels), functional (ping assignments), and procedural (handshake) characteristics are defined. RS-232C/D is an example of a physical layer definition.

Data Link Layer (Layer 2)

It takes the bits that are received by the physical layer and detects error. This establishes an error free communications path between network nodes over the physical channel, frames messages for transmission, checks integrity of received messages, manages access to and use of the channel, ensures proper sequence of transmitted data. Hence, this layer is responsible for the reliable transfer of data across the Physical link. Its responsibilities include such functions as data flow control, breaking the input data, frame formatting, transmission of the frames sequentially, error detection, and link management, etc. In order to provide a reliable service, it also offers processing of the acknowledgement frames, retransmitting lost or damaged frames, etc. Data link layer is further subdivided into Medium Access (MAC) sub layer to deal with the access control over the shared channel in broadcast networks.

Network Layer (Layer 3)

The network layer comprises software that addresses the PDUs and transports them to the ultimate destination, setting up the appropriate paths between the various nodes. Therefore, the main objective of this layer is to control the operation of the subnet. It is the layer, which provides Internet Protocol (IP) to use it. It is mainly responsible for providing routing services from source to destination across the Internet. In doing so, it allows internetworking among heterogeneous networks using different addressing, length of packet, protocols, etc. The routing may be static or dynamic. Network layer also plays important role in congestion control.

It also shields the above layers from details about the underlying network (the network topology and road map) and the routing technology that might have been deployed to connect different networks together. In addition to routing, this layer is responsible for establishing and maintaining the connection. In broadcast networks, the routing problem is simple, so the network layer is often thin or even nonexistent.

The next three layers are task oriented and have to do with the operations performed by the user rather than with the network.

Transport Layer (Layer 4)

This layer guarantees the orderly and reliable delivery of data between end systems after accepting data from the session layer. Data is accepted from the Session layer and split up into smaller units, if needed. Session layer passes the data to the Network layer and ensures that the packets arrive correctly at the receiving side.

Basically, it performs connection management based upon the throughput conditions. In normal condition, one network connection corresponds to multiple transport connections. In high throughput condition, one transport connections correspond to multiple network connection. The most popular protocol suite TCP/IP uses this layer. Transport layer also performs additional functions

such as data multiplexing and de-multiplexing. This layer divides up a transmitting message into packets and reassembles it at the receiving end. Service offered at this layer includes an error-free point-to-point channel to deliver messages in the order in which they were sent. The transport layer is a true source-to-destination or end-to-end layer. Flow control between hosts is also needed but different from between routers (similar principles will apply to both).

Session Layer (Layer 5)

The session layer is responsible for establishing, maintaining, and arbitrating the dialogs between communicating applications. It also provides enhanced services useful in some applications, for example, remote login, remote file transfer, etc. It is also responsible for the orderly recovery from failures by implementing appropriate check pointing mechanisms.

Presentation Layer (Layer 6)

The presentation layer performs functions related to the syntax and semantics of the information transmitted that include formatting and displaying of received data by terminals and printers. It is concerned with differences in the data syntax used by communicating applications. This layer is responsible for remedying those differences by resorting to mechanisms that transform the local syntax (specific to the platform in question) to a common one for the purpose of data exchange. For example, it performs encoding of data in a standard agreed upon way to facilitate information exchange among heterogeneous systems using different codes for strings, for example, conversion between ASCII and EBCDIC character codes. It facilitates data compression for reducing the number of bits to be transmitted and encrypts data for privacy and authentication, if necessary.

Application Layer (Layer 7)

The application layer provides support services for user and application tasks. It determines how the user will use the data network. It allows the user to use the network. For example, it provides network-based services to the end user. Examples of network services are distributed databases, electronic mail, resource sharing, file transfers, remote file access and network management. This layer defines the nature of the task to be performed.

The communication between two nodes in OSI model takes place horizontally as shown in Figure 10.6. Each layer in the OSI model except the physical layer is implemented based on software program or algorithm running on that particular node's a computer that connects logically the corresponding layer of another node's computer in communication with first node and vice versa. It means to say that a software and procedures process running at layer 4 on one computer can accomplish logical communication with a similar process running at layer 4 on another computer. However, the communicating nodes are considered to be physically connected at layer 1, therefore, this indicates that a process to be run on the layer, the data from the sending node must pass down the data through the layers between layer 4 and layer 1. Thereafter, the data is transmitted over the physical connection to layer 1 of the receiving node's computer and "passed up to the layer 4 of the receiving node's computer. Thus layer 4 of one node connects with layer 4 of another node even though they do not have physical connection directly. Form the Figure 10.5 it is evident that communication between two nodes also requires vertical communication within the same machine except at the physical layer.

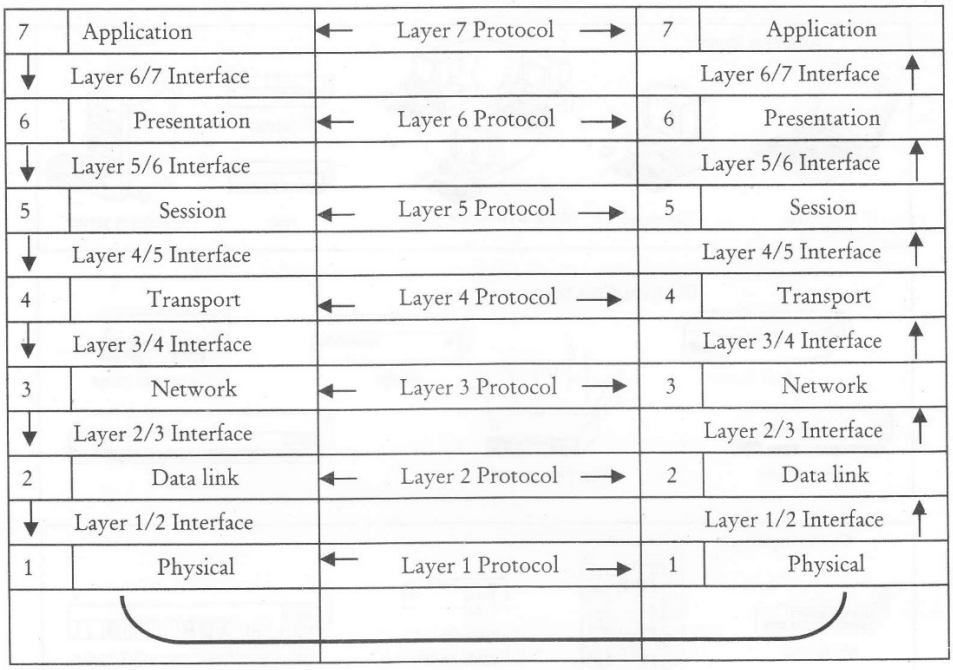


Figure 10.5: Communication between Two Computer in OSI Model

10.3.2 3-Layer Model

Another model of internetworking architecture is a 3-Layer model which is also known as the hierarchical internetworking model. The three functional layers of the network are considered to be the most important area of this model which is used to design an implement a less expensive internetwork which proves to be reliable and scalable. Like other models, it does not focus on building frames.

1. *Core layer:* This layer is the most important part of the network. It is called the backbone of the network. It contains the high-end switches and high-speed cables such as fiber cables. This layer makes sure that traffic between the network is switching as quickly as possible with high speed and thus it ensures quality results. This model cannot function without core layer which mainly refer to speed. It provides reliable delivery of packets without any disturbance. Also, packets are not manipulated by the devices in this layer. So, Core layer is mainly deals with manage traffic between the networks with reliability and speed.
2. *Distribution layer:* This layer mainly deals with Routing. LAN-based routers and switches are included in this layer .In this layer, packets are properly routed between access layer and the core. This layer is also known as the Workgroup layer.
3. *Access layer:* This layer mainly deals with switching and is surrounded by hubs and switches. This layer is also called the desktop layer as it connects client nodes to the network such as workstations. In this layer packets are delivered to end user computers.