THIRUVALLUVAR UNIVERSITY

Serkkadu, Vellore – 632 115.

E-NOTES

BCS 53/ BCA 53

Data Communication and Network

(5th Sem B.Sc. CS / BCA)

STEERED BY

Dr. S. Thamarai Selvi, M.E., Ph.D.,
Vice Chancellor, Thiruvalluvar University, Serkkadu, Vellore

PREPARED BY

1. **Dr. S. P. Ponnusamy, M.C.A., M.Phil., Ph.D.,**
   Assistant professor & Head, Department of Computer Science,
   Thiruvalluvar University Model Constituent College of Arts and Science, Tittagudi.
2. **Mrs. S. Uma, M.C.A., M.Phil., M.E., SET.,**
   Assistant Professor, Department of Computer Science and Applications,
   Thiruvalluvar University College of Arts and Science, Thiruppathur.
3. **Mrs. K. Subashini, M.C.A., M. Phil.,**
   Assistant Professor, Department of Computer Science,
   Theivanai Ammal College for Women (Autonomous), Villupuram.
4. **Mrs. V. Sharmila Devi, M.C.A., M. Phil.,**
   Assistant Professor, Department of Computer Science,
   Theivanai Ammal College for Women (Autonomous), Villupuram.
5. **Mr. K. Karnan, M.C.A., M.Phil., SET.,**
   Assistant Professor, Department of Computer Science,
   Dr. S. Ramadoss Arts and Science College, Vriddhachalam.
6. **Mrs. P. Shanthi, M.Sc., M.Phil.,**
   Assistant Professor, Department of Computer Science,
   Dr. S. Ramadoss Arts and Science College, Vriddhachalam.
7. **Mrs. K.C. Tamil Selvi, M.C.A., M.Phil., SET.,**
   Assistant Professor, Department of Computer Science,
   Jawahar Science College, Neyveli.
8. **Mrs. U. Umamaheswari, M.C. A., M.Phil., SET.,**
   Guest Lecturer, Department of Computer Science,
   Thiruvalluvar University Model Constituent College of Arts and Science, Tittagudi.
9. **Mrs. S. Valli, M.Sc., M.Phil., SET.,**
   Guest Lecturer, Department of Computer Science,
   Thiruvalluvar University Model Constituent College of Arts and Science, Tittagudi.
10. **Mr. P. Velmurugan, M.Sc., M.Phil., SET,**
    Assistant Professor, Department of Computer Science,
    Sree Raghavendra Arts and science college, Chidambaram.

ACKNOWLEDGEMENT

It is a great pleasure to prepare the e-content for Data Communication and Network to the fifth semester computer science and BCA students under the motivation and guidance from our honourable Vice Chancellor – Professor **Dr. S. Thamarai Selvi**. Her dynamism, vision, sincerity, and guidance have deeply inspired us. She worked her magic on every page in this e-content, reorganised content wherever necessary, bringing value added words in every line. She has taught us the way to present the content to the students in a best possible way to have clear and crisp understanding. She was able to tune into the task and identify the ones that diverted our team focus and energy keeping us from getting our things done. It was a great privilege and honour to work under her guidance. We are extremely grateful for what she has offered us.

Dr. S. P. Ponnusamy

Mrs. S. Uma

Mrs. K. Subashini

Mrs. V. Sharmila Devi

Mr. K. Karnan

Mrs. P. Shanthi

Mrs. K.C. Tamil Selvi

Mrs. U. Umamaheswari

Mrs. S. Valli

Mr. P. Velmurugan

DISCLAIMER

This document does not claim any originality and cannot be used as a substitute for prescribed textbooks. The information presented here is merely a collection by the committee members for their respective teaching assignments. Various sources as mentioned at the end of the document as well as freely available material from internet were consulted for preparing this document. The ownership of the information lies with the respective authors or institutions.

Content Preparation

Sl. No.	Unit No.	Topic Prepared	Faculty Name
1	1	Introductory Concepts, Network software, Physical Layer	Dr. S. P. Ponnusamy
2	1	Network Architecture	Prof. S. Uma
3	1	Network hardware, Cable television	Prof. V. Sharmiladevi
4	1	Guided transmission media	Prof. K. Subashini
5	2	Channel allocation problem - Multiple access protocols	Dr. S. P. Ponnusamy
6	2	Ethernet	Prof. K. C. Tamil Selvi
7	2	Data Link Layer - Design issues	Prof. S. Valli
8	2	Wireless LAN - 802.11 architecture	Prof. U. Umamheswari
9	3	Network Layer : Design issues, Routing Algorithms	Prof. V. Sharmiladevi
10	3	Shortest path routing, Flooding,	Prof. K. Karnan
11	3	Broadcast & Multicast routing	Dr. S. P. Ponnusamy
12	3	Congestion, Control & internetworking	Prof. P. Shanthi
13	4	Transport Layer - Transport service -Elements of transport protocols - User Datagram Protocol, Transmission Control Protocol.	Prof. S. Uma
14	5	Application Layer - DNS - Electronic mail	Prof. K. Subashini
15	5	World Wide Web - Multimedia - Network security.	Prof. P. Velmurugan

Syllabus

Data Communication & Networks

Objective:

To equip students to basics of Data Communication and prepare them for better computer networking

UNIT I

Introductory Concepts - Network hardware - Network software – Network Architecture - Physical layer - Guided transmission media - Cable television.

UNIT II

Data Link Layer - Design issues - Channel allocation problem - Multiple access protocols - Ethernet - Wireless LAN - 802.11 architecture.

UNIT III

Network Layer : Design issues, Routing Algorithms, Shortest path routing, Flooding, Broadcast & Multicast routing congestion, Control & internetworking.

UNIT IV

Transport Layer - Transport service - Elements of transport protocols - User Datagram Protocol - Transmission Control Protocol.

UNIT V

Application Layer - DNS - Electronic mail - World Wide Web - Multimedia - Network security.

TEXT BOOK

1. Tannenbaum, A.S., “Computer Networks”, 4th Edition, Prentice Hall, 2003.

REFERENCES

1. William Stallings, “Local and Metropolitan Area Networks”, 6th Edition, Pearson Education India, 2008.
2. W. Stallings, "Data and Computer Communication", Pearson Education, 5th Edition, 2001
3. Behrouz A. Forouzan, “Data Communications and Networking”, 4th Edition, McGraw Hill Education, 2007.
4. Jim Kurose; Keith Ross, “Computer Networking: A Top-Down Approach”, 6th Edition, Pearson Education, Inc, 2003.
5. Larry L. Peterson; Bruce S. Davie, “Computer Networks : A Systems Approach”, 4th Edition, Morgan Kaufmann Publishers, 2007.
6. Doug Lowe, “Networking All-in-One Desk Reference for Dummies”, 2nd Edition, Wiley Publishing, Inc,2005.

7. Ramon Nastase, “Computer Networking for Beginners”, Amazon Digital Services LLC - KDP Print US, 2018

8. Douglas Comer, “Computer Networks and Internets”, 5th Edition, Prentice Hall, 2009.

9. Russ White and Ethan Banks,” Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks”, 1st Edition, Addison-Wesley Professional.

10. Michael B. White, “Computer Networking: The Complete Guide to Understanding Wireless Technology, Network Security, Computer Architecture and Communications Systems (Including Cisco, CCNA and CCENT)”, CreateSpace Independent Publishing Platform, 2018.

11. Olivier Bonaventure, “Computer Networking: Principles, Protocols, and Practice”, The Saylor Foundation, Release 0.25, 2011.

Table of Contents

1 Introduction and Physical Layer

1.1 Introduction

In today's world, the communication is deciding the all facts of the growth. Effective, easiest, understandable, timely communications are creating the world's better growth. The growth of the internet, telecommunication field, communication devices make the people interactive, happily and wealthy. An event happens in place can be communicated to any place in the world. For example, a live sports event happened in Calcutta can be viewed by the people sitting in any place in the world.

The network allows people to communicate information to any people in the world by means of one-to-one, one-to-many or all. In this chapter, we are going to study about the introduction of networks, network hardware, network software and network architecture.

1.1.1 Data Communication

- Data

The word 'data' refers that representation of information in an understandable form by the two parties who are creating and using it. The Webster dictionary defined data as "*information in digital form that can be transmitted or processed*". The data may be in any form such as text, symbols, images, videos, signals and so on.

- Communication

Communication is a referred as exchanging information from one entity to another entity in a meaningful way. The entities may be referred as human being, machines, animals, birds, etc. The communication could be done between the two entities / parties. The meaningful way refers that the meaning of the communication must be understandable between the two entities. The figure 1.1 shows the model for communication between two people.

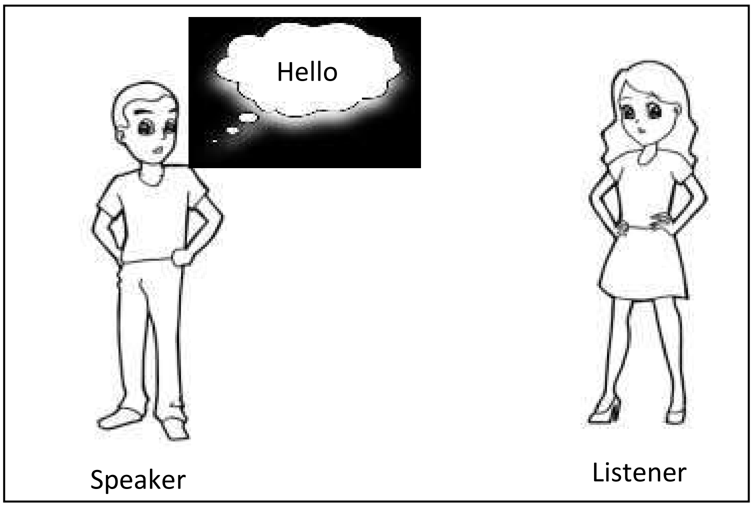


Figure 1.1 Communication between two persons

In figure 1.1 the speaker (a person) making oral communication to the listener (other person) in an understandable language '*English'* using the word "*Hello*". To provide the communication, the information must be carried by a carrier. The carrier may be either wire or wireless. In oral communication between two people, the wireless is acting as a carrier to carry the information. In computer technology, the carrier is referred as *communication medium*. In computer network, the speaker is referred as source of the information and listener is referred as the receiver or destination of the information.

- Data Communication

From the above two reference, we understand that "*Data communication is process of exchanging data between two devices through a communication medium in a meaningful way*". The devices must be part of the communication system. The communication system is made up of the both hardware equipment and software. To provide the effective communication system, the following four fundamental characteristics must be followed;

1. Delivery : The data to be communicated must be delivered to the correct destination.
2. Accuracy : The data should be delivered accurately as it is without any alteration.
3. Timeliness : The communication system must deliver the data without any delay.
4. Jitter : In network the data are split into smaller groups (packets) and send them separately. The variation of the arrival between two packets is referred as jitter.

1.1.2 Components

The following five components are the essential part of the communication system and figure 1.2 shows the representation of the components placement in the communication system.

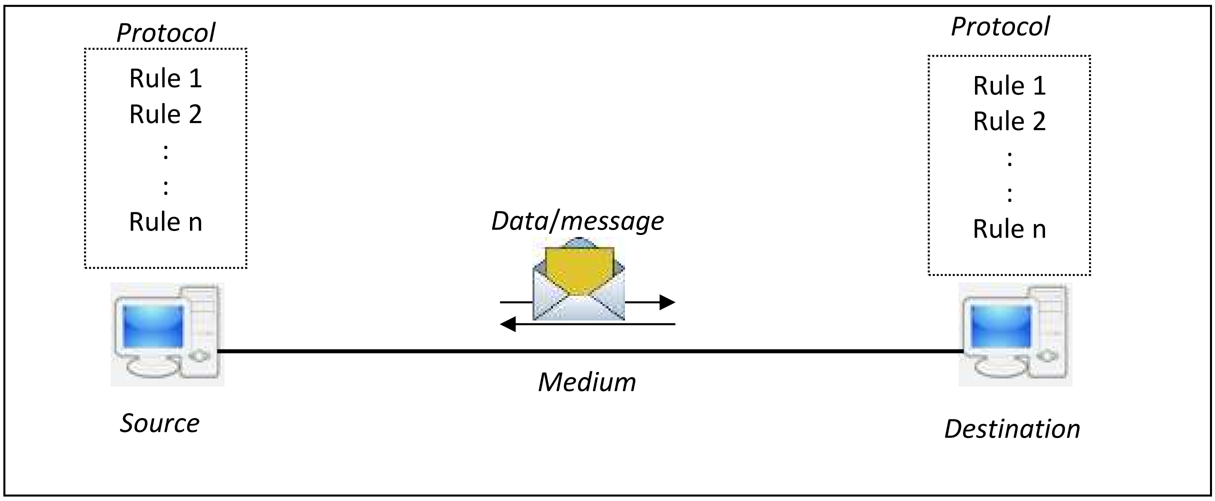


Fig 1.2 Components of Data Communication

1. Data/Message : It is the primary part of the communication system. The information is communicated between the source and destination is called data/message.

2. Source : The source is a device which generates and sends the data to the destination.
3. Destination : It is a device that receives the data.
4. Medium : It acts as carrier to carry the data from the source to the destination. The carrier provides the path through wire or wireless.
5. Protocol : It is set of rules that govern the data communication in a correct manner.

The source and destination may be computer, mobile phones, workstations, servers, video cameras and so on. The protocol provides the effective communication. This provides the methodology how to interact with each other without any loss or interference.

1.1.3 Mode of Data Flow

The data flow defines the flow direction of the data between source and destination. The data flow may be either simplex or half-duplex or full duplex. The figure 1.3 shows the three modes of the data flow.

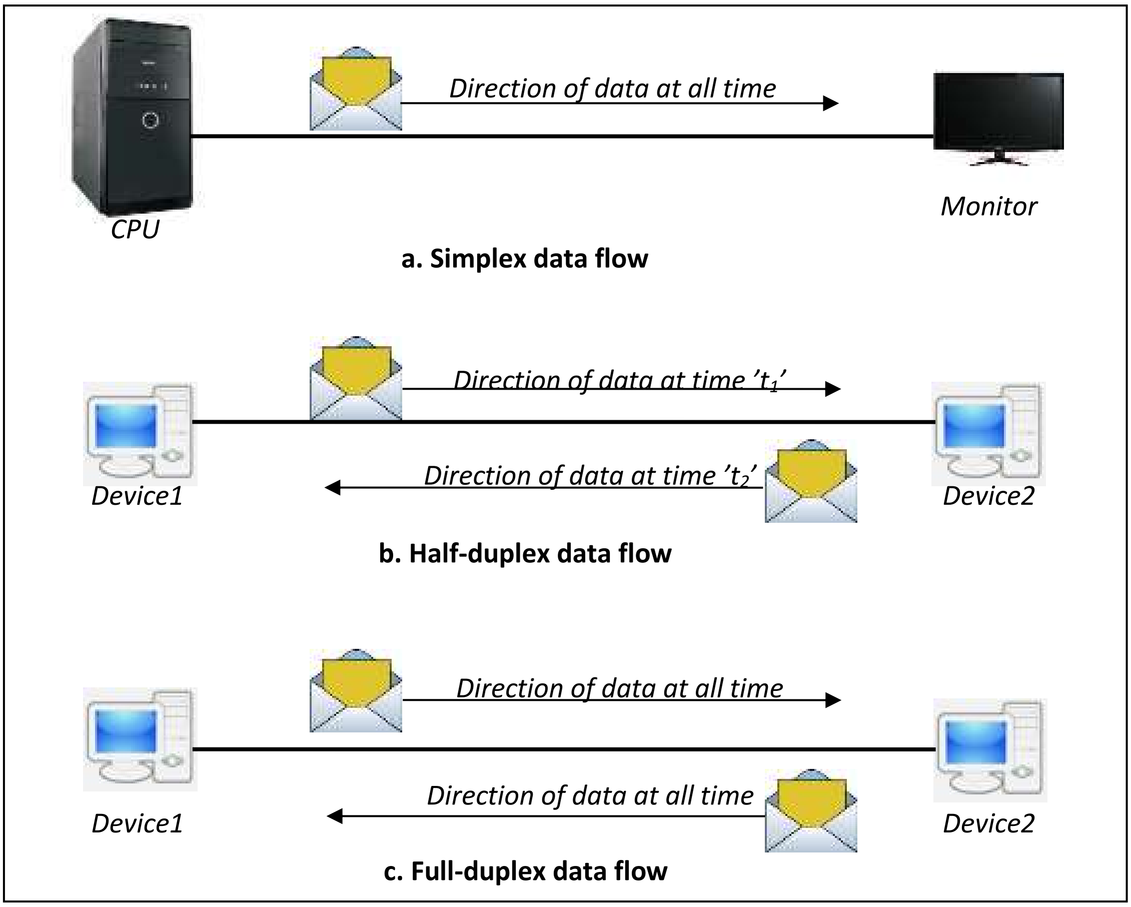

Direction of data at all time
CPU
Monitor
a. Simplex data flow
Direction of data at time 't1'
Direction of data at time 't2'
Device1
Device2
b. Half-duplex data flow
Direction of data at all time
Direction of data at all time
Device1
Device2
c. Full-duplex data flow

Fig. 1.3. Mode of Data Flow

- Simplex : In simplex mode, the direction of the data flow is unidirectional. One of the device can transmit the data and another device can receive at all time (Fig. 1.3.a). The example is the CPU sends the data to the monitor at all the time.

- Half-Duplex : In half-duplex mode, the data can be transmitted on both directions but not at the same time (device 1 to device 2 or device 2 to device 1) (Fig. 1.3.b). One device can send and another one can receive at a time. The example is walkie-talkie. The entire medium is used for the one-way transmission.
- Full-Duplex : In full-duplex mode, the data can be transmitted on both directions (device 1 to device 2 and device 2 to device 1) at the same time (Fig. 1.3.c). One device can send and another one can receive at a time. The example is telephone communication. In this, the entire medium is divided for the two-way transmission.

1.2 Networks

A network is set of interconnected devices (sometime referred as nodes) which are used to transmit data between them with agreed protocols. The networks are used to connect the people, machines, devices to share the data anywhere in the world. The devices can be computers, printers, mobile phones, servers which are capable of sending and receiving data. The data can be generated by a device.

There is considerable confusion in the literature between a computer network and a distributed system. The key distinction is that in a distributed system, a collection of independent computers appears to its users as a single coherent system. Usually, it has a single model or paradigm that it presents to the users. Often a layer of software on top of the operating system, called middleware, is responsible for implementing this model. A well-known example of a distributed system is the World Wide Web, in which everything looks like a document (Web page).

1.2.1 History of Network

A computer network is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections (data links) between nodes. These data links are established over cable media such as wires or optic cables, or wireless media such as Wi-Fi.

Computer networking as we know it today may be said to have gotten its start with the Arpanet development in the late 1960s and early 1970s. Prior to that time there were computer vendor "networks" designed primarily to connect terminals and remote job entry stations to a mainframe.

In 1940, George Sitbit used a teletype machine to send instructions for a problem set from his model at Dartmouth college to his complex number calculator in New York and received results back by the same means. In 1950's, early networks of communicating computers included the military radar system Semi-Automatic Ground Environment (SAGE) was started.

Later, in 1960s, the notion of networking between computers viewing each other as equal peers to achieve "resource sharing" was fundamental to the ARPAnet design [1]. The other strong emphasis of the Arpanet work was its reliance on the then novel technique of packet switching to efficiently share communication resources among "bursty" users, instead of the more traditional message or circuit switching. The table 1.1 gives the time frame of the computer network growth from network to internet.

Year	Event
1961	The idea of ARPANET, one of the earliest computer networks, was proposed by Leonard Kleinrock in 1961, in his paper titled "Information Flow in Large Communication Nets."
1965	The term "packet" was coined by Donald Davies in 1965, to describe data sent between computers over a network.
1969	ARPANET was one of the first computer networks to use packet switching. Development of ARPANET started in 1966, and the first two nodes, UCLA and SRI (Standford Research Institute), were connected, officially starting ARPANET in 1969.
1969	The first RFC surfaced in April 1969, as a document to define and provide information about computer communications, network protocols, and procedures.
1969	The first network switch and IMP (Interface Message Processor) was sent to UCLA on August 29, 1969. It was used to send the first data transmission on ARPANET.
1969	The Internet was officially born, with the first data transmission being sent between UCLA and SRI on October 29, 1969, at 10:30 p.m.
1970	Steve Crocker and a team at UCLA released NCP (NetWare Core Protocol) in 1970. NCP is a file sharing protocol for use with NetWare.
1971	Ray Tomlinson sent the first e-mail in 1971.
1971	ALOHAnet, a UHF wireless packet network, is used in Hawaii to connect the islands together. Although it is not Wi-Fi, it helps lay the foundation for Wi-Fi.
1973	Ethernet is developed by Robert Metcalfe in 1973 while working at Xerox PARC.
1973	The first international network connection, called SATNET, is deployed in 1973 by ARPA.
1973	An experimental VoIP call was made in 1973, officially introducing VoIP technology and capabilities. However, the first software allowing users to make VoIP calls was not available until 1995.
1974	The first routers were used at Xerox in 1974. However, these first routers were not considered true IP routers.
1976	Ginny Strazisar developed the first true IP router, originally called a gateway, in 1976.
1978	Bob Kahn invented the TCP/IP protocol for networks and developed it, with help from Vint Cerf, in 1978.
1981	Internet protocol version 4, or IPv4, was officially defined in RFC 791 in 1981. IPv4 was the first major version of the Internet protocol.
1981	BITNET was created in 1981 as a network between IBM mainframe systems in the United States.
1981	CSNET (Computer Science Network) was developed by the U.S. National Science Foundation in 1981.
1983	ARPANET finished the transition to using TCP/IP in 1983.
1983	Paul Mockapetris and Jon Postel implement the first DNS in 1983.
1986	The NSFNET (National Science Foundation Network) came online in 1986. It was a backbone for ARPANET, before eventually replacing ARPANET in the early 1990's.
1986	BITNET II was created in 1986 to address bandwidth issues with the original BITNET.
1988	The first T1 backbone was added to ARPANET in 1988.

1988	WaveLAN network technology, the official precursor to Wi-Fi, was introduced to the market by AT&T, Lucent, and NCR in 1988.
1988	Details about network firewall technology was first published in 1988. The published paper discussed the first firewall, called a packet filter firewall, that was developed by Digital Equipment Corporation the same year.
1990	Kalpana, a U.S. network hardware company, developed and introduced the first network switch in 1990.
1996	IPv6 was introduced in 1996 as an improvement over IPv4, including a wider range of IP addresses, improved routing, and embedded encryption.
1997	The first version of the 802.11 standard for Wi-Fi is introduced in June 1997, providing transmission speeds up to 2 Mbps.
1999	The 802.11a standard for Wi-Fi was made official in 1999, designed to use the 5 GHz band and provide transmission speeds up to 25 Mbps.
1999	802.11b devices were available to the public starting mid-1999, providing transmission speeds up to 11 Mbps.
1999	The WEP encryption protocol for Wi-Fi is introduced in September 1999, for use with 802.11b.
2003	802.11g devices were available to the public starting in January 2003, providing transmission speeds up to 20 Mbps.
2003	The WPA encryption protocol for Wi-Fi is introduced in 2003, for use with 802.11g.
2003	The WPA2 encryption protocol is introduced in 2004, as an improvement over and replacement for WPA. All Wi-Fi devices are required to be WPA2 certified by 2006.
2009	The 802.11n standard for Wi-Fi was made official in 2009. It provides higher transfer speeds over 802.11a and 802.11g, and it can operate on the 2.4 GHz and 5 GHz bandwidths.
2018	The Wi-Fi Alliance introduced WPA3 encryption for Wi-Fi in January 2018, which includes security enhancements over WPA2.

Table 1.1 Time period of Network growth

1.2.2 Uses of Computer Networks

The computer networks are used in different applications to meet the requirement of different people at different places in different time. The following are the uses of computer network.

a) Business Applications.

Many companies have a substantial number of computers. For example, a company may have separate computers to monitor production, keep track of inventories, and do the payroll. Initially, each of these computers may have worked in isolation from the others, but at some point, management may have decided to connect them to be able to extract and correlate information about the entire company.

1. **Resource sharing**: The main task of the connectivity of resources is resource sharing. For example, a high-volume networked printer may be installed instead of large collection of individual printers.
2. **Information Sharing** : large and medium-sized company and many small companies are vitally dependent on computerized information. This can be done by a simple client server model connected by network as illustrated in Fig.1.4.

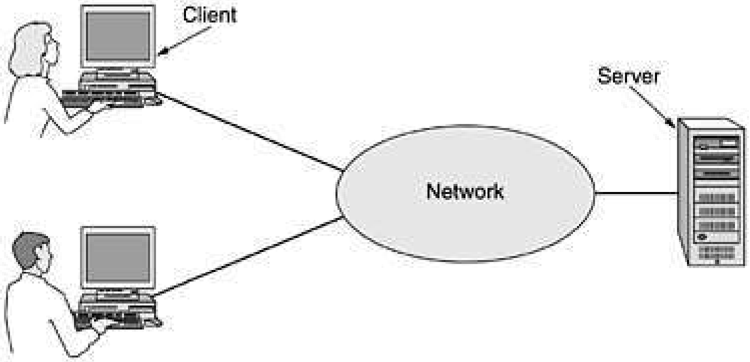


Figure 1.4 A network with two clients and one server

In client-server model in detail, two processes are involved, one on the client machine and one on the server machine. Communication takes the form of the client process sending a message over the network to the server process. The client process then waits for a reply message. When the server process gets the request, it performs the requested work or looks up the requested data and sends back a reply. These messages are shown in Fig. 1.5.

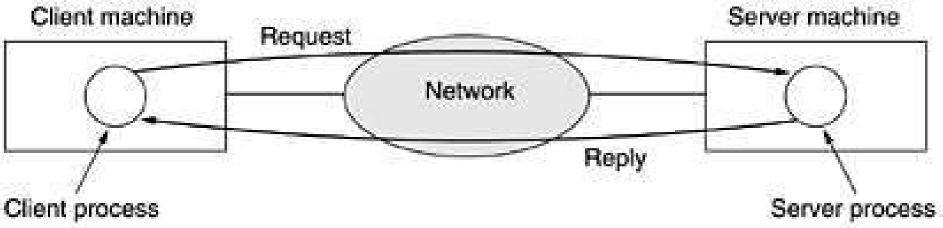


Figure 1.5 Client-server model involves requests and replies

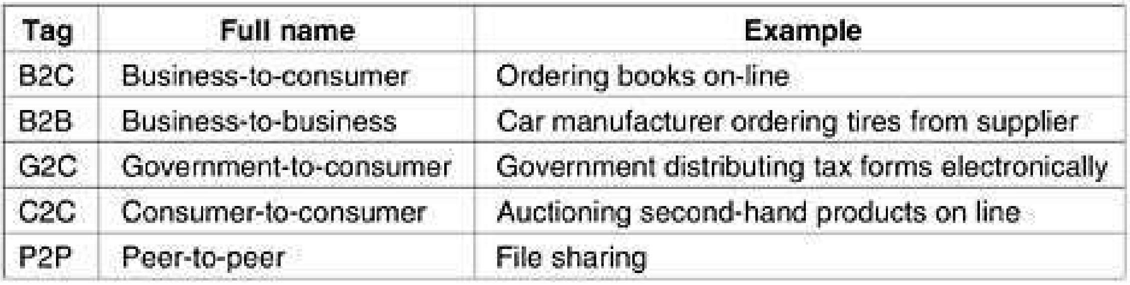
3. **Connecting People** : another use of setting up a computer network has to do with people rather than information or even computers. It is achieved through Email, Video Conferencing.

4. **E-commerce** : many companies is doing business electronically with other companies, especially suppliers and customers, and doing business with consumers over the Internet.

b) Home Applications

The computer network provides better connectivity for home applications via desktop computers, laptops, iPads, iPhones. Some of the more popular uses of the Internet for home users are as follows:

1. Access to remote information.
2. Person-to-person communication (peer-to-peer).
   i. Peer-to-peer - there are no fixed clients and servers.
   ii. Audio and Video sharing
3. Interactive entertainment.
4. Electronic commerce.



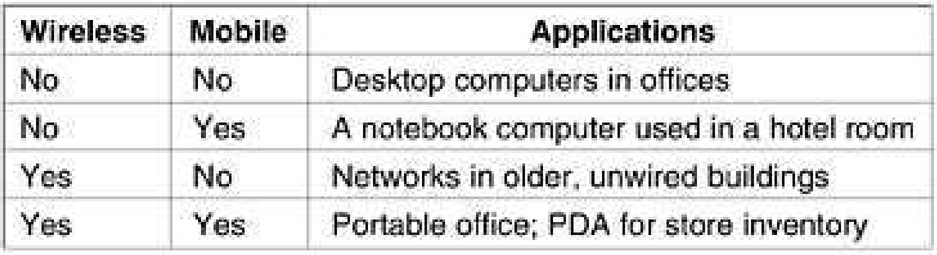
Tag	Full name	Example
B2C	Business-to-consumer	Ordering books on-line
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products on line
P2P	Peer-to-peer	File sharing

Table 1.2 Some forms of e-commerce

c) Mobile Users

As wireless technology becomes more widespread, numerous other applications are likely to emerge. Wireless networks are of great value to fleets of trucks, taxis, delivery vehicles, and repairpersons for keeping in contact with home. Wireless networks are also important to the military.

Although wireless networking and mobile computing are often related, they are not identical, as Table 1.3 shows. Here we see a distinction between fixed wireless and mobile wireless. Even notebook computers are sometimes wired. For example, if a traveller plugs a notebook computer into the telephone jack in a hotel room, he has mobility without a wireless network.



Wireless	Mobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Table 1.3 Combinations of wireless networks and mobile computing

Another area in which wireless could save money is utility meter reading. If electricity, gas, water, and other meters in people's homes were to report usage over a wireless network, there would be no need to send out meter readers.

d) Social issues

The widespread introduction of networking has introduced new social, ethical, and political problems. A popular feature of many networks are newsgroups or bulletin boards whereby people can exchange messages with like-minded individuals. As long as the subjects are restricted to technical topics or hobbies like gardening, not too many problems will arise.

The following are the issues in society due to the misbehave or misconduct of computer networks.

1. Network neutrality
2. Digital Millennium Copyright Act
3. Profiling users

4. Phishing

1.2.3 Criteria of Network

A network must have the following important criteria for effective communication.

- Performance

The performance of a network is measured by many factors such as transit time, response time. The transit time is amount of time required to travel a message from source to destination. The response time is amount of time required for inquiry and response.

- Throughput and Delay

The throughput of the network is measures as amount of data transferred for specified period of time. The high transmission within the specified period of time is called as high throughput network. The delay is measured as time difference between the transit time and actual time taken to transmit. A good network maintains high through and low delay.

- Reliability

The reliability of a network is referred as data delivery should be accurate, less frequency of break in medium, fast recovery of the physical and logical (data) errors.

- Security

The security of a network is referred as protecting the data from damages and alteration, unauthorized access of medium, devices and data, providing mechanisms for losses and intrusions.

1.2.4 Types of connection

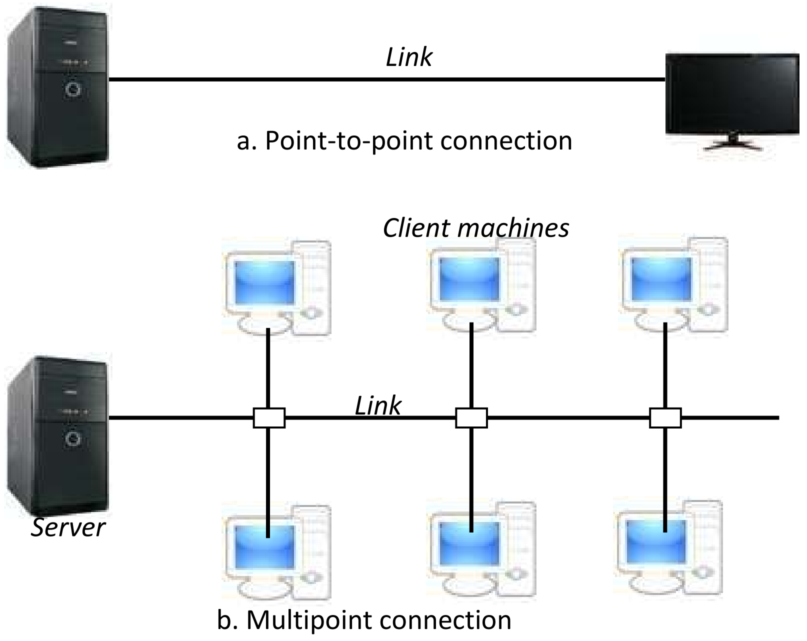
As we have already known that a network is a two or more devices interconnected through a communication medium. The medium provides the physical pathway between two devices. The connectivity between the devices is classified into point-to-point and multipoint.

- point-to-point

It provides a direct and dedicated link between two devices (normally source and destination). The entire transmission capacity of the link is shared for these two devices only (Fig 1.6.a). For example, link between monitor and computer.

- Multipoint

A link is shared by many devices and the transmission capacity is shared by all devices connected (fig 1.6.b). For example, a cable TV network or client-server network.



a. Point-to-point connection

b. Multipoint connection

Fig. 1.6. Type of connectivity

1.3 Network Hardware

1.3.1 Introduction

It is now time to turn our attention from the applications and social aspects of networking (the dessert) to the technical issues involved in network design (the spinach). There are two types of transmission technology that are in widespread use: **broadcast links** and **point-to-point links**.

Point-to-point links:

Point-to-point links connect individual pairs of machines.

- **packets :** To go from the source to the destination on a network made up of point-to-point links, short messages, called packets**.**
- **Unicasting**: Transmission with exactly one sender and exactly one receiver is sometimes called unicasting.

Broadcast links:

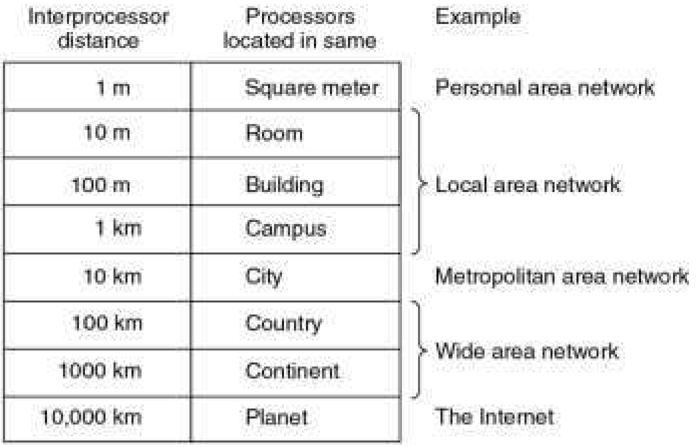
On a broadcast network, the communication channel is shared by all the machines on the network; packets sent by any machine are received by all the others. An address field within each packet specifies the intended recipient.

Upon receiving a packet, a machine checks the address field. If the packet is intended for the receiving machine, that machine processes the packet; if the packet is intended for some other machine, it is just ignored.

A wireless network is a common example of a broadcast link, with communication shared over a coverage region that depends on the wireless channel and thetransmitting machine

- **Broadcasting:** Broadcast systems usually also allow the possibility of addressing a packet to *all* destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting.
- **Multicasting:** Some broadcast systems also support transmission to a subset of the machines, which known as multicasting.

An alternative criterion for classifying networks is by scale. Distance is important as a classification metric because different technologies are used at different scales.



Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Figure 1.7 Classification of interconnected processors by scale.

In Figure 1.7we classify multiple processor systems by their rough physical size. At the top are the personal area networks, networks that are meant for one person. Beyond these come longer-range networks. These can be divided into local, metropolitan, and wide area networks, each with increasing scale. Finally, the connection of two or more networks is called an internetwork. The worldwide Internet is certainly the best-known (but not the only) example of an internetwork.

1.3.2 Personal Area Networks

PANs (**Personal Area Networks**) let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. Without using wireless, this connection must be done with cables.

- **Bluetooth:** some companies got together to design a short-range wireless network called *Bluetooth* to connect these components without wires.

The idea is that if your devices have Bluetooth, then you need no cables. You just put them down, turn them on, and they work together. For many people, this ease of operation is a big plus.

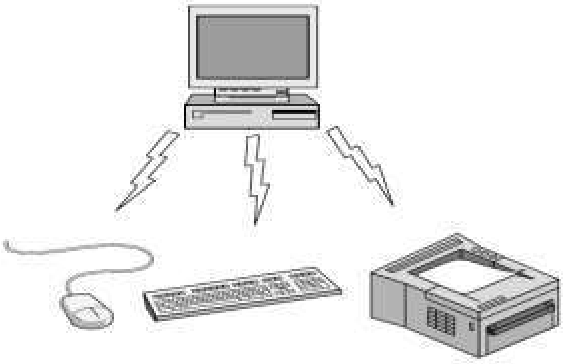


Figure 1.8 Bluetooth PAN configuration.

Bluetooth networks use the master-slave paradigm of Figure. 1.8. The system unit (the PC) is normally the master, talking to the mouse, keyboard, etc., as slaves. The master tells the slaves what addresses to use, when they can broadcast, how long they can transmit, what frequencies they can use, and so on.

Bluetooth can be used in other settings, too. It is often used to connect a headset to a mobile phone without cords and it can allow your digital music player A completely different kind of **PAN** is formed when an embedded medical device such as a pacemaker, insulin pump, or hearing aid talks to a user-operated remote control.

PANs can also be built with other technologies that communicate over short ranges, such as RFID on smartcards and library books.

1.3.3 Local Area Networks

The next step up is the **LAN** (**Local Area Network**). A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information. When LANs are used by companies, they are called **enterprise networks**.

Wireless LANs are very popular these days, especially in homes, older office buildings, cafeterias, and other places where it is too much trouble to install cables. In these systems, every computer has a radio modem and an antenna that it uses to communicate with other computers.

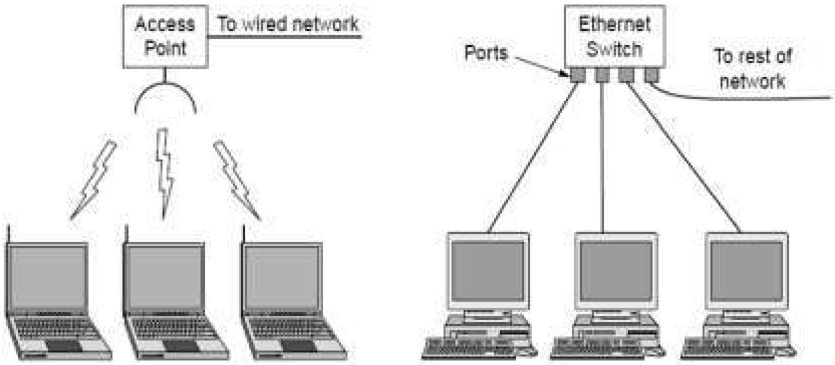


Figure 1.9 Wireless and wired LANs. (a) 802.11. (b) Switched Ethernet.

Each computer talks to a device in the ceiling as shown in Fig. 1.9(a). This device, called an **AP** (**Access Point**), **wireless router**, or **base station**, relays packets between the wireless computers and also between them and the Internet.

Being the **AP** is like being the popular kid as school because everyone wants to talk to you. However, if other computers are close enough, they can communicate directly with one another in a peer-to-peer configuration.

There is a standard for wireless LANs called **IEEE 802.11**, popularly known as **WiFi**, which has become very widespread. It runs at speeds anywhere from 11 to hundreds of Mbps. Wired LANs use a range of different transmission technologies. Most of them use copper wires, but some use optical fiber. LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance.

Typically, wired LANs run at speeds of 100 Mbps to 1 Gbps, have low delay (microseconds or nanoseconds), and make very few errors. Newer LANs can operate at up to 10 Gbps. Compared to wireless networks, wired LANs exceed them in all dimensions of performance. It is just easier to send signals over a wire or through a fiber than through the air.

- **Ethernet** :The topology of many wired LANs is built from point-to-point links. IEEE 802.3, popularly called Ethernet.
- **Switched Ethernet**. Fig. 1.9(b) shows a sample topology of **switched Ethernet**. Each computer speaks the Ethernet protocol and connects to a box called a **switch** with a point-to-point link.
- **Switch:** Each computer speaks the Ethernet protocol and connects to a box called a switch with a point-to-point link. A switch has multiple **ports**, each of which can connect to one computer. The job of the switch is to relay packets between computers that are attached to it, using the address in each packet to determine which computer to send it to.

While we could think of the home network as just another LAN, it is more likely to have different properties than other networks.

[1]. The networked devices have to be very easy to install. Wireless routers are the most returned consumer electronic item. People buy one because they want a wireless network at home, find that it does not work ‘‘out of the box,’’ and then return it rather than listen to elevator music while on hold on the technical helpline.

[2]. The network and devices have to be foolproof in operation. Air conditioners used to have one knob with four settings: OFF, LOW, MEDIUM, and HIGH.

[3]. The low price is essential for success. People will not pay a $50 premium for an Internet thermostat because few people regard monitoring their home temperature from work that important.

[4]. It must be possible to start out with one or two devices and expand the reach of the network gradually

[5]. Security and reliability will be very important. Losing a few files to an email virus is one thing; having a burglar disarm your security system from his mobile computer and then plunder your house is something quite different.

In short, Home LANs offer many opportunities and challenges. Most of the latter relate to the need for the networks to be easy to manage, dependable, and secure, especially in the hands of nontechnical users, as well as low cost.

1.3.4 Metropolitan Area Networks

A **MAN** (**Metropolitan Area Network**) covers a city. The best-known examples of MANs are the cable television networks available in many cities. These systems grew from earlier community antenna systems used in areas with poor over-the-air television reception.

In those early systems, a large antenna was placed on top of a nearby hill and a signal was then piped to the subscribers’ houses. At first, these were locally designed, ad hoc systems. Then companies began jumping into the business, getting contracts from local governments to wire up entire cities.

The next step was television programming and even entire channels designed for cable only. Often these channels were highly specialized, such as all news, all sports, all cooking, all gardening, and so on.

When the Internet began attracting a mass audience, the cable TV network operators began to realize that with some changes to the system, they could provide two-way Internet service in unused parts of the spectrum. At that point, the cable TV system began to morph from simply a way to distribute television to a metropolitan area network.

A MAN might look something like the system shown in Fig. 1.10. In this figure we see both television signals and Internet being fed into the centralized **cable head end** for subsequent distribution to people’s homes.

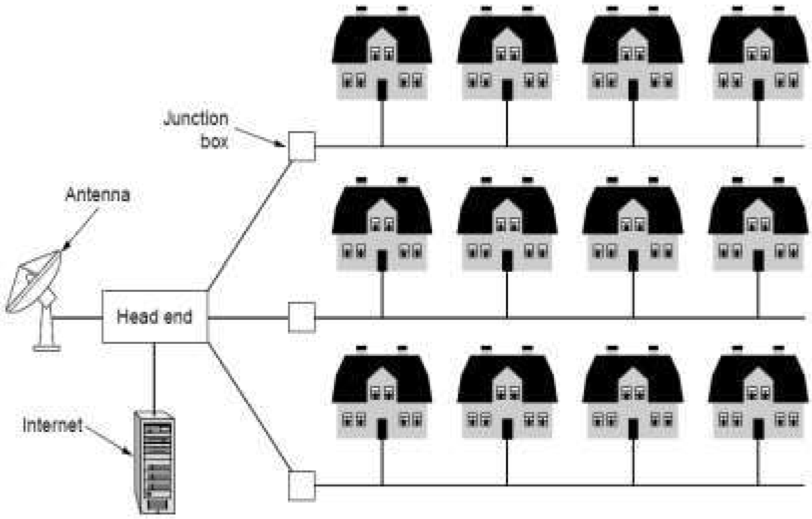


Figure 1.10 A metropolitan area network based on cable TV.

Recent developments in highspeed wireless Internet access have resulted in another MAN, which has been standardized as IEEE 802.16 and is popularly known as **WiMAX**.

1.3.5 Wide Area Networks

A **WAN** (**Wide Area Network**) spans a large geographical area, often a country or continent. We will begin our discussion with wired WANs, using the example of a company with branch offices in different cities.

The WAN in Fig.1.11 is a network that connects offices in Perth, Melbourne, and Brisbane. Each of these offices contains computers intended for running user (i.e., application) programs. We will follow traditional usage and call these machines **hosts**.

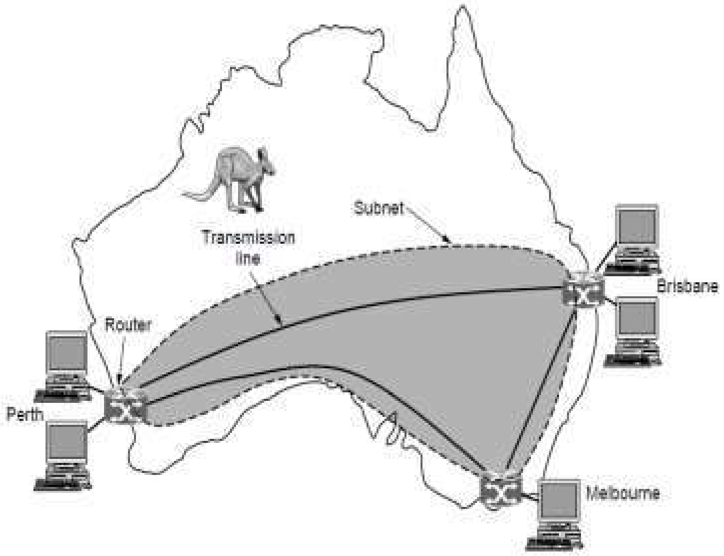


Figure 1.11 WAN that connects three branch offices in Australia.

The rest of the network that connects these hosts is then called the **communication subnet**, or just **subnet** for short. The job of the subnet is to carry messages from host to host, just as the telephone system carries words (really just sounds) from speaker to listener.

In WANs, the subnet consists of two distinct components: **Transmission Lines** and **Switching Elements.**

- **Transmission lines:** Its move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Most companies do not have transmission lines lying about, so instead they lease the lines from a telecommunications company.
- **Switching elements:** It is switching elements or switches, are specialized computers that connect two or more transmission lines. When data arrive on an incoming line, the switching element must choose an outgoing line on which to forward them.
- **Router** These switching computers have been called by various names in the past; the name **router** is now most commonly used.

The WAN as we have described it looks similar to a large wired LAN, but there are some important differences that go beyond long wires. Usually in a WAN, the hosts and subnet are owned and operated by different people.

We are now in a position to look at two other varieties of WANs. First, rather than lease dedicated transmission lines, a company might connect its offices to the Internet This allows connections to be made between the offices as virtual links that use the underlying capacity of the Internet. This arrangement, shown in Fig. 1.12, is called a **VPN** (**Virtual Private Network**).

Compared to the dedicated arrangement, a VPN has the usual advantage of virtualization, which is that it provides flexible reuse of a resource (Internet connectivity). A VPN also has the usual disadvantage of virtualization, which is a lack of control over the underlying resources. With a dedicated line, the capacity is clear. With a VPN your mileage may vary with your Internet service.

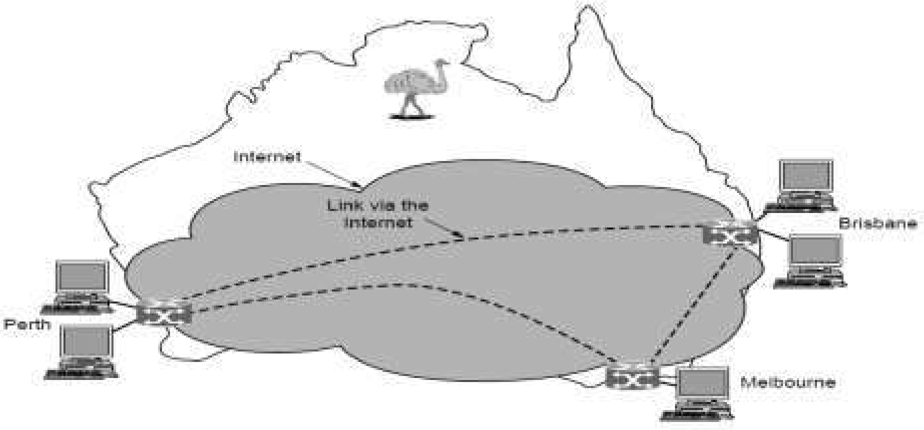


Figure 1.12 WAN using a virtual private network.

The second variation is that the subnet may be run by a different company. The subnet operator is known as a **network service provider** and the offices are its customers. This structure is shown in Fig. 1.13. The subnet operator will connect to other customers too, as long as they can pay and it can provide service.

Since it would be a disappointing network service if the customers could only send packets to each other, the subnet operator will also connect to other networks that are part of the Internet. Such a subnet operator is called an **ISP** (**Internet Service Provider**) and the subnet is an **ISP network**. Its customers who connect to the ISP receive Internet service.

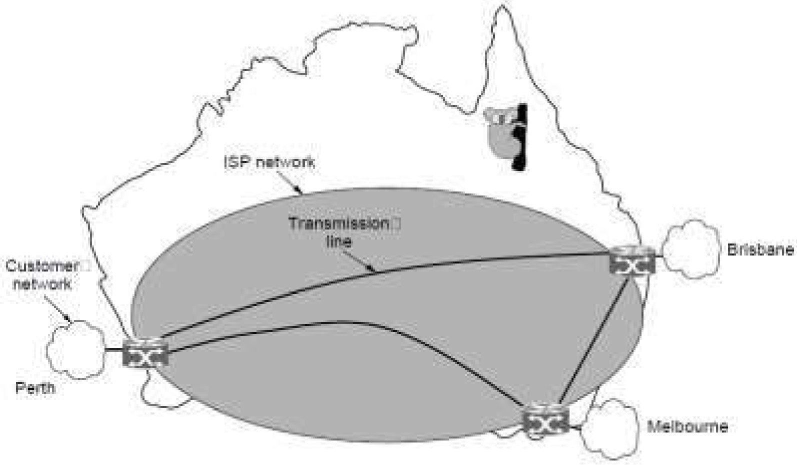


Figure 1.13 WAN using an ISP network.

1.3.6 Internetworks

People connected to one network often want to communicate with people attached to a different one. The fulfillment of this desire requires that different, and frequently incompatible, networks be connected. A collection of interconnected networks is called an **internetwork** or **internet**.

Subnets, networks, and internetworks are often confused. The term ''subnet'' makes the most sense in the context of a wide area network, where it refers to the collection of routers and communication lines owned by the network operator. A network is formed by the combination of a subnet and its hosts. A subnet might be described as a network, as in the case of the ''ISP network'' of Figure 1.12 An internetwork might also be described as a network, as in the case of the WAN in Figure 1.10

- **Gateway:** The general name for a machine that makes a connection between two or more networks and provides the necessary translation, both in terms of hardware and software, is a **gateway**. Gateways are distinguished by the layer at which they operate in the protocol hierarchy.

Since the benefit of forming an internet is to connect computers across networks, we do not want to use too low-level a gateway or we will be unable to make connections between different kinds of networks. We do not want to use too high-level a gateway either, or the connection will only work for particular applications.

The level in the middle that is ''just right'' is often called the network layer, and a router is a gateway that switches packets at the network layer. We can now spot an internet by finding a network that has routers.

1.4 Network Software

computer hardware was the main concern at the starting of computer development. Later the network software is highly required. In the following sections we examine the software structuring technique in some detail.

1.4.1 Protocol Hierarchies

To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.

Layer *n* on one machine carries on a conversation with layer n on another machine. The rules and conventions used in this conversation are collectively known as the layer *n* protocol. A five-layer network is illustrated in Fig. 1-13. The entities comprising the corresponding layers on different machines are called peers. The peers may be processes, hardware devices, or even human beings. In other words, it is the peers that communicate by using the protocol.

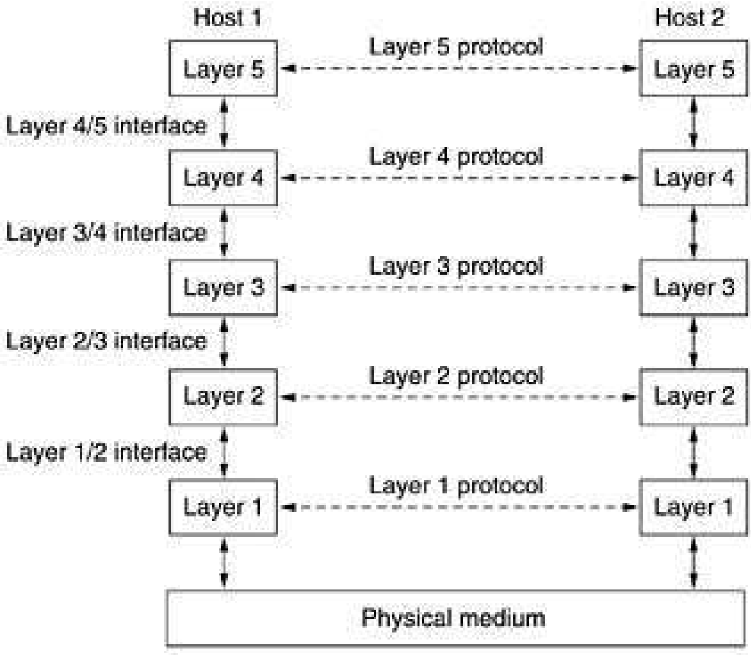


Figure 1-13. Layers, protocols, and interfaces

In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer 1 is the physical medium through which actual communication occurs. In Fig. 1-13, virtual communication is shown by dotted lines and physical communication by solid lines

Between each pair of adjacent layers is an interface. The interface defines which primitive operations and services the lower layer makes available to the upper one. A set of layers and protocols is called a ***network architecture***. List of protocols used by a certain system, one protocol per layer, is called a ***protocol stack***.

Now consider a more technical example: how to provide communication to the top layer of the five-layer network in Fig. 1-14. A message, M, is produced by an application process running in layer 5 and given to layer 4 for transmission. Layer 4 puts a header in front of the message to identify the message and passes the result to layer 3. The header includes control information, such as sequence numbers, to allow layer 4 on the destination machine to deliver messages in the right order if the lower layers do not maintain sequence. In some layers, headers can also contain sizes, times, and other control fields.

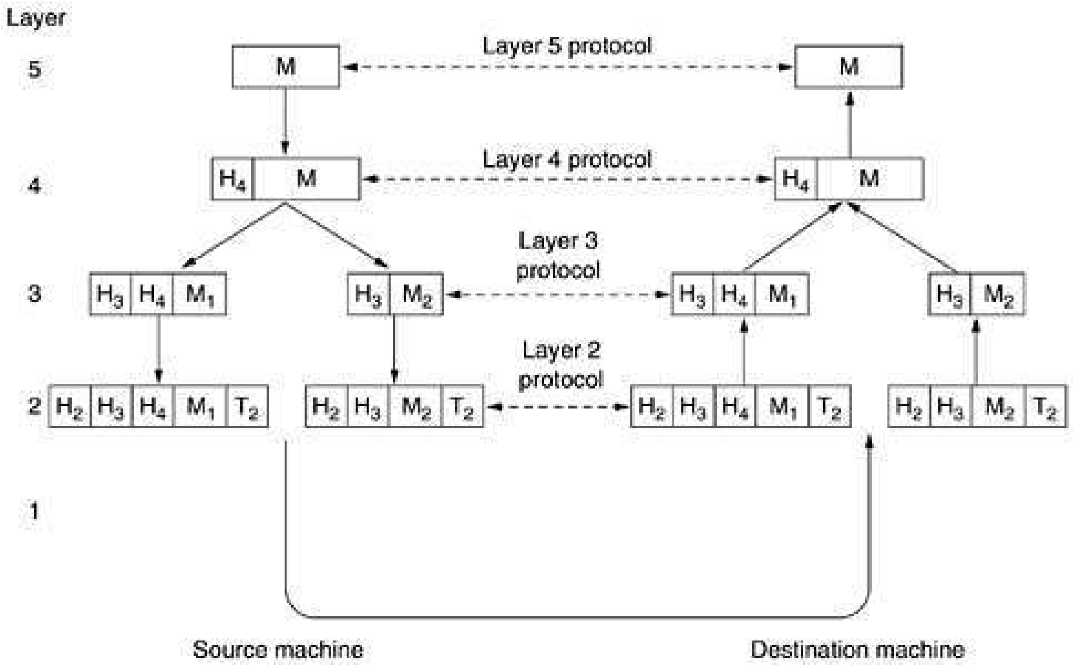


Figure 1-14. Example information flow supporting virtual communication in layer 5.

1.4.2 Design Issues for the Layers

Some of the key design issues that occur in computer networks are present in several layers. The following are briefly mention some of the more important ones.

- ***Identifying senders and receivers*** - some form of addressing is needed in order to specify a specific source and destination.
- ***Rules for data transfer*** - The protocol must also determine the direction of data flow, how many logical channels the connection corresponds to and what their

priorities are. Many networks provide at least two logical channels per connection, one for normal data and one for urgent data.

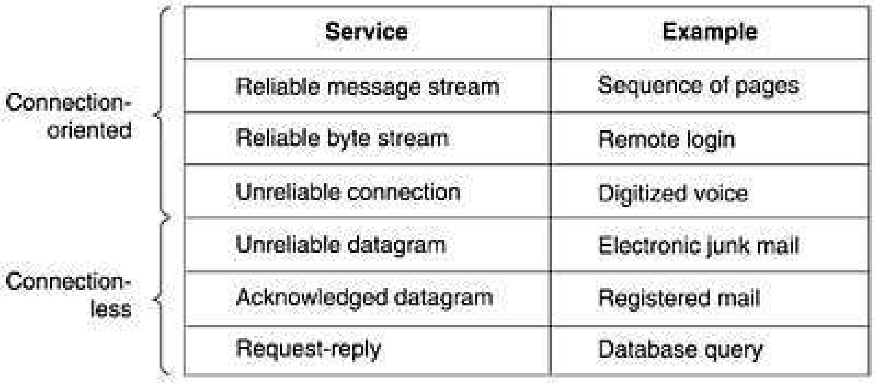
- ***Error control*** – when circuits are not perfect, both ends of the connection must agree on which error-detecting and error-correcting codes is being used.
- ***Sequencing*** - protocol must make explicit provision for the receiver to allow the pieces to be reassembled properly.
- ***Flow Control*** - how to keep a fast sender from swamping a slow receiver with data. This is done by feedback-based (receiver to sender) or agreed-on transmission rate.
- ***Segmentation and reassembly*** - several levels are the inability of all processes to accept arbitrarily long messages. It leads to mechanisms for disassembling, transmitting, and then reassembling messages.
- ***Multiplexing and demultiplexing*** – to share the communication medium by several users.
- ***Routing*** - When there are multiple paths between source and destination, a route must be chosen.

1.4.3 Connection-Oriented and Connectionless Services

Connection-oriented : the service user first establishes a connection, uses the connection, and then releases the connection. During the connection establishment, some negotiation is carried out about parameters to be used, such as maximum message size, quality of service required, and other issues. For example, it is looks like a telephone conversation.

Connectionless : the service user sends data when it is ready without checking anything. Each message carries the full destination address, and each one is routed through the system independent of all the others.

Figure 1-15 summarizes the types of services used for connection-oriented or connectionless services for different purposes.

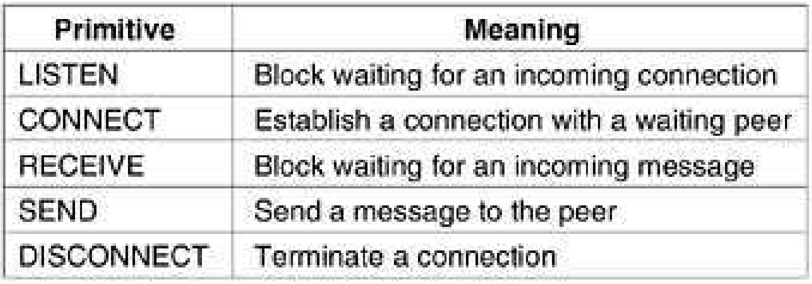


	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Figure 1-15. Six different types of service

1.4.4 Service Primitives

A service is formally specified by a set of primitives (operations) available to a user process to access the service. These primitives tell the service to perform some action or report on an action taken by a peer entity. The set of primitives available depends on the nature of the service being provided. The primitives for connection-oriented service are different from those of connectionless service.



Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

Figure 1-16. Five service primitives for implementing a simple connection-oriented service.

1. The server executes LISTEN to indicate that it is prepared to accept incoming connections.

2. The client process executes CONNECT to establish a connection with the server (1) as in figure 1.17. The client process is suspended until there is a response. When the system sees that the packet is requesting a connection, it checks to see if there is a listener. If so, it does two things: unblocks the listener and sends back an acknowledgement (2). The arrival of this acknowledgement then releases the client.

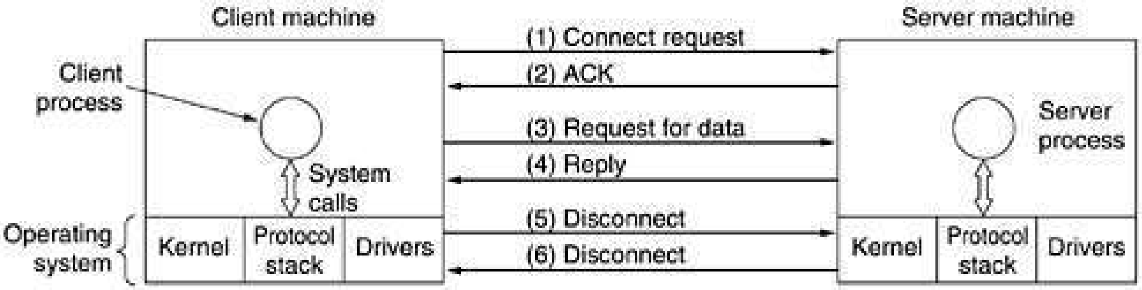


Figure 1-17. Packets sent in a simple client-server interaction on a connection-oriented network

3. The next step is for the server to execute RECEIVE to prepare to accept the first request. The RECEIVE call blocks the server.

4. Then the client executes SEND to transmit its request (3) followed by the execution of RECEIVE to get the reply.

5. The arrival of the request packet at the server machine unblocks the server process so it can process the request. After it has done the work, it uses SEND to return the answer to the client (4). The arrival of this packet unblocks the client, which can now inspect the answer.

6. If the client has additional requests, it can make them now. If it is done, it can use DISCONNECT to terminate the connection. Usually, an initial DISCONNECT is a blocking call, suspending the client and sending a packet to the server saying that the connection is no longer needed (5).

7. When the server's packet (6) gets back to the client machine, the client process is released and the connection is broken.

1.4.5 The Relationship of Services to Protocols

Services and protocols are distinct concepts, although they are frequently confused. This distinction is so important and differentiated as follows;

- ***Service :*** A service is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.

- ***Protocol*** : it is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions.

In other words, services relate to the interfaces between layers, as illustrated in Fig. 1-18. In contrast, protocols relate to the packets sent between peer entities on different machines. It is important not to confuse the two concepts.

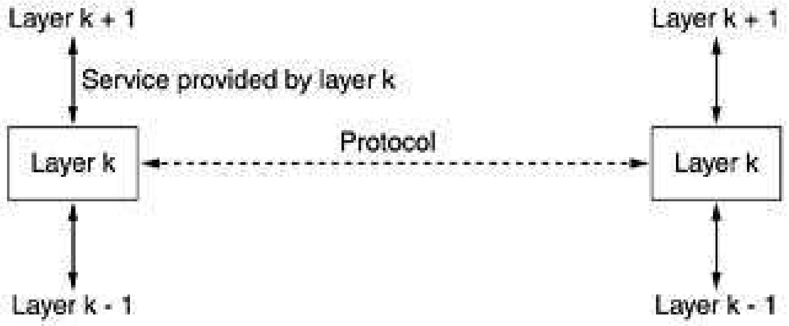


Figure 1-18. The relationship between a service and a protocol

1.5 Network Architecture

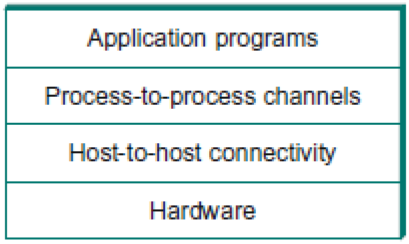
1.5.1 Introduction

One of the requirements for network design is that a computer network must provide general, cost-effective, fair, and robust connectivity among a large number of computers. Though networks do not remain fixed at any single point in time but must evolve to accommodate changes in both the underlying technologies upon which they are based as well as changes in the demands placed on them by application programs. Furthermore, networks must be manageable by humans of varying levels of skill. Designing a network to meet these requirements is not a small task.

To deal with this complexity, network designers have developed general blueprints—usually called ***network*** architectures—that guide the design and implementation of networks.

1.5.2 Layering and Protocols

The idea of an abstraction is to define a model that can capture some important aspect of the system, encapsulate this model in an object that provides an interface that can be manipulated by other components of the system, and hide the details of how the object is implemented from the users of the object. Abstractions naturally lead to layering, especially in network systems. The general idea is that start with the services offered by the underlying hardware and then add a sequence of layers, each providing a higher (more abstract) level of service. For example, a simple network as having two layers of abstraction sandwiched between the application program and the underlying hardware, as illustrated in Figure 1.19.



Application programs

Process-to-process channels

Host-to-host connectivity

Hardware

FIGURE : 1.19 Example of a layered network system.

The layer immediately above the hardware might provide host-to-host connectivity, abstracting away the fact that there may be an arbitrarily complex network topology between any two hosts. The next layer up builds on the available host-to-host communication service and provides support for process-to-process channels, abstracting away the fact that the network occasionally loses messages. Layering provides two features.

- ✓ First, it decomposes the problem of building a network into more manageable components.
- ✓ Second, it provides a more modular design.

1.5.3 Protocols

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities cannot simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

- **Syntax.** The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

- **Semantics.** The word *semantics* refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?
- **Timing.** The term *timing* refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

1.5.4 Protocol Architecture

The two most widely referenced protocol architectures that served as the basis for the development of interoperable communications standards are

[1]. OSI architecture or OSI reference model and
[2]. Internet architecture or TCPIP protocol suite

TCPIP is the most widely used interoperable architecture and OSI has become the standard model for classifying communications functions.

1.5.5 OSI Reference Model

An ISO standard that covers all aspects of network communications is the Open Systems Interconnection model. It was first introduced in the late 1970s. An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.

The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software. The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

ISO is the organization. OSI is the model.

It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network. Figure 1.20 shows the seven layers of OSI

a). Layered Architecture

The OSI model is composed of seven ordered layers:

1. Physical Layer
2. Data link Layer
3. Network layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

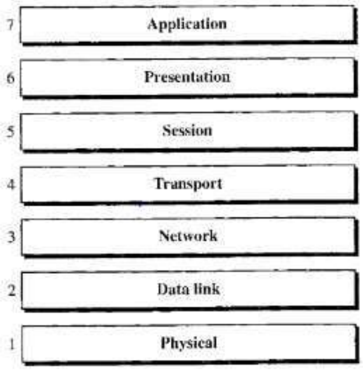


Figure 1.20 Seven layers of the OSI model

Figure 1.21 shows the layers involved when a message is sent from device A to device B. As the message travels from A to B, it may pass through many intermediate nodes. These intermediate nodes usually involve only the first three layers of the OSI model.

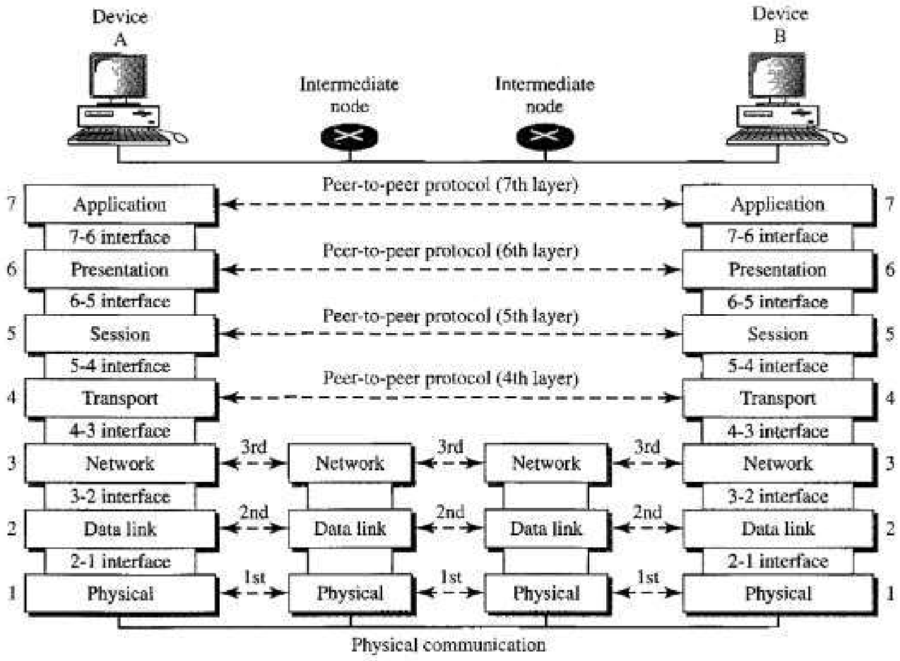


Figure 1.21 The interaction between layers in the OSI model

Within a single machine, each layer calls upon the services of the layer just below it. Layer 3, for example, uses the services provided by layer 2 and provides services for layer 4. Between machines, layer *x* on one machine communicates with layer *x* on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols. The processes on each machine that communicate at a given layer are called peer-to-peer processes. Communication between machines is therefore a peer-to-peer process using the protocols appropriate to a given layer.

b). Peer-to-Peer Processes

At the physical layer, communication is direct. In Figure 1.21, device A sends a stream of bits to device B (through intermediate nodes). At the higher layers, however, communication must move down through the layers on device A, over to device B, and then back up through the layers. Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. At layer 1 the entire package is converted to a form that can be transmitted to the receiving device.

At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it. For example, layer 2 removes the data meant for it, then passes the rest to layer 3. Layer 3 then removes the data meant for it and passes the rest to layer 4, and so on.

c). Interfaces Between Layers

The passing of the data and network information down through the layers of the sending device and back up through the layers of the receiving device is made possible by an interface between each pair of adjacent layers. Each interface defines the information and services a layer must provide for the layer above it.

d). Organization of the Layers

The seven layers can be thought of as belonging to three subgroups. Layers 1, 2, and 3-physical, data link, and network are the **network support layers**, Layers 5, 6, and 7-session, presentation, and application are **the user support layers**. The upper OSI layers are almost always implemented in software; lower layers are a combination of hardware and software, except for the physical layer, which is mostly hardware.

Figure 1.22 gives an overall view of the OSI layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on. The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order. At each layer, a **header,** or possibly a **trailer,** can be added to the data unit. Commonly, the trailer is added only at layer 2. When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link.

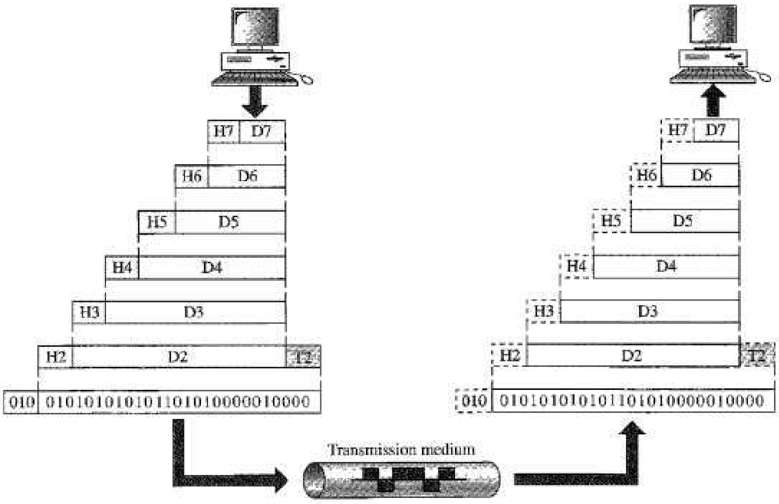


***Figure 1.22** An exchange using the OSI Model*

Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken. By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

e). Encapsulation

Figure 1.22 reveals another aspect of data communications in the OSI model: encapsulation. A packet (header and data) at level 7 is encapsulated in a packet at level 6. The whole packet at level 6 is encapsulated in a packet at level 5, and so on. In other words, the data portion of a packet at level *N* - 1 carries the whole packet (data and header and maybe trailer) from level *N*. The concept is called *encapsulation;* level *N* - 1 is not aware of which part of the encapsulated packet is data and which part is the header or trailer. For level *N* - 1, the whole packet coming from level *N* is treated as one integral unit.

1.5.6 Layers in the OSI model

The functions of each layer in the OSI model are described as follows;

1) Physical Layer

The physical layer coordinates the functions required to carry a bit stream over a physical medium. It deals with the mechanical and electrical specifications of the interface and transmission medium. It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to occur. Figure 1.23 shows the position of the physical layer with respect to the transmission medium and the data link layer.

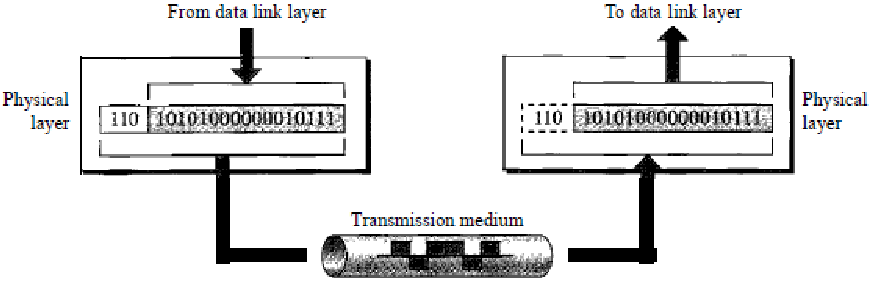


Figure 1.23 Physical layer

The physical layer is responsible for movements of individual bits from one hop (node) to the next.

The physical layer is also concerned with the following:

- **Physical characteristics of interfaces and medium.** The physical layer defines the characteristics of the interface between the devices and the transmission medium. It also defines the type of transmission medium.

- **Representation of bits.** The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals--electrical or optical. The physical layer defines the type of encoding (how 0s and I s are changed to signals).

- **Data rate.** The transmission rate-the number of bits sent each second-is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

- **Synchronization of bits**. The sender and receiver not only must use the same bit rate but also must be synchronized at the bit level. In other words, the sender and the receiver clocks must be synchronized.

- **Line configuration.** The physical layer is concerned with the connection of devices to the media. In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

- **Physical topology.** The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology (every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).

- **Transmission mode.** The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive. The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

2) Data Link Layer

The data link layer transforms the physical layer, a raw transmission facility, to a reliable link. It makes the physical layer appear error-free to the upper layer (network layer). Figure 1.24 shows the relationship of the data link layer to the network and physical layers.

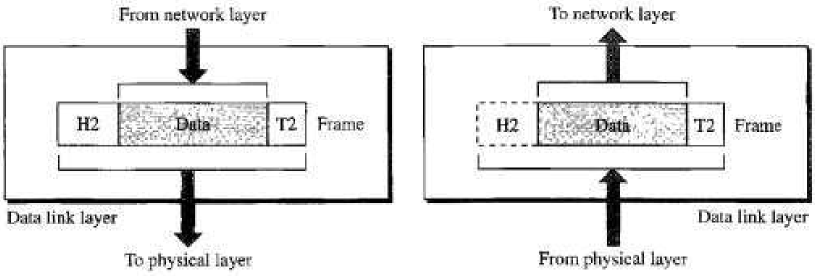


Figure 1.24 Data link layer

The data link layer is responsible for moving frames from one hop (node) to the next.

Other responsibilities of the data link layer include the following:

- **Framing.** The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
- **Physical addressing.** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame. If the frame is intended for a system outside the sender's network, the receiver address is the address of the device that connects the network to the next one.
- **Flow control.** If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.
- **Error control.** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.
- **Access control.** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Figure 1.25 illustrates hop-to-hop (node-to-node) delivery by the data link layer. As the figure 1.25 shows, communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made. First, the data link layer at A sends a frame to the data link layer at B (a router). Second, the data link layer at B sends a new frame to the data link layer at E. Finally, the data link layer at E sends a new frame to the data link layer at F.

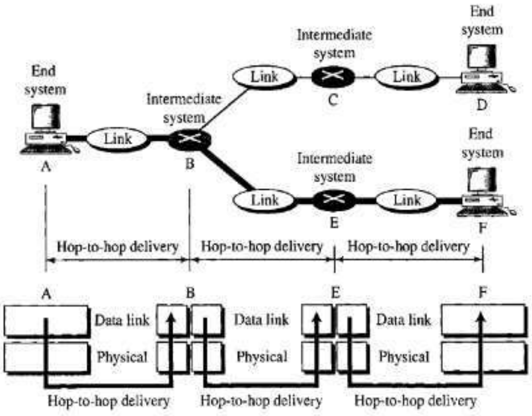


Figure 1.25 Hop-to-hop delivery

Note that the frames that are exchanged between the three nodes have different values in the headers. The frame from A to B has B as the destination address and A as the source address. The frame from B to E has E as the destination address and B as the source address. The frame from E to F has F as the destination address and E as the source address. The values of the trailers can also be different if error checking includes the header of the frame.

3) Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. Figure 1.26 shows the relationship of the network layer to the data link and transport layers.

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Other responsibilities of the network layer include the following:

- **Logical addressing.** The physical addressing implemented by the data link layer handles the addressing problem locally. If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

- **Routing.** When independent networks or links are connected to create *internetworks* (network of networks) or a large network, the connecting devices (called *routers* or *switches)* route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism. Figure 1.27 illustrates end-to-end delivery by the network layer.

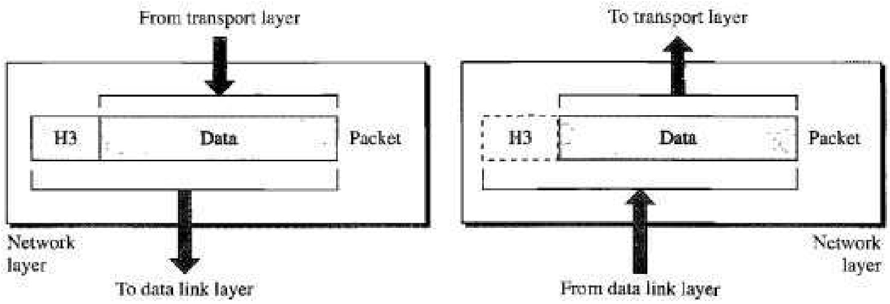


Figure 1.26 Network layer

As the figure 1.27 shows, now we need a source-to-destination delivery. The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet. Router B uses its routing table to find that the next hop is router E. The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in tum, sends the packet to the network layer at F.

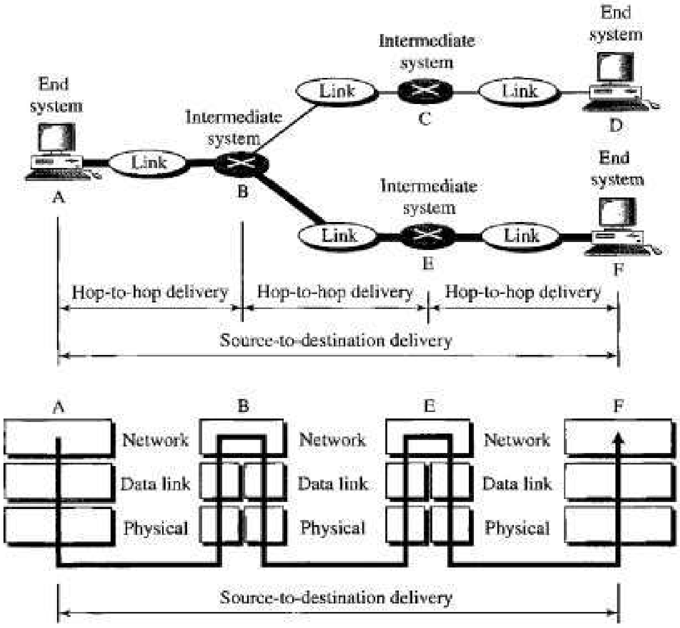


Figure 1.27 Source-to-destination delivery

4) Transport Layer

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level. Figure 1.28 shows the relationship of the transport layer to the network and session layers.

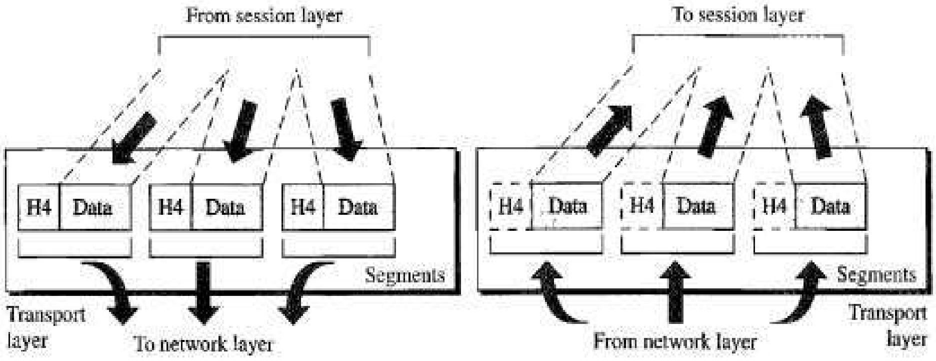


Figure 1.28 Transport layer

The transport layer is responsible for the delivery of a message from one process to another.

Other responsibilities of the transport layer include the following:

- **Service-point addressing.** Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a *service-point address* (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

- **Segmentation and reassembly.** A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

- **Connection control.** The transport layer can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

- **Flow control.** Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

- **Error control.** Like the data link layer, the transport layer is responsible for error control. However, **error** control at this layer is performed process-to-process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission. Figure 1.29 illustrates process-to-process delivery by the transport layer.

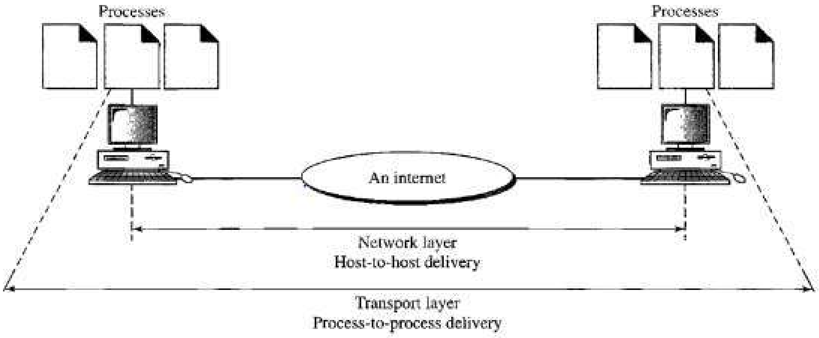


Figure 1.29 Reliable process-to-process delivery of a message

5) Session Layer

The services provided by the first three layers (physical, data link, and network) are not sufficient for some processes. The session layer is the network *dialog controller.* It establishes, maintains, and synchronizes the interaction among communicating systems.

The session layer is responsible for dialog control and synchronization.

Specific responsibilities of the session layer include the following:

- **Dialog control.** The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization.** The session layer allows a process to add checkpoints, or synchronization points, to a stream of data. For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent. Figure 1.30 illustrates the relationship of the session layer to the transport and presentation layers.

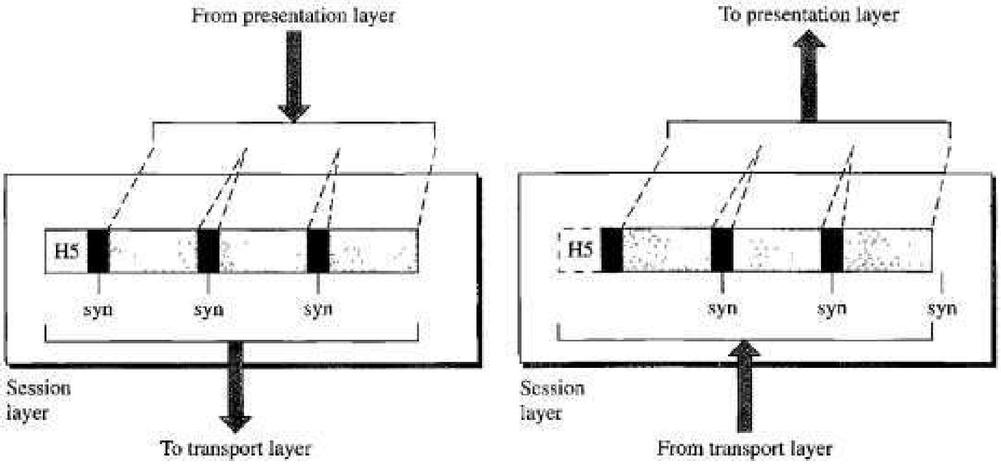


Figure 1.30 Session layer

6) Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information exchanged between two systems. Figure 1.31 shows the relationship between the presentation layer and the application and session layers.

The presentation layer is responsible for translation, compression, and encryption.

Specific responsibilities of the presentation layer include the following:

- **Translation.** The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods. The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

- **Encryption.** To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

- **Compression.** Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

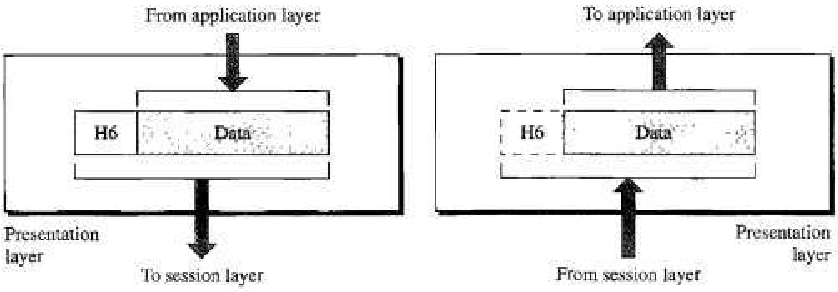


Figure 1.31 Presentation layer

7) Application Layer

The application layer enables the user, whether human or software, to access the network. It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

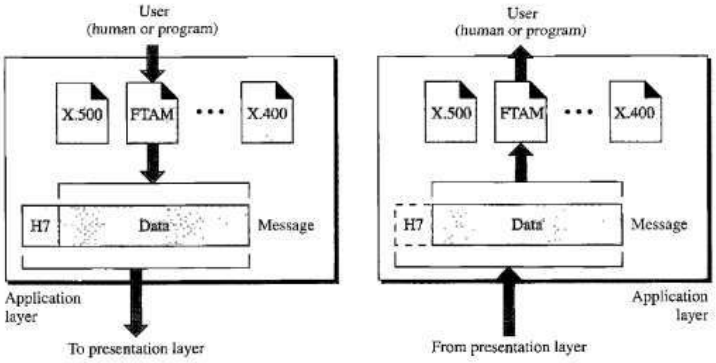


Figure 1.32 Application layer

Figure 1.32 shows the relationship of the application layer to the user and the presentation layer. Of the many application services available, the figure shows only three: *XAOO* (message-handling services), X.500 (directory services), and file transfer, access, and management (FTAM). The user in this example employs *XAOO* to send an e-mail message.

The application layer is responsible for providing services to the user.

Specific services provided by the application layer include the following:

- **Network virtual terminal.** A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
- **File transfer, access, and management.** This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- **Mail services.** This application provides the basis for e-mail forwarding and storage.
- **Directory services.** This application provides distributed database sources and access for global information about various objects and services.

1.5.7 Summary of OSI Layers

Figure 1.33 shows a summary of duties for each layer.

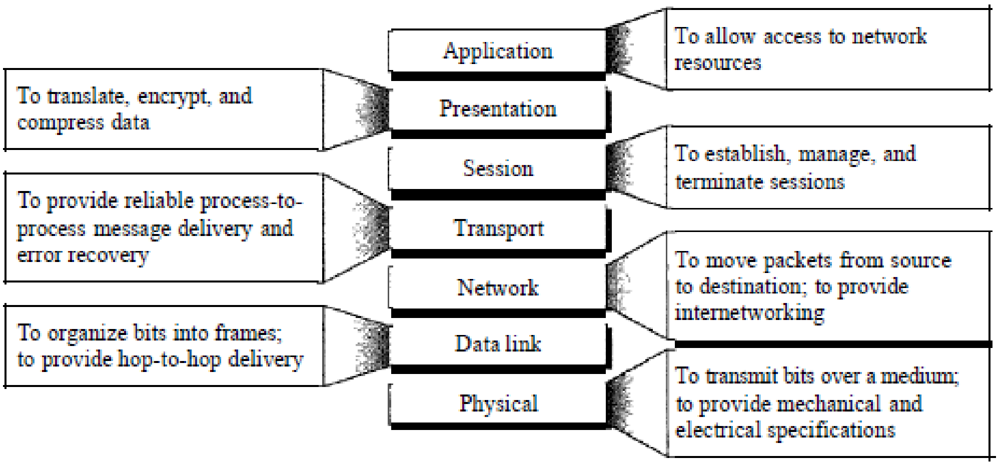

Application
To allow access to network resources
To translate, encrypt, and compress data
Presentation
Session
To establish, manage, and terminate sessions
To provide reliable process-to-process message delivery and error recovery
Transport
Network
To move packets from source to destination; to provide internetworking
To organize bits into frames; to provide hop-to-hop delivery
Data link
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

Figure 1.33 Summary of layers

1.5.8 TCP/IP Protocol Architecture

TCPIP is a result of protocol research and development conducted on the experimental packet-switched network, ARPANET, funded by the Defence Advanced Research Projects

Agency (DARPA), and is generally referred to as the TCPIP protocol suite. This protocol suite consists of a large collection of protocols that have been issued as Internet standards by the Internet Architecture Board (IAB). The communication task for TCPIP is organized into five relatively independent layers:

1. Physical layer
2. Network access layer
3. Internet layer
4. Host-to-host or transport layer
5. Application layer

1) Physical layer

The **physical layer** covers the physical interface between a data transmission device (e.g., workstation, computer) and a transmission medium or network.

This layer is concerned with specifying the characteristics of the transmission medium, the nature of the signals, the data rate, and related matters.

2) Network access layer

The **network access layer** is concerned with the exchange of data between an end system and the network to which it is attached. The sending computer must provide the network with the address of the destination computer, so that the network may route the data to the appropriate destination. The specific software used at this layer depends on the type of network to be used; different standards have been developed for circuit-switching, packet-switching (e.g., X.25), local area networks (e.g., Ethernet), and others. Thus, it makes sense to separate those functions having to do with network access into a separate layer. By doing this, the communications software, above the network access layer, need not be concerned about the specifics of the network to be used. The same higher-layer software should function properly regardless of the particular network to which the computer is attached.

The network access layer is concerned with access to and routing data across a network for two end systems attached to the same network.

3) Internet layer

In cases where two devices are attached to different networks, procedures are needed to allow data to traverse multiple interconnected networks. This is the function of the **internet layer.** The internet protocol (IP) is used at this layer to provide the routing function across multiple networks. This protocol is implemented not only in the end systems but also in routers. A router is a processor that connects two networks and whose primary function is to relay data from one network to the other on its route from the source to the destination end system.

The internet layer concerns with the routing functions across multiple networks.

4) Host-to-host layer or transport layer

Regardless of the nature of the applications that are exchanging data, there is usually a requirement that data be exchanged reliably. That is, we would like to be assured that all of the data arrive at the destination application and that the data arrive in the same order in which they were sent. The mechanisms for providing reliability are essentially independent of the nature of the applications. Thus, it makes sense to collect those mechanisms in a common layer shared by all applications; this is referred to as the **host-to-host layer** or **transport layer.** The transmission control protocol (TCP) is the most commonly-used protocol to provide this functionality.

5) Application layer

Finally, the **application layer** contains the logic needed to support the various user applications. For each different type of application, such as file transfer, a separate module is needed that is peculiar to that application.

Figure 1.34 shows how the TCPIP protocols are implemented in end systems

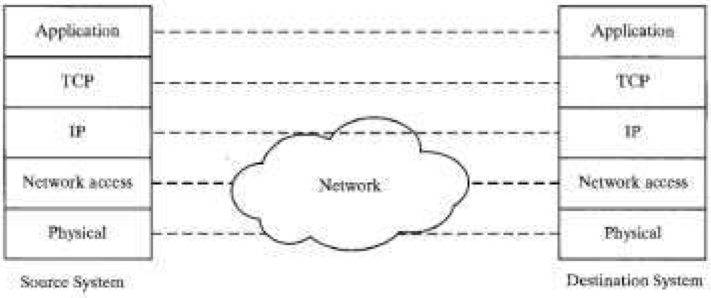


*FIGURE **1.34 TCPIP** Protocol architecture model.*

From the figure 1.34 it is observed that the physical and network access layers provide interaction between the end system and the network, whereas the transport and application layers are what is known as end-to-end protocols; they support interaction between two end systems. The internet layer has the flavor of both. At this layer, the end system communicates routing information to the network but also must provide some common functions between the two end systems.

1.6 Physical Layer

Information can be transmitted on wires by varying some physical property such as voltage or current. By representing the value of this voltage or current as a single-valued function of time, f(t), we can model the behavior of the signal and analyze it mathematically.

1.6.1 Fourier Analysis

In the early 19th century, the French mathematician Jean-Baptiste Fourier proved that any reasonably behaved periodic function, g(t) with period T can be constructed as the sum of a (possibly infinite) number of sines and cosines:

$$g(t) = \frac{1}{2}c + \sum_{n=1}^{\infty} a_n \sin(2\pi nft) + \sum_{n=1}^{\infty} \cos(2\pi nft) \qquad - \qquad (2.1)$$

where $f = 1/T$ is the fundamental frequency, a_n and b_n are the sine and cosine amplitudes of the nth harmonics (terms), and c is a constant. Such a decomposition is called a Fourier series. From the Fourier series, the function can be reconstructed; that is, if the period, T, is known and the amplitudes are given, the original function of time can be found by performing the sums of Eq. (2-1).

A data signal that has a finite duration (which all of them do) can be handled by just imagining that it repeats the entire pattern over and over forever (i.e., the interval from T to 2T is the same as from 0 to T, etc.).

1.6.2 Signals

Signal is a physical representation of data by means of analog or digital. To be transmitted, data must be transformed to electromagnetic signals. Analog data are continuous and take continuous values. Digital data have discrete states and take discrete values. Analog signals can have an infinite number of values m a range; digital signals can have only a limited number of values.

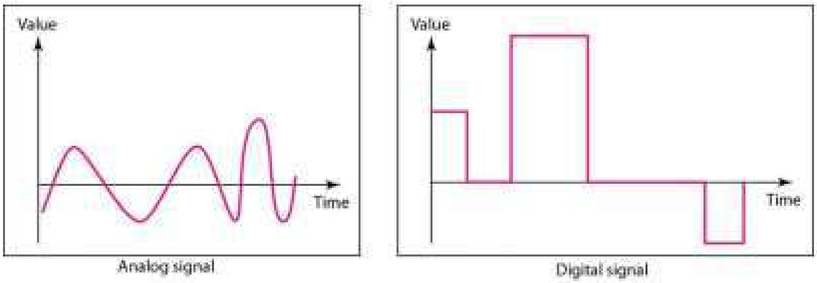


Fig. 1.35. Analog and Digital Signal

For example, an analog clock that has hour, minute, and second hands gives information in a continuous form; the movements of the hands are continuous. On the other hand, a digital clock that reports the hours and the minutes will change suddenly from 8:05 to 8:06.

a) Periodic and Nonperiodic Signals

Both analog and digital signals can take one of two forms: periodic or nonperiodic (sometimes refer to as aperiodic, because the prefix a in Greek means "non").

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time.

In data communications, we commonly use periodic analog signals (because they need less bandwidth), and nonperiodic digital signals (because they can represent variation in data).

Periodic analog signals can be classified as simple or composite. A simple periodic analog signal, a sine wave, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves. A sine wave can be represented by three parameters: the peak amplitude, the frequency, and the phase. These three parameters fully describe a sine wave.

- **Period and Frequency**

Period refers to the amount of time (*T*), in seconds, a signal needs to complete 1 cycle. Frequency (*f*) refers to the number of periods in 1s. Period is the inverse of frequency, and frequency is the inverse of period, as the following formulas show.

$$f = \frac{1}{T} \; and \; T = \frac{1}{f}$$

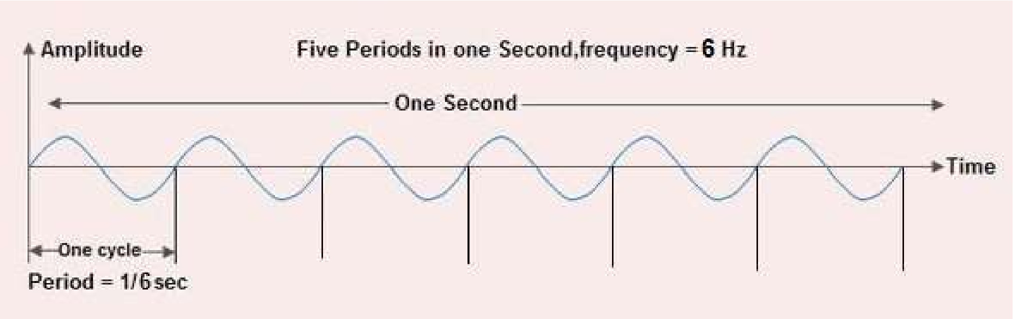


Fig. 1.36. A signal with its frequency

For example, the figure 1.36 shows a signal with frequency of 6Hz. Since, it has 6 cycles in a second.

Period is formally expressed in seconds. Frequency is formally expressed in ***Hertz*** (Hz), which is ***cycle per second***. The hertz is named after the German physicist ***Heinrich Hertz*** (1857–1894), who made important scientific contributions to the study of electromagnetism. The name was established by the International Electrotechnical Commission (IEC) in **1930**. It was adopted by the General Conference on Weights and Measures (CGPM) (Conférence générale des poids et mesures) in ***1960***. The term *cycle per second was* largely replaced by hertz by the 1970s.Units of period and frequency are shown in Table 2.1.

Unit of period	Equivalent	Unit of frequency	Equivalent
Seconds (s)	1s	Hertz (Hz)	1 Hz
Milliseconds (ms)	10^{-3}s	Kilohertz (khz)	10^{3} Hz
Microseconds (μs)	10^{-6}s	Megahertz (Mhz)	10^{6} Hz
Nanoseconds (ns)	10^{-9}s	Gigahertz (Ghz)	10^{9} Hz
Picoseconds (ps)	10^{-12}s	Terahertz (Thz)	10^{12} Hz

Table 1.4. Units of period and frequency

Frequency is the rate of change with respect to time. Change in a short span of time means high frequency. Change over a long span of time means low frequency.

- ✓ **Example 1.1**

The power we use at home has a frequency of 60Hz (50Hz in Europe). The period of this sine wave can be determined as follows:

$$T = \frac{1}{f} = \frac{1}{60} s = 0.0166\ s = 0.0166\ x\ 10^3\ ms = 16.6\ ms$$

This means that the period of the power for our lights at home is 0.0116 s, or 16.6 ms. Our eyes are not sensitive enough to distinguish these rapid changes in amplitude.

- ✓ **Example 1.2**

The period of a signal is 100 ms. What is its frequency in kilohertz?

Solution

First we change 100ms to seconds, and then we calculate the frequency from the period (1 Hz =10^{-3}kHz).

$$T = 100ms = 100\ x\ 10^{-3}s\ =\ 10^{-1}s$$

$$f = \frac{1}{T} = \frac{1}{10^{-1}} Hz = 10Hz = 10\ x\ 10^{-3} Khz = 10^{-2}\ kHz = 0.01\ kHz$$

Frequency is the rate of change with respect to time. Change in a short span of time means high frequency. Change over a long span of time means low frequency. If a signal does not change at all, it never completes a cycle, so its frequency is 0 Hz. when a signal changes instantaneously, its period is zero; since frequency is the inverse of period, in this case, the frequency is 110, or infinite (unbounded).

- **Wavelength**

Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal. It is normally considered as the ***length of one complete cycle of a signal***. However, since period and frequency are related to each other, if we represent wavelength by 'λ', propagation speed by 'c' (speed of light), and frequency by 'f', we get

$$\lambda = \frac{c}{f} \quad , where\ c = 3\ x\ 10^8 m/s$$

The wavelength is normally measured in micrometers (microns) instead of meters. For example, the wavelength of red light (frequency= 4 x 10^{14} Hz) in air is

$$\lambda = \frac{c}{f} = \frac{3\ x\ 10^8}{4\ x\ 10^{14}} = \frac{3}{4\ x\ 10^6} = 0.75\ x\ 10^{-6}\ m = 0.75\ \mu m$$

b) Composite signals

A single-frequency sine wave is not useful in data communications; we need to send a composite signal, a signal made of many simple sine waves. Any composite signal is a combination of simple sine waves with different frequencies, amplitudes, and phases. If the composite signal is periodic, the decomposition gives a series of signals with discrete frequencies; if the composite signal is nonperiodic, the decomposition gives a combination of sine waves with continuous frequencies. FM and AM radio signals are nonperiodic composite signals.

- **Bandwidth**

The range of frequencies contained in a composite signal is its bandwidth. *The bandwidth (B) of a composite signal is defined as the difference between the highest (f_H) and the lowest (f_L) frequencies contained in that signal*. Hence, the bandwidth (B) is calculates as

$$B = f_H - f_L$$

The figure 1.37 shows the representation of bandwidth.

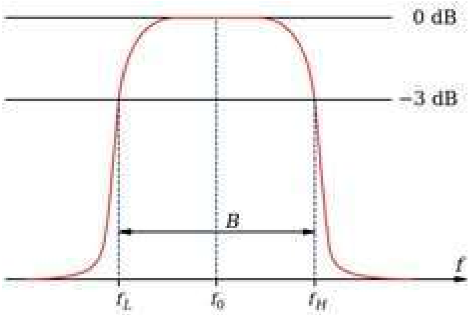


Fig. 1.37. Bandwidth representation

For example, if a composite signal contains frequencies between 1000 Hz and 5000 Hz, its bandwidth is 5000 Hz- 1000 Hz, or 4000 Hz.

✓ **Example 1.3**

If a periodic signal is decomposed into five sine waves with frequencies of 100, 300, 500, 700, and 900 Hz, what is its bandwidth?

Solution

$$Highest\ frequency\ (f_H) = 900\ Hz$$

$$Lowest\ frequency\ (f_L) = 100\ Hz$$

$$So, Bandwidth\ (B) = f_H - f_L = 900 - 100 = 800Hz$$

✓ **Example 1.4**

A periodic signal has a bandwidth of 40 kHz. The lowest frequency is 790 kHz. What is the highest frequency?

Solution

$$Bandwidth\ (B) = 40\ kHz$$

$$Lowest\ frequency\ (f_L) = 790\ kHz$$

$$Highest\ frequency\ (f_H) = B + f_L = 40 - 790 = 830\ kHz$$

✓ **Example 1.5**

A nonperiodic composite signal has a bandwidth of 200 kHz, with a middle frequency of 140 kHz. Find the frequency spectrum of the bandwidth?

$$Bandwidth\ (B) = \ 200\ kHz$$

$$Middle\ frequency\ \ = 140\ kHz$$

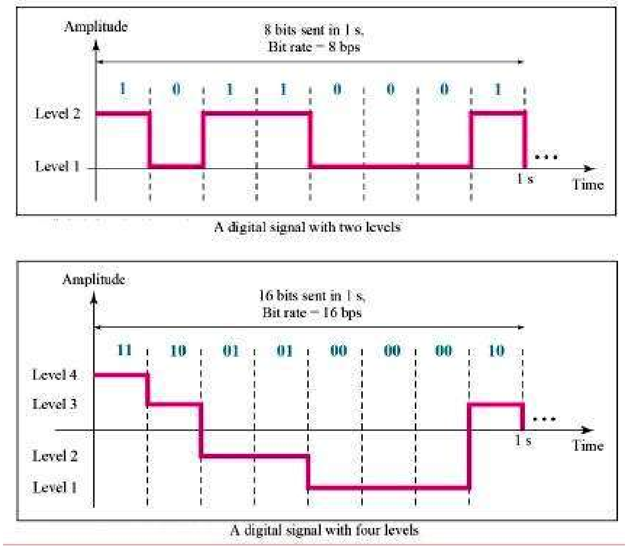
$$Highest\ frequency\ (f_H) = 140 + \frac{200}{2} = 140 + 100 = 240\ kHz$$

$$Lowest\ frequency\ (f_L) = 140 - \frac{200}{2} = 140 - 100 = 40\ kHz$$

1.6.3 Data transfer Rate

a) Bit Rate

Most digital signals are nonperiodic, and thus period and frequency are not appropriate characteristics. Another term-***bit rate*** (instead of frequency)-is used to describe digital signals. ***The bit rate is the number of bits sent in 1s, expressed in bits per second (bps).*** Figure 1.38 shows the bit rate for two signals.



A digital signal with two levels

A digital signal with four levels

Fig. 1.38. Bit rate of two signals

✓ Example 1.6

Assume we need to download text documents at the rate of 100 pages per minute. What is the required bit rate of the channel?

Solution

A page is an average of 24 lines with 80 characters in each line. If we assume that one character requires 8 bits, the bit rate is

100 X 24 X 80 X 8 = 1,636,000 bps = 1.636 Mbps

✓ Example 1.7

A digitized voice channel is made by digitizing a 4-kHz bandwidth analog voice signal. We need to sample the signal at twice the highest frequency (two samples per hertz). We assume that each sample requires 8 bits. What is the required bit rate?

Solution

The bit rate can be calculated as 2 x 4000 Hz x 8 = 64,000 bps = 64 kbps

b) Bit Length

The bit length is the distance one bit occupies on the transmission medium.

Bit length = propagation speed X bit duration

In baseband transmission, the required bandwidth is proportional to the bit rate; if we need to send bits faster, we need more bandwidth. If the available channel is a band pass channel (a channel with a bandwidth that does not start from zero), we cannot send the digital signal directly to the channel; we need to convert the digital signal to an analog signal before transmission.

c) Data Rate Limits

A very important consideration in data communications is how fast we can send data, in bits per second, over a channel. Data rate depends on three factors:

1. The bandwidth available
2. The level of the signals we use
3. The quality of the channel (the level of noise)

Two theoretical formulas were developed to calculate the data rate: one by Nyquist for a noiseless channel, another by Shannon for a noisy channel.

- **Noiseless Channel: Nyquist Bit Rate**

For a noiseless channel, the Nyquist bit rate formula defines the theoretical maximum bit rate

$$\textbf{\textit{BitRate = 2 x bandwidth x log}}_{\textbf{\textit{2}}} \textbf{\textit{ L}}$$

In this formula, bandwidth is the bandwidth of the channel, L is the number of signal levels used to represent data, and ***BitRate*** is the bit rate in bits per second. Practically there is a limit on the signal levels. Increasing the levels of a signal may reduce the reliability of the system.

✓ **Example 1.8**

Consider a noiseless channel with a bandwidth of 3000 Hz transmitting a signal with two signal levels. The maximum bit rate can be calculated as

$$\text{BitRate} = 2 \text{ x } 3000 \text{ x } \log_2 2 = 6000 \text{ bps} = 6\text{kbps}$$

✓ **Example 1.9**

Consider the same noiseless channel transmitting a signal with four signal levels (for each level, we send 2 bits). The maximum bit rate can be calculated as

$$\text{BitRate} = 2 \text{ x } 3000 \text{ x } \log_2 4 = 12000 \text{ bps} = 12 \text{ kbps}$$

✓ **Example 1.10**

We need to send 265 kbps over a noiseless channel with a bandwidth of 20 kHz. How many signal levels do we need?

Solution

We can use the Nyquist formula as shown·

$$265,000 = 2 \text{ X } 20,000 \text{ X } \log2 \text{ L}$$

$$\log2 \text{ L} = 6.625 \text{ L} = 2^{6.625} = 98.7 \text{ levels}$$

Since this result is not a power of 2, we need to either increase the number of levels or reduce the bit rate. If we have 128 levels, the bit rate is 280 kbps. If we have 64 levels, the bit rate is 240 kbps.

- **Noisy Channel: Shannon Capacity**

In reality, we cannot have a noiseless channel; the channel is always noisy. In 1944, Claude Shannon introduced a formula, called the Shannon capacity, to determine the theoretical highest data rate for a noisy channel:

Capacity= bandwidth x log2 (1 + SNR)

In this formula, bandwidth is the bandwidth of the channel, SNR is the signal-to-noise ratio, and capacity is the capacity of the channel in bits per second. Note that in the Shannon formula, there is no indication of the signal level

✓ **Example 1.11**

We can calculate the theoretical highest bit rate of a regular telephone line. A telephone line normally has a bandwidth of 3000Hz (300 to 3300 Hz) assigned for data communications. The signal-to-noise ratio is usually 3162. For this channel the capacity is calculated as

$$C = B \log_2(1 + SNR) = 3000 \log_2(1 + 3162) = 3000 \log_2 3163$$

$$= 3000 \text{ x } 11.62 = 34,860 \text{ bps}$$

This means that the highest bit rate for a telephone line is 34.860 kbps. If we want to send data faster than this, we can either increase the bandwidth of the line or improve the signal-to-noiseratio.

✓ **Example 1.12**

The signal-to-noise ratio is often given in decibels. Assume that SNR_{dB} = 36 and the channel bandwidth is 2 MHz. The theoretical channel capacity can be calculated as

$$SNR_{dB} = 10 \text{ logw}_{10} \text{ SNR} \rightarrow SNR = 10^{SNR_{dB/10}} \rightarrow SNR = 10^{3 \cdot 6} = 3981$$

$$C = B \log2 (1+ SNR) = 2 \text{ X } 10^6 \text{ X } \log_2 3982 = 24 \text{ Mbps}$$

✓ **Example 1.13**

For practical purposes, when the SNR is very high, we can assume that SNR + I is almost the same as SNR. In these cases, the theoretical channel capacity can be simplified to

$$C = B \times \frac{SNR_{dB}}{3}$$

For example, we can calculate the theoretical capacity of the previous example as

$$C = 2\ MHz \times \frac{36}{3} = 24\ Mbps$$

d) Throughput/data transfer rate

In computer network, throughput is defined ***as the actual number of bits that flows through a network connection in a given period of time***. Throughput is always ***less than or equal to bandwidth*** but can never exceed bandwidth. In a computer network, the throughput can be affected by many factors as listed below:

- Network congestion due to heavy network usage.
- Too many users are accessing the same server.
- Low bandwidth allocation between network devices.
- Medium loss of a computer network.
- Resources (CPU, RAM) of network devices.

So even if you have a high bandwidth to your ISP, it may not guarantee that you will have a high throughput due to the above factors. The figure 1.39 shows the difference between bandwidth and throughput.

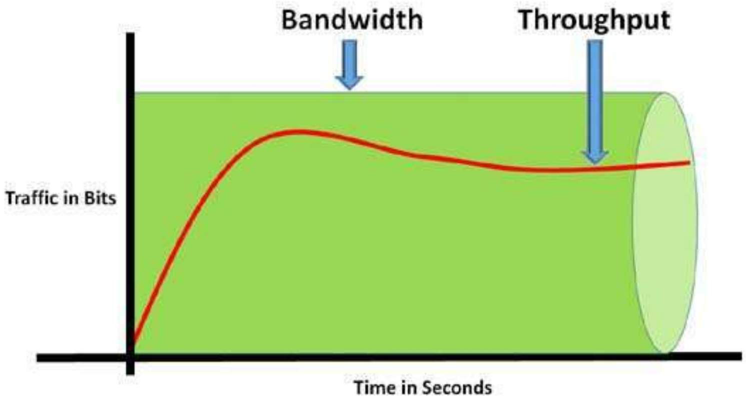


Fig 1.39 Relationship between bandwidth and throughput

The throughput is always measured in bits/s (bps). The data transfer rate (DTR) is measured as follows when the above said factors are not affected the data transmission.

$$DTR = \frac{Actual\ data\ transfered\ ib\ bits}{Time\ taken\ in\ seconds}$$

✓ **Example 1.14**

A file size of 2MB is transferred in 4 minutes over a 100 kbps bandwidth communication link. What is the data transfer rate?

Convert 2MB in bits - 2*8 Mb = 16 Mb

Convert the 16 Mb into Kb - $16 * 10^3$ kb

Convert the 4 minutes into seconds - 4*60 = 240 seconds

$$DTR = \frac{16 \times 1000\, kb}{240\, s} = \frac{400}{6} = 66.67\, kbps$$

But, when we are talking about the file transfer, it is measured in Bytes/s (Bps). Hence the file download calculation for 512 kbps connectivity may be calculated as

Download KBps speed= ((512*1000)/8)/24 = 62.5 KBps

1.7 Guided Transmission Media

Transmission media is nothing but the physical layer or medium. The physical layer is to transport bits from one machine to another. Various physical media can be used for the actual transmission. Media are roughly grouped into TWO types.

- ✓ Guided media, such as copper wire and fiber optics
- ✓ Unguided media, such as terrestrial wireless, satellite, and lasers through the air.

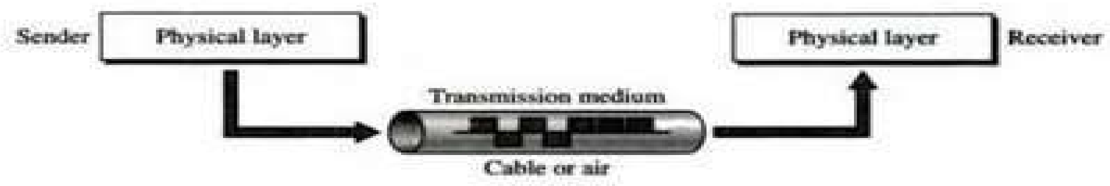


Figure 1.40 Communication

1.7.1 Guided Media

There are five types in guided media

1) Magnetic Media
2) Twisted Pairs
3) Coaxial Cable
4) Power Lines
5) Fiber Optics

1. Magnetic Media:

The most common ways to transport data from one computer to another is to write them onto magnetic tape or removable media. Physically transport the tape or disks to the destination machine, and read them back in again. A simple calculation will make this point clear.

An industry-standard Ultrium tape can hold 800 gigabytes. A box 60 × 60 × 60 cm can hold about 1000 of these tapes, for a total capacity of 800 terabytes, or 6400 terabits (6.4 petabits). A box of tapes can be delivered anywhere in the United States in 24 hours by Federal Express and other companies.

It is more cost effective, especially for applications in which high bandwidth or cost per bit transported. It has delay characteristics are poor.

2. Twisted Pairs

Its uses metallic (Copper) conductors that accept and transport signals in the form of electric current.

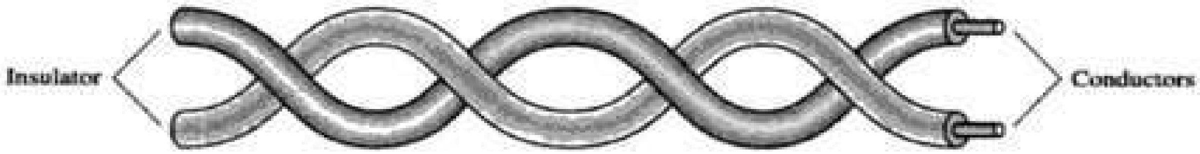


Figure 1.41 Twisted pair cable

A twisted pair consists of two insulated copper wires, typically about 1 mm thick. The wires are twisted together in a helical form. A twisted pair consists of two conductors(normally copper), each with its own plastic insulation, twisted together. One of these wires is used to carry signals to the receiver, and the other is used only as ground reference.

The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference(noise) and crosstalk may affect both wires and create unwanted signals.

If the two wires are parallel, the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the noise or crosstalk sources. This results in a difference at the receiver. Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

a). Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its own colour plastic insulator. Identification is the reason behind coloured plastic insulation. UTP cables consist of 2 or 4 pairs of twisted cable.

- **Advantages of Unshielded Twisted Pair Cable**
  - ✓ Installation is easy
  - ✓ Flexible
  - ✓ Cheap
  - ✓ It has high speed capacity,
  - ✓ 100 meter limit
  - ✓ Higher grades of UTP are used in LAN technologies like Ethernet.
- **Disadvantages of Unshielded Twisted Pair Cable**
  - ✓ Bandwidth is low when compared with Coaxial Cable
  - ✓ Provides less protection from interference.

b). Shielded Twisted Pair Cable

This cable has a metal foil or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by metal casing. Shielding also eliminates crosstalk

- **Advantages of Shielded Twisted Pair Cable**
    - ✓ Easy to install
    - ✓ Performance is adequate
    - ✓ Can be used for Analog or Digital transmission
    - ✓ Increases the signalling rate
    - ✓ Higher capacity than unshielded twisted pair
    - ✓ Eliminates crosstalk
- **Disadvantages of Shielded Twisted Pair Cable**
    - ✓ Difficult to manufacture
    - ✓ Heavy
- **Applications of Shielded Twisted Pair Cable**

In telephone lines to provide voice and data channels. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.

Local Area Network, such as 10Base-T and 100Base-T, also use twisted-pair cables.

3. Coaxial Cable:

Another common transmission medium is the **coaxial cable.** Two kinds of coaxial cable are widely used. One kind, 50-ohm cable, is commonly used when it is intended for digital transmission from the start. The other kind, 75-ohm cable, is commonly used for analog transmission and cable television.

A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. The insulator is encased by a cylindrical conductor, often as a closely woven braided mesh. The outer conductor is covered in a protective plastic sheath.

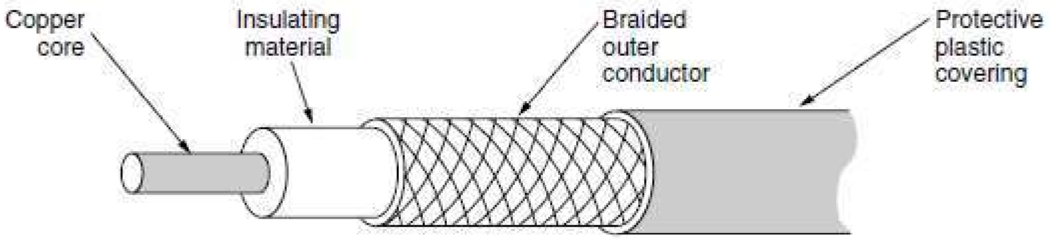


Figure 1.42 coaxial cable

The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity.

- **Advantages of Coaxial Cable**
    - ✓ Bandwidth is high
    - ✓ Used in long distance telephone lines.
    - ✓ Transmits digital signals at a very high rate of 10Mbps.
    - ✓ Much higher noise immunity

- ✓ Data transmission without distortion.
- ✓ The can span to longer distance at higher speeds as they have better shielding when compared to twisted pair cable

- **Disadvantages of Coaxial Cable**
  - ✓ Single cable failure can fail the entire network.
  - ✓ Difficult to install and expensive when compared with twisted pair.
  - ✓ If the shield is imperfect, it can lead to grounded loop.
- **Applications of Coaxial Cable**
  - ✓ Coaxial cable was widely used in analog telephone networks, where a single coaxial network could carry 10,000 voice signals.
  - ✓ Cable TV networks also use coaxial cables. In the traditional cable TV network, the entire network used coaxial cable. Cable TV uses RG-59 coaxial cable.
  - ✓ In traditional Ethernet LANs used it.

4. Power Lines

The telephone and cable television networks are not the only sources of wiring that can be reused for data communication. There is a yet more common kind of wiring: electrical power lines. Power lines deliver electrical power to houses and electrical wiring within houses distributes the power to electrical outlets.

The use of power lines for data communication is an old idea. Power lines have been used by electricity companies for low-rate communication such as remote metering for many years, as well in the home to control devices. Simply plug a TV and a receiver into the wall, which you must do anyway because they need power, and they can send and receive movies over the electrical wiring. There is no other plug or radio. The data signal is superimposed on the low-frequency power signal (on the active or ‘‘hot’’ wire) as both signals use the wiring at the same time.

The difficulty with using household electrical wiring for a network is that it was designed to distribute power signals. This task is quite different than distributing data signals, at which household wiring does a horrible job. Electrical signals are sent at 50–60 Hz and the wiring attenuates the much higher frequency(MHz) signals needed for high-rate data communication.

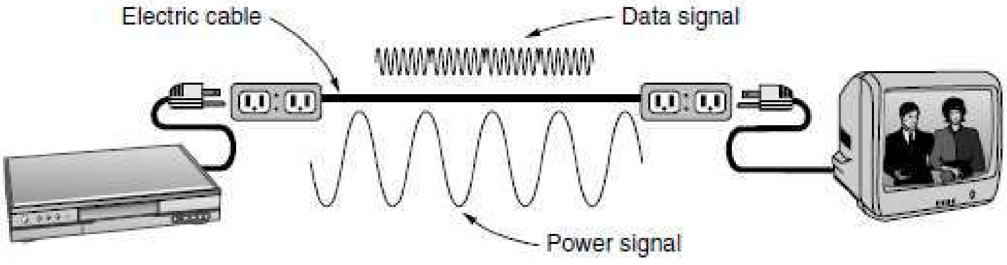


Figure 1.43 Power Lines

5. Fiber Optic Cable

A fibre-optic cable is made of glass or plastic and transmits signals in the form of light. For better understanding we first need to explore several aspects of the **nature of light**. Light travels in a straight line as long as it is mobbing through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance (of a different density), the ray changes direction. The below figure shows how a ray of light changes direction when going from a more dense to a less dense substance.

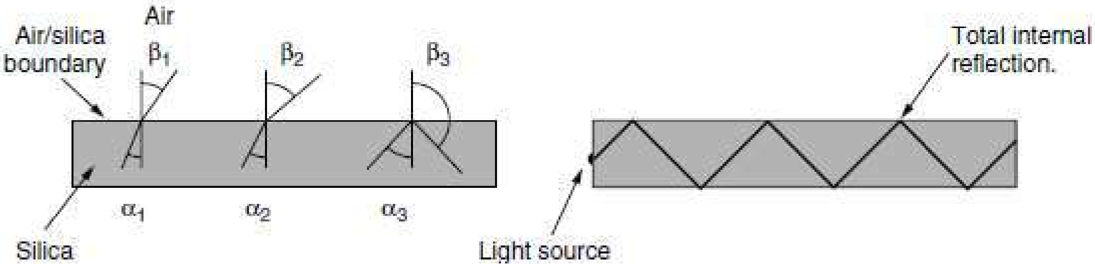


Figure 1.44 Light reflection at fiber cable

As the figure shows:

- If the **angle of incidence I**(the angle the ray makes with the line perpendicular to the interface between the two substances) is **less** than the **critical angle**, the ray **refracts** and moves closer to the surface.
- If the angle of incidence is **greater** than the critical angle, the ray **reflects**(makes a turn) and travels again in the denser substance.
- If the angle of incidence is **equal** to the critical angle, the ray refracts and **moves parallel** to the surface as shown.

Note: *The critical angle is a property of the substance, and its value differs from one substance to another.*

Optical fibres use reflection to guide light through a channel. A glass or plastic core is surrounded by a cladding of less dense glass or plastic. The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being refracted into it. Based on this concept, the fiber is classified into two categories (shown in figure 1.45):

- Single-mode fiber - Carries light pulses along single path and Uses Laser Light Source.
- Multimode fiber - Many pulses of light generated by LED travel at different angles.

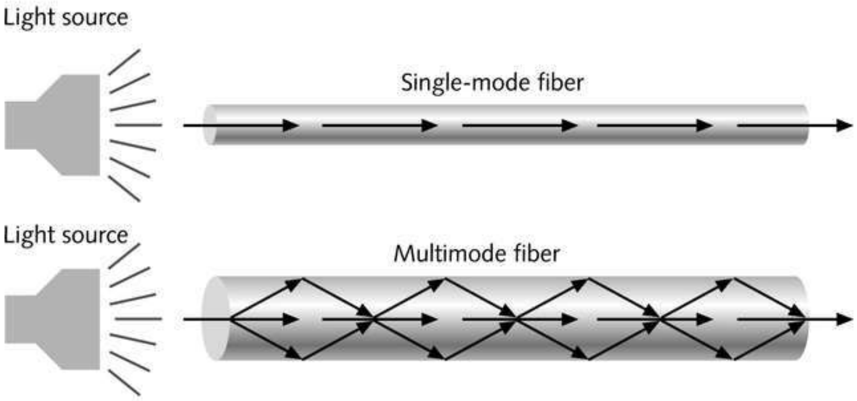


Fig 1.45 Categories of Fiber Optic

. Single-mode fibers are more expensive but are widely used for longer distances. Currently available single-mode fibers can transmit data at 100 Gbps for 100 km without amplification.

- **Transmission of Light Through Fiber**

Optical fibers are made of glass, which, in turn, is made from sand, an inexpensive raw material available in unlimited amounts. Glassmaking was known to the ancient Egyptians, but their glass had to be no more than 1 mm thick or the light could not shine through. Glass transparent enough to be useful for windows was developed during the Renaissance. The glass used for modern optical fibers is so transparent that if the oceans were full of it instead of water, the seabed would be as visible from the surface as the ground is from an airplane on a clear day.

- **Advantages of Fibre Optic Cable**

Fibre optic has several advantages over metallic cable:

- ✓ Higher bandwidth
- ✓ Less signal attenuation
- ✓ Immunity to electromagnetic interference
- ✓ Resistance to corrosive materials
- ✓ Light weight
- ✓ Greater immunity to tapping

- **Disadvantages of Fibre Optic Cable**

There are some disadvantages in the use of optical fibre:

- ✓ Installation and maintenance
- ✓ Unidirectional light propagation
- ✓ High Cost

- **Performance of Fibre Optic Cable**

Attenuation is flatter than in the case of twisted-pair cable and coaxial cable. The performance is such that we need fewer(actually one tenth as many) repeaters when we use the fibre-optic cable.

- **Applications of Fibre Optic Cable**

✓ Often found in backbone networks because its wide bandwidth is cost-effective.
✓ Some cable TV companies use a combination of optical fibre and coaxial cable thus creating a hybrid network.
✓ Local-area Networks such as 100Base-FX network and 1000Base-X also use fibre-optic cable.

- **Comparison of Fiber optic and Copper cable**

Properties	Fiber	Copper
Bandwidth	Higher	Lower
Distance between repeaters	30 KM	5 Km
Interference	Low	High
Physical	Smaller/Lighter	-
Flow	Uni-directional	Bi-directional

1.8 Cable Television

1.8.1 Introduction

There is another major player that has emerged over the past decade for Internet access: cable television networks. Many people nowadays get their telephone and Internet service over cable. In the following sections we will look at cable television as a network in more detail and contrast it with the telephone systems.

1.8.2 Community Antenna Television

Cable television was conceived in the late 1940s as a way to provide better reception to people living in rural or mountainous areas. The system initially consisted of a big antenna on top of a hill to pluck the television signal out of the air, an amplifier, called the **head end**, to strengthen it, and a coaxial cable to deliver it to people's houses, as illustrated in Fig. 1.46.

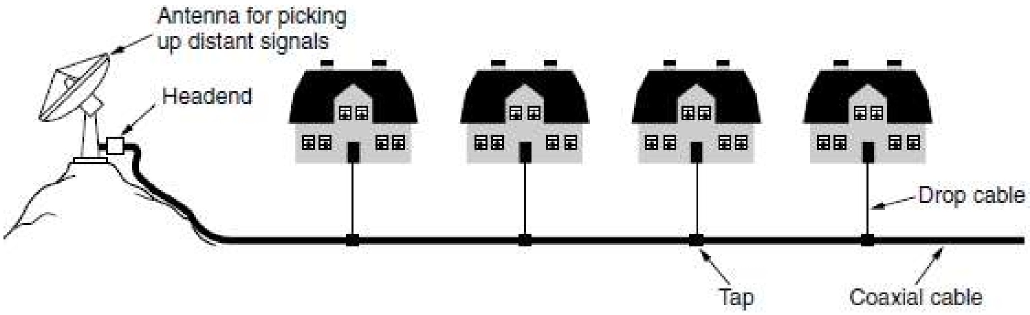


Figure 1.46 An early cable television system.

In the early years, cable television was called **Community Antenna Television**. It was very much a mom-and-pop operation; anyone handy with electronics could set up a service for his town, and the users would chip in to pay the costs. As the number of subscribers grew, additional cables were spliced onto the original cable and amplifiers were added as needed. Transmission was one way, from the headend to the users. By 1970, thousands of independent systems existed.

In 1974, Time Inc. started a new channel, Home Box Office, with new content (movies) distributed only on cable. Other cable-only channels followed, focusing on news, sports, cooking, and many other topics.

1.8.3 Internet over Cable

A system with fiber for the long-haul runs and coaxial cable to the houses is called an **HFC** (**Hybrid Fiber Coax**) system. The electro optical converters that interface between the optical and electrical parts of the system are called **fiber nodes**. Because the bandwidth of fiber is so much greater than that of coax, a fiber node can feed multiple coaxial cables. Part of a modern HFC system is shown in Fig. 1.47.

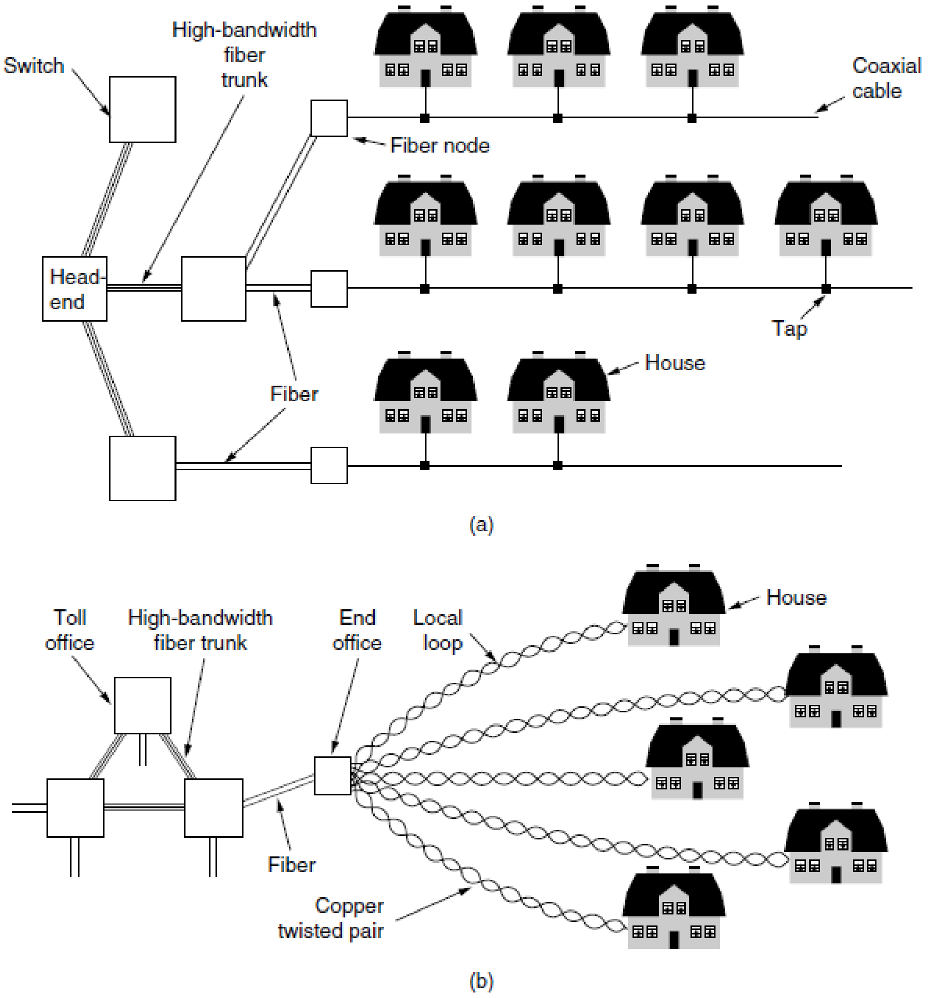


Figure 1.47 (a) Cable television. (b) The fixed telephone system.

There is another difference between the HFC system and the telephone system that is much harder to remove. Down in the neighborhoods, a single cable is shared by many houses, whereas in the telephone system, every house has its own private local loop. When used for television broadcasting, this sharing is a natural fit. All the programs are broadcast on the cable and it does not matter whether there are 10 viewers or 10,000 viewers.

When the same cable is used for Internet access, however, it matters a lot if there are 10 users or 10,000. If one user decides to download a very large file, that bandwidth is potentially being taken away from other users. The more users there are, the more competition there is for bandwidth. The telephone system does not have this particular property: downloading a large file over an ADSL line does not reduce your neighbor's bandwidth. On the other hand, the bandwidth of coax is much higher than that of twisted pairs, so you can get lucky if your neighbors do not use the Internet much.

1.8.4 Spectrum Allocation

Throwing off all the TV channels and using the cable infrastructure strictly for Internet access would probably generate a fair number of irate customers, so cable companies are hesitant to do this. Furthermore, most cities heavily regulate what is on the cable, so the cable operators would not be allowed to do this even if they really wanted to. As a consequence, they needed to find a way to have television and Internet peacefully coexist on the same cable.

The solution is to build on frequency division multiplexing. Cable television channels in North America occupy the 54–550 MHz region (except for FM radio, from 88 to 108 MHz). These channels are 6-MHz wide, including guard bands, and can carry one traditional analog television channel or several digital television channels. In Europe the low end is usually 65 MHz and the channels are 6–8 MHz wide for the higher resolution required by PAL and SECAM, but otherwise the allocation scheme is similar. The low part of the band is not used. Modern cables can also operate well above 550 MHz, often at up to 750 MHz or more. The solution chosen was to introduce upstream channels in the 5–42 MHz band (slightly higher in Europe) and use the frequencies at the high end for the downstream signals. The cable spectrum is illustrated in Fig. 1.48

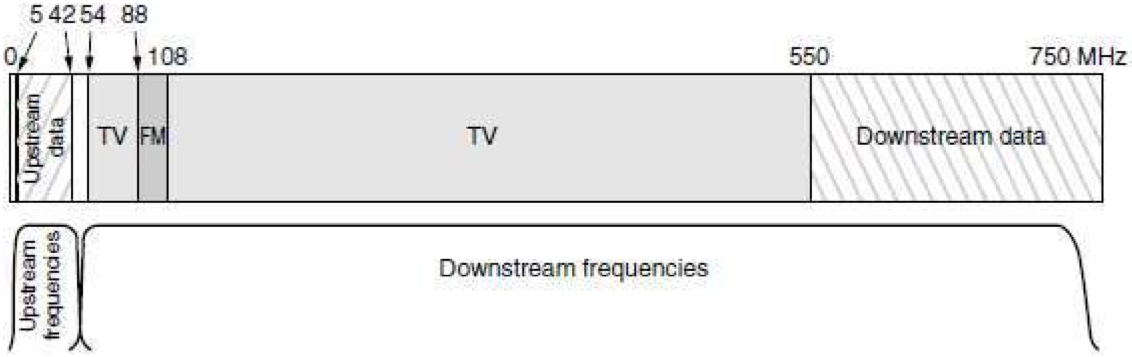


Figure 1.48 Frequency allocation in a typical cable TV system used for Internet access.

The television signals are all downstream, it is possible to use upstream amplifiers that work only in the 5–42 MHz region and downstream amplifiers that work only at 54 MHz and up, as shown in the figure. Thus, we get an asymmetry in the upstream and downstream bandwidths because more spectrum is available above television than below it. On the other hand, most users want more downstream traffic, so cable operators are not unhappy with this fact of life.

In addition to upgrading the amplifiers, the operator has to upgrade the headend, too, from a dumb amplifier to an intelligent digital computer system with a high-bandwidth fiber interface to an ISP. Often the name gets upgraded as well, from ‘‘headend’’ to **CMTS** (**Cable Modem Termination System**).

1.8.5 Cable Modems

Internet access requires a cable modem, a device that has two interfaces on it:

- to the computer
- to the cable network.

In the early years of cable Internet, each operator had a proprietary cable modem, which was installed by a cable company technician. However, it soon became apparent that an open standard would create a competitive cable modem market and drive down prices, thus encouraging use of the service. Furthermore, having the customers buy cable modems in stores and install them themselves (as they do with wireless access points) would eliminate the dreaded truck rolls.

The modem-to-computer interface is straightforward. It is normally Ethernet, or occasionally USB. The other end is more complicated as it uses all of FDM, TDM, and CDMA to share the bandwidth of the cable between subscribers.

When a cable modem is plugged in and powered up, it scans the downstream channels looking for a special packet periodically put out by the head end to provide system parameters to modems that have just come online. Upon finding this packet, the new modem announces its presence on one of the upstream channels. The headend responds by assigning the modem to its upstream and downstream channels. These assignments can be changed later if the headend deems it necessary to balance the load. The use of 6-MHz or 8-MHz channels is the FDM part.

With fewer bits per symbol on the upstream, the asymmetry between upstream and downstream rates is much more than suggested by Fig. 1.49 TDM is then used to share bandwidth on the upstream across multiple subscribers. Otherwise their transmissions would collide at the headend. Time is divided into **minislots** and different subscribers send in different minislots. To make this work, the modem determines its distance from the headend by sending it a special packet and seeing how long it takes to get the response. This process is called **ranging**.

It is important for the modem to know its distance to get the timing right. Each upstream packet must fit in one or more consecutive minislots at the head end when it is received. The head end announces the start of a new round of minislots periodically, but the starting gun is not heard at all modems simultaneously due to the propagation time down the cable. By knowing how far it is from the headend, each modem can compute how long ago the first minislot really started. Minislot length is network dependent.

If the request is accepted, the headend puts an acknowledgement on the downstream channel telling the modem which minislots have been reserved for its packet. The packet is then sent, starting in the minislot allocated to it. Additional packets can be requested using a field in the header. As a rule, multiple modems will be assigned the same minislot, which leads to contention. Two different possibilities exist for dealing with it. The first is that CDMA is used to share the minislot between subscribers. The downstream channels are managed differently from the upstream channels.

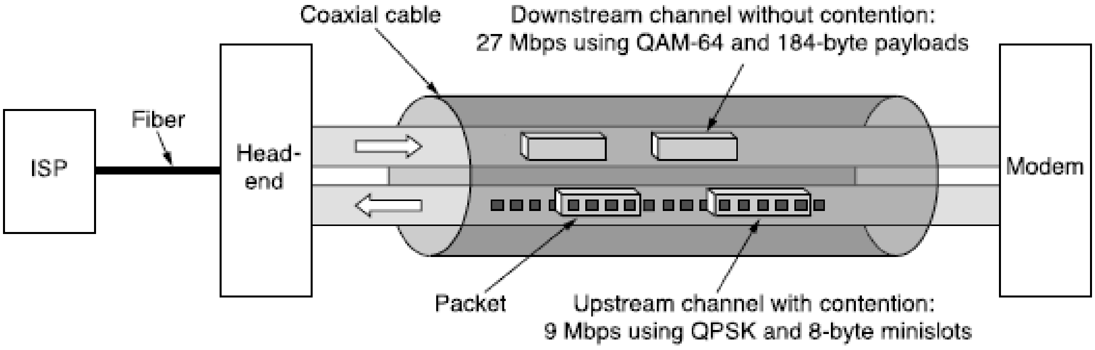

Coaxial cable
Downstream channel without contention:
27 Mbps using QAM-64 and 184-byte payloads
Fiber
ISP
Head-
end
Modem
Packet
Upstream channel with contention:
9 Mbps using QPSK and 8-byte minislots

Figure 1.49 Typical details of the upstream and downstream channels in North America.

For starters, there is only one sender (the headend), so there is no contention and no need for minislots, which is actually just statistical time division multiplexing. For another, the amount of traffic downstream is usually much larger than upstream, so a fixed packet size of 204 bytes is used. Part of that is a Reed-Solomon error-correcting code and some other overhead, leaving a user payload of 184 bytes. These numbers were chosen for compatibility with digital television using MPEG-2, so the TV and downstream data channels are formatted the same way. Logically, the connections are as depicted in Fig. 1.49.

1.8.6 ADSL Versus Cable

Let us compare ADSL and cable on a few points. Both use fiber in the backbone, but they differ on the edge. Cable uses coax; ADSL uses twisted pair. The theoretical carrying capacity of coax is hundreds of times more than twisted pair. However, the full capacity of the cable is not available for data users because much of the cable’s bandwidth is wasted on useless stuff such as television programs.

In practice, it is hard to generalize about effective capacity. ADSL providers give specific statements about the bandwidth (e.g., 1 Mbps downstream, 256 kbps upstream) and generally achieve about 80% of it consistently. Cable providers may artificially cap the bandwidth to each user to help them make performance predictions, but they cannot really give guarantees because the effective capacity depends on how many people are currently active on the user’s cable segment.

Sometimes it may be better than ADSL and sometimes it may be worse. What can be annoying, though, is the unpredictability. Having great service one minute does not guarantee great service the next minute since the biggest bandwidth hog in town may have just turned on his computer.

As an ADSL system acquires more users, their increasing numbers have little effect on existing users, since each user has a dedicated connection. With cable, as more subscribers sign up for Internet service, performance for existing users will drop. The only cure is for the cable operator to split busy cables and connect each one to a fiber node directly. Doing so costs time and money, so there are business pressures to avoid it.

Availability is an issue on which ADSL and cable differ. Everyone has a telephone, but not all users are close enough to their end offices to get ADSL. On the other hand, not everyone has cable, but if you do have cable and the company provides Internet access, you can get it. Distance to the fiber node or headend is not an issue. It is also worth noting that since cable started out as a television distribution medium, few businesses have it.

Being a point-to-point medium, ADSL is inherently more secure than cable. Any cable user can easily read all the packets going down the cable. For this reason, any decent cable provider will encrypt all traffic in both directions. Nevertheless, having your neighbor get your encrypted messages is still less secure than having him not get anything at all.

The telephone system is generally more reliable than cable. For example, it has backup power and continues to work normally even during a power outage. With cable, if the power to any amplifier along the chain fails, all downstream users are cut off instantly.

Finally, most ADSL providers offer a choice of ISPs. Sometimes they are even required to do so by law. Such is not always the case with cable operators. The conclusion is that ADSL and cable are much more alike than they are different. They offer comparable service and, as competition between them heats up, probably comparable prices.

1.9 Short Questions and Answers

1. Define Computer Network.

A network is a set of devices connected by physical media links. A network is recursively is a connection of two or more nodes (normally computers) by a physical link or two or more networks connected by one or more nodes.

2. What is a Link?

At the lowest level, a network can consist of two or more computers directly connected by some physical medium such as coaxial cable or optical fiber. Such a physical medium is called as Link.

3. What is a node?

A network can consist of two or more network devices (such as computer, laptop, routers, switches, bridges, servers and printers) directly connected by some physical medium. The connected devices are called as Nodes.

4. What is meant by data communication?

Data communication is process of exchanging data between two devices through a communication medium in a meaningful way.

5. What are the fundamental characteristics to be followed in effective communication?

To provide the effective communication system, the following four fundamental characteristics must be followed;

1. Delivery
2. Accuracy
3. Timeliness
4. Jitter

6. Define Jitter.

In network the data are split into smaller groups (packets) and send them separately. The variation of the arrival between two packets is referred as jitter.

7. List out the essential components of the communication system.

1. Data/Message
2. Source
3. Destination
4. Medium
5. Protocol

8. Define Data Flow.

The data flow defines the flow direction of the data between source and destination. The data flow may be either simplex or half-duplex or full duplex.

9. What is meant by Half-Duplex data transmission?

In half-duplex mode, the data can be transmitted on both directions (device 1 to device 2 or device 2 to device 1) but not at the same time. One device can send and another one can receive at a time. The example is walkie-talkie. The entire medium is used for the one-way transmission.

10. What is meant by Full-Duplex data transmission?

In full-duplex mode, the data can be transmitted on both directions (device 1 to device 2 and device 2 to device 1) at the same time (One device can send and another one can receive at a time. The example is telephone communication. In this, the entire medium is divided for the two-way transmission.

11. List out few applications of computer networks

a) Business Applications
b) Home Applications
c) Mobile Users
d) Social issues

12. What is point-point link?

If the physical links are directly connected to a pair of nodes it is said to be point-point link.

13. What is Multiple Access?

If the physical links are shared by more than two nodes, it is said to be Multiple Access.

14. Mention the types of transmission technology.

There are two types of transmission technology that are in widespread use:

Broadcast links and point-to-point links.

15. Define packets?

To go from the source to the destination on a network made up of point-to-point links, short messages, called packets.

16. What is unicasting?

Transmission with exactly one sender and exactly one receiver is sometimes called unicasting.

17. What is Broadcasting?

Broadcast systems usually also allow the possibility of addressing a packet to all destinations by using a special code in the address field. When a packet with this code is transmitted, it is received and processed by every machine on the network. This mode of operation is called broadcasting.

18. What is Multicasting?

Some broadcast systems also support transmission to a subset of the machines, which known as multicasting.

19. What is meant by service in layered model?

Service is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.

20. Define Protocol.

Protocol is a set of rules governing the format and meaning of the packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols to implement their service definitions.

21. What are the key elements of protocol?

The key elements of a protocol are syntax, semantics, and timing.

22. What is meant by syntax?

The term syntax refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

23. What is meant by semantics?

The word semantics refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

24. What is meant by timing?

The term timing refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

25. What are the responsibilities of data link layer?

Specific responsibilities of data link layer include the following.

a) Framing
b) Physical addressing
c) Flow control
d) Error control
e) Access control

26. Why are protocols needed?

In networks, communication occurs between the entities in different systems. Two entities cannot just send bit streams to each other and expect to be understood. For communication, the entities must agree on a protocol. A protocol is a set of rules that govern data communication.

27. Group the OSI layers by function.

The seven layers of the OSI model belonging to three subgroups. Physical, datalink and network layers are the network support layers; they deal with the physical aspects of moving data from one device to another. Session, presentation and application layers are the user support layers; they allow interoperability among unrelated software systems. The transport layer ensures end-to-end reliable data transmission.

28. What are header and trailers and how do they get added and removed?

Each layer in the sending machine adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it. This information is added in the form of headers or trailers. Headers are added to the message at the layers 6,5,4,3, and 2. A trailer is added at layer2. At the receiving machine, the headers or trailers attached to the data unit at the corresponding sending layers are removed, and actions appropriate to that layer retaken.

29. The transport layer creates a communication between the source and destination. What are the three events involved in a connection?

Creating a connection involves three steps: connection establishment, data transfer and connection release.

30. What is a switch?

A switch is a networking device that manages networked connections between devices on a star network.

31. Define Bluetooth.

Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices and building personal area networks (PANs).

32. What is LAN?

A LAN is a privately owned network that operates within and nearby a single building like a home, office or factory. LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g., printers) and exchange information.

33. List out Advantages of Ethernet.

1. Inexpensive
2. Easy to install
3. Supports various writing technologies.

34. What are the limitations of bridges?

1. Scale
2. Heterogeneity

35. Define router.

Router is a network layer device that connects networks with different physical media and translates between different network architecture.

36. Define Transmission Lines.

Its move bits between machines. They can be made of copper wire, optical fiber, or even radio links. Most companies do not have transmission lines lying about, so instead they lease the lines from a telecommunications company.

37. Define gateway.

The general name for a machine that makes a connection between two or more networks and provides the necessary translation, both in terms of hardware and software, is a gateway. Gateways are distinguished by the layer at which they operate in the protocol hierarchy.

38. Define Signals

Signal is a physical representation of data by means of analog or digital. To be transmitted, data must be transformed to electromagnetic signals.

39. What is meant by periodic and nonperiodic signals?

Both analog and digital signals can take one of two forms: periodic or nonperiodic (sometimes refer to as aperiodic, because the prefix a in Greek means "non").

A periodic signal completes a pattern within a measurable time frame, called a period, and repeats that pattern over subsequent identical periods. The completion of one full pattern is called a cycle. A nonperiodic signal changes without exhibiting a pattern or cycle that repeats over time.

40. Define Period and Frequency.

Period refers to the amount of time (T), in seconds, a signal needs to complete 1 cycle. Frequency (f) refers to the number of periods in 1s. Period is the inverse of frequency, and frequency is the inverse of period, as the following formulas show.

$$f = \frac{1}{T} \text{ and } T = \frac{1}{f}$$

Period is formally expressed in seconds. Frequency is formally expressed in ***Hertz*** (Hz), which is ***cycle per second***.

41. Define Wavelength.

Wavelength can be calculated if one is given the propagation speed (the speed of light) and the period of the signal. It is normally considered as the length of one complete cycle of a signal. However, since period and frequency are related to each other, if we represent wavelength by 'λ', propagation speed by 'c' (speed of light), and frequency by 'f', we get

$$\lambda = \frac{c}{f} \quad , where\ c = 3\ x\ 10^8 m/s$$

The wavelength is normally measured in micrometers (microns) instead of meters.

42. Define bandwidth.

The bandwidth (B) of a composite signal is defined as the difference between the highest (*f_H)* and the lowest (*f_L*) frequencies contained in that signal. Hence, the bandwidth (*B*) is calculates as

$$B = f_H - f_L$$

43. What is meant by bit rate?

The bit rate is the number of bits sent in 1s, expressed in bits per second (bps). The bit rate (instead of frequency)-is used to describe digital signals

44. Define throughput or data transfer rate.

In computer network, throughput is defined as the actual number of bits that flows through a network connection in a given period of time. Throughput is always less than or equal to bandwidth but can never exceed bandwidth.

45. What are the factors that the throughput of a computer network?

In a computer network, the throughput can be affected by many factors as listed below:

- Network congestion due to heavy network usage.
- Too many users are accessing the same server.
- Low bandwidth allocation between network devices.
- Medium loss of a computer network.
- Resources (CPU, RAM) of network devices.

46. List the Guided Media used in computer network.

There are five types in guided media used in computer network.

1. Magnetic Media
2. Twisted Pairs
3. Coaxial Cable
4. Power Lines
5. Fiber Optics

1.10 Explanatory Questions

1. What are the 4 types of network? (5)
2. Discuss about protocol hierarchies (5).
3. Explain the service primitives used in connection oriented service (5).
4. Differentiate the OSI and TCP Reference models (5).
5. How to classify the Computer Network. Explain with its merits and demerits. (10)
6. Briefly Discuss about the ISO reference model (10)
7. Explain about the TCP/IP Reference model (10)
8. Discuss about the signals (5).
9. Explain the guided transmission media with necessary diagrams (10).
10. Discuss about the cable television (10).

1.11 Objective Questions

1. The frequency is measured by unit

    (a) Hertz
    (b) bit
    (c) byte
    (d) meter

    Answer : a

2. Bandwidth of channel is calculated by

    (a) Difference between lower bound frequency and upper bound frequency
    (b) upper bound frequency
    (c) lower bound frequency
    (d) Difference between lower amplitude and upper amplitude
    Answer : a

3. Hertz is defined as

    (a) One cycle per bit
    (b) One cycle per second
    (c) One cycle per byte
    (d) All the above
    Answer : b

4. What happens to the bandwidth frequency range when the quality factor increases?

   (a) Becomes zero
   (b) Increases
   (c) Decreases
   (d) Remains the same
   Answer : b

5. The bandwidth of wireless radio LAN is

   (a) 24Mbps
   (b) 2 Mbps
   (c) 4 Mbps
   (d) 8 Mbps
   Answer : b

6. The frequency range of wireless LAN is

   (a) 900 MHz bands
   (b) 2GHz bands
   (c) 5 GHz bands
   (d) All of these

7. Signals are transmitted in terms

   (a) Raw bits
   (b) Electromagnetic waves
   (c) Electronics waves
   (d) Electrical waves

8. What is the bandwidth of the FM radio channel?

   (a) 200 MHz
   (b) 200 kHz
   (c) 200 Hz
   (d) 200 GHz

9. The audible bandwidth of human ear ranges is ___________________

   (a) 20 Hz to 20,000Hz
   (b) 20 kHz to 20,000kHz
   (c) 20 MHz to 20,000MHz
   (d) None of the above

10. What is the frequency range used in RADAR?

    (a) 1 MHz
    (b) 3 MHz
    (c) 3 to 4 MHz
    (d) 1 to 3 MHz

11. A given signal has frequencies of 3125 MHz, 635 MHz, 2000MHz and 7000MHz. Determine the bandwidth of the signal?

    (a) 5365 MHz
    (b) 5000 MHz
    (c) 6365 MHz

(d) 3875 MHz

12. The frequency of human heart rate is

(a) 1 Hz
(b) 2Hz
(c) 1.2 Hz
(d) 1.3 Hz

13. The hertz is named from

(e) Heinrich Hertz
(a) Hillarous Hertz
(b) Hamilton Hertz
(c) Henrock Hertz

14. A V.92 modem for the telephone network can transfer 56,000 bit/s downstream and 48,000 bit/s upstream over an analog telephone network. Due to filtering in the telephone exchange, the frequency range is limited to between 300 hertz and 3,400 hertz. What is the modulation efficiency?

(a) 56 (kbit/s)/kHz downstream, and 48 (kbit/s)/kHz upstream
(b) 5.6 (kbit/s)/kHz downstream, and 4.8 (kbit/s)/kHz upstream
(c) 18.1 (bit/s)/Hz downstream, and 15.5 (bit/s)/Hz upstream
(d) 56 (bit/s)/Hz downstream, and 48 (bit/s)/Hz upstream

15. The modulation efficiency in bit/s defined as

(a) The gross bitrate (including any error-correcting code) divided by the bandwidth.
(b) The gross bitrate (excluding any error-correcting code) divided by the bandwidth.
(c) The gross bitrate (including any error-correcting code) divided by the throughput.
(d) The gross bitrate (excluding any error-correcting code) divided by the bandwidth

16. How long will it take to transfer a 1.2 MB file using a modem link working at 52,00 bits/s?

(a) 184.6 s
(b) 194.6 s
(c) 191.4 s
(d) 181.4 s

17. A system manager wants to backup an 8GB data using 2 Mbps bandwidth leased line. What will be exact time for backup?

(a) 532 s
(b) 533 s
(c) 534 s
(d) 533.3 s

18. A company wants to send a 10MB data within 10 seconds. What will be minimum and maximum bandwidth requirement for a connection?

(a) 8Mbps, 80 Mbps
(b) 1Mbps , 10 Mbps
(c) 2 Mbps, 20 Mbps
(d) 8 kbps, 80 kbps

19. The throughput of communication line is defined as

(a) Maximum amount of data transferred in period of time
(b) Actual data transferred in period of time
(c) Minimum amount of data transferred in period of time
(d) All the above

20. The bit rate of signal is 3000bps. If each signal unit carries 6 bits, the baud rate of the signal rates is _____ .

(a) 500 baud/s
(b) 1000 baud/sec
(c) 3000 baud/sec
(d) 18000 baud/sec

Answer : a

21. The period of signal is 10 ms. What is the frequency in hertz?

(a) 10
(b) 100
(c) 1000
(d) 10000

Answer : b

22. An analog signal carries 4 bits in each signal unit. If 1000 signal units are sent per second, then baud rate and bit rate of the signal are ________ and ____________

(a) 4000 bauds / sec & 1000 bps
(b) 2000 bauds / sec & 1000 bps
(c) 1000 bauds / sec & 500 bps
(d) 1000 bauds / sec & 4000 bps

Answer : d

23. What is the period for a frequency of 60 Hz?

(a) 1s
(b) 1ms
(c) 16.67ms
(d) 10 ms

Answer : c

24. An analog signal has a bit rate of 6000 bps and a baud rate of 2000 baud. How many data elements are carried by each signal element?

(a) 0.336 bits/baud
(b) 3 bits/baud
(c) 120,00,000 bits/baud
(d) None of the above

Answer : b

25. Which signal has a wider bandwidth, a sine wave with a frequency of 100 Hz or a sine wave with a frequency of 200 Hz?

(a) 100Hz
(b) 200Hz
(c) same
(d) different

Answer : c

26. A device is sending out data at the rate of 1000 bps. How long does it take to send a file of 100,000 characters?

(a) 800s
(b) 80s
(c) 8 s
(d) 8 minutes

Answer : a

27. A TV channel has a bandwidth of 6 MHz. If we send a digital signal using one channel, what are the data rates if we use one five harmonics?

(a) 2 Mbps
(b) 2.4 Mbps
(c) 6Mbps
(d) 30 Mbps

Answer : b

28. If the bandwidth of the channel is 5 Kbps, how long does it take to send a frame of 100,000 bits out of this device?

(a) 10s
(b) 200s
(c) 20s
(d) 2s

Answer :c

29. A network with bandwidth of 8 Mbps can pass only an average of 20,000 frames per minute with each frame carrying an average of 12,000 bits. What is the throughput of this network?

(a) 8 Mbps
(b) 4 Mbps
(c) 12 Mbps
(d) 20 Mbps

Answer : b

30. A file contains 2 million bytes. How long does it take to download this file using a 56-Kbps channel? 1-Mbps channel?

(a) 285.7s, 2s
(b) 285.7s, 16s
(c) 571s, 32s
(d) 571s,16s

Answer : b

31. What is the bit rate for transmitting uncompressed 800 x 600 pixel colour frames with 8 bits/pixel at 40 frames/second?

(a) 2.4 Mbps
(b) 15.36 Mbps
(c) 153.6 Mbps
(d) 1536 Mbps

Answer : c

32. What is the transmission time of a packet sent by a station if the length of the packet is 1 million bytes and the bandwidth of the channel is 200 Kbps?/

(a) 4s
(b) 40s
(c) 4 mins
(d) 5s

Answer : b

33. A periodic signal completes one cycle in 0.001s. What is the frequency?

(a) 1Hz
(b) 100 Hz
(c) 1 kHz
(d) 1 MHz

Answer : c

34. If the bandwidth of the signal is 5KHz and the lowest frequency is 52KHz, what is the highest frequency?

(a) 5 KHz
(b) 52 KHz
(c) 47 KHz
(d) 57 KHz

Answer : d

35. The period of cycle is 220ns. What is the corresponding frequency in MHz?

(a) 50 MHz
(b) 5 MHz
(c) 50 KHz
(d) 500 MHz

Answer : b

36. How many KHz are in one GHz?

(a) 10^6 KHz
(b) 10^3 KHz
(c) 1000 KHz
(d) 10000KHz

Answer : a

37. The number of layers in Internet protocol stack

a) 5
b) 7
c) 6
d) None of the mentioned

Answer: a
Explanation: There are five layers in the Internet Protocol stack. The five layers in Internet Protocol stack is Application, Transport, Network, Data link and Physical layer.

38. The number of layers in ISO OSI reference model

a) 5
b) 7
c) 6
d) None of the mentioned

Answer: b
Explanation: The seven layers in ISO OSI reference model is Application, Presentation, Session, Transport, Network, Data link and Physical layer.

39. This layer is an addition to OSI model when compared with TCP IP model

a) Application layer
b) Presentation layer
c) Session layer
d) Both Session and Presentation layer

Answer: d
Explanation: The only difference between OSI model and TCP/IP model is that in OSI model two layers namely Presentation and Session layer have been added.

40. Application layer is implemented in

a) End system
b) NIC
c) Ethernet
d) None of the mentioned

Answer: a
Explanation: Not only application layer, but presentation layer, session layer and transport layer are also implemented in the end system.

41. Transport layer is implemented in

a) End system
b) NIC
c) Ethernet
d) None of the mentioned

Answer: a

Explanation: Application, Presentation, Session and Transport layer are implemented in the end system.

42. The functionalities of presentation layer includes

a) Data compression
b) Data encryption
c) Data description
d) All of the mentioned

Answer: d

Explanation: Some functions of the presentation layer include character-code translation, data conversion, data encryption and decryption, and data translation.

43. Delimiting and synchronization of data exchange is provided by

a) Application layer
b) Session layer
c) Transport layer
d) Link layer

Answer: b

Explanation: The session layer provides the mechanism for opening, closing and managing a session between end-user application processes. The session layer 5 is responsible for establishing managing synchronizing and terminating sessions.

44. In OSI model, when data is sent from device A to device B, the 5th layer to receive data at B is

a) Application layer
b) Transport layer
c) Link layer
d) Session layer

Answer: d

Explanation: In OSI reference model, the fifth layer is Session layer. Session layer provides the mechanism for opening, closing and managing a session between end-user application processes.

45. In TCP IP Model, when data is sent from device A to device B, the 5th layer to receive data at B is

a) Application layer
b) Transport layer
c) Link layer
d) Session layer

Answer: a

Explanation: In TCP/IP model, the fifth layer is application layer. when data is sent from device A to device B, the 5th layer to receive data at B is application layer.

46. In the OSI model, as a data packet moves from the lower to the upper layers, headers are _______

a) Added
b) Removed
c) Rearranged
d) None of the mentioned

Answer: b

Explanation: In OSI reference model, when data packet moves from lower layers to higher layer, headers get removed. Whereas when data packet move from higher layer to lower layers, headers are added.

47. OSI stands for

a) open system interconnection
b) operating system interface
c) optical service implementation
d) none of the mentioned

Answer: a

Explanation**:** OSI is the abbreviation for Open System Interconnection. OSI model provides a structured plan on how applications communicate over a network, which also helps us to have a structured plan for troubleshooting.

48. The OSI model has _______ layers.

a) 4
b) 5
c) 6
d) 7

Answer: d

Explanation: In OSI reference model, there are 7 layers namely Application, Presentation, Session, Transport, Network, Data Link and Physical layer.

49. TCP/IP model does not have ______ layer but OSI model have this layer

a) session layer
b) transport layer
c) application layer
d) None of the mentioned

Answer: a
Explanation: In OSI reference model, there are two layers which are not present in TCP/IP model. They are Presentation and Session layer.

50. Which layer links the network support layers and user support layers

a) session layer
b) data link layer
c) transport layer
d) network layer

Answer: c
Explanation: Physical, data link and network layers are network support layers and session, presentation and application layers are user support layers.

51. Which address is used in an internet employing the TCP/IP protocols?

a) physical address and logical address
b) port address
c) specific address
d) all of the mentioned

Answer: d
Explanation: All of the mentioned above addresses are used in TCP/IP protocol. All the addressing scheme, that is physical (MAC) and logical address, port address and specific address are employed in both TCP/IP model and OSI model.

52. TCP/IP model was developed _____ the OSI model.

a) prior to
b) after
c) simultaneous to
d) none of the mentioned

Answer: a
Explanation: Several TCP/IP prototypes were developed at multiple research centers between 1978 and 1983, whereas OSI reference model was developed in the year 1984.

53. Which layer is responsible for process to process delivery?

a) network layer
b) transport layer
c) session layer
d) data link layer

Answer: b
Explanation: The role of Transport layer (Layer 4) is to establish a logical end to end connection between two system in a network. The protocols used in Transport layer is TCP and UDP.

54. Which address identifies a process on a host?

a) physical address
b) logical address
c) port address
d) specific address

Answer: c
Explanation: A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server.

55. Which layer provides the services to user?

a) application layer
b) session layer
c) presentation layer
d) none of the mentioned

Answer: a
Explanation: In networking, a user mainly interacts with application layer to create and send information to other computer or network.

56. Transmission data rate is decided by

a) network layer
b) physical layer
c) data link layer
d) transport layer

Answer: b
Explanation: Physical layer is a layer 1 device which deals with network cables or the standards in use like connectors, pins, electric current used etc. Basically the transmission speed is determined by the cables and connectors used. Hence it is physical layer that determines the transmission speed in network.

2. Data Link Layer

The data link layer is the protocol layer in a program that handles the moving of data into and out of a physical link in a network. The data link layer is Layer 2 in the Open Systems Interconnection (OSI) architecture model for a set of telecommunication protocols. Data bits are encoded, decoded and organized in the data link layer, before they are transported as frames between two adjacent nodes on the same LAN or WAN.

The data link layer also determines how devices recover from collisions that may occur when nodes attempt to send frames at the same time. The *Figure 2.1* shows the relationship of the Data Link Layer to the network layer and physical layer.

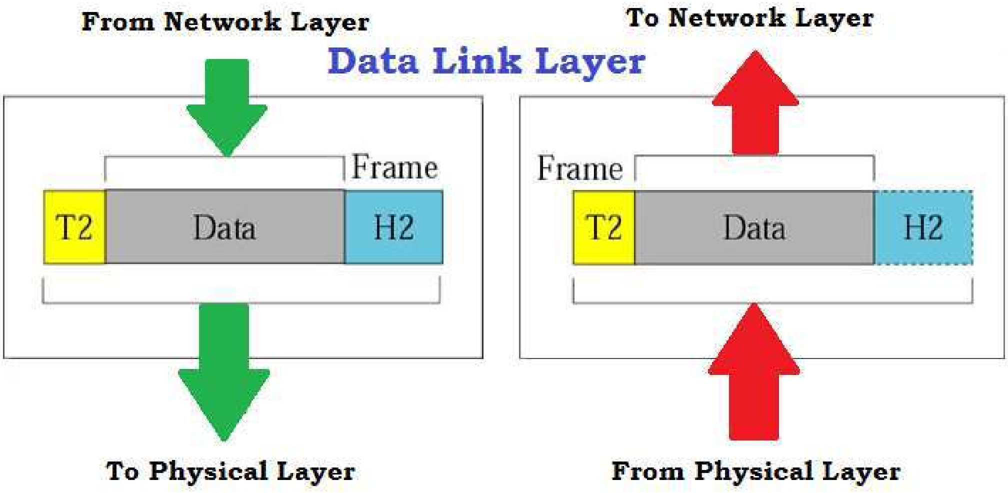


Figure 2.1 Relationship between data link layer with physical layer and network layer

2.1. Data Link Layer Design Issues

The data link layer uses the services of the physical layer to send and receive bits over communication channels. It has a number of functions, including:

1. Providing a well-defined service interface to the network layer.
2. Dealing with transmission errors.
3. Regulating the flow of data so that slow receivers are not swamped by fast senders.

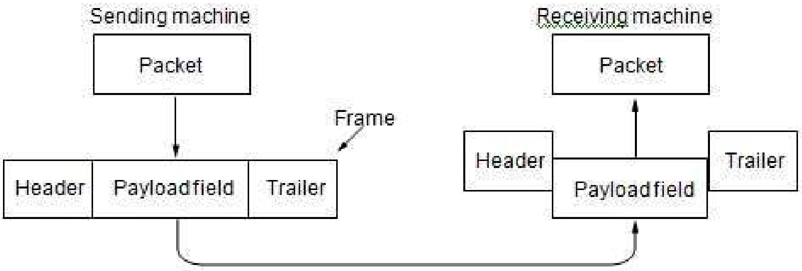


Figure 2.2 Relationship between packets and frame

To accomplish these goals, the data link layer takes the packets it gets from the network layer and encapsulates them into frames for transmission. Each frame contains a frame header, a payload field for holding the packet, and a frame trailer as shown in *Figure 2.2*. Frame management forms the heart of what the data link layer does.

2.1.1. Services Provided to the Network Layer

The function of the data link layer is to provide services to the network layer. The principal service is transferring data from the network layer on the source machine to the network layer on the destination machine. On the source machine is on entity, call it a process, in the network layer that hands some bits to the data link layer for transmission to the destination. The job of the data link layer is to transmit the bits to the destination machine so they can be handed over to the network layer there, as shown in *Figure 2.3(a)*. The actual transmission follows the path of *Figure 2.3*, but it is easier to think in terms of two data link layer processes communicating using a data link protocol. For this reason, we will implicitly use the model of *Figure 2.3(b)*.

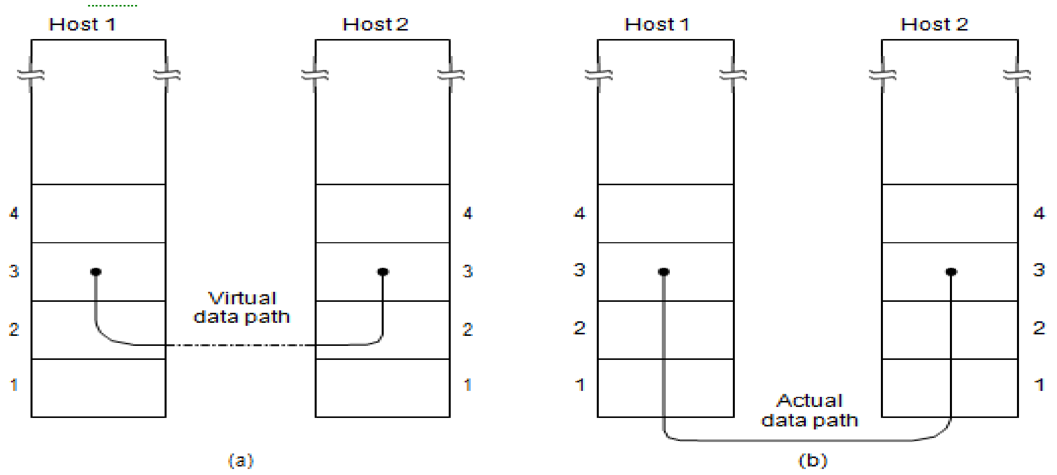


Figure 2.3 (a) Virtual communication. (b) Actual communication.

The data link layer can be designed to offer various services. The actual ser- vices that are offered vary from protocol to protocol. Three reasonable possibilities that we will consider in turn are:

1. Unacknowledged connectionless service.
2. Acknowledged connectionless service.
3. Acknowledged connection-oriented service.

1. Unacknowledged connectionless service.

Unacknowledged connectionless service consists of having the source machine send independent frames to the destination machine without having the destination machine acknowledge them.

No logical connection is established beforehand or released afterward. If a frame is lost due to noise on the line, no attempt is made to detect the loss or recover from it in the data link layer. This class of service is appropriate when the error rate is very low so that recovery is left to higher layers. It is also appropriate for real-time traffic, such as voice, in which late data are worse than bad data. Most LANs use unacknowledged connectionless service in the data link layer.

2. *Acknowledged connectionless service.*

When this service is offered, there are still no logical connections used, but each frame sent is individually acknowledged. In this way, the sender knows whether a frame has arrived correctly. If it has not arrived within a specified time interval, it can be sent again. This service is useful over unreliable channels, such as wireless systems.

3. *Connection-Oriented service.*

The most sophisticated service the data link layer can provide to the network layer is connection-oriented service. With this service, the source and destination machines establish a connection before any data are transferred. Each frame sent over the connection is numbered, and the data link layer guarantees that each frame sent is indeed received. Furthermore, it guarantees that each frame is received exactly once and that all frames are received in the right order.

When connection-oriented service is used, transfers go through three distinctc phases.

Phase 1: Connection is established

Phase 2: One or more frames are actually transmitted.

Phase 3 : The connection is released, freeing up the variables, buffers and other resources used to maintain the connection.

2.1.2. Framing

To provide service to the network layer, the data link layer must use the service provided to it by the physical layer. What the physical layer does is accept a raw bit stream and attempt to deliver it to the destination. If the channel is noisy, as it is for most wireless and some wired links, the physical layer will add some redundancy to its signals to reduce the bit error rate to a tolerable level. However, the bit stream received by the data link layer is not guaranteed to be error free.

The usual approach is for the data link layer to break up the bit stream into discrete frames, compute a short token called a checksum for each frame, and include the checksum in the frame when it is transmitted. When a frame arrives at the destination, the checksum is recomputed.

Breaking up the bit stream into frames is more difficult than it at first appears. A good design must make it easy for a receiver to find the start of new frames while using little of the channel bandwidth. We will look at four methods:

1. Byte count.

2. Flag bytes with byte stuffing.
3. Flag bits with bit stuffing.
4. Physical layer coding violations.

1. Byte count

The byte count method uses a field in the header to specify the number of bytes in the frame. When the data link layer at the destination sees the byte count, it knows how many bytes follow and hence where the end of the frame is. This technique is shown in *Figure 2.4*.(a) for four small example frames of sizes 5, 5, 8, and 8 bytes, respectively.

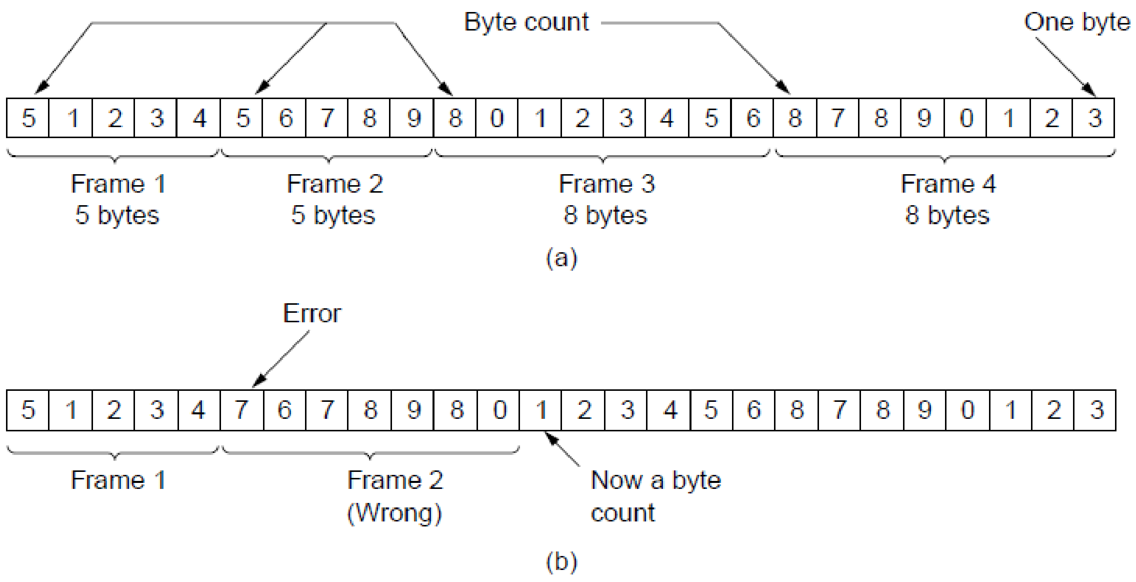


Figure 2.4 A byte stream. (a) Without errors. (b) With one error.

Frame Error

The trouble with this algorithm is that the count can be garbled by a transmission error. For example, if the byte count of 5 in the second frame of *Figure 2.4*. (b) becomes a 7 due to a single bit flip, the destination will get out of synchronization. It will then be unable to locate the correct start of the next frame. Even if the checksum is incorrect so the destination knows that the frame is bad, it still has no way of telling where the next frame starts.

Sending a frame back to the source asking for a retransmission does not help either, since the destination does not know how many bytes to skip over to get to the start of the retransmission. For this reason, the byte count method is rarely used by itself.

2. Flag bytes with byte stuffing.

The second framing method gets around the problem of resynchronization after an error by having each frame start and end with special bytes. Often the same byte, called a flag byte, is used as both the starting and ending delimiter. This byte is shown in Fig. (a) as FLAG. Two consecutive flag bytes indicate the end of one frame and the start of the next. Thus, if the receiver ever loses synchronization it can just search for two flag bytes to find the end of the current frame and the start of the next frame.

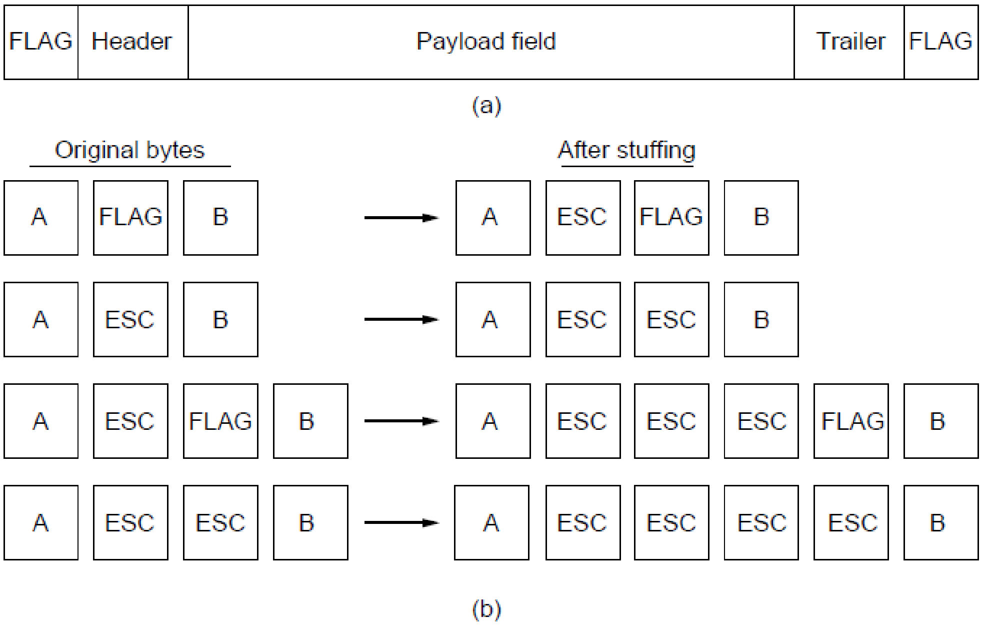


Figure 2.5 (a) A frame delimited by flag bytes. (b) Four examples of byte sequences before and after byte stuffing.

Problem in Flag

- ✓ Flag methods used for synchronization.
- ✓ The 'flag' bit pattern may occur in data transformation.
- ✓ To avoid this, byte stuffing is used with 'ESC' byte stuffing.
- ✓ Used in PPP protocol.
- ✓ Not suitable for 16-bit characters (UNICODE).

3. *Flag bits with bit stuffing.*

The third method of delimiting the bit stream gets around a disadvantage of byte stuffing, which is that it is tied to the use of 8-bit bytes. Framing can be also be done at the bit level, so frames can contain an arbitrary number of bits made up of units of any size. It was developed for the once very popular HDLC (High- level Data Link Control) protocol.

Each frame begins and ends with a special bit pattern, 01111110 or 0x7E in hexadecimal. This pattern is a flag byte. When-ever the sender's data link layer encounters five consecutive 1s in the data, it automatically stuffs a 0 bit into the outgoing bit stream.

When the receiver sees five consecutive incoming 1 bits, followed by a 0 bit, it automatically destuffs (i.e., deletes) the 0 bit. Just as byte stuffing is completely transparent to the network layer in both computers, so is bit stuffing. If the user data contain the flag pattern, 01111110, this flag is transmitted as 011111010 but stored in the receiver's memory as 01111110.

With bit stuffing, the boundary between two frames can be unambiguously recognized by the flag pattern. Thus, if the receiver loses track of where it is, all it has to do is scan the input for flag sequences, since they can only occur at frame boundaries and never within the data.

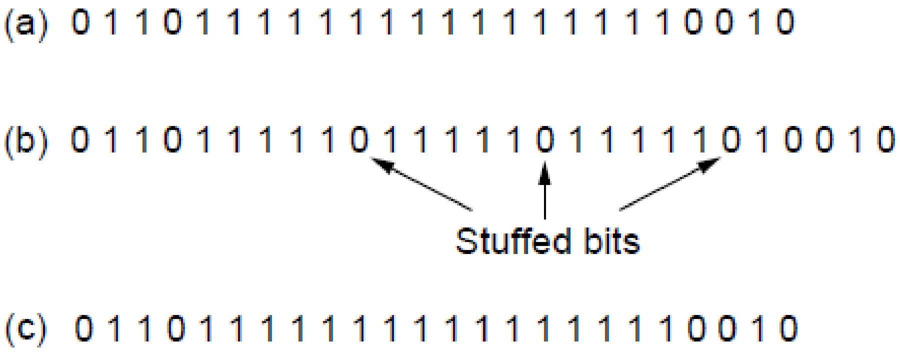

(a) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0
(b) 0 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 1 1 1 1 0 1 0 0 1 0
Stuffed bits
(c) 0 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 0 1 0

Figure 2.6 . Bit stuffing. (a) The original data. (b) The data as they appear on the line. (c) The data as they are stored in the receiver's memory after destuffing.

4. *Physical layer coding violations*

Many data link protocols use a combination of these methods for safety. A common pattern used for Ethernet and 802.11 is to have a frame begin with a well-defined pattern called a preamble. This pattern might be quite long (72 bits is typical for 802.11) to allow the receiver to prepare for an incoming packet. The preamble is then followed by a length (i.e., count) field in the header that is used to locate the end of the frame.

2.1.3. Error Control

The next issue in the data link layer is error control. The error may be happened during the transmission. The errored frames are dropped by the receiver and acknowledgement are not sent. The Acknowledgment (ACK) used for reliable delivery. If frame or ACK is lost, no ACK is sent to sender. In this case Sender uses timer to react with average round trip time (RTT) to retransmit the frame. If ACK is lost, receiver receives multiple copies of same frame. To identify multiple copies and remove the duplicated copies of the frame, sequence number is used in the frames.

2.1.4. Flow Control

Flow control is a technique that allows two stations working at different speeds to communicate with each other. It is a set of measures taken to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver.

In data link layer, flow control restricts the number of frames the sender can send before it waits for an acknowledgment from the receiver. Two approaches are commonly used.

- **Feedback based Flow Control** - the sender sends frames after it has received acknowledgments from the user. This is used in the data link layer.

- **Rate based Flow Control** - These protocols have built in mechanisms to restrict the rate of transmission of data without requiring acknowledgment from the receiver. Used in the network layer and the transport layer.

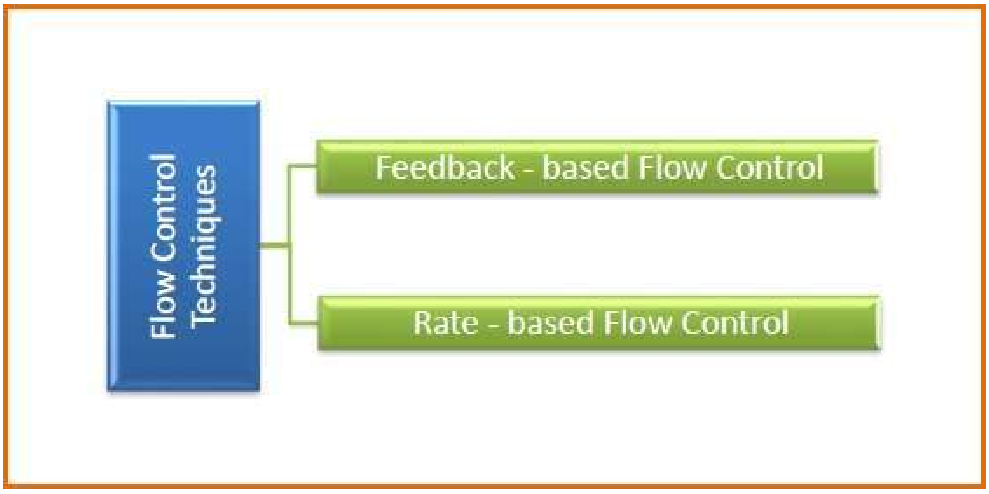


Figure 2.7 Approaches of Flow Control

2.2. Channel Allocation Problem

The network connections are categorized into two: point-to-point connections and broadcast connections. In point-to-point connections, the communication is carried out between exactly two persons. Hence, the channel is allocated only for these two persons. But, in a broadcast network, the main problem is to determine the allocation of channel when many users trying to access. These broadcast channels are sometime called as multiple access channel or random-access channel.

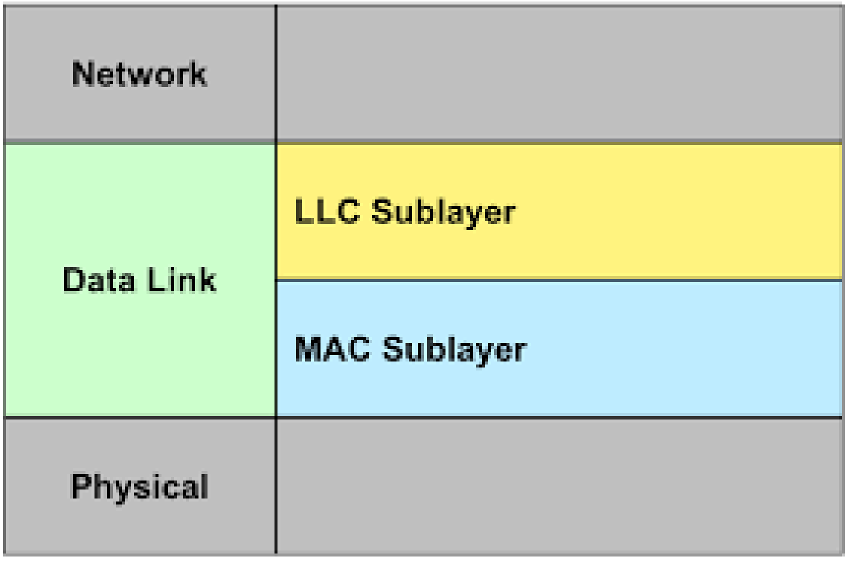


Figure 2.8 Sub Layers of Data Link Layer

The protocols used to determine who goes next on a multiaccess channel belong to a sublayer of the data link layer called the MAC (Medium Access Control) sublayer. The MAC sublayer is especially important in LANs, many of which use a multiaccess channel as the basis for communication. WANs, in contrast, use point-to-point links, except for satellite networks. The Figure 2.8 shows the sub layers of data link layer. Technically, the MAC sublayer is the bottom part of the data link layer.

The main aim of the channel allocation is how to allocate a single broadcast channel among competing users. The allocation is divided into static and dynamic channel allocation. We look into these in detail.

2.2.1. Static Channel allocation

In this scheme a Frequency Division Multiplexing (FDM) is used for allocating a single channel among competing users. For example, if we have N users, the bandwidth will be divided into N equal-size portions, then each user being assigned one portion. Since each user has a private frequency band, there is no interference between users.

It is not efficient to divide into fixed number of chunks. Now let us divide the single channel into N independent subchannels, each with capacity C/N bps. The mean input rate on each of the subchannels will now be λ/N.

$$T_{FDM} = \frac{1}{\mu\left(\frac{C}{N}\right) - (\frac{\lambda}{N})} = \frac{N}{\mu C - \lambda} = NT$$

Where,

T = mean time delay,

C = capacity of channel,

λ = arrival rate of frames,

1/μ = bits/frame,

N = number of sub channels,

T_{FDM} = Frequency Division Multiplexing Time

- Advantage : FDM is a simple and efficient allocation mechanism.
- Disadvantage : Waste of resources when the traffic is bursty, or the channel is lightly loaded

2.2.2. Dynamic Channel allocation

In dynamic channel allocation schemes, frequency channels are not permanently allotted to any user. Channels are assigned to the user as needed depending upon the network environment. The five key assumptions in dynamic channel allocation are:

1. ***Station Model*** : The model consists of *N* independent stations (terminals such as computers, telephones or persona communicators) each with a program or user that generates frames for transmission. Once a frame has been generated, the station is blocked and does nothing until the frame has been successfully transmitted.
2. ***Single Channel Assumption***: A single channel is available for communication. All stations can send or receive on the channel. All stations are equivalent, although protocol software may assign priorities to them.
3. ***Collision Assumption***: If two frames are transmitted simultaneously, they overlap. This event is called a collision. All stations can detect collisions.
    - A collided frame must be retransmitted. There are no errors other than those generated by collisions.
4. ***Transmission time division***
    a. *Continuous Time*: Frame transmission can begin at any instant. There is no master clock dividing time into discrete intervals.

    b. *Slotted Time*: Time is divided into discrete intervals (slots). Frame transmissions always begin at the start of a slot. A slot may contain 0, 1, or more frames, corresponding to an idle slot, a successful transmission, or a collision, respectively.
5. ***Carrier Sense***
    a. *With carrier sense* : Stations can tell if the channel is in use before trying to use it. If the channel is sensed as busy, no station will attempt to use it until it goes idle.

    b. *No Carrier Sense*. Stations cannot sense the channel before trying to use it. They just go ahead and transmit. Only later can they determine whether the transmission was successful.

- ***Advantages***
    - ✓ Dynamic channel allocation schemes allot channels as needed. This results in optimum utilization of network resources.
    - ✓ There are less chances of denial of services and call blocking in case of voice transmission.
    - ✓ These schemes adjust bandwidth allotment according to traffic volume, and so are particularly suitable for bursty traffic.
- ***Disadvantages***
    - ✓ Dynamic channel allocation schemes increase the computational as well as storage load on the system.

2.3. Multiple Access Protocol

The data can be transmitted between the sender and receiver using a communication link. The data communication can be done at any time without any collision by establishing a dedicated link between the sender and receiver. If we provide the dedicated link, the world is full of communication medium and not possible to create a dedicated link for any sender to any receiver. To avoid this problem, multiple users are allowed to access the single communication medium. By allowing multi user access, two or more users can try to access the communication medium at the same time. It leads to collision in the communication medium.

Hence the data link layer provides algorithm to share the communication medium and called as multiple access protocol. It means, a protocol allows multiple users to access a communication medium. The *Figure 2.9* illustrates the different categories of multiple access protocol used in data link layer.

In this chapter, we are studying random access protocols such as Aloha, CSMA, CSMA/CD, CSMA/CA.

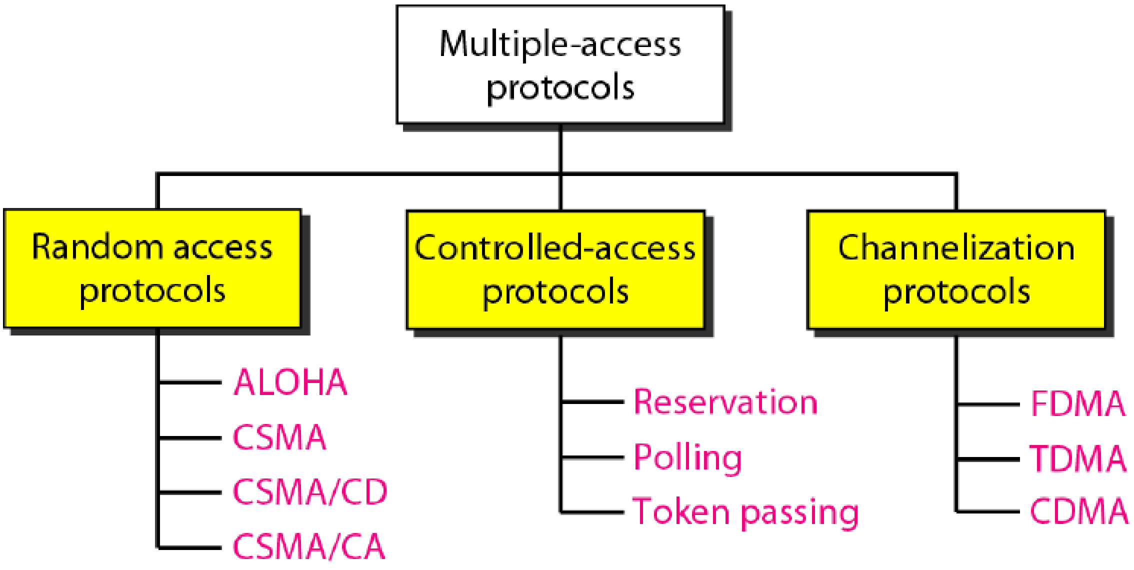


Figure 2.9 Types of Multiple Access Protocol

2.3.1. ALOHA

ALOHA is a system proposed for solving the channel allocation problem. It is used for ground-based radio broadcasting. The basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel. there are two versions of ALOHA:

a) Pure ALOHA
b) Slotted ALOHA

The basic difference with respect to timing is synchronization. The Pure ALOHA does not require global time synchronization, but, the Slotted ALOHA requires time synchronization.

a) *Pure ALOHA*

The pure ALOHA system is working as follows:

- ✓ let users transmit whenever they have data to be sent.
- ✓ expected collisions will occur.
- ✓ the collided frames will be destroyed.
- ✓ using a feedback mechanism to know about the status of frame.
- ✓ If the frame was destroyed, the sender just waits a random amount of time.
- ✓ retransmit the destroyed frame.

The waiting time must be random or the same frames will collide over and over, in lockstep. Systems in which multiple users share a common channel in a way that can lead to conflicts are widely known as contention systems.

A sketch of frame generation in a pure ALOHA and slotted ALOHA system is given in *Figure 2.10*.a.

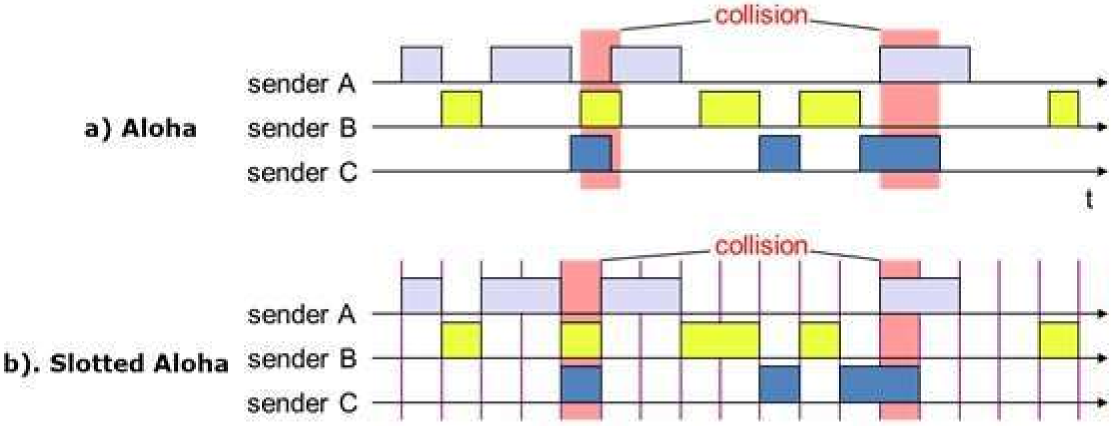


Figure 2.10 Aloha System for frame transmission

Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be garbled. Even the first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted later.

- **Vulnerable time**

Let us find the length of time, the vulnerable time, in which there is a possibility of collision.

$$\text{Pure ALOHA vulnerable time} = 2 \times T_{fr}$$

Where T_{fr} is the frame transmission time.

- **Throughput**

Let us call G the average number of frames generated by the system during one frame transmission time.

The throughput for pure ALOHA is $S = G \times e^{-2G}$.

The maximum throughput $S_{max} = 0.184$ when $G = (1/2)$.

b) Slotted Aloha

In slotted ALOHA, we divide the time into equal size slots and force the station to send only at the beginning of the time slot. The *Figure 2.10*.b shows the example of collision and successful transmission frame in slotted aloha.

Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame.

Slotted ALOHA vulnerable time = T_{fr}
The throughput for slotted ALOHA is $S =: G \times e^{-G}$.
The maximum throughput $S_{max} == 0.368$ when $G=1$.

The efficiency of pure ALOHA and slotted ALOHA is shown in Figure 2.11. The maximum throughput of pure ALOHA is 18% and slotted ALOHA is 37%.

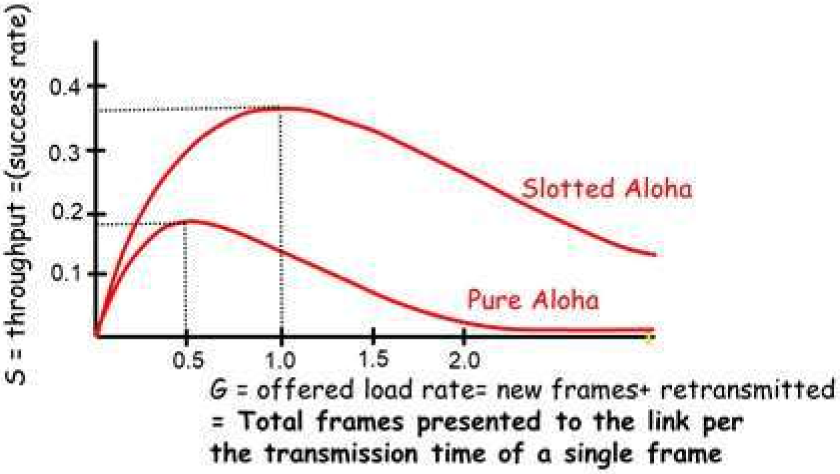


Figure 2.11. Efficiency of ALOHA methods

2.3.2. Carrier Sense Multiple Access (CSMA)

The CSMA protocol was developed to reduce the collision in multiple access. It is done by sensing the channel before transmitting by a station. If the channel is free, then the station can transmit; otherwise, the station must wait. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

Even the CSMA reduces the collision, but it cannot eliminate the collision. The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it. The vulnerable time for CSMA is the propagation time Tp.

- **Persistence Methods**

The persistence methods are used to reduce the collisions and follows CSMA scheme. What should a station do if the channel is busy? What should a station do if the channel is idle? Three methods have been devised to answer these questions:

a) 1-persistent method,
b) nonpersistent method,
c) p-persistent method.

a). 1-persistent method

In this method, a station wishing to transmit listens to the medium and obeys the following rules (shown in *Figure 2.12*):

1. If the medium is idle, transmit; otherwise, go to step 2.
2. If the medium is busy, continue to listen until the channel is sensed idle; then transmit immediately.

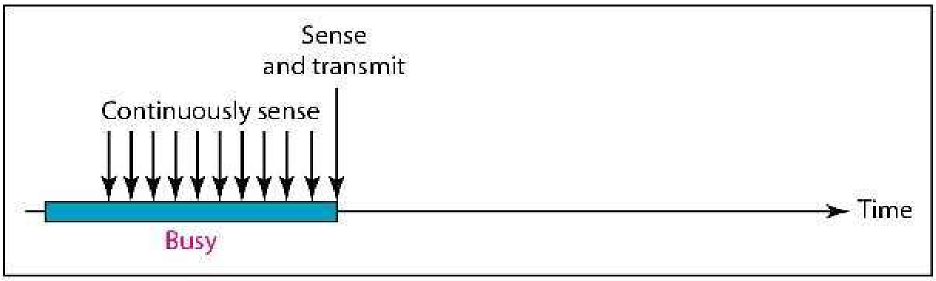


Figure 2.12. 1-Persistence Scheme

- Performance

The 1-persistent stations are selfish. If two or more stations becomes ready at the same time, collision guaranteed.

b). Nonpersistent method

In nonpersistent method, A station with frames to be sent, should sense the medium and do the follows (shown in Figure 2.13);

1. If medium is idle, transmit; otherwise, go to 2
2. If medium is busy, (backoff) wait a random amount of time and repeat 1.

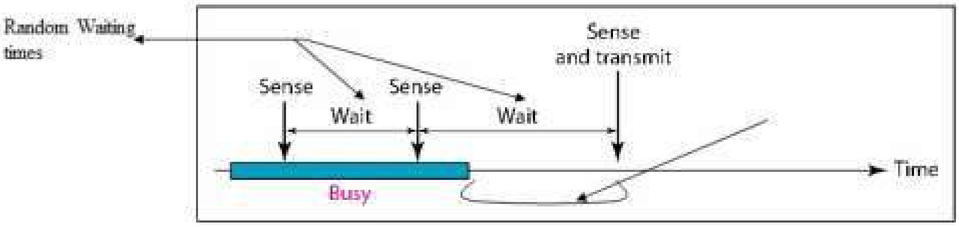


Figure 2.13 Non-persistent Scheme

- Performance
  - ✓ Non-persistent Stations are deferential (respect others).
  - ✓ Random delays reduce probability of collisions because two stations with data to be transmitted will wait for different amount of times.
  - ✓ Bandwidth is wasted if waiting time (backoff) is large because medium will remain idle following end of transmission even if one or more stations have frames to send

c). p-persistent method

Time is divided to slots where each Time unit (slot) typically equals maximum propagation delay. In p-persistent method (shown in Figure 2.14), if a station wishing to transmit listens to the medium, it follows the following steps:

1. If medium idle,
   - ✓ transmit with probability (p), OR
   - ✓ wait one-time unit (slot) with probability (1 – p), then repeat 1.
2. If medium busy, continuously listen until idle and repeat step 1

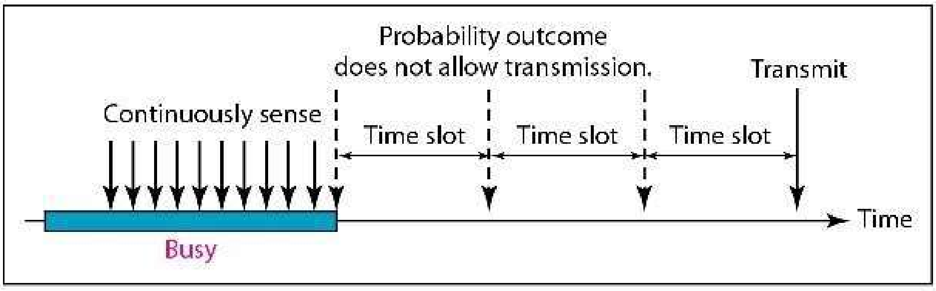


Figure 2.14. p-persistent scheme

- Performance
  - ✓ Reduces the possibility of collisions like nonpersistent.
  - ✓ Reduces channel idle time like 1-persistent.

2.3.3. Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. CSMA/CD (CSMA with Collision Detection) is widely used on LANs in the MAC sublayer. In particular, it is the basis of the popular Ethernet LAN.

CSMA/CD\uses the conceptual model of *Figure 2.15*. At the point marked t_0, a station has finished transmitting its frame. Any other station having a frame to send may now attempt to do so. If two or more stations decide to transmit simultaneously, there will be a collision. Collisions can be detected by looking at the power or pulse width of the received signal and comparing it to the transmitted signal.

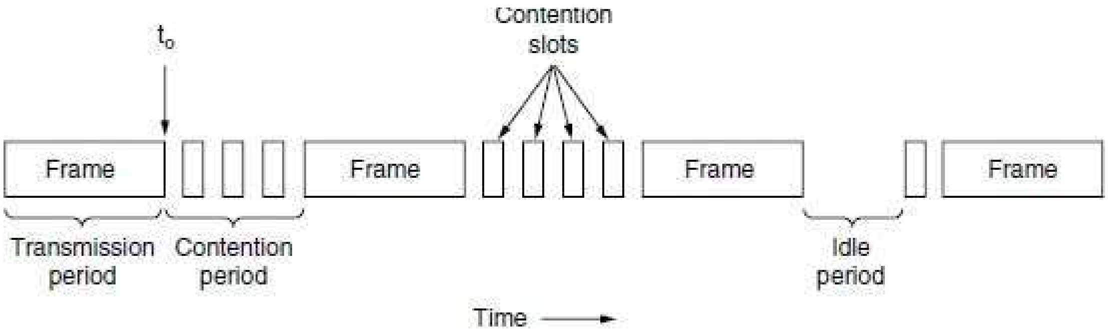


Figure 2.15 Transmission, Contention and idle states of CSMA/CD

The collision detection technology detects collisions by sensing transmissions from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission.

- **Algorithms**

The algorithm of CSMA/CD is:

1. When a frame is ready, the transmitting station checks whether the channel is idle or busy.
2. If the channel is busy, the station waits until the channel becomes idle.
3. If the channel is idle, the station starts transmitting and continually monitors the channel to detect collision.
4. If a collision is detected, the station starts the collision resolution algorithm.
5. The station resets the retransmission counters and completes frame transmission.

The algorithm of Collision Resolution is:

1. The station continues transmission of the current frame for a specified time along with a jam signal, to ensure that all the other stations detect collision.

   The jam signal is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations that they must not transmit.
2. The station increments the retransmission counter.
3. If the maximum number of retransmission attempts is reached, then the station aborts transmission.
4. Otherwise, the station waits for a backoff period which is generally a function of the number of collisions and restart main algorithm.

Though the CSMA/CD algorithm detects collisions, it does not reduce the number of collisions. It is not appropriate for large networks performance degrades exponentially when more stations are added.

2.4.Ethernet

Ethernet is a technology for connecting Local Area Networks. It is also known as IEEE 802.3. The architecture of Ethernet is shown in Figure 2.16.

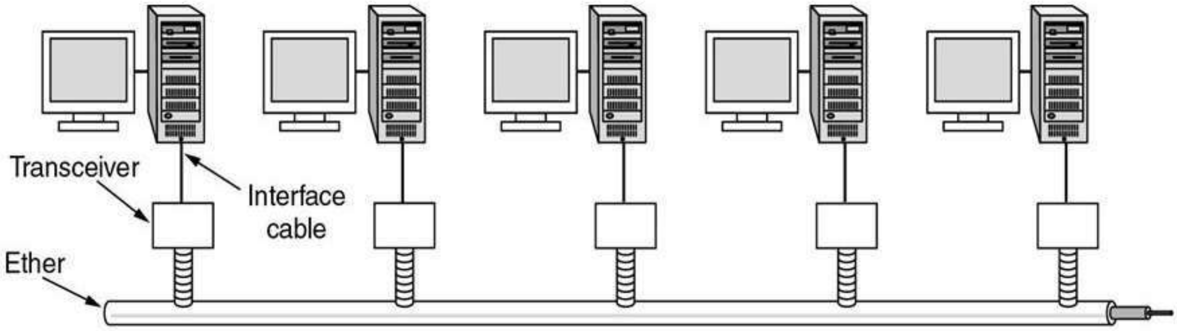


Figure 2.16. Architecture of Ethernet

Ethernet was the first Local Area Network (LAN) technology and remains the most important one. It was developed during the early 1970s by Xerox PARC. The original Ethernet enabled computers located within a few hundred yards of one another to exchange messages. By adding repeaters and bridges between multiple LANs, that distance has been extended to a few thousand yards. Thus, it is suitable for connecting the computers in a building or campus.

Ethernet architecture is based on the concept of connecting multiple computers to a long cable, sometimes called the ***ether***, thereby forming a bus structure. Each computer is fitted with an Ethernet adapter that includes a unique 48-bit address for that computer. Each computer is joined to the ether through a ***transceiver*** that forms a logical "T." The transceiver receives Ethernet messages on the cable, looks at the address, and either passes the message to its computer, if the address matches, or transmits it down the cable, if the address does not match.

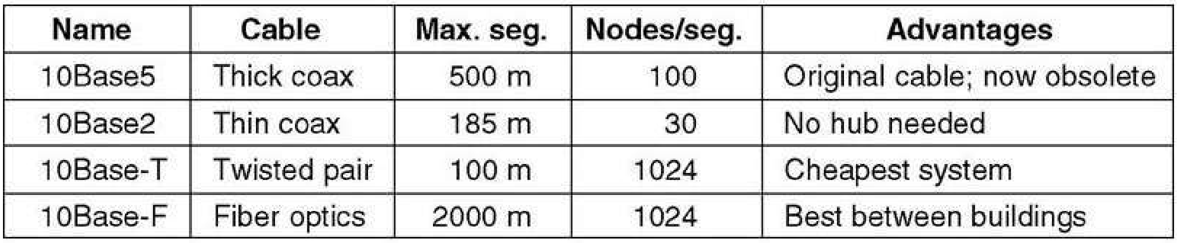
2.4.1. Ethernet Cabling

The name "Ethernet" refers to the cable (the ether). Four types of cabling are commonly used, as shown in Figure 2.17.

- **10Base5** is called thick Ethernet. Connections use vampire taps. The first number, 10, is the speed in Mbps. The word "Base" (or sometimes "BASE") to indicate baseband transmission and can support segments of up to 500 meters (for coaxial cable).
- **10Base2** is called thin Ethernet. Connections are done using T junctions. This is cheaper and easier to install. But it can run for only 185 meters per segment, each of which can handle only 30 machines.

Detecting cable breaks, excessive length, bad taps, or loose connectors can be a major problem with both media. For this reason, techniques have been developed to track them down. Basically, a pulse of known shape is injected into the cable. If the pulse hits an obstacle or the end of the cable, an echo will be generated and sent back. By carefully timing the interval between sending the pulse and receiving the echo, it is possible to localize the origin of the echo. This technique is called ***time domain reflectometry***.

- **10BaseT** uses twisted pair cable and a hub. All stations have a cable running to a central hub.



Name	Cable	Max. seg.	Nodes/seg.	Advantages
10Base5	Thick coax	500 m	100	Original cable; now obsolete
10Base2	Thin coax	185 m	30	No hub needed
10Base-T	Twisted pair	100 m	1024	Cheapest system
10Base-F	Fiber optics	2000 m	1024	Best between buildings

Figure 2.17 Most Common kinds of Ethernet Cabling

- **10BaseF** uses fiber optics. This type is expensive due to the cost of connectors and terminators. It offers good security since wiretapping fiber is difficult.

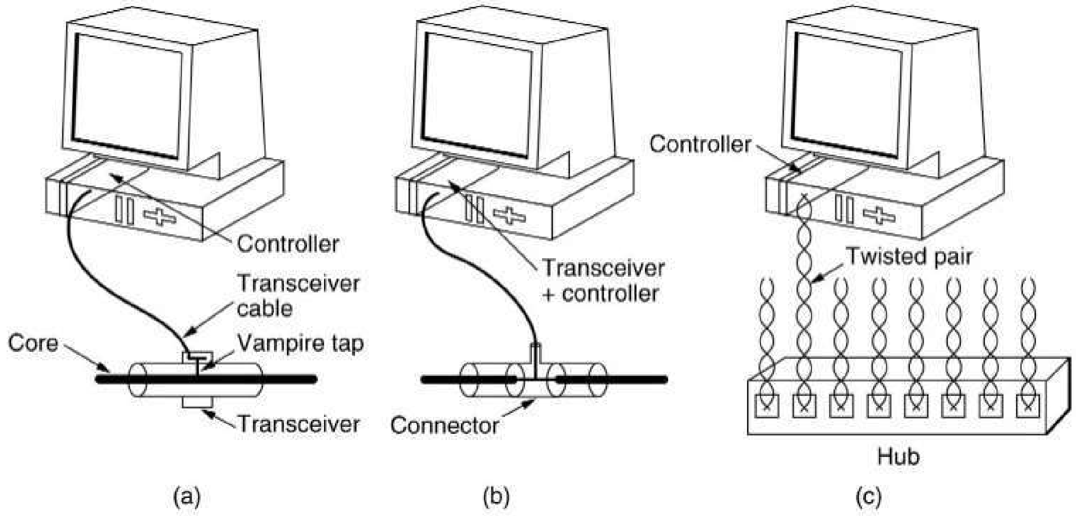


Figure 2.18. Three kinds of Ethernet cabling. (a) 10Base5. (b) 10Base2. (c) 10Base-T.

The major three wiring schemes are illustrated in Figure 2.18. For 10Base5, a transceiver is clamped securely around the cable so that its tap makes contact with the inner core. The transceiver contains the electronics that handle carrier detection and collision detection. When a collision is detected, the transceiver also puts a special invalid signal on the cable to ensure that all other transceivers also realize that a collision has occurred.

Different ways of wiring a building are shown in :

a. A single cable is snaked from room to room
b. A vertical spine runs from the basement to roof. Horizontal cables on each floor are connected to the spine.
c. Tree is the most general topology. Network with two paths between pairs of stations would suffer interference.
d. To allow large networks, multiple cables are connected by repeaters. A repeater received, amplifies and retransmits signals in both directions

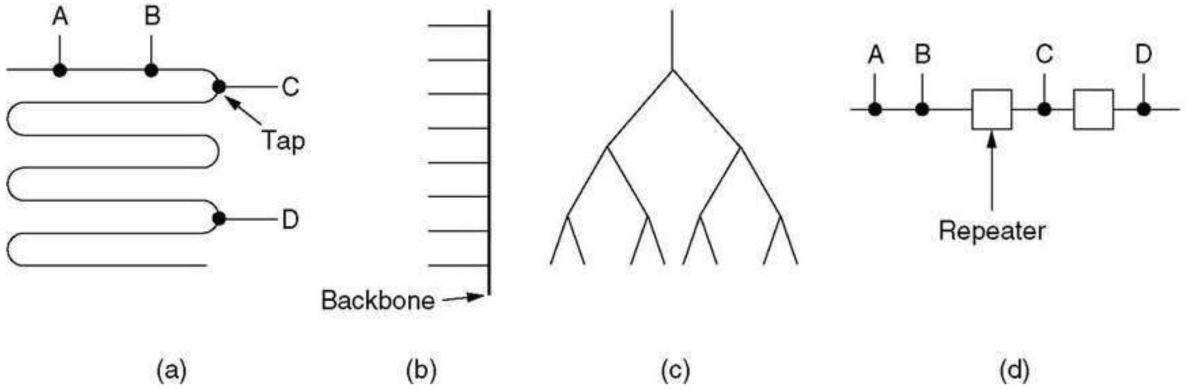


Figure 2.19 Cable topologies. (a) Linear. (b) Spine. (c) Tree. (d) Segmented

A ***repeater*** is a physical layer device. It receives, amplifies (regenerates), and retransmits signals in both directions. As far as the software is concerned, a series of cable segments connected by repeaters is no different from a single cable (except for some delay introduced by the repeaters). A system may contain multiple cable segments and multiple repeaters, but no two transceivers may be more than 2.5 km apart and no path between any two transceivers may traverse more than four repeaters.

2.4.2. Manchester Encoding

Binary encoding (Figure 2.20.a) uses only one voltage level, i.e positive voltage to represent binary 1 and zero voltage to represent binary 0. But, they cannot tell the difference between an idle sender (0 volts) and a 0 bit (0 volts). This problem can be solved by using +1 volts for a 1 and -1 volts for a 0. But still problem exists to identify the boundaries of bits, especially after a long run of consecutive 0s or a long run of consecutive 1s.

The above problem is solved in Manchester encoding and differential Manchester encoding. In Manchester encoding (Figure 2.20.b), a negative-to-positive transition represents bit 1 and a positive-to-negative transition represents binary 0.

In Differential Manchester (Figure 2.20.c), a transition means binary 0 and no transition means binary 1.

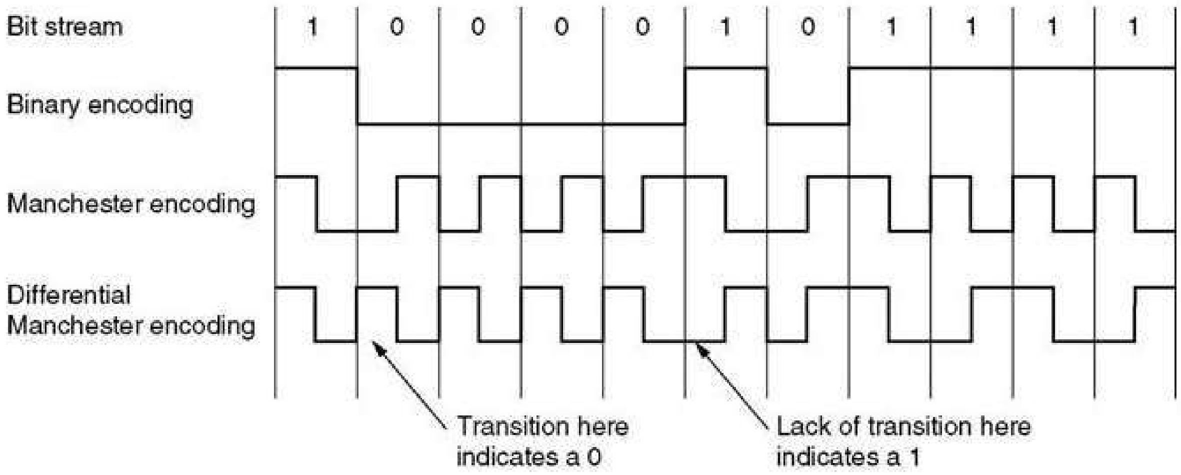

Bit stream
1
0
0
0
0
1
0
1
1
1
1
Binary encoding
Manchester encoding
Differential Manchester encoding
Transition here indicates a 0
Lack of transition here indicates a 1

Figure 2.20 (a) Binary encoding. (b) Manchester encoding. (c) Differential Manchester encoding.

2.4.3. The Ethernet MAC Sublayer Protocol

a). DIX (DEC, Intel, Xerox) frame structure

Each frame starts with a *Preamble* of 8 bytes. It is used to keep track of frame boundaries. The frame contains two addresses: *destination* and *source address*. The higher order bit of destination address is 0 for ordinary addresses and 1 for group addresses. When a frame is sent to group address, all stations in the group receive it. This is called *multicasting*. If the frame is received by all the stations it is called *broadcasting*.

Type field tells the receiver what to do with the frame, which process to give the frame to. Next come the *data*, up to 1500 bytes. If the data portion is less than 46 bytes, the *Pad* field is used to fill the remaining space. The final field is the *checksum*, to check if error has occurred.

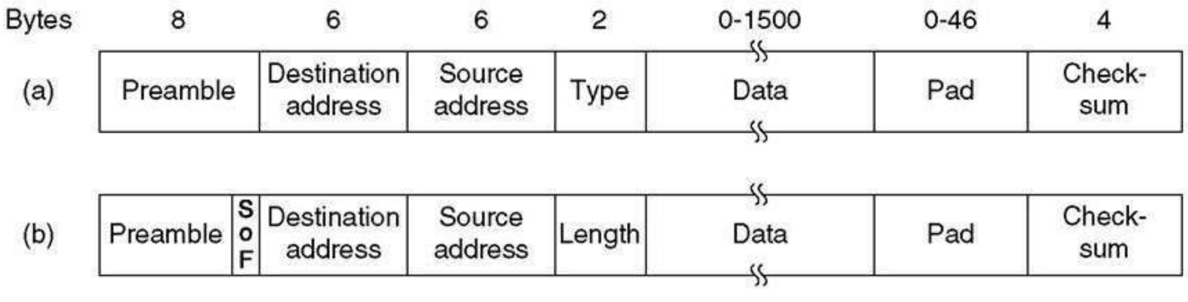


Figure 2.21Ethernet Frame formats. (a) DIX Ethernet. (b) IEEE 802.3.

b). IEEE 802.3 frame structure

The *Preamble* is only 7 bytes long, and the 8th byte is for *Start of Frame* (SoF). The *Type* field is changed to *Length* field and the other fields remain the same as in DIX Ethernet frame format.

2.4.4. Binary Exponential Backoff Algorithm

After the first collision, each station waits either 0 or 1 slot times before trying again. If two stations collide, and each picks the same random number, they will collide again. After second collision, the station picks 0,1,2 or 3 at random, and waits for that number of slots. In general, the station waits at random from interval 0 to $2^i - 1$. The randomization interval grows exponentially.

This algorithm, called binary exponential backoff, was chosen to adapt dynamically adapt to the number of stations trying to send. If few stations collide, this algorithm causes low delay. If many number of stations collide, the collision is resolved in a reasonable interval of time.

2.4.5. Switched Ethernet

As more and more stations are added to Ethernet, the traffic will go up To deal with increased load, Switched Ethernet is used. The heart of this system is a ***switch***, containing 4 to 32 plug-in line cards, each containing one to eight connectors. Each connector has a 10BaseT twisted pair connection to a host computer.

When a station wants to transmit a frame, it outputs the frame to the switch. The plug-in card checks if the destination is in the same card. If so, frame is copied there. If not, the frame is sent to the backplane to the destination's card. Collision detection is done using CSMA/CD. As in the Figure 2.22, the port can be connected to a single station or to a *hub*.

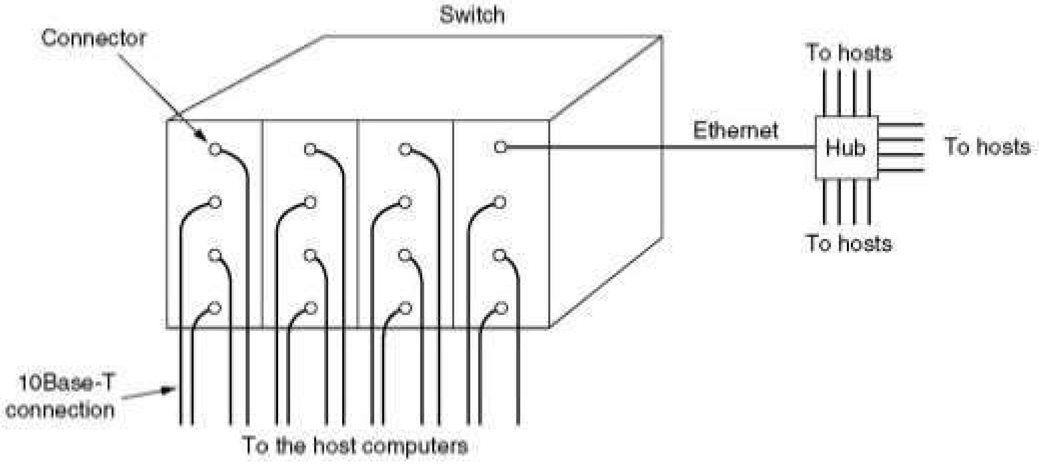


Figure 2.22 Simple Example of Switched Ethernet

2.4.6. Fast Ethernet

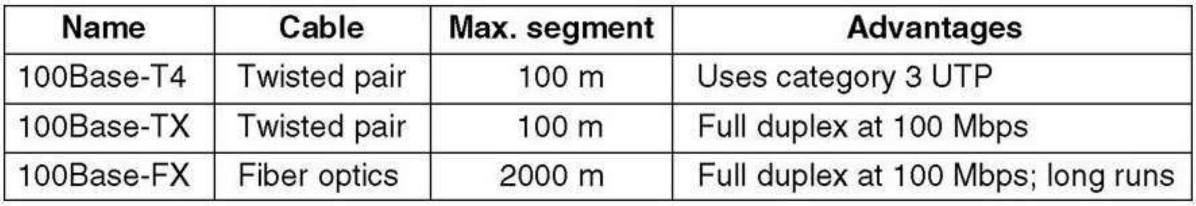
Fast Ethernet was designed to compete with LAN protocols such as FDDI or Fiber Channel (or Fibre Channel, as it is sometimes spelled). IEEE created Fast Ethernet under the name 802.3u. Fast Ethernet is backward-compatible with Standard Ethernet, but it can transmit data 10 times faster at a rate of 100 Mbps. The goals of Fast Ethernet can be summarized as follows:

1. Upgrade the data rate to 100 Mbps.

2. Make it compatible with Standard Ethernet.
3. Keep the same 48-bit address.
4. Keep the same frame format.
5. Keep the same minimum and maximum frame lengths.

It reduces the bit time from 100 nsec to 10 nsec. All Fast Ethernets use hubs and switches. Ethernet cabling used is as follows and shown in Figure 2.23:

- 100Base-T4, used a signaling speed of 25 MHz, only 25% faster than standard Ethernets. It uses category 3 cable.
- 100Base-T4 requires four twisted pairs. Of the four pairs, one is always to the hub, one is always from the hub, and the other two are switchable to the current transmission direction.
- 100Base-TX Ethernet design is simpler because the wires can handle clock rates of 125 MHz. Only two twisted pairs per station are used, one to the hub and one from it. The 100Base-TX system is full duplex Stations can transmit at 100 Mbps on one twisted pair and receive at 100 Mbps on another twisted pair at the same time.
- 100Base-FX, uses two strands of multimode fiber, one for each direction, so it, too, can run full duplex with 100 Mbps in each direction. In this setup, the distance between a station and the switch can be up to 2 km.



Name	Cable	Max. segment	Advantages
100Base-T4	Twisted pair	100 m	Uses category 3 UTP
100Base-TX	Twisted pair	100 m	Full duplex at 100 Mbps
100Base-FX	Fiber optics	2000 m	Full duplex at 100 Mbps; long runs

Figure 2.23 The original fast Ethernet cabling

2.4.7. Gigabit Ethernet

All configurations of Gigabit Ethernet (IEEE 802.3z) use point-to-point links. The need for an even higher data rate resulted in the design of the Gigabit Ethernet protocol (1000 Mbps). The IEEE committee calls the Standard 802.3z. The goals of the Gigabit Ethernet design can be summarized as follows:

1. Upgrade the data rate to 1 Gbps.
2. Make it compatible with Standard or Fast Ethernet.
3. Use the same 48-bit address.
4. Use the same frame format.
5. Keep the same minimum and maximum frame lengths.
6. To support auto-negotiation as defined in Fast Ethernet.

In the simplest configuration, illustrated in Figure 2.24(a), two computers are directly connected to each other. The more common case, however, uses a switch or a hub connected to multiple computers and possibly additional switches or hubs, as shown in Figure 2.24(b).

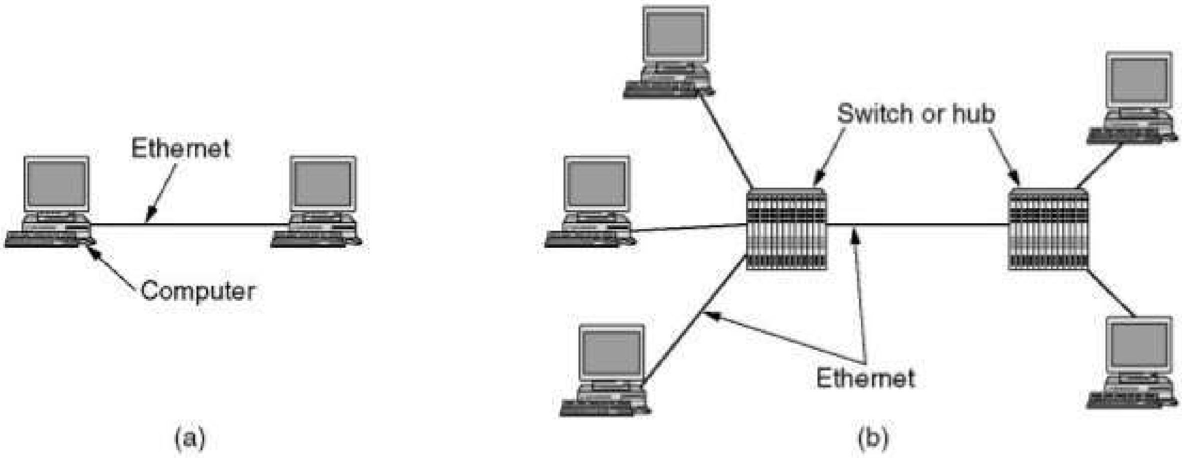


Figure 2.24 (a) A two-station Ethernet. (b) A multistation Ethernet

In both configurations, each individual Ethernet cable has exactly two devices on it, no more and no fewer. Gigabit Ethernet supports two different modes of operation: full-duplex mode and half-duplex mode.

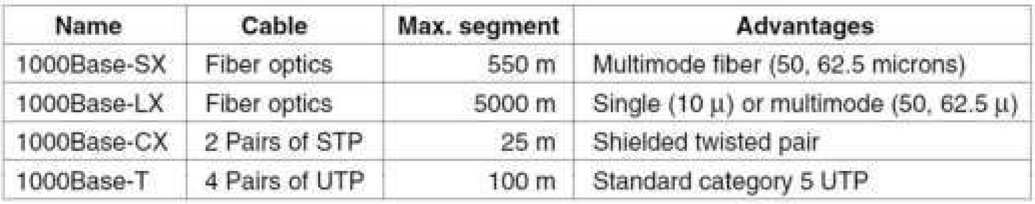
The ‘‘normal’’ mode is *full duplex* mode, which allows traffic in both directions at the same time. This mode is used when there is a central switch connected to computers (or other switches) on the periphery.

The other mode of operation, *half-duplex*, is used when the computers are connected to a hub rather than a switch. In this mode, collisions are possible, so the standard CSMA/CD protocol is required.

Gigabit Ethernet has two main features:

- The first feature, called carrier extension, essentially tells the hardware to add its own padding after the normal frame to extend the frame to 512 bytes.
- Since the second feature, called frame bursting, allows a sender to transmit a concatenated sequence of multiple frames in a single transmission

Gigabit Ethernet cabling is shown in Figure 2.25.



Name	Cable	Max. segment	Advantages
1000Base-SX	Fiber optics	550 m	Multimode fiber (50, 62.5 microns)
1000Base-LX	Fiber optics	5000 m	Single (10 μ) or multimode (50, 62.5 μ)
1000Base-CX	2 Pairs of STP	25 m	Shielded twisted pair
1000Base-T	4 Pairs of UTP	100 m	Standard category 5 UTP

Figure 2.25 Original Gigabit Ethernet cabling

Gigabit Ethernet supports both copper and fiber cabling. To support 1Gbps, lasers are required as light source. Two wavelengths are permitted: 0.85 microns (Short) and 1.3 microns (Long). Lasers at 0.85 microns are cheaper but do not work on single-mode fiber.

Three fiber diameters are permitted: 10, 50, and 62.5 microns. The first is for single mode and the last two are for multimode.

2.4.8. IEEE 802.2: Logical Link Control

It hides the differences between the various kinds of 802 networks by providing a single format and interface to the network layer. LLC forms the upper half of the data link layer, with the MAC sublayer below it, as shown in Figure 2.26.

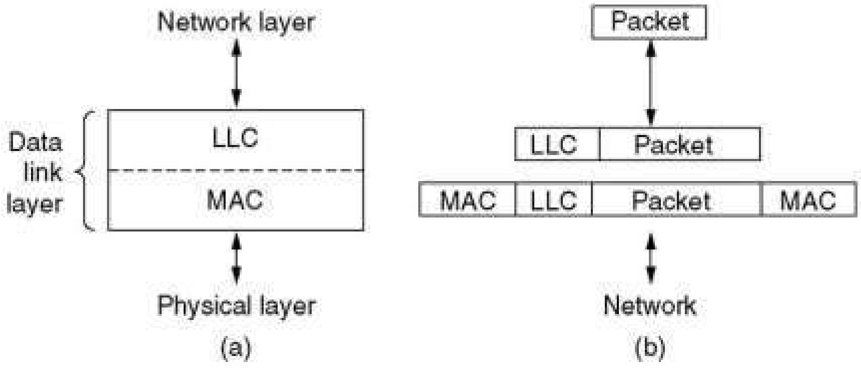


Figure 2.26 (a) Position of LLC. (b) Protocol formats

Network layer passes the packet to LLC. LLC adds an LLC header containing sequence and acknowledgement numbers. The header is attached to the payload. At the receiver, the reverse process takes place.

LLC provides three service options: a) Unreliable datagram service b)Acknowledged datagram service c)Reliable connection-oriented service. The LLC header has three fields: destination and source access points, and a control field. The control field contains sequence and acknowledgement numbers.

2.4.9. Retrospective on Ethernet

- ✓ Ethernet is simple and flexible.
- ✓ Ethernet is reliable, cheap, and easy to maintain.
- ✓ Thin Ethernet and twisted-pair wiring are relatively inexpensive
- ✓ Ethernet is easy to maintain.
- ✓ There is no software to install (other than the drivers) and not much in the way of configuration tables to manage.
- ✓ Adding new hosts is as simple as just plugging them in.
- ✓ Ethernet interworks easily with TCP/IPIP is a connectionless protocol, so it fits perfectly with Ethernet, which is also connectionless.
- ✓ Ethernet has been able to evolve in certain crucial ways.
- ✓ Speeds have gone up by several orders of magnitude; hubs and switches have been introduced.

- ✓ But these changes have not required changing the software and have often allowed the existing cabling to be reused for a time.

2.5.Wireless LAN

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless distribution method to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc. This gives users the ability to move around within the area and yet still be connected to the network (*Figure 2.27*).

Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name. Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their employees and customers.

- **Advantages of Wireless LANs**
  - ✓ ***Flexibility***: Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).
  - ✓ ***Planning***: Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.

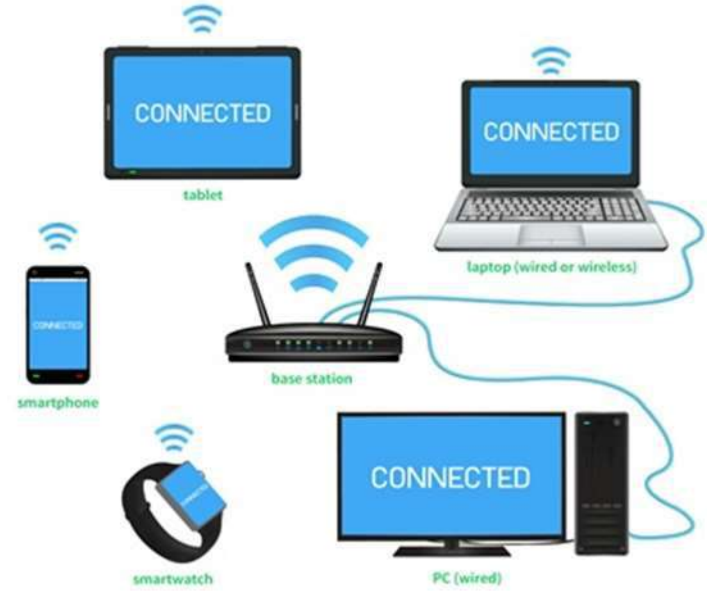


Figure 2.27 Example of Wireless Lan

  - ✓ ***Design***: Wireless networks allow for the design of independent, small devices which can for example be put into a pocket. Cables not only restrict users but also designers of small notepads, PDAs, etc.

- ✓ ***Robustness***: Wireless networks can handle disasters, e.g., earthquakes, flood etc. whereas, networks requiring a wired infrastructure will usually break down completely in disasters.
- ✓ ***Cost***: The cost of installing and maintaining a wireless LAN is on average lower than the cost of installing and maintaining a traditional wired LAN, for two reasons.
- ✓ ***Ease of Use***: Wireless LAN is easy to use and the users need very little new information to take advantage of WLANs.

- **Disadvantages of wireless LANs**
  - ✓ ***Quality of Services***: Quality of wireless LAN is typically lower than wired networks. The main reason for this is the lower bandwidth due to limitations is radio transmission, higher error rates due to interference and higher delay/delay variation due to extensive error correction and detection mechanisms.
  - ✓ ***Proprietary Solutions***: Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardization functionality plus many enhanced features. Most components today adhere to the basic standards IEEE 802.11a or 802.11b.
  - ✓ ***Restrictions***: Several govt. and non-govt. institutions world-wide regulate the operation and restrict frequencies to minimize interference.
  - ✓ ***Global operation***: Wireless LAN products are sold in all countries so, national and international frequency regulations have to be considered.
  - ✓ ***Low Power***: Devices communicating via a wireless LAN are typically power consuming, also wireless devices running on battery power. Whereas the LAN design should take this into account and implement special power saving modes and power management functions.
  - ✓ ***License free operation***: LAN operators don't want to apply for a special license to be able to use the product. The equipment must operate in a license free band, such as the 2.4 GHz ISM band.
  - ✓ ***Robust transmission technology***: If wireless LAN uses radio transmission, many other electrical devices can interfere with them (such as vacuum cleaner, train engines, hair dryers, etc.). Wireless LAN transceivers cannot be adjusted for perfect transmission is a standard office or production environment.

2.5.1. The 802.11 Protocol Stack

The protocols used by all the 802 variants, including Ethernet, have a certain commonality of structure. A partial view of the 802.11 protocol stack is given in .*Figure 2.28.*

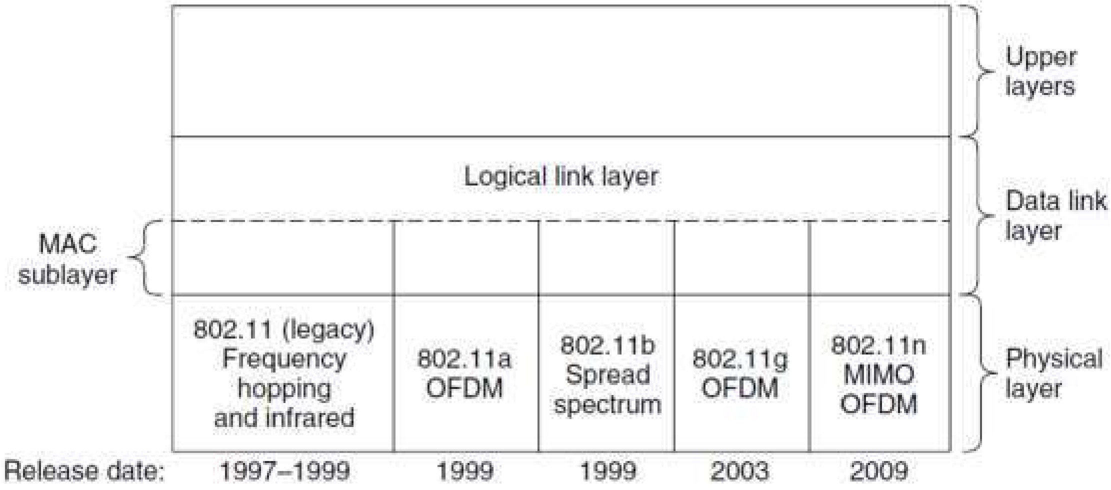


Figure 2.28 Protocol stack of 802.11

1. Physical Layer

The physical layer corresponds to the OSI physical layer fairly well. The following are the standards used in physical layer

- 802.11 Infrared (1997) – same technology as television remote controls do.
- 802.11 FHSS (1997) – used Frequency Hopping Spread Spectrum
- 802.11 DSSS (1997) – used Direct Sequence Spread Spectrum
    - Both FHSS and DSS does not require licensing (the 2.4-GHz ISM band).
    - Operate at 1 or 2 Mbps and at low enough power that they do not conflict too much.
    - Example - Radio-controlled garage door openers, Cordless telephones and microwave ovens
- 802.11a OFDM (1999) – used Orthogonal Frequency Division Multiplexing technique and operate at up to 54 Mbps.
- 802.11b HR-DSSS (1999) – used High Rate DSSS technique and operate at up to 11 Mbps.
- 802.11g OFDM (2001) – used OFDM modulation, but, different frequency band from OFDM.

2. Data Link Layer (DLL)

the data link layer in all the 802 protocols is split into two or more sublayers. In 802.11, the MAC (Medium Access Control) sublayer determines how the channel is allocated, that is, who gets to transmit next. Above it is the LLC (Logical Link Control) sublayer, whose job it is to hide the differences between the different 802 variants and make them indistinguishable as far as the network layer is concerned.

2.5.2. The 802.11 Physical Layer

Each of the five permitted transmission techniques makes it possible to send a MAC frame from one station to another.

1. Infrared

- ✓ uses diffused (i.e., not line of sight) transmission at 0.85 or 0.95 microns.
- ✓ Two capacities 1 Mbps (4-bit encoding produced 16-bit codeword) or 2 Mbps (2-bit encoding produced 4-bit codeword).
- ✓ Range is 10 to 20 meters and cannot penetrate walls.
- ✓ Does not work outdoors.

2. FHSS

- ✓ The main issue is multipath fading.
- ✓ 79 non-overlapping channels, each 1 MHz wide at low end of 2.4 GHz ISM band.
- ✓ Same pseudo-random number generator used by all stations.
- ✓ Dwell time: min. time on channel before hopping (400msec).
- ✓ Its main disadvantage is its low bandwidth.

3. DSSS

- ✓ Spreads signal over entire spectrum using pseudo-random sequence (similar to CDMA).
- ✓ Each bit transmitted using an 11 chips Barker sequence, PSK at 1Mbaud.
- ✓ Operates at 1 or 2 Mbps.

4. OFDM

- ✓ Compatible with European HiperLan2.
- ✓ 54Mbps in wider 5.5 GHz band - transmission range is limited.
- ✓ Uses 52 FDM channels (48 for data; 4 for synchronization).
- ✓ Encoding is complex (PSM up to 18 Mbps and QAM above this capacity).
- ✓ E.g., at 54Mbps 216 data bits encoded into 288-bit symbols.
- ✓ More difficulty penetrating walls.

5. HR-DSSS

- ✓ 11a and 11b shows a split in the standards committee.
- ✓ 11b approved and hit the market before 11a.
- ✓ Up to 11 Mbps in 2.4 GHz band using 11 million chips/sec.
- ✓ Note in this bandwidth all these protocols have to deal with interference from microwave ovens, cordless phones and garage door openers.
- ✓ Range is 7 times greater than 11a.
- ✓ 11b and 11a are incompatible!!

2.5.3. The 802.11 MAC Sublayer Protocol

The 802.11 MAC sublayer provides an abstraction of the physical layer to the logical link control sublayer and upper layers of the OSI network. It is responsible for encapsulating frames and describing frame formats.

MAC layer provides functionality for several tasks like control medium access, can also offer support for roaming, authentication, and power conservation. The basic services provided by MAC are the mandatory asynchronous data service and an optional time-bounded service.

IEEE 802.11 defines two MAC sub-layers :

1. Distributed Coordination Function (DCF) - DCF uses CSMA/CD as access method as wireless LAN can't implement CSMA/CD. It only offers asynchronous service.
2. Point Coordination Function (PCF) - PCP is implemented on top of DCF and mostly used for time-service transmission. It uses a centralized, contention-free polling access method. It offers both asynchronous and time-bounded service.

- **Avoidance of Collisions by 802.11 MAC Sublayer**

In wireless systems, the method of collision detection does not work. It uses a protocol called carrier sense multiple access with collision avoidance (CSMA/CA).

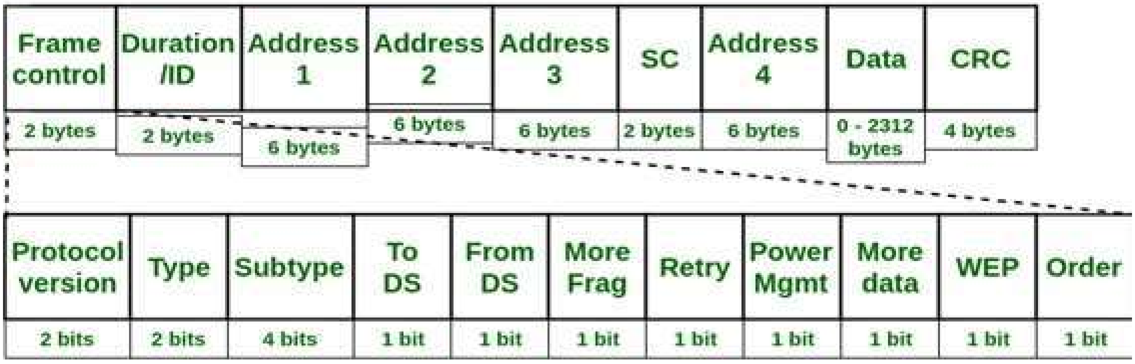
The method of CSMA/CA is

- ✓ When a frame is ready, the transmitting station checks whether the channel is idle or busy.
- ✓ If the channel is busy, the station waits until the channel becomes idle.
- ✓ If the channel is idle, the station waits for an Inter-frame gap (IFG) amount of time and then sends the frame.
- ✓ After sending the frame, it sets a timer.
- ✓ The station then waits for acknowledgement from the receiver. If it receives the acknowledgement before expiry of timer, it marks a successful transmission.
- ✓ Otherwise, it waits for a back-off time period and restarts the algorithm.

2.5.4. The 802.11 Frame Structure

The 802.11 standard defines three different classes of frames on the wire: data, control, and management. Each of these has a header with a variety of fields used within the MAC sublayer.

The MAC layer frame consists of 9 fields. The Figure 2.29 shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.



Frame control	Duration /ID	Address 1	Address 2	Address 3	SC	Address 4	Data	CRC
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 - 2312 bytes	4 bytes

Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

Figure 2.29 The 802.11 MAC Frame Structure

- ***Frame Control(FC)*** - It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:

  1) Version - It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.
  2) Type - It is a 2 bit long field which determines the function of frame i.e management(00), control(01) or data(10). The value 11 is reserved.
  3) Subtype - It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.
  4) To DS - It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).
  5) From DS - It is a 1 bit long field which when set indicates frame coming from DS.
  6) More frag (More fragments) - It is 1 bit long field which when set to 1 means frame is followed by other fragments.
  7) Retry -It is 1 bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
  8) Power Mgmt (Power management) - It is 1 bit long field which indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
  9) More data - It is 1 bit long field which is used to indicates a receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
  10) WEP - It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.

11) Order - It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

- ***Duration*** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgement occupy the channel.
- ***Address fields*** − There are three 6-byte address fields containing addresses of source, immediate destination and final endpoint respectively.
- ***Sequence*** − It a 2 bytes field that stores the frame numbers.
- ***Data*** − This is a variable sized field carries the data from the upper layers. The maximum size of data field is 2312 bytes.
- ***Check Sequence*** − It is a 4-byte field containing error detection information.

2.5.5. Services

The 802.11 standard defines the services that the clients, the access points, and the network connecting them must be a conformant wireless LAN. These services are divided into two categories: five distribution services and four station services. The distribution services relate to managing cell membership and interacting with stations outside the cell.

a. Distribution Services

The five distribution services are provided by the base stations and deal with station mobility as they enter and leave cells, attaching themselves to and detaching themselves from base stations. They are as follows.

1. ***Association***. This service is used by mobile stations to connect themselves to base stations. Typically, it is used just after a station moves within the radio range of the base station. Upon arrival, it announces its identity and capabilities. The capabilities include the data rates supported, need for PCF services (i.e., polling), and power management requirements. The base station may accept or reject the mobile station. If the mobile station is accepted, it must then authenticate itself.
2. ***Disassociation***. Either the station or the base station may disassociate, thus breaking the relationship. A station should use this service before shutting down or leaving, but the base station may also use it before going down for maintenance.
3. ***Reassociation***. A station may change its preferred base station using this service. This facility is useful for mobile stations moving from one cell to another. If it is used correctly, no data will be lost as a consequence of the handover. (But 802.11, like Ethernet, is just a best-efforts service.)
4. ***Distribution***. This service determines how to route frames sent to the base station. If the destination is local to the base station, the frames can be sent out directly over the air. Otherwise, they will have to be forwarded over the wired network.

5. ***Integration***. If a frame needs to be sent through a non-802.11 network with a different addressing scheme or frame format, this service handles the translation from the 802.11 format to the format required by the destination network.

b. Station Services

The remaining four services are intracell (i.e., relate to actions within a single cell). They are used after association has taken place and are as follows.

1. ***Authentication***. Because wireless communication can easily be sent or received by unauthorized stations, a station must authenticate itself before it is permitted to send data by challenge and response method. If the result is correct, the mobile is fully enrolled in the cell.
2. ***Deauthentication***. When a previously authenticated station wants to leave the network, it is deauthenticated. After deauthentication, it may no longer use the network.
3. ***Privacy***. For information sent over a wireless LAN to be kept confidential, it must be encrypted. This service manages the encryption and decryption. The encryption algorithm specified is RC4.
4. ***Data delivery***. Finally, data transmission is what it is all about, so 802.11 naturally provides a way to transmit and receive data. Transmission over 802.11 is not guaranteed to be reliable. Higher layers must deal with detecting and correcting errors.

2.6.IEEE 802.11 Architecture

The IEEE 802.11 standard defines the physical layer and media access control (MAC) layer for a wireless local area network. The standard defines three different physical layers for the 802.11 wireless LAN, each operating in a different frequency range and at rates of 1 Mbps and 2 Mbps.

2.6.1. Modes of Wireless LAN

802.11 networks can be used in two modes:

- Infrastructure mode
- Ad-hoc mode

- ***Infrastructure mode***

In infrastructure mode (Figure 2.30), each client is associated with an AP (Access Point) that is in turn connected to the other network. The client sends and receives its packets via the AP. Several access points may be connected together, typically by a wired network called a distribution system, to form an extended 802.11 network. In this case, clients can send frames to other clients via their APs.

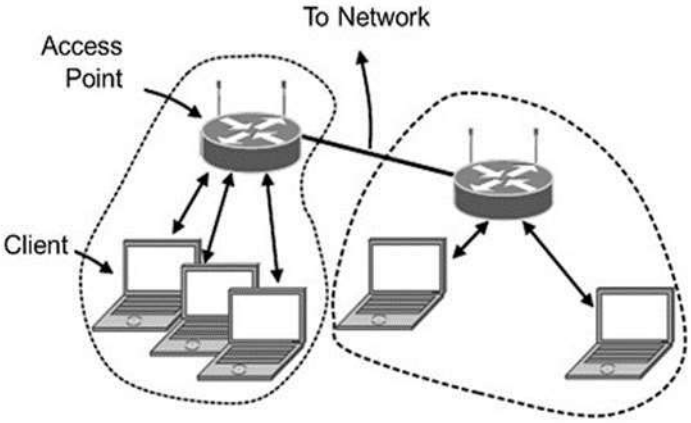


Figure 2.30 Infrastructure Mode

The most popular mode is to connect clients, such as laptops and smart phones, to another network, such as a company intranet or the Internet.

- ***Ad-hoc mode***

The other mode is an ad hoc network (Figure 2.31). This mode is a collection of computers that are associated so that they can directly send frames to each other. There is no access point. Since Internet access is the killer application for wireless, ad hoc networks are not very popular.

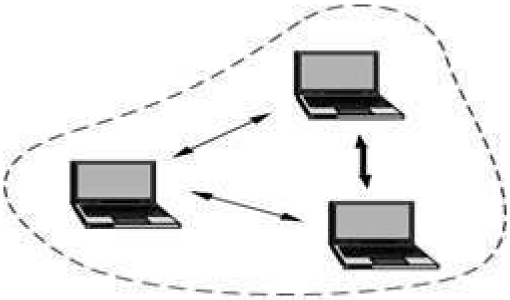


Figure 2.31 Ad-hoc Mode

2.6.2. Service Model

The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).

- ***Basic Service Set***

IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN. A basic service set is made of stationary or mobile wireless stations and an optional central base station, known as the access point (AP). Figure 2.32 shows two sets in this standard.

The BSS without an AP is a stand-alone network and cannot send data to other BSSs. It is called an ad hoc architecture. In this architecture, stations can form a network without the need of an AP; they can locate one another and agree to be part of a BSS. A BSS with an AP is sometimes referred to as an infrastructure network.

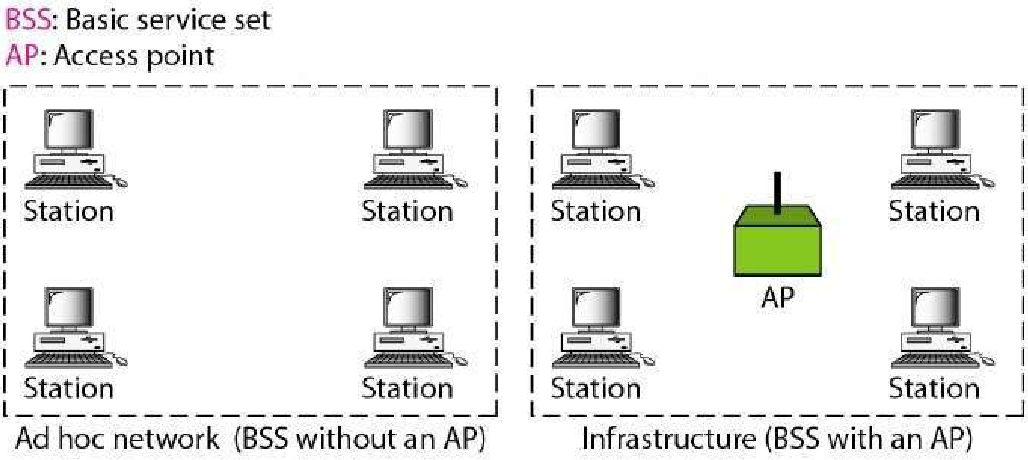


Figure 2.32 Basic Service Set

Extended Service Set

An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distribution system, which is usually a wired LAN. The distribution system connects the APs in the BSSs. IEEE 802.11 does not restrict the distribution system; it can be any IEEE LAN such as an Ethernet. Note that the extended service set uses two types of stations: mobile and stationary. The mobile stations are normal stations inside a BSS. The stationary stations are AP stations that are part of a wired LAN. Figure 2.33 shows an ESS.

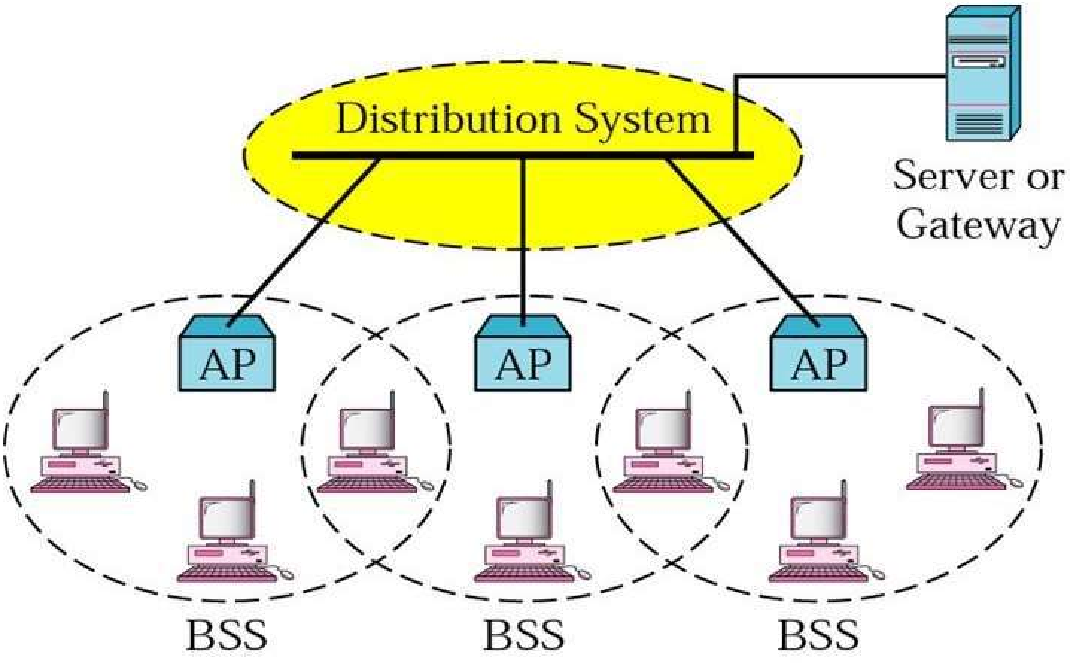


Figure 2.33 Extended Service Set

When BSSs are connected, the stations within reach of one another can communicate without the use of an AP. However, communication between two stations in two different BSSs usually occurs via two APs. The idea is similar to communication in a cellular network if we consider each BSS to be a cell and each AP to be a base station. Note that a mobile station can belong to more than one BSS at the same time.

2.7. Short Questions and Answers

1. What is meant by Data Link Layer(DLL)?

The Data Link Layer is the second layer in the OSI model, above the Physical Layer, which ensures that the error free data is transferred between the adjacent nodes in the network.

2. What are the functions included in Data Link Layer in Design Issues?

   - Providing a well-defined service interface to the network layer.
   - Dealing with transmission errors.
   - Regulating the flow of data so that slow receivers are not swamped by fast senders –flow control.

3. What are all the functions in data link control include?

   (1) Framing.
   (2) Error Control.
   (3) Flow Control.

4. What **is** Framing**?**

It breaks the datagram passed down by above layers and converts them into frames ready for transfer. This is called **Framing.**

5. What are the three distinct phases?

   1. Connection established
   2. Frames are transmitted
   3. Connection released

6. List out the framing Methods

   1. Character count.
   2. Flag bytes with byte stuffing.
   3. Starting and ending flags, with bit stuffing.
   4. Physical layer coding violations.

7. What is Fixed Size Framing?

In fixed-size framing, there is no need for defining the boundaries of the frames. The size itself can be used as a delimiter.

8. Define Character Stuffing?

In byte stuffing (or character stuffing), a special byte is added to the data section of the frame when there is a character with the same pattern as the flag. The data section is stuffed with an extra byte. This byte is usually called the escape character (ESC), which has a predefined bit pattern. Whenever the receiver encounters the ESC character, it removes it from the data section and treats the next character as data, not a delimiting flag.

9. What is Bit Stuffing?

Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.

10. What is error Control?

Having solved the problem of marking the start and end of each frame and how to make sure all frames are eventually delivered to the network layer at the destination and in the proper order.

11. Write any two disadvantage of Error Control

- If a frame vanishes, the receiver will not send an acknowledgement thus, sender will wait forever
- Sender transmits a frame , starts a Timer.

12. What are the approaches commonly used for Flow Control

  - feedback-based flow control
  - rate-based flow control

13. What is Network Interface card (NIC)?

A NIC is a component that provides networking capabilities for a computer. It may enable a wired connection (such as Ethernet)or a wireless connection(such as Wi-Fi) to a local area network.

14. How the network layer services have been designed?

a. The services should be independent of the router technology.

b. The transport layer should be shielded from the number, type, and topology of the routers present.

c. The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

15. Define Flow control.

Flow control is a technique that allows two stations working at different speeds to communicate with each other. It is a set of measures taken to regulate the amount of data that a sender sends so that a fast sender does not overwhelm a slow receiver.

16. What is meant by Channel Allocation?

A channel allocation is how to allocate a single broadcast channel among competing users. The allocation is divided into static and dynamic channel allocation.

17. Define static channel allocation.

In static channel allocation schemes, frequency channels are permanently allotted to any user.

18. Define dynamic channel allocation.

In dynamic channel allocation schemes, frequency channels are not permanently allotted to any user. Channels are assigned to the user as needed depending upon the network environment.

19. What is meant by Carrier Sense Multiple Access (CSMA)?

The CSMA protocol was developed to reduce the collision in multiple access. It is done by sensing the channel before transmitting by a station. If the channel is free, then the station can transmit; otherwise, the station must wait. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk."

20. What is Jam Signal?

The jam signal is a signal that carries a 32-bit binary pattern sent by a data station to inform the other stations that they must not transmit.

21. What is Multiple Access?

If the physical links are shared by more than two nodes, it is said to be Multiple Access.

22. Define Datagrams?

The packets are frequently called datagrams (in analogy with telegrams).

23. What is VC (virtual circuit)?

If connection-oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent. This connection is called a VC (virtual circuit):

24. What is Label Switching?

Avoiding conflicts of this kind is why routers need the ability to replace connection identifiers in outgoing packets. In some contexts, this is called label switching.

25. Define MPLS.

An example of a connection-oriented network service is MPLS (MultiProtocol Label Switching). It is used within ISP networks in the Internet, with IP packets wrapped in an MPLS header having a 20-bit connection identifier or label. MPLS is often hidden from customers, with the ISP establishing long-term connections for large amounts of traffic, but it is increasingly being used to help when quality of service is important but also with other ISP traffic management tasks.

26. What is mean by Ethernet?

Ethernet is a networking technology developed in 1970 which is governed by the IEEE 802.3 specifications. Ethernet is a Technology for connecting Local Area Networks.

27. Write the advantages of Ethernet.

1. Inexpensive 2. Easy to install 3.Supports various writing technologies.

28. What are the types of cabling?

Ethernet uses four types of cabling

- 10Base5 Thick coax
- 10Base2 Thin coax
- 10Base-T Twisted pair
- 10Base-F Fiber optics

29. What are the types of Ethernet?

There are several types of Ethernet networks, such as Fast Ethernet, Gigabit Ethernet, and Switched Ethernet.

30. Define Gigabit Ethernet?

Gigabit Ethernet is a version of the Ethernet technology broadly used in local area networks (LANs) for transmitting Ethernet frames at 1 Gbps. It is used as a backbone in many networks, particularly those of large organizations. Gigabit Ethernet is an extension to the preceding 10 Mbps and 100 Mbps 802.3 Ethernet standards. It supports 1,000 Mbps bandwidth while maintaining full compatibility with the installed base of around 100 million Ethernet nodes.

31. What is meant by exponential back-off?

It is a retransmission strategy that doubles the timeout value each time, when a packet is retransmitted. Once an adaptor has detected a collision and stopped its transmission, it waits a certain amount of time and tries again. Each time it tries to transmit but if it fails again, then the adaptor doubles the amount of time. This strategy of doubling the delay interval between each retransmission attempt is a general technique known as exponential back-off.

32. What is Manchester encoding?

Manchester encoding is an algorithm used in computer networking to digitally encode data bits. With Manchester encoding, data bits are represented in a series of different stages, which occur in a logical sequence. A negative-to-positive transition represents bit 1 and a positive-to-negative transition represents binary 0.

33. What is fast Ethernet?

Fast Ethernet is one of the versions of the Ethernet standard that enables the transmission of data over 100 megabits per second on local area networks (LAN). It was the fastest network connection of its time. Fast Ethernet is also known as 100 Base X or 100 Mbps Ethernet.

34. What is Adhoc Network?

An ad hoc network is a network that is composed of individual devices communicating with each other directly. The term implies spontaneous or impromptu construction because these networks often bypass the gatekeeping hardware or central access point such as a router. Many ad hoc networks are local area networks where computers or other devices are enabled to send data directly to one another rather than going through a centralized access point.

35. What is the use of repeater?

A network device used to regenerate or replicate a signal. Repeaters are used in transmission systems to regenerate analog or digital signals distorted by transmission loss. Analog repeaters frequently can only amplify the signal while digital repeaters can reconstruct a signal to near its original quality. In a data network, a repeater can relay messages between sub networks that use different protocols or cable types. Hubs can operate as repeaters by relaying messages to all connected computers.

36. What is IEEE 802.11?

802.11 refers to a family of specifications developed by the IEEE for Wireless LAN (WLAN) technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

37. List the type of architecture used in IEEE 802.11.

The type of architecture used in IEEE 802.11

- Infrastructure based
- Ad-hoc based

38. List out the applications of WLAN.

- Transfer of medical images
- Remote access to patient records
- Remote monitoring of patients
- Remote diagnosis of patients at home or in an ambulance
- In telemedicine
- Surveillance
- Internet supporting database.

39. What are the functions of MAC layer in IEEE 802.11?

The functions of MAC layer are

- Media Access Control
- Reliable delivery of data units
- Management functions
- Authentication encryption

40. Why are ad hoc networks needed?

Ad hoc networking is often needed where an infrastructure network cannot be deployed and managed. The presence of dynamic and adaptive routing protocols enables quick formation of ad hoc networks and is suitable for emergency situations like natural disasters, spontaneous meetings or military conflicts.

41. Define the Basic Service Set(BSS).

A basic service set is a group of stations communicating at physical layer level.

42. What are the categories of BSS?

- Infrastructure BSS – Here, the devices communicate with other devices through access points.
- Independent BSS – Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

43. What is the Wireless Access Point(WAP)?

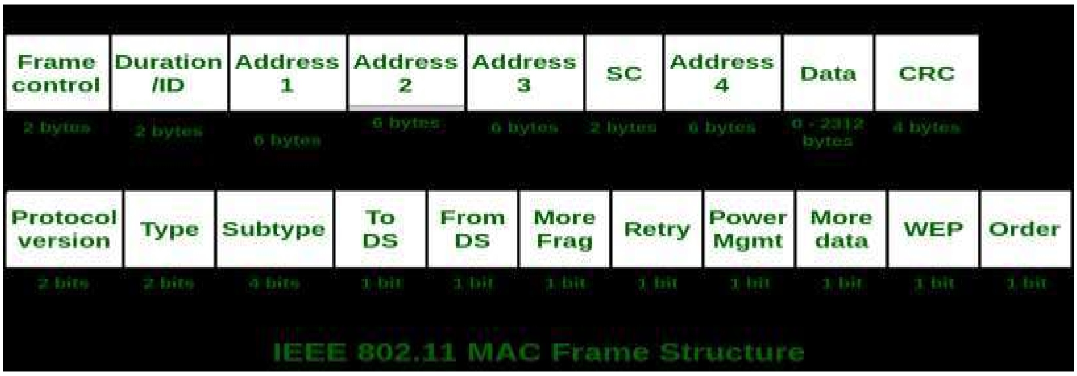
Wireless Access Points are generally wireless routers that form the base stations or access.

44. What are the services provided by IEEE 802.11?

- Association service is used by mobile stations to connect themselves to APs.
- Reassociation lets a station change its preferred AP. This facility is useful for mobile stations moving from one AP to another AP in the same extended 802.11 LAN.

45. Draw the MAC layer frame format of IEEE 802.11.

The MAC layer frame format of IEEE 802.11



Frame control	Duration /ID	Address 1	Address 2	Address 3	SC	Address 4	Data	CRC
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0 - 2312 bytes	4 bytes

Protocol version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More data	WEP	Order
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit	1 bit

IEEE 802.11 MAC Frame Structure

2.8.Explanatory Questions

1. Explain about various framing methods followed in data link layer (5 marks).
2. Discuss about error control and flow control (5 marks).
3. Explain Gigabit Ethernet (5 marks).
4. Explain Switched Ethernet (5 marks).
5. Explain Fast Ethernet (5 marks).
6. Write short notes on Pure and slotted ALOHA (5 marks).

7. Write short notes on persistent and non persistent CSMA protocols (5 marks).
8. Explain CSMA with collision detection protocol (5 marks).
9. Write short notes on (1) A bit map protocol (2) Binary countdown (5 marks)
10. Explain the MAC mechanism of IEEE 802.11 WLAN (5 marks).
11. Explain the 802.11 Mac Frame Structure (5 marks).
12. Explain the services defined by the 802.11 Standard (5 marks).
13. Explain the type of architecture used in IEEE 802.11 (5 marks).
14. Explain the 802.11 Physical layer (5 marks).
15. Discuss about data link layer design issues. (10 marks)
16. Write about channel allocation problem in detail. (10 marks)
17. Explain the Ethernet MAC Sub layer protocol. (10 marks)
18. Explain different multiple access protocol. (10 marks)
19. Discuss about various ethernet mechanism used in computer network. (10 marks)
20. Explain the Wireless LAN – 802.11 Architecture. (10 marks)

2.9. Objective Questions and Answers

1. Which among the following represents the objectives/requirements of Data Link Layer?

   a. Frame Synchronization
   b. Error & Flow Control
   c. Both a & b
   d. None of the above

   Answer: c. Both a & b

2. What are the frames issued by the secondary station of HDLC, known as?

   a. Link
   b. Command
   c. Response
   d. None of the above

   Answer: c. Response

3. Which one of the following tasks is not done by data link layer?

   a. framing
   b. error control
   c. flow control
   d. channel coding

   Answer: d. channel coding

4. Two main functions of data link layer are

   a. hardware link control and media access control

b. data link control and protocol access control
c. data link control and media access control
d. both a and c

Answer: c. data link control and media access control

5. Which of the following devices is a PC component that connects the computer to the network?

a. Bridge
b. NIC (Network Interface Card)
c. DNS Server
d. Gateway

Answer: b. NIC(Network Interface Card)

6. Switch is a Device of _________ Layer of OSI Model.

a. Network Layer
b. Data Link Layer
c. Application Layer
d. Session Layer

Answer: b. Data Link Layer

7. When 2 or more bits in a data unit has been changed during the transmission, the error is called

a. random error
b. burst error
c. inverted error
d. none of the mentioned

Answer: b. burst error

8. How the error detection is achieved at data link layer?

a. Hamming codes
b. Bit stuffing
c. Detection manager
d. None of the above

Answer: b. Bit Stuffing

9. Bridge works in which layer of the OSI model?

a. Application layer
b. Transport layer
c. Network layer
d. Data link layer

Answer: d .Data link layer.

10. HDLC is an acronym for _______.

a. High-duplex line communication
b. High-level data link control
c. Half-duplex digital link combination

d. Host double-level circuit

Answer: b. High-Level data link control

11. Data link control deals with the design and procedures for ______ communication.

a. node-to-node
b. host-to-host
c. process-to-process
d. none of the above

Answer: a. node-to-node

12. In _________ protocols, we use ________.

a. character-oriented; byte stuffing
b. character-oriented; bit stuffing
c. bit-oriented; character stuffing
d. none of the above

Answer: a . character-oriented; byte stuffing.

13. Byte stuffing means adding a special byte to the data section of the frame when there is a character with the same pattern as the ______.

a. Header
b. trailer
c. flag
d. none of the above

Answer: c. flag.

14. In fixed channel assignment strategy, each cell is allocated a predetermined set of ______

a. Voice channels
b. Control channels
c. Frequency
d. base stations

Answer : a

15. What happen to a call in fixed channel strategy, if all the channels in a cell are occupied?

a. Queued
b. Cross talk
c. Blocked
d. Delayed

Answer : c

16. What is a borrowing strategy in fixed channel assignments?

a. Borrowing channels from neighbouring cell
b. Borrowing channels from neighbouring cluster
c. Borrowing channels from same cell
d. Borrowing channels from other base station in same cell

Answer : a

17. In dynamic channel assignment strategy, voice channels are -------------- to different cells.
    a. Allocated Permanently
    b. Not Allocated Permanently
    c. Allocated time based
    d. Allocated frequency based

    Answer : b

18. In dynamic channel assignment strategy, base station requests channel from ______
    a. MSC
    b. Neighbouring cell
    c. Neighbouring cluster
    d. Neighbouring base station

    Answer : a

19. Lower sub layer of the data link layer is responsible for
    a. multiple access
    b. point to point access
    c. error detection
    d. flow control

    Answer : a

20. In ____________, each station sends a frame whenever it has a frame to send.
    a. Pure ALOHA
    b. Slotted ALOHA
    c. Both a and b
    d. Neither a nor b

    Answer : a

21. In pure ALOHA, the vulnerable time is ____________ the frame transmission time.
    a. The same as
    b. Two times
    c. Three times
    d. None of the above

    Answer : b

22. The maximum throughput for the pure ALOHA is
    a. 12.2
    b. 18.4
    c. 36.8
    d. 32.2

    Answer : b

23. In ____________, each station is forced to send only at beginning of the time slot
    a. Pure ALOHA
    b. Slotted ALOHA

c. Both a and b
d. Neither a nor b

Answer : b

24. In slotted ALOHA, the vulnerable time is ____________ the frame transmission time.

a. The same as
b. Two times
c. Three times
d. None of the above

Answer : a

25. The maximum throughput for the pure ALOHA is

a. 12.2
b. 18.4
c. 36.8
d. 32.2

Answer : c

26. In Carrier Sense Multiple Access (CSMA), if station senses medium before trying to use it then chance of collision can be

a. Increased
b. Reduced
c. Highlighted
d. Both B & **C**

Answer : b

27. Code Division Multiple Access (CDMA) differs from Time Division Multiple Access (TDMA) because there is no

a. bandwidth
b. link
c. carrier
d. timesharing

Answer : d

28. In Carrier Sense Multiple Access (CSMA), possibility of collision still exist because of

a. Propagation delay
b. sender-receiver delay
c. Sense delay
d. Transmit delay

Answer : a

29. Protocol that is used to transmit data without any schedule time is

a. random access
b. controlled access
c. channelization
d. none of the above

Answer : a

30. Carrier Sense Multiple Access (CSMA) is based on medium called

   a. Listen before talk
   b. Listen before sending
   c. Sense before transmit
   d. Sense before Collision

Answer : c

31. In ___________, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.

   a. CSMA/CA
   b. CSMA/CD
   c. MA
   d. None of the above

Answer : b

32. To avoid collision on wireless networks, _____________ was invented.

   a. CSMA/CA
   b. CSMA/CD
   c. MA
   d. None of the above

Answer : a

33. IEEE 802.11 defines basic service set as building block of a wireless

a) LAN

b) WAN protocol

c) MAN

d) All of the above

Answer: a

34. What is the access point (AP) in wireless LAN?

a) device that allows wireless devices to connect to a wired network
b) wireless devices itself
c) both device that allows wireless devices to connect to a wired network and wireless devices itself
d) none of the mentioned

Answer: a

35. IEEE 802.11 have three categories of

a) frames
b) fields
c) signals
sequences

Answer: a

36. In wireless ad-hoc network

a) access point is not required
b) access point is must
c) nodes are not required
d) none of the mentioned

Answer: a

37. Which multiple access technique is used by IEEE 802.11 standard for wireless LAN?

a) CDMA
b) CSMA/CA
c) ALOHA
d) None of the mentioned

Answer: b

38. In wireless distribution system

a) multiple access point are inter-connected with each other
b) there is no access point
c) only one access point exists
d) none of the mentioned

Answer: a

39. A wireless network interface controller can work in

a) infrastructure mode
b) ad-hoc mode
c) both infrastructure mode and ad-hoc mode
d) none of the mentioned

Answer: c

40. In wireless network an extended service set is a set of

a) all connected basic service sets
b) all stations
c) all access points
d) none of the mentioned

Answer: a

41. Mostly ________ is used in wireless LAN.

a) time division multiplexing
b) orthogonal frequency division multiplexing
c) space division multiplexing
d) none of the mentioned

Answer: b

42. Which one of the following event is not possible in wireless LAN

a) collision detection
b) acknowledgement of data frames
c) multi-mode data transmission
d) none of the mentioned

Answer: a

43. The service used by mobile stations to connect themselves to APs is.

a) collision avoidance
b) association
c) collision detection
d) reassociation

Answer: b

44. The service used by mobile stations to change its preferred AP is.

a) collision avoidance
b) collision detection
c) association
d) reassociation

Answer: d

45. DCF stands for

a) Direct Control Function
b) Distributed Control Function
c) Direct Cooperate Function
d) Distributed Coordination Function

Answer: d

46. PCF stands for

a) Point Coordination Function
b) Point Control Function
c) Process Control Function
d) Process Coordination Function

Answer: a

47. Current version in frame control field is

a) 0
b) 1
c) 2
d) 3

Answer: a

3 Network Layer

The network layer is concerned with getting packets from the source all the way to the destination. Thus, the network layer is the lowest layer that deals with end-to-end transmission.

3.1 Network Layer Design Issues

In the following sections, we will give an introduction to some of the issues that the designers of the network layer. These issues include the service provided to the transport layer and the internal design of the network.

3.1.1 Store-and-Forward Packet Switching

The *Figure 3.1* shows the environment in which the network layer protocols operate. The major components of the system are the carrier's equipment (routers connected by transmission lines), shown inside the shaded oval, and the customers' equipment, shown outside the oval.

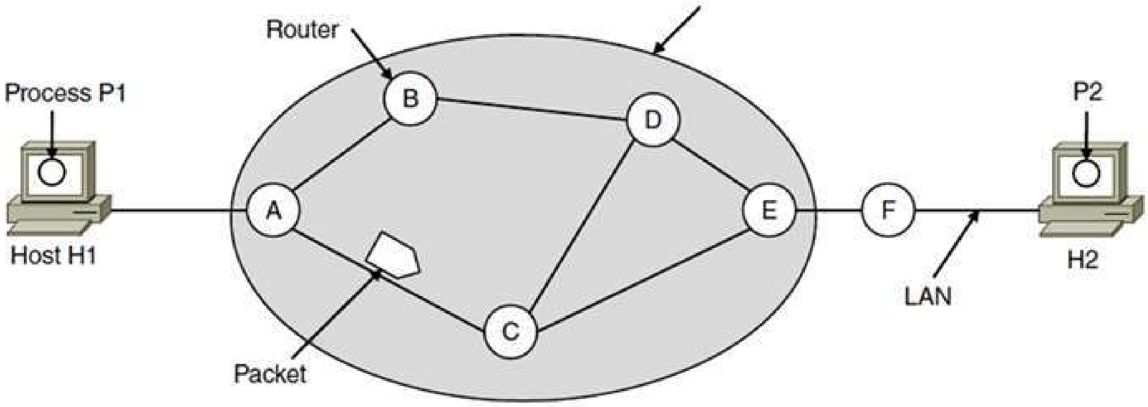


Figure 3.1 The environment of the network layer protocols.

Host H1 is directly connected to one of the carrier's routers, A, by a leased line. In contrast, H2 is on a LAN with a router, F, owned and operated by the customer. This router also has a leased line to the carrier's equipment. We have shown F as being outside the oval because it does not belong to the carrier, but in terms of construction, software, and protocols, it is probably no different from the carrier's routers.

This equipment is used as follows for store-and-forward packet switching. The *Figure 3.2* shows that how the store-and-forward packet switching works.

- A host with a packet to send transmits it to the nearest router, either on its own LAN or over a point-to-point link to the carrier.
- The packet is stored there until it has fully arrived so the checksum can be verified.
- Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered.

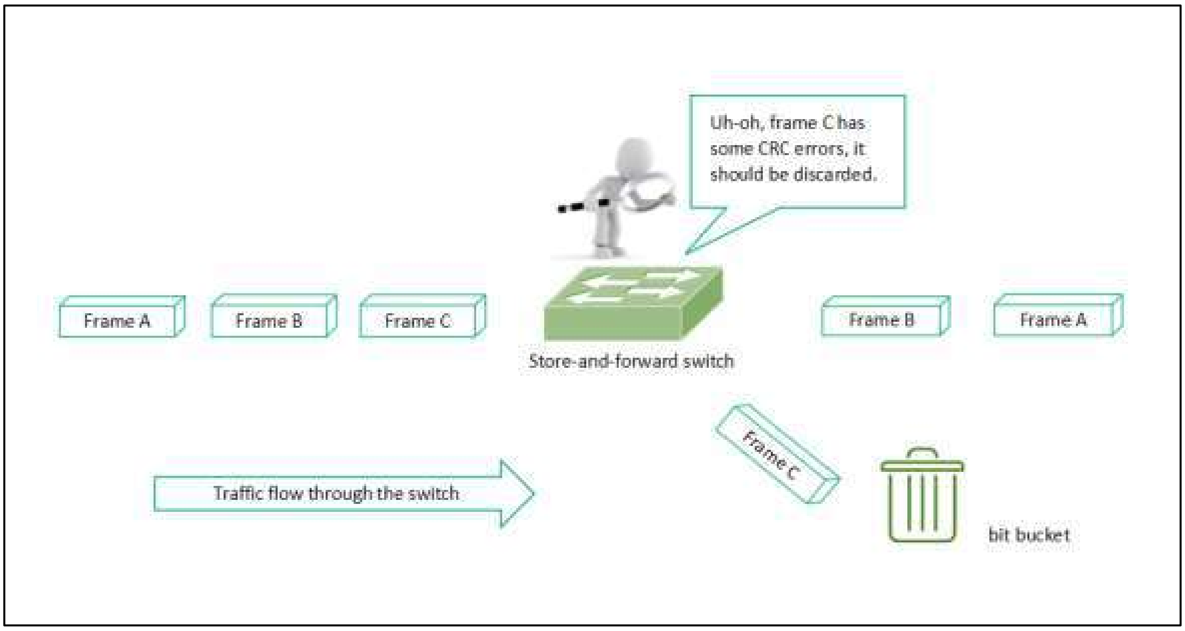

Uh-oh, frame C has some CRC errors, it should be discarded.
Frame A
Frame B
Frame C
Store-and-forward switch
Frame B
Frame A
Frame C
Traffic flow through the switch
bit bucket

Figure 3.2 Working method of store-and-forward switching

3.1.2 Services Provided to the Transport Layer

The network layer provides services to the transport layer at the network layer/transport layer interface. An important question is what kind of services the network layer provides to the transport layer. The network layer services have been designed with the following goals in mind.

1. The services should be independent of the router technology.
2. The transport layer should be shielded from the number, type, and topology of the routers present.
3. The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

With these goals, the designers of the network layer have a lot of freedom in writing detailed specifications of the services to be offered to the transport layer. This freedom often degenerates into a raging battle between two warring factions.

1. The routers' job is moving packets around and nothing else. The hosts should accept the fact that the network is unreliable and do error control (i.e., error detection and correction) and flow control themselves.
2. The subnet should provide a reliable, connection-oriented service.

These two views are best exemplified by the Internet and ATM. The Internet offers connectionless network-layer service; ATM networks offer connection-oriented network-layer service.

3.1.3 Implementation of Connectionless Service

Two different organizations are possible, depending on the type of service offered.

a. Datagram Networks

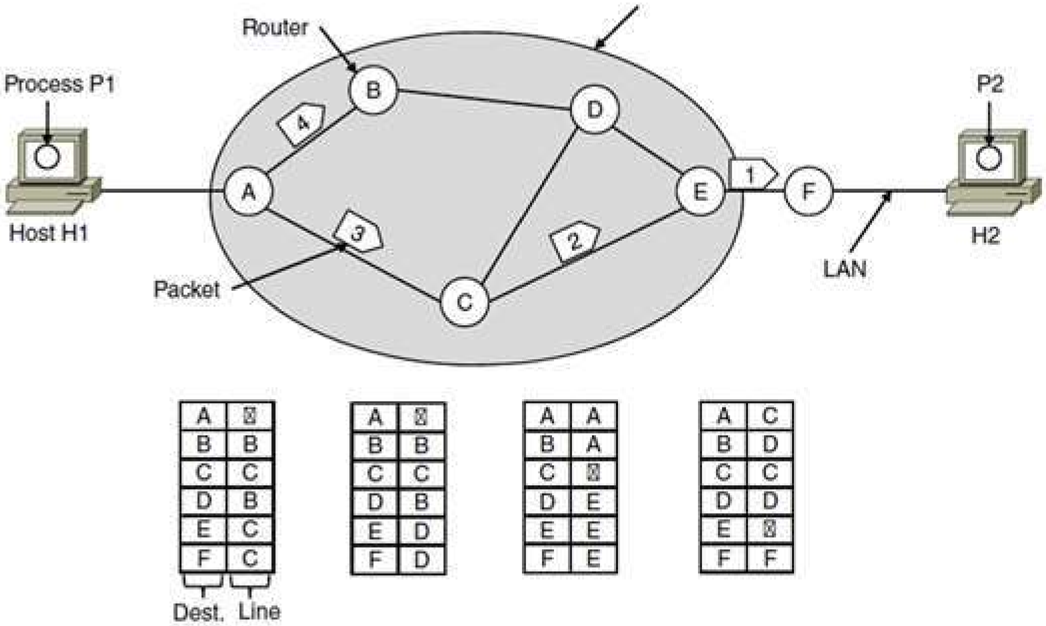
If connectionless service is offered, packets are injected into the subnet individually and routed independently of each other. No advance setup is needed.

Datagrams: A datagram is a basic transfer unit associated with a packet-switched network. Datagrams are typically structured in header and payload sections. Datagrams provide a connectionless communication service across a packet-switched network. The delivery, arrival time, and order of arrival of datagrams need not be guaranteed by the network.

> "A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network."

Datagram network: The network which uses datagram is called a datagram network.

Let us now see how a datagram network works. Suppose that the process P1 in *Figure 3.3* has a long message for P2. It hands the message to the transport layer with instructions to deliver it to process P2 on host H2.



A	⊠
B	B
C	C
D	B
E	C
F	C

A	⊠
B	B
C	C
D	B
E	D
F	D

A	A
B	A
C	⊠
D	E
E	E
F	E

A	C
B	D
C	C
D	D
E	⊠
F	F

Figure 3.3 Routing within a datagram network

The transport layer code runs on H1, typically within the operating system. It prepends a transport header to the front of the message and hands the result to the network layer, probably just another procedure within the operating system.

Let us assume that the message is four times longer than the maximum packet size, so the network layer has to break it into four packets, 1, 2, 3, and 4 and sends each of them in turn to router A using some point-to-point protocol, for example, PPP.

At this point the carrier takes over. Every router has an internal table telling it where to send packets for each possible destination. Each table entry is a pair consisting of a destination and the outgoing line to use for that destination.

Only directly-connected lines can be used. For example, in *Figure 3.3*, A has only two outgoing lines—to B and C—so every incoming packet must be sent to one of these routers, even if the ultimate destination is some other router. A's initial routing table is shown in the figure under the label "initially."

However, something different happened to packet 4. When it got to A it was sent to router B, even though it is also destined for F. For some reason, A decided to send packet 4 via a different route than that of the first three.

Perhaps it learned of a traffic jam somewhere along the ACE path and updated its routing table, as shown under the label "later." The algorithm that manages the tables and makes the routing decisions is called the routing algorithm.

b. Virtual-Circuit Model

If connection-oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent. This connection is called a VC (virtual circuit).

Virtual-Circuit Network: In analogy with the physical circuits set up by the telephone system, and the subnet is called a virtual-circuit network.

3.1.4 Implementation of Connection-Oriented Service

For connection-oriented service, we need a virtual-circuit network. Let us see how that works. The idea behind virtual circuits is to avoid having to choose a new route for every packet sent, as in *Figure 3.4*.

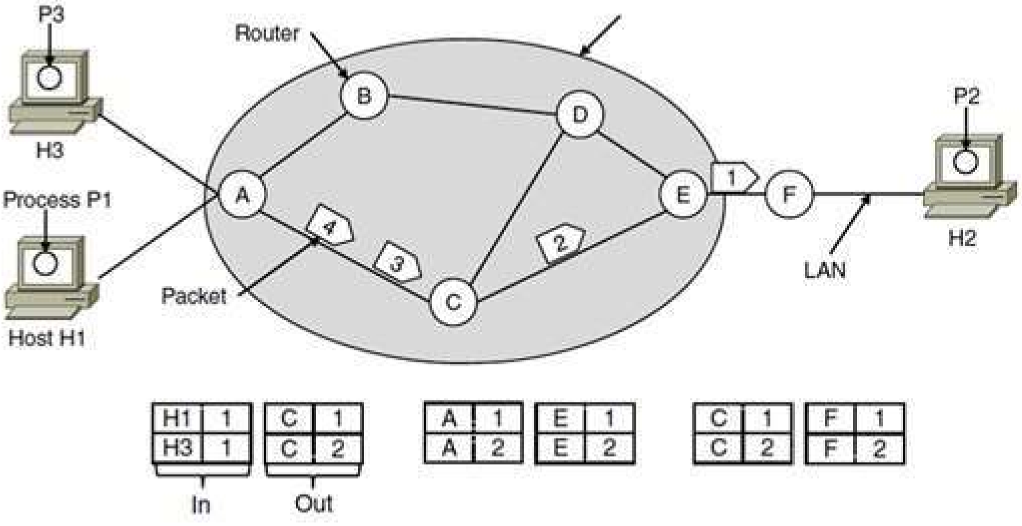


Figure 3.4 Routing within a virtual-circuit network.

- ***Connection Establish Phase***

Instead, when a connection is established, a route from the source machine to the destination machine is chosen as part of the connection setup and stored in tables inside the routers. That route is used for all traffic flowing over the connection, exactly the same way that the telephone system works.

- ***Connection Release Phase***

When the connection is released, the virtual circuit is also terminated. With connection-oriented service, each packet carries an identifier telling which virtual circuit it belongs to. As an example, consider the situation of *Figure 3.4*. Here, host H1 has established connection 1 with host H2.

It is remembered as the first entry in each of the routing tables. The first line of A's table says that if a packet bearing connection identifier 1 comes in from H1, it is to be sent to router C and given connection identifier 1. Similarly, the first entry at C routes the packet to E, also with connection identifier 1.

- ***Connection Identifier Conflicts***

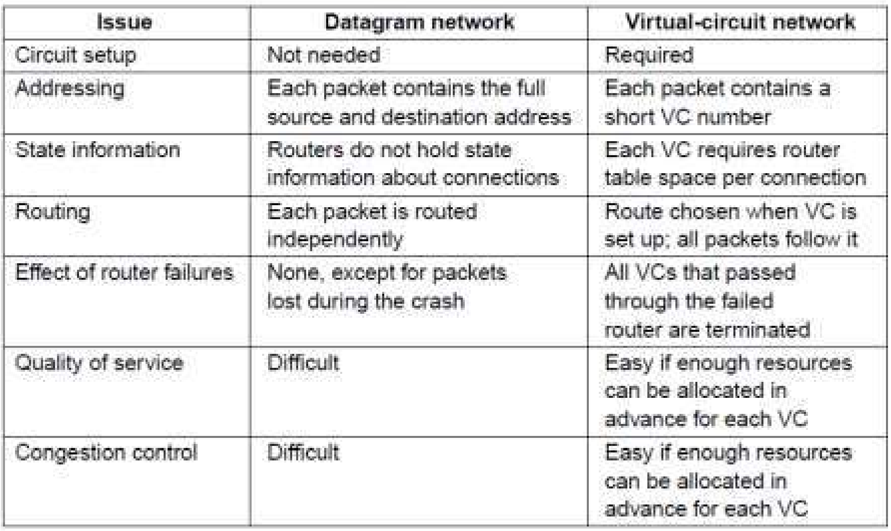
Now let us consider what happens if H3 also wants to establish a connection to H2. It chooses connection identifier 1 and tells the subnet to establish the virtual circuit. This leads to the second row in the tables.

Note that we have a conflict here because although A can easily distinguish connection 1 packets from H1 from connection 1 packets from H3, C cannot do this. For this reason, A assigns a different connection identifier to the outgoing traffic for the second connection.

- ✓ *Label Switching*: Avoiding conflicts of this kind is why routers need the ability to replace connection identifiers in outgoing packets. In some contexts, this is called label switching.
- ✓ *MPLS (MultiProtocol Label Switching)*: An example of a connection-oriented network service. It is used within ISP networks in the Internet, with IP packets wrapped in an MPLS header having a 20-bit connection identifier or label.

3.1.5 Comparison of Virtual-Circuit and Datagram Subnets

Both virtual circuits and datagrams have their supporters and their detractors. We will now attempt to summarize the arguments both ways. The major issues are listed in *Table 3-1*.



Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Table 3-1 Comparison of datagram and virtual-circuit networks.

Inside the subnet, several trade-offs exist between virtual circuits and datagrams.

1. One trade-off is between router memory space and bandwidth.
2. Another trade-off is setup time versus address parsing time. Using virtual circuits requires a setup phase, which takes time and consumes resources.
3. Yet another issue is the amount of table space required in router memory.
4. Virtual circuits have some advantages in guaranteeing quality of service and avoiding congestion.
5. Virtual circuits also have a vulnerability problem

3.2 Routing Algorithms

The main function of the network layer is routing packets from the source machine to the destination machine. In most networks, packets will require multiple hops to make the journey. The only notable exception is for broadcast networks, but even here routing is an issue if the source and destination are not on the same network segment.

3.2.1 Routers

Before going to study about the routing algorithms, it is essential to study about router and its functions.

A router can be hardware device with a software application. The router is connected to at least two networks and do the routing operations.

Mostly, router is located at the gateway and it routes packets as they travel from one network to another network(s). the routers find the path/route to forward the packet to reach the destination. It also find the alternate path, if the existing path is failed.

Routing = building maps and giving directions

Forwarding = moving packets between interfaces according to the “directions”

3.2.2 Routing Algorithms

The algorithms that choose the routes and the data structures that they use are a major area of network layer design.

Routing algorithm: It is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.

If the network uses datagrams internally, this decision must be made anew for every arriving data packet since the best route may have changed since last time. If the network uses virtual circuits internally, routing decisions are made only when a new virtual circuit is being set up.

Session routing : Thereafter, data packets just follow the already established route. The latter case is sometimes called session routing because a route remains in force for an entire session (e.g., a login session at a terminal or a file transfer)

Forwarding: It is sometimes useful to make a distinction between routing, which is making the decision which routes to use, and forwarding, which is what happens when a packet arrives.

One can think of a router as having two processes inside it. One of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing tables. This process is forwarding.

- ***Properties of routing algorithms***

Regardless of whether routes are chosen independently for each packet or only when new connections are established, certain properties are desirable in a routing algorithm:

- ✓ correctness,
- ✓ simplicity,
- ✓ robustness,
- ✓ stability,
- ✓ fairness,
- ✓ and optimality.

Fairness and optimality may sound obvious surely no reasonable person would oppose them, but as it turns out, they are often contradictory goals. As a simple example of this conflict, look at *Figure 3.5*.

Suppose that there is enough traffic between A and A', between B and B', and between C and C' to saturate the horizontal links. To maximize the total flow, the X to X' traffic should be shut off altogether. Unfortunately, X and X' may not see it that way.

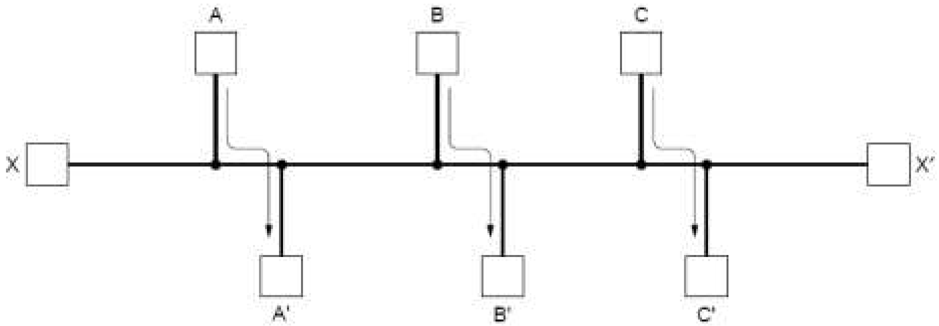


Figure 3.5 Network with a conflict between fairness and efficiency

3.2.3 Types of Routing Algorithms

Routing algorithms can be grouped into two major classes:

1. Non Adaptive
2. Adaptive.

Nonadaptive algorithms do not base their routing decisions on any measurements or estimates of the current topology and traffic.

Static routing: The choice of the route to use to get from I to J (for all I and J) is computed in advance, offline, and downloaded to the routers when the network is booted.

Adaptive algorithms change their routing decisions to reflect changes in the topology, and sometimes changes in the traffic as well. These dynamic routing algorithms changes routes dynamically at run time in the following cases.

- ✓ Initially, get their information from locally, from adjacent routers, or from all routers.
- ✓ When the topology changes,
- ✓ When metric is used for optimization (e.g., distance, number of hops, or estimated transit time).

3.2.4 The Optimality Principle

It is necessary to find optimal routes without regard to network topology or traffic. The principal of optimality as follows;

- ✓ Find an optimal path has the property that whatever the initial conditions and control variables (choices) over some initial period.
- ✓ The control (or decision variables) chosen over the remaining period must be optimal for the remaining problem, with the state resulting from the early decisions taken to be the initial condition.

The optimality principle states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.

- **Sink Tree**

As a consequence of that principle, 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 and shown in *Figure 3.6.*

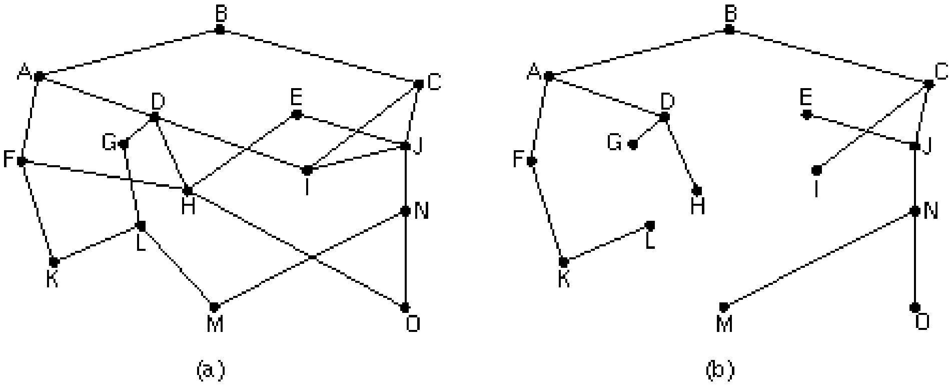


Figure 3.6 (a) A subnet. (b) A sink tree for router B.

Note that a sink tree is not necessarily unique; other trees with the same path lengths may exist. The goal of all routing algorithms is to discover and use the sink trees for all routers. Since a sink tree is indeed a tree, it does not contain any loops, so each packet will be delivered within a finite and bounded number of hops.

3.3 Shortest Path Routing Algorithm

Shortest path algorithm works on graph of network, each node in graph represents router and each edge represents a communication link.

To choose route between given source and destination, this algorithm finds shortest path between them. Number of hopes, geographical distance, delay are some of the criteria on base of which, algorithm finds shortest path.

One way of measuring path length is the number of hops. Using this metric, the paths ABC and ABE in Figure 3.7 are equally long. Another metric is the geographic distance in kilometers. Many other metrics are also possible. For example, each arc could be labelled with the mean queuing and transmission delay for some standard test packet as determined by hourly test runs.

In the general case, the labels on the arcs could be computed as a function of the distance, bandwidth, average traffic, communication cost, mean queue length, measured delay, and other factors. By changing the weighting function, the algorithm would then compute the "shortest" path measured according to any one of a number of criteria or to a combination of criteria.

The arrows indicate the working node. To illustrate how the labelling algorithm works, look at the weighted, undirected graph of Figure 3.7(a), where the weights represent, for example, distance.

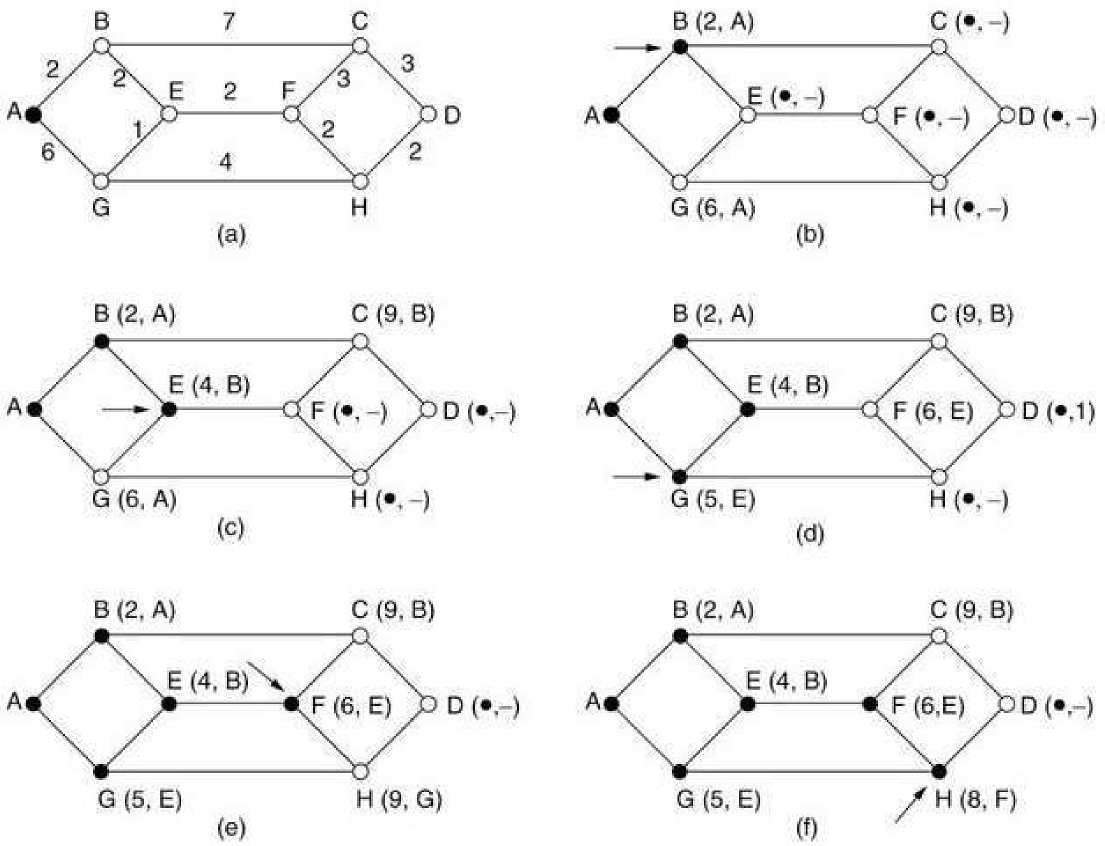


Figure 3.7 Computing the shortest path from A to D

We want to find the shortest path from A to D. We start out by marking node A as permanent, indicated by a filled-in circle. Then we examine, in turn, each of the nodes adjacent to A (the working node), relabeling each one with the distance to A. Whenever a node is relabeled, we also label it with the node from which the probe was made so that we can reconstruct the final path later.

Having examined each of the nodes adjacent to A, we examine all the tentatively labeled nodes in the whole graph and make the one with the smallest label permanent, as shown in Figure 3.7(b). This one becomes the new working node.

We now start at B and examine all nodes adjacent to it. If the sum of the label on B and the distance from B to the node being considered is less than the label on that node, we have a shorter path, so the node is relabeled.

After all the nodes adjacent to the working node have been inspected and the tentative labels changed if possible, the entire graph is searched for the tentatively-labeled node with the smallest value. This node is made permanent and becomes the working node for the next round. Figure 3.7 shows the first five steps of the algorithm.

To see why the algorithm works, look at Figure 3.7(c). At that point we have just made E permanent. Suppose that there were a shorter path than ABE, say AXYZE. There are two possibilities: either node Z has already been made permanent, or it has not been. If it has, then

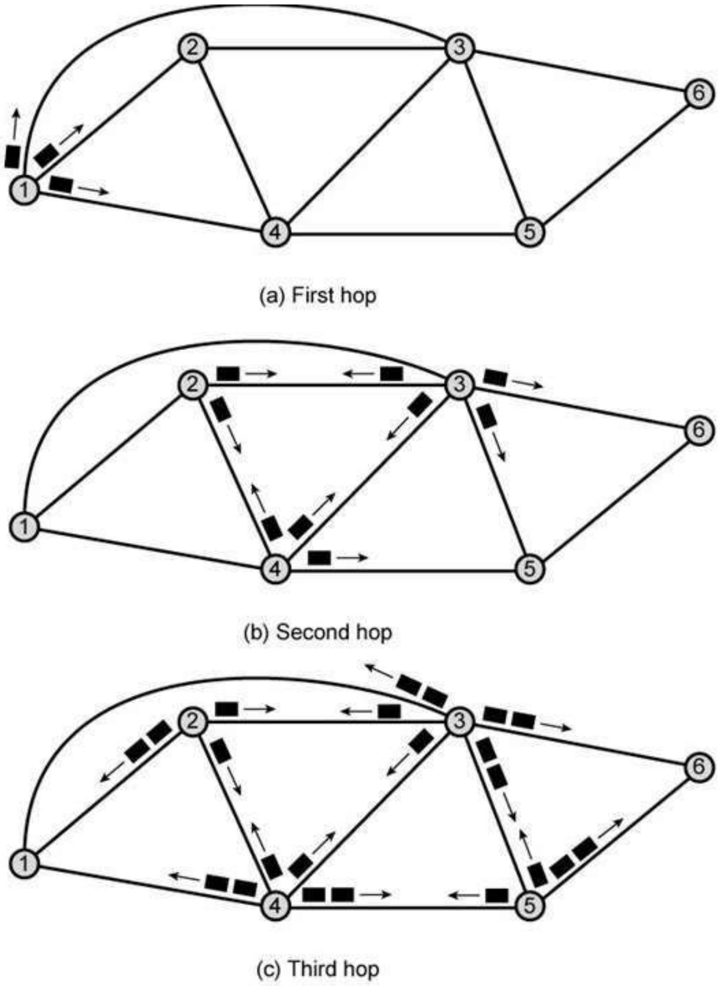
E has already been probed (on the round following the one when Z was made permanent), so the AXYZE path has not escaped our attention and thus cannot be a shorter path.

Now consider the case where Z is still tentatively labeled. Either the label at Z is greater than or equal to that at E, in which case AXYZE cannot be a shorter path than ABE, or it is less than that of E, in which case Z and not E will become permanent first, allowing E to be probed from Z.

3.4 Flooding

Another static algorithm is flooding, in which every incoming packet is sent out on every outgoing line except the one it arrived on. Flooding obviously generates vast numbers of duplicate packets, in fact, an infinite number unless some measures are taken to damp the process.

One such measure is to have a hop counter contained in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero.



(a) First hop

(b) Second hop

(c) Third hop

Figure 3.8 Flooding of Packets at each hop

The Figure 3.8 shows the example of flooding at each hop. Ideally, the hop counter should be initialized to the length of the path from source to destination. If the sender does not know how long the path is, it can initialize the counter to the worst case, namely, the full diameter of the subnet.

To prevent the list from growing without bound, each list should be augmented by a counter, k, meaning that all sequence numbers through k have been seen. When a packet comes in, it is easy to check if the packet is a duplicate; if so, it is discarded. Furthermore, the full list below *k* is not needed, since k effectively summarizes it.

- **Selective Flooding**

A variation of flooding that is slightly more practical is selective flooding. In this algorithm the routers do not send every incoming packet out on every line, only on those lines that are going approximately in the right direction. There is usually little point in sending a westbound packet on an eastbound line unless the topology is extremely peculiar and the router is sure of this fact.

- **Applications**

  ✓ In military applications, where large numbers of routers may be blown to bits at any instant.
  ✓ In distributed database applications, it is sometimes necessary to update all the databases concurrently.
  ✓ In wireless networks, all messages transmitted by a station can be received by all other stations within its radio range.
  ✓ Flooding always chooses the shortest path because it chooses every possible path in parallel.

3.5 Broadcast Routing

In broadcast routing, packets are sent to all nodes even if they do not want it. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices. A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses.

In some application, hosts need to send messages to many or all other host. *Sending a packet to all destination simultaneously is called broadcasting*. The broadcasting routing can be achieved using the following methods;

1. Using unicasting - source send a distinct packet to each destination. It wastes bandwidth and slow.
2. Flooding
3. Multi-destination routing
4. Spanning Tree Method
5. Reverse path forwarding

3.5.1 Multi-destination routing

In multi-destination routing, each packet contains entire list of destination. When packet comes at router, it finds line for all destination. Then router generates new copy of packet for each output line, that packet contains only those lists of destination that are to use that line.

Eventually after some hopes, each packet will carry only one destination like normal packet. Requires less bandwidth but much work from router.

3.5.2 Spanning Tree Method

A fourth broadcast algorithm makes explicit use of the sink tree for the router initiating the broadcast—or any other convenient spanning tree for that matter. A spanning tree is a subset of the subnet that includes all the routers but contains no loops.

Each router forwards packets on all lines on the spanning tree (except the one the packet arrived on). Efficient but needs to generate the spanning tree and routers must have that information.

3.5.3 Reverse path forwarding

Router checks whether broadcast packet arrived on interface that is used to send packets to source of broadcast.

- ✓ If so, it's likely that it followed best route and thus not a duplicate; router forwards packet on all lines.
- ✓ If not, packet discarded as likely duplicate.

An example of reverse path forwarding is shown in Figure 3.9. Part (a) shows a subnet, part (b) shows a sink tree for router I of that subnet, and part (c) shows how the reverse path algorithm works.

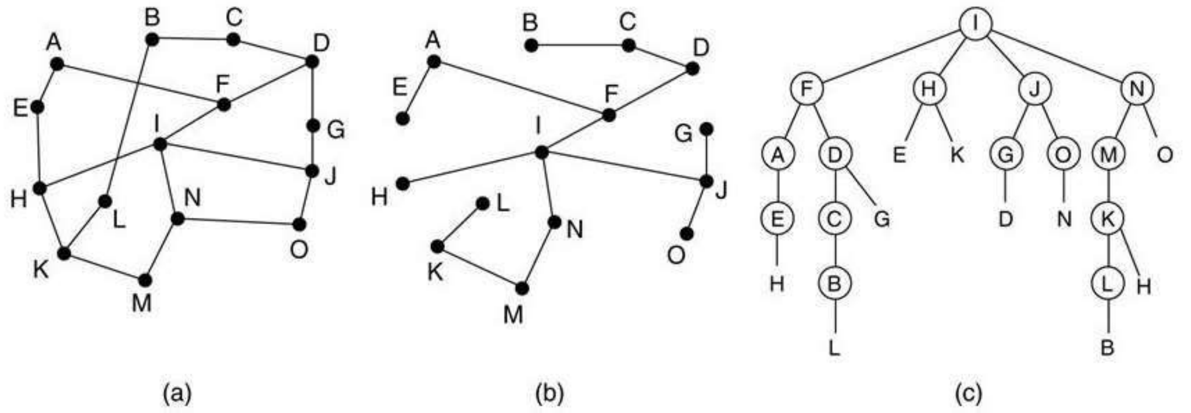


Figure 3.9 Reverse path forwarding. (a) A subnet. (b) A sink tree. (c) Tree built by reverse path forwarding.

On the first hop, I sends packets to F, H, J, and N, as indicated by the second row of the tree. Each of these packets arrives on the preferred path to I (assuming that the preferred path falls along the sink tree) and is so indicated by a circle around the letter.

On the second hop, eight packets are generated, two by each of the routers that received a packet on the first hop. As it turns out, all eight of these arrive at previously unvisited routers, and five of these arrive along the preferred line.

Of the six packets generated on the third hop, only three arrive on the preferred path (at C, E, and K); the others are duplicates. After five hops and 24 packets, the broadcasting terminates, compared with four hops and 14 packets had the sink tree been followed exactly.

Advantages

- ✓ Efficient and easy to implement.
- ✓ It does not require routers to know about spanning trees,
- ✓ Nor does it have the overhead of a destination list or bit map in each broadcast packet as does multidestination addressing.
- ✓ Nor does it require any special mechanism to stop the process, as flooding does

3.6 Multicast Routing

Sending a message to group of stations is called multicast. Routing algorithm used in multicast is called multicast routing. If the group is small, it can just send each other member a point-to-point message. If group is dense, then broadcast using spanning tree is good option. But broadcast will deliver the packets to some of member that are not part of group. Which is waste of bandwidth.

3.6.1 Group Management

Multicasting requires group management. Some way is needed to create and destroy groups, and to allow processes to join and leave groups. It is important that routers know which of their hosts belong to which groups. Either hosts must inform their routers about changes in group membership, or routers must query their hosts periodically. Either way, routers learn about which of their hosts are in which groups. Routers tell their neighbors, so the information propagates through the subnet.

3.6.2 Multicast Spanning Tree

Another option is to prune “broadcast spanning tree” by removing links that do not leads to group member. This is called “multicast spanning tree”. Multicast spanning tree is used to deliver a packet to a group.

To do multicast routing, each router computes a spanning tree covering all other routers. For example, in Figure 3.10(a) we have two groups, 1 and 2. Some routers are attached to hosts that belong to one or both of these groups, as indicated in the figure. A spanning tree for the leftmost router is shown in Figure 3.10(b).

When a process sends a multicast packet to a group, the first router examines its spanning tree and prunes it, removing all lines that do not lead to hosts that are members of the group. In our example, Figure 3.10(c) shows the pruned spanning tree for group 1. Similarly, Figure 3.10(d) shows the pruned spanning tree for group 2. Multicast packets are forwarded only along the appropriate spanning tree. One potential disadvantage of this algorithm is that it scales poorly to large networks.

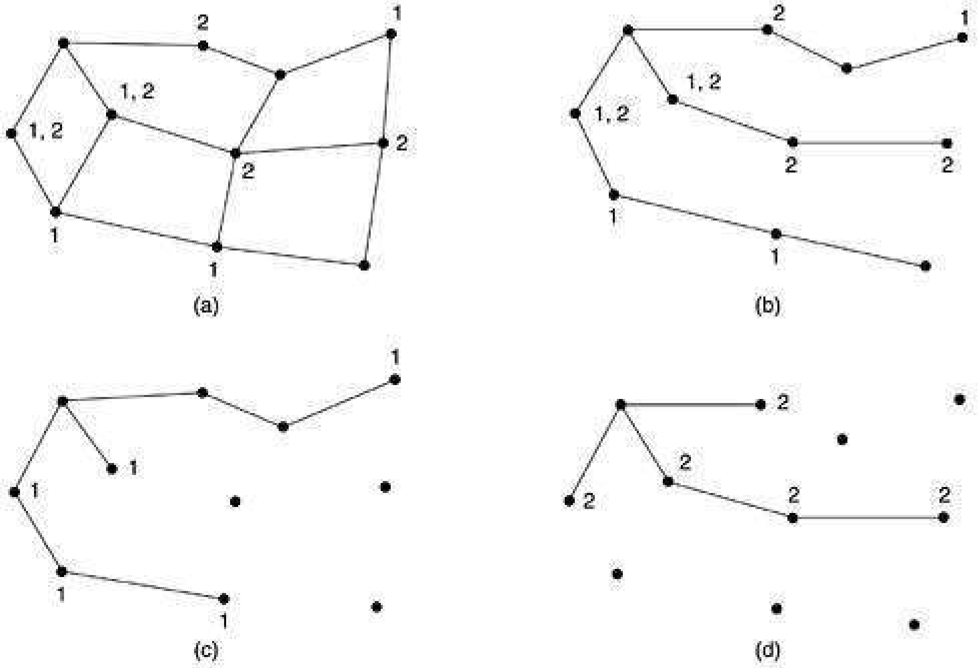


Figure 3.10 (a) A network. (b) A spanning tree for the leftmost router. (c) A multicast tree for group 1. (d) A multicast tree for group 2.

- **Methods of pruning the spanning tree**
  - ✓ Link state routing is used and each router is aware of the complete topology.
  - ✓ With distance vector routing, reverse path forwarding algorithm can applied

3.6.3 Core-based trees

An alternative design uses core-based trees. Here, a single spanning tree per group is computed, with the root (the core) near the middle of the group. To send a multicast message, a host sends it to the core, which then does the multicast along the spanning tree.

3.7 Congestion Control

3.7.1 Introduction

An important issue in a packet-switched network is congestion. A state occurring in network layer when the message traffic is so heavy that it slows down network response time.

Congestion in a network may occur if the load on the network, the number of packets sent to the network, is greater than the capacity of the network, the number of packets a network can handle.

Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

When too many packets are present in the subnet performance degrades (Figure 3.11). This situation is called Congestion. The number of packets dumped into the subnet are within it carrying capacity, they are all delivered.

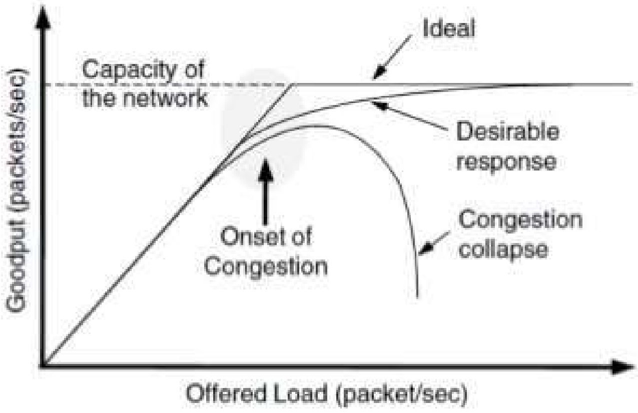


Figure 3.11 Congestion Control

However, if the traffic increases too far, the routers are unable to cope and begin losing packets. At very high traffic, performance collapse completely and almost no packets are delivered.

- **Factors will lead to congestion**

1. Incoming capacity greater than the outgoing capacity

   If all of a sudden, streams of packets begin arriving on three or four input lines and only one output line queue will build up. If there is insufficient memory to hold all of them, packets will be lost. Adding infinite memory congestion gets worse, because by the time packets get to the front of the queue, the time out and duplicates have been sent.

2. Slow processors (routers) can cause congestion.

   A slow processor performs the book keeping tasks very slow, queues will build up.

3. Low band-width lines also cause congestion

   Upgrading lines but not changing the processor and vice-versa shifts the bottleneck.

This problem will persist until all components are in balance.

- **Difference Between Flow Control and Congestion control**

Congestion control is different than flow control. Flow control is a data link issue, and concerns only one sender outrunning a single receiver (e.g. a point-to-point link). Congestion control is a network layer issue, and is thus concerned with what happens when there is more data in the network than can be sent with reasonable packet delays, no lost packets, etc. Flow control is a local, congestion control is global.

One means of handling congestion is by using a flow control mechanism to reduce the traffic put on the net by a particular host, hence the confusion.

Example (**Figure 3.12**)

- ✓ Consider a network with a capacity of 1000Gbps on which a super computer is trying to transfer a file to a personal computer at 1Gbps.Here a flow control is needed.
- ✓ Consider a network with 1Mbps lines and 1000 large computers, more than half are trying to transfer files a 100kbps to the other half. The problem is here is the total offered traffic exceeds than the network handle.

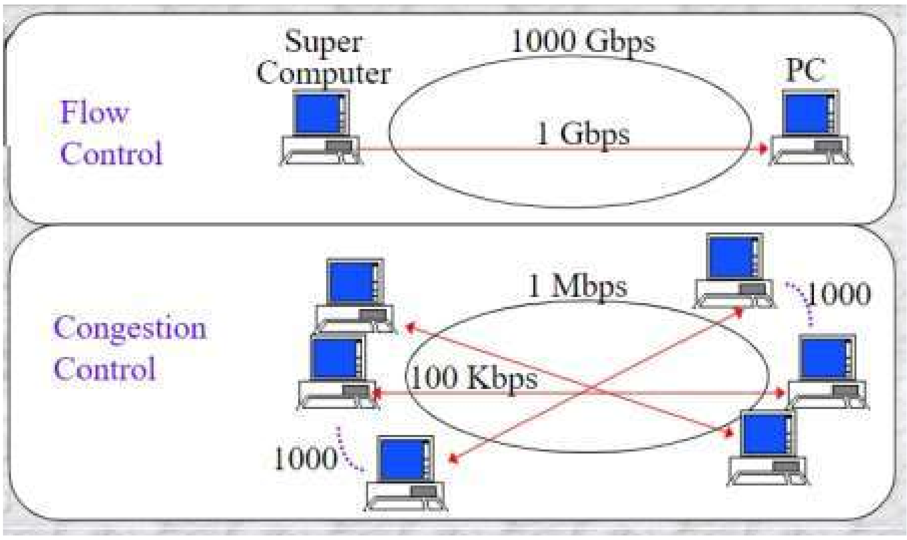


Figure 3.12 Example of Flow Control Vs Congestion Control

3.7.2 General Principles of Congestion Control

The congestion control can be done by two methods; Open loop and Closed loop.

1. Open loop

These solutions attempt to solve the problem by good design, to make sure that it does not occur in the first place. Once the system is up and running, midcourse corrections are not made.

Tools for doing open-loop control include deciding when to accept new traffic, deciding when to discard packets and which ones, and making scheduling decisions at various points in the network.

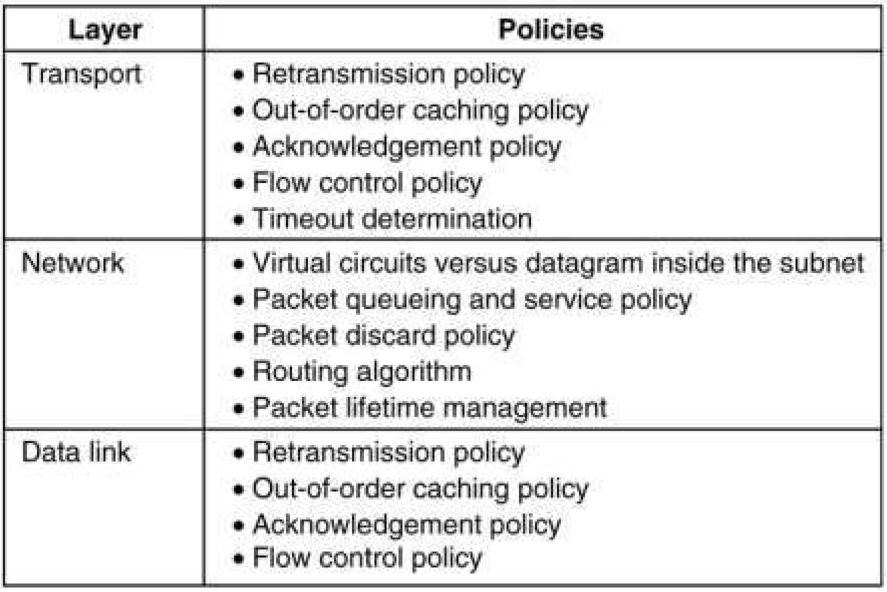
2. Closed Loop

In contrast, closed loop solutions are based on the concept of a feedback loop. This approach has three parts when applied to congestion control:

1. Monitor the system to detect when and where congestion occurs.
2. Pass this information to places where action can be taken.
3. Adjust system operation to correct the problem.

3.7.3 Congestion Prevention Policies

Let us begin our study of methods to control congestion by looking at open loop systems. These systems are designed to minimize congestion in the first place, rather than letting it happen and reacting after the fact. They try to achieve their goal by using appropriate policies at various levels. In Figure 3.13, different data link, network, and transport policies that can affect congestion.



Layer	Policies
Transport	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy • Timeout determination
Network	• Virtual circuits versus datagram inside the subnet • Packet queueing and service policy • Packet discard policy • Routing algorithm • Packet lifetime management
Data link	• Retransmission policy • Out-of-order caching policy • Acknowledgement policy • Flow control policy

Figure 3.13 Policies that affect congestion

- **Retransmission policy** : it is concerned with how fast a sender times out and what it transmits upon timeout. A jumpy sender that times out quickly and retransmits all outstanding packets using go back n will put a heavier load.
- **Acknowledgement** policy also affects congestion. If each packet is acknowledged immediately, the acknowledgement packets generate extra traffic.
- The choice between using virtual circuits and using datagrams affects congestion since many congestion control algorithms work only with virtual-circuit subnets.
- A good **routing algorithm** can help avoid congestion by spreading the traffic over all the lines, whereas a bad one can send too much traffic over already congested lines.
- **Discard policy** is the rule telling which packet is dropped when there is no space.
- **Packet lifetime management** deals with how long a packet may live before being discarded.
- If the **timeout interval** is too short, extra packets will be sent unnecessarily. If it is too long, congestion will be reduced but the response time will suffer whenever a packet is lost.

- ***Traffic shaping***

One of the causes of congestion is the inherent burstiness of computer network traffic. Traffic shaping means to smooth, or otherwise alter, the offered traffic as a function of time. Smooth traffic is easier to deal with the bursty traffic. A subnet may be able to handle on average 10 M packets in an hour, but it probably can't handle 10M packets in one minute and nothing for the next 59 minutes.

Related to traffic shaping is the whole idea of agreeing with a network service provider to a flow specification. A flow specification describes what sort of traffic you will put into the net, and what sort of quality if service you expect from it. Some of the quality of service parameters are:

- ✓ loss sensitivity (number of lost bytes per unit of time)
- ✓ loss interval (the unit of time for calculating loss)
- ✓ burst loss sensitivity (how long of a loss burst can be tolerated)
- ✓ minimum delay (how large of a delay before the app notices)
- ✓ maximum delay variation (the variance or jitter in the inter-packet delay)
- ✓ quality of guarantee (how serious the spec is to the application)

3.7.4 Congestion Control in Virtual-Circuit Subnets

In this context, we are discussing some approaches to dynamically controlling congestion in virtual- circuit subnets.

1. Admission Control

This technique that is widely used to keep congestion that has already started from getting worse. In this approach, once congestion is detected, no more virtual circuits are allowed to set up until congestion gets over. Thus, attempts to set up new transport layer connections fail.

Example

In the telephone system, when a switch gets overloaded, it also practices admission control by not giving dial tones.

2. Creating New Virtual Circuits

An alternative approach is to allow new virtual circuits but carefully route all new virtual circuits around problem areas. For example, consider the subnet of Figure 3.14 (a), in which two routers are congested, as indicated.

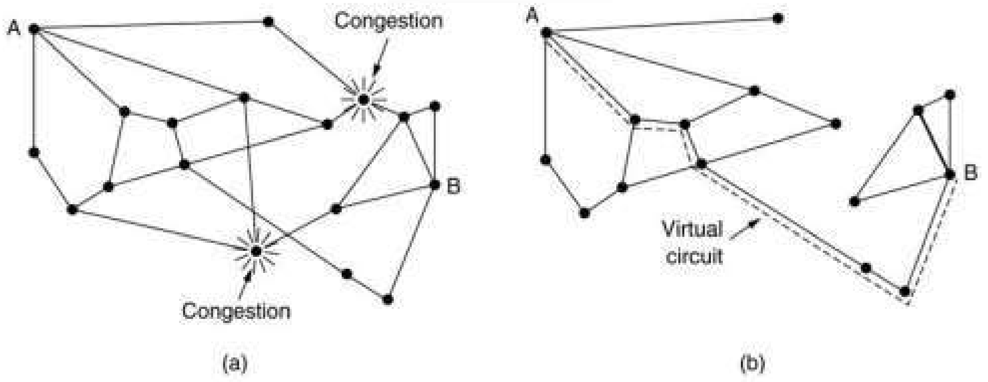


Figure 3.14 (a) A congested subnet. (b) A redrawn subnet with new virtual circuit

Suppose that a host attached to router A wants to set up a connection to a host attached to router B. Normally, this connection would pass through one of the congested routers. To avoid this situation, we can redraw the subnet as shown in Figure 3.14(b), omitting the congested routers and all of their lines. The dashed line shows a possible route for the virtual circuit that avoids the congested routers.

3. Feedback

Another strategy in virtual circuit subnet is, when VC is established, sender gives details volume and shape of traffic and other parameter and subnet reserves resources so congestion will unlikely to occur.

3.7.5 Congestion Control in Datagram Subnets

Each router can easily monitor the utilization of its output lines and other resources. It can estimate each line about the recent utilization of that line (*u*). Periodically a sample at the instantaneous line utilization (*f*) can be mad and *u* updated.

$$u_{new} = au_{old} + (1-a)f$$

where *a* is constant determines how fast the router forgets recent history.

Whenever u moves above the threshold, the output line enters a 'warning' state. Each new arriving packet is checked if its output line is warning state. If it is some action is taken. The following are the actions to be taken.

- ***The Warning Bit***

When the output line reaches to warning state it is signalled by setting a special bit in the packet's header. When the packet arrived at its destination, the transport entity copied the bit into the next acknowledgement sent back to source. The source then cut back on traffic. As long as the router was in warning state, it continued to set warning bit. As long as the warning bits continued to flow in, the source continued to decrease its transmission rate.

- ***Choke packets***

In this algorithm, the router sends a choke packet back to the source host. The original packet is tagged so that it will not generate any more choke packets farther along the path and is then forwarded in the usual way.

When the source host gets the choke packet, it is required to reduce the traffic sent to the specified destination by X percent. Since other packets aimed at the same destination are probably already under way and will generate yet more choke packets, the host should ignore choke packets referring to that destination for a fixed time interval. After that period has expired, the host listens for more choke packets for another interval. If one arrives, the line is still congested, so the host reduces the flow still more and begins ignoring choke packets again. If no choke packets arrive during the listening period, the host may increase the flow again. The first choke packet causes the data rate to be reduced to 0.50 of its previous rate, the next one causes a reduction to 0.25, and so on. Increases are done in smaller increments to prevent congestion from reoccurring quickly.

- ***Hop by Hop choke packets***

For example, let the host A is sending packets to D. as shown in step 1. If D runs out of buffers, it will take sometime for a choke packet to reach A to tell it to slow down. This is shown in step 2,3,4. In this time another packets will be sent. Only after some more time the router D will be noticing a slower flow (step 7).

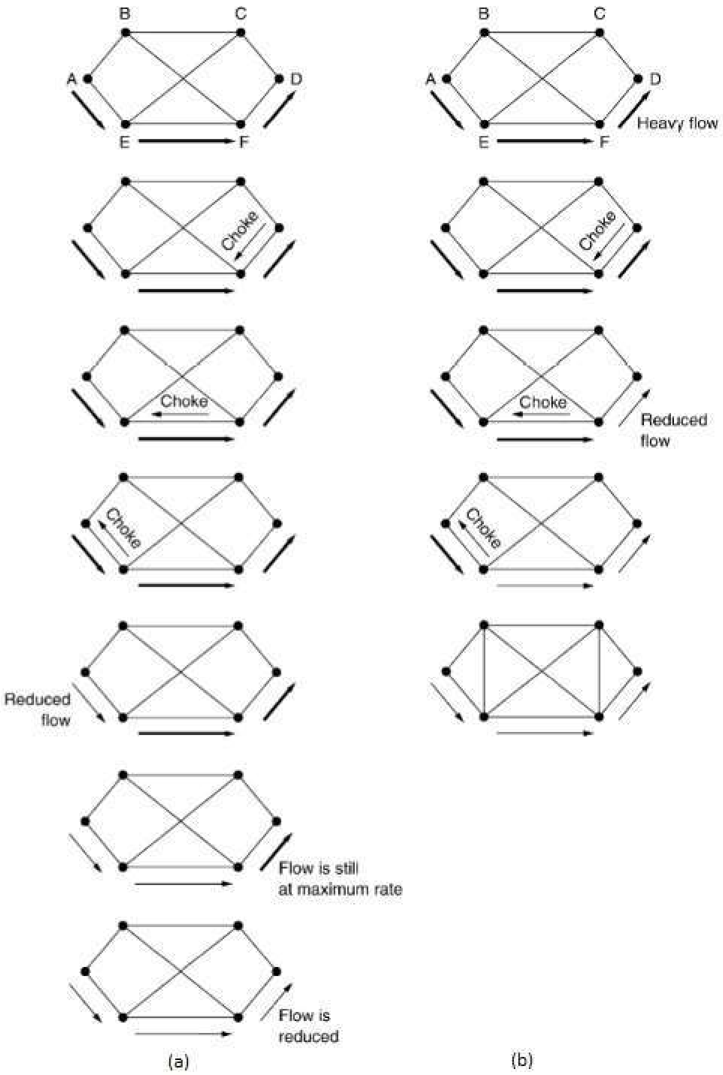


Figure 3.15 (a) A choke packet that affects only the source (b) A choke packet that affects each hop it passes through

In other approach, as soon as choked packet reaches to F it cuts down the flow to D and D will get immediate relief. (like a headache remedy in a TV). In the next set up, when choke reaches to E it also cuts down the flow to F which in turn gives relief to F. Finally, when the choke packet richer A and the flow genuinely slows down.

The net effect of this hop-by-hop scheme is to provide quick relief at the point of congestion at the price of using up more buffers upstream. In this way, congestion can be nipped in the bud without losing any packets.

3.7.6 Load Shedding

When none of the approach work, finally router stats discarding packet. This ss called load shedding. Instead of randomly discarding packets, if packets are discarded on base of application, less retransmission will occur.

For example, in case of file transfer, old packet worth more so newer (called as wine) should be discarded. While in case of multimedia transfer, new packets worth more (called as milk). To implement intelligent dropping policy requires support from sender. Sender will mark packet with priority. Packets with lower priority will be discarded first.

- **Random Early Detection (RED)**

RED provides congestion avoidance by controlling the queue size at the gateway. RED notifies the source before the congestion actually happens rather than wait till it actually occurs. RED provides a mechanism for the gateway to provide some feedback to the source on congestion status. The RED algorithm works as follows;

For Each incoming packet

- ✓ If AvgQ <= minQ
  - o queue packet
- ✓ If minQ <= AvgQ < maxQ
  - o Mark packet with probability P
- ✓ If maxQ <= AvgQ
  - o Mark the packet

where minQ is Minimum queue threshold, maxQ is Maximum queue threshold, AvgQ is Average Queue length (calculated dynamically), maxP is Maximum drop probability (maxP) and P is Drop probability (calculated dynamically).

Advantages

- ✓ If the RED gateway drops packets when avgQ reached maxQ, the avgQ will never exceed maxQ.
- ✓ Appropriate time scales
- ✓ Source will not be notified of transient congestion.
- ✓ No Global Synchronization.
- ✓ All connection wont back off at same time.
- ✓ Simple
- ✓ High link utilization
- ✓ Fair

Disadvantages

- ✓ Fine tuning minQ, maxQ, maxP and weight needed for optimum performance.
- ✓ RED needs to be deployed at the edge of the network.

3.7.7 Jitter Control

In Computer Networking, jitter refers to the delay variation in the packets' arrival, i.e., a scenario where the time a network packet takes to traverse from one host to the other differ.

Since network-based applications often rely on the timely delivery of network packets, they can suffer from those delay variation (if not handled properly), leading to perceivable abnormalities. As depicted in the example below, the sender sends packets at a constant rate (say one packet per second; black line), but the packets reach the receiver at a variable rate (blue line) , due to the network jitter.

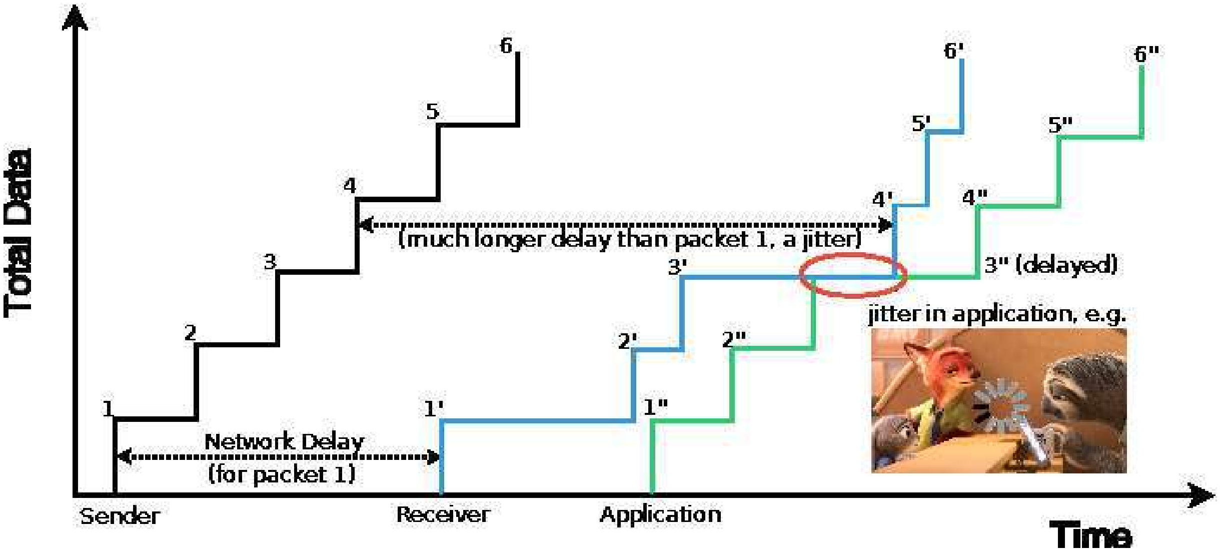


Figure 3.16 Jitter delay

As shown in Figure 3.16, packet 4 takes much longer time to travel across the network than packet 1. Meanwhile, let's assume an application is consuming the received packets at a constant rate (again, one packet per second). The application was able to get packet 1 and 2 timely, but failed when it tried to obtain packet 3 as the packet 3 was not yet delivered! Depending on the application, the missing packet will cause variations in the user experience. For example, the annoying freezes when we watch online video streams.

Therefore, people sometimes refer to network applications' variation in user experience (e.g. video re-buffering) as jitters, too. A perhaps interesting observation is that network jitters can indeed propagate to the application, leading to the "user experience jitters".

3.8 Internetworking

When two or more networks are connected it is called Internet. There will be a variety of different networks will always be around, for the following reasons.

1. Different networks will use different technologies like personal computers run TCP/IP, mainframes run on IBM's SNA.

2. As computers and networks get cheaper, the place where decisions get made moves downwards in organizations.
3. As new hardware developments occur, new software will be created to fit the new hardware.

There are various types of network like LAN, MAN, WAN, ad hoc network, ATM etc. Different types of network varies from each other mainly due to protocol suite and technology used by network and various other parameters.

As an example of how different networks might be connected, consider the example of Figure 3.17. Here we see a corporate network with multiple locations tied together by a wide area ATM network. At one of the locations, an FDDI optical backbone is used to connect an Ethernet, an 802.11 wireless LAN, and the corporate data center's SNA mainframe network.

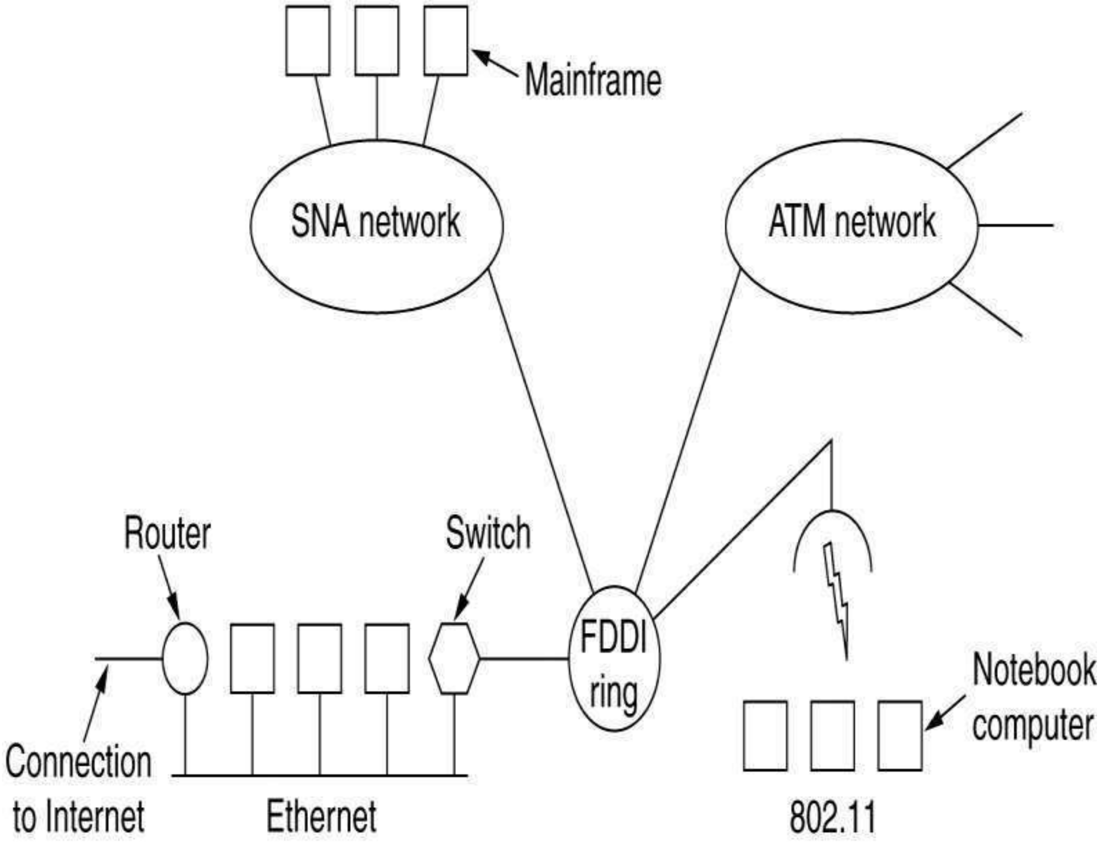


Figure 3.17 A collection of interconnected networks

The purpose of interconnecting all these networks is to allow users on any of them to communicate with users don all the other ones to allow users on any of them to access data on any of them. Networks differ in many ways. In the network layer the following differences can occur.

- ✓ Some of the differences, such as different modulation techniques or frame formats, are in the physical and data link layers.
- ✓ The differing maximum packet sizes used by different networks can be a major nuisance.

- ✓ Address conversions will also be needed, which may require some kind of directory system.
- ✓ Passing multicast packets through a network that does not support multicasting requires generating separate packets for each destination.
- ✓ Error, flow, and congestion control often differ among different networks.
- ✓ Different security mechanisms, parameter settings, and accounting rules, and even national privacy laws also can cause problems

3.8.1 How networks can be connected?

Networks can inter connected by different devices. In the physical layer networks are connected by repeaters or hubs, which just move the bits from one network to an identical network.

At the Data Link layer bridges and switches are used. In network layer, routers are used to connect two network layers, the router may be able to translate between the packet formats. A router that can handle multiple protocols is called a 'multi protocol' router.

In the transport layer we find transport gateways, which can interface between two transport connections (allow packets to flow between a TCP network and an SNA network). Finally, in the application layer, application gateways translate message semantics (gateways between Internet e-mail (RFC 822) and X.400 e-mail).

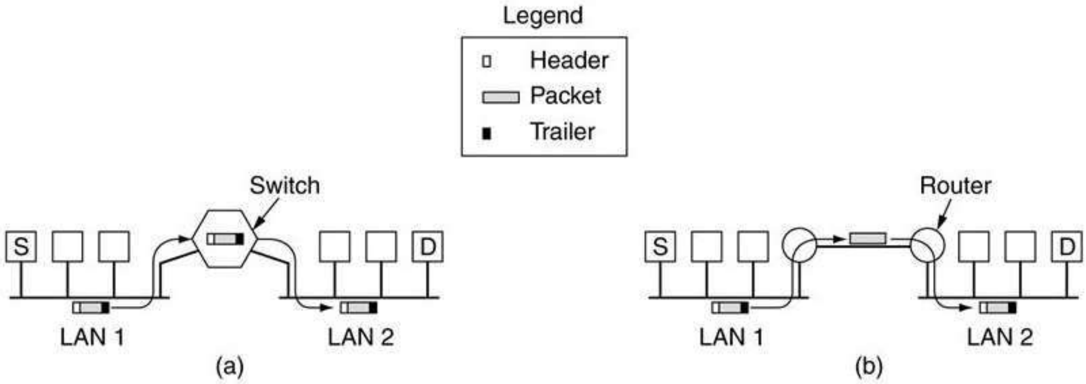


Figure 3.18 Two Ethernets connected by (a) a switch. (b) routers.

To see how that differs from switching in the data link layer, examine Figure 4.1. In a switched network (Figure 3.18.a) the entire frame is transported on the basis of its MAC address. With router(Figure 3.18.b), the packet is extracted from the frame and the address in the packet is used for deciding where to send it. Switches do not have to understand the network layer protocol used to switch packets. Routers do.

3.8.2 Concatenated Virtual Circuits

Two ways of internetworking is possible.(i) a connection-oriented concatenated virtual subnets and (ii) datagram internet. In the past most networks were connection oriented. Then with the rapid acceptance of the Internet, datagrams became more popular. With growing importance of multimedia networking, it is likely that connection-orientation is back in one form or another since it is easier to guarantee quality of service with connections than without them.

In the concatenated virtual-circuit model (see Figure 3.19) a sequence of virtual circuit is set up from the source through one or more gateways to the destination. Each gateway maintains tables telling which virtual circuit pass through it, where they are to be routed, and what the new virtual –circuit number.

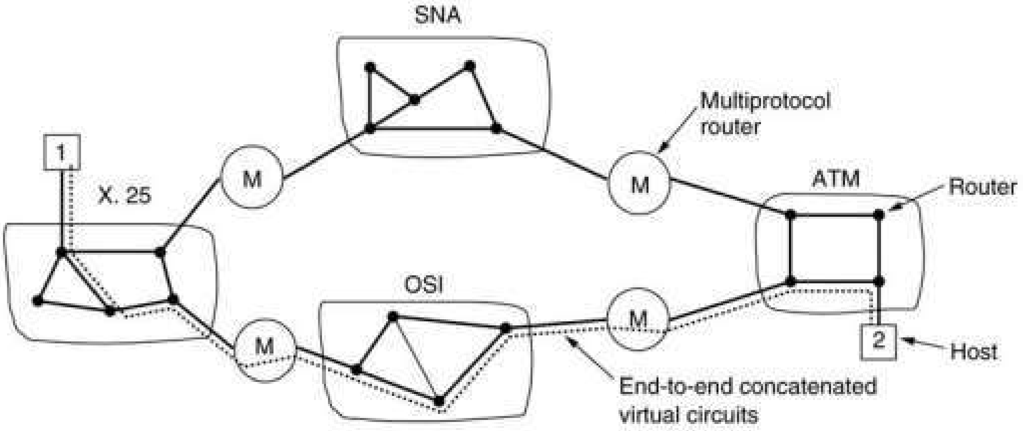


Figure 3.19 Internetworking using concatenated virtual circuits

The essential feature of this approach is that a sequence of virtual circuits is set up from the source through one or more gateways to the destination. Each gateway maintains tables telling which virtual circuits pass through it, where they are to be routed, and what the new virtual-circuit number is.

Concatenated virtual circuits are also common in the transport layer. In particular, it is possible to build a bit pipe using, say, SNA, which terminates in a gateway, and have a TCP connection go from the gateway to the next gateway. In this manner, an end-to-end virtual circuit can be built spanning different networks and protocols.

- **Advantages**
  - ✓ Buffers can be reserved in advance
  - ✓ Sequencing can be guaranteed
  - ✓ Short headers can be used,
  - ✓ The troubles caused by delayed duplicate packets can be avoided.
- **Disadvantages**
  - ✓ Table space required in the routers for each open connection,
  - ✓ No alternate routing to avoid congested areas,
  - ✓ Vulnerability to router failures along the path,
  - ✓ Difficult to implement if one of the networks involved is an unreliable datagram network.

3.8.3 Connectionless Internetworking

The alternative internetwork model is the datagram model, shown in Figure 3.20. In datagrams from one host to other host the packets will be routed in different routes through the inter network. A routing decision is made separately for each packet, possibly depending on the traffic at the moment the packet is sent. This strategy can use multiple routes and thus achieve a higher bandwidth than the concatenated virtual circuit model.

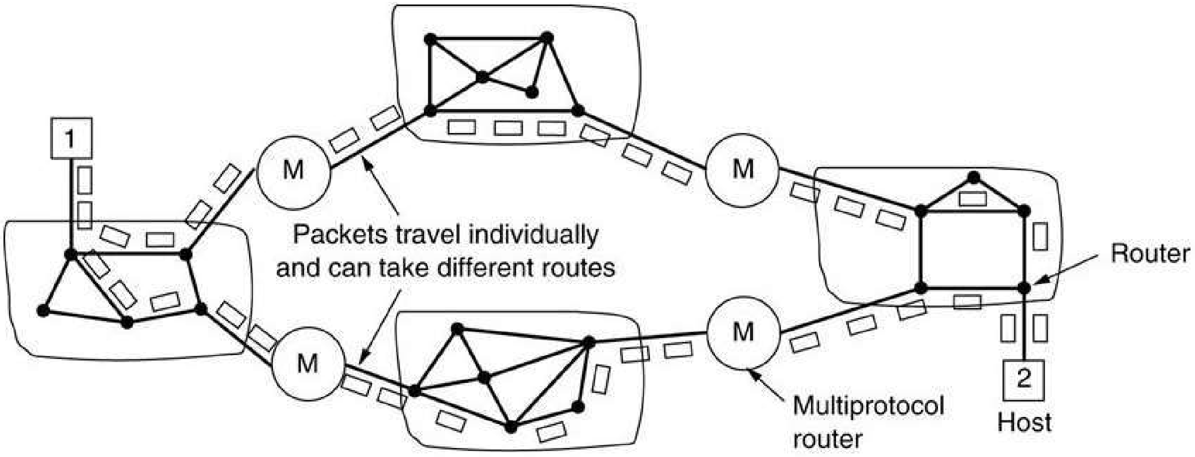


Figure 3.20 A connectionless internet

- **Issues**
  - ✓ If each network has its own network layer protocol, it is not possible for a packet from one network to transit another one.
  - ✓ A more serious problem is addressing. Imagine a simple case: a host on the Internet is trying to send an IP packet to a host on an adjoining SNA network. The IP and SNA addresses are different.
- **Solution**
  - ✓ Design a universal "internet" packet and have all routers recognize it.
- **Advantages**
  - ✓ It can be used over subnets that do not use virtual circuits inside.
- **Disadvantages**
  - ✓ more potential for congestion, but also more potential for adapting to it
  - ✓ robustness in the face of router failures
  - ✓ longer headers needed,
  - ✓ for every packet, route needs to decided.

3.8.4 Tunneling

The source and destination hosts are on the same type of network but there is a different network in between 'Tunneling' will be used. An ex, think of an organization with TCP/IP based Ethernet at one place and a TCP/IP base Ethernet in other place, and a PTT WAN in between as shown in Figure 3.21.

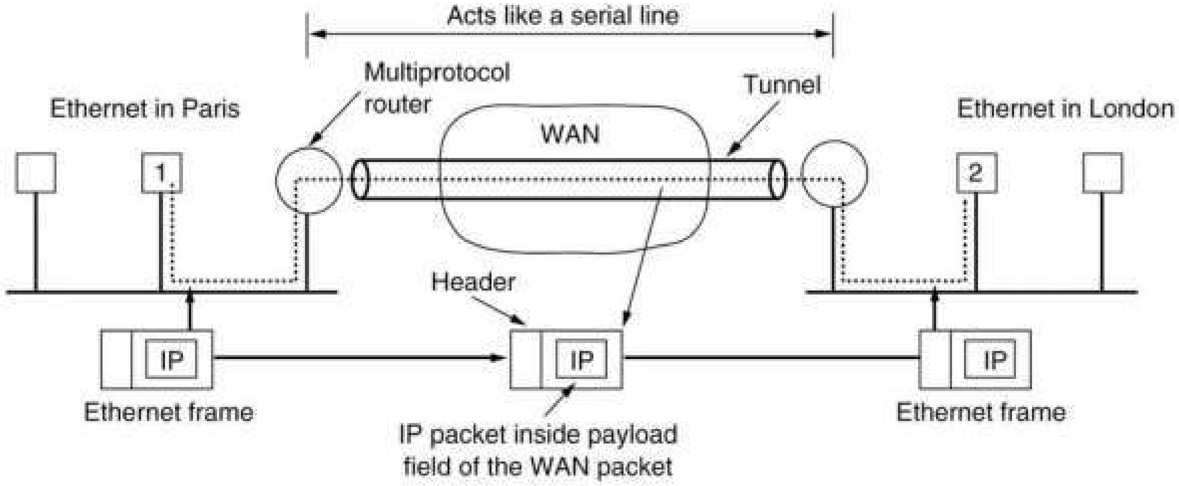


Figure 3.21 Tunneling a packet from Paris to London

Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation. The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.

Tunneling of packets through a foreign network works the same way. To send an IP packet to host 2, host 1, constructs the packet containing IP address of host 2, inserts it into an Ethernet frame addressed to the multi-protocol router, and puts it on the Ethernet. When the multiprotocol router gets the frame, it removes the IP packet, inserts it in the payload field of the WAN network layer packet, and addresses the latter to the WAN address of the other multi-protocol router to the other. Only the multiprotocol router has to understand IP and WAN packets.

Consider an example a person driving his car from one place to other under its own power. Let in between he has to cross a river, which has no bridge. Hence his car has to be kept on a boat and transported to another end. From there, the car continues to move under its own power.

3.8.5 Fragmentation

Each network imposes some maximum size on its packets. These limits have various causes, among them:

1. Hardware (e.g., the size of an Ethernet frame).
2. Operating system (e.g., all buffers are 512 bytes).
3. Protocols (e.g., the number of bits in the packet length field).
4. Compliance with some (inter)national standard.
5. Desire to reduce error-induced retransmissions to some level.
6. Desire to prevent one packet from occupying the channel too long.

The result of all these factors is that the network designers are not free to choose any maximum packet size they wish. Maximum payloads range from 48 bytes (ATM cells) to 65,515 bytes (IP packets), although the payload size in higher layers is often larger.

The only solution to the problem is to allow gateways to break up packets into ***fragments***, sending each fragment as a separate internet packet.

Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held a frame i.e., its Maximum Transmission Unit (MTU). The network layer divides the datagram received from transport layer into fragments so that data flow is not disrupted.

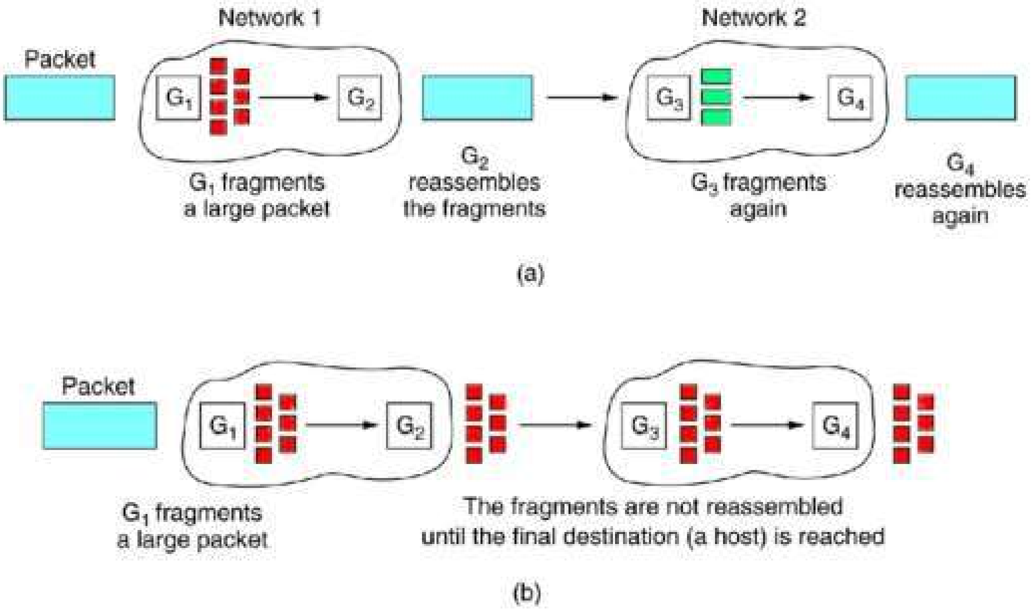

Network 1
Network 2
Packet
G_1
G_2
G_3
G_4
G_1 fragments a large packet
G_2 reassembles the fragments
G_3 fragments again
G_4 reassembles again
(a)
Packet
G_1
G_2
G_3
G_4
G_1 fragments a large packet
The fragments are not reassembled until the final destination (a host) is reached
(b)

Figure 3.22 (a) Transparent fragmentation. (b) Non-transparent fragmentation.

Two opposing strategies exist as shown in Figure 3.22 for recombining the fragments back into the original packet.

- ***Transparent Fragmentation Issues***
  - ✓ The exit gateway fragments the big packet into small packets based on the transmission.
  - ✓ All the host should have capability of reassembly based on the next transmission.
  - ✓ Repeated work of fragment and reassemble.
- ***Non-transparent Fragmentation Issues:***
  - ✓ Exit gateway need to know about all the packets that were part of same big packet.
  - ✓ all the small packets that belongs to same big packet need to travel through same exit gateway.
  - ✓ Small packets increase overhead because each packet carries header.

3.9 Short Questions and Answers

1. What is datagram?

A datagram is a basic transfer unit associated with a packet-switched network. Datagrams are typically structured in header and payload sections. Datagrams provide a connectionless communication service across a packet-switched network. The delivery, arrival time, and order of arrival of datagrams need not be guaranteed by the network.

2. Define datagram.

The RFC 1594 standard defines datagram as "A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network."

3. What is meant by virtual circuit?

If connection-oriented service is used, a path from the source router to the destination router must be established before any data packets can be sent. This connection is called a VC (virtual circuit).

4. What are the responsibilities of Network Layer?

The Network Layer is responsible for the source-to-destination delivery of packet possibly across multiple networks (links).

   a. Logical Addressing
   b. Routing.

5. What is routing?

Routing is a process of selecting paths in a network through which network traffic is sent.

6. Define router.

A router can be hardware device with a software application. The router is connected to at least two networks and do the routing operations.

7. Define Routing algorithm.

It is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.

8. Define Session routing.

Data packets just follow the already established route. The latter case is sometimes called ***session routing*** because a route remains in force for an entire session (e.g., a login session at a terminal or a file transfer)

9. What is forwarding in Routing Algorithm?

It is sometimes useful to make a distinction between routing, which is making the decision which routes to use, and forwarding, which is what happens when a packet arrives.

One can think of a router as having two processes inside it. One of them handles each packet as it arrives, looking up the outgoing line to use for it in the routing tables. This process is ***forwarding***.

10. List the properties of routing algorithms.

- ✓ correctness,
- ✓ simplicity,
- ✓ robustness,
- ✓ stability,
- ✓ fairness,
- ✓ and optimality

11. How will we the classify Routing algorithms?

Routing algorithms can be grouped into two major classes:

- **Non Adaptive algorithms** do not base their routing decisions on any measurements or estimates of the current topology and traffic.
- **Adaptive algorithms** change their routing decisions to reflect changes in the topology, and sometimes changes in the traffic as well. These *dynamic routing* algorithms differ in where they get their information (e.g.,locally, from adjacent routers, or from all routers)

12. What is meant by sink tree?

As a consequence of that principle, 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.

13. What is Flooding in routing?

Flooding is a static algorithm, in which every incoming packet is sent out on every outgoing line except the one it arrived on. Flooding obviously generates vast numbers of duplicate packets.

14. What is meant by Selective Flooding?

A variation of flooding that is slightly more practical is selective flooding. In this algorithm the routers do not send every incoming packet out on every line, only on those lines that are going approximately in the right direction.

15. What is broadcast routing?

In broadcast routing, packets are sent to all nodes even if they do not want it. Routers create broadcast domains. But it can be configured to forward broadcasts in some special cases. A broadcast message is destined to all network devices. A router creates a data packet and then sends it to each host one by one. In this case, the router creates multiple copies of single data packet with different destination addresses.

16. What is multicast routing?

Multicast routing is a networking method for efficient distribution of one-to-many traffic. A multicast source, such as a live video conference, sends traffic in one stream to a multicast group. The multicast group contains receivers such as computers, devices, and IP phones.

17. Define congestion.

Congestion in a network may occur if the load on the network, the number of packets sent to the network, is greater than the capacity of the network, the number of packets a network can handle.

18. What is congestion control?

Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

19. What are the factors will lead to congestion?

- ✓ Incoming capacity greater than the outgoing capacity
- ✓ Slow processors (routers) can cause congestion.
- ✓ Low band-width lines also cause congestion

20. Differentiate congestion control and flow control

Congestion control is different than flow control. Flow control is a data link issue, and concerns only one sender outrunning a single receiver (e.g. a point-to-point link). Congestion control is a network layer issue, and is thus concerned with what happens when there is more data in the network than can be sent with reasonable packet delays, no lost packets, etc. Flow control is a local, congestion control is global.

One means of handling congestion is by using a flow control mechanism to reduce the traffic put on the net by a particular host, hence the confusion.

21. How do you overcome congestion in virtual circuit network?

The following approaches used to dynamically control congestion in virtual- circuit subnets.

- ✓ Admission control
- ✓ Creating new virtual circuit
- ✓ Feedback mechanism

22. How do you overcome congestion in datagram network?

The following approaches are used to control congestion in datagram network.

- ✓ The warning bit method
- ✓ Choke packets

23. What is meant by load shedding?

When none of the approach work, finally router stats discarding packet. This ss called load shedding. Instead of randomly discarding packets, if packets are discarded on base of application, less retransmission will occur.

24. What is meant by Random Early Detection (RED)?

RED provides congestion avoidance by controlling the queue size at the gateway. RED notifies the source before the congestion actually happens rather than wait till it actually occurs. RED provides a mechanism for the gateway to provide some feedback to the source on congestion status.

25. Define jitter.

In Computer Networking, jitter refers to the delay variation in the packets' arrival, i.e., a scenario where the time a network packet takes to traverse from one host to the other differ.

26. What is meant by fragmentation?

Fragmentation is done by the network layer when the maximum size of datagram is greater than maximum size of data that can be held a frame i.e., its Maximum Transmission Unit (MTU). The network layer divides the datagram received from transport layer into fragments so that data flow is not disrupted.

27. What is meant by Tunneling?

Tunneling involves allowing private network communications to be sent across a public network, such as the Internet, through a process called encapsulation. The encapsulation process allows for data packets to appear as though they are of a public nature to a public network when they are actually private data packets, allowing them to pass through unnoticed.

3.10 Explanatory Questions

1. Discuss about Store-and-Forward Packet Switching. (5 marks)
2. Write about the implementation methods of connectionless service. (5 marks)
3. Write about the implementation methods of connection-oriented service. (5 marks)
4. Compare Virtual-Circuit and Datagram Subnets. (5 marks)
5. Discuss about the types of routing algorithms. (5 marks)
6. Explain about shortest path routing algorithm. (5 marks)
7. Discuss about the flooding algorithm. (5 marks)
8. Write about broadcast routing algorithm. (5 marks)
9. Explain the multicast routing algorithm. (5 marks)
10. Write about congestion prevention policies. (5 marks)
11. How do control congestion in virtual-circuit subnets? Explain. (5 marks)
12. How do control congestion in datagram subnets? Explain. (5 marks)
13. Discuss about load shedding in congestion control. (5 marks)
14. Explain about jitter control. (5 marks)
15. Write short notes on Tunneling. (5 marks)
16. Discuss about data fragmentation in network layer. (5 marks)
17. Explain data link layer design issues. (10 marks)
18. Discuss in detail about the routing algorithms. (10 marks)

19. Explain the congestion control mechanism followed in network layer. (10 marks)
20. Write detail notes about internetworking achieved in computer network. (10 marks)

3.11 Objective Questions

1. The network layer concerns with

a) bits
b) frames
c) packets
d) none of the mentioned

Answer : c

2. Which one of the following is not a function of network layer?

a) routing
b) inter-networking
c) congestion control
d) none of the mentioned

Answer : d

3. In virtual circuit network each packet contains

a) full source and destination address
b) a short VC number
c) only source address
d) only destination address

Answer : b

4. Which one of the following routing algorithm can be used for network layer design?

a) shortest path algorithm
b) distance vector routing
c) link state routing
d) all of the mentioned

Answer : d

5. Multidestination routing

a) is same as broadcast routing
b) contains the list of all destinations
c) data is not sent by packets
d) none of the mentioned

Answer : c

6. A subset of a network that includes all the routers but contains no loops is called

a) spanning tree
b) spider structure
c) spider tree

d) none of the mentioned

Answer : a

7. Which one of the following algorithm is not used for congestion control?

a) traffic aware routing
b) admission control
c) load shedding
d) none of the mentioned

Answer : d

8. The network layer protocol of internet is

a) ethernet
b) internet protocol
c) hypertext transfer protocol
d) none of the mentioned

Answer : b

9. Datagram switching is done at which layer of OSI model?

a) Network layer
b) Physical layer
c) Application layer
d) Transport layer

Answer : a

10. Packets in datagram switching are referred to as

a) Switches
b) Segments
c) Datagrams
d) Data-packets

Answer : c

11. Datagram networks mainly refers to

a) Connection oriented networks
b) Connection less networks
c) Telephone networks
d) Internetwork

Answer : b

12. Datagrams are routed to their destinations with the help of

a) Switch table
b) Segments table
c) Datagram table
d) Routing table

Answer : c

13. The main contents of the routing table in datagram networks are

a) Source and Destination address
b) Destination address and Output port
c) Source address and Output port
d) Input port and Output port

Answer : b

14. Which of the following remains same in the header of the packet in a datagram network during the entire journey of the packet?

a) Destination address
b) Source address
c) Checksum
d) Padding

Answer : a

15. Which of the following is true with respect to the delay in datagram networks?

a) Delay is greater than in a virtual circuit network
b) Each packet may experience a wait at a switch
c) Delay is not uniform for the packets of a message
d) All of the mentioned

Answer : d

16. During datagram switching, the packets are placed in __________ to wait until the given transmission line becomes available.

a) Stack
b) Queue
c) Hash
d) Routing table

Answer : b

17. Which of the following is true with respect to the datagram networks?

a) Number of flows of packets are not limited
b) Packets may not be in order at the destination
c) Path is not reserved
d) All of the mentioned

Answer : d

18. Which of the following is not a characteristic of Virtual Circuit Network?

a) There are setup and teardown phases in addition to the data transfer phase
b) Resources can be allocated during setup phase or on demand
c) All packets follow the same path established during the connection
d) Virtual circuit network is implemented in application layer

Answer : d

19. The address that is unique in the scope of the network or internationally if the network is part of an international network is called as ______

a) Global address
b) Network address
c) Physical address
d) IP address

Answer : a

20. The Identifier that is used for data transfer in virtual circuit network is called _______

a) Global address
b) Virtual circuit identifier
c) Network identifier
d) IP identifier

Answer : b

21. Which of the following is not a phase of virtual circuit network?

a) Setup phase
b) Data transfer phase
c) Termination phase
d) Teardown phase

Answer : c

22. Steps required in setup process are ___________

a) Setup request and acknowledgement
b) Setup request and setup response
c) Setup request and setup termination
d) Setup and termination steps

Answer : a

23. During teardown phase, the source, after sending all the frames to destination, sends a _____ to notify termination.

a) teardown response
b) teardown request
c) termination request
d) termination response

Answer : b

24. Delay of the resource allocated during setup phase during data transfer is ________

a) constant
b) increases for each packet
c) same for each packet
d) different for each packet

Answer : c

25. Delay of the resource allocated on demand during data transfer is ________

a) constant
b) increases for each packet
c) same for each packet
d) different for each packet

Answer : d

26. In virtual circuit network, the number of delay times for setup and teardown respectively are _______

a) 1 and 1
b) 1 and 2
c) 2 and 1
d) 2 and 2

Answer : a

27. In data transfer phase, how many columns does the table contain?

a) 1
b) 2
c) 3
d) 4

Answer : d

28. Alternate and adaptive routing algorithm belongs to ……….

a). static routing
b). permanent routing
c). standard routing
d). dynamic routing

Answer : d

29. In multicast routing, each involved router needs to construct a ……… path tree for each group.

a). average
b). longest
c). shortest
d). very longest

Answer : c

30. A subset of a network that includes all the routers but contains no loops is called

a). spanning tree
b). spider structure
c). spider tree
d). none of the mentioned

Answer : a

31. What is the function of a router?

   a). converting the data from one format to another
   b). Forward the packet to the up links
   c). error detection in data
   d). None of the above

   Answer : b

32. What does Router do in a network?

   a). Forwards a packet to all outgoing links
   b). Forwards a packet to the next free outgoing link
   c). Determines on which outing link a packet is to be forwarded
   d). Forwards a packet to all outgoing links except the originated link

   Answer : c

33. In multicast communication, the relationship is

   a). One to one
   b). One to many
   c). Many to one
   d). Many to many

   Answer : b

34. Two broad categories of congestion control are

   a) Open-loop and Closed-loop
   b) Open-control and Closed-control
   c) Active control and Passive control
   d) Active loop and Passive loop

   Answer : a

35. In open-loop control, policies are applied to __________

   a) Remove after congestion occurs
   b) Remove after sometime
   c) Prevent before congestion occurs
   d) Prevent before sending packets

   Answer : c

36. Retransmission of packets must not be done when _______

   a) Packet is lost
   b) Packet is corrupted
   c) Packet is needed
   d) Packet is error-free

   Answer : d

37. Discarding policy is mainly done by _______

a) Sender
b) Receiver
c) Router
d) Switch

Answer : c

38. Closed-Loop control mechanisms try to _________

a) Remove after congestion occurs
b) Remove after sometime
c) Prevent before congestion occurs
d) Prevent before sending packets

Answer : a

39. The technique in which a congested node stops receiving data from the immediate upstream node or nodes is called as _______

a) Admission policy
b) Backpressure
c) Forward signaling
d) Backward signaling

Answer : b

40. Backpressure technique can be applied only to _______

a) Congestion networks
b) Closed circuit networks
c) Open circuit networks
d) Virtual circuit networks

Answer : d

41. The packet sent by a node to the source to inform it of congestion is called _______

a) Explicit
b) Discard
c) Choke
d) Backpressure

Answer : c

4 Transport Layer

4.1 Introduction

The transport layer is responsible for process-to-process delivery of the entire message. A process is an application program running on a host. Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does. The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

> The transport layer is responsible for the delivery of a message from one process to another.

Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process on one computer to a specific process on the other. The transport layer header must therefore include a type of address called a *service-point address* in the OSI model and port number or port addresses in the Internet and TCP/IP protocol suite.

A transport layer protocol can be either connectionless or connection-oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data is transferred, the connection is terminated. In the transport layer, a message is normally divided into transmittable segments.

A connectionless protocol, such as UDP, treats each segment separately. A connection-oriented protocol, such as TCP and SCTP, creates a relationship between the segments using sequence numbers. Like the data link layer, the transport layer may be responsible for flow and error control. However, flow and error control at this layer is performed end to end rather than across a single link. UDP, is not involved in flow or error control. On the other hand, the other two protocols, TCP and SCTP, use sliding windows for flow control and an acknowledgment system for error control

4.2 Transport Services

The services that a transport protocol should provide to higher-level protocols are illustrated in Figure 4.1.

In a system, there is a transport entity that provides services to Transport Service (TS) users, which might be an application process or a session-protocol entity. This local transport entity communicates with some remote-transport entity, using the services of some lower layer, such as the network layer.

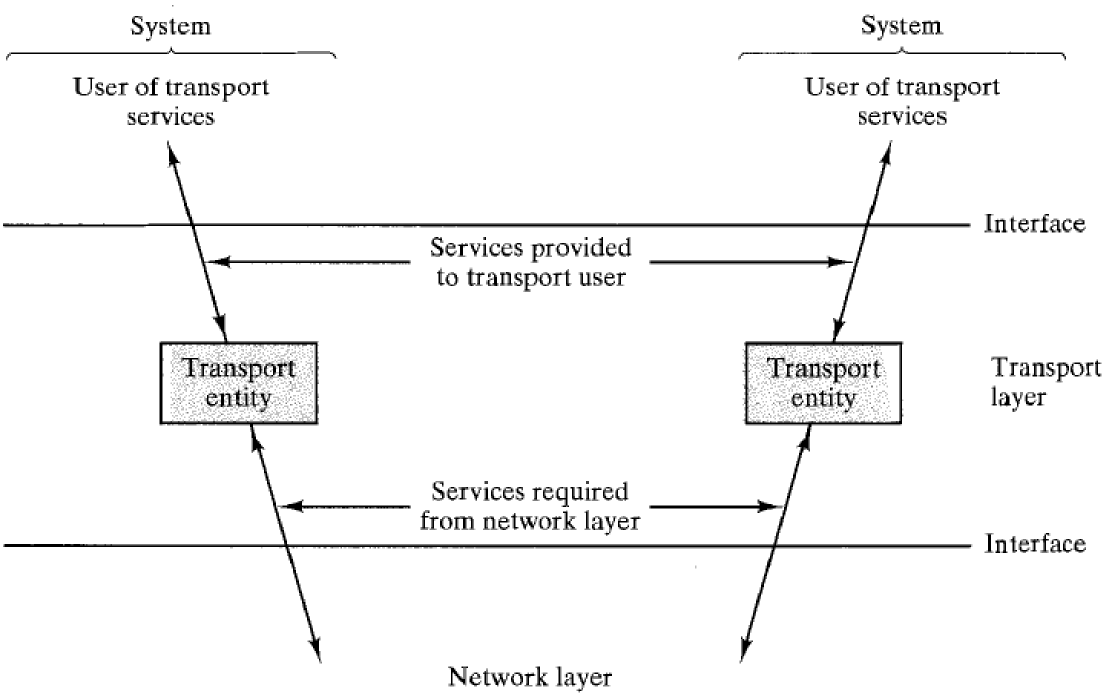

System
User of transport services
System
User of transport services
Interface
Services provided to transport user
Transport entity
Transport entity
Transport layer
Services required from network layer
Interface
Network layer

Figure 4.1 Transport entity context.

The general service provided by a transport protocol is the end-to-end transport of data in a way that shields the TS user from the details of the underlying communications systems.

The specific services that a transport protocol provides are

- ✓ Quality of service
- ✓ Data transfer
- ✓ User interface
- ✓ Connection management
- ✓ Expedited delivery
- ✓ Status reporting
- ✓ Security

- **Type of Service**

Two basic types of service are possible:

- ✓ connection-oriented and
- ✓ connectionless, or datagram service.

A connection-oriented service provides for the establishment, maintenance, and termination of a logical connection between TS users. This has been the most common type of protocol service available and has a wide variety of applications. The connection-oriented service generally implies that the service is reliable. The strengths of the connection-oriented approach are clear. It allows for connection-related features such as flow control, error control, and sequenced delivery.

At lower layers (internet, network), connectionless service is more robust. In addition, it represents a "least common denominator" of service to be expected at higher layers. Further, even at transport and above, there is justification for a connectionless service. There are instances in which the overhead of connection establishment and maintenance is unjustified or even counterproductive.

Some examples follow:

- **Inward data collection.** Involves the periodic active or passive sampling of data sources, such as sensors, and automatic self-test reports from security equipment or network components. In a real-time monitoring situation, the loss of an occasional data unit would not cause distress, as the next report should arrive shortly.
- **Outward data dissemination.** Includes broadcast messages to network users, the announcement of a new node or the change of address of a service, and the distribution of real-time clock values.
- **Request-response.** Applications in which a transaction service is provided by a common server to a number of distributed TS users, and for which a single request-response sequence is typical. Use of the service is regulated at the application level, and lower-level connections are often unnecessary and cumbersome.
- **Real-time applications.** Such as voice and telemetry, involving a degree of redundancy and/or a real-time transmission requirement; these must not have connection-oriented functions, such as retransmission.

Thus, there is a place at the transport level for both a connection-oriented and a connectionless type of service.

4.2.1 Quality of Service

The transport protocol entity should allow the TS user to specify the quality of transmission service to be provided. The transport entity will attempt to optimize the use of the underlying link, network, and internet resources to the best of its ability, so as to provide the collective requested services.

Examples of services that might be requested are

- ✓ Acceptable error and loss levels
- ✓ Desired average and maximum delay
- ✓ Desired average and minimum throughput
- ✓ Priority levels

Of course, the transport entity is limited to the inherent capabilities of the underlying service. For example, IP does provide a quality-of-service parameter. It allows for specification of eight levels of precedence or priority as well as a binary specification for normal or low delay, normal or high throughput, and normal or high reliability. Thus, the transport entity can "pass the buck" to the internetwork entity. However, the internet protocol entity is itself limited; routers have some freedom to schedule items preferentially from buffers, but beyond that are still dependent on the underlying transmission facilities. Here is another example: X.25 provides for throughput class negotiation as an optional user facility. The network may alter flow control parameters and the amount of network resources allocated on a virtual circuit to achieve desired throughput.

The transport layer may also resort to other mechanisms to try to satisfy TS user requests, such as splitting one transport connection among multiple virtual circuits to enhance throughput.

The TS user of the quality-of-service feature needs to recognize that

- Depending on the nature of the transmission facility, the transport entity will have varying degrees of success in providing a requested grade of service.
- There is bound to be a trade-off among reliability, delay, throughput, and cost of services.

Nevertheless, certain applications would benefit from, or even require, certain qualities of service and, in a hierarchical or layered architecture, the easiest way for an application to extract this quality of service from a transmission facility is to pass the request down to the transport protocol.

Examples of applications that might request particular qualities of service are as follows:

- A file transfer protocol might require high throughput. It may also require high reliability to avoid retransmissions at the file transfer level.
- A transaction protocol (e.g., web browser-web server) may require low delay.
- An electronic mail protocol may require multiple priority levels.

One approach to providing a variety of qualities of service is to include a quality-of-service facility within the protocol; we have seen this with IP and will see that transport protocols typically follow the same approach. An alternative is to provide a different transport protocol for different classes of traffic; this is to some extent the approach taken by the ISO-standard family of transport protocols.

4.2.2 Data Transfer

The whole purpose of a transport protocol is to transfer data between two transport entities. Both user data and control data must be transferred, either on the same channel or separate channels. Full-duplex service must be provided. Half-duplex and simplex modes may also be offered to support peculiarities of particular TS users.

4.2.3 User Interface

It is not clear that the exact mechanism of the user interface to the transport protocol should be standardized. Rather, it should be optimized to the station environment.

As examples, a transport entity's services could be invoked by

- ✓ Procedure calls.
- ✓ Passing of data and parameters to a process through a mailbox.
- ✓ Use of direct memory access (DMA) between a host user and a front-end processor containing the transport entity.

A few characteristics of the interface may be specified, however. For example, a mechanism is needed to prevent the TS user from swamping the transport entity with data. A similar mechanism is needed to prevent the transport entity from swamping a TS user with data. Another aspect of the interface has to do with the timing and significance of confirmations. Consider the following: A TS user passes data to a transport entity to be delivered to a remote TS user. The local transport entity can acknowledge receipt of the data immediately, or it can wait until the remote transport entity reports that the data have made it through to the other end. Perhaps the most useful interface is one that allows immediate acceptance or rejection of requests, with later confirmation of the end-to-end significance.

4.2.4 Connection Management

When connection-oriented service is provided, the transport entity is responsible for establishing and terminating connections. A symmetric connection-establishment procedure should be provided, which allows either TS user to initiate connection establishment. An asymmetric procedure may also be provided to support simplex connections. Connection termination can be either *abrupt* or *graceful.* With an abrupt termination, data in transit may be lost. A graceful termination prevents either side from shutting down until all data have been delivered.

4.2.5 Expedited Delivery

A service similar to that provided by priority classes is the expedited delivery of data. Some data submitted to the transport service may supersede data submitted previously. The transport entity will endeavor to have the transmission facility transfer the data as rapidly as possible. At the receiving end, the transport entity will interrupt the TS user to notify it of the receipt of urgent data. Thus, the expedited data service is in the nature of an interrupt mechanism, and is used to transfer occasional urgent data, such as a break character from a terminal or an alarm condition. In contrast, a priority service might dedicate resources and adjust parameters such that, on average, higher priority data are delivered more quickly.

4.2.6 Status Reporting

A status reporting service allows the TS user to obtain or be notified of information concerning the condition or attributes of the transport entity or a transport connection.

Examples of status information are

- ✓ Performance characteristics of a connection (e.g., throughput, mean delay)
- ✓ Addresses (network, transport)
- ✓ Class of protocol in use
- ✓ Current timer values
- ✓ State of protocol "machine" supporting a connection

✓ Degradation in requested quality of service

4.2.7 Security

The transport entity may provide a variety of security services. Access control may be provided in the form of local verification of sender and remote verification of receiver. The transport service may also include encryption/decryption of data on demand. Finally, the transport entity may be capable of routing through secure links or nodes if such a service is available from the transmission facility.

4.3 Elements of Transport Protocols

The transport service is implemented by a **transport protocol** used between the two transport entities. In some ways, transport protocols resemble the data link protocols. Both the protocols have to deal with error control, sequencing, and flow control among other issues.

However, significant differences between the two also exist. These differences are due to major dissimilarities between the environments in which the two protocols operate, as shown in Figure 4.2. At the data link layer, two routers communicate directly via a physical channel, whereas at the transport layer, this physical channel is replaced by the entire subnet. This difference has many important implications for the protocols.

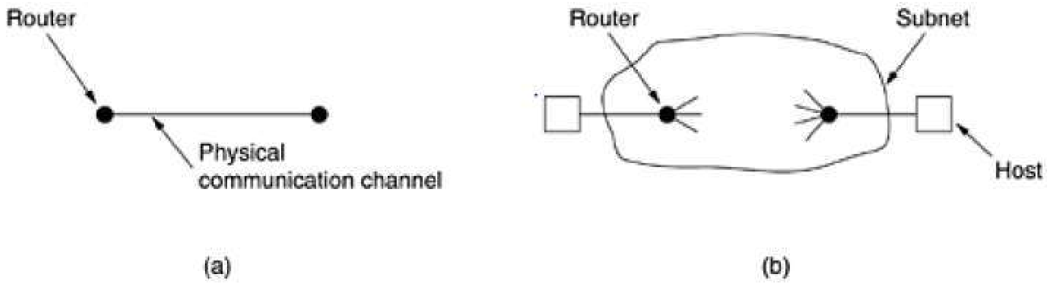


Figure 4.2. (a) Environment of the data link layer. (b) Environment of the transport layer.

For one thing, in the data link layer, it is not necessary for a router to specify which router it wants to talk to—each outgoing line uniquely specifies a particular router. In the transport layer, explicit addressing of destinations is required.

For another thing, the process of establishing a connection over the wire of Figure 4.2(a) is simple: the other end is always there (unless it has crashed, in which case it is not there). Either way, there is not much to do. In the transport layer, initial connection establishment is more complicated.

Another, exceedingly annoying, difference between the data link layer and the transport layer is the potential existence of storage capacity in the subnet. When a router sends a frame, it may arrive or be lost, but it cannot bounce around for a while, go into hiding in a far corner of the world, and then suddenly emerge at an inopportune moment 30 sec later. If the subnet uses datagrams and adaptive routing inside, there is a non-negligible probability that a packet may be stored for a number of seconds and then delivered later. The consequences of the subnet's ability to store packets can sometimes be disastrous and can require the use of special protocols.

A final difference between the data link and transport layers is one of amount rather than of kind. Buffering and flow control are needed in both layers, but the presence of a large and dynamically varying number of connections in the transport layer may require a different approach than we used in the data link layer. Some of the protocols allocate a fixed number of buffers to each line, so that when a frame arrives a buffer is always available. In the transport layer, the larger number of connections that must be managed make the idea of dedicating many buffers to each one less attractive.

4.3.1 Addressing

The issue concerned with addressing is simply this: A user of a given transport entity wishes to either establish a connection with or make a connectionless data transfer to a user of some other transport entity. The target user needs to be specified by all of the following:

- User identification
- Transport entity identification
- Station address
- Network number

The transport protocol must be able to derive the information listed above from the TS user address. Typically, the user address is specified as *station* or port. The *port* variable represents a particular TS user at the specified station; in OSI, this is called a transport service access point (TSAP). Generally, there will be a single transport entity at each station, so a transport entity identification is not needed. If more than one transport entity is present, there is usually only one of each type. In this latter case, the address should include a designation of the type of transport protocol (e.g., TCP, UDP). In the case of a single network, *station* identifies an attached network device. In the case of an internet, station is a global internet address. In TCP, the combination of port and station is referred to as a socket. Because routing is not a concern of the transport layer, it simply passes the station portion of the address down to the network service. Port is included in a transport header, to be used at the destination by the destination transport protocol.

One question remains to be addressed: How does the initiating TS user know the address of the destination TS user? Two static and two dynamic strategies suggest themselves:

a. The TS user must know the address it wishes to use ahead of time; this is basically a system configuration function. For example, a process may be running that is only of concern to a limited number of TS users, such as a process that collects statistics on performance. From time to time, a central network management routine connects to the process to obtain the statistics. These processes generally are not, and should not be, well-known and accessible to all.

2. Some commonly used services are assigned "well-known addresses" (for example, time sharing and word processing).

3. A name server is provided. The TS user requests a service by some generic or global name. The request is sent to the name server, which does a directory lookup and returns an address. The transport entity then proceeds with the connection. This service is useful for commonly used applications that change location from time to time. For example, a data entry process may be moved from one station to another on a local network in order to balance load.

4. In some cases, the target user is to be a process that is spawned at request time. The initiating user can send a process request to a well-known address. The user at that address is a privileged system process that will spawn the new process and return an address. For example, a programmer has developed a private application (e.g., a simulation program) that will execute on a remote mainframe but be invoked from a local minicomputer. An RJE-type request can be issued to a remote job-management process that spawns the simulation process

4.3.2 Connection Establishment and Connection Release

A TCP connection begins with a client (caller) doing an active open to a server (callee). Assuming that the server had earlier done a passive open, the two sides engage in an exchange of messages to establish the connection. Only after this connection establishment phase is over do the two sides begin sending data. Likewise, as soon as a participant is done sending data, it closes one direction of the connection, which causes TCP to initiate a round of connection termination messages.

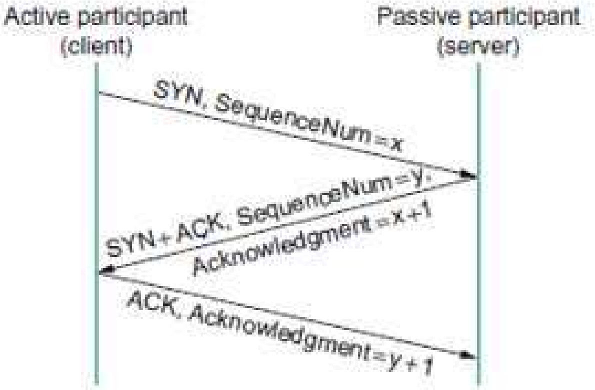


Figure 4.3 Timeline for three-way handshake algorithm

Notice that, while connection setup is an asymmetric activity (one side does a passive open and the other side does an active open), connection teardown is symmetric (each side has to close the connection independently). Therefore, it is possible for one side to have done a close, meaning that it can no longer send data, but for the other side to keep the other half of the bidirectional connection open and to continue sending data.

- **Three-Way Handshake**

The algorithm used by TCP to establish and terminate a connection is called a *three-way handshake*. The three-way handshake involves the exchange of three messages between the client and the server, as illustrated by the timeline given in Figure 4.3.

The idea is that two parties want to agree on a set of parameters, which, in the case of opening a TCP connection, are the starting sequence numbers the two sides plan to use for their respective byte streams. In general, the parameters might be any facts that each side wants the other to know about.

1. First, the client (the active participant) sends a segment to the server (the passive participant) stating the initial sequence number it plans to use (Flags = SYN, SequenceNum = x).
2. The server then responds with a single segment that both acknowledges the client's sequence number (Flags = ACK, Ack = x+1) and states its own beginning sequence number (Flags = SYN, SequenceNum = y). That is, both the SYN and ACK bits are set in the Flags field of this second message.
3. Finally, the client responds with a third segment that acknowledges the server's sequence number (Flags = ACK, Ack = y +1).

The reason why each side acknowledges a sequence number that is one larger than the one sent is that the Acknowledgment field actually identifies the "next sequence number expected," thereby implicitly acknowledging all earlier sequence numbers. Although not shown in this timeline, a timer is scheduled for each of the first two segments, and if the expected response is not received the segment is retransmitted. It would be simpler if each side simply started at some "well-known" sequence number, such as 0. In fact, the TCP specification requires that each side of a connection select an initial starting sequence number at random.

The reason for the client and server to exchange starting sequence numbers with each other at connection setup time is to protect against two incarnations of the same connection reusing the same sequence numbers too soon—that is, while there is still a chance that a segment from an earlier incarnation of a connection might interfere with a later incarnation of the connection.

- **State-Transition Diagram**

TCP is complex enough that its specification includes a state-transition diagram. A copy of this diagram is given in *Figure 4.4*. This diagram shows only the states involved in opening a connection (everything above ESTABLISHED) and in closing a connection (everything below ESTABLISHED). Everything that goes on while a connection is open—that is, the operation of the sliding window algorithm—is hidden in the ESTABLISHED state.

TCP's state-transition diagram is fairly easy to understand. Each circle denotes a state that one end of a TCP connection can find itself in. All connections start in the CLOSED state. As the connection progresses, the connection moves from state to state according to the arcs. Each arc is labelled with a tag of the form *event/action*. Thus, if a connection is in the LISTEN state and a SYN segment arrives (i.e., a segment with the SYN flag set), the connection makes a transition to the SYN RCVD state and takes the action of replying with an ACK+SYN segment. Notice that two kinds of events trigger a state transition: (1) a segment arrives from the peer (e.g., the event on the arc from LISTEN to SYN RCVD), or (2) the local application process invokes an operation on TCP (e.g., the *active open* event on the arc from CLOSED to

SYN SENT). In other words, TCP's state-transition diagram effectively defines the *semantics* of both its peer-to-peer interface and its service interface, The *syntax* of these two interfaces is given by the segment format and by some application programming interface respectively.

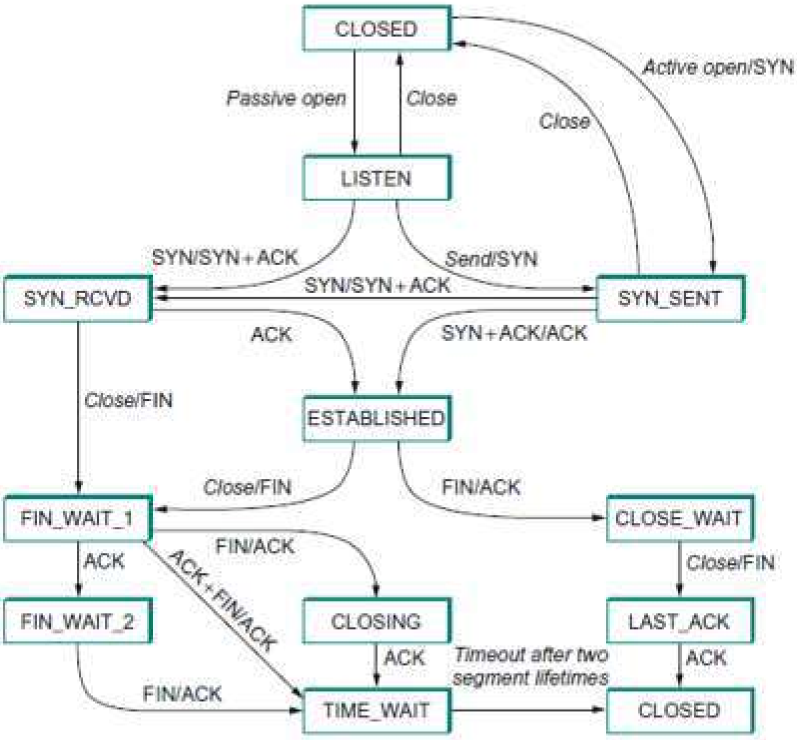


Figure 4.4TCP State-Transition diagram

Now let's trace the typical transitions taken through the diagram in Figure 4.4. Keep in mind that at each end of the connection, TCP makes different transitions from state to state.

1. When opening a connection, the server first invokes a passive open operation on TCP, which causes TCP to move to the LISTEN state. At some later time, the client does an active open, which causes its end of the connection to send a SYN segment to the server and to move to the SYN SENT state.

2. When the SYN segment arrives at the server, it moves to the SYN RCVD state and responds with a SYN+ACK segment. The arrival of this segment causes the client to move to the ESTABLISHED state and to send an ACK back to the server.

3. When this ACK arrives, the server finally moves to the ESTABLISHED state. In other words, we have just traced the three-way handshake. There are three things to notice about the connection establishment half of the state-transition diagram.

First, if the client's ACK to the server is lost, corresponding to the third leg of the three-way handshake, then the connection still functions correctly. This is because the client side is already in the ESTABLISHED state, so the local application process can start sending data to the other end. Each of these data segments will have the ACK flag set, and the correct value in the Acknowledgment field, so the server will move to the ESTABLISHED state when the first data segment arrives. This is actually an important point about TCP—every segment report what sequence number the sender is expecting to see next, even if this repeats the same sequence number contained in one or more previous segments.

The second thing to notice about the state-transition diagram is that there is a funny transition out of the LISTEN state whenever the local process invokes a *send* operation on TCP. That is, it is possible for a passive participant to identify both ends of the connection (i.e., itself and the remote participant that it is willing to have connect to it), and then for it to change its mind about waiting for the other side and instead actively establish the connection. To the best of our knowledge, this is a feature of TCP that no application process actually takes advantage of.

The final thing to notice about the diagram is the arcs that are not shown. Specifically, most of the states that involve sending a segment to the other side also schedule a timeout that eventually causes the segment to be present if the expected response does not happen. These retransmissions are not depicted in the state-transition diagram. If after several tries the expected response does not arrive, TCP gives up and returns to the CLOSED state. Turning our attention now to the process of terminating a connection, the important thing to keep in mind is that the application process on both sides of the connection must independently close its half of the connection. If only one side closes the connection, then this means it has no more data to send, but it is still available to receive data from the other side. This complicates the state-transition diagram because it must account for the possibility that the two sides invoke the *close* operator at the same time, as well as the possibility that first one side invokes close and then, at some later time, the other side invokes close.

Thus, on any one side there are three combinations of transitions that get a connection from the ESTABLISHED state to the CLOSED state:

- This side closes first: ESTABLISHED→FIN WAIT 1→FIN WAIT 2→TIME WAIT→CLOSED.
- The other side closes first: ESTABLISHED→CLOSE WAIT→LAST ACK→CLOSED.
- Both sides close at the same time: ESTABLISHED→FIN WAIT 1→CLOSING→TIME WAIT→CLOSED.

There is actually a fourth, although rare, sequence of transitions that leads to the CLOSED state; it follows the arc from FIN WAIT 1 to TIME WAIT. We leave it as an exercise for you to figure out what combination of circumstances leads to this fourth possibility. The main thing to recognize about connection teardown is that a connection in the TIME WAIT state cannot move to the CLOSED state until it has waited for two times the maximum amount of time an IP datagram might live in the Internet (i.e., 120 seconds). The reason for this is that, while the local side of the connection has sent an ACK in response to the other side's FIN segment, it does not know that the ACK was successfully delivered. As a consequence, the other side might retransmit its FIN segment, and this second FIN segment might be delayed in the network.

If the connection were allowed to move directly to the CLOSED state, then another pair of application processes might come along and open the same connection (i.e., use the same pair of port numbers), and the delayed FIN segment from the earlier incarnation of the connection would immediately initiate the termination of the later incarnation of that connection.

4.3.3 Flow Control and Buffering

Having examined connection establishment and release in some detail, let us now look at how connections are managed while they are in use. One of the key issues has come up before: flow control. In some ways the flow control problem in the transport layer is the same as in the data link layer, but in other ways it is different. The basic similarity is that in both layers a sliding window or other scheme is needed on each connection to keep a fast transmitter from overrunning a slow receiver. The main difference is that a router usually has relatively few lines, whereas a host may have numerous connections. This difference makes it impractical to implement the data link buffering strategy in the transport layer.

In the data link protocols, frames were buffered at both the sending router and at the receiving router. In protocol 6, for example, both sender and receiver are required to dedicate *MAX_SEQ* + 1 buffers to each line, half for input and half for output. For a host with a maximum of, say, 64 connections, and a 4-bit sequence number, this protocol would require 1024 buffers.

In the data link layer, the sending side must buffer outgoing frames because they might have to be retransmitted. If the subnet provides datagram service, the sending transport entity must also buffer, and for the same reason. If the receiver knows that the sender buffers all TPDUs until they are acknowledged, the receiver may or may not dedicate specific buffers to specific connections, as it sees fit. The receiver may, for example, maintain a single buffer pool shared by all connections. When a TPDU comes in, an attempt is made to dynamically acquire a new buffer. If one is available, the TPDU is accepted; otherwise, it is discarded. Since the sender is prepared to retransmit TPDUs lost by the subnet, no harm is done by having the receiver drop TPDUs, although some resources are wasted. The sender just keeps trying until it gets an acknowledgement.

In summary, if the network service is unreliable, the sender must buffer all TPDUs sent, just as in the data link layer. However, with reliable network service, other trade-offs become possible. In particular, if the sender knows that the receiver always has buffer space, it need not retain copies of the TPDUs it sends. However, if the receiver cannot guarantee that every incoming TPDU will be accepted, the sender will have to buffer anyway. In the latter case, the sender cannot trust the network layer's acknowledgement, because the acknowledgement means only that the TPDU arrived, not that it was accepted. We will come back to this important point later.

Even if the receiver has agreed to do the buffering, there still remains the question of the buffer size. If most TPDUs are nearly the same size, it is natural to organize the buffers as a pool of identically-sized buffers, with one TPDU per buffer, as in Figure 4.5(a). However, if there is wide variation in TPDU size, from a few characters typed at a terminal to thousands of characters from file transfers, a pool of fixed-sized buffers presents problems. If the buffer size is chosen equal to the largest possible TPDU, space will be wasted whenever a short TPDU arrives. If the buffer size is chosen less than the maximum TPDU size, multiple buffers will be needed for long TPDUs, with the attendant complexity.

Another approach to the buffer size problem is to use variable-sized buffers, as in Figure 4.5(b). The advantage here is better memory utilization, at the price of more complicated buffer management. A third possibility is to dedicate a single large circular buffer per connection, as in Figure 4.5(c). This system also makes good use of memory, provided that all connections are heavily loaded, but is poor if some connections are lightly loaded.

The optimum trade-off between source buffering and destination buffering depends on the type of traffic carried by the connection. For low-bandwidth bursty traffic, such as that produced by an interactive terminal, it is better not to dedicate any buffers, but rather to acquire them dynamically at both ends. Since the sender cannot be sure the receiver will be able to acquire a buffer, the sender must retain a copy of the TPDU until it is acknowledged. On the other hand, for file transfer and other high-bandwidth traffic, it is better if the receiver does dedicate a full window of buffers, to allow the data to flow at maximum speed. Thus, for low-bandwidth bursty traffic, it is better to buffer at the sender, and for high bandwidth smooth traffic, it is better to buffer at the receiver.

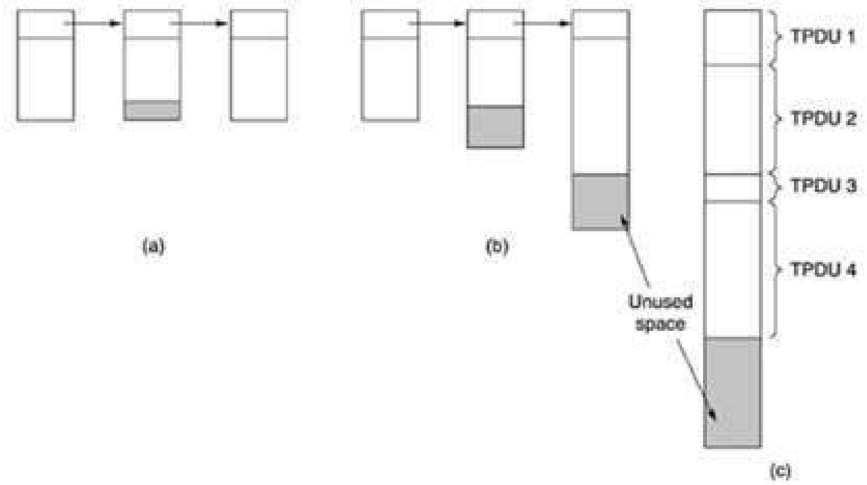
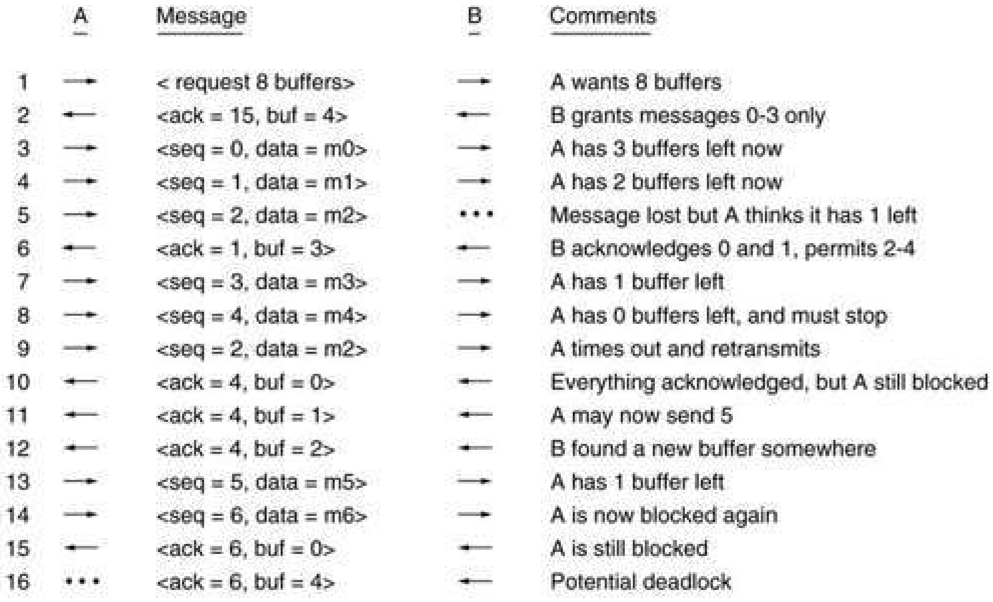


Figure 4.5 (a) Chained fixed-size buffers. (b) Chained variable-sized buffers. (c) One large circular buffer per connection.

As connections are opened and closed and as the traffic pattern changes, the sender and receiver need to dynamically adjust their buffer allocations. Consequently, the transport protocol should allow a sending host to request buffer space at the other end. Buffers could be allocated per connection, or collectively, for all the connections running between the two hosts. Alternatively, the receiver, knowing its buffer situation (but not knowing the offered traffic) could tell the sender "I have reserved *X* buffers for you." If the number of open connections should increase, it may be necessary for an allocation to be reduced, so the protocol should provide for this possibility.

A reasonably general way to manage dynamic buffer allocation is to decouple the buffering from the acknowledgements, in contrast to the sliding window protocols of Data Link Layer. Dynamic buffer management means, in effect, a variable-sized window. Initially, the sender requests a certain number of buffers, based on its perceived needs. The receiver then grants as many of these as it can afford. Every time the sender transmits a TPDU, it must decrement its allocation, stopping altogether when the allocation reaches zero. The receiver then separately piggybacks both acknowledgements and buffer allocations onto the reverse traffic.

Figure 4.6 shows an example of how dynamic window management might work in a datagram subnet with 4-bit sequence numbers. Assume that buffer allocation information travels in separate TPDUs, as shown, and is not piggybacked onto reverse traffic. Initially, *A* wants eight buffers, but is granted only four of these. It then sends three TPDUs, of which the third is lost. TPDU 6 acknowledges receipt of all TPDUs up to and including sequence number 1, thus allowing *A* to release those buffers, and furthermore informs *A* that it has permission to send three more TPDUs starting beyond 1 (i.e., TPDUs 2, 3, and 4). *A* knows that it has already sent number 2, so it thinks that it may send TPDUs 3 and 4, which it proceeds to do. At this point it is blocked and must wait for more buffer allocation. Timeout-induced retransmissions (line 9), however, may occur while blocked, since they use buffers that have already been allocated. In line 10, *B* acknowledges receipt of all TPDUs up to and including 4 but refuses to let *A* continue. Such a situation is impossible with the fixed window protocols of Data Link Layer. The next TPDU from *B* to *A* allocates another buffer and allows *A* to continue.



	A	Message	B	Comments
1	→	< request 8 buffers>	→	A wants 8 buffers
2	←	<ack = 15, buf = 4>	←	B grants messages 0-3 only
3	→	<seq = 0, data = m0>	→	A has 3 buffers left now
4	→	<seq = 1, data = m1>	→	A has 2 buffers left now
5	→	<seq = 2, data = m2>	• • •	Message lost but A thinks it has 1 left
6	←	<ack = 1, buf = 3>	←	B acknowledges 0 and 1, permits 2-4
7	→	<seq = 3, data = m3>	→	A has 1 buffer left
8	→	<seq = 4, data = m4>	→	A has 0 buffers left, and must stop
9	→	<seq = 2, data = m2>	→	A times out and retransmits
10	←	<ack = 4, buf = 0>	←	Everything acknowledged, but A still blocked
11	←	<ack = 4, buf = 1>	←	A may now send 5
12	←	<ack = 4, buf = 2>	←	B found a new buffer somewhere
13	→	<seq = 5, data = m5>	→	A has 1 buffer left
14	→	<seq = 6, data = m6>	→	A is now blocked again
15	←	<ack = 6, buf = 0>	←	A is still blocked
16	• • •	<ack = 6, buf = 4>	←	Potential deadlock

Figure 4.6 . Dynamic buffer allocation. The arrows show the direction of transmission. An ellipsis (...) indicates a lost TPDU.

Potential problems with buffer allocation schemes of this kind can arise in datagram networks if control TPDUs can get lost. Look at line 16. *B* has now allocated more buffers to *A*, but the allocation TPDU was lost. Since control TPDUs are not sequenced or timed out, *A* is now deadlocked. To prevent this situation, each host should periodically send control TPDUs giving the acknowledgement and buffer status on each connection. That way, the deadlock will be broken, sooner or later.

Until now we have tacitly assumed that the only limit imposed on the sender's data rate is the amount of buffer space available in the receiver. As memory prices continue to fall dramatically, it may become feasible to equip hosts with so much memory that lack of buffers is rarely, if ever, a problem.

When buffer space no longer limits the maximum flow, another bottleneck will appear: the carrying capacity of the subnet. If adjacent routers can exchange at most *x* packets/sec and there are *k* disjoint paths between a pair of hosts, there is no way that those hosts can exchange more than *kx* TPDUs/sec, no matter how much buffer space is available at each end. If the sender pushes too hard (i.e., sends more than *kx* TPDUs/sec), the subnet will become congested because it will be unable to deliver TPDUs as fast as they are coming in.

What is needed is a mechanism based on the subnet's carrying capacity rather than on the receiver's buffering capacity. Clearly, the flow control mechanism must be applied at the sender to prevent it from having too many unacknowledged TPDUs outstanding at once. Belsnes (1975) proposed using a sliding window flow control scheme in which the sender dynamically adjusts the window size to match the network's carrying capacity. If the network can handle *c* TPDUs/sec and the cycle time (including transmission, propagation, queueing, processing at the receiver, and return of the acknowledgement) is *r*, then the sender's window should be *cr*. With a window of this size the sender normally operates with the pipeline full. Any small decrease in network performance will cause it to block.

In order to adjust the window size periodically, the sender could monitor both parameters and then compute the desired window size. The carrying capacity can be determined by simply counting the number of TPDUs acknowledged during some time period and then dividing by the time period. During the measurement, the sender should send as fast as it can, to make sure that the network's carrying capacity, and not the low input rate, is the factor limiting the acknowledgement rate. The time required for a transmitted TPDU to be acknowledged can be measured exactly and a running mean maintained. Since the network capacity available to any given flow varies in time, the window size should be adjusted frequently, to track changes in the carrying capacity. As we will see later, the Internet uses a similar scheme.

4.3.4 Multiplexing

The addressing mechanism allows multiplexing and demultiplexing by the transport layer, as shown in Figure 4.7.

- ***Multiplexing***

At the sender site, there may be several processes that need to send packets. However, there is only one transport layer protocol at any time. This is a many-to-one relationship and requires multiplexing. The protocol accepts messages from different processes, differentiated by their assigned port numbers. After adding the header, the transport layer passes the packet to the network layer.

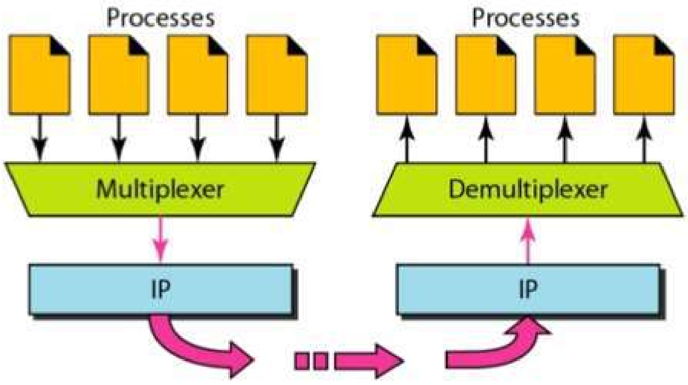


Figure 4.7Multiplexing and demultiplexing

- ***Demultiplexing***

At the receiver site, the relationship is one-to-many and requires demultiplexing. The transport layer receives datagrams from the network layer. After error checking and dropping of the header, the transport layer delivers each message to the appropriate process based on the port number.

4.3.5 Crash Recovery

If hosts and routers are subject to crashes, recovery from these crashes becomes an issue. If the transport entity is entirely within the hosts, recovery from network and router crashes is straightforward. If the network layer provides datagram service, the transport entities expect lost TPDUs all the time and know how to cope with them. If the network layer provides connection-oriented service, then loss of a virtual circuit is handled by establishing a new one and then probing the remote transport entity to ask it which TPDUs it has received and which ones it has not received. The latter ones can be retransmitted.

A more troublesome problem is how to recover from host crashes. In particular, it may be desirable for clients to be able to continue working when servers crash and then quickly reboot. To illustrate the difficulty, let us assume that one host, the client, is sending a long file to another host, the file server, using a simple stop-and-wait protocol. The transport layer on the server simply passes the incoming TPDUs to the transport user, one by one. Partway through the transmission, the server crashes. When it comes back up, its tables are reinitialized, so it no longer knows precisely where it was.

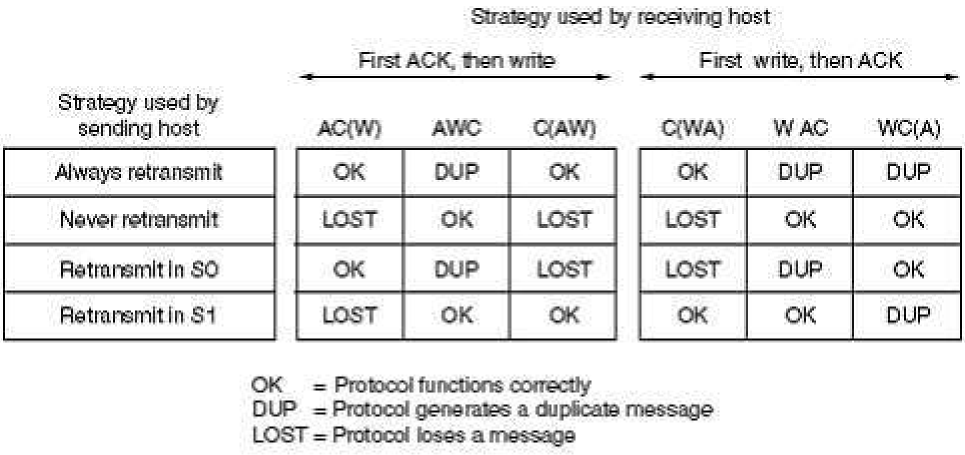
In an attempt to recover its previous status, the server might send a broadcast TPDU to all other hosts, announcing that it had just crashed and requesting that its clients inform it of the status of all open connections. Each client can be in one of two states: one TPDU outstanding, *S1*, or no TPDUs outstanding, *S0*. Based on only this state information, the client must decide whether to retransmit the most recent TPDU.

At first glance it would seem obvious: the client should retransmit only if and only if it has an unacknowledged TPDU outstanding (i.e., is in state *S1*) when it learns of the crash. However, a closer inspection reveals difficulties with this naive approach. Consider, for example, the situation in which the server's transport entity first sends an acknowledgement, and then, when the acknowledgement has been sent, writes to the application process. Writing a TPDU onto the output stream and sending an acknowledgement are two distinct events that cannot be done simultaneously. If a crash occurs after the acknowledgement has been sent but before the write has been done, the client will receive the acknowledgement and thus be in state *S0* when the crash recovery announcement arrives. The client will therefore not retransmit, (incorrectly) thinking that the TPDU has arrived. This decision by the client leads to a missing TPDU.

At this point it may be that: "That problem can be solved easily. i.e reprogram the transport entity to first do the write and then send the acknowledgement." Try again. Imagine that the write has been done but the crash occurs before the acknowledgement can be sent. The client will be in state *S1* and thus retransmit, leading to an undetected duplicate TPDU in the output stream to the server application process.

No matter how the client and server are programmed, there are always situations where the protocol fails to recover properly. The server can be programmed in one of two ways: acknowledge first or write first. The client can be programmed in one of four ways: always retransmit the last TPDU, never retransmit the last TPDU, retransmit only in state *S0*, or retransmit only in state *S1*. This gives eight combinations, for each combination there is some set of events that makes the protocol fail.

Three events are possible at the server: sending an acknowledgement (*A*), writing to the output process (*W*), and crashing (*C*). The three events can occur in six different orderings: *AC*(*W*), *AWC*, *C*(*AW*), *C*(*WA*), *WAC*, and *WC*(*A*), where the parentheses are used to indicate that neither *A* nor *W* can follow *C* (i.e., once it has crashed, it has crashed). Figure 4.8 shows all eight combinations of client and server strategy and the valid event sequences for each one. Notice that for each strategy there is some sequence of events that causes the protocol to fail. For example, if the client always retransmits, the *AWC* event will generate an undetected duplicate, even though the other two events work properly.



	Strategy used by receiving host					
	First ACK, then write			First write, then ACK		
Strategy used by sending host	AC(W)	AWC	C(AW)	C(WA)	W AC	WC(A)
Always retransmit	OK	DUP	OK	OK	DUP	DUP
Never retransmit	LOST	OK	LOST	LOST	OK	OK
Retransmit in S0	OK	DUP	LOST	LOST	DUP	OK
Retransmit in S1	LOST	OK	OK	OK	OK	DUP

OK = Protocol functions correctly
DUP = Protocol generates a duplicate message
LOST = Protocol loses a message

Figure 4.8 Different combinations of client and server strategy.

Making the protocol more elaborate does not help. Even if the client and server exchange several TPDUs before the server attempts to write, so that the client knows exactly what is about to happen, the client has no way of knowing whether a crash occurred just before or just after the write. The conclusion is inescapable: under our ground rules of no simultaneous events, host crash and recovery cannot be made transparent to higher layers.

Put in more general terms, this result can be restated as recovery from a layer *N* crash can only be done by layer *N* + 1, and then only if the higher layer retains enough status information. As mentioned above, the transport layer can recover from failures in the network layer, provided that each end of a connection keeps track of where it is.

4.4 Transport-Level Protocols

The TCP/IP protocol suite includes two transport-level protocols: the Transmission Control Protocol (TCP), which is connection-oriented, and the User Datagram Protocol (UDP), which is connectionless.

4.4.1 User Datagram Protocol (UDP)

The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to-process communication instead of host-to-host communication. Also, it performs very limited error checking. UDP is a very simple protocol using a minimum of overhead. If a process wants to send a small message and does not care much about reliability, it can use UDP. Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP or Stream Control Transmission Protocol (SCTP).

Well-Known Ports for UDP

Table 4-1 shows some well-known port numbers used by UDP. Some port numbers can be used by both UDP and TCP.

Table 4-1 Well-known ports used with UDP

Port	Protocol	Description
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	BOOTPs	Server port to download bootstrap information

68	BOOTPc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol(trap)

- **User Datagram**

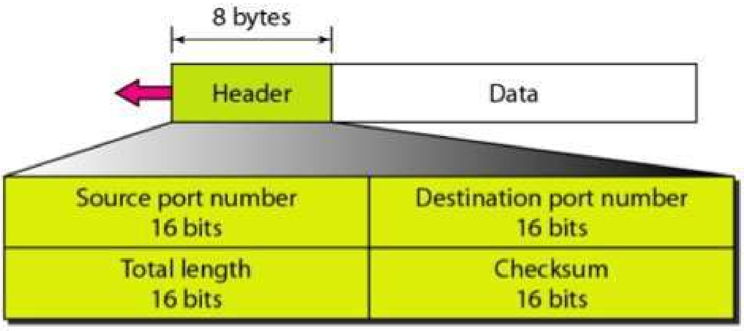
UDP packets, called user datagrams, have a fixed-size header of 8 bytes. Figure 4.9 shows the format of a user datagram. The fields are as follows:

1. Source port number

This is the port number used by the process running on the source host. It is 16 bits long, which means that the port number can range from 0 to 65,535. If the source host is the client (a client sending a request), the port number, in most cases, is an ephemeral port number requested by the process and chosen by the UDP software running on the source host. If the source host is the server (a server sending a response), the port number, in most cases, is a well-known port number.

2. Destination port number

This is the port number used by the process running on the destination host. It is also 16 bits long. If the destination host is the server (a client sending a request), the port number, in most cases, is a well-known port number. If the destination host is the client (a server sending a response), the port number, in most cases, is an ephemeral port number. In this case, the server copies the ephemeral port number it has received in the request packet.



Note

UDP length
= IP length – IP header's length

Figure 4.9 User datagram format

3. Length

This is a 16-bit field that defines the total length of the user datagram, header plus data. The 16 bits can define a total length of 0 to 65,535 bytes. However, the total length needs to be much less because a UDP user datagram is stored in an IP datagram with a total length of 65,535 bytes.

The length field in a UDP user datagram is actually not necessary. A user datagram is encapsulated in an IP datagram. There is a field in the IP datagram that defines the total length. There is another field in the IP datagram that defines the length of the header. So if we subtract the value of the second field from the first, we can deduce the length of a UDP datagram that is encapsulated in an IP datagram.

UDP length = IP length - IP header's length

However, the designers of the UDP protocol felt that it was more efficient for the destination UDP to calculate the length of the data from the information provided in the UDP user datagram rather than ask the IP software to supply this information. We should remember that when the IP software delivers the UDP user datagram to the UDP layer, it has already dropped the IP header.

Checksum

This field is used to detect errors over the entire user datagram (header plus data). The UDP checksum calculation is different from the one for IP and ICMP. Here the checksum includes three sections: a pseudoheader, the UDP header, and the data coming from the application layer.

The pseudoheader is the part of the header of the IP packet in which the user datagram is to be encapsulated with some fields filled with 0s (see Figure 4.10).

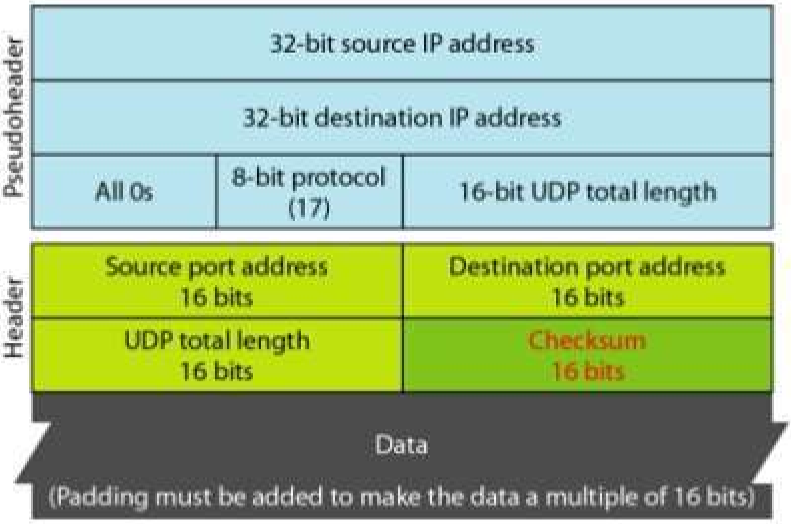

Pseudoheader
32-bit source IP address
32-bit destination IP address
All 0s
8-bit protocol (17)
16-bit UDP total length
Header
Source port address 16 bits
Destination port address 16 bits
UDP total length 16 bits
Checksum 16 bits
Data
(Padding must be added to make the data a multiple of 16 bits)

Figure 4.10 Pseudoheader for checksum calculation

If the checksum does not include the pseudoheader, a user datagram may arrive safe and sound. However, if the IP header is corrupted, it may be delivered to the wrong host. The protocol field is added to ensure that the packet belongs to UDP, and not to other transport-layer protocols. If a process can use either UDP or TCP, the destination port number can be the same. The value of the protocol field for UDP is 17. If this value is changed during transmission, the checksum calculation at the receiver will detect it and UDP drops the packet. It is not delivered to the wrong protocol.

Example 4.1

Figure 4.11 shows the checksum calculation for a very small user datagram with only 7 bytes of data. Because the number of bytes of data is odd, padding is added for checksum calculation.

The pseudoheader as well as the padding will be dropped when the user datagram is delivered to IP.

- **Optional Use of the Checksum**

The calculation of the checksum and its inclusion in a user datagram are optional. If the checksum is not calculated, the field is filled with 1s. Note that a calculated checksum can never be all 1s because this implies that the sum is all 0s, which is impossible because it requires that the value of fields to be 0s.

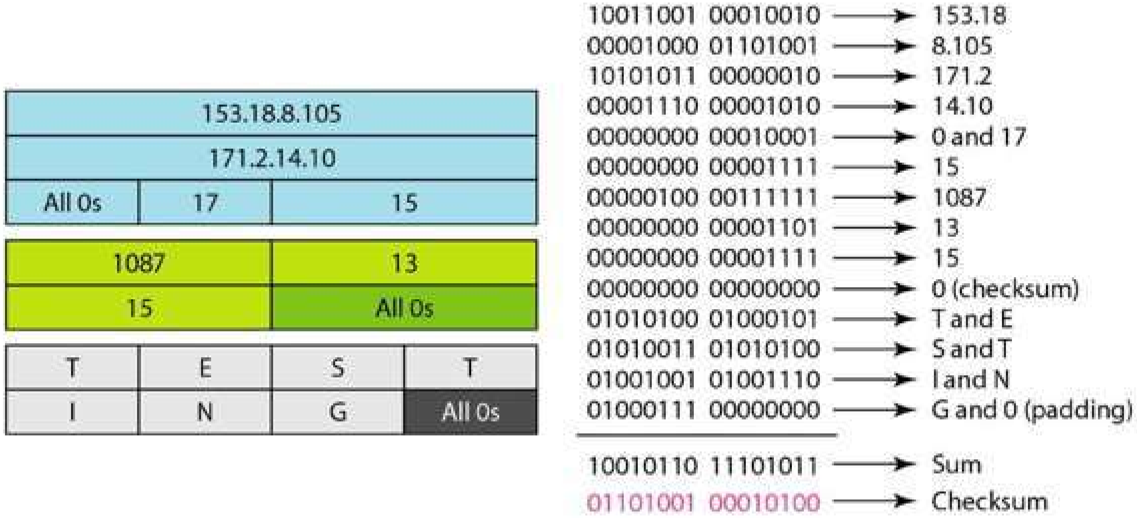


Figure 4.11 Checksum calculation of a simple UDP user datagram

- **UDP Operation**

UDP uses concepts common to the transport layer.

Connectionless Services

UDP provides a connectionless service. This means that each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagrams even if they are coming from the same source process and going to the same destination program. The user datagrams are not numbered.

Also, there is no connection establishment and no connection termination, as is the case for TCP. This means that each user datagram can travel on a different path. One of the ramifications of being connectionless is that the process that uses UDP cannot send a stream of data to UDP and expect UDP to chop them into different related user datagrams. Instead each request must be small enough to fit into one user datagram. Only those processes sending short messages should use UDP.

Flow and Error Control

UDP is a very simple, unreliable transport protocol. There is no flow control and hence no window mechanism. The receiver may overflow with incoming messages. There is no error control mechanism in UDP except for the checksum. This means that the sender does not know if a message has been lost or duplicated. When the receiver detects an error through the checksum, the user datagram is silently discarded. The lack of flow control and error control means that the process using UDP should provide these mechanisms.

Encapsulation and Decapsulation

To send a message from one process to another, the UDP protocol encapsulates and decapsulates messages in an IP datagram.

Queuing

In UDP, queues are associated with ports (see Figure 4.12).

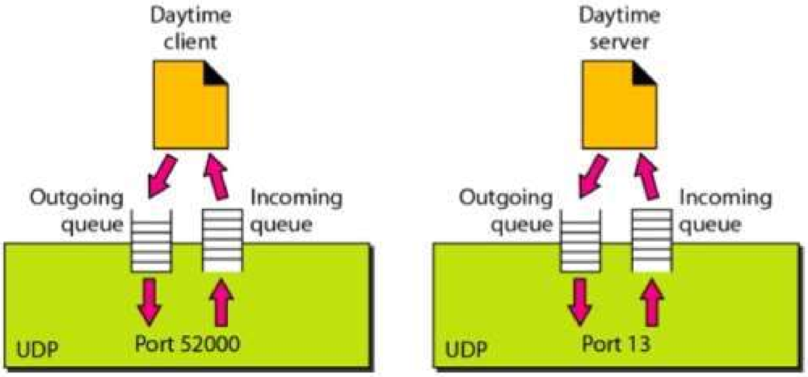


Figure 4.12 Queues in UDP

At the client site, when a process starts, it requests a port number from the operating system. Some implementations create both an incoming and an outgoing queue associated with each process. Other implementations create only an incoming queue associated with each process.

Note that even if a process wants to communicate with multiple processes, it obtains only one port number and eventually one outgoing and one incoming queue. The queues opened by the client are, in most cases, identified by ephemeral port numbers. The queues function as long as the process is running. When the process terminates, the queues are destroyed.

The client process can send messages to the outgoing queue by using the source port number specified in the request. UDP removes the messages one by one and, after adding the UDP header, delivers them to IP. An outgoing queue can overflow. If this happens, the operating system can ask the client process to wait before sending any more messages.

When a message arrives for a client, UDP checks to see if an incoming queue has been created for the port number specified in the destination port number field of the user datagram. If there is such a queue, UDP sends the received user datagram to the end of the queue. If there is no such queue, UDP discards the user datagram and asks the ICMP protocol to send a *port unreachable* message to the server. All the incoming messages for one particular client program, whether coming from the same or a different server, are sent to the same queue. An incoming queue can overflow. If this happens, UDP drops the user datagram and asks for a port unreachable message to be sent to the server.

At the server site, the mechanism of creating queues is different. In its simplest form, a server asks for incoming and outgoing queues, using its well-known port, when it starts running. The queues remain open as long as the server is running.

When a message arrives for a server, UDP checks to see if an incoming queue has been created for the port number specified in the destination port number field of the user datagram. If there is such a queue, UDP sends the received user datagram to the end of the queue. If there is no such queue, UDP discards the user datagram and asks the ICMP protocol to send a port unreachable message to the client. All the incoming messages for one particular server, whether coming from the same or a different client, are sent to the same queue. An incoming queue can overflow. If this happens, UDP drops the user datagram and asks for a port unreachable message to be sent to the client.

When a server wants to respond to a client, it sends messages to the outgoing queue, using the source port number specified in the request. UDP removes the messages one by one and, after adding the UDP header, delivers them to IP. An outgoing queue can overflow. If this happens, the operating system asks the server to wait before sending any more messages.

- Use of UDP

The following lists some uses of the UDP protocol:

- ✓ UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control. It is not usually used for a process such as FTP that needs to send bulk data
- ✓ UDP is suitable for a process with internal flow and error control mechanisms. For example, the Trivial File Transfer Protocol (TFTP) process includes flow and error control. It can easily use UDP.
- ✓ UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.

- ✓ UDP is used for management processes such as SNMP
- ✓ UDP is used for some route updating protocols such as Routing Information Protocol (RIP)

4.4.2 Transmission Control Protocol (TCP)

TCP, like UDP, is a process-to-process (program-to-program) protocol. TCP, therefore, like UDP, uses port numbers. Unlike UDP, TCP is a connection oriented protocol; it creates a virtual connection between two TCPs to send data. In addition, TCP uses flow and error control mechanisms at the transport level. In brief, TCP is called a *connection-oriented, reliable* transport protocol. It adds connection-oriented and reliability features to the services of IP.

- **TCP Services**

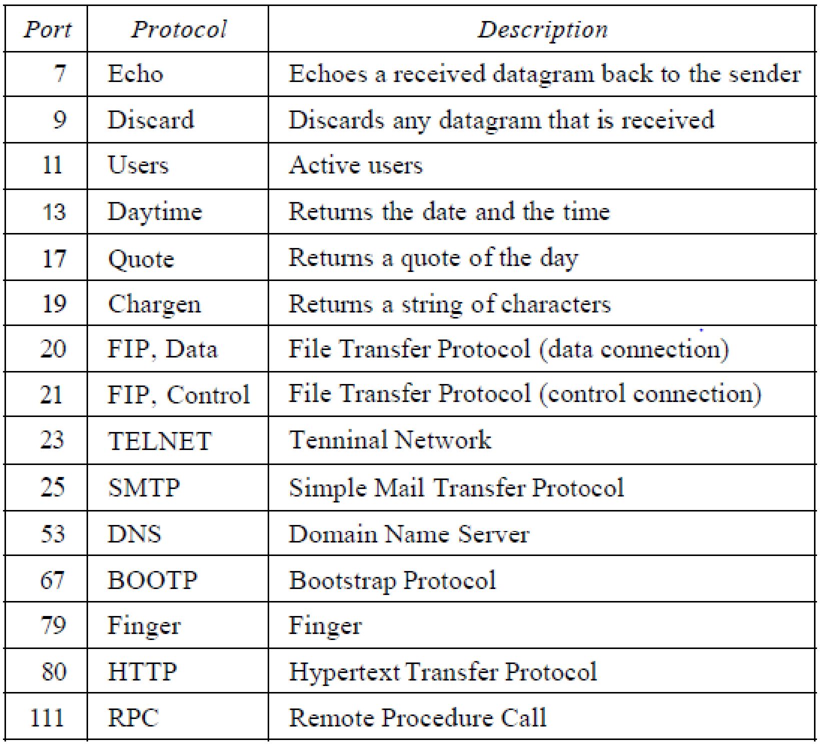
The services offered by TCP to the processes at the application layer:

Process-to-Process Communication

Like UDP, TCP provides process-to-process communication using port numbers.

Table *4-2* lists some well-known port numbers used by TCP.

Table 4-2 Well-known ports used by TCP



Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FIP, Data	File Transfer Protocol (data connection)
21	FIP, Control	File Transfer Protocol (control connection)
23	TELNET	Tenninal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

Stream Delivery Service

TCP, unlike UDP, is a stream-oriented protocol. In UDP, a process (an application program) sends messages, with predefined boundaries, to UDP for delivery. UDP adds its own header to each of these messages and delivers them to IP for transmission. Each message from the process is called a user datagram and becomes, eventually, one IP datagram. Neither IP nor UDP recognizes any relationship between the datagrams.

TCP, on the other hand, allows the sending process to deliver data as a stream of bytes and allows the receiving process to obtain data as a stream of bytes. TCP creates an environment in which the two processes seem to be connected by an imaginary "tube" that carries their data across the Internet. This imaginary environment is depicted in Figure 4.13 *Stream delivery*. The sending process produces (writes to) the stream of bytes, and the receiving process consumes (reads from) them.

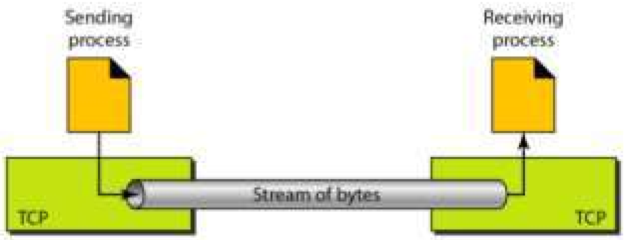


Figure 4.13 Stream delivery

Sending and Receiving Buffers : Because the sending and the receiving processes may not write or read data at the same speed, TCP needs buffers for storage. There are two buffers, the sending buffer and the receiving buffer, one for each direction. One way to implement a buffer is to use a circular array of I-byte locations as shown in Figure 4.14. For simplicity, we have shown two buffers of 20 bytes each; normally the buffers are hundreds or thousands of bytes, depending on the implementation. We also show the buffers as the same size, which is not always the case.

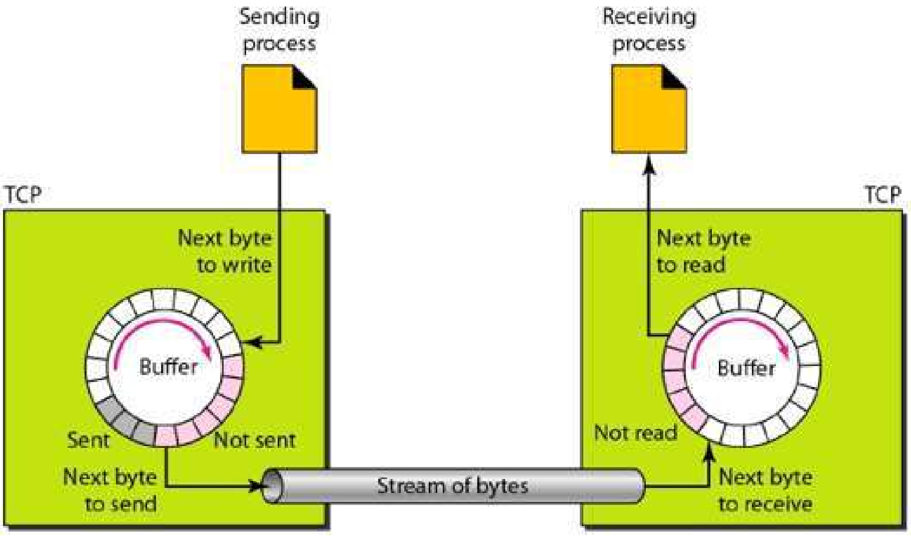


Figure 4.14 Sending and receiving buffers

Figure 4.14 shows the movement of the data in one direction. At the sending site, the buffer has three types of chambers. The white section contains empty chambers that can be filled by the sending process (producer). The gray area holds bytes that have been sent but not yet acknowledged. TCP keeps these bytes in the buffer until it receives an acknowledgment. The colored area contains bytes to be sent by the sending TCP. TCP may be able to send only part of this colored section. This could be due to the slowness of the receiving process or perhaps to congestion in the network. Also note that after the bytes in the gray chambers are acknowledged, the chambers are recycled and available for use by the sending process. This is why we show a circular buffer.

The operation of the buffer at the receiver site is simpler. The circular buffer is divided into two areas (shown as white and colored). The white area contains empty chambers to be filled by bytes received from the network. The colored sections contain received bytes that can be read by the receiving process. When a byte is read by the receiving process, the chamber is recycled and added to the pool of empty chambers.

- **Segments**:

Although buffering handles the disparity between the speed of the producing and consuming processes, we need one more step before we can send data. The IP layer, as a service provider for TCP, needs to send data in packets, not as a stream of bytes. At the transport layer, TCP groups a number of bytes together into a packet called a segment.

TCP adds a header to each segment (for control purposes) and delivers the segment to the IP layer for transmission. The segments are encapsulated in IP datagrams and transmitted. This entire operation is transparent to the receiving process. Later we will see that segments may be received out of order, lost, or corrupted and resent. All these are handled by TCP with the receiving process unaware of any activities. *Figure 4.15* shows how segments are created from the bytes in the buffers.

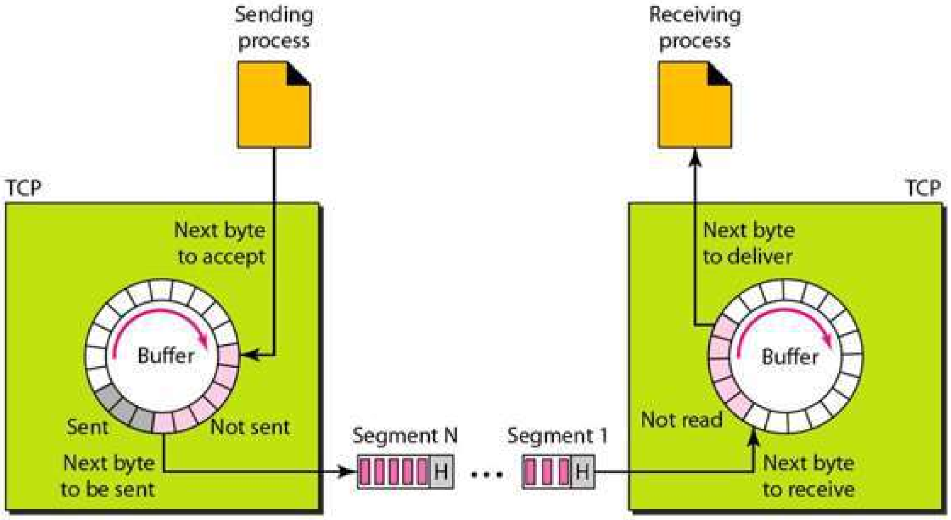


Figure 4.15 TCP segments

Note that the segments are not necessarily the same size. In Figure 4.15, for simplicity, we show one segment carrying 3 bytes and the other carrying 5 bytes. In reality, segments carry hundreds, if not thousands, of bytes.

Full-Duplex Communication

TCP offers full-duplex service, in which data can flow in both directions at the same time. Each TCP then has a sending and receiving buffer, and segments move in both directions.

Connection-Oriented Service

TCP, unlike UDP, is a connection-oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:

1. The two TCPs establish a connection between them.

2. Data are exchanged in both directions.

3. The connection is terminated.

Note that this is a virtual connection, not a physical connection. The TCP segment is encapsulated in an IP datagram and can be sent out of order, or lost, or corrupted, and then resent. Each may use a different path to reach the destination. There is no physical connection.

TCP creates a stream-oriented environment in which it accepts the responsibility of delivering the bytes in order to the other site. The situation is similar to creating a bridge that spans multiple islands and passing all the bytes from one island to another in one single connection.

Reliable Service

TCP is a reliable transport protocol. It uses an acknowledgment mechanism to check the safe and sound arrival of data. We will discuss this feature further in the section on error control.

- **TCP Features**

TCP has several features that are briefly summarized in this section

Numbering System

Although the TCP software keeps track of the segments being transmitted or received, there is no field for a segment number value in the segment header. Instead, there are two fields called the sequence number and the acknowledgment number. These two fields refer to the byte number and not the segment number.

a. Byte Number

TCP numbers all data bytes that are transmitted in a connection. Numbering is independent in each direction. When TCP receives bytes of data from a process, it stores them in the sending buffer and numbers them. The numbering does not necessarily start from O. Instead, TCP generates a random number between 0 and 232 - 1 for the number of the first byte. For example, if the random number happens to be 1057 and the total data to be sent are 6000 bytes, the bytes are numbered from 1057 to 7056. This byte numbering is used for flow and error control.

> The bytes of data being transferred in each connection are numbered by TCP. The numbering starts with a randomly generated number.

b. Sequence Number

After the bytes have been numbered, TCP assigns a sequence number to each segment that is being sent. The sequence number for each segment is the number of the first byte carried in that segment.

Example 4.2

Suppose a TCP connection is transferring a file of 5000 bytes. The first byte is numbered 10,00l. What are the sequence numbers for each segment if data are sent in five segments, each carrying 1000 bytes?

Solution

The following shows the sequence number for each segment:

Segment 1 Sequence Number: 10,001 (range: 10,001 to 11,(00)

Segment 2 Sequence Number: 11,001 (range: 11,001 to 12,000)

Segment 3 Sequence Number: 12,001 (range: 12,001 to 13,000)

Segment 4 Sequence Number: 13,001 (range: 13,001 to 14,000)

Segment 5 Sequence Number: 14,001 (range: 14,001 to 15,000)

> The value in the sequence number field of a segment defines the number of the first data byte contained in that segment.

When a segment carries a combination of data and control information (piggybacking), it uses a sequence number. If a segment does not carry user data, it does not logically define a sequence number. The field is there, but the value is not valid. However, some segments, when carrying only control information, need a sequence number to allow an acknowledgment from the receiver. These segments are used for connection establishment, termination, or abortion. Each of these segments consumes one sequence number as though it carried 1 byte, but there are no actual data. If the randomly generated sequence number is *x,* the first data byte is numbered *x* + 1. The byte *x* is considered a phony byte that is used for a control segment to open a connection.

c. Acknowledgment Number

Communication in TCP is full duplex; when a connection is established, both parties can send and receive data at the same time. Each party numbers the bytes, usually with a different starting byte number.

The sequence number in each direction shows the number of the first byte carried by the segment. Each party also uses an acknowledgment number to confirm the bytes it has received. However, the acknowledgment number defines the number of the next byte that the party expects to receive. In addition, the acknowledgment number is cumulative, which means that the party takes the number of the last byte that it has received, safe and sound, adds I to it, and announces this sum as the acknowledgment number.

The term *cumulative* here means that if a party uses 5643 as an acknowledgment number, it has received all bytes from the beginning up to 5642. Note that this does not mean that the party has received 5642 bytes because the first byte number does not have to start from 0.

- ✓ The value of the acknowledgment field in a segment defines the number of the next byte a party expects to receive.
- ✓ The acknowledgment number is cumulative.

Flow Control

TCP, unlike UDP, provides *flow control.* The receiver of the data controls the amount of data that are to be sent by the sender. This is done to prevent the receiver from being overwhelmed with data. The numbering system allows TCP to use a byte-oriented flow control.

Error Control

To provide reliable service, TCP implements an error control mechanism. Although error control considers a segment as the unit of data for error detection (loss or corrupted segments), error control is byte-oriented.

Congestion Control

TCP, unlike UDP, takes into account congestion in the network. The amount of data sent by a sender is not only controlled by the receiver (flow control), but is also determined by the level of congestion in the network.

- **Segment**

A packet in TCP is called a segment.

Format

The format of a segment is shown in Figure 4.16. The segment consists of a 20- to 60-byte header, followed by data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options.

1. *Source port address*. This is a 16-bit field that defines the port number of the application program in the host that is sending the segment. This serves the same purpose as the source port address in the UDP header.
2. *Destination port address*. This is a 16-bit field that defines the port number of the application program in the host that is receiving the segment. This serves the same purpose as the destination port address in the UDP header.

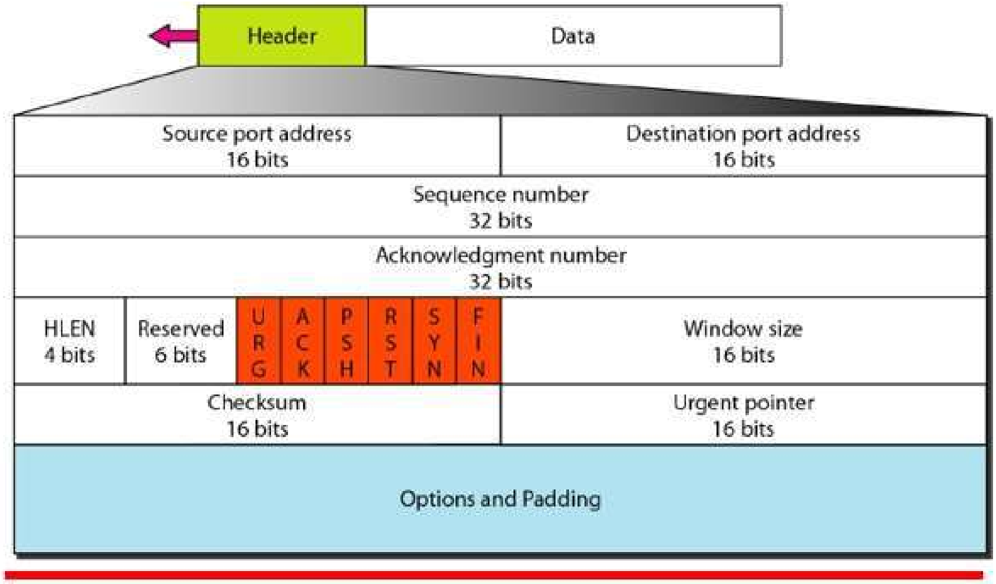


Figure 4.16 TCP segment format

3. *Sequence number*. This 32-bit field defines the number assigned to the first byte of data contained in this segment. As we said before, TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. The sequence number tells the destination which byte in this sequence comprises the first byte in the segment. During connection establishment, each party uses a random number generator to create an initial sequence number (ISN), which is usually different in each direction.

4. *Acknowledgment number*. This 32-bit field defines the byte number that the receiver of the segment is expecting to receive from the other party. If the receiver of the segment has successfully received byte number *x* from the other party, it defines *x* + I as the acknowledgment number. Acknowledgment and data can be piggybacked together.

5. *Header length*. This 4-bit field indicates the number of 4-byte words in the TCP header. The length of the header can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 (5 x 4 =20) and 15 (15 x 4 =60).

6. *Reserved*. This is a 6-bit field reserved for future use.

7. *Control*. This field defines 6 different control bits or flags as shown in Figure 4.17.One or more of these bits can be set at a time.

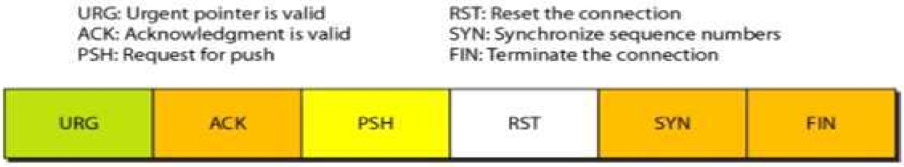
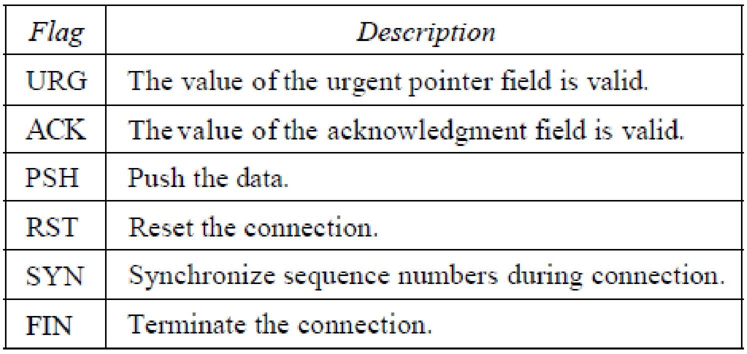

URG: Urgent pointer is valid
ACK: Acknowledgment is valid
PSH: Request for push
RST: Reset the connection
SYN: Synchronize sequence numbers
FIN: Terminate the connection
URG
ACK
PSH
RST
SYN
FIN

Figure 4.17 Control field

These bits enable flow control, connection establishment and termination, connection abortion, and the mode of data transfer in TCP. A brief description of each bit is shown in Table 4-3.

Table 4-3 Description of flags in the control field



Flag	*Description*
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	Reset the connection.
SYN	Synchronize sequence numbers during connection.
FIN	Terminate the connection.

8. *Window size*. This field defines the size of the window, in bytes, that the other party must maintain. Note that the length of this field is 16 bits, which means that the maximum size of the window is 65,535 bytes. This value is normally referred to as the receiving window (rwnd) and is determined by the receiver. The sender must obey the dictation of the receiver in this case.

9. *Checksum***.** This 16-bit field contains the checksum. The calculation of the checksum for TCP follows the same procedure as the one described for UDP. However, the inclusion of the checksum in the UDP datagram is optional, whereas the inclusion of the checksum for TCP is mandatory. The same pseudoheader, serving the same purpose, is added to the segment. For the TCP pseudoheader, the value for the protocol field is 6.

10. *Urgent pointer*. This l6-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

11. *Options***.** There can be up to 40 bytes of optional information in the TCP header.

- **A TCP Connection**

TCP is connection-oriented. A connection-oriented transport protocol establishes a virtual path between the source and destination. All the segments belonging to a message are then sent over this virtual path. Using a single virtual pathway for the entire message facilitates the acknowledgment process as well as retransmission of damaged or lost frames. You may wonder how TCP, which uses the services of IP, a connectionless protocol, can be connection-oriented. The point is that a TCP connection is virtual, not physical. TCP operates at a higher level. TCP uses the services of IP to deliver individual segments to the receiver, but it controls the connection itself. If a segment is lost or corrupted, it is retransmitted. Unlike TCP, IP is unaware of this retransmission. If a segment arrives out of order, TCP holds it until the missing segments arrive; IP is unaware of this reordering.

- **TCP Transmission**

In TCP, connection-oriented transmission requires three phases: connection establishment, data transfer, and connection termination.

a. Connection Establishment

TCP transmits data in full-duplex mode. When two TCPs in two machines are connected, they are able to send segments to each other simultaneously. This implies that each party must initialize communication and get approval from the other party before any data are transferred.

Three-Way Handshaking The connection establishment in TCP is called three-way handshaking. In our example, an application program, called the client, wants to make a connection with another application program, called the server, using TCP as the transport layer protocol.

The process starts with the server. The server program tells its TCP that it is ready to accept a connection. This is called a request for a *passive open.* Although the server TCP is ready to accept any connection from any machine in the world, it cannot make the connection itself.

The client program issues a request for an *active open.* A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. TCP can now start the three-way handshaking process as shown in Figure 4.18.

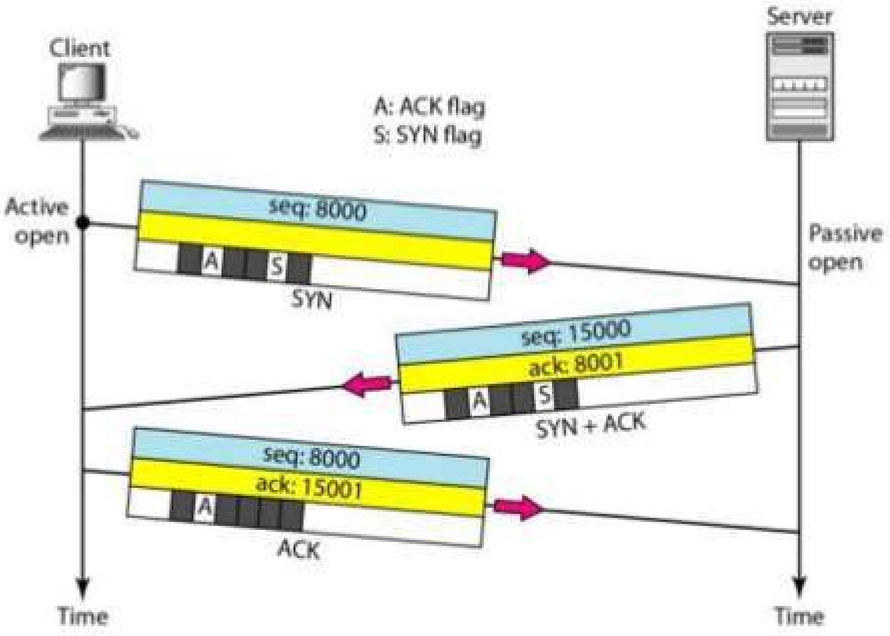


Figure 4.18 Connection establishment using three-way handshaking

To show the process, we use two time lines: one at each site. Each segment has values for all its header fields and perhaps for some of its option fields, too. However, we show only the few fields necessary to understand each phase. We show the sequence number, the acknowledgment number, the control flags (only those that are set), and the window size, if not empty. The three steps in this phase are as follows.

1. The client sends the first segment, a SYN segment, in which only the SYN flag is set. This segment is for synchronization of sequence numbers. It consumes one sequence number. When the data transfer starts, the sequence number is incremented by 1. We can say that the SYN segment carries no real data, but we can think of it as containing 1 imaginary byte.

A SYN segment cannot carry data, but it consumes one sequence number.

2. The server sends the second segment, a SYN +ACK segment, with 2 flag bits set: SYN and ACK. This segment has a dual purpose. It is a SYN segment for communication in the other direction and serves as the acknowledgment for the SYN segment. It consumes one sequence number.

A SYN +ACK segment cannot carry data, but does consume one sequence number.

3. The client sends the third segment. This is just an ACK segment. It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field. Note that the sequence number in this segment is the same as the one in the SYN segment; the ACK segment does not consume any sequence numbers.

An ACK segment, if carrying no data, consumes no sequence number.

Simultaneous Open: A rare situation, called a simultaneous open, may occur when both processes issue an active open. In this case, both TCPs transmit a SYN + ACK segment to each other, and one single connection is established between them.

SYN Flooding Attack: The connection establishment procedure in TCP is susceptible to a serious security problem called the SYN flooding attack. This happens when a malicious attacker sends a large number of SYN segments to a server, pretending that each of them is corning from a different client by faking the source IP addresses in the datagrams.

The server, assuming that the clients are issuing an active open, allocates the necessary resources, such as creating communication tables and setting timers. The TCP server then sends the SYN +ACK segments to the fake clients, which are lost. During this time, however, a lot of resources are occupied without being used. If, during this short time, the number of SYN segments is large, the server eventually runs out of resources and may crash. This SYN flooding attack belongs to a type of security attack known as a denial-of-service attack, in which an attacker monopolizes a system with so many service requests that the system collapses and denies service to every request.

Some implementations of TCP have strategies to alleviate the effects of a SYN attack. Some have imposed a limit on connection requests during a specified period of time. Others filter out datagrams coming from unwanted source addresses. One recent strategy is to postpone resource allocation until the entire connection is set up, using cookie.

b. Data Transfer

After connection is established, bidirectional data transfer can take place. The client and server can both send data and acknowledgments. Data travels in the same direction as an acknowledgment are carried on the same segment.

The acknowledgment is piggybacked with the data. Figure 4.19 shows an example. In this example, after connection is established (not shown in the figure), the client sends 2000 bytes of data in two segments. The server then sends 2000 bytes in one segment.

The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgment because there are no more data to be sent. Note the values of the sequence and acknowledgment numbers. The data segments sent by the client have the PSH (push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received.

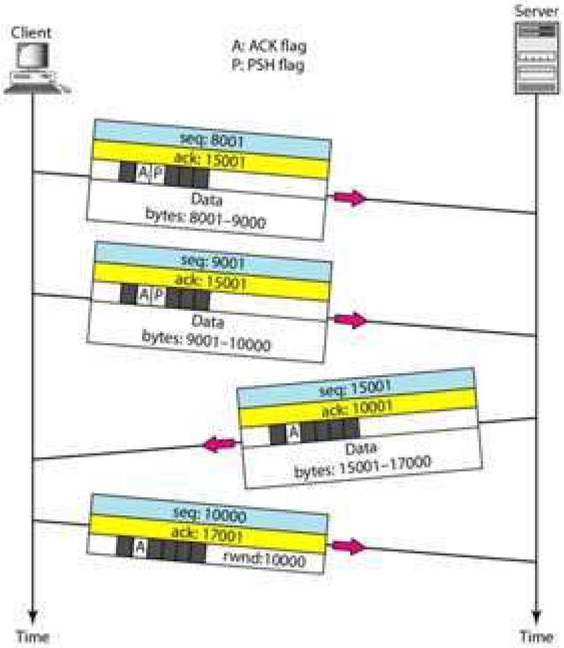


Figure 4.19 Data transfer

The segment from the server, on the other hand, does not set the push flag. Most TCP implementations have the option to set or not set this flag.

Pushing Data: The sending TCP uses a buffer to store the stream of data coming from the sending application program. The sending TCP can select the segment size. The receiving TCP also buffers the data when they arrive and delivers them to the application program when the application program is ready or when it is convenient for the receiving TCP. This type of flexibility increases the efficiency of TCP.

However, on occasion the application program has no need for this flexibility_ For example, consider an application program that communicates interactively with another application program on the other end. The application program on one site wants to send a keystroke to the application at the other site and receive an immediate response. Delayed transmission and delayed delivery of data may not be acceptable by the application program.

TCP can handle such a situation. The application program at the sending site can request a *push* operation. This means that the sending TCP must not wait for the window to be filled. It must create a segment and send it immediately. The sending TCP must also set the push bit (PSH) to let the receiving TCP know that the segment includes data that must be delivered to the receiving application program as soon as possible and not to wait for more data to come.

Although the push operation can be requested by the application program, most current implementations ignore such requests. TCP can choose whether or not to use this feature.

Urgent Data TCP is a stream-oriented protocol. This means that the data are presented from the application program to TCP as a stream of bytes. Each byte of data has a position in the stream. However, on occasion an application program needs to send *urgent* bytes. This means that the sending application program wants a piece of data to be read out of order by the receiving application program. As an example, suppose that the sending application program is sending data to be processed by the receiving application program. When the result of processing comes back, the sending application program finds that everything is wrong. It wants to abort the process, but it has already sent a huge amount of data. If it issues an abort command (control +C), these two characters will be stored at the end of the receiving TCP buffer. It will be delivered to the receiving application program after all the data have been processed.

The solution is to send a segment with the URG bit set. The sending application program tells the sending TCP that the piece of data is urgent. The sending TCP creates a segment and inserts the urgent data at the beginning of the segment. The rest of the segment can contain normal data from the buffer. The urgent pointer field in the header defines the end of the urgent data and the start of normal data.

When the receiving TCP receives a segment with the URG bit set, it extracts the urgent data from the segment, using the value of the urgent pointer, and delivers them, out of order, to the receiving application program.

c. Connection Termination

Any of the two parties involved in exchanging data (client or server) can close the connection, although it is usually initiated by the client. Most implementations today allow two options for connection termination: three-way handshaking and four-way handshaking with a half-close option.

Three-Way Handshaking Most implementations today allow *three-way handshaking* for connection termination as shown in Figure 4.20.

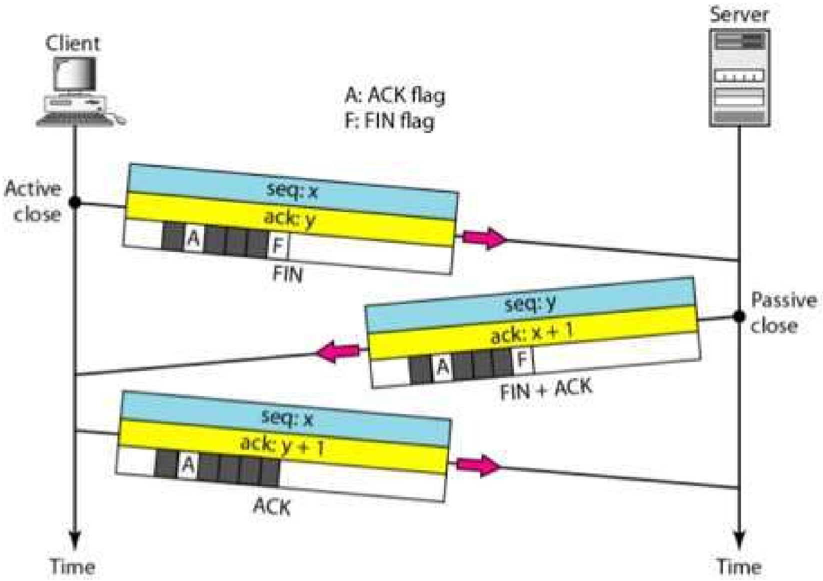


Figure 4.20 Connection termination using three-way handshaking

1. In a normal situation, the client TCP, after receiving a close command from the client process, sends the first segment, a FIN segment in which the FIN flag is set.

Note that a FIN segment can include the last chunk of data sent by the client, or it can be just a control segment as shown in Figure 4.20. If it is only a control segment, it consumes only one sequence number.

The FIN segment consumes one sequence number if it does not carry data.

2. The server TCP, after receiving the FIN segment, informs its process of the situation and sends the second segment, a FIN +ACK segment, to confirm the receipt of the FIN segment from the client and at the same time to announce the closing of the connection in the other direction. This segment can also contain the last chunk of data from the server. If it does not carry data, it consumes only one sequence number.

The FIN +ACK segment consumes one sequence number if it does not carry data.

3. The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server. This segment contains the acknowledgment number, which is 1 plus the sequence number received in the FIN segment from the server. This segment cannot carry data and consumes no sequence numbers. Half-Close In TCP, one end can stop sending data while still receiving data. This is called a half-close. Although either end can issue a half-close, it is normally initiated by the client. It can occur when the server needs all the data before processing can begin.

Figure 4.21 shows an example of a half-close. The client half-closes the connection by sending a FIN segment. The server accepts the half-close by sending the ACK segment.

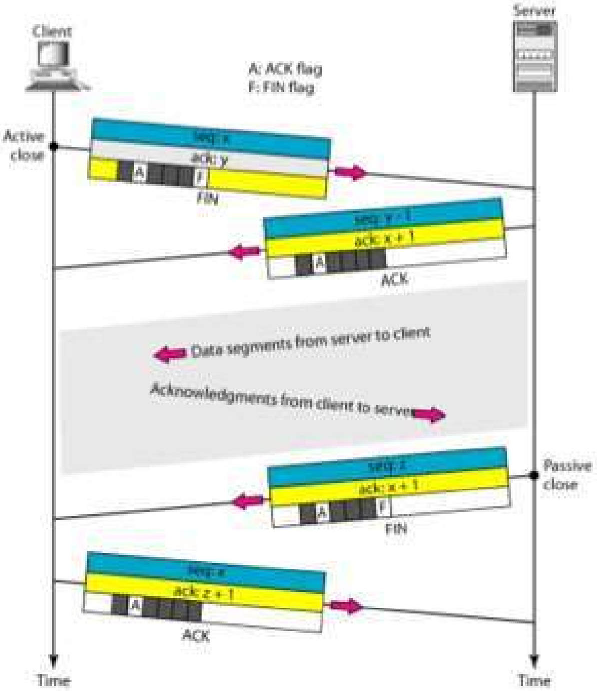


Figure 4.21 Half-close

The data transfer from the client to the server stops. The server, however, can still send data. When the server has sent all the processed data, it sends a FIN segment, which is acknowledged by an ACK from the client.

After half-closing of the connection, data can travel from the server to the client and acknowledgments can travel from the client to the server. The client cannot send any more data to the server. Note the sequence numbers we have used. The second segment (ACK) consumes no sequence number. Although the client has received sequence number *y* - 1 and is expecting *y,* the server sequence number is still *y* - 1. When the connection finally closes, the sequence number of the last ACK segment is still *x,* because no sequence numbers are consumed during data transfer in that direction.

4.5 Short Questions and Answers

1. What is function of transport layer?

The protocol in the transport layer takes care in the delivery of data from one application program on one device to an application program on another device. They act as a link between the upper layer protocols and the services provided by the lower layer.

2. What are the duties of the transport layer?

The services provided by the transport layer

- ✓ End-to- end delivery
- ✓ Addressing
- ✓ Reliable delivery Flow control Multiplexing

3. What is the difference between network layer delivery and the transport layer delivery?

Network Layer Delivery	Transport Layer Delivery
The network layer is responsible for the source-to-destination delivery of packet across multiple network links.	The transport layer is responsible for source-to-destination delivery of the entire message.

4. What are the four aspects related to the reliable delivery of data?

The four aspects are;

- ✓ Error control,
- ✓ Sequence control,
- ✓ Loss control
- ✓ Duplication control

5. What is meant by segment?

At the sending and receiving end of the transmission, TCP divides long transmissions into smaller data units and packages each into a frame called a segment.

6. What is meant by segmentation?

When the size of the data unit received from the upper layer is too long for the network layer datagram or data link layer frame to handle, the transport protocol divides it into smaller usable blocks. The dividing process is called segmentation.

7. What is meant by Concatenation?

The size of the data unit belonging to a single session are so small that several can fit together into a single datagram or frame, the transport protocol combines them into a single data unit. The combining process is called concatenation.

8. What are the types of multiplexing?

The types of multiplexing are, Upward multiplexing Downward multiplexing

9. What are the two possible transport services?

Two basic types of transport services are, Connection-oriented service , Connectionless services.

10. The transport layer creates the connection between source and destination. What are the three events involved in the connection?

For security , the transport layer may create a connection between the two end ports.

A connection is a single logical path between the source and destination that is associated with all packets in a message. Creating a connection involves three steps:

- ✓ Connection establishment
- ✓ Data transfer
- ✓ Connection release.

11. What are the techniques used in multiplexing?

The three basic techniques of multiplexing are,

- ✓ Frequency-division multiplexing
- ✓ Time-division multiplexing
- ✓ Wave-division multiplexing

12. What is meant by congestion?

Congestion in a network occur if user send data into the network at a rate greater than that allowed by network resources.

13. Why the congestion occurs in network?

Congestion occur because the switches in a network have a limited buffer size to store arrived packets.

14. How will the congestion be avoided?

The congestion may be avoided by two bits

- ✓ BECN - Backward Explicit Congestion Notification
- ✓ FECN - Forward Explicit Congestion Notification

15. What is the function of BECN BIT?

The BECN bit warns the sender of congestion in network. The sender can respond to this warning by simply reducing the data rate.

16. What is the function of FECN?

The FECN bit is used to warn the receiver of congestion in the network. The sender and receiver are communicating with each other and are using some types of flow control at a higher level.

17. What is meant by quality of service?

The quality of service defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute each service class is associated with a set of attributes.

18. What are the two categories of QoS attributes?

The two main categories are User Oriented and Network Oriented

19. List out the user related attributes?

User related attributes are

- ✓ SCR – Sustainable Cell Rate
- ✓ PCR – Peak Cell Rate
- ✓ MCR- Minimum Cell Rate
- ✓ CVDT – Cell Variation Delay Tolerance

20. What are the networks related attributes?

The network related attributes are, Cell loss ratio (CLR) , Cell transfer delay (CTD) ,Cell delay variation (CDV), Cell error ratio (CER)

21. What is frame?

A frame consists of one complete cycle of time slots, including one or more slot dedicated to each sending device.

22. What is interleaving?

The switch moves from device to device at a constant rate and fixed order. This process is called interleaving.

23. What is framing bits?

One or more synchronization bits are usually added to the beginning of each frame. These bitts are called framing bits.

24. What is the difference between service point address, logical address and physical address?

Service Point Addressing	Logical Addressing	Physical Addressing
The transport layer header includes a type of address called a service point address or port address, which makes a data delivery from a specific process on one computer to a specific process on another process.	If a packet passes the network boundary we need another addressing to differentiate the source and destination systems. The network layer adds a header, which indicate the logical address of the sender and receiver	If the frames are to be distributed to different systems on the network, the data link layer adds the header, which defines the source machine's address and the destination machine's address,

25. What are the fields on which the UDP checksum is calculated? Why?

UDP checksum includes a pseudo header, the UDP header and the data coming from the application layer.

26. What are the advantages of using UDP over TCP?

- ✓ UDP does not include the overhead needed to detect reliability
- ✓ It does not need to maintain the unexpected deception of data flow
- ✓ UDP requires less processing at the transmitting and receiving of hosts.
- ✓ It is simple to use for a network
- ✓ The OS does not need to maintain UDP connection information.

27. What is TCP?

TCP provides a connection oriented, reliable byte stream service. The connection oriented means the two applications using TCP must establish a TCP connection with each other before they can exchange data.

28. List the flag used in TCP header.

TCP header contains six flags. They are URG, ACK, PSH, RST, SYN, FIN

29. Give the approaches to improve the QoS

Fine grained approaches, which provide QoS to individual applications or flows. Integrated services, QoS architecture developed in the IETE and often associated with RSVP.

30. What do you mean by QoS?

Quality of Service is used in some organizations to help provide an optimal end user experience for audio and video communications. QoS is most commonly used on networks where bandwidth is limited with a large number of network packets competing for a relatively small amount of available and width.

31. What is multiplexing?

The job of gathering data chunks at the sources host from different sockets, encapsulating each data chunks with header information to create segments, and passing the segments to the network layer is called multiplexing.

32. What is de-multiplexing?

The job of delivering the data in a transport layer segment to the correct socket is called demultiplexing.

33. What is RTT?

RTT is an acronym for Round Trip Time: it is a measure of the time it takes for a packet to travel from a computer, across a network to another computer, and back.

34. What is the segment?

Transport layer protocols send data as a sequence of packets. In TCP/IP these packets are called segments.

35. What is a port?

Applications running on different hosts communicate with TCP with the help of a concept called as ports. A port is a 16 bit unique number allocated to a particular application.

36. List the services of end to end services.

- ✓ Guarantee message delivery.
- ✓ Delivery messages in the same order they are sent.
- ✓ Deliver at most one copy of each message.
- ✓ Support arbitrarily large message.
- ✓ Support synchronization.

37. What are the functions of transport layer?

- ✓ Breaks messages into packets.
- ✓ Connection control.
- ✓ Addressing.
- ✓ Provide reliability.

38. List the three types of addresses in TCP/IP.

Three types of addresses are used by systems using the TCP/IP protocol: the physical address, the internetwork address (IP address), and the port address.

39. What are the flow characteristics related to QoS?

The flow characteristics related to QoS are

- ✓ Reliability

- ✓ Delay
- ✓ Jitter
- ✓ Bandwidth

40. What are the techniques to improve QoS?

The techniques to improve QoS are

- ✓ Scheduling
- ✓ Traffic shaping
- ✓ Resource reservation
- ✓ Admission control

41. Define Socket address.

The combination of IP address and port address is called Socket address.

42. What are the two types of protocols used in Transport layer?

The two types of protocols used in Transport layer are TCP and UDP

43. Define Throughput.

It is defined as a number of packets passing through the network in a unit of time.

44. Define UDP

User datagram protocol is a Unreliable, connectionless protocol, used along with the IP protocol.

45. What is the need of port numbers?

Port numbers are used as an addressing mechanism in transport layer.

46. What are the types of port numbers used in transport layer?

- ✓ Well-known port
- ✓ Registered port
- ✓ Dynamic port

47. Why TCP services are called Stream delivery services?

TCP allows the sending process to deliver data as a stream of bytes and the receiving process to deliver data as a stream of bytes. So it is called as stream of bytes.

48. Compare connectionless service & connection oriented service

In connection less service there is no connection between transmitter & receiver Ex: UDP
In connection oriented service there is a connection between transmitter & receiver Ex: TCP

49. Write the main idea of UDP.

User Datagram Protocol. Transport protocol that provides a connectionless datagram service to application level processes. The basic idea is for a source process to send a message to a port and for the destination process to receive the message from a port.

50. What are the different fields in pseudo header?

- ✓ Protocol number
- ✓ Source IP address
- ✓ Destination IP addresses.

51. Define TCP.

Transmission Control Protocol. Connection-oriented transport protocol. It guarantees reliable, byte-stream delivery service. It is a full-duplex protocol, each TCP connection supports a pair of byte streams, one flowing in each direction.

52. State the two kinds of events trigger a state transition.

- ✓ A segment arrives from the peer.
- ✓ The local application process invokes an operation on TCP.

53. Define Gateway.

A device used to connect two separate networks that use different communication protocols.

54. What is meant by quality of service? What are the two categories of it?

The quality of service defines a set of attributes related to the performance of the connection. For each connection, the user can request a particular attribute each service class is associated with a set of attributes. The two main categories are,

- ✓ User Oriented
- ✓ Network Oriented

4.6 Explanatory Questions

1. Explain about the transport Service. (5 marks)
2. What are the transport service primitives? (5 marks)
3. Explain briefly about the elements of transport protocols. (5 marks)
4. Describe the addressing scheme in elements of transport protocols. (5 marks)
5. Discuss on the working of TCP protocol in Transport layer. (5 marks)
6. Explain the functioning of UDP. (5 marks)
7. Discuss the working of TCP congestion Control Mechanism. (5 marks)
8. Explain the duties of transport layer. (10 marks)
9. Explain UDP & TCP. (10 marks)
10. Explain about congestion control. (10 marks)
11. Explain the Congestion Avoidance techniques in detail. (10 marks)
12. Explain how QoS is provided through Integrated Services & Differentiated Services. (10 marks)

13. Discuss the method of establishing and releasing connection in Transport Protocol. (10 marks)

4.7 Objective Questions and Answers

1. The receiver of the data controls the amount of data that are to be sent by the sender is referred as ___________

   a) Flow control b) Error control c) Congestion control d) Error detection

   Answer: a

   Explanation: Flow control is done to prevent the receiver from being overwhelmed with data.

2. Size of TCP segment header ranges between ___________

   a) 16 and 32 bytes b) 16 and 32 bits c) 20 and 60 bytes d) 20 and 60 bits

   Answer: c

   Explanation: The header is 20 bytes if there are no options and upto 60 bytes if it contains options.

3. Connection establishment in TCP is done by which mechanism?

   a) Flow control b) Three-Way Handshaking c) Forwarding d) Synchronization

   Answer: b

   Explanation: Three-Way Handshaking is used to connect between client and server.

4. The server program tells its TCP that it is ready to accept a connection. This process is called ___________

   a) Active open b) Active close c) Passive close d) Passive open

   Answer: d

   Explanation: This is the first step in the Three-Way Handshaking process and is started by the server.

5. The process of, A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server is ___________

   a) Active open b) Active close c) Passive close d) Passive open

   Answer: a

   Explanation: This is the second step in the Three-Way Handshaking process and is done by the client once it finds the open server.

6. In Three-Way Handshaking process, the situation where both the TCP's issue an active open is ___________

   a) Mutual open b) Mutual Close c) Simultaneous open d) Simultaneous close

Answer: c

Explanation: Here, both TCP's transmit a SYNC+ACK segment to each other and one single connection is established between them.

7. The situation when a malicious attacker sends a large number of SYNC segments to a server, pretending that each of them is coming from a different client by faking the source IP address in the datagrams.

   a) SYNC flooding attack b) Active attack c) Passive attack
   d) Denial-of-service attack

   Answer: a

   Explanation: This is the serious security problem during the connection establishment.

8. SYNC flooding attack belongs to a type of security attack known as ___________

   a) SYNC flooding attack b) Active attack c) Passive attack

   d) Denial-of-service attack

   Answer: d

   Explanation: During SYNC flooding the system collapses and denies service to every request.

9. Size of source and destination port address of TCP header respectively are ___________

   a) 16-bits and 32-bits b) 16-bits and 16-bits c) 32-bits and 16-bits
   d) 32-bits and 32-bits

   Answer: b

   Explanation: Size of source and destination ports must be 32-bits.

10. What allows TCP to detect lost segments and in turn recover from that loss?

    a) Sequence number b) Acknowledgment number c) Checksum
    d) Both Sequence & Acknowledgment number

    Answer: b

    Explanation: TCP header contains separate fields for sequence number and acknowledgment number. Its these values that allow TCP to detect lost segments and in turn recover from that loss.

11. Which mode of IPsec should you use to assure security and confidentiality of data within the same LAN?

    a) AH transport mode b) ESP transport mode c) ESP tunnel mode
    d) AH tunnel mode

    Answer: b

    Explanation: ESP transport mode should be used to ensure the integrity and confidentiality of data that is exchanged within the same LAN.

12. Which two types of encryption protocols can be used to secure the authentication of computers using IPsec?

a) Kerberos V5 b) SHA c) MD5 d) Both SHA and MD5

Answer: d

Explanation: SHA or MD5 can be used. Kerberos V5 is an authentication protocol, not an encryption protocol; therefore, answer A is incorrect. Certificates are a type of authentication that can be used with IPsec, not an encryption protocol; therefore, answer B is incorrect.

13. Which two types of IPsec can be used to secure communications between two LANs?

a) AH tunnel mode b) ESP tunnel mode
c) Both AH tunnel mode and ESP tunnel mode d) ESP transport mode

Answer: c

Explanation: A tunnel mode IPsec should be used. Option c is for data transfer purpose, option d is for integrity & confidentiality purpose.

14. ______ provides authentication at the IP level.

a) AH b) ESP c) PGP d) SSL

Answer: a

Explanation: It provides integrity checking and anti-reply security.

15. IPsec defines two protocols: _______ and ________

a) AH; SSL b) PGP; ESP c) AH; ESP d) All of the mentioned

Answer: c

Explanation: Authentication header and Encryption security payload.

16. IP Security operates in which layer of the OSI model?

a) Network b) Transport c) Application d) Physical

Answer: a

Explanation: Network layer is mainly used for security purpose, so IPsec in mainly operates in network layer.

17. ESP provides

a) source authentication b) data integrity
c) privacy d) all of the mentioned

Answer: d

Explanation: Encrypted security payload provides source, data integrity and privacy.

18. In computer security… means that computer system assets can be modified only by authorized parities.

a) Confidentiality b) Integrity c) Availability d) Authenticity

Answer: b

Explanation: Integrity means that computer system assets can be modified only by authorized parities.

19. In computer security… means that the information in a computer system only be accessible for reading by authorized parities.

a) Confidentiality b) Integrity c) Availability d) Authenticity

Answer: a

Explanation: Confidentiality means that the information in a computer system only be accessible for reading by authorized parities.

20. Which of the following organizations is primarily concerned with military encryption systems?

a) NSA b) NIST c) IEEE d) ITU

Answer: a

Explanation: The NSA is primarily responsible for military encryption systems. The NSA designs, evaluates, and implements encryption systems for the military and government agencies with high security needs.

21. Which of the following is true with respect to TCP

a)Connection-oriented b)Process-to-process c)Transport layer protocol d)All of the mentioned

Answer: d

Explanation: TCP is a transport layer protocol, process-to-process, and creates a virtual connection between two TCP's.

22. In TCP, sending and receiving data is done as

a) Stream of bytes b) Sequence of characters c) Lines of data d) Packets

Answer: a

Explanation: In TCP, data is sent and received in terms of Stream of bytes.

23. TCP process may not write and read data at the same speed. So we need __________ for storage.

a) Packets b) Buffers c) Segments d) Stacks

Answer: b

Explanation: TCP needs buffers for storage to overcome this problem.

24. TCP groups a number of bytes together into a packet called

a) Packet b) Buffer c) Segment d) Stack

Answer: c

Explanation: Segment is a grouping of number of bytes together into a packet.

25. Communication offered by TCP is

a) Full-duplex b) Half-duplex c) Semi-duplex d) Byte by byte

Answer: a

Explanation: Data flow in both the directions at the same time during TCP communication hence, Full-duplex.

26. To achieve reliable transport in TCP, ___________ is used to check the safe and sound arrival of data.

a) Packet b) Buffer c) Segment d) Acknowledgment

Answer: d

Explanation: Acknowledgment mechanism is used to check the safe and sound arrival of data.

27. In segment header, sequence number and acknowledgement number field refers to

a) Byte number b) Buffer number c) Segment number d) Acknowledgment

Answer: a

Explanation: Sequence number and acknowledgement number field refers to byte number.

28. Suppose a TCP connection is transferring a file of 1000 bytes. The first byte is numbered 10001. What is the sequence number of the segment if all data is sent in only one segment.

a) 10000 b) 10001 c) 12001 d) 11001

Answer: b

Explanation: The sequence number of each segment is the number of first byte carried in that segment.

29. Bytes of data being transferred in each connection are numbered by TCP. These numbers starts with a

a) Random number b) Zero c) One d) Sequence of zero's and one's

Answer: d

Explanation: These numbers starts with a random number.

30. The value of acknowledgement field in a segment defines

a) Number of previous bytes to receive b) Total number of bytes to receive
c) Number of next bytes to receive d) Sequence of zero's and one's

Answer: c

Explanation: Acknowledgement field in a segment defines the number of next bytes to receive.

31. Transport layer aggregates data from different applications into a single stream before passing it to

a) network layer b) data link layer c) application layer d) physical layer

Answer: a

Explanation: The flow of data in the OSI model flows in following manner Application -> Presentation -> Session -> Transport -> Network -> Data Link -> Physical.

32. Which one of the following is a transport layer protocol used in networking?

a) TCP b) UDP c) Both TCP and UDP d) None of the mentioned

Answer: c

Explanation: Both TCP and UDP are transport layer protocol in networking. TCP is an abbreviation for Transmission Control Protocol and UDP is an abbreviation for User Datagram Protocol. TCP is connection oriented whereas UDP is connectionless.

33. User datagram protocol is called connectionless because

a) all UDP packets are treated independently by transport layer
b) it sends data as a stream of related packets
c) it is received in the same order as sent order
d) none of the mentioned

Answer: a

Explanation: UDP is an alternative for TCP and it is used for those purposes where speed matters most whereas loss of data is not a problem. UDP is connectionless whereas TCP is connection oriented.

34. Transmission control protocol is

a) connection oriented protocol
b) uses a three way handshake to establish a connection
c) receives data from application as a single stream
d) all of the mentioned

Answer: d

Explanation: Major internet applications like www, email, file transfer etc rely on tcp. TCP is connection oriented and it is optimized for accurate delivery rather than timely delivery.

It can incur long delays.

35. An endpoint of an inter-process communication flow across a computer network is called

a) socket b) pipe c) port d) none of the mentioned

Answer: a

Explanation: Socket is one end point in a two way communication link in the network. TCP layer can identify the application that data is destined to be sent by using the port number that is bound to socket.

36. Socket-style API for windows is called

a) wsock b) winsock c) wins d) none of the mentioned

Answer: b

Explanation: Winsock is a programming interface which deals with input output requests for internet applications in windows OS. It defines how windows network software should access network services.

37. Which one of the following is a version of UDP with congestion control?

a) datagram congestion control protocol b) stream control transmission protocol
c) structured stream transport d) none of the mentioned

Answer: a

Explanation: The datagram congestion control is a transport layer protocol which deals with reliable connection setup, teardown, congestion control, explicit congestion notification, feature negotiation.

38. A _____ is a TCP name for a transport service access point.

a) port b) pipe c) node d) none of the mentioned

Answer: a

Explanation: Just as the IP address identifies the computer, the network port identifies the application or service running on the computer. A port number is 16 bits.

39. Transport layer protocols deals with

a) application to application communication
b) process to process communication
c) node to node communication
d) none of the mentioned

Answer: b

Explanation: Transport layer is 4th layer in TCP/IP model and OSI reference model. It deals with logical communication between process. It is responsible for delivering a message between network host.

40. Which one of the following is a transport layer protocol?

a) stream control transmission protocol
b) internet control message protocol
c) neighbor discovery protocol
d) dynamic host configuration protocol

Answer: a

Explanation: There are many protocols in transport layer. The most prominent are TCP and UDP. Some of the other protocols are RDP, RUDP, SCTP, DCCP etc.

41. Which of the following is false with respect to UDP

a) Connection-oriented b) Unreliable c) Transport layer protocol
d) All of the mentioned

Answer: a

Explanation: UDP is an unreliable, connectionless transport layer protocol.

42. Return value of the UDP port "Chargen" is

a) String of characters b) String of integers c) Array of characters with integers d) Array of zero's and one's

Answer: a

Explanation: Chargen with port number 19 returns string of characters.

43. Beyond IP, UDP provides additional services such as

a) Routing and switching b) Sending and receiving of packets

c) Multiplexing and demultiplexing d) Demultiplexing and error checking

Answer: d

Explanation: UDP is a simple protocol which provides demultiplexing and error checking.

44. The main advantage of UDP is

a) More overload b) Reliable c) Less overload d) Fast

Answer: c

Explanation: UDP is an unreliable, connectionless transport layer protocol and uses minimum overload.

45. Port number used by Network Time Protocol(NTP) with UDP is

a) 161 b) 123 c) 162 d) 124

Answer: b

Explanation: Port number used by Network Time Protocol with UDP is 123.

46. What is the header size of UDP packet?

a) 8 bytes b) 8 bits c) 16 bytes d) 124 bytes

Answer: a

Explanation: The fixed size of the UDP packet header is 8 bytes.

47. The port number is "ephemeral port number", if the source host is ……

a) NTP b) Echo c) Server d) Client

Answer: d

Explanation: If the source host is the client, the port number in most cases will be ephemeral port number.

48. “Total length” field in UDP packet header is the length of

a) Only UDP header b) Only data c) Only checksum d) UDP header plus data

Answer: d

Explanation: Total length is the 16 bit field which contains the length of UDP header and the data.

49. Correct expression for UDP user datagram length is

a) UDP length = IP length – IP header’s length
b) UDP length = UDP length – UDP header’s length
c) UDP length = IP length + IP header’s length
d) UDP length = UDP length + UDP header’s length

Answer: a

Explanation: A user datagram is encapsulated in an IP datagram. There is a field in the IP datagram defines the total length. There is another field in the IP datagram that defines the length of the header. So if we subtract the length of a UDP datagram that is encapsulated in an IP datagram, we get the length of UDP user datagram.

50. The field used to detect errors over the entire user datagram is

a) UDP header b) Checksum c) Source port d) Destination port

Answer: b

Explanation: Checksum field is used to detect errors over the entire user datagram.

5 Application Layer

5.1 Introduction

An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network. The application layer abstraction is used in both of the standard models of computer networking: the Internet Protocol Suite (TCP/IP) and the OSI model. Although both models use the same term for their respective highest-level layer, the detailed definitions and purposes are different.

In TCP/IP, the application layer contains the communications protocols and interface methods used in process-to-process communications across an Internet Protocol (IP) computer network. The application layer only standardizes communication and depends upon the underlying transport layer protocols to establish host-to-host data transfer channels and manage the data exchange in a client-server or peer-to-peer networking model. Though the TCP/IP application layer does not describe specific rules or data formats that applications must consider when communicating, the original specification (in RFC 1123) does rely on and recommend the robustness principle for application design.

In the OSI model, the definition of the application layer is narrower in scope. The OSI model defines the application layer as the user interface responsible for displaying received information to the user. In contrast, the Internet Protocol Suite does not concern itself with such detail. OSI also explicitly distinguishes additional functionality below the application layer, but above the transport layer at two additional levels: the session layer, and the presentation layer. OSI specifies a strict modular separation of functionality at these layers and provides protocol implementations for each layer.

5.2 Domain Name System

This is primarily used for mapping host and e-mail destinations to IP addresses but can also be used other purposes. DNS is defined in RFCs 1034 and 1035. DNS is a hierarchical, domain-based naming scheme and a distributed database system for implementing this naming scheme. To map a name to an IP address, an application program calls a library procedure called the resolver passing it the name as parameter. This sends a UDP packet to a local DNS server, which looks up the name and returns the IP address.

- **Working Method**

1. To map a name onto an IP address, an application program calls a library procedure called Resolver, passing it the name as a parameter.
2. The resolver sends a UDP packet to a local DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller.
3. Armed with the IP address, the program can then establish a TCP connection with the destination, or send it UDP packets.

5.2.1 Components of DNS

1. The DNS name space.
2. Resource Records.
3. Name Servers.

1. *The DNS Name Space*

The Internet is divided into several hundred top level domains, where each domain covers many hosts. Each domain is partitioned into sub domains, and these are further partitioned as so on. All these domains can be represented by a tree, in which the leaves represent domains that have no sub domains. A leaf domain may contain a single host, or it may represent a company and contains thousands of hosts. Each domain is named by the path upward from it to the root. The components are separated by periods (pronounced "dot")

Eg: Sun Microsystems Engg. Department = eng.sun.com.

- The top domain comes in 2 flavours:-
    1) ***Generic***: com(commercial), edu(educational instructions), mil(the U.S armed forces, government), int (certain international organizations), net(network providers), org (non profit organizations).
    2) ***Country***: include 1 entry for every country. Domain names can be either absolute (ends with a period e.g. eng.sum.com) or relative (doesn't end with a period). Domain names are case sensitive and the component names can be up to 63 characters long and full path names must not exceed 255 characters.

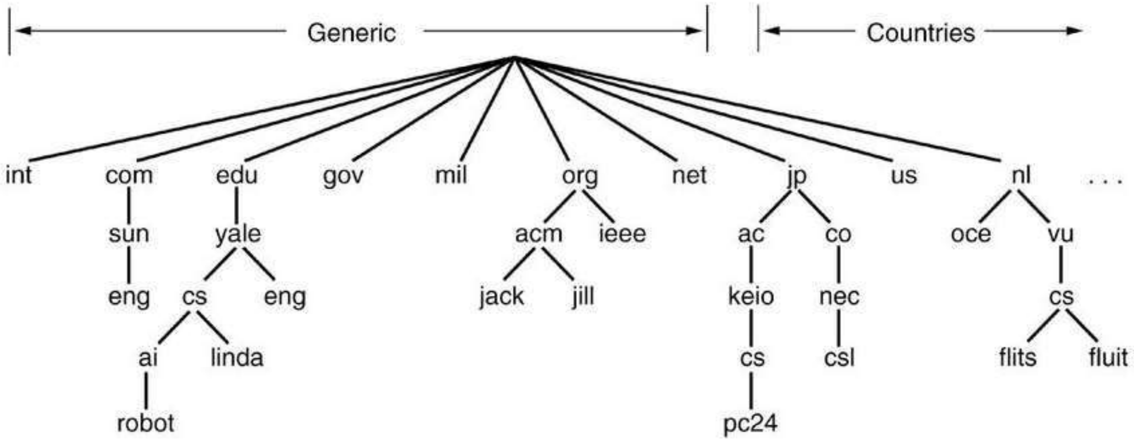
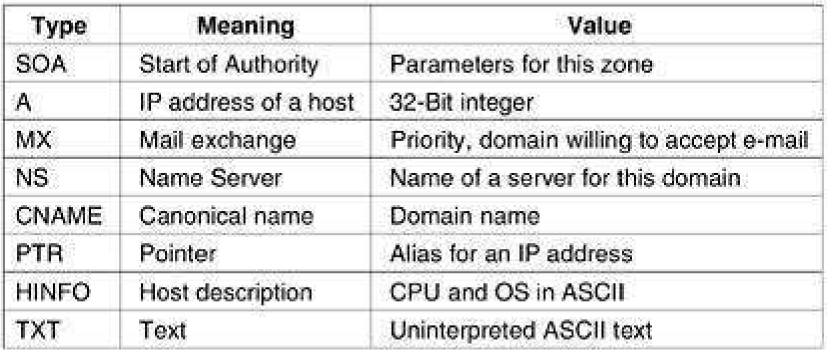


Figure 5.1 Top two domains

2. *Resource Records*

Every domain can have a set of resource records associated with it. For a single host, the most common resource record is just its IP address. When a resolver gives a domain name to DNS, it gets both the resource records associated with that name i.e., the real function of DNS is to map domain names into resource records. A resource record is a 5-tuple and its format is shown in Figure 5.2:

Domain	Name	Time to live	Type	Class	Value



Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

Figure 5.2 Resource record and Type values

1. **Domain _name :** Tells the domain to which this record applies.
2. **Time- to- live :** Gives an identification of how stable the record is (High Stable = 86400 i.e. no. of seconds /day) (High Volatile = 1 min)
3. **Type:** Tells what kind of record this is (*Figure 5.2*).
4. **Class:** It is IN for the internet information and codes for non internet information
5. **Value:** This field can be a number a domain name or an ASCII string

3. Name Servers

It contains the entire database and responds to all queries about it. DNS name space is divided up into non-overlapping zones, in which each zone contains some part of the tree and also contains name servers holding the authoritative information about that zone.

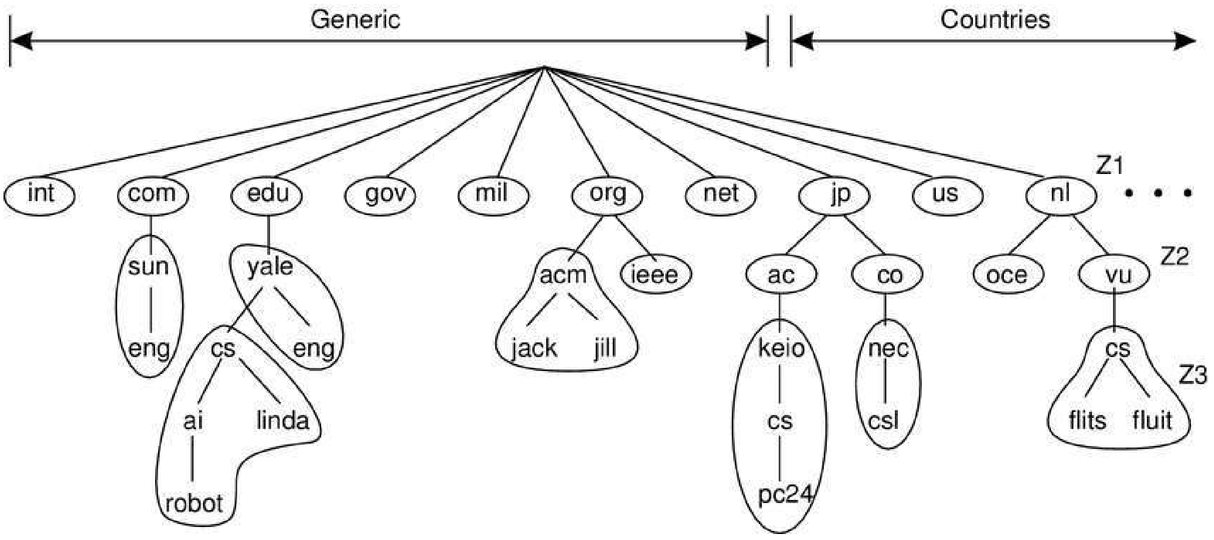


Figure 5.3. Part of the DNS name space showing the division into zones.

When a resolver has a query about a domain name, it passes the query to one of the local name servers:

1. If the domain being sought falls under the jurisdiction of name server, it returns the authoritative resource records (that comes from the authority that manages the record, and is always correct).
2. If the domain is remote and no information about the requested domain is available locally the name server sends a query message to the top level name server for the domain requested.

   E.g.: A resolver of flits.cs.vle.nl wants to know the IP address of the host Linda.cs.yale.edu (*Figure 5.4*)

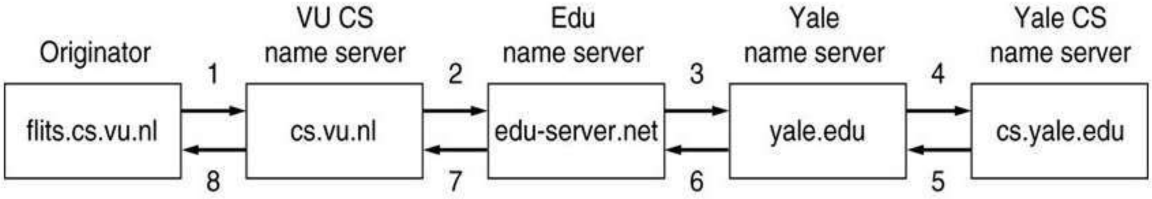


Figure 5.4 How a resolver looks up a remote name in eight steps

- Step 1: Resolver sends a query containing domain name sought the type and the class to local name server, cs.vu.nl.
- Step 2: Suppose local name server knows nothing about it, it asks few others nearby name servers. If none of them know, it sends a UDP packet to the server for edu-server.net.
- Step 3: This server knows nothing about Linda.cs.yale.edu or cs.yale.edu and so it forwards the request to the name server for yale.edu.
- Step 4: This one forwards the request to cs.yale.edu which must have authoritative resource records.
- Step 5 to 8: The resource record requested works its way back in steps 5-8 This query method is known as Recursive Query

3. When a query cannot be satisfied locally, the query fails but the name of the next server along the line to try is returned.

5.3 Electronic Mail

Short for electronic mail, e-mail or email is information stored on a computer that is exchanged between two users over telecommunications. More plainly, e-mail is a message that may contain text, files, images, or other attachments sent through a network to a specified individual or group of individuals.

The first e-mail was sent by Ray Tomlinson in 1971. Tomlinson sent the e-mail to himself as a test e-mail message, containing the text "something like QWERTYUIOP." However, despite sending the e-mail to himself, the e-mail message was still transmitted through ARPANET.

The first e-mail systems simply consisted of file transfer protocols, with the convention that the first line of each message (i.e., file) contained the recipient's address. As time went on, the limitations of this approach became more obvious.

Some of the complaints were as follows:

1. Sending a message to a group of people was inconvenient. Managers often need this facility to send memos to all their subordinates.
2. Messages had no internal structure, making computer processing difficult. For example, if a forwarded message was included in the body of another message, extracting the forwarded part from the received message was difficult.
3. The originator (sender) never knew if a message arrived or not.
4. If someone was planning to be away on business for several weeks and wanted all incoming e-mail to be handled by his secretary, this was not easy to arrange.
5. The user interface was poorly integrated with the transmission system requiring users first to edit a file, then leave the editor and invoke the file transfer program.
6. It was not possible to create and send messages containing a mixture of text, drawings, facsimile, and voice.

5.3.1 Architecture and Services

E-mail systems consist of two subsystems. They are:-

(1). User Agents, which allow people to read and send e-mail

(2). Message Transfer Agents, which move messages from source to destination

E-mail systems support 5 basic functions:-

a) ***Composition***: It refers to the process of creating messages and answers. Any text editor is used for body of the message. While the system itself can provide assistance with addressing and numerous header fields attached to each message.

b) ***Reporting***: It has to do with telling the originator what happened to the message that is, whether it was delivered, rejected (or) lost.

c) ***Transfer***: It refers to moving messages from originator to the recipient.

d) ***Displaying***: Incoming messages are to be displayed so that people can read their email.

e) ***Disposition***: It concerns what the recipient dose with the message after receiving it. Possibilities include throwing it away before reading (or) after reading, saving it and so on.

Most systems allow users to create mailboxes to store incoming e-mail. Commands are needed to create and destroy mailboxes, inspect the contents of mailboxes, insert and delete messages from mailboxes, and so on.

A key idea in e-mail systems is the distinction between the envelope and its contents. The envelope encapsulates the message. It contains all the information needed for transporting the message, such as the destination address, priority, and security level, all of which are distinct from the message itself. The message transport agents use the envelope for routing, just as the post office does.

The message inside the envelope consists of two parts: the header and the body. The header contains control information for the user agents. The body is entirely for the human recipient. Envelopes and messages are illustrated in Fig. 7-7.

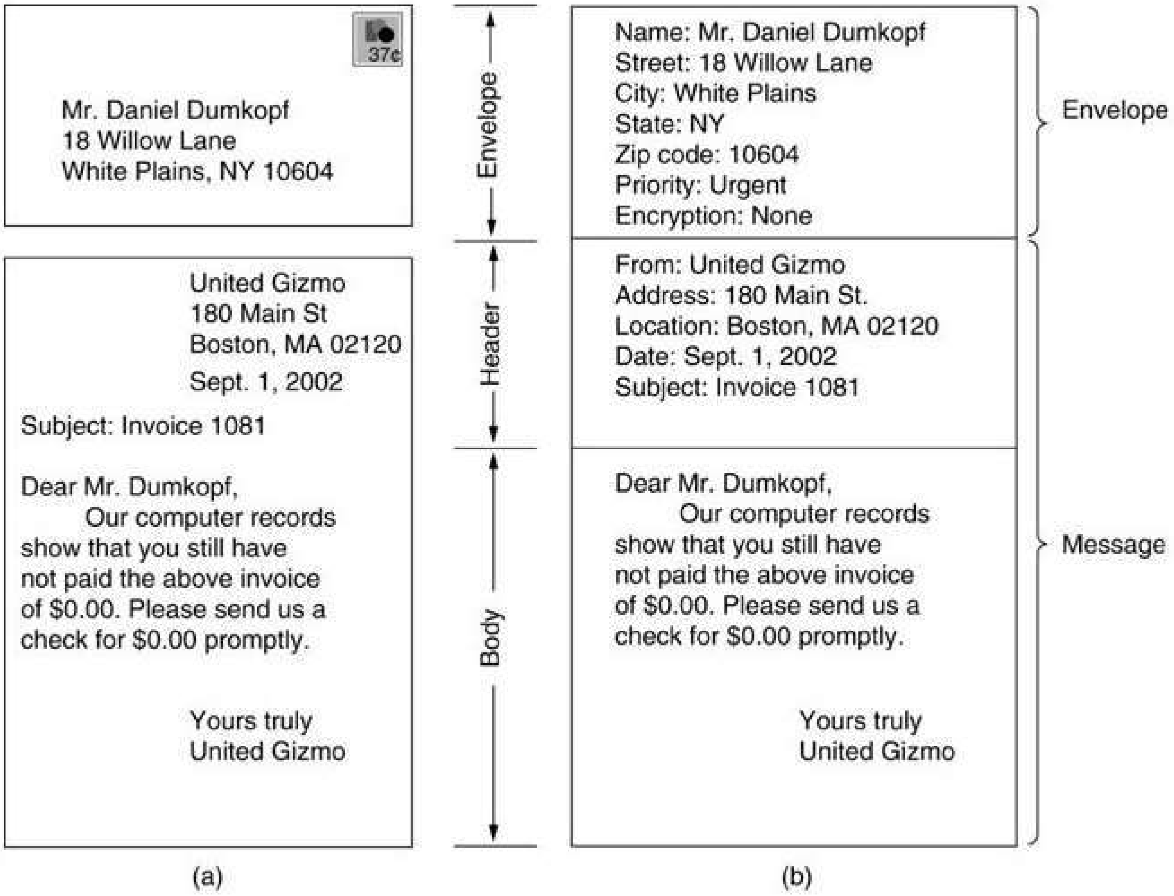


Figure 5.5 Envelopes and messages. (a) Paper mail. (b) Electronic mail.

5.3.2 The User Agent

A user agent is normally a program (sometimes called a mail reader) that accepts a variety of commands for composing, receiving, and replying to messages, as well as for manipulating mailboxes.

- **Sending E-Mail**

To send an e-mail message, a user must provide the message, the destination address, and possibly some other parameters. The message can be produced with a free-standing text editor, a word processing program, or possibly with a specialized text editor built into the user agent. The destination address must be in a format that the user agent can deal with. Many user agents expect addresses of the form user@dns-address.

- **Reading E-Mail**

When a user agent is started up, it looks at the user's mailbox for incoming e-mail before displaying anything on the screen. Then it may announce the number of messages in the mailbox or display a one-line summary of each one and wait for a command.

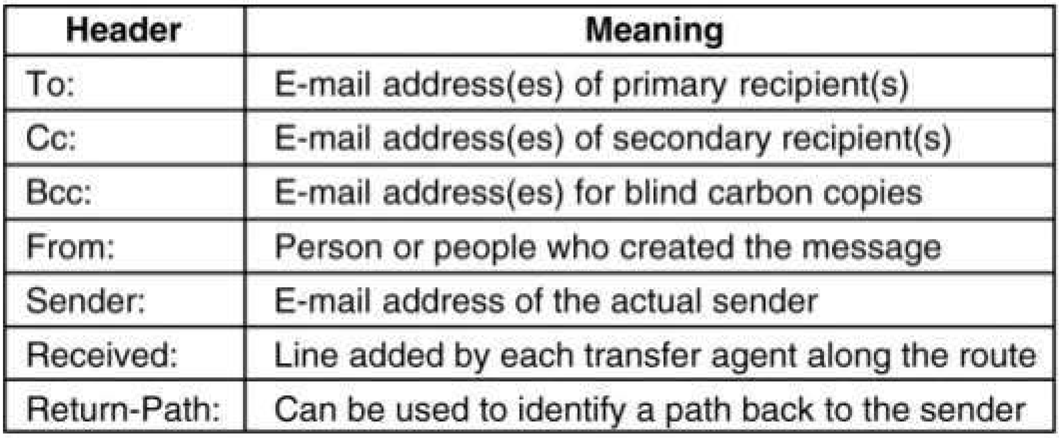
5.3.3 Message Formats

The format of the e-mail messages has two types. First, basic ASCII e-mail using RFC 822 and second is multimedia extensions to RFC 822.

- **RFC 822**

Messages consist of a primitive envelope (described in RFC 821), some number of header fields, a blank line, and then the message body. Each header field (logically) consists of a single line of ASCII text containing the field name, a colon, and, for most fields, a value. The principal header fields related to message transport are listed in Figure 5.6.

- ✓ ***To***: field gives the DNS address of the primary recipient. Having multiple recipients is also allowed.
- ✓ ***Cc***: field gives the addresses of any secondary recipients. In terms of delivery, there is no distinction between the primary and secondary recipients. The term Cc: (Carbon copy) is a bit dated, since computers do not use carbon paper, but it is well established.
- ✓ ***Bcc***: (Blind carbon copy) field is like the Cc: field, except that this line is deleted from all the copies sent to the primary and secondary recipients. This feature allows people to send copies to third parties without the primary and secondary.



Header	Meaning
To:	E-mail address(es) of primary recipient(s)
Cc:	E-mail address(es) of secondary recipient(s)
Bcc:	E-mail address(es) for blind carbon copies
From:	Person or people who created the message
Sender:	E-mail address of the actual sender
Received:	Line added by each transfer agent along the route
Return-Path:	Can be used to identify a path back to the sender

Figure 5.6 RFC 822 header fields related to message transport

- ✓ ***From: and Sender***:, tell who wrote and sent the message, respectively. These need not be the same. The From: field is required, but the Sender: field may be omitted if it is the same as the From: field. These fields are needed in case the message is undeliverable and must be returned to the sender.
- ✓ ***Received***: is added by each message transfer agent along the way. The line contains the agent's identity, the date and time the message was received, and other information that can be used for finding bugs in the routing system.

✓ ***Return-Path***: field is added by the final message transfer agent and was intended to tell how to get back to the sender.

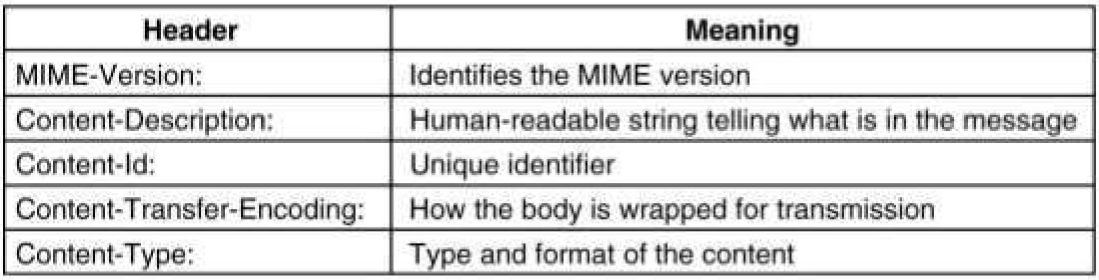
- **MIME — The Multipurpose Internet Mail Extensions**

RFC 822 specified the headers but left the content entirely up to the users. Nowadays, on the worldwide Internet, this approach is no longer adequate. The problems include sending and receiving.

1. Messages in languages with accents (e.g., French and German).
2. Messages in non-Latin alphabets (e.g., Hebrew and Russian).
3. Messages in languages without alphabets (e.g., Chinese and Japanese).
4. Messages not containing text at all (e.g., audio or images).

A solution was proposed in RFC 1341 called MIME (Multipurpose Internet Mail Extensions).

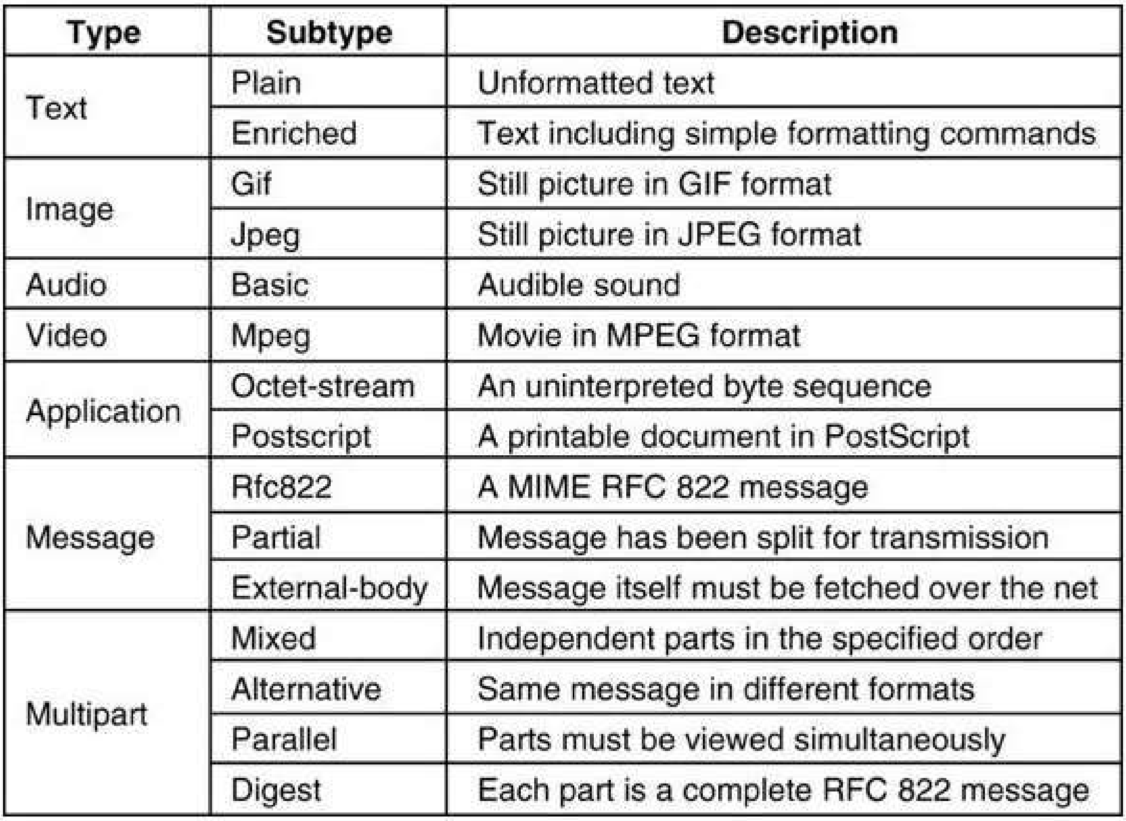
The basic idea of MIME is to continue to use the RFC 822 format, but to add structure to the message body and define encoding rules for non-ASCII messages. By not deviating from RFC 822, MIME messages can be sent using the existing mail programs and protocols. All that has to be changed are the sending and receiving programs, which users can do for themselves. MIME defines five new message headers, as shown in Figure 5.7.



Header	Meaning
MIME-Version:	Identifies the MIME version
Content-Description:	Human-readable string telling what is in the message
Content-Id:	Unique identifier
Content-Transfer-Encoding:	How the body is wrapped for transmission
Content-Type:	Type and format of the content

Figure 5.7 RFC 822 headers added by MIME

The subtype must be given explicitly in the header; no defaults are provided. The initial list of types and subtypes specified in RFC 2045 is given in Figure 5.8. Many new ones have been added since then, and additional entries are being added all the time as the need arises.



Type	Subtype	Description
Text	Plain	Unformatted text
	Enriched	Text including simple formatting commands
Image	Gif	Still picture in GIF format
	Jpeg	Still picture in JPEG format
Audio	Basic	Audible sound
Video	Mpeg	Movie in MPEG format
Application	Octet-stream	An uninterpreted byte sequence
	Postscript	A printable document in PostScript
Message	Rfc822	A MIME RFC 822 message
	Partial	Message has been split for transmission
	External-body	Message itself must be fetched over the net
Multipart	Mixed	Independent parts in the specified order
	Alternative	Same message in different formats
	Parallel	Parts must be viewed simultaneously
	Digest	Each part is a complete RFC 822 message

Figure 5.8The MIME types and subtypes defined in RFC 2045

5.3.4 Message Transfer

The message transfer system is concerned with relaying messages from the originator to the recipient. The simplest way to do this is to establish a transport connection from the source machine to the destination machine and then just transfer the message.

- ***SMTP—The Simple Mail Transfer Protocol***

SMTP is a simple ASCII protocol. After establishing the TCP connection to port 25, the sending machine, operating as the client, waits for the receiving machine, operating as the server, to talk first. The server starts by sending a line of text giving its identity and telling whether it is prepared to receive mail. If it is not, the client releases the connection and tries again later.

Even though the SMTP protocol is completely well defined, a few problems can still arise. One problem relates to message length. Some older implementations cannot handle messages exceeding 64 KB.

Another problem relates to timeouts. If the client and server have different timeouts, one of them may give up while the other is still busy, unexpectedly terminating the connection. Finally, in rare situations, infinite mailstorms can be triggered.

For example, if host 1 holds mailing list A and host 2 holds mailing list B and each list contains an entry for the other one, then a message sent to either list could generate a never-ending amount of e-mail traffic unless somebody checks for it.

5.3.5 Final Delivery

With the advent of people who access the Internet by calling their ISP over a modem, it breaks down.

- **POP3**

One solution is to have a message transfer agent on an ISP machine accept e-mail for its customers and store it in their mailboxes on an ISP machine. Since this agent can be on-line all the time, e-mail can be sent to it 24 hours a day.

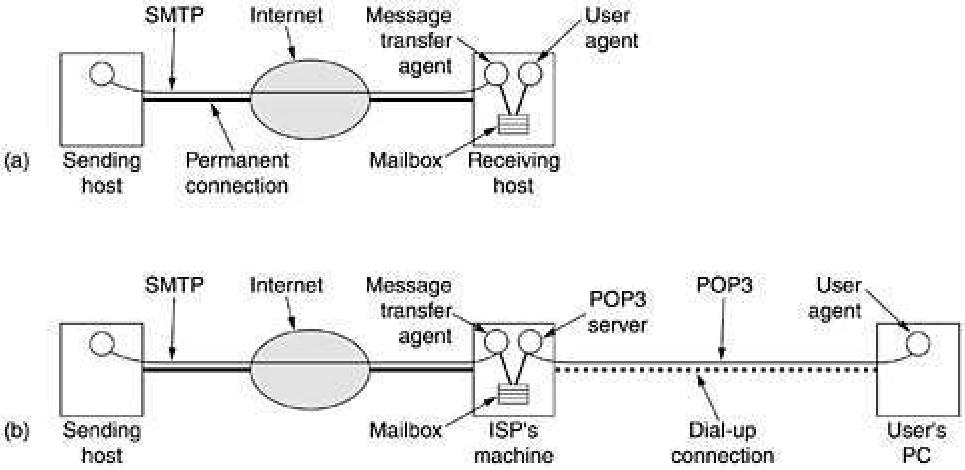


Figure 5.9(a) Sending and reading mail when the receiver has a permanent Internet connection and the user agent runs on the same machine as the message transfer agent. (b) Reading e-mail when the receiver has a dial-up connection to an ISP

POP3 begins when the user starts the mail reader. The mail reader calls up the ISP (unless there is already a connection) and establishes a TCP connection with the message transfer agent at port 110. Once the connection has been established, the POP3 protocol goes through three states in sequence:

1. Authorization - The authorization state deals with having the user log in.
2. Transactions - deals with the user collecting the e-mails and marking them for deletion from the mailbox.
3. Update - actually causes the e-mails to be deleted.

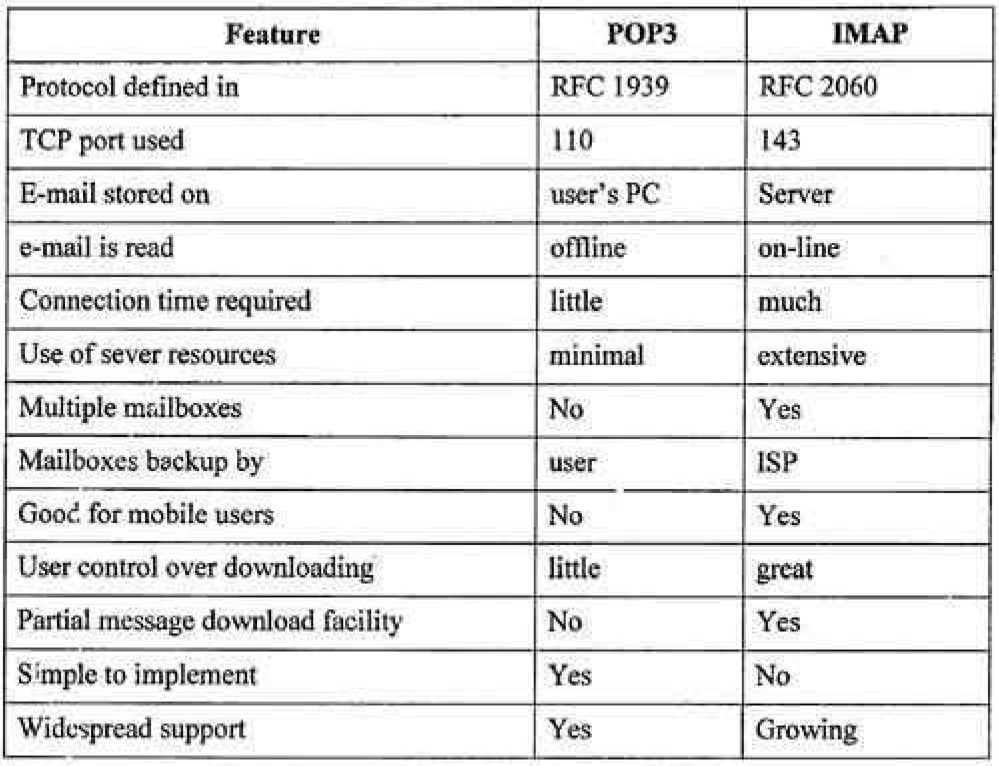
- **IMAP (Internet Message Access Protocol).**

POP3 normally downloads all stored messages at each contact, the result is that the user's e-mail quickly gets spread over multiple machines, more or less at random; some of them not even the user's.

This disadvantage gave rise to an alternative final delivery protocol, IMAP (Internet Message Access Protocol).

IMAP assumes that all the e-mail will remain on the server indefinitely in multiple mailboxes. IMAP provides extensive mechanisms for reading messages or even parts of messages, a feature useful when using a slow modem to read the text part of a multipart message with large audio and video attachments.

A comparison of POP3 and IMAP is given in Figure 5.10. It should be noted, however, that not every ISP supports both protocols and not every e-mail program supports both protocols. Thus, when choosing an e-mail program, it is important to find out which protocol(s) it supports and make sure the ISP supports at least one of them.



Feature	POP3	IMAP
Protocol defined in	RFC 1939	RFC 2060
TCP port used	110	143
E-mail stored on	user's PC	Server
e-mail is read	offline	on-line
Connection time required	little	much
Use of sever resources	minimal	extensive
Multiple mailboxes	No	Yes
Mailboxes backup by	user	ISP
Good for mobile users	No	Yes
User control over downloading	little	great
Partial message download facility	No	Yes
Simple to implement	Yes	No
Widespread support	Yes	Growing

Figure 5.10 A comparison of POP3 and IMAP.

The interesting part is how e-mail is delivered. Basically, when the user goes to the e-mail Web page, a form is presented in which the user is asked for a login name and password. When the user clicks on Sign In, the login name and password are sent to the server, which then validates them. If the login is successful, the server finds the user's mailbox and builds a listing, only formatted as a Web page in HTML. The Web page is then sent to the browser for display. Many of the items on the page are clickable, so messages can be read, deleted, and so on.

5.4 World Wide Web (WWW)

5.4.1 Introduction

The World Wide Web is an architectural framework for accessing linked documents spread out over millions of machines all over the Internet. World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet. These websites contain text pages, digital images, audios, videos, etc. Users can access the content of these sites from any part of the world over the internet using their devices such as computers, laptops, cell phones, etc. The WWW, along with internet, enables the retrieval and display of text and media to your device.

The Web (also known as WWW) began in 1989 at CERN, the European center for nuclear research. The initial proposal for a web of linked documents came from CERN physicist Tim Berners-Lee in March 1989. The first (text-based) prototype was operational 18 months later. In December 1991, a public demonstration was given at the Hypertext '91 conference in San Antonio, Texas.

In 1994, CERN and M.I.T. signed an agreement setting up the World Wide Web Consortium (sometimes abbreviated as W3C), an organization devoted to further developing the Web, standardizing protocols, and encouraging interoperability between sites. Berners-Lee became the director. Since then, several hundred universities and companies have joined the consortium. Although there are now more books about the Web than you can shake a stick at, the best place to get up-to-date information about the Web is (naturally) on the Web itself. The consortium's home page is at www.w3.org. Interested readers are referred there for links to pages covering all of the consortium's numerous documents and activities.

5.4.2 Architectural Overview

From the users' point of view, the Web consists of a vast, worldwide collection of documents or Web pages, often just called pages for short. Each page may contain links to other pages anywhere in the world. Users can follow a link by clicking on it, which then takes them to the page pointed to. This process can be repeated indefinitely. The idea of having one page point to another, now called hypertext, was invented by a visionary M.I.T. professor of electrical engineering, Vannevar Bush, in 1945, long before the Internet was invented.

- **Browser**

Pages are viewed with a program called a *browser*, of which Internet Explorer and Netscape Navigator are two popular ones. The browser fetches the page requested, interprets the text and formatting commands on it, and displays the page, properly formatted, on the screen.

- **Hyperlinks**

Strings of text that are links to other pages, called *hyperlinks*, are often highlighted, by underlining, displaying them in a special color, or both. To follow a link, the user places the mouse cursor on the highlighted area, which causes the cursor to change, and clicks on it.

- **Uniform Resource Locator**

A web page is given an online address called a *Uniform Resource Locator* (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., www.facebook.com, www.google.com, etc. So, the World Wide Web is like a huge electronic book whose pages are stored on multiple servers across the world.

- **Webservers**

Small websites store all of their Web Pages on a single server, but big websites or organizations place their Web Pages on different servers in different countries so that when users of a country search their site, they could get the information quickly from the nearest server.

So, the web provides a communication platform for users to retrieve and exchange information over the internet. Unlike a book, where we move from one page to another in a sequence, on World Wide Web we follow a web of hypertext links to visit a web page and from that web page to move to other web pages. You need a browser, which is installed on your computer, to access the Web.

- **Web Page Working Model**

The basic model of how the Web works is shown in Fig. 7-19. Here the browser is displaying a Web page on the client machine. When the user clicks on a line of text that is linked to a page on the abcd.com server, the browser follows the hyperlink by sending a message to the abcd.com server asking it for the page. When the page arrives, it is displayed. If this page contains a hyperlink to a page on the xyz.com server that is clicked on, the browser then sends a request to that machine for the page, and so on indefinitely.

a). Client Side

When a user clicks on a hyperlink, the browser carries out a series of steps in order to fetch the page pointed to. Let us trace the steps that occur when this link is selected.

1. The browser determines the URL (by seeing what was selected).
2. The browser asks DNS for the IP address of www.itu.org.
3. DNS replies with 156.106.192.32.
4. The browser makes a TCP connection to port 80 on 156.106.192.32.
5. It then sends over a request asking for file /home/index.html.
6. The www.itu.org server sends the file /home/index.html.
7. The TCP connection is released.
8. The browser displays all the text in /home/index.html.
9. The browser fetches and displays all images in this file.

b). Server Side

Now let us take a look at the server side. That server, like a real Web server, is given the name of a file to look up and return. In both cases, the steps that the server performs in its main loop are:

1. Accept a TCP connection from a client (a browser).
2. Get the name of the file requested.
3. Get the file (from disk).
4. Return the file to the client.
5. Release the TCP connection.

Modern Web servers do more than just accept file names and return files. In fact, the actual processing of each request can get quite complicated. For this reason, in many servers each processing module performs a series of steps. The front end passes each incoming request to the first available module, which then carries it out using some subset of the following steps, depending on which ones are needed for that particular request.

1. Resolve the name of the Web page requested.
2. Authenticate the client.
3. Perform access control on the client.
4. Perform access control on the Web page.
5. Check the cache.
6. Fetch the requested page from disk.
7. Determine the MIME type to include in the response.
8. Take care of miscellaneous odds and ends.
9. Return the reply to the client.
10. Make an entry in the server log.

c). URLs—Uniform Resource Locators

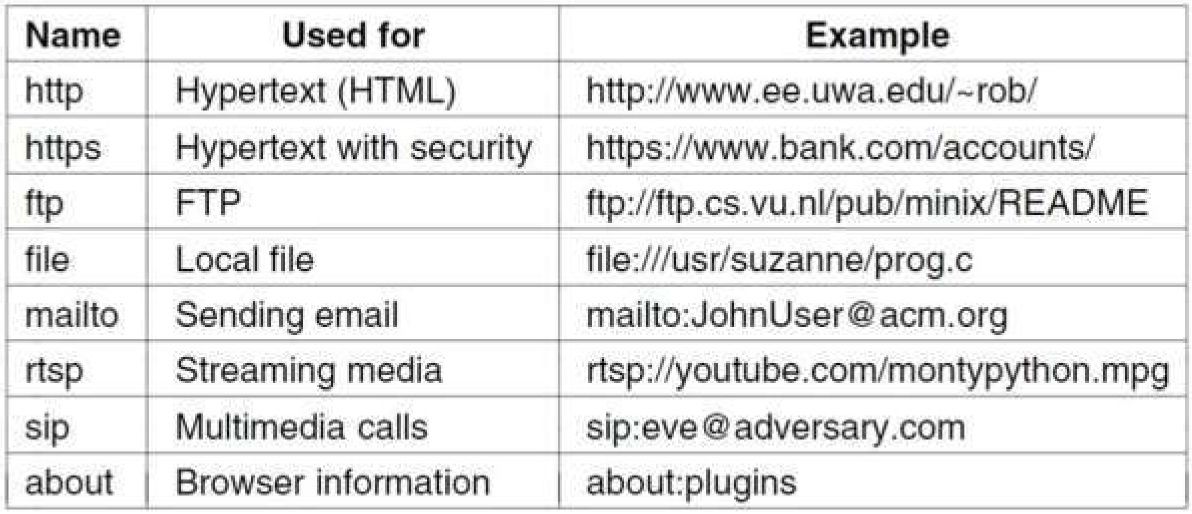
We have repeatedly said that Web pages may contain pointers to other Web pages. Now it is time to see in a bit more detail how these pointers are implemented. When the Web was first created, it was immediately apparent that having one page point to another Web page required mechanisms for naming and locating pages. In particular, three questions had to be answered before a selected page could be displayed:

1. What is the page called?
2. Where is the page located?
3. How can the page be accessed?

If every page were somehow assigned a unique name, there would not be any ambiguity in identifying pages. Nevertheless, the problem would not be solved. Consider a parallel between people and pages. In the United States, almost everyone has a social security number, which is a unique identifier, as no two people are supposed to have the same one. Nevertheless, if you are armed only with a social security number, there is no way to find the owner's address, and certainly no way to tell whether you should write to the person in English, Spanish, or Chinese. The Web has basically the same problems.

The solution chosen identifies pages in a way that solves all three problems at once. Each page is assigned a URL (Uniform Resource Locator) that effectively serves as the page's worldwide name. URLs have three parts: the protocol (also known as the scheme), the DNS name of the machine on which the page is located, and a local name uniquely indicating the specific page (usually just a file name on the machine where it resides). As an example, the Web site for the author's department contains several videos about the university and the city of Amsterdam. The URL for the video page is http://www.cs.vu.nl/video/index-en.html.

This URL consists of three parts: the protocol (http), the DNS name of the host (www.cs.vu.nl), and the file name (video/index-en.html), with certain punctuation separating the pieces. The file name is a path relative to the default Web directory at cs.vu.nl. Slightly simplified forms of the more common ones are listed in Figure 5.11.



Name	Used for	Example
http	Hypertext (HTML)	http://www.ee.uwa.edu/~rob/
https	Hypertext with security	https://www.bank.com/accounts/
ftp	FTP	ftp://ftp.cs.vu.nl/pub/minix/README
file	Local file	file:///usr/suzanne/prog.c
mailto	Sending email	mailto:JohnUser@acm.org
rtsp	Streaming media	rtsp://youtube.com/montypython.mpg
sip	Multimedia calls	sip:eve@adversary.com
about	Browser information	about:plugins

Figure 5.11 Common URL

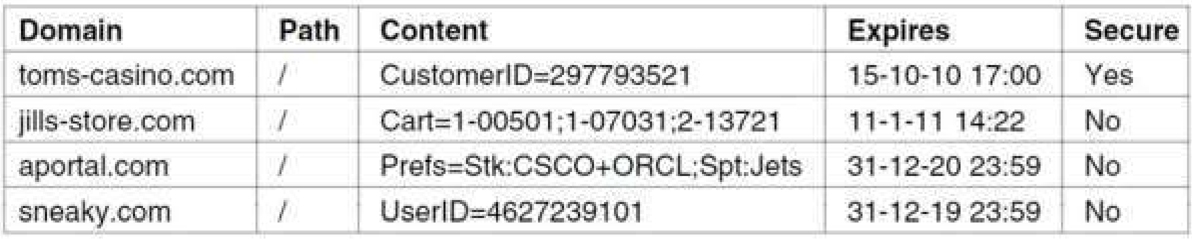
d). Statelessness and Cookies

The Web is basically stateless. There is no concept of a login session. The browser sends a request to a server and gets back a file. Then the server forgets that it has ever seen that particular client.

Netscape devised a much-criticized technique called cookies. The name derives from ancient programmer slang in which a program calls a procedure and gets something back that it may need to present later to get some work done. In this sense, a UNIX file descriptor or a Windows object handle can be considered as a cookie. Cookies were later formalized in RFC 2109.

When a client requests a Web page, the server can supply additional information along with the requested page. This information may include a cookie, which is a small (at most 4 KB) file (or string). Browsers store offered cookies in a cookie directory on the client's hard disk unless the user has disabled cookies. Cookies are just files or strings, not executable programs. In principle, a cookie could contain a virus, but since cookies are treated as data, there is no official way for the virus to actually run and do damage. However, it is always possible for some hacker to exploit a browser bug to cause activation.

A cookie may contain up to five fields, as shown in Fig. 7-25. The Domain tells where the cookie came from. Browsers are supposed to check that servers are not lying about their domain. Each domain may store no more than 20 cookies per client. The Path is a path in the server's directory structure that identifies which parts of the server's file tree may use the cookie. It is often /, which means the whole tree.



Domain	Path	Content	Expires	Secure
toms-casino.com	/	CustomerID=297793521	15-10-10 17:00	Yes
jills-store.com	/	Cart=1-00501;1-07031;2-13721	11-1-11 14:22	No
aportal.com	/	Prefs=Stk:CSCO+ORCL;Spt:Jets	31-12-20 23:59	No
sneaky.com	/	UserID=4627239101	31-12-19 23:59	No

Figure 5.12 Examples of cookies

5.4.3 Static Web Documents

The basis of the Web is transferring Web pages from server to client. In the simplest form, Web pages are static, that is, are just files sitting on some server waiting to be retrieved. In this context, even a video is a static Web page because it is just a file. Here, we will discuss about the languages and concepts used to create static web pages.

- **HTML – The HyperText Markup Language**

HTML allows users to produce Web pages that include text, graphics, and pointers to other Web pages. HTML is a markup language, a language for describing how documents are to be formatted. The term "markup" comes from the old days when copyeditors actually marked up documents to tell the printer—in those days, a human being—which fonts to use, and so on. Markup languages thus contain explicit commands for formatting.

A Web page consists of a head and a body, each enclosed by <html> and </html> tags (formatting commands), although most browsers do not complain if these tags are missing. The head is bracketed by the <head> and </head> tags and the body is bracketed by the <body> and </body> tags. The strings inside the tags are called directives. Most HTML tags have this format, that is they use, <something> to mark the beginning of something and </something> to mark its end.

- **Forms**

HTML 1.0 was basically one-way. the inclusion of forms starting in HTML 2.0. Forms contain boxes or buttons that allow users to fill in information or make choices and then send the information back to the page's owner. They use the <input> tag for this purpose. It has a variety of parameters for determining the size, nature, and usage of the box displayed. The most common forms are blank fields for accepting user text, boxes that can be checked, active maps, and submit buttons.

- **XML and XSL**

The W3C has developed an enhancement to HTML to allow Web pages to be structured for automated processing. Two new languages have been developed for this purpose. First, XML (eXtensible Markup Language) describes Web content in a structured way and second, XSL (eXtensible Style Language) describes the formatting independently of the content.

XML can be used for purposes other than describing Web pages. One growing use of it is as a language for communication between application programs. In particular, SOAP (Simple Object Access Protocol) is a way for performing RPCs between applications in a language- and system-independent way. The client constructs the request as an XML message and sends it to the server, using the HTTP protocol. The server sends back a reply as an XML formatted message. In this way, applications on heterogeneous platforms can communicate.

5.4.4 Dynamic Web Documents

In early days, the client sends a file name to the server, which then returns the file. In the early days of the Web, all content was, in fact, static like this (just files). However, in recent years, more and more content has become dynamic, that is, generated on demand, rather than stored on disk. Content generation can take place either on the server side or on the client side. Let us now examine each of these cases in turn.

- **Server-Side Dynamic Web Page Generation**

The traditional way to handle forms and other interactive Web pages is a system called the CGI (Common Gateway Interface). It is a standardized interface to allow Web servers to talk to back-end programs and scripts that can accept input (e.g., from forms) and generate HTML pages in response. Usually, these back-ends are scripts written in the Perl scripting language.

CGI scripts are not the only way to generate dynamic content on the server side. Another common way is to embed little scripts inside HTML pages and have them be executed by the server itself to generate the page. A popular language for writing these scripts is PHP (PHP: Hypertext Preprocessor).

Already we have seen, two different ways to generate dynamic HTML pages: CGI scripts and embedded PHP. There is also a third technique, called JSP (JavaServer Pages), which is similar to PHP, except that the dynamic part is written in the Java programming language instead of in PHP. Pages using this technique have the file extension jsp. A fourth technique, ASP (Active Server Pages), is Microsoft's version of PHP and JavaServer Pages.

The collection of technologies for generating content on the fly is sometimes called dynamic HTML.

- **Client-Side Dynamic Web Page Generation**

It is necessary to have scripts embedded in HTML pages that are executed on the client machine rather than the server machine. Starting with HTML 4.0, such scripts are permitted using the tag <script>. The most popular scripting language for the client side is JavaScript, so we will now take a quick look at it.

JavaScript is a full-blown programming language, with all the power of C or Java. It has variables, strings, arrays, objects, functions, and all the usual control structures. It also has a large number of facilities specific for Web pages, including the ability to manage windows and frames, set and get cookies, deal with forms, and handle hyperlinks.

JavaScript is not the only way to make Web pages highly interactive. Another popular method is through the use of applets. These are small Java programs that have been compiled into machine instructions for a virtual computer called the JVM (Java Virtual Machine).

Applets can be embedded in HTML pages (between <applet> and </applet>) and interpreted by JVM-capable browsers.

5.4.5 Performance Enhancements

The popularity of the Web has almost been its undoing. Servers, routers, and lines are frequently overloaded. As a consequence of these endless delays, researchers have developed various techniques for improving performance. The techniques are : *caching, server replication,* and *content delivery networks*.

- **Caching**

Caching (pronounced "cashing") is the process of storing data in a cache memory. A cache is a temporary storage area. For example, the files you automatically request by looking at a Web page are stored on your hard disk in a cache subdirectory under the directory for your browser. When you return to a page you've recently looked at, the browser can get those files from the cache rather than the original server, saving you time and saving the network the burden of additional traffic.

The usual procedure is for some process, called a **proxy**, to maintain the cache. To use caching, a browser can be configured to make all page requests to a proxy instead of to the page's real server. If the proxy has the page, it returns the page immediately. If not, it fetches the page from the server, adds it to the cache for future use, and returns it to the client that requested it.

The main task of the caching is who should do the caching. A scheme involving multiple caches tried in sequence is called hierarchical caching. In this the content is searched in the order like local PC, LAN proxy, ISP proxy or from server.

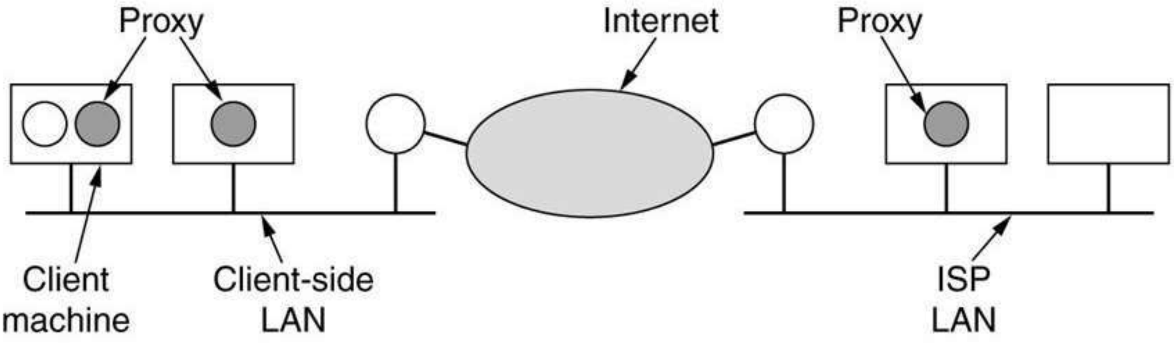


Figure 5.13 Hierarchical caching with three proxies

The Second key issue is how long the cache can be kept. It is depending on the staleness of the content. The next issue is what cached content should be removed from the cache memory if cache is not available. Many algorithms are proposed to replace the cache by researchers.

- **Server Replication**

Caching is a client-side technique for improving performance, but server-side techniques also exist. The most common approach that servers take to improve performance is to replicate their contents at multiple, widely-separated locations. This technique is sometimes called mirroring.

Mirrored sites are generally completely static. The company decides where it wants to place the mirrors, arranges for a server in each region, and puts more or less the full content at each location (possibly omitting the snow blowers from the Miami site and the beach blankets from the Anchorage site). The choice of sites generally remains stable for months or years.

- **Content Delivery Networks**

CDN is short for content delivery network. A content delivery network (CDN) is a system of distributed servers (network) that deliver pages and other web content to a user, based on the geographic locations of the user, the origin of the webpage and the content delivery server.

This service is effective in speeding the delivery of content of websites with high traffic and websites that have global reach. The closer the CDN server is to the user geographically, the faster the content will be delivered to the user. CDNs also provide protection from large surges in traffic.

5.5 Multimedia

Multimedia is an interactive media and provides multiple ways to represent information to the user in a powerful manner. It provides an interaction between users and digital information. It is a medium of communication with the use of a combination of text, audio, video, graphics and animation.

- Multi − it means more than one
- Medium − it is singular and it means intermediary or mean
- Media − it is plural and it means conveying the information

5.5.1 Components of Multimedia

- **Text**

All multimedia productions contain some amount of text. The text can have various types of fonts and sizes to suit the profession presentation of the multimedia software.

- **Graphics**

Graphics make the multimedia application attractive. In many cases people do not like reading large amount of textual matter on the screen. Therefore, graphics are used more often than text to explain a concept, present background information etc. There are two types of Graphics:

- ✓ Bitmap images- Bitmap images are real images that can be captured from devices such as digital cameras or scanners. Generally, bitmap images are not editable. Bitmap images require a large amount of memory.
- ✓ Vector Graphics- Vector graphics are drawn on the computer and only require a small amount of memory. These graphics are editable.

- **Audio**

A multimedia application may require the use of speech, music and sound effects. These are called audio or sound element of multimedia. Speech is also a perfect way for teaching. Audio are of analog and digital types. Analog audio or sound refers to the original sound signal. Computer stores the sound in digital form. Therefore, the sound used in multimedia application is digital audio.

- **Video**

The term video refers to the moving picture, accompanied by sound such as a picture in television. Video element of multimedia application gives a lot of information in small duration of time. Digital video is useful in multimedia application for showing real life objects. Video have highest performance demand on the computer memory and on the bandwidth if placed on the internet. Digital video files can be stored like any other files in the computer and the quality of the video can still be maintained. The digital video files can be transferred within a computer network. The digital video clips can be edited easily.

- **Animation**

Animation is a process of making a static image look like it is moving. An animation is just a continuous series of still images that are displayed in a sequence. The animation can be used effectively for attracting attention. Animation also makes a presentation light and attractive. Animation is very popular in multimedia application

5.5.2 Multimedia Hardware

Most of the computers now-a-days come equipped with the hardware components required to develop/view multimedia applications. Following are the various categories in which we can define the various types of hardwares required for multimedia application

- ✓ ***Input Devices*** - Following are the various types of input devices which are used in multimedia systems.
- ✓ ***Keyboard***- Most common and very popular input device is keyboard. The keyboard helps in inputting the data to the computer. The layout of the keyboard is like that of traditional typewriter, although there are some additional keys provided for performing some additional functions. Keyboards are of two sizes 84 keys or 101/102 keys, but now 104 keys or 108 keys keyboard is also available for Windows and Internet.
- ✓ ***Scanner*** - Scanner is an input device, which works more like a photocopy machine. It is used when some information is available on a paper and it is to be transferred to the hard disc of the computer for further manipulation. Scanner captures images from the source which are then converted into the digital form that can be stored on the disc. These images can be edited before they are printed.
- ✓ ***Bar Code Readers*** - Bar Code Reader is a device used for reading bar coded data (data in form of light and dark lines). Bar coded data is generally used in labelling goods, numbering the books, etc. It may be a hand-held scanner or may be

embedded in a stationary scanner. Bar Code Reader scans a bar code image, converts it into an alphanumeric value, which is then fed to the computer to which bar code reader is connected.

- ✓ ***Optical Mark Reader (OMR)*** - OMR is a special type of optical scanner used to recognize the type of mark made by pen or pencil. It is used where one out of a few alternatives is to be selected and marked. It is specially used for checking the answer sheets of examinations having multiple choice questions.
- ✓ ***Voice Systems*** - Following are the various types of input devices which are used in multimedia systems.
  - ▪ Microphone- Microphone is an input device to input sound that is then stored in digital form. The microphone is used for various applications like adding sound to a multimedia presentation or for mixing music.
  - ▪ Speaker- Speaker is an output device to produce sound which is stored in digital form. The speaker is used for various applications like adding sound to a multimedia presentation or for movies displays etc.
- ✓ ***Digital Camera*** - Digital camera is an input device to input images that is then stored in digital form. The digital camera is used for various applications like adding images to a multimedia presentation or for personal purposes.
- ✓ ***Digital Video Camera*** - Digital Video camera is an input device to input images/video that is then stored in digital form. The digital video camera is used for various applications like adding videos to a multimedia presentation or for personal purposes.

5.5.3 Introduction to Digital Audio

An audio (sound) wave is a one-dimensional acoustic (pressure) wave. When an acoustic wave enters the ear, the eardrum vibrates, causing the tiny bones of the inner ear to vibrate along with it, sending nerve pulses to the brain. These pulses are perceived as sound by the listener. In a similar way, when an acoustic wave strikes a microphone, the microphone generates an electrical signal, representing the sound amplitude as a function of time. The representation, processing, storage, and transmission of such audio signals are a major part of the study of multimedia systems.

The frequency range of the human ear runs from 20 Hz to 20,000 Hz. Some animals, notably dogs, can hear higher frequencies. The ear hears logarithmically, so the ratio of two sounds with power A and B is conventionally expressed in dB (decibels).

If we define the lower limit of audibility (a pressure of about 0.0003 dyne/cm2) for a 1-kHz sine wave as 0 dB, an ordinary conversation is about 50 dB and the pain threshold is about 120 dB, a dynamic range of a factor of 1 million.

Audio waves can be converted to digital form by an ADC (Analog Digital Converter). An ADC takes an electrical voltage as input and generates a binary number as output.

5.5.4 Audio Compression

CD-quality audio requires a transmission bandwidth of 1.411 Mbps. Clearly, substantial compression is needed to make transmission over the Internet practical. The most popular one is MPEG audio, which has three layers (variants), of which MP3 (MPEG audio layer 3) is the most powerful. MP3 belongs to the audio portion of the MPEG video compression standard.

Audio compression can be done in one of two ways. In ***waveform coding*** the signal is transformed mathematically by a Fourier transform into its frequency components. The amplitude of each component is then encoded in a minimal way. The goal is to reproduce the waveform accurately at the other end in as few bits as possible.

The other way, ***perceptual coding***, exploits certain flaws in the human auditory system to encode a signal in such a way that it sounds the same to a human listener, even if it looks quite different on an oscilloscope. Perceptual coding is based on the science of psychoacoustics—how people perceive sound. MP3 is based on perceptual coding.

The key property of perceptual coding is that some sounds can ***mask*** other sounds. The frequency masking is the ability of a loud sound in one frequency band to hide a softer sound in another frequency band that would have been audible in the absence of the loud sound.

5.5.5 Streaming Audio

Streaming audio is listening to sound over the Internet. This is also called music on demand. The Internet is full of music Web sites, many of which list song titles that users can click on to play the songs. Some of these are free sites (e.g., new bands looking for publicity); others require payment in return for music, although these often offer some free samples as well (e.g., the first 15 seconds of a song).

The media server uses RTSP (Real Time Streaming Protocol), as indicated by the scheme name RTSP. It is described in RFC 2326.

The media player has four major jobs to do:

1. Manage the user interface.
2. Handle transmission errors.
3. Decompress the music.
4. Eliminate jitter.

5.5.6 Internet Radio

Once it became possible to stream audio over the Internet, commercial radio stations got the idea of broadcasting their content over the Internet as well as over the air. Not so long after that, college radio stations started putting their signal out over the Internet. Then college students started their own radio stations. With current technology, virtually anyone can start a radio station. The whole area of Internet radio is very new and in a state of flux, but it is worth saying a little bit about. There are two general approaches to Internet radio.

1. In the first one, the programs are prerecorded and stored on disk. Listeners can connect to the radio station's archives and pull up any program and download it

for listening. The advantages of this approach are that it is easy to do, all the techniques we have discussed work here too, and listeners can pick and choose among all the programs in the archive.

2. The other approach is to broadcast live over the Internet. Some stations broadcast over the air and over the Internet simultaneously, but there are increasingly many radio stations that are Internet only. Some of the techniques that are applicable to streaming audio are also applicable to live Internet radio, but there are also some key differences.

5.5.7 Voice over IP

Voice over Internet Protocol (VoIP), also called IP telephony, is a method and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The terms Internet telephony, broadband telephony, and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public Internet, rather than via the public switched telephone network (PSTN), also known as plain old telephone service (POTS).

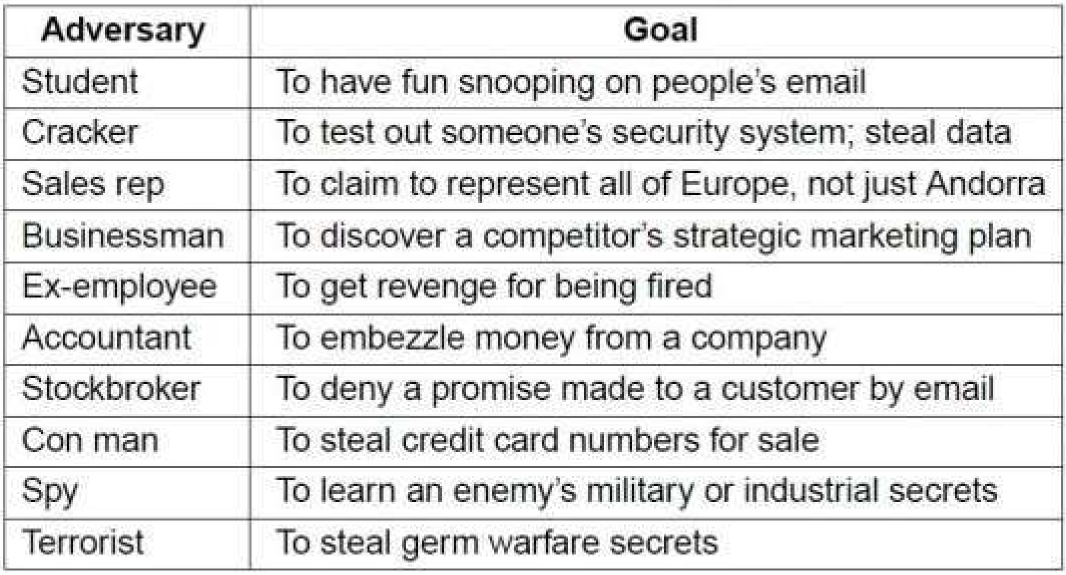
The steps and principles involved in originating VoIP telephone calls are similar to traditional digital telephony and involve signaling, channel setup, digitization of the analog voice signals, and encoding. Instead of being transmitted over a circuit-switched network, the digital information is packetized and transmission occurs as IP packets over a packet-switched network. They transport media streams using special media delivery protocols that encode audio and video with audio codecs and video codecs. Various codecs exist that optimize the media stream based on application requirements and network bandwidth; some implementations rely on narrowband and compressed speech, while others support high-fidelity stereo codecs.

The most widely speech coding standards in VoIP are based on the linear predictive coding (LPC) and modified discrete cosine transform (MDCT) compression methods. Popular codecs include the MDCT-based AAC-LD (used in FaceTime), the LPC/MDCT-based Opus (used in WhatsApp), the LPC-based SILK (used in Skype), μ-law and A-law versions of G.711, G.722, and an open source voice codec known as iLBC, a codec that uses only 8 kbit/s each way called G.729.

5.6 Network Security

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system. An example of network security is an antivirus system.

Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. A few of the most common perpetrators are listed in Figure 5.14.



Adversary	Goal
Student	To have fun snooping on people's email
Cracker	To test out someone's security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor's strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by email
Con man	To steal credit card numbers for sale
Spy	To learn an enemy's military or industrial secrets
Terrorist	To steal germ warfare secrets

Figure 5.14 Some people who cause security problems

5.6.1 Security Services

The classification of security services are as follows:

- ***Confidentiality***: Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.
- ***Authentication***: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
- ***Integrity***: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
- ***Non repudiation***: Requires that neither the sender nor the receiver of a message be able to deny the transmission.
- ***Access control***: Requires that access to information resources may be controlled by or the target system.
- ***Availability***: Requires that computer system assets be available to authorized parties when needed.

Network Security cannot be done in one single place. Every layer has something to contribute.

- ✓ In the physical layer, wiretapping can be foiled by enclosing transmission lines in sealed tubes containing gas at high pressure. Any attempt to drill into a tube will release some gas, reducing the pressure and triggering an alarm. Some military systems use this technique.
- ✓ In the data link layer, packets on a point-to-point line can be encrypted as they leave one machine and decrypted as they enter another.

- ✓ In the network layer, firewalls can be installed to keep good packets and bad packets out. IP security also functions in this layer.
- ✓ In the transport layer, entire connections can be encrypted, end to end, that is, process to process. For maximum security, end-to-end security is required.
- ✓ Finally, issues such as user authentication and nonrepudiation can only be handled in the application layer.

Since security does not fit neatly into any layer. Except for physical layer security, nearly all security is based on cryptographic principles.

5.6.2 Cryptography

- ***Definition of 'Cryptography'***

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

It is essential to make a distinction between ciphers and codes

- ***Cipher*** : cipher is a character-for-character or bit-for-bit transformation, without regard to the linguistic structure of the message.
- ***Code*** : a code replaces one word with another word or symbol.

The most successful code ever devised was used by the U.S. armed forces during World War II in the Pacific.

- ***Introduction to Cryptography***

Historically, four groups of people have used and contributed to the art of cryptography: the Military, the diplomatic corps, diarists, and lovers.

Of these, the military has had the most important role and has shaped the field over the centuries. Within military organizations, the messages to be encrypted have traditionally been given to poorly-paid, low-level code clerks for encryption and transmission. These conflicting requirements have given rise to the model of Figure 5.15.

- ✓ The messages to be encrypted, known as the ***plaintext***, are transformed by a function that is parameterized by a *key*.
- ✓ The output of the encryption process, known as the ***ciphertext***, is then transmitted, often by messenger or radio.
- ✓ The ***key*** consists of a (relatively) short string that selects one of many potential encryptions.

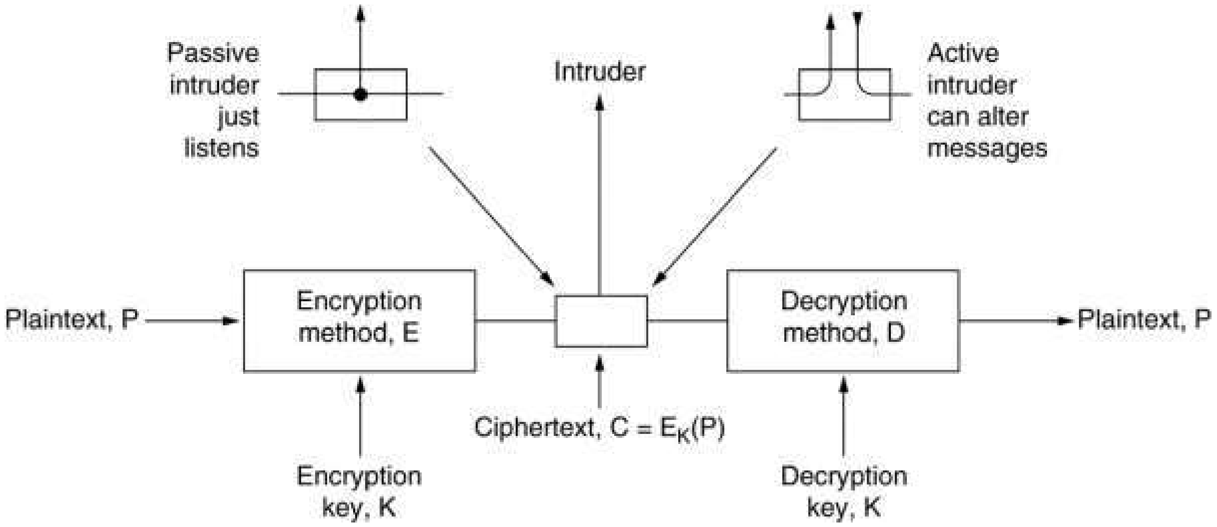


Figure 5.15 The encryption model (for a symmetric-key cipher)

We assume that the enemy, or intruder, hears and accurately copies down the complete ciphertext. However, unlike the intended recipient, the does not know what the decryption key is and so cannot decrypt the ciphertext easily. Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder).

- ✓ The art of breaking ciphers, called ***cryptanalysis***, and the art devising them (cryptography) is collectively known as ***cryptology***.

- ***Relationship between plaintext, ciphertext, and keys***.

The relationship between plaintext, ciphertext, and keys is shown in Figure 5.16. We will use *C = EK(P)* to mean that the encryption of the plaintext P using key K gives the ciphertext C. Similarly, *P = DK(C)* represents the decryption of C to get the plaintext again. $D_K(E_K(P)) =$ P.

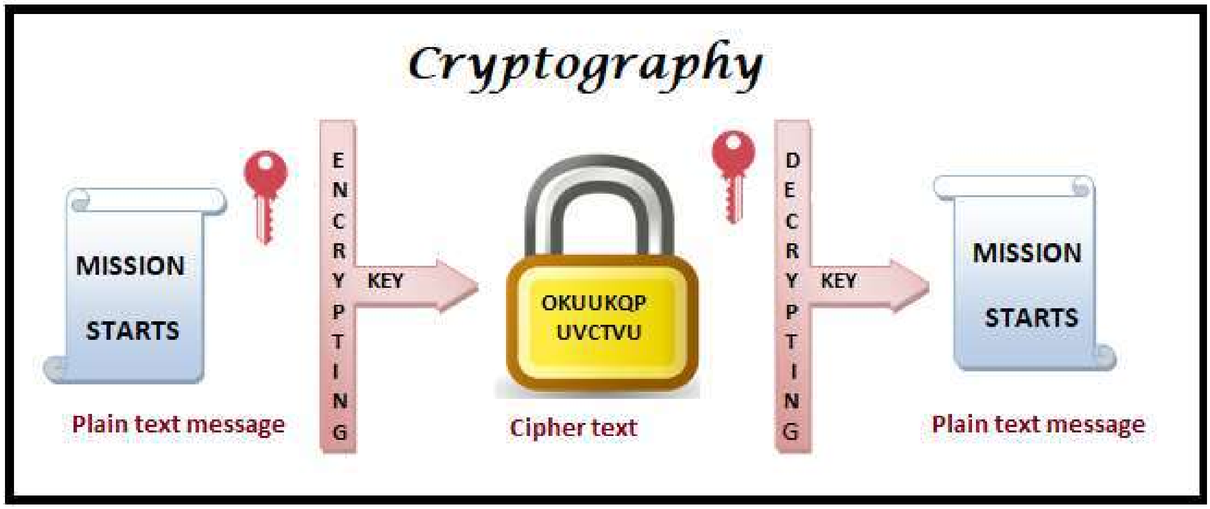


Figure 5.16 Relationship between plaintext, ciphertext, and keys.

Secrecy lies exclusively in the keys is called Kerckhoff's principle, named after the Flemish military cryptographer Auguste Kerckhoff who first stated it in 1883 (Kerckhoff, 1883).

Kerckhoff's principle: All algorithms must be public; only the keys are secret. Trying to keep the algorithm secret is known in the trade as security by ***obscurity***. The longer the key, the higher the work factor the cryptanalyst has to deal with.

From the cryptanalyst's point of view, the cryptanalysis problem has three principal variations.

- ✓ When he has a quantity of ciphertext and no plaintext, he is confronted with the ***ciphertext-only problem***. The cryptograms that appear in the puzzle section of newspapers pose this kind of problem.
- ✓ When the cryptanalyst has some matched ciphertext and plaintext, the problem is called the ***known plaintext problem***.
- ✓ Finally, when the cryptanalyst has the ability to encrypt pieces of plaintext of his own choosing, we have the ***chosen plaintext problem***.

Newspaper cryptograms could be broken trivially if the cryptanalyst were allowed to ask such questions as: What is the encryption of ABCDEFGHIJKL?

5.6.3 Types of Network Security

We have talked about the different types of network security controls. Now let's take a look at some of the different ways you can secure your network.

- ***Network Access Control***

To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices. Network access control (NAC) can be set at the most granular level. For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.

- ***Antivirus and Antimalware Software***

Antivirus and antimalware software protect an organization from a range of malicious software, including viruses, ransomware, worms and trojans. The best software not only scans files upon entry to the network but continuously scans and tracks files.

- ***Firewall Protection***

Firewalls, as their name suggests, act as a barrier between the untrusted external networks and your trusted internal network. Administrators typically configure a set of defined rules that blocks or permits traffic onto the network. For example, Forcepoint's Next Generation Firewall (NGFW) offers seamless and centrally managed control of network traffic, whether it is physical, virtual or in the cloud.

- ***Virtual Private Networks***

Virtual private networks (VPNs) create a connection to the network from another endpoint or site. For example, users working from home would typically connect to the organization's network over a VPN. Data between the two points is encrypted and the user would need to authenticate to allow communication between their device and the network. Forcepoint's Secure Enterprise SD-WAN allows organizations to quickly create VPNs using drag-and-drop and to protect all locations with our Next Generation Firewall solution.

- ***Web Security***

This network security solution determines the levels of user access, differentiates between authorized and unauthorized users, identifies vulnerabilities of applications, and thus, protects the sensitive data of an organization from being compromised.

- ***Mobile Device Security***

All security measures that are designed to protect data, either stored on or transmitted by mobile devices (such as smartphones, laptops, and tablets) fall under the Mobile Device Security type. With IT organizations switching to mobile devices for the support of corporate applications, it is important to control the devices accessing your network.

5.6.4 Classification of Security Attacks

There are various types of threats, attacks and vulnerabilities present to corrupt and breach the system security. Security attacks are the computer attacks that compromise the security of the system. Conceptually, the security attacks can be classified into two types that are active and passive attacks where the attacker gains illegal access to the system's resources.

The major difference between active and passive attacks is that in active attacks the attacker intercepts the connection and modifies the information. Whereas, in a passive attack, the attacker intercepts the transit information with the intention of reading and analyzing the information not for altering it.

- ***Active Attacks***

Active attacks are the attacks in which the attacker tries to modify the information or creates a false message(shown in Figure 5.17). The prevention of these attacks is quite difficult because of a broad range of potential physical, network and software vulnerabilities. Instead of prevention, it emphasizes on the detection of the attack and recovery from any disruption or delay caused by it.

An active attack usually requires more effort and often more dangerous implication. When the hacker attempts to attack, the victim gets aware of it.

The active attacks are in the form of interruption, modification and fabrication.

✓ ***Interruption*** is known as masquerade attack in which unauthorized attacker tries to pose as another entity.

- ✓ ***Modification*** can be done using two ways replay attack and alteration. In the replay attack, a sequence of events or some data units is captured and resent by them. While alteration of the message involves some change to the original message, either one of them can cause alteration.

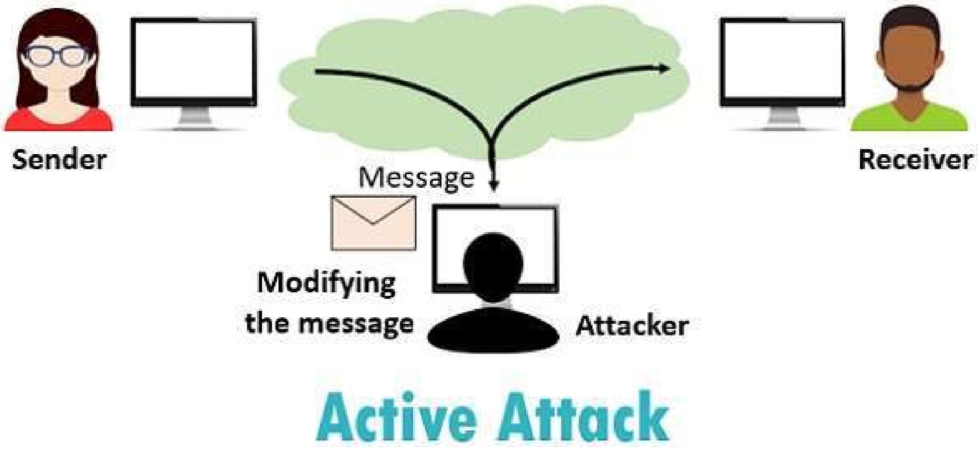


Figure 5.17 Active Attack

- ✓ ***Fabrication*** causes Denial Of Service (DOS) attacks in which attacker strive to prevent licit users from accessing some services, which they are permitted to or in simple words the attacker gain access to the network and then lock the authorized user out.

- ***Passive Attacks***

Passive attacks are the attacks where the attacker indulges in unauthorized eavesdropping, just monitoring the transmission or gathering information (shown in Figure 5.18). The eavesdropper does not make any changes to the data or the system.

Unlike active attack, the passive attack is hard to detect because it doesn't involve any alteration in the data or system resources. Thus, the attacked entity doesn't get any clue about the attack. Although, it can be prevented using encryption methods in which the data is firstly encoded in the unintelligible language at the sender's end and then at the receivers end it is again converted into human understandable language.

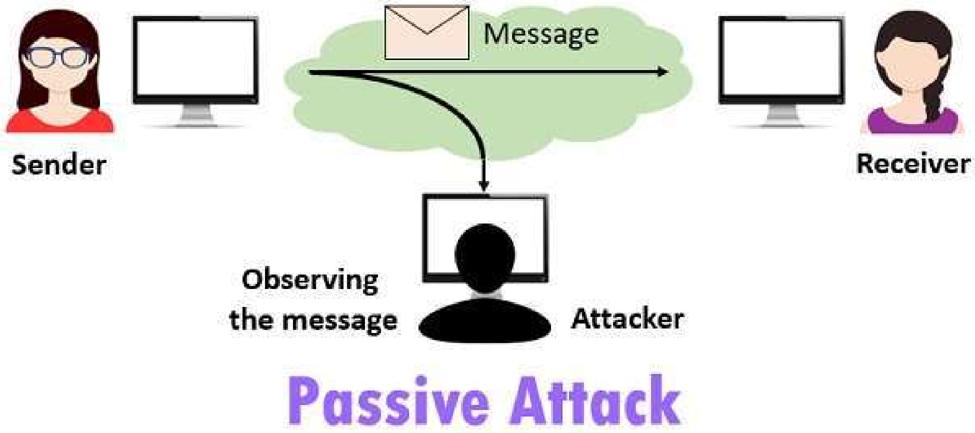


Figure 5.18 Passive Attack

In this way, at the time of transit, the message is in an unintelligible form which could not be understood by the hackers. That is the reason, in passive attacks, the prevention has more concern than detection. The passive attacks entangle the open ports that are not protected by firewalls. The attacker continuously searches for the vulnerabilities and once it is found the attacker gains access to network and system.

The passive attacks are further classified into two types, first is the release of message content and second is traffic analysis.

- ✓ The ***release of message content*** can be expressed with an example, in which the sender wants to send a confidential message or email to the receiver. The sender doesn't want the contents of that message to be read by some interceptor.
- ✓ By using encryption a message could be masked in order to prevent the extraction of the information from the message, even if the message is captured. Though still attacker can analyse the traffic and observe the pattern to retrieve the information. This type of passive attack refers to as ***traffic analysis***.

5.7 Short Questions and Answers

1. What is the purpose of Domain Name System?

Domain Name System can map a name to an address and conversely an address to name.

2. Discuss the three main division of the domain name space.

Domain name space is divided into three different sections: generic domains, country domains & inverse domain.

- ✓ **Generic domain:** Define registered hosts according to their generic behavior, uses generic suffixes.
- ✓ **Country domain:** Uses two characters to identify a country as the last suffix.
- ✓ **Inverse domain:** Finds the domain name given the IP address.

3. Discuss the TCP connections needed in FTP.

FTP establishes two connections between the hosts. One connection is used for data transfer, the other for control information. The control connection uses very simple rules of communication. The data connection needs more complex rules due to the variety of data types transferred.

4. Discuss the basic model of FTP.

The client has three components: the user interface, the client control process, and the client data transfer process. The server has two components: the server control process and the server data transfer process. The control connection is made between the control processes. The data connection is made between the data transfer processes.

5. What is the function of SMTP?

The TCP/IP protocol supports electronic mail on the Internet is called Simple Mail Transfer Protocol (SMTP). It is a system for sending messages to other computer users based on e- mail addresses. SMTP provides mail exchange between users on the same or different computers.

6. What is the difference between a User Agent (UA) and a Mail Transfer Agent (MTA)?

The UA prepares the message, creates the envelope, and puts the message in the envelope. The MTA transfers the mail across the Internet.

7. How does MIME enhance SMTP?

MIME is a supplementary protocol that allows non-ASCII data to be sent through SMTP. MIME transforms non-ASCII data at the sender site to NVT ASCII data and deliverers it to the client SMTP to be sent through the Internet. The server SMTP at the receiving side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original data.

8. Why is an application such as POP needed for electronic messaging?

Workstations interact with the SMTP host which receives the mail on behalf of every host in the organization, to retrieve messages by using a client-server protocol such as Post Office Protocol, version 3(POP3). Although POP3 is used to download messages from the server, the SMTP client still needed on the desktop to forward messages from the workstation user to its SMTP mail server.

9. Write down the three types of WWW documents.

The documents in the WWW can be grouped into three broad categories: static, dynamic and active.

- ✓ **Static:** Fixed-content documents that are created and stored in a server.
- ✓ **Dynamic:** Created by web server whenever a browser requests the document.
- ✓ **Active:** A program to be run at the client side.

10. What is the purpose of HTML?

HTML is a computer language for specifying the contents and format of a web document. It allows additional text to include codes that define fonts, layouts, embedded graphics and hypertext links.

11. Define CGI.

CGI is a standard for communication between HTTP servers and executable programs. It is used in crating dynamic documents.

12. Name four factors needed for a secure network.

- ✓ **Privacy:** The sender and the receiver expect confidentiality.
- ✓ **Authentication:** The receiver is sure of the sender's identity and that an imposter has not sent the message.
- ✓ **Integrity:** The data must arrive at the receiver exactly as it was sent.
- ✓ **Non-Reputation:** The receiver must able to prove that a received message came from a specific sender.

13. How is a secret key different from public key?

In secret key, the same key is used by both parties. The sender uses this key and an encryption algorithm to encrypt data; the receiver uses the same key and the corresponding decryption algorithm to decrypt the data.

In public key, there are two keys: a private key and a public key. The private key is kept by the receiver. The public key is announced to the public.

14. What is a digital signature?

Digital signature is a method to authenticate the sender of a message. It is similar to that of signing transactions documents when you do business with a bank. In network transactions, you can create an equivalent of an electronic or digital signature by the way you send data.

15. What are the advantages & disadvantages of public key encryption?

Advantages:

- ✓ Remove the restriction of a shared secret key between two entities. Here each entity can create a pair of keys, keep the private one, and publicly distribute the other one.
- ✓ The no. of keys needed is reduced tremendously. For one million users to communicate, only two million keys are needed.

Disadvantage:

- ✓ If you use large numbers the method to be effective. Calculating the cipher text using the long keys takes a lot of time. So, it is not recommended for large amounts of text.

16. What are the advantages & disadvantages of secret key encryption?

Advantage:

- ✓ Secret Key algorithms are efficient: it takes less time to encrypt a message. The reason is that the key is usually smaller. So, it is used to encrypt or decrypt long messages.

Disadvantages:

- ✓ Each pair of users must have a secret key. If N people in world want to use this method, there needs to be N (N-1)/2 secret keys. For one million people to communicate, a half- billion secret keys are needed.
- ✓ The distribution of the keys between two parties can be difficult.

17. Define permutation.

Permutation is transposition in bit level.

- ✓ **Straight permutation:** The number of bits in the input and output are preserved.
- ✓ **Compressed permutation:** The number of bits is reduced (some of the bits are dropped).
- ✓ **Expanded permutation:** The number of bits is increased (some bits are repeated).

18. Define substitutional & transpositional encryption.

- ✓ **Substitutional:** A character level encryption in which each character is replaced by another character in the set.

- ✓ **Transpositional:** A Character level encryption in which the characters retain their plaintext but the position of the character changes.

19. What is WWW?

The World Wide Web is an architectural framework for accessing linked documents spread out over millions of machines all over the Internet. World Wide Web, which is also known as a Web, is a collection of websites or web pages stored in web servers and connected to local computers through the internet.

20. What is meant by hyperlinks?

Strings of text that are links to other pages, called *hyperlinks*, are often highlighted, by underlining, displaying them in a special color, or both. To follow a link, the user places the mouse cursor on the highlighted area, which causes the cursor to change, and clicks on it.

21. What is URL?

A web page is given an online address called a *Uniform Resource Locator* (URL). A particular collection of web pages that belong to a specific URL is called a website, e.g., www.facebook.com, www.google.com, etc.

22. What is Cookie?

Cookies are small files which are stored on a user's computer. They are designed to hold a modest amount of data specific to a particular client and website, and can be accessed either by the web server or the client computer.

23. What is HTML?

HTML allows users to produce Web pages that include text, graphics, and pointers to other Web pages. HTML is a markup language, a language for describing how documents are to be formatted.

24. What is the use of Common Gateway Interface?

The CGI (Common Gateway Interface) is a standardized interface to allow Web servers to talk to back-end programs and scripts that can accept input (e.g., from forms) and generate HTML pages in response.

25. What is meant by caching?

Caching (pronounced “cashing”) is the process of storing data in a cache memory. A cache is a temporary storage area. For example, the files you automatically request by looking at a Web page are stored on your hard disk in a cache subdirectory under the directory for your browser. When you return to a page you've recently looked at, the browser can get those files from the cache rather than the original server, saving you time and saving the network the burden of additional traffic.

26. Define Content Delivery Network (CDN).

A content delivery network (CDN) is a system of distributed servers (network) that deliver pages and other web content to a user, based on the geographic locations of the user, the origin of the webpage and the content delivery server.

27. Define multimedia.

Multimedia is an interactive media and provides multiple ways to represent information to the user in a powerful manner. It provides an interaction between users and digital information. It is a medium of communication with the use of a combination of text, audio, video, graphics and animation.

28. What are the Multimedia Elements?

- ✓ Text
- ✓ Graphics
- ✓ Audio
- ✓ Video
- ✓ Animation

29. What is meant by waveform coding?

Waveform coding is an audio compression technique in which the signal is transformed mathematically by a Fourier transform into its frequency components. The amplitude of each component is then encoded in a minimal way. The goal is to reproduce the waveform accurately at the other end in as few bits as possible.

30. What is meant by perceptual coding?

The perceptual coding exploits certain flaws in the human auditory system to encode a signal in such a way that it sounds the same to a human listener, even if it looks quite different on an oscilloscope. Perceptual coding is based on the science of psychoacoustics—how people perceive sound. MP3 is based on perceptual coding.

31. What are the Multimedia Input Devices?

- ✓ Keyboard
- ✓ Scanner.
- ✓ Bar Code Readers
- ✓ Optical Mark Reader (OMR).
- ✓ Microphone
- ✓ Digital Camera
- ✓ Digital Video Camera

32. What is Network Security?

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system. An example of network security is an antivirus system.

33. List out the security services.

- ✓ Confidentiality
- ✓ Authentication
- ✓ Integrity
- ✓ Non repudiation

- ✓ Availability
- ✓ Access control

34. What is Cryptography?

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

35. What is Active Attack?

Active attacks are the attacks in which the attacker tries to modify the information or creates a false message. The prevention of these attacks is quite difficult because of a broad range of potential physical, network and software vulnerabilities

36. What is Passive Attack?

Passive attacks are the attacks where the attacker indulges in unauthorized eavesdropping, just monitoring the transmission or gathering information. The eavesdropper does not make any changes to the data or the system.

5.8 Explanatory Questions

1. Discuss about the History of WWW. (5 marks)
2. What are the Purposes of HTML? Explain. (5 marks)
3. What are the Static and dynamic Web Documents? Explain. (5 marks)
4. Discuss about components of domain name system. (5 marks)
5. How do you enhance performance of web content delivery? Explain. (5 marks)
6. Discuss about the message format of the email. (5 marks)
7. What are the protocols used in email system? Explain. (5 marks)
8. Explain Multimedia Components. (5 marks)
9. List the Multimedia Hardware? Discuss in detail. (5 marks)
10. Explain Audio Streaming. (5 marks)
11. What is meant by cryptograph? Discuss in detail. (5 marks)
12. Describe Network Security services. (5 marks)
13. Classify Security Attacks. (5 marks)
14. How to create dynamic Web Documents? Explain with examples. (10 marks)
15. Explain the domain name system. (10 marks)
16. Explain the email service system with its protocols and components. (10 marks)
17. Describe about Multimedia Components. (10 marks)
18. Discuss in detail about Digital Audio. (10 marks)
19. Explain about different types of Network Security. (10 marks)

5.9 Objective Questions and answers

1. The entire hostname has a maximum of ___________

a) 255 characters
b) 127 characters

c) 63 characters
d) 31 characters

Answer: a

Explanation: An entire hostname can have a maximum of 255 characters. Although each label must be from 1 to 63 characters long. Host name is actually a label that is given to a device in a network.

2. A DNS client is called _________

a) DNS updater
b) DNS resolver
c) DNS handler
d) none of the mentioned

Answer: b

Explanation: DNS client also known as DNS resolver also known as DNS lookup helps to resolve DNS requests using an external DNS server.

3. Servers handle requests for other domains _______
a) directly
b) by contacting remote DNS server
c) it is not possible
d) none of the mentioned

Answer: b

Explanation: Whenever a request is received at server from other domains, it handles this situation by contacting remote DNS server.

4. DNS database contains _______

a) name server records
b) hostname-to-address records
c) hostname aliases
d) all of the mentioned

Answer: d

Explanation: Domain Name system not only deals with mapping IP addresses with the hostname but also deals with exchange of information in the server.

5. If a server has no clue about where to find the address for a hostname then _______

a) server asks to the root server
b) server asks to its adjacent server
c) request is not processed
d) none of the mentioned

Answer: a

Explanation: Root name servers are actually very important and critical as they are the first step in translating human readable hostnames into IP addresses for carrying out communication.

6. Which one of the following allows client to update their DNS entry as their IP address change?

a) dynamic DNS
b) mail transfer agent
c) authoritative name server
d) none of the mentioned

Answer: a

Explanation: Dynamic DNS or in short DDNS or DynDNS helps in automatically updating a name server in the DNS. This does not require manual editing.

7. Wildcard domain names start with label _______

a) @
b) *
c) &
d) #

Answer: b

Explanation: A wildcard DNS record matches requests to a non existent domain name. This wildcard DNS record is specified by using asterisk "*" as the starting of a domain name.

8. The right to use a domain name is delegated by domain name registers which are accredited by _______

a) internet architecture board
b) internet society
c) internet research task force
d) internet corporation for assigned names and numbers

Answer: d

Explanation: The ICANN (Internet Corporation for Assigned Names and Numbers) deals with IP address space allocation, protocol identifier assignment, generic and country code Top Level domain name system management (gTLD and ccTLD).

9. The domain name system is maintained by _______

a) distributed database system
b) a single server
c) a single computer
d) none of the mentioned

Answer: a

Explanation: A domain name system is maintained by a distributed database system. It is a collection of multiple, logically interrelated databases distributed over a computer network.

10. Which one of the following is not true?

a) multiple hostnames may correspond to a single IP address
b) a single hostname may correspond to many IP addresses
c) a single hostname may correspond to a single IP address
d) none of the mentioned

Answer: c

Explanation: It need not be that a single hostname will correspond to a ip address. For example facebook.com and fb.com both correspond to same ip address. So there can be multiple hostnames for a single ip address.

11. When the mail server sends mail to other mail servers it becomes ____________

a) SMTP server
b) SMTP client
c) Peer
d) Master

Answer: b

Explanation: SMTP clients are the entities that send mails to other mail servers. The SMTP servers cannot send independent mails to other SMTP servers as an SMTP server. There are no masters or peers in SMTP as it is based on the client-server architecture.

12. If you have to send multimedia data over SMTP it has to be encoded into _______

a) Binary
b) Signal
c) ASCII
d) Hash

Answer: c

Explanation: Since only 7-bit ASCII codes are transmitted through SMTP, it is mandatory to convert binary multimedia data to 7-bit ASCII before it is sent using SMTP.

13. 13. Expansion of SMTP is ________

b) Simple Message Transfer Protocol
c) Simple Mail Transmission Protocol
d) Simple Message Transmission Protocol

Answer: a

Explanation: SMTP or Simple Mail Transfer Protocol is an application layer protocol used to transport e-mails over the Internet. Only 7-bit ASCII codes can be sent using SMTP.

14. In SMTP, the command to write receiver's mail address is written with the command _______

a) SEND TO
b) RCPT TO
c) MAIL TO
d) RCVR TO

Answer: b

Explanation: RCPT TO command is followed by the recipient's mail address to specify where or to whom the mail is going to through the internet. If there is more than one receiver, the command is repeated for each address continually.

15. The underlying Transport layer protocol used by SMTP is ________

a) TCP
b) UDP
c) Either TCP or UDP
d) IMAP

Answer: a

Explanation: TCP is a reliable protocol, and Reliability is a mandatory requirement in e-mail transmission using SMTP.

16. Choose the statement which is wrong incase of SMTP?

a) It requires message to be in 7bit ASCII format
b) It is a pull protocol
c) It transfers files from one mail server to another mail server
d) SMTP is responsible for the transmission of the mail through the internet

Answer: b

Explanation: In SMTP, the sending mail server pushes the mail to receiving mail server hence it is push protocol. In a pull protocol such as HTTP, the receiver pulls the resource from the sending server.

17. Internet mail places each object in _________

a) Separate messages for each object
b) One message
c) Varies with number of objects
d) Multiple messages for each object

Answer: b

Explanation: It places all objects into one message as it wouldn't be efficient enough if there are different messages for each object. The objects include the text and all the multimedia to be sent.

18. Typically the TCP port used by SMTP is _________

a) 25

b) 35
c) 50
d) 15

Answer: a

Explanation: The ports 15, 35 and 50 are all UDP ports and SMTP only uses TCP port 25 for reliability.

19. A session may include ________

a) Zero or more SMTP transactions
b) Exactly one SMTP transactions
c) Always more than one SMTP transactions
d) Number of SMTP transactions cant be determined

Answer: a

Explanation: An SMTP session consists of SMTP transactions only even if no transactions have been performed. But no transactions in the session might mean that the session is inactive or is just initiated.

20. Which of the following is an example of user agents for e-mail?

a) Microsoft Outlook
b) Facebook
c) Google
d) Tumblr

Answer: a

Explanation: Among the options, only Microsoft Outlook is an e-mail agent. Google is a search engine and Facebook, and Tumblr are social networking platforms`. Gmail and Alpine are some other examples of e-mail agent.

21. Network Security provides authentication and access control for resources.

a) True

b) False

View Answer

Answer: a

Explanation: The statement is true. AFS is an example. It helps us protect vital information.

22. Which is not an objective of network security?

a) Identification
b) Authentication
c) Access control
d) Lock
Answer: d

Explanation: The Identification, Authentication and Access control are the objectives of network security. There is no such thing called lock.

23. Which of these is a part of network identification?

a) UserID
b) Password
c) OTP
d) fingerprint
View Answer

Answer: a

Explanation: The answer is UserID. UserID is a part of identification. UserID can be a combination of username, user student number etc.

24. The process of verifying the identity of a user.

a) Authentication
b) Identification
c) Validation
d) Verification
View Answer

Answer: a

Explanation: It is called an authentication. It is typically based on passwords, smart card, fingerprint, etc.

25. A concern of authentication that deals with user rights.

a) General access
b) Functional authentication
c) Functional authorization
d) Auto verification
View Answer

Answer: c

Explanation: Functional authorization is concerned with individual user rights. Authorization is the function of specifying access rights to resources related to information security.

26. CHAP stands for?

a) Challenge Handshake authentication protocol
b) Challenge Hardware authentication protocol
c) Circuit Hardware authentication protocol
d) Circuit Handshake authentication protocol
View Answer

27. Security features that control that can access resources in the OS.

a) Authentication
b) Identification
c) Validation
d) Access control
View Answer

28. An algorithm in encryption is called _____________

a) Algorithm
b) Procedure
c) Cipher
d) Module
View Answer

Answer: c

Explanation: An algorithm used in encryption is referred to as a cipher. cipher is an algorithm for performing encryption or decryption

29. The information that gets transformed in encryption is ____________

a) Plain text
b) Parallel text
c) Encrypted text
d) Decrypted text
View Answer

Answer: a

Explanation: The text that gets transformed is called plain text. The algorithm used is called cipher.

30. These ciphers replace a character or characters with a different character or characters, based on some key.

a) Polyalphabetic substitution based
b) Transposition-based
c) Substitution based
d) Mono alphabetic substitution based

Answer: d

Explanation: In mono alphabetic substitution-based cipher, a character is replaced with some other character or multiple characters, based on some key.

31. A type of cipher that uses multiple alphabetic strings.

a) Substitution based

b) Transposition-based
c) Polyalphabetic substitution based
d) Mono alphabetic substitution based

Answer: c
Explanation: These ciphers are similar to that of mono alphabetic ciphers. Multiple strings are used to encode the plain text.

32. An encryption technique with 2 keys is ______________

a) Monoalphabetic Cipher
b) Cryptography
c) Private key cryptography
d) Public key cryptography

Answer: d

Explanation: It is called as public key cryptography. It has 2 keys: a private key and a public key.

33. In public key cryptography, a key that decrypts the message.

a) public key
b) unique key
c) private key
d) security key

Answer: c

Explanation: Public key cryptography has 2 keys. They are private key and a public key. The public key encrypts the message. The private key decrypts the message.

34. Protocol is the client/server program used to retrieve the

a). IP
b). Header
c). Document
d). Cache

Answer : c

35. In World Wide Web (WWW), an electronic store (e-commerce) can use a cookie for its

a). Client Shopper
b). Server Usage
c). Server Data
d). Client Data

Answer : a

36. Uniform Resource Locator (URL), is a standard for specifying any kind of information on the

a). Server-End
b). Client-End

c). WebPage
d). Internet

Answer : d

37. World Wide Web (WWW), was originally designed as a

a). Stateless Document
b). Stateless Program
c). Stateless Entity
d). Stateless IP

Answer : c

38. Webpages are stored at the

a). Server
b). Client
c). Domain
d). Mail Server

Answer : a

39. In Audio and Video Compression, each frame is divided into small grids, called picture elements or

a). Frame
b). Packets
c). Pixels
d). Mega Pixels

Answer : c

40. Encryption and decryption provide secrecy, or confidentiality, but not

a). Authentication
b). Integrity
c). Privacy
d). All of the above

Answer : b

Acknowledgments

1. https://en.wikipedia.org/wiki/Computer_network
2. Sunshine C.A., A Brief History of Computer Networking. In: Sunshine C.A. (eds) Computer Network Architectures and Protocols. Applications of Communications Theory", Springer, Boston, MA, 1989.
3. Tannenbaum, A.S., "Computer Networks", 4th Edition, Prentice Hall, 2003.
4. William Stallings, "Local and Metropolitan Area Networks", 6th Edition, Pearson Education India, 2008.
5. W. Stallings, "Data and Computer Communication", Pearson Education, 5th Edition, 2001
6. Behrouz A. Forouzan, "Data Communications and Networking", 4th Edition, McGraw Hill Education, 2007.
7. Jim Kurose; Keith Ross, "Computer Networking: A Top-Down Approach", 6th Edition, Pearson Education, Inc, 2003.
8. Larry L. Peterson; Bruce S. Davie, "Computer Networks : A Systems Approach", 4th Edition, Morgan Kaufmann Publishers, 2007.
9. Doug Lowe, "Networking All-in-One Desk Reference for Dummies", 2nd Edition, Wiley Publishing, Inc,2005.
10. Ramon Nastase, "Computer Networking for Beginners", Amazon Digital Services LLC - KDP Print US, 2018
11. Douglas Comer, "Computer Networks and Internets", 5th Edition, Prentice Hall, 2009.
12. Russ White and Ethan Banks," Computer Networking Problems and Solutions: An innovative approach to building resilient, modern networks", 1st Edition, Addison-Wesley Professional.
13. Michael B. White, "Computer Networking: The Complete Guide to Understanding Wireless Technology, Network Security, Computer Architecture and Communications Systems (Including Cisco, CCNA and CCENT)", CreateSpace Independent Publishing Platform, 2018.
14. Olivier Bonaventure, "Computer Networking: Principles, Protocols, and Practice", The Saylor Foundation, Release 0.25, 2011.
15. https://www.tutorialspoint.com
16. https://www.computerhope.com/jargon/e/email.htm
17. https://www.quora.com
18. https://www.webopedia.com
19. https://www.hackingarticles.in
20. https://techdifferences.com
21. https://www.slideshare.net