CMR INSTITUTE OF TECHNOLOGY

* UGC AUTONOMOUS *

* Approved by AICTE * Accredited by NAAC with 'A' Grade * All B.Tech programs Accredited by NBA*

(Kandlakoya (v),Medchal Road,Hyderabad - 501 401)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

II – B.Tech – II – Sem (CSE ‘C’ & CSE – DS ‘A’)

COMPUTER NETWORKS (20-CS-PC-224)
(R20 Regulations)

By

Dr.A.Nirmal Kumar

COMPUTER NETWORKS

SYLLABUS

Unit	Title/Topics	Hours
I	**Overview of the Internet, Physical layer and Data link layer**	10
	Overview of the Internet: Protocols and standards, Layering scenario, TCP/IP Protocol Suite, The OSI model, Internet history and administration, Comparison of the OSI and TCP/IP reference model. **Physical layer:** Transmission Media, Guided Media, wireless transmission Media. **Data link layer**: Design issues, CRC Codes, Elementary Data Link layer Protocols, sliding Window Protocol. ***Task:*** *Write a program to compute CRC code for the polynomials.*	
II	**Multiple Access protocols**	9
	Multiple Access protocols-Aloha, CSMA, Collision free protocols, Ethernet –Physical layer, Ethernet Mac sub layer, Data link layer switching and use of bridges, learning bridges ,Spanning tree bridges, repeaters, hubs, bridges, switches ,routers and gateways. ***Task:*** *Write a program for 1 bit collision free protocol.*	
III	**Network layer and Routing Algorithms**	5+5=10
	Part-A: Network layer: Network layer Design issues, store and forward packet switching connection less and connection oriented networks. ***Task:*** *Write a program to implement i) Character stuffing ii) Bit stuffing.*	
	Part-B: Routing Algorithms: Optimality principle, shortest path, flooding, distance vector routing, count to infinity problem, hierarchical routing, congestion control algorithms and admission control. ***Task:*** *Implement distance vector routing algorithm for obtaining routing tables at each node.*	
IV	**Internetworking and Transport Layer**	9
	Internetworking: Tunneling, internetwork Routing, Packet fragmentation, IPV4, IPV6 Protocol, IP addresses, CIDR, ICMP, ARP, RARP, DHCP. **Transport Layer**: Services provided to the upper layers elements of transport protocol-addressing connection establishment, connection release. ***Task:*** *Write a program to demonstrate ARP.*	
V	**TCP/IP and Application Layer**	10
	TCP/IP: The internet Transport protocols UD-RPC, Real time Transport protocols, The internet Transport protocols-Introduction to TCP, The TCP services model ,The TCP segment Header, The connection Establishment, The TCP Connection release, The TCP Connection management modeling, The TCP Sliding Window, The TCP Congestion Control. **Application Layer**: Introduction, Providing services, Applications layer paradigms, HTTP, FTP, electronic mail, DNS, SSH. ***Task:*** *Write a program to implement RPC.*	

TEXT BOOKS & REFERENCES

Textbooks:
1. Data Communications and Networking – Behrouz A Forouzan, Fourth Edition, TMH. 2. Computer Networks - Andrew S Tanenbaum, 4th Edition. Pearson Education/PHI
References:
1. Introduction to Data communication and Networking, Tamasi, Pearson Education 2. Computer Networking: A Top-Down Approach Featuring the Internet, James F. Kurose, Keith W. Ross, 3rd Edition, Pearson.

COURSE OUTCOMES

Upon completion of the course, the student will be able

CO 1: To outline the basics of computer networks and various layers (Unit – I)

CO 2: To demonstrate multiple access protocols **(Unit – II)**

CO 3: To interpret network layer and routing algorithms **(Unit – III)**

CO 4: To illustrate internetworking and various transport protocols **(Unit – IV)**

CO 5: To make use of various protocols of application layer **(Unit – V)**

UNIT – I

Overview of the Internet: Protocols and standards, Layering scenario, TCP/IP Protocol Suite, The OSI model, Internet history and administration, Comparison of the OSI and TCP/IP reference model.

Physical layer: Transmission Media, Guided Media, wireless transmission Media.

Data link layer: Design issues, CRC Codes, Elementary Data Link layer Protocols, sliding Window Protocol.

DATA COMMUNICATIONS

The term telecommunication means communication at a distance. The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

Figure: *Components of a data communication system*

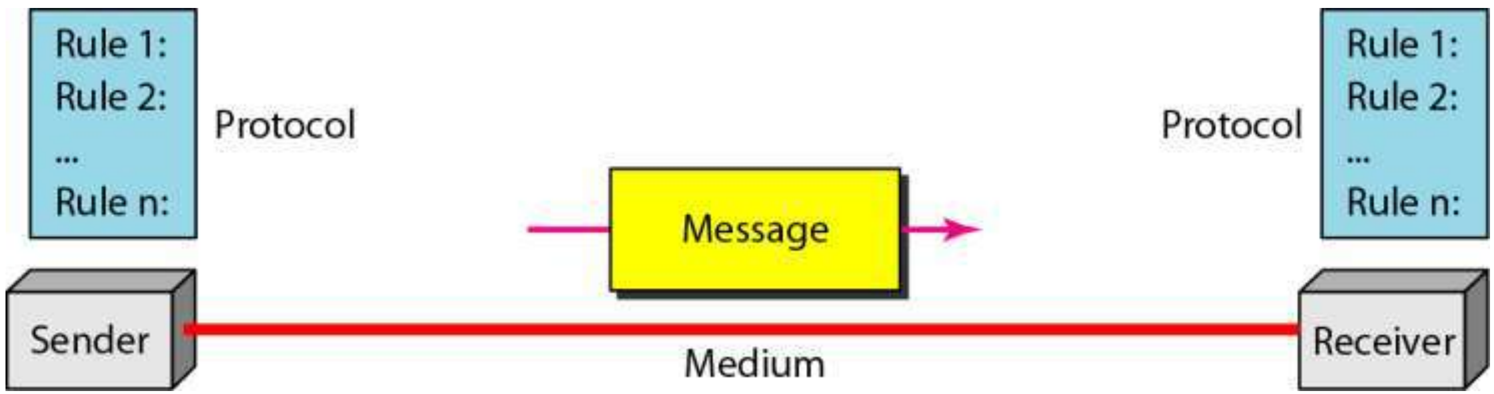
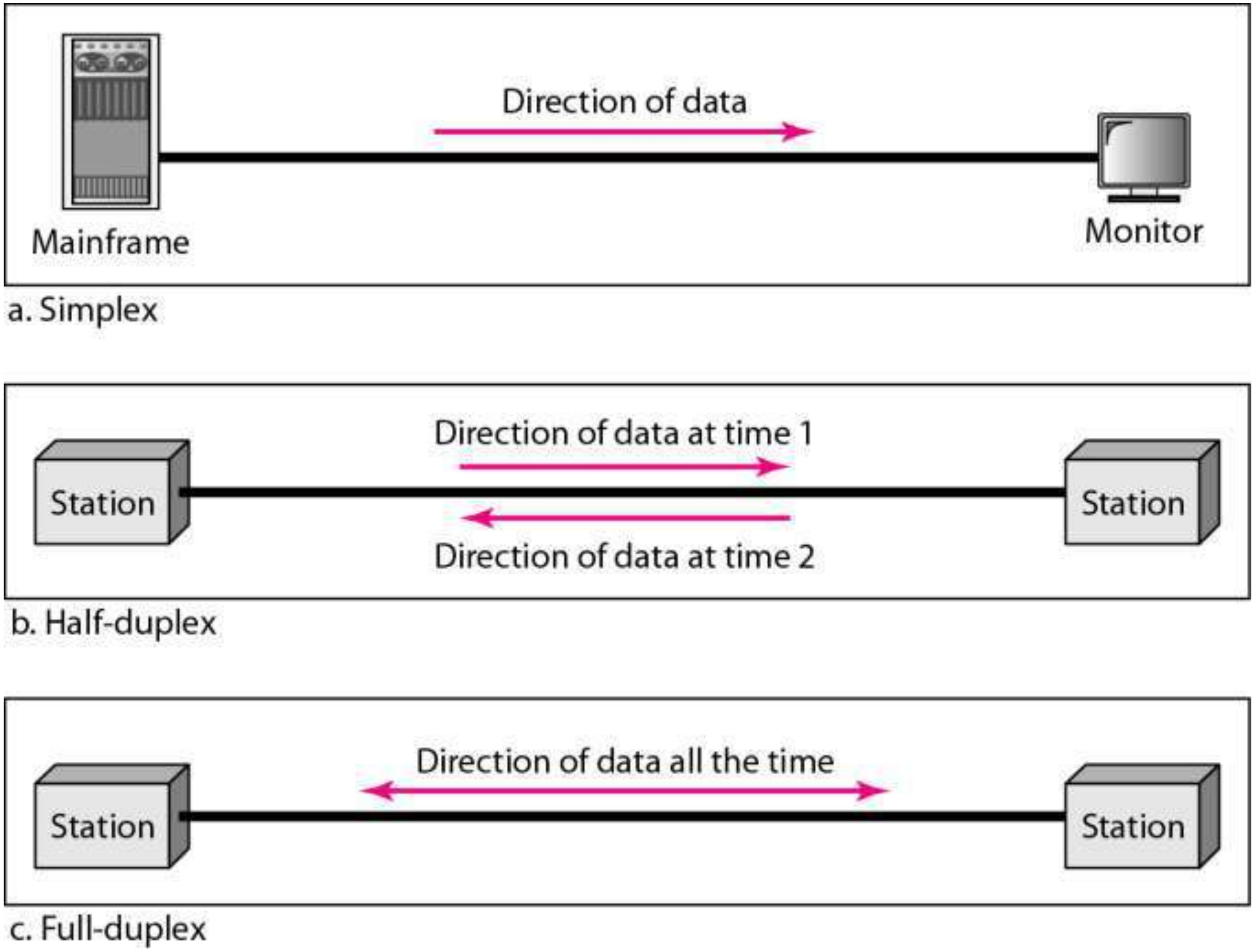


Figure: *Data flow (simplex, half-duplex, and full-duplex)*



NETWORKS

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network. A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.

Topics discussed in this section:

- Network Criteria
- Physical Structures
- Categories of Networks

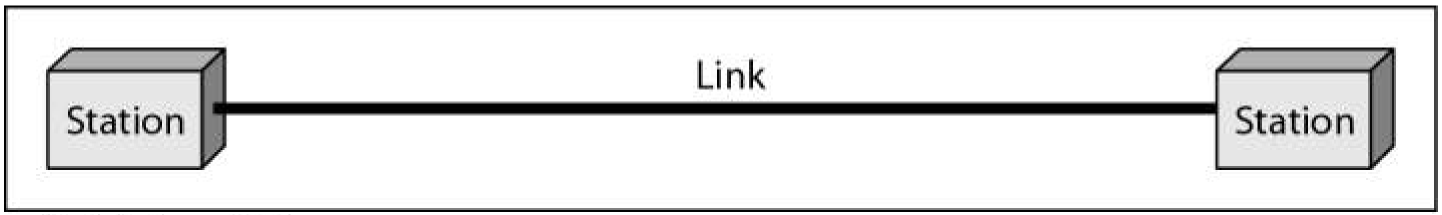
Network Criteria

- **Performance**
  - **Depends on Network Elements**
  - **Measured in terms of Delay and Throughput**
- **Reliability**
  - **Failure rate of network components**
  - **Measured in terms of availability/robustness**
- **Security**
  - **Data protection against corruption/loss of data due to:**
    - **Errors**
    - **Malicious users**

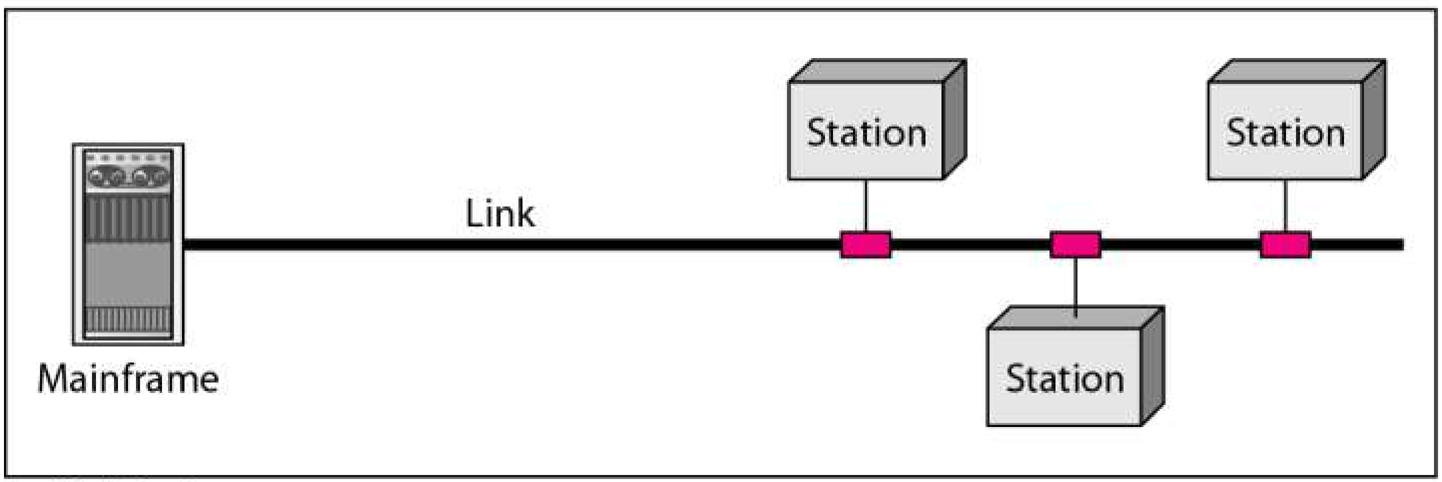
Physical Structures

- **Type of Connection**
  - **Point to Point - single transmitter and receiver**
  - **Multipoint - multiple recipients of single transmission**
- **Physical Topology**
  - **Connection of devices**
  - **Type of transmission - unicast, mulitcast, broadcast**

Figure: *Types of connections: point-to-point and multipoint*



a. Point-to-point



b. Multipoint

Figure: *Categories of topology*

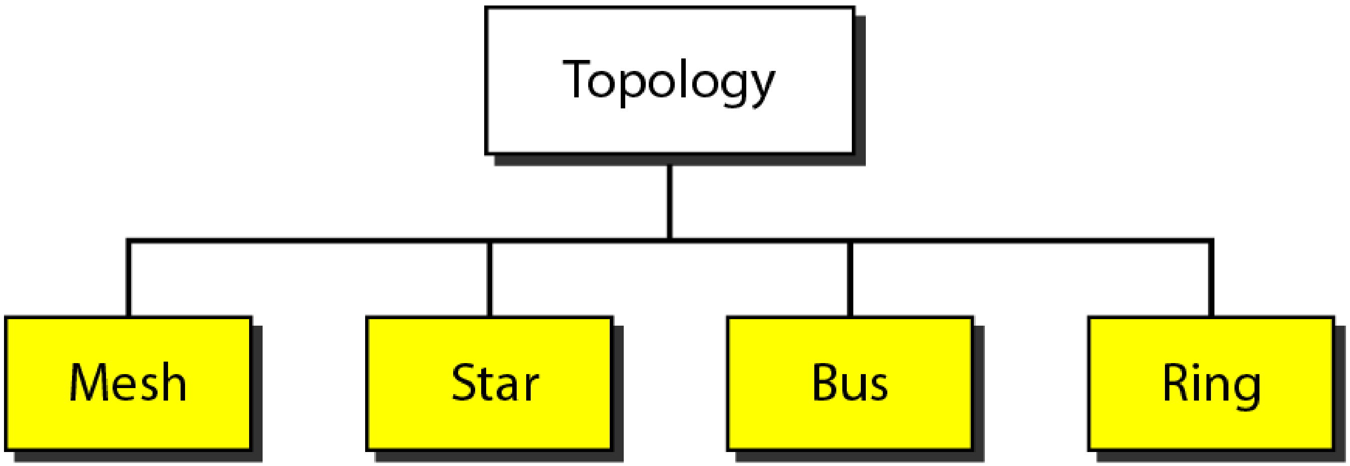


Figure: *A fully connected mesh topology (five devices)*

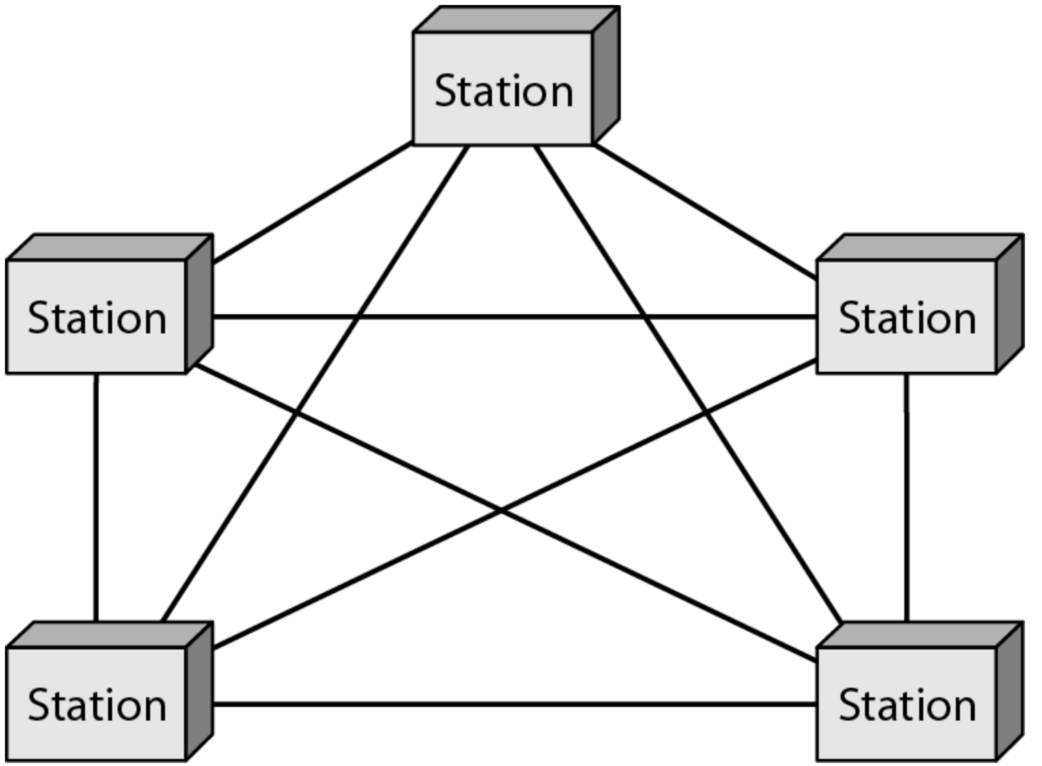


Figure: *A star topology connecting four stations*

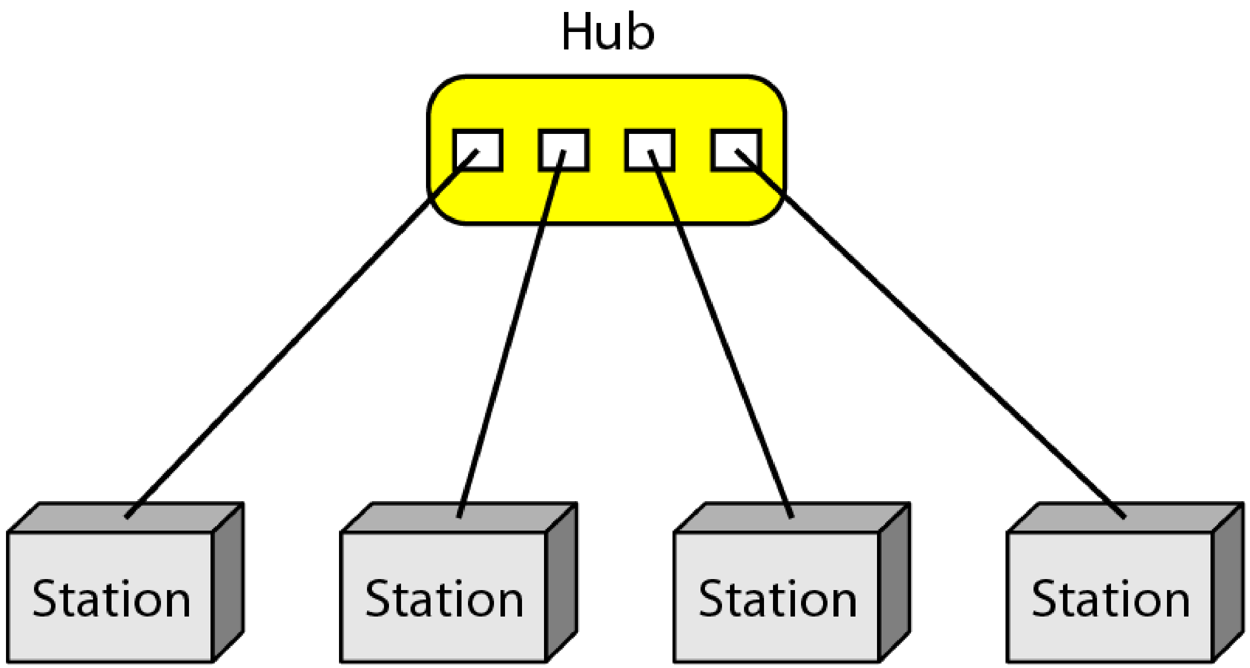


Figure: *A bus topology connecting three stations*

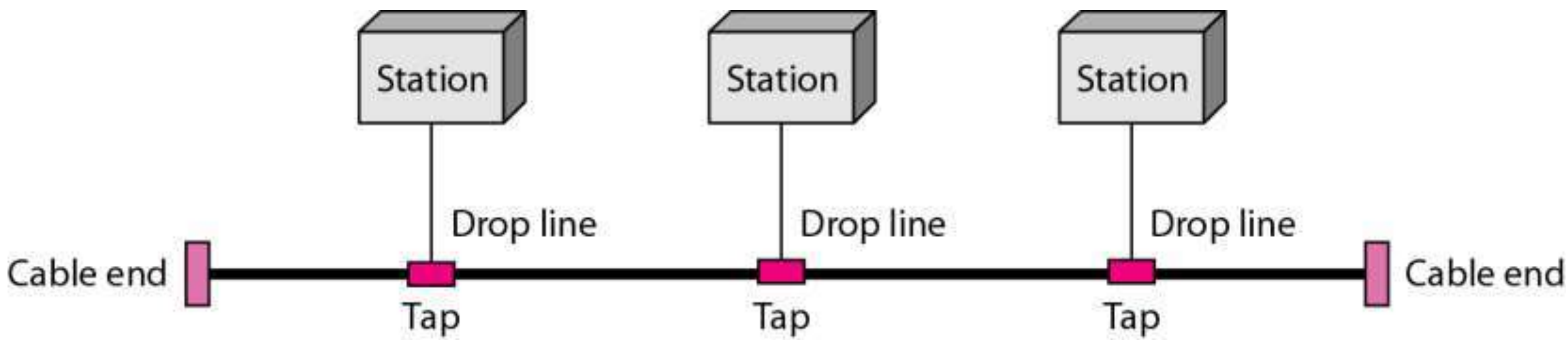


Figure: *A ring topology connecting six stations*

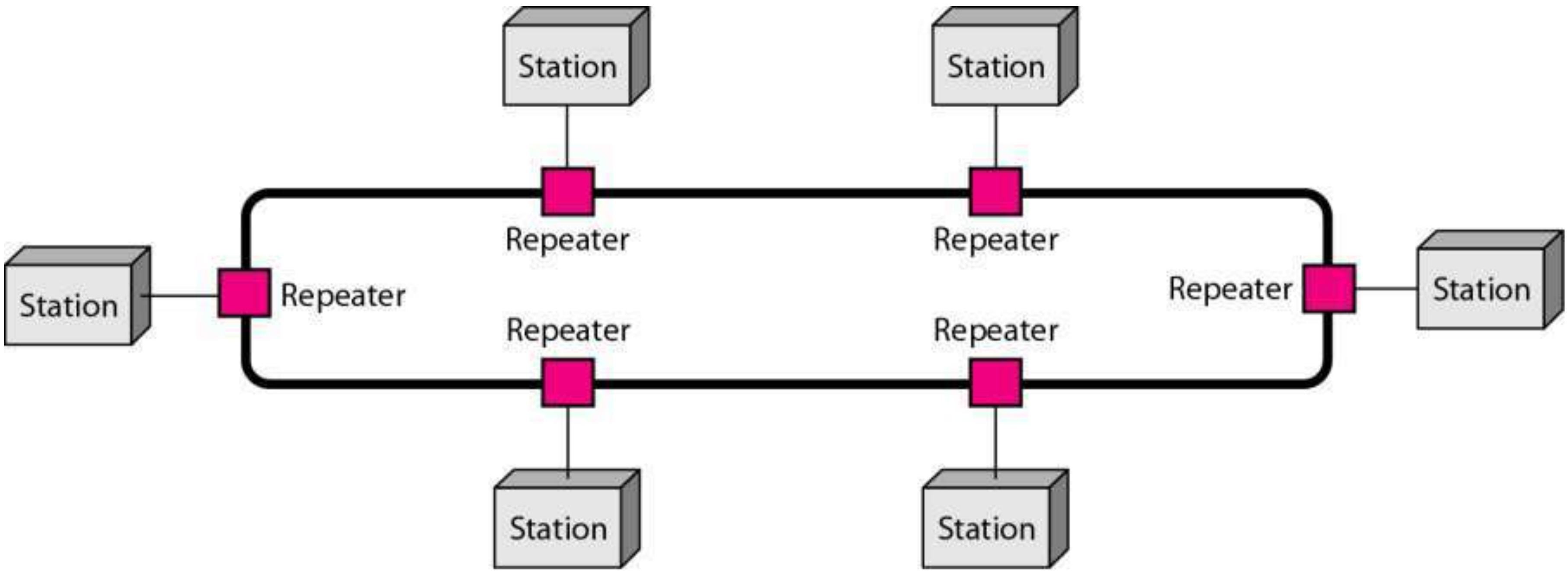
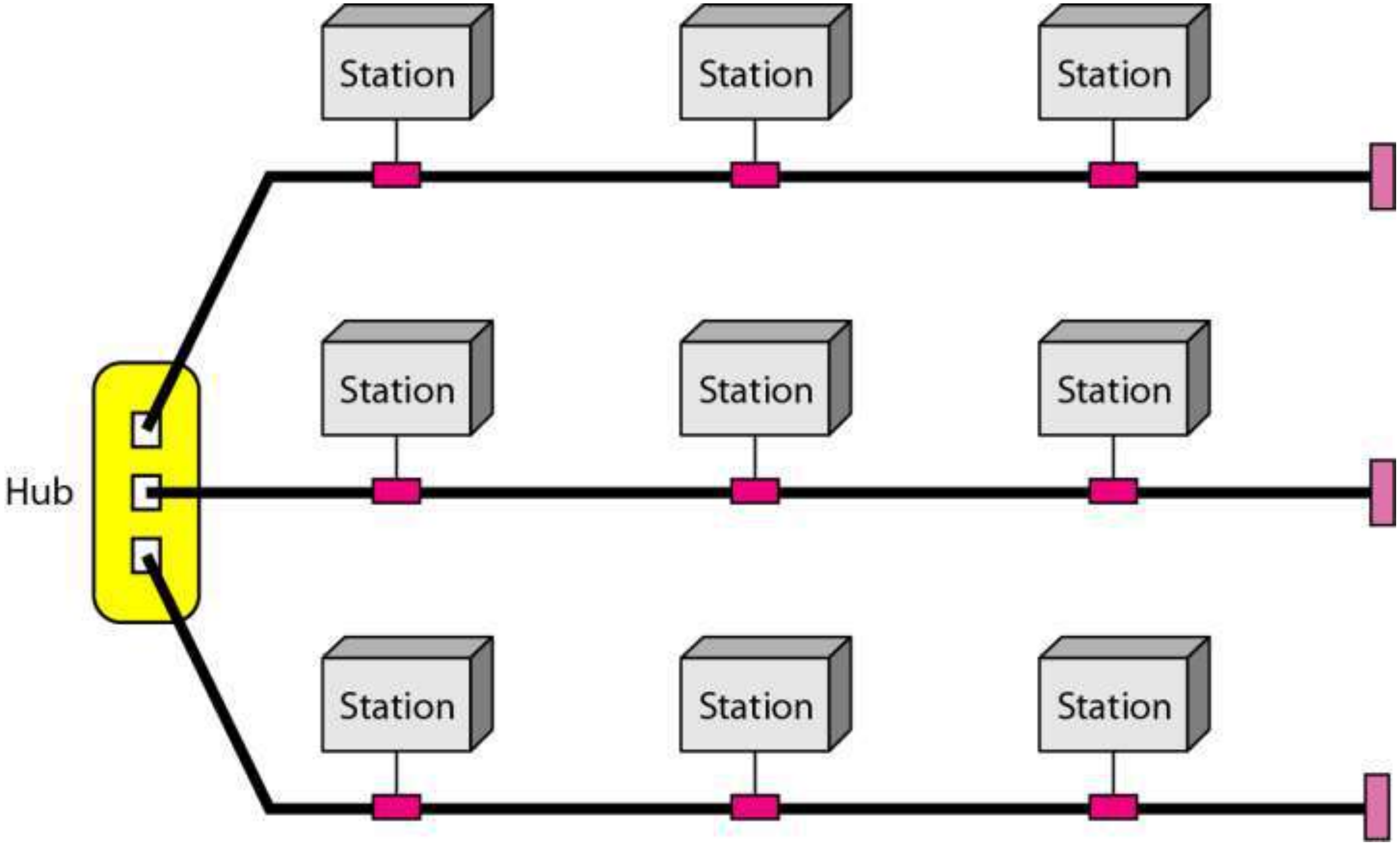


Figure: *A hybrid topology: a star backbone with three bus networks*



Categories of Networks

- **Local Area Networks (LANs)**
  - **Short distances**
  - **Designed to provide local interconnectivity**
- **Wide Area Networks (WANs)**
  - **Long distances**
  - **Provide connectivity over large areas**
- **Metropolitan Area Networks (MANs)**
  - **Provide connectivity over areas such as a city, a campus**

Figure: *An isolated LAN connecting 12 computers to a hub in a closet*

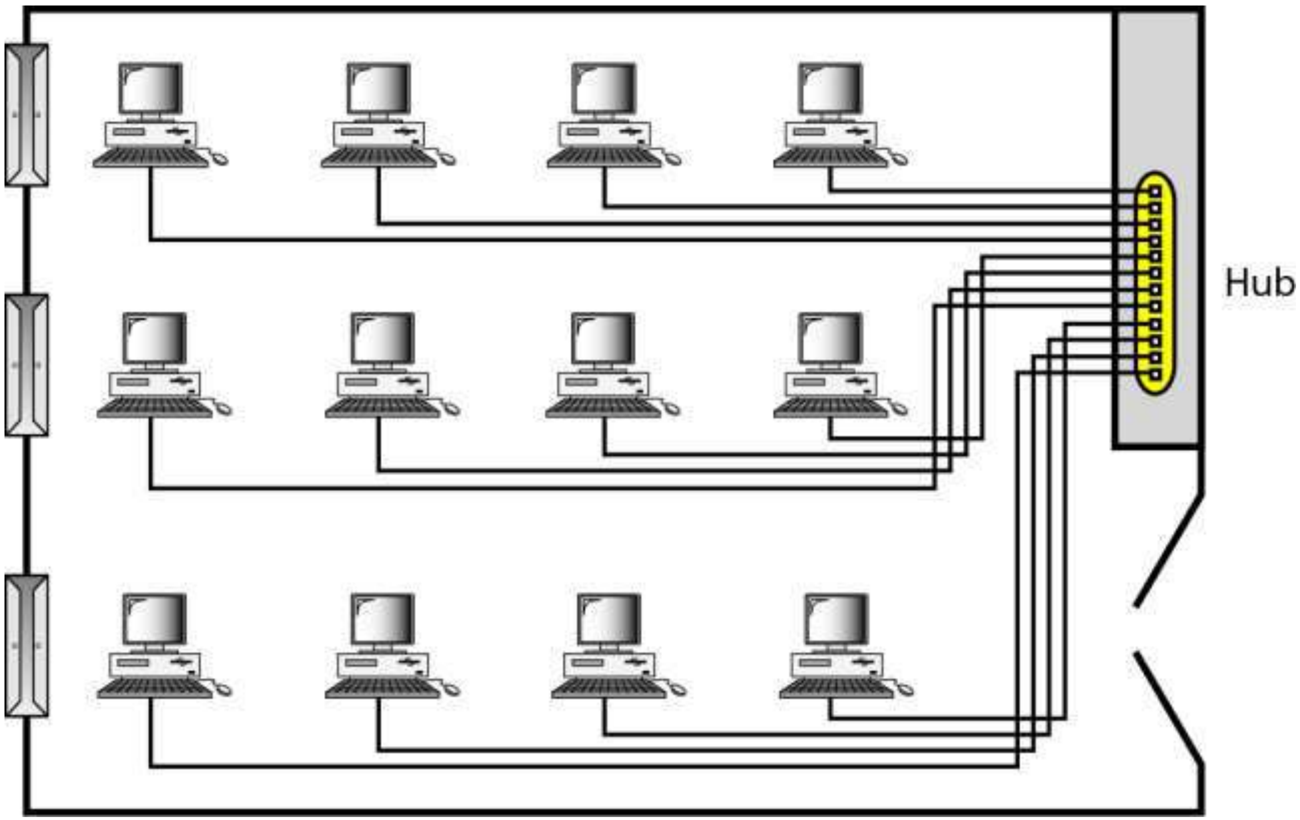
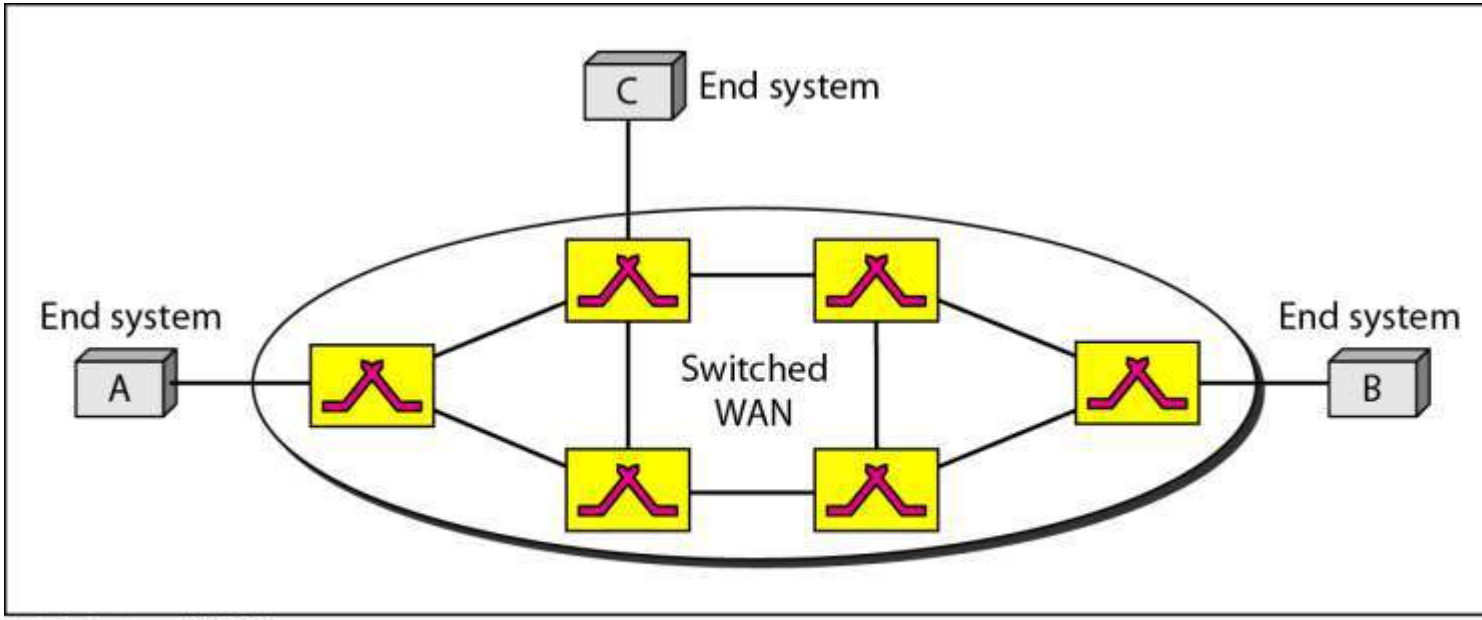
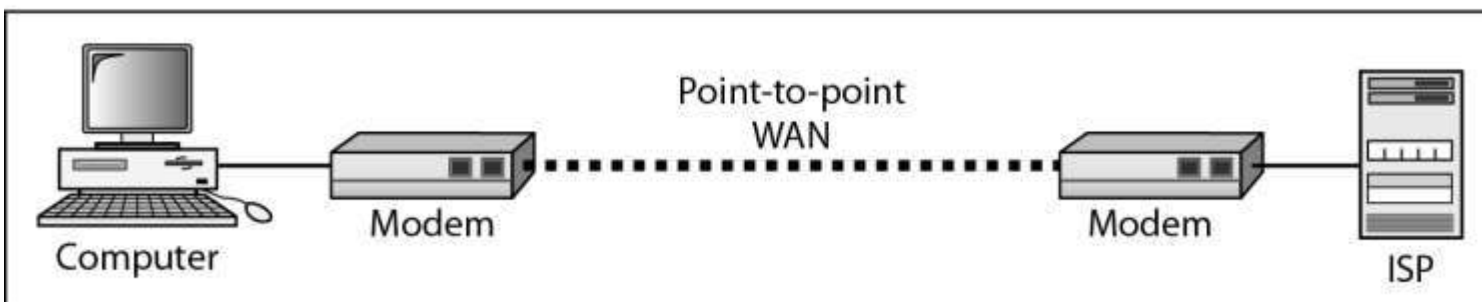


Figure: *WANs: a switched WAN and a point-to-point WAN*

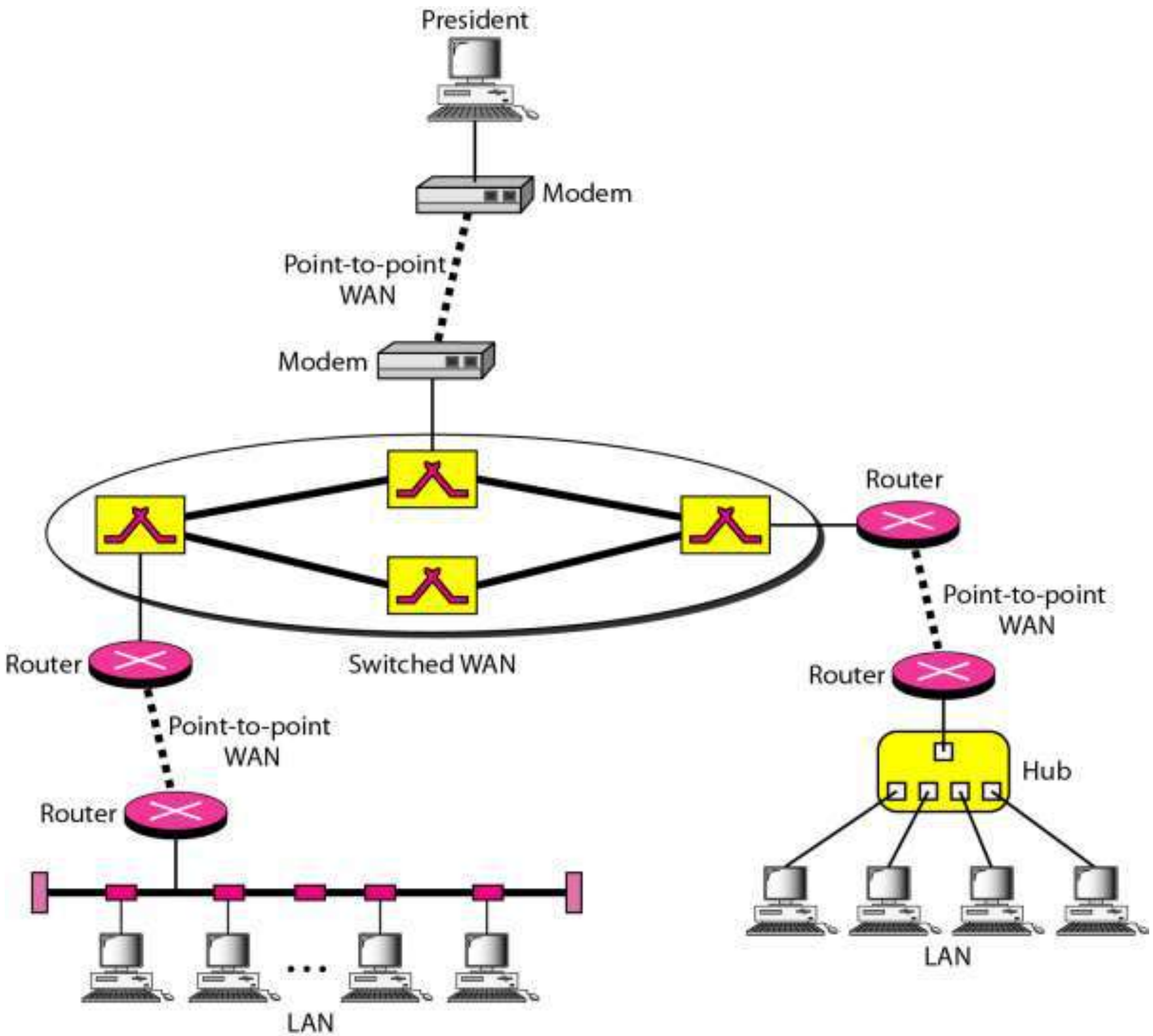


a. Switched WAN



b. Point-to-point WAN

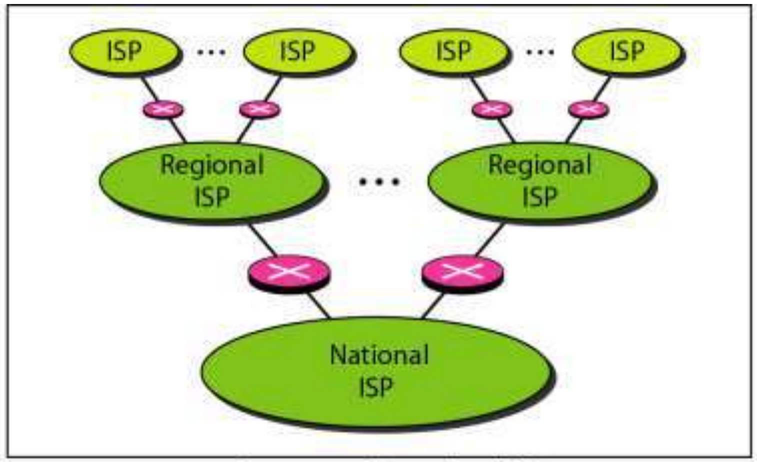
Figure: *A heterogeneous network made of four WANs and two LANs*



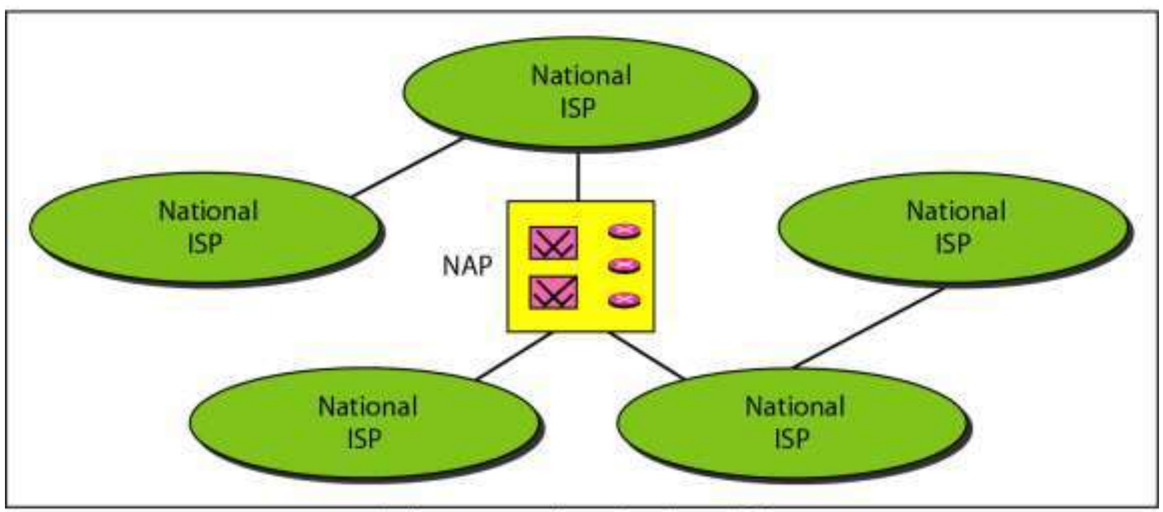
THE INTERNET

The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time. The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.

Figure: *Hierarchical organization of the Internet*



a. Structure of a national ISP



b. Interconnection of national ISPs

PROTOCOLS

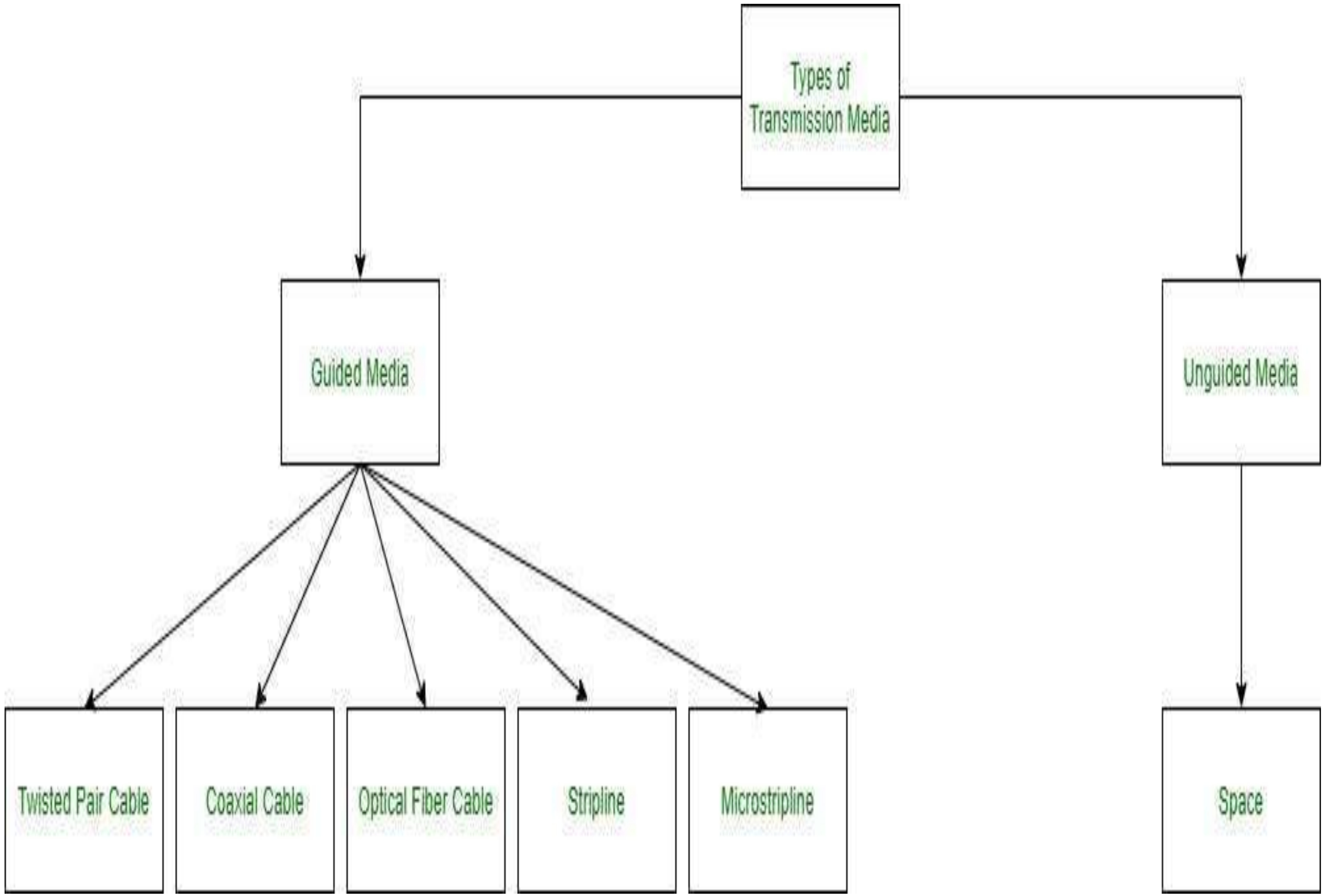
A protocol is synonymous with rule. It consists of a set of rules that govern data communications. It determines what is communicated, how it is communicated and when it is communicated. The key elements of a protocol are syntax, semantics and timing

Elements of a Protocol

- **Syntax**
  - **Structure or format of the data**
  - **Indicates how to read the bits - field delineation**
- **Semantics**
  - **Interprets the meaning of the bits**
  - **Knows which fields define what action**
- **Timing**
  - **When data should be sent and what**
  - **Speed at which data should be sent or speed at which it is being received.**

Physical Layer – Transmission Media

- A transmission medium is a physical path between the transmitter and the receiver.
- Transmission media is a communication channel that carries the information in the form of bits through **LAN**(Local Area Network) from the sender to the receiver. Data is transmitted through the electromagnetic signals.
- In OSI(Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component.
- The transmission media is available in the lowest layer of the OSI reference model, i.e., Physical layer.

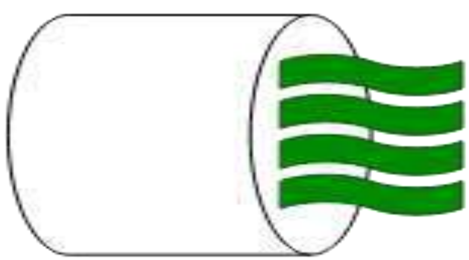

Types of
Transmission Media
Guided Media
Unguided Media
Twisted Pair Cable
Coaxial Cable
Optical Fiber Cable
Stripline
Microstripline
Space

1. Guided Media:

- It is also referred to as Wired or Bounded transmission media. Signals being transmitted are directed and confined in a narrow pathway by using physical links. **Features:**
- High Speed
- Secure
- Used for comparatively shorter distances

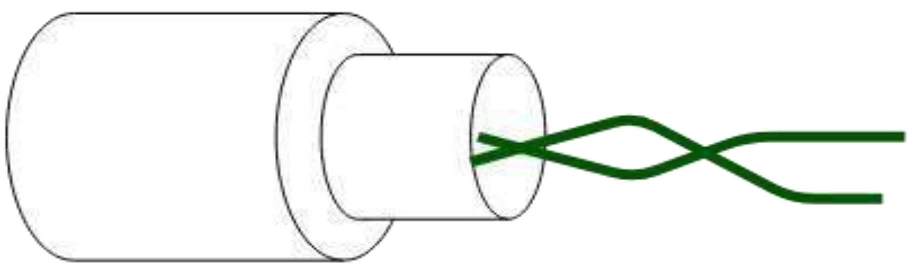
(i) Twisted Pair Cable –

Unshielded Twisted Pair (UTP): UTP consists of two insulated copper wires twisted around one another. This type of cable has the ability to block interference and does not depend on a physical shield for this purpose. It is used for telephonic applications.



Unshielded Twisted Pair

Shielded Twisted Pair (STP): This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference. It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



Shielded Twisted Pair

(ii) Coaxial Cable –

It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover. The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges). Cable TVs and analog television networks widely use Coaxial cables.

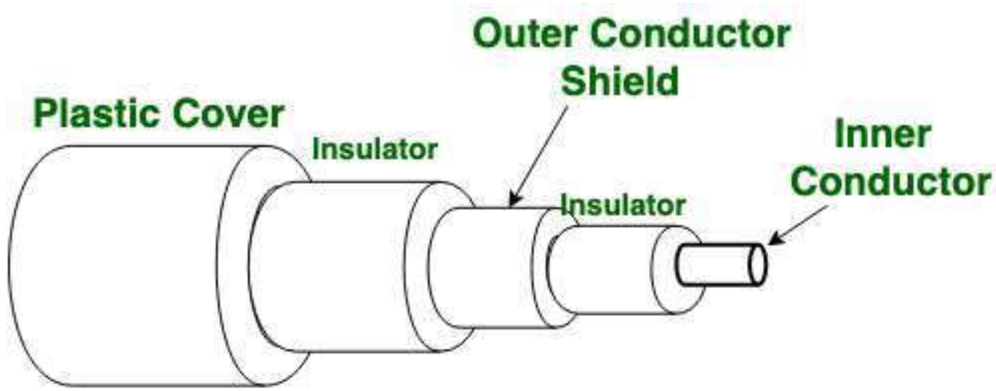
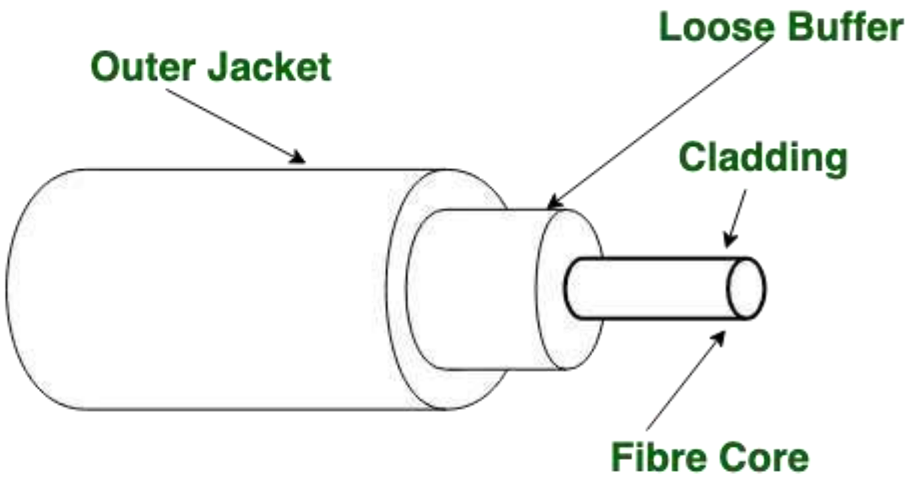


Figure of Coaxial Cable

(iii) Optical Fiber Cable – It uses the concept of reflection of light through a core made up of glass or plastic. The core is surrounded by a less dense glass or plastic covering called the cladding. It is used for the transmission of large volumes of data.

- The cable can be unidirectional or bidirectional. The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.



(iv) Stripline

- Stripline is a transverse electromagnetic (TEM) transmission line medium invented by Robert M. Barrett of the Air Force Cambridge Research Centre in the 1950s. Stripline is the earliest form of the planar transmission line. It uses a conducting material to transmit high-frequency waves it is also called a waveguide. This conducting material is sandwiched between two layers of the ground plane which are usually shorted to provide EMI immunity.

(v) Microstripline

- In this, the conducting material is separated from the ground plane by a layer of dielectric.

2. Unguided Media: It is also referred to as Wireless or Unbounded transmission media. No physical medium is required for the transmission of electromagnetic signals.

(i) Radio waves – These are easy to generate and can penetrate through buildings. The sending and receiving antennas need not be aligned. Frequency Range:3KHz – 1GHz. AM and FM radios and cordless phones use Radio waves for transmission.

(ii) Microwaves – It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

(iii) Infrared – Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

Protocols

In information technology, a protocol (from the Greek *protocollon*, which was a leaf of paper glued to a manuscript volume, describing its contents) is the special set of rules that end points in a telecommunication connection use when they communicate. Protocols exist at several levels in a telecommunication connection. For example, there are protocols for the data interchange at the hardware device level and protocols for data interchange at the application program level. In the standard model known as Open Systems Interconnection (OSI), there are one or more protocols attach layer in the telecommunication exchange that both ends of the exchange must recognize and observe. Protocols are often described in an industry or international standard.

Standards

A common set of rules.

Standards Organization

Standards creation Communities

IEEE (Institute of Electrical and Electronics Engineers)

IEEE's Constitution defines the purposes of the organization as "scientific and educational, directed toward the advancement of thetheory and practice of Electrical, Electronics, Communications and Computer Engineering, as well as Computer Science, the allied branches of engineering and the related arts and sciences." The IEEE is incorporated under the Not-for-Profit Corporation Law of the state of New York, United States. It was formed in 1963 by the merger of the Institute of Radio Engineers (IRE, founded 1912) and the American Institute of Electrical Engineers (AIEE, founded 1884). It has more than 400,000 members in more than 160 countries, 45% outside the United States.In pursuing these goals, the IEEE serves as a major publisher of scientific journals and a conference organizer. It is also a leading developer of industrial standards (having developed over 900 active industry standards) in a broad range of disciplines, including electric power and energy, biomedical technology and health care, information technology, information assurance, telecommunications, consumer electronics, transportation, aerospace, and nanotechnology. IEEE develops and participates in educational activities such as accreditation of electrical engineering programs in institutes of higherlearning.

IEEE is one of the leading standards-making organizations in the world. IEEE performs its standards making and maintaining functions through the IEEE Standards

Association (IEEE-SA). IEEE standards affect a wide range of industries including: power and energy, biomedical and health care, Information Technology (IT), telecommunications, transportation, nanotechnology, information assurance, and many more. In 2005, IEEE had close to 900 active standards, with 500 standards under development. One of the more notable IEEE standards is the IEEE 802 LAN/MAN group of standards which includes the IEEE 802.3 Ethernet standard and the IEEE 802.11 Wireless Networking standard.

ANSI (American National Standards Institute)

Though ANSI itself does not develop standards, the Institute oversees the development and use of standards by accrediting the procedures of standards developing organizations. ANSI accreditation signifies that the procedures used by standards developing organizations meet the Institute's requirements for openness, balance, consensus, and due process. ANSI was originally formed in 1918, when five engineering societies and three government agencies founded the American Engineering Standards Committee (AESC). In 1928, the AESC became the American Standards Association (ASA). In 1966, the ASA was reorganized and became the United States of America Standards Institute (USASI). The present name was adopted in 1969.Prior to1918, these five engineering societies:

- American Institute of Electrical Engineers (AIEE, now IEEE)
- American Society of Mechanical Engineers (ASME)
- American Society of Civil Engineers (ASCE)
- American Institute of Mining Engineers (AIME, now American Institute of Mining, Metallurgical, and Petroleum Engineers)
- American Society for Testing and Materials (now ASTM International)

ANSI also designates specific standards as American National Standards, or ANS, when the Institute determines that the standards were developed in an environment that is equitable, accessible and responsive to the requirements of various stakeholders.

The American National Standards process involves:

- consensus by a group that is open to representatives from allinterested parties
- broad-based public review and comment on draft standards
- consideration of and response to comments
- incorporation of submitted changes that meet the same consensusrequirements into a draft standard

- availability of an appeal by any participant alleging that these
principles were not respected during the standards-developmentprocess.

ITU (International Telecommunications Union - formerlyCCITT)

The **International Telecommunication Union** is the specialized agency of the United Nations which is responsible for information and communication technologies. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards.ITU also organizes worldwide and regional exhibitions and forums, such as ITU TELECOM WORLD, bringing together representatives of government and the telecommunications and ICT industry to exchange ideas, knowledge and technology.The ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks.

ISO (International Organization for Standards)

The **International Organization for Standardization** widely knownas **ISO**, is an international standard-setting body composed of representatives from various national standards organizations. Founded on February 23, 1947, the organization promulgates worldwide proprietary industrial and commercial standards. It has its headquarters in Geneva, Switzerland. While ISO defines itself as a non-governmental organization, its ability to set standards that oftenbecome law, either through treaties or national standards, makes it more powerful than most non-governmental organizations. In practice,ISO acts as a consortium with strong links to governments.

ISO, is an international standard-setting body composed of representatives from various national standards organizations the organization promulgates worldwide proprietary industrial and commercial standards.ISO's main products are the International Standards. ISO also publishes Technical Reports, Technical Specifications, Publicly Available Specifications, Technical Corrigenda,and Guides .

EIA (Electronic Industries Association)

The **Electronic Industries Alliance** (EIA, until 1997 *Electronic Industries Association*) was a standards and trade organization composed as an alliance of trade associations for electronics manufacturers in the United States. They developed standards to ensure the equipment of different manufacturers was compatible and interchangable.In 1924 the *Associated Radio Manufacturers* alliance was formed, which was renamed to *Radio Manufacturers Association (RMA)* the same year.

Upcoming new electronic technologies brought new members and further name changes: *Radio Television Manufacturers Association (RTMA)* (1950), *Radio Electronics Television Manufacturers (RETMA)* (1953) and *Electronics Industries Association (EIA)* (1957). The last renaming took place in 1997, when EIA became *Electronics Industries Alliance (EIA)*, reflecting the change away from a pure manufacturers associationA standard defining serial communication between computers and modems e. g. was originally drafted by the radio sector as RS-232. Later it was taken over by the EIA as *EIA-232*. Later this standard was managed by the TIA and the name was changed to the current *TIA-232*. Because the EIA was accredited by ANSI to help develop standards in its areas, the standards are often described as e. g. *ANSI TIA-232* (or formerly as*ANSI EIA/TIA-232')*.

ETSI (European Telecommunications StandardsInstitute)

The **European Telecommunications Standards Institute** (**ETSI**) is an independent, non-profit, standardization organization in the telecommunications industry (equipment makers and network operators) in Europe, with worldwide projection. ETSI has been successful in standardizing the Low Power Radio, Short Range Device,GSM cell phone system and the TETRA professional mobile radio system. Significant ETSI standardisation bodies include TISPAN (for fixed networks and Internetmachine-to-machine communications). ETSIinspired the creation of, and is a partner in 3GPP. ETSI was created by CEPT in 1988 and is officially recognized by theEuropean Commission and the EFTA secretariat. Based in Sophia Antipolis (France), ETSI is officially responsible for standardization ofInformation and Communication Technologies (ICT) within Europe.

These technologies include telecommunications, broadcasting and related areas such as intelligent transportation and medical electronics.ETSI has 740 members from 62 countries/provinces inside and outside Europe, including manufacturers, network operators, administrations, service providers, research bodies and users — in fact, all the key players in the ICT arena. convergence) and M2M (for ETSI has been successful in standardizing the Low Power Radio, Short Range Device, GSMTETRA professional mobile radio system.ETSI was created by CEPTin 1988 and is officially recognized by the European Commission and the EFTASophia Antipolis (France), ETSI is officially responsible for standardization of Information and Communication Technologies (ICT) within Europe. These technologies include telecommunications, broadcasting and related areas such as intelligent transportation andmedical electronics.

W3C - World Wide Web Consortium

The **World Wide Web Consortium** (**W3C**) is the main international standards organizationWorld Wide Web (abbreviated WWW or W3). Founded and headed by Tim Berners-Lee,the consortium is made up of member organizations which maintain full-time staff for the purpose of working together in the development of standards for the

World Wide Web. As of 18 February 2011, the World Wide Web Consortium (W3C) has 322 members. W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web. W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web.W3C was created to ensure compatibility and agreement among industry members in the adoption of new standards. Prior to its creation, incompatible versions of HTML were offered by different vendors, increasing the potential for inconsistency between web pages. The consortium was created to get all those vendors to agree on a set ofcore principles and components which would be supported by everyone.

INTERNET HISTORY

Now that we have given an overview of the Internet, let us give a brief history of the internet. This brief history makes it clear how the Internet has evolved from a private network to a global one in less than 40 years.

Early History

There were some communication networks, such as telegraph and telephone networks, before 1960. These networks were suitable for constant-rate communication at that time, which means that after a connection was made between two users, the encoded message (telegraphy) or voice (telephony) could be exchanged.

ARPANET

In the mid-1960s, mainframe computers in research organizations were stand-alone devices. Computers from different manufacturers were unable to communicate with one another. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DOD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort. In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for the Advanced Research Projects Agency Network (ARPANET), a small network of connected computers. The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an interface message processor (IMP). The IMPs, in turn, would be connected to each other. Each IMP had to be able to communicate with other IMPs as well as with its own attached host.

Birth of the Internet

In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internet ting Project. TCPI/P Cerf and Kahn's landmark 1973 paper outlined the protocols to achieve end-to-end delivery of data. This was a new version of NCP. This paper on transmission control protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway. Transmission Control Protocol (TCP) and Internet Protocol (IP). IP would handle datagram routing while TCP would be responsible for higher level functions such as segmentation, reassembly, and error detection. The new combination became known as TCPIIP.

MILNET

In 1983, ARPANET split into two networks: Military Network (MILNET) for military users and ARPANET for non military users.

CSNET

Another milestone in Internet history was the creation of CSNET in 1981. Computer Science Network (CSNET) was a network sponsored by the National Science Foundation (NSF).

NSFNET

With the success of CSNET, the NSF in 1986 sponsored the National Science Foundation Network (NSFNET), a backbone that connected five supercomputer centers located throughout the United States.

ANSNET

In 1991, the U.S. government decided that NSFNET was not capable of supporting the rapidly increasing Internet traffic. Three companies, IBM, Merit, and Verizon, filled the void by forming a nonprofit organization called Advanced Network & Services (ANS) to build a new, high-speed Internet backbone called Advanced Network Services Network (ANSNET).

Internet Today

Today, we witness a rapid growth both in the infrastructure and new applications. The Internet today is a set of pier networks that provide services to the whole world. What has made the internet so popular is the invention of new applications.

World Wide Web

The 1990s saw the explosion of Internet applications due to the emergence of the World Wide Web (WWW). The Web was invented at CERN by Tim Berners-Lee. This invention has added the commercial applications to the Internet.

Multimedia

Recent developments in the multimedia applications such as voice over IP (telephony), video over IP (Skype), view sharing (YouTube), and television over IP (PPLive) has increased the number of users and the amount of time each user spends on the network.

STANDARDS AND ADMINISTRATION

In the discussion of the Internet and its protocol, we often see a reference to a standard or an administration entity. In this section, we introduce these standards and administration entities for those readers that are not familiar with them; the section can be skipped if the reader is familiar with them.

INTERNET STANDARDS

An Internet standard is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An Internet draft is a working document (a work in progress) with no official status and a six-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a Request for Comment (RFC). Each RFC is edited, assigned a number, and made available to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level.

Maturity Levels

An RFC, during its lifetime, falls into one of six maturity levels: proposed standard, draft standard, Internet standard, historic, experimental, and informational. A proposed standard is a specification that is stable, well understood, and of sufficient interest to the Internet community. At this level, the specification is usually tested and implemented by several different groups.

Draft Standard.

A proposed standard is elevated to draft standard status after at least two successful independent and interoperable implementations. Barring difficulties, a draft standard, with modifications if specific problems are encountered, normally becomes an Internet standard.

Internet Standard

A draft standard reaches Internet standard status after demonstrations of successful implementation.

Historic

The historic RFCs are significant from a historical perspective. They either have been superseded by later specifications or have never passed the necessary maturity levels to become an Internet standard.

Experimental

An RFC classified as experimental describes work related to an experimental situation that does not affect the operation of the Internet. Such an RFC should not be implemented in any functional Internet service.

Informational

An RFC classified as informational contains general, historical, or tutorial information related to the Internet. It is usually written by someone in a non-Internet organization, such as a vendor.

Requirement Levels

RFCs are classified into five requirement levels: required, recommended, elective, limited use, and not recommended.

Required

An RFC is labeled required if it must be implemented by all Internets systems to achieve minimum conformance. For example, IF and ICMP are required protocols.

Recommended

An RFC labeled recommended is not required for minimum conformance; it is recommended because of its usefulness. For example, FTP and TELNET are recommended protocols.

Elective

An RFC labeled elective is not required and not recommended. However, a system can use it for its own benefit.

Limited Use

An RFC labeled limited use should be used only in limited situations. Most of the experimental RFCs fall under this category.

Not Recommended

An RFC labeled not recommended is inappropriate for general use. Normally a historic (deprecated) RFC may fall under this category.

INTERNET ADMINISTRATION

The Internet, with its roots primarily in the research domain, has evolved and gained a broader user base with significant commercial activity. Various groups that coordinate Internet issues have guided this growth and development. Appendix G gives the addresses, e-rnail addresses, and telephone numbers for some of these groups. E-rnail addresses and telephone numbers for some of these groups.

Isoc

The Internet Society (ISOC) is an international, nonprofit organization formed in 1992 to provide support for the Internet standards process. ISOC accomplishes this through maintaining and supporting other Internet administrative bodies such as lAB, IETF,IRTF, and IANA (see the following sections). ISOC also promotes research and other scholarly activities relating to the Internet.

lAB

The Internet Architecture Board (lAB) is the technical advisor to the ISOC. The main purposes of the lAB are to oversee the continuing development of the TCP/IP Protocol Suite and to serve in a technical advisory capacity to research members of the Internet community. lAB accomplishes this through its two primary components, the Internet Engineering Task Force (IETF) and the Internet Research Task Force (IRTF). Another responsibility of the lAB is the editorial management of the RFCs, described earlier. lAB is also the external liaison between the Internet and other standards organizations and forums.

JETF

The Internet Engineering Task Force (IETF) is a forum of working groups managed by the Internet Engineering Steering Group (IESG). IETF is responsible for identifying operational problems and proposing solutions to these problems. IETF also develops and reviews specifications intended as Internet standards. The working groups are collected into areas, and each area concentrates on a specific topic. Currently nine areas have been defined. The areas include applications, protocols, routing, network management next generation (lPng), and security.

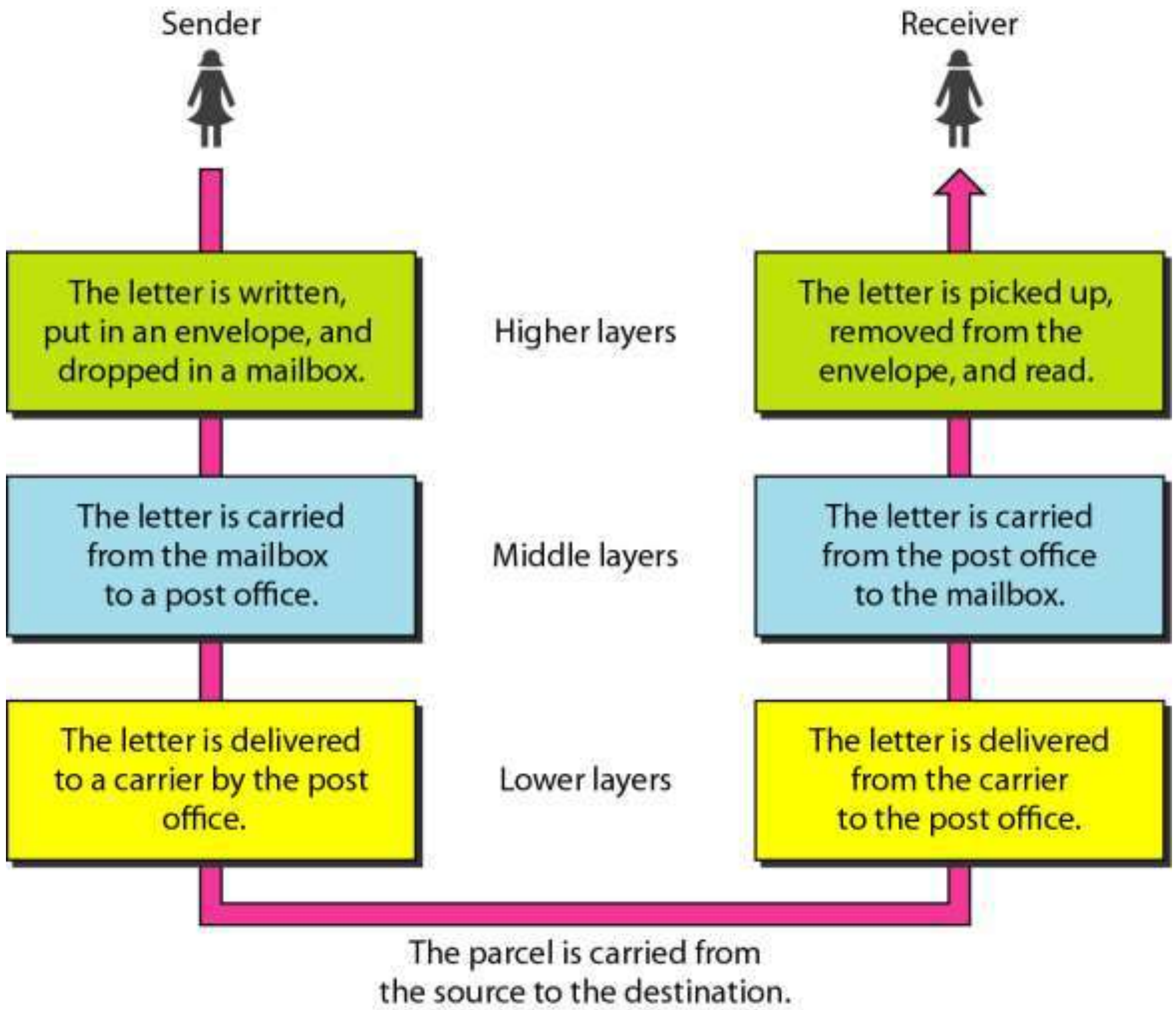
JRTF

The Internet Research Task Force (IRTF) is a forum of working groups managed by the Internet Research Steering Group (IRSG). IRTF focuses on long-term research topics related to Internet protocols, applications, architecture, and technology.

LAYERING SCENARIO

We use the concept of layers in our daily life. As an example, let us consider two friends who communicate through postal mail. The process of sending a letter to a friend would be complex if there were no services available from the post office.

Tasks involved in sending a letter



Principles of Protocol Layering

First Principle

The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction. For example, the third layer task is to listen (in one direction) and talk (in the other direction). The second layer needs to be able to encrypt and decrypt. The first layer needs to send and receive mail.

Second Principle

The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical. For example, the object under layer 3 at both sites should be a plaintext letter. both sites should be a cipher text letter. The object under layer 1 at both sites should be a piece of mail.

Logical Connections

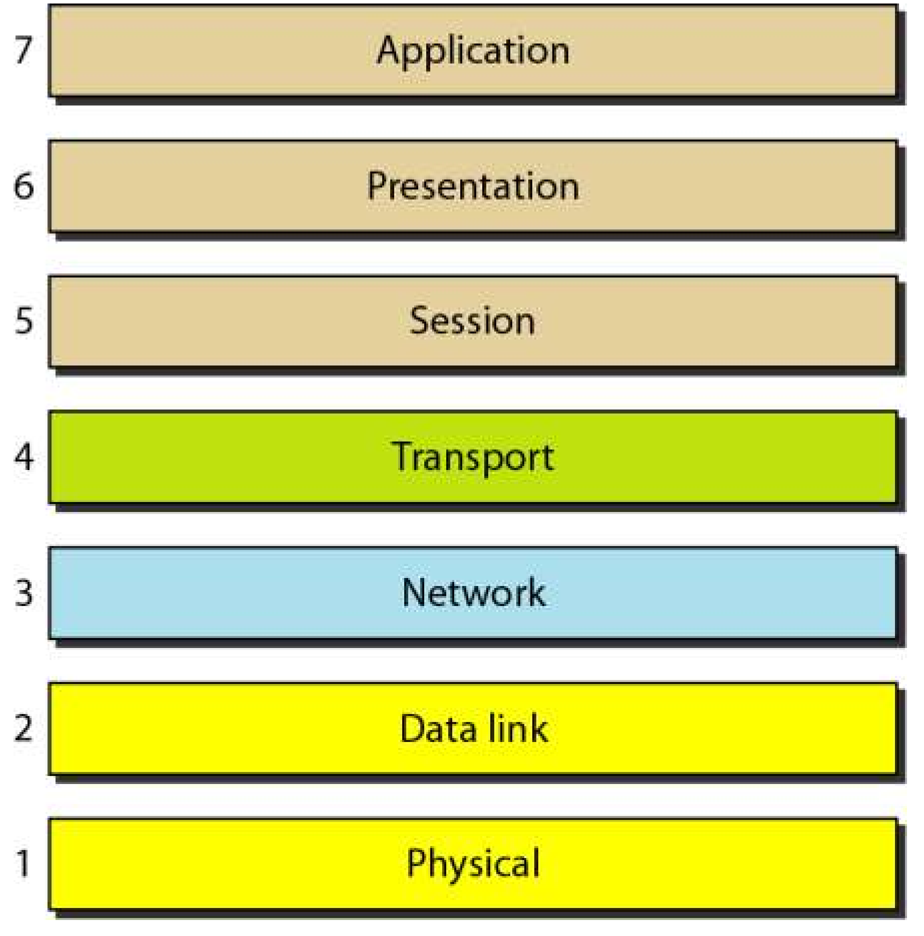
After following the above two principles, we can think about logical connection between each layer as shown in below figure. This means that we have layer-to-layer communication. Maria and Ann can think that there is a logical (imaginary) connection at each layer through which they can send the object created from that layer. We will see that the concept of logical connection will help us better understand the task of layering. We encounter in data communication and networking.

THE OSI MODEL

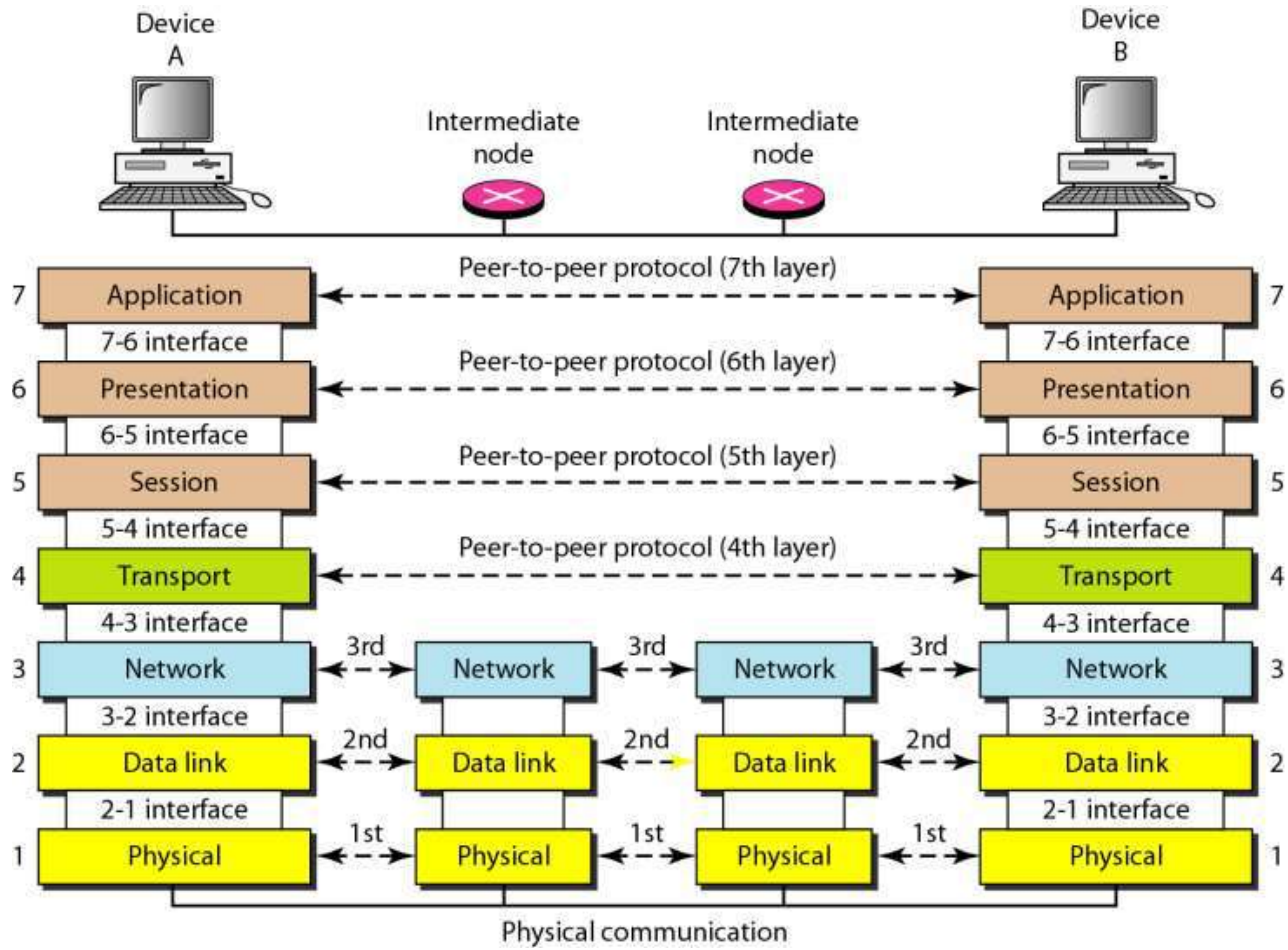
Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards. An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

ISO is the organization.
OSI is the model.

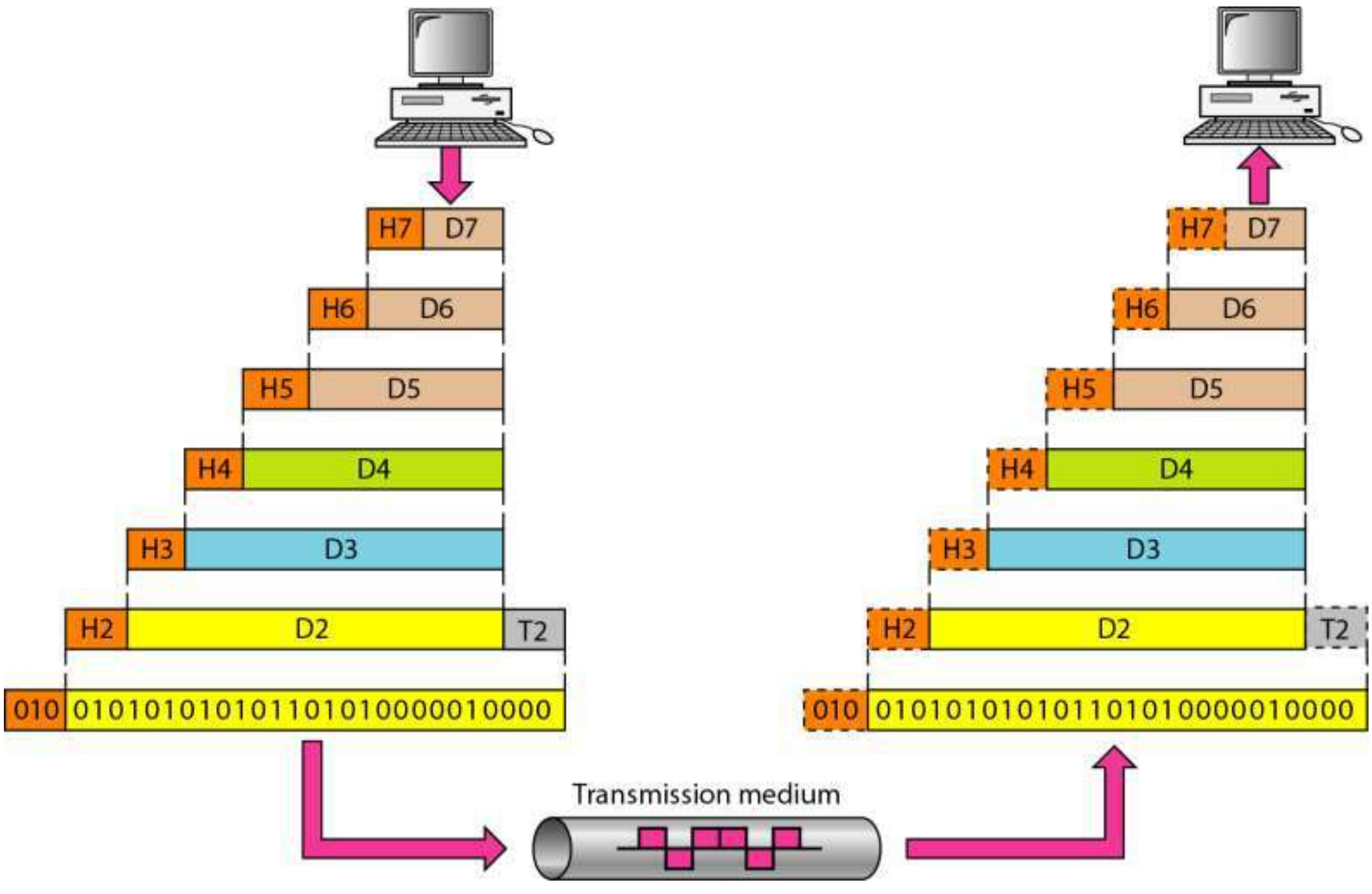
Seven layers of the OSI model



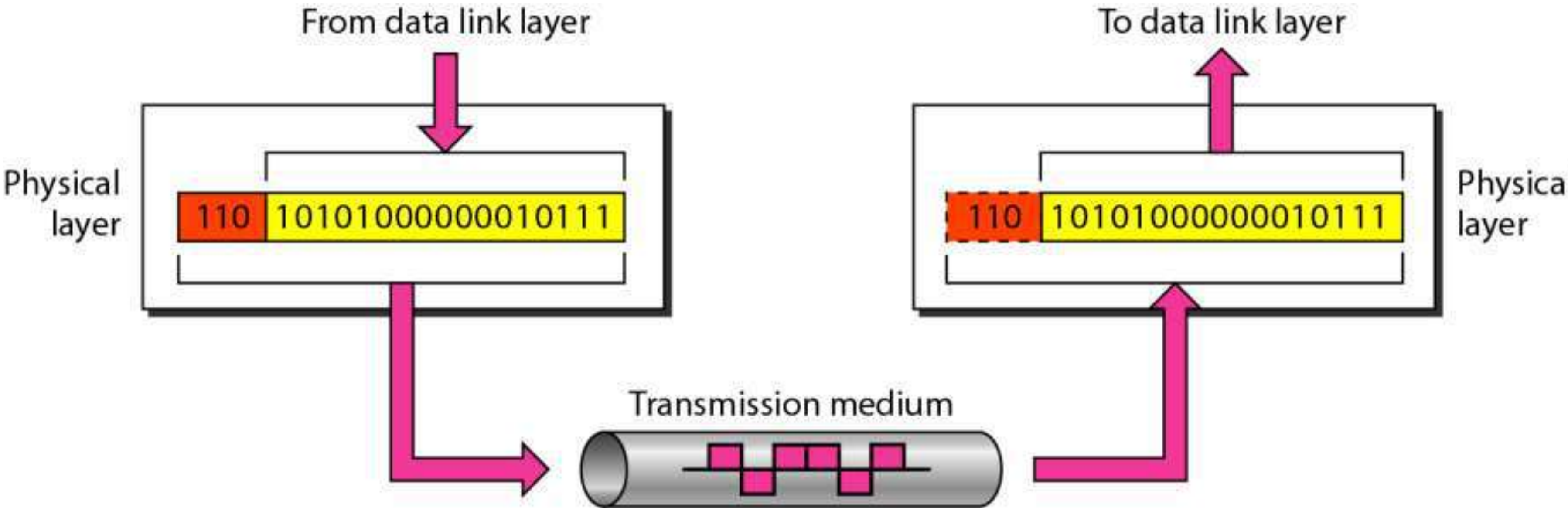
The interaction between layers in the OSI model



An exchange using the OSI model



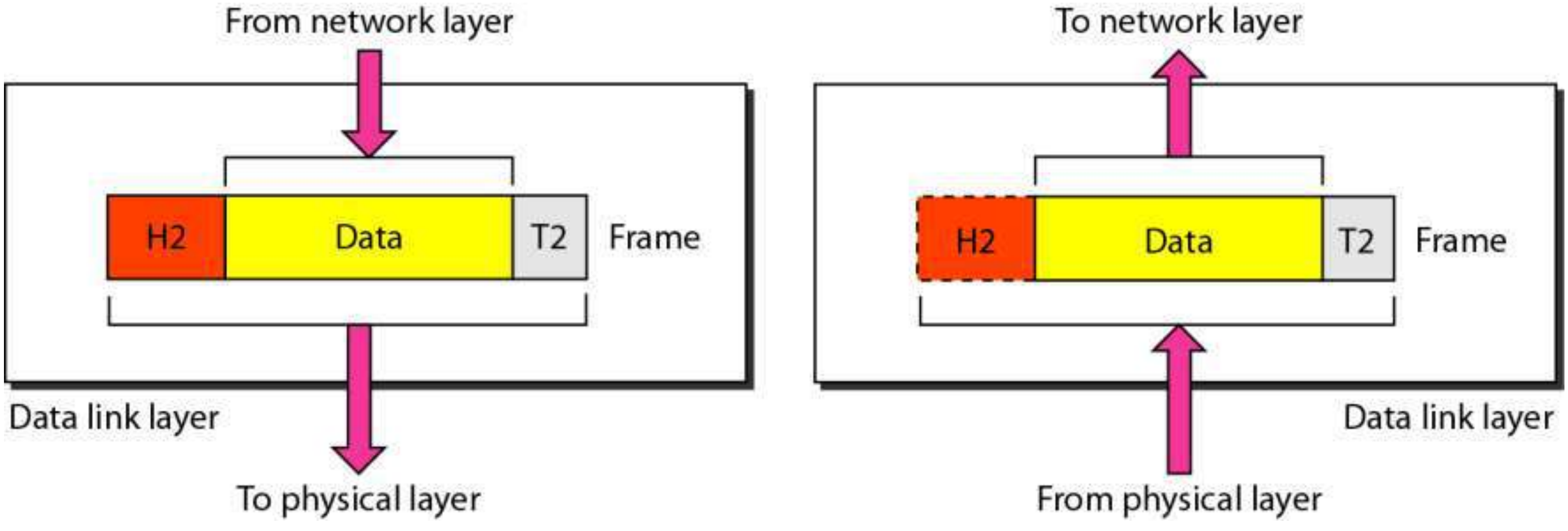
Physical layer



Note

•The physical layer is responsible for movements of individual bits from one hop (node) to the next.
Physical Characteristics of interfaces&medium
•Representation of bit
•Data rate
•Synchronization
•Line of configuration
•Physical topology
•Transmission Mode

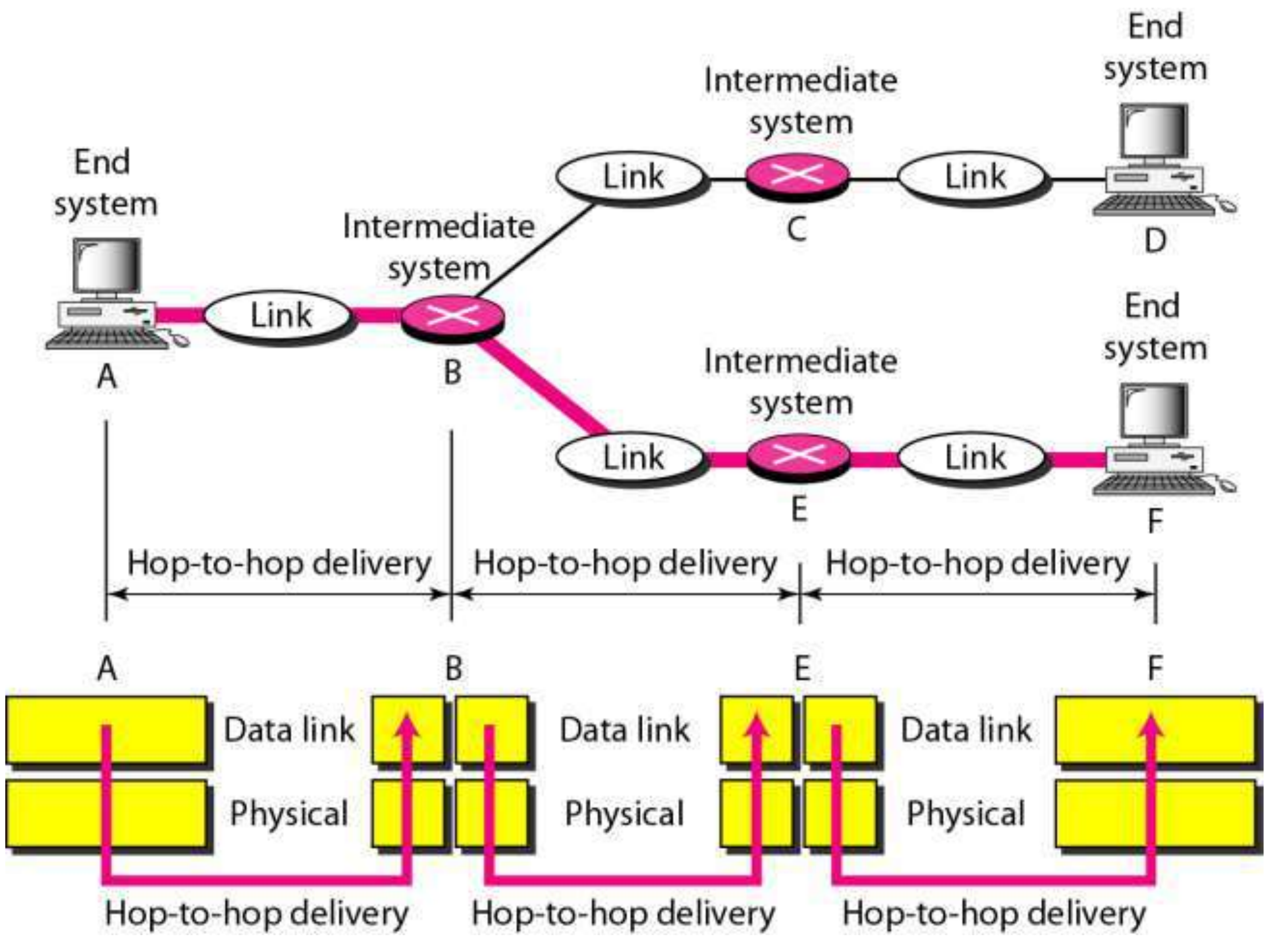
Data link layer



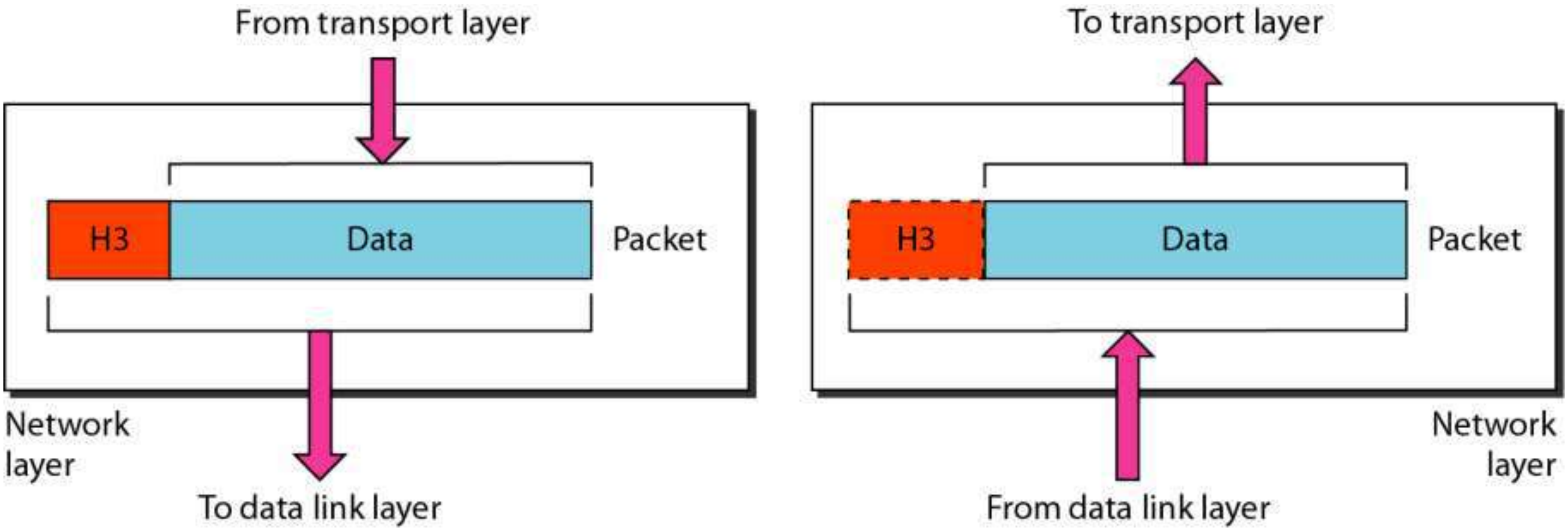
Note

- The data link layer is responsible for moving frames from one hop (node) to the next.
- Framing
- Physical addressing
- Flow Control
- Error Control
- Access Control

Hop-to-hop delivery



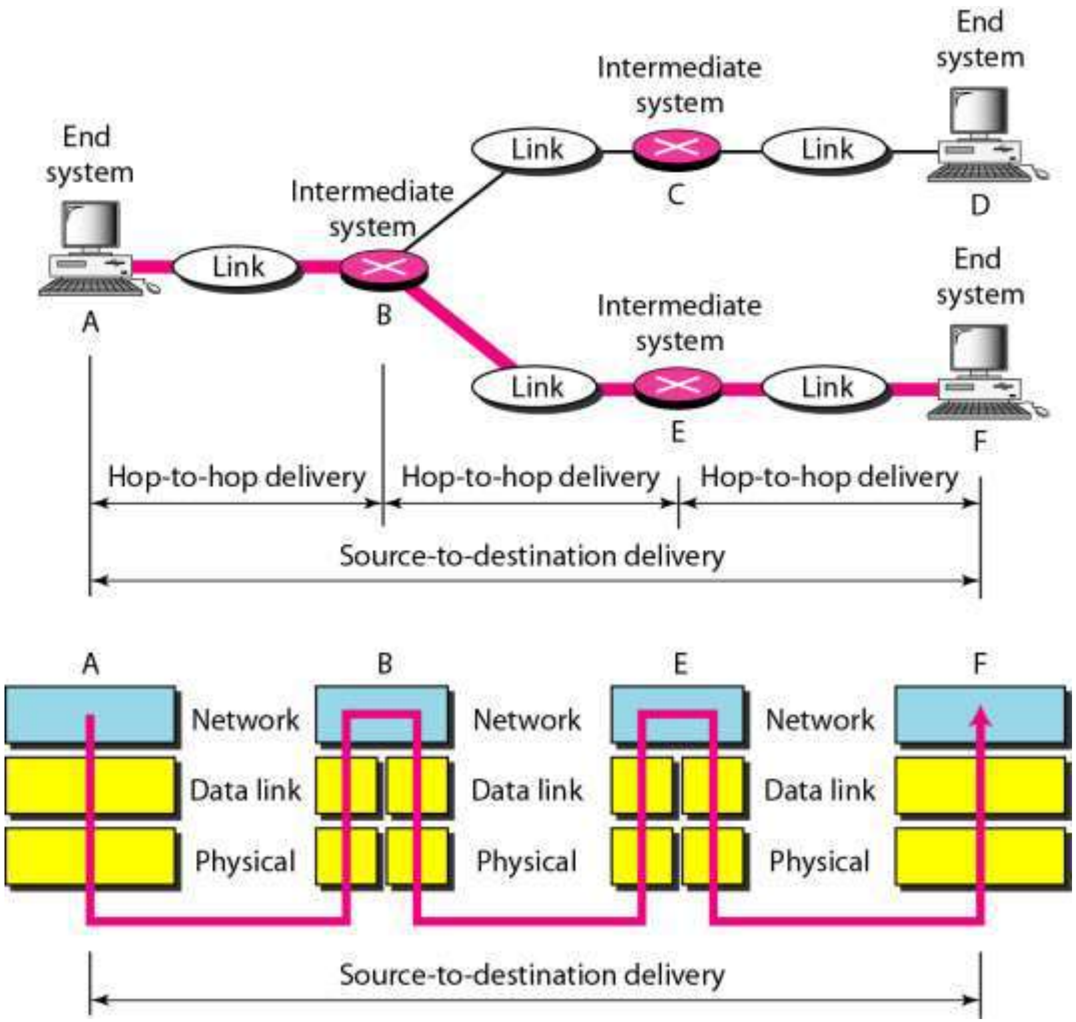
Network layer



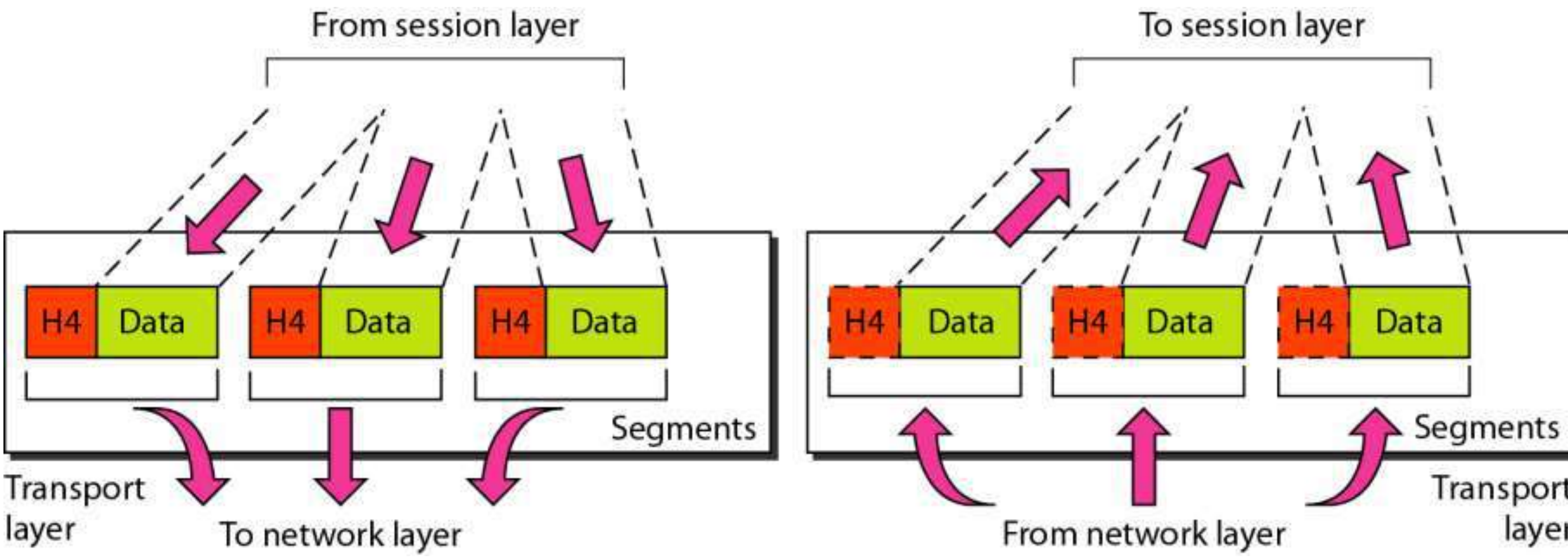
Note

- **The network layer is responsible for the delivery of individual packets from the source host to the destination host.**
- **Logical Addressing**
- **Routing**

Source-to-destination delivery



Transport layer



Note

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

•Service-point addressing

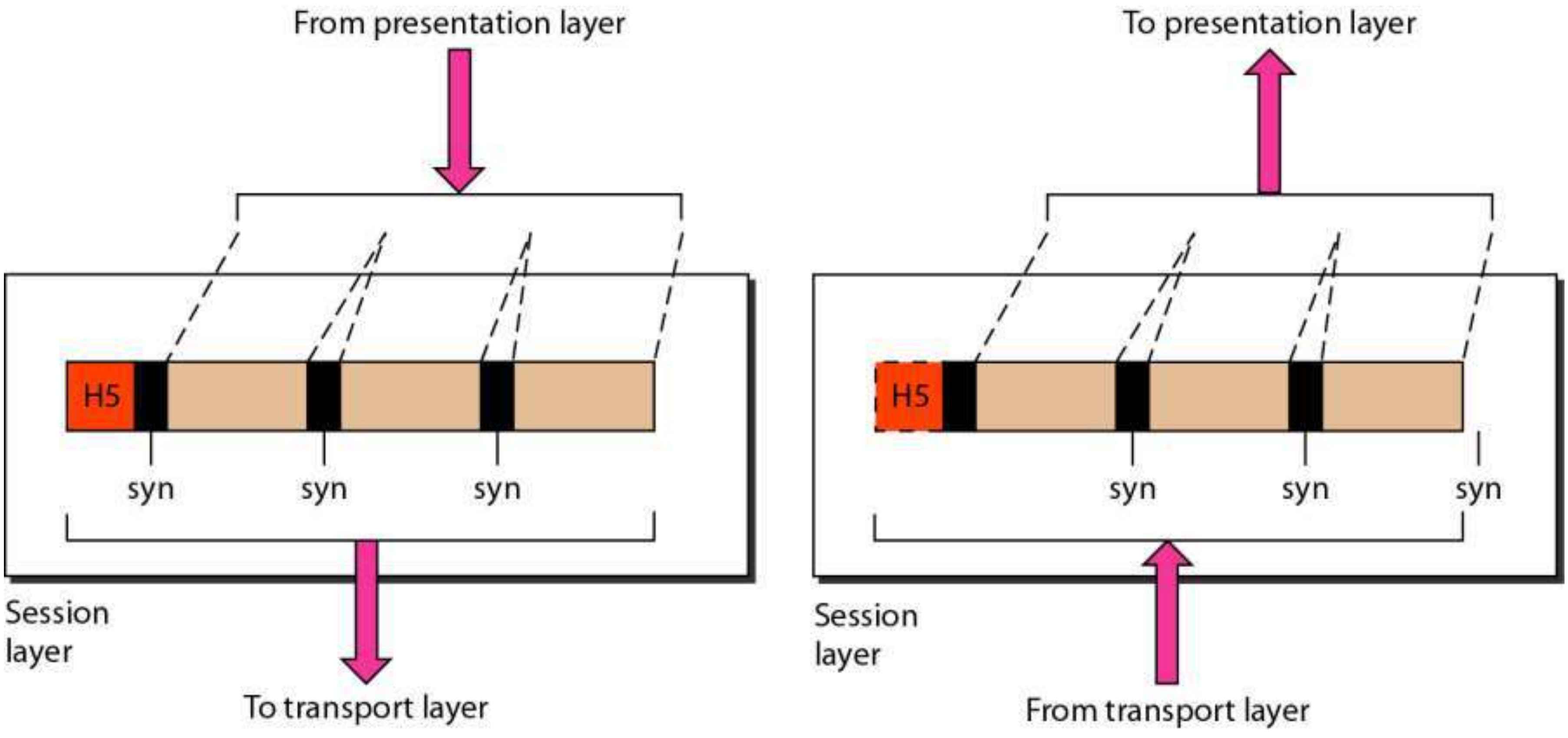
•Segmentation and reassembly

•Connection Control

•Flow Control

•Error control

Session layer



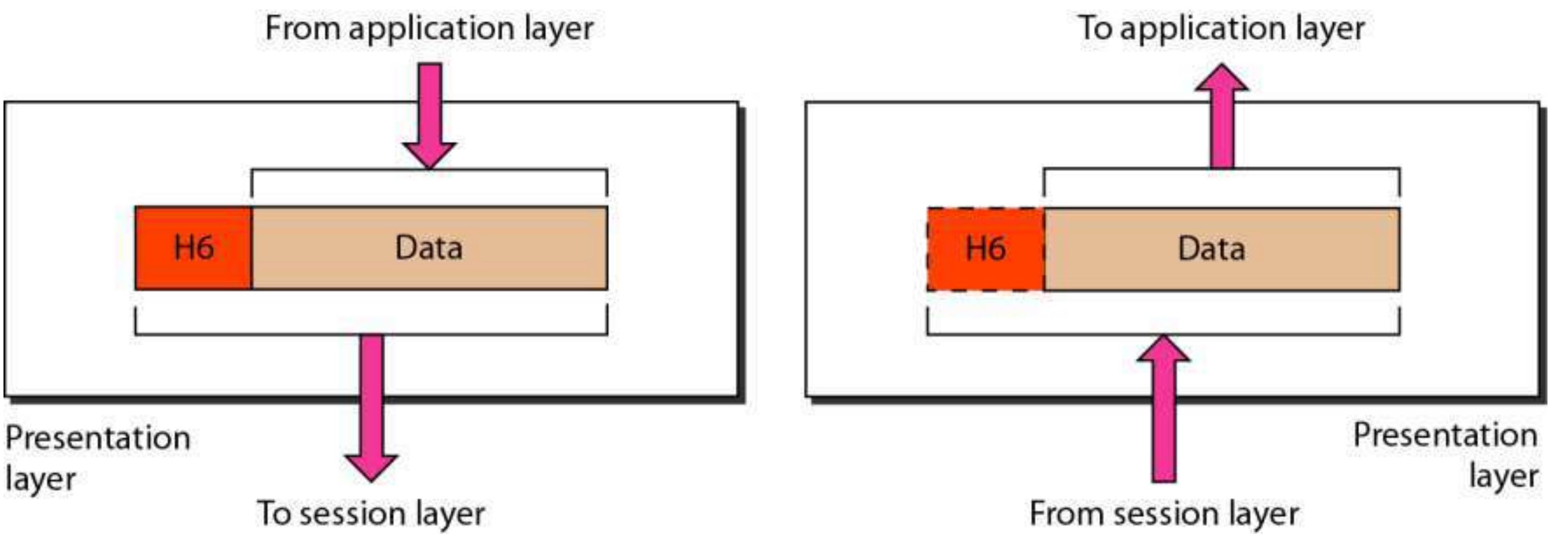
Note

The session layer is responsible for dialog control and synchronization.

Session layer

- The session layer defines how to start, control and end conversations (called sessions) between applications.
- This includes the control and management of multiple bi-directional messages using dialogue control.
- It also synchronizes dialogue between two hosts' presentation layers and manages their data exchange.
- The session layer offers provisions for efficient data transfer.

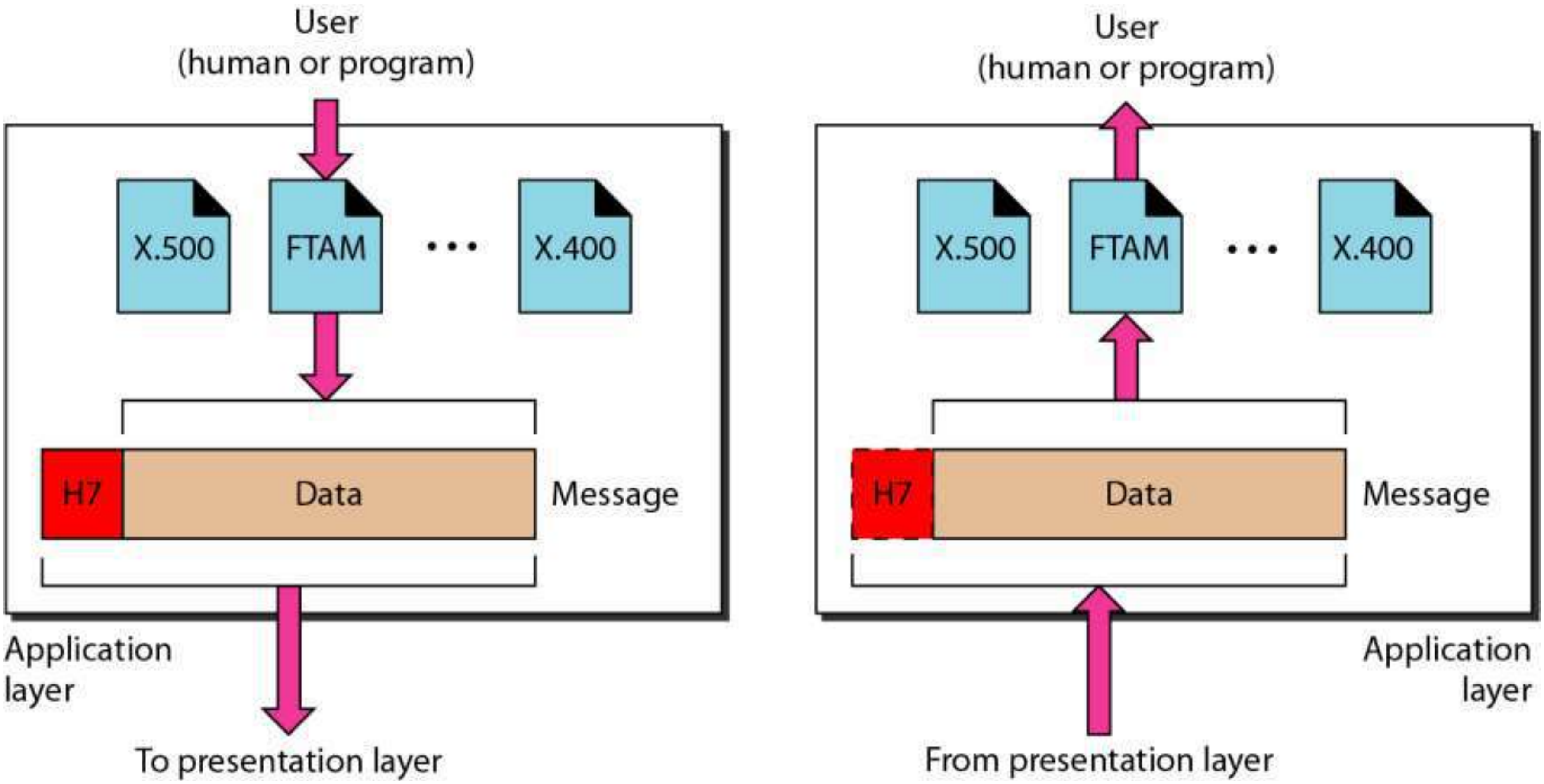
Presentation layer



Note

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

Application layer



Note

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

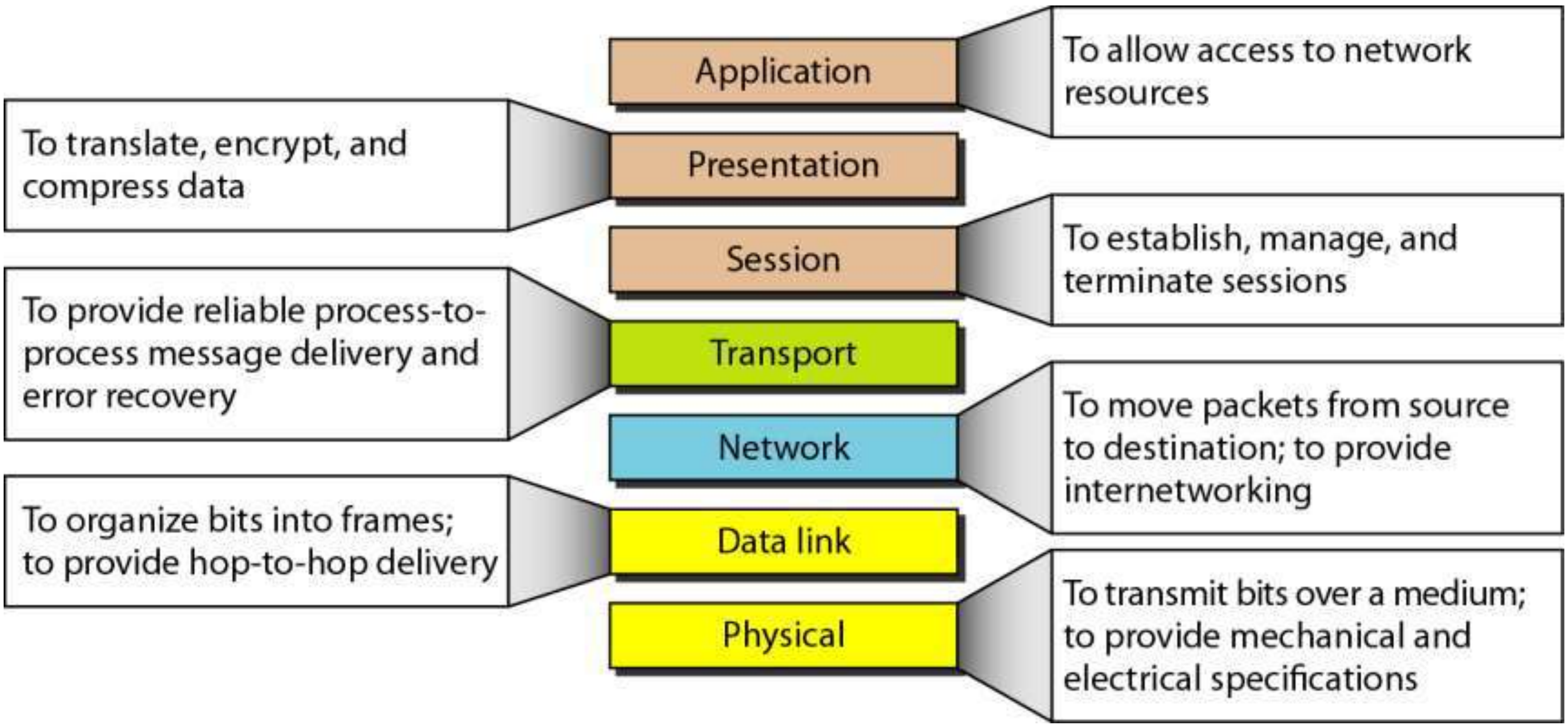
Network virtual terminal

File transfer and access , management

Mail services

Directory services

Summary of OSI layers

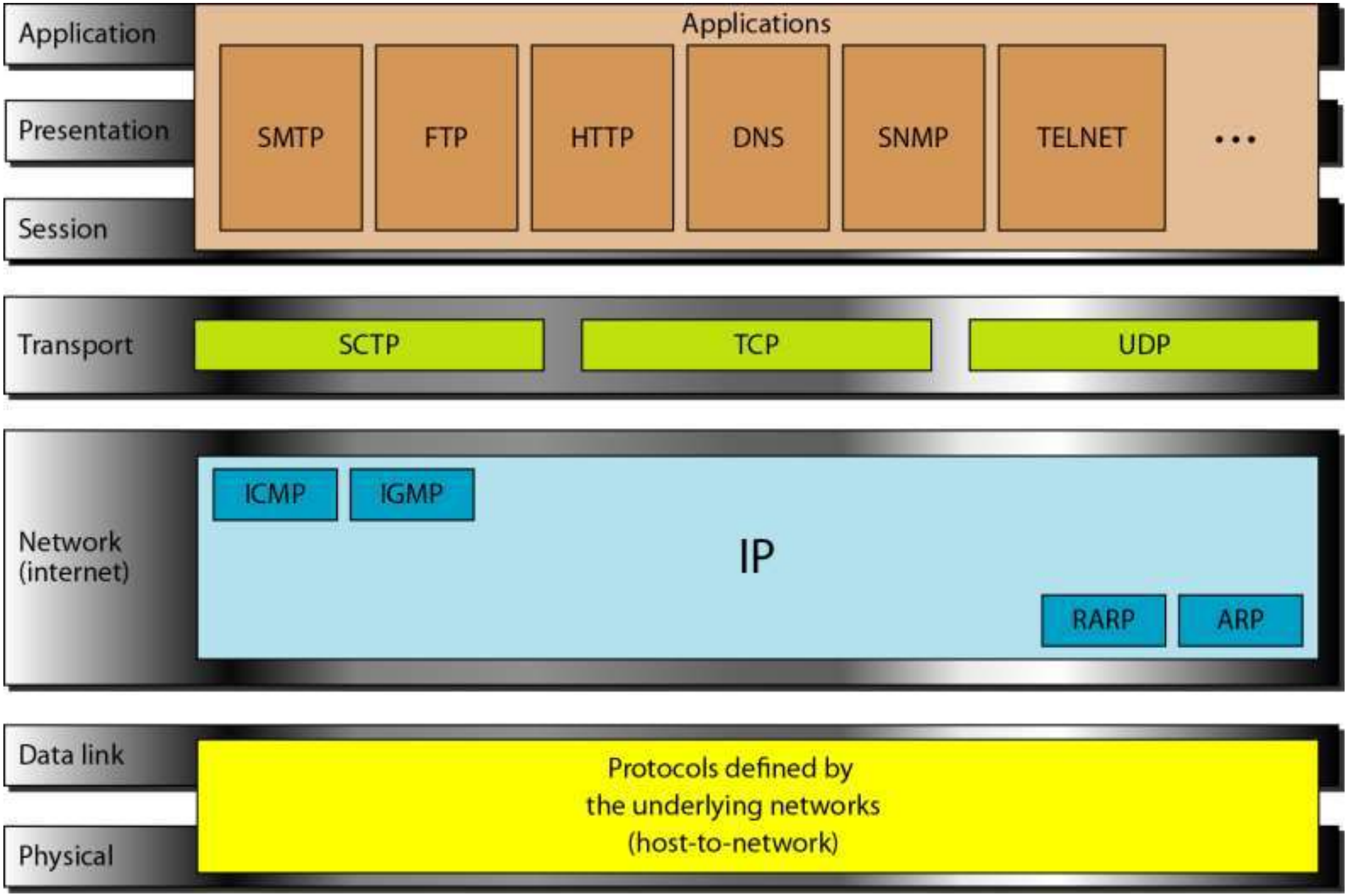


TCP/IP PROTOCOL SUITE

The layers in the TCP/IP protocol suite do not exactly match those in the OSI model. The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application. However, when TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers:

physical,
data link,
network,
transport,
application.

TCP/IP and OSI model



Network layer

At the network layer TCP/IP , supports the internetworking protocol(IP).in turn it uses four supporting protocols: ARP,RARP,ICMP,IGMP.

Address Resolution Protocol(ARP):

It is used to associate a logical address with a physical address. It is used to find the physical address of the node when its internet address is known.

Reverse Address Resolution Protocol(RARP):

It allows a host to discover its internet address when it knows only its physical address.

Internet Control Message Protocol(ICMP): Is a mechanism used by hosts and gateways to send notification of datagram problems.

Internet Group Message Protocol(IGMP): Is used to facilitate the simultaneous transmission of a message to a group of rcipients.

Transport layer:
UDP and TCP are transport level protocols responsible for delivery of a message from process to process.

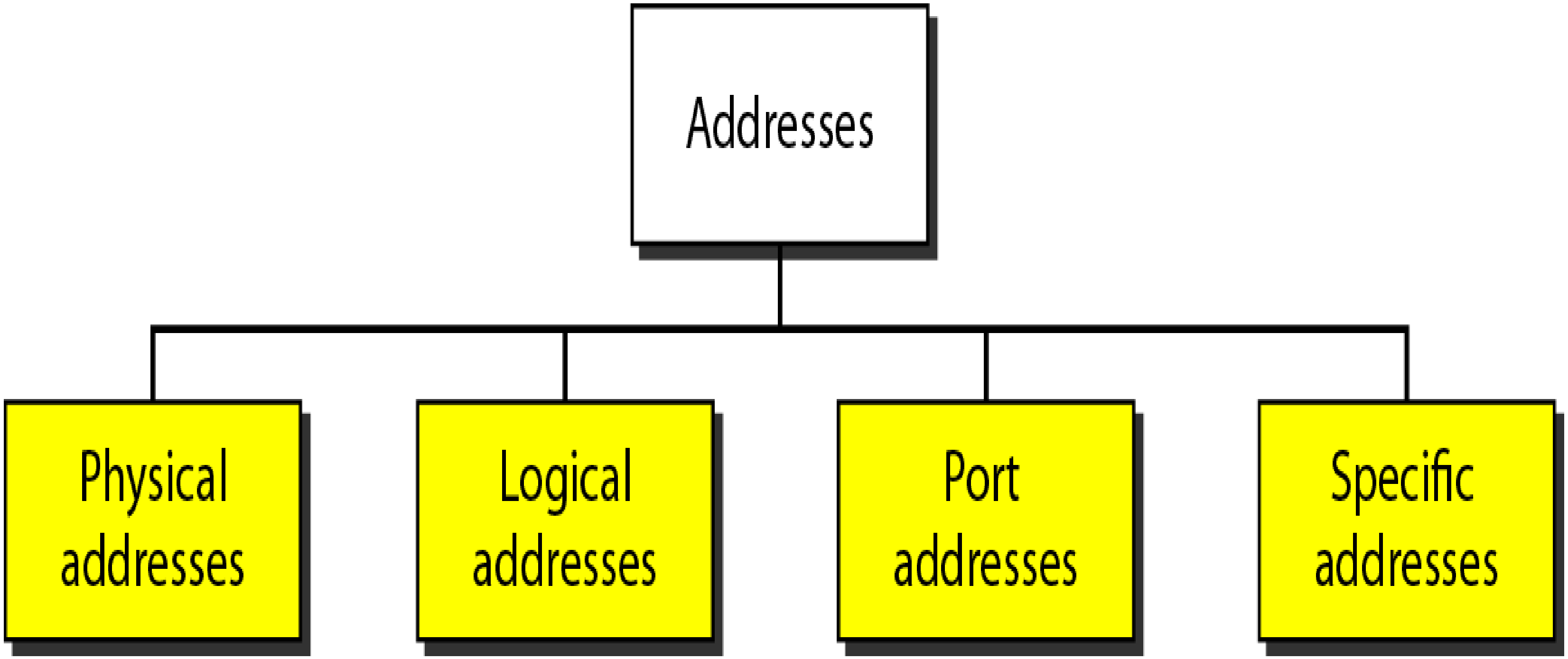
User Datagram Protocol(UDP): It is a process-to process protocol that adds only port address, checksum, error control and length information .

Transmission Control Protocol(TCP): It provides full transport layer services to applications. It collects each data gram as it comes in and reorders the transmission based on sequence numbers.

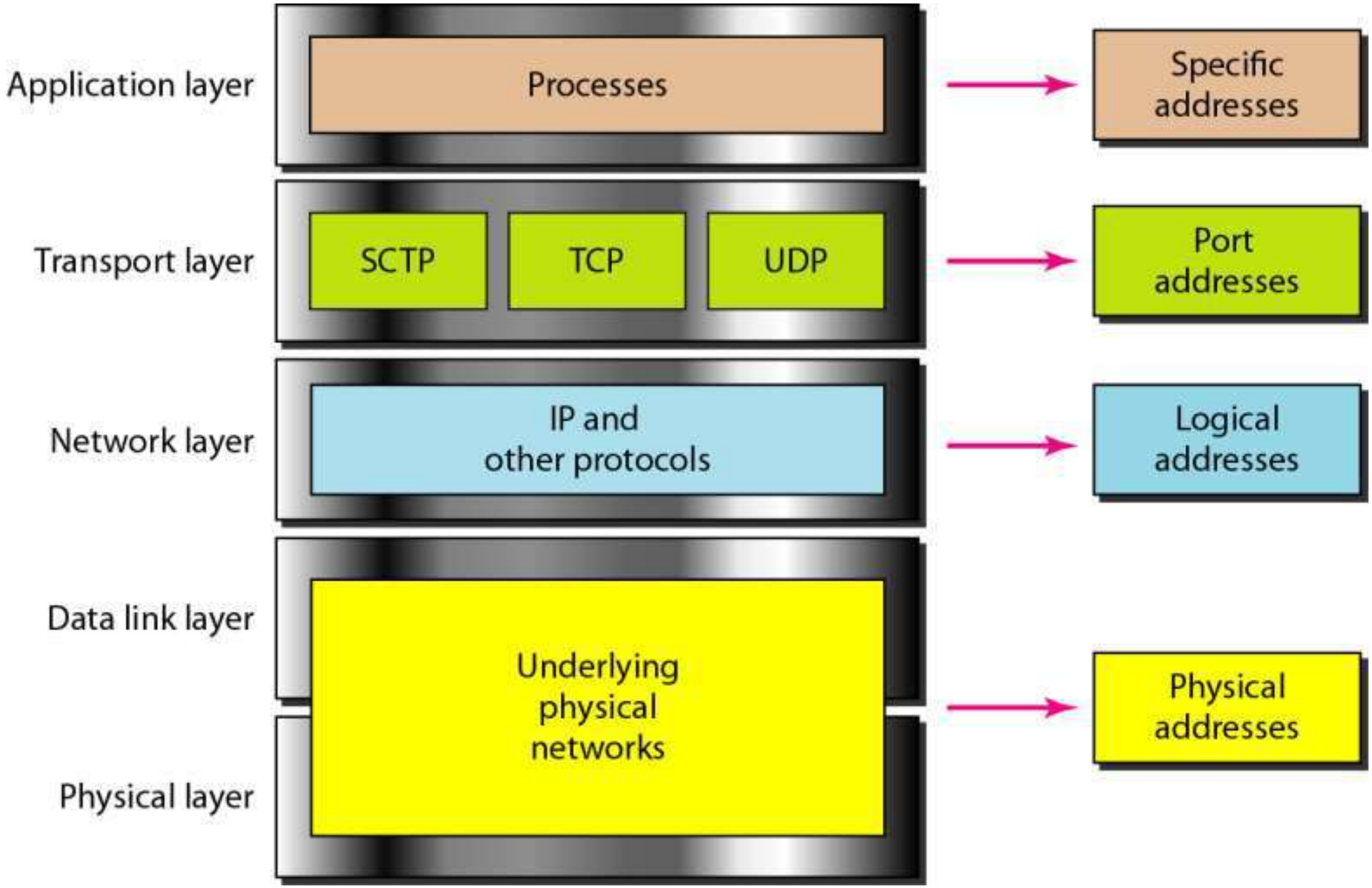
Stream Control Transmission Protocol(SCTP): It provides support for newer applications such as voice over to internet.

ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.



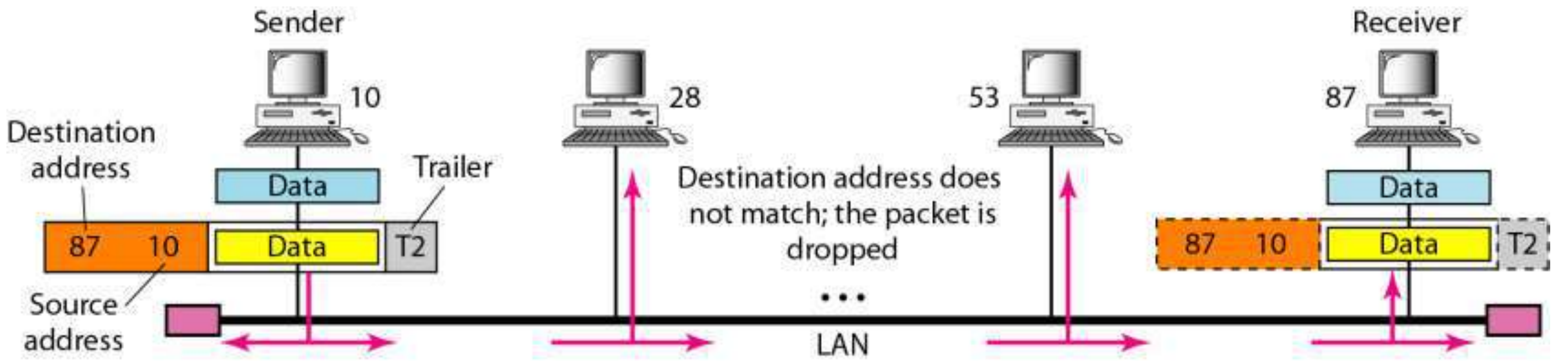
Relationship of layers and addresses in TCP/IP



Example 2.1

In Figure 2.19 a node with physical address 10 sends a frame to a node with physical address 87. The two nodes are connected by a link (bus topology LAN). As the figure shows, the computer with physical address 10 is the sender, and the computer with physical address 87 is the receiver.

Figure 2.19 *Physical addresses*



Example 2.2

Most local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:

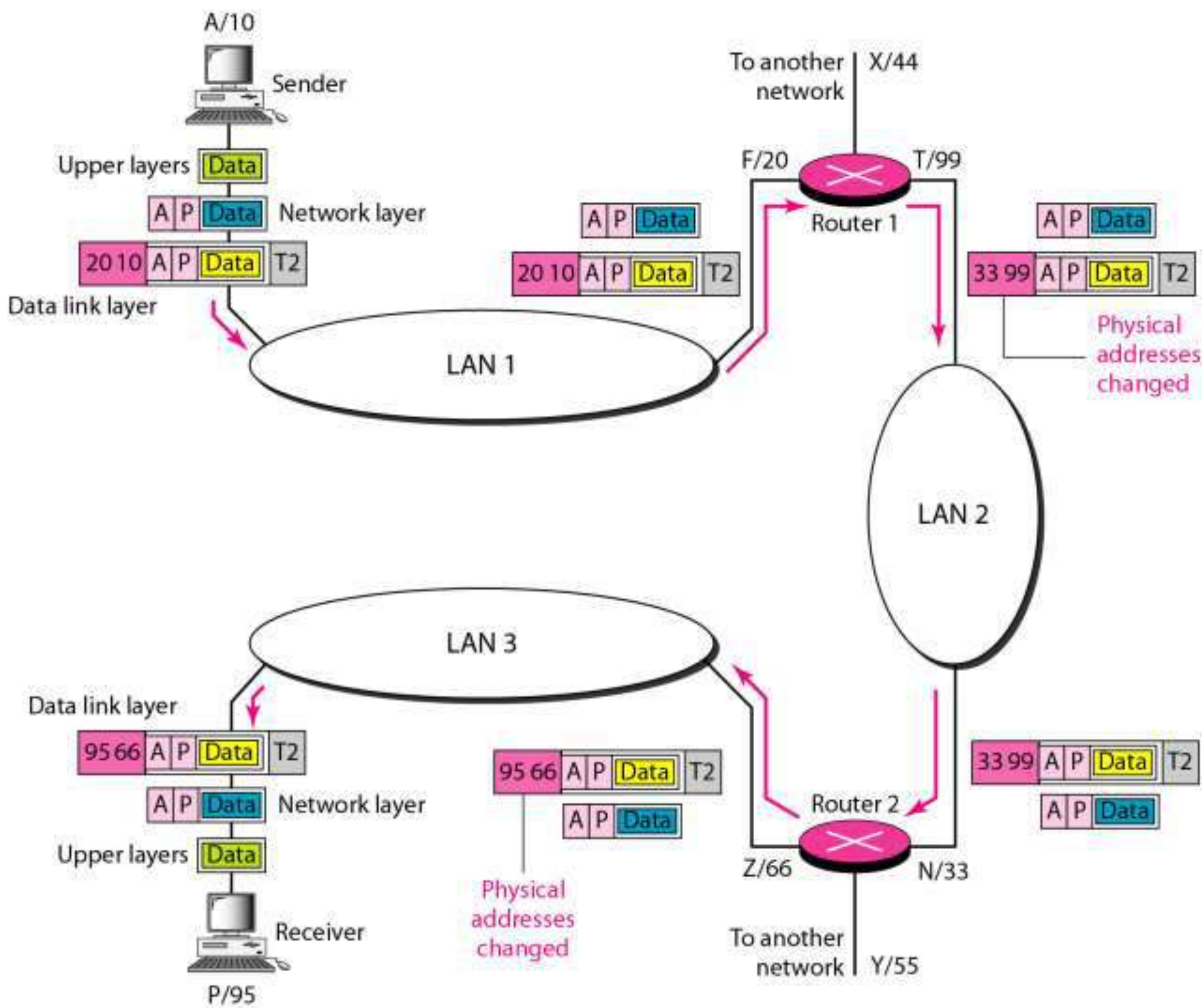
07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.

Example 2.3

Figure 2.20 shows a part of an internet with two routers connecting three LANs. Each device (computer or router) has a pair of addresses (logical and physical) for each connection. In this case, each computer is connected to only one link and therefore has only one pair of addresses. Each router, however, is connected to three networks (only two are shown in the figure). So each router has three pairs of addresses, one for each connection.

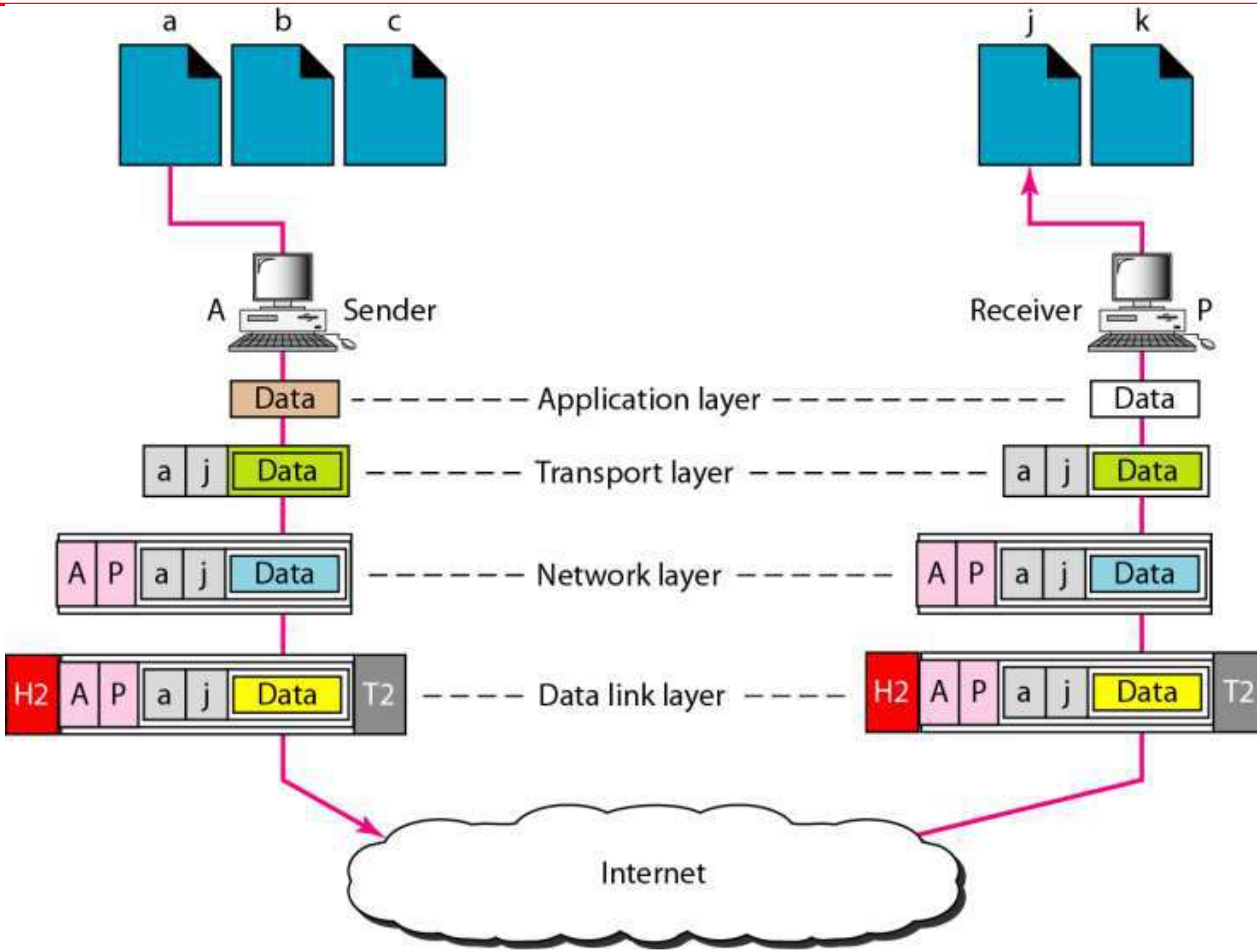
Figure 2.20 *IP addresses*



Example 2.4

Figure 2.21 shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses a, b, and c. The receiving computer is running two processes at this time with port addresses j and k. Process a in the sending computer needs to communicate with process j in the receiving computer. Note that although physical addresses change from hop to hop, logical and port addresses remain the same from the source to destination.

Figure 2.21 *Port addresses*



Note

The physical addresses will change from hop to hop, but the logical addresses usually remain the same.

Example 2.5

A port address is a 16-bit address represented by one decimal number as shown.

753 **A 16-bit port address represented as one single number.**

OSI Model	TCP/IP Model
It stands for **Open System Interconnection.**	It stands for **Transmission Control Protocol.**
OSI model has been developed by ISO (International Standard Organization).	It was developed by ARPANET (Advanced Research Project Agency Network).
It is an independent standard and generic protocol used as a communication gateway between the network and the end user.	It consists of standard protocols that lead to the development of an internet. It is a communication protocol that provides the connection among the hosts.
In the OSI model, the transport layer provides a guarantee for the delivery of the packets.	The transport layer does not provide the surety for the delivery of packets. But still, we can say that it is a reliable model.
This model is based on a vertical approach.	This model is based on a horizontal approach.
In this model, the session and presentation layers are separated, i.e., both the layers are different.	In this model, the session and presentation layer are not different layers. Both layers are included in the application layer.
It is also known as a reference model through which various networks are built. For example, the TCP/IP model is built from the OSI model. It is also referred to as a guidance tool.	It is an implemented model of an OSI model.
In this model, the network layer provides both connection-oriented and connectionless service.	The network layer provides only connectionless service.
Protocols in the OSI model are hidden and can be easily replaced when the technology changes.	In this model, the protocol cannot be easily replaced.
It consists of 7 layers.	It consists of 4 layers.
OSI model defines the services, protocols, and interfaces as well as provides a proper distinction between them. It is protocol independent.	In the TCP/IP model, services, protocols, and interfaces are not properly separated. It is protocol dependent.
The usage of this model is very low.	This model is highly used.
It provides standardization to the devices like router, motherboard, switches, and other hardware devices.	It does not provide the standardization to the devices. It provides a connection between various computers.

Design Issues in Data Link Layer

- **Data-link layer** is the second layer after the physical layer. The data link layer is responsible for maintaining the data link between two hosts or nodes.
- Before going through the design issues in the data link layer. Some of its sub-layers and their functions are as following below.
- The data link layer is divided into two sub-layers :

1.Logical Link Control Sub-layer (LLC) – Provides the logic for the data link, Thus it controls the synchronization, flow control, and error checking functions of the data link layer. Functions are –

(i) Error Recovery.

(ii) It performs the flow control operations.

(iii) User addressing.

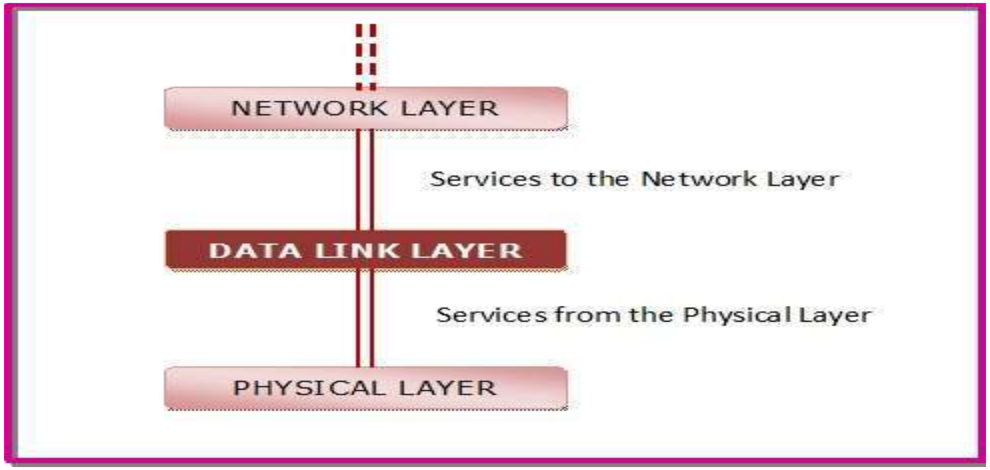
2.Media Access Control Sub-layer (MAC) – It is the second sub-layer of data-link layer. It controls the flow and multiplexing for transmission medium. Transmission of data packets is controlled by this layer. This layer is responsible for sending the data over the network interface card.

Functions are –

- **(i)** To perform the control of access to media.
- **(ii)** It performs the unique addressing to stations directly connected to LAN.
- **(iii)** Detection of errors.

Design issues with data link layer are :

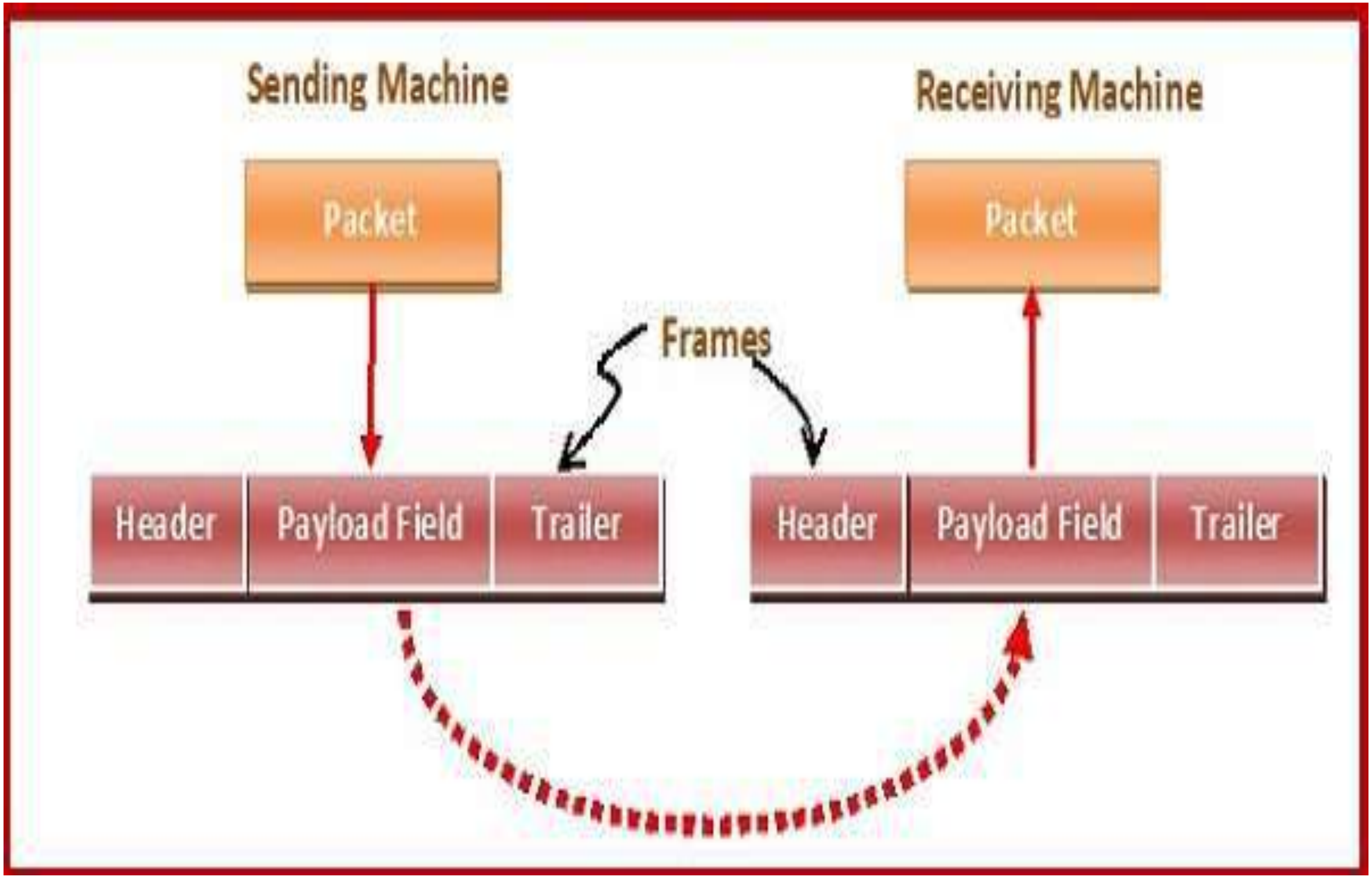
1. **Services provided to the network layer –** The data link layer act as a service interface to the network layer. The principle service is transferring data from network layer on sending machine to the network layer on destination machine. This transfer also takes place via DLL (Dynamic Link Library).



- **2. Frame synchronization** – The source machine sends data in the form of blocks called frames to the destination machine. The starting and ending of each frame should be identified so that the frame can be recognized by the destination machine. The data link layer encapsulates each data packet from the network layer into frames that are then transmitted.

  A frame has three parts, namely –

  - Frame Header
  - Payload field that contains the data packet from network layer
  - Trailer


Sending Machine
Receiving Machine
Packet
Packet
Frames
Header
Payload Field
Trailer
Header
Payload Field
Trailer

3. Flow control – Flow control is done to prevent the flow of data frame at the receiver end. The source machine must not send data frames at a rate faster than the capacity of destination machine to accept them.

- The data link layer regulates flow control so that a fast sender does not drown a slow receiver. When the sender sends frames at very high speeds, a slow receiver may not be able to handle it. There will be frame losses even if the transmission is error-free. The two common approaches for flow control are −
  - Feedback based flow control
  - Rate based flow control

4. Error control –
Error control is done to prevent duplication of frames. The errors introduced during transmission from source to destination machines must be detected and corrected at the destination machine.

- The data link layer ensures error free link for data transmission. The issues it caters to with respect to error control are −
  - Dealing with transmission errors
  - Sending acknowledgement frames in reliable connections
  - Retransmitting lost frames
  - Identifying duplicate frames and deleting them
  - Controlling access to shared channels in case of broadcasting

Framing in Data Link Layer

- Frames are the units of digital transmission, particularly in computer networks and telecommunications. Frames are comparable to the packets of energy called photons in the case of light energy. Frame is continuously used in Time Division Multiplexing process.
- Framing is a point-to-point connection between two computers or devices consists of a wire in which data is transmitted as a stream of bits. However, these bits must be framed into discernible blocks of information. Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. Ethernet, token ring, frame relay, and other data link layer technologies have their own frame structures. Frames have headers that contain information such as error-checking codes.

Types of framing – There are two types of framing:

- **1. Fixed size –** The frame is of fixed size and there is no need to provide boundaries to the frame, the length of the frame itself acts as a delimiter.
- **Drawback:** It suffers from internal fragmentation if the data size is less than the frame size
- **Solution:** Padding

2. **Variable size –** In this, there is a need to define the end of the frame as well as the beginning of the next frame to distinguish. This can be done in two ways:

- **Length field –** We can introduce a length field in the frame to indicate the length of the frame. Used in **Ethernet(802.3)**. The problem with this is that sometimes the length field might get corrupted.
- **End Delimiter (ED) –** We can introduce an ED(pattern) to indicate the end of the frame. Used in **Token Ring**. The problem with this is that ED can occur in the data. This can be solved by:

1. **Character/Byte Stuffing:** Used when frames consist of characters. If data contains ED then, a byte is stuffed into data to differentiate it from ED.

2. Bit Stuffing: Let ED = 01111 and if data = 01111

–> Sender stuffs a bit to break the pattern i.e. here appends a 0 in data = 0111**0**1.

–> Receiver receives the frame.

–> If data contains 011101, receiver removes the 0 and reads the data.

Error Detection in Computer Networks

Error

A condition when the receiver’s information does not match with the sender’s information. During transmission, digital signals suffer from noise that can introduce errors in the binary bits travelling from sender to receiver. That means a 0 bit may change to 1 or a 1 bit may change to 0.

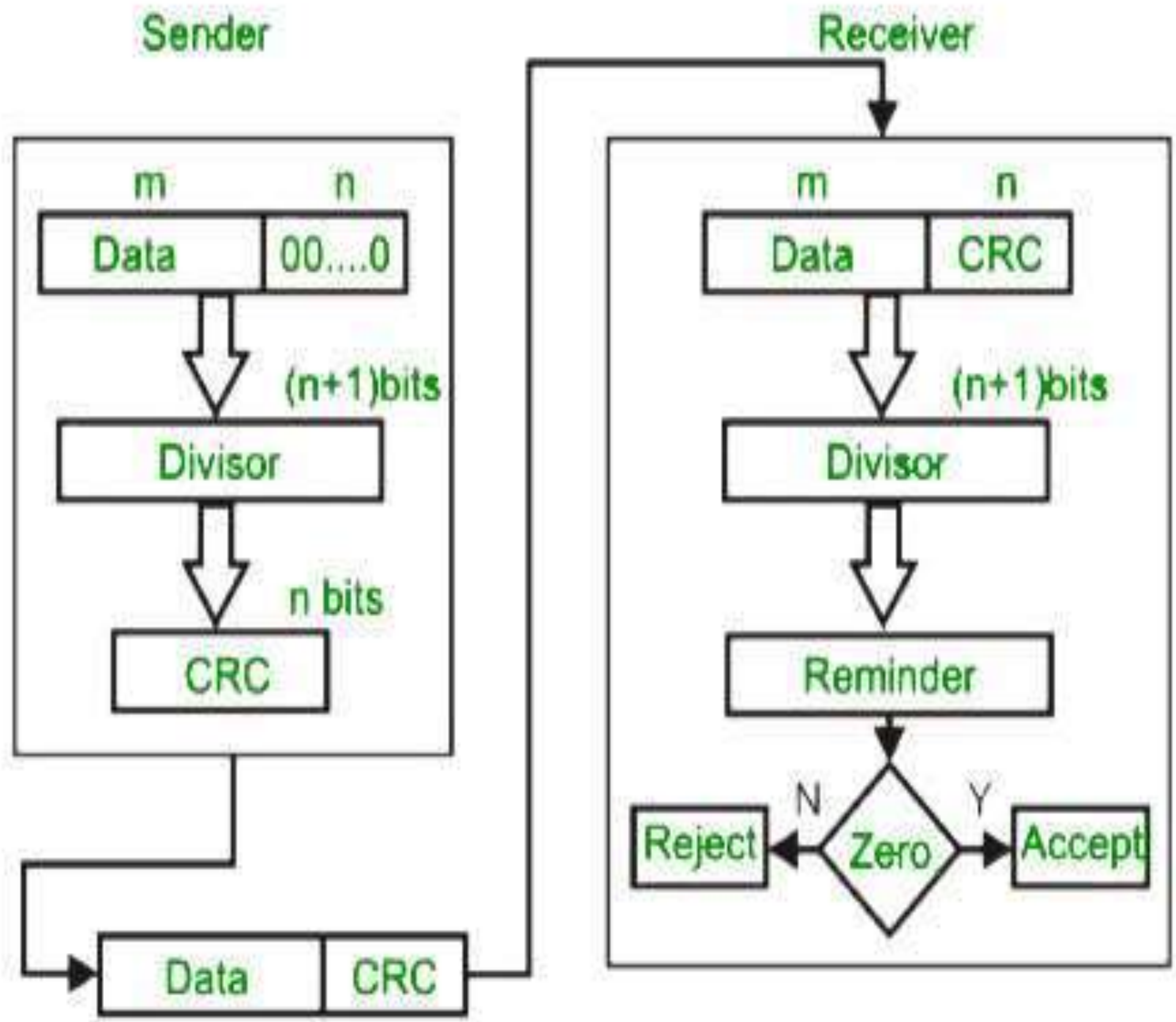
Error Detecting Codes (Implemented either at Data link layer or Transport Layer of OSI Model)

Whenever a message is transmitted, it may get scrambled by noise or data may get corrupted. To avoid this, we use error-detecting codes which are additional data added to a given digital message to help us detect if any error has occurred during transmission of the message.

- Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.
- Some popular techniques for error detection are:
  1. Simple Parity check
  2. Two-dimensional Parity check
  3. Checksum
  4. Cyclic redundancy check

Cyclic redundancy check (CRC)

- Unlike checksum scheme, which is based on addition, CRC is based on binary division.
- In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
- At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
- A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



Sender
Receiver
m
n
Data
00....0
(n+1)bits
Divisor
n bits
CRC
m
n
Data
CRC
(n+1)bits
Divisor
Reminder
N
Y
Reject
Zero
Accept
Data
CRC

original message

1 0 1 0 0 0 0

@ means X-OR

Generator polynomial

x^3+1

$1.x^3+0.x^2+0.x^1+1.x^0$

CRC generator

1 0 0 1 4-bit

If CRC generator is of n bit then append (n-1) zeros in the end of original message

Sender

```
1001 | 1010000000
      @1001
       0011000000
        @1001
          01010000
          @1001
           0011000
            @1001
              01010
              @1001
               0011
```

Message to be transmitted

```
1010000000
      +011
1010000011
```

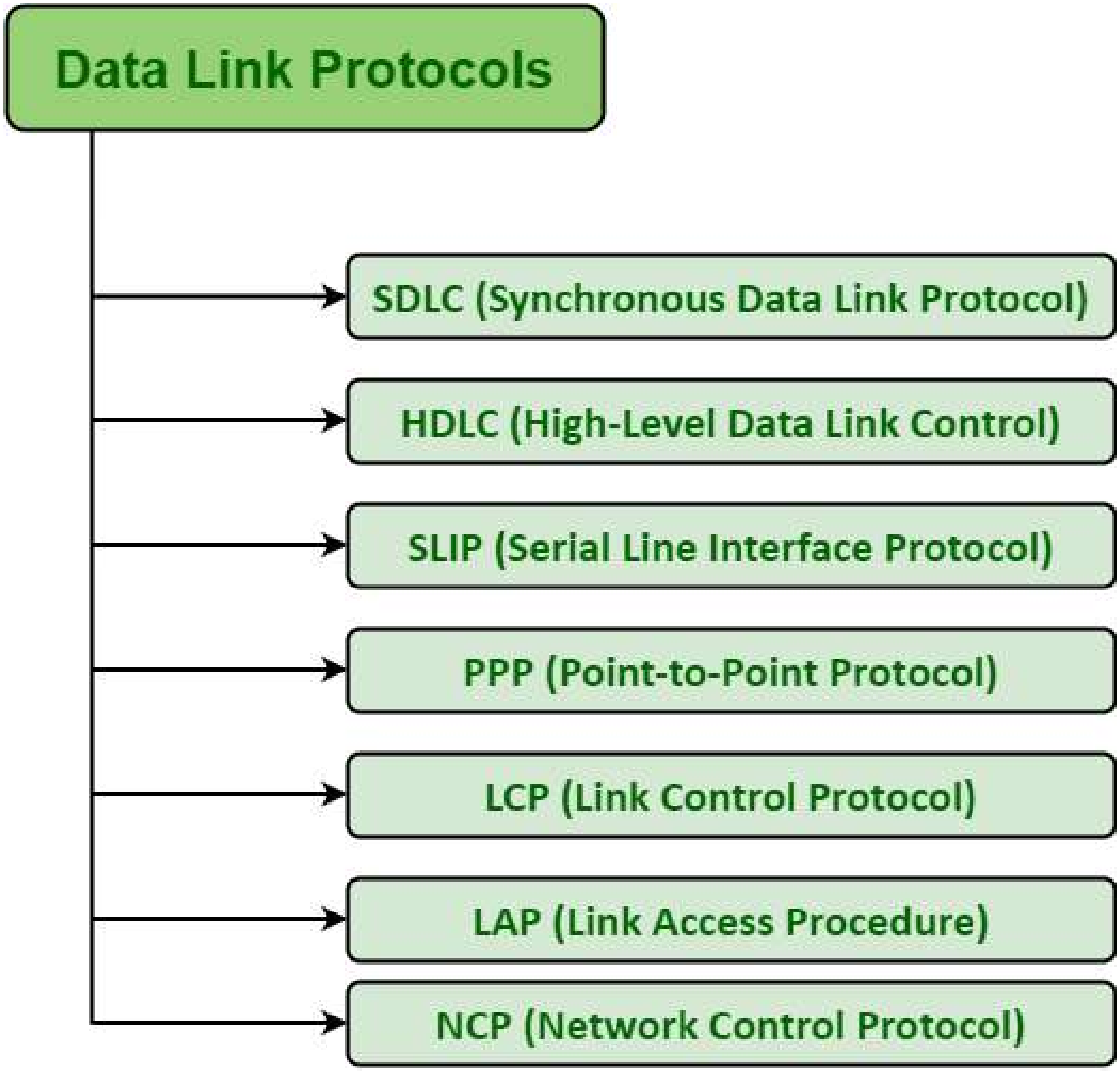
```
1001 | 1010000011
      @1001
       0011000011
        @1001
          01010011
          @1001
           0011011
            @1001
              01001
              @1001
               0000
```

Receiver

Zero means data is accepted

Elementary Data Link layer Protocols

Data Link Layer protocols are generally responsible to simply ensure and confirm that the bits and bytes that are received are identical to the bits and bytes being transferred. It is basically a set of specifications that are used for implementation of data link layer just above the physical layer of the Open System Interconnections (OSI) Model.



Data Link Protocols
SDLC (Synchronous Data Link Protocol)
HDLC (High-Level Data Link Control)
SLIP (Serial Line Interface Protocol)
PPP (Point-to-Point Protocol)
LCP (Link Control Protocol)
LAP (Link Access Procedure)
NCP (Network Control Protocol)

1. Synchronous Data Link Protocol (SDLC) – SDLC is basically a communication protocol of computer. It usually supports multipoint links even error recovery or error correction also. It is usually used to carry SNA (Systems Network Architecture) traffic and is present precursor to HDLC. It is also designed and developed by IBM in 1975. It is also used to connect all of the remote devices to mainframe computers at central locations may be in point-to-point (one-to-one) or point-to-multipoint (one-to-many) connections. It is also used to make sure that the data units should arrive correctly and with right flow from one network point to next network point.

2. High-Level Data Link Protocol (HDLC) – HDLC is basically a protocol that is now assumed to be an umbrella under which many Wide Area protocols sit. It is also adopted as a part of X.25 network. It was originally created and developed by ISO in 1979. This protocol is generally based on SDLC. It also provides best-effort unreliable service and also reliable service. HDLC is a bit-oriented protocol that is applicable for point-to-point and multipoint communications both.

3. Serial Line Interface Protocol (SLIP) – SLIP is generally an older protocol that is just used to add a framing byte at end of IP packet. It is basically a data link control facility that is required for transferring IP packets usually among Internet Service Providers (ISP) and a home user over a dial-up link. It is an encapsulation of the TCP/IP especially designed to work with over serial ports and several router connections simply for communication. It is some limitations like it does not provide mechanisms such as error correction or error detection.

4. Point to Point Protocol (PPP) –

PPP is a protocol that is basically used to provide same functionality as SLIP. It is most robust protocol that is used to transport other types of packets also along with IP Packets. It can also be required for dial-up and leased router-router lines. It basically provides framing method to describe frames. It is a character-oriented protocol that is also used for error detection. It is also used to provides two protocols i.e. NCP and LCP. LCP is used for bringing lines up, negotiation of options, bringing them down whereas NCP is used for negotiating network-layer protocols. It is required for same serial interfaces like that of HDLC.

•

5. **Link Control Protocol (LCP) –** It was originally developed and created by IEEE 802.2. It is also used to provide HDLC style services on LAN (Local Area Network). LCP is basically a PPP protocol that is used for establishing, configuring, testing, maintenance, and ending or terminating links for transmission of data frames.

6. Link Access Procedure (LAP) –

LAP protocols are basically a data link layer protocols that are required for framing and transferring data across point-to-point links. It also includes some reliability service features. There are basically three types of LAP i.e. LAPB (Link Access Procedure Balanced), LAPD (Link Access Procedure D-Channel), and LAPF (Link Access Procedure Frame-Mode Bearer Services). It is actually originated from IBM SDLC, which is being submitted by IBM to the ISP simply for standardization.

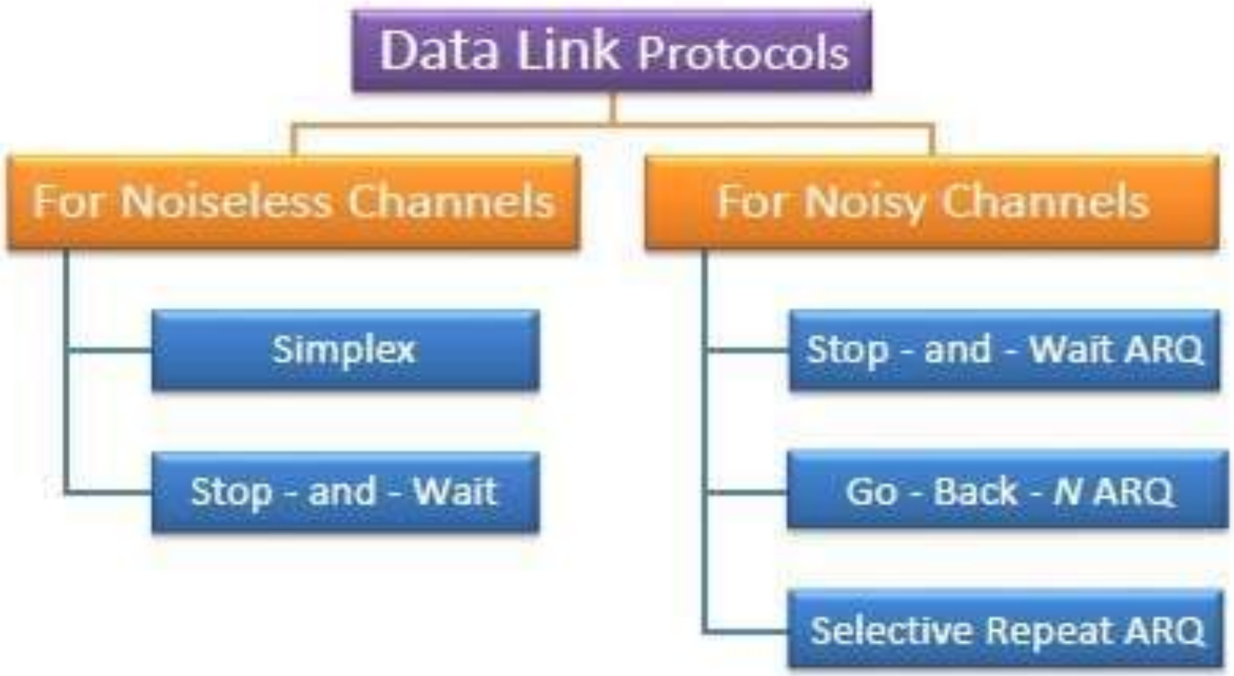
•

7. Network Control Protocol (NCP) – NCP was also an older protocol that was implemented by ARPANET. It basically allows users to have access to use computers and some of the devices at remote locations and also to transfer files among two or more computers. It is generally a set of protocols that is forming a part of PPP. NCP is always available for each and every higher-layer protocol that is supported by PPP. NCP was replaced by TCP/IP in the 1980s.

-

Types of Data Link Protocols

- Data link protocols can be broadly divided into two categories, depending on whether the transmission channel is noiseless or noisy.



Sliding Window Protocol

- Sliding window protocols are data link layer protocols for reliable and sequential delivery of data frames. The sliding window is also used in Transmission Control Protocol.
- In this protocol, multiple frames can be sent by a sender at a time before receiving an acknowledgment from the receiver. The term sliding window refers to the imaginary boxes to hold frames. Sliding window method is also known as windowing.

- The sliding window is a technique for sending multiple frames at a time. It controls the data packets between the two devices where reliable and gradual delivery of data frames is needed. It is also used in TCP (Transmission Control Protocol)
- In this technique, each frame has sent from the sequence number. The sequence numbers are used to find the missing data in the receiver end. The purpose of the sliding window technique is to avoid duplicate data, so it uses the sequence number.

Types of Sliding Window Protocols

- The Sliding Window ARQ (Automatic Repeat reQuest) protocols are of two categories –

Go – Back – *N* ARQ

- Go – Back – *N* ARQ provides for sending multiple frames before receiving the acknowledgment for the first frame. It uses the concept of sliding window, and so is also called sliding window protocol. The frames are sequentially numbered and a finite number of frames are sent. If the acknowledgment of a frame is not received within the time period, all frames starting from that frame are retransmitted.

Selective Repeat ARQ

- This protocol also provides for sending multiple frames before receiving the acknowledgment for the first frame. However, here only the erroneous or lost frames are retransmitted, while the good frames are received and buffered.