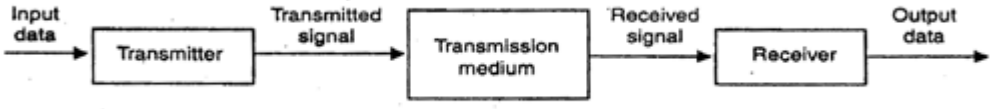
Syllabus

Unit	Contents
Unit -I	Data communication system, data communication links,
	character codes, digital data rates, serial data formats, encoded data formats, telephones systems,
	error detection & correction.
Unit- II	Model, data topologies, data switching, type of networks, networking medium
	twisted pairs, coaxial cable, optical fibers, system network architecture, SNA operating system.
	Introduction to OSI & TCP/IP.
Unit- III	Limits of communication, RS449 interface standards, RS422 & RS423, F5K & V0 modems,
	multiplexing methods, sampling theorem and quantization, delta modulation, digital T carrier, CODEC.
Unit- IV	Data link protocol, character oriented protocol & bit oriented protocol,
	Network architecture protocols, Ethernet & token ring
Unit- V	Integrated services & routing protocols,
	B-ISDN, DSL& ATM, and Internet

Unit I

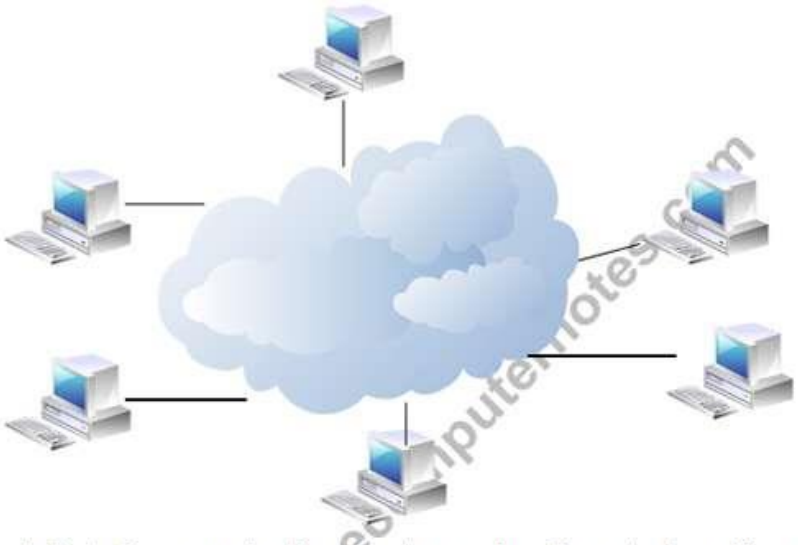
Data Communication System:

Data communication refers to the exchange of data between a source and a receiver. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area. The meanings of source and receiver are very simple. The device that transmits the data is known as source and the device that receives the transmitted data is known as receiver. Data communication aims at the transfer of data and maintenance of the data during the process but not the actual generation of the information at the source and receiver.
Datum mean the facts information statistics or the like derived by calculation or experimentation. The facts and information so gathered are processed in accordance with defined systems of procedure. Data can exist in a variety of forms such as numbers, text, bits and bytes. The Figure is an illustration of a simple data communication system.



Simple Data Communication System

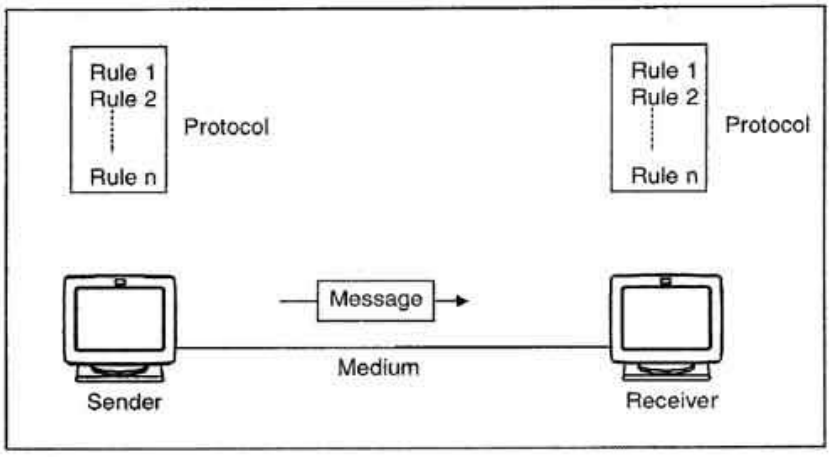
A data communication system may collect data from remote locations through data transmission circuits, and then outputs processed results to remote locations. Figure provides a broader view of data communication networks. The different data communication techniques which are presently in widespread use evolved gradually either to improve the data communication techniques already existing or to replace the same with better options and features. Then, there are data communication jargons to contend with such as baud rate, modems, routers, LAN, WAN, TCP/IP, ISDN, during the selection of communication systems. Hence, it becomes necessary to review and understand these terms and gradual development of data communication methods.



A Data Communication System using Remote Locations

A Communication system has following components:
1. **Message**: It is the information or data to be communicated. It can consist of text, numbers, pictures, sound or video or any combination of these.
2. **Sender**: It is the device/computer that generates and sends that message.
3. **Receiver**: It is the device or computer that receives the message. The location of receiver computer is generally different from the sender computer. The distance between sender and receiver depends upon the types of network used in between.
4. **Medium:** It is the channel or physical path through which the message is carried from sender to the receiver. The medium can be wired like twisted pair wire, coaxial cable, fiber-optic cable or wireless like laser, radio waves, and microwaves.
5. **Protocol**: It is a set of rules that govern the communication between the devices. Both sender and receiver follow same protocols to communicate with each other.

A protocol performs the following functions:
1. **Data sequencing.** It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.
2. **Data routing.** Data routing defines the most efficient path between the source and destination.
3. **Data formatting.** Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.
4. **Flow control**. A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.
5. **Error control**. These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.
6. **Precedence and order of transmission**. These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.
7. **Connection establishment and termination**. These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.



8. **Data security**. Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

9. **Log information**. Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

Communication Links:

Coaxial Cable

At one time, coaxial cable was the most widely used network cabling. There were a couple of reasons for coaxial cable's wide usage: it was relatively inexpensive, and it was light, flexible, and easy to work with. In its simplest form, coaxial cable consists of a core of copper wire surrounded by insulation, a braided metal shielding, and an outer cover. Figure 2.1 shows the various components that make up a coaxial cable.

The term shielding refers to the woven or stranded metal mesh (or other material) that surrounds some types of cabling. Shielding protects transmitted data by absorbing stray electronic signals, called noise, so that they do not get onto the cable and distort the data. Cable that contains one layer of foil insulation and one layer of braided metal shielding is referred to as dual shielded. For environments that are subject to higher interference, quad shielding is available. Quad shielding consists of two layers of foil insulation and two layers of braided metal shielding.

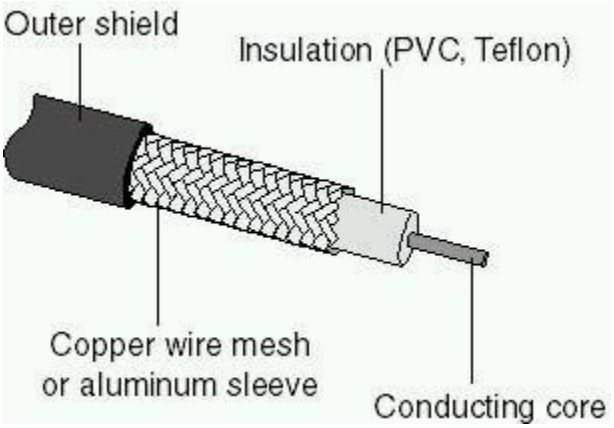


Figure 2.1 Coaxial cable showing various layers

The core of a coaxial cable carries the electronic signals that make up the data. This wire core can be either solid or stranded. If the core is solid, it is usually copper.

Surrounding the core is a dielectric insulating layer that separates it from the wire mesh. The braided wire mesh acts as a ground and protects the core from electrical noise and crosstalk. (Crosstalk is signal overflow from an adjacent wire. For a more detailed discussion of crosstalk, see the section Unshielded Twisted-Pair (UTP) Cable, later in this lesson.)

The conducting core and the wire mesh must always be kept separate from each other. If they touch, the cable will experience a short, and noise or stray signals on the mesh will flow onto the copper wire. An electrical short occurs when any two conducting wires or a conducting wire and a ground come into contact with each other. This contact causes a direct flow of current (or data) in an unintended path. In the case of household electrical wiring, a short will cause sparking and the blowing of a fuse or circuit breaker. With electronic devices that use low voltages, the result is not as dramatic and is often undetectable. These low-voltage shorts generally cause the failure of a device; and the short, in turn, destroys the data.

A non conducting outer shield—usually made of rubber, Teflon, or plastic—surrounds the entire cable.

Coaxial cable is more resistant to interference and attenuation than twisted-pair cabling. As shown in Figure 2.2, attenuation is the loss of signal strength that begins to occur as the signal travels farther along a copper cable.

Figure 2.2 *Attenuation causes signals to deteriorate*

The stranded, protective sleeve absorbs stray electronic signals so that they do not affect data being sent over the inner copper cable. For this reason, coaxial cabling is a good choice for longer distances and for reliably supporting higher data rates with less sophisticated equipment.

Types of Coaxial Cable

There are two types of coaxial cable:

- Thin (thinnet) cable
- Thick (thicknet) cable

Thinnet Cable *Thinnet* cable is a flexible coaxial cable about 0.64 centimeters (0.25 inches) thick. Because this type of coaxial cable is flexible and easy to work with, it can be used in almost any type of network installation. Figure 2.3 shows thinnet cable connected directly to a computer's network interface card (NIC).

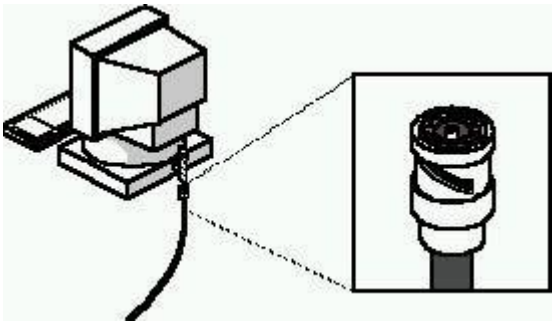


Figure 2.3 Close-up view of thinnet cable showing where it connects to a computer

Thinnet coaxial cable can carry a signal for a distance of up to approximately 185 meters (about 607 feet) before the signal starts to suffer from attenuation.

Cable manufacturers have agreed upon specific designations for different types of cable. (Table 2.1 lists cable types and descriptions.) Thinnet is included in a group referred to as the RG-58 family and has 50ohm impedance. (Impedance is the resistance, measured in ohms, to the alternating current that flows in a wire.) The

principal distinguishing feature of the RG-58 family is the center core of copper. Figure 2.4 shows two examples of RG-58 cable, one with a stranded wire core and one with a solid copper core.

Figure 2.4 RG-58 coaxial cable showing stranded wire and solid copper cores

Table 2.1 Cable Types

Cable	Description
RG-58/U	Solid copper core
RG-58 A/U	Stranded wire core
RG-58 C/U	Military specification of RG-58 A/U
RG-59	Broadband transmission, such as cable television
RG-6	Larger in diameter and rated for higher frequencies than RG-59, but also used for broadband transmissions
RG-62	ArcNet networks

Thicknet Cable *Thicknet* cable is a relatively rigid coaxial cable about 1.27 centimeters (0.5 inches) in diameter. Figure 2.5 shows the difference between thinnet and thicknet cable. Thicknet cable is sometimes referred to as Standard Ethernet because it was the first type of cable used with the popular network architecture Ethernet. Thicknet cable's copper core is thicker than a thinnet cable core.

Figure 2.5 *Thicknet cable has a thicker core than thinnet cable*

The thicker the copper core, the farther the cable can carry signals. This means that thicknet can carry signals farther than thinnet cable. Thicknet cable can carry a signal for 500 meters (about 1640 feet). Therefore, because of thicknet's ability to support data transfer over longer distances, it is sometimes used as a backbone to connect several smaller thinnet-based networks.

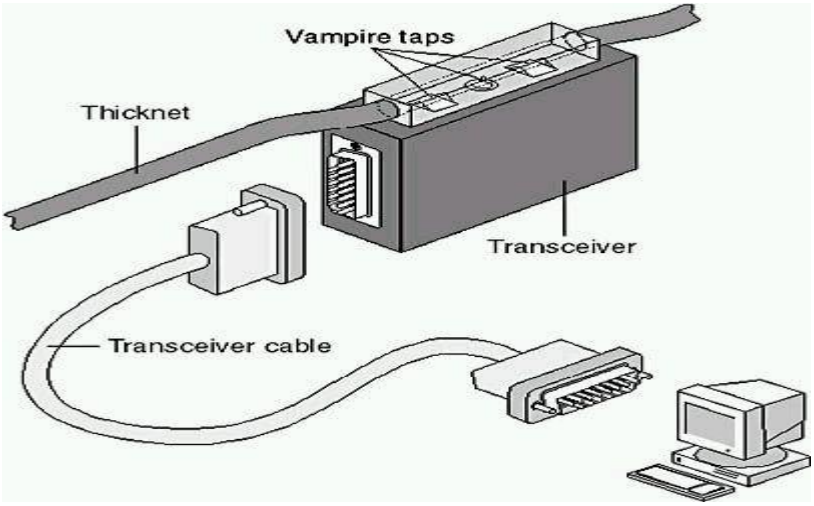


Figure 2.6 Thicknet cable transceiver with detail of a vampire tap piercing the core

Figure 2.6 shows a device called a transceiver. A *transceiver* connects the thinnet coaxial cable to the larger thicknet coaxial cable. A transceiver designed for thicknet Ethernet includes a connector known as a *vampire tap*, or a piercing tap, to make the actual physical connection to the thicknet core. This connector is pierced through the insulating layer and makes direct contact with the conducting core. Connection from the transceiver to the NIC is made using a transceiver cable (drop cable) to connect to the *attachment unit interface* (AUI) port connector on the card. An AUI port connector for thicknet is also known as a*Digital Intel Xerox (DIX) connector* (named for the three companies that developed it and its related standards) or as a DB-15 connector.

Twisted-Pair Cable: In its simplest form, twisted-pair cable consists of two insulated strands of copper wire twisted around each other. Figure 2.12 shows the two types of twisted-pair cable: unshielded twisted-pair (UTP) and shielded twisted-pair (STP) cable.

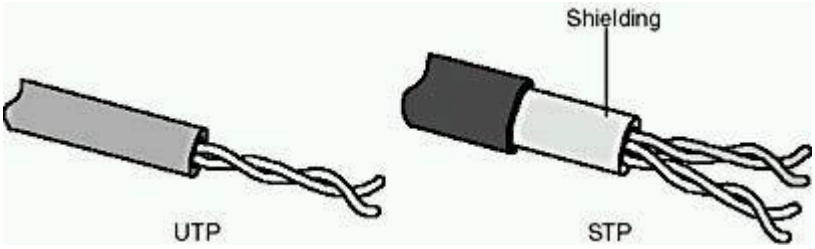


Figure 2.12 Unshielded twisted-pair and shielded twisted-pair cables

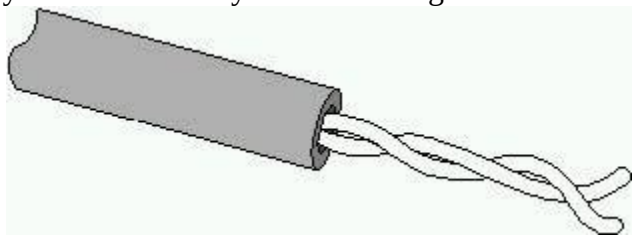
A number of twisted-pair wires are often grouped together and enclosed in a protective sheath to form a cable. The total number of pairs in a cable varies. The twisting cancels out electrical noise from adjacent pairs and from other sources such as motors, relays, and transformers.

Unshielded Twisted-Pair (UTP) Cable

UTP, using the 10BaseT specification, is the most popular type of twisted-pair cable and is fast becoming the most popular LAN cabling. The maximum cable length segment is 100 meters, about 328 feet.

Traditional UTP cable, as shown in Figure 2.13, consists of two insulated copper wires. UTP specifications govern how many twists are permitted per foot of cable; the number of twists allowed depends on the purpose

to which the cable will be put. In North America, UTP cable is the most commonly used cable for existing telephone systems and is already installed in many office buildings.



Character Codes:

Computer works only with binary numbers. It stores all types of data in the form binary digits. The data is converted to binary form before it is stored inside the computer the process of converting data into binary form is known encoding. Data can be converted into binary form by using different coding schemes.

Types of coding schemes

Different types of coding schemes are as follows:

1. BCD Code

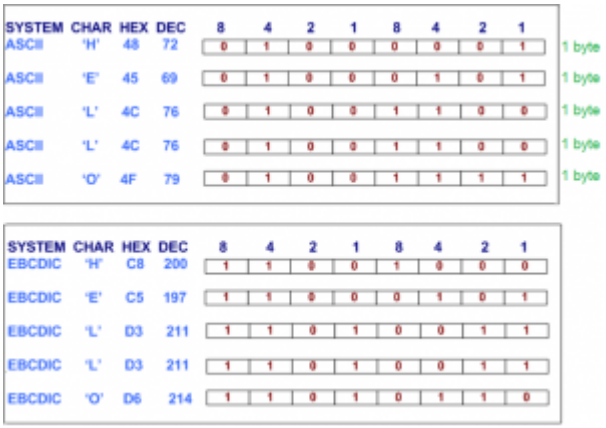
BCD stands for binary coded decimal. It is a 4-bit code. It means that each decimal digit is represented by 4 binary digits. It was used by early computers.

2. EBCDIC Code

EBCDIC stands for extended binary coded decimal interchange code. It is an 8-bit code. It is normally used in mainframe computers. It can represent 256 characters.

3. ASCII

ASCII stands for American standard code for information interchange. It was published in 1968 by ANSI (American National Standard Institute). It is the most widely used coding scheme for personal computers. The 7-bit code can represent 128 characters. It is not enough to represent some graphical characters displayed on computer screens. An 8-bit code can represent 256 characters. The extended 128 unique codes represent graphic symbols.



SYSTEM	CHAR	HEX	DEC	8	4	2	1	8	4	2	1	
ASCII	'H'	48	72	0	1	0	0	0	0	0	1	1 byte
ASCII	'E'	45	69	0	1	0	0	0	1	0	1	1 byte
ASCII	'L'	4C	76	0	1	0	0	1	1	0	0	1 byte
ASCII	'L'	4C	76	0	1	0	0	1	1	0	0	1 byte
ASCII	'O'	4F	79	0	1	0	0	1	1	1	1	1 byte

SYSTEM	CHAR	HEX	DEC	8	4	2	1	8	4	2	1
EBCDIC	'H'	C8	200	1	1	0	0	1	0	0	0
EBCDIC	'E'	C5	197	1	1	0	0	0	1	0	1
EBCDIC	'L'	D3	211	1	1	0	1	0	0	1	1
EBCDIC	'L'	D3	211	1	1	0	1	0	0	1	1
EBCDIC	'O'	D6	214	1	1	0	1	0	1	1	0

4. unicode

Unicode is a 16-bit code. It can represent 65536 characters. It has started to replace ASCII code. It can represent the characters of all languages in the world.

Data transmission mode:

The way in which data is transmitted from one place to another is called data transmission mode.

Types of transmission modes

There are three types of data transmission modes:

1. Simplex mode 2. Half duplex mode 3. Full duplex mode

1. Simplex mode

In simplex mode, data can flow only in one direction. It cannot be moved in both directions. It operates in a manner similar to a one-way street. The direction of flow never changes. A device with simplex mode can either send or receive data. It cannot perform both changes. A device with simplex mode can either send or receive data. It cannot perform both actions.

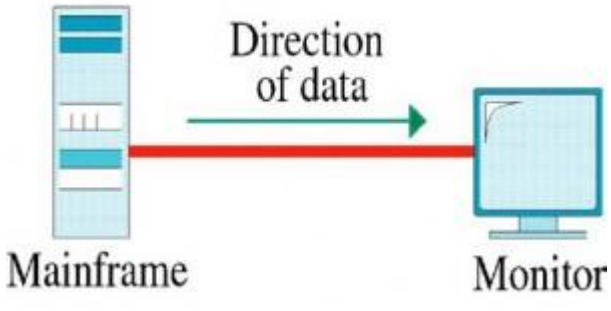


Figure: simplex mode

Example

An example is a traditional television broadcast. The signal is sent from the transmitter to TV antenna. There is no return signal.

2. Half-Duplex Traffic

In half-duplex mode, data can flow in both directions but not at the same time. It is transmitted one-way at one time. A device with half-duplex mode can send or receive data but not at the same time. That is why the speed of half-duplex mode is slow.

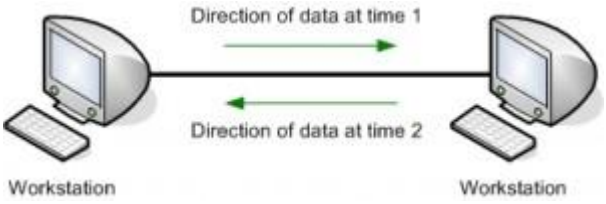


Figure: Half Duplex

Example

Internet surfing is an example of half-duplex communication. The user issues a request for a web page. The web page is downloaded and displayed before the user issues another request.

3. Full-Duplex Mode

In full-duplex mode, data can travel in both directions simultaneously. Full duplex mode is a faster way of data transmission as compared to half duplex. Time is not wasted in changing the direction of data flow.

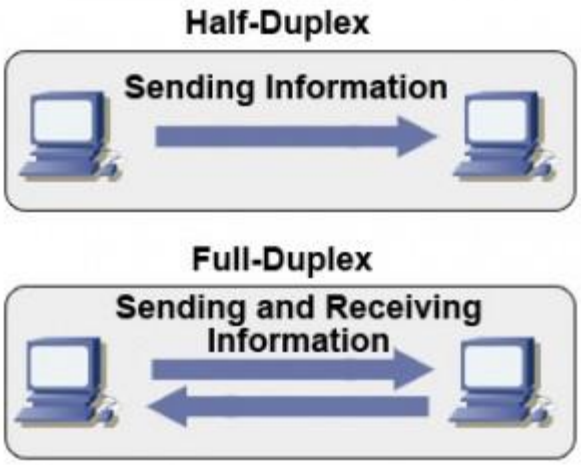


Figure: Full Duplex

Example

A telephone is a full-duplex communication is automobile traffic on a two-lane road. The traffic can move in both directions at the same time.

ASCII

Short for American Standard Code for Information Interexchange, ASCII is an standard that assigns letters, numbers, and other characters within the 256 slots available in the 8-bit code. The ASCII decimal (Dec) number is created from binary, which is the language of all computers. As shown in the table below, the lower case "h" character (Char) has a decimal value of 104, which is "01101000" in binary.

The ASCII table is divided in 3 different sections.

- Non printable, system codes between 0 and 31.
- Lower ASCII, between 32 and 127. This table originates from the older, American systems, which worked on 7-bit character tables.
- Higher ASCII, between 128 and 255. This portion is programmable; characters are based on the language of your operating system or program you are using. Foreign letters are also placed in this section.

Standard or Lower ASCII characters and codes

Char	Dec	Binary	Char	Dec	Binary	Char	Dec	Binary
!	033	00100001	A	065	01000001	a	097	01100001
"	034	00100010	B	066	01000010	b	098	01100010
#	035	00100011	C	067	01000011	c	099	01100011

$	036	00100100	**D**	068	01000100	**d**	100	01100100
%	037	00100101	**E**	069	01000101	**e**	101	01100101
&	038	00100110	**F**	070	01000110	**f**	102	01100110
'	039	00100111	**G**	071	01000111	**g**	103	01100111
(	040	00101000	**H**	072	01001000	**h**	104	01101000
)	041	00101001	**I**	073	01001001	**i**	105	01101001
*****	042	00101010	**J**	074	01001010	**j**	106	01101010
+	043	00101011	**K**	075	01001011	**k**	107	01101011
,	044	00101100	**L**	076	01001100	**l**	108	01101100
-	045	00101101	**M**	077	01001101	**m**	109	01101101
.	046	00101110	**N**	078	01001110	**n**	110	01101110
/	047	00101111	**O**	079	01001111	**o**	111	01101111
0	048	00110000	**P**	080	01010000	**p**	112	01110000
1	049	00110001	**Q**	081	01010001	**q**	113	01110001
2	050	00110010	**R**	082	01010010	**r**	114	01110010

3	051	00110011	**S**	083	01010011	**s**	115	01110011
4	052	00110100	**T**	084	01010100	**t**	116	01110100
5	053	00110101	**U**	085	01010101	**u**	117	01110101
6	054	00110110	**V**	086	01010110	**v**	118	01110110
7	055	00110111	**W**	087	01010111	**w**	119	01110111
8	056	00111000	**X**	088	01011000	**x**	120	01111000
9	057	00111001	**Y**	089	01011001	**y**	121	01111001
:	058	00111010	**Z**	090	01011010	**z**	122	01111010
;	059	00111011	**[**	091	01011011	**{**	123	01111011
<	060	00111100	\	092	01011100	|	124	01111100
=	061	00111101	**]**	093	01011101	**}**	125	01111101
>	062	00111110	^	094	01011110	~	126	01111110
?	063	00111111	**_**	095	01011111	**_**	127	01111111
@	064	01000000	`	096	01100000			

- Extended ASCII uses eight instead of seven bits, which adds 128 additional characters. This gives extended ASCII the ability for extra characters, such as special symbols, foreign language letters, and drawing characters as shown below.

Extended or Higher ASCII characters and codes

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	└	224	E0	α
129	81	ü	161	A1	í	193	C1	┴	225	E1	ß
130	82	é	162	A2	ó	194	C2	┬	226	E2	Γ
131	83	â	163	A3	ú	195	C3	├	227	E3	π
132	84	ä	164	A4	ñ	196	C4	─	228	E4	Σ
133	85	à	165	A5	Ñ	197	C5	┼	229	E5	σ
134	86	å	166	A6	ª	198	C6	╞	230	E6	µ
135	87	ç	167	A7	º	199	C7	╟	231	E7	τ
136	88	ê	168	A8	¿	200	C8	╚	232	E8	Φ
137	89	ë	169	A9	⌐	201	C9	╔	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	╩	234	EA	Ω
139	8B	ï	171	AB	½	203	CB	╦	235	EB	δ
140	8C	î	172	AC	¼	204	CC	╠	236	EC	∞
141	8D	ì	173	AD	¡	205	CD	═	237	ED	ø
142	8E	Ä	174	AE	«	206	CE	╬	238	EE	ε
143	8F	Å	175	AF	»	207	CF	╧	239	EF	∩
144	90	É	176	B0	░	208	D0	╨	240	F0	≡
145	91	æ	177	B1	▒	209	D1	╤	241	F1	±
146	92	Æ	178	B2	▓	210	D2	╥	242	F2	≥
147	93	ô	179	B3	│	211	D3	╙	243	F3	≤
148	94	ö	180	B4	┤	212	D4	╘	244	F4	⌠
149	95	ò	181	B5	╡	213	D5	╒	245	F5	⌡
150	96	û	182	B6	╢	214	D6	╓	246	F6	÷
151	97	ù	183	B7	╖	215	D7	╫	247	F7	≈
152	98	ÿ	184	B8	╕	216	D8	╪	248	F8	°
153	99	Ö	185	B9	╣	217	D9	┘	249	F9	∙
154	9A	Ü	186	BA	║	218	DA	┌	250	FA	·
155	9B	¢	187	BB	╗	219	DB	█	251	FB	√
156	9C	£	188	BC	╝	220	DC	▄	252	FC	ⁿ
157	9D	¥	189	BD	╜	221	DD	▌	253	FD	²
158	9E	₧	190	BE	╛	222	DE	▐	254	FE	■
159	9F	ƒ	191	BF	┐	223	DF	▀	255	FF	

EBCDIC: EBCDIC(pronounced "ebb see dick") is short for extended binary coded decimal interchange code is eight bits, or one *byte*, wide. This is a coding system used to represent characters-letters, numerals, punctuation marks, and other symbols in computerized text. A character is represented in EBCDIC by eight bit. EBCDIC mainly used on IBM mainframe and IBM midrange computer operating systems. Each byte consists of two *nibbles*, each four bits wide. The first four bits define the class of character, while the second nibble defines the specific character inside that class.

EBCDIC is different from, and incompatible with, the ASCII character set used by all other computers. The EBCDIC code allows for 256 different characters. For personal computers, however, ASCII is the standard. If

you want to move text between your computer and a mainframe, you can get a *file conversion* utility that will convert between EBCDIC and ASCII.

EBCDIC was adapted from the character codes used in IBM's pre electronic PUNCHED CARD machines, which made it less than ideal for modern computers. Among its many inconveniences were the use of non-contiguous codes for the alphabetic characters, and the absence of several punctuation characters such as the square brackets [] used by much modern software.

For example, setting the first nibble to all-ones,*1111*, defines the character as a number, and the second nibble defines which number is encoded. EBCDIC can code up to 256 different characters.

There have been six or more incompatible versions of EBCDIC, the latest of which do include all the ASCII characters, but also contain characters that are not supported in ASCII.

Digital Data Rate:

The data transfer rate (DTR) is the amount of digital data that is moved from one place to another in a given time. The data transfer rate can be viewed as the speed of travel of a given amount of data from one place to another. In general, the greater the bandwidth of a given path, the higher the data transfer rate.

In telecommunications, data transfer is usually measured in bits per second. For example, a typical low-speed connection to the Internet may be 33.6 kilobits per second (Kbps). On Ethernet local area networks, data transfer can be as fast as 10 megabits per second. Network switches are planned that will transfer data in the terabit range. In earlier telecommunication systems, data transfer was sometimes measured in characters or blocks (of a certain size) per second. Data transfer time between the microprocessor or RAM and devices such as the hard disk and CD-ROM player is usually measured in milliseconds.

In computers, data transfer is often measured in bytes per second. The highest data transfer rate to date is 14 terabits per second over a single optical fiber, reported by Japan's Nippon Telegraph and Telephone (NTT DoComo) in 2006.

Encoded Data Formats:

This format converts selected data into the following formats: Base64, UUencode, Quoted-Printable, Intel HEX and Motorola S-Records.

Its single parameter Algorithm lets you choose the format to be used.

Below is an example of a data encoded in Base64:

YXMAAAlhdWRpb3NpemUAQXJv9mAAAAAACGhhc0F1ZGlvAQEACmF1ZGlvZGVsYXkA

UUencode:

```
begin 666 c:\file.bin
M87,```EA=61I;W-I>F4`07)O]F``````"&AA<T%U9&EO`0$`"F%U9&EO9&5L
#87D`
`end
```

Quoted-Printable:

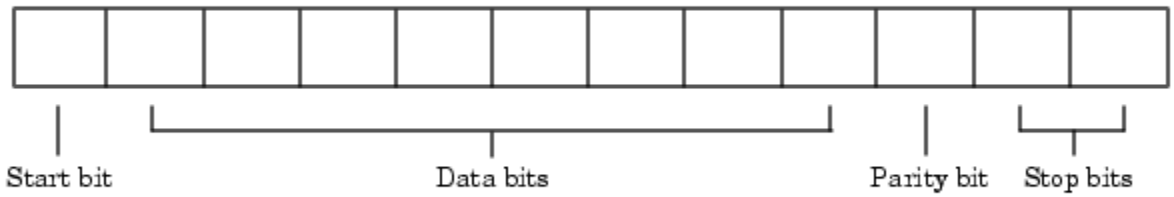
```
as=00=00        audiosize=00Aro=F6`=00=00=00=00=08hasAudio=01=01=00=0Aau=
diodelay=00
```

Intel HEX:

```
:10000000CFBEC96422B97C49A6963FA3E62F8FA331
:08001000010000032000000B5
:00000001FF
```

Motorola S-Records
S1130000CFBEC96422B97C49A6963FA3E62F8FA32D
S10B00100100000032000000B1
S5030002FA

Serial Data Format
The serial data format includes one start bit, between five and eight data bits, and one stop bit. A parity bit and an additional stop bit might be included in the format as well. The diagram below illustrates the serial data format.



The format for serial port data is often expressed using the following notation
number of data bits - parity type - number of stop bits
For example, 8-N-1 is interpreted as eight data bits, no parity bit, and one stop bit, while 7-E-2 is interpreted as seven data bits, even parity, and two stop bits.
The data bits are often referred to as a character because these bits usually represent an ASCII character. The remaining bits are called framing bits because they frame the data bits.

Synchronous and Asynchronous Communication
The RS-232 standard supports two types of communication protocols: synchronous and asynchronous.
Using the synchronous protocol, all transmitted bits are synchronized to a common clock signal. The two devices initially synchronize themselves to each other, and then continually send characters to stay synchronized. Even when actual data is not really being sent, a constant flow of bits allows each device to know where the other is at any given time. That is, each bit that is sent is either actual data or an idle character.
Synchronous communications allows faster data transfer rates than asynchronous methods, because additional bits to mark the beginning and end of each data byte are not required.
Using the asynchronous protocol, each device uses its own internal clock resulting in bytes that are transferred at arbitrary times. So, instead of using time as a way to synchronize the bits, the data format is used.
In particular, the data transmission is synchronized using the start bit of the word, while one or more stop bits indicate the end of the word. The requirement to send these additional bits causes asynchronous communications to be slightly slower than synchronous. However, it has the advantage that the processor does not have to deal with the additional idle characters. Most serial ports operate asynchronously.
Note When used in this guide, the terms "synchronous" and "asynchronous" refer to whether read or write operations block access to the MATLAB command line. Refer to Controlling Access to the MATLAB Command Line for more information.
Use of Bits Transmitted:

By definition, serial data is transmitted one bit at a time. The order in which the bits are transmitted is given below:
The start bit is transmitted with a value of 0.
The data bits are transmitted. The first data bit corresponds to the least significant bit (LSB), while the last data bit corresponds to the most significant bit (MSB).
The parity bit (if defined) is transmitted.
One or two stop bits are transmitted, each with a value of 1.
The number of bits transferred per second is given by the baud rate. The transferred bits include the start bit, the data bits, the parity bit (if defined), and the stop bits.

Start and Stop Bits

As described in Synchronous and Asynchronous Communication, most serial ports operate asynchronously. This means that the transmitted byte must be identified by start and stop bits. The start bit indicates when the data byte is about to begin and the stop bit(s) indicates when the data byte has been transferred. The process of identifying bytes with the serial data format follows these steps:
When a serial port pin is idle (not transmitting data), then it is in an "on" state.
When data is about to be transmitted, the serial port pin switches to an "off" state due to the start bit.
The serial port pin switches back to an "on" state due to the stop bit(s). This indicates the end of the byte.

Data Bits

The data bits transferred through a serial port might represent device commands, sensor readings, error messages, and so on. The data can be transferred as either binary data or ASCII data.
Most serial ports use between five and eight data bits. Binary data is typically transmitted as eight bits. Text-based data is transmitted as either seven bits or eight bits. If the data is based on the ASCII character set, then a minimum of seven bits is required because there are 27 or 128 distinct characters. If an eighth bit is used, it must have a value of 0. If the data is based on the extended ASCII character set, then eight bits must be used because there are 28 or 256 distinct characters.

The Parity Bit

The parity bit provides simple error (parity) checking for the transmitted data. The types of parity checking are given below.

Table 8-2: Parity Types

Parity Type	Description
Even	The data bits plus the parity bit result in an even number of 1's.
Mark	The parity bit is always 1.
Odd	The data bits plus the parity bit result in an odd number of 1's.
Space	The parity bit is always 0.

Mark and space parity checking are seldom used because they offer minimal error detection. You might choose to not use parity checking at all.

The parity checking process follows these steps:

The transmitting device sets the parity bit to 0 or to 1 depending on the data bit values and the type of parity checking selected.
The receiving device checks if the parity bit is consistent with the transmitted data. If it is, then the data bits are accepted. If it is not, then an error is returned.
Note Parity checking can detect only 1-bit errors. Multiple-bit errors can appear as valid data.

For example, suppose the data bits 01110001 are transmitted to your computer. If even parity is selected, then the parity bit is set to 0 by the transmitting device to produce an even number of 1's. If odd parity is selected, then the parity bit is set to 1 by the transmitting device to produce an odd number of 1's.

Error Detection and Correction methods:

Error detection and correction has great practical importance in maintaining data (information) integrity across noisy Communication Networks channels and lessthan- reliable storage media.

Correction : Send additional information so incorrect data can be corrected and accepted. Error correction is the additional ability to reconstruct the original, error-free data.

There are two basic ways to design the channel code and protocol for an error correcting system :

• **Automatic Repeat-Request (ARQ) :** The transmitter sends the data and also an error detection code, which the receiver uses to check for errors, and request retransmission of erroneous data. In many cases, the request is implicit; the receiver sends an acknowledgement (ACK) of correctly received data, and the transmitter re-sends anything not acknowledged within a reasonable period of time.

• **Forward Error Correction (FEC) :** The transmitter encodes the data with an error-correcting code (ECC) and sends the coded message. The receiver never sends any messages back to the transmitter. The receiver decodes what it receives into the "most likely" data. The codes are designed so that it would take an "unreasonable" amount of noise to trick the receiver into misinterpreting the data.

Error Detection : Send additional information so incorrect data can be detected and rejected. Error detection is the ability to detect the presence of errors caused by noise or other impairments during transmission from the transmitter to the receiver.

Error Detection Schemes : In telecommunication, a redundancy check is extra data added to a message for the purposes of error detection. Several schemes exist to achieve error detection, and are generally quite simple. All error detection codes transmit more bits than were in the original data. Most codes are "systematic": the transmitter sends a fixed number of original data bits, followed by fixed number of check bits usually referred to as redundancy which are derived from the data bits by some deterministic algorithm.

The receiver applies the same algorithm to the received data bits and compares its output to the received check bits; if the values do not match, an error has occurred at some point during the transmission. In a system that uses a "non-systematic" code, such as some raptor codes, data bits are transformed into at least as many code bits, and the transmitter sends only the code bits.

Repetition Schemes : Variations on this theme exist. Given a stream of data that is to be sent, the data is broken up into blocks of bits, and in sending, each block is sent some predetermined number of times. For example, if we want to send "1011", we may repeat this block three times each. Suppose we send "1011 1011 1011", and this is received as "1010 1011 1011".

As one group is not the same as the other two, we can determine that an error has occurred. This scheme is not very efficient, and can be susceptible to problems if the error occurs in exactly the same place for each group e.g. "1010 1010 1010" in the example above will be detected as correct in this scheme. The scheme however is extremely simple, and is in fact used in some transmissions of numbers stations.

Parity Schemes : A parity bit is an error detection mechanism . A*parity bit* is an extra bit transmitted with a data item, chose to give the resulting bitseven or odd parity. *Parity* refers to the number of bits set to 1 in the data item. There are 2 types of parity

- ***Even parity*** - an even number of bits are 1 Even parity - data: 10010001, parity bit 1
- ***Odd parity*** - an odd number of bits are 1 Odd parity - data: 10010111, parity bit 0
-

The stream of data is broken up into blocks of bits, and the number of 1 bits is counted. Then, a "parity bit" is set (or cleared) if the number of one bits is odd (or even).This scheme is called even parity; odd parity can also be used. There is a limitation to parity schemes. A parity bit is only guaranteed to detect an odd number of bit errors (one, three, five, and so on). If an even number of bits (two, four, six and so on) are flipped, the parity bit appears to be correct, even though the data is corrupt. For example

- Original data and parity: 10010001+1 (even parity)
- Incorrect data: 10110011+1 (even parity!)

Parity usually used to catch one-bit errors

Checksum : A checksum of a message is an arithmetic sum of message code words of a certain word length, for example byte values, and their carry value. The sum is negated by means of ones-complement, and stored or transferred as an extra code word extending the message. On the receiver side, a new checksum may be calculated, from the extended message.

If the new checksum is not 0, error is detected.Checksum schemes include parity bits, check digits, and longitudinal redundancy check. Suppose we have a fairly long message, which can reasonably be divided into shorter words (a 128 byte message, for instance). We can introduce an accumulator with the same width as a word (one byte, for instance), and as each word comes in, add it to the accumulator.

When the last word has been added, the contents of the accumulator are appended to the message (as a 129th byte, in this case). The added word is called a *checksum*. Now, the receiver performs the same operation, and checks the checksum. If the checksums agree, we assume the message was sent without error.

Hamming Distance Based Checks : If we want to detect d bit errors in an n bit word we can map every n bit word into a bigger n+d+1 bit word so that the minimum Hamming distance between each valid mapping is d+1.

This way, if one receives n+d+1 bit word that doesn't match any word in the mapping (with a Hamming distance x <= d+1 from any word in the mapping) it can successfully detect it as an errored word. Even more, d or fewer errors will never transform a valid word into another, because the Hamming distance between each valid word is at least d+1, and such errors only lead to invalid words that are detected correctly.

Given a stream of m*n bits, we can detect x <= d bit errors successfully using the above method on every n bit word. In fact, we can detect a maximum of m*d errors if every n word is transmitted with maximum d errors. The *Hamming distance* between two bit strings is the number of bits you have to change to convert one to the other. The basic idea of an error correcting code is to use extra bits to increase the dimensionality of the hypercube, and make sure the Hamming distance between any two valid points is greater than one.

- If the Hamming distance between valid strings is only one, a single bit error results in another valid string. This means we can't detect an error.

- If it's two, then changing one bit results in an invalid string, and can be detected as an error. Unfortunately, changing just one more bit can result in another valid string, which means we can't detect which bit was wrong; so we can detect an error but not correct it.

- If the Hamming distance between valid strings is three, then changing one bit leaves us only one bit away from the original error, but two bits away from any other valid string. This means if we have a one-bit error, we can figure out which bit is the error; but if we have a two-bit error, it looks like one bit from the other direction. So we can have single bit correction, but that's all.

- Finally, if the Hamming distance is four, then we can correct a single-bit error and detect a double-bit error. This is frequently referred to as a SECDED (Single Error Correct, Double Error Detect) scheme.
-

Cyclic Redundancy Checks : For CRC following some of Peterson & Brown's notation here . . .

- ***k*** is the length of the message we want to send, *i.e.*, the number of information bits.

- ***n*** is the total length of the message we will end up sending the information bits followed by the check bits. Peterson and Brown call this a *code polynomial*.

- ***n-k*** is the number of check bits. It is also the degree of the generating polynomial. The basic (mathematical) idea is that we're going to pick the n-k check digits in such a way that the code polynomial is divisible by the generating polynomial. Then we send the data, and at the other end we look to see whether it's still divisible by the generating polynomial; if it's not then we know we have an error, if it is, we hope there was

no error. The way we calculate a CRC is we establish some predefined n-k+1 bit number P (called the Polynomial, for reasons relating to the fact that modulo-2 arithmetic is a special case of polynomial arithmetic). Now we append n-k 0's to our message, and divide the result by P using modulo-2 arithmetic. The remainder is called the Frame Check Sequence. Now we ship off the message with the remainder appended in place of the 0's. The receiver can either recompute the FCS or see if it gets the same answer, or it can just divide the whole message (including the FCS) by P and see if it gets a remainder of 0. As an example, let's set a 5-bit polynomial of 11001, and compute the CRC of a 16 bit message:

•

11001)10011101010101100000

11001

- - - - -

1010101010101100000

11001

- - - - -

1100010101011000 00

11001

- - - - -

00011010101100000

11001

- - - - -

0011101100000

11001

- - - - -

100100000

11001

- - - - -

10110000

11001

- - - - -

1111000

11001

- - - - -

11100

11001

- - - - -

0101

In division don't bother to keep track of the quotient; we don't care about the quotient. Our only goal here is to get the remainder (0101), which is the FCS. CRC's can actually be computed in hardware using a shiftregister and some number of exclusive-or gates.

Telephone System: Device that coverts sound and electrical waves into audible relays, and is used for communication. The telephone consists of two essential parts; a microphone and a speaker. This allows the user to speak into the device and also hear transmissions from the other user. The invention of the first telephone dates back to 1896. Some of the first telephones required an operator to connect calls between users, but with the advancement of technology, calls are now connected automatically. Telephones formally utilized analog signals to transmit sounds, but most calls are now placed over digital networks.

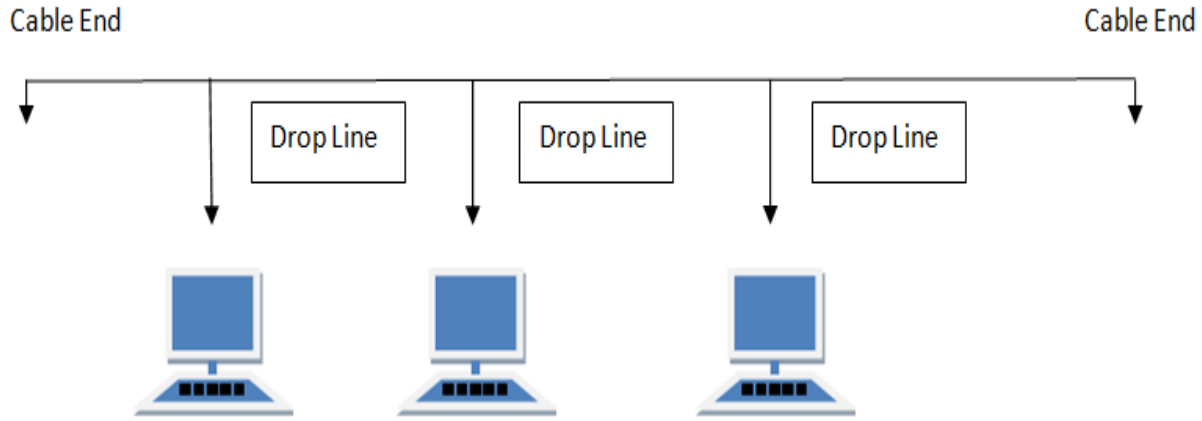
Telephones are made in a variety of forms, including a subset of the device called a cell phone or mobile phone. Also called phone.

UNIT- II

Network Topology is the schematic description of a network arrangement, connecting various nodes(sender and receiver) through lines of connection.

BUS Topology

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

Advantages of Bus Topology

1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

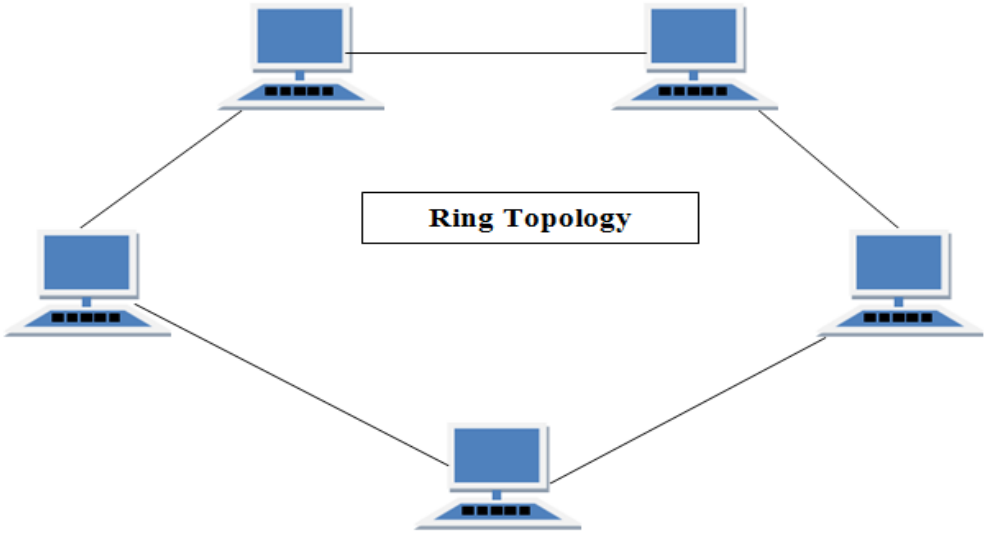
Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.

3. Cable has a limited length.
4. It is slower than the ring topology.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called **Dual Ring Topology**.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

Advantages of Ring Topology

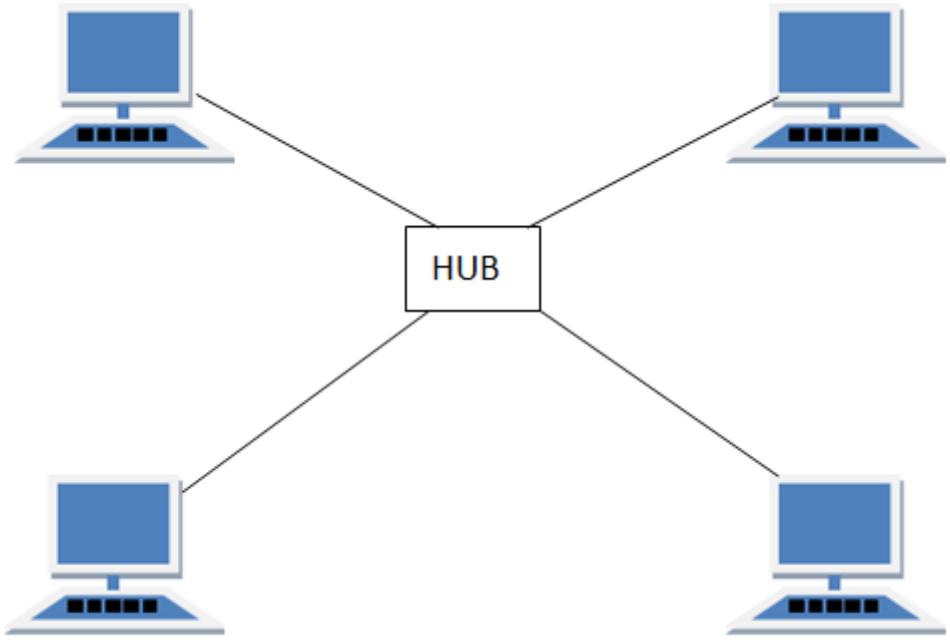
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

STAR Topology

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

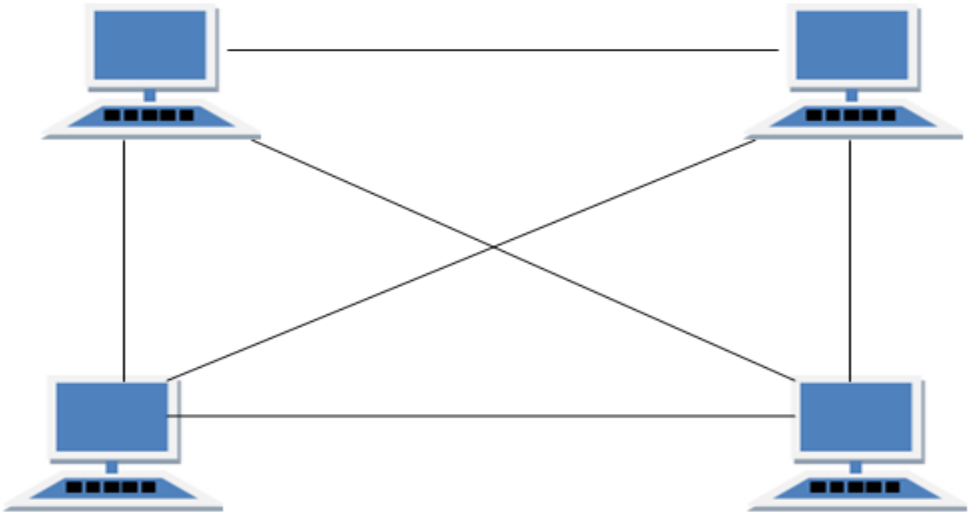
1. Routing
2. Flooding

Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



Types of Mesh Topology

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

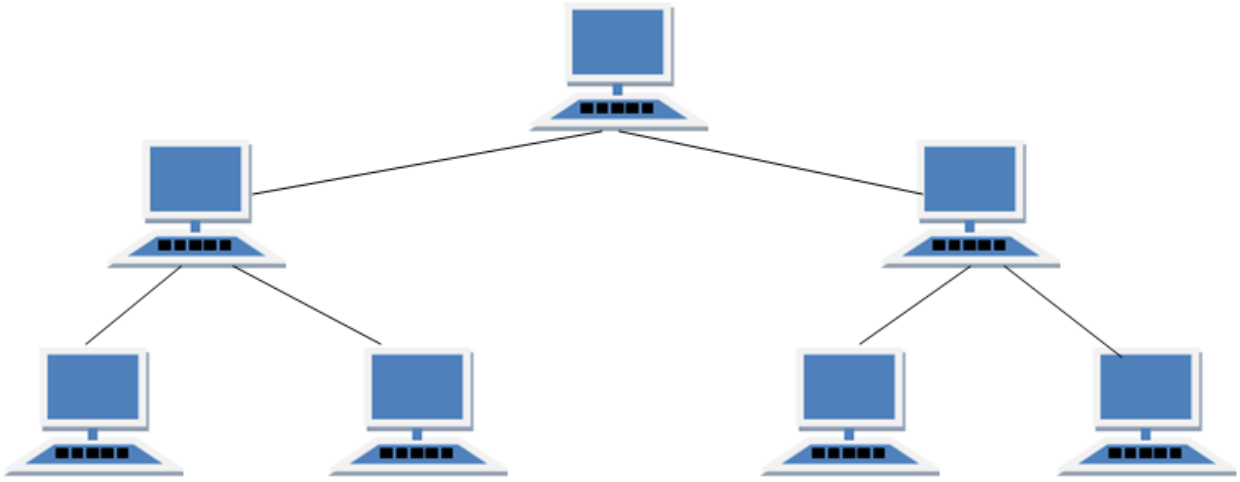
Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.

3. Bulk wiring is required.

TREE Topology

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

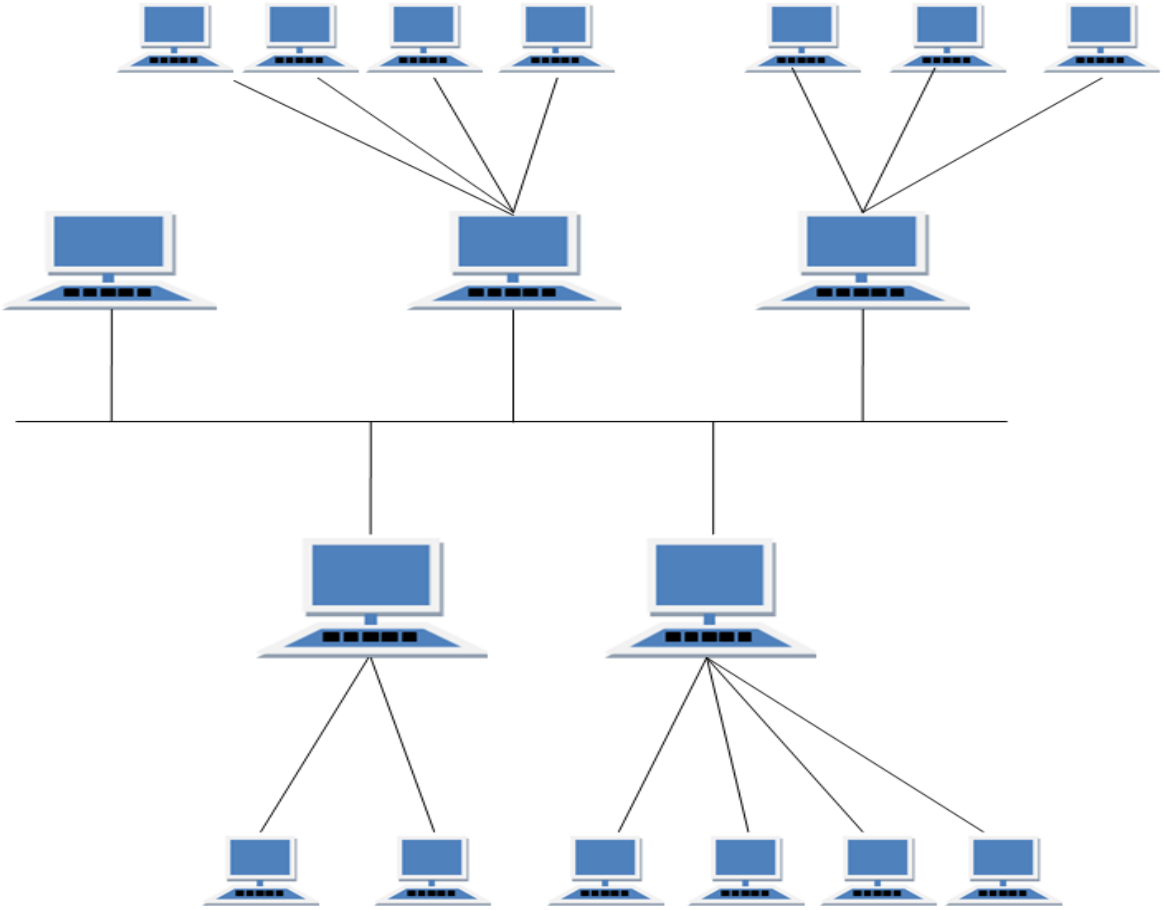
Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.

4. Central hub fails, network fails.

HYBRID Topology

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

Switching Techniques - In large networks there might be multiple paths linking sender and receiver. Information may be switched as it travels through various communication channels. There are four typical switching techniques available for digital traffic.

* Circuit Switching
* Packet Switching
* Message Switching
* Cell Switching

Circuit Switching :

- Circuit switching is a technique that directly connects the sender and the receiver in an unbroken path.
- Telephone switching equipment, for example, establishes a path that connects the caller's telephone to the receiver's telephone by making a physical connection.
- With this type of switching technique, once a connection is established, a dedicated path exists between both ends until the connection is terminated.
- Routing decisions must be made when the circuit is first established, but there are no decisions made after that time
- Circuit switching in a network operates almost the same way as the telephone system works.
- A complete end-to-end path must exist before communication can take place.
- The computer initiating the data transfer must ask for a connection to the destination.
- Once the connection has been initiated and completed to the destination device, the destination device must acknowledge that it is ready and willing to carry on a transfer.

Advantages:

- The communication channel (once established) is dedicated.

Disadvantages:

- Possible long wait to establish a connection, (10 seconds, more on long- distance or international calls.) during which no data can be transmitted.
- More expensive than any other switching techniques, because a dedicated path is required for each connection.
- Inefficient use of the communication channel, because the channel is not used when the connected systems are not using it.

Packet Switching

* Packet switching can be seen as a solution that tries to combine the advantages of message and circuit switching and to minimize the disadvantages of both.
* There are two methods of packet switching: Datagram and virtual circuit.
* In both packet switching methods, a message is broken into small parts, called packets.
* Each packet is tagged with appropriate source and destination addresses.
* Since packets have a strictly defined maximum length, they can be stored in main memory instead of disk; therefore access delay and cost are minimized.
* Also the transmission speeds, between nodes, are optimized.
* With current technology, packets are generally accepted onto the network on a first-come, first-served basis. If the network becomes overloaded, packets are delayed or discarded (``dropped").
The size of the packet can vary from 180 bits, the size for the Datakit virtual circuit switch designed by Bell Labs for communications and business applications; to 1,024 or 2,048 bits for the 1PSS switch, also designed by Bell Labs for public data networking; to 53 bytes for ATM switching, such as Lucent Technologies' packet switches
* In packet switching, the analog signal from your phone is converted into a digital data stream. That series of digital bits is then divided into relatively tiny clusters of bits, called packets. Each packet has at its beginning the digital address -- a long number -- to which it is being sent. The system blasts out all those tiny packets, as fast as it can, and they travel across the nation's digital backbone systems to their destination: the telephone, or rather the telephone system, of the person you're calling.
* They do not necessarily travel together; they do not travel sequentially. They don't even all travel via the same route.
But eventually they arrive at the right point -- that digital address added to the front of each string of digital data -- and at their destination are reassembled into the correct order, then converted to analog form, so your friend can understand what you're saying.
* Datagram packet switching is similar to message switching in that each packet is a self-contained unit with complete addressing information attached.
* This fact allows packets to take a variety of possible paths through the network.
* So the packets, each with the same destination address, do not follow the same route, and they may arrive out of sequence at the exit point node (or the destination).
* Reordering is done at the destination point based on the sequence number of the packets.
* It is possible for a packet to be destroyed if one of the nodes on its way is crashed momentarily. Thus all its queued packets may be lost.
* In the virtual circuit approach, a preplanned route is established before any data packets are sent.
* A logical connection is established when a sender send a "call request packet" to the receiver and the receiver send back an acknowledge packet "call accepted packet" to the sender if the receiver agrees on conversational parameters.
• The conversational parameters can be maximum packet sizes, path to be taken, and other variables necessary to establish and maintain the conversation.
• Virtual circuits imply acknowledgements, flow control, and error control, so virtual circuits are reliable. That is, they have the capability to inform upper-protocol layers if a transmission problem occurs
• In virtual circuit, the route between stations does not mean that this is a dedicated path, as in circuit switching.
* A packet is still buffered at each node and queued for output over a line.
• The difference between virtual circuit and datagram approaches:
* With virtual circuit, the node does not need to make a routing decision for each packet.
* It is made only once for all packets using that virtual circuit. VC's offer guarantees that the packets sent arrive in the order sent with no duplicates or omissions with no errors (with high probability) regardless of how they are implemented internally

Advantages:

• Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.

• Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).

• Packet can be rerouted if there is any problem, such as, busy or disabled links.

* The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth.

Disadvantages:

• Protocols for packet switching are typically more complex.

• It can add some initial costs in implementation.

• If packet is lost, sender needs to retransmit the data. Another disadvantage is that packet-switched systems still can't deliver the same quality as dedicated circuits in applications requiring very little delay - like voice conversations or moving images.

Message Switching

- With message switching there is no need to establish a dedicated path between two stations.
- When a station sends a message, the destination address is appended to the message.
- The message is then transmitted through the network, in its entirety, from node to node.
- Each node receives the entire message, stores it in its entirety on disk, and then transmits the message to the next node.
- This type of network is called a store-and-forward network.

A message-switching node is typically a general-purpose computer. The device needs sufficient secondary-storage capacity to store the incoming messages, which could be long. A time delay is introduced using this type of scheme due to store- and-forward time, plus the time required to find the next node in the transmission path.

Advantages:

- Channel efficiency can be greater compared to circuit-switched systems, because more devices are sharing the channel.
- Traffic congestion can be reduced, because messages may be temporarily stored in route.
- Message priorities can be established due to store-and-forward technique.
- Message broadcasting can be achieved with the use of broadcast address appended in the message

Disadvantages

- Message switching is not compatible with interactive applications.
- Store-and-forward devices are expensive, because they must have large disks to hold potentially long messages

Cell Switching

Cell Switching is similar to packet switching, except that the switching does not necessarily occur on packet boundaries. This is ideal for an integrated environment and is found within Cell-based networks, such as ATM. Cell-switching can handle both digital voice and data signals.

Computer Network: Computer network is collection of related system which are capable of exchanging their information at a remote distance.There are so many different types of computer networks in existence, it can be hard to understand the differences between them, particularly the ones with very similar-sounding names. This lesson explains the structures and functions of some of the most popular computer networks.

Types of Networks

There are several different types of computer networks. Computer networks can be characterized by their size as well as their purpose.

The size of a network can be expressed by the geographic area they occupy and the number of computers that are part of the network. Networks can cover anything from a handful of devices within a single room to millions of devices spread across the entire globe.

Some of the different networks based on size are:

1. Personal area network, or PAN
2. Local area network, or LAN
3. Metropolitan area network, or MAN
4. Wide area network, or WAN

In terms of purpose, many networks can be considered general purpose, which means they are used for everything from sending files to a printer to accessing the Internet. Some types of networks, however, serve a very particular purpose. Some of the different networks based on their main purpose are:

1. Storage area network, or SAN
2. Enterprise private network, or EPN
3. Virtual private network, or VPN

Personal Area Network

A personal area network, or PAN, is a computer network organized around an individual person within a single building. This could be inside a small office or residence. A typical PAN would include one or more computers, telephones, peripheral devices, video game consoles and other personal entertainment devices.

If multiple individuals use the same network within a residence, the network is sometimes referred to as a home area network, or HAN. In a very typical setup, a residence will have a single wired Internet connection connected to a modem. This modem then provides both wired and wireless connections for multiple devices. The network is typically managed from a single computer but can be accessed from any device.

This type of network provides great flexibility. For example, it allows you to:

Send a document to the printer in the office upstairs while you are sitting on the couch with your laptop.

Upload a photo from your cell phone to your desktop computer.

Watch movies from an online streaming service to your TV.

If this sounds familiar to you, you likely have a PAN in your house without having called it by its name.

Local Area Network

A local area network, or LAN, consists of a computer network at a single site, typically an individual office building. A LAN is very useful for sharing resources, such as data storage and printers. LANs can be built with relatively inexpensive hardware, such as hubs, network adapters and Ethernet cables.

The smallest LAN may only use two computers, while larger LANs can accommodate thousands of computers. A LAN typically relies mostly on wired connections for increased speed and security, but wireless connections can also be part of a LAN. High speed and relatively low cost are the defining characteristics of LANs.

LANs are typically used for single sites where people need to share resources among themselves but not with the rest of the outside world. Think of an office building where everybody should be able to access files on a central server or be able to print a document to one or more central printers. Those tasks should be easy for everybody working in the same office, but you would not want somebody just walking outside to be able to send a document to the printer from their cell phone! If a local area network, or LAN, is entirely wireless, it is referred to as a wireless local area network, or WLAN.

Metropolitan Area Network

A metropolitan area network, or MAN, consists of a computer network across an entire city, college campus or small region. A MAN is larger than a LAN, which is typically limited to a single building or site. Depending on the configuration, this type of network can cover an area from several miles to tens of miles. A MAN is often used to connect several LANs together to form a bigger network. When this type of network is specifically designed for a college campus, it is sometimes referred to as a campus area network, or CAN.

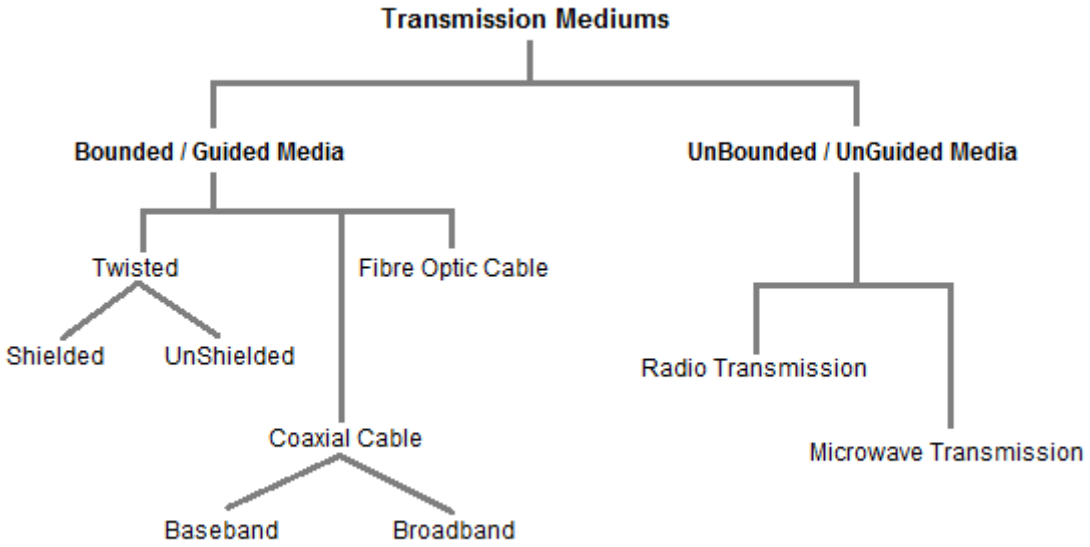
Wide Area Network

A wide area network, or WAN, occupies a very large area, such as an entire country or the entire world. A WAN can contain multiple smaller networks, such as LANs or MANs. The Internet is the best-known example of a public WAN.

Networking Medium:

Data is represented by computers and other telecommunication devices using signals. Signals are transmitted in the form of electromagnetic energy from one device to another. Electromagnetic signals travel through vacuum, air or other transmission mediums to travel between one point to another(from source to receiver). Electromagnetic energy (includes electrical and magnetic fields) includes power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.

Transmission medium is the means through which we send our data from one place to another. The first layer (physical layer) of Communication Networks OSI Seven layer model is dedicated to the transmission media, we will study the OSI Model later.



Factors to be considered while choosing Transmission Medium

1. Transmission Rate
2. Cost and Ease of Installation
3. Resistance to Environmental Conditions
4. Distances

Bounded/Guided Transmission Media

It is the transmission media in which signals are confined to a specific path using wire or cable. The types of Bounded/ Guided are discussed below.

Twisted Pair Cable

This cable is the most commonly used and is cheaper than others. It is lightweight, cheap, can be installed easily, and they support many different types of network. Some important points :

- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 μs/km.
- Repeater spacing is 2km.

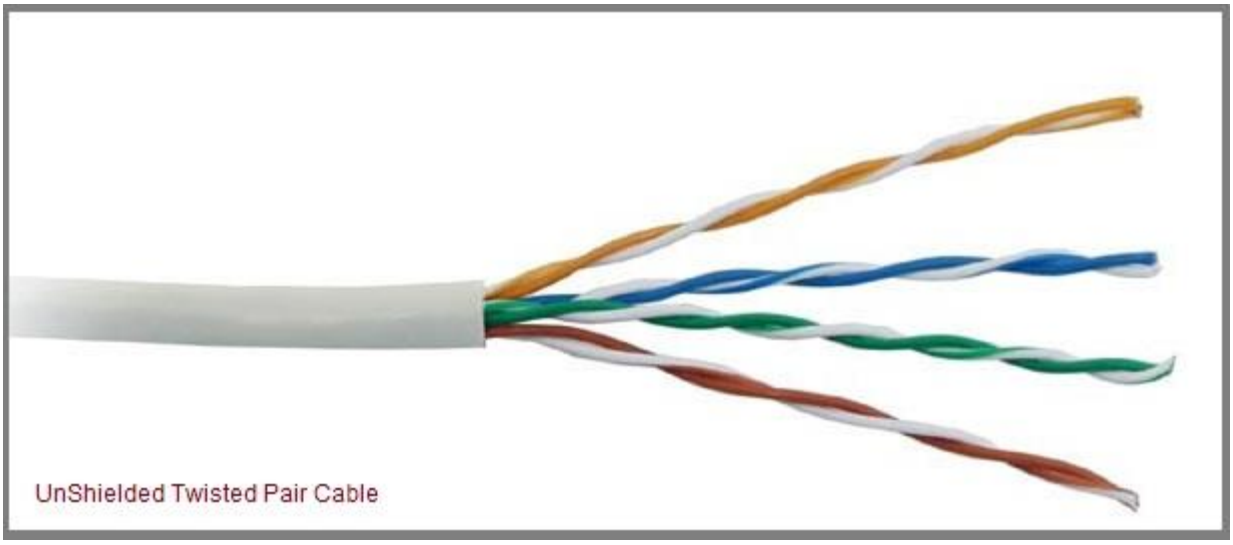
Twisted Pair is of two types :

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

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. Cable with 2 pair use **RJ-11** connector and 4 pair cable use**RJ-45** connector.



Advantages :

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages :

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

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 (explained in KEY TERMS Chapter).

It has same attenuation as unshielded twisted pair. It is faster the unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

Advantages :

- 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 :

- Difficult to manufacture
- Heavy

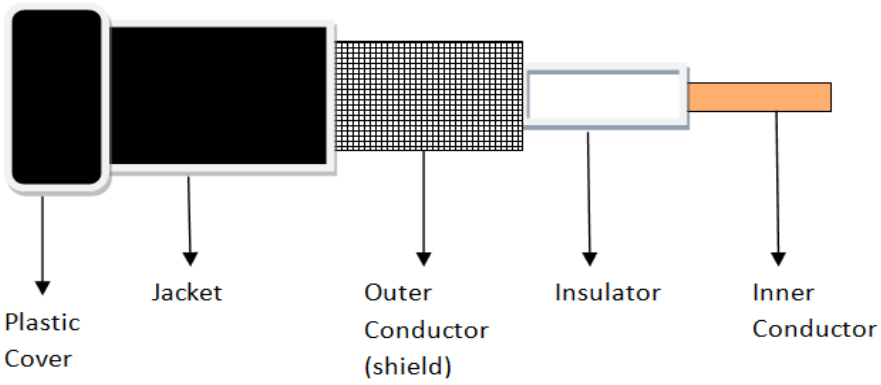
Coaxial Cable

Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as centre conductor which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath which is encased in an outer conductor of metal foil, barid or both.

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.



There are two types of Coaxial cables :

BaseBand

This is a 50 ohm (Ω) coaxial cable which is used for digital transmission. It is mostly used for LAN's. Baseband transmits a single signal at a time with very high speed. The major drawback is that it needs amplification after every 1000 feet.

BroadBand

This uses analog transmission on standard cable television cabling. It transmits several simultaneous signal using different frequencies. It covers large area when compared with Baseband Coaxial Cable.

Advantages :

- 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 :

- 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.

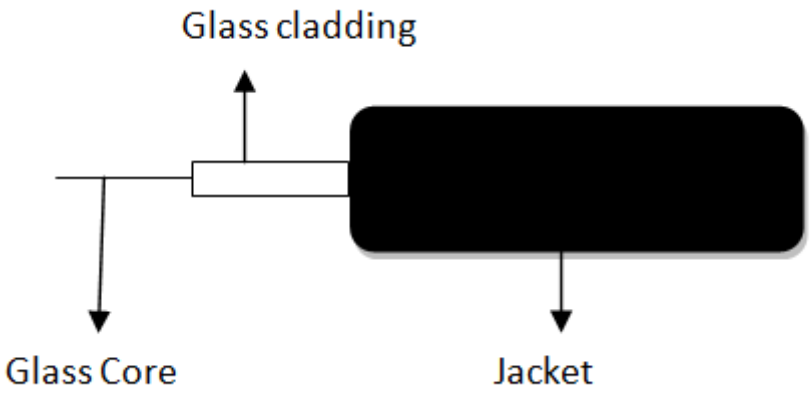
Fiber Optic Cable

These are similar to coaxial cable. It uses electric signals to transmit data. At the centre is the glass core through which light propagates.

In multimode fibres, the core is 50microns, and In single mode fibres, the thickness is 8 to 10 microns.

The core in fiber optic cable is surrounded by glass cladding with lower index of refraction as compared to core to keep all the light in core. This is covered with a thin plastic jacket to protect the cladding. The fibers are grouped together in bundles protected by an outer shield.

Fiber optic cable has bandwidth more than **2 gbps (Gigabytes per Second)**



Advantages :

- Provides high quality transmission of signals at very high speed.
- These are not affected by electromagnetic interference, so noise and distortion is very less.
- Used for both analog and digital signals.

Disadvantages :

- It is expensive
- Difficult to install.
- Maintenance is expensive and difficult.
- Do not allow complete routing of light signals.

UnBounded/UnGuided Transmission Media

Unguided or wireless media sends the data through air (or water), which is available to anyone who has a device capable of receiving them. Types of unguided/ unbounded media are discussed below :

- Radio Transmission
- MicroWave Transmission

Radio Transmission

Its frequency is between 10 kHz to 1GHz. It is simple to install and has high attenuation. These waves are used for multicast communications.

Types of Propogation

Radio Transmission utilizes different types of propogation :

- **Troposphere :** The lowest portion of earth's atmosphere extending outward approximately 30 miles from the earth's surface. Clouds, jet planes, wind is found here.
- **Ionosphere :** The layer of the atmosphere above troposphere, but below space. Contains electrically charged particles.

Microwave Transmission

It travels at high frequency than the radio waves. It requires the sender to be inside of the receiver. It operates in a system with a low gigahertz range. It is mostly used for unicast communication.

There are 2 types of Microwave Transmission :

1. Terrestrial Microwave
2. Satellite Microwave

Advantages of Microwave Transmission

- Used for long distance telephone communication
- Carries 1000's of voice channels at the same time

Disadvantages of Microwave Transmission

- It is Very costly

Terrestrial Microwave

For increasing the distance served by terrestrial microwave, repeaters can be installed with each antenna .The signal received by an antenna can be converted into transmittable form and relayed to next antenna as shown in below figure. It is an example of telephone systems all over the world

There are two types of antennas used for terrestrial microwave communication :

1. Parabolic Dish Antenna

In this every line parallel to the line of symmetry reflects off the curve at angles in a way that they intersect at a common point called focus. This antenna is based on geometry of parabola.

2. Horn Antenna

It is a like gigantic scoop. The outgoing transmissions are broadcast up a stem and deflected outward in a series of narrow parallel beams by curved head.

Satellite Microwave

This is a microwave relay station which is placed in outer space. The satellites are launched either by rockets or space shuttles carry them.

These are positioned 3600KM above the equator with an orbit speed that exactly matches the rotation speed of the earth. As the satellite is positioned in a geo-synchronous orbit, it is stationery relative to earth and always stays over the same point on the ground. This is usually done to allow ground stations to aim antenna at a fixed point in the sky.

Features of Satellite Microwave :

- Bandwidth capacity depends on the frequency used.
- Satellite microwave deployment for orbiting satellite is difficult.

Advantages of Satellite Microwave :

- Transmitting station can receive back its own transmission and check whether the satellite has transmitted information correctly.

- A single microwave relay station which is visible from any point.

Disadvantages of Satellite Microwave :

- Satellite manufacturing cost is very high
- Cost of launching satellite is very expensive
- Transmission highly depends on whether conditions, it can go down in bad weather

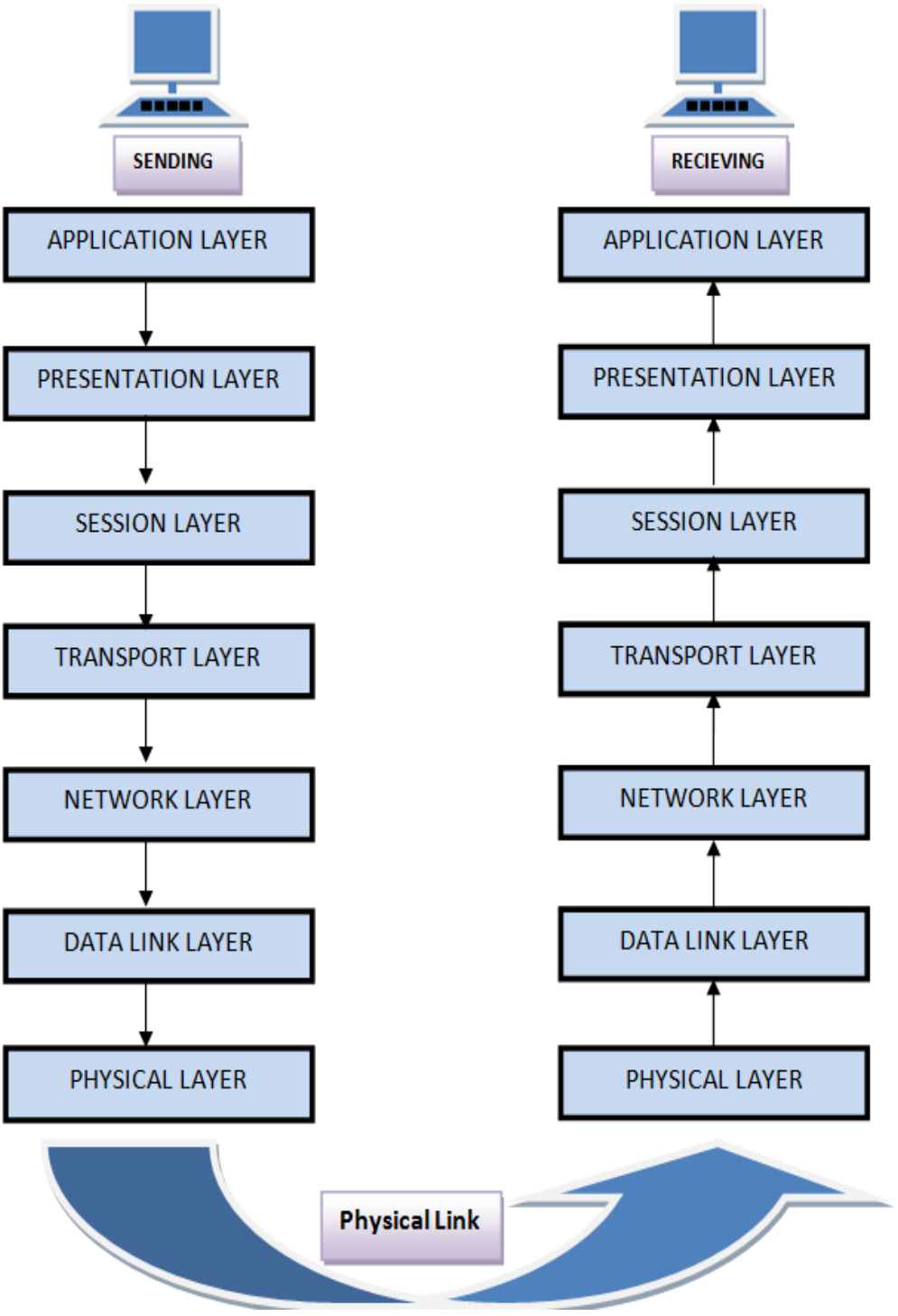
Reference Models in Communication Networks

The most important reference models are :

1. OSI reference model.
2. TCP/IP reference model.

Introduction to ISO-OSI Model:

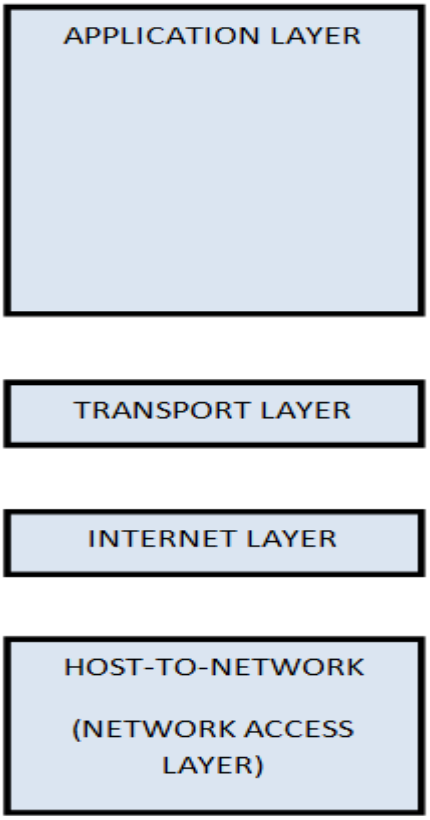
There are many users who use computer network and are located all over the world. To ensure national and worldwide data communication ISO (ISO stands for International Organization of Standardization.) developed this model. This is called a model for open system interconnection (OSI) and is normally called as OSI model.OSI model architecture consists of seven layers. It defines seven layers or levels in a complete communication system. OSI Reference model is explained in other chapter.



Introduction to TCP/IP REFERENCE Model

TCP/IP is transmission control protocol and internet protocol. Protocols are set of rules which govern every possible communication over the internet. These protocols describe the movement of data between the host computers or internet and offers simple naming and addressing schemes.

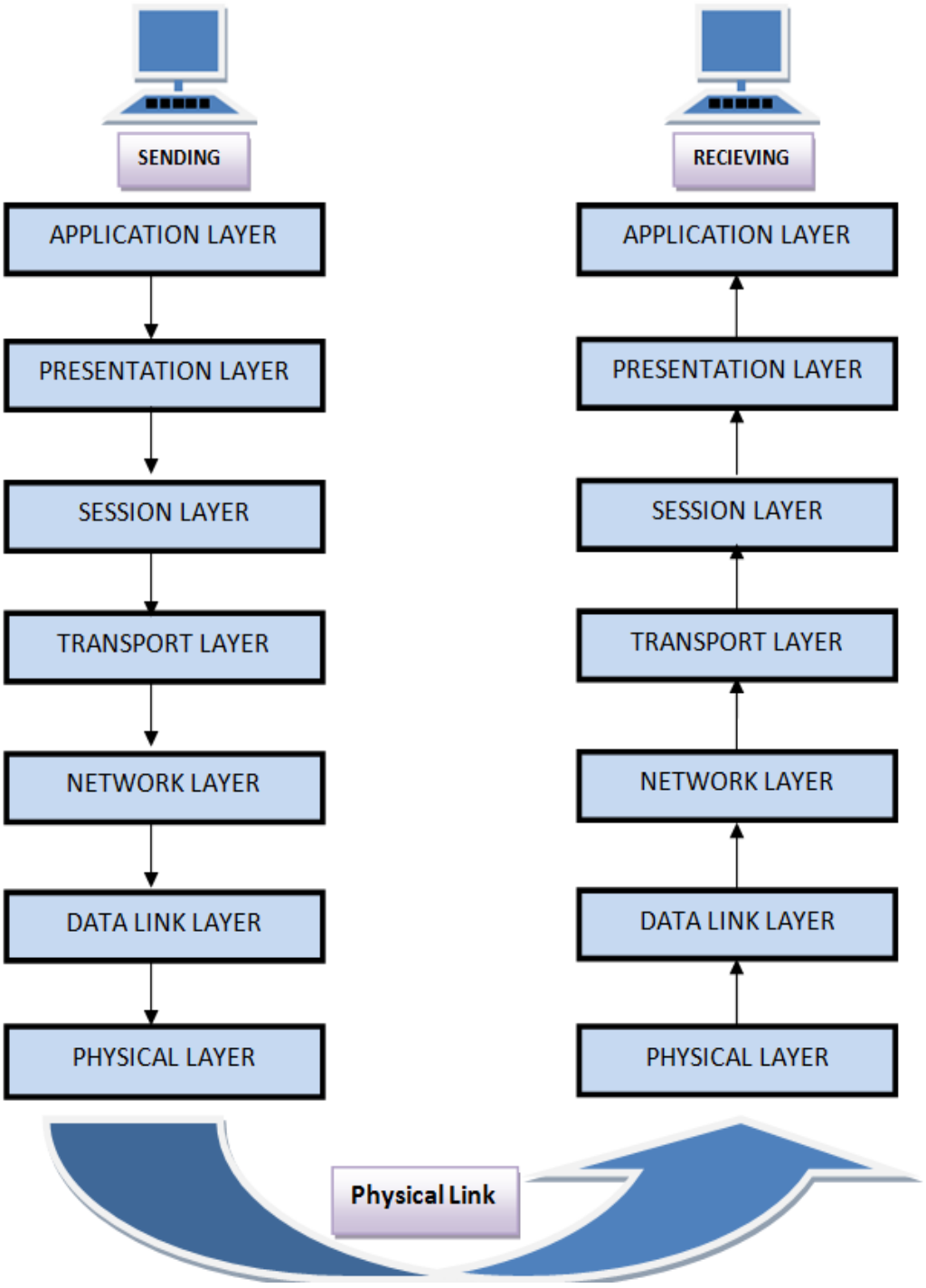
TCP/IP Reference model is explained in details other chapter.



ISO/OSI Model in Communication Networks

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other. ISO has developed this. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system.



Feature of OSI Model :

1. Big picture of communication over network is understandable through this OSI model.

2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Functions of Different Layers :

Layer 1: The Physical Layer :

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

Layer 2: Data Link Layer :

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

Layer 3: The Network Layer :

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Layer 4: Transport Layer :

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer :

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Layer 6: The Presentation Layer :

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages(syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.

4. It perfroms Data compression, Data encryption, Data conversion etc.

Layer 7: Application Layer :

1. It is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model:

1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model:

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

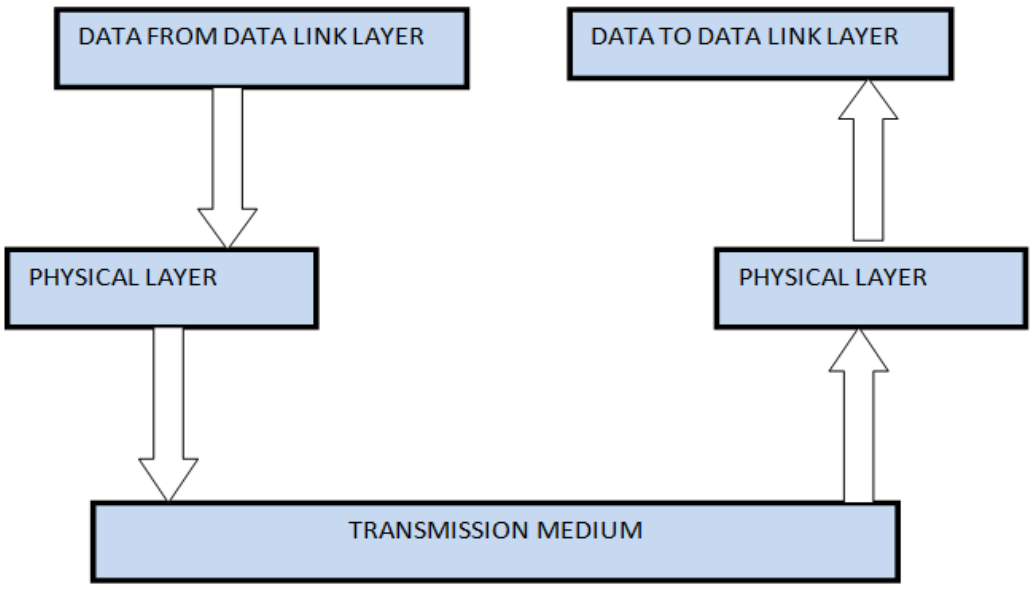
PHYSICAL Layer - OSI Model

Physical layer is the lowest layer of all. It is responsible for sending bits from one computer to another. This layer is not concerned with the meaning of the bits and deals with the physical connection to the network and with transmission and reception of signals.

This layer defines electrical and physical details represented as 0 or a 1. How many pins a network will contain, when the data can be transmitted or not and how the data would be synchronized.

FUNCTIONS OF PHYSICAL LAYER:

1. **Representation of Bits:** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.
2. **Data Rate:** This layer defines the rate of transmission which is the number of bits per second.
3. **Synchronization:** It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
4. **Interface:** The physical layer defines the transmission interface between devices and transmission medium.
5. **Line Configuration:** This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.
6. **Topologies:** Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.
7. **Transmission Modes:** Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, Full Duplex.
8. Deals with baseband and broadband transmission.

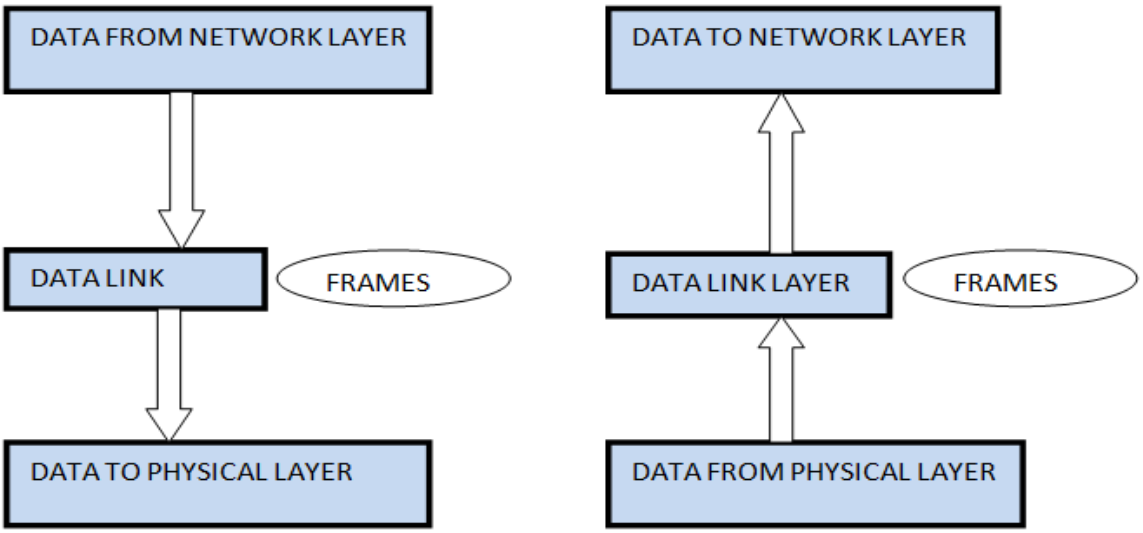


Data link layer is most reliable node to node delivery of data. It forms frames from the packets that are received from network layer and gives it to physical layer. It also synchronizes the information which is to be transmitted over the data. Error controlling is easily done. The encoded data are then passed to physical.

Error detection bits are used by the data link layer. It also corrects the errors. Outgoing messages are assembled into frames. Then the system waits for the acknowledgements to be received after the transmission. It is reliable to send message.

FUNCTIONS OF DATA LINK LAYER:

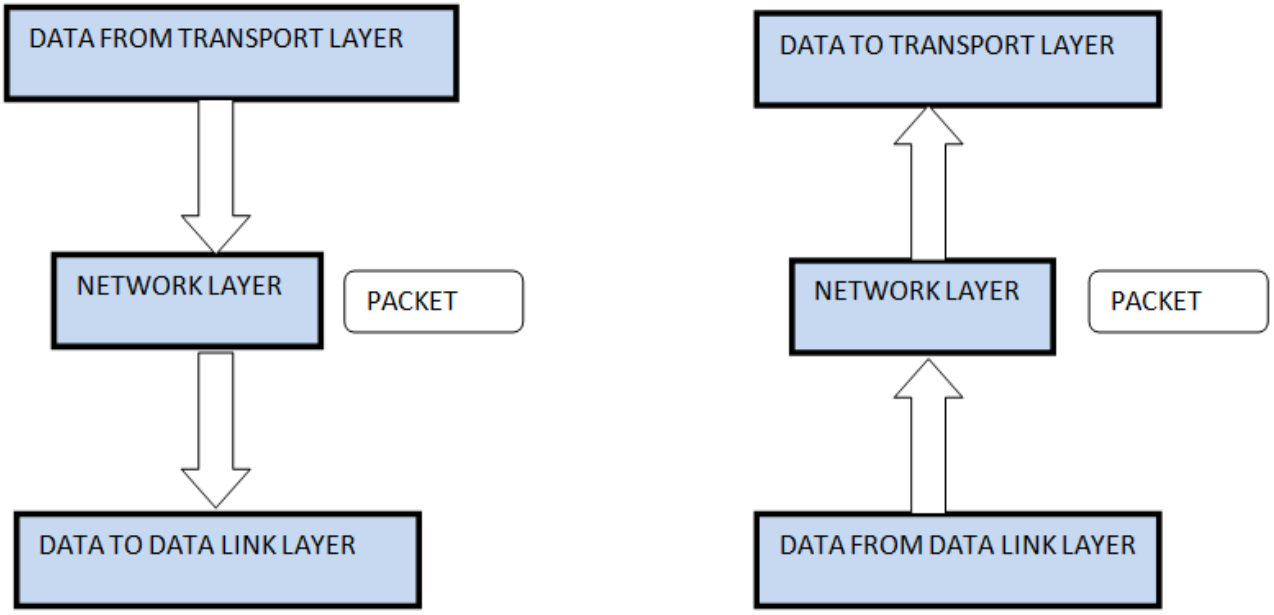
1. **Framing:** Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
2. **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.
3. **Flow Control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
4. **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
5. **Access Control:** Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



Network Layer - OSI Model

The main aim of this layer is to deliver packets from source to destination across multiple links (networks). If two computers (system) are connected on the same link then there is no need for a network layer. It routes the signal through different channels to the other end and acts as a network controller.

It also divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels.



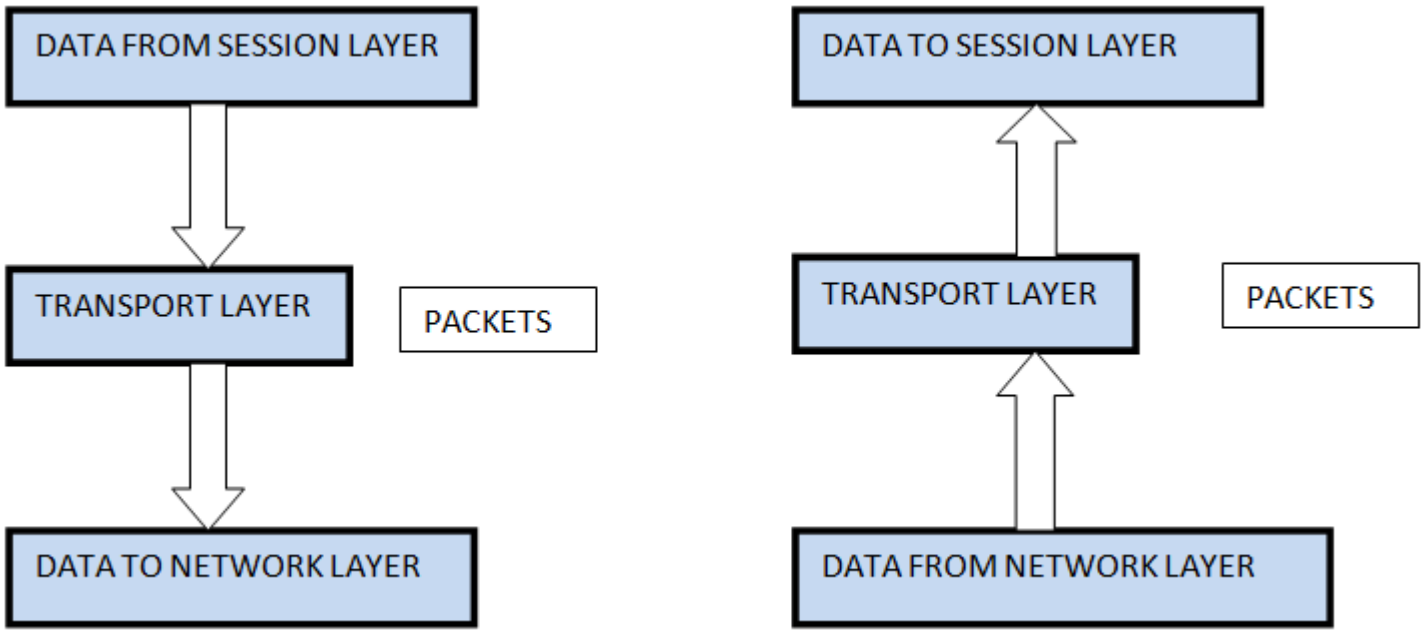
FUNCTIONS OF NETWORK LAYER:

1. It translates logical network address into physical address. Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.

Transport Layer - OSI Model

The main aim of transport layer is to be delivered the entire message from source to destination. Transport layer ensures whole message arrives intact and in order, ensuring both error control and flow control at the source to destination level. It decides if data transmission should be on parallel path or single path

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer and ensures that message arrives in order by checking error and flow control.

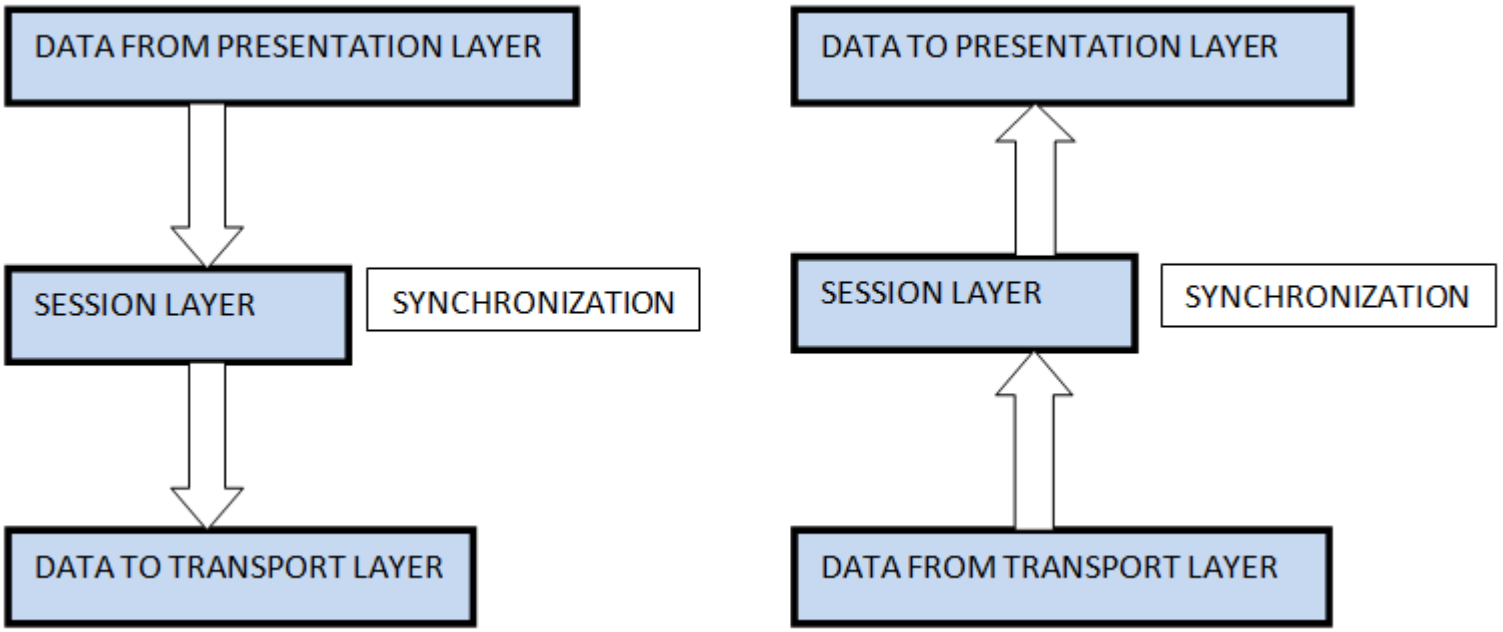


FUNCTIONS OF TRANSPORT LAYER:

1. **Service Point Addressing :** Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
2. **Segmentation and Reassembling :** A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.
3. **Connection Control :** It includes 2 types :
   - Connectionless Transport Layer : Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
   - Connection Oriented Transport Layer : Before delivering packets, connection is made with transport layer at the destination machine.
4. **Flow Control :** In this layer, flow control is performed end to end.
5. **Error Control :** Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.

Session Layer - OSI Model

Its main aim is to establish, maintain and synchronize the interaction between communicating systems. Session layer manages and synchronize the conversation between two different applications. Transfer of data from one destination to another session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

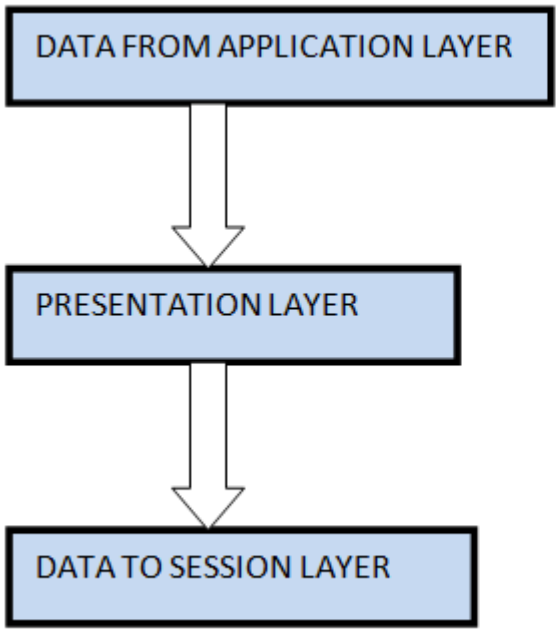


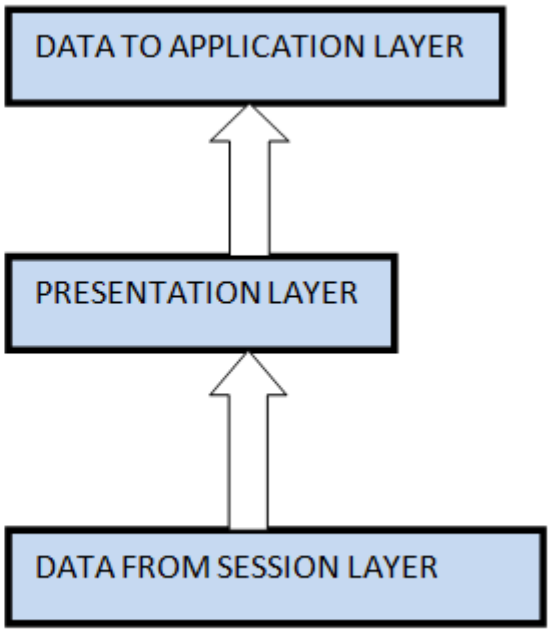
FUNCTIONS OF SESSION LAYER:

1. **Dialog Control :** This layer allows two systems to start communication with each other in half-duplex or full-duplex.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. Example: If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended. This ensures that 50 page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.

Presentation Layer - OSI Model

The primary goal of this layer is to take care of the syntax and semantics of the information exchanged between two communicating systems. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.



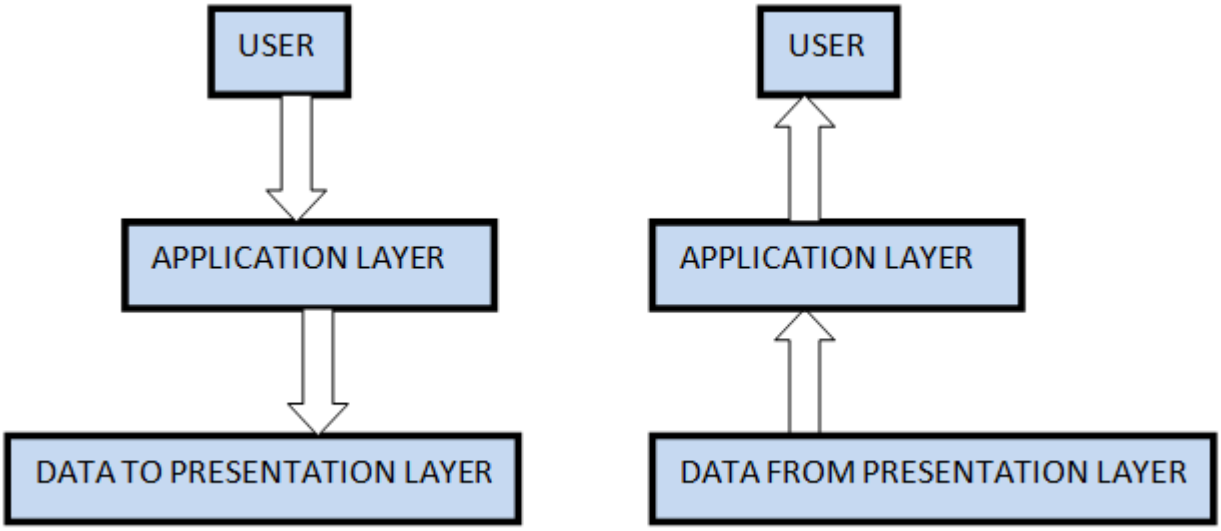


FUNCTIONS OF PRESENTATION LAYER:

1. **Translation :** Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.
2. **Encryption :** It carries out encryption at the transmitter and decryption at the receiver.
3. **Compression :** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be 0transmitted. It is important in transmitting multimedia such as audio, video, text etc.

Application Layer - OSI Model

It is the top most layer of OSI Model. Manipulation of data (information) in various ways is done in this layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring of files, distributing the results to user, directory services, network resource etc.



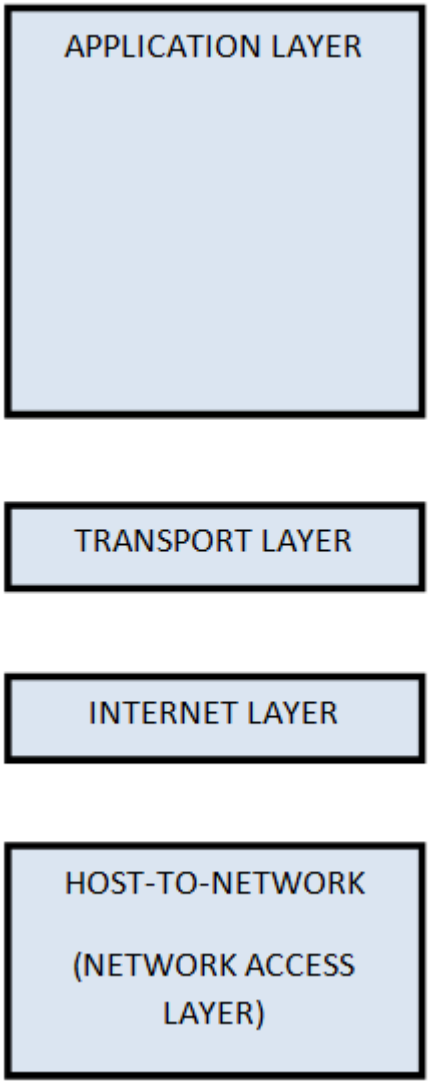
FUNCTIONS OF APPLICATION LAYER:

1. **Mail Services :** This layer provides the basis for E-mail forwarding and storage.
2. **Network Virtual Terminal :** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
3. **Directory Services :** This layer provides access for global information about various services.
4. **File Transfer, Access and Management (FTAM) :** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.

The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a

network. These protocols describe the movement of data between the source and destination or the internet. These protocols offer simple naming and addressing schemes.



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.

- The network was robust, and connections remained intact untill the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Description of different TCP/IP protocols

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP(File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP(Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS(Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.
4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol

8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model