

Q.1 Draw the tcp/ip network architectural model & explain the features of various layers. Iso list the important protocol at each layers & describe its purpose. Briefly describe the difference between the osi and tcp/ip architectural model?

Ans:

Introduction to Network Protocols

Just as diplomats use diplomatic protocols in their meetings, computers use network protocols to communicate in computer networks. There are many network protocols in existence; TCP/IP is a family of network protocols that are used for the Internet.

A **network protocol** is a standard written down on a piece of paper (or, more precisely, with a text editor in a computer). The standards that are used for the Internet are called **Requests for Comment (RFC)**. RFCs are numbered from 1 onwards. There are more than 4,500 RFCs today. Many of them have become out of date, so only a handful of the first thousand RFCs are still used today.

The **International Standardization Office (ISO)** has standardized a system of network protocols called as **ISO OSI**. Another organization that issues communication standards is the **International Telecommunication Union (ITU)** located in Geneva. The ITU was formerly known as the CCITT and, being founded in 1865, is one of the oldest worldwide organizations (for comparison, the Red Cross was founded in 1863). Some standards are also issued by the **Institute of Electrical and Electronics Engineers (IEEE)**. RFC, standards released by **RIPE (Réseaux IP Euro peens)**, and **PKCS (Public Key Cryptography Standard)** are freely available on the Internet and are easy to get hold of. Other organizations (ISO, ITU, and so on) do not provide their standards free of charge—you have to pay for them. If that presents a problem, then you have to spend some time doing some library research.

First of all, let's have a look at why network communication is divided into several protocols. The answer is simple although this is a very complex problem that reaches across many different professions. Most books concerning network protocols explain the problem using a metaphor of two foreigners (or philosophers, doctors, and so on) trying to communicate with each other. Each of the two can only communicate in his or her respective language. In order for them to be able to communicate with each other, they need a translator as shown in the following figure:

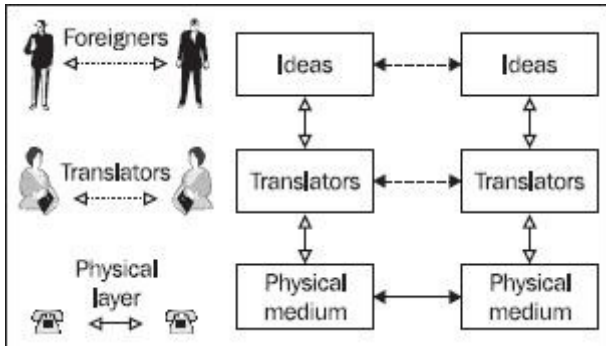


Figure 1.1: Three-layer communication architecture

The two foreigners exchange ideas, i.e., they communicate. But they only do so virtually. In reality, they are both handing over information to their interpreters, who then transmit this information by sending vibrations through the surrounding air with their vocal cords. Or if the parties are far away from each other, the interpreters communicate over the phone; thus the information is physically transmitted over phone lines. We can therefore talk about virtual communication in the horizontal direction (philosophical communication, the shared language between interpreters, and electronic signals transmitted via phone lines) and real communication in the vertical direction (foreigner-to-interpreter and interpreter-to-phone). We can thus distinguish three levels of communication:

1. Between two foreigners
2. Between interpreters
3. Physical transmission of information using media (phone lines, sound waves, etc.)

Communication between the two foreigners and between the two interpreters is only virtual. In fact, the only real communication happens between the foreigner and his or her interpreter.

Even more layers are used in computer networks. The number of layers depends on which system of network protocols you choose to use. The system of network protocols is sometimes referred to as the *network model*. You most commonly work with a system that uses the Internet, which is also referred to as the TCP/IP family. In addition to TCP/IP, we will also come across the ISO OSI model that was standardized by the ISO.

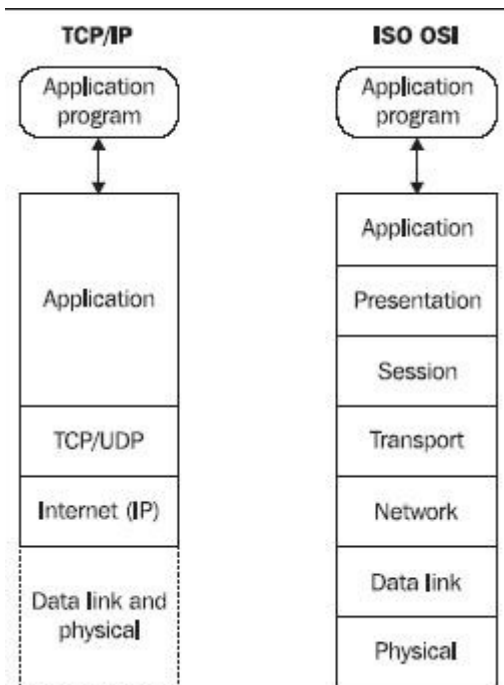


Figure 1.2: Comparison of TCP/IP and ISO OSI network models

The TCP/IP family uses four layers while ISO OSI uses seven layers as shown in the figure above. The TCP/IP and ISO OSI systems differ from each other significantly, although they are very similar on the network and transport layers.

Except for some exceptions like SLIP or PPP, the TCP/IP family does not deal with the link and physical layers. Therefore, even on the Internet, we use the link and physical protocols of the ISO OSI model.

1.1 ISO OSI

Communication between two computers is shown in the following figure:

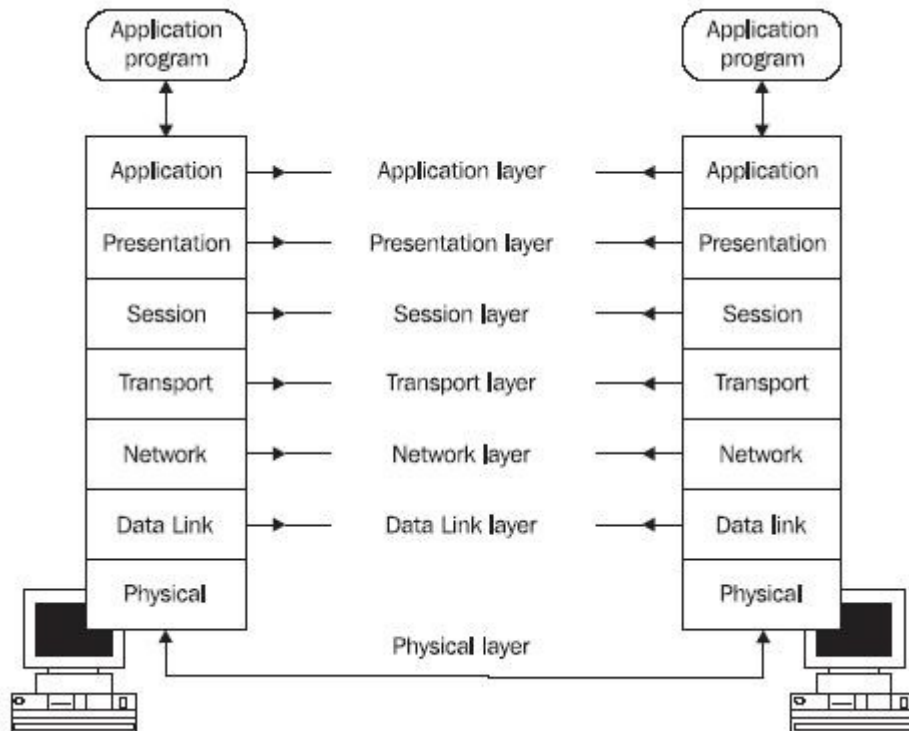


Figure 1.3: Seven-layer architecture of ISO OSI

1.1.1 Physical Layer

The physical layer is responsible for activating the physical circuit between the **Data Terminal Equipment (DTE)** and **Data Circuit-terminating Equipment (DCE)**, communicating through it, and then deactivating it. Additionally, the physical layer is also responsible for the communication between DCEs (see Figure 1.3a). A computer or router can represent the DTE. The DCE, on the other hand, is usually represented by a modem or a multiplexer.

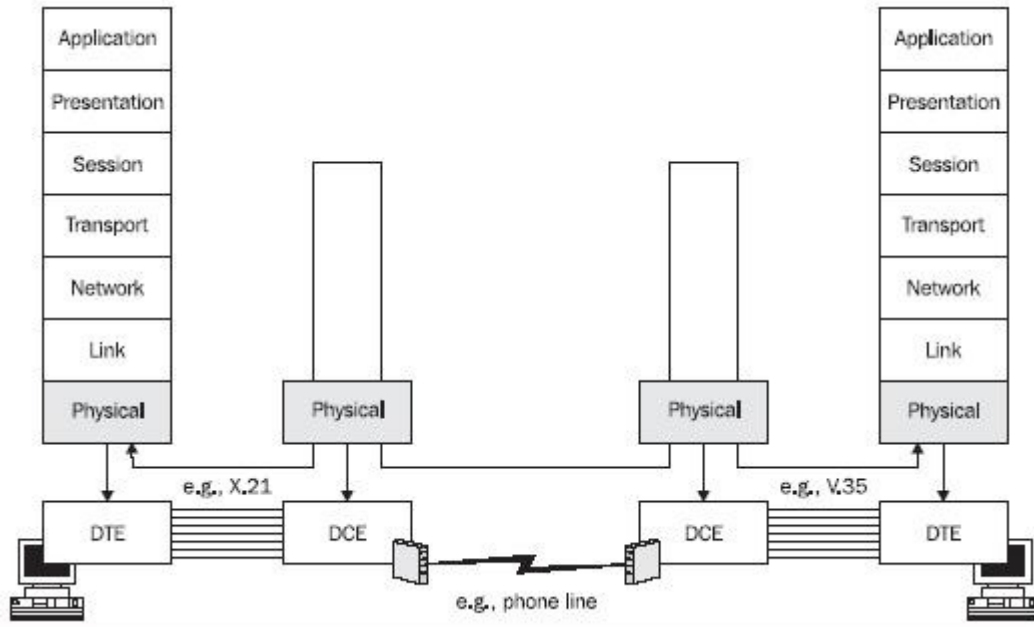


Figure 1.3a: DTE and DCE

To put it differently, the physical layer describes the electric or optical signals used for communicating between two computers. Physical circuits are created on the physical layer. Other appliances such as modems modulating a signal for a phone line are often put in the physical circuits created between two computers.

Physical layer protocols specify the following:

- Electrical signals (for example, +1V)
- Connector shapes (for example, V.35)
- Media type (twisted pair, coaxial cable, optical fiber, etc.)
- Modulation (for example, FM, PM, etc.)
- Coding (for example, RZ, NRZ, etc.)
- Synchronization (synchronous and asynchronous communication, time source, and so on)

1.1.2 Data Link Layer

As for serial links, the link layer provides data exchange between neighboring computers as well as data exchange between computers within a local network.

For the link layer, the basic unit of data transfer is the data link packet frame (see Figure 1.4). A data frame is composed of a header, payload, and trailer.

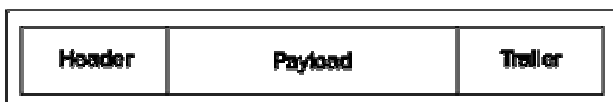


Figure 1.4: Data link packet or frame

A frame carries the destination link address, source link address, and other control information in the header. The trailer usually contains the checksum of the transported data. By using the checksum, we can find out whether the payload has been damaged during transfer. The network-layer packet is usually included in the payload.

In Figure 1.3a, the link layer does not engage in a conversation between DTE and DCE (the link layer *does not see* the DCE). It is engaged, however, in the frame exchange between DTEs. (It relies on the physical layer to handle the DCE issue.)

The following figure illustrates that different protocols can be used for each end of the connection on the physical layer. In our case, one of the ends uses the X.21 protocol while the other end uses the V.35 protocol. This rule is valid not only for serial links, but also for local networks. In local networks, you are more likely to encounter more complicated setups in which a switch that converts the link frames of one link protocol into link frames of a second one (for example, Ethernet into FDDI) is inserted between the two ends of the connection. This obviously results in different protocols being used on the physical layer.

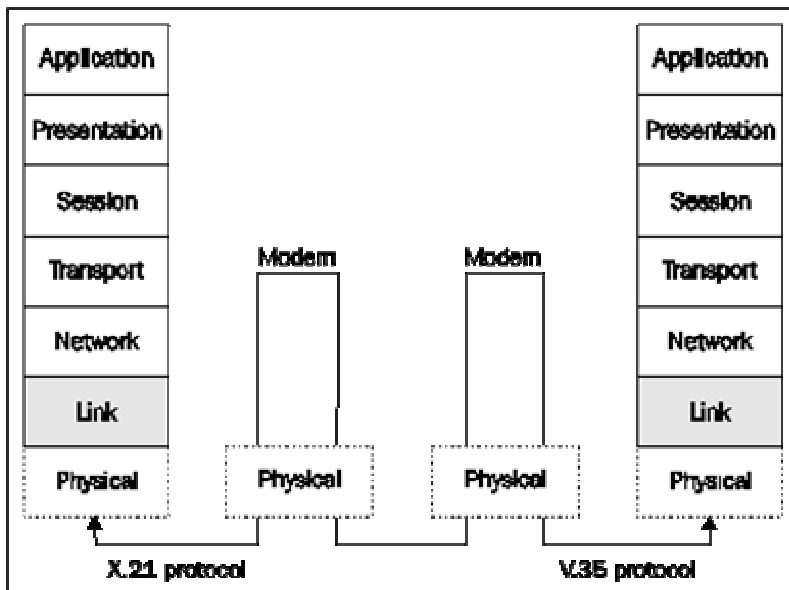


Figure 1.5: Link layer communication

A serial port or an Ethernet card can serve as a link interface. A link interface has a link address that is unique within a particular **Local Area Network (LAN)**.

1.1.3 Network Layer

The network layer ensures the data transfer between two remote computers within a particular **Wide Area Network (WAN)**. The basic unit of transfer is a datagram that is wrapped (encapsulated) in a frame. The datagram is also composed of a header and data field. Trailers are not very common in network protocols.

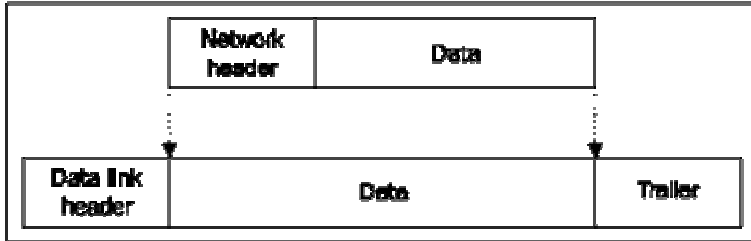


Figure 1.6: Network packet and its insertion in the link frame

As shown in the figure above, the datagram header, together with data (network-layer payload), creates the payload or data field of the frame.

There is usually at least one router on WANs between two computers. The connection between two neighboring routers on the link layer is always direct. The router unpacks the datagram from a frame, only to wrap it again into a different frame (or, more generally, in a frame of different link protocol) before sending it to a different line. The network layer does not see the appliances on the physical and link layers (modems, repeaters, switches, etc.).

The network layer does not care about what kind of link protocols are used on route between the source and the destination.

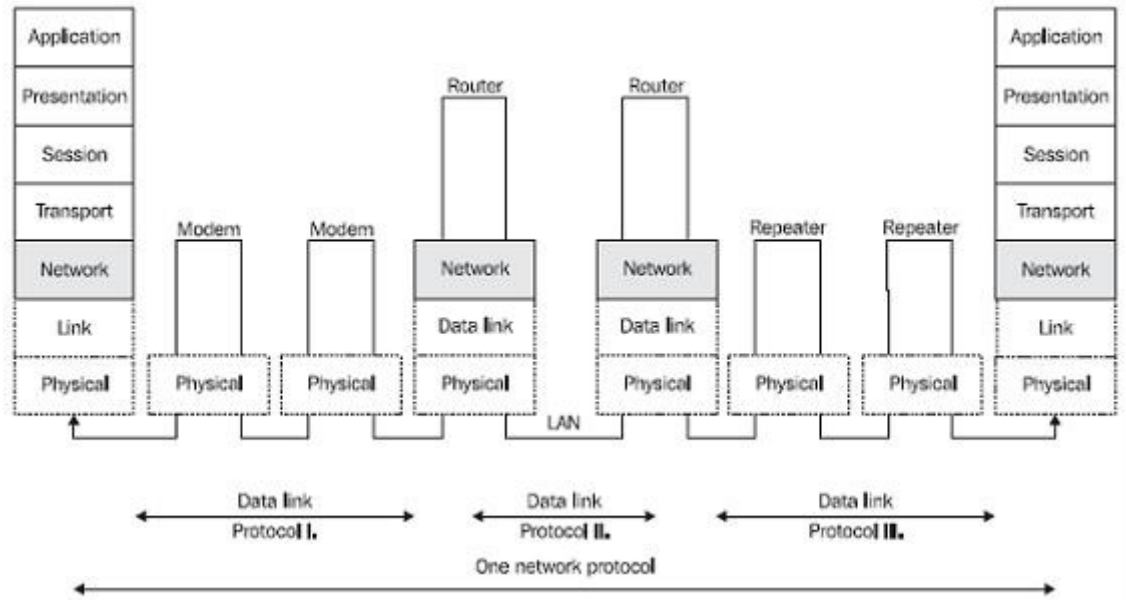


Figure 1.7: Network layer communication

A serial port or an Ethernet card can be used as a network interface. A network interface has a one or more unique address within a particular WAN.

1.1.4 Transport Layer

A network layer facilitates the connection between two remote computers. As far as the transport layer is concerned, it acts as if there were no modems, repeaters, bridges, or routers

along the way. The transport layer relies completely on the services of lower layers. It also expects that the connection between two computers has been established, and it can therefore fully dedicate its efforts to the cooperation between two distant computers. Generally, the transport layer is responsible for communication between two applications running on different computers.

There can be several transport connections between two computers at any given time (for example, one for a virtual terminal and another for email). On the network layer, the transport packets are directed based on the address of the computer (or its network interface). On the transport layer, individual applications are addressed. Applications use unique addresses within one computer, so the transport address is usually composed of both the network and transport addresses.

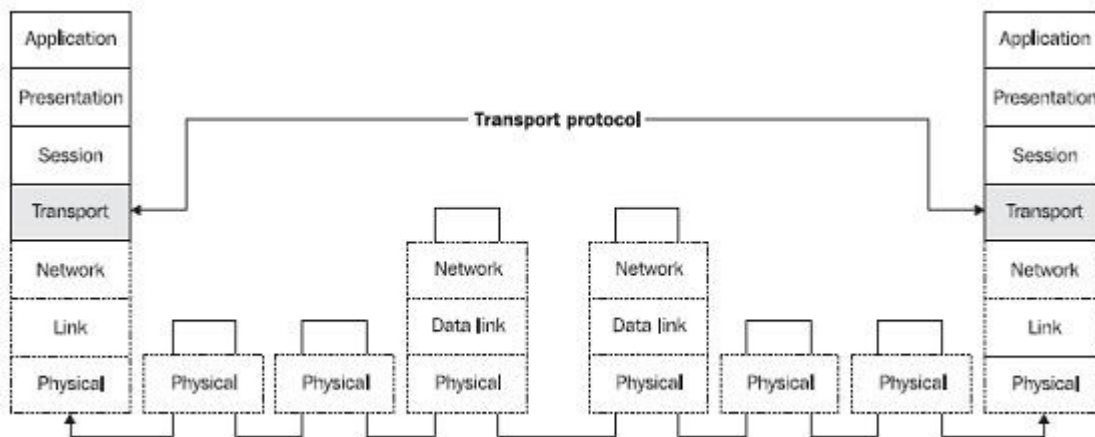


Figure 1.8: Transport layer connection

In this case, the basic transmission unit is the segment that is composed of a header and payload. The transport packet is transmitted within the payload of the network packet.

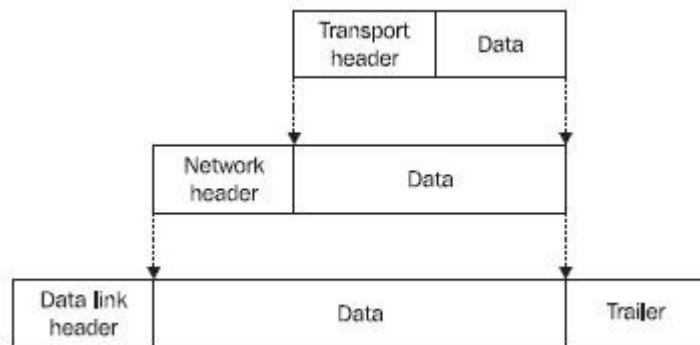


Figure 1.9: Inserting transport packets into network packets that are then inserted into link frames

1.1.5 Session Layer

The session layer facilitates exchange of data between two applications. In other words, it serves as a checkpoint and is involved in synchronizing transactions, correctly closing files, and so on. Sharing a network disk is a good example of a session. The disk can be shared for a certain period of time, but the disk is not used for the entire time. When we need to work with a file on the network disk, a connection is established on the transport layer from the time when the file is opened to when it is closed. The session, however, exists on the session layer for the entire time the disk is being shared.

The basic unit is a session layer PDU (Protocol Data Unit), which is inserted in a segment. Other books often illustrate this with a figure of a session-layer PDU, composed of the session header and payload, being inserted in the segment. Starting with the session layer, however, this does not necessarily have to be the case. The session layer information can be transmitted inside the payload. This situation is even more noticeable if, for example, the presentation layer encrypts the data, and thus changes the whole content of the session-layer PDU.

1.1.6 Presentation Layer

The presentation layer is responsible for representing and securing data. The representation can differ on different computers. For example, it deals with the problem of whether the highest bit is in the byte on the right or on the left. By securing, we mean encrypting, ensuring data integrity, digital signing, and so forth.

1.1.7 Application Layer

The application layer defines the format in which the data should be received from or handed over to the applications. For example, the OSI Virtual Terminal protocol describes how data should be formatted as well as the dialogue used between the two ends of the connection.

| | |
|--------------|--------------------------|
| Application | X.400, FTAM, CMIP |
| Presentation | X.226, X.216, ASN.1 |
| Session | X.225, X.215 |
| Transport | TP 0-4, TP noncontinuous |
| Network | X.25, X.75, ISDN |
| Data Link | HDLC, LAPB, ISDN |
| Physical | V.24, V.35, X.21, ISDN |

Figure 1.10: Examples of network protocols from the ISO OSI protocols family

1.2 TCP/IP

With a few exceptions, the TCP/IP family does not deal with the physical or link layers. In practice, Internet protocols often use protocols that adhere to the ISO OSI standards for the physical and link layers.

What is the correlation between the ISO OSI protocols and TCP/IP? Each group of protocols has its definition of its own layers as well as the protocols used on these layers. Generally speaking, ISO OSI protocols and TCP/IP are incompatible. In practice, ISO OSI-compliant communication appliances need to be used for transferring IP datagrams, or on the other hand, services based on ISO OSI need to be provided via the Internet.

1.2.1 Internet Protocol

Internet Protocol (IP) basically corresponds to the network layer. IP is used for transmitting IP datagram's between remote computers. Each IP datagram header contains the destination address, which is the complete routing information used for delivering the IP datagram to its destination. Therefore, the network can only transmit each datagram individually. IP datagram's of one session can be transmitted through different paths and can thus be received by the destination in a different order than they were sent.

Each network interface on the large Internet network has one or more IP address that is unique worldwide. (One network interface can have several IP addresses, but one IP address cannot be used by many network interfaces.) The Internet is composed of individual networks that are interconnected via routers. Routers are also referred to as gateways in old literature.

1.2.2 TCP and UDP

TCP and UDP correspond to the transportation layer. TCP transports data using TCP segments that are addressed to individual applications. UDP transports data using UDP datagram's.

TCP and UDP arrange a connection between applications that run on remote computers. TCP and UDP can also facilitate communication between processes running on the same computer, but this is not very interesting for our purposes.

The difference between TCP and UDP is that TCP is a connection-oriented service—the destination confirms the data received. If some data (TCP segments) gets lost, the destination requests a retransmission of the lost data. UDP transports data using datagram's (the delivery is not guaranteed). In other words, the source party sends the datagram without worrying about whether it has been received. UDP is connectionless-oriented service.

The port is used as the address. To understand the difference between an IP address and port number, think of it as a mailing address. The IP address corresponds to the address of a house, while the port tells you the name of the person that should receive the letter.

TCP is described in Chapter 9 and UDP in Chapter 10.

1.2.3 Application Protocols

Application protocols correspond to several ISO OSI layers. The session, presentation, and application ISO OSI layers are reduced to one TCP/IP application layer.

The absence of a presentation layer is made up for by introducing specialized presentation-application protocols such as SSL and S/MINE that specialize in securing data or the Virtual Terminal and ASN.1 protocols that are designed for presenting data. The Virtual Terminal protocol (not to be confused with the ISO OSI protocol of the same name) specifies the network data presentation for character-oriented network protocols (Telnet, FTP, SMTP, and, partly, HTTP). Similarly, ASN.1 is often used for binary-oriented network transport. ASN.1 (including BER or DER encoding) was initially used by SNMP, but today it is also used by S/MINE.

There are many different application protocols. For practical purposes, they can be divided into two groups:

- User protocols utilized by user applications (HTTP, SMTP, Telnet, FTP, IMAP, PIP3, and so on).
- Service protocols, i.e., the protocols that ordinary Internet users rarely encounter. These protocols make sure the Internet functions correctly. For example, these could be routing protocols that are used for mutual communication by routers to correctly set their routing tables. Another example is SNMP usage in network administration.

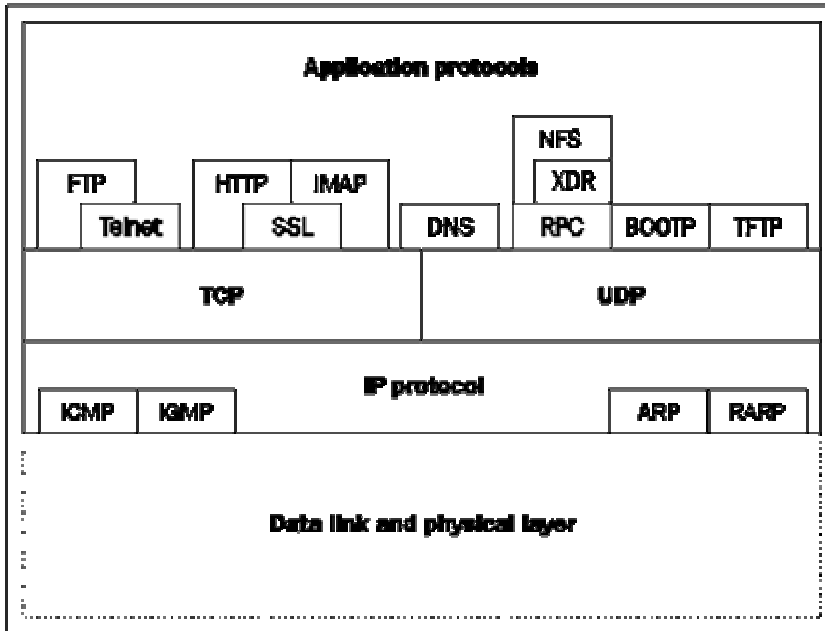


Figure 1.11: Some protocols of the TCP/IP family

1.3 Methods of Information Transmission

There are many different network protocols and several protocols can be available even on a single layer. Especially with lower-layer protocols, we distinguish between the types of transmission that they facilitate, whether they provide connection-oriented or connection-less services, if the protocol uses virtual circuits, and so on. We also distinguish between synchronous, packet, and asynchronous transmission.

1.3.1 Synchronous Transmission

Synchronous transmission is needed when it is necessary to provide a stable (guaranteed) bandwidth, for example, in audio and video. If the source does not use the provided bandwidth it remains unused. Synchronous transmission uses frames that are of fixed length and are transmitted at constant speeds.



Figure 1.12: Frames divided into slots in synchronous transmission

In synchronous transmission, the guaranteed bandwidth is established by dividing the transmitted frames into slots (see Figure 1.12). One or more slots in any transmitted frame are reserved for a particular connection. Let's say that each frame has slot 1 reserved for our connection. Since the frames follow each other steadily in a network, our application has a

guaranteed bandwidth consisting of the number of slot 1s that can be transmitted through the network in one second.

The concept becomes even clearer if we draw several frames under each other, creating a 'super-frame' (see Figure 1.13). The slots located directly under each other belong to the same connection.

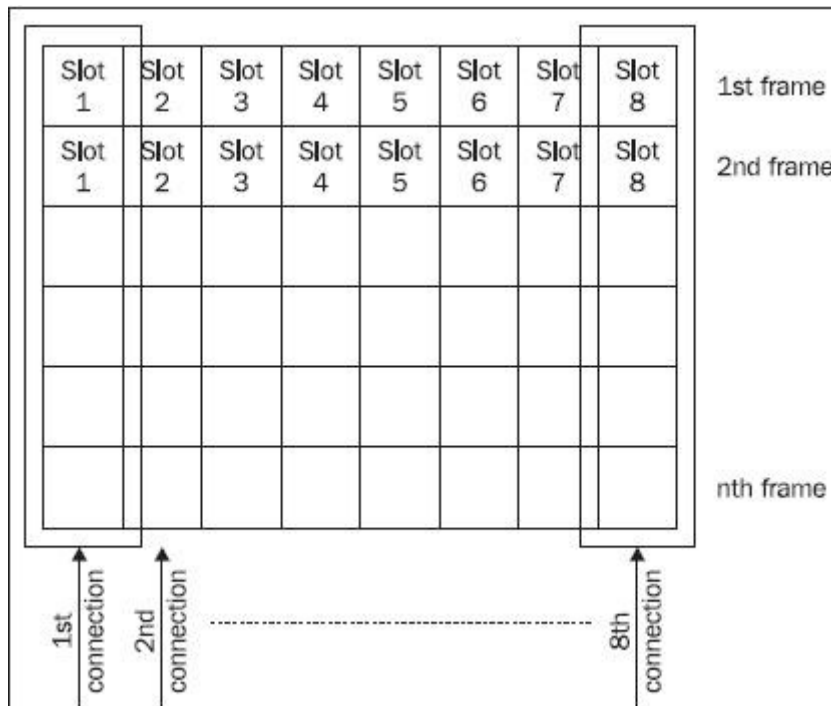


Figure 1.13: Super-frame

Synchronous transmission is used to connect your company switchboard to the phone company exchange. In this case, we use an E1(or T1 in United States) link containing 32 slots of 64 Kbps each. A slot can be used for making a phone call. Therefore, in theory, 32 calls are guaranteed at the same time (although some slots are probably used for servicing).

The Internet does not use synchronous transmission, i.e., in general, does not guarantee bandwidth. Quality audio or video transmission on the Internet is usually achieved by over-dimensioning the transmission lines. Recently, there has been a steady increase in requests for audio and video transmission via the Internet, so more and more often we come across systems that guarantee bandwidth even on the Internet with the help of Quality of Service (QoS). In order for us to reach the expected results, however, all appliances on route from the source to the destination must support these services. Today, we are more likely to get involved with only those areas on the Internet that guarantee bandwidth such as within a particular Internet provider.

1.3.2 Packet Transmission

(From now onwards we will use the term **packet** to refer to 'packet', 'datagram', 'segment', 'protocol data unit'.) Packet transmission is especially valuable for transferring data. Packets usually carry data of variable size.



Figure 1.14: Packet data transmission

One packet always carries data of one particular application (of one connection). It is not possible to guarantee bandwidth, because the packets are of various lengths. On the other hand, we can use the bandwidth more effectively because if one application does not transmit data, then other applications can use the bandwidth instead.

1.3.3 Asynchronous Transmission

Asynchronous transmission is used in the ATM protocol. This transmission type combines features of packet transmission with features of synchronous transmission.

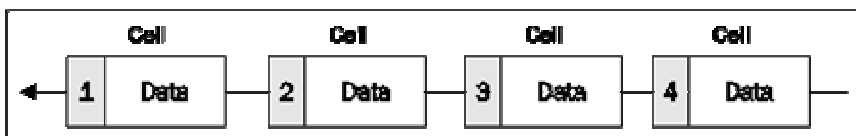


Figure 1.15: Asynchronous data transfer

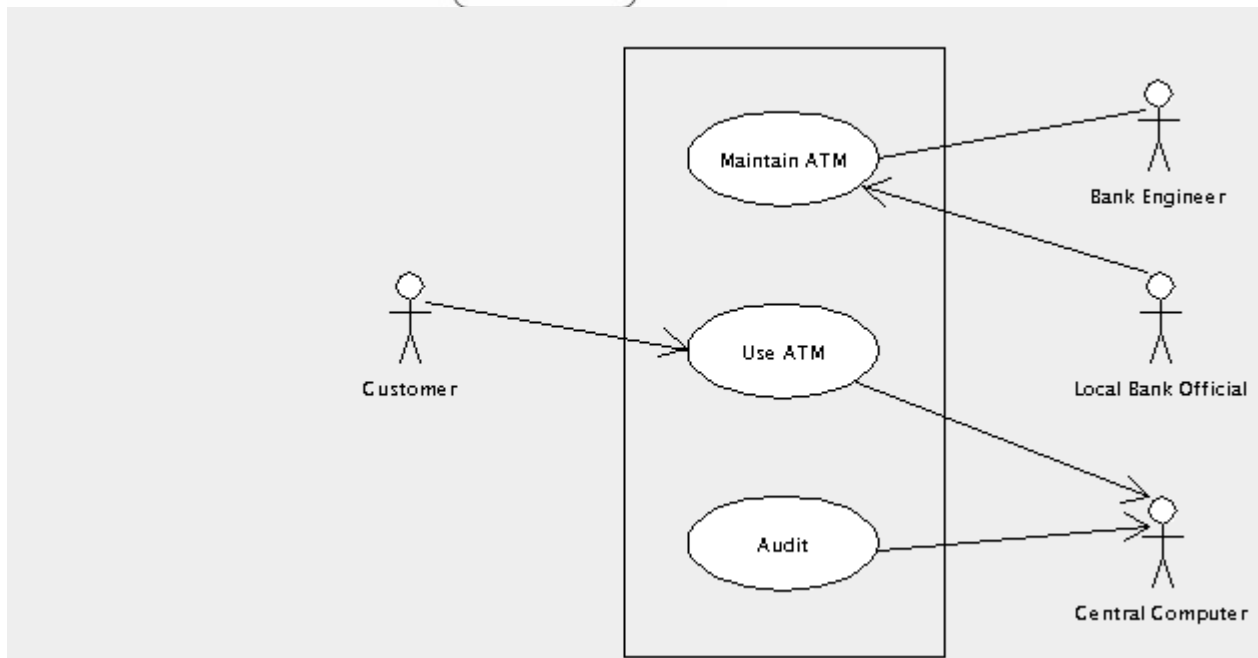
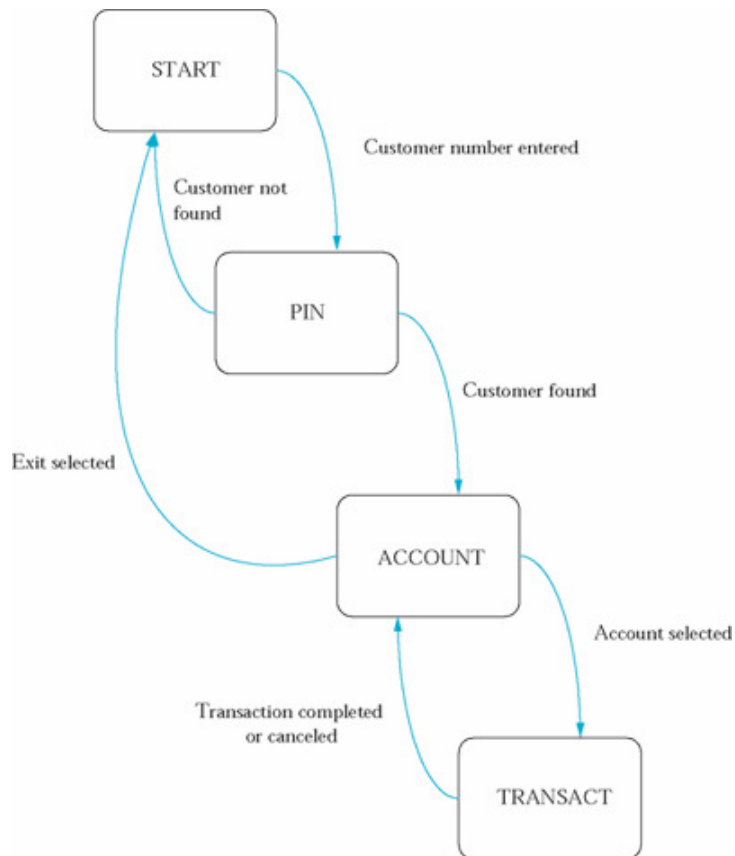
Similarly to synchronous transmission, in asynchronous transmission, the data are transmitted in packets that are rather small, but are all of the same size; these packets are called **cells**. Similarly to packet transmission, data for one application (one connection) is transmitted in one cell. All cells have the same length; so if we guarantee that the nth cell will be available for a certain application (a particular connection), the bandwidth will be guaranteed by this as well. Additionally, it doesn't really matter if the application does not send the cell since a different application's cell might be sent instead.

Q.2 How does ATM works? Explain through a diagram?

Answer

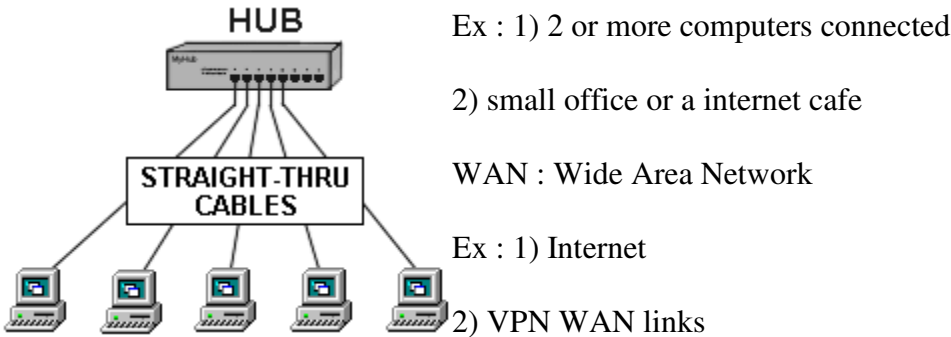
An automated teller machine (ATM) is an electronic computerized telecommunications device that allows a financial institution's customers to directly use a secure method of communication to access their bank accounts, order or make cash withdrawals (or cash advances using a credit card) and check their account balances without the need for a human bank teller (or cashier in the UK). Many ATMs also allow people to deposit cash or cheques, transfer money between their bank accounts, top up their mobile phones' pre-paid accounts or even buy postage stamps.

An ATM is also known, in English, as an Automated Banking Machine or Bank Machine (Australia, Canada), Bancomat (Central Europe, Eastern Europe, Italy, and Switzerland), Cash point (New Zealand and United Kingdom), Cash Machine (United Kingdom), Hole-in-the-wall (UK slang) or MAC (certain United States areas).



Q3. List and describe five examples of lan and wan applications?

LAN : Local Area network



Q4: DIFFERENTIATE BETWEEN THE FOLLOWING WITH THE HELP OF DIAGRAMS

- 1) hub and switches
- 2) transparent and spanning tree bridge
- 3) basic rate interface and primary rate interface

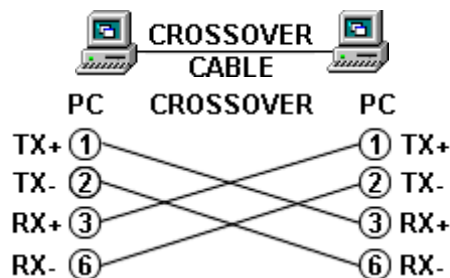
Ans:

Although hubs and switches both glue the PCs in a network together, a switch is more expensive and a network built with switches is generally considered faster than one built with hubs. Why?

When a hub receives a packet (chunk) of data (a frame in Ethernet lingo) at one of its ports from a PC on the network, it transmits (repeats) the packet to all of its ports and, thus, to all of the other PCs on the network. If two or more PCs on the network try to send packets at the same time a collision is said to occur. When that happens all of the PCs have to go through a routine to resolve the conflict. The process is prescribed in the Ethernet Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol. Each Ethernet Adapter has both a receiver and a transmitter. If the adapters didn't have to listen with their receivers for collisions they would be able to send data at the same time they are receiving it (full duplex). Because they have to operate at half duplex (data flows one way at a time) and a hub retransmits data from one PC to all of the PCs, the maximum bandwidth is 100 MHz and that bandwidth is shared by all of the PC's connected to the hub. The result is when a person using a computer on a hub downloads a large file or group of files from another computer the network becomes congested. In a 10 MHz 10Base-T network the affect is to slow the

network to nearly a crawl. The affect on a small, 100 Mbps (million bits per second), 5-port network is not as significant.

Two computers can be connected directly together in an Ethernet with a [crossover cable](#). A crossover cable doesn't have a collision problem. It hardwires the Ethernet transmitter on one computer to the receiver on the other. Most 100BASE-TX Ethernet Adapters can detect when listening for collisions is not required with a process known as auto-negotiation and will operate in a full duplex mode when it is permitted. The result is a crossover cable doesn't have delays caused by collisions, data can be sent in both directions simultaneously, the maximum available bandwidth is 200 Mbps, 100 Mbps each way, and there are no other PC's with which the bandwidth must be shared.



An Ethernet switch automatically divides the network into multiple segments, acts as a high-speed, selective bridge between the segments, and supports simultaneous connections of multiple pairs of computers which don't compete with other pairs of computers for network bandwidth. It accomplishes this by maintaining a table of each destination address and its port. When the switch receives a packet, it reads the destination address from the header information in the packet, establishes a temporary connection between the source and destination ports, sends the packet on its way, and then terminates the connection.

Picture a switch as making multiple temporary crossover cable connections between pairs of computers (the cables are actually straight-thru cables; the crossover function is done inside the switch). High-speed electronics in the switch automatically connect the end of one cable (source port) from a sending computer to the end of another cable (destination port) going to the receiving computer on a per packet basis. Multiple connections like this can occur simultaneously. It's as simple as that. And like a crossover cable between two PCs, PC's on an Ethernet switch do not share the transmission media, do not experience collisions or have to listen for them, can operate in a full-duplex mode, have bandwidth as high as 200 Mbps, 100 Mbps each way, and do not share this bandwidth with other PCs on the switch

Q4 2)ans:

Transparent Bridging

Transparent bridges were first developed at Digital Equipment Corporation (Digital) in the early 1980s. Digital submitted its work to the Institute of Electrical and Electronic Engineers (IEEE), which incorporated the work into the IEEE 802.1 standard. Transparent bridges are very popular in Ethernet/IEEE 802.3 networks. This chapter provides an overview of transparent bridging's handling of traffic and protocol components.

Transparent Bridging Operation

Transparent bridges are so named because their presence and operation are transparent to network hosts. When transparent bridges are powered on, they learn the workstation locations by analyzing the source address of incoming frames from all attached networks. For example, if a bridge sees a frame arrive on port 1 from Host A, the bridge concludes that Host A can be reached through the segment connected to port 1. Through this process, transparent bridges build a table (the learning process)

Spanning-Tree Algorithm

The *spanning-tree algorithm (STA)* was developed by Digital Equipment Corporation, a key Ethernet vendor, to preserve the benefits of loops while eliminating their problems. Digital's algorithm subsequently was revised by the IEEE 802 committee and was published in the IEEE 802.1d specification. The Digital algorithm and the IEEE 802.1d algorithm are not compatible.

The STA designates a loop-free subset of the network's topology by placing those bridge ports that, if active, would create loops into a standby (blocking) condition. Blocking bridge ports can be activated in the event of a primary link failure, providing a new path through the internet work.

The STA uses a conclusion from graph theory as a basis for constructing a loop-free subset of the network's topology. Graph theory states the following:

For any connected graph consisting of nodes and edges connecting pairs of nodes, a spanning tree of edges maintains the connectivity of the graph but contains no loops.

Figure 23-3 illustrates how the STA eliminates loops. The STA calls for each bridge to be assigned a unique identifier. Typically, this identifier is one of the bridge's *Media Access Control (MAC)* addresses, plus an administratively assigned priority. Each port in every bridge also is assigned a unique identifier (within that bridge), which is typically its own MAC address. Finally, each bridge port is associated with a path cost, which represents the cost of transmitting a frame onto a LAN through that port. In Figure 23-3, path costs are noted on the lines emanating from each bridge. Path costs are usually defaulted but can be assigned manually by network administrators.

Q4)3 ANS:

ISDN offers simultaneous exchange of voice, video and data on a single telephone line. It enables multiple computers to connect with the Internet or any other network, while the digital technology upon which this service is based enables faster data transfer and superior call quality.

The service offers exceptional reliability & feasibility. Some of the applications it makes possible are:

- | | |
|--|---|
| File transfer at high speeds | Video-Conferencing |
| Internet access | Point-to-point applications involving remote access |
| Leased Line backup | Telephony - connecting ISDN to PABX as direct lines |
| Remote LAN (Local Area Network) access | |

Key Features & Benefits

Simultaneous usage:

With ISDN, one phone number and one phone line can do it all; carrying images from your fax, conversations

Reliability:

The increased capacity that ISDN displays in dealing with greater volumes of traffic allows it to serve as a

from your phone and data from your computer - all simultaneously.

Integration:

Integrate the various lines used for your phones, faxes and data transfer into a single powerful communications network, by converting a standard telephone line into a reliable high-speed digital connection. This makes your connection a central point of contact for all types of information - voice, data, image and video.

backup in the case of leased line failure. Its proven track record makes it the first choice for replacing dedicated data connections common among multi-national organizations.

Cost Effective:

The service leads to reduced costs, made possible by faster connectivity, high speed operations and shorter download & transmission times. It also does not require heavy network investments, as it runs on the existing network.

Q5.(1) What is the Difference between datagram network and virtual circuit network?

ANS:

In a Datagram Network, there's no "network-layer-connection" between the two hosts. So There's no guaranteed band with and the packets may take different paths.

In a Virtual Circuit network, its oppositely and a connection is established.

Q5 (2). List three factors which can cause congestion in the network?

When too many packets are present in a subnet, performance degrades. This situation is called Congestion.

Update:

In any network when there is too much the data traffic at a node that the network slows down or starts losing data, it is known as network congestion. It degrades quality of service and also can lead to delays, lost data or e.g. dropped calls on a telephone network.

The list below contains the 8 factors of which number list 2 18 9 54 6 27 3 1 choices 18 54 27 or 24?

Well, which of these choices is evenly divisible by all the numbers on the list? $54=2 \times 27, 3 \times 18, 6 \times 9, \text{ and } 1 \times 54$. 54 is the only one from the options that is a mixture of the number choices provided, so this is the answer. Please write again if you still are having trouble.