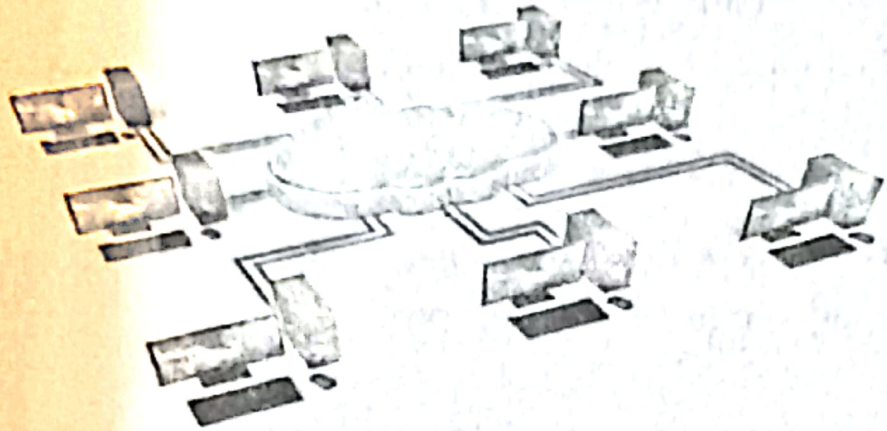


3

TCP/IP PROTOCOL SUITE

INTRODUCTION

- The TCP/IP protocol suite has been developed during the initial days of research on the Internet and it evolved over the years making it is a simple yet efficient architecture for computer networking.
- The ISO/OSI architecture developed subsequently has not caught on very well because the Internet had spread very fast and the large installation base of TCP/IP based networks could not be replaced with the ISO-OSI protocol suite.
- The TCP/IP protocol suite is now an integral part of most of the operating systems making every computer 'network-ready'.
- Even very small embedded systems are being provided with TCP/IP support of make them network-enabled, these systems include web cameras, web TVs etc.

3.1 PROTOCOL

- We may formally define protocol as a set of rules governing the exchange of data between the two entities.

3.1.1 Elements of Protocol

- The key elements of protocols are :

1. Syntax 2. Semantics 3. Timing.

1. **Syntax :** It includes the data format and signal level.

2. **Semantics :** It includes controls information for coordination and error handling.

3. **Timing :** Timing includes speed matching and sequencing.

3.1.2 Functions Performed by a Protocol

Some of important functions performed by a protocol are :

1. Encapsulation
2. Segmentation and reassembly
3. Connection control
4. Ordered delivery
5. Flow control
6. Error control
7. Addressing
8. Multiplexing and transmission services.

3.1.3 Protocol Hierarchies

- Most networks are organised as a services of layers or levels.
- To reduce the design complexity networks are organised as a series of layers or levels, one above the other.
- The number of layers, the name of layer, the contents of each layer and the function of each layer differ from network to network.

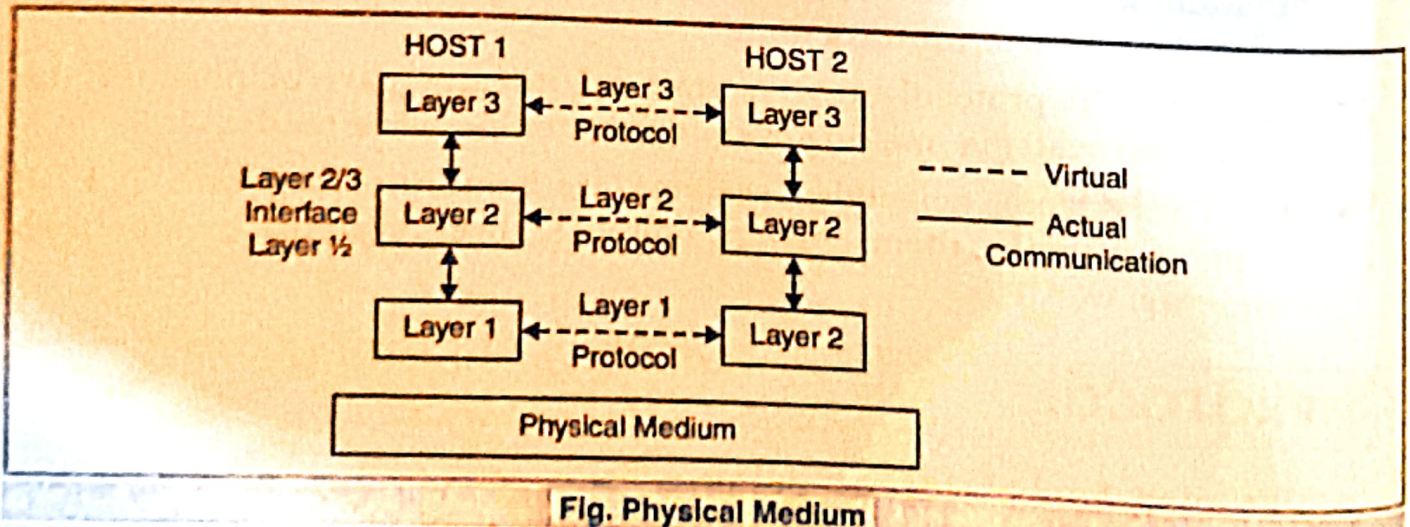


Fig. Physical Medium

- The purpose of each layer is to offer certain services to higher layers.
- The rules and conventions used in conversation are collectively known as layer *n* protocol.

- Basically a protocol is an agreement between the two machines as communication link should be established, maintained and released.
- The error control may be implemented in two different ways :
  1. Error detection
  2. Retransmission of error or lost data.
- For error detection, the sender inserts an error code in the transmitted PDU.
- The receiver checks the value of the code on the incoming PDU. It an error is detected, the receiver discards this PDU and requests for retransmission.

1. Encapsulation :

The control information in each PDU falls into three general categories.

- **Address :** It indicates the address of the sender and/or receiver.
- **Error detecting code :** Some king of frame check sequence is often included for error detecting.
- **Protocol control :** Additional information is included to implement the protocol function.

2. Segmentation and Reassembly

- When the application entity sends data, the lower level protocol may need to break up the data into smaller blocks. This is called as segmentation.
- Reassembly is exactly the opposite process of segmentation.

3. Connection Control

- Connection oriented data transfer is essential if a lengthy exchange of data is expected to take place.
- There are three phases in the connection oriented services
  1. Connection establishment
  2. Data transfer
  3. Connection termination
- A protocol can help undergoing all these phases. The more sophisticated protocol may also include connection interrupt phases to cope with errors.

4. Ordered Delivery

- If two communicating entities are residing in different hosts connected by a network, then there is possibility that PDUs will not arrive in the order in which they were sent.
- This is because the PDUs may traverse different paths through the network.
- But in connection oriented protocols it is required that PDU order be maintained.
- So unique sequence number is given to PDU. However there are some problems even with scheme.

5. Flow Control

- Flow control is a function performed by a receiving entity to limit the rate of data being sent by the transmitting entity.
- The simplest form of flow control is stop and wait procedure but more sophisticated procedures are also available.

6. Error Control

- Error control is necessary to guard against the loss or damage of the data and control information.

7. Addressing

- Addressing level refers to the level in the communication architecture at which the entity is named.
- It covers the various issues like
  1. Addressing level.
  2. Addressing scope
  3. Connection identifiers
  4. Addressing mode.

8. Multiplexing

- The concept of multiplexing is related to addressing.
- Multiplexing can be used in two directions
  (i) Upward multiplexing
  (ii) Downward multiplexing

- The upward multiplexing occurs when a number of higher level connections are multiplexed on or shared a single lower level connection.
- The downward multiplexing or splitting means a single higher level connection is built on top of multiple lower level connections, the traffic on higher connection being divided among various low level connections.

9. Transmission Services

- A protocol can provide different additional services to the entities which use it. Some of them are.
  (i) Priority
  (ii) Quality of service
  (iii) Security

3.2 TCP/IP

This is the other reference model which was used earlier by ARPANET and later on it is being used in the internet.

- ICP/IP is a short form of Transmission control protocol and Internet protocol.
- It includes many universities and Government Agencies for using the leased telephone lines. Later on satellite and radio networks are added to it.
- This new architecture is known as TCP/IP reference model due to the use of the two protocols TCP and IP.
- While designing the new model certain goals were to be achieved. Some of them were as

3.2.1 Service Provided by IP

IP provides the following services :

1. Addression :

- IP header contains 32-bit addresses which identify the sending and receiving hosts.
- These addresses are used by intermediate routers to select a path through the network for the packet.

2. Fragmentation :

- IP packet may be split or fragmented, into a smaller packets.
- This permits large packet to travel across a network which can handle only smaller packets–IP fragments and reassemble packets transparently.

3. Packet Time out :

- Each packet contains a time to live (TTL) field, which is decremented every time a router handles a packet.
- If TTL reaches to zero, the packet is discorded, preventing packets from running in circle forever and flooding in network.

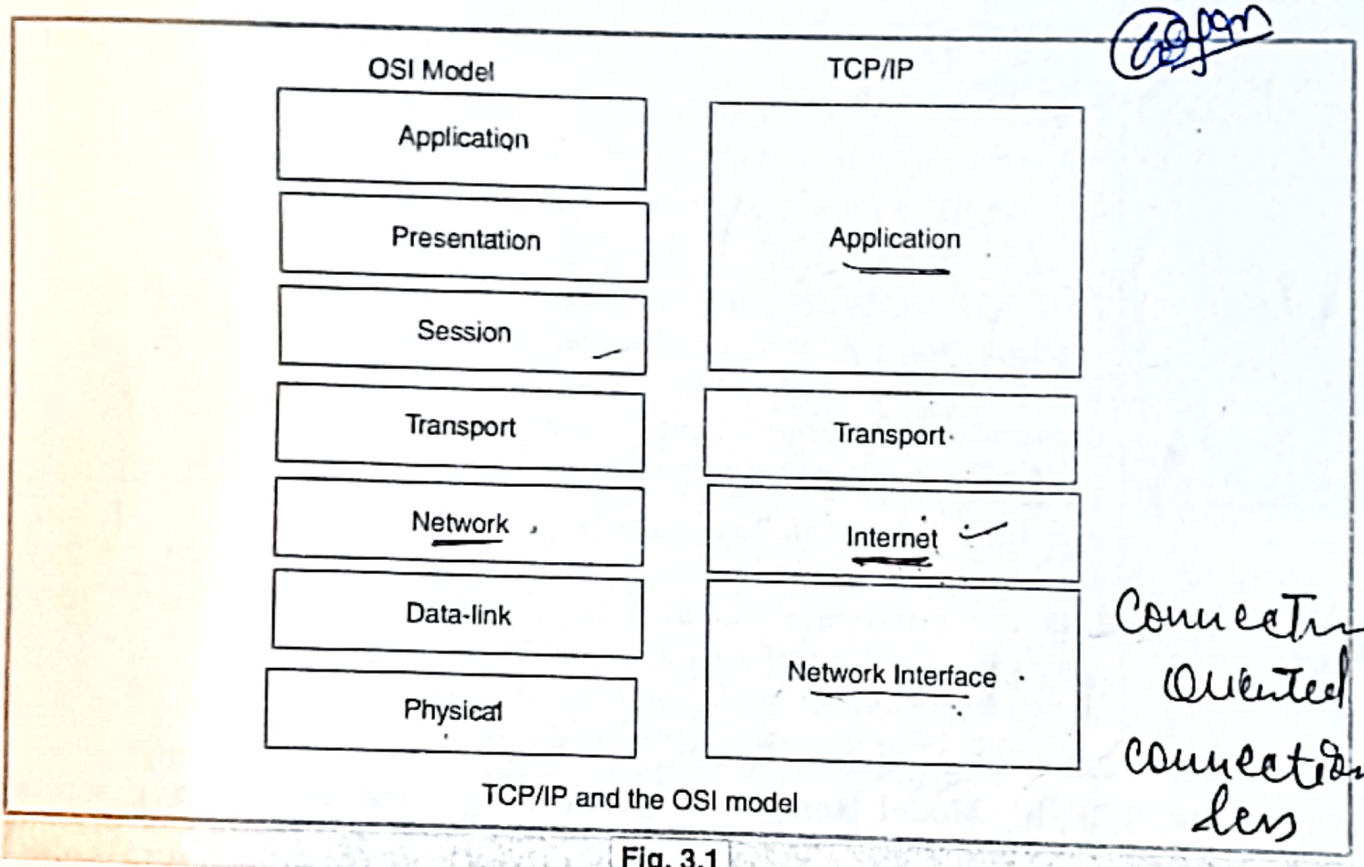
3.2.2 Goals of TCP/IP Reference Model

1. First design goal was to have an ability to connect multiple network together.
2. Another goal was that the network should be able to survive loss of subnet hardware with existing conversation not being broken.
3. A flexible architecture was needed to deal successfully with the divergent requirement various applications.
   - The internet protocol is like any other communication Protocol a set of rules which will govern every possible Communication over the internet.
   - The development of ARPANET, TCP/IP together emerged as controlling body. It is being used in computers of not only in US but all over the world for all types and sizes of the computers.
   - It has become the language of the internet.
   - TCP/IP are two protocols : Transmission control protocol and Internet protocol . These two protocols describe the movement of data between the host computer on internet.
   - It offers a simple naming and addressing scheme through which different resources on internet can be easily located.
   - Information on the internet is carried in 'packets'. The IP protocol is used to put a message into a "packet".
   - Each packet has the address of the sender and recipient's address. These addresses are known as the "IP address".
   - Using the TCP protocol, a single large message is divided into a sequence of packets and each is put into an IP packet. The

packets are passed from one network to another until they reach their destination.

- At the destination the TCP software reassembles the packets into a complete message.

The 7 layer OSI model that maps to four layers of the TCP/IP model are shown as follows:



TCP/IP and the OSI model

Fig. 3.1

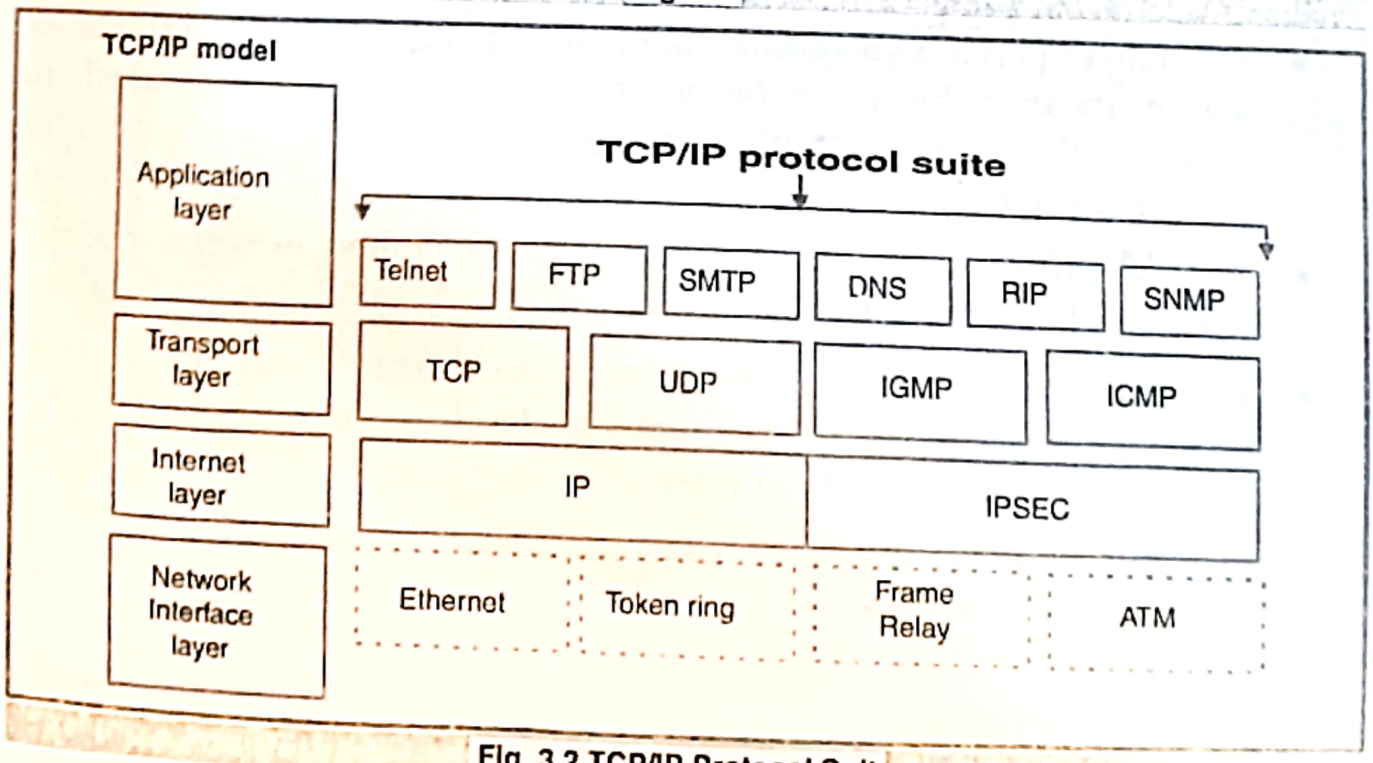


Fig. 3.2 TCP/IP Protocol Suit

The types of services performed and protocols used at each layer within the TCP/IP model are described in detail in the following table.

Layer	Description	Protocols
Application	Defines TCP/IP application protocols and how host programs interface with transport layer services to use the network.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows, other application protocols
Transport	Provides communication session management between host computers. Defines the level of service and status of the connection used when transporting data.	TCP, UDP, RTP
Internet	Packages data into IP datagrams, which contain source and destination address information that is used to forward the datagrams between hosts and across networks. Performs routing of IP datagrams.	IP, ICMP, ARP, RARP
Network interface	Specifies details of how data is physically sent through the network, including how bits are electrically signaled by hardware devices that interface directly with a network medium, such as coaxial cable, optical fiber, or twisted-pair copper wire.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35

- The TCP/IP Model separates networking functions into discrete layers.
- Each layer performs a specific function and is transparent to the layer above it and the layer below it. Network models are used to conceptualize how networks should work, so that hardware and network protocols can interoperate.
- The TCP/IP model is one of the two most common network models, the other being the OSI Model.
- The TCP/IP Model of networking is a different way of looking at networking. Because the .nodel was developed to describe TCP/IP, it is the closest model of the Internet, which uses TCP/IP.
- The TCP/IP network model breaks down into four (4) layers:
  1. **Application Layer**
  2. **Transport Layer**
  3. **Internet Layer**
  4. **Network Interface or Network Access Layer**

1. Application Layer

- The protocol related to this layer are all higher level protocols such as virtual terminals (TELNET), File Transfer Protocol (FTP) and electronic mail (SMTP).

Application Layer	TELNET, FTP, SMTP, DNS HTTP, NNTP
Transport Layer	TCP, UDP
Internet	IP
Host-to network	ARPANET, SATNET LAN

- Many other protocols have been added to these over these years such as Domain Name Service (DNS), NNTP, HTTP etc.
- In the application layer some of the important protocols are providing the services like :
- **TELNET :** It provides the terminal emulation network. And provides the remote computer login.
- **FTP :** It provides to send the file from one system to another.
- **SMTP :** Provides the basic email facility *i.e.* a mechanism for transferring message among separate hosts.
- **HTTP :** Provides the transferring of Hyper Text.

2. Transport Layer :

- It allows the peer to peer conversation between the source and destination machine.
- TCP is a reliable connection oriented protocol. It allows a byte stream transmitted from one machine to be delivered to the other machine with introducing any error.
- UDP is an unreliable, connectionless protocol and used for application which donot want TCP sequencing or flow control.
- UDP is preferred over TCP in those applications in which prompt delivery is more important than accurate delivery. It is used in transmitting speech or video.

3. Internet Layer

- This layer is called as internet layer as it holds the architecture together.

- The task of this layer is to allow the host to insert the packets int any network and then make them travel independently to th destination.
- This layer is supposed to deliver the IP packet to their destination.
- Routing and congestion is most important issue related to this layer.
- Hence TCP/IP internet layer is very similar to network layer.
- This layer maintains the addressing scheme of the internet.

4. Network Access Layer

- The Network Access Layer provides access to the physical network.

  This is the network interface card. Ethernet, FDDI, Token Ring, ATM OC, HSSI, or even Wi-Fi are all examples of network interfaces.
- The purpose of a network interface is to allow your computer to acces the wire, wireless or fiber optic network infrastructure and send data to other computers.
- The Network Access Layer transmits data on the physical network when sending and transmits data to the Internet Layer when receiving.
- All Internet-based applications and their data, whether it is a web browser downloading a web page, Microsoft Outlook sending an e-mail, a file, an instant message, a Skype video or voice call; the data is chopped into data segments and encapsulated in Transport Layer Protocol Data Units or PDU's (TCP or UDP segments).
- The Transport Layer PDU's are then encapsulated in Internet Layer's Internet Protocol packets. The Internet Protocol packets are then chopped into frames at the Network Access layer and transmitted across the physical media (copper wires, fiber optic cables or the air) to the next station in the network.
- After a long discussion the TCP/IP protocol suit succeeded over OSI in 1990's.
- It dominated over commercial architecture because it was introduced before standardization of alternative protocols.
- The internet is built on the foundation of TCP/IP suite and because of the growth of internet obviously TCP/IP has got victory over OSI.

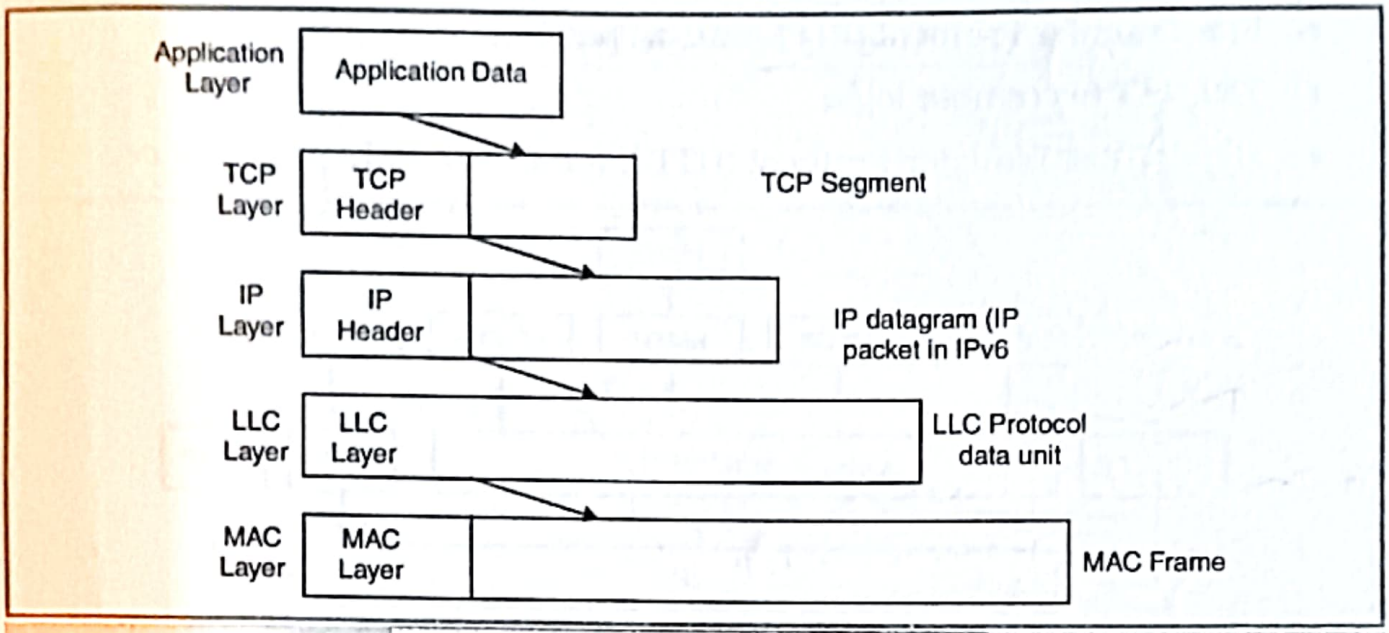


Fig. 3.3 Protocol Encapsulation in TCP/IP

- As in OSI architecture, peer-to-peer communication applies to the TCP/IP architecture as well.
- The application process (say for transferring a file) generates an application byte stream which is divided into TCP segments and sent to the IP layer.
- The TCP segment is encapsulated in the IP datagram and sent to the datalink layer.
- The IP datagram is encapsulated in the datalink layer frame.
- Since datalink layer can be subdivided into LLC layer and MAC layer, IP datagram is encapsulated in the LLC layer and then passed on to the MAC layer.
- MAC frame is sent over the physical medium.
- At the destination, each layer strips off the header, does the necessary processing based on the information in the header and passes the remaining portion of the data to the higher layer.
- This mechanism for protocol encapsulation is depicted in Fig. 3.3.

The complete TCP/IP protocol stack is shown in Fig. 3.4 indicating various application layer protocols. The various application layer protocols are :

- Simple Mail Transfer Protocol (SMTP), for electronic mail containing ASCII text.
- Multimedia Internet Mail Extension (MIME), for electronic mail which multi-media content.

- File Transfer Protocol (FTP) for file transfer.
- TELNET for remote login.
- Hyper Text Transfer Protocol (HTTP) for World Wide Web service.

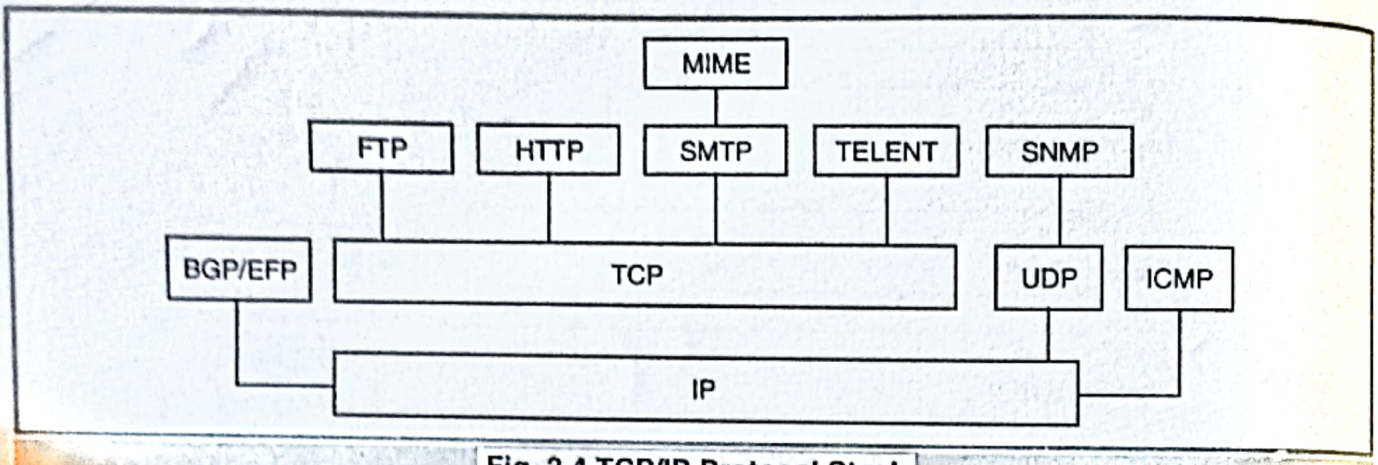


Fig. 3.4 TCP/IP Protocol Stack

In addition, the following protocols are also depicted :

- Border Gateway Protocol (BGP), a routing protocol to exchange routing information between routers. Exterior Gateway Protocol (EGP) is another routing protocol.
- Internet Control Message Protocol (ICMP), which is at the same level as IP, but uses IP service.
- Simple Network Management Protocol (SNMP) for network management. Note that SNMP uses UDP and not TCP.

3.3 OPERATION OF TCP AND IP

- Consider the internet shown in Fig. 3.5.
- Each end system will be running the TCP/IP protocol stack including the application layer software.
- Each Router will be running the IP layer software.
- If the networks use different protocols (e.g., one is tan Ethernet LAN and another is an X.25 WAN), the router will do the necessary protocol conversion as well.
- Suppose End System A wants to transfer a file to End System B.
- Each End System must have a unique address—this address is the IP address.
- In addition, the process in End System A should establish a connection with the process running in End System B to transfer the file.

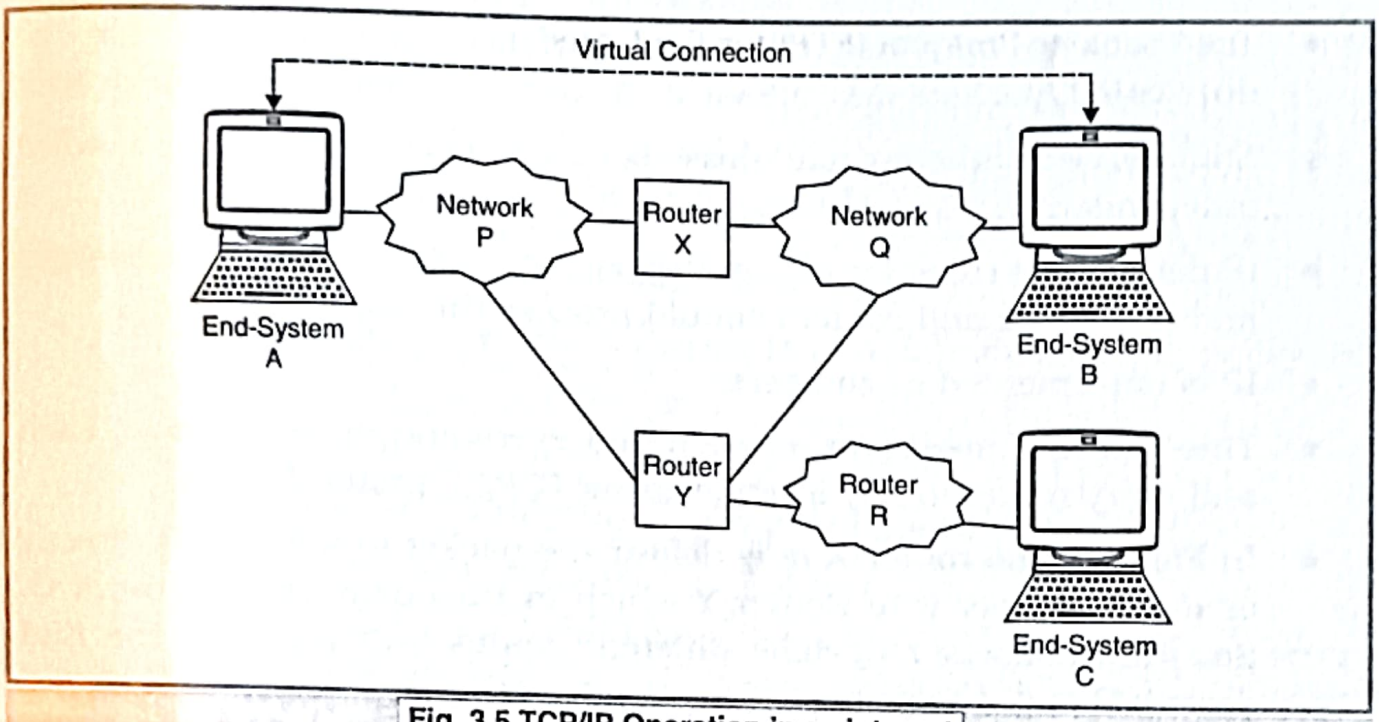


Fig. 3.5 TCP/IP Operation in an internet

- Another address is assigned to this address, known as port address.
- For each application, a specific port address is specified. When port "1" of A whishes to exchange data with port "2" on B, the procedure is :

1. Process on A gives message to its TCP : " Send to B, port 2".
2. TCP on A gives the message to its IP : "Send to host B" (Note : IP layer need not know the port of B).
3. IP on A gives message to the datalink layer with instructions to send it to router X.
4. Router X examines the IP address and routes it to B.
5. B receives the packet, each layer strips off the header and finally the message is delivered to the process at port 2.

3.4 INTERNET PROTOCOL (IP)

- Internet Protocol (IP) is the protocol that makes various networks talk to each other.
- IP defines the data formats for transferring data between various networks, it also specifies the addressing and routing mechanisms.
- The service delivered by IP is unreliable connectionless packet service.
- The service is unreliabale because there is no guarantee that the packets will be delivered —packets may be lost if there is congestion, though best-effort is made for the delivery.

- The packets may not be received in sequence, packets may be duplicated, packets may arrive at the destination with variable delay.
- The service is connectionless because each packet is handled independently.
- IP defines the rules for discarding packets, generating error messages and how hosts and routers should process the packets.
- IP is implemented as software.
- This software must run on each and every end system and on each and every router in any internet using TCP/IP protocol suite.
- In Fig. 3.5, the router X may deliver the packet to Network Q directly or it may deliver it to Router Y which in turn delivers to Network Q. So, the packets may take different routes and arrive at the End system B out of sequence.
- It is the TCP layer which takes care of presenting the data in proper format to the application layer.

3.5 TRANSMISSION CONTROL PROTOCOL (TCP)

- It is the job of transport layer protocol to ensure that the data is delivered to the application layer without any errors. So, the functions of the transported layer are :
  - To check whether the packets are received in sequence or not. If they are not in sequence, they have to be arranged in sequence.
  - To check whether each packet is received without errors using the checksum. If packets are received in error, TCP layer has to ask for retransmissions.
  - To check whether all packets are received or whether some packets are lost. It may so happen thay one of the routers may drop a packets (discard it) as its buffer is full the router itself may go faulty. If packets are lost, the TCP layer has to inform the other end system to retransmit the packet. Dropping a packet is generally due to congestion on the network.
- Sometimes, one system may send the packets very fast and the router or end system may not be able to receive the packets at that speed.
- So, flow control is required to be done by the transport layer.
- It is the job of the transport layer to provide an end-to-end

(end system to end system) reliable transfer of data even if the underlying IP layer does not provide a reliable service.

- The Transmission Control Protocol (TCP) does all the above functions, through flow control and acknowledgments.

3.5.1 Flow Control and Acknowledgments

- To provide a reliable transmission, the acknowledgement policy is used.
- The two protocols for this mechanism :
  (i) Stop-and-Wait Protocol
  (ii) Sliding-Window Protocol.
- These protocols take care of lost packets, flow control as well as error detection.

3.5.1.1 Stop-and-Wait Protocol

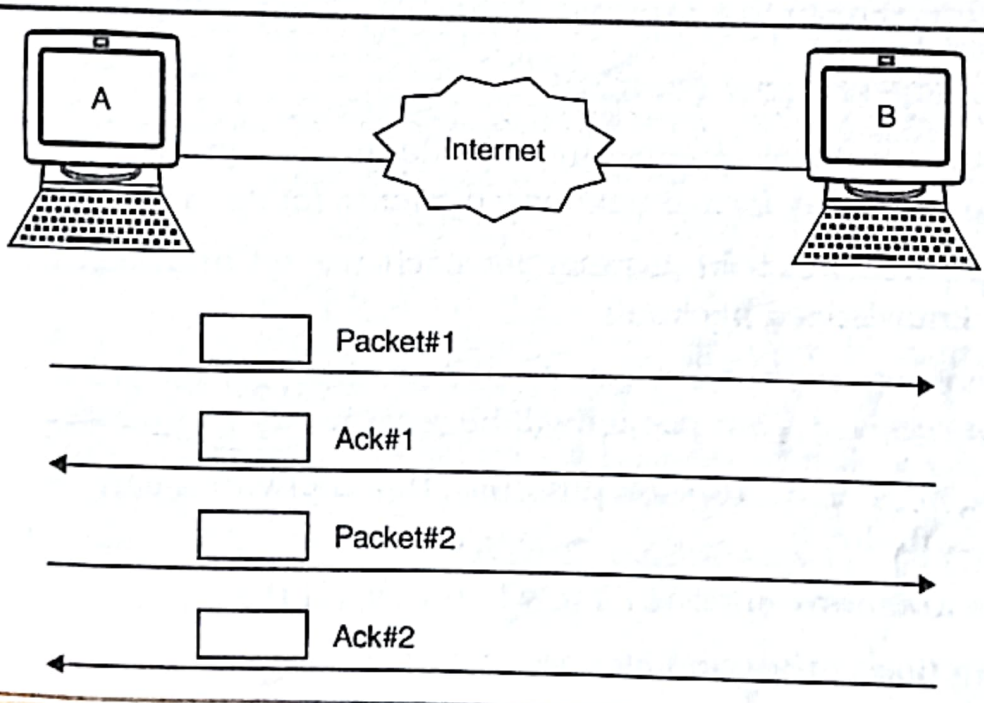


Fig 3.6 Stop-and-Wait Protocol

- When the source (end system A) sends the first packet to the destination (end system B).
- B sends an acknowledgement packet.
- Then A sends the second packet, and B sends the acknowledgement. This is a very simple protocol.
- But the problem is that if the acknowledgment for a packet is lost, what has to be done ? So, A sends the first packet and then starts a timer.

- The destination, after receiving the packet, sends a acknowledgement.
- If the acknowledgement is received before the expiry of the timer, th source sends the next packet and resends the timer.
- If the packet sent by the source is lost, or if the acknowledgemen sent by the destination is lost, the timer will expire and the sourc resends the packet.
- This protocol is very simple to implement. However, the **drawback i that the throughput will be very poor and the channel bandwidt is not used efficiently.**
- For instance, if this protocol is used in a satellite network, A will sen a packet, and after one second it will receive the acknowledgement.
- During this one second, the satellite channel is free and hence th channel is not utilized effectively.
- A refinement to this protocol is the sliding window protocol.

3.5.1.2 Sliding-Window Protocol

- In this protocol, the source sends a certain number of packet without waiting for the acknowledgments for each packet.
- The source will have a timer for each packet and keeps track of th unacknowledged packets.
- If the timer expires for a particular packet and the acknowledgemen is not received, that packet will be resent.
- This way, the throughput on the network can be increase substantially.
- There are many options as to when to send the acknowledgement.
- One option is the window size.
- If the sliding window size is 7, the source can send up to 7 packet without waiting for the acknowledgement.
- The destination can send and acknowledgement after receiving all th 7 packets.
- If the destination has not received packet 4, it can send a acknowledgement indicating that up to packet 3 were received.
- As shown in Fig. 3.7, if B sends ACK 3, the source knows that up t packet 3 were received correctly and it sends all the packets from onwards again.

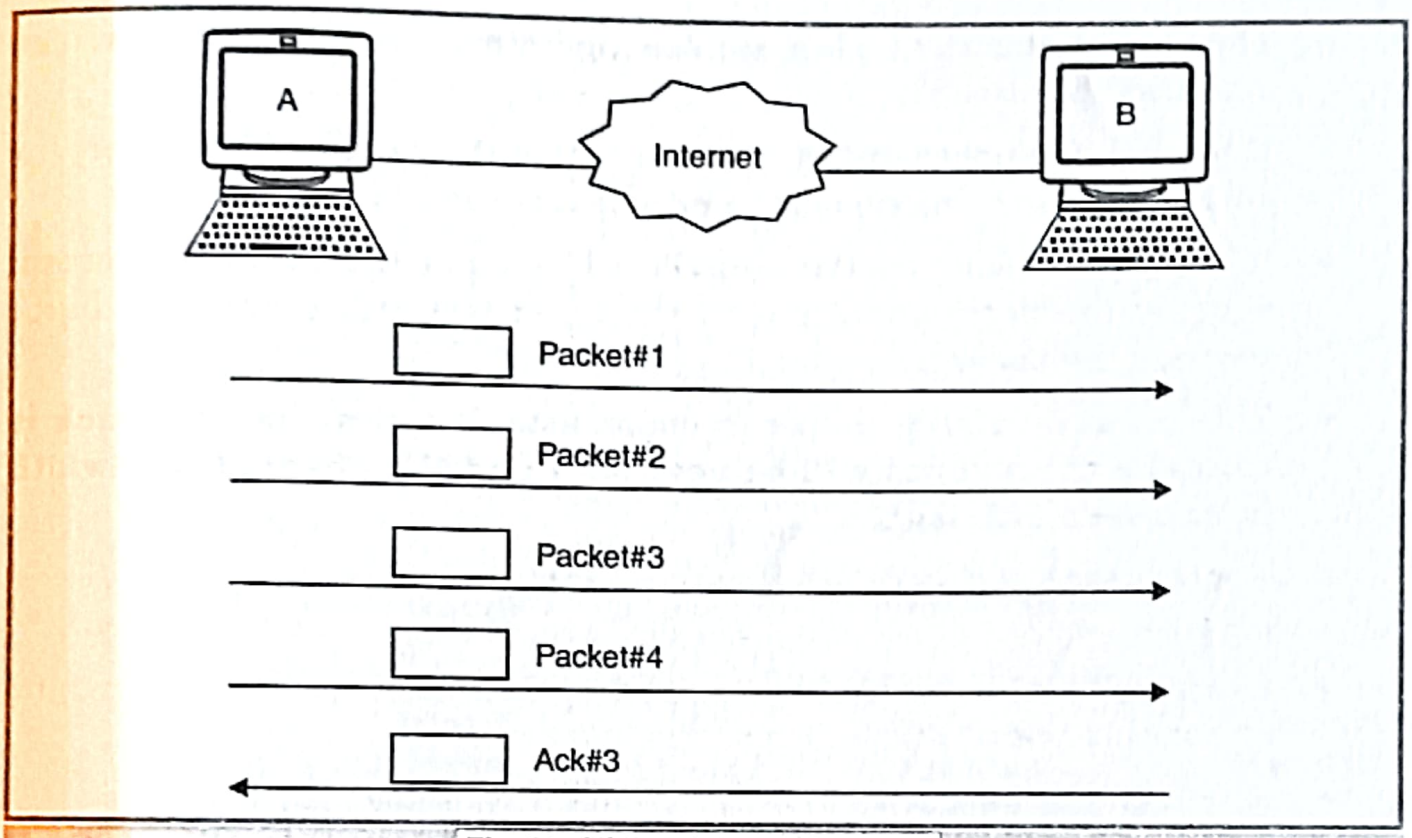


Fig. 3.7 Sliding-Window Protocol

- So, another option is the sliding window protocol is when to send the acknowledgements.
- A positive acknowledgment can be sent indicating that up to packet #n all packets are received.
- Alternatively, a negative acknowledgement may be sent indicating that packet #n is not received.
- The sliding window protocol also addresses the flow control. If the destination cannot receive packets with the speed with which the source sends the packets, the destination can control the packets flow.
- Using this simple protocol, TCP layer will take care of flow control, error control and acknowledge the source that the packets are being received.

3.6 COMPARISON BETWEEN OSI AND TCP/IP REFERENCE MODEL IN TABULAR FORM

The OSI Model uses seven layers, and differs quite a bit from the TCP/IP model. The TCP/IP model does a better job of representing how TCP/IP works in a network, but the OSI Model is still the networking model most

technical people refer to during troubleshooting or network architecture discussions.

	OSI Model Reference	TCP/IP Model Reference
Similarities	OSI is based on the concept of a stack of independent protocols. The functionality of the layers is roughly similar.	TCP/IP is also based on the concept of a stack of independent protocols. The functionality of the layers is roughly similar.
Definition	**OSI:** Open Systems Interc-onnection. It was developed by ISO as a first step toward international standardization of the protocol used in various layers. It deals with connecting open system.	**TCP/IP:** Transport Control Protocol/Internet Protocol. TCP is used in connection with IP and operates at the transport layer. IP is the set of convention used to pass packets from one host to another.
Numbers Link Layer	Seven layers, Network(Internet), Transport and Application layers being similar to TCP/IP 1. Physical Layer 2. Data of layers 3. Network Layer 4. Transport Layer 5. Session Layer 6. Presentation Layer 7. Application Layer	**Only four layers.** 1. Network Interface Layer 2. Internet Layer 3. Transport Layer 4. Application Layer
	OSI makes the distinction between services, interfaces, and protocol.	TCP/IP does not originally clearly distinguish between services, interface, and protocol.
Service, interface and protocol	Protocols in the OSI model are better hidden and can be replaced relatively easily as the technology changes, which is one of the main objectives of layered protocols.	Service, interface and protocol are not clearly defined. For example, the only real services offered by the Internet layer are –Send IP Packet –Receive IP Packet
Function alities	Because models were invented before protocols, functionalities put in each layer are not very optimized.	In this case, the protocols have been invented before models, so the functiona-lities are perfectly described.
Connection-less/ Conne-ction-oriented communication	Both connectionless and connection-oriented communication is supported in the network layer, but only connection-oriented communication in the transport layer.	Only one mode in the network layer (connection- less) but both modes in the transport layer are supported, giving the users a choice.
Data link/ Physical vs. Network interface	OSI has Data Link/Physical layers. Data link layer deal with error detection and corection. Physical layer refer to the physical connection of network.	The lower layers below the Interface or Network layer of TCP/IP seldom discussed. This protocol has not defined and varies from host to host and network to network.

Network vs Internet	• A connection-oriented protocol. • Virtual circuit approach is used. • Logical connection or virtual circuit is established before any packet are sent i.e. Call Setup phase.	• A connectionless oriented protocol. • Data-gram approach is used. • Each packet is treated independently
Transport Layer vs Transport Layer	Only connection-oriented communication is present in the transport layer.	Both connection-oriented(TCP) and connection- less (UDP) modes in the transport layer are suppo-rted,giving the users a choice.
Application Layer vs Application Layer	• Application entities in OSI may have many. • End-user applications developed using common application-development infrastructure	• Application entities in TCP/IP have a single service element. • Each application was developed independently, from "top" to "bottom".

3.7 TCP/IP OVER SATELLITE LINKS

- The TCP/IP protocol stack can be used in any network—the transmission medium can be cable, optical fiber, terrestrial radio or satellite radio.
- However, when TCP/IP is used in satellite networks, the stack poses problems.
- This is due to the characteristics of the satellite channels. The problems are :
  - The satellite channel has a large propagation delay. Large delaye causes timeouts in the flow control protocol. The source assumes that the packets have not reached the destination receives duplicate packets. This introduces congestion in the network.
  - The satellite channels have a larger Bit Error Rate (BER) as compared to the terrestrial channels. As a result, the packet losses will be more resulting in more retransmissions. When retransmission of packets is required, TCP automatically reduces the window size, though network is not congested. As a result, the throughput of the channel goes down.

To overcome these problems, a number of solutions are proposed, which include :

- To improve the linked performance, error-correcting codes are used, Hence, errors can be corrected at the destination and retransmissions can be reduced.

- Instead of using the flow control protocols at the transport layer, these protocols can be implemented at datalink layer, so that the TCP layer does not reduce the window size.
- Instead of using a default window size of 16 bits in the TCP segment, 32 bits can be used to increase the throughput.
- For bulk transfer of information from the source to the destination, multiple TCP connections can be established.
- Another interesting technique used is called 'spoofing'. A small piece of software will be running at the source which generates the acknowledgements locally. So, the local TCP layer is 'cheated' by the spoofing software. The spoofing software in turn receives the actual acknowledgement from the destination and discards it. If actually a packet is to be retransmitted as it was received in error at the destination, the spoofing software requests the TCP layer to resend the packet.

So, many improvements in the TCP/IP protocol layers are required for its use in satellite networks.

3.8 INTER-PLANETARY INTERNET (IPN)

- The Internet, as we know it, is a network of connected networks spread across the Earth.
- The optical fiber based backbone (the set of high-capacity, high-availability communication links between network traffic hubs) of the Internet supports very high data rates with negligible delay and negligible errors rates, and continuous connectivity is assured.
- If there is loss of packets, it implies congestion of the network.
- Now, imagine internets resident on other planets and spacecraft in transit. How do we go about interconnecting these internets with the Earth's Internet ? Or think of having an Internet Service Provider to the entire solar system.
- The brainchild of Vincent Cerf, the Interplanetary Internet (InterPlaNet or IPN), aims at achieving precisely this. IPN's objective is to define the architecture and protocols of permit interoperation of the Internet on the Earth ane other remotely located Internets situated on other planets and spacecraft in transit, or to build an Internet of Internets.

- The deep space communication channels are characterised by high data loss due to errors and transient link outages, asymmetric data rates and unidirectional channels and power constrained end systems.
- To develop protocols to work in this type of communication environment is a technology challenge ; also such protocols will lead to better solutions even to develop systems on the Earth.

The three basic objectives of the IPN are :

- To deploy low delay Internets on other planets and remote spacecraft.
- Connect these distributed (or 'disconnected') Internets through Interplanetary backbone that can handle the high delay.
- Create gateways and relays to interface between high delay and low delay environments.

The TCP/IP protocol suite cannot be used for the IPN for the following reasons :

- Communication capacity is very expensive, every bit counts and hence protocol overhead has to be minimised.
- Interactive protocols do not work and hence
- Reliable in-order delivery takes too long a time.
- Negotiation is not practical.
- It is difficult to implement flow control and congestion control protocols.
- Retransmission for error recovery is expensive.
- Protocols need to be connectionless.

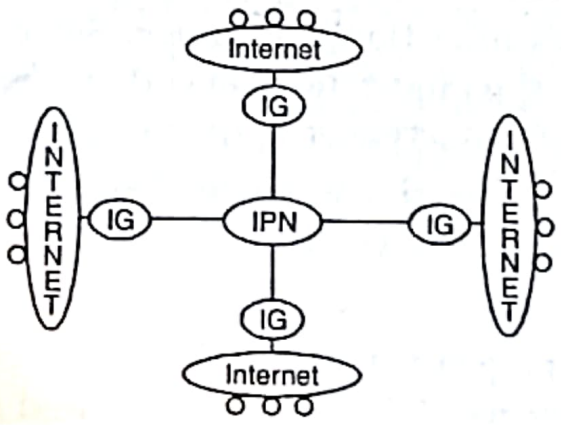


Fig. 3.8 Architecture of Inter-Planetary Internet

The proposed IPN architecture is shown in Fig. 3.8. The thrust areas for implementation of this architecture are :

- Deployment of Internets on various planets and spacecraft
- Inter-Internet protocols
- Interplanetary Gateways (IG)
- Stable backbone
- Security of the user data and the backbone.
- Presently work is underway by IPNSIG (Interplanetary Intenet Special Interest Group : http://www.ipnsig.org) to define and test the new set of protocols and the backbone architecture.
- The work includes defining new layers in the place of TCP and IP, using RF instead of fiber for the backbone network as well as the addressing issues. (A few years from now, if you have to send mail to someone, you may need to specify .earth or.mars extension to refer to the Internets of Earth and Mars).

SUMMARY

This chapter presented an overview of the TCP/IP protocol stack. Above the physical and datalink layers, the Internet Protocol (IP) layer runs which takes care of addressing and routing. IP provides a connectionless service and there is no guarantee that all the packets will be received. The packets also may received out of sequence. It is the job of transport layer protocol to take care of these problems. The transport layer provides end-to-end reliable service by taking care of flow control, error control and acknowledgements. Above the TCP layer, different application layer protocols will be running such as Simple Mail Transfer Protocol (SMTP) for email, File Transfer Protocol (FTP) for transferring the files, Hyper Text Transfer Protocol (HTTP) for World Wide Web etc. The User Datagram Protocol (UDP) also runs above the IP but it provides a connectionless service. Since the processing involved in UDP is very less it is used for network management and real-time communication applications. The TCP/IP protocol stack presents problems when used in satellite networks because the satellite networks have high propagation delay. The TCP layer has to lie suitably modified for use in satellite networks.

Another innovative project is the Inter Planetary Internet which envisages interconnection of Internets of different planets and spacecrafts. The results of this research will help improve the TCP/IP protocol stack performance in high-delay networks.

EXERCISE

SHORT ANSWER QUESTIONS

1. Explain the functions of different layers in the TCP/IP protocol architecture.
2. Explain the operation of TCP and IP.
3. IP does not provide a reliable service, but TCP provides an end-to-end reliable service. How ?
4. What are the limitations of TCP/IP protocol stack ?
5. Differentiate between TCP and UDP.
6. List the problems associated with running the TCP/IP protocol stack in satellite network.
7. Explain how congestion control is done in TCP/IP networks.

DESCRIPTIVE QUESTIONS

1. Write a technical report on Inter Planetary Internet.
2. Prepare a technical report on running the TCP/IP protocol stack on a satellite network.
3. Two systems, A and B, are connected by a point link, but the communication is only from A to B. Work out a mechanism to transfer a file from A to B using UDP as the transport protocol.
4. Discuss the benefits of using UDP for data applications if the transmission link is very reliable and if there is no congestion in the network.
5. Compare the performance of stop-and-wait protocol and sliding-window protocol in terms of delay and throughput.

□□□□□