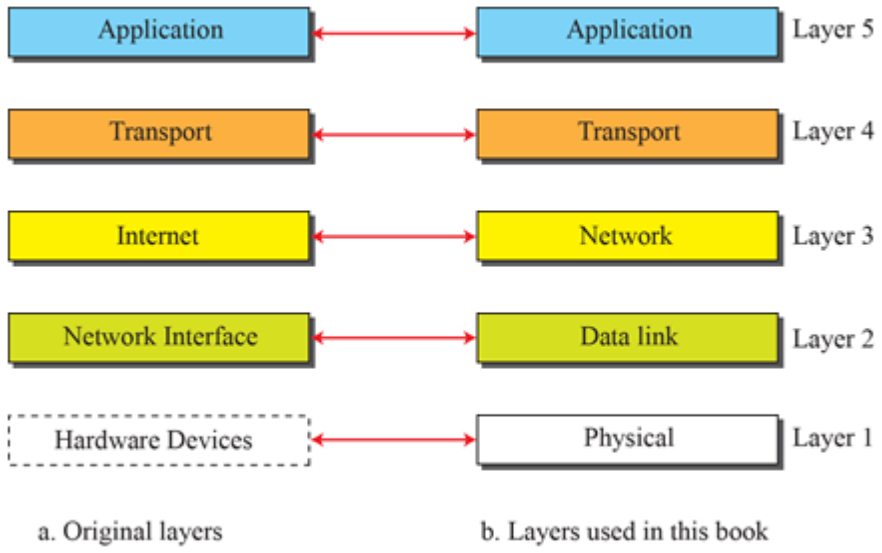
Internal Assessment Test 1 – March 2019

DATACOMMUNICATIONS					Sub Code:	17CS46	Branch:	CSE	
7/3/19	Duration:	90 min's	Max Marks:	50	Sem / Sec:	IV-A,B,C &D			OBE

1 Explain the TCP/IP suite of computer networks with a neat diagram.

TCP/IP is a protocol suite (a set of protocols organized in different layers) used in the Internet today. It is a hierarchical protocol made up of interactive modules, each of which provides a specific functionality. The term hierarchical means that each upper level protocol is supported by the services provided by one or more lower level protocols. The original TCP/IP protocol suite was defined as four software layers built upon the hardware. Today, however, TCP/IP is thought of as a five-layer model. Figure below shows both configurations.

Figure 2.4: Layers in the TCP/IP protocol suite

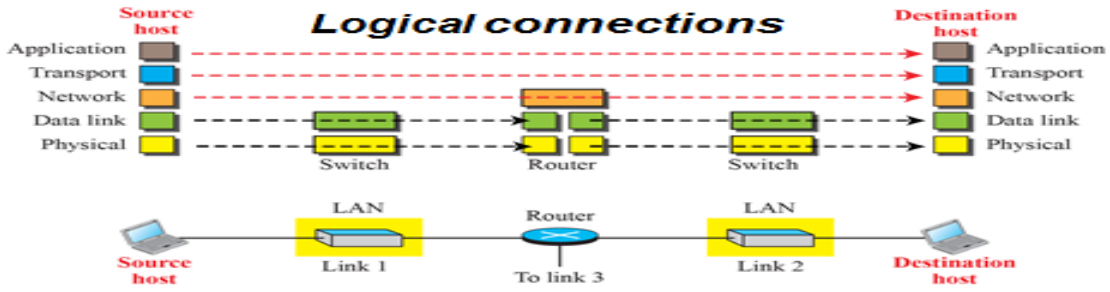


2.13

Layers in the TCP/IP Protocol Suite

To better understand the duties of each layer, we need to think about the logical connections between layers. Figure below shows logical connections in our simple internet.

Figure 2.6: Logical connections between layers in TCP/IP

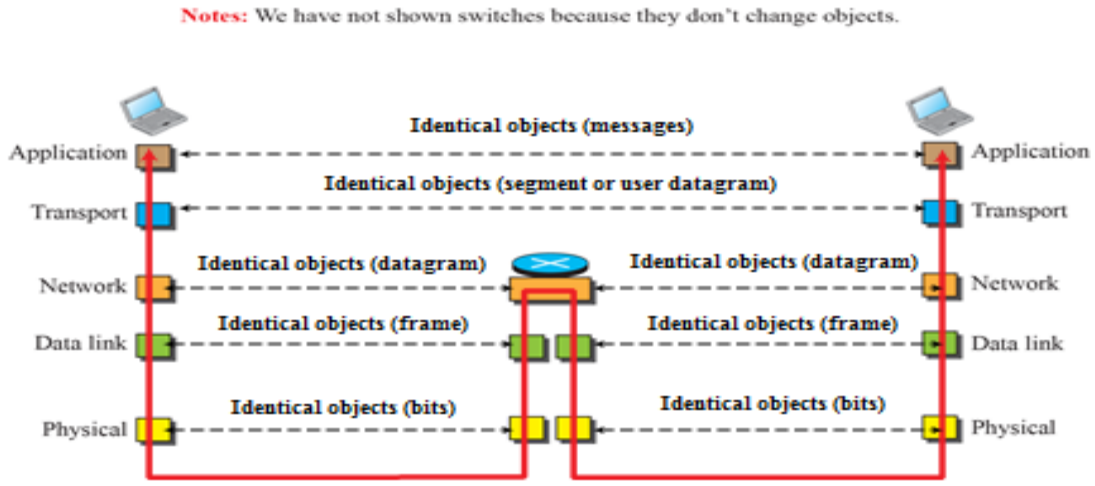


2.17

Using logical connections makes it easier for us to think about the duty of each layer. As the figure shows, the duty of the application, transport, and network layers is end-to-end. However, the duty of the data-link and physical layers is hop-to-hop, in which a hop is a host or router. In other words, the domain of duty of the top three layers is the internet, and the domain of duty of the two lower layers is the link. Another way of thinking of the logical connections is to think about the data unit created from each layer. In the top three layers, the data unit (packets) should not be

changed by any router or link-layer switch. In the bottom two layers, the packet created by the host is changed only by the routers, not by the link-layer switches.

Figure 2.7: Identical objects in the TCP/IP protocol suite



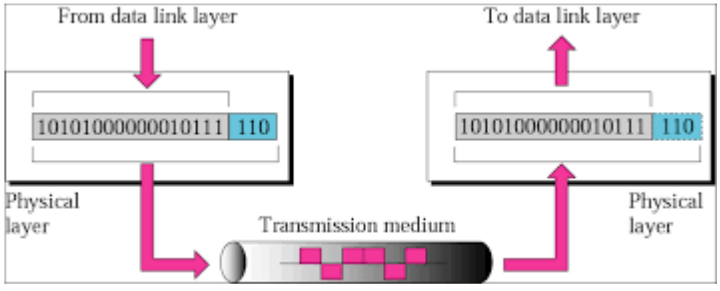
2.18

The logical connection at the network layer is between the two hosts, we can only say that identical objects exist between two hops in this case because a router may fragment the packet at the network layer and send more packets than received .Note that the link between two hops does not change the object.

Description of Each Layer

Physical Layer

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



The physical layer is also concerned with the following:

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

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

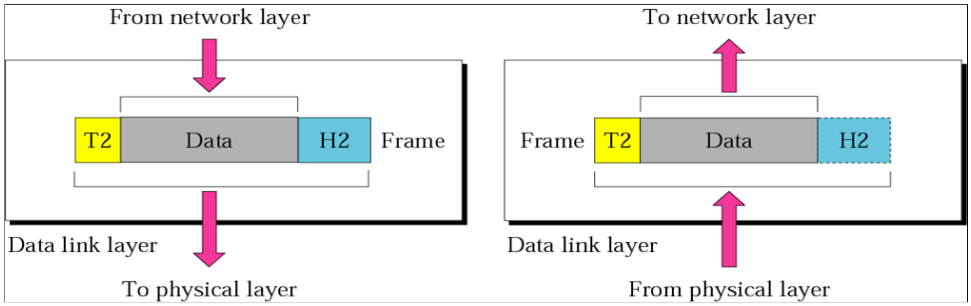
Data rate. The transmission rate--the number of bits sent each second--is also defined by the physical layer. In other words, the physical layer defines the duration of a bit, which is how long it lasts.

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

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

Physical topology. The physical topology defines how devices are connected to make a network. Devices can be connected by using a mesh topology (every device is connected to every other device), a star topology (devices are connected through a central device), a ring topology (each device is connected to the next, forming a ring), a bus topology(every device is on a common link), or a hybrid topology (this is a combination of two or more topologies).
Transmission mode. The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex. In simplex mode, only one device can send; the other can only receive.The simplex mode is a one-way communication. In the half-duplex mode, two devices can send and receive, but not at the same time. In a full-duplex (or simply duplex) mode, two devices can send and receive at the same time.

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

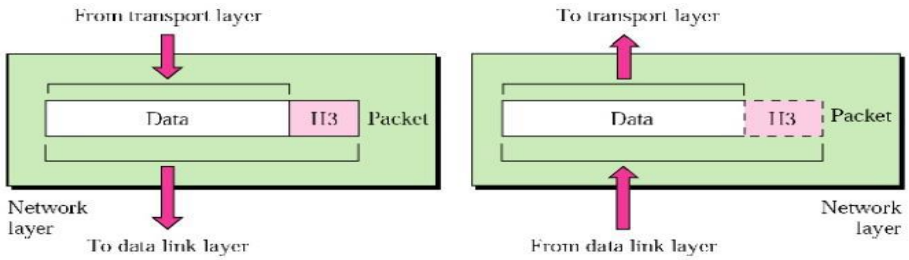


Other responsibilities of the data link layer include the following:
Framing. The data link layer divides the stream of bits received from the network layer into manageable data units called frames.
Physical addressing. If frames are to be distributed to different systems on the network, the data link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

Communication at the data link layer occurs between two adjacent nodes. To send data from A to F, three partial deliveries are made. First, the data link layer at A sends a frame to the data link layer at B (a router). Second, the data link layer at B sends a new frame to the data link layer at E. Finally, the data link layer at E sends a new frame to the data link layer at F.

Network Layer
The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination. If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery. The figure shows the relationship of the network layer to the data link and transport layers.

Network Layer



Other responsibilities of the network layer include the following:

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

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

The network layer at A sends the packet to the network layer at B. When the packet arrives at router B, the router makes a decision based on the final destination (F) of the packet. As we will see in later chapters, router B uses its routing table to find that the next hop is router E. The network layer at B, therefore, sends the packet to the network layer at E. The network layer at E, in turn, sends the packet to the network layer at F.

Transport Layer

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

Other responsibilities of the transport layer include the following:

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

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

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

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

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

Application Layer

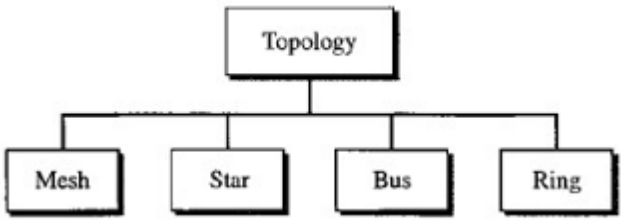
The application layer enables the user, whether human or software, to access the network. The two application layers exchange messages between each other as though there were a bridge between the two layers. However, we should know that the communication is done through all the layers. Communication at the application layer is between two processes (two programs running at this layer). To communicate, a process sends a request to the other process and receives a response. Process-to-process communication is the duty of the application layer. The application layer in the Internet includes many predefined protocols, but a user can also create a pair of processes to be run at the two hosts.It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

- The Simple Mail Transfer Protocol (SMTP) is the main protocol used in electronic mail (e-mail) service.
- The File Transfer Protocol (FTP) is used for transferring files from one host to another.
- The Terminal Network (TELNET) and Secure Shell (SSH) are used for accessing a site remotely.
- The Simple Network Management Protocol (SNMP) is used by an administrator to manage the Internet at global and local levels.
- The Domain Name System (DNS) is used by other protocols to find the network-layer address of a computer

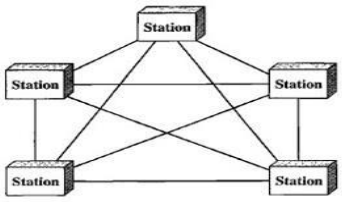
2Explain the four basic network topologies and cite any two advantages and disadvantages of each type.

Physical Topology

The term physical topology refers to the way in which a network is laid out physically. Two or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring.



Mesh In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to n-1 nodes, node 2 must be connected to n-1 nodes, and finally node n must be connected to n-1 nodes. We need n (n-1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n(n - 1) / 2 Duplex- mode links.



Advantages

1 .The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.

2. A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system.

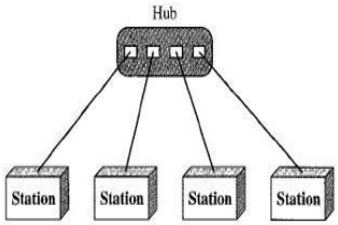
Disadvantages.

1. Because every device must be connected to every other device, installation and reconnection are difficult.

2. The sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can

accommodate.

Star Topology: In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

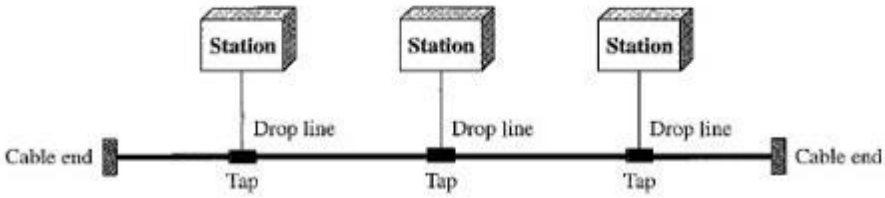


Advantages:
1. A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure. Far less cabling needs to be housed, and additions, moves, and deletions involve only one connection: between that device and the hub.

2. Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.

Disadvantages:
1. One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead.
2. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies.

Bus Topology The preceding examples all describe point-to-point connections. A bus topology ,on the other hand, is multipoint. One long cable acts as a backbone to link all the devices in a network.Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.



Advantages:
1. Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies.
2. In a bus, redundancy is eliminated. Only the backbone cable stretches through the entiry facility. Each drop line has to reach only as far as the nearest point on the backbone.

Disadvantages:
1. Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices.
2. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

Ring Topology In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

Advantages:
1. A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors.
2. To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices).

Disadvantages:
1. Unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using as dual ring or a switch capable of closing off the break.

3. Explain the IP address classification. Identify the following IP addresses and their address class (i)200.58.20.165 (ii) 128.127.23.20 (iii) 16.196.128.50 (iv) 150.156.10.10

200.58.20.165- first byte is between 192-223 so CLASS C address

128.127.23.20- first byte is between 128 to 191 so CLASS B address

16.196.128.50- first byte is between 0 to 127 so CLASS A address

150.156.10.10 first byte is between 128 to 191 so CLASS B address

Find the network ID and host ID in the IP address 14.12.72.8/24

Network ID 14.12.72.0
Host ID :14.12.72.8

4. Explain IP datagram header format with a neat diagram and give description of each field

.

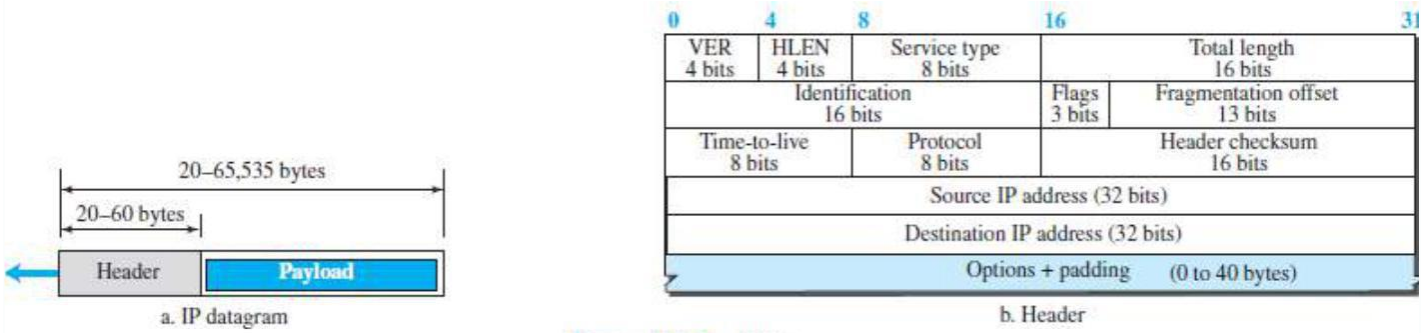


Figure 19.2 *IP datagram*

Internet Protocol (IP)
IP is main protocol responsible for packetizing, forwarding & delivery of a packet at network layer.
IP is an unreliable datagram protocol.
IP provides a best-effort delivery service.
The term best-effort means that the packets can be corrupted be lost or arrive out-of-order.

If reliability is important, IP must be paired with a TCP which is reliable transport-layer protocol.
IP is a connectionless protocol.
IP uses the datagram approach.
Each datagram is handled independently.
Each datagram can follow a different route to the destination.
Datagrams may arrive out-of-order at the destination.

1) Payload
Payload (or Data) is the main reason for creating a datagram .Payload is the packet coming from other protocols that use the service of IP.
Header
Header contains information essential to routing and delivery.IP header contains following fields:
1) Version Number (VER)
This field indicates version number used by the packet. Current version=4

2) Header Length (HLEN)
This field specifies length of header. When a device receives a datagram, the device needs to know when the header stops and when the data starts.

3) Service Type
This field specifies priority of packet based on delay, throughput, reliability & cost requirements

4) Total Length
This field specifies the total length of the datagram (header plus data).
Maximum length=65535 bytes.

5) Identification, Flags, and Fragmentation Offset
These 3 fields are used for fragmentation and reassembly of the datagram.
Fragmentation occurs when the size of the datagram is larger than the MTU of the network.

6) Time-to-Live (TTL)
This field is indicates amount of time, the packet is allowed to remain in the network.
If TTL becomes 0 before packet reaches destination, the router reaches destination, the router discards packet and sends an error-message back to the source.

7) Protocol
This field specifies upper-layer protocol that is to receive the packet at the destination-host.
For example (Figure 19.3) For TCP, protocol = 6 For UDP, protocol = 17

8) Header Checksum
This field is used to verify integrity of header only.
If the verification process fails, packet is discarded.

9) Source and Destination Addresses
These 2 fields contain the IP addresses of source and destination hosts.

10) Options
This field allows the packet to request special features such as
security level route to be taken by packet and time stamp at each router.
This field can also be used for network testing and debugging.

11) Padding
This field is used to make the header a multiple of 32-bit words.

5 Explain ICMP protocol

.

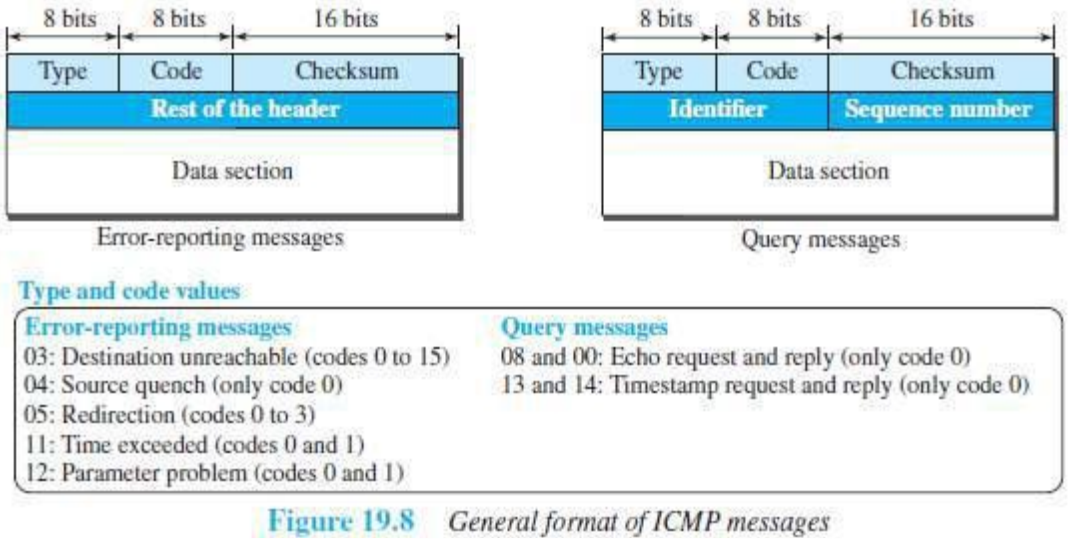


Figure 19.8 *General format of ICMP messages*

ICMP
ICMP is a network-layer protocol.
This is used to handle error and other control messages.

MESSAGES
ICMP messages are divided into 2 broad categories:
Error-Reporting Messages
These messages report problems that a router or a host may encounter during the processing of datagram.
Query Messages
These messages help a host or a network manager get specific information from a router or Another host. For example: Nodes can discover their neighbors.
Hosts can discover and learn about routers on their network.
Routers can help a node redirect the messages.
Fields of ICMP messages
Type: This field identifies the type of message.
Type 03 = problem reaching the destinations Type 11 = problem related to time exceeded.
Code: This field specifies the reason for the particular message type. For example,
Checksum: This field is used to detect errors in the ICMP message.
Data section: This field can be used for diagnostic purposes by matching the information in the ICMP message with the original data in the IP packet.

Error Reporting Messages
Main responsibility of ICMP: To report some errors that may occur during the processing of the datagram. These messages report problems that a router or a host may encounter during the processing of datagram. ICMP does not correct errors; ICMP simply reports the errors to the source.for reporting messages: No error-message will be generated for a datagram having a multicast address (or special

address). No error-message will be generated in response to a datagram carrying an ICMP error-message. No error-message will be generated for a fragmented datagram that is not the first fragment.

1) Destination Unreachable (Type=3)
This message is related to problem reaching the destinations.

This message uses different codes (0 to 15) to define type of error-message.

Possible values for code field:

Code 0 = network unreachable
Code 1 = host unreachable
Code 2 = protocol unreachable
Code 3 = port unreachable

2) Source Quench (Type=4)
This message informs the sender that network has encountered congestion and datagram has been dropped. The source needs to slow down sending more datagrams. In other words, ICMP adds a kind of congestion control mechanism to the IP protocol.

3) Redirection Message (Type=5)
This is used when the source uses a wrong router to send out its message. The router redirects the message to the appropriate router & informs the source to change its default router in the future. The IP address of the default router is sent in the message.
TTL prevents a datagram from being aimlessly circulated in the Internet. When TTL becomes 0, the datagram is dropped by the visiting router and a time exceeded message (type 11) is sent to the source.

4) Parameter Problem (Type=12)
This message can be sent when either there is a problem in the header of a datagram (code 0) or some options are missing or cannot be interpreted (code 1).

These messages help a network manager to get specific information from a router or host.
• Two types of query messages: request (type 8) and reply (type 0).

Echo Request & Echo Reply

- ➢ These messages are used to determine whether a remote-host is alive.
- ➢ A source-host sends an echo request message to destination-host;

If the destination-host is alive, it responds with an echo reply message.
Type=8 is used for echo request Type=0 is used for echo reply.
These messages can be used in two debugging tools: ping and traceroute.

Timestamp Request & Timestamp Reply
These messages are used to find the round-trip time between two devices or check whether the clocks in two devices are synchronized.
Type=13 is used for timestamp request Type=14 is used for timestamp reply.

A host is sending 100 datagrams to another host. If the identification number of the first datagram is 1024. What is the identification number of the last?

1123

In an IPV4 datagram the value of the header length (HLEN) field is (6)16 .How Many bytes of options have been added to the packet?

If HLEN =6 , the actual length will be 6*4=24
In which 20 bytes will be used for header and **4 bytes will be used for options**

7 Explain the two debugging tools ping and traceroute used in the internet for Debugging.

.

Debugging Tools

There are several tools that can be used in the Internet for debugging.
We can determine the viability of a host or router.
We can trace the route of a packet.
Two tools used for debugging: 1) Ping and 2) Traceroute.

Ping

The ping program can be used to find if a host is alive and responding Here, ping is used to see how it uses ICMP packets The source host sends ICMP echo-request messages;
The destination, if alive, responds with ICMP echo-reply messages. The ping program sets the identifier field in the echo-request and echo-reply message and starts the sequence number from 0; this number is incremented by 1 each time a new message is sent. Ping can calculate the round-trip time. It inserts the sending time in the data section of the message. When the packet arrives, it subtracts the arrival time from the departure time to get the round-trip time (RTT).

Traceroute

The traceroute program can be used to trace the path of a packet from a source to the destination.
It can find the IP addresses of all the routers that are visited along the path. The program is usually set to check for the maximum of 30 hops (routers) to be visited. The traceroute program is different from the ping program. The ping program gets help from 2 query messages;

Traceroute

The traceroute program gets help from two error-reporting messages: time-exceeded and destination-unreachable. The traceroute is an application layer program, but only the client program is needed. In other words, there is no traceroute server program. The traceroute application program is encapsulated in a UDP user datagram, but traceroute intentionally uses a port number that is not available at the destination.

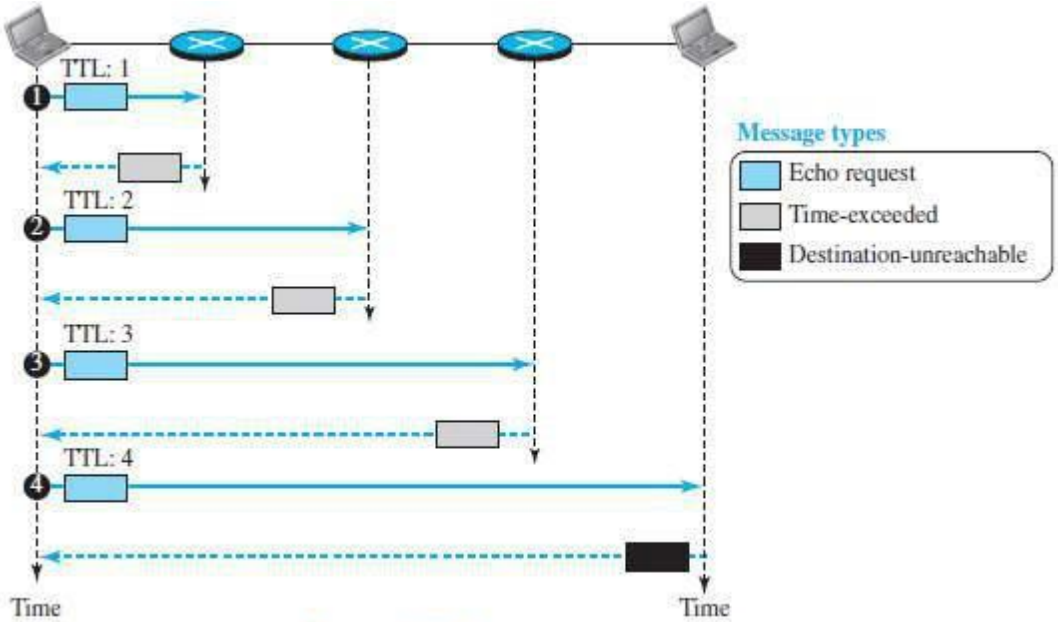


Figure 19.10 *Use of ICMPv4 in traceroute*

8. An IP datagram of size 4000 bytes arrive at a router. The link through which this datagram to be forwarded has an MTU limit of 1000 bytes. Show the details of each fragment (identification, offset, flag)

If MTU limit is 1000 bytes than the datagram will have 20 byte header and 980 bytes fragments

Fragment	Bytes	ID	OFFSET	Flag
Fragment1	980	666	0/8=0 *;0*	1-indictates there is next fragment to arrive
Fragment2	980	666	980/8=122 *; 980*	1
Fragment3	980	666	1960/8=245 *; 980+980=1960*	1
Fragment4	980	666	2940/8=367 *;980+980+980=2940*	1
Fragment5	80	666	3920/8=490 *;980+980+980+980=3920*	0 -which tells there are no more fragments