# PRINCIPLES OF TCP/IP

**SUBJECT CODE:18BCASD44**

## UNIT-1

1. What are the two levels of interconnections?
   - **a. Application and Network**
   - b. Application and Packet
   - c. Network and Packet
   - d. Physical and Application
2. What are IP routers?
   - a. Devices used for connecting networks
   - **b. Devices used for connecting network and routing**
   - c. Devices used for routing
   - d. Devices used for handling IP
3. What are application gateways?
   - a. Devices
   - b. Routers
   - **c. Application-level interconnecting**
   - d. Software
4. What do you mean by internetworking?
   - **a. The connection of different physical networks**
   - b. The connection of a few networks.
   - c. The connection of different computers
   - d. Connection of networks present inside a building.
5. What are the two portions of IP Address?
   - **a. Network and host**
   - b. Network and sub network
   - c. Sub network and host
   - d. Host, network and sub network
6. What is the size of an IP address in IPv4?
   - a. 16 bit
   - **b. 32 bit**
   - c. 64 bit
   - d. 128 bit
7. What are the various classes of IP addressing in classful addressing scheme?
   - a. X, Y, Z, A and B
   - **b. A, B, C, D, and E**
   - c. M, N, G, O and P
   - d. A, B, C, M and N
8. What is the number of network possible in Class A addressing system?
   - **a. 128**
   - b. 255
   - c. 64
   - d. 32

9. What is the number of network possible in Class B addressing system?
   - a. 128
   - b. 256
   - c. 640
   - **d. 16384**
10. What is the number of network possible in Class C addressing system?
    - **a. 2097152**
    - b. 16384
    - c. 640
    - d. 128

**(Questions for understanding)**

11. What do you think by broadcasting?
    - a. Sending the packet to every workstation of all the neighboring networks.
    - **b. Sending the copy of the message packet to all the workstations of a given network.**
    - c. Sending a msg packet to an individual workstation.
    - d. Sending the copy to a specific host.
12. What do you think by Unicasting?
    - a. **Reply from the specific workstation to specific destination in the network**.
    - b. Reply from all to a specific destination
    - c. Reply from a specific to all.
    - d. Reply from all to all.
13. What do you think by multicasting?
    - a. Sending the packet to every workstation of all the neighboring networks.
    - b. Sending the copy of the message packet to all the workstations of a given network.
    - c. Sending a msg packet to an individual workstation.
    - d. **Sending the copy to a specific multiple host**.
14. Can you clarify the loopback address from below?
    - a. 10.1.1.1
    - **b. 127.0.0.0**
    - c. 192.168.0.1
    - d. 255.255.255.255
15. What do you think by ARP?
    - a. Address resolution protocol.
    - b. Address resolution problem.
    - **c. Either a or b**
    - d. None of the above.
16. Can you illustrate resolution cache from below?
    - a. A RAM to store IP address
    - **b. A small memory to store IP-MAC address pair.**
    - c. Memory to store ARP
    - d. None of the above.
17. What do you think the purpose of HARDWARE TYPE field in the ARP protocol format?
    - a. To explain the computer hardware
    - b. To explain the network media
    - **c. To explain the network device in the computer.**

d. To explain the network protocol.

18. What do you think the purpose of PROTOCOL TYPE field in the ARP protocol format?
    a. To explain the computer hardware
    b. To explain the network media
    c. To explain the network device in the computer.
    **d. To explain the network protocol.**
19. What do you think the purpose of HLEN and PLEN field in the ARP protocol format?
    **a. Hardware address length and protocol length**
    b. Header length and protocol length
    c. Header and payload length
    d. Hardware and payload length.
20. What do you think the purpose of OPERATION field in the ARP protocol format?
    **a. Field specifies ARP request and response.**
    b. Current operation of the ARP packet
    c. A useless field
    d. A useful field.
21. What do you think RARP?
    a. Repeated Address Resolution Protocol
    b. Responsive Address Resolution Protocol
    **c. Reverse Address Resolution Protocol**
    d. None of the above
22. What do you think is IAB?
    **a. Internet Architecture Board.**
    b. Internet Addressing Board.
    c. Intranet Access Board.
    d. Internet Access Board.
23. What do you think MILNET?
    a. Milman Network
    b. Military Network
    c. Mil Network
    d. None of the above.
24. What do you think DARPA?
    **a. Defense Advanced Research Project Agency**
    b. Different Advanced Research Project Agency
    c. Defense Advanced Rework Project Agency.
    d. Different Advanced Rework Project Agency.
25. What do you think is the full form of CSNET?
    a. Communication network
    **b. Computer Science Network**
    c. Common Network
    d. None of the above

**Essay questions**

1. **What is the process of interconnection through IP routers? Explain the same through the diagram.**

- In an actual internet that includes many networks and routers, each router needs to know about the networks to which it connects.
- In a TCPIIP internet, special computers called IP routers or IP gateways provide interconnections among physical networks.
- In this example, three network interconnected by two routers. Router $R_1$ must transfer from network1 to network 2 all packets destined for computers on either network 2 or network 3.

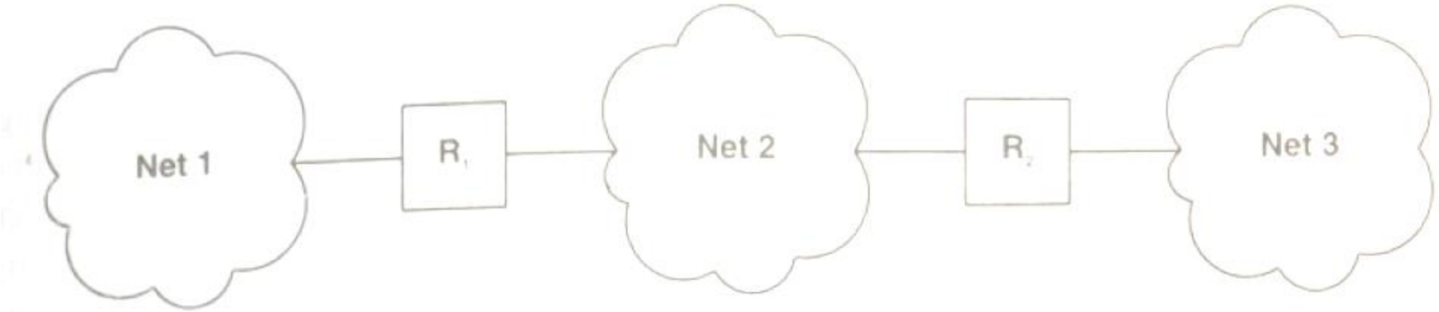


Figure: Three networks interconnected by two routers.

- Routers must each know how to forward packets toward their destination. They often have little disk storage and modest main memories.
- The trick to building a small internet router is: **Routers use the destination network, not the destination computer, when forwarding a packet.**
- If packet forwarding is based on networks, the amount of information that a router needs to keep is proportional to the number of networks in the internet, not the number of computers. Because routers play a key role in internet communication.

2. **Can you describe the path of a message traversing the Internet from the sender through two intermediate routers to the receiver? Draw the diagram to support.**

- A sender on the original machine transmits a message which the IP layer places in a datagram and sends across network.
- On intermediate routers, the datagram passes up to the IP layer which sends it back out again (on a different network).
- Only when it reaches the final destination machine, does IP extract the message and pass it up to higher layers of protocol software.
- So, the path of a message traversing the Internet from the sender through two intermediate routers to the receiver. Intermediate routers only send the datagram to the 1P software layer.

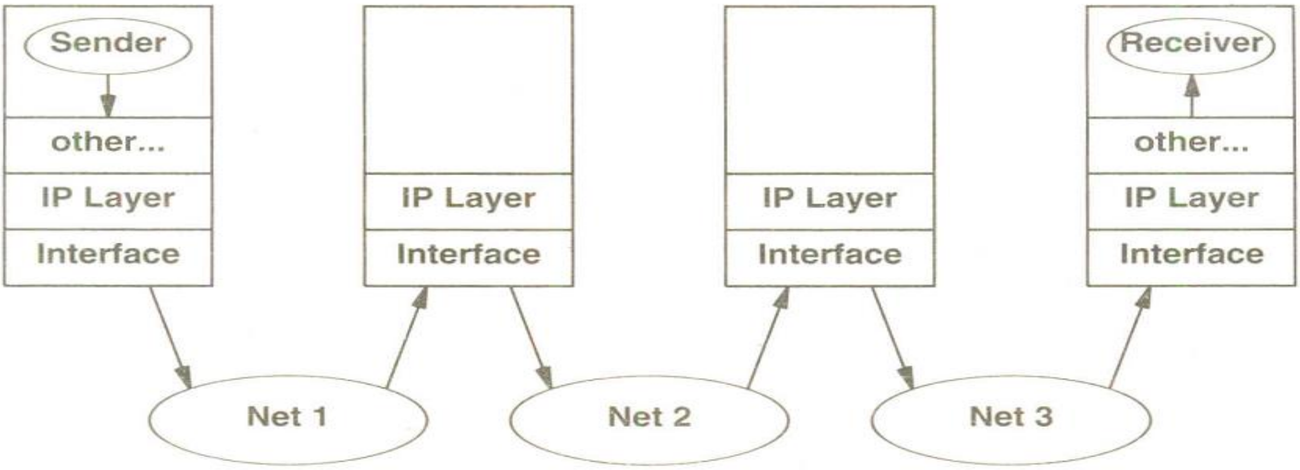


Figure: The path of a message traversing the Internet from the sender through two intermediate routers to the receiver.

3. **What is the conceptual layer of a protocol software? Prove the same with the help of adiagram.**

If the modules of protocol software on each machine as being stacked vertically into layers, each layer takes responsibility for handling one part of the problem.

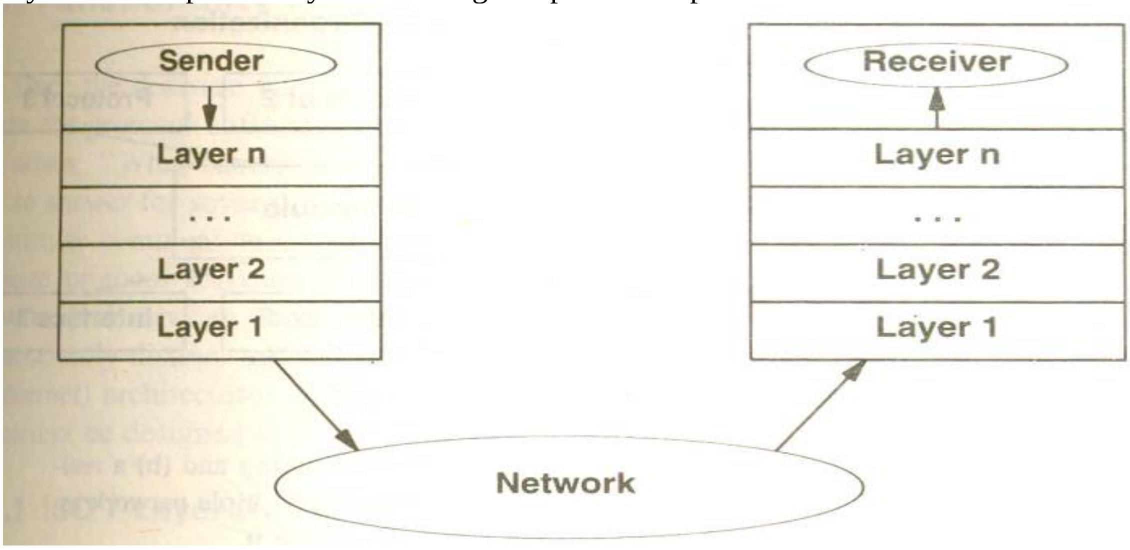


Figure: Conceptual organization of protocol software in layers

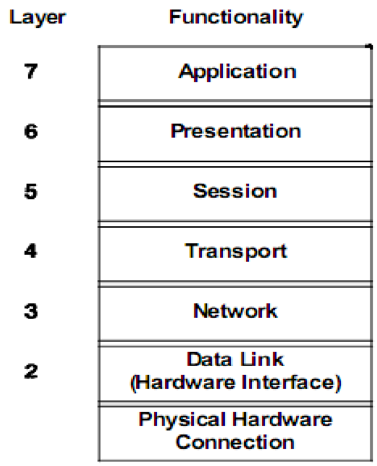
Conceptually, sending a message from an application program on one machine to an application program on another means transforming the message down through successive layers of protocol software on the sender’s machine, forwarding the message across the network, and transforming the message up through successive layers of protocol software on the receiver's machine.

In practice, the protocol software is much more complex than the simple model Each layer makes decisions about the correctness of the message and chooses an appropriate action based on the message type or destination address.

For example, one layer on the receiving machine must decide whether to keep the message or forward it to another machine. Another layer must decide which application program should receive the message.

An Internet layer between a high-level protocol layer and a network interface layer. The IP software may communicate with multiple high-level protocol modules and with multiple network interfaces.

## 4. Definition of the 7 layers of ISO OSI reference model.

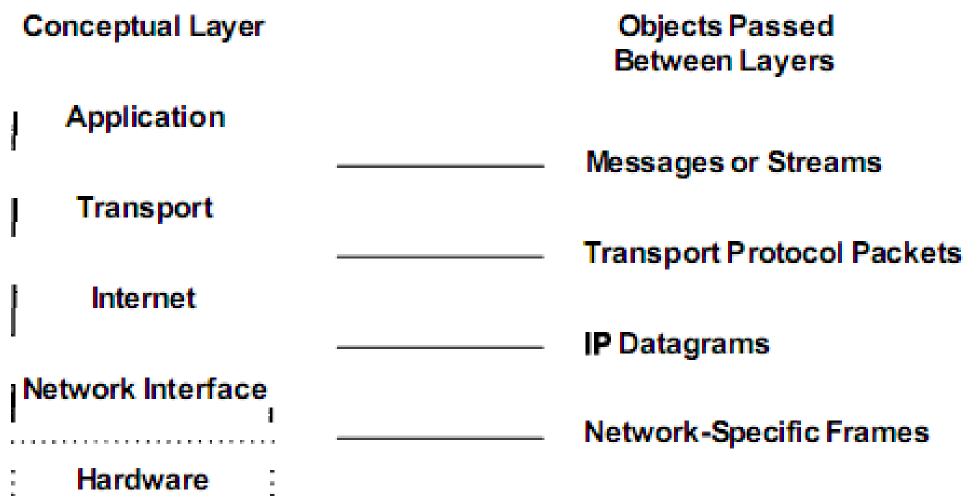


| Layer | Functionality |
|---|---|
| 7 | Application |
| 6 | Presentation |
| 5 | Session |
| 4 | Transport |
| 3 | Network |
| 2 | Data Link<br>(Hardware Interface) |
|  | Physical Hardware<br>Connection |

The IS0 model, built to describe protocols for a single network, does not contain a specific layer for internetwork routing in the same way protocols do.

- Physical Layer
  The lowest layer of the OSI Model is concerned with electrically or optically transmitting raw unstructured data bits across the network.
- Data Link Layer
  At the data link layer, directly connected nodes are used to perform node-to-node data transfer where data is packaged into frames.
- Network Layer
  The network layer is responsible for receiving frames from the data link layer, and delivering them to their intended destinations among based on the addresses contained inside the frame.
- Transport Layer
  The transport layer manages the delivery and error checking of data packets. It regulates the size, sequencing, and ultimately the transfer of data between systems and hosts. Example: TCP .
- Session Layer
  The session layer controls the conversations between different computers. Session layer services also include authentication and reconnections.
- Presentation Layer
  The presentation layer formats or translates data for the application layer based on the syntax or semantics that the application accepts.
- Application Layer
  At this layer, both the end user and the application layer interact directly with the software application. This layer sees network services provided to end-user applications.

## 5. Find the definition of the five layers of the TCP/IP model.



**Application Layer.** An application interacts with one of the transport layers protocols to send or receive data. Each application program chooses the style of transport needed, which can be either a sequence of individual messages or a continuous stream of bytes.

**Transport Layer.** The primary duty of the transport layer is to provide communication from one application program to another. The receiving machine uses the checksum to verify that the packet arrived intact, and uses the destination code to identify the application program to which it should be delivered.

**Internet Layer.** The Internet layer handles communication from one machine to another. It accepts a request to send a packet from the transport layer along with an identification of the machine to which the packet should be sent. It encapsulates the packet in an IP datagram, fills in the datagram header, uses the routing algorithm to determine whether to deliver the datagram directly or send it to a router, and passes the datagram to the appropriate network interface for transmission.

**Network Interface Layer**. Network interface layer, responsible for accepting IP datagram and transmitting them over specific network. A network interface may consist of a device driver or a complex subsystem that uses its own data link protocol.

6. **What are the layering principles using routers for different network? Explain.**

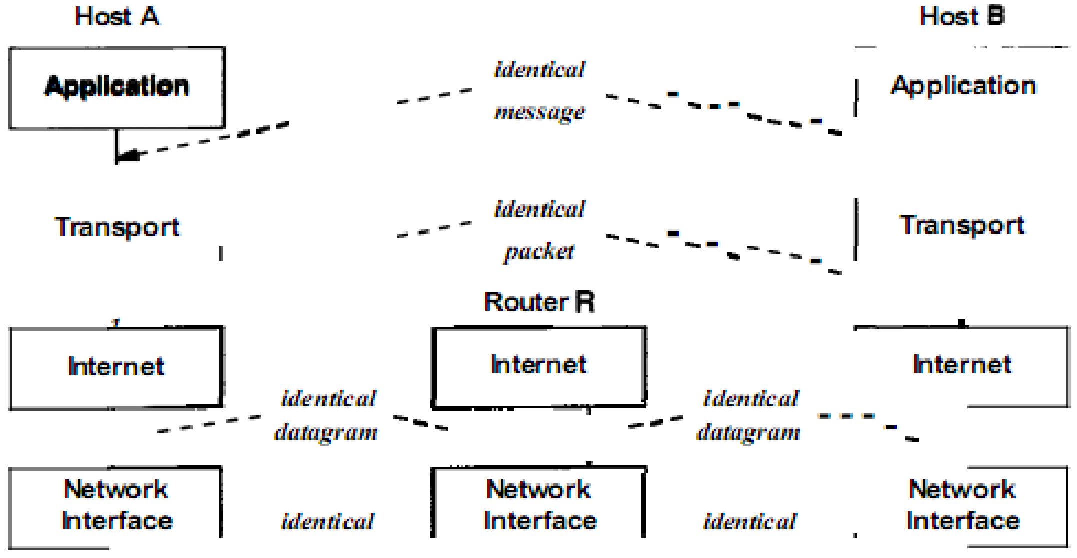


Figure: The layering principle when a router is used. The frame delivered to router R is exactly the frame sent from host A, but differs from the frame sent between R and B.

- As the figure shows, message delivery uses two separate network frames, one for the transmission from host A to router R, and another from router R to host B.
- The network layering principle states that the frame delivered to R is identical to the frame sent by host A.
- The layering principle states that the packet received by the transport layer at the ultimate destination is identical to the packet sent by the transport layer at the original source.
- Datagrams travel from original source to ultimate destination, and the layering principle guarantees that the ultimate destination receives exactly the datagram that the original source sent.

**7. Can you explain classful addressing scheme with the help of a diagram?**

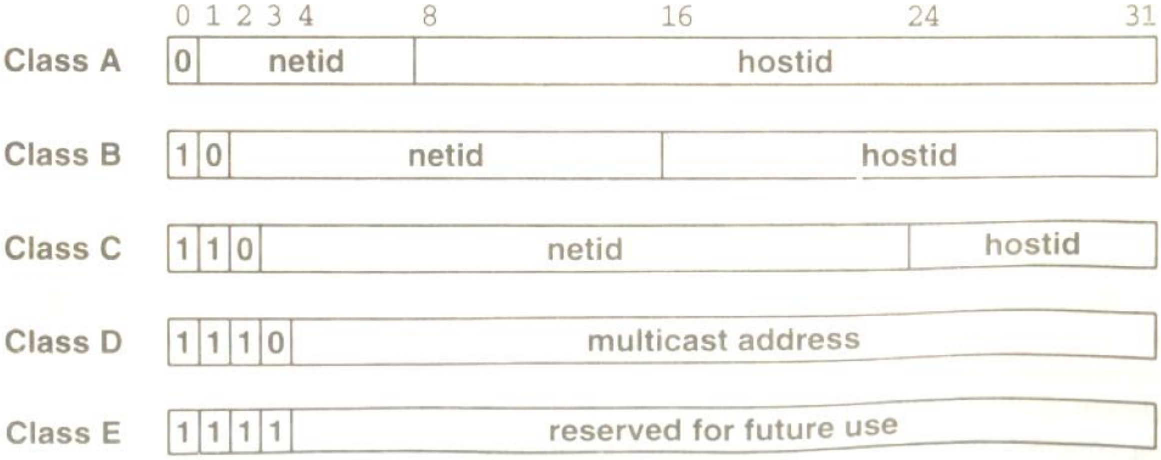


Figure: The five forms of Internet addresses used with the original classful addressing scheme. The three primary classes, A. Band C. can be distinguished by the first three bits.

- The details of IP addresses help clarify the abstract ideas. Each host attached to an internet is assigned a 32-bit universal identifier as its internet address. A prefix of an IP address identifies a network. Each address is a pair (net id, host id), where net id identifies a network, and host id identifies a host on that network.
- Class A addresses, used for the handful of networks that have more than $2^{16}$(i.e., 65,536) hosts, devote 7 bits to net id and 24 bits to host id.
- Class B addresses, used for intermediate size networks that have between $2^{8}$ (i.e., 256) and 216 hosts, allocate 14 bits to the net id and 16 bits to the host id.
- Class C addresses, used for networks that have less than 28hosts, allocate 21 bits to the net id and only 8 bits to the host id.
- Class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.
- Class E are reserved for experimental and research purposes. This class doesn’t have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.

**8. Can you explain the dotted decimal representation of IP addressing with explanation?**

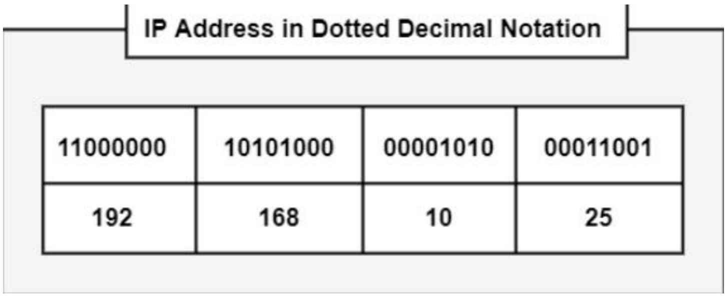
IP addresses are defined using binary notation with a 32-bit long string. Dotted decimal notations are used to make strings easily, in which periods or dots separate four decimal numbers from 0 to 255, describing 32 bits.

We have seen that the IPv4 address is expressed as a 32-bit number in dotted decimal notation. IP addresses may have a fixed part and variable part depending upon the allocation of total addresses to you or your organization.

The fixed part of the address may be from one octet to three octets, and the remaining octets will then be available for the variable part.

For example, you can take an IP address like 192.168.10.25. Now set all constant bits to 1 and set all variable bits to 0. This gives 11111111 11111111 00000000 00000000. On converting it in dotted-decimal notation, the outcome is 255.255.0.0.

This dotted-decimal notation with constant and variable methods can address prefixes to 192.168.10.25 and is represented as 192.168.10.25, 255.255.0.0. This method of expressing the prefix length as a dotted-decimal number is known as a network mask or subnet mask notation.



IP Address in Dotted Decimal Notation

| 11000000 | 10101000 | 00001010 | 00011001 |
|---|---|---|---|
| 192 | 168 | 10 | 25 |

9. **Can you clarify the meaning of Address resolution problem?**

Consider two machines A and B that connect to the same physical network. Each has an assigned IP address ZA and ZB and a physical address PA and PB. The goal is to devise low-level software that hides physical addresses and allows higher-level programs to work only with internet addresses. Ultimately, however, communication must be carried out by physical networks using whatever physical address scheme the underlying network hardware supplies. Suppose machine A wants to send a packet to machine B across a physical network to which they both attach, but A has only B’s internet address IB. First, at the last step of delivering a packet, the packet must be sent across one physical network to its final destination. The computer sending the packet must map the final destination’s Internet address to the destination’s physical address. Second, at any point along the path from the source to the destination other than the final step, the packet must be sent to an intermediate router. Thus, the sender must map the intermediate router’s Internet address to a physical address.

The problem of mapping high-level addresses to physical addresses is known as the address resolution problem and has been solved in several ways. Some protocol suites keep tables in each machine that contain pairs of high-level and physical addresses. Others solve the problem by encoding hardware addresses in high-level addresses.

10. **Can you explain in your own words about how to resolve the physical address using direct mapping?**

ProNET uses small integers for physical addresses and allows the user to choose a hardware address when installing an interface board in a computer. The key to making address resolution easy with such network hardware lies in observing that as long as one has the freedom to choose both IP and physical addresses, they can be selected such that parts of them are the same. Typically, one assigns IP addresses with the host id portion equal to 1, 2, 3, and so on, and then, when installing network interface hardware, selects a physical address that corresponds to the IP address. For example, the system administrator or would select physical address 3 for a computer with the IP address 192.5.48.3 because 192.5.48.3 is a class C address with the host portion equal to 3. For networks like proNET, computing a physical address from an IP address is trivial. The computation consists of extracting the host portion of the IP address. Extraction is computationally without reference to external data. Finally, new computers can be added to the network without changing existing assignments or recompiling code. Conceptually, choosing a numbering scheme that makes address resolution efficient means selecting a function f that maps IP addresses to physical addresses. The designer may be able to select a physical address numbering scheme as well, depending on the hardware. Resolving IP address IA means computing

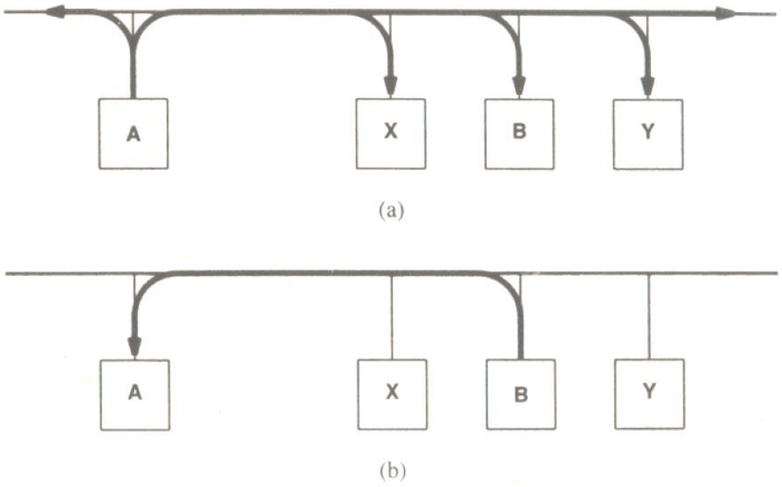
$PA=f(IA)$

We want the computation off to be efficient. If the set of physical addresses is constrained, it may be possible to arrange efficient mappings other than the one given in the example above.

**11. How do you explain about the resolution of the physical address using dynamicbinding?**

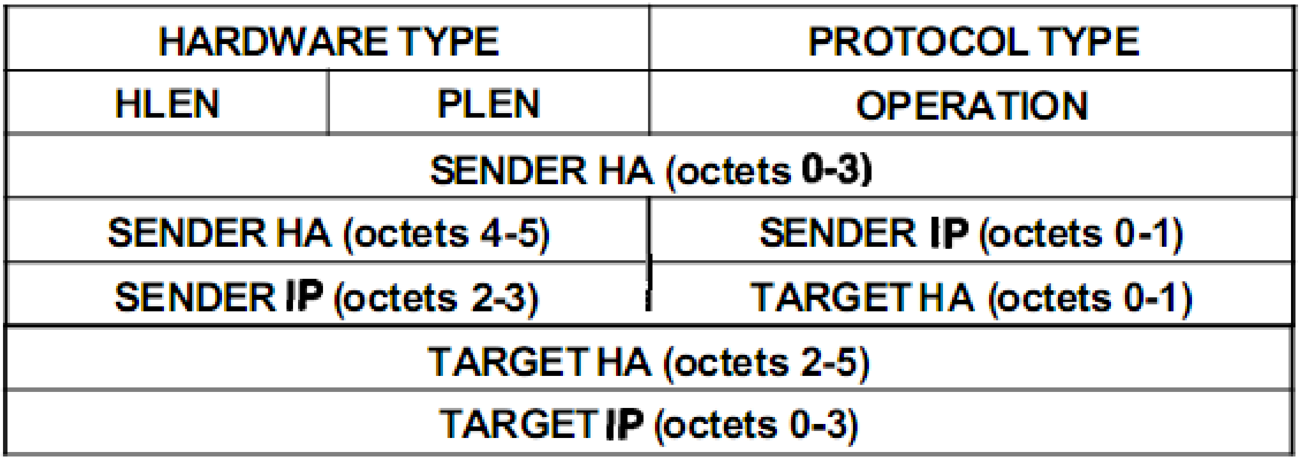
Designers of protocols found a creative solution to the address resolution problem for networks like the Ethernet that have broadcast capability. The solution allows new hosts or routers to be added to the network without recompiling code, and does not require maintenance of a centralized database. To avoid maintaining a table of mappings, the designers chose to use a low-level protocol to bind addresses dynamically. Termed the Address Resolution Protocol (ARP), the protocol provides a mechanism that is both reasonably efficient and easy to maintain.

As Figure 4.1 shows, the idea behind dynamic resolution with ARP is simple: when host A wants to resolve IP address ZB, it broadcasts a special packet that asks the host with IP address le to respond with its physical address, PB. AU hosts, including B, receive the request, but only host B recognizes its IP address and sends a reply that contains its physical address. When A receives the reply, it uses the physical address to send the internet packet directly to B. We can summarize:



**12. Can you write a brief outline about ARP protocol format with the aid of a diagram?**

The ARP message format is general enough to allow it to be used with arbitrary physical addresses and arbitrary protocol addresses.



| | | |
|---|---|---|
| HARDWARE TYPE | | PROTOCOL TYPE |
| HLEN | PLEN | OPERATION |
| SENDER HA (octets 0-3) | | |
| SENDER HA (octets 4-5) | | SENDER IP (octets 0-1) |
| SENDER IP (octets 2-3) | | TARGET HA (octets 0-1) |
| TARGET HA (octets 2-5) | | |
| TARGET IP (octets 0-3) | | |

An example of the ARP message format when used for IP- to-Ethernet address resolution.

- The length of fields depends on the hardware and protocol address lengths, which are 6 octets for an Ethernet address and 4 octets for an IP address.
- Field HARDWARE TYPE specifies a hardware interface type for which the sender seeks an answer; it contains the value 1 for Ethernet.
- Similarly, field PROTOCOL TYPE specifies the type of high-level protocol address the sender has supplied.
- Field OPERATION specifies an ARP request (I), ARP response (2), RARP request (3), or RARP response (4).
- Fields HLEN and PLEN allow ARP to be used with arbitrary networks because they specify the length of the hardware address and the length of the high-level protocol address.
- The sender supplies its hardware address and IP address, if known, in fields SENDER HA and SENDER IP.
- When making a request, the sender also supplies the target hardware address or target IP address, using fields TARGET HA or TARGET IP.
- Before the target machine responds, it fills in the missing addresses, swaps the target and sender pairs, and changes the operation to a reply.

## UNIT 2

Multiple Choice Questions

1. Can you clarify the contents of the general form of IP datagram________?
   - **a.** IP header only
   - **b.** IP Data only
   - **c. IP header and Data**
   - **d.** IP header, Data and control signals
2. Can you clarify the VERS field in the IP datagram specifies_______?
   - **a. IP Version** b. Data Version c. Protocol Version d. All the above
3. Can you illustrate the HLEN field in the IP datagram specifies?
   - **a.** Length of the total IP Datagram
   - **b. Length of the IP Header**
   - **c.** Length of the Body of the IP datagram
   - **d.** Total length of IP datagram
4. Can you illustrate the Time To Live field refers to______?
   - **a.** The time taken by the IP datagram to reach the destination.
   - **b.** The time taken by the IP datagram to start from the source.
   - **c. The total time that the IP datagram is active.**
   - **d.** The time taken by the IP datagram to survive in the network.
5. Can you illustrate the direct IP datagram delivery refers to______?
   - **a.** The delivery of the datagram directly to the outside network.
   - **b. The delivery of the datagram to the same network**
   - **c.** The delivery of the datagram to router.
   - **d.** The simple way of delivery of datagram.
6. Can you illustrate the indirect delivery refers to______?
   - **a.** Delivery of datagram to a single network.
   - **b.** Delivery of datagram to a multiple network.
   - **c. Delivery of datagram to a different network.**
   - **d.** Delivery of datagram to both single and multiple networks.
7. Can you specify the IP routing table is needed for?
   - **a.** IP datagram delivery to an inside network
   - **b.** IP datagram delivery to outside network
   - **c.** IP datagram delivery to internetwork.
   - **d. All the above.**
8. What would you think the router which is useful when a site has a small set of local addresses and only one connection to the rest of the internet?
   - **a.** Host specific routers
   - **b.** Table driven routers
   - **c. Default routers**
   - **d.** All the above
9. What would you think the purpose of the routing information protocol is?
   - **a.** To inform the routing to the routers.
   - **b. To dynamically update the routing table with latest updating.**
   - **c.** To route the IP datagram
   - **d.** To manage the routers and hosts.
10. Can you clarify the active participants in RIP operation?
    - **a.** Advertising themselves.
    - **b.** Listening to advertisements.
    - **c. Both Advertising and Listening.**

**d.** None of the Above.

11. How would you mention the router update routing information time?

**a.** 10 secs. b. 20 secs. **c. 30 secs.** d. 40 secs.

12. Can you clarify which protocol is used to find out the hop count?

**a.** RIP b. BGP c. IGP **d. HELLO**

13. Can you clarify the protocol which computes the shortest delay path to the destination?

**a.** **HELLO** b. IGP c. BGP d. RIP

14. How would you mention any protocol used to pass routing information between two autonomous systems?

**a.** IGP b**. EGP** c. RIP d. ARP

15. Can you clarify which is the EGP used for passing routing information between two autonomous system__________?

**a.** **BGP** b. IGP c. ARP. d. HELLO

16. Can you clarify which is the protocol used to map a single IP Network prefix into two physical networks______?

**a.** ARP **b. Proxy ARP** c. BGP d. HELLO

17. What do you think ARP Hack is another name given to__________?

**a.** ARP **b. Proxy ARP** c. BGP d. HELLO

18. How would you say which addressing has three parts in the IP address.

**a.** ARP **b. subnet addressing** c. Proxy ARP d. Classfull

19. What do you think -1 in subnet addressing represents_________?

**a.** **All ones.** b. ones compliment c. Twos compliment d. None

20. Can you explain VLSM stands for_____?

**a.** Value added Length Supernet Mask

**b.** Value Length Subnet Mask

**c.** **Variable Length Subnet Mas**

**d.** None of the above

21. What do you think OSPF is meant by?

**a.** **Open Source Shortest Path Finder.**

**b.** Open Source Smart Path Finder

**c.** Operation Source Smart Path Finder

**d.** Optional Source Smart Path Finder.

22. Can you illustrate the protocol which uses distance vector algorithm?

**a.** ARP b. HTTP c. **HELLO** d. FTP

23. Can you illustrate the TOTAL LENGTH field in IP datagram is for______?

**a.** To find the length of the header

**b.** To find the length of the data

**c.** **To find the total length of the IP datagram**

**d.** None of the above.

24. What do you think the maximum size of the IP datagram is

**a.** 65535 octates b. 12466 octates

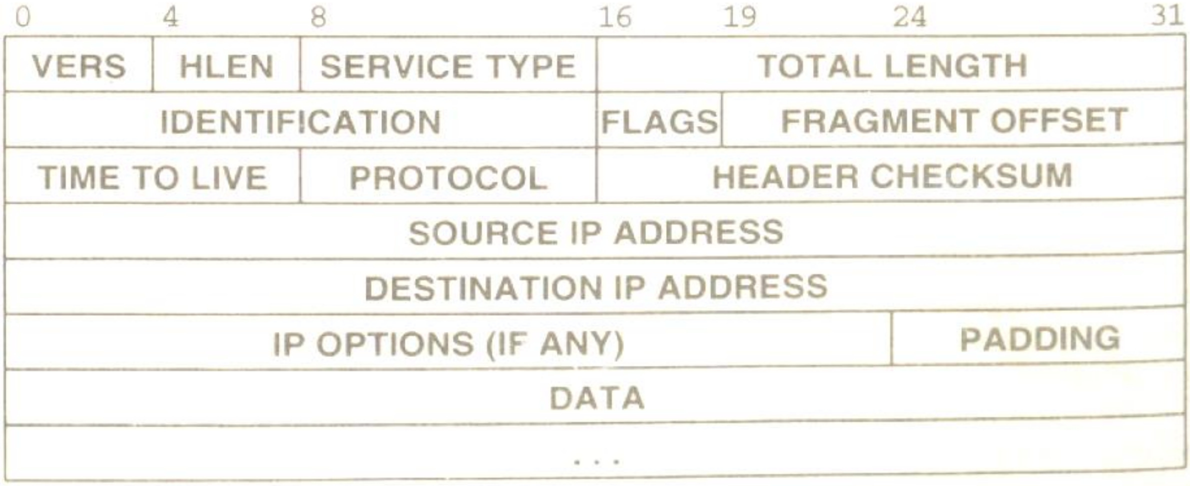
c. 565 octates d. 32250 octaes

25. What is the main idea in Forwarding the IP datagram is through?

**a.** RIP b**. Routing Table.** c. switch d. Hub

## Essay Questions

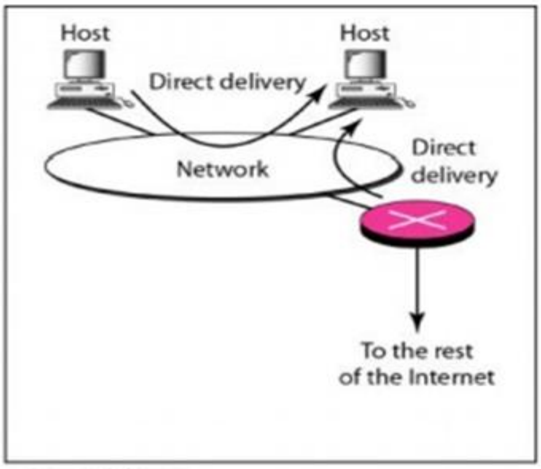
**1. Can you explain in your own words about the format of IP datagram? Draw the diagram for your statement.**



<table>
<tr><th>0</th><th>4</th><th>8</th><th>16</th><th>19</th><th>24 31</th></tr>
<tr><td>VERS</td><td>HLEN</td><td>SERVICE TYPE</td><td colspan="3">TOTAL LENGTH</td></tr>
<tr><td colspan="3">IDENTIFICATION</td><td>FLAGS</td><td colspan="2">FRAGMENT OFFSET</td></tr>
<tr><td colspan="2">TIME TO LIVE</td><td>PROTOCOL</td><td colspan="3">HEADER CHECKSUM</td></tr>
<tr><td colspan="6">SOURCE IP ADDRESS</td></tr>
<tr><td colspan="6">DESTINATION IP ADDRESS</td></tr>
<tr><td colspan="5">IP OPTIONS (IF ANY)</td><td>PADDING</td></tr>
<tr><td colspan="6">DATA</td></tr>
<tr><td colspan="6">. . .</td></tr>
</table>

Datagram processing occurs in software, the contents and format are not constrained by any hardware. For example, the first 4-bit field in a datagram (VERS) contains the version of the IP protocol that was used to create the datagram. It is used to verify that the sender, receiver, and any routers in between them agree on the format of the datagram. All IP software is required to check the version field before processing a datagram to ensure it matches the format the software expects. The header length field (HLEN), also 4 bits, gives the datagram header length measured in 32-bit words. As we will see, all fields in the header have fixed length except for the IP OPTIONS and corresponding PADDING fields. The most common header, which contains no options and no padding, measures 20 octets and has a header length field equal to 5. The TOTAL LENGTH field gives the length of the IP datagram measured in octets, including octets in the header and data. The size of the data area can be computed by subtracting the length of the header (HLEN) from the TOTAL LENGTH. Because the TOTALLENGTH field is 16 bits long, the maximum possible size of an IP datagram is 216 or 65,535 octets. In most applications this is not a severe limitation. It may become more important in the future if higher speed networks can carry data packets larger than 65,535octets.

**2. How would you explain the delivery of a datagram over a single network?**



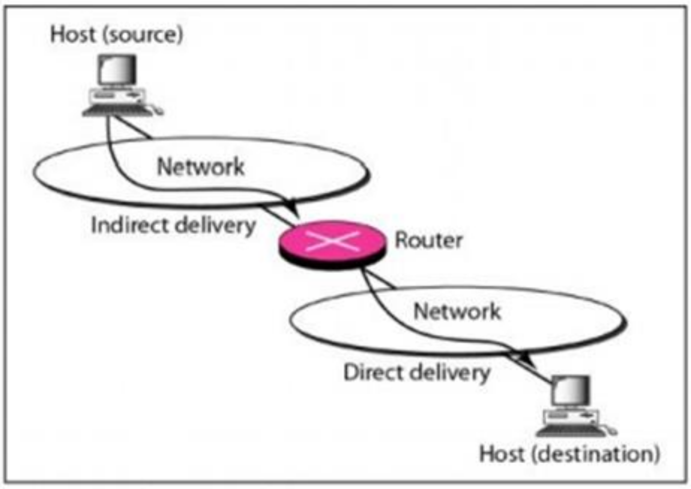
One machine on a given physical network can send a physical frame directly to another machine on the same network. To transfer an IP datagram, the sender encapsulates the datagram in a physical frame, maps the destination IP address into a physical address, and uses the network hardware to deliver it.

Transmission of an IP datagram between two machines on a single physical network does not involve routers. The sender encapsulates the datagram in a physical frame, binds the destination IP address to a physical hardware address, and sends the resulting frame directly to the destination.

To see if a destination lies on one of the directly connected networks, the sender extracts the network portion of the destination IP address and compares it to the network portion of its own IP address(es). A match means the datagram can be sent directly. Here we see one of the advantages of the Internet address scheme, namely:

Because the internet addresses of all machines on a single network include a common network pre& and extracting that pre& requires only a few machine instructions, testing whether a machine can be reached directly is extremely efficient.

**3. How would you explain the indirect delivery of the datagram?**



Indirect delivery is more difficult than direct delivery because the sender must identify a router to which the datagram can be sent. The router must then forward the datagram on toward its destination network. To visualize how indirect routing works, imagine a large internet with many networks interconnected by routers but with only two hosts at the far ends. When one host wants to send to the other, it encapsulates the datagram and sends it to the nearest outer. We know that the host can reach a router because all physical networks are interconnected, so there must be a router attached to each network. Thus, the originating host can reach a router using a single physical network. Once the frame reaches the router, software extracts the encapsulated datagram, and the IP software selects the next router along the path towards the destination. The datagram is again placed in a frame and sent over the next physical network to a second router, and so on, until it can be delivered directly. These ideas can be summarized:

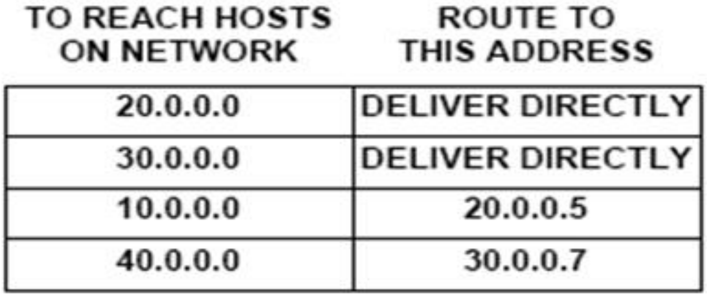
**Routers in a TCP/IP internet form a cooperative, interconnected structure. Datagram pass from router to router until they reach a router that can deliver the datagram directly.**

**4. Can you explain in your own words the process of Table-Driven IP forwarding?**

- An Internet routing table (sometimes called an IP routing table) on each machine that stores information about possible destinations and how to reach them.
- Routers use *Routing Tables* to determine out which interface the packet will be sent.

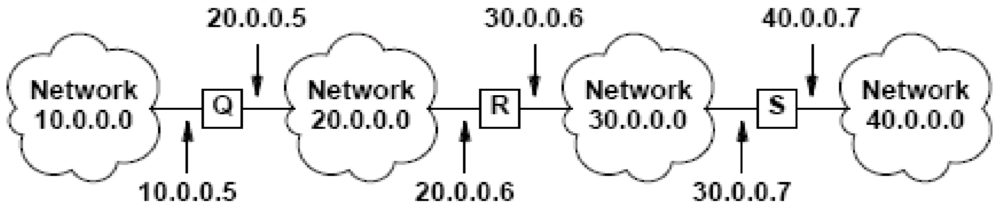
- Because both hosts and routers route datagrams, both have IP routing tables.
- Whenever the IP routing software in a host or router needs to transmit a datagram, it consults the routing table to decide where to send the datagram.
- If every routing table contained information about every possible destination address, it would be impossible to keep the tables current. Furthermore, because the number of possible destinations is large, machines would have insufficient space to store the information.
- Conceptually, we would like to use the principle of information hiding and allow machines to make routing decisions with minimal information. For example, we would like to isolate information about specific hosts to the local environment in which they exist and arrange for machines that are far away to route packets to them without knowing such details.
- It also means that routing tables only need to contain network prefixes and not full IP addresses.

Eg:

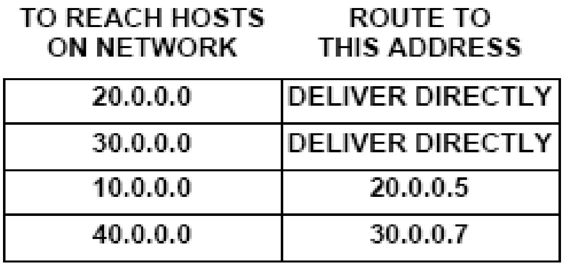


| TO REACH HOSTS ON NETWORK | ROUTE TO THIS ADDRESS |
|---|---|
| 20.0.0.0 | DELIVER DIRECTLY |
| 30.0.0.0 | DELIVER DIRECTLY |
| 10.0.0.0 | 20.0.0.5 |
| 40.0.0.0 | 30.0.0.7 |

**5. Can you illustrate the concept on next hop forwarding?**



(a)



| TO REACH HOSTS ON NETWORK | ROUTE TO THIS ADDRESS |
|---|---|
| 20.0.0.0 | DELIVER DIRECTLY |
| 30.0.0.0 | DELIVER DIRECTLY |
| 10.0.0.0 | 20.0.0.5 |
| 40.0.0.0 | 30.0.0.7 |

- Using the network portion of a destination address instead of the complete host address makes routing efficient and keeps routing tables small.
- More important, it helps hide information, keeping the details of specific hosts confined to the local environment in which those hosts operate.
- Typically, a routing table contains pairs (N, R), where N is the IP address of a destination network, and R is the IP address of the "next" router along the path to network N.
- Router R is called the next hop, and the idea of using a routing table to store a next hop for each destination is called next-hop routing.

- The size of the routing table depends on the number of networks in the internet; it only grows when new networks are added. However, the table size and contents are independent of the number of individual hosts connected to the networks.
- ***To hide information, keep routing tables small, and make routing decisions efficient, IP routing software only keeps information about destination network addresses, not about individual host addresses.***

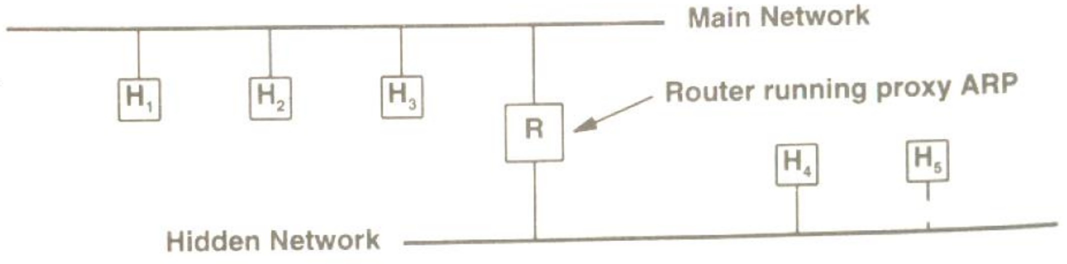
**6. Can you explain in your own words about the various goals of OSPF protocol?**

To encourage the adoption of link state technology, a working group of the Internet Engineering Task Force has designed an interior gateway protocol that uses the link state algorithm called Open SPF (OSPF), the new protocol tackles several ambitious goals.

- As the name implies, the specification is available in the published literature. Making it an open standard that anyone can implement without paying license fees has encouraged many vendors to support OSPF.
- OSPF is among the first TCP/IP protocols to offer type of service routing.
- OSPF provides load balancing. If a manager specifies multiple routes to a given destination at the same cost, OSPF distributes traffic over all routes equally.
- To permit growth and make the networks at a site easier to manage, OSPF allows a site to partition its networks and routers into subsets called areas.
- The OSPF protocol specifies that all exchanges between routers can be authenticated. OSPF allows a variety of authentication schemes, and even allows one area to choose a different scheme than another area.
- OSPF includes support for host-specific, subnet-specific, and classless routes as well as classful network-specific routes. All types may be needed in a large internet.
- To accommodate multi-access networks like Ethernet, OSPF extends the SPF algorithm.
- To permit maximum flexibility, OSPF allows managers to describe a virtual network topology that abstracts away from the details of physical connections.
- OSPF allows routers to exchange routing information learned from other (external) sites. Basically, one or more routers with connections to other sites learn information about those sites and include it when sending update messages.

**7. Can you explain in your own words about Proxy ARP? Draw the diagram for the explanation.**

Proxy ARP technique (the ARP hack) allows one network address to be shared between two physical nets. Router *R* answers ARP requests on each network for hosts on the other network, giving its hardware address and then routing datagrams correctly when they arrive. In essence, *R* lies about IP-lo-physical address bindings.

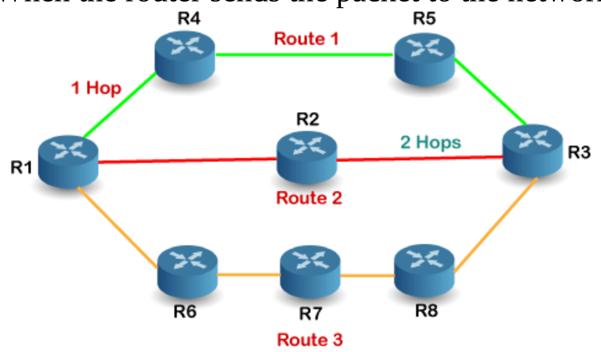


In the figure two network share a single IP network address. Imagine that labeled *Main Network* was the original network, and that the second, labeled network a hidden network, was added later. The router connecting the two networks, *R, kn*ows which host lie on which physical network and uses ARP to maintain the illusion that only one network exists, To make the illusion work, *R* keeps the location of hosts completely hidden, allowing all other machines on the network to communicate as if directly connected. In our example when host $H_1$needs to communicate with host $H_{4,}$ it first invokes ARP to map $H_4$'s IP address into a physical address. Once it has a physical address. $H_1$can send the datagram directly to that physical address.

Because *R* runs proxy ARP software, it captures the broadcast ARP request from *H* decides that the machine in question lies on the other physical network, and responds to the ARP request by sending its own physical address. *HI* receives the ARP response, installs the mapping in its ARP table, and then uses the mapping to send datagrams destined for $H_4$ to *R.* When *R* receives a datagram, It searches a special, routing table to determine how to route the datagram. *R* must forward datagrams destined for *H* over the hidden network. To allow hosts on the hidden network to reach hosts on 4, the main network, *R* performs the proxy ARP service on that network as well.

**8. Analyze the working of RIP.**

RIP uses a distance vector algorithm to decide which path to put a packet on to get to its destination. Each RIP router maintains a routing table, which is a list of all the destinations the router knows how to reach. Each router broadcasts its entire routing table to its closest neighbors every 30 seconds. When the router sends the packet to the network segment, then it is counted as a single hop.



when the router 1 forwards the packet to the router 2 then it will count as 1 hop count. Similarly, when the router 2 forwards the packet to the router 3 then it will count as 2 hop count, and when the router 3 forwards the packet to router 4, it will count as 3 hop count. In the same way, RIP can support maximum up to 15 hops, which means that the 16 routers can be configured in a RIP.If there are 8 routers in a network where Router 1 wants to send the data to Router 3. If the network is configured with RIP, it will choose the route which has the least number of hops. There are three routes in the above network, i.e., Route 1, Route 2, and Route 3. The Route 2 contains the least number of hops, i.e., 2 where Route 1 contains 3 hops, and Route 3 contains 4 hops, so RIP will choose Route 2.

**9. Analyze the working of HELLO protocol.**

- The HELLO protocol uses a distance-vector algorithm however, is that unlike RIP ,HELLO does ***not*** use hop count as a metric. Instead, it attempts to select the best route by assessing network delays and choosing the path with the shortest delay.
- it synchronizes the clocks among a set of machines, and it allows each machine to compute shortest delay paths to destinations.
- each machine participating in the HELLO exchange maintains a table of its best estimate of the clocks in neighboring machines.
- HELLO messages also allow participating machines to compute new routes.
- The protocol uses a modified distance-vector scheme that uses a metric of delay instead of hop count.

- Each machine sends its neighbors a table of destinations it can reach and an estimated delay for each.
- When a message arrives from machine X, the receiver examines each entry in the message and changes the next hop to X if the route through X is less expensive than the current route.

**10. Analyze the working of BGP.**

Border Gateway Protocol (BGP) refers to a gateway protocol that enables the internet to exchange routing information between autonomous systems (AS). As networks interact with each other, they need a way to communicate. Without it, networks would not be able to send and receive information with each other.

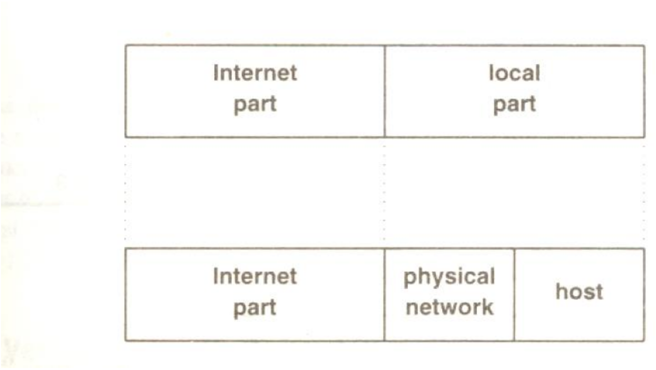
When you have a network router that connects to other networks, it does not know which network is the best one to send its data to. BGP takes into consideration all the different peering options a router has and chooses the one closest to where the router is. Each potential peer communicates the routing information it has and that gets stored within a routing information base (RIB). BGP can access this information and use it to choose the best peering option.

It can be characterized by the following:

- BGP has Inter-autonomous System Configuration
- BGP Supports Next-hop Paradigm
- BGP Coordination Among Multiple BGP Speakers Within an Autonomous System
- Within the BGP advertisement system is the path information that includes the next destination and which destinations are reachable.
- An administrator can design and implement policies by programming them into the BGP system.
- Classless Inter-Domain Routing (CIDR) refers to a way to allocate Internet Protocol (IP) addresses .
- While BGP does not have any security features inherent to it.

**11. What factors would you change if a single network is divided into subnet?**

- The process of dividing a single network into multiple sub networks is called as **subnetting**. The sub networks so created are called as **subnets**.
- Subnet addressing allows an autonomous system made up of multiple networks to share the same Internet address.
- The subnetwork capability of TCP/IP also makes it possible to divide a single network into multiple logical networks (subnets). For example, an organization can have a single Internet network address that is known to users outside the organization, yet it can configure its network internally into departmental subnets. In either case, fewer Internet network addresses are required while local routing capabilities are enhanced.
- A standard Internet Protocol address field has two parts:
- a network address and a local address.
- To make subnets possible, the local address part of an Internet address is divided into a subnet number and a host number. The subnet is identified so that the local autonomous system can route messages reliably.



Internet part
local part
Internet part
physical network
host

## UNIT 3

## MCQ Questions

1. How is UDP similar to?
    a. Unified Datagram Protocol
    b. Unnamed Datagram Protocol
    **c. User Datagram Protocol**
    d. Universal Datagram Protocol
2. Do you know the protocol which is used to send the datagram from one application to another application_____?
    **a.** FTP b. HTTP c. BGP d. **UDP**
3. Analyze the Multiple programs executing in a single machine which is distinguished by _____
    a. Gateways b. **Ports** c. connectors d. software
4. Analyze the one that uses UDP to accept full responsibility for handling the problem of reliability, including message loss, duplication, delay, out-of-order delivery, and loss of connectivity
    **a. An Application Program**
    b. A connecting port
    c. A Protocol
    d. Network device
5. Which concept that uses UDP datagram to accept datagrams from multiple application program?
    a. Mixing b. Shuffling. **c. Multiplexing** d. Demultiplexing.
6. Which concept that separates the UDP messages from the arrived datagram to appropriate software?
    **a.** Mixing b. Shuffling. c. Multiplexing **d. Demultiplexing.**
7. Analyze the properties of the reliable delivery services
    a. Stream orientation b. virtual circuit connection
    c. buffered transfer d. **All the above.**
8. What do you suggest the view of the data when two application programs transfer large volumes of data.
    a. Bits b. **a stream of bits** c. Individual Bits. d. Data
9. Which event should happen where before transfer of data can start, both sending and receiving application programs interact with each other?
    a. Telephonic connection
    b. Network connection
    **c. Virtual connection**
    d. Data connection
10. What do you suggest when connections provided by the stream service allow concurrent transfer in both directions?
    a. Simplex b. Half Duplex **c. Full Duplex** d. All the above.
11. Analyze the stream service that does not honor structured data streams is called ______
    a. **Unstructured stream** b. structured stream c. data stream d. data bytes.
12. Analyze the reply from the receiver for all the packets that are received from source is called _______
    a. Simple reply **b. Acknowledgement** c. Message d. Packet
13. What do you suggest for what the sliding window protocol is used ____________
    **a. Send Multiple Packets before receiving the acknowledgement.**

b. Wait for the acknowledgement before sending the next packet.
c. Keep on sending the packets to the destination.
d. Keep on receiving the acknowledgement.

14. Analyze TCP is___________type of protocol
   a. **Connection oriented** b. Connectionless c. Both d. None of the above
15. Analyze the protocol that requires both endpoints to agree to participate?
   a. UDP **b. TCP** c. IP d. HTTP
16. Analyze the application program on one end performs a__________open function by contacting its operating system and indicating that it will accept an incoming connection. At that time the operating system assigns a TCP port number for its end of the connection.
   a. **Passive** b. Active c. Both d. None of the above.
17. ____________is the creation of a listening socket, to accept incoming connections.
   a. **Passive open** b. Active open c. Ports open d. None
18. ___________is the creation of a connection to a listening port by a client.
   a. Passive open b. **Active open** c. Ports open d. None
19. Passive Open uses________operation.
   **a.** socket () b. bind () c. listen () d**. All of the above**
20. Active Opens uses________operation.
   a. **Connect ()** b. blind () c. listen () d. None
21. ___________protocols use network bandwidth better because they allow the sender to transmit multiple packets before waiting for an acknowledgement.
   a. **Sliding window** b. stream delivery c. silly window d. none

22. What would you see the possible outcome where the application programs start exchanging data only after? ___________
   a. Active Port is open
   b. Passive Port is open
   c. Connection is established
   **d. All the above**

23. What would you see the possible outcome where to establish a connection, TCP uses ______?
   a. Single hand shake
   b. Two-way hand shake
   **c. Three-way hand shake**
   d. No hand shakes
24. What would you see the possible outcome where to close a connection, TCP uses ______?
   a. Single hand shake
   b. Two-way hand shake
   **c. Modified Three-way hand shake**
   d. No hand shakes
25. What would you see the possible outcome where the application programs in TCP can begin to pass the data only after? _______
   a. After communicating
   **b. Establishing a connection.**
   c. Opening the Ports
   d. All the Above

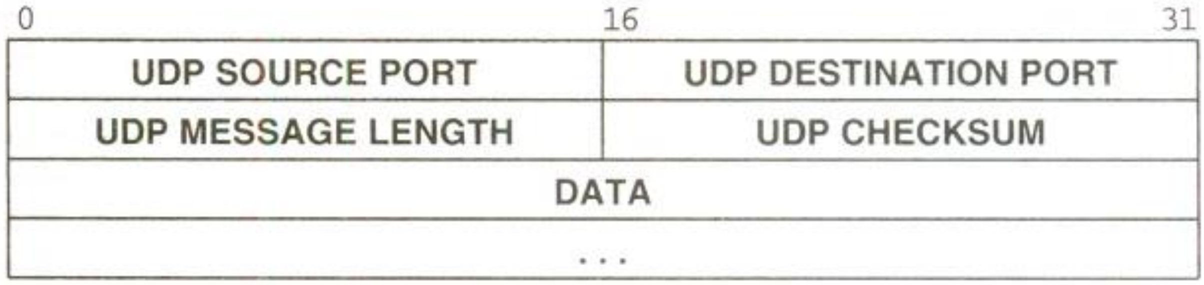
## Essay Questions:

### 1. Can you explain UDP?

- In the protocol suite, the User Datagram Protocol or UDP provides the primary mechanism that application programs use to send datagrams to other application programs.
- That is, in addition to the data sent, each UDP message contains both a destination port number and a source port number, making it possible for the UDP software at the destination to deliver the message to the correct recipient and for the recipient to send a reply.
- UDP uses the underlying internet layer to transport a message from one machine to another, and provides the same unreliable, connectionless datagram delivery semantics as IP.
- The User Datagram Protocol (UDP) provides an unreliable connectionless delivery service using IP to transport messages between machines.
- It does not use acknowledgements to make sure messages arrive; it does not order incoming messages, nor does it provide feedback to control the rate at which information flows between the machines.
- An application program that uses UDP accepts full responsibility for handling the problem of reliability, including message loss, duplication, delay, out-of-order delivery, and loss of connectivity.
- Application programmers often ignore these problems when designing software. Furthermore, because programmers often test network software using highly reliable, low-delay local area networks, testing may not expose potential failures.
- Thus, many application programs that rely on UDP work well in a local environment, but fail in dramatic ways when used in the global Internet.

### 2. How would you explain the UDP message format with the help of a diagram?

- Each UDP message is called a user datagram. Conceptually, a user datagram consists of two parts: a UDP header and a UDP data area.
- The header is divided into four 16-bit fields that specify the port from which the message was sent, the port to which the message is destined, the message length, and a UDP checksum.



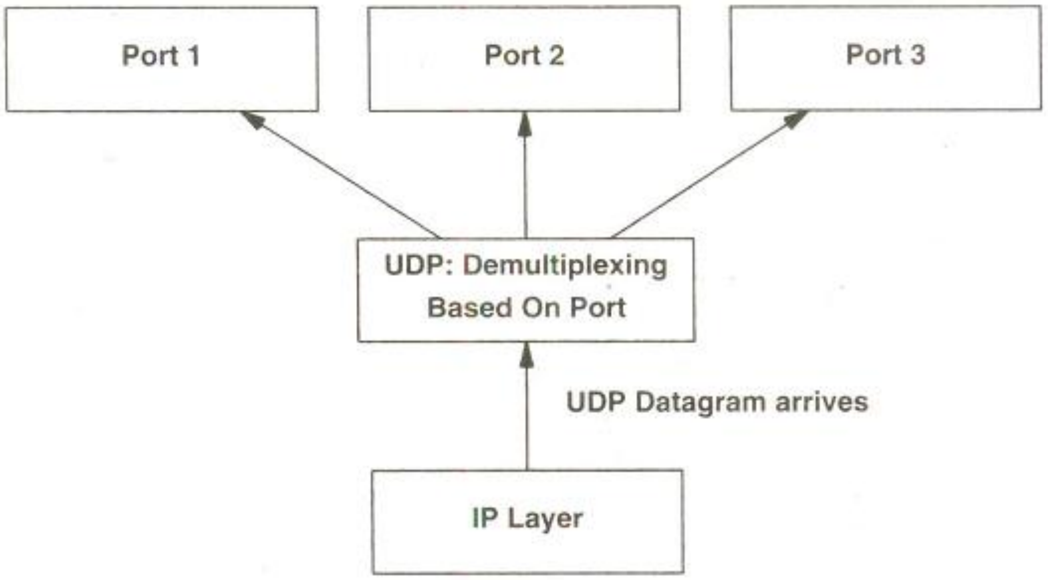
0 16 31

| | |
|---|---|
| UDP SOURCE PORT | UDP DESTINATION PORT |
| UDP MESSAGE LENGTH | UDP CHECKSUM |
| DATA | |
| . . . | |

- The SOURCE PORT and DESTINATION PORT fields contain the 16-bit UDP protocol port numbers used to demultiplex datagrams among the processes waiting to receive them. The SOURCE PORT is optional. When used, it specifies the port to which replies should be sent; if not used, it should be zero.
- The LENGTH field contains a count of octets in the UDP datagram, including the UDP header and the user data. Thus, the minimum value for LENGTH is eight, the length of the header alone.
- The UDP checksum is optional and need not be used at all; a value of zero in the CHECKSUM field means that the checksum has not been computed. The designers chose to make the checksum optional to allow implementations to operate with little computational overhead when using UDP across a highly reliable local area network.

- The UDP checksum includes a pseudo-header that has fields for the source and destination IP addresses.

**3. How would you explain the process of multiplexing and Demultiplexing the UDP datagrams?**



- UDP software provides another example of multiplexing and demultiplexing.
- It accepts UDP datagrams from many application programs and passes them to IP for transmission, and it accepts arriving UDP datagrams from IP and passes each to the appropriate application program.
- all multiplexing and demultiplexing between UDP software and application programs occur through the port mechanism.
- While processing input, UDP accepts incoming datagrams from the IP software and demultiplexes based on the UDP destination port.
- When UDP 8 receives a datagram, it checks to see that the destination port number matches one of the ports currently in use.
- If not, it sends error message and discards the datagram.
- If a match is found, UDP enquires the new datagram at the port where an application program can access it.

**4. Can you illustrate TCP?**

- The protocol specifies the format of the data and acknowledgements that two computers exchange to achieve a reliable transfer, as well as the procedures the computers use to ensure that the data arrives correctly.
- ***TCP is a communication protocol but not a piece of software.***
- It specifies how TCP software distinguishes among multiple destinations on a given machine, and how communicating machines recover from errors like lost or duplicated packets.
- The protocol also specifies how two computers initiate a TCP stream transfer and how they agree when it is complete.
- TCP can run over a variety of hardware mechanisms such as a dialup telephone line, a local area network, a high-speed fiber optic network, a satellite connection, or a noisy wireless connection in

which many packets are lost. The large variety of delivery systems TCP can use is one of its strengths.

- TCP specification describes how application programs use TCP in general terms, it does not dictate the details of the interface between an application program and TCP.
- TCP can be used with a variety of packet delivery systems. In particular, because it does not require the underlying system to be reliable or fast.
- TCP can run over a variety of hardware mechanisms such as a dialup telephone line, a local area network, a high-speed fiber optic network, a satellite connection, or a noisy wireless connection in which many packets are lost.

**5. Can you illustrate the passive opens and the active opens?**

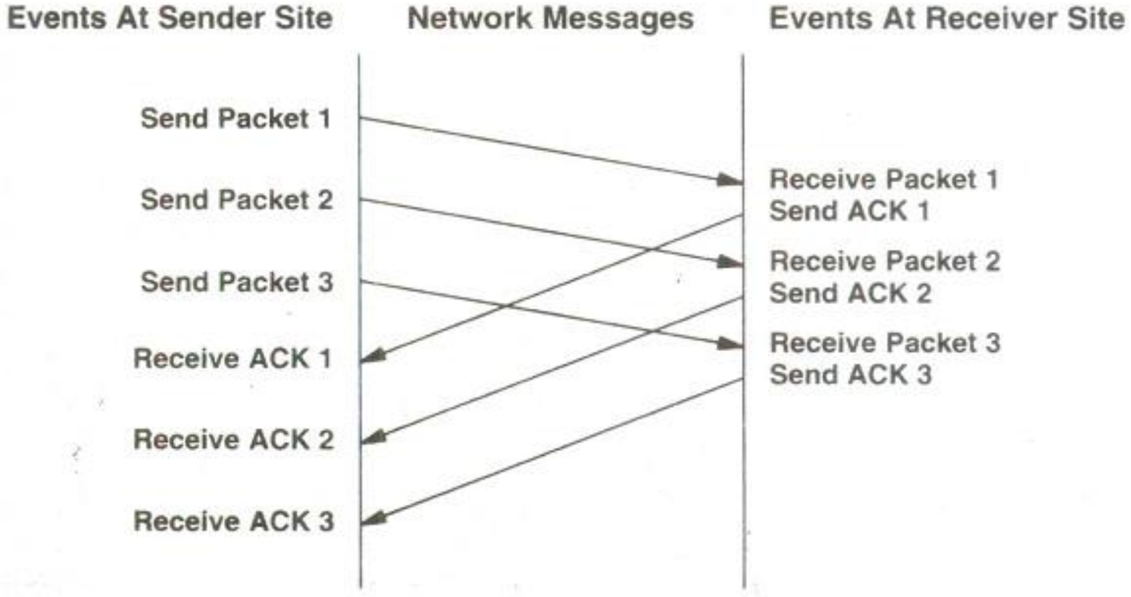
- TCP is a connection-oriented protocol that requires both endpoints to agree to participate. That is, before TCP traffic can pass across an internet, application programs at both ends of the connection must agree that the connection is desired.
- To do so, the application program on one end performs a passive open function by contacting its operating system and indicating that it will accept an incoming connection.
- At that time the operating system assigns a TCP port number for its end of the connection. The application program at the end must then contact its operating system using an active open request to establish a connection.
- The two TCP software modules communicate to establish and verify a connection. Once a connection has been created, application programs can begin to pass data; the TCP software modules at each end exchange messages that guaranty the reliable delivery.
- A passive open is the creation of a listening socket, to accept incoming connections. It uses socket(), bind(), listen(), followed by an accept() loop.
- An active open is the creation of a connection to a listening port by a client. It uses socket() and connect().

**6. List and analyze the properties of reliable delivery service.**

- **Stream Orientation:** When two application programs transfer large volumes of data, the data is viewed as a stream of bits, divided into 8-bit octets or bytes. The stream delivery service on the destination machine passes to the receiver exactly the same sequence of octets that the sender passes to it on the source machine.
- **Virtual Circuit Connection**. Making a stream transfer is analogous to placing a telephone call. Before transfer can start, both the sending and receiving application programs interact with their respective operating systems, informing them of the desire for a stream transfer.
- **Buffered Transfer.** Application programs send a data stream across the virtual circuit by repeatedly passing data octets to the protocol software. When transferring data, an application uses whatever size pieces it finds convenient, which can be as small as a single octet. At the receiving end, the protocol software delivers octets from the data stream in exactly the same order they were sent, making them available to the receiving application program as soon as they have been received and verified.
- **Unstructured Stream.:** Application programs using the stream service must understand stream content and agree on stream format before they initiate a connection.
- **Full Duplex Connection**. Connections provided by the stream service allow concurrent transfer in both directions. Such connections are called full duplex. The advantage of a full duplex connection is that the underlying protocol software can send control information for one stream back to the source in datagrams carrying data in the opposite direction.

**7. Analyze with the aid of a diagram three packet transmission using sliding window.**

Sliding window protocols use network bandwidth better because they allow the sender to transmit multiple packets before waiting for an acknowledgement. Sender transmits all three packets before receiving any 'acknowledgements.

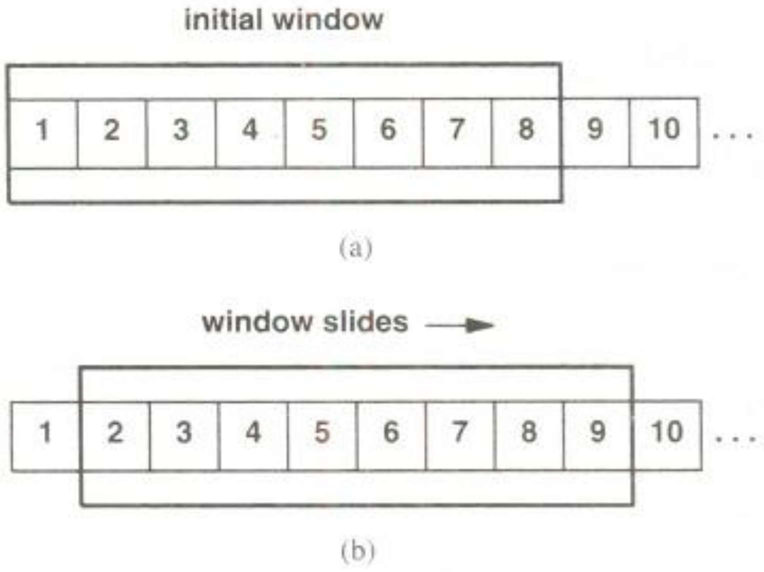


- An example of three packets transmitted using a sliding window protocol. The key concept is that the sender can transmit all packets in the window without waiting for an acknowledgement.
- The window partitions the sequence of packets into three sets:
- those packets to the left of the window have been successfully transmitted, received, and acknowledged;
- those packets to the right have not yet been transmitted;
- and those packets that lie in the window are being transmitted.
- The lowest numbered packet in the window is the first packet in the sequence that has not been acknowledged.

**8. What are some of the motives behind the sliding window? Explain.**

- The concept, known as a sliding window, makes stream transmission efficient.
- A simple positive acknowledgement protocol wastes a substantial amount of network bandwidth because it must delay sending a new packet until it receives an acknowledgement for the previous packet.
- Sliding window protocols use network bandwidth better because they allow the sender to transmit multiple packets before waiting for an acknowledgement.
- The protocol places a small, fixed size window on the sequence and transmits all packets that lie inside the window.
- A sliding window protocol with eight packets in the window
- The window sliding so that packet 9 can be sent when an acknowledgement has been received for packet 1. Only un acknowledged packets are retransmitted.
- Once the sender receives an acknowledgement for the first packet inside the window, it "slides" the window along and sends the next packet. The window continues to slide as long as acknowledgements are received.
- Packet is unacknowledged if it has been transmitted but no acknowledgement has been received.

- the number of packets that can be unacknowledged at any given time is constrained by the window size, which is limited to a small, fixed number.
- For example, in a sliding window protocol with window size 8, the sender is permitted to transmit 8 packets before it receives an acknowledgement.



(a)

(b)

9. **Analyze the methods in establishing a TCP connection? Explain with the diagram.**

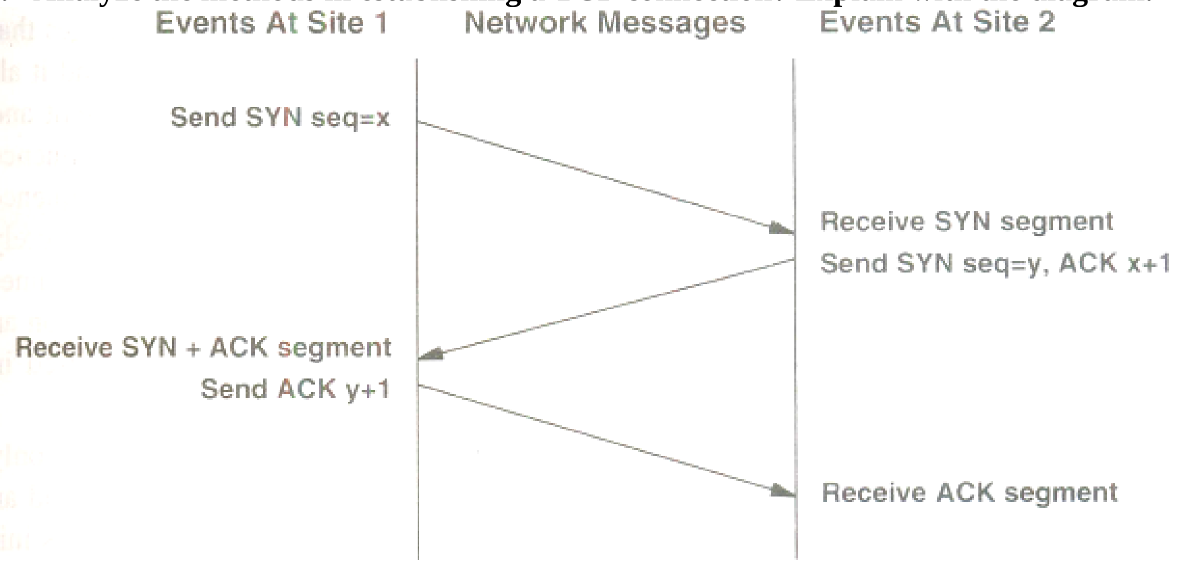


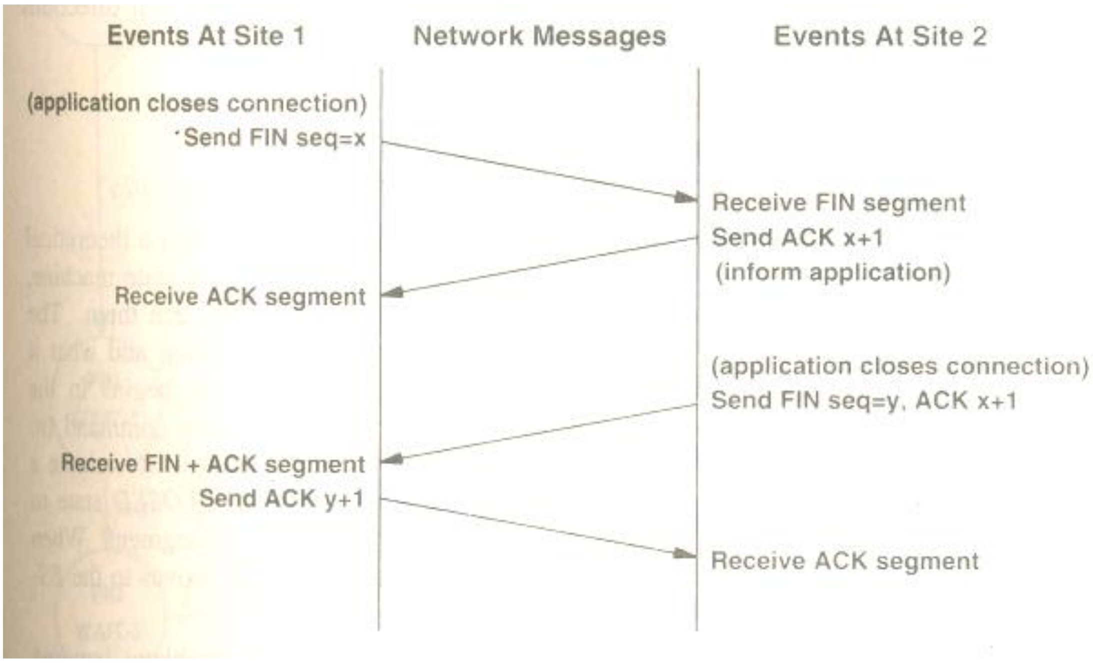
Figure: The sequence of messages in a three-way handshake. Time proceeds down the page; diagonal lines represent segments sent between sites. SYN segments carry initial sequence number information.

- To establish a connection, TCP uses a three-way handshake.
- The first segment of a handshake can be identified because it has the SYN bit set in the code field.
- The second message has both the SYN and ACK bits set, indicating that it acknowledges the first SYN segment as well as continuing the handshake.
- The final handshake message is only an acknowledgement and is merely used to inform the destination that both sides agree that a connection has been established.
- A connection can be established from either end or from both ends simultaneously. Once the connection has been established, data can flow in both directions equally well.

- The three-way handshake is both necessary and sufficient for correct synchronization between the two ends of the connection.

**10. Analyze the methods of closing a TCP connection? Explain with the diagram.**

Two programs that use TCP to communicate can terminate the conversation gracefully using the close operation. TCP connections are full duplex and that we view them as containing two independent stream transfers, one going in each direction. When an application program tells TCP that it has no more data to send, TCP will close the connection in one direction. To close its half of a connection, the sending TCP finishes transmitting the remaining data, waits for the receiver to acknowledge it, and then sends a segment with the FIN bit set. The receiving TCP acknowledges the FIN segment and informs the application program on its end that no more data is available



The modified three-way handshake used to close connections. The site that receives the first FIN segment acknowledges it immediately, and then delays before sending the second FIN segment.

The difference between three-way handshakes used to establish and break connections occurs after a machine receives the initial FIN segment. Instead of generating a second FIN· segment immediately, TCP sends an acknowledgement and then informs the application of the request to shut down. Informing the application program of the request and obtaining a response may take considerable time. The acknowledgement prevents retransmission of the initial FIN segment during the wait. Finally, when the application program instructs TCP to shut down the connection completely.

**11. Analyze the need for Stream Delivery.**

- At the lowest level, computer communication networks provide unreliable packet delivery. Packets can be lost or destroyed when transmission errors interfere with data, when network hardware fails, or when networks become too heavily loaded to accommodate the load presented.
- Packet switching systems change routes dynamically, deliver packets out of order, deliver them after a substantial delay. or deliver duplicates.
- At the highest level, application programs often need to send large volumes of data from one computer to another.
- Using an unreliable connectionless delivery system for large volume transfers becomes tedious and annoying, and it requires that programmers build error detection and recovery into each application

program. Because it is difficult to design, understand, or modify software that correctly provides reliability, few application programmers have the necessary technical background.

- As a consequence, one goal of network protocol research has been to find general purpose solutions to the problems of providing reliable stream delivery, making it possible for experts to build a single instance of stream protocol software that all application programs use. Having a single general-purpose protocol helps isolate application programs from the details of networking, and makes it possible to define a uniform interface for the stream transfer service.

## UNIT 4
## Multiple Choice Questions.

**(Questions for Understanding)**

1. Can you clarify the problem that can arise in poor implementations of the transmission control protocol (TCP) when the receiver is only able to accept a few bytes at a time or when the sender transmits data in small segments repeatedly?
   **a.** Delayed Transmission b. **Silly Window Syndrome**
   c. Silly Window Avoidance d. Fast Transmission
2. Can you illustrate the tinygrams which are_____?
   a. **Small Packets** b. IP Packets c. UDP Packets d. Control Packets
3. Can you write the concept of multipoint delivery of datagram?
   a. Multiple Delivery b. All Casting c. **Multicasting** d. Unicasting
4. Can you clarify the system delivery in which the network delivers one copy of a packet to each destination?
   a. **Broadcast** b. Unicast c. Multicast d. Nocast.
5. Can you illustrate the concept of systems choosing many systems of different networks to participate in a network?

a. Unicast b. **Multicast** c. Broadcast d. Nocast

6. What do you think the address reserved for Multicasting is ?
   **a.** Class A b. Class B c. Class C d**. Class D**
7. What do you think the technique of having an acknowledgement that can be pure if contains no data and is just for acknowledging one or more segments, or it can be *not pure* when apart from the *ACK* it contains data that is sent back from destination to source is ?
   **a.** Tallback b. Small Back c. Tinyback **d. piggyback**
8. The purpose to reduce the number of *ACKs* required to acknowledge the segments is _____

   a. Positive Acknowledgement b. Negative Acknowledgement
   **c. Delayed Acknowledgement d.** Simple Acknowledgement
9. Can you clarify the destination retaining the *ACK* segment a period of time 200 ms in Microsoft Windows by default?
   a. Positive Acknowledgement b. Negative Acknowledgement
   **c. Delayed Acknowledgement d.** Simple Acknowledgement
10. What do you think is the algorithm that concatenates the small packets?
    a. Routing Algorithm b. ARP algorithm
    c. Hash Algorithm **d. Nagel's Algorithm**
11. Analyze from below which are used to ensure that excessive delays are not encountered during communications
    a. Acknowledgements b. TCP Connectors
    **c. TCP Timers** d. IP Timers
12. Identify TCP implementation which uses __________timers.
    a. 1 b. 2 c. 3 **d. 4**
13. Analyze the timer that is used during TCP connection termination.
    a. **Time Wait** b. Keep Alive c. Persistant d. Time out
14. Which factor is used for many hardware technologies to use the mechanisms to send packets to multiple destinations Simultaneously?

a. Software IP Multicast b. Hardware Broadcast
c. **Hardware Multicast** d. All off the above.

15. Analyze the internet abstraction of hardware multicasting.
**a.** Hardware Multicasting b. **IP- Multicasting**
c. Hybrid Multicasting d. Anycasting

16. Which factor is used to communicate with the group members the IP multicast protocol?
a. HTTP b. **IGMP** c. TFTP d. Class D

17. Analyze the domain name system which uses___________naming scheme?
a. normal b. sequential c. **Hierarchical** d. None of the above

18. Analyze the domain name to IP address after the domain resolution which will be stored in ____
a. **cache** b. RAM c. Secondary memory d. None

19. Can you mention which protocol uses the simple textual remote terminal access?
a. R-Login b. **TelNet** c. FTP d. SNMP

20. Can you mention the BSD Unix version of TelNet protocol?
a. TelNet b. BSD c**. Rlogin** d. IMAP

21. Analyze RDP?
a. **Remote Desktop Protocol** b. Remote Distance Protocol
c. Remote Destination Protocol d. None of the above

22. Can you illustrate the concept of systems choosing many systems of different networks to participate in a network?
a. Unicast b. **Multicast** c. Broadcast d. Nocast

23. IGMP stands for___________

a. **Internet Group Management Protocol** b. Internet Graphical Message Protocol

b. Internet Group Message Protocol d. None.

24. DNS stands for____________
a. Data Network Server b. **Domain Name System** c. Domain Network Server d. None

25. The protocol suite includes a simple textual remote terminal protocol called __________

a. **TELNET** b. DNS c. VPN d. SNTP

**Essay Questions**
**(Questions for Understanding)**

1. **Can you write a brief outline of DNS with the help of an example?**

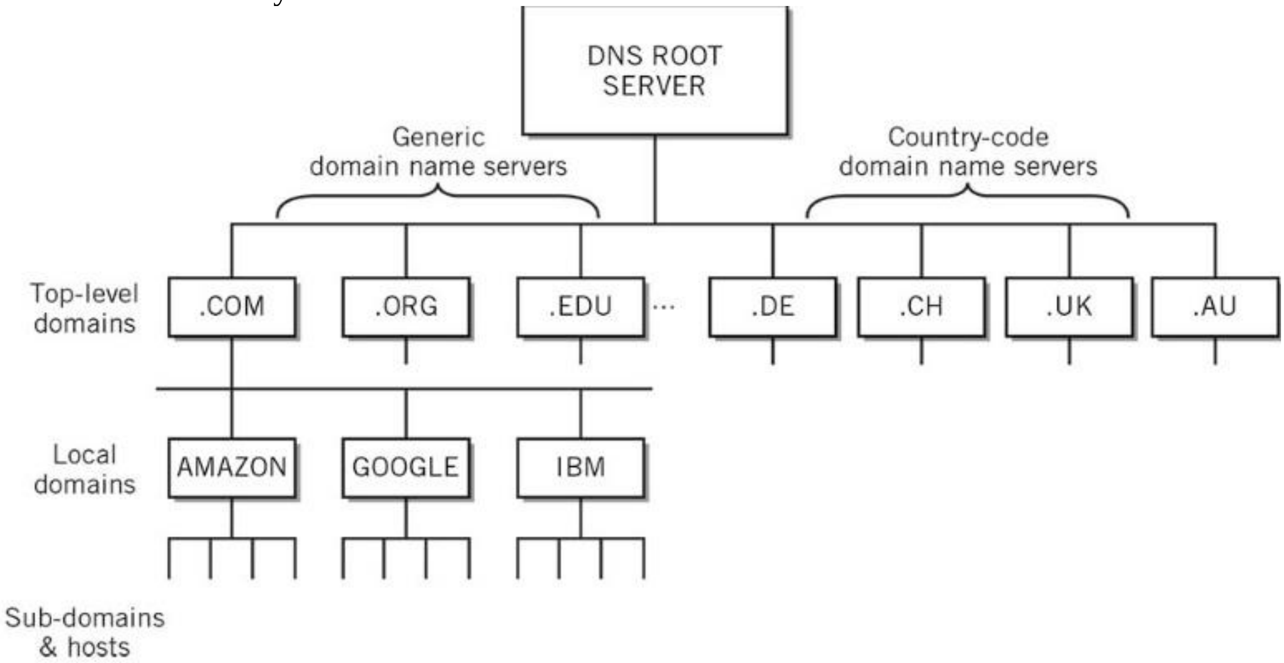
The Domain Name System (DNS) is the system that provides name to address mapping for the Internet. DNS has two, conceptually independent aspects. The first is abstract: it specifies the name syntax and rules for delegating authority over names. The second is concrete: it specifies the implementation of a distributed computing system that efficiently maps names to addresses. This section considers the name syntax, and later sections examine the implementation. The domain name system uses a hierarchical naming scheme known as domain names. A domain name consists of a sequence of sub names separated by a delimiter character, the period. In our examples we said that individual sections of the name might represent sites or groups, but the domain name system simply calls each section a label. Thus, the domain name

***cs.purdue.edu***

contains three labels: cs, purdue, and edu. Any suffix of a label in a domain name is also called a domain. In the above example, the lowest-level domain is cs. purdue. edu, (the domain name for the Computer Science Department at Purdue University), these cond level domain is purdue. edu (the domain name for Purdue University), and the top-level domain is edu (the domain name for educational institutions). As the example shows, domain names are written with the local label first and the top domain last. As we will see; writing them in this order makes it possible to compress messages that contain multiple domain names.

2. **Can you illustrate the method of resolution of Domain name?**

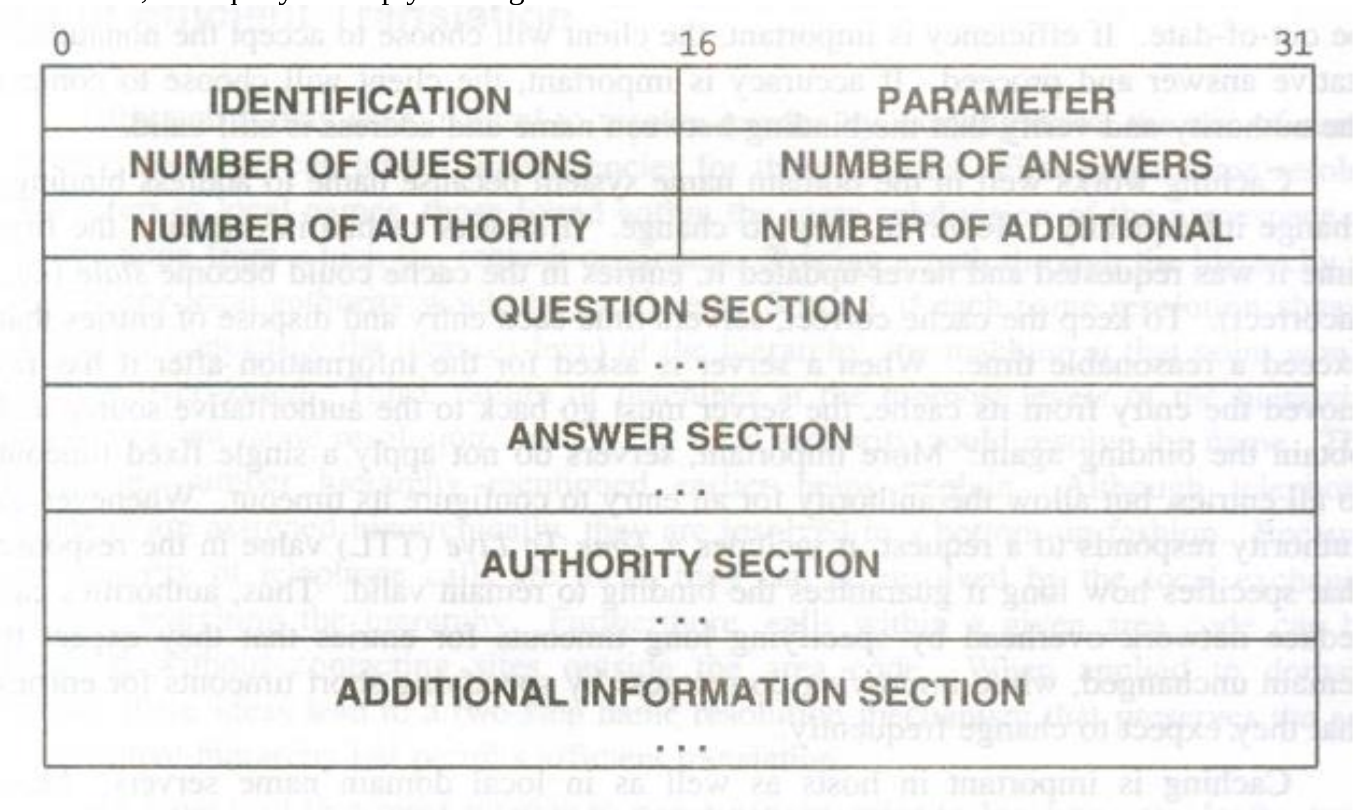
Domain resolution is the process of converting domain names to IP addresses. The resolution of the domain name is done by the DNS server.



Although the conceptual tree makes understanding the relationship between servers easy, it hides several subtle details. Conceptually, domain name resolution proceeds top-down, starting with the root name server and proceeding to servers located at the leaves of the tree. There are two ways to use the domain name system: by contacting name servers one at a time or asking the name server system to perform the complete translation. In either case, the client software forms a domain name query that contains the name to be resolved, a declaration of the class of the name, the type of answer desired, and a code that specifies whether the name server should translate the name completely. It sends the query to a name server for resolution. When a domain name server receives a query, it checks to see if the name lies in the sub domain for which it is an authority. If so, it translates the name to an address according to its database, and appends an answer to the query before sending it back to the client. If the name server cannot resolve the name completely, it checks to see what type of interaction the client specified. If the client requested complete translation, the server contacts a domain name server that can resolve the name and returns the answer to the client. If the client requested non-recursive resolution (iterative resolution), the name server cannot supply an answer. It generates a reply that specifies the name server the client should contact next to resolve the name.

**3. How would you explain the DNS message format? Draw the diagram for theexplanation.**

DNS is a query/response protocol. DNS Query is a request sent from a DNS Client to a DNS Server, asking for the IP Address related. DNS Response is a reply from the DNS server to the DNS client. Furthermore, both query and reply messages have the same format.



| 0 | 16 31 |
|---|---|
| IDENTIFICATION | PARAMETER |
| NUMBER OF QUESTIONS | NUMBER OF ANSWERS |
| NUMBER OF AUTHORITY | NUMBER OF ADDITIONAL |
| QUESTION SECTION<br>. . . | |
| ANSWER SECTION<br>. . . | |
| AUTHORITY SECTION<br>. . . | |
| ADDITIONAL INFORMATION SECTION<br>. . . | |

- The first 12 bytes is the header section, which has a number of fields. The first field is a 16-bit number that identifies the query. This identifier is copied into the reply message to a query, allowing the client to match received replies with sent queries.
- There are a number of flags in the flag or Parameter field. A 1-bit query/reply flag indicates whether the message is a query (0) or a reply (1). A 1-bit authoritative flag is set in a reply message when a DNS server is an authoritative server for a queried name.
- In the header, there are also four number-of fields. These fields indicate the number of occurrences of the four types of data sections that follow the header.
- The question section contains information about the query that is being made. This section includes (1) a name field that contains the name that is being queried, and (2) a type field that indicates the type of questions being asked about the name.
- In a reply from a DNS server, the answer section contains the resource records for the name that was originally queries. Recall that in each resource record there is the Type, the Value, and the TTL.
- The authority section contains records of other authoritative servers.
- The additional section contains other helpful records. For example, the answer field in a reply to an MX query contains a resource record providing the canonical hostname of a mail server.

4. **Can you clarify the Telnet protocol?**

The protocol suite includes a simple textual remote terminal protocol called TELNET that allows a user to log into a computer across an internet. TELNET establishes a TCP connection, and then passes keystrokes from the user's keyboard directly to the remote computer as if they had been typed on a keyboard attached to the remote machine. TELNET also carries textual output from the remote machine back to the user's screen. The service is called transparent because it gives the appearance that the user's keyboard and display attach directly to the remote machine.

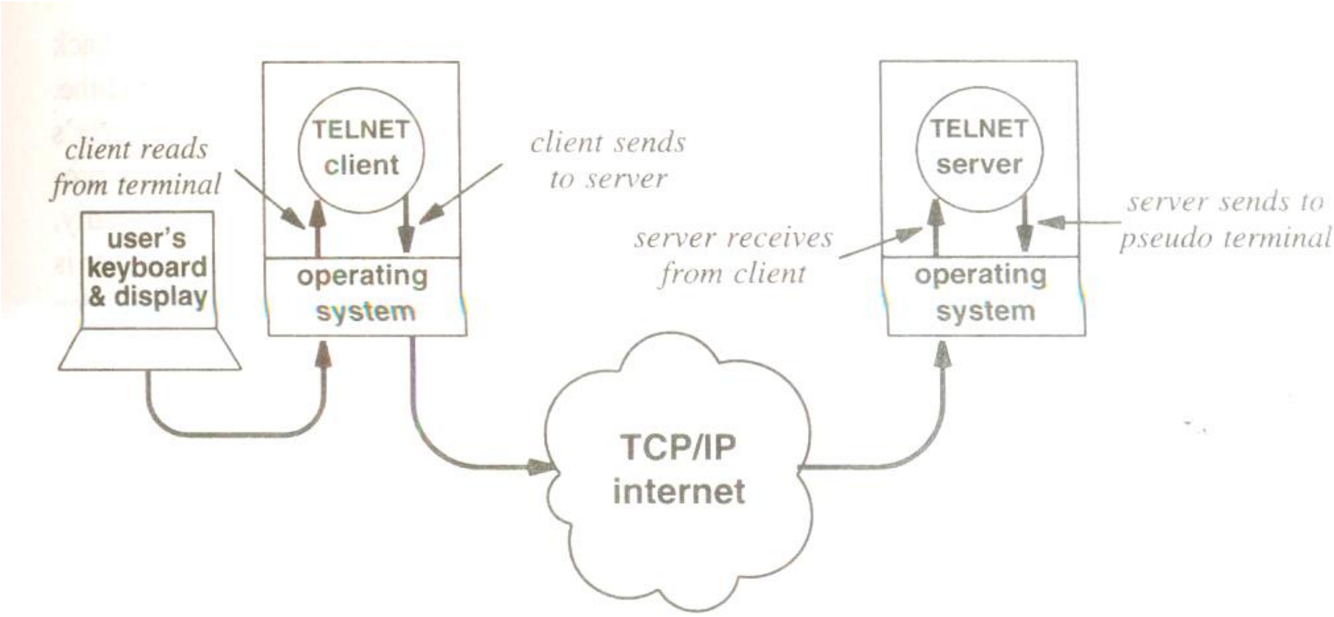
TELNET offers three basic services. First, it defines a network virtual terminal that provides a standard interface to remote systems. Client programs do not have to understand the details of all possible remote systems; they are built to use the standard interface. Second, TELNET includes a mechanism that allows the client and server to negotiate options, and it provides a set of standard options (e.g., one of the options controls whether data passed across the connection uses the standard 7-bit ASCII character set or an 8-bit character set). Finally, TELNET treats both ends of the connection symmetrically. In particular, TELNET does not force client input to come from a keyboard, nor does it force the client to display output on a screen. Thus, TELNET allows an arbitrary program to become a client. Furthermore, either end can negotiate options.

5. **Analyze Rlogin and VNC with explanation.**

**Rlogin,** one of the earliest alternatives to TELNET, devised as part of the BSD Unix operating system, was known as rlogin. Rlogin pioneered an idea that has been used with subsequent services, including SSH: trusted hosts. In essence, the mechanism allows system administrators to choose a set of machines over which login names and file access protections are shared and to establish equivalences among user logins. Users can control access to their personal accounts by authorizing remote login based on remote host and remote user names. Thus, it is possible for a user to have login name X on one machine and Yon another, and still be able to remotely login from one of the machines to the other without typing a password each time.

**Virtual Network Computing** (VNC). Unlike TELNET, rlogin, or SSH, VNC provides a remote desktop capability instead of a textual interface. That is, VNC allows a user on one computer to see an exact copy of the desktop on another computer and to use the keyboard and mouse to interact with the remote computer - the user can see the windows, icons, and other graphics. More important, VNC software runs across multiple platforms. As a result, the client can run on a computer that uses Linux, even if the server runs on a computer that uses Windows.

6. **Analyze the procedure of application programs implementing a Telnet client with theTelnet server with the help of a diagram**



- The path of data in a TELNET remote terminal session as it travels from the user's keyboard to the remote operating system.
- As the figure shows, when a user invokes TELNET, an application program on the user's machine becomes the client.
- The client establishes a TCP connection to the server over which they will communicate.
- Once the connection has been established, the client accepts keystrokes from the user's keyboard and sends them to the server, while it concurrently accepts characters that the server sends back and displays them on the user's screen.
- The client also checks for an escape character that a user can type to control the client.
- The server accepts a TCP connection from the client, and then relays data between the TCP connection and the local operating system.
- We use the term pseudo terminal to describe the operating system entry point that allows a running program like the TELNET server to transfer characters to the operating system as if they came from a keyboard.
- It is impossible to build a TELNET server unless the operating system supplies such a facility. If the system supports a pseudo terminal abstraction, the TELNET server can be implemented with application programs.

**7. Can you explain the procedure of IP Multicasting?**

Some hardware technologies support a second, less common form of multi-point delivery called multicasting. Unlike broadcasting, multicasting allows each system to choose whether it wants to participate in a given multicast. Typically, a hardware technology reserves a large set of addresses for use with multicast. When a group of machines want to communicate, they choose one particular multicast address to use for communication. After configuring their network interface hardware to recognize the selected multicast address, all machines in the group will receive a copy of any packet sent to that multicast address.

At a conceptual level, multicast addressing can be viewed as a generalization of all other address forms. For example, we can think of a conventional unicast address as a form of multicast addressing in which there is exactly one computer in the multicast group. Similarly, we can think of directed broadcast addressing as a form of multicasting in which all computers on a particular network are members of the multicast group. Other multicast addresses can correspond to arbitrary sets of machines. Unicast and broadcast addresses identify a computer or a set of computers attached to one physical segment, so forwarding depends on the network topology. A multicast address identifies an arbitrary set of listeners, so the forwarding mechanism must propagate the packet to all segments. For example, consider two LAN segments connected by an adaptive bridge that has learned host addresses. If a host on segment 1 sends a unicast frame to another host on segment 1, the bridge will not forward the frame to segment 2. If a host uses a multicast address, however, the bridge will forward the frame. Thus, we can conclude: Although it may help us to think of multicast addressing as a generalization that subsumes unicast and broadcast addresses, the underlying forwarding and delivery mechanisms can make multicast less efficient.

**8. Analyze the various characteristics of IP Multicast.**

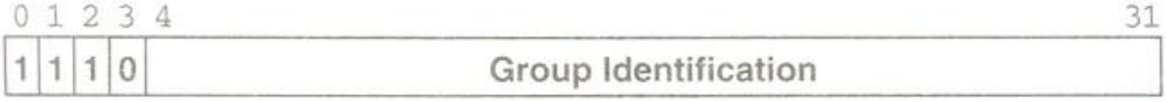
IP multicasting has the following general characteristics:

- Group Address. Each multicast group is a unique class D address. A few IP multicast addresses are permanently assigned by the Internet authority, and correspond to groups that always exist even if they have no current members. Other addresses are temporary, and are available for private use.
- Number Of Groups. IP provides addresses for up to 228 simultaneous multicast groups. Thus, the number of groups is limited by practical constraints on routing table size rather than addressing.
- Dynamic Group Membership. A host can join or leave an IP multicast group at any time. Furthermore, a host may be a member of an arbitrary number of multicast groups.
- Use Of Hardware. If the underlying network hardware supports multicast, IP uses hardware multicast to send IP multicast. If the hardware does not support multicast, IP uses broadcast or unicast to deliver IP multicast.
- Inter-network Forwarding. Because members of an IP multicast group can attach to multiple physical networks, special multicast routers are required to forward IP multicast; the capability is usually added to conventional routers.
- Delivery Semantics. IP multicast uses the same best-effort delivery semantics as other IP datagram delivery, meaning that multicast datagrams can be lost, delayed, duplicated, or delivered out of order.
- Membership And Transmission. An arbitrary host may send datagrams to any multicast group; group membership is only used to determine whether the host receives datagrams sent to the group.

**9. Can you explain the Class D addressing scheme for IP Multicasting?**

Class D addressing scheme for IP Multicasting

- Two types of multicast addresses are permanently assigned and for temporary use.
- Permanent addresses are called well-known; they are used for major services on the global Internet as well as for infrastructure maintenance.
- Other multicast addresses correspond to transient multicast groups that are created when needed and discarded when the count of group members reaches zero.
- Like hardware multicasting, IP multicasting uses the datagram's destination address to specify that a particular datagram must be delivered via multicast.
- IP reserves class D addresses for multicast



- The format of class D IP addresses used for multicasting. Bits 4 through 31 identify a particular multicast group.
- The first 4 bits contain 1110 and identify the address as a multicast. The remaining 28 bits specify a particular multicast group. There is no further structure in the group bits. In particular, the group field is not partitioned into bits that identify the origin or owner of the group, nor does it contain administrative information such as whether all members of the group are on one physical network.

- When expressed in dotted decimal notation, multicast addresses range from 224.0.0.0 through 239.255.255.255
- Many parts of the address space have been assigned special meaning. For example, the lowest address, 224.0.0.0, is reserved; it cannot be assigned to any group. Address 224.0.0.1 is permanently assigned to the all systems group, and address 224.0.0.2 is permanently assigned to the all routers group.

**10. Analyze IGMP with explanation.**

IGMP (Internet Group Management Protocol):

**IGMP** is acronym for **Internet Group Management Protocol**. IGMP is a communication protocol used by hosts and adjacent routers for multicasting communication with IP networks and uses the resources efficiently to transmit the message/data packets. Multicast communication can have single or multiple senders and receivers and thus, IGMP can be used in streaming videos, gaming or web conferencing tools. IGMP runs between roots and nodes.

IGMP version 1 is the first version that hosts can use to announce to a router that they want to receive multicast traffic from a specific group. It’s a simple protocol that uses only two messages:

- Membership report
- Membership query

When a host wants to join a multicast group, it will send a **membership report** to the group address that it wants to receive. When the multicast-enabled router receives this message, it will start forwarding the requested multicast traffic on the interface where it received the IGMP membership report on.

IGMP version 2 is the “enhanced” version of IGMP version 1. One of the major reasons for a new version was to improve the “leave” mechanism. In IGMP version 1, hosts just stop listening to the multicast group address but they never report this to the router.

Here are the new features:

- Leave group messages
- Group specific membership query
- MRT (Maximum Response Time) field
- Querier election process

IGMP version 3 adds support for “source filtering”. IGMP version 1 and version 2 allow hosts to join multicast groups but they don’t check the source of the traffic. Any source is able to receive traffic to the multicast group(s) that they joined.

## Unit – 5

### (MCQ)

1. Analyze the protocol used to share a file of a large size.
   a. SNMP **b. FTP** c. TFTP d. POP
2. Analyze the protocol which is connection oriented for communication?
   a. **FTP** b. TFTP c. SNMP d. POP
3. Analyze the protocol which uses two separate lines for control and data communication?
   **a.** POP b. SNMP c. TFTP **d. FTP**
4. Analyze the protocol which provides an inexpensive and unsophisticated service?
   a. POP b. SNMP **c. TFTP** d. FTP
5. Analyze the software which is much smaller and can be encoded within a ROM?
   a. POP b. SNMP **c. TFTP** d. FTP
6. Can you mention the sending side of TFTP transmits the file with how many fixed block sizes?
   a. **512 bytes** b. 1024 bytes c. 2048bytes d. Any random size.
7. Can you identify the company which developed Network File System?
   a. Microsoft b. Intel **c. Sun Microsystem** d. None
8. Can you mention the protocol used for simple text mail transmission?
   a. **SMTP** b. FTP c. TFTP d. MIME
9. Can you mention the protocol which transfers the mail from a mail box to the local computer?
   a. SMTP b. FTP **c. POP** d. HTTP
10. Analyze the protocol which allows the mail messages from multiple locations and ensures that all copies are synchronized and consistent?
    a. SMTP b. **IMAP** c. POP d. HTTP
11. Analyze the protocol that is used to send non ASCII data through e mail
    a. **MIME** b. POP c. HTTP d. SMTP
12. Can you mention the variable length option field is the feature in?
    **a.** IPV4 b. IP c. TCP **d. IPV6**

### (Questions for Skill)

13. Which one of the below has the flexible header format?
    **a.** IPV4 b. IP c.TCP **d. IPV6**
14. Which of the following has provision for extension?
    **a.** IPV4 b. IP c. TCP **d. IPV6**
15. Can you find out a correct option from the below for protocol which has support for autoconfiguration and renumbering.
    **a.** IPV4 b. IP c. TCP **d. IPV6**
16. Can you find out a correct option from the below for the protocol where it has compulsory base header and optional extension header.
    **a.** IPV4 b. IP c. TCP **d. IPV6**
17. Which one from the below has the HOP LIMIT field?
    **a.** IPV4 b. IP c. TCP **d. IPV6**
18. Which protocol has the PAY LOAD LENGTH?

**a.** IPV4 b. IP c. TCP **d. IPV6**

19. Which protocol has the TRAFFIC CLASS available?

**a.** IPV4 b. IP c. TCP **d. IPV6**

20. Can you find out the RCPT command available in which Protocol?

a. TFTP **b. SMTP** c. FTP d. MIME

21. Can you find out the protocol which does not require reliable connection for file transmission?

a. FTP **b. TFTP** c. SNMP d. MIME

22. Which message type is used by the client to establish a connection for writing a file from the server?

a. **TFTP WRQ** b. TFTP DATA c. TFTP RRQ d. TFTP ACK

23. Which of the connection remains connected during the entire interactive FTP session?

a. **Control** b. Data c. Hardware d. None

24. Which field has been replaced by a HOP LIMIT field?

a. **TIME-TO-LIVE** b. PAYLOAD LENGTH
c. FLOW LABEL field. d. PROTOCOL

25. NFS stands for

a. **Network File System** b. Neural File Server
c. Non-commercial File server d. None

**Essay Questions.**

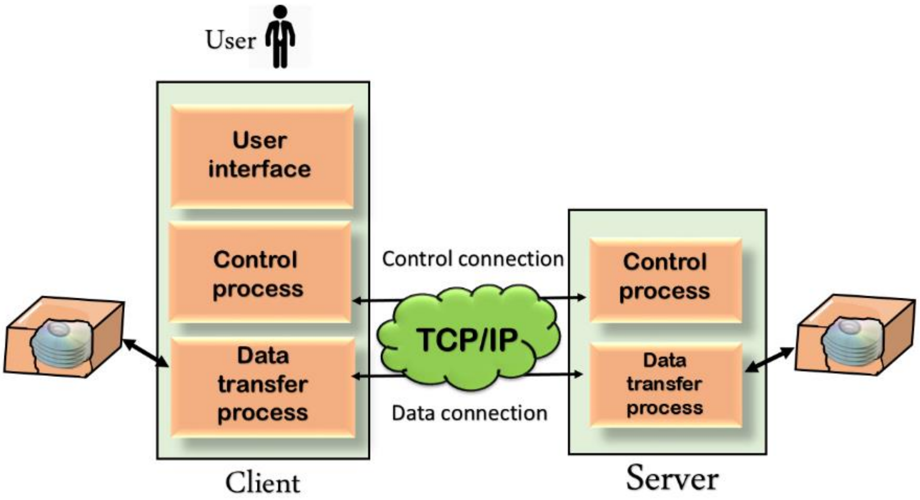
1. **Find the features of FTP.**

The File Transfer Protocol is a standard communication protocol used for the transfer of computer files from a server to a client on a computer network. FTP is built on a client–server model architecture using separate control and data connections between the client and the server. It is mainly used for transferring the web page files from their creator to the computer that acts as a server for other computers on the internet. It is also used for downloading the files to computer from other servers.

In addition, FIP offers many facilities beyond the transfer function itself.

- Interactive Access. Although FTP is designed to be used by programs, most implementations also provide an interactive interface that allows humans to interact with remote servers.
- Format Specification. FTP allows the client to specify the type and representation of stored data. For example, the user can specify whether a file contains text or binary data and whether text files use the ASCII or EBCDIC character sets.
- Authentication Control. FTP requires clients to authorize themselves by sending a login name and password to the server before requesting file transfers. The server refuses access to clients that cannot supply a valid login and password.

2. **Design a model of FTP with the help of the diagram.**



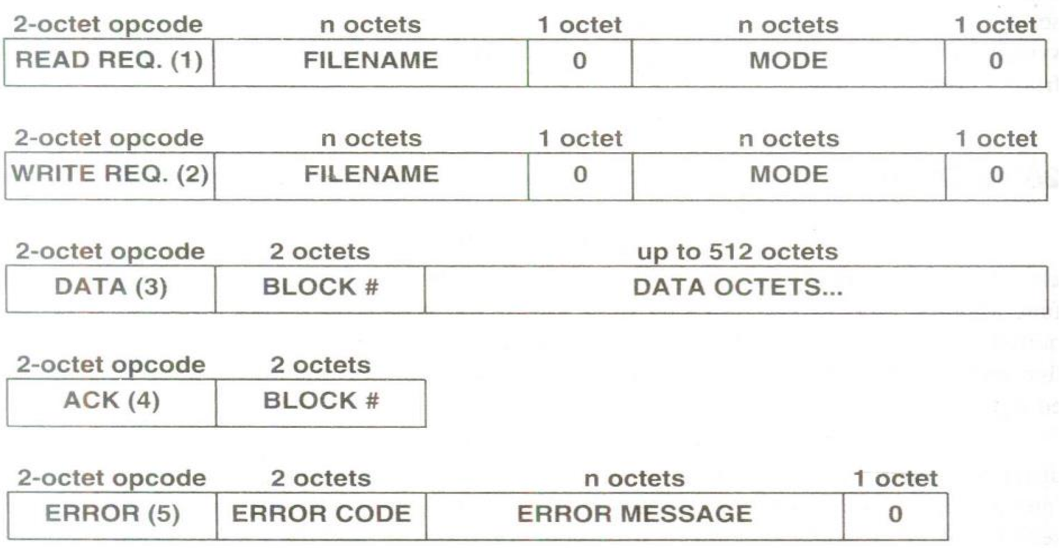
The above figure shows the basic model of the FTP. The FTP client has three components: the user interface, control process, and data transfer process. The server has two components: the server control process and the server data transfer process.

**There are two types of connections in FTP:**

- Control Connection: The control connection uses very simple rules for communication. Through control connection, we can transfer a line of command or line of response at a time. The control connection is made between the control processes. The control connection remains connected during the entire interactive FTP session.
- Data Connection: The Data Connection uses very complex rules as data types may vary. The data connection is made between data transfer processes. The data connection opens when a command comes for transferring the files and closes when the file is transferred.

TP client is a program that implements a file transfer protocol which allows you to transfer files between two hosts on the internet. It allows a user to connect to a remote host and upload or download the files. It has a set of commands that we can use to connect to a host, transfer the files between you and your host and close the connection. The FTP program is also available as a built-in component in a Web browser. This GUI based FTP client makes the file transfer very easy and also does not require to remember the FTP commands.

### 3. Find out the five TFTP packet types with the aid of a diagram



| 2-octet opcode | n octets | 1 octet | n octets | 1 octet |
|---|---|---|---|---|
| READ REQ. (1) | FILENAME | 0 | MODE | 0 |

| 2-octet opcode | n octets | 1 octet | n octets | 1 octet |
|---|---|---|---|---|
| WRITE REQ. (2) | FILENAME | 0 | MODE | 0 |

| 2-octet opcode | 2 octets | up to 512 octets |
|---|---|---|
| DATA (3) | BLOCK # | DATA OCTETS... |

| 2-octet opcode | 2 octets |
|---|---|
| ACK (4) | BLOCK # |

| 2-octet opcode | 2 octets | n octets | 1 octet |
|---|---|---|---|
| ERROR (5) | ERROR CODE | ERROR MESSAGE | 0 |

1. **The TFTP RRQ (Read Request)** message type is used by the client to establish a connection for

reading a file from the server. Opcode field of TFTP RRQ (Read Request) packet is 16-bits in length. TFTP RRQ packets have an opcode of "1”. The TFTP RRQ packet has a file name, which is name of the file requested. File name is string of variable size. Filenam
e is terminated by a byte of all zeros. Mode field contains information about the data transfer mode. The end of TFTP RRQ packets is with a byte length field of all 0s.

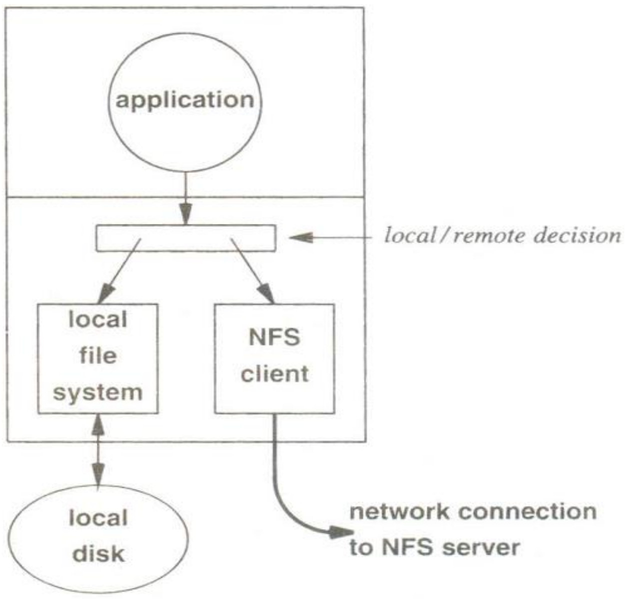
2. **The TFTP WRQ (Write Request)** message type is used by the client to establish a connection for writing a file from the server. Opcode field of TFTP WRQ packet is 16-bits in length. TFTP WRQ packets have an opcode of "2”. The TFTP WRQ packet has a file name, which is name of the file requested. Mode field contains information about the data transfer mode. The end of TFTP WRQ packets is with a byte length field of all 0s.

3. **The TFTP DATA** packet is used for sending blocks of data, belongs to a file. TFTP DATA packets have an opcode value of "3”. The Block Number field on Data Packets starts with one and then increase sequentially by one for each new packet. This type of numbering allows TFTP applications to identify between new DATA packets and duplicates. The DATA field size is from 0 to 512 bytes. DATA field size of all the packets are 512 bytes in length, except the last packet. If the size of the DATA field is between 0 to 511 bytes, that is the last DATA packet belongs to the current transmission.

4. **The TFTP ACK** packet is used to acknowledge the receipt of a DATA packet. The TFTP ACK packet is 4 bytes long. TFTP ACK (Acknowledge) Packets have an opcode of "4”. Block Number field of TFTP ACK packet contains the number of the DATA block received. The Block Number of the ACK of a TFTP WRQ packets is 0.

5.**The TFTP ERROR** packet is used to notify a problem during data transmission or when a TFTP connection cannot be established. Opcode field of TFTP ERROR packet is 16-bits (2-bytes) in length. TFTP ERROR packets have an opcode value of "5". The error code of TFTP ERROR packet is an integer showing the type of the error. Error Message field of the TFTP ERROR packet is a variable size field. Error Message field is a human readable field and is in ASCII. The TFTP ERROR packet is terminated with one byte of all zeros.

**4. Design a model of NFS with the help of a diagram.**



- NFS is a mechanism for storing files on a network. It is a distributed file system that allows users to access files and directories located on remote computers and treat those files and directories as if they were local.

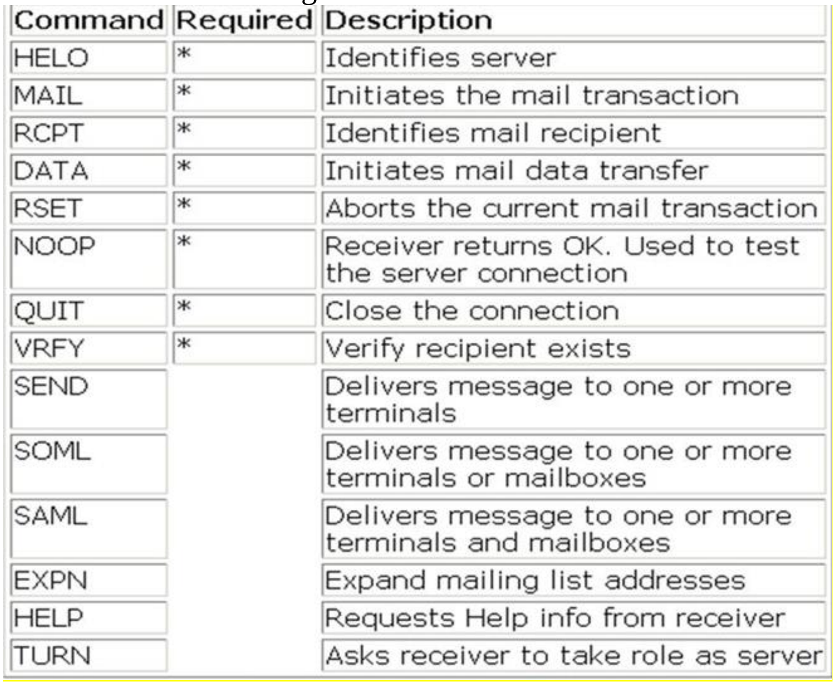
For example, users can use operating system commands to create, remove, read, write, and set file attributes for remote files and directories.

- Implementation of NFS in an operating system. When an application requests a file operation, the operating system must pass the request to the local file system or to the NFS client software.
- When an application program executes, it calls the operating system to open a file, to read data from a file, or to write data into a file. The file access mechanism accepts the request, and automatically passes it to either the local file system software or to the NFS client, depending on whether the file is on the local disk or on a remote machine. When it receives a request, the client software uses the NFS protocol to contact the appropriate server on a remote machine and perform the requested operation. When the remote server replies, the client software returns the results to the application program.

**5. Debate on SMTP.**

- The TCP/lP protocol suite specifies a standard for the exchange of mail between machines. That is, the standard specifies the exact format of messages a client on one machine uses to transfer mail to a server on another. The standard transfer protocol is known as the Simple Mail Transfer Protocol (SMTP).
- The SMTP protocol focuses specifically on how the underlying mail delivery system passes messages across an internet from one machine to another. It does not specify how the mail system accepts mail from a user or how the user interface presents the user with incoming mail. Also, SMTP does not specify how mail is stored or how frequently the mail system attempts to send messages.
- SMTP is surprisingly straightforward. Communication between a client and server consists of readable ASCII text. As with other' application protocols, programs read the abbreviated commands and 3-digit numbers at the beginning of lines; the remaining text is intended to help humans debug mail software.

SMTP has the following commands:

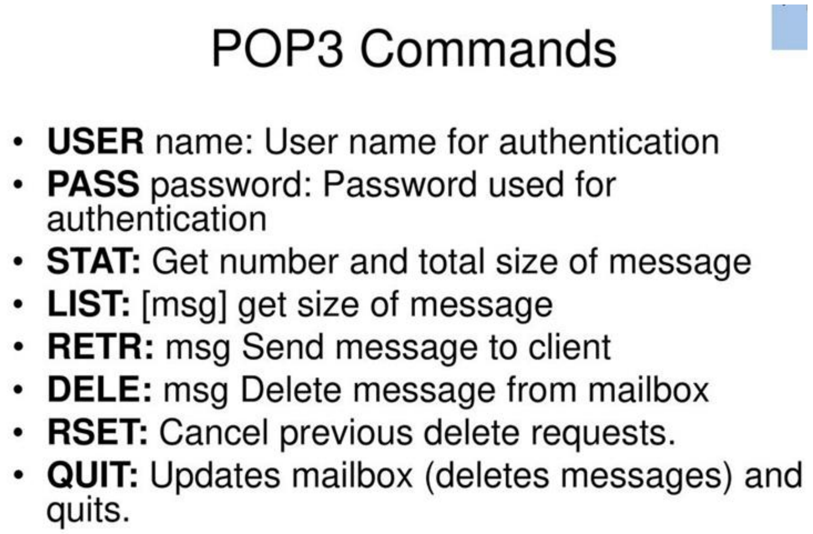


| Command | Required | Description |
|---|---|---|
| HELO | * | Identifies server |
| MAIL | * | Initiates the mail transaction |
| RCPT | * | Identifies mail recipient |
| DATA | * | Initiates mail data transfer |
| RSET | * | Aborts the current mail transaction |
| NOOP | * | Receiver returns OK. Used to test the server connection |
| QUIT | * | Close the connection |
| VRFY | * | Verify recipient exists |
| SEND | | Delivers message to one or more terminals |
| SOML | | Delivers message to one or more terminals or mailboxes |
| SAML | | Delivers message to one or more terminals and mailboxes |
| EXPN | | Expand mailing list addresses |
| HELP | | Requests Help info from receiver |
| TURN | | Asks receiver to take role as server |

**6. Find the feature of Post Office Protocol.**

POP is a short form of Post Office Protocol. It is another protocol present at the Application Layer of the OSI reference model. POP is mainly a message access protocol.

- POP is basically an internet standard protocol and works on the application layer and is used by the local email software in order to retrieve emails from the remote email server over the TCP/IP connection.
- The Post office Protocol (POP) does not allow any search facility.
- This protocol mainly allows one protocol to be created on the server.
- As this protocol supports offline access to the messages and so less internet usage time is required by this.



POP3 Commands

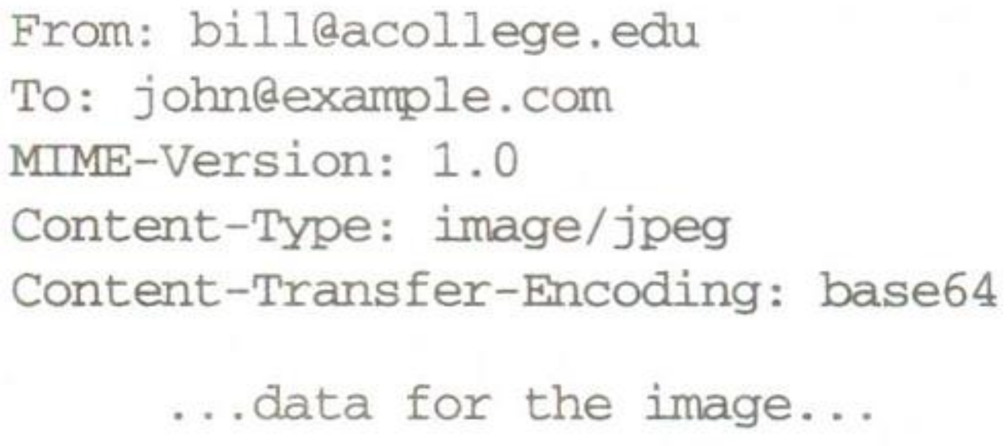
- **USER** name: User name for authentication
- **PASS** password: Password used for authentication
- **STAT:** Get number and total size of message
- **LIST:** [msg] get size of message
- **RETR:** msg Send message to client
- **DELE:** msg Delete message from mailbox
- **RSET:** Cancel previous delete requests.
- **QUIT:** Updates mailbox (deletes messages) and quits.

**7. Debate on IMAP.**

- Internet Message Access Protocol (lMAP4) is an alternative to POP3 that allows users to view and manipulate messages; a secure version of IMAP has been defined, and is known as IMAPS.
- Like POP3, IMAP4 defines an abstraction known as a mailbox; mailboxes are located on the same computer as a server. Also like POP3, a user runs an IMAP4 client that contacts the server to manipulate messages.
- IMAP4 allows a user to access mail messages from multiple locations (e.g., from work and from home), and ensures that all copies are synchronized and consistent.
- IMAP4 also provides extended functionality for message retrieval and processing. A user can obtain information about a message or examine header fields without retrieving the entire message.
- In addition, a user can search for a specified string and retrieve portions of a message. Partial retrieval is especially useful for slow-speed dialup connections because it means a user does not need to download useless information.
- User can Create, delete, rename mailboxes on the mail server. User can also create hierarchical of mailbox in a folder for email storage.

8. Design a model of MIME message with the help of a diagram.

MIME stands for Multipurpose Internet Mail Extensions. The MIME protocol allows the users to exchange various types of digital content such as pictures, audio, video, and various types of documents and files in the e-mail.



```
From: bill@acollege.edu
To: john@example.com
MIME-Version: 1.0
Content-Type: image/jpeg
Content-Transfer-Encoding: base64

        ...data for the image...
```

MIME adds five additional fields to the header portion of the actual e-mail to extend the properties of the simple email protocol. These fields are as follows:

- **MIME Version**
  It defines the version of the MIME protocol. This header usually has a parameter value 1.0, indicating that the message is formatted using MIME.
- **Content Type**
  It describes the type and subtype of information to be sent in the message. These messages can be of many types such as Text, Image, Audio, Video, and they also have many subtypes such that the subtype of the image can be png or jpeg. Similarly, the subtype of Video can be WEBM, MP4 etc.
- **Content Type Encoding**
  In this field, it is told which method has been used to convert mail information into ASCII or Binary number, such as 7-bit encoding, 8-bit encoding, etc.
- **Content Id**
  In this field, a unique "Content Id" number is appended to all email messages so that they can be uniquely identified.
- **Content description**
  This field contains a brief description of the content within the email. This means that information about whatever is being sent in the mail is clearly in the "Content Description". This field also provides the information of name, creation date, and modification date of the file.

**9. Debate on the need of IPv6.**

The primary function of IPv6 is to allow for more unique TCP/IP address identifiers to be created, now that we’ve run out of the 4.3 billion created with IPv4. This is one of the main reasons why IPv6 is such an important innovation for the Internet of Things (IoT). Internet-connected products are becoming increasingly popular, and while IPv4 addresses couldn’t meet the demand for IoT products, IPv6 gives IoT products a platform to operate on for a very long time.

- New Computer And Communication Technologies. Computer and network hardware continues to evolve. As new technologies emerge, they are incorporated into the Internet.
- New Applications. As programmers invent new ways to use , additional protocol support is needed. For example, the emphasis on IP telephony has led to investigations of protocols for real-time data delivery.
- Increases In Size And Load. The global Internet has experienced many years of sustained exponential growth, doubling in size every nine months or faster. In 1999, on the average, a new host appeared on the Internet every two seconds.Traffic has also increased rapidly as animated graphics and video proliferate.

10. **Debate on the features of IPv6**.

The proposed IPv6 protocol retains many of the features that contributed to the success of IPv4. In fact, the designers have characterized IPv6 as being basically the same as IPv4 with a few modifications. For example, IPv6 still supports connectionless allows the sender to choose the size of a datagram, and requires the sender to specify the maximum number of hops a datagram can make before being terminated. As we will see, IPv6 also retains most of the concepts provided by IPv4 options, including facilities for fragmentation and source routing. Despite many conceptual similarities, IPv6 changes most of the protocol details.

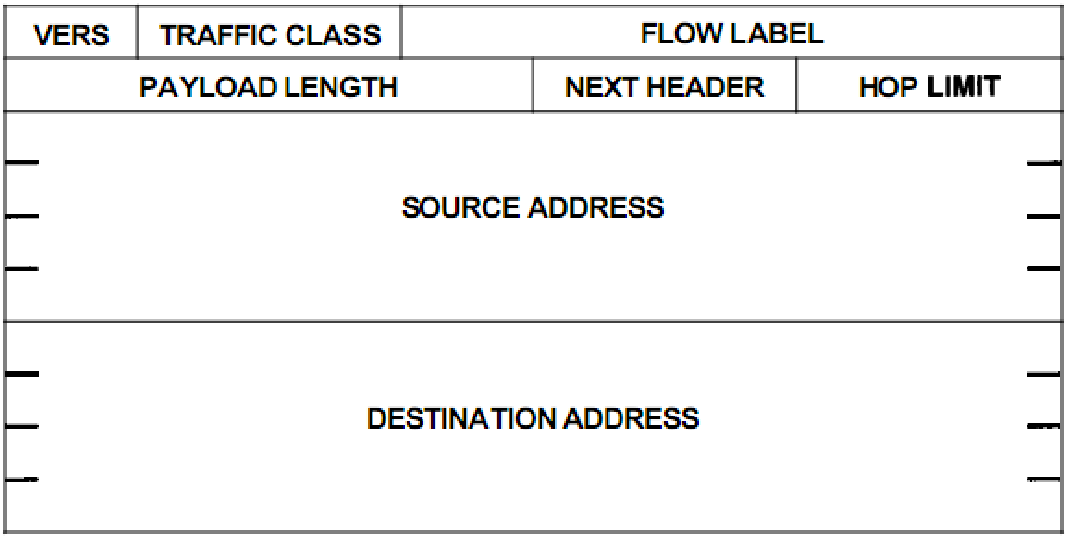
Detailed features of IPV6 over ipv4 are:

- Extended Address Hierarchy.
- Flexible Header Format.
- Improved Options.
- Provision For Protocol Extension
- Support For Auto Configuration and Renumbering
- Support For Resource Allocation.

11. **Find the list of seven different categories of changes introduced in IPV6.**

- Larger Addresses. The new address size is the most noticeable change. IPv6 quadruples the size of an IPv4 address from 32 bits to 128 bits. The IPv6 address space is so large that it cannot be exhausted in the foreseeable future.
- Extended Address Hierarchy. IPv6 uses the larger address space to create additional levels of addressing hierarchy. In particular, Pv6 can define a hierarchy of ISPs as well as a hierarchical structure within a given site.
- Flexible Header Format. IPv6 uses an entirely new and incompatible datagram format. Unlike the IPv4 fixed-format header, IPv6 defines a set of optional headers.
- Improved Options. Like IPv4, IPv6 allows a datagram to include optional control information. IPv6 includes new options that provide additional facilities not available in IPv4.
- Provision For Protocol Extension. Perhaps the most significant change in IPv6 is a move away from a protocol that fully specifies all details to a protocol that can permit additional features. The extension capability has the potential to allow the IETF to adapt the protocol to changes in underlying network hardware or to new applications.
- Support For Auto Configuration and Renumbering. IPv6 provides facilities that allow computers on an isolated network to assign themselves addresses and begin communicating without depending on a router or manual configuration. The protocol also includes a facility that permits a manager to renumber networks dynamically.
- Support For Resource Allocation. IPv6 has two facilities that permit reallocation of network resources: a flow abstraction and a differentiated service specification. The latter will use the same approach as IPv4's differentiated services.

12. **Find the format of the IPV6 datagram with the help of a diagram and explain the same.**



**Version (4-bits):** Indicates version of Internet Protocol which contains bit sequence 0110.
**Traffic Class (8-bits):** The Traffic Class field indicates class or priority of IPv6 packet which is similar to *Service Field* in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded. As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.
**Flow Label (20-bits):** Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time.
**Payload Length (16-bits):** It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers(if any) and an upper-layer packet.
**Next Header (8-bits):** Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper-layer packets, such as TCP, UDP.
**Hop Limit (8-bits):** Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.
**Source Address (128-bits):** Source Address is the 128-bit IPv6 address of the original source of the packet.
**Destination Address (128-bits):** The destination Address field indicates the IPv6 address of the final destination(in most cases). All the intermediate nodes can use this information in order to correctly route the packet.