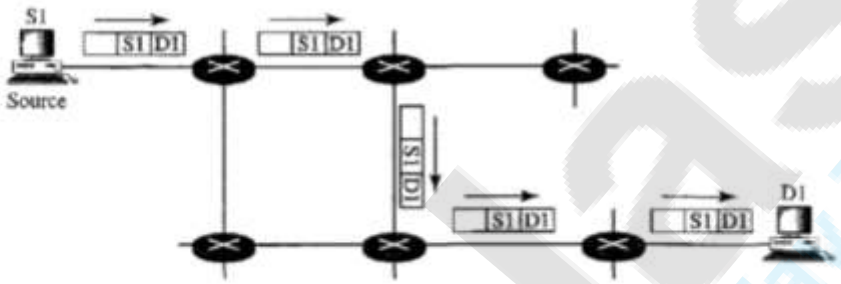
Unit-6

1) Explain Unicast Routing? Explain Protocol in Unicast routing? (RIP, OSPF, BGP)
Answer: -

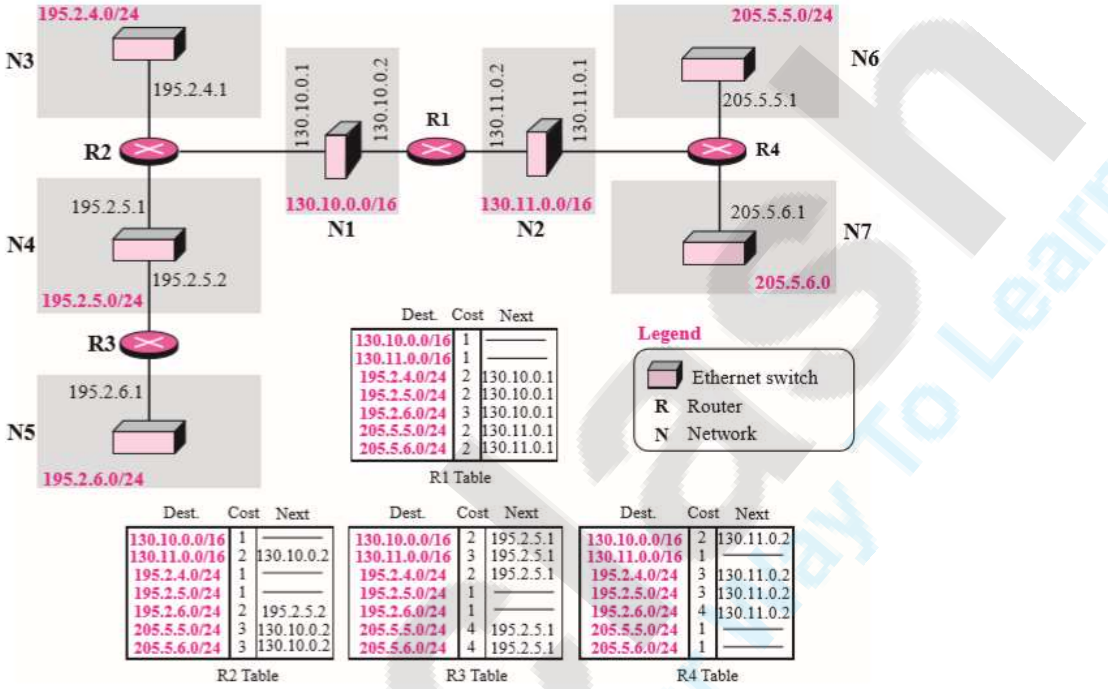
1) In unicast communication, there is one source and one destination. The relationship between the source and the destination is one-to-one. In this type of communication, both the source and destination addresses, in the IP datagram, are the unicast addresses assigned to the hosts (or host interfaces, to be more exact).

Figure 22.33 *Unicasting*



2) In Figure 22.33, a unicast packet staI1s from the source S1 and passes through routers to reach the destination D1. We have shown the networks as a link between the routers to simplify the figure. Note that in unicasting, when a router receives a packet, it forwards the packet through only one of its interfaces (the one belonging to the optimum path) as defined in the routing table. The router may discard the packet if it cannot find the destination address in its routing table.
3) **Routing Information Protocol (RIP)** is an intra domain (interior) routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing. RIP implements distance vector routing directly with some considerations:
   a) In an autonomous system, we are dealing with routers and networks (links), what was described as a node.
   b) The destination in a routing table is a network, which means the first column defines a network address.
   c) The metric used by RIP is very simple; the distance is defined as the number of links (networks) that have to be used to reach the destination. For this reason, the metric in RIP is called a hop count.
   d) Infinity is defined as 16, which means that any route in an autonomous system using RIP cannot have more than 15 hops.
   e) The next node column defines the address of the router to which the packet is to be sent to reach its destination.

Figure 11.10 *Example of a domain using RIP*



Dest.	Cost	Next
130.10.0.0/16	1	——
130.11.0.0/16	1	——
195.2.4.0/24	2	130.10.0.1
195.2.5.0/24	2	130.10.0.1
195.2.6.0/24	3	130.10.0.1
205.5.5.0/24	2	130.11.0.1
205.5.6.0/24	2	130.11.0.1

R1 Table

Dest.	Cost	Next
130.10.0.0/16	1	——
130.11.0.0/16	2	130.10.0.2
195.2.4.0/24	1	——
195.2.5.0/24	1	——
195.2.6.0/24	2	195.2.5.2
205.5.5.0/24	3	130.10.0.2
205.5.6.0/24	3	130.10.0.2

R2 Table

Dest.	Cost	Next
130.10.0.0/16	2	195.2.5.1
130.11.0.0/16	3	195.2.5.1
195.2.4.0/24	2	195.2.5.1
195.2.5.0/24	1	——
195.2.6.0/24	1	——
205.5.5.0/24	4	195.2.5.1
205.5.6.0/24	4	195.2.5.1

R3 Table

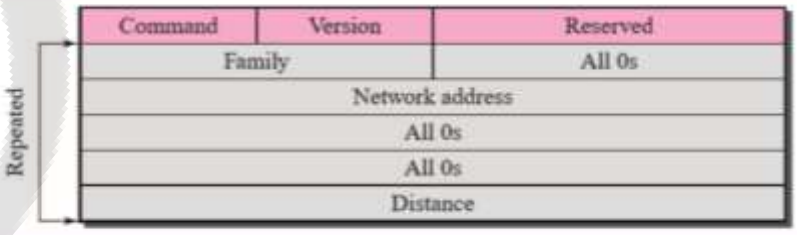
Dest.	Cost	Next
130.10.0.0/16	2	130.11.0.2
130.11.0.0/16	1	——
195.2.4.0/24	3	130.11.0.2
195.2.5.0/24	3	130.11.0.2
195.2.6.0/24	4	130.11.0.2
205.5.5.0/24	1	——
205.5.6.0/24	1	——

R4 Table

4) Figure 11.10 shows an autonomous system with seven networks and four routers. The table of each router is also shown. Let us look at the routing table for R1. The table has seven entries to show how to reach each network in the autonomous system. Router R1 is directly connected to networks 130.10.0.0 and 130.11.0.0, which means that there are no next hop entries for these two networks. To send a packet to one of the three networks at the far left, router R1 needs to deliver the packet to R2. The next node entry for these three networks is the interface of router R2 with IP address 130.10.0.1. To send a packet to the two networks at the far right, router R1 needs to send the packet to the interface of router R4 with IP address 130.11.0.1. The other tables can be explained similarly

5) **RIP Message Format**

Figure 11.11 *RIP message format*

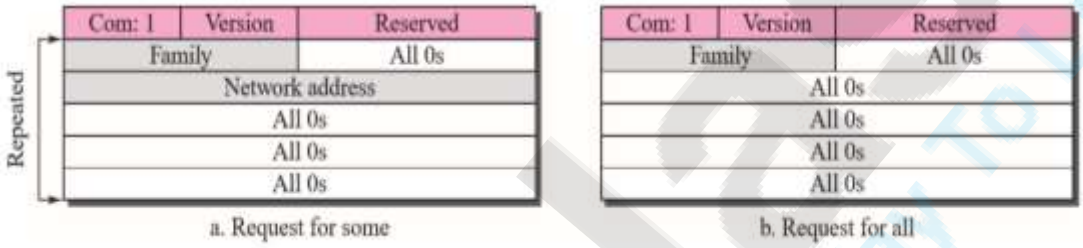


a) Command. This 8-bit field specifies the type of message: request (1) or response
b) Version. This 8-bit field defines the version. In this book we use version 1, but at the end of this section, we give some new features of version 2.

c) Family. This 16-bit field defines the family of the protocol used. For TCP/IP the value is 2.
d) Network address. The address field defines the address of the destination network. RIP has allocated 14 bytes for this field to be applicable to any protocol. However, IP currently uses only 4 bytes. The rest of the address is filled with 0s.
e) Distance. This 32-bit field defines the hop count (cost) from the advertising router to the destination network.

6) Requests and Responses

Figure 11.12 *Request messages*



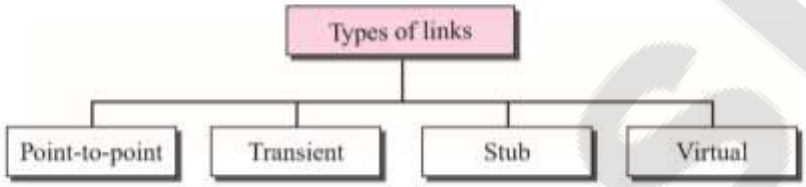
A) RIP has two types of messages: request and response.
B) Request A request message is sent by a router that has just come up or by a router that has some time-out entries. A request can ask about specific entries or all entries.
C) A response can be either solicited or unsolicited. A solicited response is sent only in answer to a request. It contains information about the destination specified in the corresponding request. An unsolicited response, on the other hand, is sent periodically, every 30 seconds or when there is a change in the routing table. The response is sometimes called an update packet.

7) OSPF

A) The Open Shortest Path First or OSPF protocol is an intra domain routing protocol based on link state routing. Its domain is also an autonomous system.
B) Areas To handle routing efficiently and in a timely manner, OSPF divides an autonomous system into areas.
C) An area is a collection of networks, hosts, and routers all contained within an autonomous system. An autonomous system can be divided into many different areas. All networks inside an area must be connected. Routers inside an area flood the area with routing information.
D) At the border of an area, special routers called area border routers summarize the information about the area and send it to other areas. Among the areas inside an autonomous system is a special area called the backbone; all the areas inside an autonomous system must be connected to the backbone. In other words, the backbone serves as a primary area and the other areas as secondary areas. This does not mean that the routers within areas cannot be connected to each other, however.
E) The routers inside the backbone are called the backbone routers. Note that a backbone router can also be an area border router. If, because of some problem, the connectivity between a backbone and an area is broken, a virtual link between

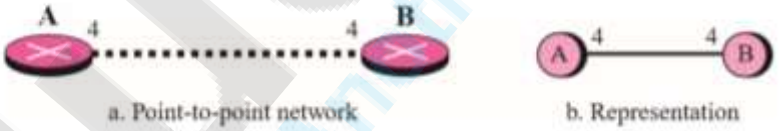
routers must be created by an administrator to allow continuity of the functions of the backbone as the primary area. Each area has area identification. The area identification of the backbone is zero. Figure 22.24 shows an autonomous system and its areas.

F) **Types of Links in OSPF** terminology, a connection is called a link. Four types of links have been defined: point-to-point, transient, stub, and virtual.



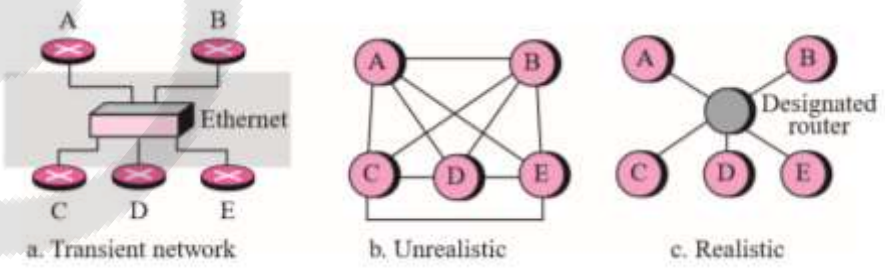
G) **Point-to-Point Link** A point-to-point link connects two routers without any other host or router in between. In other words, the purpose of the link (network) is just to connect the two routers. An example of this type of link is two routers connected by a telephone line or a T-line. There is no need to assign a network address to this type of link. Graphically, the routers are represented by nodes, and the link is represented by a bidirectional edge connecting the nodes. The metrics, which are usually the same, are shown at the two ends, one for each direction. In other words, each router has only one neighbour at the other side of the link

Figure 11.23 *Point-to-point link*



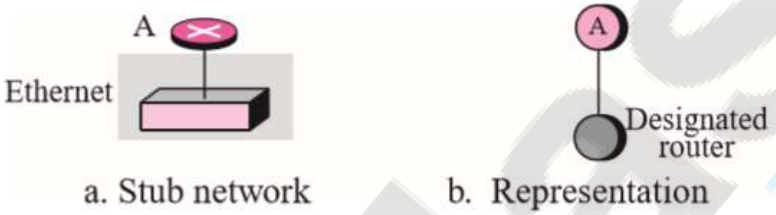
H) **Transient Link** A transient link is a network with several routers attached to it. The data can enter through any of the routers and leave through any router. All LANs and some WANs with two or more routers are of this type. In this case, each router has many neighbours. For example, consider the Ethernet in Figure 11.24a. Router A has routers B, C, D, and E as neighbours. Router B has routers A, C, D, and E as neighbours. If we want to show the neighbourhood relationship in this situation, we have the graph shown in Figure 11.24b

Transient link



I) **Stub Link** A stub link is a network that is connected to only one router. The data packets enter the network through this single router and leave the network through this same router. This is a special case of the transient network. We can show this situation using the router as a node and using the designated router for the network. However, the link is only one directional, from the router to the network (see Figure 11.25).

Stub link

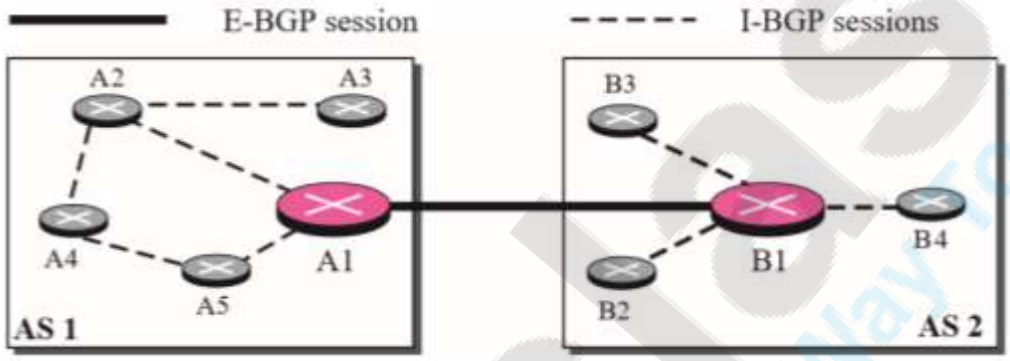


J) **Virtual Link** When the link between two routers is broken, the administration may create a virtual link between them using a longer path that probably goes through several routers.

8) **Border Gateway Protocol (BGP)** is an inter domain routing protocol using path vector routing. It first appeared in 1989 and has gone through four versions.
9) **Types of Autonomous Systems** As we said before, the Internet is divided into hierarchical domains called autonomous systems. For example, a large corporation that manages its own network and has full control over it is an autonomous system. A local ISP that provides services to local customers is an autonomous system. We can divide autonomous systems into three categories: stub, multi homed, and transit. o
10) **Stub AS**. A stub AS has only one connection to another AS. The inter domain data traffic in a stub AS can be either created or terminated in the AS. The hosts in the AS can send data traffic to other ASs. The hosts in the AS can receive data coming from hosts in other ASs. Data traffic, however, cannot pass through a stub AS. A stub AS is either a source or a sink. A good example of a stub AS is a small corporation or a small local ISP.
11) **Multi-homed AS.** A multi homed AS has more than one connection to other ASs, but it is still only a source or sink for data traffic. It can receive data traffic from more than one AS. It can send data traffic to more than one AS, but there is no transient traffic. It does not allow data coming from one AS and going to another AS to pass through. A good example of a multi homed AS is a large corporation that is connected to more than one regional or national AS that does not allow transient traffic.
12) **Transit AS.** A transit AS is a multi-homed AS that also allows transient traffic. Good examples of transit ASs are national and international ISPs (Internet backbones).
13) **BGP Sessions** The exchange of routing information between two routers using BGP takes place in a session. A session is a connection that is established between two BGP routers only for the sake of exchanging routing information. To create a reliable

environment, BGP uses the services of TCP. In other words, a session at the BGP level, as an application program, is a connection at the TCP level. However, there is a subtle difference between a connection in TCP made for BGP and other application programs. When a TCP connection is created for BGP, it can last for a long time, until something unusual happens. For this reason, BGP sessions are sometimes referred to as semi-permanent connections.

Internal and external BGP sessions



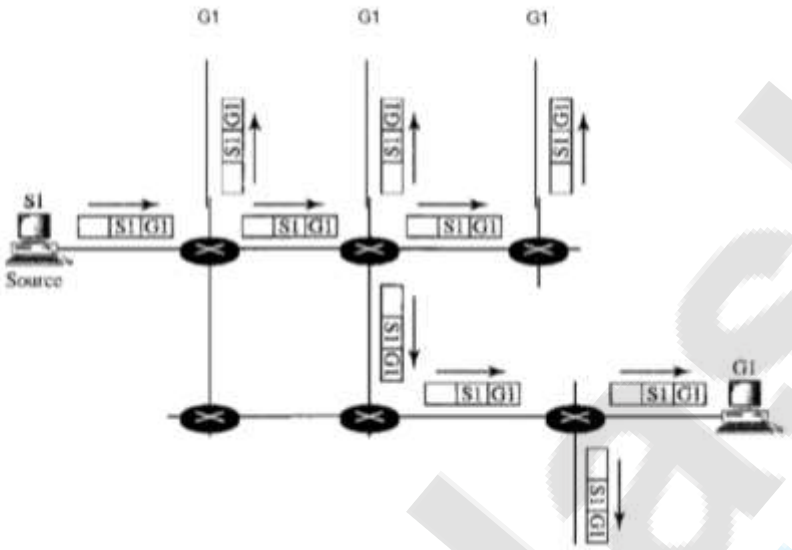
14) External and Internal BGP If we want to be precise, BGP can have two types of sessions: external BGP (E-BGP) and internal BGP (I-BGP) sessions. The E-BGP session is used to exchange information between two speaker nodes belonging to two different autonomous systems. The I-BGP session, on the other hand, is used to exchange routing information between two routers inside an autonomous system. Figure 22.32 shows the idea.

2) Explain Multicast Routing? Explain Protocol in Multicast routing? (MOSPF,DVMRP)

Answer: -

1) In multicast communication, there is one source and a group of destinations. The relationship is one-to-many. In this type of communication, the source address is a unicast address, but the destination address is a group address, which defines one or more destinations. The group address identifies the members of the group.

Figure 22.34 *Multicasting*



2) A multicast packet starts from the source S1 and goes to all destinations that belong to group G1. In multicasting, when a router receives a packet, it may forward it through several of its interfaces.
3) **Applications:** - Multicasting has many applications today such as access to distributed databases, information dissemination, teleconferencing, and distance learning.
4) **Access to Distributed Databases:** -Most of the large databases today are distributed. That is, the information is stored in more than one location, usually at the time of production. The user who needs to access the database does not know the location of the information. A user's request is multicast to all the database locations, and the location that has the information responds.
5) **Information Dissemination:** -Businesses often need to send information to their customers. If the nature of the information is the same for each customer, it can be multicast. In this way a business can send one message that can reach many customers. For example, a software update can be sent to all purchasers of a particular software package.
6) **Dissemination of News:** -In a similar manner news can be easily disseminated through multicasting. One single message can be sent to those interested in a particular topic. For example, the statistics of the championship high school basketball tournament can be sent to the sports editors of many newspapers.
7) **Teleconferencing:** -Teleconferencing involves multicasting. The individuals attending a teleconference all need to receive the same information at the same time. Temporary or permanent groups can be formed for this purpose. For example, an engineering group that holds meetings every Monday morning could have a permanent group while the group that plans the holiday party could form a temporary group.
8) **Distance Learning:** -One growing area in the use of multicasting is distance learning. Lessons taught by one single professor can be received by a specific group

of students. This is especially convenient for those students who find it difficult to attend classes on campus.

9) Multicast Link State Routing: MOSPF

A) Multicast Open Shortest Path First (MOSPF) protocol is an extension of the OSPF protocol that uses multicast link state routing to create source-based trees. The protocol requires a new link state update packet to associate the unicast address of a host with the group address or addresses the host is sponsoring.

B) This packet is called the group membership LSA. In this way, we can include in the tree only the hosts (using their unicast addresses) that belong to a particular group. In other words, we make a tree that contains all the hosts belonging to a group, but we use the unicast address of the host in the calculation.

C) For efficiency, the router calculates the shortest path trees on demand (when it receives the first multicast packet). In addition, the tree can be saved in cache memory for future use by the same source/group pair.

D) MOSPF is a data-driven protocol; the first time an MOSPF router sees a datagram with a given source and group address, the router constructs the Dijkstra shortest path tree.

10) Multicast Distance Vector: DVMRP

A) Unicast distance vector routing is very simple; extending it to support multicast routing is complicated. Multicast routing does not allow a router to send its routing table to its neighbours.

B) The idea is to create a table from scratch using the information from the unicast distance vector tables. Multicast distance vector routing uses source-based trees, but the router never actually makes a routing table.

C) When a router receives a multicast packet, it forwards the packet as though it is consulting a routing table. We can say that the shortest path tree is evanescent. After its use (after a packet is forwarded) the table is destroyed.

D) To accomplish this, the multicast distance vector algorithm uses a process based on four decision-making strategies.

E) Each strategy is built on its predecessor. We explain them one by one and see how each strategy can improve the shortcomings of the previous one.

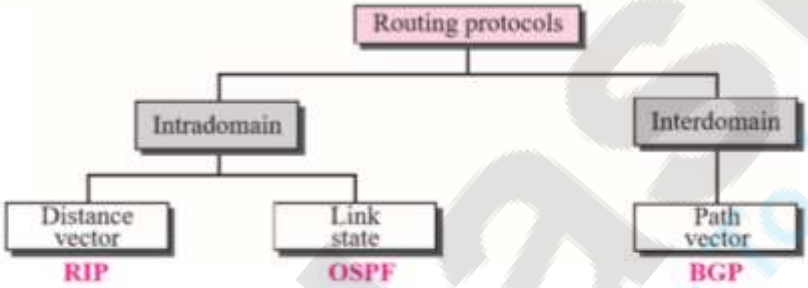
3) Explain intra and inter domain routing?

Answer: -

1) Today, an internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems. An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is referred to as intra-domain routing. Routing between autonomous systems is referred to as inter-domain routing. Each autonomous system can choose one or more intra-domain routing protocols to handle routing inside the autonomous system. However, only one inter-domain routing protocol handles routing between autonomous systems.
2) Several intra-domain and inter-domain routing protocols are in use. In this chapter, we cover only the most popular ones. We discuss two intra-domain routing protocols: distance vector and link state.

3) Routing Information Protocol (RIP) is the implementation of the distance vector protocol. Open Shortest Path First (OSPF) is the implementation of the link state protocol. Border Gateway Protocol (BGP) is the implementation of the path vector protocol. RIP and OSPF are interior routing protocols; BGP is an exterior routing protocol.

Figure 11.2 *Popular routing protocols*



4) Explain IPv4 in detail?
Note Study from Internet.

5) Explain IPv6 in detail?
Answer: -

1) In the early 1990s, the Internet Engineering Task Force began an effort to develop a successor to the IPv4 protocol. A prime motivation for this effort was the realization that the 32-bit IP address space was beginning to be used up, with new subnets and IP nodes being attached to the Internet (and being allocated unique IP addresses) at a breath-taking rate. To respond to this need for a large IP address space, a new IP protocol, IPv6, was developed. The designers of IPv6 also took this opportunity to tweak and augment other aspects of IPv4, based on the accumulated operational experience with IPv4.
2) IPv6 Datagram Format The format of the IPv6 datagram is shown in Figure 4.24. The most important changes introduced in IPv6 are evident in the datagram format:
   A) **Expanded addressing capabilities.** IPv6 increases the size of the IP address from 32 to 128 bits. This ensures that the world won't run out of IP addresses. Now, every grain of sand on the planet can be IP-addressable. In addition to unicast and multicast addresses, IPv6 has introduced a new type of address, called an anycast address, which allows a datagram to be delivered to any one of a group of hosts. (This feature could be used, for example, to send an HTTP GET to the nearest of a number of mirror sites that contain a given document.)
   B) **A streamlined 40-byte header.** As discussed below, a number of IPv4 fields have been dropped or made optional. The resulting 40-byte fixed-length header allows for faster processing of the IP datagram. Anew encoding of options allows for more flexible options processing.
   C) **Flow labelling and priority.** IPv6 has an elusive definition of a flow. RFC 1752 and RFC 2460 state that this allows "labelling of packets belonging to particular flows for which the sender requests special handling, such as a non-default quality of service or real-time service." For example, audio and video transmission might

likely be treated as a flow. On the other hand, the more traditional applications, such as file transfer and e-mail, might not be treated as flows. It is possible that the traffic carried by a high-priority user (for example, someone paying for better service for their traffic) might also be treated as a flow. What is clear, however, is that the designers of IPv6 foresee the eventual need to be able to differentiate among the flows, even if the exact meaning of a flow has not yet been determined. The IPv6 header also has an 8-bit traffic class field. This field, like the TOS field in IPv4, can be used to give priority to certain datagrams within a flow, or it can be used to give priority to datagrams from certain applications (for example, ICMP) over datagrams from other applications (for example, network news).

3) The following fields are defined in IPv6:

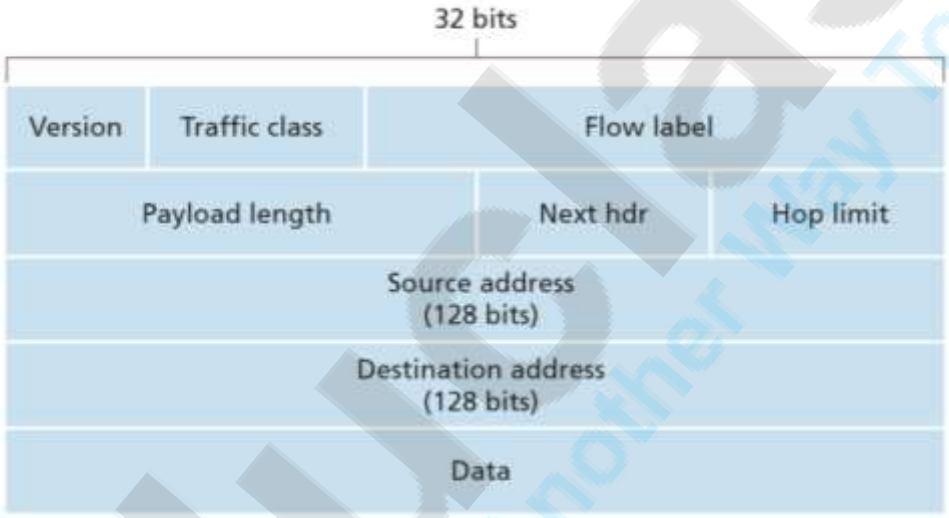


Figure 4.24 ♦ IPv6 datagram format

A) **Version.** This 4-bit field identifies the IP version number. Not surprisingly, IPv6 carries a value of 6 in this field. Note that putting a 4 in this field does not create a valid IPv4 datagram. (If it did, life would be a lot simpler—see the discussion below regarding the transition from IPv4 to IPv6.)

B) **Traffic class**. This 8-bit field is similar in spirit to the TOS field we saw in IPv4.

C) **Flow label.** As discussed above, this 20-bit field is used to identify a flow of datagrams.

D) **Payload length.** This 16-bit value is treated as an unsigned integer giving the number of bytes in the IPv6 datagram following the fixed-length, 40-byte datagram header.

E) **Next header.** This field identifies the protocol to which the contents (data field) of this datagram will be delivered (for example, to TCP or UDP). The field uses the same values as the protocol field in the IPv4 header.

F) **Hop limit**. The contents of this field are decremented by one by each router that forwards the datagram. If the hop limit count reaches zero, the datagram is discarded.

G) **Source and destination addresses.** The various formats of the IPv6 128-bit address.

H) **Data.** This is the payload portion of the IPv6 datagram. When the datagram reaches its destination, the payload will be removed from the IP datagram and passed on to the protocol specified in the next header field.

4) several fields appearing in the IPv4 datagram are no longer present in the IPv6 datagram:

A) **Fragmentation/Reassembly**. IPv6 does not allow for fragmentation and reassembly at intermediate routers; these operations can be performed only by the source and destination. If an IPv6 datagram received by a router is too large to be forwarded over the outgoing link, the router simply drops the datagram and sends a "Packet Too Big" ICMP error message (see below) back to the sender. The sender can then resend the data, using a smaller IP datagram size. Fragmentation and reassembly is a time-consuming operation; removing this functionality from the routers and placing it squarely in the end systems considerably speeds up IP forwarding within the network.

B) **Header checksum**. Because the transport-layer (for example, TCP and UDP) and link-layer (for example, Ethernet) protocols in the Internet layers perform check summing, the designers of IP probably felt that this functionality was sufficiently redundant in the network layer that it could be removed. Once again, fast processing of IP packets was a central concern. Recall from our discussion of IPv4 in Section 4.4.1 that since the IPv4 header contains a TTL field (similar to the hop limit field in IPv6), the IPv4 header checksum needed to be recomputed at every router. As with fragmentation and reassembly, this too was a costly operation in IPv4. Options. An options field is no longer a part of the standard IP header. However, it has not gone away. Instead, the options field is one of the possible next headers pointed to from within the IPv6 header. That is, just as TCP or UDP protocol headers can be the next header within an IP packet, so too can an options field. The removal of the options field results in a fixed-length, 40byte IP header.

6) Explain in brief MPLS?
OR
Explain the MPLS as a mechanism to transmit IP data over a reliable network?
Answer: -

1) The network layer of the Internet, we have focused exclusively on packets as datagrams that are forwarded by IP routers. There is also another kind of technology that is starting to be widely used, especially by ISPs, in order to move Internet traffic across their networks. This technology is called **MPLS (Multi-Protocol Label Switching)** and it is perilously close to circuit switching.
2) MPLS adds a label in front of each packet, and forwarding is based on the label rather than on the destination address. Making the label an index into an internal table makes finding the correct output line just a matter of table lookup. Using this technique, forwarding can be done very quickly. This advantage was the original

motivation behind MPLS, which began as proprietary technology known by various names including tag switching. The main benefits over time have come to be routing that is flexible and forwarding that is suited to quality of service as well as fast.

3) IP packets were not designed for virtual circuits, there is no field available for virtual-circuit numbers within the IP header. For this reason, a new MPLS header had to be added in front of the IP header. On a router-to-router line using PPP as the framing protocol, the frame format, including the PPP, MPLS, IP, and TCP headers, is as shown in Fig.

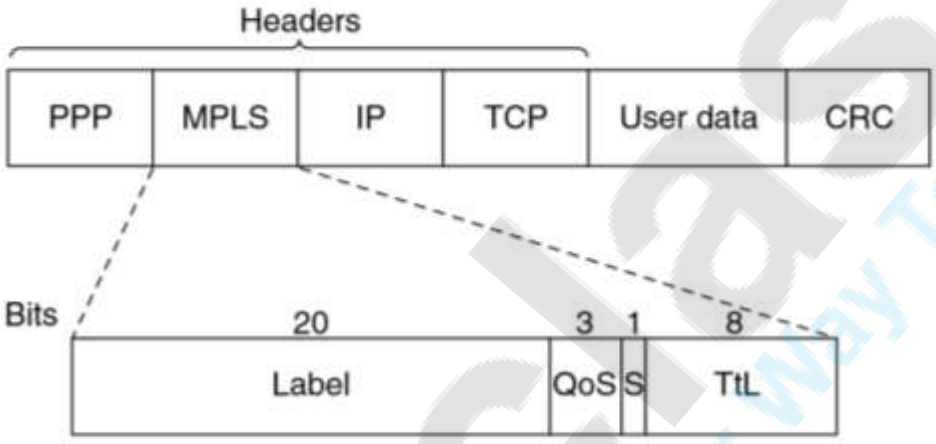


Figure 5-62. Transmitting a TCP segment using IP, MPLS, and PPP.

4) The generic MPLS header is 4 bytes long and has four fields. Most important is the Label field, which holds the index. The QoS field indicates the class of service. The S field relates to stacking multiple labels (which is discussed below). The TTL (Time To Live) field indicates how many more times the packet may be forwarded. It is decremented at each router, and if it hits 0, the packet is discarded. This feature prevents infinite looping in the case of routing instability.
5) MPLS falls between the IP network layer protocol and the PPP link layer protocol. It is not really a layer 3 protocol because it depends on IP or other network layer addresses to set up label paths. It is not really a layer 2 protocol either because it forwards packets across multiple hops, not a single link. For this reason, MPLS is sometimes described as a layer 2.5 protocol. It is an illustration that real protocols do not always fit neatly into our ideal layered protocol model.
6) The MPLS headers are not part of the network layer packet or the data link layer frame, MPLS is to a large extent independent of both layers. Among other things, this property means it is possible to build MPLS switches that can forward both IP packets and non-IP packets, depending on what shows up. This feature is where the ‘‘multiprotocol’’ in the name MPLS came from. MPLS can also carry IP packets over non-IP networks.
7) MPLS-enhanced packet arrives at a LSR (Label Switched Router), the label is used as an index into a table to determine the outgoing line to use and also the new label to use. This label swapping is used in all virtual-circuit networks. Labels have only local significance and two different routers can feed unrelated packets with the same label

into another router for transmission on the same outgoing line. To be distinguishable at the other end, labels have to be remapped at every hop. We saw this mechanism in action in Fig. 5-3. MPLS uses the same technique.

8) Forwarding is the process of finding the best match for a destination address in a table to decide where to send packets. An example is the longest matching prefix algorithm used for IP forwarding. In contrast, switching uses a label taken from the packet as an index into a forwarding table. It is simpler and faster. These definitions are far from universal, however. Since most hosts and routers do not understand MPLS, we should also ask when and how the labels are attached to packets. This happens when an IP packet reaches the edge of an MPLS network. The LER (Label Edge Router) inspects the destination IP address and other fields to see which MPLS path the packet should follow, and puts the right label on the front of the packet. Within the MPLS network, this label is used to forward the packet. At the other edge of the MPLS network, the label has served its purpose and is removed, revealing the IP packet again for the next network. This process is shown in Fig.

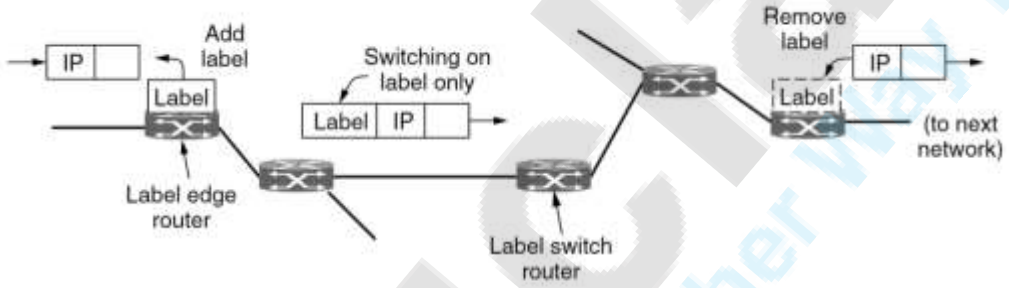


Figure 5-63. Forwarding an IP packet through an MPLS network.

7) Explain Routing Algorithm?

Answer: -

1) Distance Vector Routing Algorithm (Global Routing Algorithm)
2) Link state Routing Algorithm (Decentralized Algorithm)

8) Explain Hierarchical Routing?

Answer: -

1) The network simply as a collection of interconnected routers. One router was indistinguishable from another in the sense that all routers executed the same routing algorithm to compute routing paths through the entire network. In practice, this model and its view of a homogenous set of routers all executing the same routing algorithm is a bit simplistic for at least two important reasons:
2) **Scale.** As the number of routers becomes large, the overhead involved in computing, storing, and communicating routing information (for example, LS updates or least-cost path changes) becomes prohibitive. Today's public Internet consists of hundreds of millions of hosts. Storing routing information at each of these hosts would clearly require enormous amounts of memory. The overhead required to broadcast LS updates among all of the routers in the public Internet would leave no bandwidth left for sending data packets! A distance-vector algorithm that iterated among such a large number of routers would surely never converge. Clearly, something must be done to

reduce the complexity of route computation in networks as large as the public Internet.

3) **Administrative autonomy.** Although researchers tend to ignore issues such as a company's desire to run its routers as it pleases (for example, to run whatever routing algorithm it chooses) or to hide aspects of its network's internal organization from the outside, these are important considerations. Ideally, an organization should be able to run and administer its network as it wishes, while still being able to connect its network to other outside networks.
4) Both of these problems can be solved by organizing routers into **autonomous systems (ASs),** with each AS consisting of a group of routers that are typically under the same administrative control (e.g., operated by the same ISP or belonging to the same company network). Routers within the same AS all run the same routing algorithm (for example, an LS or DV algorithm) and have information about each other—exactly as was the case in our idealized model in the preceding section. The routing algorithm running within an autonomous system is called an intra-autonomous system routing protocol. It will be necessary, of course, to connect ASs to each other, and thus one or more of the routers in an AS will have the added task of being responsible for forwarding packets to destinations outside the AS; these routers are called gateway routers.
5) Figure 4.32 provides a simple example with three ASs: AS1, AS2, and AS3. In this figure, the heavy lines represent direct link connections between pairs of routers. The thinner lines hanging from the routers represent subnets that are directly connected to the routers. AS1 has four routers—1a, 1b, 1c, and 1d— which run the intra-AS routing protocol used within AS1. Thus, each of these four routers knows how to forward packets along the optimal path to any destination within AS1. Similarly, autonomous systems AS2 and AS3 each have three routers. Note that the intra-AS routing protocols running in AS1, AS2, and AS3 need not be the same. Also note that the routers 1b, 1c, 2a, and 3a are all gateway routers.

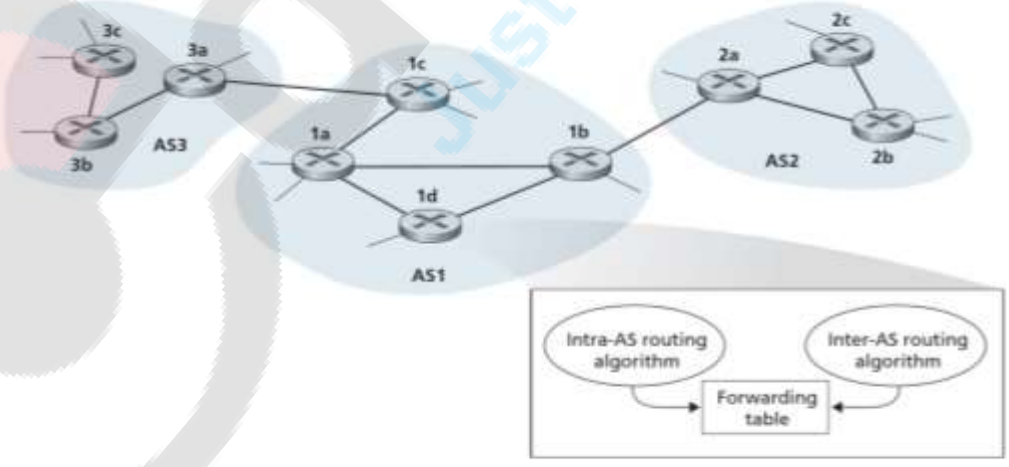


Figure 4.32 • An example of interconnected autonomous systems

9) Concept of NAT? Why NAT is required?
Answer: -

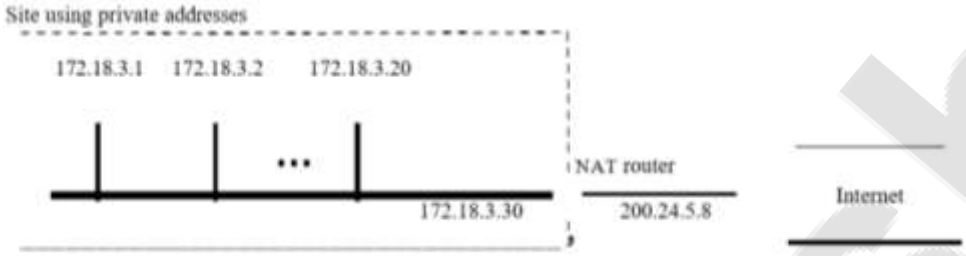
1) The number of home users and small businesses that want to use the Internet is ever increasing. In the beginning, a user was connected to the Internet with a dial-up line, which means that she was connected for a specific period of time. An ISP with a block of addresses could dynamically assign an address to this user. An address was given to a user when it was needed. But the situation is different today. Home users and small businesses can be connected by an ADSL line or cable modem. In addition, many are not happy with one address; many have created small networks with several hosts and need an IP address for each host. With the shortage of addresses, this is a serious problem.
2) A quick solution to this problem is called **network address translation (NAT).** NAT enables a user to have a large set of addresses internally and one address, or a small set of addresses, externally. The traffic inside can use the large set; the traffic outside, the small set. To separate the addresses used inside the home or business and the ones used for the Internet, the Internet authorities have reserved three sets of addresses as private addresses, shown in Table 19.3.

Table 19.3 *Addresses for private networks*

Range			*Total*
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

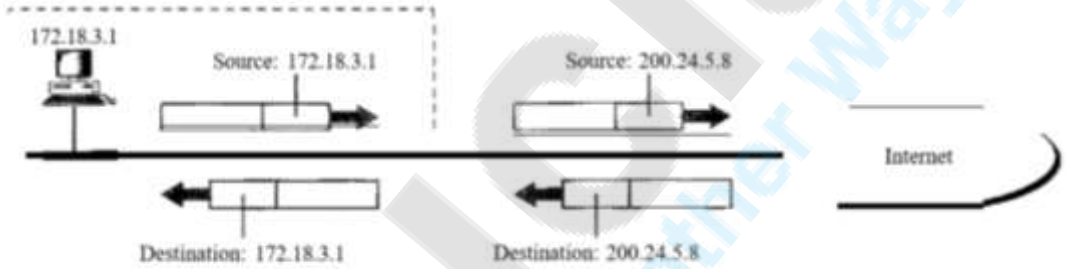
3) Any organization can use an address out of this set without permission from the Internet authorities. Everyone knows that these reserved addresses are for private networks. They are unique inside the organization, but they are not unique globally. No router will forward a packet that has one of these addresses as the destination address. The site must have only one single connection to the global Internet through a router that runs the NAT software. Figure 19.10 shows a simple implementation of NAT. As Figure 19.10 shows, the private network uses private addresses. The router that connects the network to the global address uses one private address and one global address. The private network is transparent to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8.
4) **Address Translation:** -All the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address. All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT router global address) with the appropriate private address. Figure 19.11 shows an example of address translation.

Figure 19.10 *A NAT implementation*



5) **Translation Table: -**The reader may have noticed that translating the source addresses for outgoing packets is straightforward. But how does the NAT router know the destination address for a packet coming from the Internet? There may be tens or hundreds of private IP addresses, each belonging to one specific host. The problem is solved if the NAT router has a translation table.

Figure 19.11 *Addresses in a NAT*



10) Explain Network Layer Services?

Answer: -

1) The network service model defines the characteristics of end-to-end transport of packets between sending and receiving end systems.
2) In the sending host, when the transport layer passes a packet to the network layer, specific services that could be provided by the network layer include:
3) **Guaranteed delivery.** This service guarantees that the packet will eventually arrive at its destination.
4) **Guaranteed delivery with bounded delay.** This service not only guarantees delivery of the packet, but delivery within a specified host-to-host delay bound (for example, within 100 msec).
5) Furthermore, the following services could be provided to a flow of packets between a given source and destination:
6) In-order packet delivery. This service guarantees that packets arrive at the destination in the order that they were sent.
7) **Guaranteed minimal bandwidth.** This network-layer service emulates the behaviour of a transmission link of a specified bit rate (for example, 1 Mbps) between sending and receiving hosts. As long as the sending host transmits bits (as part of

packets) at a rate below the specified bit rate, then no packet is lost and each packet arrives within a pre-specified host-to-host delay (for example, within 40 msec).

8) **Guaranteed maximum jitter.** These service guarantees that the amount of time between the trans-mission of two successive packets at the sender is equal to the amount of time between their receipt at the destination (or that this spacing changes by no more than some specified value).
9) **Security services.** Using a secret session key known only by a source and destination host, the network layer in the source host could encrypt the payloads of all datagrams being sent to the destination host. The network layer in the destination host would then be responsible for decrypting the payloads. With such a service, confidentiality would be provided to all transport-layer segments (TCP and UDP) between the source and destination hosts. In addition to confidentiality, the network layer could provide data integrity and source authentication services.

11) Explain Virtual Circuit and Datagram Networks?

Answer: -

1) In the network layer, these services are host-to-host services provided by the network layer for the transport layer. In the transport layer these services are process to-process services provided by the transport layer for the application layer.
2) In all major computer network architectures to date (Internet, ATM, frame relay, and so on), the network layer provides either a host-to-host connectionless service or a host-to-host connection service, but not both.
3) Computer networks that provide only a **connection service** at the network layer are called **virtual-circuit (VC)** networks; computer networks that provide only a **connectionless service** at the network layer are called **datagram networks**.
4) Virtual-Circuit: -
   A) While the Internet is a datagram network, many alternative network architectures including those of ATM and frame relay—are virtual-circuit networks and, therefore, use connections at the network layer. These network-layer connections are called virtual circuits (VCs).
   B) AVC consists of (1) a path (that is, a series of links and routers) between the source and destination hosts, (2) VC numbers, one number for each link along the path, and (3) entries in the forwarding table in each router along the path. A packet belonging to a virtual circuit will carry a VC number in its header. Because a virtual circuit may have a different VC number on each link, each intervening router must replace the VC number of each traversing packet with a new VC number. The new VC number is obtained from the forwarding table.

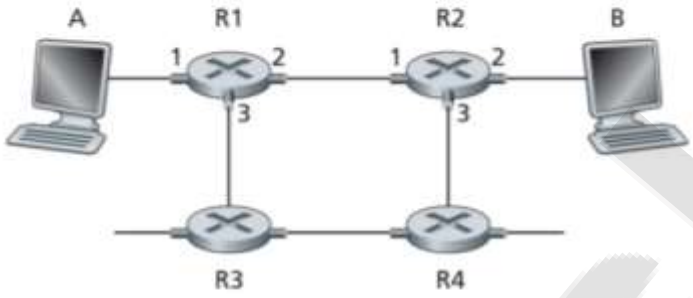


Figure 4.3 ♦ A simple virtual circuit network

C) To illustrate the concept, consider the network shown in Figure 4.3. The numbers next to the links of R1 in Figure 4.3 are the link interface numbers. Suppose now that Host A requests that the network establish a VC between itself and Host B. Suppose also that the network chooses the path A-R1-R2-B and assigns VC numbers 12, 22, and 32 to the three links in this path for this virtual circuit. In this case, when a packet in this VC leaves Host A, the value in the VC number field in the packet header is 12; when it leaves R1, the value is 22; and when it leaves R2, the value is 32.

D) In a VC network, the network's routers must maintain connection state information for the ongoing connections. Specifically, each time a new connection is established across a router, a new connection entry must be added to the router's forwarding table; and each time a connection is released, an entry must be removed from the table. Note that even if there is no VC-number translation, it is still necessary to maintain connection state information that associates VC numbers with output interface numbers.

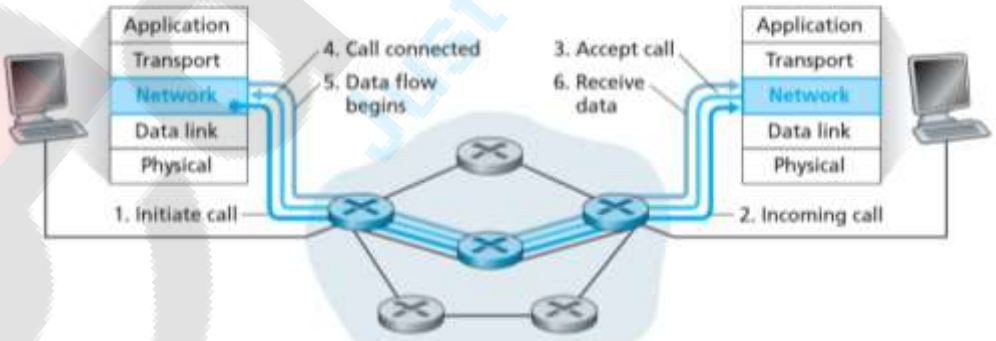


Figure 4.4 ♦ Virtual-circuit setup

E) There are three identifiable phases in a virtual circuit:

F) **VC setup.** During the setup phase, the sending transport layer contacts the network layer, specifies the receiver's address, and waits for the network to set up the VC. The network layer determines the path between sender and receiver, that

is, the series of links and routers through which all packets of the VC will travel. The network layer also determines the VC number for each link along the path. Finally, the network layer adds an entry in the forwarding table in each router along the path. During VC setup, the network layer may also reserve resources (for example, bandwidth) along the path of the VC.

G) **Data transfer.** As shown in Figure 4.4, once the VC has been established, packets can begin to flow along the VC.

H) **VC teardown.** This is initiated when the sender (or receiver) informs the network layer of its desire to terminate the VC. The network layer will then typically inform the end system on the other side of the network of the call termination and update the forwarding tables in each of the packet routers on the path to indicate that the VC no longer exists.

5) **Datagram Networks: -**

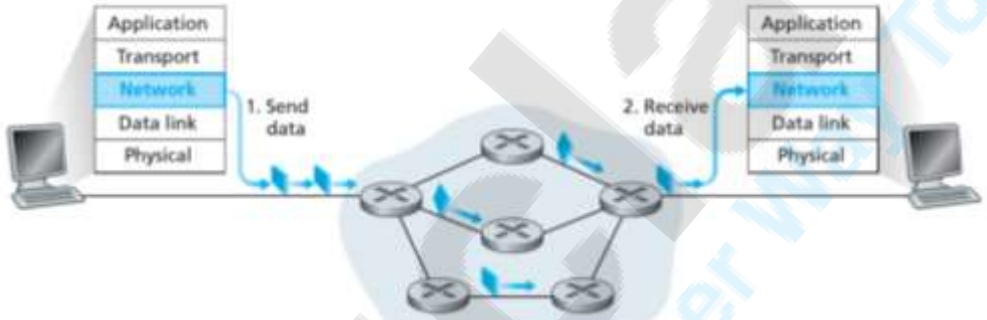


Figure 4.5 ♦ Datagram network

A) In a datagram network, each time an end system wants to send a packet, it stamps the packet with the address of the destination end system and then pops the packet into the network.

B) As shown in Figure 4.5, there is no VC setup and routers do not maintain any VC state information (because there are no VCs!). As a packet is transmitted from source to destination, it passes through a series of routers.

C) Each of these routers uses the packet's destination address to forward the packet. Specifically, each router has a forwarding table that maps destination addresses to link interfaces; when a packet arrives at the router, the router uses the packet's destination address to look up the appropriate output link interface in the forwarding table.

D) The router then intentionally forwards the packet to that output link interface. To get some further insight into the lookup operation, let's look at a specific example. Suppose that all destination addresses are 32 bits (which just happens to be the length of the destination address in an IP datagram).

E) A brute-force implementation of the forwarding table would have one entry for every possible destination address. Since there are more than 4 billion possible addresses, this option is totally out of the question.

12) Difference between Unicast and Multicast?

Answer: -

BASIS FOR COMPARISON	UNICAST	MULTICAST
Basic	One sender and one receiver.	One sender and multiple receivers.
Bandwidth	Multiple unicasting utilizes more bandwidth as compared to multicast.	Multicasting utilizes bandwidth efficiently.
Scale	It does not scale well for streaming media.	It does not scale well across large networks.
Mapping	One-to-one.	One-to-many.
Examples	Web surfing, file transfer.	Multimedia delivery, stock exchange.