Contents

Unit 7
The Network Layer

Structure of the Unit

7.1 Unit Outcomes

After the successful completion of this unit, the student will be able to:

- Describe the host-to-host communication service.
- Differentiate connectionless and connection-oriented services
- Describe the two techniques of forwarding the IP packets
- Compare Virtual Circuit and Datagram Networks
- Comprehend the address fields in an IP address

7.2 Network Layer -Introduction

In the OSI Reference Model, the Network layer is the third layer from below or the layer below the transport layer. It is also referred to as the Internet Layer in the TCP/IP model. This layer provides various services but the primary function is to transfer data from source to destination across multiple networks or is responsible for end-to-end delivery.

Fig. 7.1 shows the same scenario discussed in Section 3.2 with appropriate changes showing the communication at the network layer. The Internet is made up of many LANs and WANs connected using various connecting devices like switches, and routers.

The figure shows that the network link layer is involved at the source host, routers R2, R4, R5, R7, and

the destination host. The source and destination hosts use all five layers but the routers use only three layers for routing the packets. At Jay's computer, the network layer accepts the segments from the transport layer, encapsulates them in a packet (datagram), and delivers it to the data link layer which frames it and sends it through the physical layer to the nearby router R2. At Ram's computer, the packet is decapsulated and delivered to the corresponding transport layer. So the routers forward the packets from the input links to the appropriate output links.

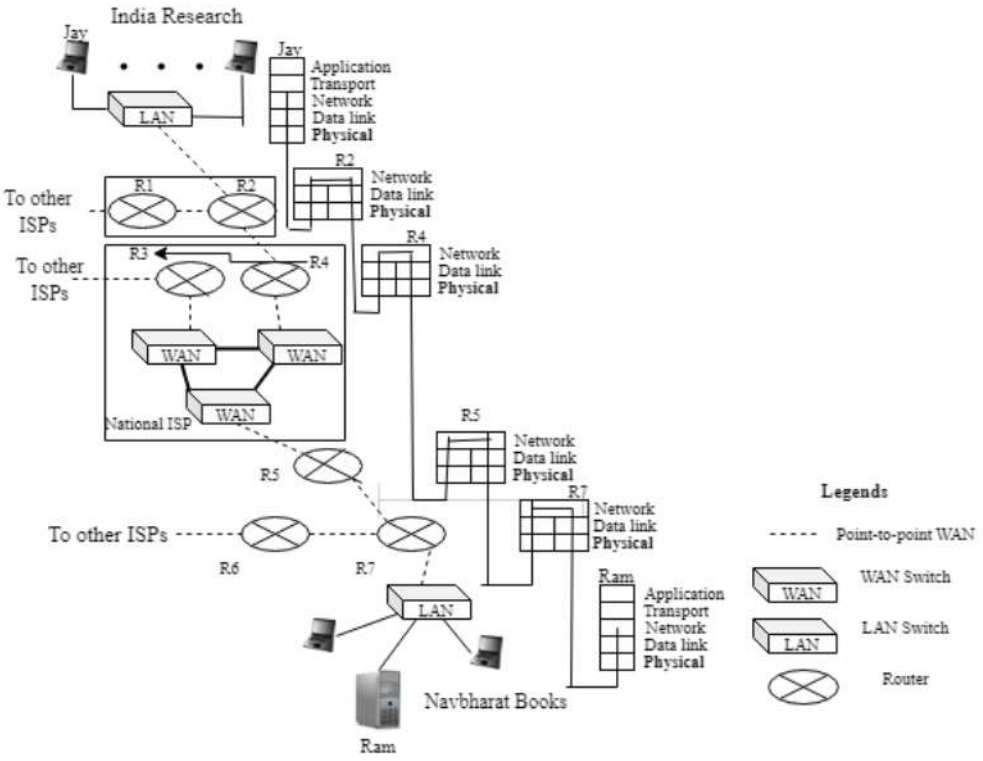


Fig. 7.1 Communication at the Network Layer

As we see in Fig. 7.1, the application layer and the transport layer are not a part of the routers but the network layer is a part of all the devices. So the design of this layer is the most challenging and the most complex in the protocol stack.

The below topics are discussed in the following sections:

- Four design issues at the Network layer
- Services provided by the Network Layer
- Approaches for structuring packet delivery
- Role of addressing in packet delivery to the destination
- Difference between forwarding and routing functions of the network layer

7.3 Network Layer Design Issues

To provide the important services that are discussed in the next section, the Network Layer has to be designed considering the following four issues:

1. Store and Forward packet switching

2. Services to be provided to the transport layer
3. Connectionless service implementation
4. Connection-oriented service implementation

7.3.1 Store and Forward packet switching

The network layer data unit is called a packet. A packet travels through many networks and links during its transmission from the source to its destination. The size of the packet that can be encapsulated within a frame by the link layer may depend on the restrictions placed by the physical layer below it. So a large-sized packet on one link may be fragmented into smaller-sized packets at some routers and transmitted on a link that can transmit a smaller-sized frame. The packet fragments will be reassembled later by some other router. At these routers, the packet fragments are stored until all the fragments are received and then the complete packet is forwarded to the next hop.

7.3.2 Services to be provided to the transport layer

The network layer provides types of services to the transport layer in the form of connected-oriented and connectionless services which have already been discussed in the previous unit. In the connected-oriented service, a connection or path is set up between the source and destination before the data transfers take place, and all the packets of a message are routed through that path.

Whereas, in the connectionless service, every packet in the message is individually routed on a different path from its source to destination and every packet acts as an independent entity.

While providing the above two services, three issues are to be considered: the routing technology should not affect the services, the transport layer should not be concerned with the configuration of the routers, and there should be a uniform addressing scheme available to the transport layer, irrespective of the type of network.

7.3.3 Connectionless service implementation

In this service, the network does not keep any state information in regard to the packet fragments of a particular packet stream. Also, the network does not set aside the resources required by the data traffic as it does not have any knowledge of the amount of data sent by the users. This in turn makes it difficult to achieve a specific Quality of Service (QoS) for the traffic.

7.3.4 Connection-oriented service implementation

This service is implemented through a virtual circuit subnet. This avoids choosing a new route for every packet sent by a source. During the connection setup phase, a route a chosen for all the packets in a message and they are stored in the routers inside a table. The packets are identified through a virtual circuit identifier. When the connection is released, the virtual circuit is terminated.

7.4 Services of the Network Layer

All the network layer services are provided by different protocols running at this layer. There are two important network layer services:

- Packetizing
- Routing and Forwarding

7.4.1 Packetizing

This service includes encapsulating the data (payload) in the network layer packet at the source and decapsulating the payload at the destination. This way the network layer acts like a carrier such as a postal department, which delivers packages from source to destination without using or changing the contents in it.

At the source, the payload is received from the upper-layer protocols, then a header is added which contains the source and destination address and other important information required by the network layer protocol and then delivers it to the link layer. If the payload is too large for delivery, it is fragmented.

At the destination, this layer receives the packet, decapsulates it, and delivers the payload to the corresponding upper-layer protocol. If the packet is fragmented at the source or any of the routers, then they are reassembled and delivered to the upper layer protocol.

The routers do not decapsulate the packets unless they are fragmented. Also, they do not change the source and destination address but inspect the addresses for forwarding the packets to the next network in its path.

7.4.2 Routing and Forwarding

Both these services are network layer functions and are provided at the routers only. Though both of these terms are different content-wise, they are used interchangeably.

Whereas, forwarding is a router-level local process of actually transferring the packet from an input link interface to an appropriate output link interface.

7.4.2.1 Routing

Routing is a network-level process used to find end-to-end paths that packets take from source to destination. As a result of this process, a router prepares a forwarding table by following the steps given below:

- It first extracts the routing information using different routing algorithms.
- The routing algorithms also help in calculating the paths for the packet travel.
- These paths are entered into the forwarding tables.

7.4.2.2 Forwarding

Forwarding is a router-level local process of actually transferring the packet from an input link interface to an appropriate output link interface by referring to the forwarding table.
Every router maintains a forwarding table. It has a mapping of the forwarding value (in the header of

the packet) to the output interface. So the header value indexes the router's outgoing link interface where the packet has to be forwarded.

Fig. 7.2 shows the forwarding process.

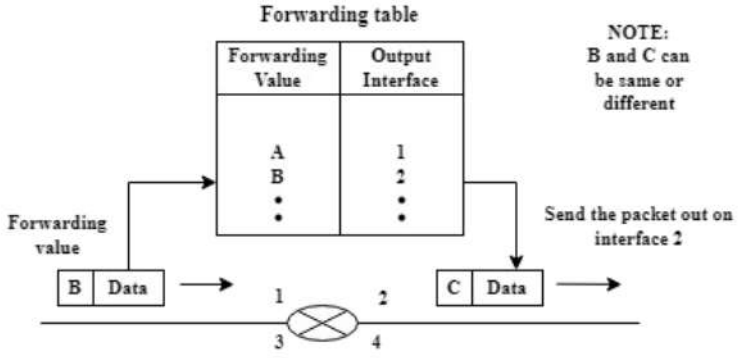


Fig. 7.2 Forwarding Process

Types of forwarding processes:

The forwarding process is performed at the routers and can be done in two ways: First, it can be based on the destination address when Internet Protocol (IP) is used as a connectionless protocol, and second, it is done based on a label attached to a packet when IP is used as a connection-oriented protocol.

1. Forwarding Based on Destination Address

A packet is sent out by a host or an incoming packet at a router is forwarded by a router by looking into a table maintained at these devices. This table is called the forwarding table. This table helps to find the next hop for a packet in its path to the destination.

In the case of classless addressing, the whole address space is considered as one entity. One row of information in the table is used for one block of address space which refers to a network address. The address on the row gives the first address in the block and this address gives no information about the destination address. To resolve this, the addresses include a mask value

For Eg: If the destination address is given as 120.23.116.30/n, then n is the mask value.

The mask value helps in extracting the network address from the destination address of the incoming packet and then forwarding it to the appropriate interface.

A forwarding table has four pieces of information: Network address with mask, Next-hop IP address, and the interface number.

Let us understand the forwarding concept with a diagram as shown in Fig. 7.3.

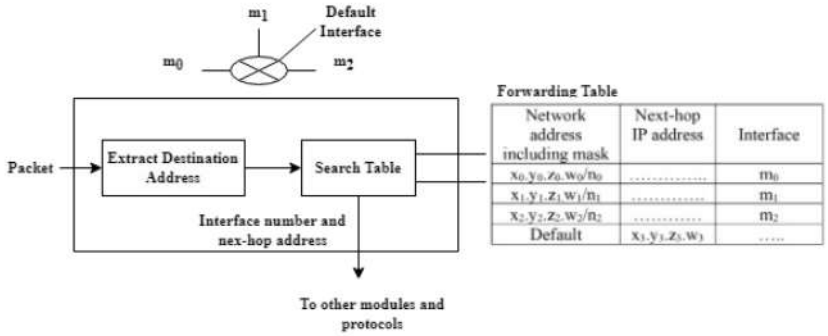


Fig.7.3: Forwarding module in classless address

The forwarding module helps in searching the table row-by-row by following the steps below:

1. The n_0 leftmost bits of the incoming packet are preserved and the remaining bits are made zero. If this value matches the network address on the first row, then the next-hop IP address and the interface values are taken out to be used in the next step.
2. The packet is then forwarded to the m_0 interface.
3. If it does not match, steps 1 and 2 are repeated for all the rows.
4. If none of the addresses match, the default values in the last row will be chosen.

Let us understand the process of forwarding with an example.

Example: For the configuration shown in Fig.7.4, detail the forwarding process for a packet with 180.70.65.130 as the destination address, arriving at the router R1.The forwarding table is given in Table.7.1

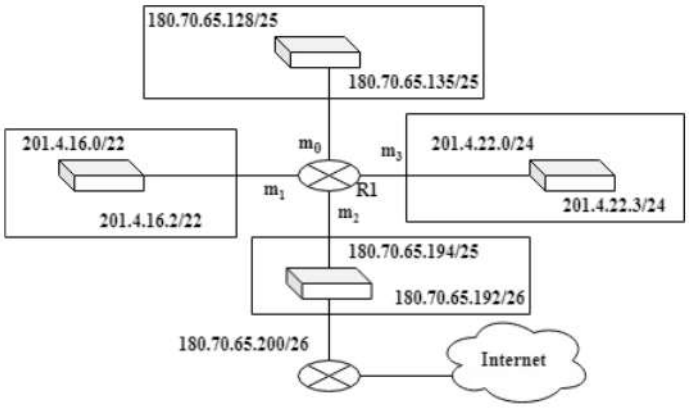


Fig. 7.4: A sample configuration for understanding forwarding process

Table:7.1: Forwarding table for router R1 for configuration in Fig.7.4

Network address/mask	Next hop	Interface
180.70.65.192/26	------	**m_2**
180.70.65.128/25	------	**m_0**
201.4.22.0/24	------	**m_3**
201.4.16.0/22	------	**m_1**
Default	**180.70.65.200**	**m_2**

Fig. 7.4 shows four subnets connected to a router R1.

The router forwards the packet after referring to the Table. 7.1 and the steps are as below:

1. The destination address given is: 180.70.65.130
   The destination address in bits = 10110100 01000110 01000001 10000010
   The first mask $n_0 = 26$ is applied to the destination address and will make bits 0 to 5 (MSBs) (32 bits – 26 bits = 6 bits) = 0's
   10110100 01000110 01000001 10000000 = 180.70.65.128
   This address does not match the first-row network address.
2. The second mask $n_1 = 25$ is applied to the destination address and will make bits 0 to 6 (MSBs) (32 bits – 25 bits = 7 bits) = 0's
   10110100 01000110 01000001 10000000 = 180.70.65.128
   This address matches with the second-row network address, so the interface m_0 the next hop address specified in this row, is chosen for forwarding the packet.

2. Forwarding Based on Label

In the connection-oriented (or Virtual-circuit) network, a packet is forwarded by a switch based on the label attached to it (to be discussed in 7.5.3.1). The label is used as an index to access the rows to search for the next label. This label is attached to the packet and forwarded. Fig.7.5 shows the forwarding process based on a label. Here, the label 0002 of the incoming packet indexes the 3rd row in the switching table and extracts 0002 as the next label. It changes the label of the packet and is sent out on Interface 2.

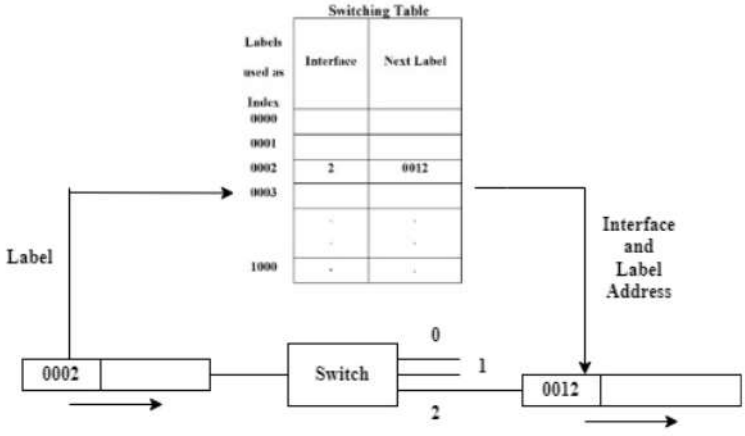


Fig.7.5: Forwarding based on label

7.4.3 Other services

The other services expected by the network layer are Error Control, Flow control, Congestion Control, Quality of service, and Security. To keep the network layer simple, these services are implemented at the upper layers. Let us briefly understand these terms which form an important part of a data communication system.

1. **Error Control:** At this layer error control is provided only for the header with the help of the checksum field. This is done because if the packet is fragmented, all the fragments have to be

checked for errors at each router which is inefficient.

Internet Control Message Protocol (ICMP) provides error control if the header has unknown information or when a packet is discarded.

2. **Flow Control:** If the source host sends data at a rate that overwhelms the receiver, then the receiver should send feedback and notify the source to reduce the data-sending rate. As the network layer functionality is very simple, the above situation rarely arises. Also, the transport layer can implement buffers to save the high data rate incoming data to use later.
3. **Congestion Control**: Congestion occurs when there are too many packets present in a part of a network that may be beyond the capacity of the routers or network. Here, the routers may drop some packets. If this situation is not controlled, no packets are delivered, and the system collapses.
4. **Quality of Services:** With multimedia applications, especially real-time communication of audio and video streaming entering the Internet, quality of services(QoS) has become a very important design issue. QoS is implemented in the upper layers.
5. **Security:** There are two types of services provided by the Internet, Connection-oriented and connectionless (to be discussed in detail in the following sections). Providing security for a connectionless system is of prime concern and this is being implemented by adding a virtual layer called IPsec (Internet Protocol Security) which converts the connectionless service to a connection-oriented service.

7.5 Virtual Circuits and Datagram Networks

Communication between two or more devices can be established in two ways: connection-oriented and connection-less. On the Internet, both transport and network layers can offer these two different types of services to the upper layers for transferring data.

In this section, we discuss connection-oriented and connection-less services as types of packet-switching methods.

7.5.1 Connection-oriented services

These services involve the establishment of the connection using a handshake method before transmission and termination of the connection after transmission. It is analogous to a telephone service. This system requires the creation of a path between a sender and a receiver and authentication from the receiver. As there is a virtual path created before transmission, all the packets follow the same path and so they are received in the same order as sent.

Fig. 7.6 shows a connection-oriented packet-switched network.

- First, a virtual path is established between the sender and the receiver via the routers R1, R3, and R4.
- The source sends two packets that follow this path and are received in the same order as they are sent.

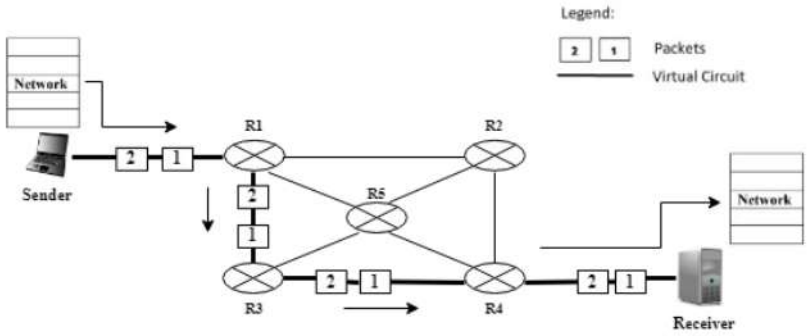


Fig. 7.6: A connection-oriented packet-switched network

The bandwidth requirement of the link is high but there is data reliability. At the transport layer, the protocol used for this service is Transmission Control Protocol (TCP).
More details are covered in 7.4.3.1 (Virtual Circuit Networks)

7.5.2 Connectionless services

These services do not require any connection creation and termination processes for transferring data. It is analogous to a postal service. This system does not require the creation of a virtual path between a sender and a receiver and authentication from the receiver. As there is no path created before transmission the packets can travel on different paths and so they are not received in the same order as sent.

Fig. 7.7 shows a connectionless packet-switched network.

- The source sends three packets that follow different paths and they may be received out of order.
- The transport layer reorders the packets.

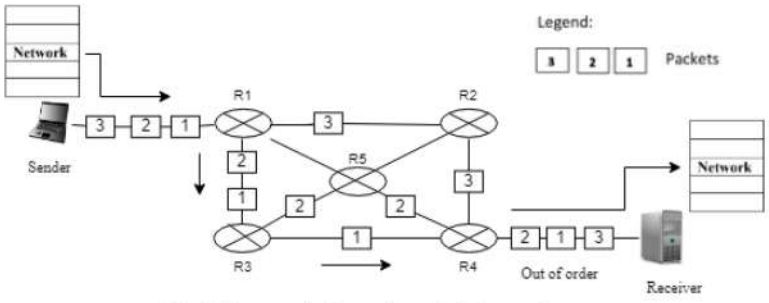


Fig. 7.7: A connectionless packet-switched network

The bandwidth requirement of the link is low, but there is no data reliability. At the transport layer, the protocol used for this service is User Datagram Protocol (UDP). More details are covered in 7.4.3.2 (Datagram Networks)

7.5.3 Implementation of Connection-oriented and connectionless services at the network layer

At the network layer, these two services are provided from host to host and are implemented on the end systems and the routers. But at the transport layer, they are process-to-process services and are implemented only at the end systems.

At the network layer, only one of these services can be provided, and never both. The networks that provide only connection-oriented service at the network layer are called virtual-circuit (VC) networks and those that provide only connectionless service are called datagram networks.

7.5.3.1 Virtual-Circuit Networks

In these networks, before the packets can be sent, a virtual connection is set up and a path is defined for the packets. All the packets contain the source and destination address and a virtual circuit identifier or a label. Each packet is forwarded from an input link to an output link at the router based on the label, as shown in Fig. 7.8

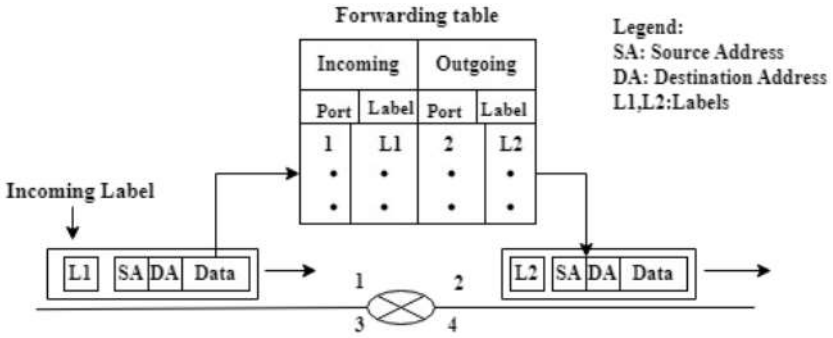


Fig. 7.8 Forwarding Process in a router when used in a virtual-circuit

This whole service is a three-phase process: setup, data transfer and tear down.

Let us understand the three phases with the help of figures 7.9, 7.10, and 7.11.

Setup Phase: In this phase, a router creates an entry for a virtual circuit by exchanging two auxiliary packets between the sender and the receiver: the request packet and the acknowledgment packet.

1. **Request packet:** This is an auxiliary packet sent from source to destination and contains the source and destination addresses. Fig.7.9 shows how a request packet is sent from A to B.
    - Router R1 obtains the information that the packet has to use port 3 for the outgoing link and creates the entry in the forwarding table.
    - The router assigns the incoming port 1, available incoming label 14, and outgoing port 3.
    - Only three columns are filled and the outgoing label is obtained during the acknowledgment step.
    - The above three steps are followed at R3, and R4.

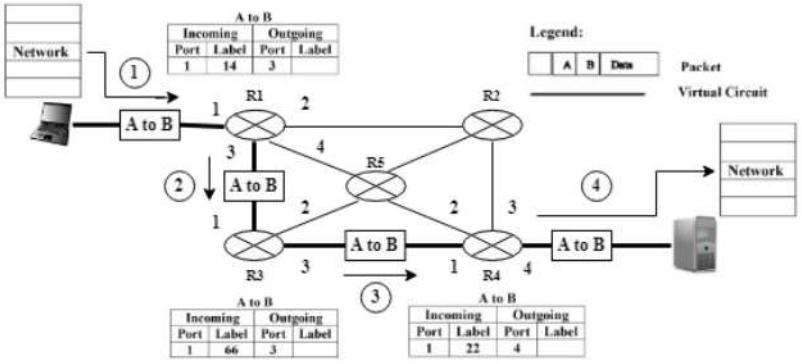


Fig. 7.9: Sending request packet in a virtual-circuit network

2. **Acknowledgement packet:** This packet is sent from B to A, and completes the entries in the forwarding (switching) tables as shown in Fig. 7.10.

- The destination host first sends an acknowledgment packet to R4, which contains the global source and destination addresses and a label 77 chosen by it, and uses this as the incoming label for packets from A. R4 completes the table entries and uses label 77 as

  an outgoing label for R4.

  - R4 sends an acknowledgment for R3 and the same procedure as followed in the above step is followed at R3 and R1.
  - The table entries at all the routers are completed.

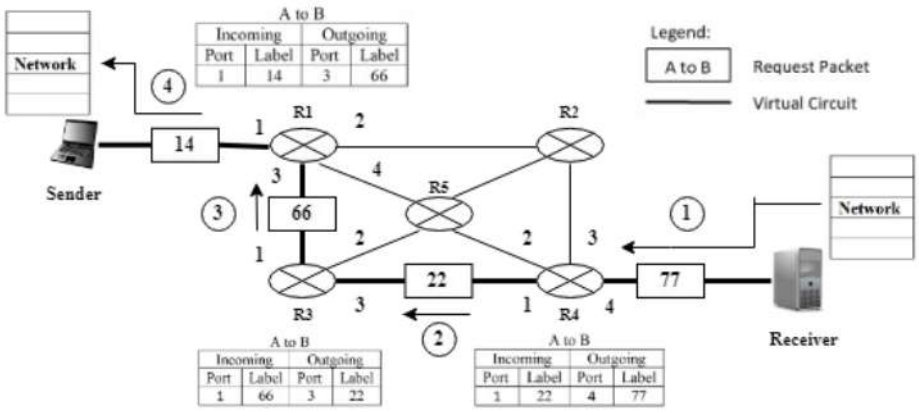


Fig. 7.10: Sending acknowledgement packet in a virtual-circuit network

Data Transfer Phase:

- After the creation of the routing table for a specific virtual circuit, the network layer packets of a single message are sent from the sender in a sequence.
- The same procedure is followed for all the packets and all the packets belonging to one message use the same sequence of labels and the packets arrive in order at the destination. Fig.7.11 shows the flow of one single packet of a message.

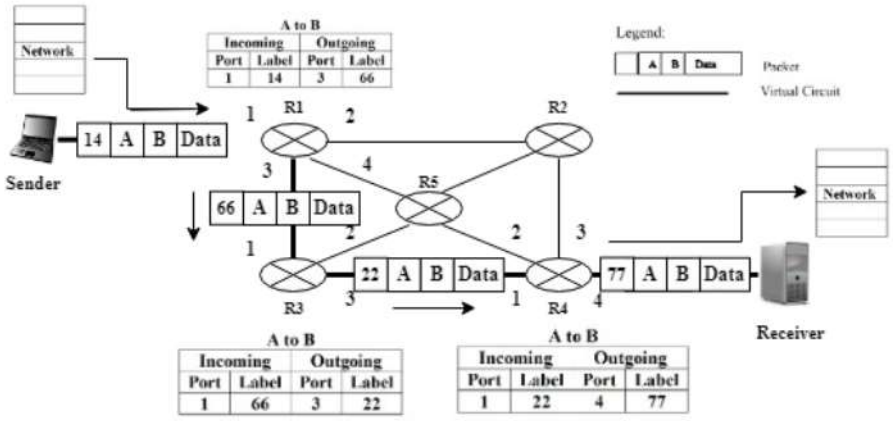


Fig. 7.11: One packet flow in a virtual-circuit network

Teardown Phase:

The source sends a special packet called a teardown packet after sending all the packets. The destination host responds by sending a confirmation packet. Then all the routers delete the entries corresponding to this VC from their tables.

7.5.3.2 Datagram Networks

In these networks, the network layer protocol treats each packet independently as if there is no relationship with other packets. The main goal of the protocol here is to deliver the packets from source to destination. Based on the information in the header: source and destination address, each packet is routed at the router. The source address can be used to send error messages in case a packet is dropped. The packet forwarding process at the router is shown in Fig. 7.12. Here based on the forwarding table, the packet destined for B will be sent on the output interface 2.

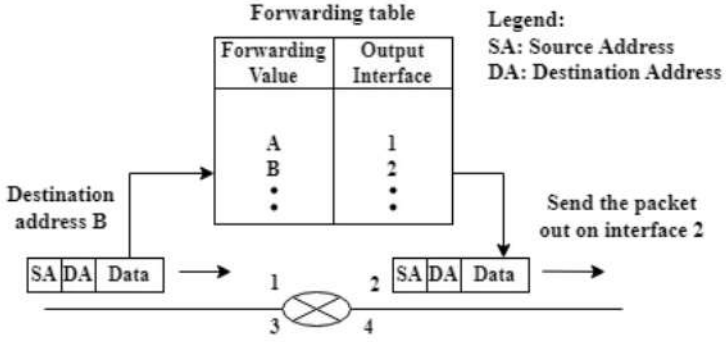


Fig. 7.12: Forwarding process in a router for a datagram network

7.6 Differences between a Virtual Circuit and Datagram Networks

Table 7.2 outlines the differences between a Virtual Circuit and Datagram Networks

Table 7.2: Differences between Virtual-Circuit and Datagram Networks

Virtual-Circuit	Datagram Networks
Used for connection-oriented service.	Used for connectionless service.
Resources along the path are reserved.	Resources along the path are not reserved.
Routing tables are static for a specific connection.	Routers are updated dynamically as packets can use any available path.
Packets arrive in the same order as sent by the source.	Packets are reordered at the destination.
A global header is added only for the first packet of a connection.	All the packets must contain a header with information about the source and the upper-layer data.
Reliable Networks	Networks not reliable
Less delay, low efficiency.	More Delay, High efficiency
Used in Asynchronous Transfer Mode (ATM) Networks	Used widely on the Internet.

7.7 The Internet Protocol (IP): Forwarding and Addressing in the Internet

The three important components of the network layer are IP Protocol, Routing protocols, and Internet Control Message Protocol (ICMP). In this section, only the IP protocol is discussed. The ICMP and routing protocols are discussed in the later sections.

Computing devices on the Internet send different types of messages to other computing devices. A message can be, a very small ping message to check if another device is connected or it can be an entire webpage. As there is a limit on the size of data that can be transmitted at a time by the physical network connections between devices, the size of the message also has a limitation. So many of the networking protocols split each message into multiple smaller **packets.**

The IP protocol is responsible for addressing and forwarding the packets on the Internet. There are two versions of this protocol: IPv4 and IPv6. The ICMP helps in handling errors in the As of packets. There are two more auxiliary protocols called Internet Group Management Protocol (IGMP) and Address Resolution Protocol (ARP). The IGMP is used to manage multicasting in IPv4 and ARP is used to map network-layer addresses to data-link-layer addresses.
The features of the IPv4 protocol are listed below:

- It is a connectionless protocol, where each packet can independently follow a route to its destination, so can arrive out of order at the destination.
- It is an unreliable protocol using a best-effort delivery service. The packets can be lost, corrupted, can be delayed, and can cause congestion in the network.

NOTE: IPv4 depends on the upper-layer protocols to solve the above problems.

7.7.1 Packet (Datagram) Format

The IP protocol also describes the structure (format) of the packet. Each IP packet contains two parts. Header and Data. The header can vary from 20 to 60 bytes in length and the data is of variable length. The header includes the IP addresses of the source and destination and other fields that help the routers route the packet.

The IPv4 packet format is shown in Fig. 7.13.

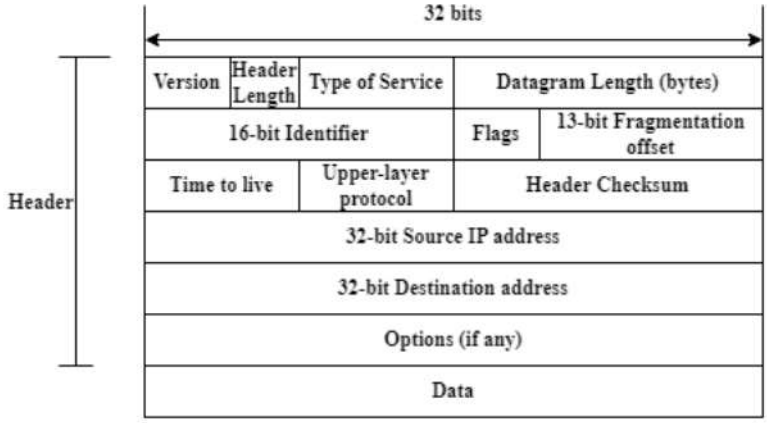


Fig.7.13: IPv4 Packet Format

The various fields in the packets are described below:

1. Version number: It is a 4-bit field, and specifies the IP protocol version of the packet. A router interprets the rest of the packet based on this field. It can be IPv4 or IPv6.
2. Header length: As the IPv4 packet can have a variable number of options, the beginning point of the data can also change. So the 4-bit header length value specifies where the data actually begins in the packet. If there are no options specified, an IP packet has a 20-byte header.
3. Type of service: Different types of services requiring low delay, high throughput, or high reliability can be specified with 8-bit combinations in this field. A router administrator issues different policies for providing different services.
4. Datagram length: This field specifies the total packet length which includes the header and the data. The size of this field is 16 bits, so the maximum size of the IP packet can be 65,535 bytes.
5. Identifier, flags, fragmentation offset: These 16 bits are considered if packet fragmentation is used. IPv6 does not allow fragmentation at routers.
6. Time-to-live: At every router, this field content (an 8-bit number) is decremented by 1. If this value becomes zero before a packet reaches its destination, then the packet will be dropped. This field ensures that a packet does not circulate in an infinite loop in the network.
7. Protocol: This field (8 bits) is used at the destination host to determine, to which transport layer protocol the data portion of the datagram would be passed (either TCP or UDP).
8. Header Checksum: This field (16 bits) helps the router to detect bit errors in the header section of

the IPv4 packet. It is the 16-bit 1' complement of the 1' complement sum of all 16-bit words in the header. If there is no corruption, then the result of summing the entire IP header, including checksum, should be zero. It is recalculated at every router if the header changes.

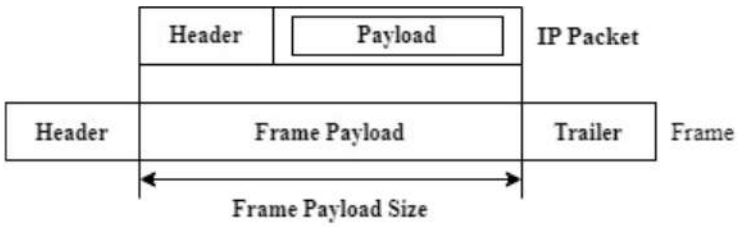
9. Source and Destination IP addresses: These addresses are inserted at the source when a packet is created.
10. Options: This field of variable length allows the IP header length to be extended. All datagrams may not contain this field.
11. Data (payload): This field contains the transport layer (TCP or UDP) segment to be delivered to the destination. This field can sometimes carry an ICMP message also. This field is of variable length.

7.7.1.1 IP Packet Fragmentation

This is another important function of the network layer. Fragmentation refers to breaking a larger packet into several small fragments with their own headers and trailers added, for them to travel independently. This process of fragmentation can be performed by the source node or any router in the path. The fragments are reassembled at the destination node.

A packet travels through different networks and links. Each link-layer protocol has its own format and can carry different-sized packets. So each frame can encapsulate a maximum size of the payload and this is referred to as Maximum Transfer Unit (MTU). This value is different for different physical layer protocols which in turn depend on restrictions imposed by the hardware and software components of the network.
For Eg: WAN links can carry a maximum of 576 bytes of data whereas Ethernet frames can carry up to 1500 bytes of data.

Fig. 7.14 shows the MTU at the link-layer frame.



MTU: Maximum size of frame payload

Fig. 7.14: Maximum transfer unit (MTU)

When a packet is fragmented, it is the payload portion of it that gets divided. Most part of the header remains the same except for three fields: identification, flags, and fragmentation offset.

Identification field: This field value is set by the source and remains the same for all the fragments in case of fragmentation. This is followed for the reassembly process to identify all the fragments of the original packet. A combination of the source IP address and Identification field uniquely defines a datagram.

Flags: There are three bits in this field.

- The leftmost is reserved and not used.
- The second bit (D) is called the do not fragment bit.
  - If it is set to 1, the packet payload cannot be fragmented. If such a packet cannot pass over a physical link, it will be discarded and an ICMP message will be sent to the source host.
  - If this bit is 0, then it can be fragmented.
- The third bit (M) is the more fragment bit. To indicate that a fragment is not the last fragment, it is set to 1. If its value is 0, then it indicates that it is the last or the only segment.

Offset field: This field shows the relative position of the fragment with respect to the whole packet.

Example 1: If a packet of size 4000 bytes is fragmented into three fragments, then show the offset value in the three fragments.

Solution 1: The 4000 bytes in the original packet are numbered from 0 to 3999

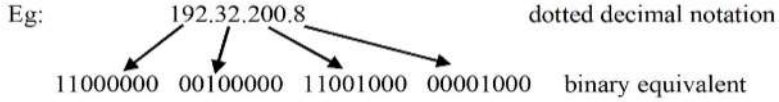
The offset values in the packets are measured in units of 8 bytes.

1. The 1400 bytes in the first fragment are numbered from 0 to 1399, and the offset value is 0/8 = 0
2. The 1400 bytes in the second fragment are numbered from 1400 to 2799, the offset value is 1400/8 = 175
3. The remaining 1200 bytes in the third fragment are numbered from 2800 to 3999, the offset value is 2800/8 = 350

7.7.2 IPv4 Addressing

We have already seen in 2.3.4 that at the network layer, all the nodes and connecting devices on the Internet are identified by an address called an IP address which is global in nature. Also, Fig.7.1 shows that the source and destination nodes have a single link to the network, whereas the routers can have two or more links to the network to forward the packets from one link to other links. The boundary between a host (node) and the physical link or between a router and the physical link is called an **interface.** A host has a single interface, whereas, a router can have multiple interfaces. As every host and router can send and receive IP packets, the IP protocol requires each host and router interface to have its own IP address.

An IP address is 32-bits long, so there can be a total of 2^{32} possible IP addresses. These addresses use a dotted-decimal notation, where each byte of the address is written in a decimal form separated by a period (dot).



IP addresses are globally managed by the Internet Corporation for Assigned Names and Numbers (ICANN) authority. The authority allocates blocks of addresses to five regional registries which will in

turn manage them within their regions to different organizations and Internet Service Providers (ISPs).

7.7.2.1 Hierarchical Addressing

All communication networks use hierarchical or levels in addressing. The postal networks use country, state, city, street, house number, and the name of the recipient in their postal address. Similarly, in the telephone network, the telephone number consists of the country code, area code, local exchange, and connection number.

A TCP/IP-wide area network is a collection of networks. The routers that are forwarding the packets between the networks do not know the exact location of the destination host, but only have knowledge about the network to which the host is connected. The routers use this information and the routing table to route the packet to the destination host's network. Once the packet reaches the destination's network, it is delivered to the destined host.

For the above routing process to work, a 32-bit IP address is divided into two parts: prefix and suffix. The prefix part of the address defines the network and the suffix part defines the connection of a node to the internet.

Fig. 7.15 shows this hierarchical address for a network of computers.

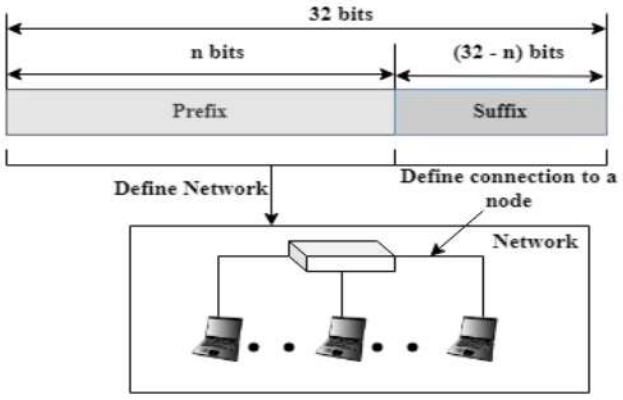


Fig. 7.15: Heirarchical Addressing

Subnet Mask:

When an IP network is divided into subnetworks, a subnet mask (a 32-bit number) is used to determine the network ID and the host ID. This is created by setting host bits to all 0's and network bits to all 1's. So, a subnet mask separates a given IP address into host and network addresses. The TCP/IP protocol uses the subnet mask to determine if a host is on the local subnet or on another remote network.

Fig. 7.16 demonstrates the concept of hierarchical addressing with interface addresses and subnets for a three-subnet network connected by a router.

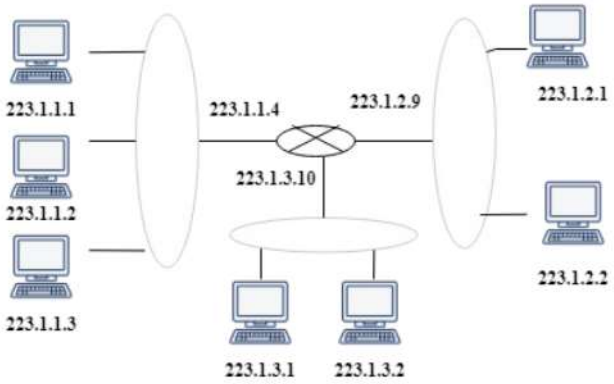


Fig. 7.16: Interface addresses and subnets

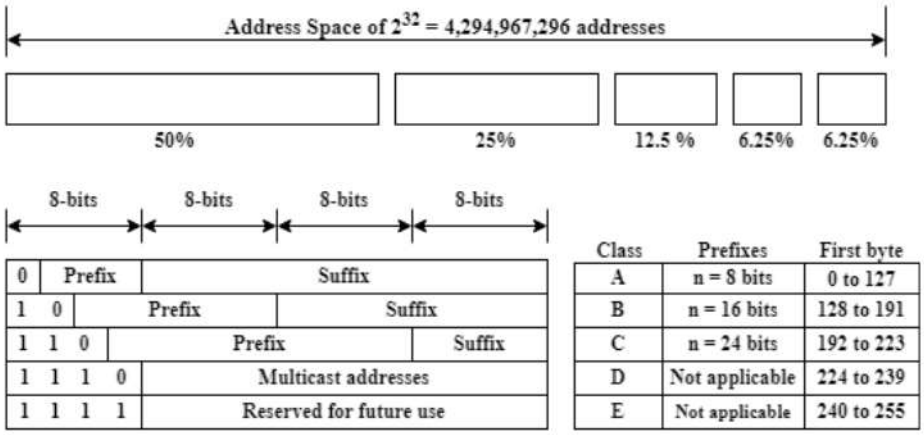
The three subnets are connected by a router via three interfaces. Each host gets connected to one of these subnets.

Let us first consider the three hosts connected to the left side of the router. They have an IP address of the form, 223.1.1.xxx, which indicates that the leftmost three bytes or 24 bits have the same value. All these hosts may be a part of an Ethernet LAN connected by a switch or a wireless access point. So, the network connecting these three host interfaces to one router interface is called a subnet. The address assigned by IP addressing to this subnet is 223.1.1.0/24, also known as the subnet mask. This indicates that the 24 bits on the left of the 32-bit IP address define the subnet address. So, some portion of the IP address is determined by the subnet (subnetwork) to which it is connected.

7.7.2.2 Classful Addressing

The prefix in the address part can be fixed or variable. The earlier IPv4 used the fixed prefix format and the addressing is called classful addressing.

In classful addressing, the whole address space is divided into 5 classes: A, B, C, D, and E with different prefix bit sizes as shown in Fig.7.17. Here, the most significant bit identifies a class. In every class, the number of networks and the number of hosts in each network are different.



Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Fig. 7.17: Address space in Classful addressing

For Eg: In class A, the network identifier is 7 bits, so there can be only 128 (2^7) class A networks in the world.

In class B, the network identifier is 14 bits, so there can be only 16384 (2^{14}) class B networks in the world.

NOTE: A multicast address is an address shared by a group of hosts.

The default subnet masks for Class A, B, and C networks:

Class A – 255.0.0.0

Class B – 255.255.0.0

Class C – 255.255.255.0

Example 2: Identify the class of the three IP addresses 10.52.36.10, 172.16.52.63 and 192.163.123.132

Solution 2: There are two ways in which the class of an IP address can be found:

1. By considering the binary notation of the first octet or first 8 bits of an address.
2. By considering the range of addresses in each class indicated by the first byte of the decimal notation.

For the IP address: 10.52.36.10

The binary notation of the first octet is 00001010. As the MSB is 0, it is a Class A address. Also, the range of addresses in Class A is 0 to 127, and the first byte 10 lies in this range.

For the IP address: 172.16.52.63

The binary notation of the first octet is 10101100. As the first two MSBs are 10, it is a Class B address. Also, the range of addresses in Class B is 128 to 191, and the first byte 172 lies in this range.

For the IP address: 192.163.123.132

The binary notation of the first octet is 11000000. As the first three MSBs are 110, it is a Class C address also the range of addresses in Class C is 192 to 223, and the first byte 192 lies in this range.

7.7.2.3 Address Depletion

This is a situation when there are no addresses remaining for usage. This is a problem that existed because the addresses were not distributed properly, and many addresses in a class were not used and were wasted. This problem was solved to some extent by Subnetting and Supernetting, but not completely.

Subnetting and Supernetting:

In subnetting, a class A or class B block will be divided into many subnets. Each subnet can have a larger prefix length than the original network. This allows the addresses to be allocated to many organizations if all the addresses in a network are not used. In another way, if we think of a class A network, there can be 2^{24} hosts, and managing them is difficult. So this large network can be divided into much smaller manageable networks.

Let us understand subnetting with an example.

Example: Consider a class C network with network ID 200.10.1.0. This network with 24 bits for network ID and 8 bits for host ID can address 256 hosts of which the first IP address (Network address) and the last IP address (broadcast address) cannot be used. So there will be 254 addresses available for hosts.

The host address range will be 200.10.1.1 to 200.10.1.254

In Binary the above address range is represented as: **11001000. 00001010. 00000001.** 00000001

11001000. 00001010. 00000001. 10000000

NOTE: The first address is **11001000. 00001010. 00000001.** 00000000 and the last address is **11001000. 00001010. 00000001**. 11111111. These are not used for host addressing.

If these hosts are logically divided into two networks, there will be 127 hosts in each network. As the number of hosts decreases by half, the number of bits in the host address will also decrease by one bit. In this case, instead of 8 bits, only 7 bits can be used to address the hosts and the most significant bit can be used to address the two subnets.

The two Subnet address ranges are 200.10.1.1 to 200.10.1.126 and 200.10.1.129 to 200.10.1.254.

In Binary:

Subnet 1 range is represented by: **11001000. 00001010. 00000001. 0**0000001

11001000. 00001010. 00000001. 01111110

Subnet 2 range is represented by: **11001000. 00001010. 00000001. 1**0000001

11001000. 00001010. 00000001. 11111110

NOTE: Here two more addresses are lost for network IDs and broadcast IDs, so in all four addresses are lost for use (200.10.1.0, 200.10.1.127, 200.10.1.128, 200.10.1.255). So the number of available addresses will be 252 (256 – 4).

In **Supernetting**, many smaller blocks are combined into a large block or aggregating networks together, which can increase the number of addresses available on a network.

For Eg: If more than 256 class C addresses are needed by an organization, several class C blocks can be combined into a large block.

Supernetting also reduces the size of the routing tables on a router, by combining or aggregating routes pointing to the same next hop. It also slows down the exhaustion of IP addresses by the use of Classless Inter-Domain Routing (CIDR).

7.7.2.3 Classless Addressing

As subnetting and supernetting did not solve the address depletion problem completely, the IPv6 with a 128-bit address was devised as a long-term solution. But as IPv4 is still used, another addressing distribution technique called classless addressing is used to solve the problem.

Here, the whole address space is divided into variable-length blocks, with a limitation that the number of addresses in each block should be a power of 2. The prefix length can range from 0 to 32. The more the prefix length, the lesser the number of networks. Fig. 7.18 shows the address space in classless addressing with nonoverlapping blocks.

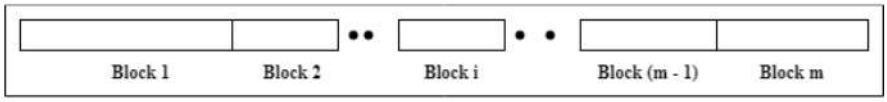


Fig. 7.18: Variable length blocks in Classless addressing

Prefix Length: Slash Notation:

An address in classless addressing does not define the block or network as the prefix length is not specified in the address as in classful addressing. So the prefix length is specified by a slash notation class classless interdomain routing or CIDR notation as shown in Fig. 7.19.

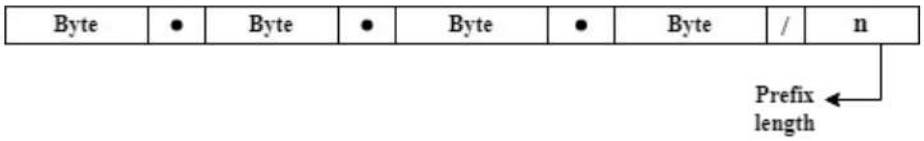


Fig. 7.19: Slash Notation

Extracting Information from an address:

There are three pieces of information to be extracted from a classless CIDR notation address: the number of addresses, the first address, and the last address in the block. These are obtained in three steps as given below:

- The number of addresses, $N = 2^{32-n}$
- The first address = the n leftmost addresses, with (32 – n) bits all set to 0s.
- The last address = the n leftmost addresses, with (32 – n) bits all set to 1s.

Example: For the classless address 167.199.170.82/27, determine the number of addresses, the first and last address.

Solution: 1. From the address, we have n = 27, so $N = 2^{32-27} = 2^5 = 32$ addresses.

2. The given address (in bits) is 10100111 11000111 10101010 01010010, so the first address is obtained by keeping the leftmost 27 bits of the address with the remaining bits set to 0s = 10100111 11000111 10101010 01000000

3. The last address is obtained by keeping the leftmost 27 bits of the address with the remaining bits set to 1s = 10100111 11000111 10101010 01011111

Special Addresses:

There are five addresses used for special purposes only. They are this-host, limited-broadcast, loopback, and multicast addresses.

This-host Address:

This address is when a host does not know its own address and wants to send an IP packet. The address used in this case is 0.0.0.0/32

Limited-broadcast Address:

This address is used to send a packet to all the devices in a network, but at a router, this packet is blocked as this is the destination address and cannot travel outside the network. The address used in this case is 255.255.255.255/32

Loopback Address:

The loopback address is 127.0.0.0/8. A packet with this as the destination address does not leave the host. It is used to test a piece of software in the host.

Private Address:

There are four blocks of addresses allocated as private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, and 169.254.0.0/16. They are usually used for security purposes.

Multicast Address:

The block of address 224.0.0.0/4 is reserved for the multicast or group address.

7.7.2.4 Dynamic Host Configuration Protocol (DHCP)

When devices are moved from one subnet to another in a TCP/IP network, IP addresses are removed from the first network and are to be manually assigned to the device again. This address configuration can also be done automatically through the DHCP protocol. The devices can be fixed or mobile hosts that are connected wired or wirelessly.

This protocol uses a client-server architecture and has two components: a centrally installed network DHCP server and client instances of the protocol stack on every device. DHCP allows the host to

obtain an IP address automatically.

When a device gets connected to a DHCP-based network to access to its resources, it sends a request for an IP address. This is received up a DHCP server. The server responds and sends an IP address to the device. The server can take back the IP address after a specified amount of time or when the device shuts down. The IP address will be returned to the pool of addresses managed by the DHCP server. The server can reassign the same address to another device when it seeks access to the network.

The DHCP server can be configured to assign the same IP address to a host device every time or can be different. The DHCP also allows a host to obtain additional information, such as the address of the first hop router or the subnet mask, or the Domain Name Server (DNS)

The important benefits of the protocol: Reduced network administration, IP address optimization, Reliable IP address configuration, and Mobility.

7.8 Self-Assessment Questions

Q1. What is packet forwarding? (2 marks, L2)
Q2. Explain the forwarding process with the help of a forwarding table. (10 marks, L3)
Q3. What are the different types of forwarding methods? Explain briefly. (6 marks, L3)
Q4. Compare Virtual Circuit and Datagram Networks. (10 marks, L4)
Q5. Briefly describe the IP packet format. (8 marks, L3)
Q6. Discuss IPv4 addressing. (10 marks, L3)
Q7. Describe briefly the DHCP architecture. (5 marks, L3)

7.9 Multiple-Choice Questions

Q1. Placing a packet in its route to its destination is called, [1 mark, L1]
   A. Framing
   B. Forwarding
   C. Delivering
   D. None of the above

Q2. The device is used to forward the packets based on the destination IP address is _____, [1 mark, L1]
   A. Repeater
   B. Hub
   C. Switch
   D. Router

Q3. The function of a router is, ___ [1 mark, L1]
   A. To change the data from one format to another
   B. To detect errors in data

C. To send the packet to the uplinks

D. None of the above.

Q4. The network with network layer connectionless service is called _____ network.

A. Datagram

B. Virtual Circuit

C. Both A and B

D. None of the above

Q5. What is the standard form of CIDR ? [1 mark, L1]

A. Classful Interdomain Routing

B. Classless Interdomain routing

C. Classless Intradomain routing

D. None of the above

Q6. Which of the below options is not a network layer function? [1 mark, L1]

A. Addressing

B. Congestion Control

C. Routing

D. Internetworking

Q7. A IP address consists of _____ [1 mark, L1]

A. Only host address

B. Only network address

C. Both host and network address

D. None of the above

Q8. IPv4 address is of ____ bits.

A. 16

B. 32

C. 64

D. 128

Q9. IPv6 address is of ____ bits.

A. 16

B. 32

C. 64

D. 128

7.10 Keys to Multiple-Choice Questions

Q1. Forwarding (B)

Q2. Router (D)

Q3. To send packets to the uplinks (C)

Q4. Datagram (A)

Q5. Classless Interdomain Routing (B)

Q6. Congestion Control (B)

Q7. Both host and network address (C)

Q8. 32 (B)

Q9. 128 (D)

7.11 Summary of the Unit

This unit covers the important layer covering the core area of the network i.e Network Layer. As the network layer involves all hosts and routers, the design of protocols is challenging. The important services provided by the network layer are packetizing, routing, and forwarding. The first section of this unit discussed the forwarding process with an example that also included the use of a forwarding table. It also discussed two forwarding techniques: using the destination address and using a label. The second section dealt with the important services of the layer. To make the router's job simple, many measures have been taken. To reduce packet processing time and complexity, connectionless or datagram services are provided at this layer. Here the packet header is fixed in size and no fragmentation is done. This provides a best-effort service. On the other hand, a connection-oriented network layer provides a more reliable service. The third section also includes the comparison of Datagram and Virtual-circuit networks. The last section deals with the popular network layer protocol: IP protocol. This discussion includes the packet format and packet fragmentation which is used to support different link layer protocols. The discussion concludes with the IPv4 addressing technique which is used to identify all the hosts on the Internet with a unique address.

7.12 Recommended Learning Resources

[1] James F Kurose and Keith W Ross, Computer Networking, A Top-Down Approach, Sixth Edition, Pearson,2017.

[2] Behrouz A Forouzan, Data and Communications and Networking, Fifth Edition, McGraw Hill, Indian Edition

7.13 References

[1] https://www.slideshare.net/dama2211/nl-design-issuespptx

[2] https://www.geeksforgeeks.org/design-issues-in-network-layer/

[3] https://www.tutorialspoint.com/network-layer-design-issues

[4] https://www.baeldung.com/cs/routing-vs-forwarding-tables

[5] https://www.thecoldwire.com/what-is-the-difference-between-routing-and-forwarding/

[6] https://www.quora.com/What-is-the-difference-between-a-routing-table-and-a-forwarding-table

MCQs:

[1] https://t4tutorials.com/router-mcqs-networking-devices/