BACHELOR OF COMPUTER APPLICATIONS

SEMESTER 4

DCA2201

COMPUTER NETWORKING

Unit 6

Network Layer – Internetworking

Table of Contents

1. INTRODUCTION

We have discussed datalink layer sliding window protocols in the previous unit. The essence of sliding window protocol is that both sender and receiver agree on the number of data frames it sends and receives before sending an acknowledgement. Framing and flow control are the major functions of datalink layer. The data link layer accepts the packet from the network layer and converts it into frames. In this unit, we will discuss Network layer and its functions. The main function of network layer is to transfer packets from source to destination. In order to achieve its goals, the network layer must know about the topology of the network and has to choose appropriate paths through it, even for large networks. It should also take care while choosing routes. Routes should be taken in such a way that it shouldn't overload a few of the communication lines and routers while leaving others idle.

We will start this unit with an introduction to a network layer. In this unit, we are going to discuss two broad approaches towards structuring network-layer packet delivery such as virtual circuits and datagram networks. In the last session, we discussed about the Internet protocols, we will also discuss IPV4 and IPV6 addressing on the internet.

1.1 Objectives:

After studying this unit, you should be able to:

- *Describe virtual circuit networks*
- *Explain datagram networks*
- *Describe Internet Protocol (IP)*
- *Explain IPV4 addressing*
- *Explain IPV6 addressing*

2. VIRTUAL CIRCUITS AND DATAGRAM NETWORKS

A network layer provides connectionless and connection-oriented services between two hosts. These services are host-to-host services provided by network layer for the transport layer. In all major computer network architectures (such as Internet, ATM and so on), the network layer provides either a host-to-host connectionless service or a host-to-host connection-oriented service, but not both. Computer networks that provide only a connection-oriented service at the network layer is called ***virtual-circuit (VC) networks*** whereas computer networks that provide only a connectionless service at the network layer are called ***datagram networks.***

Virtual-Circuit Networks

As discussed earlier, networks having connection-oriented services in the network layer are called Virtual Circuit networks and these network layer connections are called virtual circuits (VCs). Let's now consider how a VC service can be implemented in a computer network. A virtual circuit consists of a path between the source and destination hosts, Virtual circuit number (one number for each link along the path), and 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. Consider the network shown in figure 6.1.

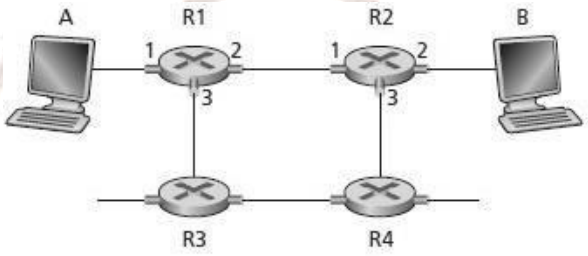

Fig 6.1: A simple virtual circuit network

Figure 6.1 illustrates the concept of a virtual circuit. The numbers next to R1 are link interface numbers. Suppose host A requests that the network establish a VC between itself and Host B. Also, 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. The router knows the replacement VC number for a packet traversing the router by using router's forwarding table. The forwarding table includes VC number translation. For example, the forwarding table in R1 might look like table 6.1.

Table 6.1: Forwarding table in R1

Incoming Interface	Incoming VC#	Outgoing Interface	Outgoing VC#
1	12	2	22
2	63	1	18
3	7	2	17
…….	…….	……..	……..

Whenever a new VC is established across a router, an entry is added to the forwarding table. Similarly, whenever a VC terminates, the appropriate entries in each table along its path are removed.

The reason for using different VC numbers on each of the links is that, first, replacing the number from link to link reduces the length of the VC field in the packet header. Second, and more importantly, VC setup is considerably simplified by permitting a different VC number at each link along the path of the VC. Specifically, with multiple VC numbers, each link in the path can choose a VC number independently of the VC numbers chosen at other links along the path. If a common VC number were required for all links along the path, the routers would have to exchange and process a substantial number of messages to agree on a common VC number to be used for a connection.

In a virtual circuit network, routers must maintain a connection state information for the ongoing connections. Whenever 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. There are three stages in a virtual circuit. They are:

1) *VC Setup:* in this stage, the network layer determines the path between sender and receiver based on receiver's address. This path includes a series of links and routers through which packets will travel. 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 and also reserve resources along the path of the VC.
2) *Data transfer:* Once the VC has been established, packets can flow along the VC. Virtual circuit setup and packet flow is shown in the below figure 6.2.
3) *VC teardown:* when the sender or receiver informs the network layer to terminate the VC, the network layer will inform the end system on the other side of the network about 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.

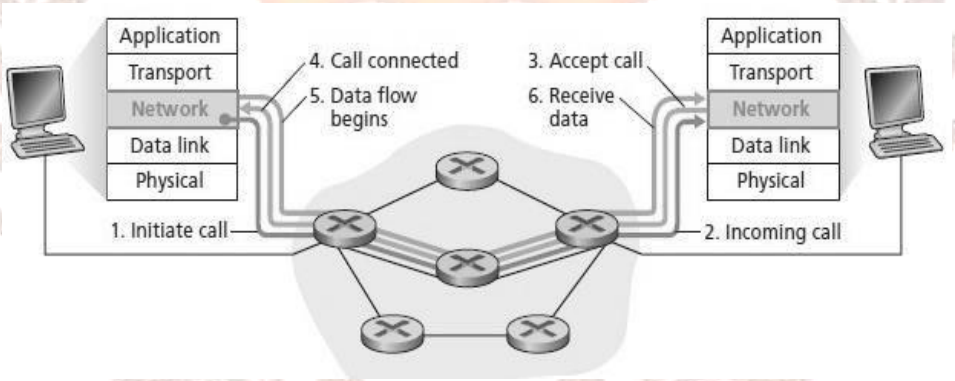

Fig 6.2: Virtual-circuit Setup

The messages that the end systems send into the network to initiate or terminate a VC, and the messages passed between the routers to set up the VC are known as signaling messages, and the protocols used to exchange these messages are often referred to as *signaling protocols.*

Datagram Networks

In datagram networks, whenever an end system wants to send a packet, it affixes the packet with the address of the destination and then throws the packet into the network. The circuit is shown in figure 6.3. We can see in the figure that there is no circuit setup and routers do not maintain any VC state information.

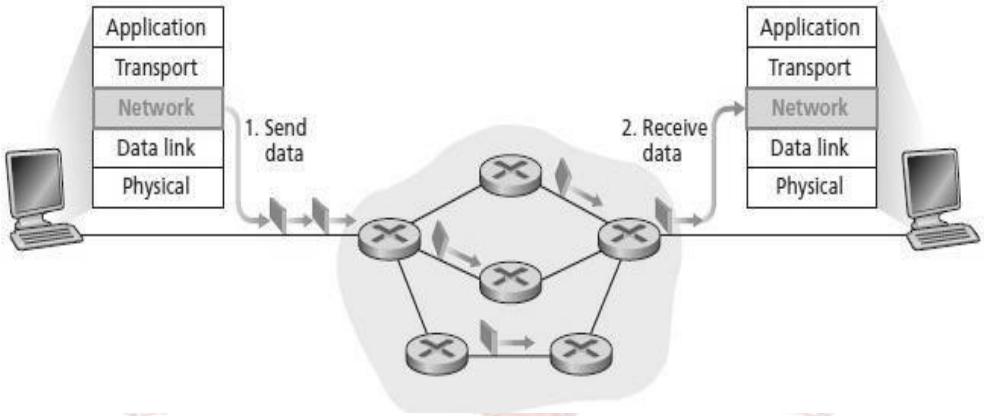

Fig 6.3: Datagram Network

As a packet is transmitted from source to destination, it passes through a series of routers. 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. The router then forwards the packet to that output link interface.

Although routers in datagram networks maintain no connection state information, they still maintain forwarding state information in their forwarding tables. However, the time scale at which this forwarding state information changes is relatively slow. In a datagram network the forwarding tables are modified by routing algorithms, which typically update a forwarding table every one to five minutes or so. In a VC network, a forwarding table in a router is modified whenever a new connection is set up through the router or whenever an existing connection through the router is released. This could easily happen at a microsecond timescale in a router.

Comparison of Virtual-Circuit and Datagram Networks

The following table 6.2 illustrates the comparison between virtual circuits and datagram networks.

Table 6.2: Comparison of Virtual-Circuit and Datagram Networks

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Virtual circuit requires a setup phase, which consumes time and resources, but it is more reliable. In a datagram network, no setup is needed but a more complicated lookup procedure is required to locate the entry for the destination. A related issue is that the destination addresses used in datagram networks are longer than circuit numbers used in virtual-circuit networks because they have a global meaning. Another issue is the amount of table space required in router memory. A datagram network needs to have an entry for every possible destination, whereas a virtual-circuit network just needs an entry for each virtual circuit. Virtual circuits have some advantages in guaranteeing quality of service and avoiding congestion within the network because resources (e.g., buffers, bandwidth, and CPU cycles) can be reserved in advance, when the connection is established. Virtual circuits also have a vulnerability problem. If a router crashes and loses its memory, even if it comes back up a second later, all the virtual circuits passing through it will have to be aborted. In contrast, if a datagram router goes down, only those users whose packets were queued in the router at the time need suffer. Datagrams also allow the routers to balance the traffic throughout the

network, since routes can be changed partway through a long sequence of packet transmissions.

SELF-ASSESSMENT QUESTIONS – 1

1. Computer networks that provide only a connection-oriented service at the network layer is called _____.
2. Computer networks that provide only a connectionless service at the network layer are called _____.
3. The network layer connections are called Virtual circuits. (True/False)
4. The messages passed between the routers to set up the VC are known as
5. Each packet is routed independently in _____networks.

3. THE INTERNET PROTOCOL (IP)

As we know, computers communicate through the Internet. We need a global addressing scheme to forward packets to the destination through different LANs and routers. Internet addressing and forwarding are important components of the Internet Protocol (IP). There are two versions of IP in use today. First, we will discuss IP protocol version 4, which is usually referred to simply as IPv4. In this, the addresses are 32 bits in length; this gives a maximum of 2^{32} addresses. Next version is IP protocol version 6 (IPV6). Here, the Internet uses 128-bit addresses that give much greater flexibility in address allocation.

3.1 Internet protocol version 4 (IPV4)

IPV4 is a connectionless protocol and is unreliable. It is primarily responsible for addressing and routing packets between hosts. A higher layer protocol such as TCP or an application protocol must acknowledge delivered packets and recover lost packets if required. IPV4 is defined in RFC 791. Figure 6.4 shows the datagram format of IPV4. It consists of IPV4 header and Payload. Header consists of Source address, destination address, identification number, checksum etc.

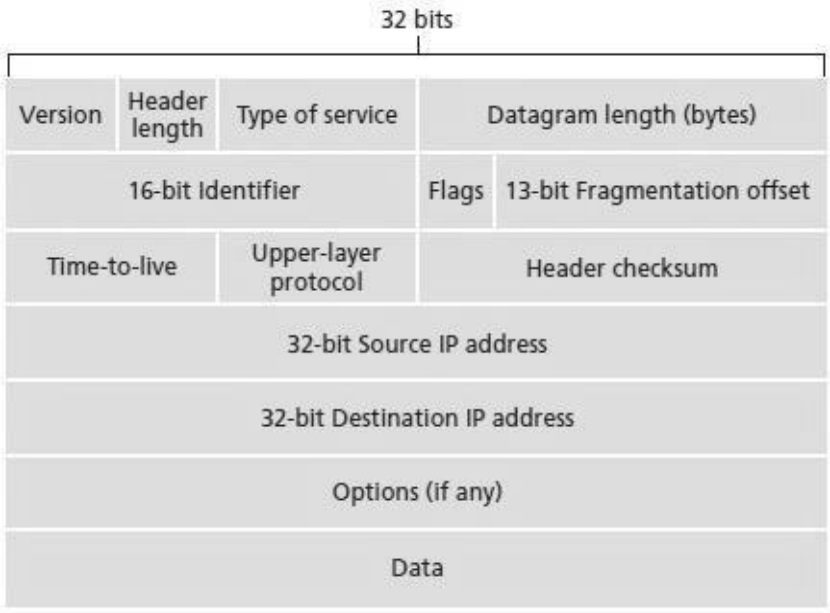

Fig 6.4: IPV4 datagram format

Here, version number specifies the IP protocol version of the datagram. 4 bits Header length indicates where in the IP datagram the data actually begins. The *type of service* (TOS) bits is included in the IPv4 header to allow different types of IP datagrams to be distinguished from each other. *Datagram length* is the total length of the IP datagram (header plus data), measured in bytes. *Identifier, flags, fragmentation offset* are the three fields used in IP fragmentation, which we will discuss later. *Time-to-live* (TTL) field is included to ensure that datagrams do not circulate forever in the network. This field is decremented by one each time the datagram is processed by a router. If the TTL field reaches 0, the datagram must be dropped. *Protocol* field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport-layer protocol to which the data portion of this IP datagram should be passed. The *header checksum* aids a router in detecting bit errors in a received IP datagram. When a source creates a datagram, it inserts its IP address into the *source IP address field* and inserts the address of the ultimate destination into the *destination IP address field*. The options fields allow an IP header to be extended. The *data field* of the IP datagram contains the transport-layer segment (TCP or UDP) to be delivered to the destination.

Fragmentation and reassembly

If a router receives an IPV4 packet that is too large for the network segment on which the packet is being forwarded, IPV4 on the router fragments the original packet into smaller packets that fit on the forwarding network segment. When the packets arrive at their final destination, IPV4 on the destination host reassembles the fragments into the original payload. This process is referred to as fragmentation and reassembly. Fragmentation can occur in environments that have a mix of networking technologies, such as Ethernet or Token Ring.

IPV4 addressing

An IP address is an identifier that is assigned at the Internet layer to an interface or a set of interfaces. Each IP address can identify the source or destination of IP packets. The IPV4 address is a logical address because it is assigned at the Internet layer and has no relation to the addresses that are used at the Network Interface layer. IPV4 addresses are 32 bits long.

IPV4 address syntax

Since IPV4 addresses are 32 bits long, using binary notation is very difficult to express and remember and hence dotted decimal notation is used to represent this address. For example, the IPV4 address 11000000101010000000001100011000 is expressed as 192.168.3.24 in dotted decimal notation. That is, separate the digits into 8 blocks, convert each to decimal and separate the blocks with periods.

When referring to an IPV4 address, use the notation w.x.y.z. Figure 6.5 shows the IPV4 address structure.

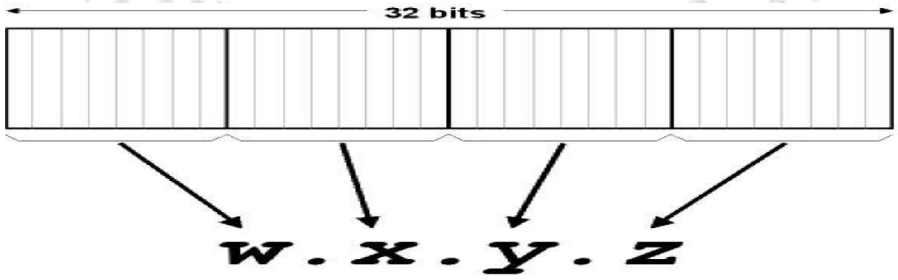

Fig 6.5: The IPV4 address in dotted decimal notation

IPV4 address prefixes

Each bit of a unique IPV4 address has a defined value. However, IPV4 address prefixes express ranges of IPV4 addresses in which zero or more of the high-order bits are fixed at specific values and the rest of the low-order variable bits are set to zero. To express an IPV4 address prefix, you must identify the number of high-order bits that are fixed and their value. Then you can use prefix length notation or dotted decimal notation.

Prefix length notation

If you use prefix length notation, you express address prefixes as *Starting Address/Prefix Length,* in which:

- *Starting Address* is the dotted decimal expression of the first mathematically possible address in the range. To form the starting address, set the fixed bits at their defined values, and set the remaining bits to 0.
- *Prefix Length* is the number of high-order bits in the address that are fixed.

For example, the IPV4 address prefix 131.107.0.0/16 specifies a range of 65,536 addresses. The prefix length, 16, specifies that all addresses in the range begin with the same 16 bits as the starting address. Because the first 16 bits of the starting address are fixed at 10000011 01101011 (131 107 in decimal), all addresses in the range have 131 as the first octet and 107 as the second octet. With 16 variable bits in the last two octets, there is a total of 2^{16} or 65,536 possible addresses. Prefix length notation is also known as *Classless Inter-Domain Routing (CIDR)* notation.

Types of IPV4 addresses

Internet standards define the following types of IPV4 addresses:

- **Unicast:** Assigned to a single network interface located on a specific subnet; used for one-to-one communication.
- **Multicast:** Assigned to one or more network interfaces located on various subnets; used for one-to-many communication.
- **Broadcast:** Assigned to all network interfaces located on a subnet; used for one-to-everyone on a subnet communication.

IPV4 Unicast Addresses

Each IPV4 unicast address includes a subnet prefix and a host ID portion. The subnet prefix (also known as a network identifier or network address) portion of an IPV4 unicast address identifies the set of interfaces that are located on the same physical or logical network segment, whose boundaries are defined by IPV4 routers. A network segment on TCP/IP networks is also known as a subnet or a link. All nodes on the same physical or logical subnet must use the same subnet prefix, and the subnet prefix must be unique within the entire TCP/IP network.

The host ID (also known as a host address) portion of an IPV4 unicast address identifies a network node's interface on a subnet. The host ID must be unique within the network segment.

Internet Address Classes

The class of address defined how many bits were used for the subnet prefix and how many bits were used for the host ID. Address classes also defined the possible number of networks and the number of hosts per network. Of five address classes, class A, B, and C addresses are reserved for IPV4 unicast addresses. Class D addresses are reserved for IPV4 multicast addresses, and class E addresses were reserved for experimental uses.

Class A address prefixes are assigned to networks with very large numbers of hosts. The prefix length of Class A address prefixes is only 8 bits, allowing the remaining 24 bits to identify up to 16,777,214 host IDs. However, the short prefix length limits the number of networks that can receive class A address prefixes to 126. First, the high-order bit in class A address prefixes is always set to 0. That convention decreases the number of class A address prefixes from 256 to 128. Second, addresses in which the first eight bits are set to 00000000 cannot be assigned because they constitute a reserved address prefix. Third, addresses in which the first eight bits are set to 01111111 (127 in decimal) cannot be assigned because they are reserved for loopback addresses. Those last two conventions decrease the number of class A address prefixes from 128 to 126.

For any IPV4 address prefix, the two host IDs in which all the host bits are set to 0 (the all-zero's host ID) or to 1 (the all-ones host ID) are reserved and cannot be assigned to network

node interfaces. This convention reduces the number of host IDs in each class A network from 16,777,216 (224) to 16,777,214.

Figure 6.6 illustrates the structure of class A addresses.

Fig 6.6: Structure of class A addresses

Class B address prefixes are assigned to medium to large-sized networks. In addresses for these networks, the first 16 bits specify a particular network, and the last 16 bits specify a particular host. However, the two high-order bits in a class B address are always set to 10. With 14 bits to express class B address prefixes and 16 bits to express host IDs, class B addresses can be assigned to 16,384 networks with up to 65,534 hosts per network.

Figure 6.7 below illustrates the structure of class B addresses.

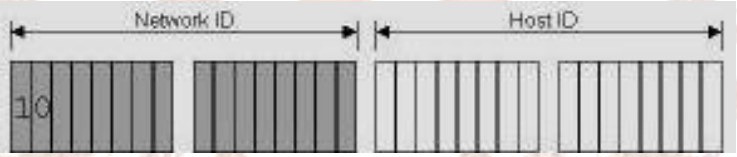

Fig 6.7: Structure of class B addresses

Class C address prefixes are assigned to small networks. In addresses for these networks, the first 24 bits specify a particular network, and the last 8 bits specify particular hosts. However, the three high order bits in a class C address prefix are always set to 110, which makes the address prefix for all class C networks and addresses 192.0.0.0/3 (or 192.0.0.0, 224.0.0.0). With 21 bits to express class C address prefixes and 8 bits to express host IDs, class C addresses can be assigned to 2,097,152 networks with up to

254 hosts per network. Figure 6.8 illustrates the structure of class C addresses.

Fig 6.8: Structure of class C addresses

Class D addresses are reserved for IPV4 multicast addresses. The four high-order bits in a class D address are always set to 1110, which makes the address prefix for all class D addresses 224.0.0.0/4 (or 224.0.0.0, 240.0.0.0). Class E addresses are reserved for experimental use. The high-order bits in a class E address are set to 1111, which makes the address prefix for all class E addresses 240.0.0.0/4 (or 240.0.0.0, 240.0.0.0).

Modern Internet Addresses

The Internet address classes are an obsolete method of allocating unicast addresses because it proved inefficient. For example, a large organization with a class A address prefix can have up to 16,777,214 hosts. However, if the organization uses only 70,000 host IDs, 16,707,214 potential IPV4 unicast addresses for the Internet are wasted.

Since 1993, IPV4 address prefixes are assigned to organizations based on the organization's actual need for Internet-accessible IPV4 unicast addresses. This method is known as Classless Inter-Domain Routing (CIDR). CIDR is a way to allocate and specify internet addresses used in inter-domain routing more flexibly than with the original system of internet protocol address classes. As a result, the number of available internet addresses has been greatly increased. For example, an organization determines that it needs 2,000 Internet-accessible IPV4 unicast addresses. The Internet Corporation for Assigned Names and Numbers (ICANN) or an Internet service provider (ISP) allocates an IPV4 address prefix in which 21 bits are fixed, leaving 11 bits for host IDs. From the 11 bits for host IDs, you can create 2,046 possible IPV4 unicast addresses.

3.2 IPV6 Addressing

IPV6 is a routable protocol that addresses, routes, fragments, and reassembles packets. The IPV6 Internet layer consists of the following protocols:

- IPV6
- ICMPv6
- ND
- MLD

The below sections describe these protocols in more detail.

IPV6

Like IPV4, IPV6 is a connectionless, unreliable datagram protocol that is primarily responsible for addressing and routing packets between hosts. RFC 2460 defines IPV6 packet structure. An IPV6 packet consists of an IPV6 header and an IPV6 payload. The IPV6 payload consists of zero or more IPV6 extension headers and an upper layer protocol data unit, such as an ICMPv6 message, a TCP segment, or a UDP message. Figure 6.9 shows the IPV6 datagram format.

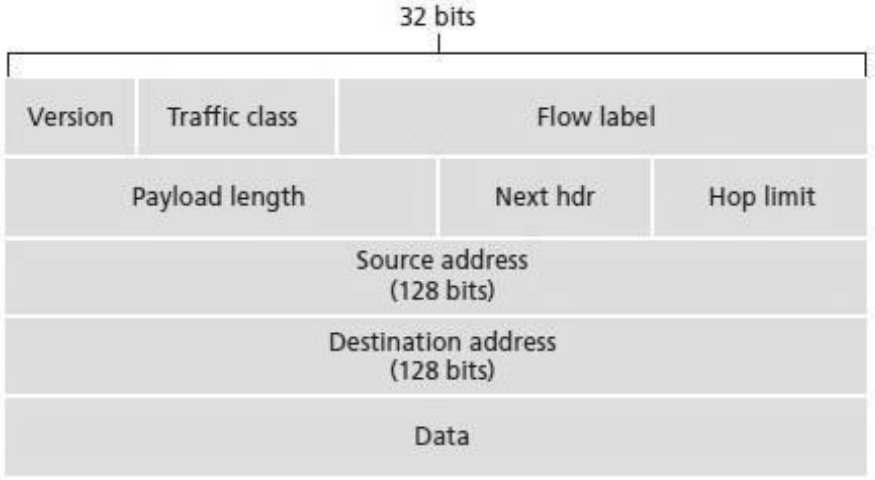

Fig 6.9: IPV6 Datagram format

Version. Is a 4-bit field that identifies the IP version number. IPv6 carries a value of 6 in this field. *Traffic class* is an 8-bit field similar to the TOS field we saw in IPv4. A *flow label* is a 20-bit field used to identify a flow of datagrams. *Payload length* is a 16-bit value and is treated as an unsigned integer giving the number of bytes in the IPv6 datagram following the fixed-length, 40-byte datagram header. *Next header* is the field identifies the protocol to which the contents (data field) of this datagram will be delivered. The contents of *Hop limit* field are decremented by one by each router that forwards the datagram. If the hop limit count reaches zero, the datagram is discarded. *Source and destination addresses* contain source and destination IP addresses and data field contains the payload.

Fragmentation in IPV6

In IPV6, only a sending host can fragment the packet. But in IPV4, if a router receives a packet which is too large, router itself will fragment the packet. In IPV6, if a router receives a larger packet, router sends an ICMPv6 Packet Too Big message to the sending host and discards the

packet. Only the sending host can fragment the packet and destination host can reassemble it through the use of the Fragment extension header.

Internet Control Message Protocol for IPV6 (ICMPv6)

IPV6 doesn't report errors like IPV4. It uses an updated version of Internet Control Message Protocol known as ICMPv6. This protocol reports errors in delivery or forwarding and provides a simple echo service for troubleshooting. It also provides a message structure for ND and MLD messages.

Neighbor Discovery (ND)

Neighbor Discovery (ND) is a set of ICMPv6 messages and processes that determine relationships between neighboring nodes. Different functionalities provided by ND are:

- Hosts use ND to discover neighboring routers and discover and automatically configure addresses and other configuration parameters.
- Routers use ND to advertise their presence, host addresses, and other configuration parameters and inform hosts of a better next-hop address to forward packets for a specific destination.
- Nodes (hosts and routers) use ND to resolve the link -layer address (also known as a MAC address) of a neighboring node to which an IPV6 packet is being forwarded, to dynamically advertise changes in MAC addresses and to determine whether a neighbor is still reachable.

Multicast Listener Discovery (MLD)

Multicast Listener Discovery (MLD) is a set of ICMPv6 messages exchanged by routers and nodes, enabling routers to discover the set of IPV6 multicast addresses for which there are listening nodes for each attached interface. MLD discovers only those multicast addresses that include at least one listener, not the list of individual multicast listeners for each multicast address. RFC 2710 defines MLD. The three types of MLD messages are:

- **Multicast Listener Query:** Routers use this message to query a subnet for multicast listeners.
- **Multicast Listener Report:** Multicast listeners use Multicast Listener Report messages to either report interest in receiving multicast traffic for a specific multicast address or to respond to a Multicast Listener Query message.

- **Multicast Listener Done:** Multicast listeners use Multicast Listener Done messages to report that they might be the last multicast group member on the subnet

IPV6 Addressing

An IPV6 address is 128 bits long, which is four times larger than an IPV4 address. A 128-bit address space allows for 2^{128} or 340,282,366,920, 938,463,463,374,607,431,768,211,456 (or $3.4*10^{38}$) possible addresses. The relatively large size of the IPV6 address space is designed for efficient address allocation and routing that reflects the topology of the modern-day Internet and to accommodate 64-bit media access control (MAC) addresses that newer networking technologies are using. The use of 128 bits allows for multiple levels of hierarchy and flexibility in designing hierarchical addressing and routing, which the IPV4-based Internet lacks. RFC 3513 describes the IPV6 addressing architecture.

IPV6 Address Syntax

IPV4 addresses are represented in dotted decimal notation. For IPV6, the 128-bit address is divided along 16-bit boundaries, each 16-bit block is converted to a 4-digit hexadecimal number (the Base16 numbering system), and adjacent 16-bit blocks are separated by colons. The resulting representation is known as colon-hexadecimal.

The following is an IPV6 address in binary form:
00111111111111100010100100000000110100000000010100000000000000000
00000010101010100000000011111111111111100010100010011100010110 10

The 128-bit address is divided along 16-bit boundaries:
0011111111111110 0010100100000000 1101000000000101 0000000000000000
0000001010101010 0000000011111111 1111111000101000 1001110001011010

Each 16-bit block is converted to hexadecimal, and adjacent blocks are separated with colons. The result is:
3FFE:2900:D005:0000:02AA:00FF:FE28:9C5A

IPV6 representation can be further simplified by removing the leading zeros within each 16-bit block. However, each block must have at least a single digit. With leading zero suppression, the address becomes:
3FFE:2900:D005:0:2AA: FF: FE28:9C5A

Types of IPV6 addresses

IPV6 has three types of addresses: a *Unicast* address identifies a single interface within the scope of the type of unicast address, A *Multicast* address identifies multiple interfaces and *Anycast* address identifies multiple interfaces. An anycast address is used for communication from one source to one of multiple destinations, with delivery to a single interface.

Unicast addresses are again classified into five different categories. They are:

1. ***Global unicast addresses:*** Global unicast addresses are equivalent to public IPV4 addresses. They are globally routable and reachable on the IPV6 portion of the Internet, known as the IPV6 Internet. Global unicast addresses are unique across their scope, which is the entire IPV6 Internet.
2. ***Link-local addresses:*** Nodes use link-local addresses when communicating with neighboring nodes on the same link, also known as a subnet.
3. ***Site-local addresses:*** Private intranets that do not have a direct, routed connection to the IPV6 Internet can use site-local addresses without conflicting with global addresses. Site-local addresses are not reachable from other sites, and routers must not forward site-local traffic outside the site. The scope of a site-local address is a site.
4. ***Special IPV6 addresses:*** the special IPV6 addresses are:
   a. *Unspecified address:* The unspecified address (0:0:0:0:0:0:0:0 or::) indicates the absence of an address. The unspecified address is never assigned to an interface or used as a destination address. They are used as a source address for packets attempting to verify the uniqueness of a tentative address.
   b. *Loopback address:* The loopback address (0:0:0:0:0:0:0:1 or::1) identifies a loopback interface. This address enables a node to send packets to itself. Packets addressed to the loopback address are never sent on a link or forwarded by an IPV6 router.
5. ***Compatibility addresses:*** these addresses aid in the transition from IPV4 to IPV6. The following are the different compatibility addresses.
   a. IPV4-compatible address: The IPV4-compatible address, 0:0:0:0:0:0:

w.x.y.z or ::*w.x.y.z* (where w.x.y.z is the dotted decimal representation of a public IPV4 address), is used by IPV6/IPV4 nodes that are communicating using IPV6. IPV6/IPV4 nodes are nodes with both IPV4 and IPV6 protocols.

   b. *IPV4-mapped address:* The IPV4-mapped address, 0:0:0:0:0: FFFF:

w.x.y.z or:: FFFF: w.x.y.z, represents an IPV4-only node to an IPV6 node. IPV4-mapped addresses are used for internal representation only. The IPV4-mapped address is never used as a source or destination address of an IPV6 packet. IPV6 for Windows Server 2003 and Windows XP does not support IPV4-mapped addresses.

c. *6to4 address:* The 6to4 address is used for communicating between two nodes running both IPV4 and IPV6 over the Internet. 6to4 address can be formed by combining the global prefix 2002::/16 with the 32 bits of a public IPV4 address of the node, forming a 48-bit prefix.
d. *ISATAP address:* The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) defines ISATAP addresses used between two nodes running both IPV4 and IPV6 over a private intranet. ISATAP addresses use the locally administered interface ID:0:5EFE:w.x.y.z in which w.x.y.z is any unicast IPV4 address, public or private.
e. *Teredo address:* The Teredo address is used for communicating between two nodes running both IPV4 and IPV6 over the Internet when one or both of the endpoints are located behind an IPV4 network address translation (NAT) device.

IPV6 Multicast Addresses

IPV6 multicast addresses have the first eight bits fixed at 1111 1111. Therefore, the address prefix for all IPV6 multicast addresses is FF00::/8. Beyond the first eight bits, multicast addresses include additional structure to identify flags, their scope, and the multicast group.

IPV6 Addresses for a Host

An IPV6 host has multiple IPV6 addresses even with a single interface. IPV6 hosts typically have at least two addresses with which they can receive packets. They are: a link-local address for local link traffic and a routable site-local or global address.

IPV6 Addresses for a Router

An IPV6 router is assigned the following unicast and anycast addresses: A link-local address for each interface, Unicast addresses for each interface, A Subnet-Router anycast address, Additional anycast addresses (optional) and the loopback address (::1) for the loopback interface.

Additionally, each router listens for traffic on the following multicast addresses: The interface-local scope, all-nodes multicast address (FF01::1), The interface-local scope, all-routers multicast address (FF01::2), The link-local scope, all-nodes multicast address (FF02::1), The link-local scope, all-routers multicast address (FF02::2), The site-local scope, all-routers multicast address (FF05::2), The solicited-node address for each unicast address on each interface, The multicast addresses of joined groups on each interface.

Comparing IPV4 and IPV6 Addressing

Table 6.3 lists IPV4 addresses and addressing concepts and their IPV6 equivalents.

Table 6.3: Comparison of IPV4 and IPV6 Addressing

IPv4 Address	IPv6 Address
Internet address classes	Not applicable in IPv6
IPv4 multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses: network broadcast, subnet broadcast, all-subnets directed broadcast, limited broadcast	Not applicable in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IPv4 addresses	Global unicast addresses
Private IPv4 addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Site-local addresses (FEC0::/10)
APIPA addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)
Address syntax: dotted decimal notation	Address syntax: colon hexadecimal format with suppression of leading zeros and zero compression. Embedded IPv4 addresses are expressed in dotted decimal notation.
Address prefix syntax: prefix length or dotted decimal (subnet mask) notation	Address prefix syntax: prefix length notation only

SELF-ASSESSMENT QUESTIONS – 2

6. Internet addressing and forwarding are important components of _____
7. In IPV4, addresses are _____bits in length.
8. In IPV6, addresses are _____bits in length.
9. Field ensure that datagrams do not circulate_____forever in the network.
10. Addresses which are used for one-to-one communication is known as _____
11. Addresses used for one-to-everyone on a subnet communication is called _____
12. In IPV6,_____protocol reports errors in delivery or forwarding.
13. _____is a set of ICMPv6 messages and processes that determine relationships between neighboring nodes.
14. Nodes use _____addresses when communicating with neighboring nodes on the same link.
15. Addresses which aid in the transition from IPV4 to IPV6 is known as _____.

6. SUMMARY

Let us recapitulate the important concepts discussed in this unit:

- A network layer can provide connectionless and connection-oriented services between two hosts.
- Computer networks that provide only a connection-oriented service at the network layer is called *virtual-circuit (VC) networks* and computer networks that provide only a connectionless service at the network layer are called *datagram networks.*
- The messages that the end systems send into the network to initiate or terminate a VC, and the messages passed between the routers to set up the VC are known as signaling messages, and the protocols used to exchange these messages are often referred to as signaling protocols.
- IPV4 is a connectionless protocol and is unreliable. It is primarily responsible for addressing and routing packets between hosts.
- IPV6 is a routable protocol that addresses, routes, fragments, and reassembles packets.
- *Internet Control Message Protocol for IPV6 (ICMPv6)* reports errors in delivery or forwarding and provides a simple echo service for troubleshooting.
- Neighbor Discovery (ND) is a set of ICMPv6 messages and processes that determine relationships between neighboring nodes.
- Multicast Listener Discovery (MLD) is a set of ICMPv6 messages exchanged by routers and nodes, enabling routers to discover the set of IPV6 multicast addresses for which there are listening nodes for each attached interface

5. TERMINAL QUESTIONS

1. Differentiate between Virtual circuits and Datagram networks.
2. Write short notes on virtual circuits.
3. Describe IPV4 Addressing.
4. Explain IPV6 Addressing.
5. Which are the different types of IPV6 addresses? Explain.

6. ANSWERS

Self-Assessment Questions

1. Virtual circuit network (VC)
2. Datagram Networks
3. (a) True
4. Signaling messages
5. Datagram networks
6. Internet Protocol (IP)
7. 32
8. 128
9. Time-to-live (TTL)
10. Unicast
11. Broadcast
12. ICMPV6 (Internet Control Message Protocol for IPV6)
13. ND (Neighbor Discovery)
14. Link-local
15. Compatibility Addresses

Terminal Questions

1. Computer networks that provide only a connection-oriented service at the network layer is called *virtual-circuit (VC) networks*; computer networks that provide only a connectionless service at the network layer are called *datagram networks.* (Refer section 2 for more details).
2. Networks having connection-oriented services in the network layer are called Virtual Circuit networks and these network layer connections are called virtual circuits (VCs).

Let's now consider how a VC service can be implemented in a computer network. (Refer section 2 for more details).

3. IPV4 is a connectionless protocol and is unreliable. It is primarily responsible for addressing and routing packets between hosts. A higher layer protocol such as TCP or an application protocol must acknowledge delivered packets and recover lost packets if required. (Refer section 3.1 for more details)
4. IPV6 is a routable protocol that addresses, routes, fragments, and reassembles packets. IPV6 is a connectionless, unreliable datagram protocol that is primarily responsible for addressing and routing packets between hosts. (Refer section 3.2 for more details).
5. IPV6 has three types of addresses: a *Unicast* address identifies a single interface within the scope of the type of unicast address, A *Multicast* address identifies multiple interfaces and *Anycast* address identifies multiple interfaces. An anycast address is used for communication from one source to one of multiple destinations, with delivery to a single interface. Unicast addresses are again classified into five different categories. (Refer section 3.2 for more details).

References:

- Andrew S Tanenbaum, David J. Wetherall, "*Computer Networks*," Fifth edition.
- Larry L. Peterson, Bruce S. Davie, "Computer *Networks – a Systems Approach*," Fifth edition.
- James F. Kurose, Keith W. Ross, *"Computer Networking – A top-down approach*," Sixth edition.
- Behrouz A. Forouzan, Sophia Chung Fegan, "*Data Communication and Networking*," Fourth edition.
- William Stallings, *"Computer Networking with Internet Protocols and Technology,"* Third edition.