Module 7

Internet And Internet Protocol Suite

Lesson

23

IPv6

Version 1 ECE , IIT Kharagpur

LESSON OBJECTIVE

General

The lesson will explain a more advanced network layer protocol, i.e. the Internet Protocol version 6

Specific

The focus areas of this lesson are:

1. the next generation IP
2. addressing in IPv6
3. packet formats of IPv6

7.3.0 INTRODUCTION

The network layer protocol in the Internet is currently IPv4. IPv4 provides the host-host communication systems in the Internet. Although IPv4 is well designed, data communications has evolved a lot since it was introduced in the 1970s. IPv4 has some deficiencies that make it unsuitable for the fast growing Internet.

IPv4 has a two level address structure (*netid* and *hostid*) categorized into five classes which is an inefficient use of the address space.

The modern internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the IPv4 design.

The internet must accommodate encryption and authentication of data. IPv4 does not provide any security measure.

Internet Protocol version 6 (IPv6) or Internetworking Protocol, next generation (IPng) was proposed and is now a standard.

The next generation IP or IPv6 has some advantages over IPv4 as follows:

Larger Address space is provided in IPv6. An IPv6 address is 128 bits long. Compared with the 32-bit address of IPv4 this amounts to a huge (2^{96}) increase in the address space. This was done so that in the future when household appliances also become a part of the Internet they can have sufficient number of addresses.

Better header format. Ipv6 uses a new header format in which options are separated from the base header and inserted as required. This simplifies the routing process.

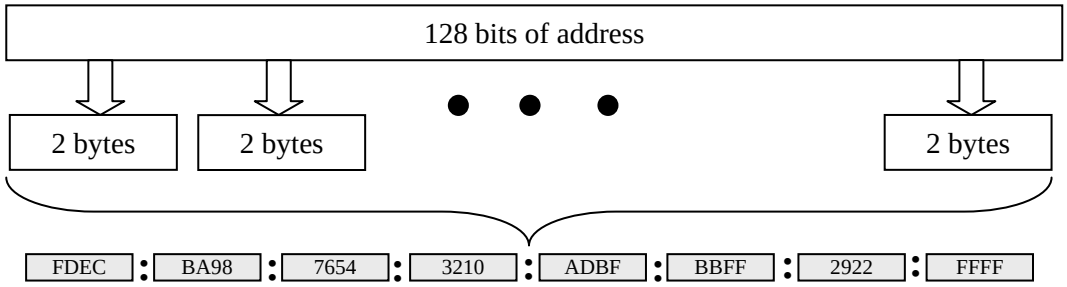
Support for more security. The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

New Options. Ipv6 has new options for additional functionalities.

Allowance for extension. Ipv6 is designed so that the protocol may be extended if required by new technologies.

7.3.1 IPV6 ADDRESSES:

An IPv6 address consists of 16 bytes. To make the address more readable, IPv6 specifies hexadecimal colon notation the use of which can be explained with the help of figure below



Abbreviation:

Although the IP address even in hexadecimal format is very long, many of the digits are zeros, hence we can abbreviate the address by omitting only the leading zeros of a section (four digits between two colons) as shown in the diagram. Further abbreviation is possible if there are consecutive sections consisting of zeros only. They can be removed altogether and replaced with a double semicolon.

CIDR notation

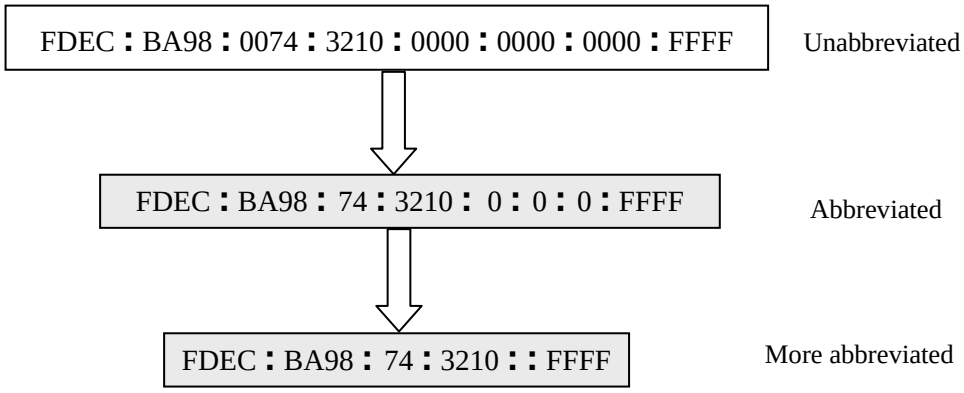
IPv6 allows classless addressing and CIDR notation. The diagram shows how to define a prefix of 60 bits using CIDR.

Categories of Addresses:

*Unicast—d*efines a single computer

Anycast—defines a group of computer with addresses that have the same prefix

Multicast—defines a group of computers that may or may not share the same prefix and may or may not be connected to the same physical network.



7.3.2 IPV6 PACKET FORMAT

Each packet consists of a packet header followed by the payload. The payload has two parts: optional extension header and data from upper layer. The base header is of 40 bytes and the payload may be up to 65536 bytes.

Base Header:

Version (4 bits)

It indicates the IP version number.

Priority (4 bits)

It specifies the priority of the packet with respect to traffic congestion.

Flow label (24 bits)

It is designed to provide special handling for a particular flow of data.

Payload length (16 bits)

It specifies total length of IP datagram excluding base header.

Next header (8 bits)

It specifies the header that follows the base header. It may be one of the optional extension headers or an upper layer protocol header.

Hop limit (8 bits)

Similar to the TTL field in the IPv4

Source address (128 bits)

Destination address (128 bits)

It generally specifies the final destination of datagram. However if source routing is used, this field contains the address of the next router

Extension headers:

The following extension headers have been defined in the IPv6 standard.

Hop-by-hop options header: defines special options that require hop-by-hop processing

Routing header: provides extended routing

Fragment header: contains fragmentation and reassembling information

Authentication header: provides packet integrity and authentication

Encapsulation security payload header: provides privacy

Destination options header: contains optional information to be examined by the destination node

Extension Headers:

Extension headers are supplied to provide extra information, but encoded in an efficient way. Six kinds of extension headers are defined at present. Each one is optional. But in case of more than one header is present, they must appear directly after the fixed base header, and preferably in the order listed.

Headers can have either a fixed format a variable number of variable-length fields. For these, each item is encoded as tuple (Type, Length, and Value). The *Type* is a 1-byte field telling which option this is. The choices are: skip the option, discard the packet, discard the packet and send back an ICMP packet, and the same as the previous one, except do not send ICMP packets for multicast addresses. The *Length* is also a 1-byte field informing about the length of the value (0 to 255 bytes). The *Value* is any information required, up to 255 bytes.

The **hop-by-hop** header is used to send information that all routers along the path must examine. Datagrams using this header are called Jumbograms.

The **routing** header enlists one or more routers that have to be visited on the way to the destination. Both strict routing (full path specified) and loose routing (selected routers are supplied) are available.

The **fragment** header deals with fragmentation in a way similar to IPv4. it holds the datagram identifier, fragment number, and a bit telling whether more fragments are coming. Unlike IPv4, only source host, and not the routers along the way, can fragment a packet. If an intermediate

router receives a packet that is too long, it simply discards it and sends an ICMP message back.

Authentication header provides a mechanism to the receiver of a packet to be sure of the sender. The encrypted security payload makes it possible to encrypt the contents of a packet so that only the intended recipient can read it.

The **destination option** header is intended for fields that need only be interpreted at the destination host.

Objective Questions

23.01 IPv6 has a ____ bit address field.

23.02 The base header in IPv6 is of ____ bytes.

23.03 The payload length is specified in ____ bits.

Subjective Questions

23.11 Compare IPv6 with IPv4.

23.12 What are the different categories of addresses in IPv6?

23.13 Describe the base header format in IPv6.

23.14 Discuss the extension headers in IPv6.

Level 2 Questions

23.21