Module 6

Internetworking

Lesson 2

Internet Protocol (IP)

Specific Instructional Objectives

At the end of this lesson, the students will be able to:

- Explain the relationship between TCP/IP and OSI model
- Explain different classes of IP addresses
- Explain the concept of subnetting and subnet masking
- Explain the ARP/RARP protocol
- Explain fragmentation and reassembly
- Explain the ICMP protocols
- State the key features of IPv6

6.2.1 Introduction

In the previous lesson we have discussed various devices required for internetworking. In addition to these devices, several protocols are required to provide necessary functionality for internetworking. The software that provide these protocols is known as Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP acts as a glue to link different types of LAN and WAN to provide Internet, a single integrated network for seamless communication. The IP provides unreliable, connectionless best-effort datagram delivery service, whereas TCP provides reliable, efficient and cost-effective end-to-end delivery of data. The relationship between TCP/IP and the OSI model is shown in Fig. 6.2.1. This lesson introduces the IP protocol and various issues related to it.

6.2.2 Addressing

To send a packet from a source node to a destination node correctly through a network, the packet must contain enough information about the destination address. It is also common to include the source address, so that retransmission can be done, if necessary. The addressing scheme used for this purpose has considerable effect on routing.

There are two possible approaches used for addressing; *flat* and *hierarchical*. In *flat addressing* every possible node is assigned a unique number. When a new node is added to the network, it must be given an address within the allowed address range. Addressing used in Ethernet is an example of flat addressing, where addresses (48-bits long) are allocated centrally, blocks of addresses are apportioned to manufactures, so that no two devices in the world will have the same address. Flat addressing has the advantage that if a node is moved from one location to another, it can retain its unique address.

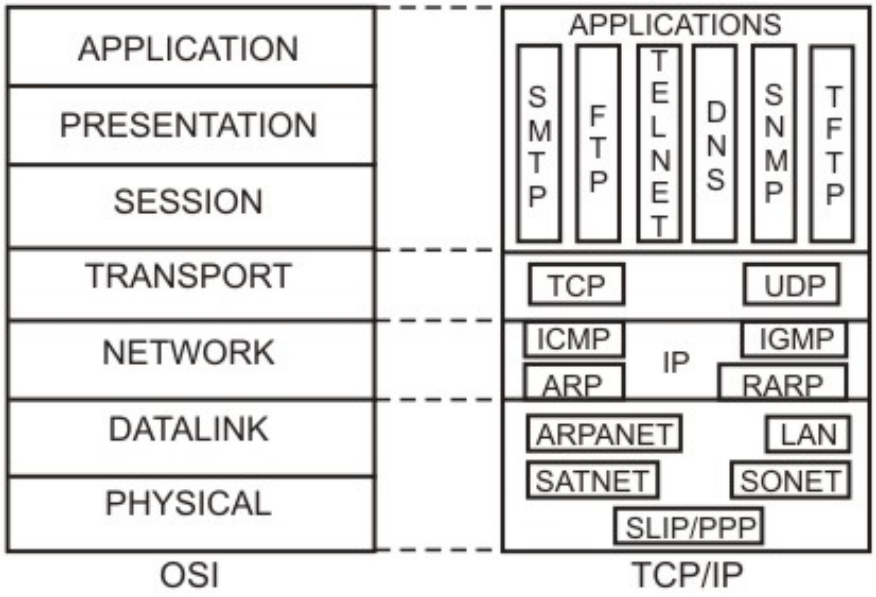


Figure 6.2.1 Relationship between the TCP/IP and the OSI model

In *hierarchical addressing*, each address consists of a number of fields; as each field is inspected, the packet is taken nearer to the destination. This is very similar to the addressing used in postal system. A significant advantage of hierarchical addressing is that it is possible to relate a hierarchical address structure to the topology of the network, so that routing is simplified. This scheme has the disadvantage that if a host moves from one location to another, a new address needs to be allocated to it, in the same manner that an address change is required as we change house.

6.2.2 IP Addressing

Every host and router on the internet is provided with a unique standard form of network address, which encodes its network number and host number. The combination is unique; no two nodes have the same IP addresses. The IP addresses are 32-bit long having the formats shown in Fig 6.2.2. The three main address formats are assigned with network addresses (net id) and host address (host id) fields of different sizes. The class A format allows up to 126 networks with 16 million hosts each. Class B allows up to 16,382 networks with up to 64 K hosts each. Class C allows 2 million networks with up to 254 hosts each. The Class D is used for multicasting in which a datagram is directed to multiple hosts. Addresses beginning with 11110 are reserved for future use. Network addresses are usually written in dotted decimal notation, such as 126.12.15.220, where each byte is written in decimal number corresponding to the binary value. Figure 6.2.3 illustrates how the dotted decimal representation is obtained for a particular IP address in binary form. Range of IP addresses for different classes is given in Fig. 6.2.4. Some IP addresses, which are used in special situations such as the same host, a host the same network, broadcast on the same network, broadcast on a distant network, or loopback are given in Fig. 6.2.5. This approach of representing IP addresses in terms of classes is known as *classful addressing*. In mid 90's another approach known as *classlees*

addressing has been proposed, which may supersede the existing classful addressing approach in future.

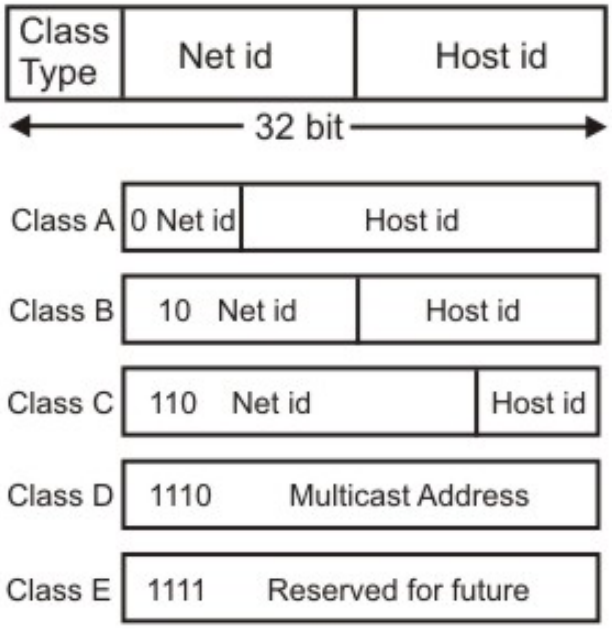


Figure 6.2.2 IP address formats

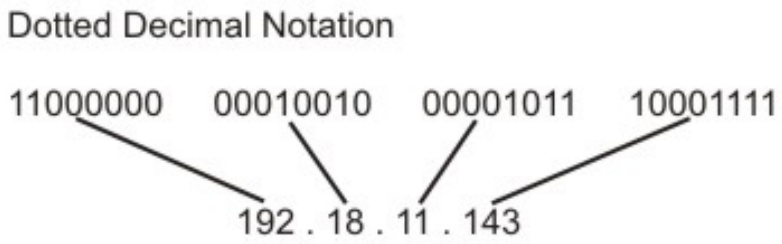


Figure 6.2.3 Dotted decimal representation

Range of Host Addresses		
Class A	1.0.0.0	to 127.255.255.255
Class B	128.0.0.0	to 191.255.255.255
Class C	192.0.0.0	to 233.255.255.255
Class D	244.0.0.0	to 239.255.255.255
Class E	240.0.0.0	to 247.255.255.255

Figure 6.2.4 Dotted decimal notation of the IP addresses

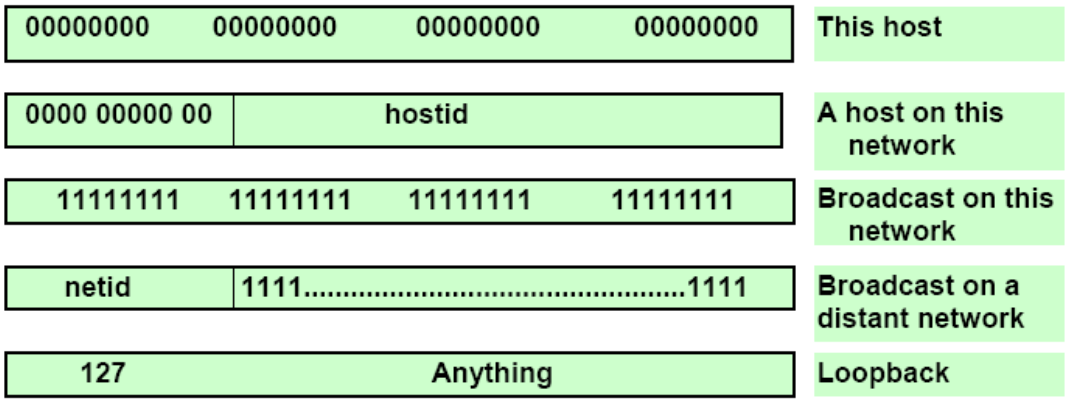


Figure 6.2.5 Special IP addresses

6.2.3 Subnetting

To filter packets for a particular network, a router uses a concept known as *masking*, which filters out the net id part (by ANDing with all 1's) by removing the host id part (by ANDing with all 0's). The net id part is then compared with the network address as shown in Fig. 6.2.6. All the hosts in a network must have the same network number. This property of IP addressing causes problem as the network grows. To overcome this problem, a concept known as *subnets* is used, which splits a network into several parts for internal use, but still acts like a single network to the outside world. To facilitate routing, a concept known as *subnet mask* is used. As shown in Fig. 6.2.7, a part of hostid is used as subnet address with a corresponding subnet mask. Subnetting reduces router table space by creating a three-level hierarchy; net id, subnet id followed by hosted.

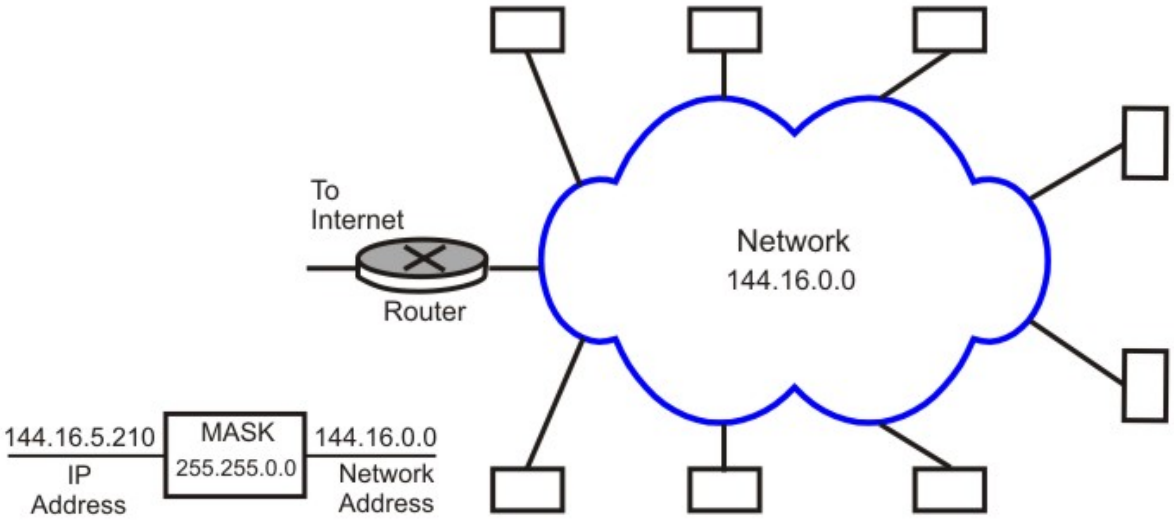


Figure 6.2.6 Masking with the help of router

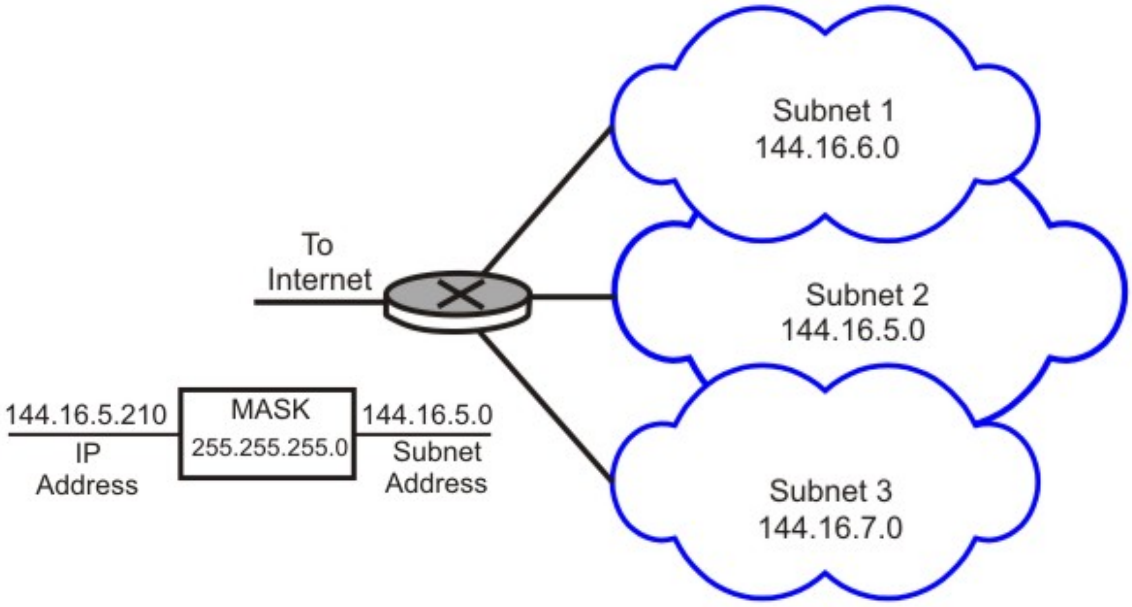


Figure 6.2.7 Subnet masking with the help of router

6.2.4 Network Address Translation (NAT)

With the increasing number of internet users requiring an unique IP address for each host, there is an acute shortage of IP addresses (until everybody moves to IPV6). The *Network Address Translation* (NAT) approach is a quick interim solution to this problem. NAT allows a large set of IP addresses to be used in an internal (private) network and a handful of addresses to be used for the external internet. The internet authorities has set aside three sets of addresses to be used as private addresses as shown in Table 6.2.1. It may be

noted that these addresses can be reused within different internal networks simultaneously, which in effect has helped to increase the lifespan of the IPV4. However, to make use of the concept, it is necessary to have a router to perform the operation of address translation between the private network and the internet. As shown in Fig. 6.2.8, the NAT router maintains a table with a pair of entries for private and internet address. The source address of all outgoing packets passing through the NAT router gets replaced by an internet address based on table look up. Similarly, the destination address of all incoming packets passing through the NAT router gets replaced by the corresponding private address, as shown in the figure. The NAT can use a pool of internet addresses to have internet access by a limited number of stations of the private network at a time.

Table 6.2.1 Addresses for Private Network

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

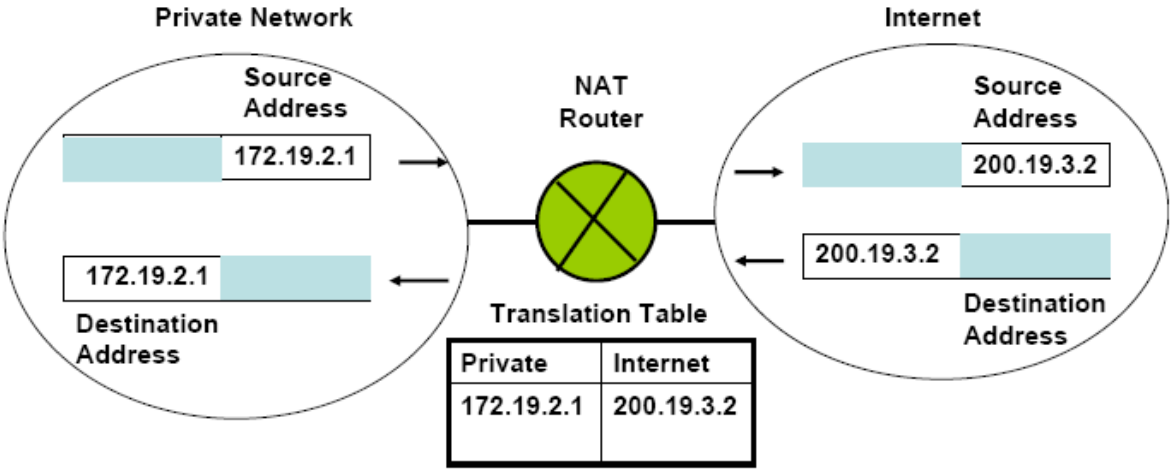


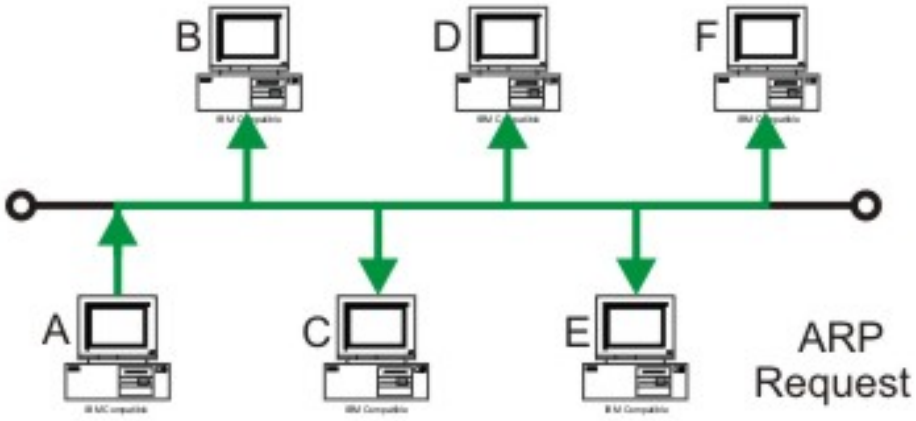
Figure 6.2.8 NAT Address translation

6.2.5 Address Resolution Protocol (ARP)

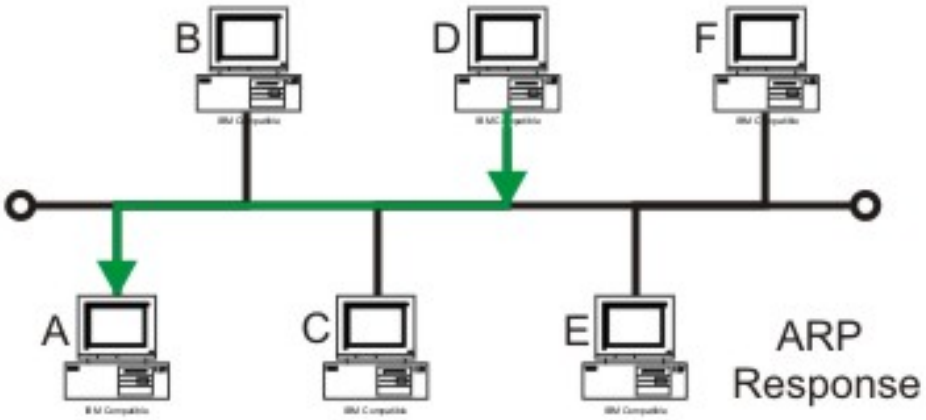
It may be noted that the knowledge of hosts' IP address is not sufficient for sending packets, because *data link hardware does not understand internet addresses*. For example, in an Ethernet network, the Ethernet controller card can send and receive using 48-bit Ethernet addresses. The 32-bit IP addresses are unknown to these cards. This requires a mapping of the IP addresses to the corresponding Ethernet addresses. This mapping is accomplished by using a technique known as *Address Resolution Protocol (ARP)*.

One possible approach is to have a *configuration file* somewhere in the system that maps IP addresses onto the Ethernet addresses. Although this approach is straightforward, maintaining an up-to0-date table has a high overhead on the system. Another elegant approach is to broadcast packet onto the Ethernet asking "*who owns the destination IP address*?". The destination node responds with its Ethernet address after hearing the request. This protocol of asking the question and getting the reply is called ARP (Addressing Resolution Protocol), which is widely used. ARP is a dynamic mapping approach for finding a physical address for a known IP address. It involves following two basic steps as shown in Fig. 6.2.9.

- An ARP request is broadcast to all stations in the network
- An ARP reply is an unicast to the host requesting the mapping



(a)



(b)

Figure 6.2.9 (a) ARP request with a broadcast to all the stations and
(b) ARP response is a unicast only to the requesting host

Various optimizations are commonly used to improve the efficiency of the ARP protocol. One possible approach is to use cache memory to hold the recently acquired frame containing the physical address. As a consequence, no broadcasting is necessary in near future. Figure 6.2.10 shows how an ARP packet is encapsulated into the data field of a MAC frame.

Reverse ARP (RARP)

The TCP/IP protocols include another related protocol known as reverse ARP, which can be used by a computer such as a diskless host to find out its own IP address. It involves the following steps:

- Diskless host A broadcasts a RARP request specifying itself as the target
- RARP server responds with the reply directly to host A
- Host A preserves the IP address in its main memory for future use until it reboots

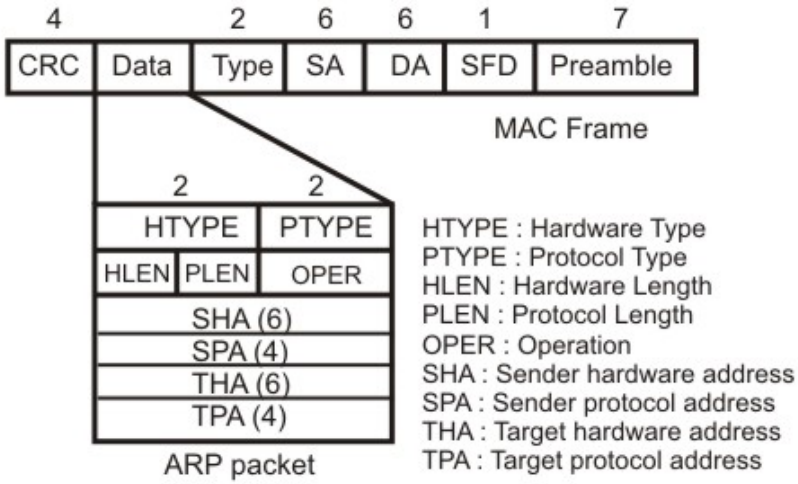


Figure 6.2.10 An ARP packet is encapsulated directly into the data field a MAC frame

6.2.6 IP Datagram

As we have mentioned earlier, IP is an unreliable and connectionless *best-effort* delivery service protocol. By best effort we mean that there is no error and flow control. However, IP performs error detection and discards a packet, if it is corrupted. To achieve reliability, it is necessary to combine it with a reliable protocol such as TCP. Packets in IP layer are called *datagrams.* The IP header provides information about various functions the IP performs. The IP header format is shown in Fig. 6.2.11. The 20 to 60 octets of header has a number of fields to provide:

- Source and destination IP addresses
- Non transparent fragmentation
- Error checking

- Priority
- Security
- Source routing option
- Route Recording option
- Stream identification
- Time stamping

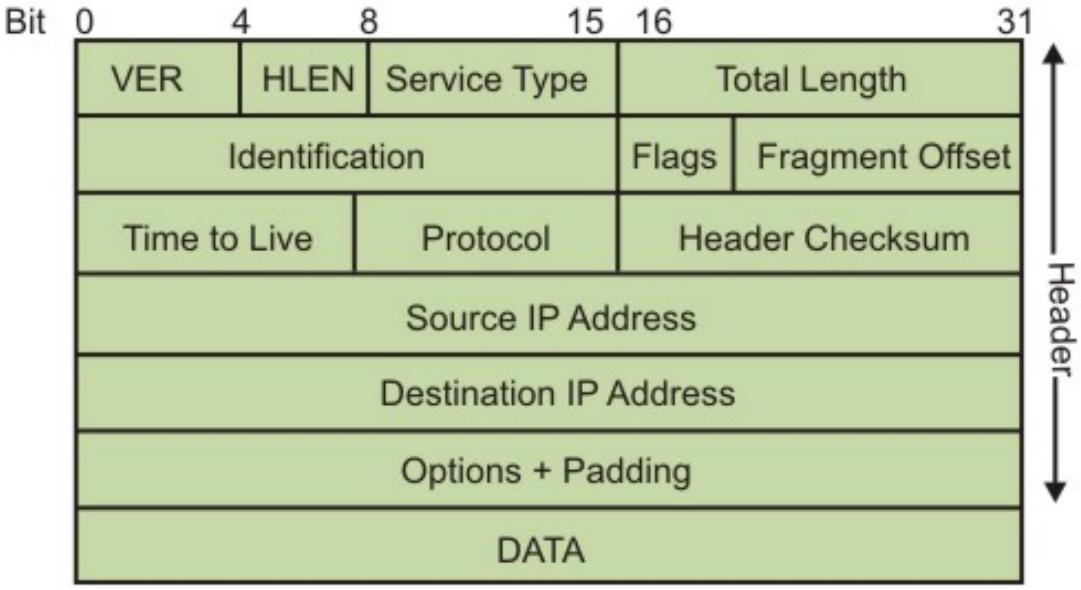


Figure 6.2.11 IP packet format

A brief description of each of the fields are given below:

- VER (4 bits): Version of the IP protocol in use (typically 4).
- HLEN (4 bits): Length of the header, expressed as the number of 32-bit words. Minimum size is 5, and maximum 15.
- Total Length (16 bits): Length in bytes of the datagram, including headers. Maximum datagram size is (2^{16}) 65536 bytes.
- Service Type (8 bits): Allows packet to be assigned a priority. Router can use this field to route packets. Not universally used.
- Time to Live (8 bits): Prevents a packet from traveling forever in a loop. Senders sets a value, that is decremented at each hop. If it reaches zero, packet is discarded.
- Protocol: Defines the higher level protocol that uses the service of the IP layer
- Source IP address (32 bits): Internet address of the sender.
- Destination IP address (32 bits): Internet address of the destination.
- Identification, Flags, Fragment Offset: Used for handling fragmentation.
- Options (variable width): Can be used to provide more functionality to the IP datagram
- Header Checksum (16 bits):

- Covers only the IP header.
- Steps:
  - Header treated as a sequence of 16-bit integers
  - The integers are all added using ones complement arithmetic
  - Ones complement of the final sum is taken as the checksum
  - Datagram is discarded in case of mismatch in checksum values

6.2.7 Multiplexing and Demultiplexing

IP datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, etc. The Protocol field in the datagram specifies the final destination protocol to which IP datagram to be delivered. When the datagram arrives at the destination, the information in this field is used to perform demultiplex the operation. The multiplexing and demultiplexing operations are shown in Fig. 6.2.12.

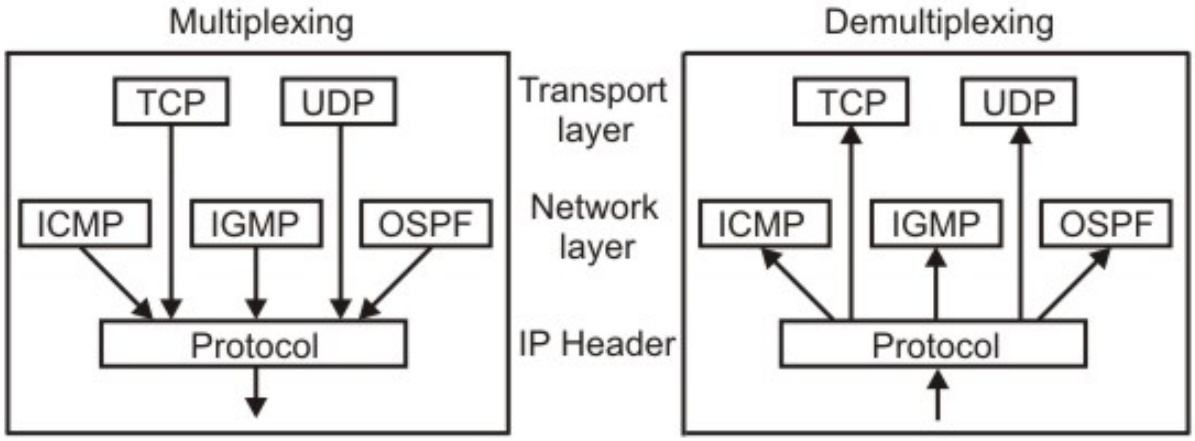


Figure 6.2.12 Multiplexing and demultiplexing in the IP layer

6.2.8 Fragmentation and Reassembly

Each network imposes a limit on maximum size, known as *maximum transfer unit* (MTU) of a packet because of various reasons. One approach is to prevent the problem to occur in the first place, i.e. send packets smaller than the MTU. Second approach is to deal with the problem using fragmentation. When a gateway connects two networks that have different maximum and or minimum packet sizes, it is necessary to allow the gateway to break packets up into fragments, sending each one as an internet packet. The technique is known as *fragmentation*. The following fields of an IP datagram are related to fragmentation:

- **Identification**: A16-bit field identifies a datagram originating from the source host.
- **Flags**: There are 3 bits, the first bit is reserved, the second bit is *do not fragment* bit, and the last bit *is more fragment* bit.
- **Fragmentation offset**: This 13-bit field shows the relative position of the segment with respect to the complete datagram measured in units of 8 bytes.

Figure 6.2.13 shows a fragmentation example, where a packet is fragmented into packets of 1600 bytes. So, the offset of the second fragmented packet is 1600/8 = 200 and the offset of the third fragmented packet is 400 and so on.

The reverse process, known as *reassembly*, which puts the fragments together, is a more difficult task. There are two opposing strategies for performing the re-assembly. In the first case, the fragmentation in one network is made transparent to any subsequent networks. This requires that packets to be reassembled before sending it to subsequent networks as shown in Fig. 6.2.14(a). This strategy is used in ATM. As re-assembly requires sufficient buffer space for storage of all the fragments, this approach has large storage overhead. To overcome this problem in the second strategy, re-assembly is done only at the ultimate destination. This approach does not require large buffer but additional fields are to be added to each packet for independent addressing and to indicate the fragment number as shown in Fig. 6.2.14(b).

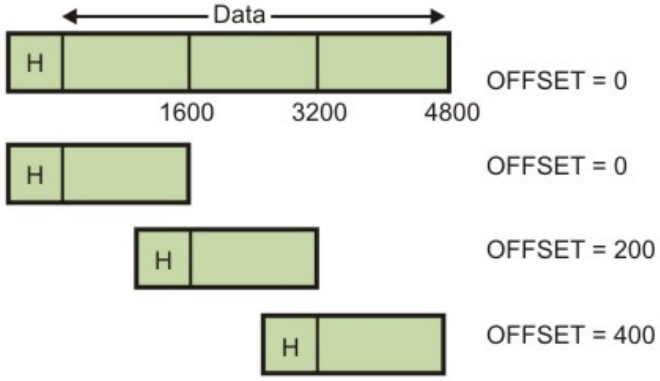
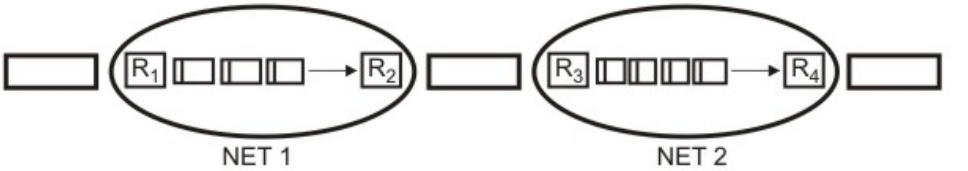
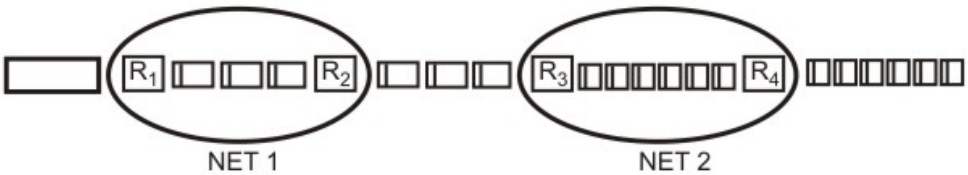


Figure 6.2.13 Fragmentation example



(a)



. (b)

Figure 6.2.14 (a) Transparent Fragmentation (ATM),
(b) Nontransparent fragmentation (IP)

6.2.9 ICMP

To make efficient use of the network resources, IP was designed to provide unreliable and connectionless best-effort datagram delivery service. As a consequence, IP has no error-control mechanism and also lacks mechanism for host and management queries. A companion protocol known as *Internet Control Message Protocol* (ICMP), has been designed to compensate these two deficiencies. ICMP messages can be broadly divided into two broad categories: error reporting messages and query messages as follows.

- Error reporting Messages: Destination unreachable, Time exceeded, Source quench, Parameter problems, Redirect
- Query: Echo request and reply, Timestamp request and reply, Address mask request and reply

The frame formats of these query and messages are shown in Fig. 6.2.15.

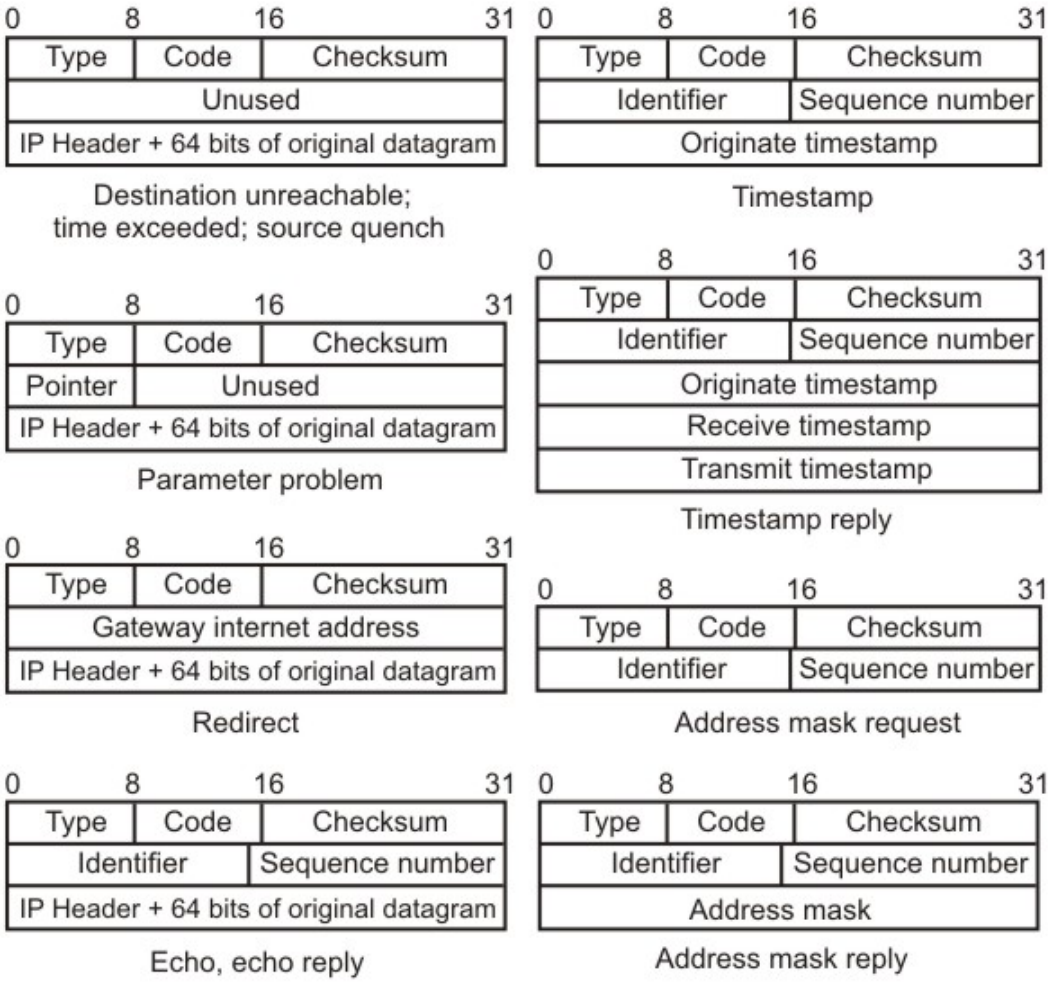


Figure 6.2.15 ICMP message formats

6.2.10 IPV6

The network layer that is present in use in commonly referred to as IPv4. Although IPv4 is well designed and has helped the internet to grow rapidly, it has some deficiencies, These deficiencies has made it unsuitable for the fast growing internet. To overcome these deficiencies, Internet Protocol, Version 6 protocol has been proposed and it has evolved into a standard. Important features of IPv6 are highlighted below:

- IPv6 uses 128-bit address instead of 32-bit address to provide larger address space
- Uses more flexible header format, which simplifies and speeds up the routing process
- Basic header followed by extended header
- Resource Allocation options, which was not present in IPv4
- Provision of new/future protocol options
- Support for security with the help of encryption and authentication
- Support for fragmentation at source

Review Questions

Q1.	Fill in the blanks :
(a)	Two possible addressing techniques are _____ addressing and _____ addressing.
(b)	Ethernet address is an example of _____ addressing while IP address is an example of _____ addressing.
(c)	The Class C address class can have _____ networks and about _____ hosts in each network.
(d)	The mapping of the IP address to the corresponding Ethernet Address is done by a protocol named as _____.

Ans:

Q1.	Fill in the blanks :
(a)	flat, hierarchical
(b)	Flat,hierarchical
(c)	254, 2 million
(d)	ARP

Q2.Why do you need ARP protocol?
Ans: Two machines on a network can communicate only if they know each other's physical address. So, IP address is not enough to deliver a packet to the destination node. It is necessary to know its physical (LAN) address. The ARP protocol allows a host to find out the physical address of a destination host on the same physical network, given only the IP address of the destination host.

Q3.What is the purpose of dotted decimal representation? Give dotted decimal representation of the IP address 11011101 10001111 11111101 00001111.
Ans: To represent the 32-bit IP address in short and easy to read form, Internet addresses are represented in decimal form with decimal points separating the bytes. This is known

as dotted decimal notation. For the given IP address the dotted decimal representation is 221.143.253.15.

Q4.How is masking is related to subnetting?
Ans: Masking is a process that extracts the physical network address part from the 32-bit IP address. When subnetting is done, the masking is performed to get the subnetwork address rather than the network address.

Q5. What is the function of NAT?
Ans: The *Network Address Translation* (NAT) approach is a quick interim solution to this problem of acute shortage of IP addresses for individual hosts in IPv4. NAT allows a large set of IP addresses to be used in an internal (private) network and a handful of addresses to be used for the global internet.

Q6. What is the function of the ICMP?
Ans: The ICMP has been designed as companion protocol to compensate two important deficiencies of the IP protocol, namely error-control mechanism and the lack of mechanism for host and management queries.