UNIT 2 IP : INTERNET PROTOCOL

Structure

2.0 INTRODUCTION

In UDP IP provides an unreliable, connectionless datagram delivery service. There is no guarantee that an IP datagram will reach the destination. If a router temporarily runs out of buffers, IP runs an algorithm and throws away the datagram and tries to send an ICMP message back to the source. Required reliability is provided by TCP.

IP does not maintain any state information about successive datagrams. Each datagrams is handled independently from all other datagrams. If a source sends two consecutive datagrams (A and B) to the same destination, each is routed independently and can take different routes, with B arriving before A. In this unit we will discuss IP in quite detail.

2.1 OBJECTIVES

After going through this unit, you will be able to understand the following:

- Frame format of IP
- IP routing mechanism

2.2 IP HEADER

The Internet Protocol (IP), defined by IETF (Internet Engineering Task Force) RFC791, is the routing layer datagram service of the TCP/IP suite. All other protocols within the TCP/IP suite, except ARP and RARP, use IP to route frames from host to host. The IP frame header contains routing information and control information associated with datagram delivery.

The IP header structure is as follows:

Ver.	IHL	Type of service	Total length	
		Identification	Flags	Fragment offset
Time to live		Protocol	Header checksum	
Source address				
Destination address				
Option + Padding				
Data				

Figure 1 : IP header structure

Explanation of the header structure

Version

Version field keeps track of which version of the protocol, the datagram belongs to:

IHL

Internet Header length is the length of the Internet header in 32-bit words. It Points to the beginning of the data. The minimum value for a correct header is 5 which applies when no options are present.

Type of Service

Indicates the quality of service desired by the host from the subnet. Various combinations of reliability and speed are possible.

For digitised voice, fast delivery beats accurate delivery. For file transfer, error free transmission is more important than fast transmission.

Total Length

Length of the datagram measured in bytes, including the Internet header and data. This field allows the length of a datagram to be up to 65,535 bytes, although such long datagrams are impractical for most hosts and networks. All hosts must be prepared to accept datagrams of up to 576 bytes, regardless or whether they arrive whole or in fragments. It is recommended that hosts send datagrams larger than 576 bytes only if the destination is prepared to accept the larger datagrams. With future gigabits larger datagrams will be needed.

Identification

Identifying value assigned by the sender to aid in assembling the fragments of a datagram.

All the fragments of a datagram contain the same identification value. Next comes an unused bit and then two bit 1 fields. DF Stands for Don't Fragment. It is an order to

routers not fragment the datafram because the definiation is incapatable of putting the pieces back together again.

MF stands for More Fragment. All fragments except the last one have this bit set. It is needed to known when all fragments of a datagram have arrived.

Fragment offset

Indicates where this fragment belongs in the datagram. The fragment offset is measured in units of 8 bytes (64 bits). The first fragment has offset zero.

Since 13 bits are provided there is a maximum of 8192 fragments per datagram, giving a maximum datagram length of 651536 bytes.

Time to live

Indicates the maximum time the datagram is allowed to remain in the Internet system. If this field contains the value zero, the datagram must be destroyed. This field is modified in Internet header processing. The time is measured in units of seconds, allowing a maximum lifetime of 255 sec. It must be decremented on each hop and is supposed to be decremented multiple times when queued for a long time in a router. In practice, it just counts hops.

Protocol

Indicates the next level protocol used in the data portion of the Internet datagram. It still tells the network layer which transport process to give it to. TCP is one possibility, but so are UDP and some others.

Header checksum

A checksum verifies the header only. Since some header fields change, e.g., 'Time To Live', this is recomputed and verified at each point that the Internet header is processed.

Source address/destination address

32 bits each. A distinction is made between names, addresses and routes. A name indicates an objects to be sought. An address indicates the location of the object. A route indicates how to arrive at the object. The Internet protocol deals primarily with addresses. It is the task of higher level protocols (such as host-to-host or application) to make the mapping from names to addresses. The Internet module maps Internet addresses to local net addresses. It is the task of lower level procedures (such as local net or gateways) to make the mapping from local net addresses to routes. It indicates the network number and host number.

Options

Options may or may not appear in datagrams. They must be implemented by all IP modules (host and gateways). What is optional is their transmission in any particular datagram, not their implementation. In some environments, the security option may be required in all datagrams. The option field is variable in length. There may be zero or more options.

2.2.1 IP Addresses

To understand IP address format the following definitions are important.

- **Physical network**: A collection of computers, communications devices, wiring, etc. that communicate directly with one another (e.g., Ethernet, Token Ring).

- **Host** : A computer, connected to a physical network, that exchanges information with another computer via TCP/IP.
- **Gateway:** A computer that interconnects two or more physical networks and that routes TCP/IP information among those networks (accurately referred to as a **router**).
- IP addresses are unique, 32-bit addresses;
- correspond to connections, not hosts (generally, move connection ==>change IP address);
- are referenced by humans via dotted decimal (or dotted quad) notation, one number per 8 bits (1 octet or byte), e.g., 129.192.6.7.
- consist of three primary classes A, B and C (Class D is for multicast) of the form [netid, hostid].

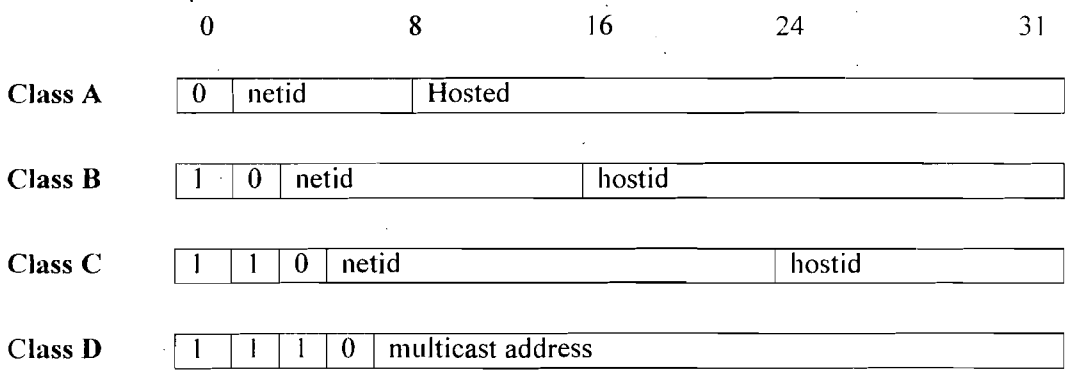

Figure 2: Class Formats

In order to communicate on the Internet, each network adapter card on a computer must be assigned an *unique* IP Address. This is an unique four-part, period delimited, address called an *Internet Protocol (IP) address or IP number.*

www.xxx.yyy.zzz

The first two might be reserved for any organization/institution/university etc. for example, IGNOU. The third part yyy of the address identifies what *subnet* the computer is in. In some organizations it is determined by what building/department the computer is located. For example School of Computer Science. Although more than one subnet number may be in use within a single building, no single subnet number can be used in one building if it is already in use in another. The final part of the address zzz is assigned arbitrary number to a given machine in the local subnet so that the entire number is unique.

2.2.2 . IP Address Components

Like other network layer protocols, the IP addressing scheme is integral to the process of routing IP data through an internetwork.

Each host on a TCP/IP network is assigned a unique 32-bit logical address. The IP address is divided into two main parts; the Network Number and the Host Number.

The network number identifies the network and must be assigned by the Internet Network Information Center (InterNIC) if the network is to be part of the Internet.

The host number identifies a host in the network and is assigned by the local network administrator.

2.2.3 IP Address Format & Classes

IP Address Format

Let us examine now IP address format and IP address Classes in detail.

The 32-bit IP address is grouped 8 bits at a time, each group of 8 bits is an octet. Each of the four octets are separated by a dot, and represented in decimal format, this is known as dotted decimal notation. Each bit in an octet has a binary weight (128, 64, 32, 16, 8, 4, 2, 1). The minimum value for an octet is 0 (all bits set to 0), and the maximum value for an octet is 255 (all bits set to 1).

The following figure shows the basic format of a typical IP address:

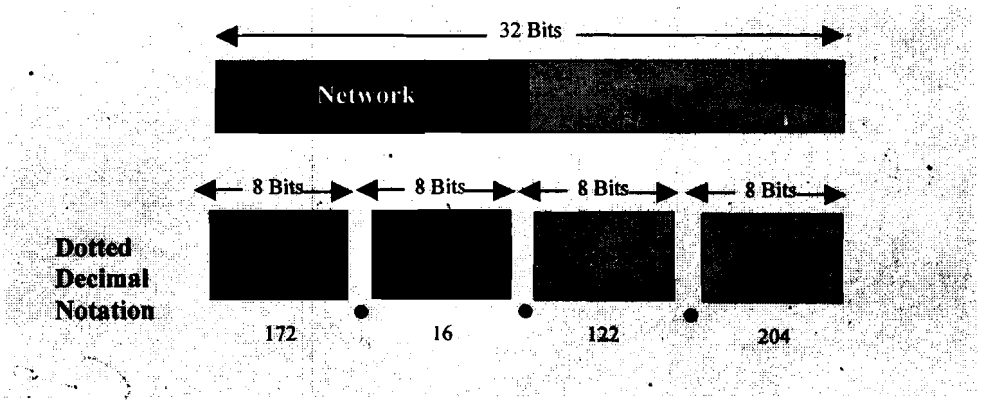

Figure 3: Basic format of IP address

IP Address Classes

IP addressing supports three different commercial address classes; Class A, Class B, and Class C.

In a class A address, the first octet is the network portion, so the class A address of, 10.1.25.1, has a major network address of 10. Octets 2, 3, and 4 (the next 24 bits) are for the hosts. Class A addresses are used for networks that have more than 65,536 hosts (actually, up to 16,581,375 hosts!).

In a class B address, the first two octets are the network portion, so the class B address of, 172.16.122.204, has a major network address of 172,16. Octets 3 and 4 (the next 16 bits) are for the hosts, Class B addresses are used for networks that have between 256 and 65,536 hosts.

In a class C address, the first three octets are the network portion. The class C address of, 193.18.9.45, has a major network address of 193.18.9. Octet 4 (the last 8 bits) is for hosts. Class C addresses are used for networks with less than 254 hosts.

2.2.4 IP Routing

When a router receives a packet, it makes a routing decision based on the destination address portion of the packet. It then looks up the destination address in its routing table. If the destination address is within a known network/subnetwork, the router forwards the packet to the next hop gateway for that destination network/subnetwork. Once the packet leaves the router, it is the responsibility of the next hop gateway to forward the packet to its final destination. If the router does not have the destination network in its routing table, it may forward the packet to a predetermined default gateway if configured and let the default gateway handle getting the packet to the destination

network or it will drop the packet and inform the sending host that the network is not reachable.

The routing table is list of networks that router knows about. It can learn these routes by 3 means: a routing protocol such as: RIP, IGRP, and OSPF, a static route that has been manually been set by a network administrator, or by being directly connected to that network on one of its interfaces.

The routing table will contain many pieces of information about the learned network, but the main information is the network address and the next hop gateway.

The network address can be either a full class network address or a subnetwork address, depending on the netmask being used. The next hop gateway is the IP address of the gateway to hand off the outbound packet to.

Keep in mind that all of the routers must know of a way to reach each other. The receiving host must have a path to get back to the sending host in order for data to pass.

- Both hosts and routers participate in routing
- **Direct routing:** Transmitting a datagram from one computer directly to another on same physical network.
- **Indirect routing**: Destination host not on same network --> datagram sent to a router for delivery.
- Routing based on IP routing table of the form **(netmask, net-address, next-hop)**

1. Extract destination IP address **ipdest** from datagram
2. Starting at the beginning of the routing table (and for each entry)
   a. Calculate network portion of **ipdest --> ipnet** =AND **(netmask, ipdest)**
   b. If **ipnet** equals **net-address**, send datagram to **next-hop**
   c. If **ipnet** does not equal **net-address**, repeat steps 1 and 2
   d. If no table entry matches, declare a routing error

2.2.5 IP Subnet Addressing

All Classes of IP networks can be divided into smaller networks called subnetworks (or subnets).

Dividing the major class network is called subnetting. Subnetting provides network administrators with several benefits. It provides extra flexibility, makes efficient use of network address utilization, and contains broadcast traffic because a broadcast will not cross a router.

Subnets are under local administration. As such, the outside world sees an organization as a single network, and has not detailed knowledge of the organization's internal network structure.

A given network address can be broken up into many subnetworks. For example, 172.16.1.0, 172.16.2.0, 172.16.3.0, and 172.16.4.0 are all subnets of the Class B network 171.16.0.0.

2.2.6 Subnet Mask

A subnet address is created by "borrowing" bits from the host field and designating them as the subnet field. The number of borrowed bits is variable and specified by the subnet mask.

The following figure shows how bits are "borrowed" from the host address field to create the subnet address field:

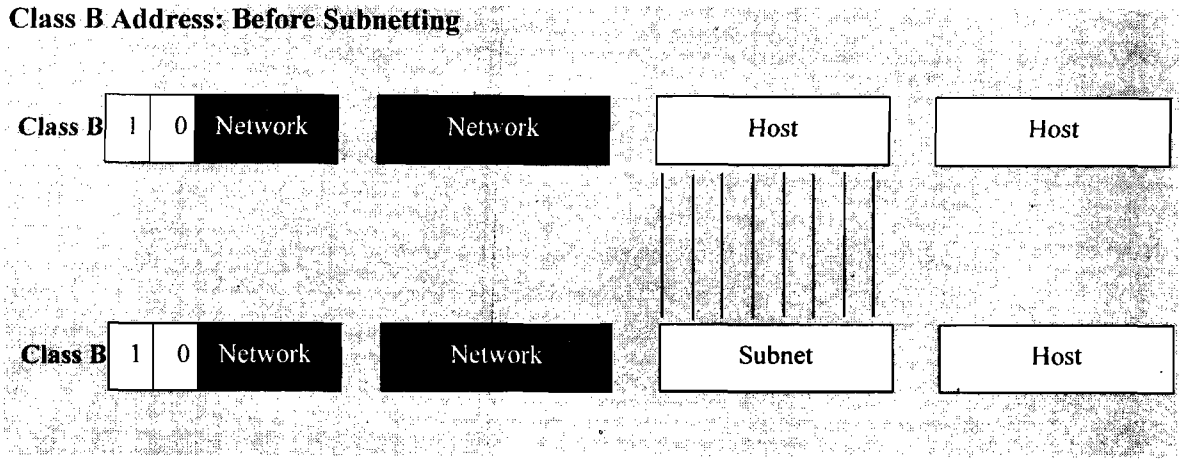

Figure 4: Class B Address: Before & After Subnetting

Subnet masks use the same format and representation technique as network mask format, the subnet mask has binary 1s in all bits specifying the network and subnetwork fields, and binary 0s in all bits specifying the host field.

The following figure shows a sample subnet mask:

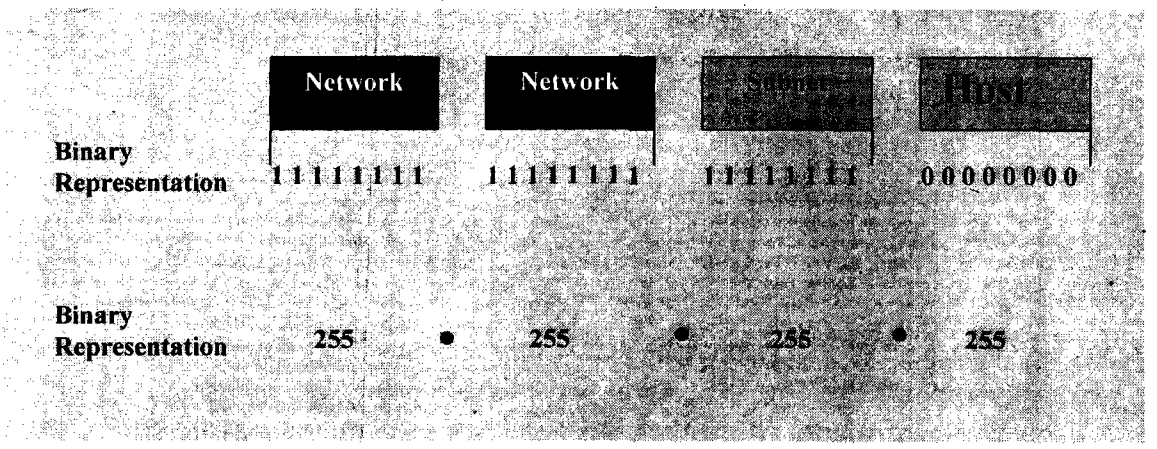

Figure 5.: Subnet mask for Class B address

Check Your Progress

1) What are the various flags in IP header?

.....

.....

2) Explain the various class formats of IP address.

.....

.....

3) What do you understand by IP address?

.....

.....

2.3 SUMMARY

IP (Internet Protocol) is an unreliable (delivery not guaranteed), connectionless (packets are independent of one another) and best effort (attempt to delivery packets) packet delivery mechanism. Its basic unit is datagram (upto 65,535 bytes). This unit mainly covered topics related to IP addressing routing etc.

2.3 MODEL ANSWERS

Question	1	-	Refer to 2.2
Question	2	-	Refer to 2.2.3
Question	3	-	Refer to 2.2.1