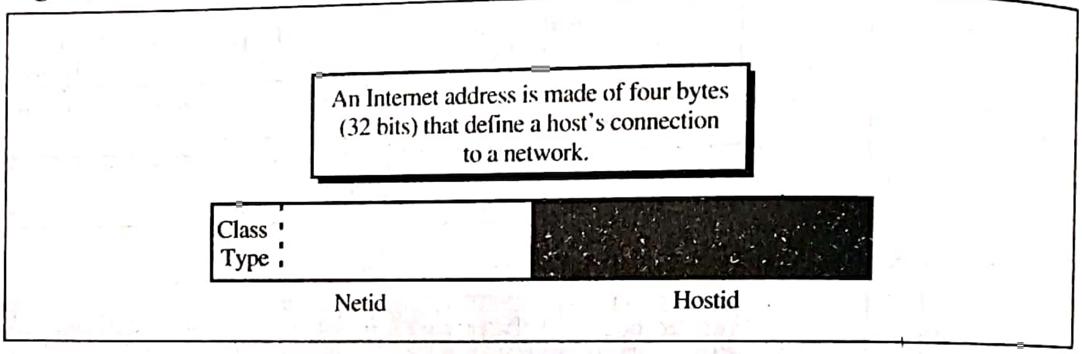
24.3 ADDRESSING

In addition to the physical addresses (contained on NICs) that identify individual devices, the Internet requires an additional addressing convention: an address that identifies the connection of a host to its network.

Each **Internet address** consists of four bytes (32 bits), defining three fields: class type, netid, and hostid. These parts are of varying lengths, depending on the class of the address (see Figure 24.4).

Figure 24.4 *Internet address*



Classes

There are currently five different field-length patterns in use, each defining a **class of address.** The different classes are designed to cover the needs of different types of organizations. For example, class A addresses are numerically the lowest. They use only one byte to identify class type and netid, and leave three bytes available for hostid numbers. This division means that class A networks can accommodate far more hosts than can class B or class C networks, which provide two- and one-byte hostid fields, respectively. Currently both class A and class B are full. Addresses are available in class C only.

Class D is reserved for **multicast addresses. Multicasting** allows copies of a datagram to be passed to a select group of hosts rather than to an individual host. It is similar to **broadcasting,** but, where broadcasting requires that a packet be passed to all possible destinations, multicasting allows transmission to a selected subset. Class E addresses are reserved for future use. Figure 24.5 shows the structure of each **IP address class.**

Example 24.1

What is the class of each of the following addresses?

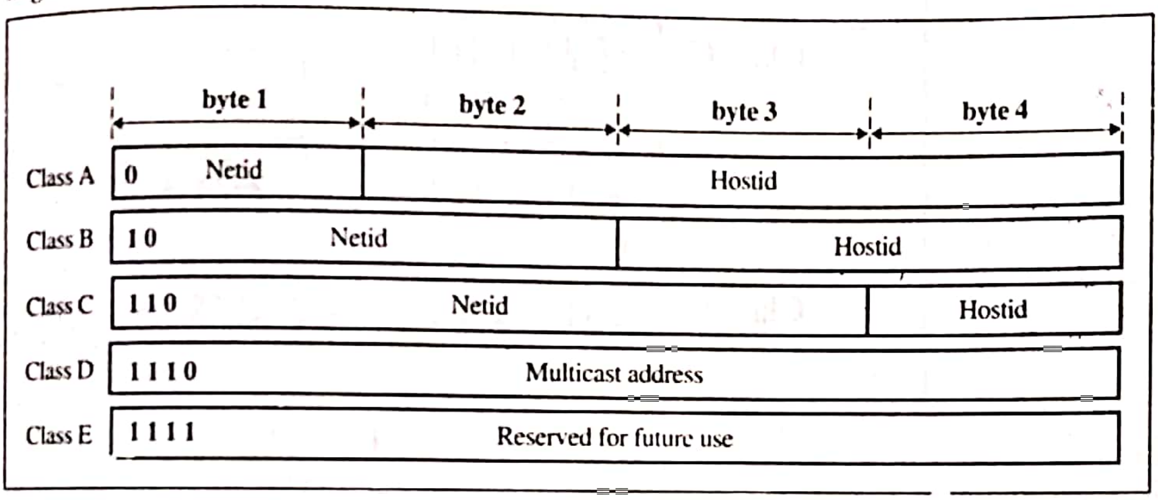
a. 10011101 10001111 11111100 11001111
b. 11011101 10001111 11111100 11001111
c. 01111011 10001111 11111100 11001111
d. 11101011 10001111 11111100 11001111
e. 11110101 10001111 11111100 11001111

Solution

The first bits define the class:

a. Class B
b. Class C
c. Class A
d. Class D
e. Class E

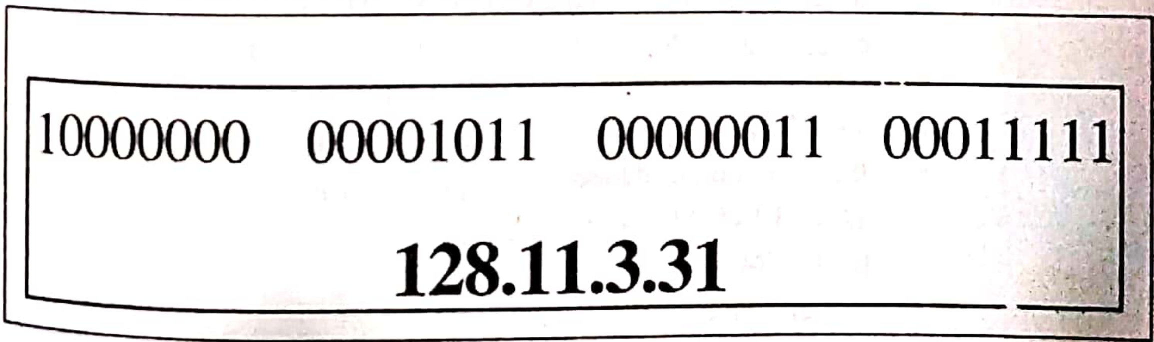
Figure 24.5 *Internet classes*



Dotted-Decimal Notation

To make the 32-bit form shorter and easier to read, Internet addresses are usually written in decimal form with decimal points separating the bytes—**dotted-decimal notation**. Figure 24.6 shows the bit pattern and decimal format of a possible address.

Figure 24.6 *IP addresses in decimal notation*



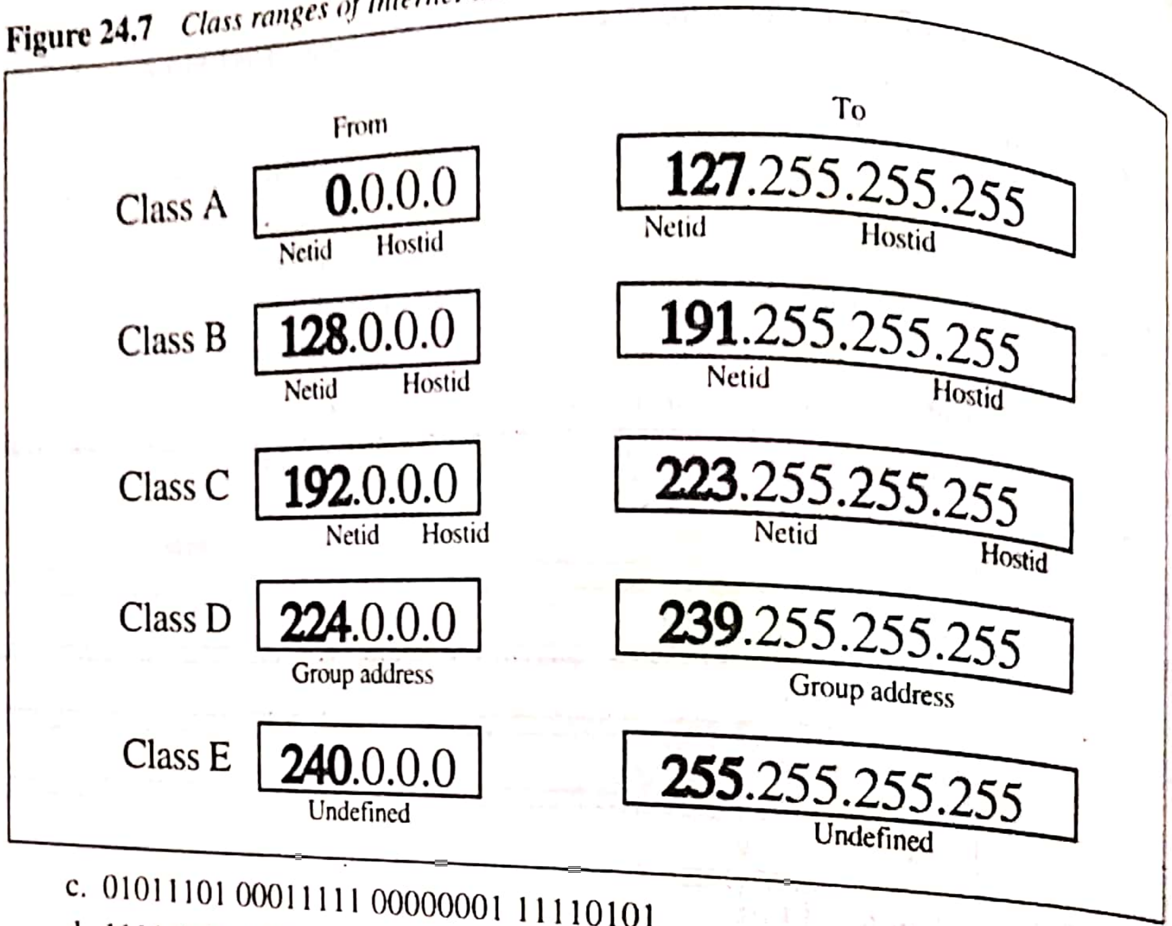
Looking at the first byte of an address in decimal form allows us to determine at a glance to which class a particular address belongs (see Figure 24.7).

Example 24.2

Write each of following in dotted-decimal notation:

a. 10011101 10001111 11111100 11001111
b. 11011101 10001111 11111101 00001111

Figure 24.7 *Class ranges of Internet addresses*



c. 01011101 00011111 00000001 11110101

d. 11111101 10001010 00001111 00111111

e. 11111110 10000001 01111110 00000001

Solution

Each byte is converted to a decimal number between 0 and 255.

a. 157.143.252.207

b. 221.143.253.15

c. 93.31.1.245

d. 253.138.15.63

e. 254.129.126.1

Example 24.3

Find the class of each address:

a. 4.23.145.90

b. 227.34.78.7

c. 246.7.3.8

d. 29.6.8.4

e. 198.76.9.23

Solution

The first byte defines the class.

a. Class A

b. Class D

c. Class E

d. Class B
e. Class C

Example 24.4

Find the netid and the hostid for each address:

a. 4.23.145.90
b. 227.34.78.7
c. 246.7.3.8
d. 129.6.8.4
e. 198.76.9.23

Solution

First find the class and then find the netid and hostid.

a. Class A, netid: 4 hostid: 23.145.90
b. Class D, no hostid or netid
c. Class E, no hostid or netid
d. Class B, netid: 129.6 hostid:8.4
e. Class C, netid: 198.76.9 hostid: 23

Example 24.5

Find the network address for each address:

a. 4.23.145.90
b. 227.34.78.7
c. 246.7.3.8
d. 129.6.8.4
e. 198.76.9.23

Solution

First find the class and then find the network address.

a. Class A, network address: 4.0.0.0
b. Class D, no network address
c. Class E, no network address
d. Class B, network address: 129.6.0.0
e. Class C, network address: 198.76.9.0

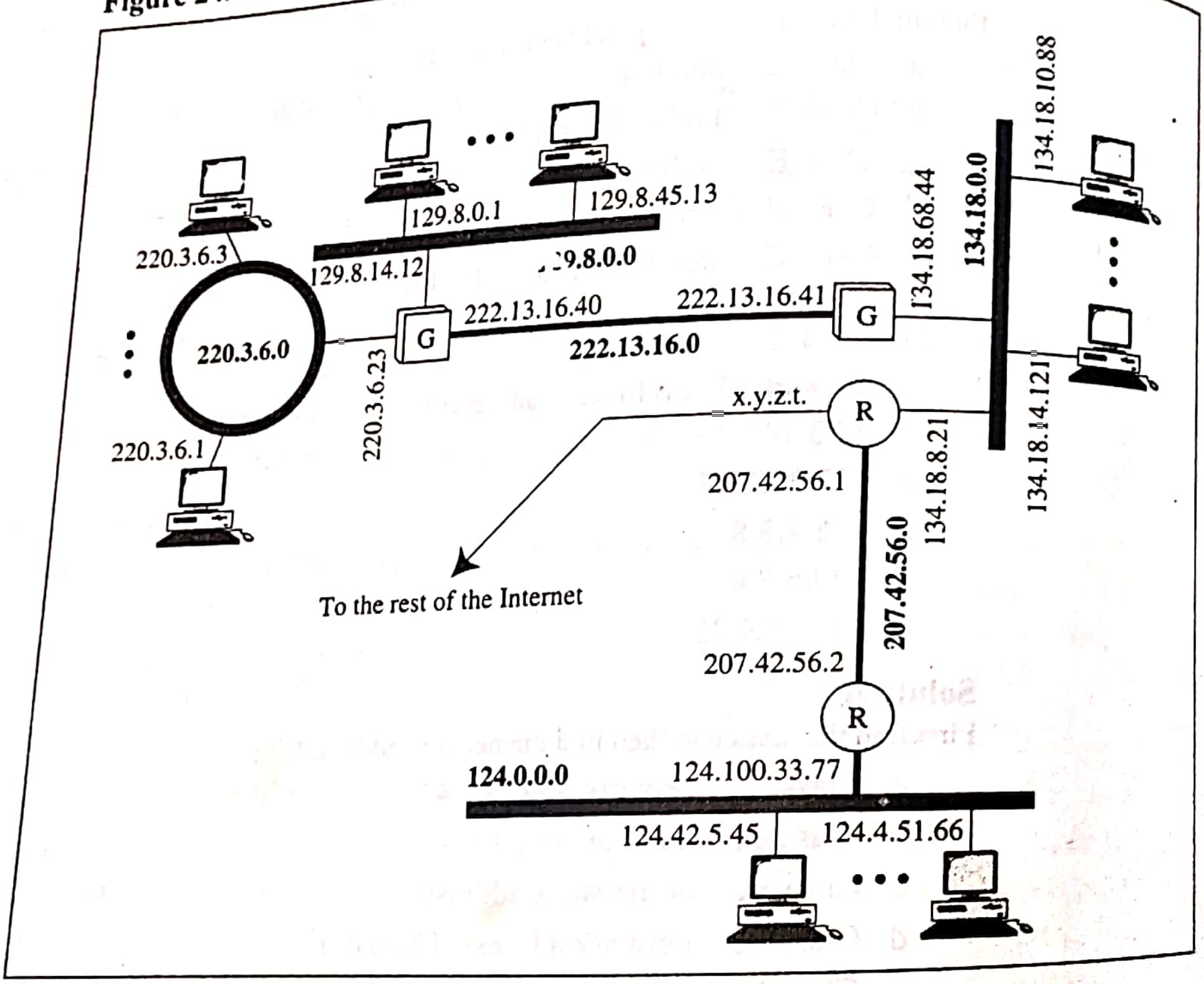
Nodes with More Than One Address

As we have said, an internet address defines the node's connection to its network. It follows, therefore, that any device connected to more than one network (e.g., any router) must have more than one internet address. In fact, a device has a different address for each network connected to it.

A Sample Internet

An internet address specifies both the network to which a host belongs **(netid)** and the host itself **(hostid)**. Figure 24.8 shows a portion of the Internet made up of LANs (three Ethernets and a Token Ring). Routers are indicated by circles containing Rs. Gateways are indicated by boxes containing Gs. Each has a separate address for each of its connected networks. The figure also shows the network addresses in color. A network address is the netid with the hostid part set to 0s. The network addresses in the figure are 129.8.0.0 (class B), 124.0.0.0 (class A), 134.18.0.0 (class B), and 220.3.6.0 (class C).

Figure 24.8 *Network and host addresses*

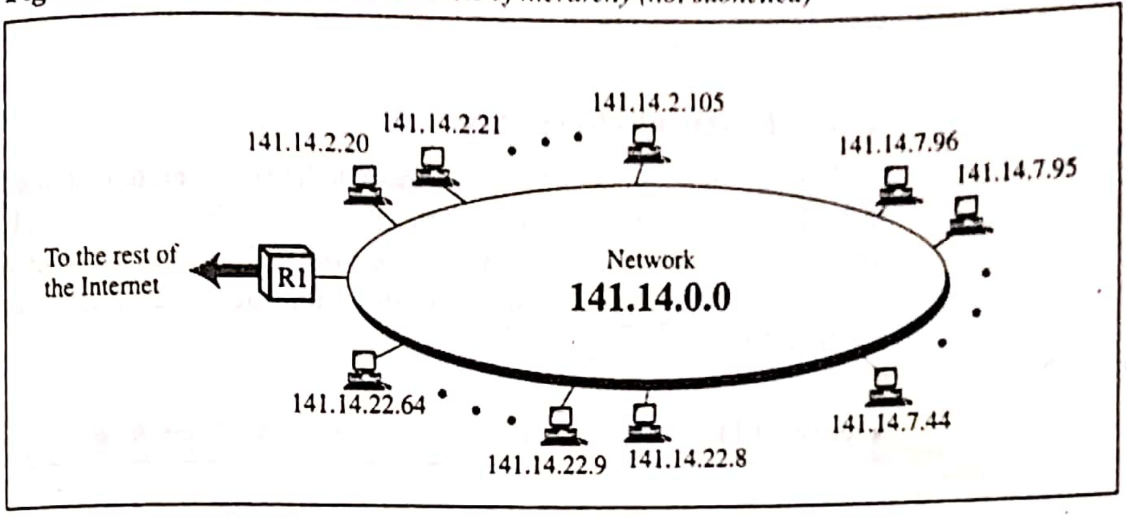


24.4 SUBNETTING

As we previously discussed, an **IP address** is 32 bits long. One portion of the address indicates a network (netid), and the other portion indicates the host (or router) on the network (hostid). This means that there is a sense of hierarchy in IP addressing. To reach a host on the Internet, we must first reach the network using the first portion of the address (netid). Then we must reach the host itself using the second portion (hostid). In other words, classes A, B, and C in IP addressing are designed with two levels of hierarchy.

However, in many cases, these two levels of hierarchy are not enough. For example, imagine an organization with a class B address. The organization has two-level hierarchical addressing, but it cannot have more than one physical network (see Figure 24.9).

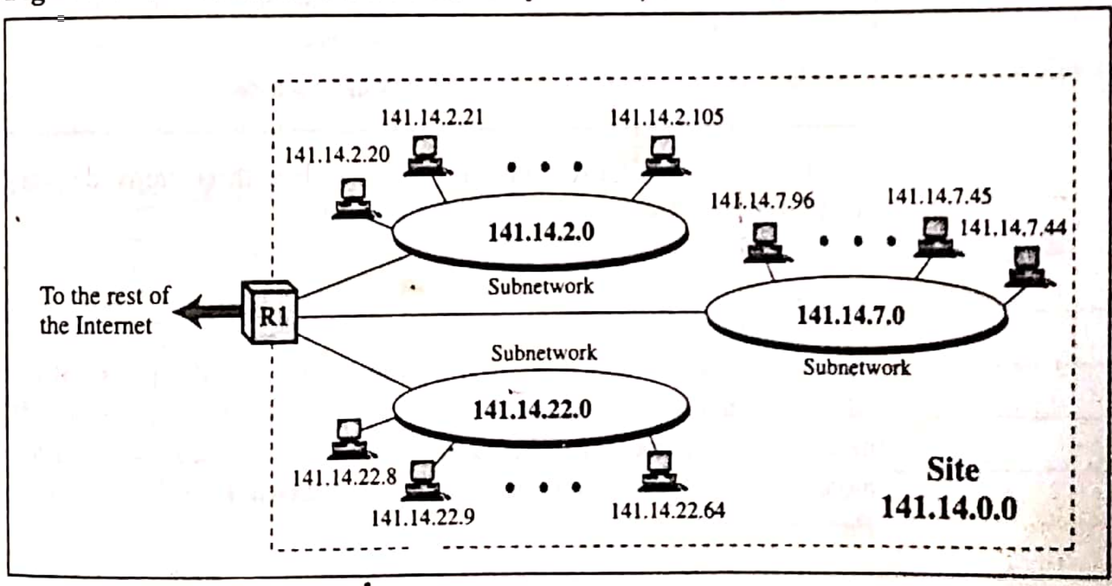
Figure 24.9 *A network with two levels of hierarchy (not subnetted)*



With this scheme, the organization is limited to two levels of hierarchy. The hosts cannot be organized into groups, and all of the hosts are at the same level. The organization has one network with many hosts.

One solution to this problem is **subnetting,** the further division of a network into smaller networks called **subnetworks.** For example, Figure 24.10 shows the network in Figure 24.9 divided into three subnetworks.

Figure 24.10 *A network with three levels of hierarchy (subnetted)*



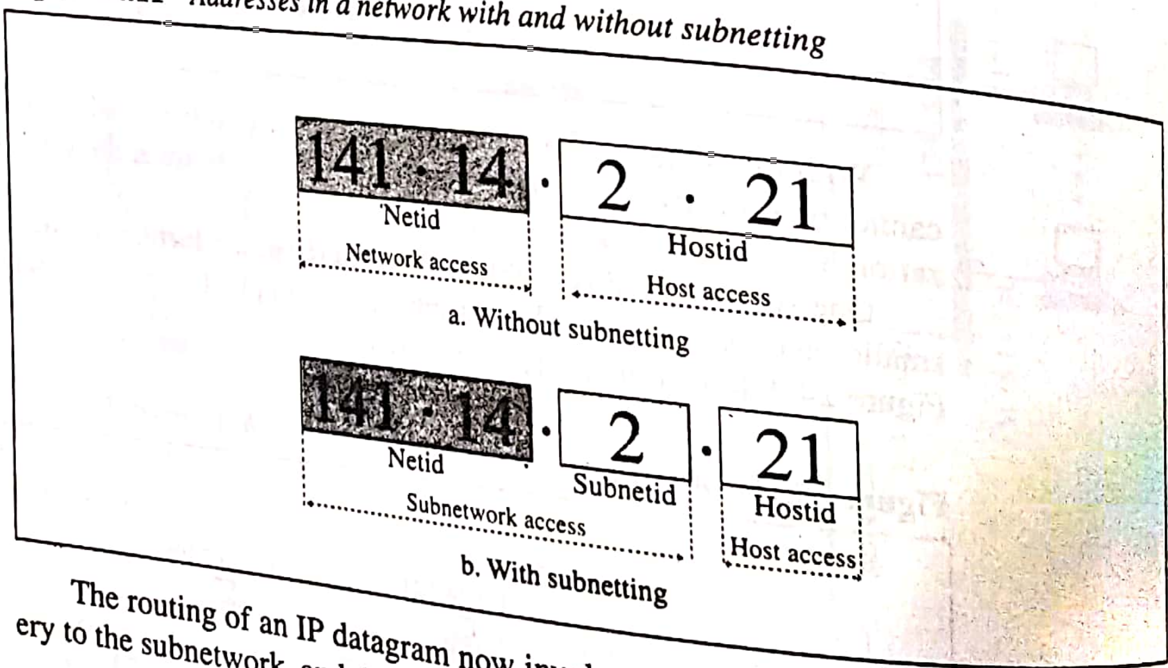
In this example, the rest of the Internet is not aware that the network is divided into three physical subnetworks: the three subnetworks still appear as a single network to the rest of the Internet. A packet destined for host 141.14.2.21 still reaches router R1. The destination address of the IP datagram is still a class B address where 141.14 defines the netid and 2.21 defines the hostid.

However, when the packet arrives at router R1, the interpretation of the IP address changes. Router R1 knows that the network 141.14 is physically divided into three subnetworks. It knows that the last two octets define two things: subnetid and hostid. Therefore, 2.21 must be interpreted as subnetid 2 and hostid 21. The router R1 uses the first two octets (141.14) as the netid, the third octet (2) as the subnetid, and the fourth octet (21) as the hostid.

Three Levels of Hierarchy

Adding subnetworks creates an intermediate level of hierarchy in the IP addressing system. Now we have three levels: netid, subnetid, and hostid. The netid is the first level; it defines the site. The second level is the *subnetid;* it defines the physical subnetwork. The hostid is the third level; it defines the connection of the host to the subnetwork. See Figure 24.11.

Figure 24.11 *Addresses in a network with and without subnetting*



The routing of an IP datagram now involves three steps: delivery to the site, delivery to the subnetwork, and delivery to the host.

Masking

Masking is a process that extracts the address of the physical network from an IP address. Masking can be done whether we have subnetting or not. If we have not subnetted the network, masking extracts the network address from an IP address. If we have subnetted, masking extracts the **subnetwork address** from an IP address (see Figure 24.12).

Masks without Subnetting

To be compatible, routers use a mask even if there is no subnetting. The masks for networks that are not subnetted can be defined in Table 24.1.

Figure 24.12 *Masking*

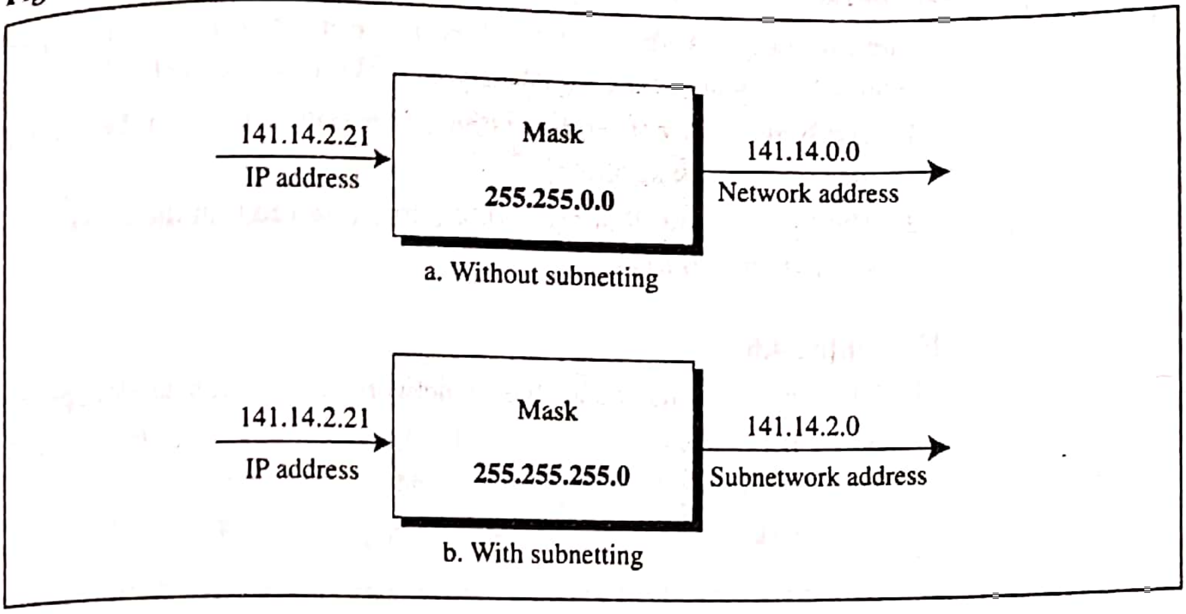


Table 24.1 *Mask for unsubnetted networks*

Class	*Mask*	*Address (Example)*	*Network Address (Example)*
A	255.0.0.0	15.32.56.7	15.0.0.0
B	255.255.0.0	135.67.13.9	135.67.0.0
C	255.255.255.0	201.34.12.72	201.34.12.0
D	N/A	N/A	N/A
E	N/A	N/A	N/A

Masks with Subnetting

When there is subnetting, the mask can vary. Table 24.2 shows some examples of masks used for subnetting.

Table 24.2 *Masks for subnetted networks*

Class	*Mask*	*Address (Example)*	*Network Address (Example)*
A	255.255.0.0	15.32.56.7	15.32.0.0
B	255.255.255.0	135.67.13.9	135.67.13.0
C	255.255.255.192	201.34.12.72	201.34.12.64
D	N/A	N/A	N/A
E	N/A	N/A	N/A

Finding the Subnetwork Address

To find the subnetwork address, apply the mask to the IP address.

Boundary-Level Masking

If the masking is at the boundary level (the mask numbers are either 255 or 0), finding the subnetwork address is very easy. Follow these two rules:

1. The bytes in the IP address that correspond to 255 in the mask will be repeated in the subnetwork address.
2. The bytes in the IP address that correspond to 0 in the mask will change to 0 in the subnetwork address.

Example 24.6

The following shows how to get the subnetwork address from an IP address:

IP address	45 .	23 .	21 .	8
Mask	255 .	255 .	0 .	0
Subnetwork address	45 .	23 .	0 .	0

Example 24.7

The following shows how to get the subnetwork address from an IP address:

IP address	173 .	23 .	21 .	8
Mask	255 .	255 .	255 .	0
Subnetwork address	173 .	23 .	21 .	0

Nonboundary-Level Masking

If the masking is not at the boundary level (the mask numbers are not just 255 or 0), finding the subnetwork address involves using the bit-wise AND operator. Follow these three rules:

1. The bytes in the IP address that correspond to 255 in the mask will be repeated in the subnetwork address.
2. The bytes in the IP address that correspond to 0 in the mask will change to 0 in the subnetwork address.
3. For other bytes, use the bit-wise AND operator.

Example 24.8

The following shows how to get the network address from an IP address:

IP address	45 .	123 .	21 .	8
Mask	255 .	192 .	0 .	0
Subnetwork address	45 .	64 .	0 .	0

As you can see, three bytes are easy to determine. However, the second byte needs the *bit-wise AND* operation. The bit-wise AND operation is very simple. If two bits are both 1s, the result is 1; otherwise, the result is 0.

123	0 1 1 1 1 0 1 1
192	1 1 0 0 0 0 0 0
64	0 1 0 0 0 0 0 0

Example 24.9

The following shows how to get the subnetwork address from an IP address:

IP address	213	. 23	. 47	. 37
Mask	255	. 255	. 255	. 240
Subnetwork address	213	. 23	. 47	. 32

As you can see, three bytes are easy to determine. However, the fourth byte needs the bit-wise AND operation.

37	0 0 1 0 0 1 0 1
240	1 1 1 1 0 0 0 0
32	0 0 1 0 0 0 0 0

24.5 OTHER PROTOCOLS IN THE NETWORK LAYER

TCP/IP supports four other protocols in the network layer: ARP, RARP, ICMP, and IGMP.

Address Resolution Protocol (ARP)

The **address resolution protocol (ARP)** associates an IP address with the physical address. On a typical physical network, such as a LAN, each device on a link is identified by a physical or station address usually imprinted on the network interface card (NIC).

Physical addresses have local jurisdiction and can be changed easily. For example, if the NIC on a particular machine fails, the physical address changes. The IP addresses, on the other hand, have universal jurisdiction and cannot be changed. ARP is used to find the physical address of the node when its Internet address is known.

25. Describe ... protocol.

Multiple Choice Questions

26. Which OSI layer corresponds to the TCP-UDP layer?
    a. physical
    b. data link
    c. network
    d. transport
27. Which OSI layer corresponds to the IP layer?
    a. physical
    b. data link
    c. network
    d. transport
28. Which OSI layer(s) correspond to TCP/IP's application layer?
    a. application
    b. presentation
    c. session
    d. all of the above

29. Which of the following is true about the IP address?
    a. It's divided into exactly two classes.
    b. It contains a fixed-length hostid.
    c. It was established as a user-friendly interface.
    d. It is 32 bits long.
30. Which IP address class has few hosts per network?
    a. A
    b. B
    c. C
    d. D
31. For what does the data link layer look for as it sends a frame from one link to another?
    a. hostid
    b. IP address
    c. domain name
    d. station address
32. The purpose of ARP on a network is to find the ______ given the ________.
    a. Internet address, domain name
    b. Internet address, netid
    c. Internet address, station address
    d. station address, Internet address
33. Which of the following apply to UDP?
    a. is unreliable and connectionless
    b. contains destination and source port addresses
    c. reports certain errors
    d. all of the above
34. Which of the following applies(y) to both UDP and TCP?
    a. transport layer protocols
    b. port-to-port communication
    c. services of IP layer used
    d. all of the above
35. Which of the following is a class A host address?
    a. 128.4.5.6
    b. 117.4.5.1
    c. 117.0.0.0
    d. 117.8.0.0
36. Which of the following is a class B host address?
    a. 230.0.0.0
    b. 130.4.5.6
    c. 230.0.0.0

d. 30.4.5.6

37. Which of the following is a class C host address?
    a. 230.0.0.0
    b. 130.4.5.6
    c. 200.1.2.3
    d. 30.4.5.6
38. The data unit in the TCP/IP application layer is called a ______.
    a. message
    b. segment
    c. datagram
    d. frame
39. The data unit in the TCP/IP data link layer is called a ______.
    a. message
    b. segment
    c. datagram
    d. frame
40. The data unit in the TCP/IP IP layer is called a ______.
    a. message
    b. segment
    c. datagram
    d. frame
41. The data unit from the transport layer that uses UDP is called a ______.
    a. user datagram
    b. message
    c. segment
    d. frame
42. TCP/IP's ______ layer corresponds to the OSI model's top three layers.
    a. application
    b. presentation
    c. session
    d. transport
43. When a host knows its physical address but not its IP address, it can use ______.
    a. ICMP
    b. IGMP
    c. ARP
    d. RARP
44. This transport layer protocol is connectionless.
    a. UDP
    b. TCP
    c. FTP