COMPUTER NETWORK

UNIT 4: NETWORK LAYER

PROF. Ishani Saha

TOPICS

- IPV4 addressing, subnet mask, classless inter domain routing (CIDR)
- IPV6
- Address mapping – ARP, RARP, and DHCP

IPv4

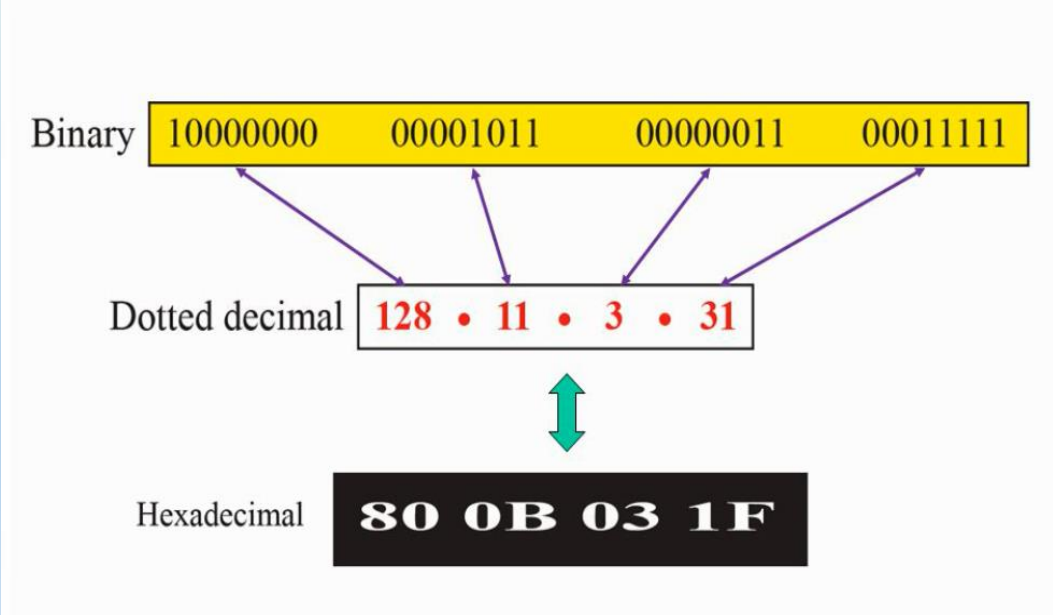
- The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address.
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a device (for example, a computer or a router) to the Internet.
- The IPv4 addresses are unique and universal.

IPv4 ADDRESSING

ADDRESS SPACE:

- An address space is the total number of addresses used by the protocol.
- If a protocol uses b bits to define an address , the address space is 2^b.

Notation: There are three common notations to show an IPv4 address: Binary notation(base 2), Dotted decimal notation (base 256), and hexadecimal notation (base 16)



IPv4 ADDRESSING

- Change the following IPv4 addresses from binary notation to dotted-decimal notation.

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution:

We replace each group of 8 bits with its equivalent decimal number and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

IPv4 ADDRESSING

Find the error, if any, in the following IPv4 addresses.

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Solution

a. There must be no leading zero (045).

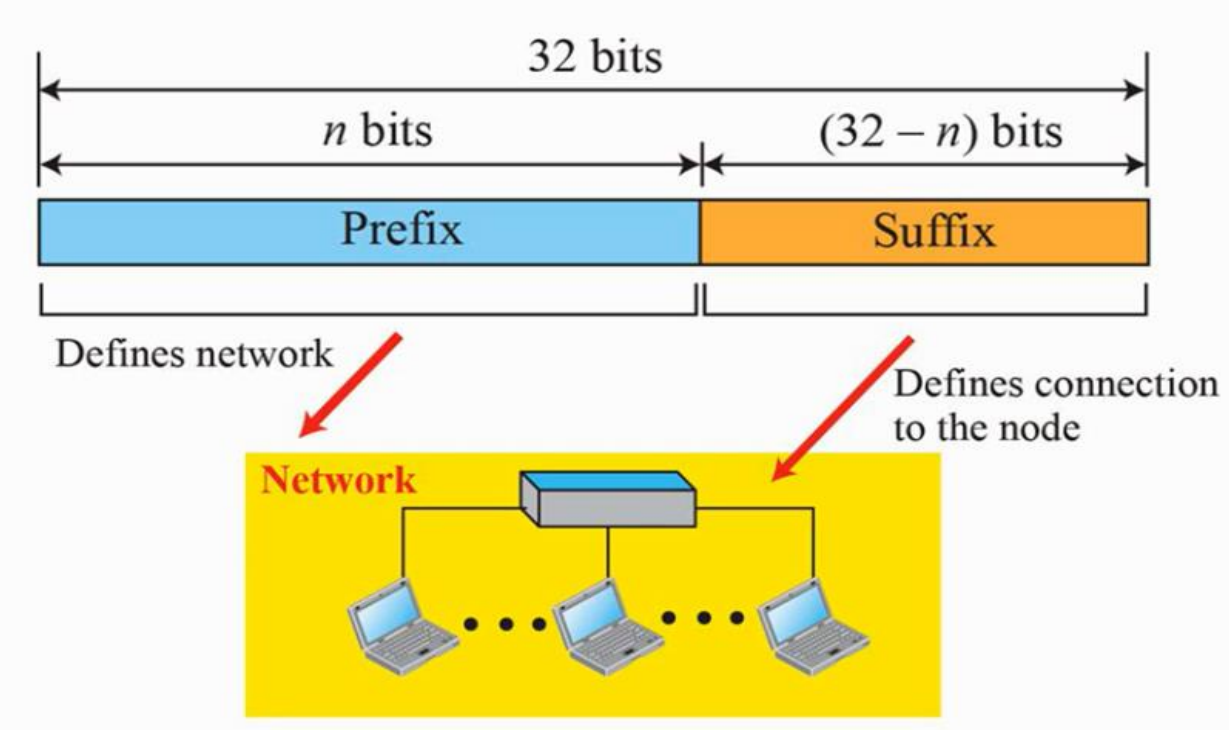
b. There can be no more than four numbers in an IPv4 address.

c. Each number needs to be less than or equal to 255 (301 is outside this range).

d. A mixture of binary notation and dotted-decimal notation is not allowed.

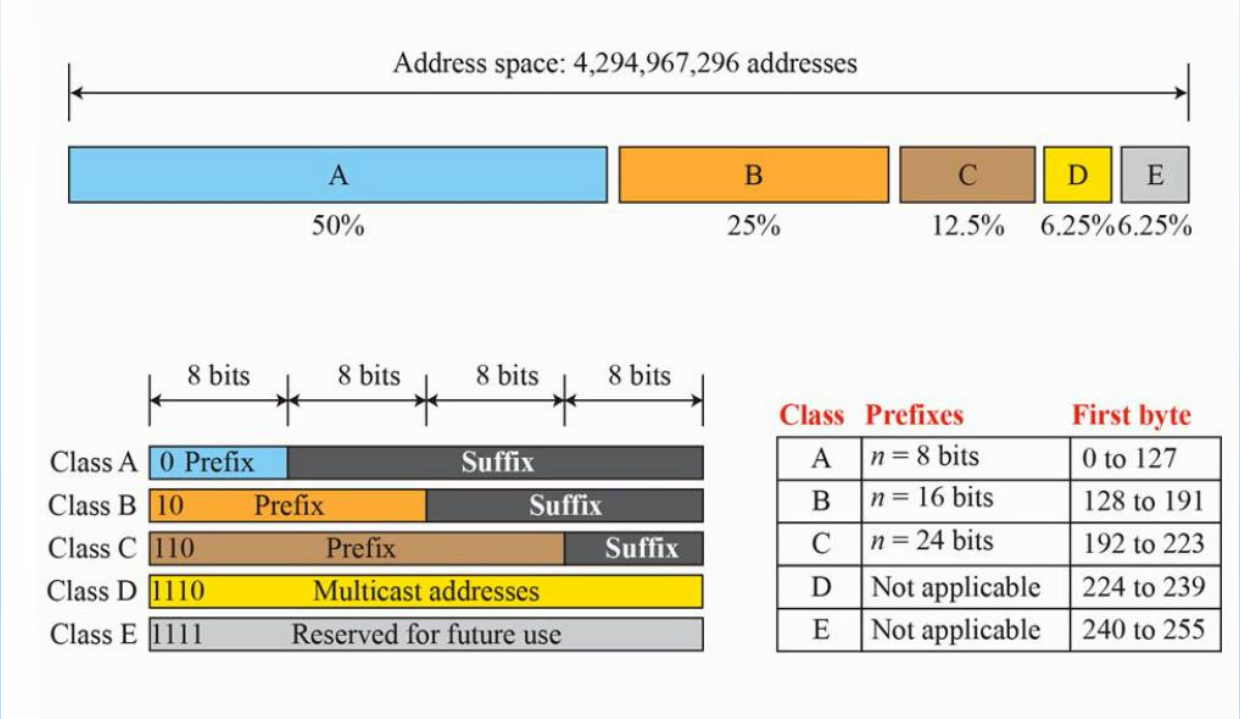
IPv4 ADDRESSING

- A 32-bit IPv4 address is hierarchical and divided into two parts.
- The first part of the address , called the prefix , defines the network ; the second part of the address, called the suffix, defines the node.



IPv4 ADDRESSING: CLASSFUL ADDRESSING

- An IPv4 address is designed with a fixed length prefix, but to accommodate both small and large networks, three fixed length prefixes were designed instead of one(n=8,n=16,n=24)
- The whole address space is divided into five classes (class A,B,C,D and E).



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

IPv4 ADDRESSING: CLASSFUL ADDRESSING

Table 19.1 *Number of blocks and block size in classful IPv4 addressing*

Class	*Number of Blocks*	*Block Size*	*Application*
A	128	16,777,216	Unicast
B	16,384	65,536	Unicast
C	2,097,152	256	Unicast
D	1	268,435,456	Multicast
E	1	268,435,456	Reserved

IPv4 ADDRESSING: CLASSFUL ADDRESSING

Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first bit is O. This is a class A address.

b. The first 2 bits are 1; the third bit is O. This is a class C address.

c. The first byte is 14 (between 0 and 127); the class is A.

d. The first byte is 252 (between 240 and 255); the class is E.

IPv4 ADDRESSING: CLASSLESS ADDRESSING

- To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme, there are no classes, but the addresses are still granted in blocks.

Address Blocks

- In classless addressing, when an entity, small or large, needs to be connected to the Internet, it is granted a block (range) of addresses.
- The size of the block (the number of addresses) varies based on the nature and size of the entity. For example, a household may be given only two addresses; a large organization may be given thousands of addresses.
- An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve. The Internet authorities impose three restrictions on classless address blocks:

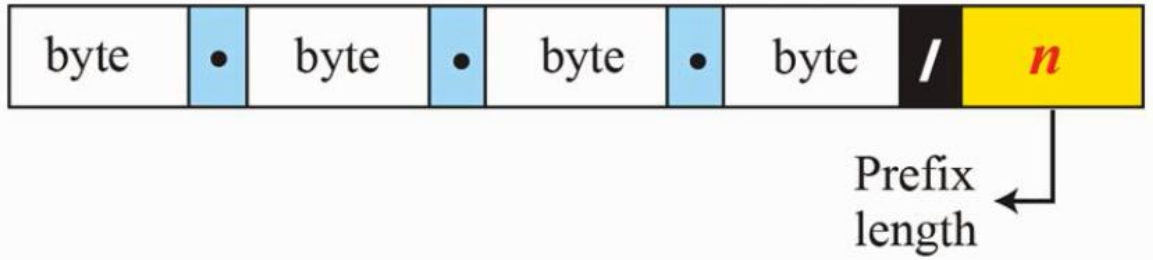
1. The addresses in a block must be contiguous, one after another.
2. The number of addresses in a block must be a power of 2 (1, 2, 4, 8, ...).
3. The first address must be evenly divisible by the number of addresses.

IPv4 ADDRESSING: CLASSLESS ADDRESSING

- In classless addressing, the whole address space is divided into variable length blocks.
- The prefix in an address defines the block(network) ; the suffix defines the node (device).
- The prefix length in classless addressing is variable and can range from 0 to 32.
- The size of the network is inversely proportional to the length of the prefix.

IPv4 ADDRESSING: CLASSLESS ADDRESSING

- **PREFIX LENGTH**
- The prefix length , n , is added to the address, separated by a slash.
- The notation is informally referred to as Slash notation and formally as Classless Interdomain Routing (CIDR).

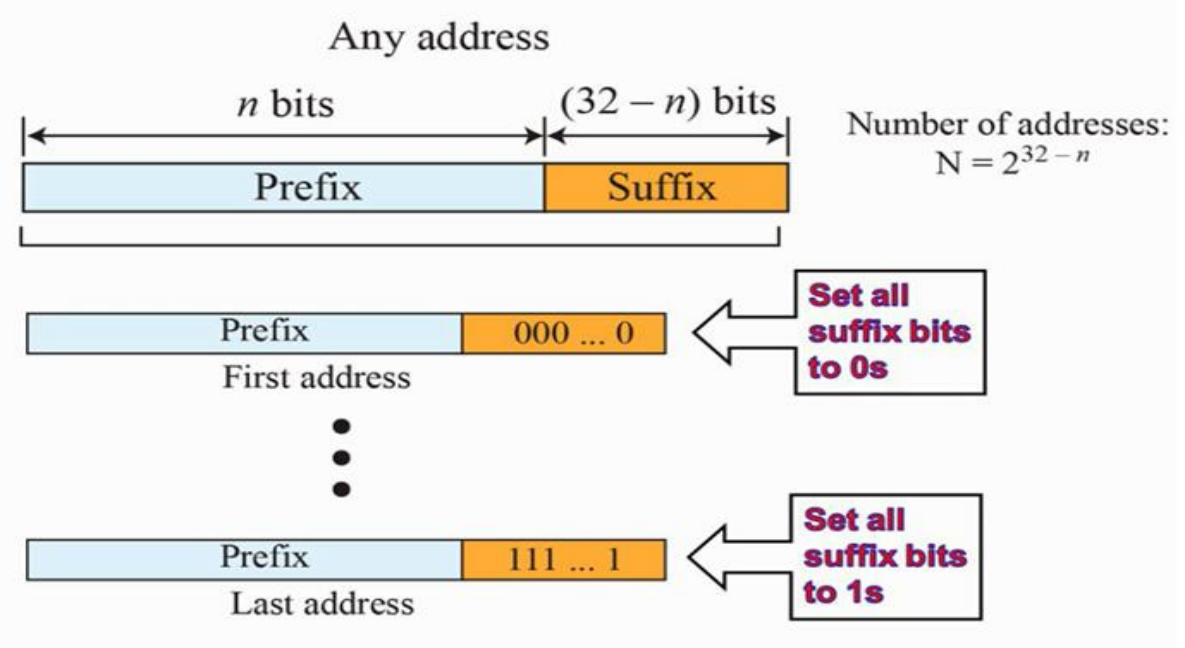


Examples:
12.24.76.8/**8**
23.14.67.92/**12**
220.8.24.255/**25**

IPv4 ADDRESSING: CLASSLESS ADDRESSING

INFORMATION EXTRACTION IN CLASSSLESS ADDRESSING

1. The number of addresses in the block is found as N= 2^{32-n}.
2. To find the first address, keep the leftmost bits and set the (32-n) rightmost bits all to 0s
3. To find the last address, keep the leftmost bits and set the (32-n) rightmost bits all to 1s



MASKING

- A block of addresses is granted to a small organization. We know that one of the addresses is 205.16.37.39/28. What is the first and last address in the block?

Solution

- The binary representation of the given address is

11001101 00010000 00100101 00100111

If we set 32 - 28 rightmost bits to 0, we get

11001101 00010000 00100101 0010000

or

205.16.37.32

If we set 32 - 28 rightmost bits to 1, we get

11001101 00010000 00100101 00101111

or

205.16.37.47

SUBNETTING

- During the era of classful addressing, subnetting was introduced.
- If an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors.
- Subnetting increases the number of 1s in the mask.

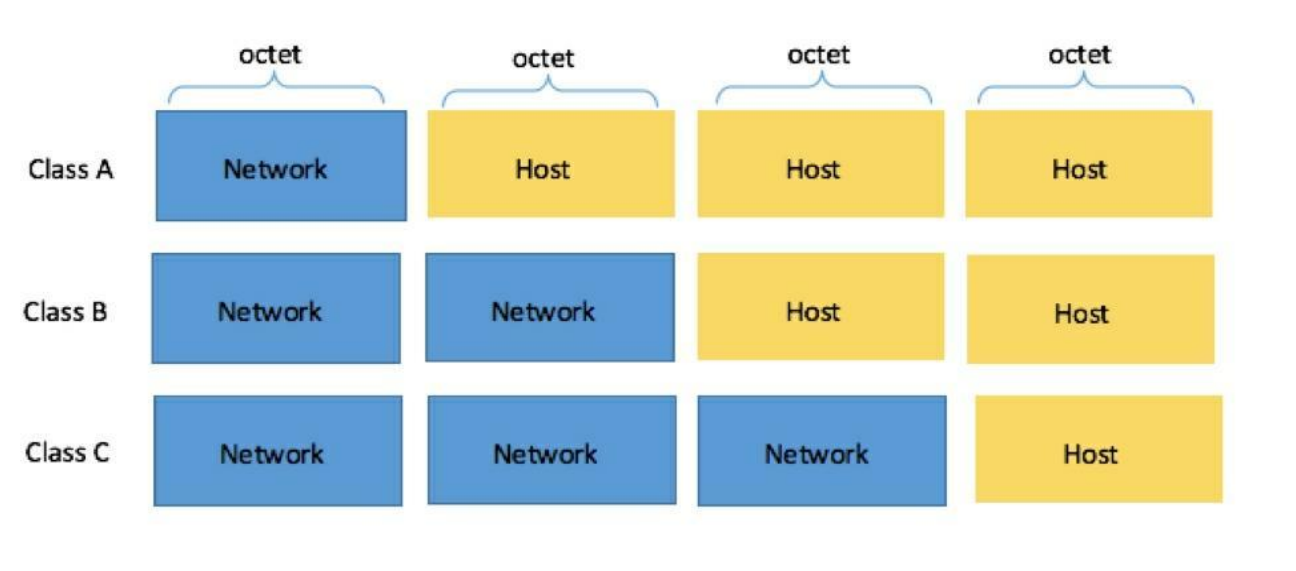
SUBNETTING

- Each IP address consists of a subnet mask. All the class types, such as Class A, Class B and Class C include the subnet mask known as the default subnet mask.
- The default subnet mask is as follows:

Class A: 255.0.0.0

Class B: 255.255.0.0

Class C: 255.255.255.0



SUBNETTING

- Subnetting is the strategy used to partition a single physical network into more than one smaller logical sub-networks (subnets).
- Subnetting take places when we extend the default subnet mask.

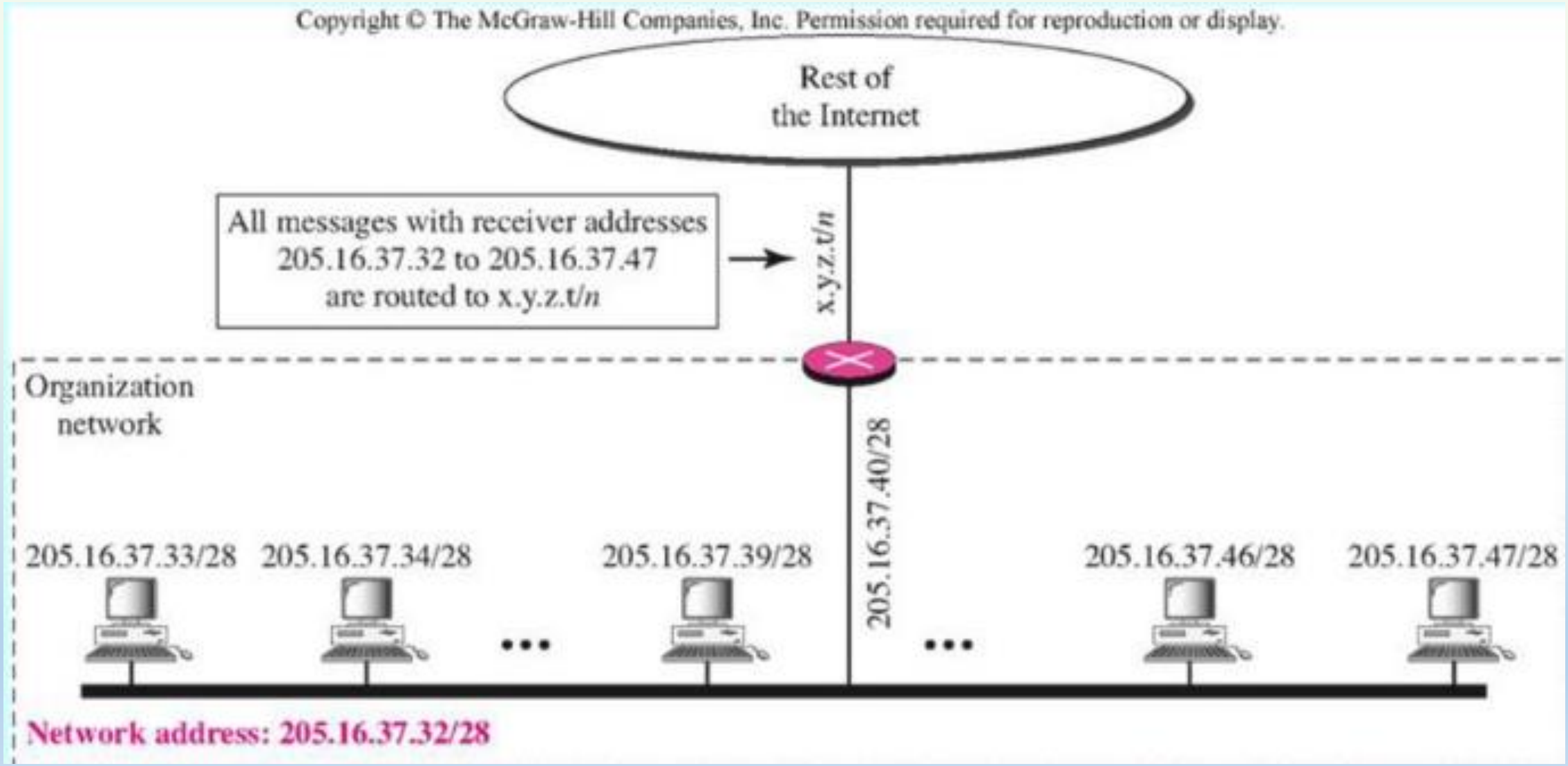
Example:

- Address given: 188.25.45.48/20
- This address belong to class B and class B has default subnet mask 255.255.0.0[/16 in CIDR].
- Subnet mask in binary would be 11111111. 11111111.11110000.00000000.
- Subnet mask is 255.255.240.0

NETWORK ADDRESS

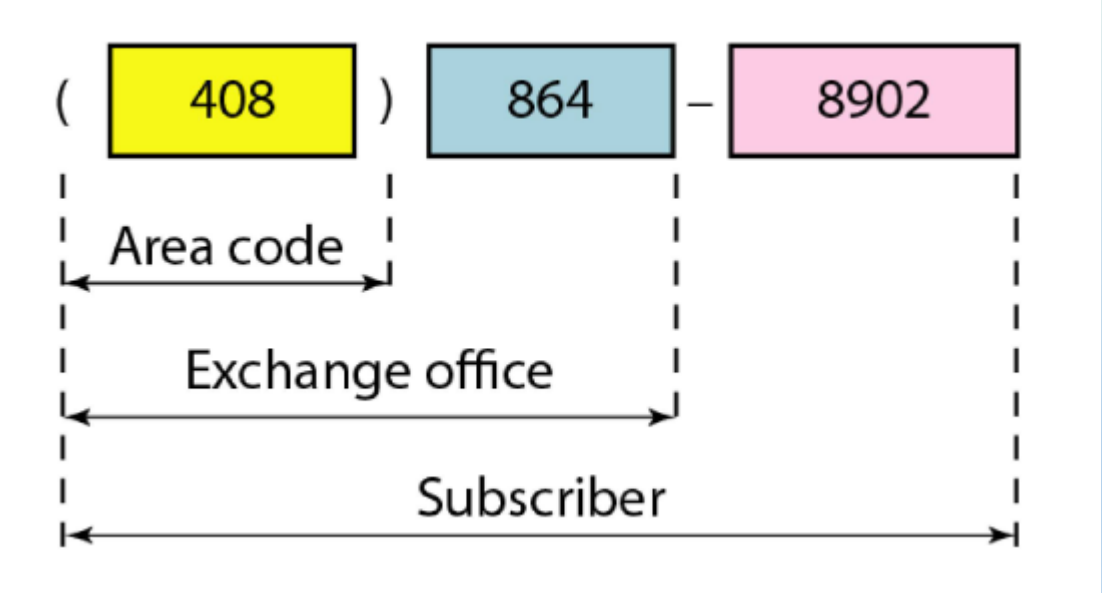
- A very important concept in IP addressing is the network address.
- When an organization is given a block of addresses, the organization is free to allocate the addresses to the devices that need to be connected to the Internet.
- The first address in the class, however, is normally (not always) treated as a special address.
- The first address is called the network address and defines the organization network.
- It defines the organization itself to the rest of the world.

NETWORK ADDRESS



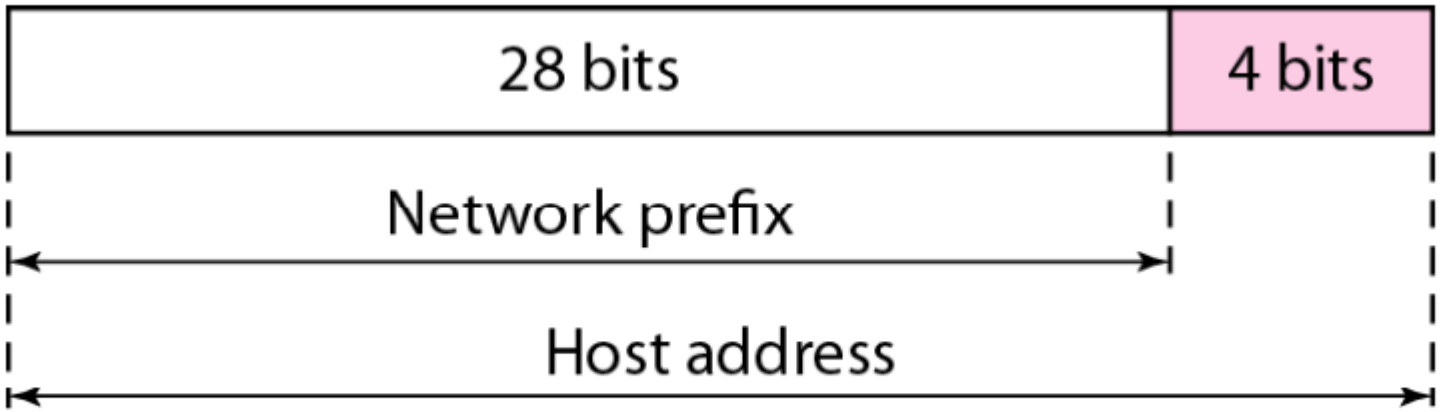
HIERARCHY

- IP addresses, like other addresses or identifiers we encounter these days, have levels of hierarchy.
- For example, a telephone network in North America has three levels of hierarchy.
- The leftmost three digits define the area code, the next three digits define the exchange, the last four digits define the connection of the local loop to the central office.

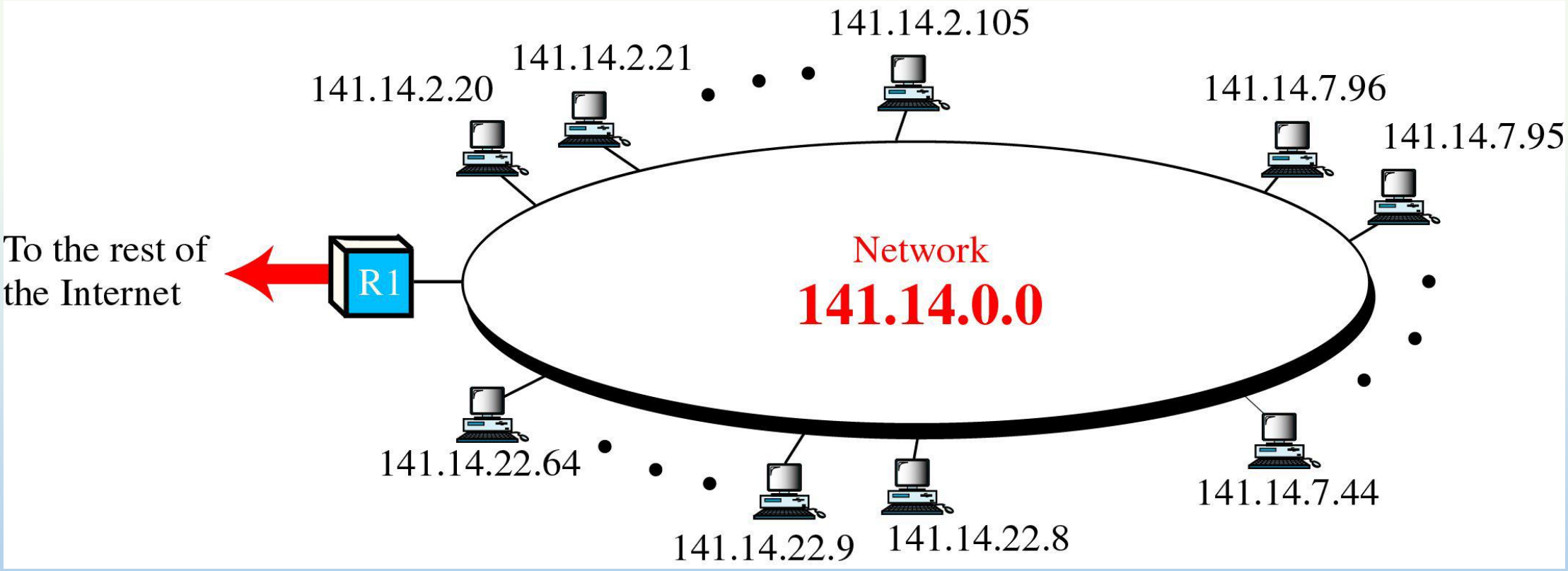


NETWORK WITH TWO LEVELS OF HIERARCHY

- An IP address can define only two levels of hierarchy when not subnetted.
- The n leftmost bits of the address x.y.z.t/n define the network (organization network); the 32 – n rightmost bits define the particular host (computer or router) to the network.
- The two common terms are prefix and suffix. The part of the address that defines the network is called the prefix; the part that defines the host is called the suffix.



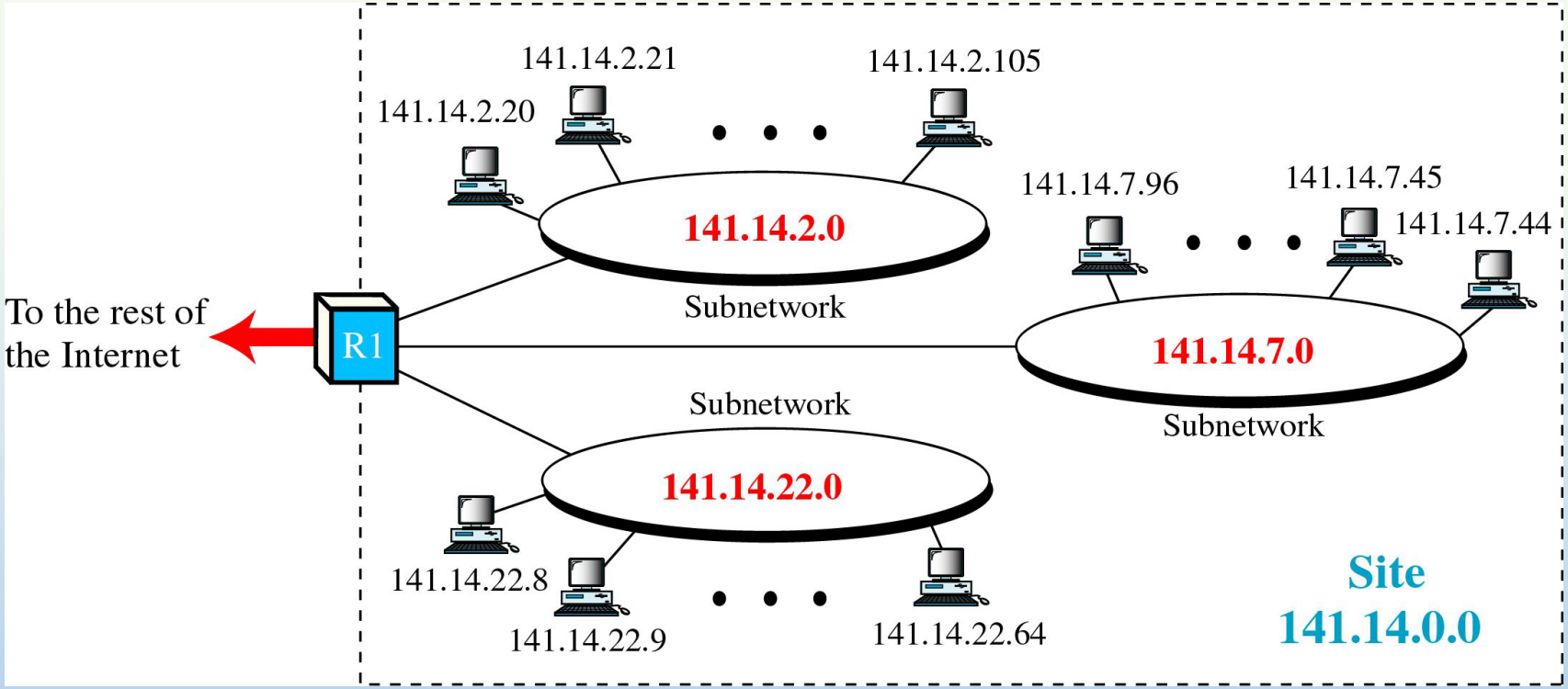
NETWORK WITH TWO LEVELS OF HIERARCHY



NETWORK WITH THREE LEVELS OF HIERARCHY

- An organization that is granted a large block of addresses may want to create clusters of networks (called subnets) and divide the addresses between the different subnets.
- The rest of the world still sees the organization as one entity; however, internally there are several subnets.
- All messages are sent to the router address that connects the organization to the rest of the Internet; the router routes the message to the appropriate subnets.
- The organization, however, needs to create small sub blocks of addresses, each assigned to specific subnets. The organization has its own mask; each subnet must also have its own.

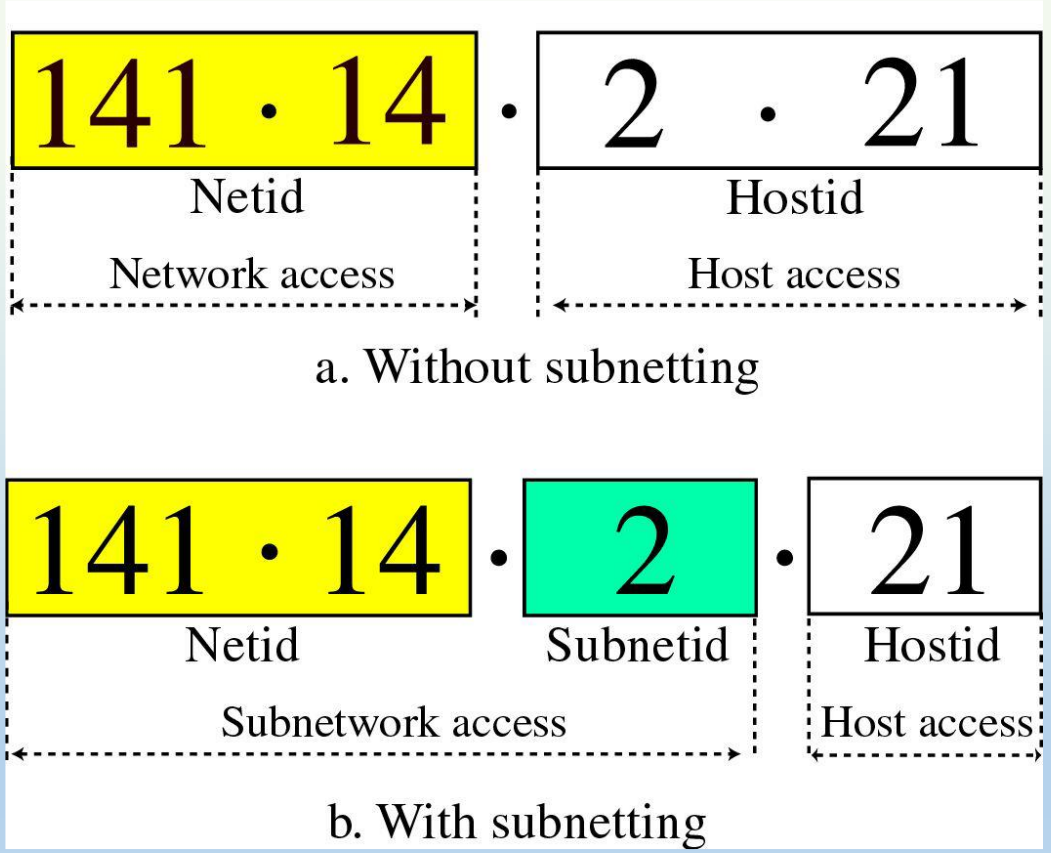
NETWORK WITH THREE LEVELS OF HIERARCHY



NETWORK WITH THREE LEVELS OF HIERARCHY

- Adding subnetworks creates an intermediate level of hierarchy in the IP addressing system.
- Thus the three levels are

1. Netid
2. Subnetid
3. Hostid



HIERARCHY

An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses). The ISP needs to distribute these addresses to three groups of customers as follows:

a. The first group has 64 customers; each needs 256 addresses.

b. The second group has 128 customers; each needs 128 addresses.

c. The third group has 128 customers; each needs 64 addresses.

Design the subblocks and find out how many addresses are still available after these allocations.

HIERARCHY

Solution

Figure 19.9 shows the situation.

Group 1

For this group, each customer needs 256 addresses. This means that 8 (log2 256) bits are needed to define each host. The prefix length is then 32 − 8 = 24. The addresses are

1st Customer:	*190.100.0.0/24*	*190.100.0.255/24*
2nd Customer:	*190.100.1.0/24*	*190.100.1.255/24*
. . .		
64th Customer:	*190.100.63.0/24*	*190.100.63.255/24*

Total = 64 × 256 = 16,384

HIERARCHY

Group 2

For this group, each customer needs 128 addresses. This means that 7 (log2 128) bits are needed to define each host. The prefix length is then 32 − 7 = 25. The addresses are

1st Customer:	*190.100.64.0/25*	*190.100.64.127/25*
2nd Customer:	*190.100.64.128/25*	*190.100.64.255/25*
. . .		
128th Customer:	*190.100.127.128/25*	*190.100.127.255/25*

Total = 128 × 128 = 16,384

HIERARCHY

Group 3

For this group, each customer needs 64 addresses. This means that 6 ($log_2 64$) bits are needed to each host. The prefix length is then 32 − 6 = 26. The addresses are

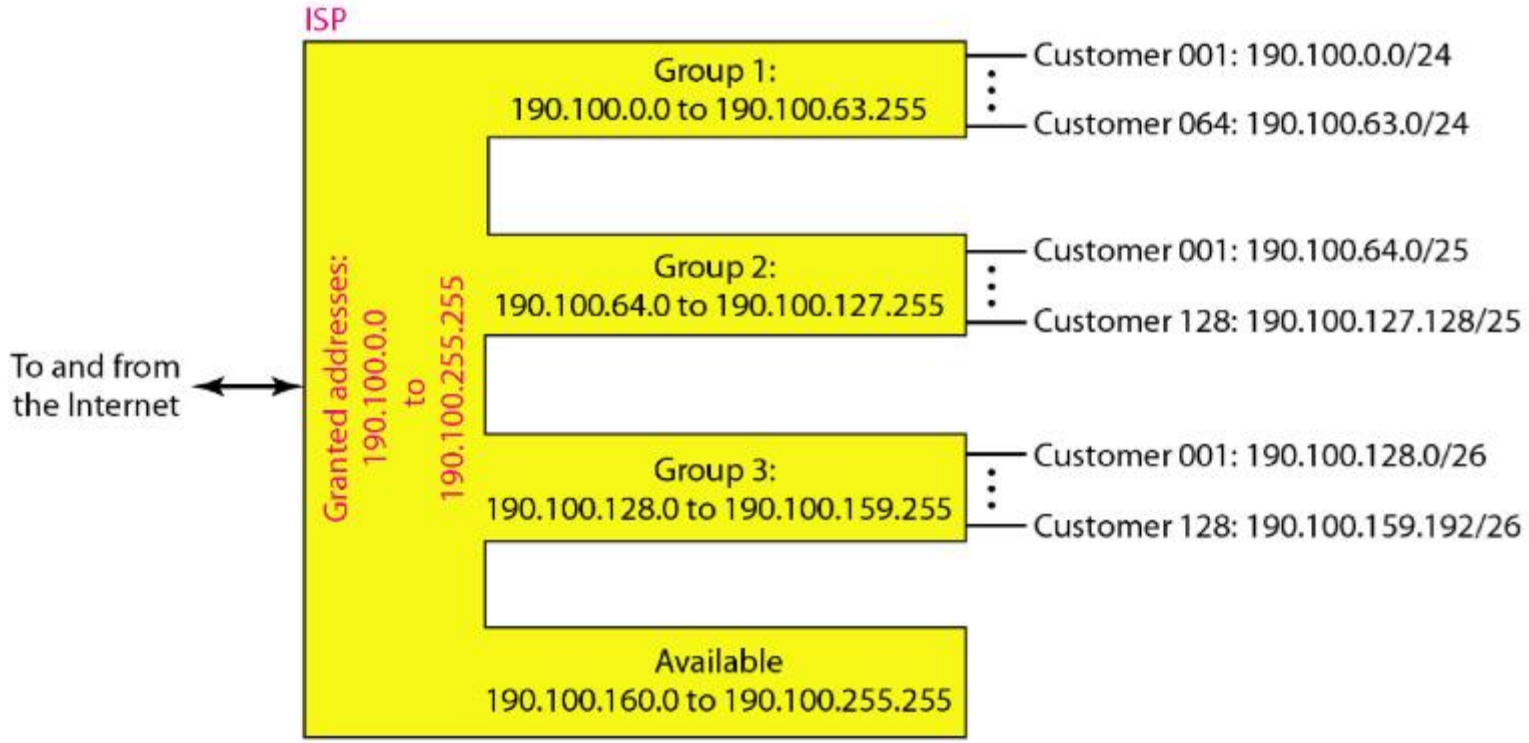
1st Customer:	*190.100.128.0/26*	*190.100.128.63/26*
2nd Customer:	*190.100.128.64/26*	*190.100.128.127/26*
. . .		
128th Customer:	*190.100.159.192/26*	*190.100.159.255/26*

Total = 128 × 64 = 8192

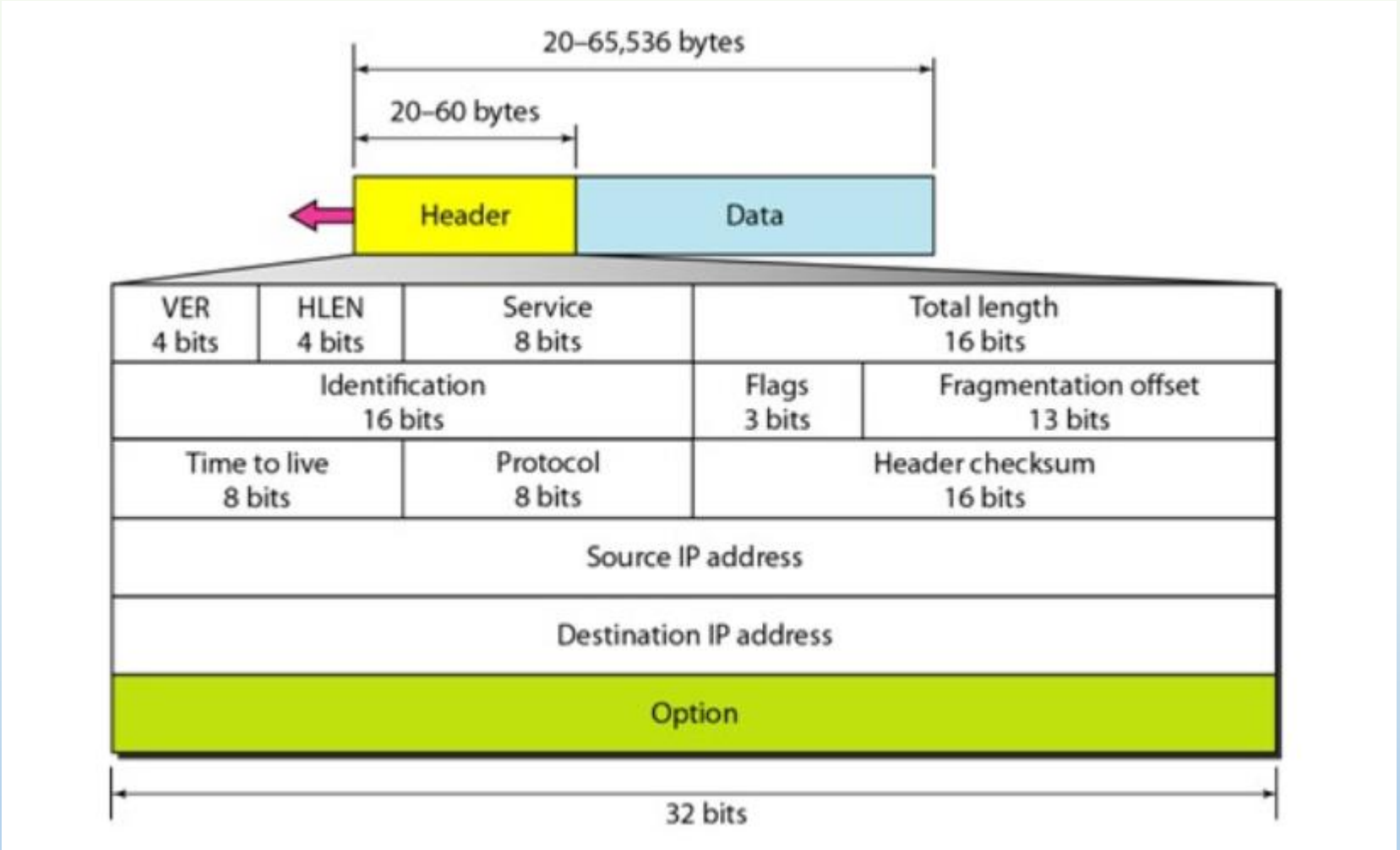
Number of granted addresses to the ISP: 65,536
Number of allocated addresses by the ISP: 40,960
Number of available addresses: 24,576

HIERARCHY

Figure 19.9 *An example of address allocation and distribution by an ISP*



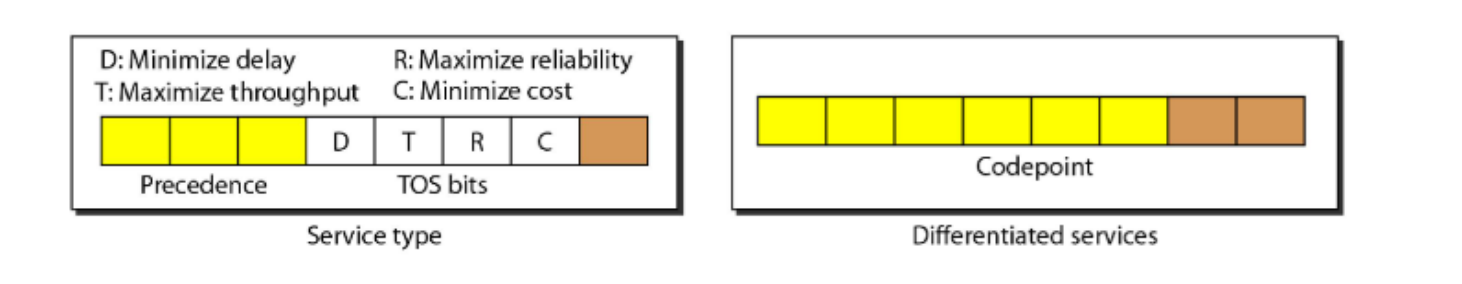
INTERNET PROTOCOL



IPv4 Datagram Format

INTERNET PROTOCOL

- **Version (VER):** This 4-bit field defines the version of the IPv4 protocol. Currently the version is 4.
- **Header length (HLEN).** This 4-bit field defines the total length of the datagram header in 4-byte words. This field is needed because the length of the header is variable (between 20 and 60 bytes).
- **Services:** IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.



- **Total length.** This is a 16-bit field that defines the total length (header plus data) of the IPv4 datagram in bytes.
- **Identification.** This 16-bit field identifies a datagram originating from the source host.
- **Flags**. This is a 3-bit field. The first bit is reserved. The second bit is called the donotfragment bit. The third bit is called the more fragment bit.

INTERNET PROTOCOL

- **Fragmentation offset**. This 13-bit field shows the relative position of this fragment with respect to the whole datagram
- **Time to live.** A datagram has a limited lifetime in its travel through an internet
- **Protocol:** This 8-bit field defines the higher-level protocol that uses the services of the IPv4 layer. An IPv4 datagram can encapsulate data from several higher-level protocols such as TCP, UDP, ICMP, and IGMP.
- **Checksum:** The checksum in the IPv4 packet covers only the header, not the data.
- **Source address:** This 32-bit field defines the IPv4 address of the source. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.
- **Destination address:** This 32-bit field defines the IPv4 address of the destination. This field must remain unchanged during the time the IPv4 datagram travels from the source host to the destination host.

INTERNET PROTOCOL

- **Options:** The header of the IPv4 datagram is made of two parts: a fixed part and a variable part. The variable part comprises the options that can be a maximum of 40 bytes. Options, as the name implies, are not required for a datagram. They can be used for network testing and debugging.

Figure 20.6 *Service type or differentiated services*

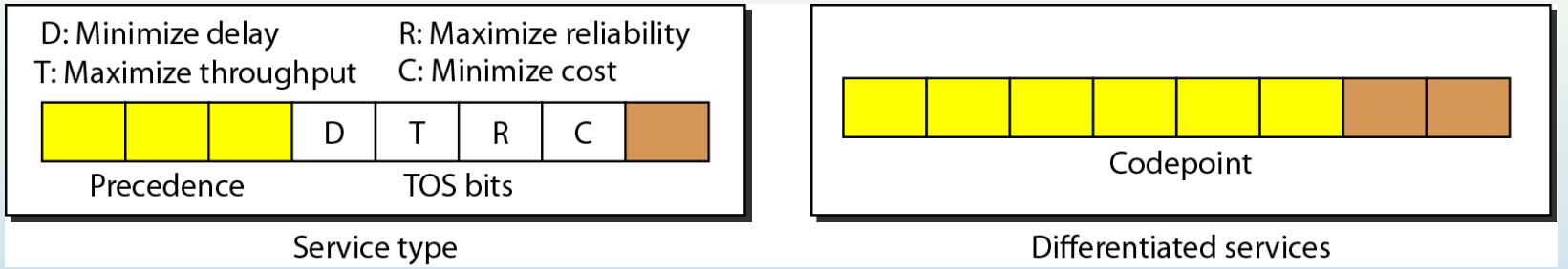


Table 20.1 *Types of service*

TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Table 20.2 *Default types of service*

Protocol	*TOS Bits*	*Description*
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

Figure 20.8 *Protocol field and encapsulated data*

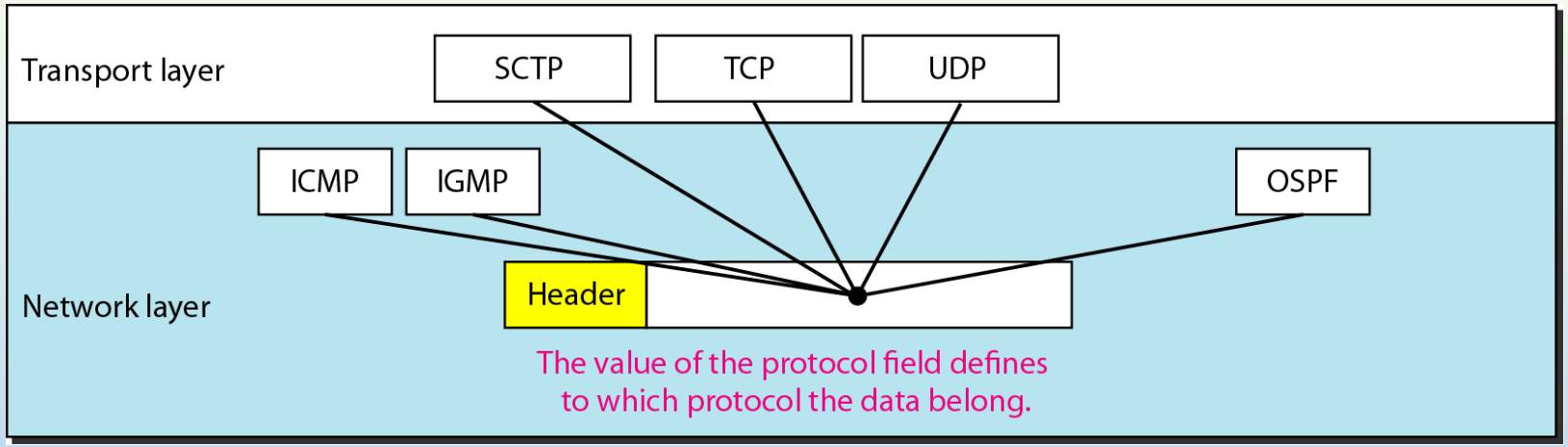


Figure 20.10 *Flags used in fragmentation*

Figure 20.11 *Fragmentation example*

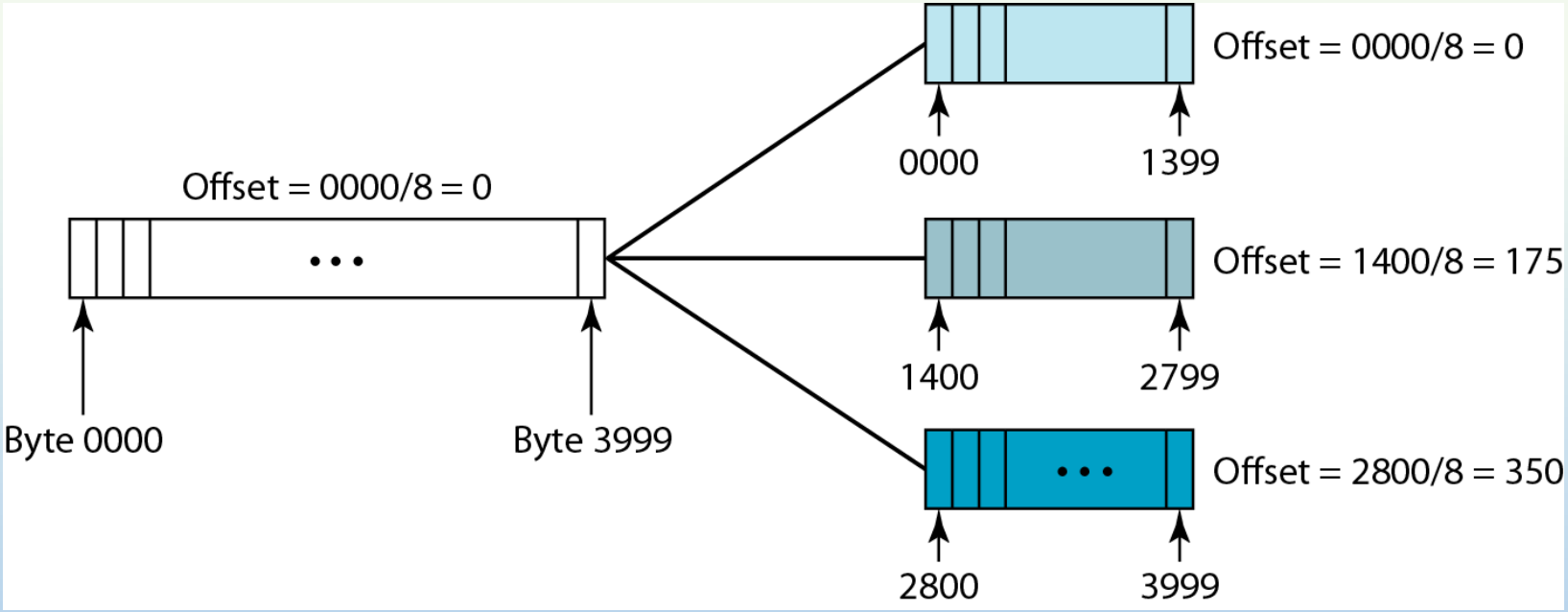
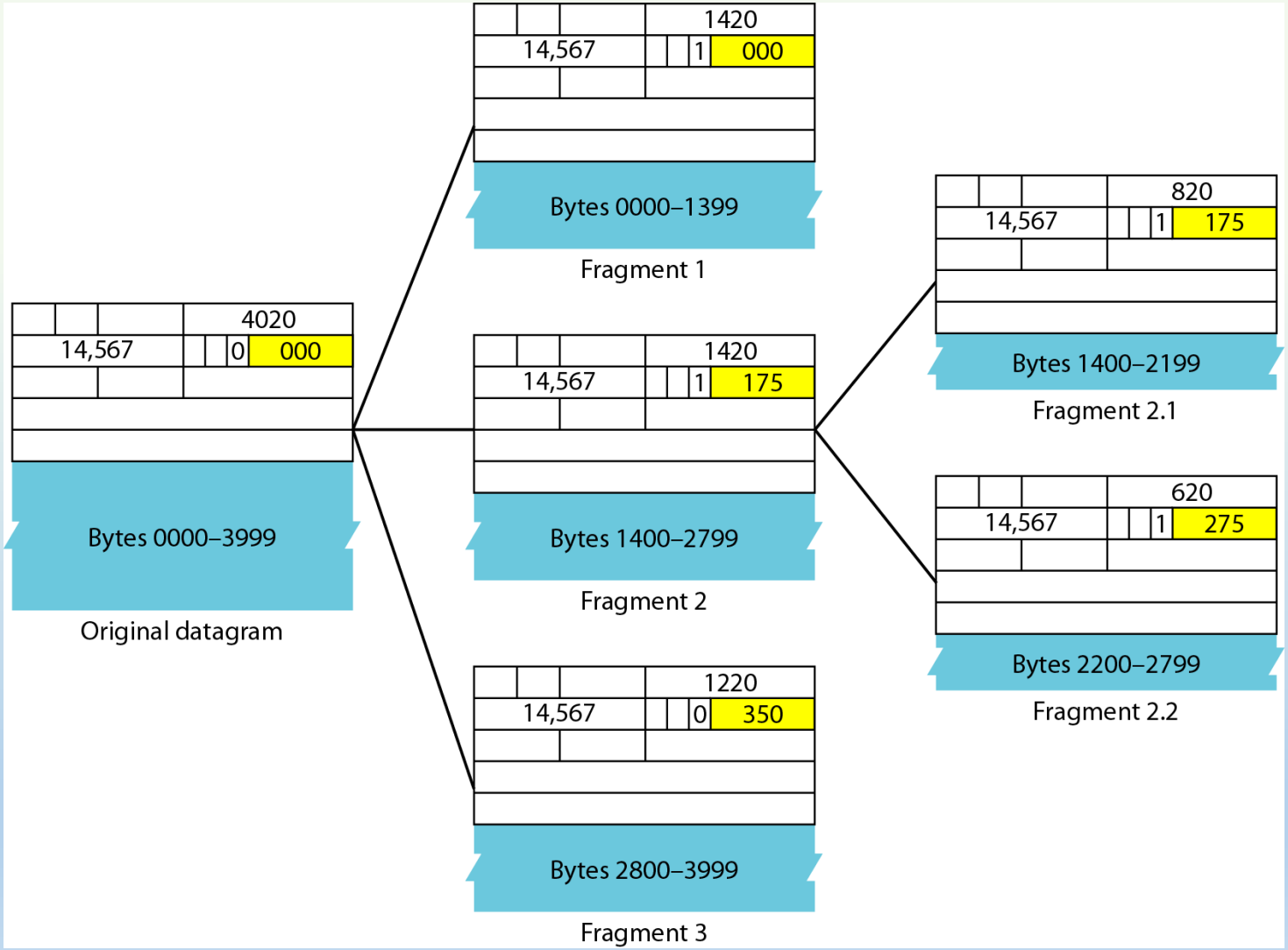


Figure 20.12 *Detailed fragmentation example*



IPv6 ADDRESSING

- The network layer protocol in the TCP/IP protocol suite is currently IPv4.
- IPv4 has some deficiencies that make it unsuitable for the fast-growing Internet.

1. Despite all short-term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long-term problem in the Internet.
2. The 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.
3. The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

IPv6 ADDRESSING

- An IPv6 address consists of 16 bytes (octets); it is 128 bits long.
- IPv6 addresses are represented using two notations: Binary and Colon hexadecimal.
- The colon hexadecimal divides the address into eight sections each made of four hexadecimal digits separated by colons.

  Original Address:8000:0000:0000:0000:0123:4567:89AB:CDEF

  Compressed Address: 8000::123:4567:89AB:CDEF

- The address space of IPv6 contains 2^{128} addresses. This address is 2^{96} times the IPv4 address.

IPv6 ADDRESSING

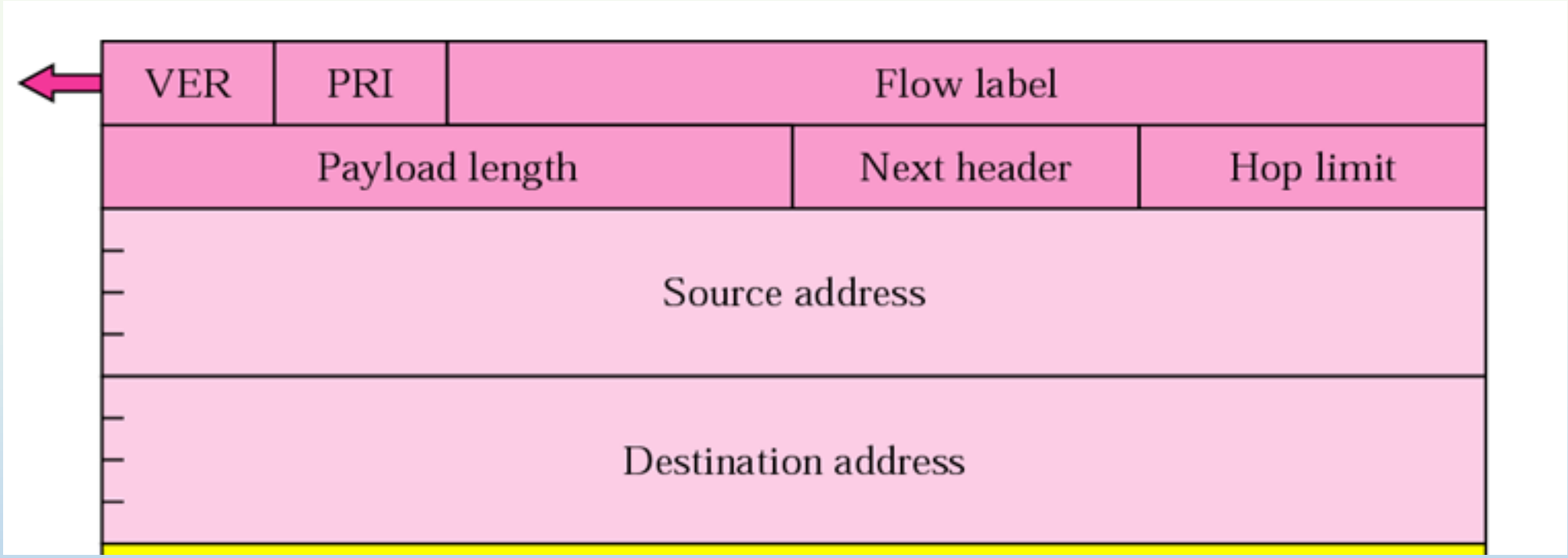
Expand the address 0:15::1:12:1213 to its original.

Solution:

This means that the original address is

0000:0015:0000:0000:0000:0001 :0012:1213

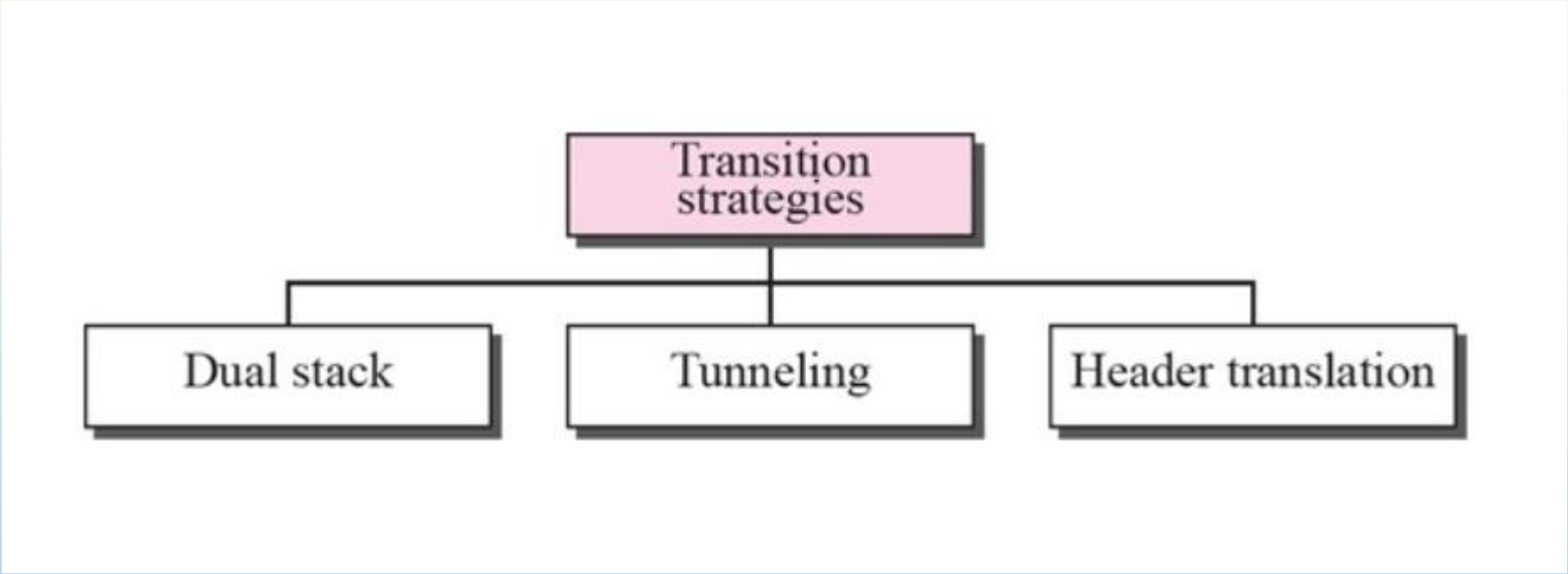
IPv6 ADDRESSING



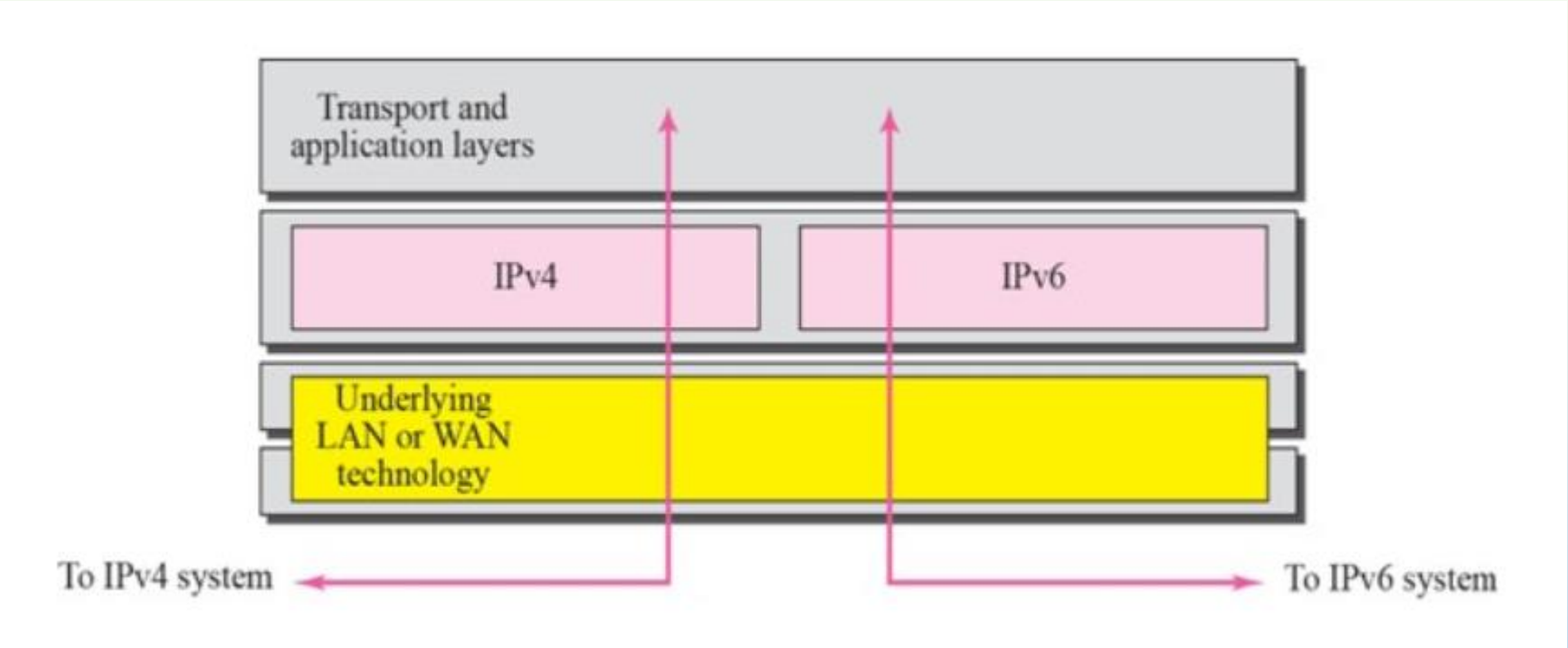
IPv6 ADDRESSING

- **Version:** This 4-bit field defines the version number of the IP. For IPv6, the value is 6.
- **Priority:** The 4-bit priority field defines the priority of the packet with respect to traffic congestion.
- **Flow label:** The flow label is a 3-byte (24-bit) field that is designed to provide special handling for a particular flow of data.
- **Payload length:** The 2-byte payload length field defines the length of the IP datagram excluding the base header.
- **Next header:** The next header is an 8-bit field defining the header that follows the base header in the datagram. The next header is either one of the optional extension headers used by IP or the header of an encapsulated packet such as UDP or TCP.
- **Hop limit:** This 8-bit hop limit field serves the same purpose as the TIL field in IPv4.
- **Source address:** The source address field is a 16-byte (128-bit) Internet address that identifies the original source of the datagram.
- **Destination address:** The destination address field is a 16-byte (128-bit) Internet address that usually identifies the final destination of the datagram

TRANSITION FROM IPv4 to IPv6

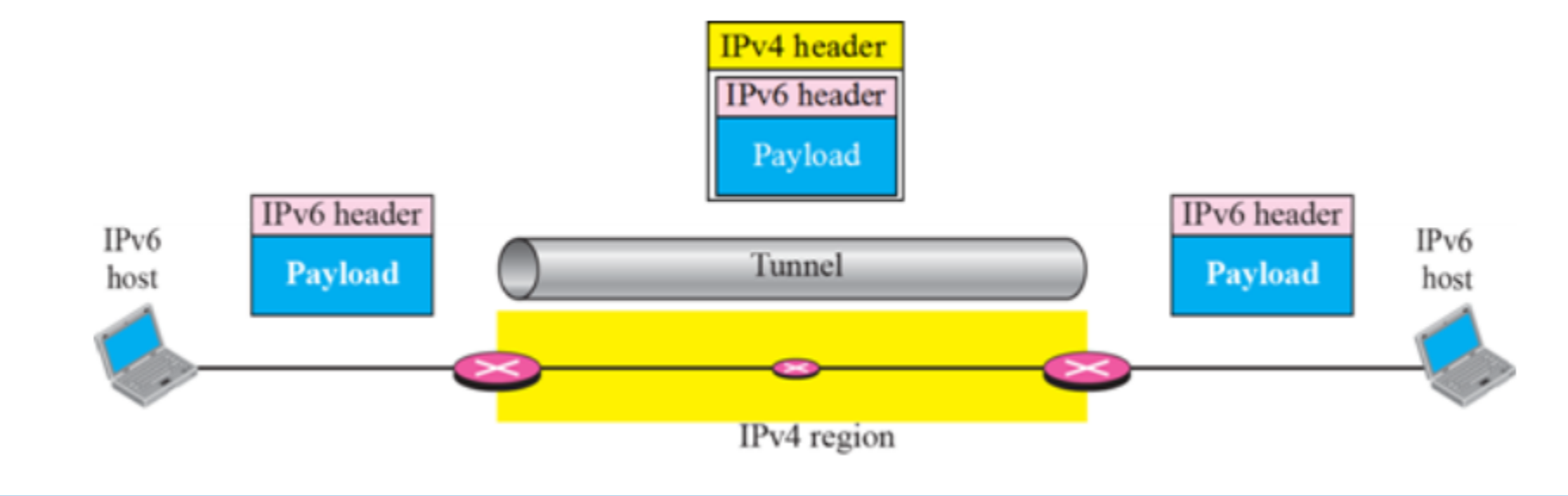


TRANSITION FROM IPv4 to IPv6



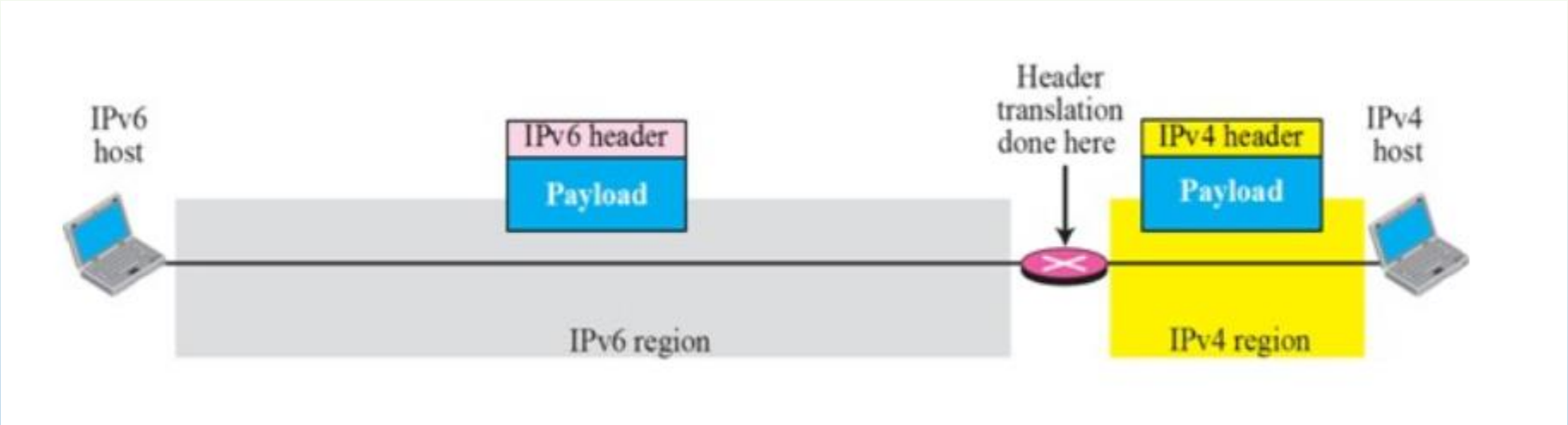
Dual Stack

TRANSITION FROM IPv4 to IPv6



Tunneling

TRANSITION FROM IPv4 to IPv6



Header Translation

ADDRESS MAPPING

- An internet is made of a combination of physical networks connected by internetworking devices such as routers.
- A packet starting from a source host may pass through several different physical networks before finally reaching the destination host.
- The hosts and routers are recognized at the network level by their logical (IP) addresses. However, packets pass through physical networks to reach these hosts and routers.
- At the physical level, the hosts and routers are recognized by their physical addresses.
- A physical address is a local address.
- The physical address and the logical address are two different identifiers.
- This means that delivery of a packet to a host or a router requires two levels of addressing: logical and physical.
- We need to be able to map a logical address to its corresponding physical address and vice versa. These can be done by using either static or dynamic mapping.

MAPPING LOGICAL TO PHYSICAL ADDRESS: ARP

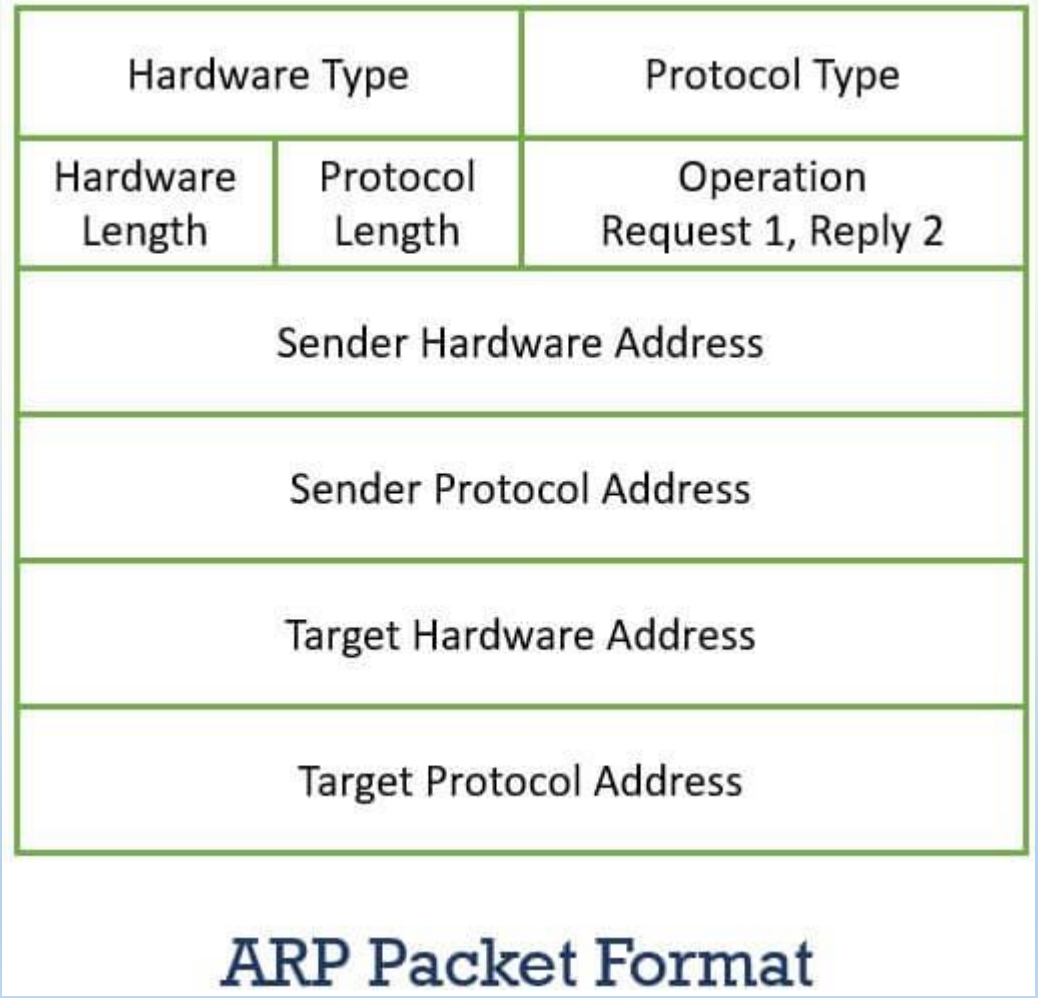
- Anytime a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the receiver.
- The logical (IP) address is obtained from the DNS if the sender is the host or it is found in a routing table if the sender is a router.
- But the IP datagram must be encapsulated in a frame to be able to pass through the physical network. This means that the sender needs the physical address of the receiver.
- The host or the router sends an ARP query packet. The packet includes the physical and IP addresses of the sender and the IP address of the receiver.
- Because the sender does not know the physical address of the receiver, the query is broadcast over the network.
- Every host or router on the network receives and processes the ARP query packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.
- The response packet contains the recipient's IP and physical addresses.
- The packet is unicast directly to the inquirer by using the physical address received in the query packet.

MAPPING LOGICAL TO PHYSICAL ADDRESS: ARP

Cache Memory

- Using ARP is inefficient if system A needs to broadcast an ARP request for each IP packet it needs to send to system B.
- It could have broadcast the IP packet itself. ARP can be useful if the ARP reply is cached (kept in cache memory for a while) because a system normally sends several packets to the same destination.

MAPPING LOGICAL TO PHYSICAL ADDRESS: ARP



ARP Packet Format

MAPPING PHYSICAL TO LOGICAL ADDRESS

- There are occasions in which a host knows its physical address, but needs to know its logical address. This may happen in two cases:

1. A diskless station is just booted. The station can find its physical address by checking its interface, but it does not know its IP address.

2. An organization does not have enough IP addresses to assign to each station; it needs to assign IP addresses on demand. The station can send its physical address and ask for a short time lease.

MAPPING PHYSICAL TO LOGICAL ADDRESS: RARP

- Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address.
- Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine.
- To create an IP datagram, a host or a router needs to know its own IP address or addresses.
- The IP address of a machine is usually read from its configuration file stored on a disk file. However, a diskless machine is usually booted from ROM, which has minimum booting information.
- The ROM is installed by the manufacturer. It cannot include the IP address because the IP addresses on a network are assigned by the network administrator.
- The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol.

MAPPING PHYSICAL TO LOGICAL ADDRESS: RARP

- A RARP request is created and broadcast on the local network.
- Another machine on the local network that knows all the IP addresses will respond with a RARP reply.
- The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.
- There is a serious problem with RARP: Broadcasting is done at the data link layer.
- The physical broadcast address, all is in the case of Ethernet, does not pass the boundaries of a network.
- This means that if an administrator has several networks or several subnets, it needs to assign a RARP server for each network or subnet.
- This is the reason that RARP is almost obsolete.

MAPPING PHYSICAL TO LOGICAL ADDRESS: DHCP

- The Dynamic Host Configuration Protocol (DHCP) has been devised to provide static and dynamic address allocation that can be manual or automatic.
- **Static Address Allocation:** A DHCP server has a database that statically binds physical addresses to IP addresses.
- **Dynamic Address Allocation:** DHCP has a second database with a pool of available IP addresses. This second database makes DHCP dynamic.
- When a DHCP client requests a temporary IP address, the DHCP server goes to the pool of available (unused) IP addresses and assigns an IP address for a negotiable period of time.
- When a DHCP client sends a request to a DHCP server, the server first checks its static database. If an entry with the requested physical address exists in the static database, the permanent IP address of the client is returned.
- On the other hand, if the entry does not exist in the static database, the server selects an IP address from the available pool, assigns the address to the client, and adds the entry to the dynamic database.

MAPPING PHYSICAL TO LOGICAL ADDRESS: DHCP

- The dynamic aspect of DHCP is needed when a host moves from network to network or is connected and disconnected from a network.
- The addresses assigned from the pool are temporary addresses.
- The DHCP server issues a lease for a specific time. When the lease expires, the client must either stop using the IP address or renew the lease. The server has the option to agree or disagree with the renewal. If the server disagrees, the client stops using the address.
- **Manual and Automatic Configuration:** DHCP allows both manual and automatic configurations. Static addresses are created manually; dynamic addresses are created automatically.