The Internet Protocol (IP)

Forwarding and Addressing in the Internet

- Internet addressing and forwarding are important components of the Internet Protocol (IP).
- There are two versions of IP in use today
  - IP protocol version 4, which is usually referred to simply as IPv4
  - IP version 6

The Internet Protocol (IP)

Internet’s network layer has three major components.

- The first component is the IP protocol.
- The second major component is the routing component, which determines the path a datagram follows from source to destination.
- The final component of the network layer is a facility to report errors in datagrams and respond to requests for certain network-layer information.

The Internet Protocol (IP)

Internet Control Message Protocol (ICMP)

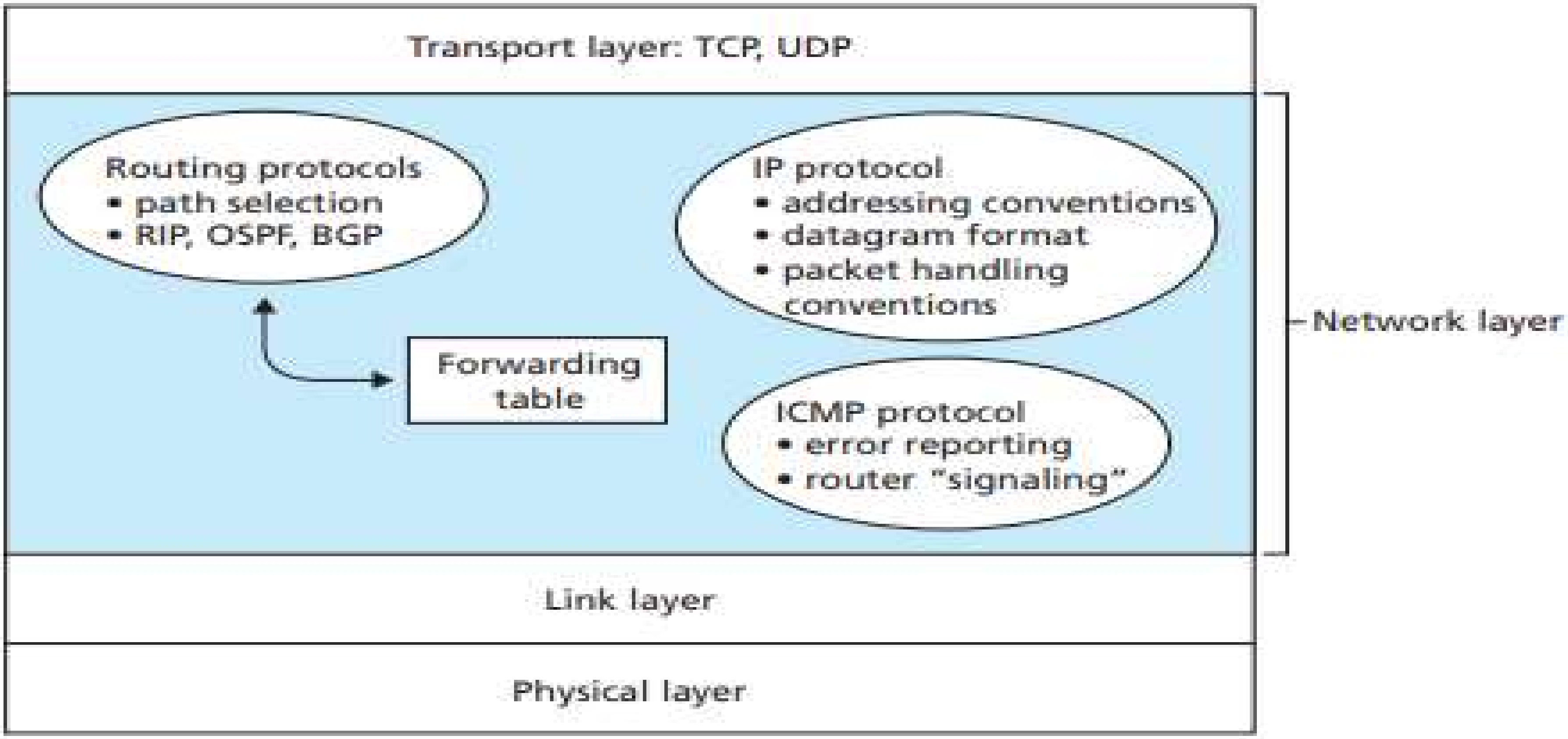
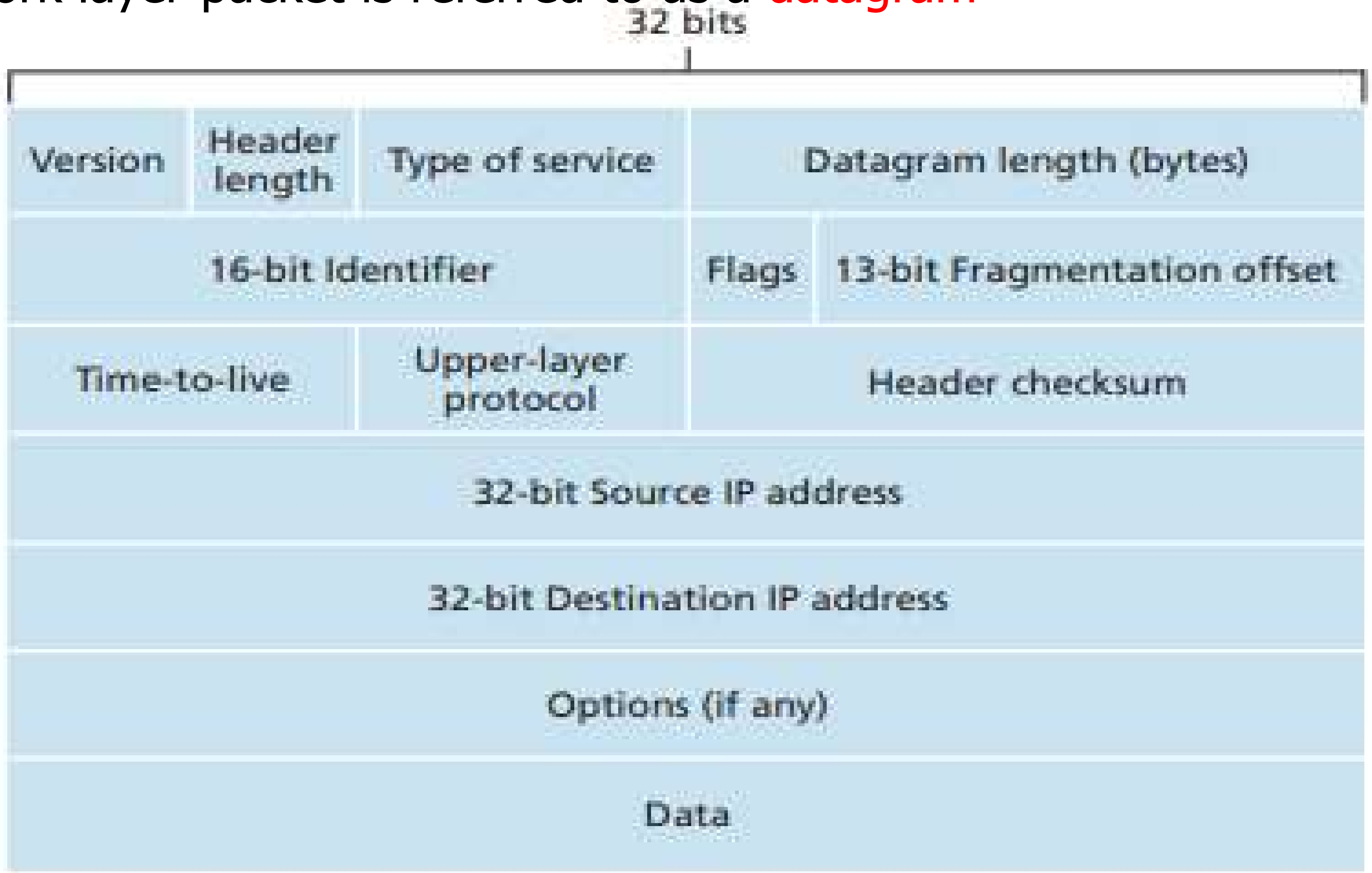


Figure 4.12 • A look inside the Internet's network layer

[James F Kurose and Keith W Ross, "Computer Networking: A Top - Down Approach", Pearson Education; 6 th Edition (2017)]

The Internet Protocol (IP): Datagram Format

- A network-layer packet is referred to as a datagram



32 bits

<table>
<tr><td colspan="4">Version</td><td colspan="4">Header length</td><td colspan="8">Type of service</td><td colspan="16">Datagram length (bytes)</td></tr>
<tr><td colspan="16">16-bit Identifier</td><td colspan="3">Flags</td><td colspan="13">13-bit Fragmentation offset</td></tr>
<tr><td colspan="8">Time-to-live</td><td colspan="8">Upper-layer protocol</td><td colspan="16">Header checksum</td></tr>
<tr><td colspan="32">32-bit Source IP address</td></tr>
<tr><td colspan="32">32-bit Destination IP address</td></tr>
<tr><td colspan="32">Options (if any)</td></tr>
<tr><td colspan="32">Data</td></tr>
</table>

Figure 4.13 ♦ IPv4 datagram format

[James F Kurose and Keith W Ross, "Computer Networking: A Top - Down Approach", Pearson Education; 6 th Edition (2017)]

IPv4 Datagram Format

- Version number: These 4 bits specify the IP protocol version of the datagram. By looking at the version number, the router can determine how to interpret the remainder of the IP datagram.

- Header length: Because an IPv4 datagram can contain a variable number of options (which are included in the IPv4 datagram header), these 4 bits are needed to determine where in the IP datagram the data actually begins.
- Most IP datagrams do not contain options, so the typical IP datagram has a 20-byte header.

IPv4 Datagram Format

- Type of service: The type of service (ToS) bits were included in the IPv4 header to allow different types of IP datagrams (for example, datagrams particularly requiring low delay, high throughput, or reliability) to be distinguished from each other. For example, it might be useful to distinguish real-time datagrams (such as those used by an IP telephony application) from non-real-time traffic (for example, FTP).

- Datagram length: This is the total length of the IP datagram (header plus data), measured in bytes. Since this field is 16 bits long, the theoretical maximum size of the IP datagram is 65,535 bytes. However, datagrams are rarely larger than 1,500 bytes.

IPv4 Datagram Format

- Identifier, flags, fragmentation offset: These three fields have to do with so-called IP fragmentation.

- Time-to-live: The time-to-live (TTL) field is included to ensure that datagrams do not circulate forever in the network. This field is decremented by one each time the datagram is processed by a router. If the TTL field reaches 0, the datagram must be dropped.

- Protocol: This field is used only when an IP datagram reaches its final destination. The value of this field indicates the specific transport layer protocol. For example, a value of 6 indicates that the data portion is passed to TCP, while a value of 17 indicates that the data is passed to UDP.

IPv4 Datagram Format

- Header checksum: The header checksum aids a router in detecting bit errors in a received IP datagram. The header checksum is computed by treating each 2 bytes in the header as a number and summing these numbers using 1s complement arithmetic.

- Source and destination IP addresses: When a source creates a datagram, it inserts its IP address into the source IP address field and inserts the address of the ultimate destination into the destination IP address field. Often the source host determines the destination address via a DNS lookup.

IPv4 Datagram Format

- Options : The options fields allow an IP header to be extended.

- Data(payload) : The data field of the IP datagram contains the transport-layer segment (TCP or UDP) to be delivered to the destination. However, the data field can carry other types of data, such as ICMP messages.

- Note that an IP datagram has a total of 20 bytes of header (assuming no options). If the datagram carries a TCP segment, then each (nonfragmented) datagram carries a total of 40 bytes of header (20 bytes of IP header + 20 bytes of TCP header) along with the application-layer message.

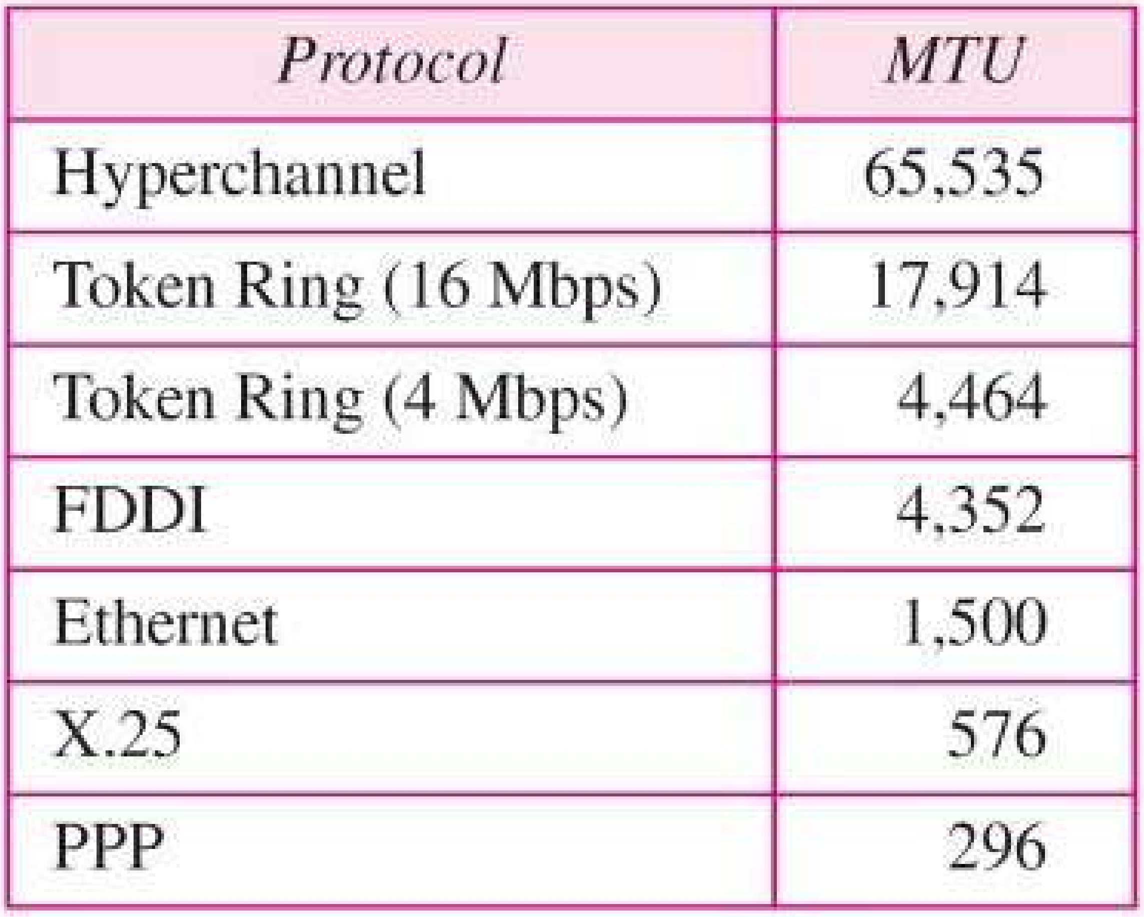
IP Datagram Fragmentation

- Not all link-layer protocols can carry network-layer packets of the same size.
- Some protocols can carry big datagrams, whereas other protocols can carry only little packets.
- For example, Ethernet frames can carry up to 1,500 bytes of data, whereas frames for some wide-area links can carry no more than 576 bytes.
- The maximum amount of data that a link-layer frame can carry is maximum transmission unit (MTU).

IP Datagram Fragmentation

- A router that interconnects several links, each running different link layer protocols with different MTUs.

MTUs for some networks



Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

IP Datagram Fragmentation

- Suppose router receive an IP datagram from one link. The forwarding table determine the outgoing link, and this outgoing link has an MTU that is smaller than the length of the IP datagram.

IP Datagram Fragmentation

- How are you going to squeeze this oversized IP datagram into the payload field of the link-layer frame?

IP Datagram Fragmentation

- How are you going to squeeze this oversized IP datagram into the payload field of the link-layer frame?

- The solution is to fragment the data in the IP datagram into two or more smaller IP datagrams, encapsulate each of these smaller IP datagrams in a separate link-layer frame; and send these frames over the outgoing link.
- Each of these smaller datagrams is referred to as a fragment.
- Fragments need to be reassembled before they reach the transport layer at the destination.
- The designers of IPv4 decided to put the job of datagram reassembly in the end systems rather than in network routers.

IP Datagram Fragmentation

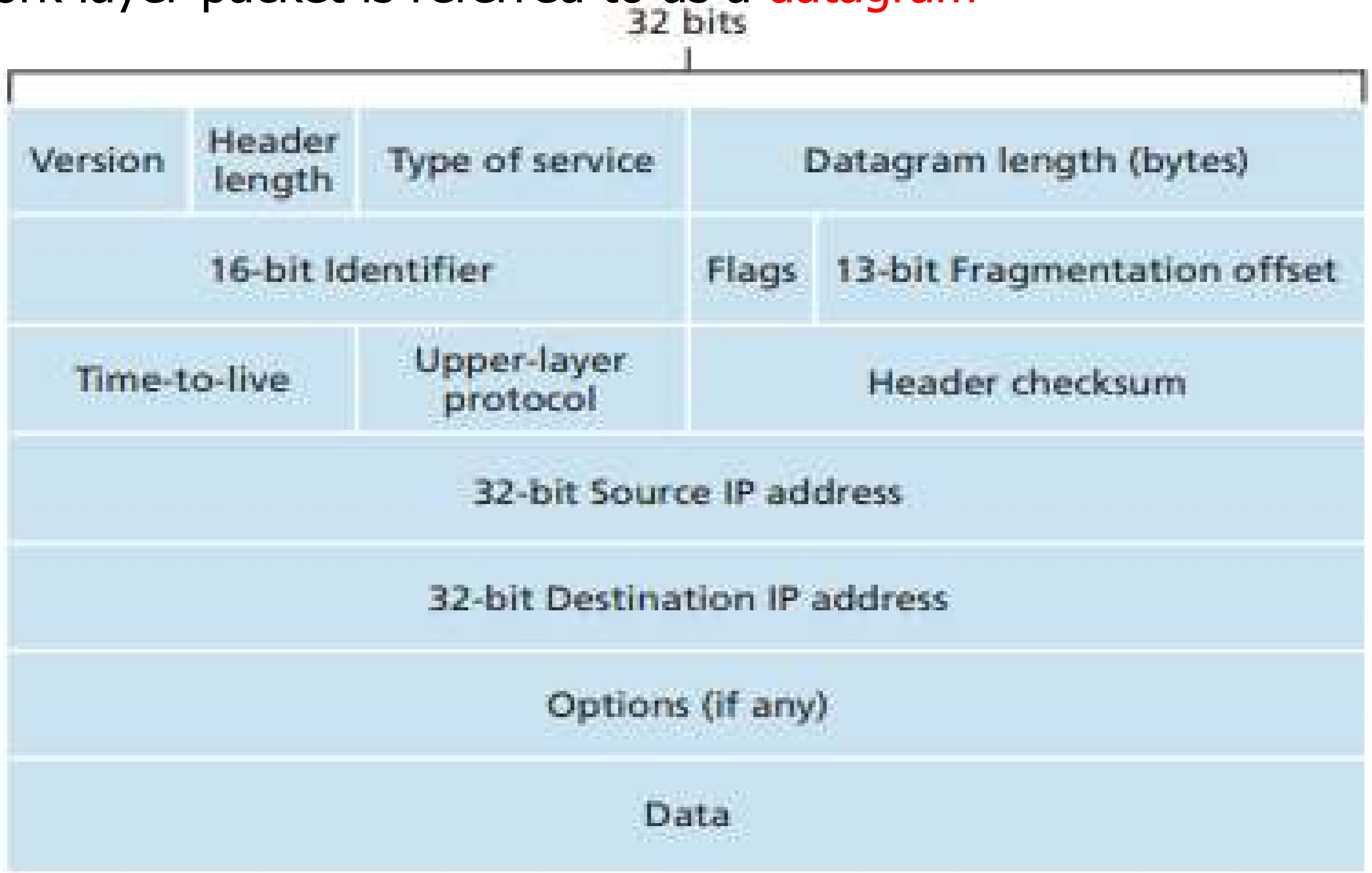
- When a destination host receives a series of datagrams from the same source, it needs to determine whether any of these datagrams are fragments of some original, larger datagram.

- If some datagrams are fragments, it must further determine when it has received the last fragment and how the fragments it has received should be pieced back together to form the original datagram.

- To allow the destination host to perform these reassembly tasks, the designers of IP (version 4) put identification, flag, and fragmentation offset fields in the IP datagram header.

The Internet Protocol (IP): Datagram Format

- A network-layer packet is referred to as a datagram



32 bits

Version | Header length | Type of service | Datagram length (bytes)

16-bit Identifier | Flags | 13-bit Fragmentation offset

Time-to-live | Upper-layer protocol | Header checksum

32-bit Source IP address

32-bit Destination IP address

Options (if any)

Data

Figure 4.13 ◆ IPv4 datagram format

[James F Kurose and Keith W Ross, "Computer Networking: A Top - Down Approach", Pearson Education; 6 th Edition (2017)]

IP Datagram Fragmentation

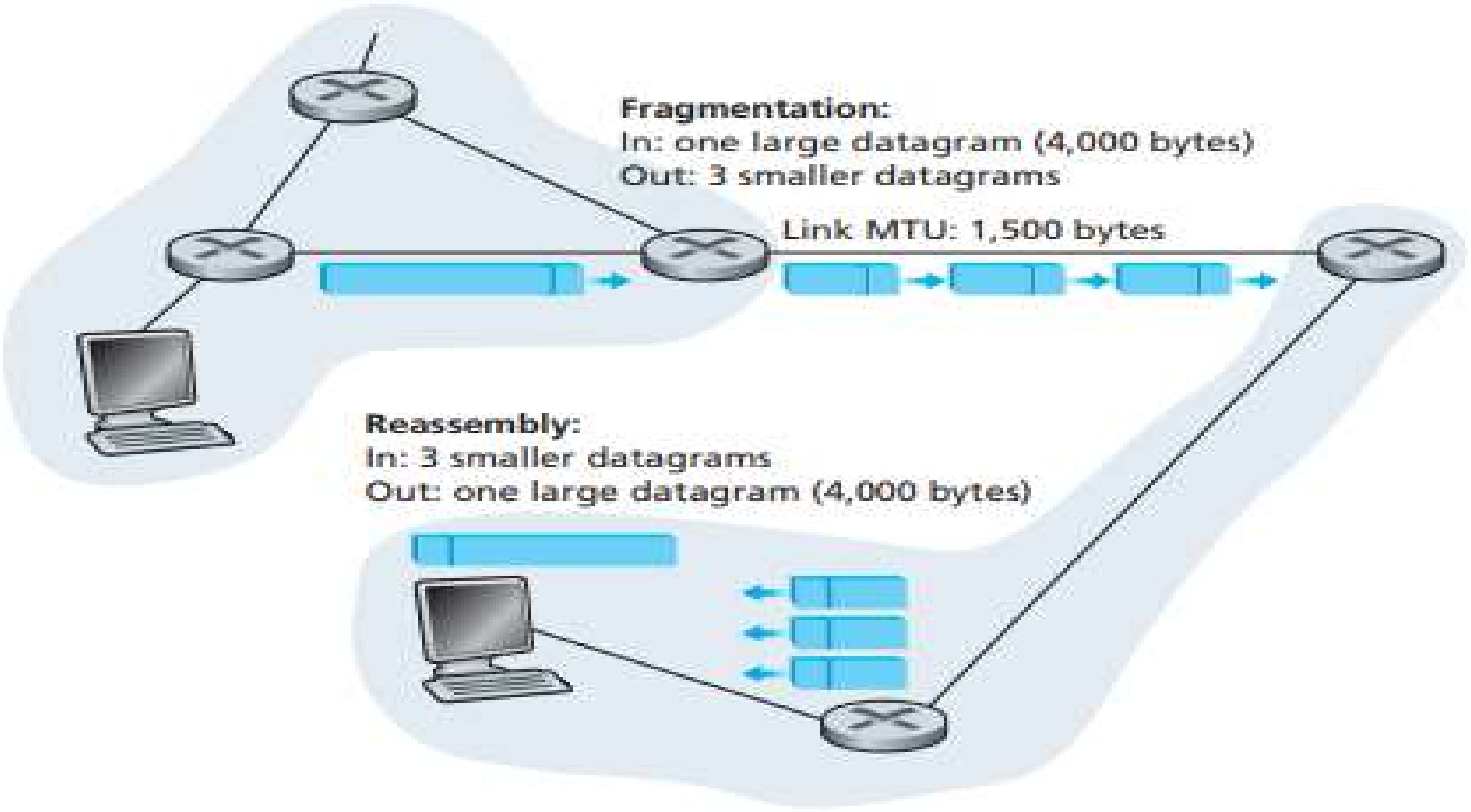


Figure 4.14 • IP fragmentation and reassembly

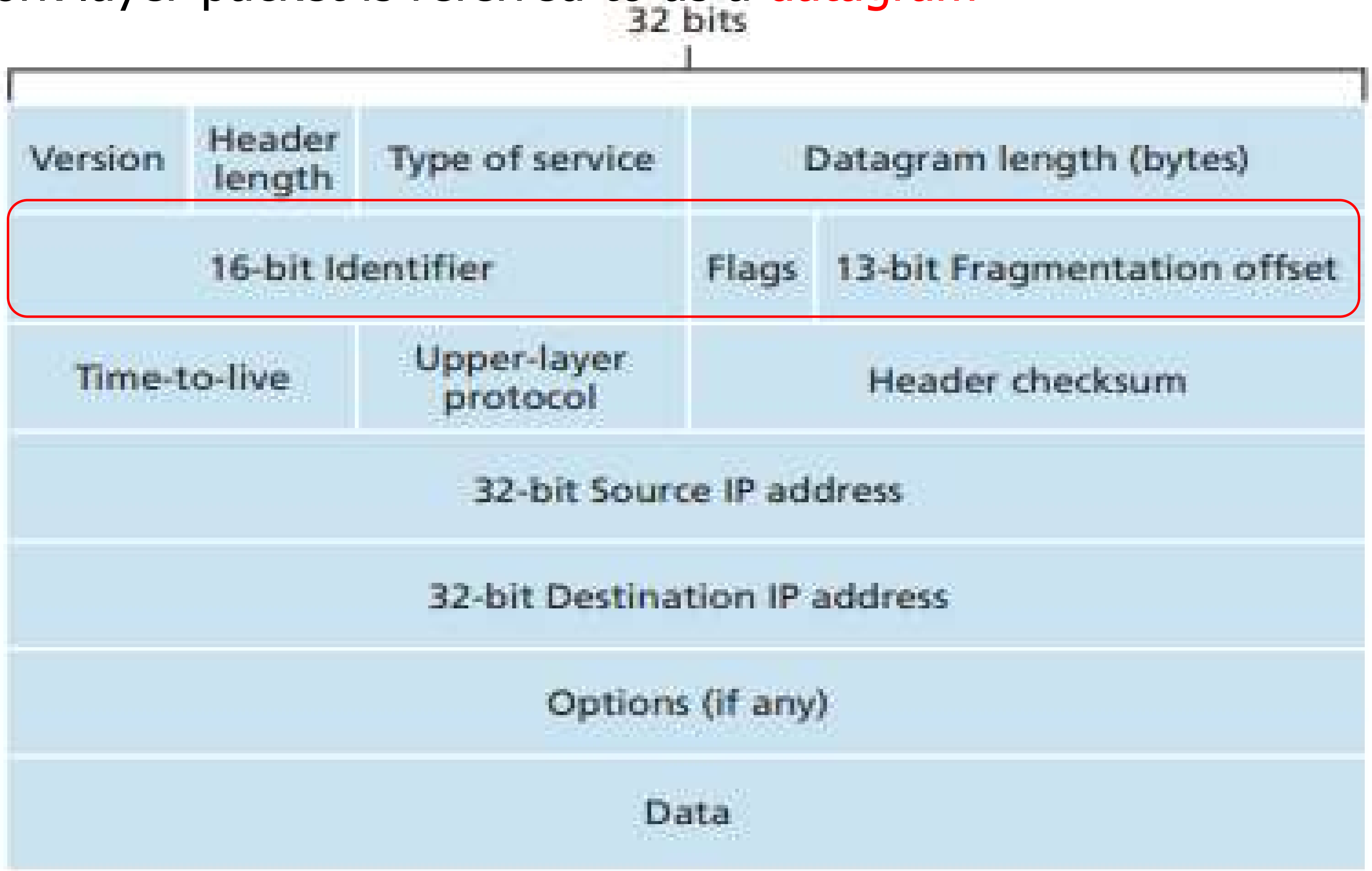
[James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)]

IP Datagram Fragmentation

- At the destination, the payload of the datagram is passed to the transport layer only after the IP layer has fully reconstructed the original IP datagram.
- If one or more of the fragments does not arrive at the destination, the incomplete datagram is discarded and not passed to the transport layer.

The Internet Protocol (IP): Datagram Format

- A network-layer packet is referred to as a datagram



32 bits

<table>
<tr><td>Version</td><td>Header length</td><td>Type of service</td><td colspan="2">Datagram length (bytes)</td></tr>
<tr><td colspan="3">16-bit Identifier</td><td>Flags</td><td>13-bit Fragmentation offset</td></tr>
<tr><td colspan="2">Time-to-live</td><td>Upper-layer protocol</td><td colspan="2">Header checksum</td></tr>
<tr><td colspan="5">32-bit Source IP address</td></tr>
<tr><td colspan="5">32-bit Destination IP address</td></tr>
<tr><td colspan="5">Options (if any)</td></tr>
<tr><td colspan="5">Data</td></tr>
</table>

Figure 4.13 ♦ IPv4 datagram format

[James F Kurose and Keith W Ross, "Computer Networking: A Top - Down Approach", Pearson Education; 6 th Edition (2017)]

Fields Related to Fragmentation

- Identification: This 16-bit field identifies a datagram originating from the source host.
- The combination of the identification and source IP address must uniquely define a datagram as it leaves the source host.
- When a datagram is fragmented, the value in the identification field is copied into all fragments.
- The identification number helps the destination in reassembling the datagram. It knows that all fragments having the same identification value should be assembled into one datagram.

Fields Related to Fragmentation

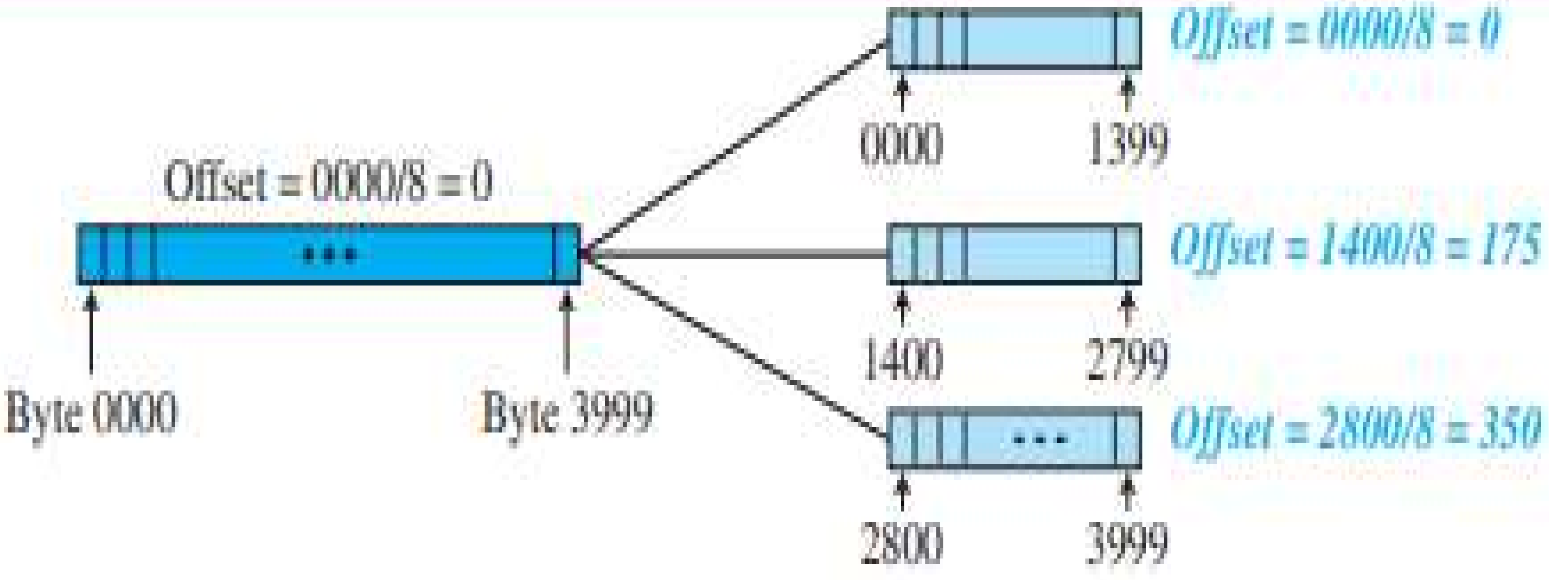
- Flags: This is a three-bit field. The first bit is reserved (not used).
- The second bit is called the do not fragment bit.
- If its value is 1, the machine must not fragment the datagram.
- If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host.
- If its value is 0, the datagram can be fragmented if necessary.

Fields Related to Fragmentation

- The third bit is called the more fragment bit.
- If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one.
- If its value is 0, it means this is the last or only fragment.
- The 13-bit fragmentation offset field shows the relative position of this fragment with respect to the whole datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.

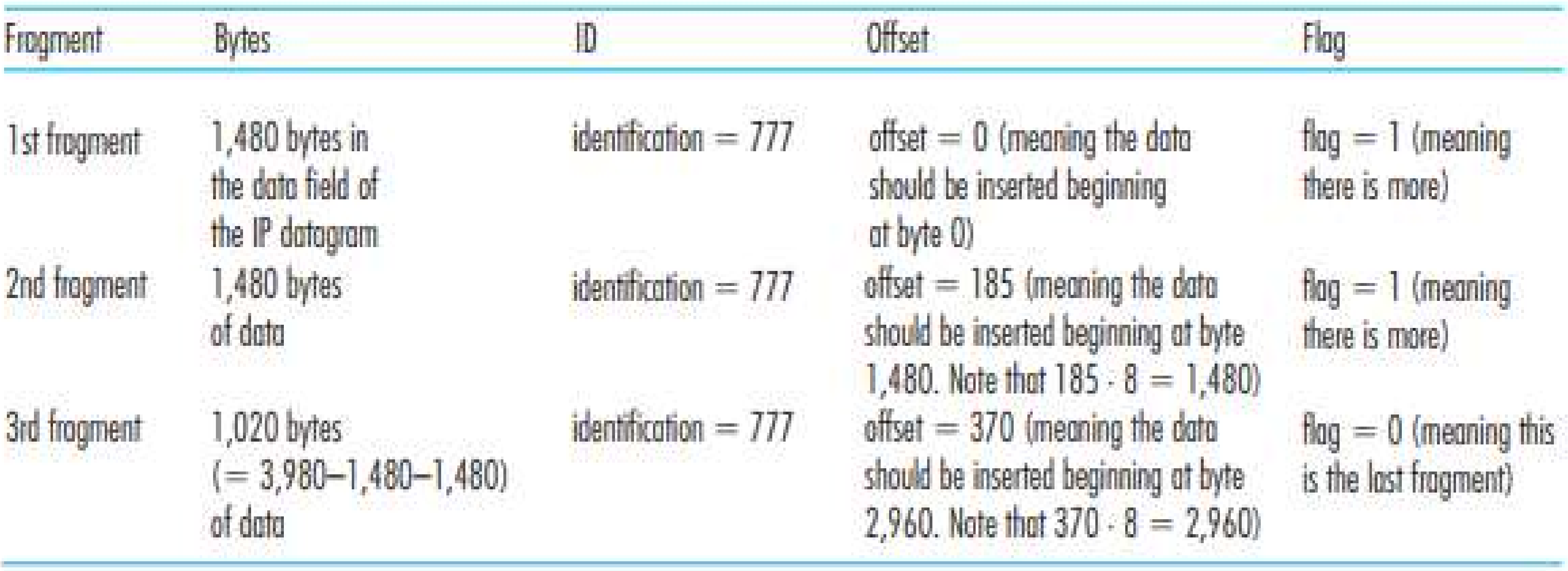
Fields Related to Fragmentation

Figure 4.27 *Fragmentation example*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Fields Related to Fragmentation



Fragment	Bytes	ID	Offset	Flag
1st fragment	1,480 bytes in the data field of the IP datagram	identification = 777	offset = 0 (meaning the data should be inserted beginning at byte 0)	flag = 1 (meaning there is more)
2nd fragment	1,480 bytes of data	identification = 777	offset = 185 (meaning the data should be inserted beginning at byte 1,480. Note that 185 · 8 = 1,480)	flag = 1 (meaning there is more)
3rd fragment	1,020 bytes (= 3,980–1,480–1,480) of data	identification = 777	offset = 370 (meaning the data should be inserted beginning at byte 2,960. Note that 370 · 8 = 2,960)	flag = 0 (meaning this is the last fragment)

Table 4.2 ♦ IP fragments

- A datagram of 4,000 bytes (20 bytes of IP header plus 3,980 bytes of IP payload) arrives at a router and must be forwarded to a link with an MTU of 1,500 bytes. This implies that the 3,980 data bytes in the original datagram must be allocated to three separate fragments (each of which is also an IP datagram).
- Suppose that the original datagram is stamped with an identification number of 777

[James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)]

IP Datagram Fragmentation

- Fragmentation also has its costs.
- First, it complicates routers and end systems, which need to be designed to accommodate datagram fragmentation and reassembly.
- Second, fragmentation can be used to create DoS attacks, whereby the attacker sends a series of unexpected fragments, where the attacker sends a stream of small fragments to the target host, none of which has an offset of zero.

IP Datagram Fragmentation

- The target can collapse as it attempts to rebuild datagrams out of the degenerate packets.
- Another class of exploits sends overlapping IP fragments, fragments whose offset values are set so that the fragments do not align properly.
- Vulnerable operating systems, not knowing what to do with overlapping fragments, can crash .
- A new version of the IP protocol, IPv6, does away with fragmentation altogether, thereby streamlining IP packet processing and making IP less vulnerable to attack.

IPv4 Addressing

- A host typically has only a single link into the network; when IP in the host wants to send a datagram, it does so over this link.
- The boundary between the host and the physical link is called an interface.
- A router has multiple interfaces, one for each of its links.
- Because every host and router is capable of sending and receiving IP datagrams, IP requires each host and router interface to have its own IP address.
- Thus, an IP address is technically associated with an interface.
- Each IP address is 32 bits long (equivalently, 4 bytes), and there are thus a total of 2^{32} possible IP addresses.

IPv4 Addressing

- The identifier used in the IP layer of the TCP/IP protocol suite to identify each device connected 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 host or a router to the Internet.
- An IP address is the address of the interface.
- The IPv4 addresses are unique and universal.

IP Address Notation

There are three common notations to show an IPv4 address:

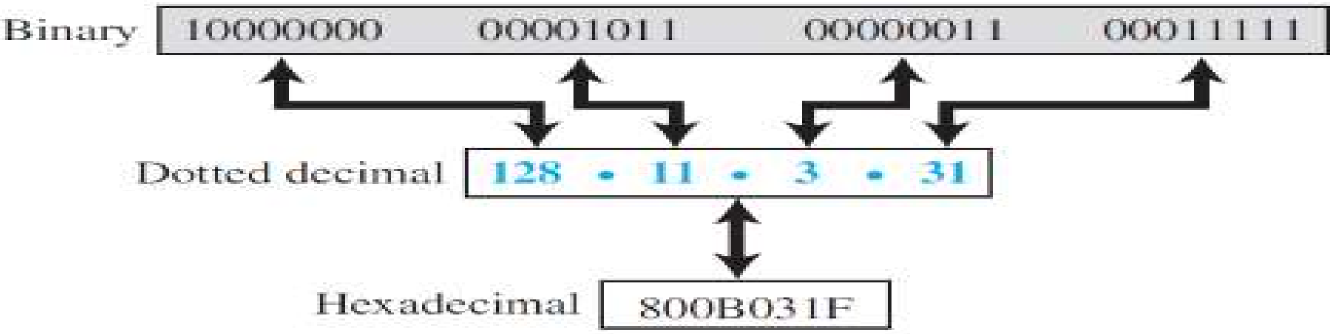
1.binary notation (base 2)

2.dotted-decimal notation (base 256)

3.hexadecimal notation (base 16)

- The most prevalent, however, is base 256. Because each byte (octet) is only 8 bits, each number in the dotted-decimal notation is between 0 and 255

Figure 4.29 *Three different notations in IPv4 addressing*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

IP Address Notation

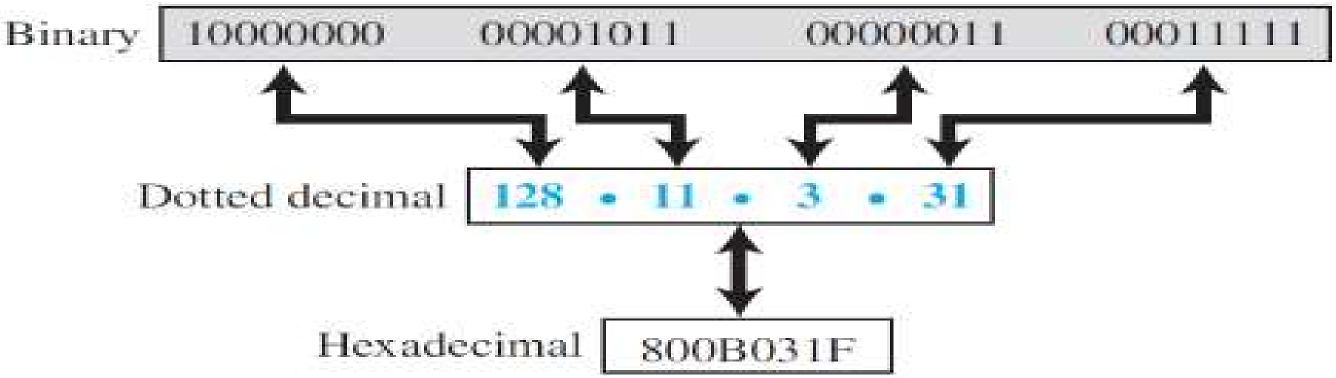


Figure 4.29 *Three different notations in IPv4 addressing*

[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

- Each byte of the address is written in its decimal form and is separated by a period (dot) from other bytes in the address.
- For example, consider the IP address 193.32.216.9. The 193 is the decimal equivalent of the first 8 bits of the address; the 32 is the decimal equivalent of the second 8 bits of the address, and so on.
- The address 193.32.216.9 in binary notation is 11000001 00100000 11011000 00001001

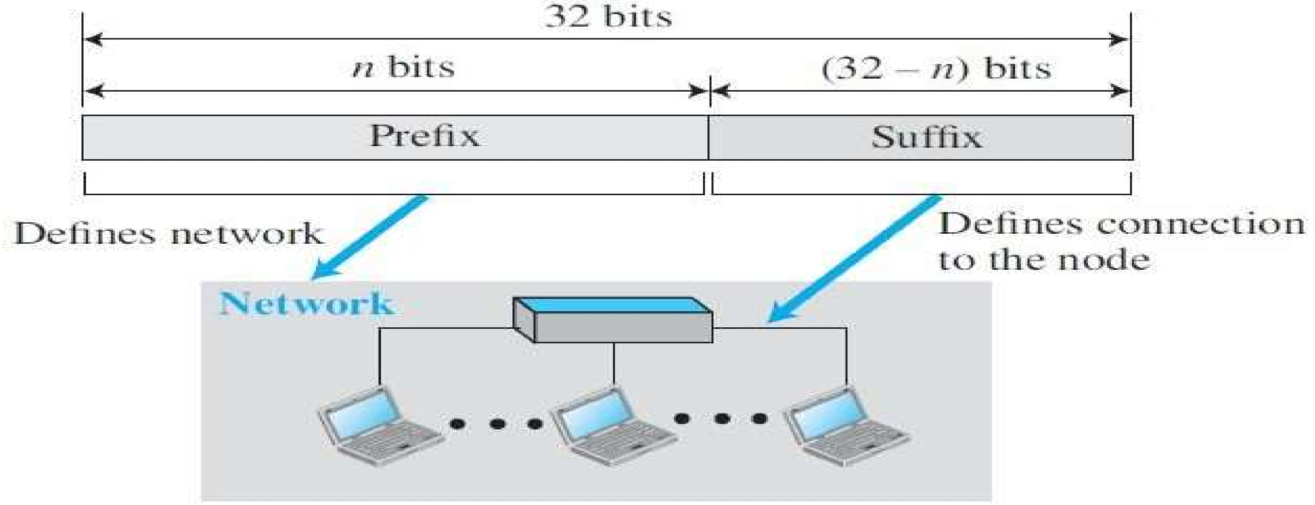
IP Address Notation

- Each interface on every host and router in the global Internet must have an IP address that is globally unique.
- A portion of an interface’s IP address will be determined by the subnet to which it is connected.

Hierarchy in Addressing

- A 32-bit IPv4 address is also hierarchical, but divided only 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 (connection of a device to the Internet).
- Figure shows the prefix and suffix of a 32-bit IPv4 address.

Figure 4.30 *Hierarchy in addressing*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Hierarchy in Addressing

- The prefix length is n bits and the suffix length is (32 – n) bits.
- A prefix can be fixed length or variable length.
- The network identifier in the IPv4 was first designed as a fixed-length prefix. This scheme, which is now obsolete, is referred to as classful addressing.
- The new scheme, which is referred to as classless addressing, uses a variable-length network prefix.

Classful Addressing

Classful addressing

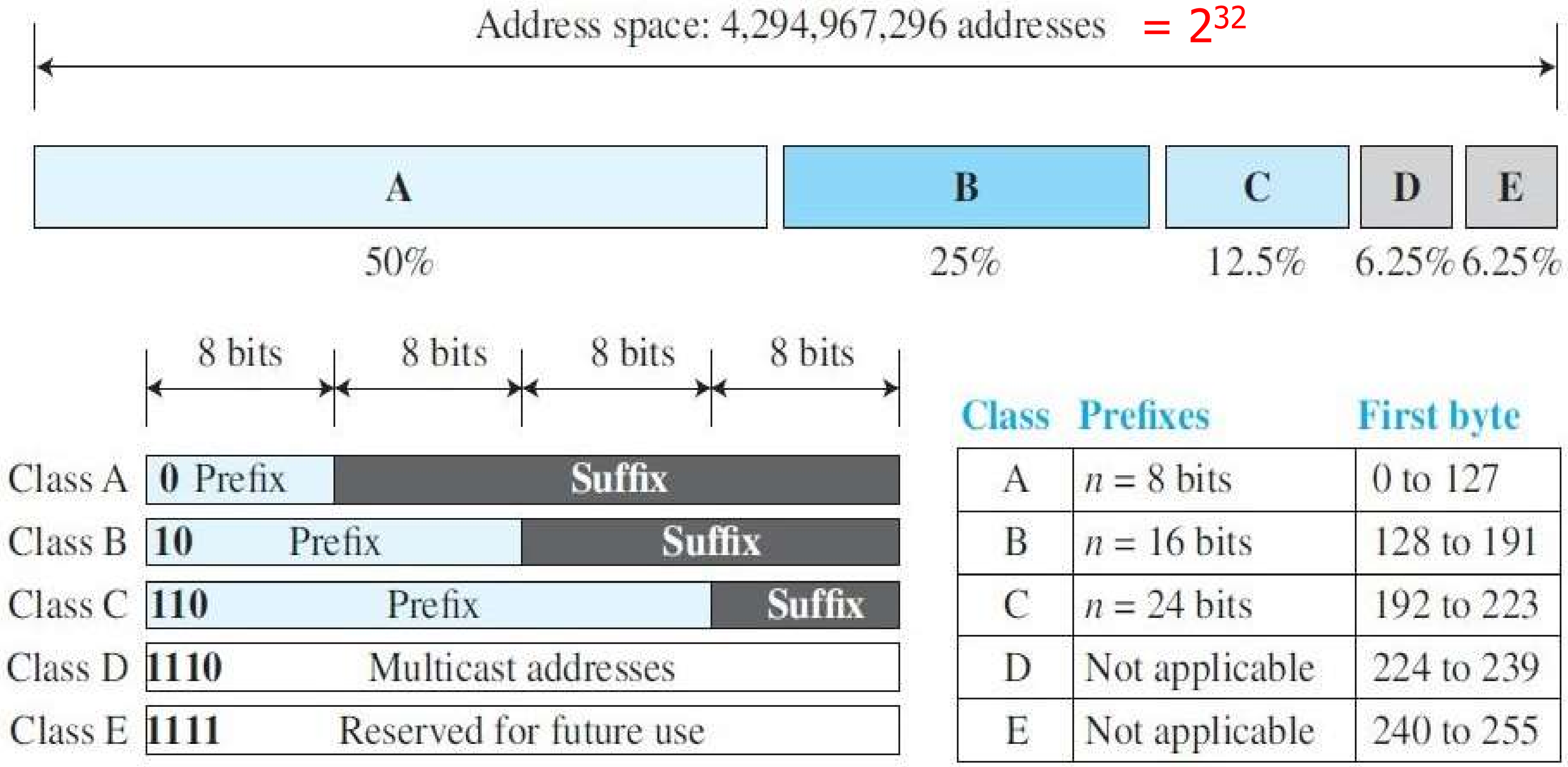
- When the Internet started, an IPv4 address was designed with a fixed-length prefix, but to accommodate both small and large networks, three fixed-length prefixes were designed instead of one (n = 8, n = 16, and n = 24).

- The whole address space was divided into five classes (class A, B, C, D, and E),

- This scheme is referred to as classful addressing.

Classful Addressing

Figure 4.31 *Occupation of the address space in classful addressing*

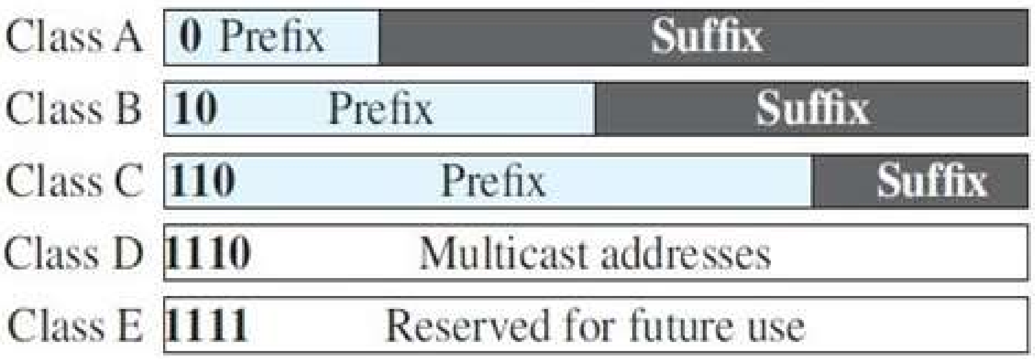


Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

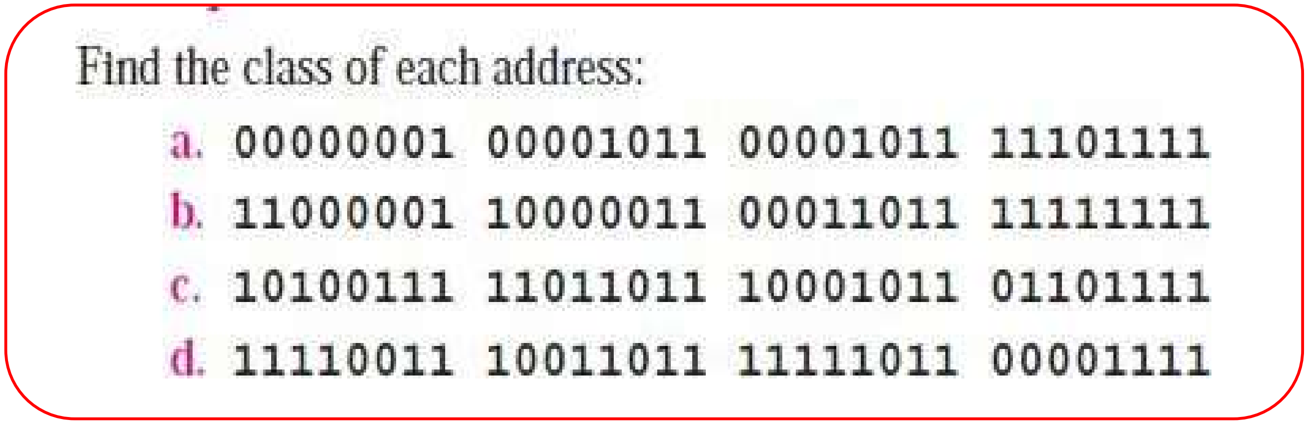
[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Classful Addressing

Finding Class of an IP Address



Class A	0 Prefix	Suffix
Class B	10 Prefix	Suffix
Class C	110 Prefix	Suffix
Class D	1110 Multicast addresses	
Class E	1111 Reserved for future use	



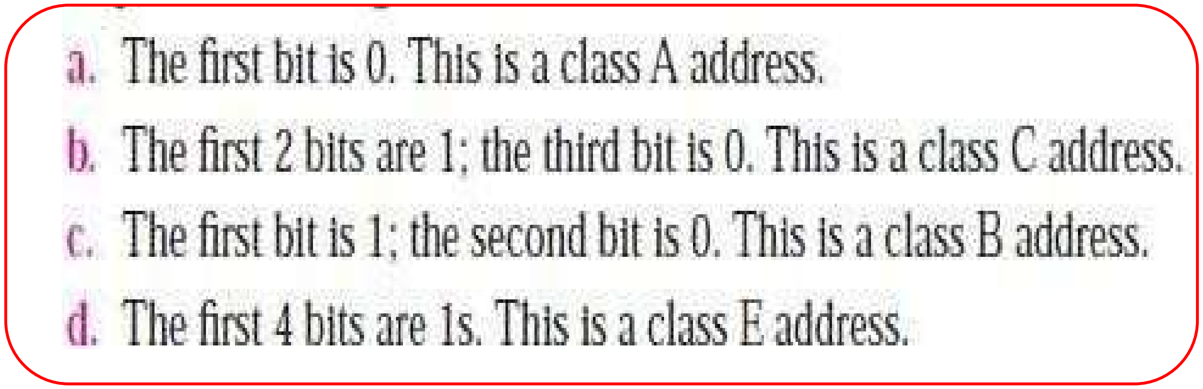
Find the class of each address:

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 10100111 11011011 10001011 01101111

d. 11110011 10011011 11111011 00001111



a. The first bit is 0. This is a class A address.

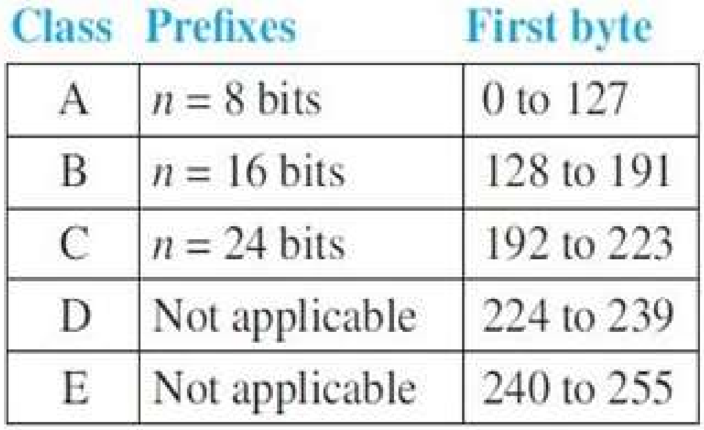
b. The first 2 bits are 1; the third bit is 0. This is a class C address.

c. The first bit is 1; the second bit is 0. This is a class B address.

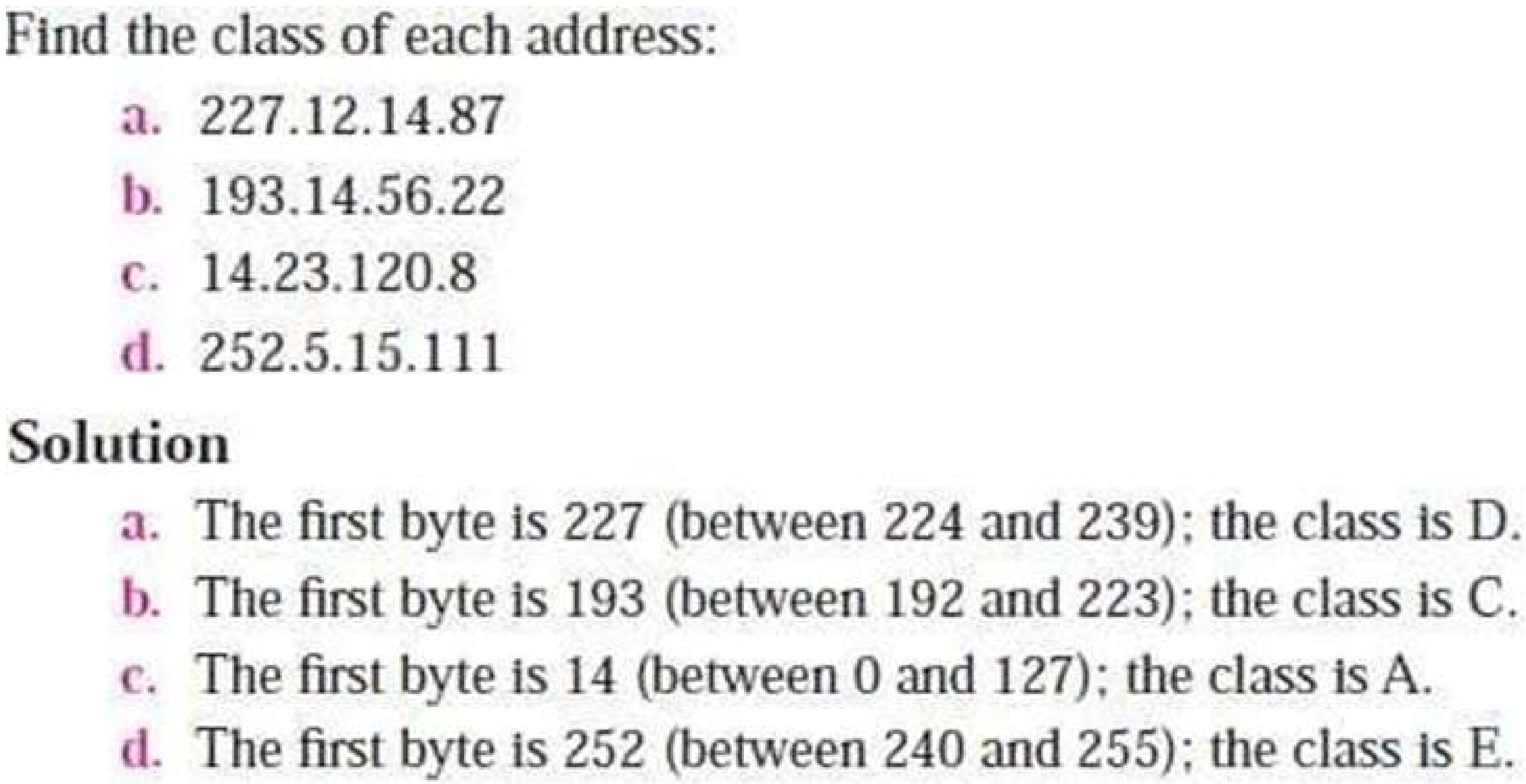
d. The first 4 bits are 1s. This is a class E address.

Classful Addressing

Finding Class of an IP Address



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



Find the class of each address:

a. 227.12.14.87

b. 193.14.56.22

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first byte is 227 (between 224 and 239); the class is D.

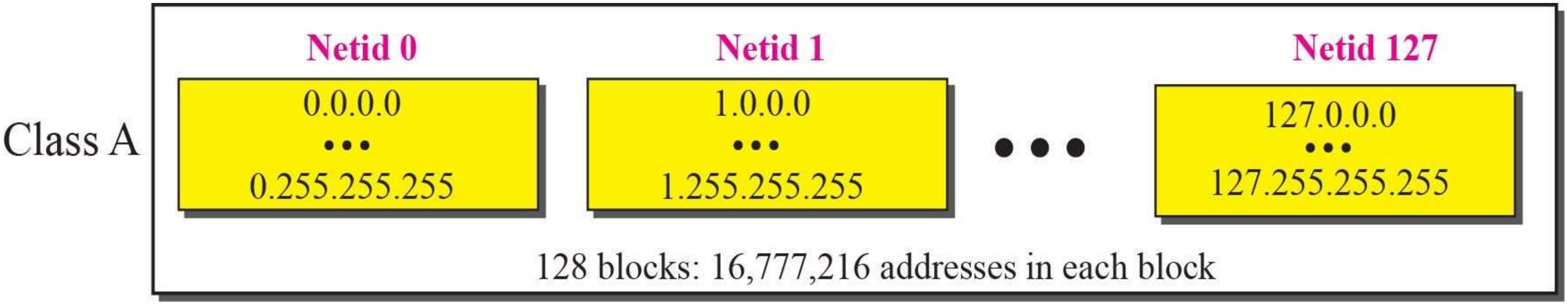
b. The first byte is 193 (between 192 and 223); the class is C.

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.

Classful Addressing

- One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size.
- In class A, the network length is 8 bits, but since the first bit, which is 0, defines the class, we can have only seven bits as the network identifier.
- This means there are only 2^7 = 128 networks/blocks in the world that can have a class A address.



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Classful Addressing

- In class B, the network length is 16 bits, but since the first two bits, which are (10), define the class, we can have only 14 bits as the network identifier. This means there are only 2^14 = 16,384 networks/blocks in the world that can have a class B address.
- All addresses that start with $(110)_2$ belong to class C. In class C, the network length is 24 bits, but since three bits define the class, we can have only 21 bits as the network identifier. This means there are 2^21 = 2,097,152 networks in the world that can have a class C address.
- Class D is not divided into prefix and suffix. It is used for multicast addresses.
- All addresses that start with 1111 in binary belong to class E. As in Class D, Class E is not divided into prefix and suffix and is used as reserve.

Classful Addressing

Address Depletion

- The reason that classful addressing has become obsolete is address depletion.
- Since the addresses were not distributed properly, the Internet was faced with the problem of the addresses being rapidly used up, resulting in no more addresses available for organizations and individuals that needed to be connected to the Internet.

Classful Addressing

Address Depletion

- Let us think about class A.
- This class can be assigned to only 128 organizations in the world, but each organization needs to have one single network (seen by the rest of the world) with 16,777,216 nodes (computers in this single network).
- Since there may be only a few organizations that are this large, most of the addresses in this class were wasted (unused).

Classful Addressing

Address Depletion

- Class B addresses were designed for midsize organization, but many of the addresses in this class also remained unused.

- Class C addresses have a completely different flaw in design. The number of addresses that can be used in each network (256) was so small that most companies were not comfortable using a block in this address.

- Class E addresses were almost never used, wasting the whole class.

Classful Addressing

Subnetting and Supernetting

- To alleviate address depletion, two strategies were proposed and implemented: subnetting and supernetting.

- In subnetting, a class A or class B block is divided into several subnets.
- Each subnet has a larger prefix length than the original network.
- For example, if a network in class A is divided into four subnets, each subnet has a prefix of $n_{sub} = 10$.
- At the same time, if all of the addresses in a network are not used, subnetting allows the address to be divided among several organizations.
- This idea did not work because most large organizations were not happy about dividing the block and giving some of the unused addresses to smaller organizations.

Classful Addressing

Subnetting and Supernetting

- While subnetting was devised to divide a large block into smaller ones, supernetting was devised to combine several class C blocks into a larger block to be attractive to organizations that need more than the 256 addresses available in a class C block.

- This idea did not work either because it makes the routing of packets more difficult.

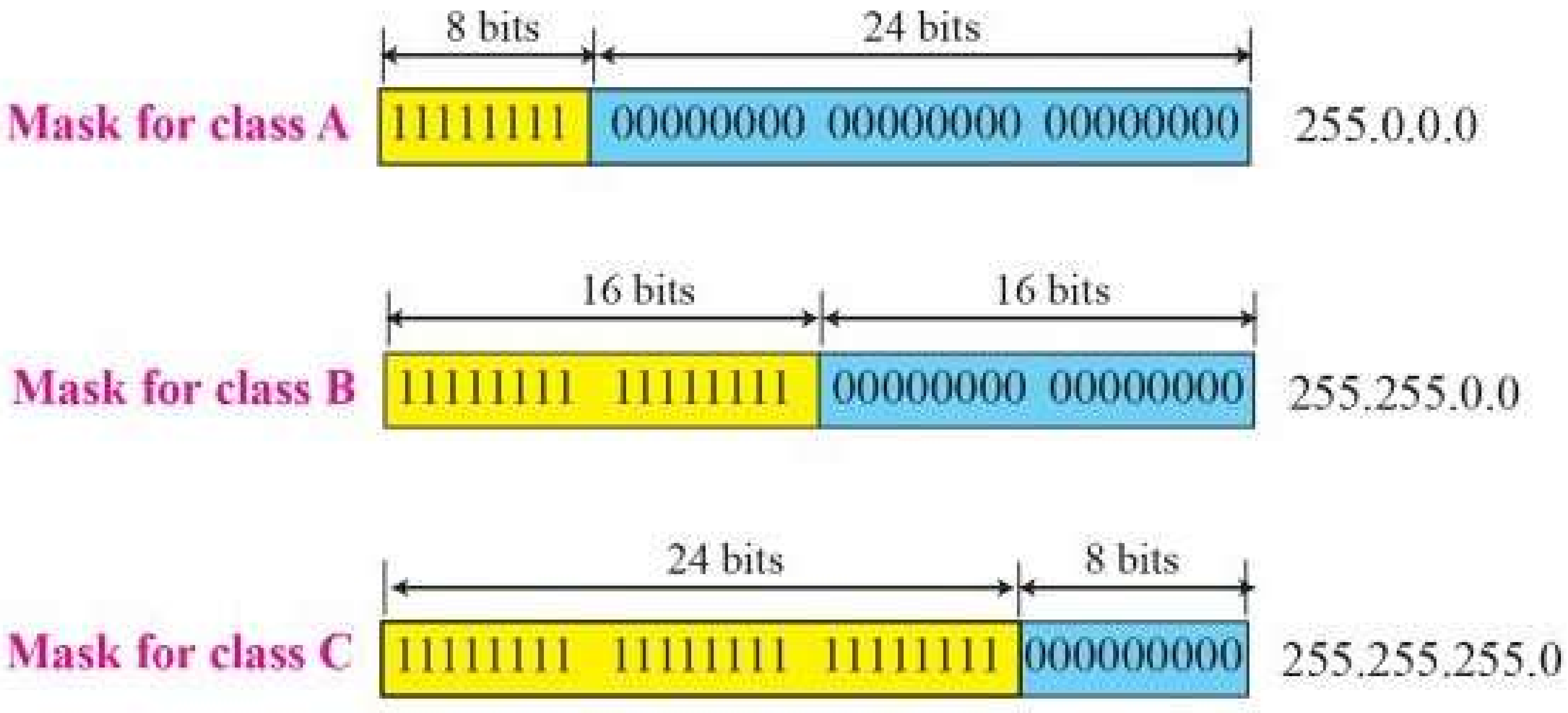
Advantage of Classful Addressing

- Although classful addressing had several problems and became obsolete, it had one advantage:

- Given an address, we can easily find the class of the address and, since the prefix length for each class is fixed, we can find the prefix length immediately.

- In other words, the prefix length in classful addressing is inherent in the address; no extra information is needed to extract the prefix and the suffix.

Network mask : Classful Addressing



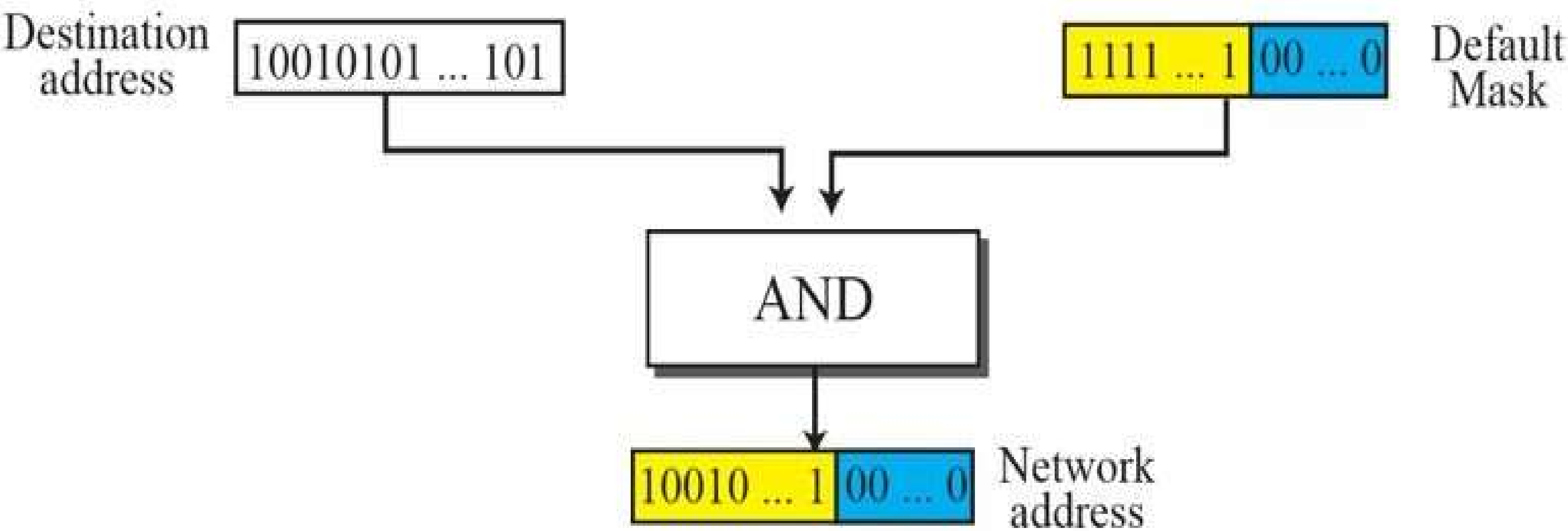
	8 bits	24 bits	
Mask for class A	11111111	00000000 00000000 00000000	255.0.0.0
	16 bits	16 bits	
Mask for class B	11111111 11111111	00000000 00000000	255.255.0.0
	24 bits	8 bits	
Mask for class C	11111111 11111111 11111111	000000000	255.255.255.0

- The address mask is a 32-bit number in which the n leftmost bits are set to 1s and the rest of the bits (32 – n) are set to 0s.
- A subnet mask is a 32-bit address that segregates(separates) an IP address into network bits that identify the network and host bits that identify the host device operating on that network.

[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]

Network mask : Classful Addressing

- Finding a network address using the default mask

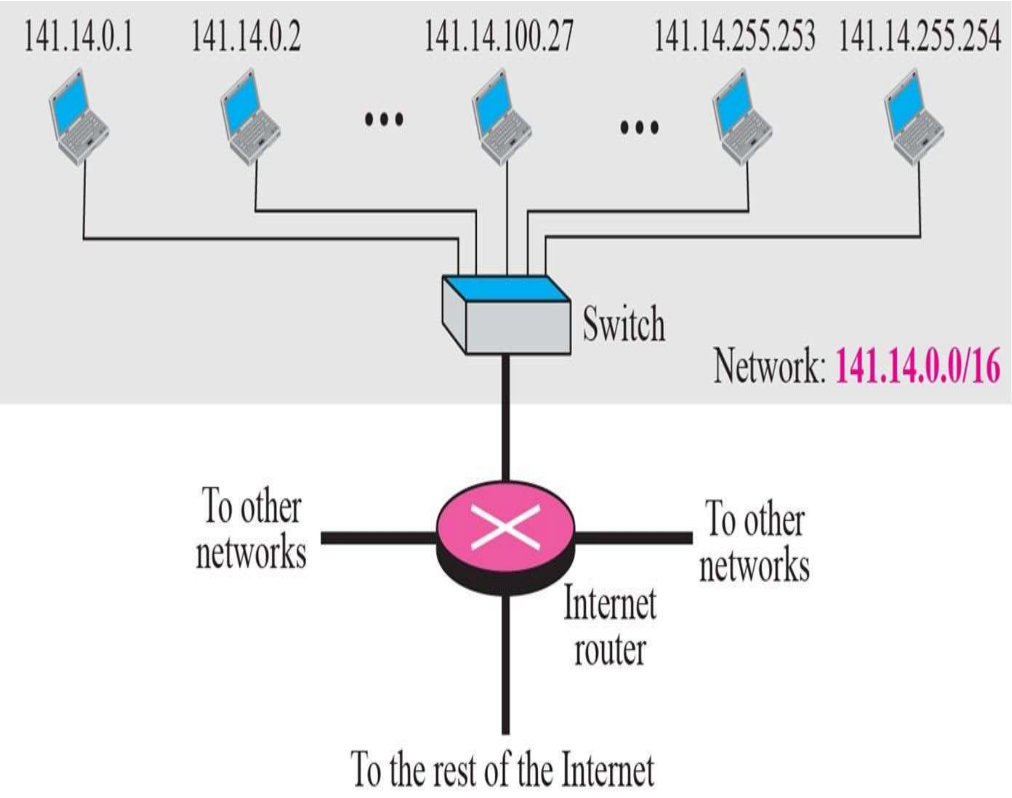


[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Three-Level Addressing: Subnetting

- The idea of splitting a block to smaller blocks is referred to as subnetting.
- In subnetting, a network is divided into several smaller smaller subnetworks (subnets) with each subnetwork having its own subnetwork address.

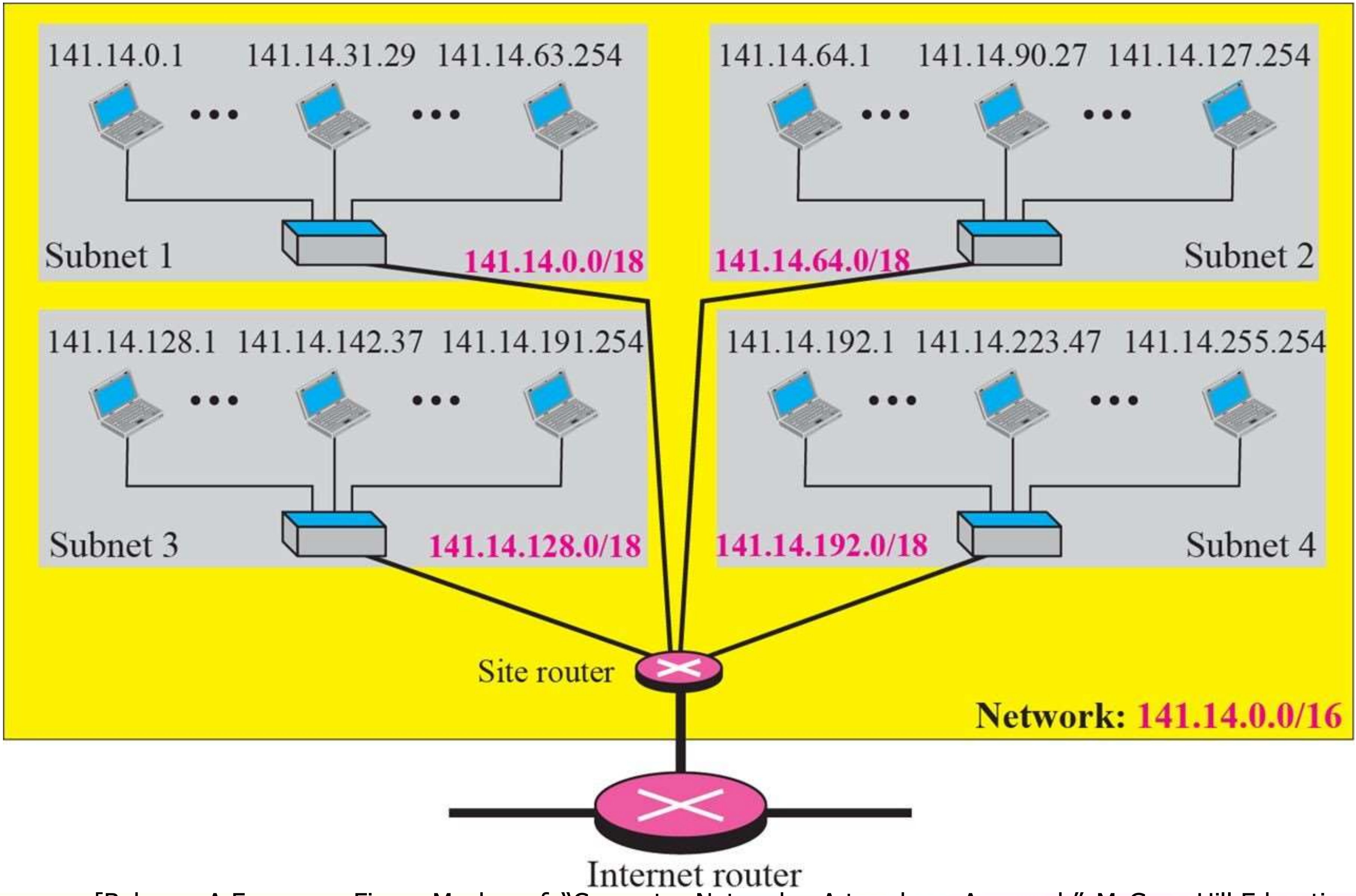
Before Subnetting



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

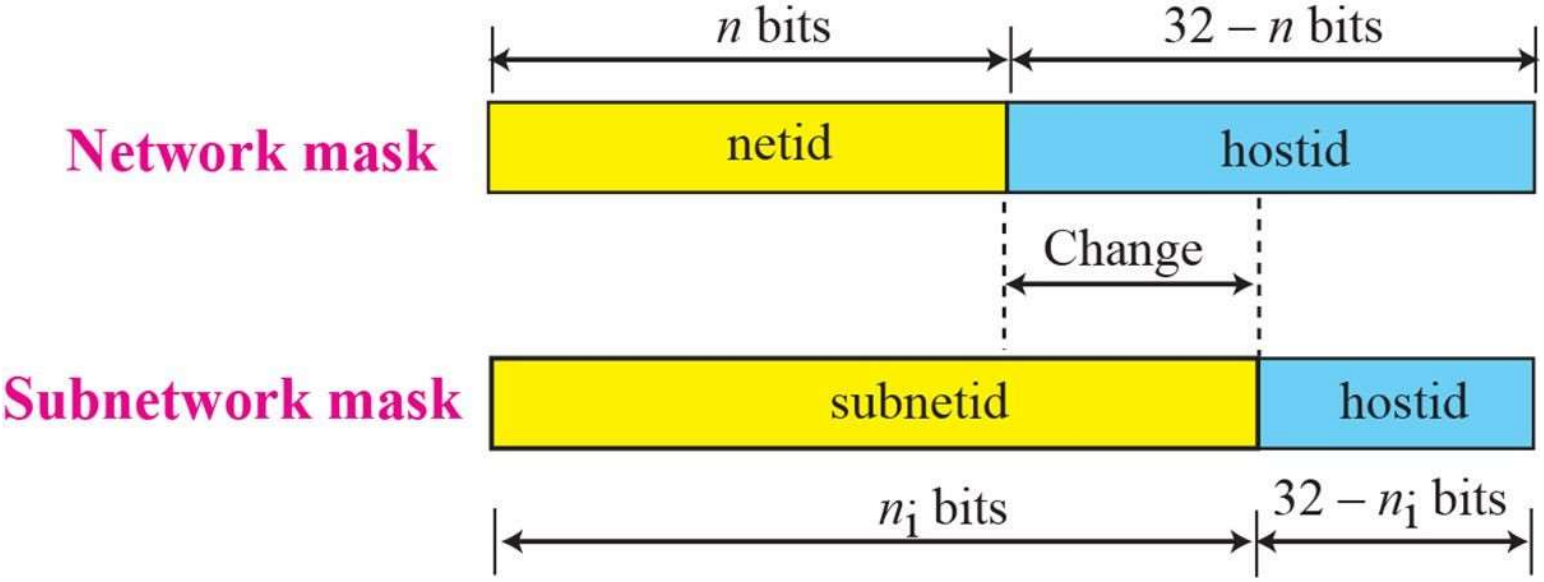
- Figure shows a network using class B(1st bit 128-191) addresses before subnetting.
- We have just one network with almost 2^{16} hosts.
- Note that we have shown /16 to show the length of the netid (class B), where the /16 notation, sometimes known as a subnet mask, indicates that the leftmost 16 bits of the 32-bit quantity define the subnet address.

After Subnetting



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Network Mask and Subnetwork Mask



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Classless Addressing

- Subnetting and supernetting in classful addressing did not really solve the address depletion problem.

- With the growth of the Internet, it was clear that a larger address space was needed as a long-term solution.

- The larger address space requires that the length of IP addresses also be increased, which means the format of the IP packets needs to be changed.

Classless Addressing

- Although the long-range solution has already been devised and is called IPv6, a short-term solution was also devised to use the same address space but to change the distribution of addresses to provide a fair share to each organization.

- The short-term solution still uses IPv4 addresses, but it is called classless addressing.

- In other words, the class privilege was removed from the distribution to compensate for the address depletion.

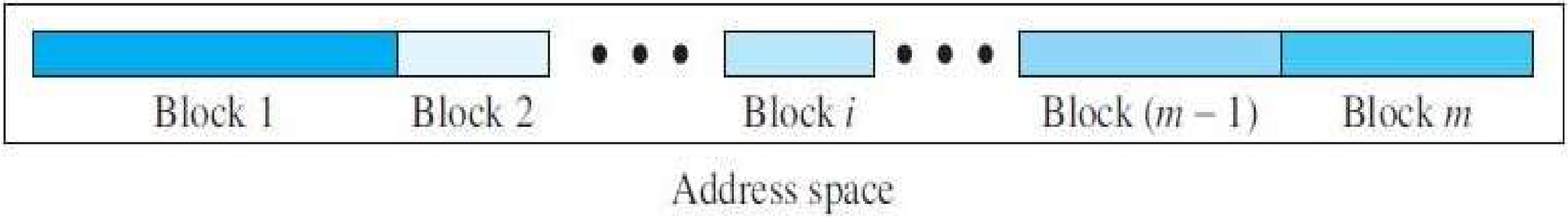
Classless Addressing

- In 1996, the Internet authorities announced a new architecture called classless addressing.
- In classless addressing, variable-length blocks are used that belong to no classes.
- We can have a block of 1 address, 2 addresses, 4 addresses, 128 addresses, and so on.
- 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).

Classless Addressing

- One of the restrictions, is that the number of addresses in a block needs to be a power of 2.
- An organization can be granted one block of addresses.
- Figure shows the division of the whole address space into non overlapping blocks.

Figure 4.32 *Variable-length blocks in classless addressing*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Classless Addressing

- Unlike classful addressing, the prefix length in classless addressing is variable.
- We can have a prefix length that ranges from 0 to 32.
- The size of the network is inversely proportional to the length of the prefix.
- A small prefix means a larger network; a large prefix means a smaller network.
- The idea of classless addressing can be easily applied to classful addressing.
- An address in class A can be thought of as a classless address in which the prefix length is 8.
- An address in class B can be thought of as a classless address in which the prefix is 16, and so on.
- In other words, classful addressing is a special case of classless addressing.

Prefix Length: Slash Notation (CIDR Notation)

How to find the prefix length if an address is given.

- Since the prefix length is not inherent in the address, we need to separately give the length of the prefix.
- In this case, 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 or CIDR (pronounced cider) strategy.

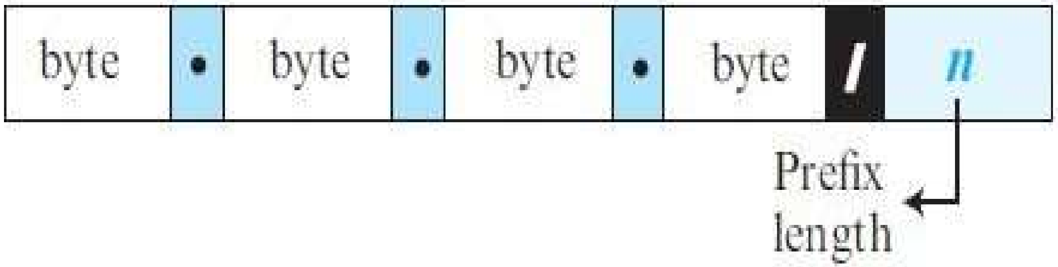
Extracting Information from an Address

- Given any address in the block, we normally like to know three pieces of information about the block to which the address belongs:

- The number of addresses
- The first address in the block
- The last address

- Since the value of prefix length, n, is given, we can easily find these three pieces of information,

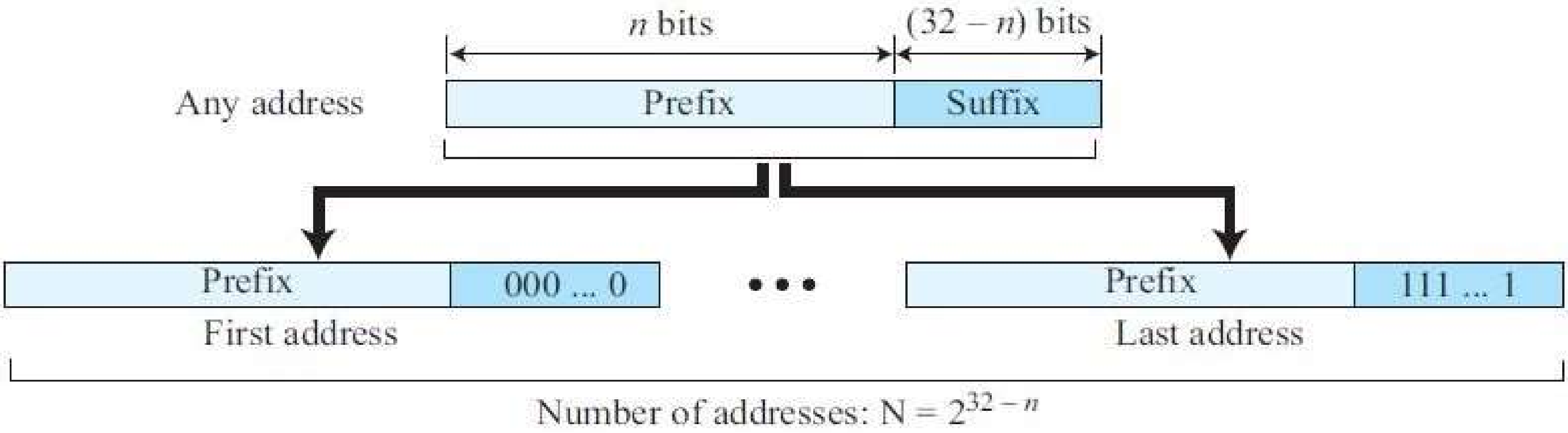
Figure 4.33 *Slash notation (CIDR)*



Examples:
12.24.76.8/8
23.14.67.92/12
220.8.24.255/25

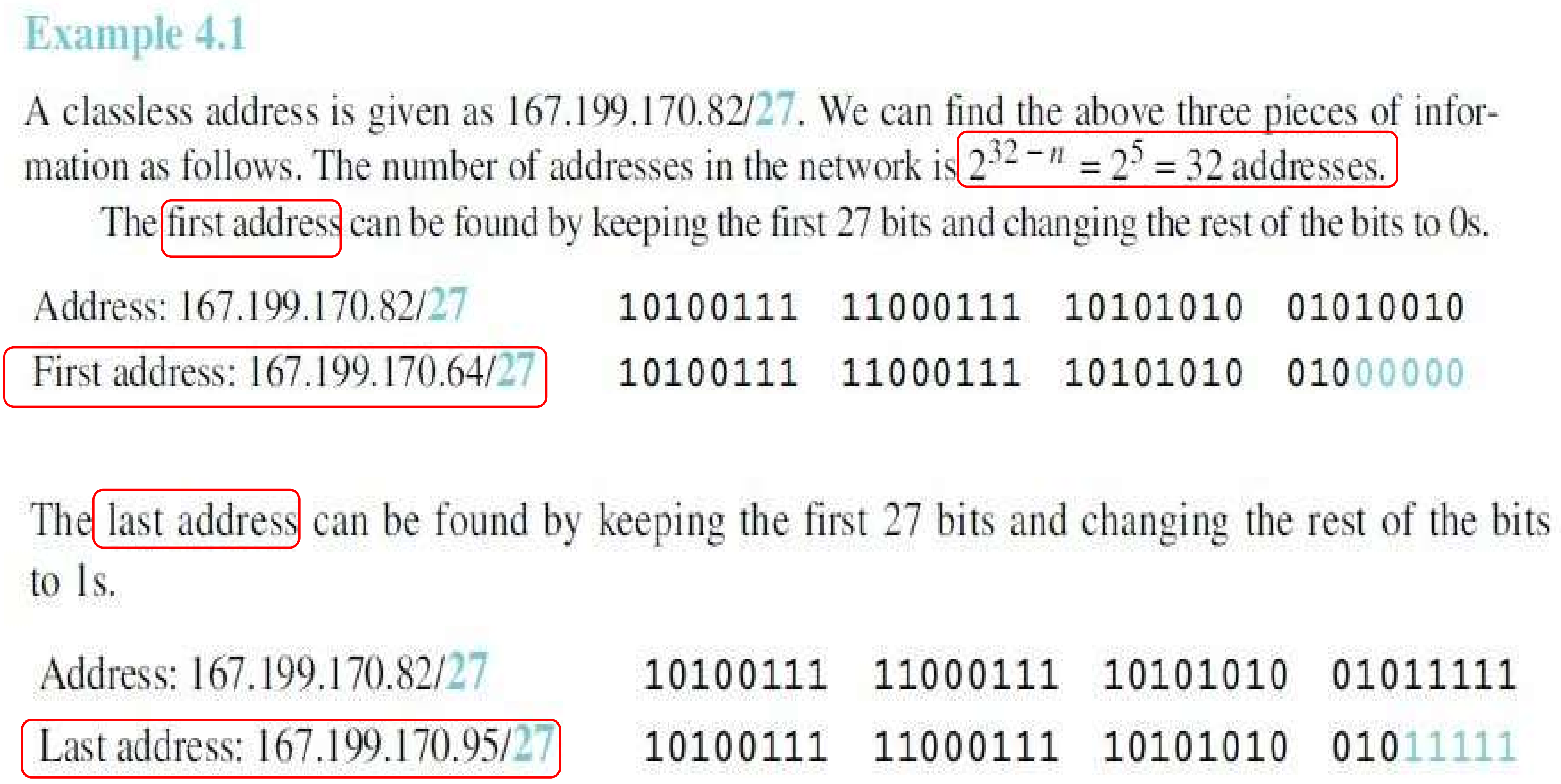
[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Figure 4.34 *Information extraction in classless addressing*



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

[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]



Example 4.1

A classless address is given as 167.199.170.82/27. We can find the above three pieces of information as follows. The number of addresses in the network is $2^{32-n} = 2^5 = 32$ addresses.

The first address can be found by keeping the first 27 bits and changing the rest of the bits to 0s.

Address: 167.199.170.82/27	10100111 11000111 10101010 01010010
First address: 167.199.170.64/27	10100111 11000111 10101010 01000000

The last address can be found by keeping the first 27 bits and changing the rest of the bits to 1s.

Address: 167.199.170.82/27	10100111 11000111 10101010 01011111
Last address: 167.199.170.95/27	10100111 11000111 10101010 01011111

[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Address Mask

The address mask is a 32-bit number in which the n leftmost bits are set to 1s and the rest of the bits (32 – n) are set to 0s.

Block Allocation

The next issue in classless addressing is block allocation. How are the blocks allocated?

- The ultimate responsibility of block allocation is given to a global authority called the Internet Corporation for Assigned Names and Numbers (ICANN).

- However, ICANN does not normally allocate addresses to individual Internet users.

- It assigns a large block of addresses to an ISP (or a larger organization that is considered an ISP in this case).

Block Allocation

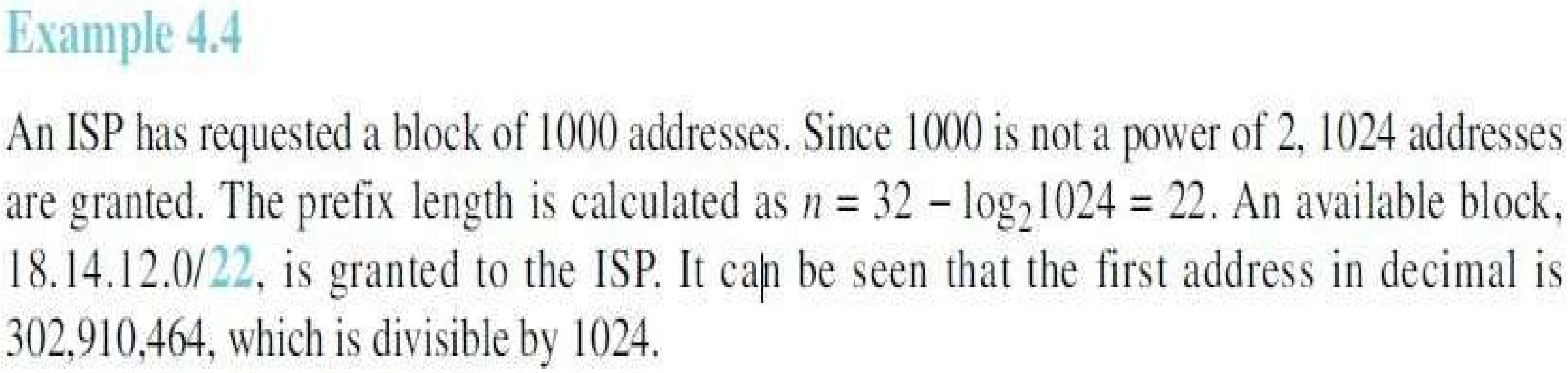
For the proper operation of the CIDR, two restrictions need to be applied to the allocated block.

1. The number of requested addresses, N, needs to be a power of 2. The reason is that if N is not a power of 2, we cannot have an integer value for n.

$$N = 2^{32-n} \text{ or } n = 32 - \log_2 N.$$

2. The requested block needs to be allocated where there are a contiguous number of available addresses in the address space. However, there is a restriction on choosing the first address in the block. The first address needs to be divisible by the number of addresses in the block.

Block Allocation



Example 4.4

An ISP has requested a block of 1000 addresses. Since 1000 is not a power of 2, 1024 addresses are granted. The prefix length is calculated as $n = 32 - \log_2 1024 = 22$. An available block, 18.14.12.0/22, is granted to the ISP. It can be seen that the first address in decimal is 302,910,464, which is divisible by 1024.

[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

Dynamic Host Configuration Protocol (DHCP)

- A large organization or an ISP can receive a block of addresses directly from ICANN(Internet Corporation for Assigned Names and Numbers) and a small organization can receive a block of addresses from an ISP.
- After a block of addresses are assigned to an organization, the network administration can manually assign addresses to the individual hosts or routers.
- Address assignment in an organization can be done automatically using the Dynamic Host Configuration Protocol (DHCP).
- DHCP is an application-layer program, using the client-server paradigm, that actually helps TCP/IP at the network layer.

Dynamic Host Configuration Protocol (DHCP)

- Given host receives the same IP address each time it connects to the network, or a host may be assigned a temporary IP address that will be different each time the host connects to the network.
- In addition to host IP address assignment, DHCP also allows a host to learn additional information, such as its subnet mask, the address of its first-hop router (often called the default gateway), and the address of its local DNS server.

- Because of DHCP's ability to automate the network-related aspects of connecting a host into a network, it is often referred to as a plug-and- play protocol.

Dynamic Host Configuration Protocol (DHCP)

- DHCP is also enjoying widespread use in residential Internet access networks and in wireless LANs, where hosts join and leave the network frequently.
- Consider, for example, the student who carries a laptop from a dormitory room to a library to a classroom. It is likely that in each location, the student will be connecting into a new subnet and hence will need a new IP address at each location.
- DHCP is ideally suited to this situation, as there are many users coming and going, and addresses are needed for only a limited amount of time.

.

Dynamic Host Configuration Protocol (DHCP)

- DHCP is similarly useful in residential ISP access networks.
- Consider, for example, a residential ISP that has 2,000 customers, but no more than 400 customers are ever online at the same time. In this case, rather than needing a block of 2,048 addresses, a DHCP server that assigns addresses dynamically needs only a block of 512 addresses
- As the hosts join and leave, the DHCP server needs to update its list of available IP addresses.
- Each time a host joins, the DHCP server allocates an arbitrary address from its current pool of available addresses; each time a host leaves, its address is returned to the pool.

Dynamic Host Configuration Protocol (DHCP)

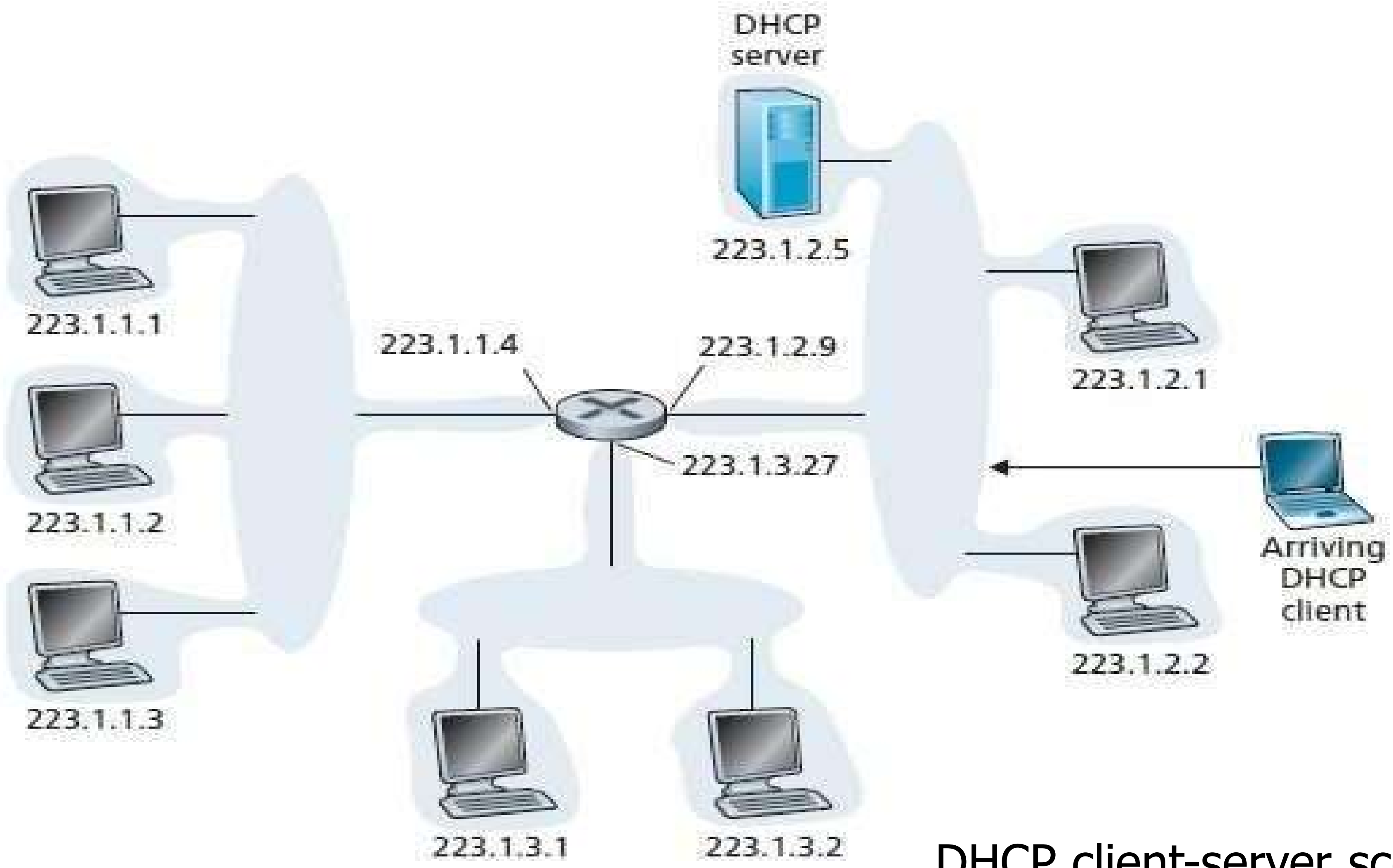
- DHCP is a client-server protocol. A client is typically a newly arriving host wanting to obtain network configuration information, including an IP address for itself.

- In the simplest case, each subnet will have a DHCP server.

- If no server is present on the subnet, a DHCP relay agent (typically a router) that knows the address of a DHCP server for that network is needed.

- Figure shows a DHCP server attached to subnet 223.1.2/24, with the router serving as the relay agent for arriving clients attached to subnets 223.1.1/24 and 223.1.3/24.

Dynamic Host Configuration Protocol (DHCP)



DHCP client-server scenario

[James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)]

Dynamic Host Configuration Protocol (DHCP)

For a newly arriving host, the DHCP protocol is a four-step process:

1. DHCP server discovery

-The first task is to find a DHCP server with which to interact. This is done using a DHCP discover message, which a client sends within a UDP packet to port 67.

-The UDP packet is encapsulated in an IP datagram.

-The DHCP client creates an IP datagram containing its DHCP discover message along with the broadcast destination IP address of 255.255.255.255 and a “this host” source IP address of 0.0.0.0.

-The DHCP client passes the IP datagram to the link layer, which then broadcasts this frame to all nodes attached to the subnet.

Dynamic Host Configuration Protocol (DHCP)

2. DHCP server offer(s)

-A DHCP server receiving a DHCP discover message responds to the client with a DHCP offer message that is broadcast to all nodes on the subnet, again using the IP broadcast address of 255.255.255.255.

-Each server offer message contains the transaction ID of the received discover message, the proposed IP address for the client, the network mask, and an IP address lease time—the amount of time for which the IP address will be valid.

Dynamic Host Configuration Protocol (DHCP)

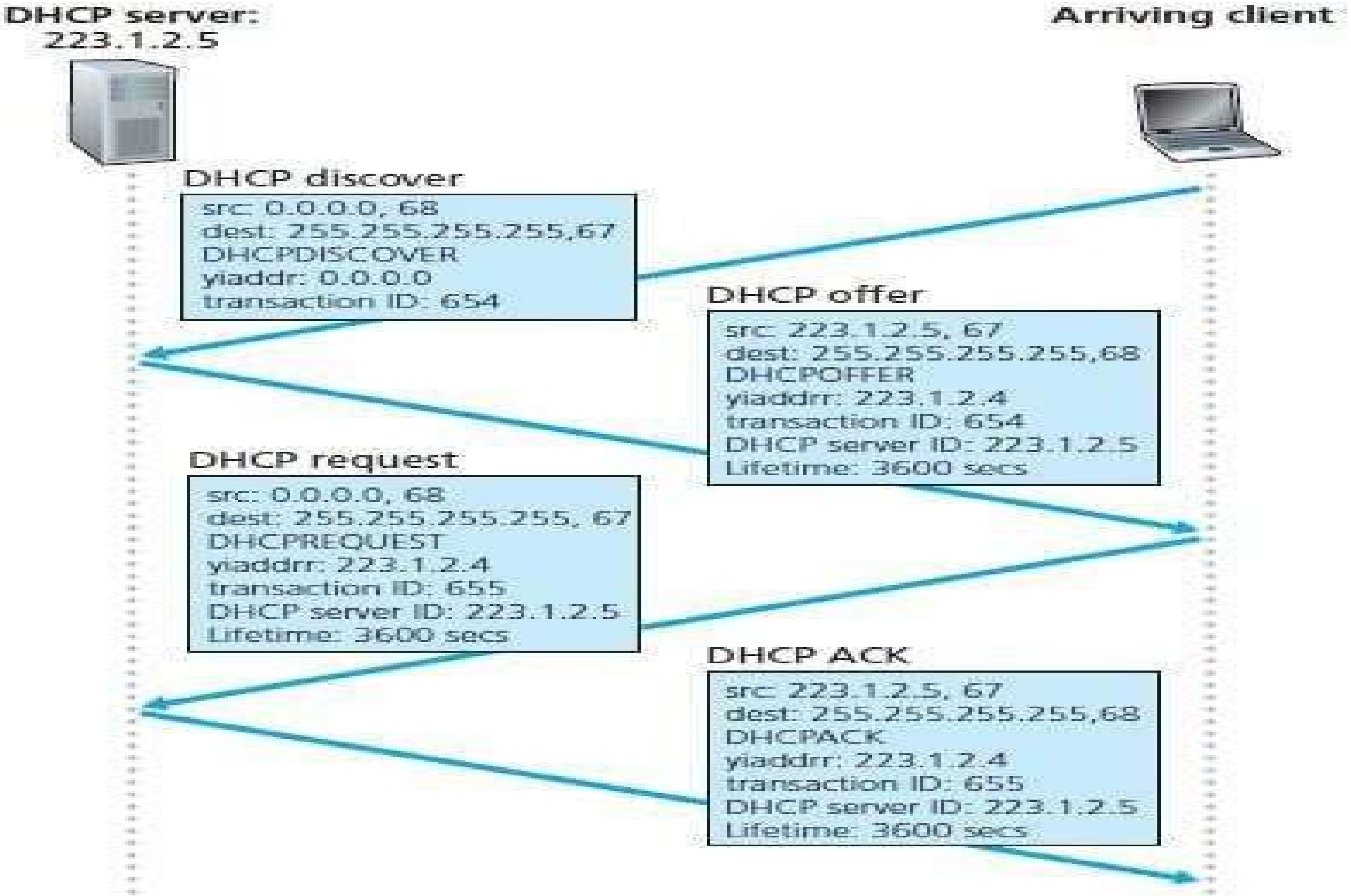
3.DHCP request

- The newly arriving client will choose from among one or more server offers and respond to its selected offer with a DHCP request message, echoing back the configuration parameters.

4.DHCP ACK

- The server responds to the DHCP request message with a DHCP ACK message, confirming the requested parameters. Once the client receives the DHCP ACK, the interaction is complete and the client can use the DHCP-allocated IP address for the lease duration.

Dynamic Host Configuration Protocol (DHCP)



DHCP discover

src: 0.0.0.0, 68
dest: 255.255.255.255,67
DHCPDISCOVER
yiaddr: 0.0.0.0
transaction ID: 654

DHCP offer

src: 223.1.2.5, 67
dest: 255.255.255.255,68
DHCPOFFER
yiaddrr: 223.1.2.4
transaction ID: 654
DHCP server ID: 223.1.2.5
Lifetime: 3600 secs

DHCP request

src: 0.0.0.0, 68
dest: 255.255.255.255, 67
DHCPREQUEST
yiaddrr: 223.1.2.4
transaction ID: 655
DHCP server ID: 223.1.2.5
Lifetime: 3600 secs

DHCP ACK

src: 223.1.2.5, 67
dest: 255.255.255.255,68
DHCPACK
yiaddrr: 223.1.2.4
transaction ID: 655
DHCP server ID: 223.1.2.5
Lifetime: 3600 secs

DHCP client-server interaction

[James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)]

Network Address Translation (NAT)

- What if the ISP had already allocated the contiguous portions of the SOHO (small office, home office) network's current address range?
- And what typical homeowner wants (or should need) to know how to manage IP addresses in the first place?
- There is a simpler approach to address allocation that has found increasingly widespread use in such scenarios: network address translation (NAT) [RFC 2663; RFC 3022; Zhang 2007].

Network Address Translation (NAT)

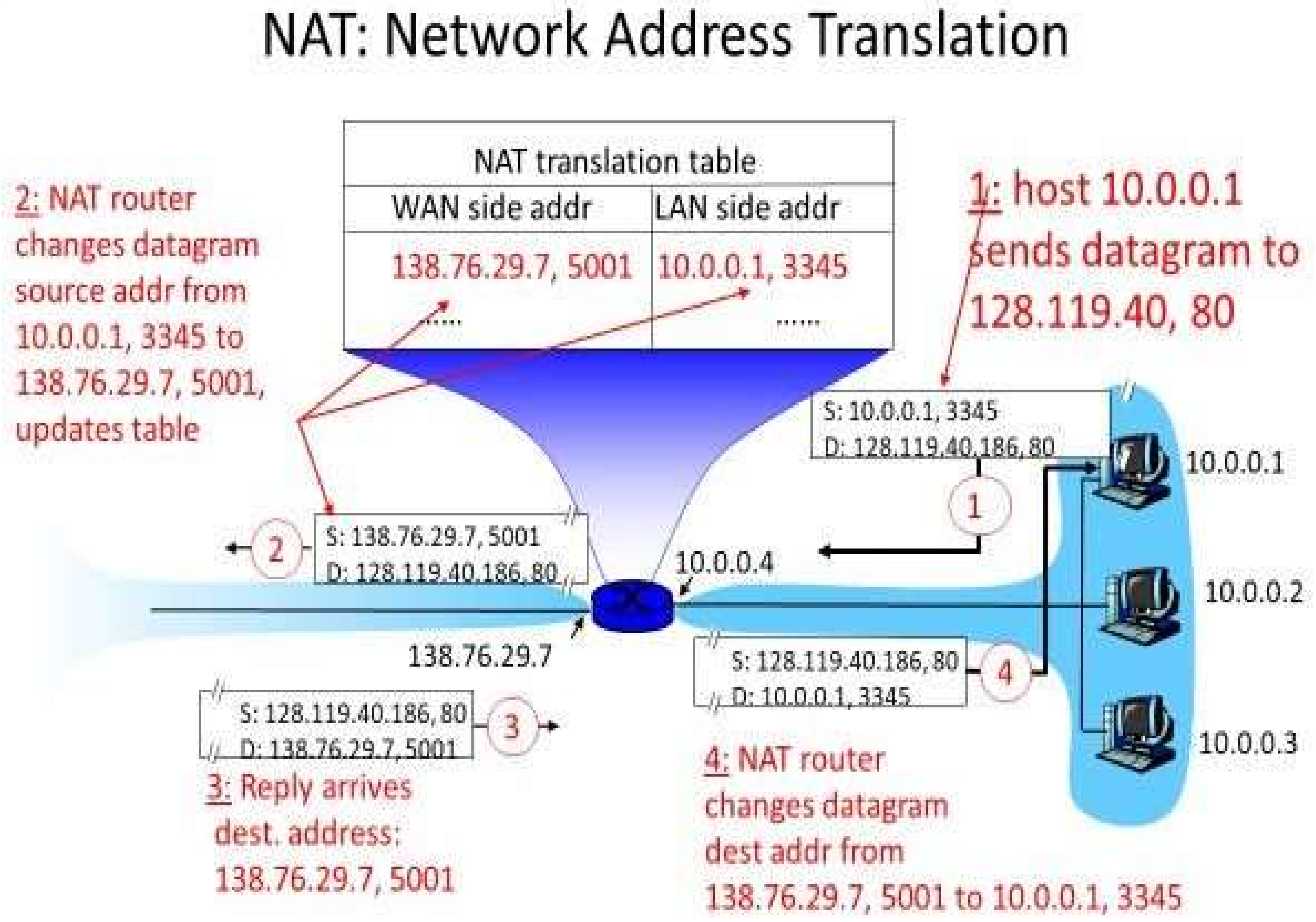
- Use a **NAT translation table** at the NAT router, and to include port numbers as well as IP addresses in the table entries.

- Suppose a user sitting in a home network behind host 10.0.0.1 requests a Web page on some Web server (port 80) with IP address 128.119.40.186.

- The host 10.0.0.1 assigns the (arbitrary) source port number 3345 and sends the datagram into the LAN.

- The NAT router receives the datagram, generates a new source port number 5001 for the datagram, replaces the source IP address with its WAN-side IP address 138.76.29.7, and replaces the original source port number 3345 with the new source port number 5001.

Network Address Translation (NAT)



NAT: Network Address Translation

NAT translation table	
WAN side addr	LAN side addr
138.76.29.7, 5001	10.0.0.1, 3345
……	……

1: host 10.0.0.1 sends datagram to 128.119.40, 80

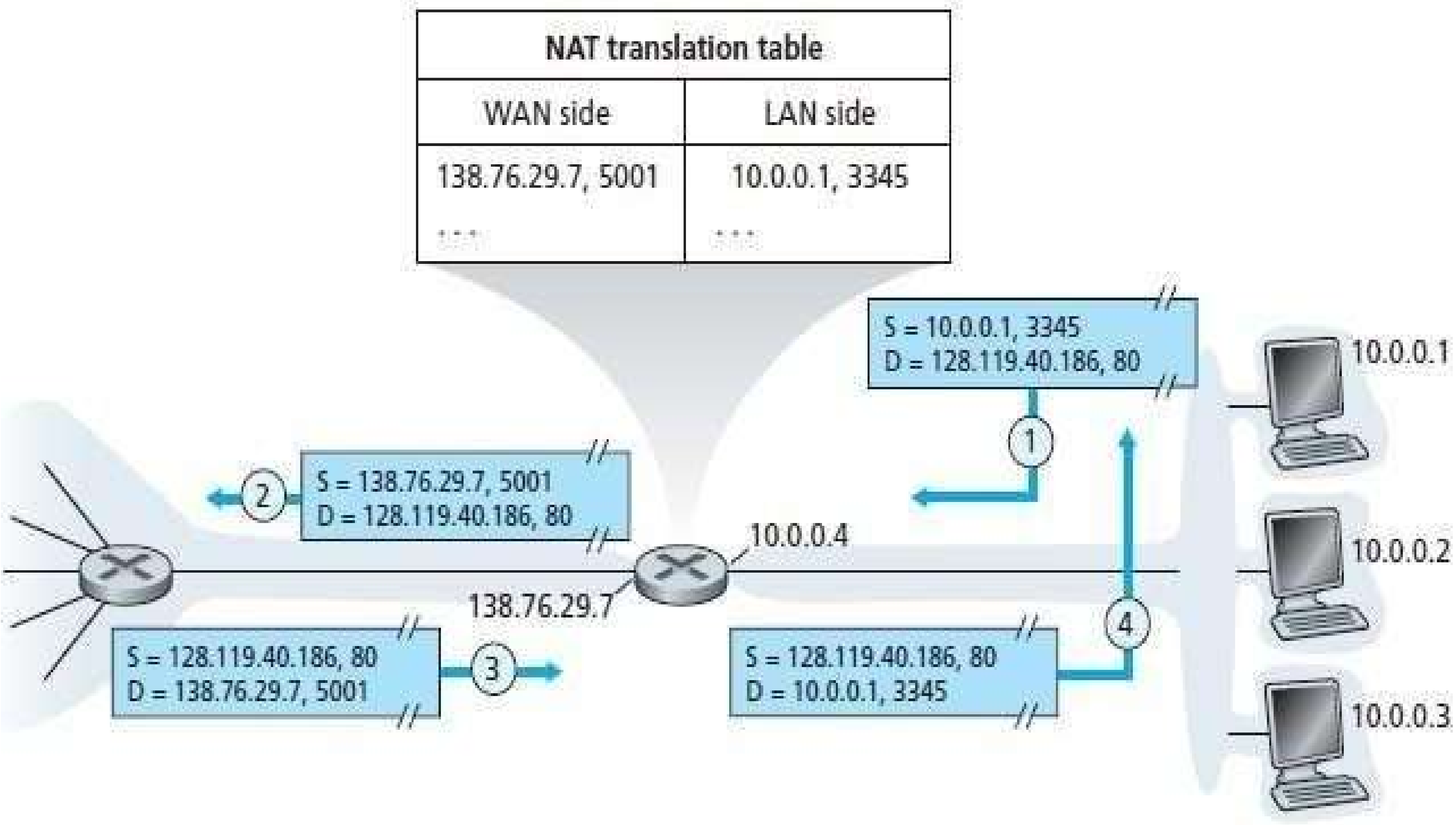
2: NAT router changes datagram source addr from 10.0.0.1, 3345 to 138.76.29.7, 5001, updates table

3: Reply arrives dest. address: 138.76.29.7, 5001

4: NAT router changes datagram dest addr from 138.76.29.7, 5001 to 10.0.0.1, 3345

[James F Kurose and Keith W Ross, "Computer Networking: A Top - Down Approach", Pearson Education; 6 th Edition (2017)]

Network Address Translation (NAT)



NAT translation table

WAN side	LAN side
138.76.29.7, 5001	10.0.0.1, 3345
. . .	. . .

[James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)]

Network Address Translation (NAT)

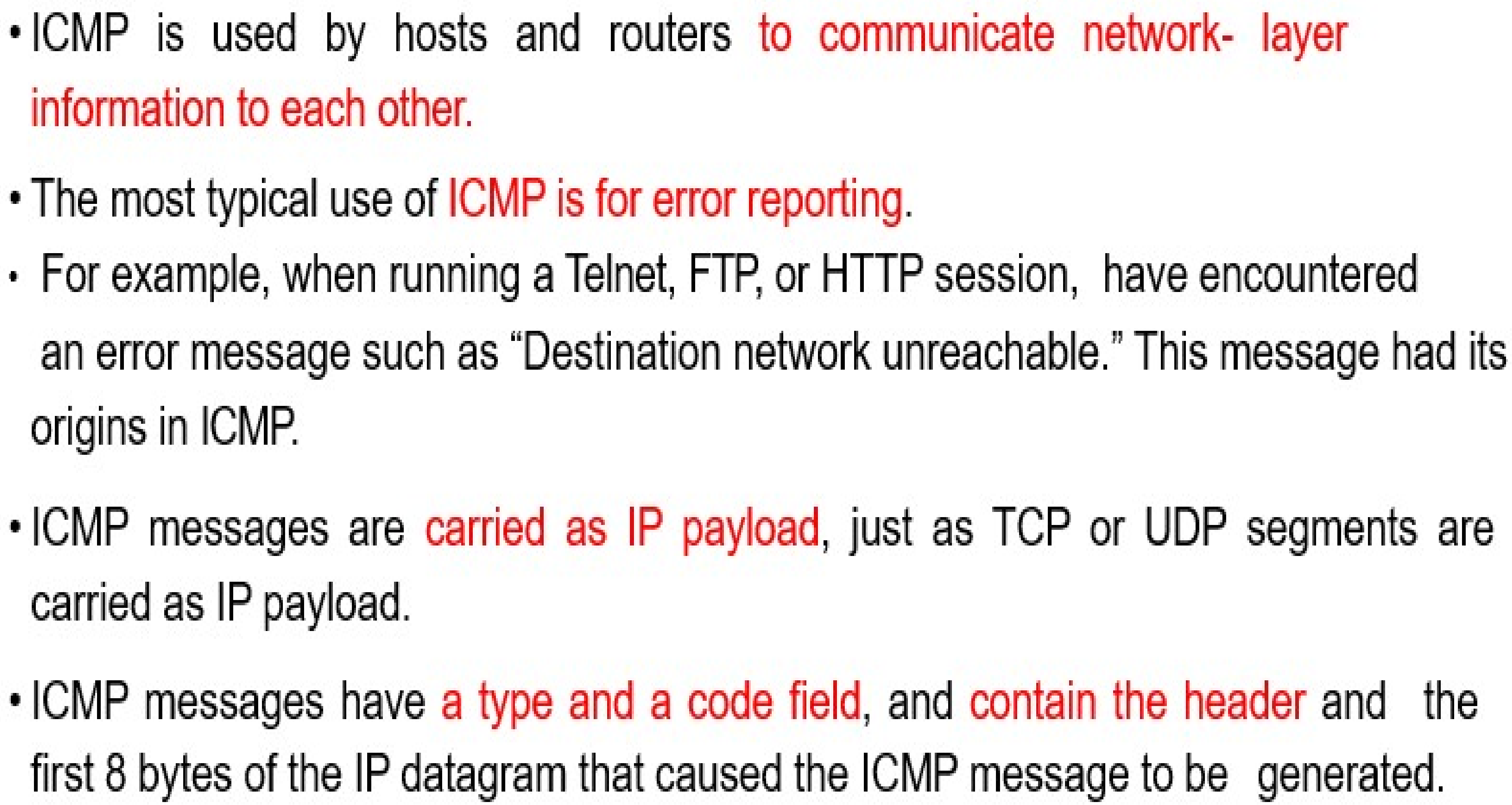
Private Address Ranges

- The organizations that distribute IP addresses to the world reserves a range of IP addresses for private networks. 256x256
  - 192.168.0.0 – 192.168.255.255 (65,536 IP addresses) 256x256 x 16
  - 172.16.0.0 – 172.31.255.255 (1,048,576 IP addresses)
  - 10.0.0.0 – 10.255.255.255 (16,777,216 IP addresses) 256x256 x 256
- An IP address within these ranges is therefore considered non-routable, as it is not unique.
- Any private network that needs to use IP addresses internally can use any address within these ranges without any coordination with IANA or an Internet registry.
- Addresses within this private address space are only unique within a given private network.
- All addresses outside these ranges are considered public.

Network Address Translation (NAT)

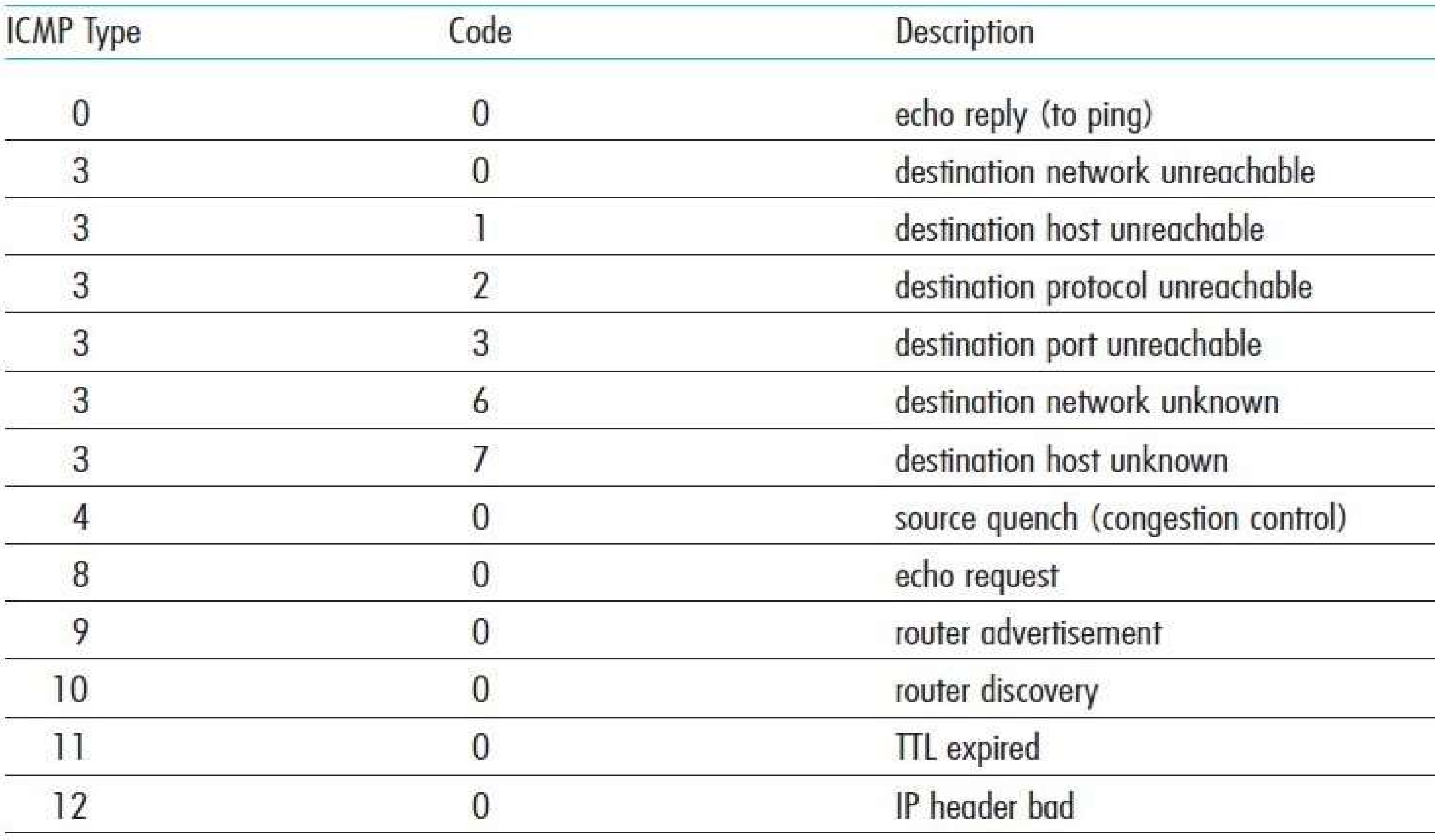
- Devices within a given home network can send packets to each other using 10.0.0.0/24 addressing.
- However, packets forwarded beyond the home network into the larger global Internet clearly cannot use these addresses.
- The NAT-enabled router does not look like a router to the outside world.
- Instead the NAT router behaves to the outside world as a single device with a single IP address.
- All traffic leaving the home router for the larger Internet has a source IP address of 138.76.29.7, and all traffic entering the home router must have a destination address of 138.76.29.7.
- The NAT-enabled router is hiding the details of the home network from the outside world.

Internet Control Message Protocol (ICMP)



- ICMP is used by hosts and routers to communicate network- layer information to each other.
- The most typical use of ICMP is for error reporting.
- For example, when running a Telnet, FTP, or HTTP session, have encountered an error message such as "Destination network unreachable." This message had its origins in ICMP.
- ICMP messages are carried as IP payload, just as TCP or UDP segments are carried as IP payload.
- ICMP messages have a type and a code field, and contain the header and the first 8 bytes of the IP datagram that caused the ICMP message to be generated.

Internet Control Message Protocol (ICMP)



ICMP Type	Code	Description
0	0	echo reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	3	destination port unreachable
3	6	destination network unknown
3	7	destination host unknown
4	0	source quench (congestion control)
8	0	echo request
9	0	router advertisement
10	0	router discovery
11	0	TTL expired
12	0	IP header bad

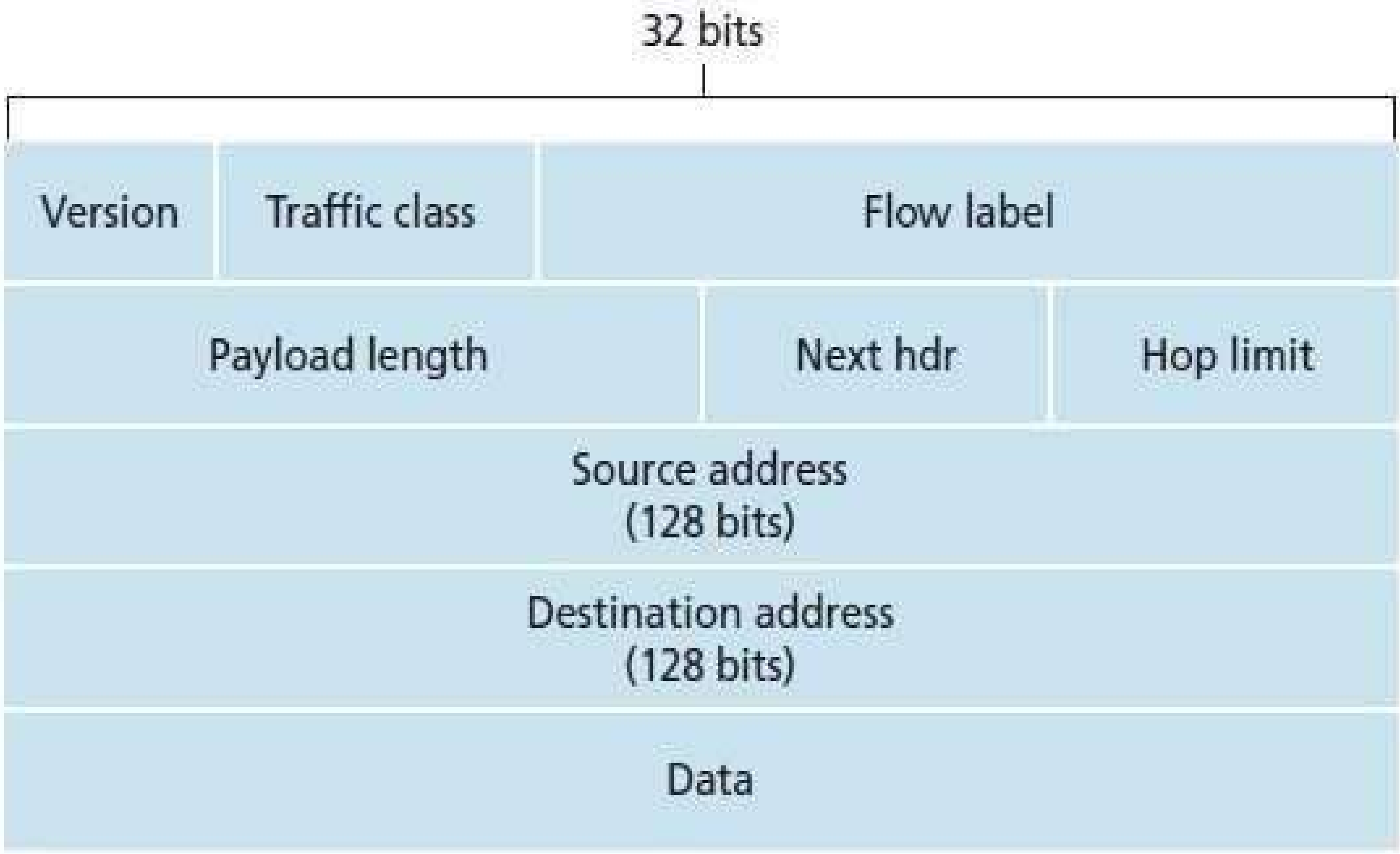
Figure 4.23 ◆ ICMP message types

[James F Kurose and Keith W Ross, "Computer Networking: A Top - Down Approach", Pearson Education; 6 th Edition (2017)]

IPv6

- The 32-bit IP address space was beginning to be used up, with new subnets and IP nodes being attached to the Internet (and being allocated unique IP addresses) at a breathtaking rate.
- Need for a large IP address space, a new IP protocol, IPv6, was developed.

IPv6 Datagram Format



IPv6 datagram format

[James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)]

IPv6 Datagram Format

- Version. 4-bit field identifies the IP version number.
- Traffic class. 8-bit field is similar to the ToS(Type of Service) field in IPv4.
- Flow label. 20-bit field is used to identify a flow of datagrams.
- Payload length. 16-bit value is treated as an unsigned integer giving the number of bytes in the IPv6 datagram following the fixed- length, 40-byte datagram header(32+32+128x2 bits).
- Next header. This field identifies the protocol to which the contents (data field) of this datagram will be delivered (for example, to TCP or UDP). The field uses the same values as the protocol field in the IPv4 header.

IPv6 Datagram Format

- Hop limit. The contents of this field are decremented by one by each router that forwards the datagram. If the hop limit count reaches zero, the datagram is discarded.
- Source and destination addresses. The various formats of the IPv6 128-bit address are described in RFC 4291.
- Data. This is the payload portion of the IPv6 datagram. When the datagram reaches its destination, the payload will be removed from the IP datagram and passed on to the protocol specified in the next header field.

IPv6 Datagram Format

The most important changes introduced in IPv6 are

- Expanded addressing capabilities. IPv6 increases the size of the IP address from 32 to 128 bits. This ensures that the world won’t run out of IP addresses.
- In addition to unicast and multicast addresses, IPv6 has introduced a new type of address, called an anycast address, which allows a datagram to be delivered to any one of a group of hosts.
- A streamlined 40-byte header. A number of IPv4 fields have been dropped or made optional. The resulting 40-byte fixed-length header allows for faster processing of the IP datagram.

IPv6 Datagram Format

The most important changes introduced in IPv6 are

Flow labeling and priority. IPv6 has an elusive definition of a flow.

- Labeling of packets belonging to particular flows for which the sender requests special handling, such as a nondefault quality of service or real-time service.
- For example, audio and video transmission might likely be treated as a flow. On the other hand, the more traditional applications, such as file transfer and e-mail, might not be treated as flows.
- It is possible that the traffic carried by a high-priority user (for example, someone paying for better service for their traffic) might also be treated as a flow.
- The designers of IPv6 foresee the eventual need to be able to differentiate among the flows, even if the exact meaning of a flow has not yet been determined.

IPv6 Datagram Format

The most important changes introduced in IPv6 are

- The IPv6 header also has an 8-bit traffic class field.
- This field, like the TOS field in IPv4, can be used to give priority to certain datagrams within a flow, or it can be used to give priority to datagrams from certain applications (for example, ICMP) over datagrams from other applications (for example, network news).

IPv6 Datagram Format

The most important changes introduced in IPv6 are

- IPv6 does not allow for fragmentation and reassembly at intermediate routers; these operations can be performed only by the source and destination.
- If an IPv6 datagram received by a router is too large to be forwarded over the outgoing link, the router simply drops the datagram and sends a "Packet Too Big" ICMP error message back to the sender.
- The sender can then resend the data, using a smaller IP datagram size.
- Fragmentation and reassembly is a time-consuming operation; removing this functionality from the routers and placing it squarely in the end systems considerably speeds up IP forwarding within the network.

IPv6 Datagram Format

The most important changes introduced in IPv6 are

- Because the transport-layer (for example, TCP and UDP) and link-layer (for example, Ethernet) protocols in the Internet layers perform checksumming, this functionality was sufficiently redundant in the network layer and is removed.
- Fast processing of IP packets was a central concern.
- The removal of the options field results in a fixed-length, 40-byte IP header.

IPv6 Datagram Format

The most important changes introduced in IPv6 are

- Options. An options field is no longer a part of the standard IP header.
- It has not gone away. Instead, the options field is one of the possible next headers pointed to from within the IPv6 header.
- That is, just as TCP or UDP protocol headers can be the next header within an IP packet, so too can an options field.
- The removal of the options field results in a fixed-length, 40-byte IP header.

How will the public Internet, which is based on IPv4, be transitioned to IPv6?

- One option would be to declare a flag day—a given time and date when all Internet machines would be turned off and upgraded from IPv4 to IPv6.
- Dual-stack approach, where IPv6 nodes also have a complete IPv4 implementation. Such a node, referred to as an IPv6/IPv4 node.
- Tunneling: Suppose two IPv6 nodes want to interoperate using IPv6 datagrams but are connected to each other by intervening IPv4 routers. We refer to the intervening set of IPv4 routers between two IPv6 routers as a tunnel. With tunneling, the IPv6 node on the sending side of the tunnel takes the entire IPv6 datagram and puts it in the data (payload) field of an IPv4 datagram.

Dual-stack approach

- Dual-stack approach, where IPv6 nodes also have a complete IPv4 implementation.
- Such a node, referred to as an IPv6/IPv4 node has the ability to send and receive both IPv4 and IPv6 datagrams.
- When interoperating with an IPv4 node, an IPv6/IPv4 node can use IPv4 datagrams; when interoperating with an IPv6 node, it can speak IPv6.
- IPv6/IPv4 nodes must have both IPv6 and IPv4 addresses.

Dual-stack approach

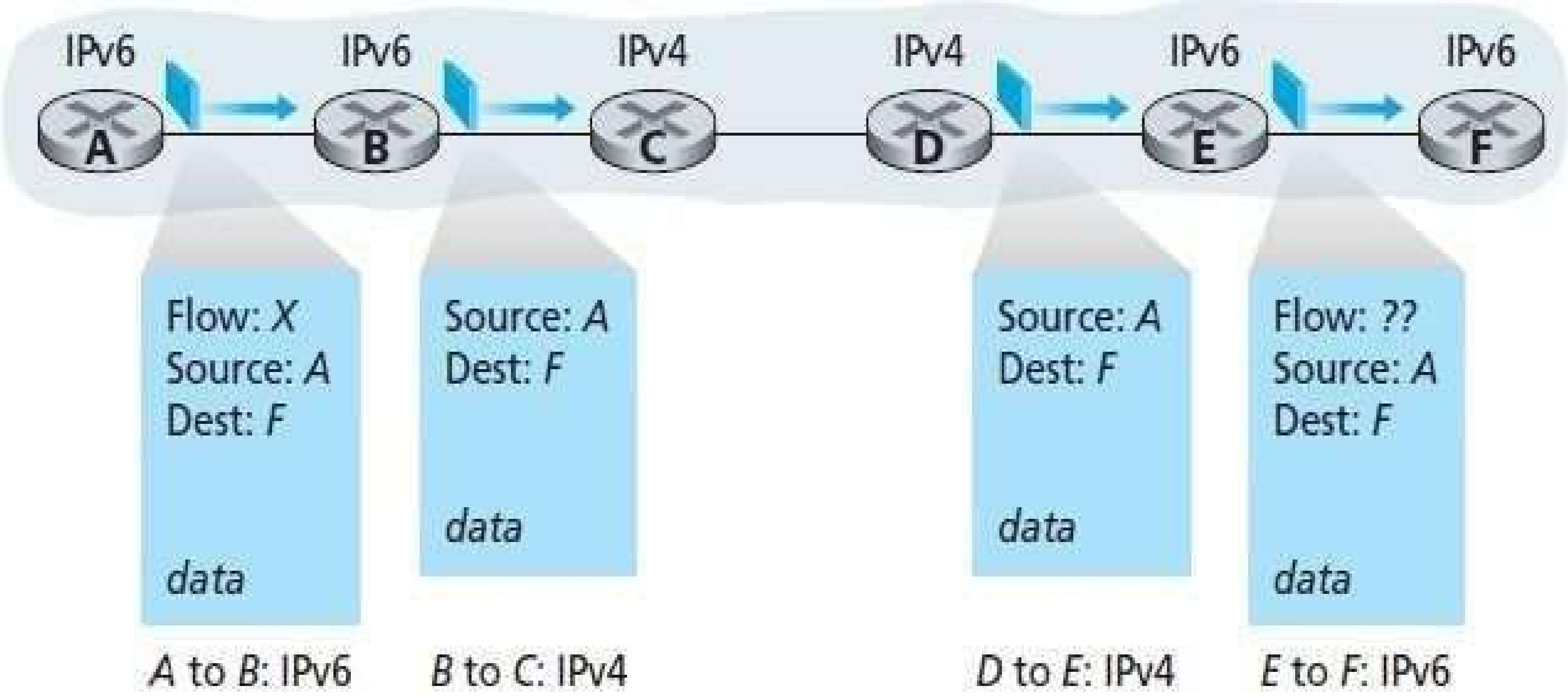


Figure 4.25 ♦ A dual-stack approach

[James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)]

Dual-stack approach

- In the dual-stack approach, if either the sender or the receiver is only IPv4- capable, an IPv4 datagram must be used.

- As a result, it is possible that two IPv6- capable nodes can end up, sending IPv4 datagrams to each other.

- This is illustrated in the above Figure 4.25.

Dual-stack approach

- Suppose Node A is IPv6-capable and wants to send an IP datagram to Node F, which is also IPv6-capable.
- Nodes A and B can exchange an IPv6 datagram.
- However, Node B must create an IPv4 datagram to send to C.
- The data field of the IPv6 datagram can be copied into the data field of the IPv4 datagram and appropriate address mapping can be done.
- However, in performing the conversion from IPv6 to IPv4, there will be IPv6-specific fields in the IPv6 datagram (for example, the flow identifier field) that have no counterpart in IPv4.
- The information in these fields will be lost. Thus, even though E and F can exchange IPv6 datagrams, the arriving IPv4 datagrams at E from D do not contain all of the fields that were in the original IPv6 datagram sent from A.

Tunneling

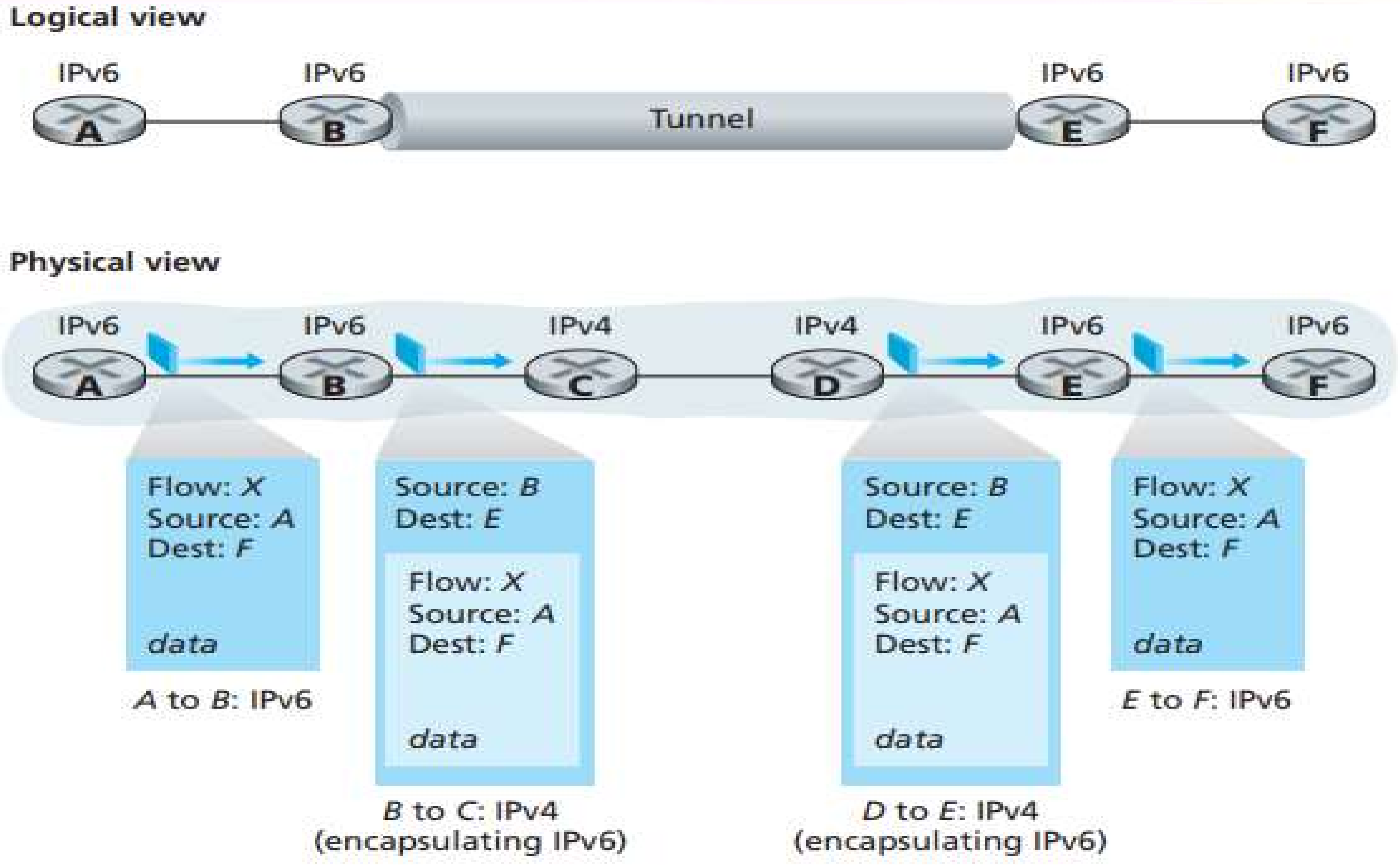


Figure 4.26 ♦ Tunneling

[James F Kurose and Keith W Ross, “Computer Networking: A Top - Down Approach”, Pearson Education; 6 th Edition (2017)]

Tunneling

- Tunneling : Suppose two IPv6 nodes want to interoperate using IPv6 datagrams but are connected to each other by intervening IPv4 routers.
- Intervening set of IPv4 routers between two IPv6 routers as a tunnel.
- With tunneling, the IPv6 node on the sending side of the tunnel takes the *entire* IPv6 datagram and puts it in the data (payload) field of an IPv4 datagram.

IP Security

- IP Security (IPSec) is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level.

- IPSec helps create authenticated and confidential packets for the IP layer.

- IPsec protocol has been designed to be backward compatible with IPv4 and IPv6.

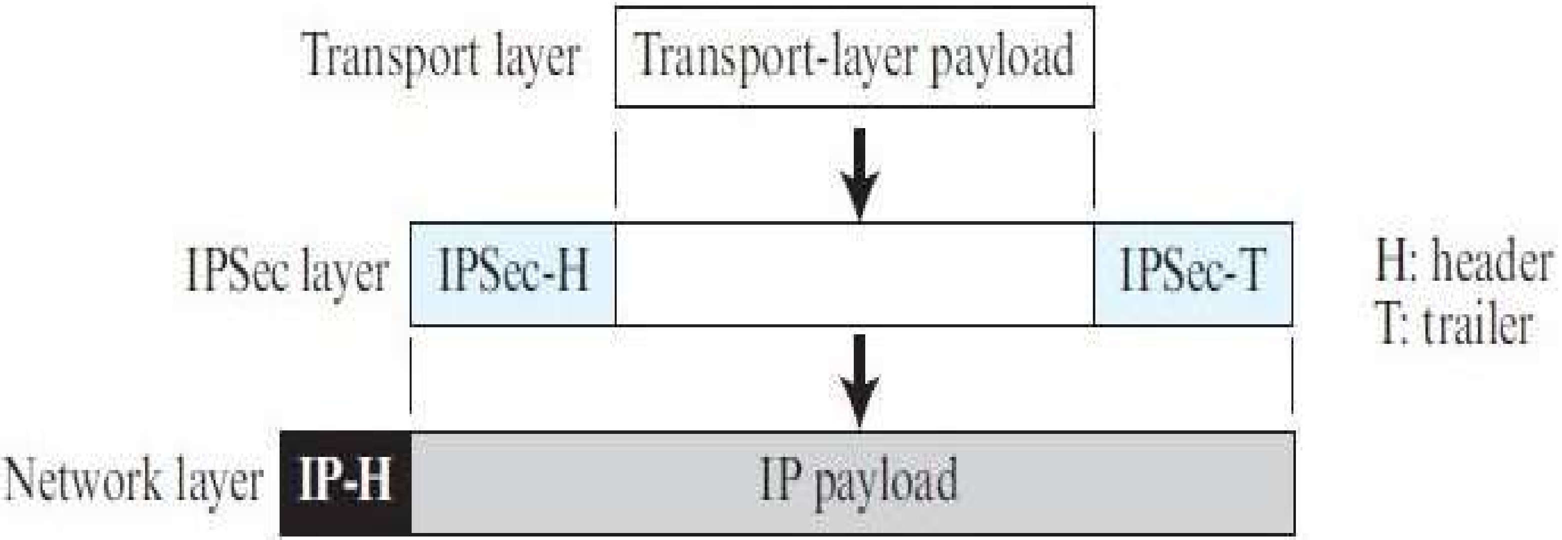
IP Security

IPSec operates in one of two different modes: transport mode or tunnel mode.

- Transport Mode - In transport mode, IPSec protects what is delivered from the transport layer to the network layer.
- Transport mode protects the payload to be encapsulated in the network layer
- Transport mode does not protect the IP header.
- In other words, transport mode does not protect the whole IP packet; it protects only the packet from the transport layer (the IP-layer payload).
- In this mode, the IPSec header (and trailer) are added to the information coming from the transport layer.
- The IP header is added later

IP Security

Figure 10.46 *IPSec in transport mode*



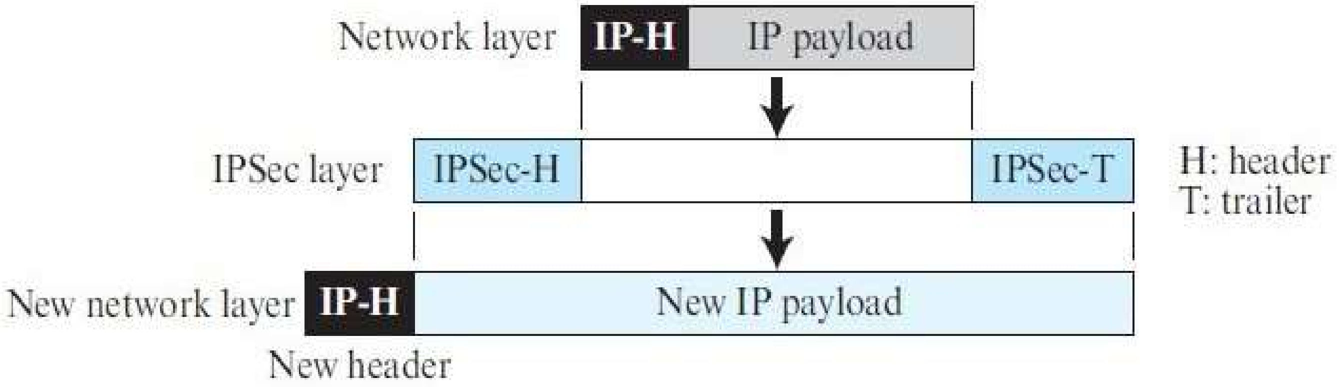
[Behrouz A Forouzan, Firouz Mosharraf, “Computer Networks: A top down Approach”, McGraw Hill Education]

IP Security

Tunnel Mode

- In tunnel mode, IPSec protects the entire IP packet.
- It takes an IP packet, including the header, applies IPSec security methods to the entire packet, and then adds a new IP header

Figure 10.48 *IPSec in tunnel mode*



[Behrouz A Forouzan, Firouz Mosharraf, "Computer Networks: A top down Approach", McGraw Hill Education]

The services provided by an IPsec session

- Cryptographic agreement. Mechanisms that allow the two communicating hosts to agree on cryptographic algorithms and keys.
- Encryption of IP datagram payloads. When the sending host receives a segment from the transport layer, IPsec encrypts the payload. The payload can only be decrypted by IPsec in the receiving host.
- Data integrity. IPsec allows the receiving host to verify that the datagram's header fields and encrypted payload were not modified
- Origin authentication. When a host receives an IPsec datagram from a trusted source the host is assured that the source IP address in the datagram is the actual source of the datagram.