Introduction to Network Layer

Dr Mohit Kumar

Dept. of Information Technology

National Institute of Technology

Jalandhar, Punjab, India

kumarmohit@nitj.ac.in

Outline

1 NETWORK-LAYER SERVICES

2 PACKET SWITCHING

3 NETWORK-LAYER PERFORMANCE

4 IPv4 ADDRESSES

5 FORWARDING OF IP PACKETS

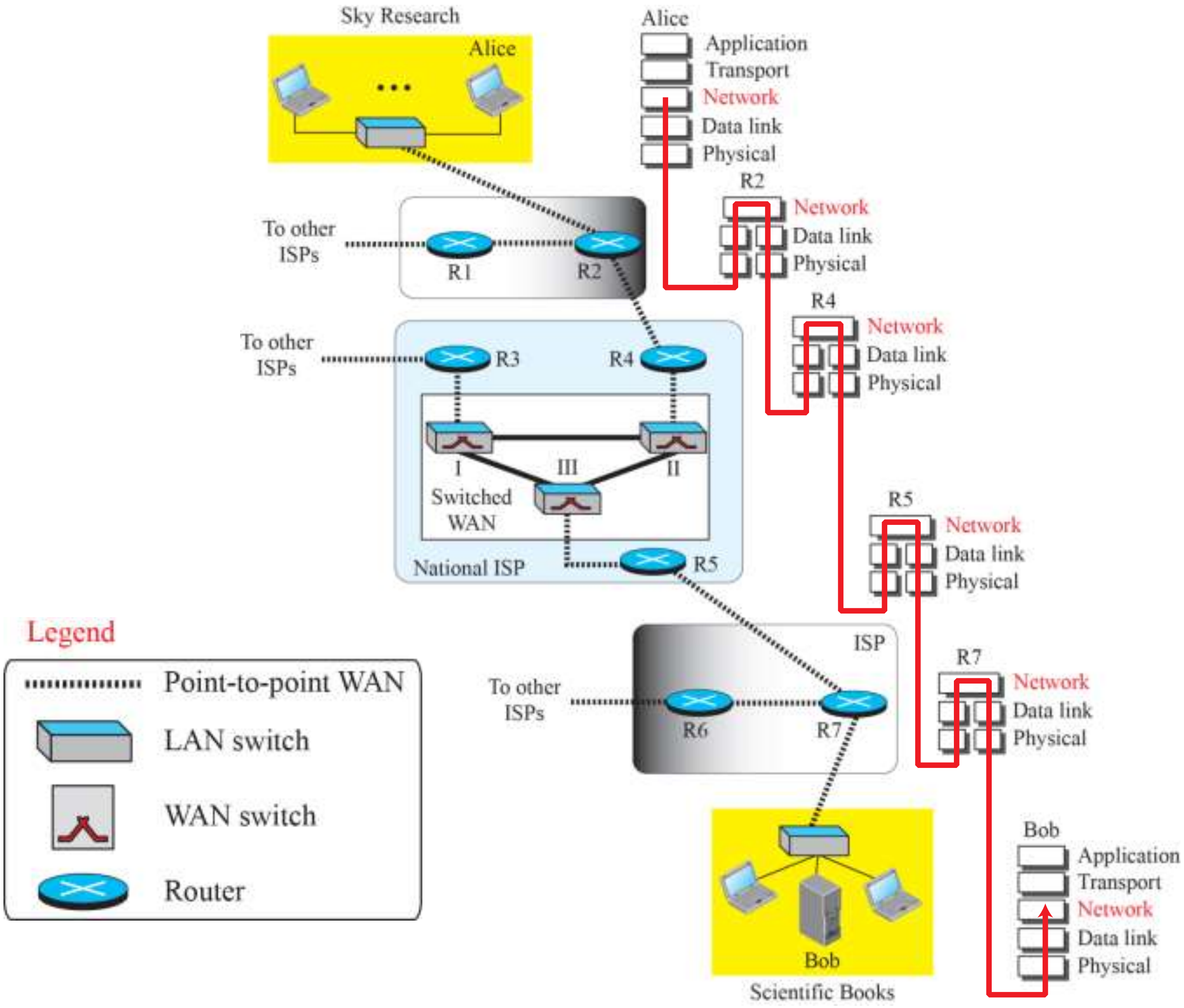
1 NETWORK-LAYER SERVICES

Before discussing the network layer in the Internet today, let’s briefly discuss the network-layer services that, in general, are expected from a network-layer protocol.

Figure 1 shows the communication between Alice and Bob at the network layer.

This is the same scenario which is use to show the communication at the physical and the data-link layers, respectively.

Figure 1: Communication at the network layer



1 Packetizing

The first duty of the network layer is definitely packetizing: encapsulating the payload in a network-layer packet at the source and decapsulating the payload from the network-layer packet at the destination.

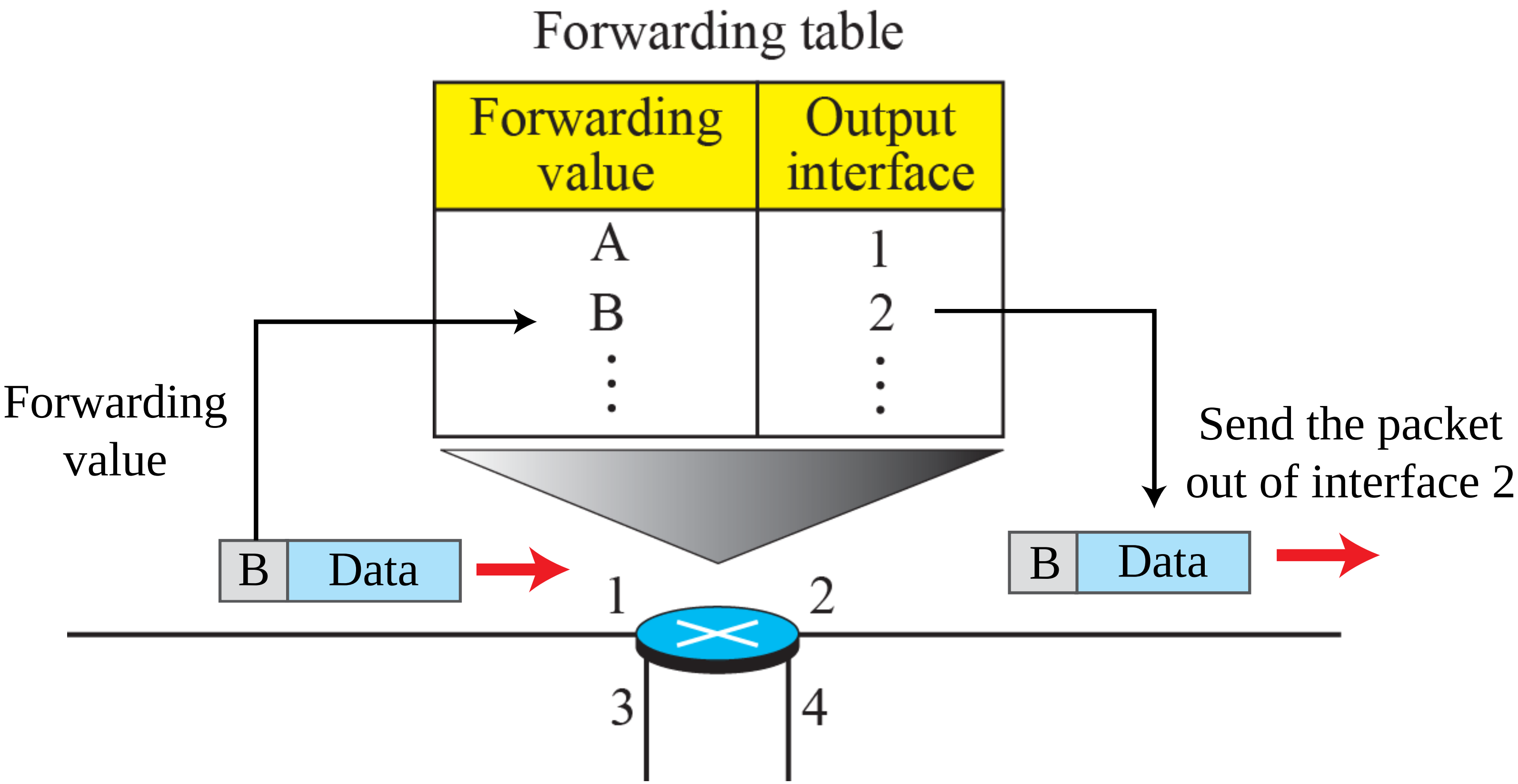
In other words, one duty of the network layer is to carry a payload from the source to the destination without changing it or using it.

The network layer is doing the service of a carrier such as the postal office, which is responsible for delivery of packages from a sender to a receiver without changing or using the contents.

2 Routing and Forwarding

Other duties of the network layer, which are as important as the first, are routing and forwarding, which are directly related to each other.

Figure 2: Forwarding process



Forwarding table

Forwarding value	Output interface
A	1
B	2
⋮	⋮

2 NETWORK-LAYER PERFORMANCE

The upper-layer protocols that use the service of the network layer expect to receive an ideal service, but the network layer is not perfect.

The performance of a network can be measured in terms of delay, throughput, and packet loss.

Congestion control is an issue that can improve the performance.

2.1 Delay

All of us expect instantaneous response from a network, but a packet, from its source to its destination, encounters delays.

The delays in a network can be divided into four types: transmission delay, propagation delay, processing delay, and queuing delay.

Let us first discuss each of these delay types and then show how to calculate a packet delay from the source to the destination..

Transmission Delay:

It is simply time required to put data bits on the wire/communication medium. It depends on length of packet and bandwidth of network.

Transmission Delay = Data size / bandwidth = (L/B) second

Propagation delay:

Time taken by the first bit to travel from sender to receiver end of the link.

Propagation delay = distance/transmission speed = d/s

Processing delay:

Processing delay = Time required to process a packet in a router or a destination host

Queuing delay:

Queuing delay: Time a packet waits in input and output queues in a router

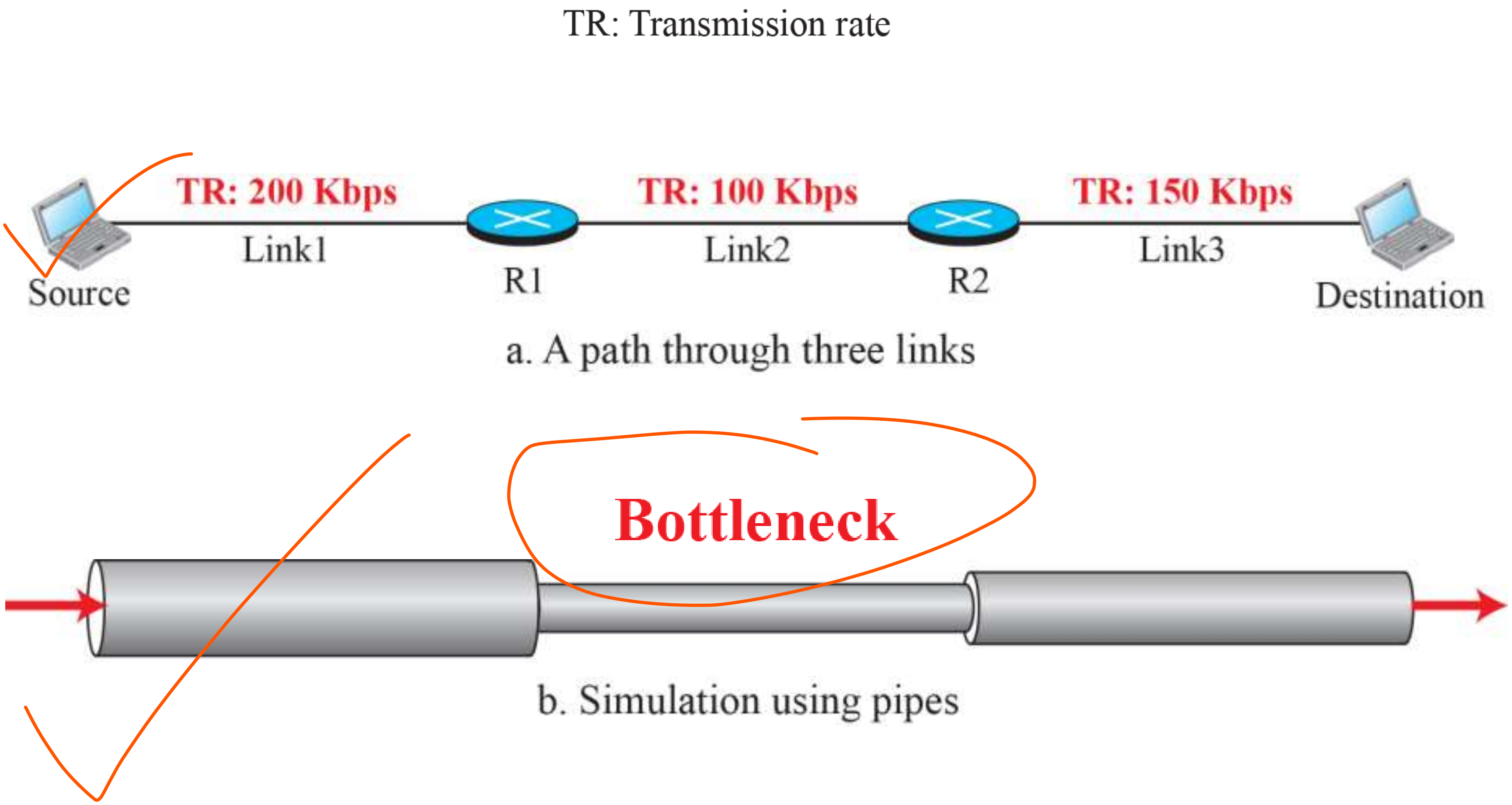
2.2 Throughput

Throughput at any point in a network is defined as the number of bits passing through the point in a second, which is actually the transmission rate of data at that point.

In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate.

How, then, can we determine the throughput of the whole path? To see the situation, assume that we have three links, each with a different transmission rate, as shown in Figure 10.

Figure 10: Throughput in a path with three links in a series



a. A path through three links

b. Simulation using pipes

Figure 11: A path through the Internet backbone

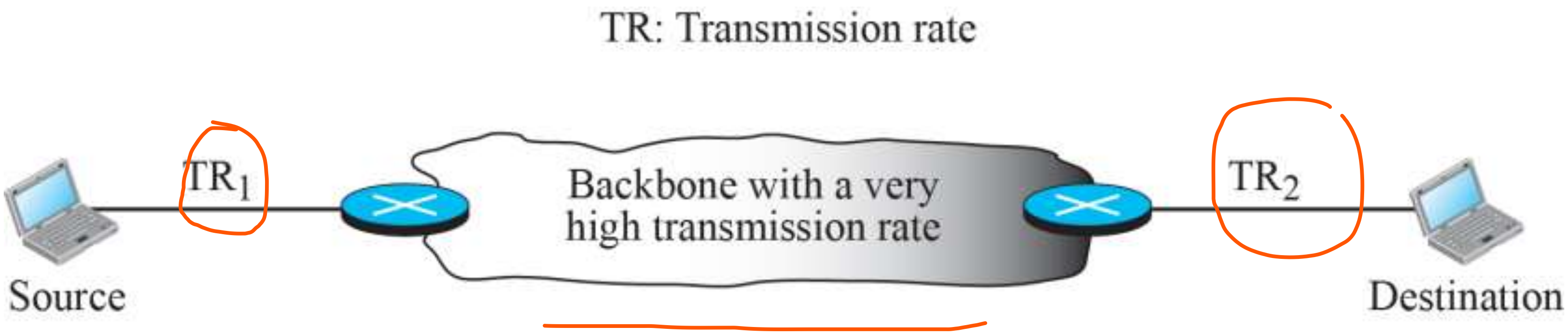
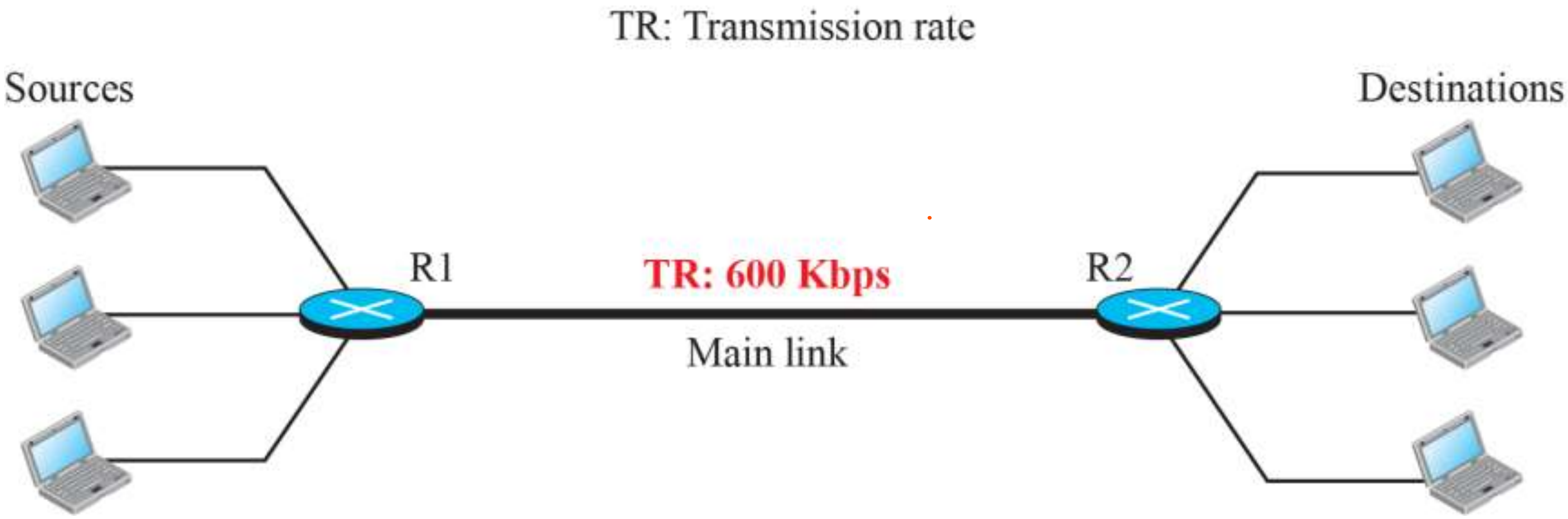


Figure 12: *Effect of throughput in shared links*



2.3 Packet Loss

Another issue that severely affects the performance of communication is the number of packets lost during transmission.

When a router receives a packet while processing another packet, the received packet needs to be stored in the input buffer waiting for its turn.

A router, however, has an input buffer with a limited size. A time may come when the buffer is full and the next packet needs to be dropped.

The effect of packet loss on the Internet network layer is that the packet needs to be resent, which in turn may create overflow and cause more packet loss.

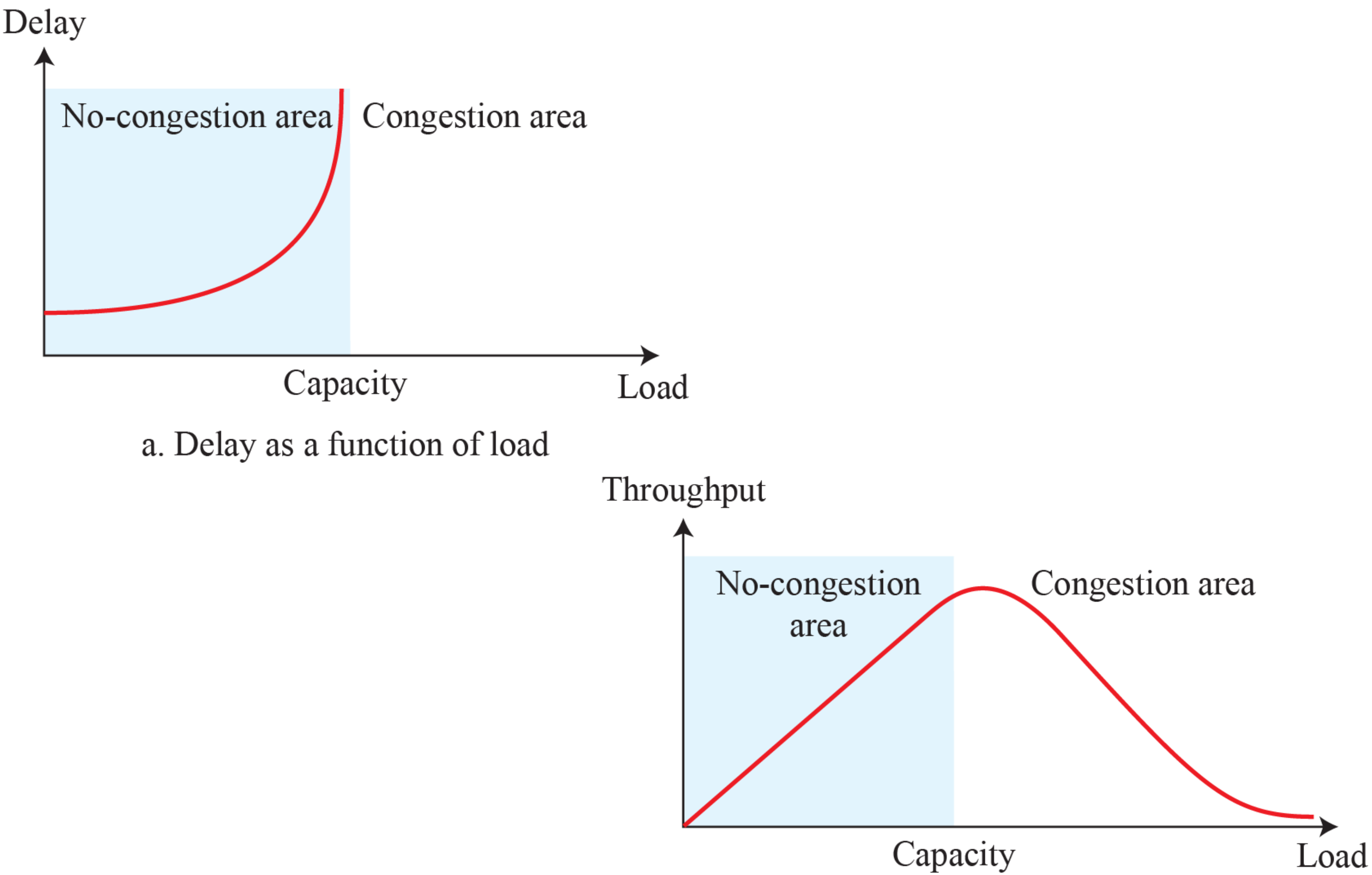
2.4 Congestion Control

Congestion control is a mechanism for improving performance.

Although congestion at the network layer is not explicitly addressed in the Internet model, the study of congestion at this layer may help us to better understand the cause of congestion at the transport layer and find possible remedies to be used at the network layer.

Congestion at the network layer is related to two issues, throughput and delay, which we discussed in the previous section.

Figure 13. Packet delay and throughput as functions of load



a. Delay as a function of load

b. Throughput as a function of load

Logical Addressing

- A computer somewhere in the world needs to communicate with another computer somewhere else in the world.
- Usually, computers communicate through the Internet.
- The packet transmitted by the sending computer may pass through several LANs or WANs before reaching the destination computer.
- The Internet addresses are 32 bits in length; this gives us a maximum of 232 addresses.

  2^32
- These addresses are referred to as IPv4 (IP version 4) addresses or simply IP addresses

3 IPv4 ADDRESSES

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.

IPv4 addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet.

Two devices on the Internet can never have the same address at the same time.

3.1 Address Space

A protocol like IPv4 that defines addresses has an address space.

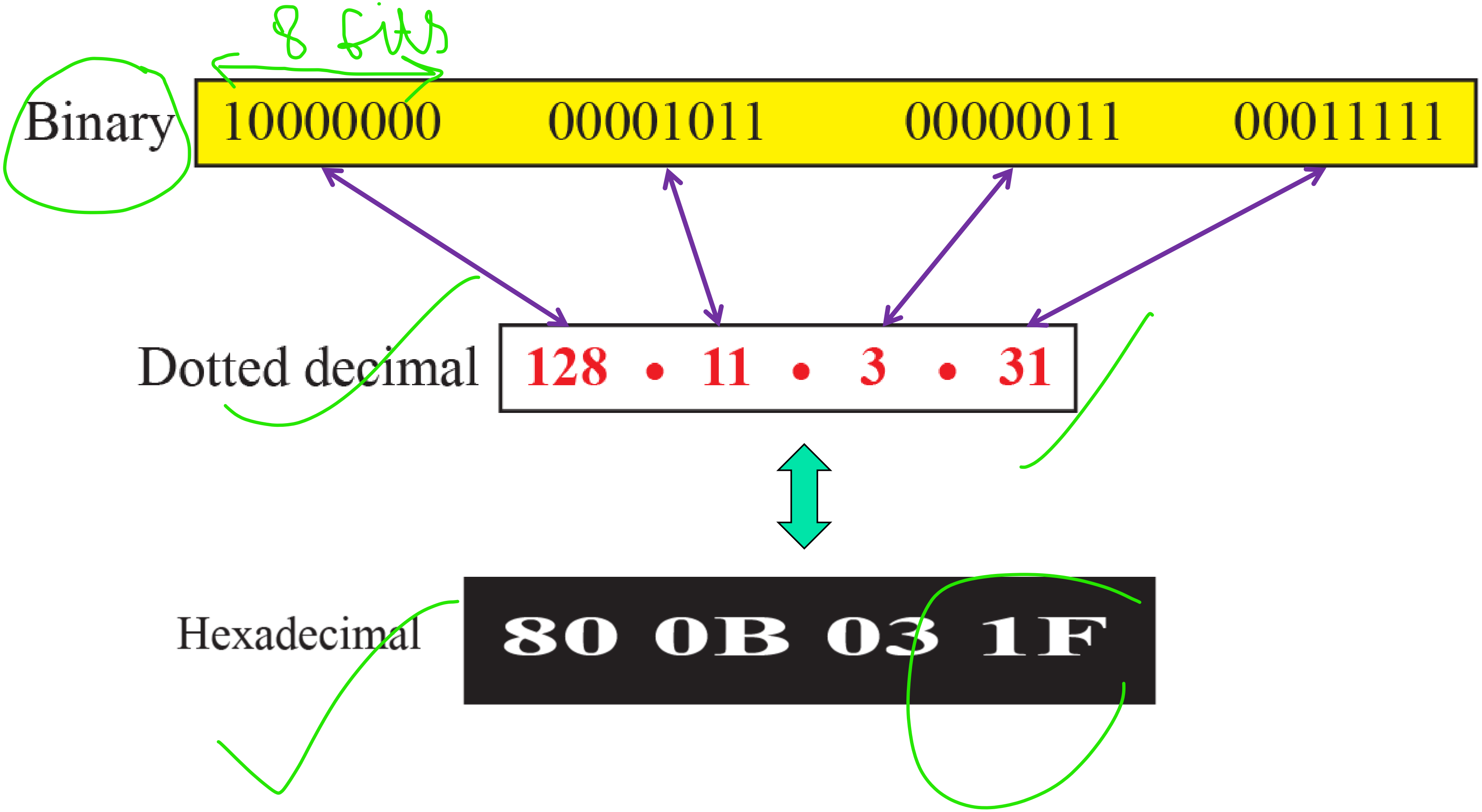
An address space is the total number of addresses used by the protocol.

If a protocol uses b bits to define an address, the address space is 2^b because each bit can have two different values (0 or 1).

IPv4 uses 32-bit addresses, which means that the address space is 2^32 or 4,294,967,296 (more than four billion).

If there were no restrictions, more than 4 billion devices could be connected to the Internet.

Figure 16: *Three different notations in IPv4 addressing*



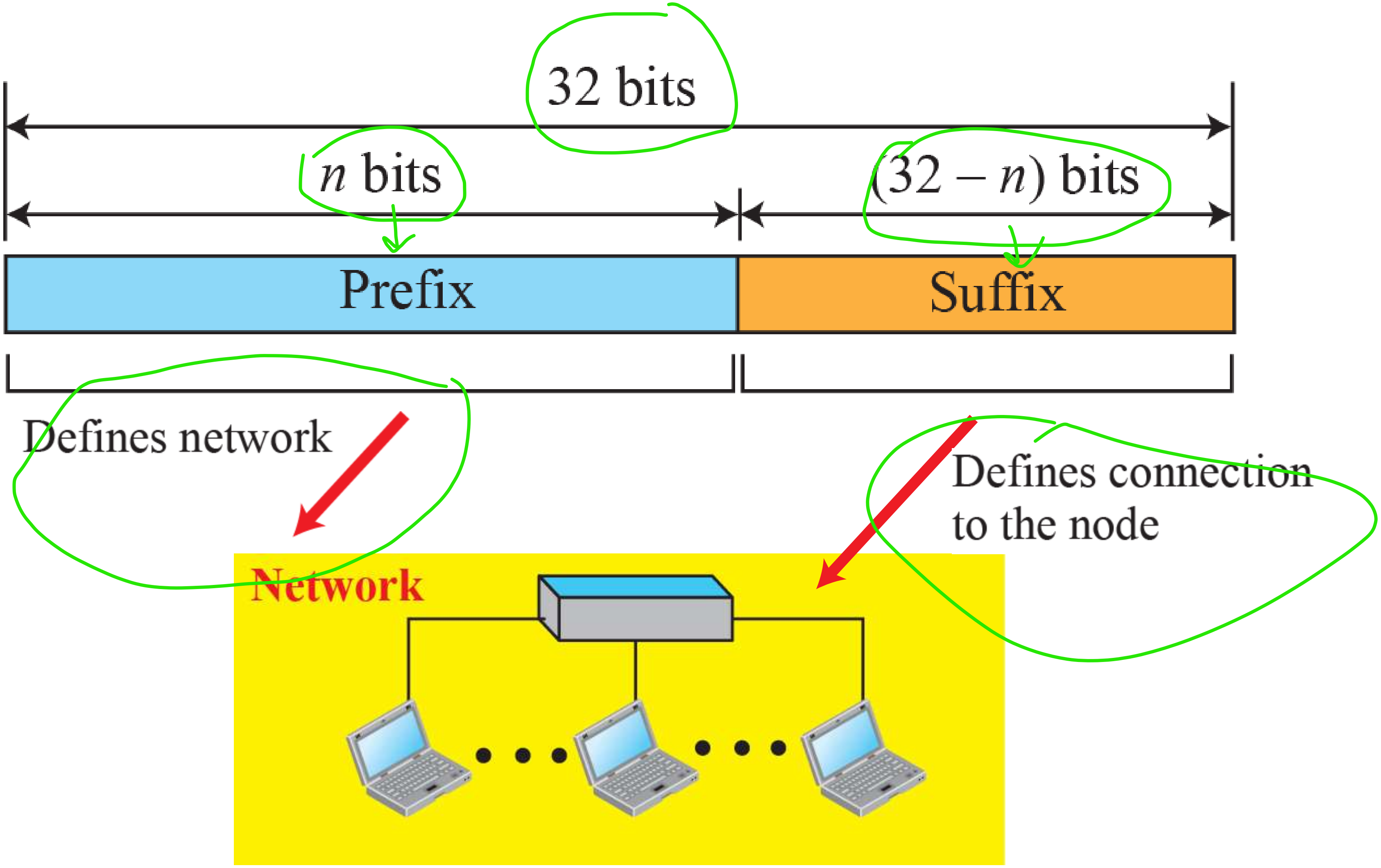
8 bits

Binary 10000000 00001011 00000011 00011111

Dotted decimal 128 • 11 • 3 • 31

Hexadecimal 80 0B 03 1F

Figure 17: Hierarchy in addressing

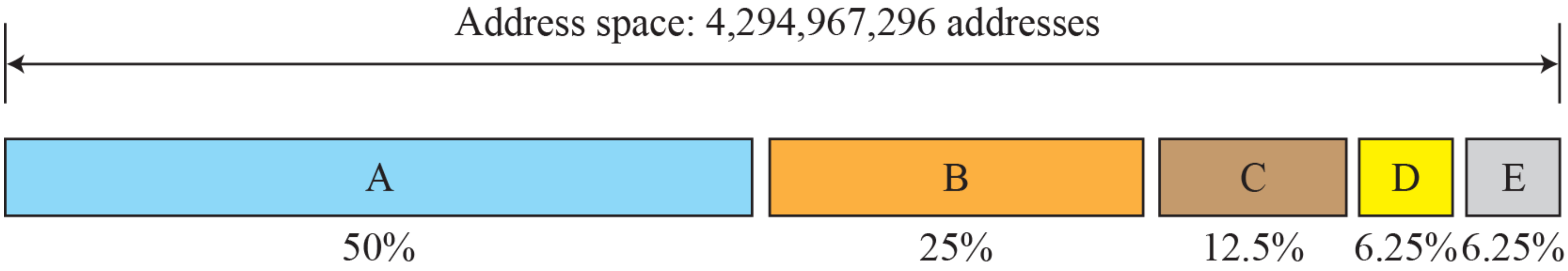


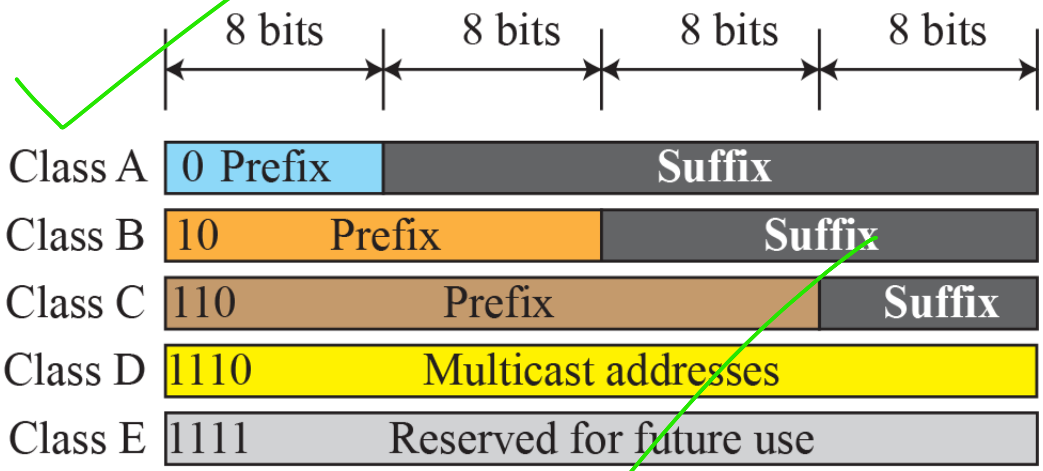
3.2 Classful Addressing

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), as shown in Figure 18. This scheme is referred to as classful addressing. Although classful addressing belongs to the past, it helps us to understand classless addressing, discussed later.

Figure 18: Occupation of the address space in classful addressing

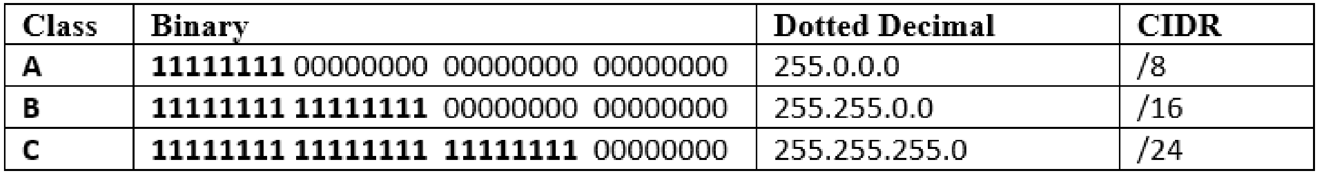




Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Netid, Hostid and Mask

- An IP address of class A, B and C is divided into netid and hosted.
- These parts are of varying lengths, depending on the class of the address.
- Although the length of netid and hosted is predetermined in classful addressing, we can also use a mask, a 32 number made of contiguous 1's followed by contiguous 0s.



Class	Binary	Dotted Decimal	CIDR
A	**11111111** 00000000 00000000 00000000	255.0.0.0	/8
B	**11111111 11111111** 00000000 00000000	255.255.0.0	/16
C	**11111111 11111111 11111111** 00000000	255.255.255.0	/24

Subnetting and Supernetting

Subnetting: 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.

Supernetting: An organization can combine several class C blocks to create a larger range of addresses.

3.3 Classless Addressing

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, however, requires that the length of IP addresses also be increased, which means the format of the IP packets needs to be changed.

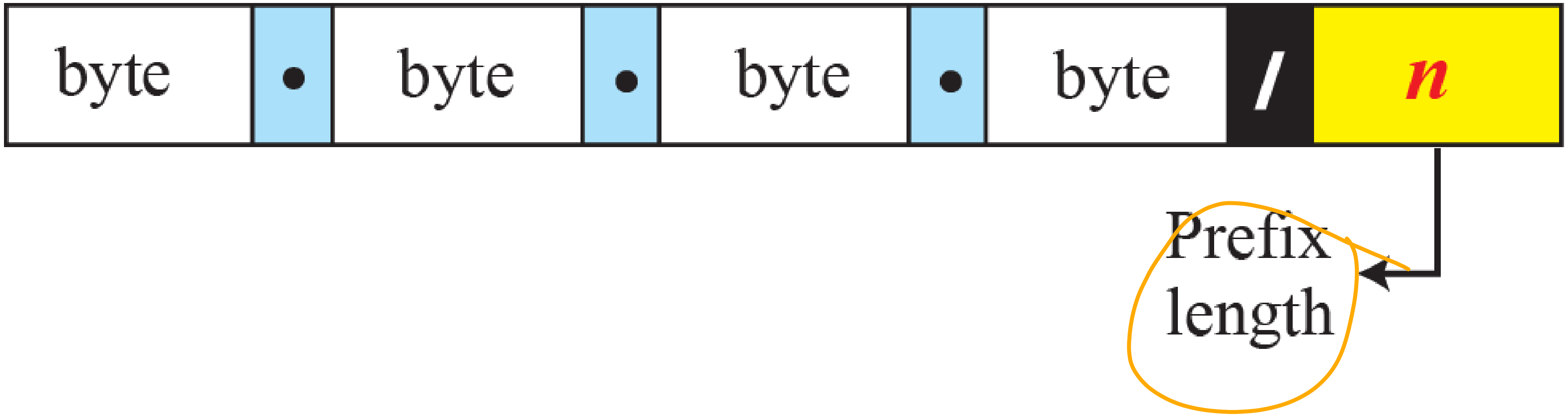
Although the long-range solution has already been devised and is called IPv6, a short-term solution was also devised to use the same address space but to change the distribution of addresses to provide a fair share to each organization.

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

Classless addressing

- To simplify the handling of addresses, the internet authorities impose three restrictions on classless address blocks
- The addresses in the block must be contiguous, one after another.
- The number of addresses in a block must be power of 2.
- The first address must be evenly divisible by the number of addresses.

Figure 20: Slash notation (CIDR)



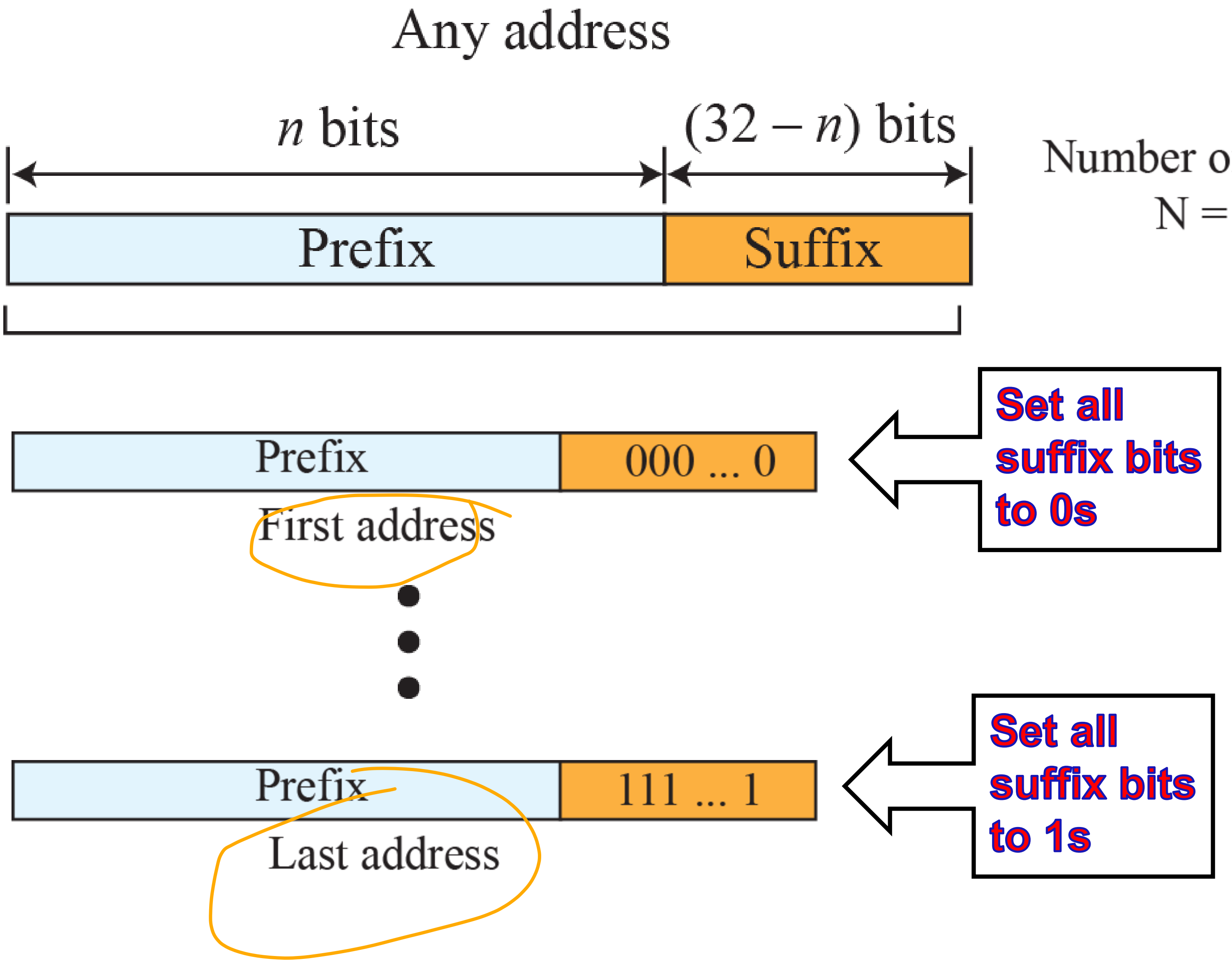
Examples:

12.24.76.8/**8**

23.14.67.92/**12**

220.8.24.255/**25**

Figure 21: *Information extraction in classless addressing*



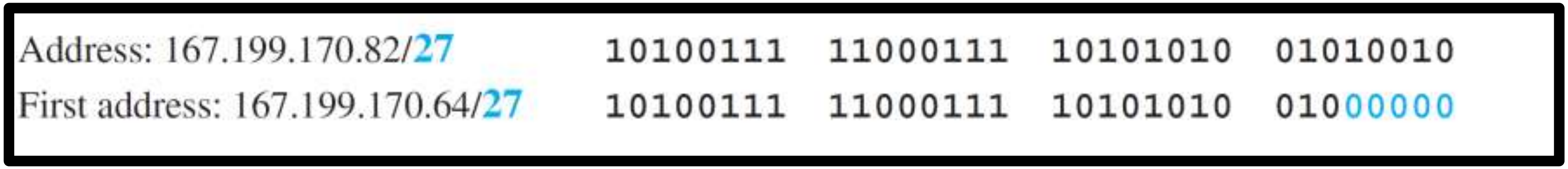
Number of addresses:
$N = 2^{32-n}$

Set all suffix bits to 0s

Set all suffix bits to 1s

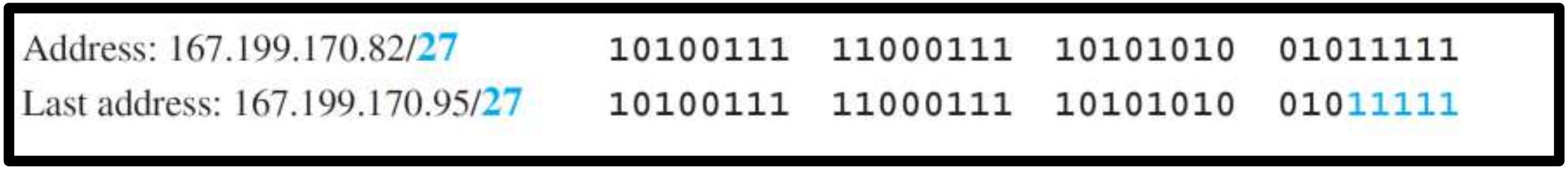
Example 1

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

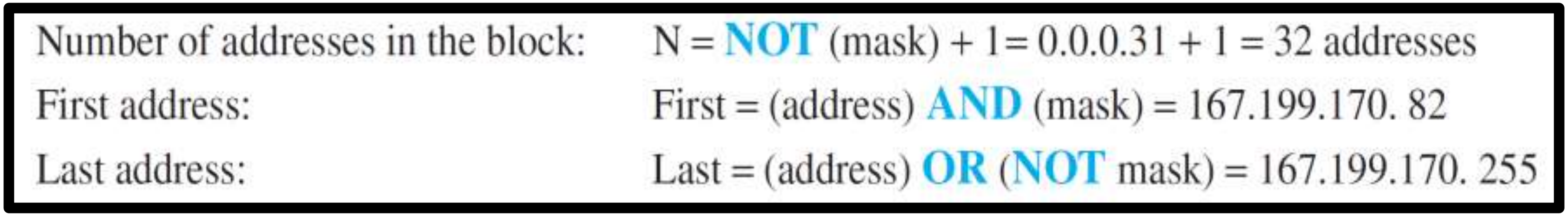
The last address can be found by keeping the first 27 bits and changing the rest of the bits to 1s.



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

Example 2

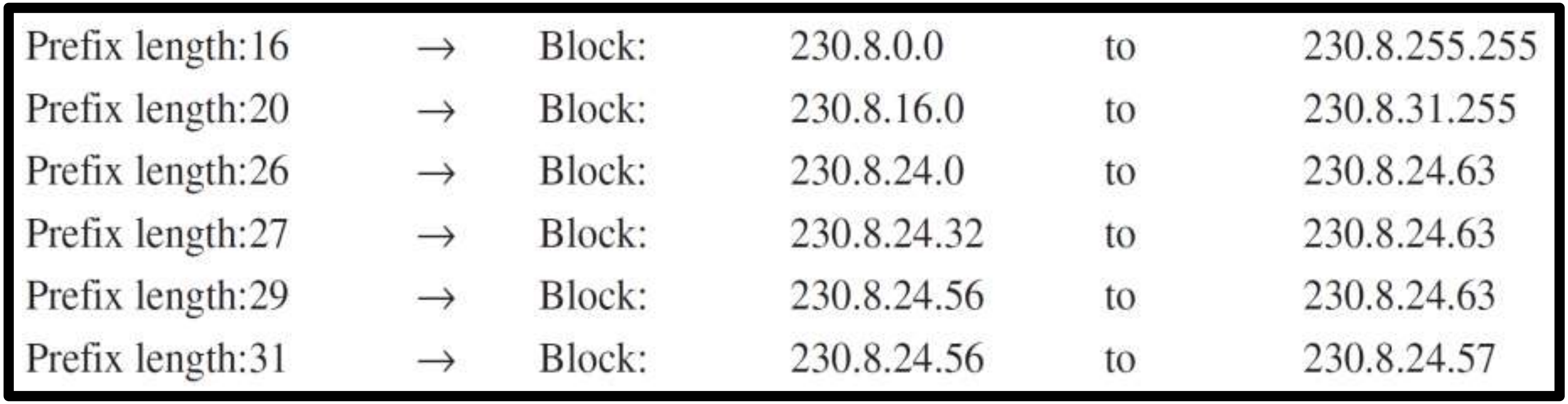
We repeat Example 1 using the mask. The mask in dotted-decimal notation is 256.256.256.224 The AND, OR, and NOT operations can be applied to individual bytes using calculators and applets at the book website.



Number of addresses in the block:	N = **NOT** (mask) + 1= 0.0.0.31 + 1 = 32 addresses
First address:	First = (address) **AND** (mask) = 167.199.170. 82
Last address:	Last = (address) **OR** (**NOT** mask) = 167.199.170. 255

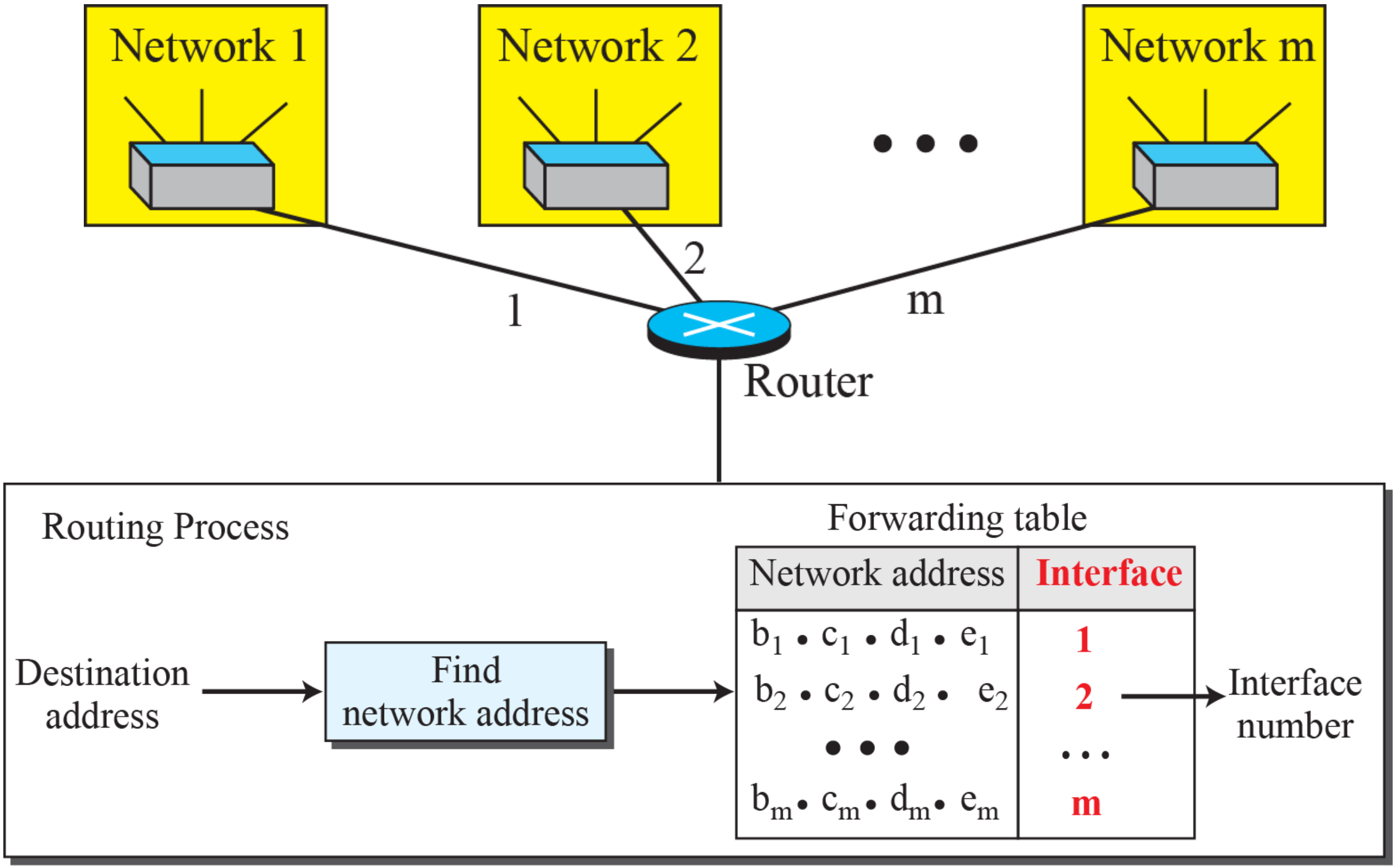
Example 3

In classless addressing, an address cannot per se define the block the address belongs to. For example, the address 230.8.24.56 can belong to many blocks. Some of them are shown below with the value of the prefix associated with that block.



Prefix length:16	→	Block:	230.8.0.0	to	230.8.255.255
Prefix length:20	→	Block:	230.8.16.0	to	230.8.31.255
Prefix length:26	→	Block:	230.8.24.0	to	230.8.24.63
Prefix length:27	→	Block:	230.8.24.32	to	230.8.24.63
Prefix length:29	→	Block:	230.8.24.56	to	230.8.24.63
Prefix length:31	→	Block:	230.8.24.56	to	230.8.24.57

Figure 22: Network address



Forwarding table

Network address	Interface
$b_1 \bullet c_1 \bullet d_1 \bullet e_1$	1
$b_2 \bullet c_2 \bullet d_2 \bullet e_2$	2
• • •	. . .
$b_m \bullet c_m \bullet d_m \bullet e_m$	m

Example 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.

Example 5

An organization is granted a block of addresses with the beginning address 14.24.74.0/**24**. The organization needs to have 3 subblocks of addresses to use in its three subnets: one subblock of 10 addresses, one subblock of 60 addresses, and one subblock of 120 addresses. Design the subblocks.

Solution

There are $2^{32-24} = 256$ addresses in this block. The first address is 14.24.74.0/**24**; the last address is 14.24.74.255/**24**. To satisfy the third requirement, we assign addresses to subblocks, starting with the largest and ending with the smallest one.

Example 5 (continued)

a. The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2. We allocate 128 addresses. The subnet mask for this subnet can be found as $n_1 = 32 - \log_2 128 = 25$. The first address in this block is 14.24.74.0/**25**; the last address is 14.24.74.127/**25**.

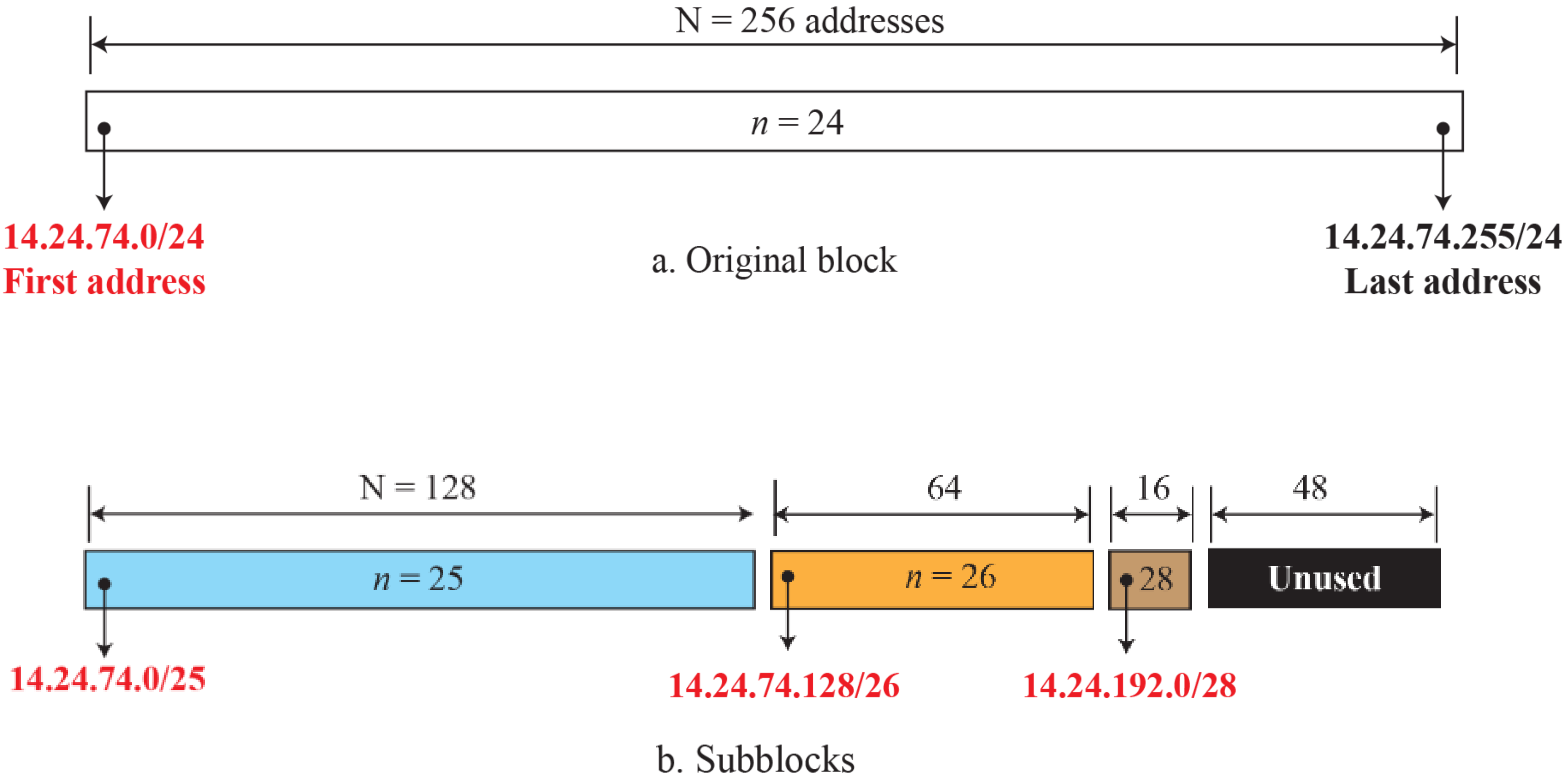
b. The number of addresses in the second largest subblock, which requires 60 addresses, is not a power of 2 either. We allocate 64 addresses. The subnet mask for this subnet can be found as $n_2 = 32 - \log_2 64 = 26$. The first address in this block is 14.24.74.128/**26**; the last address is 14.24.74.191/**26**.

Example 5 (continued)

c. The number of addresses in the largest subblock, which requires 120 addresses, is not a power of 2. We allocate 128 addresses. The subnet mask for this subnet can be found as $n_1 = 32 - \log_2 128 = 25$. The first address in this block is 14.24.74.0/**25**; the last address is 14.24.74.127/**25**.

If we add all addresses in the previous subblocks, the result is 208 addresses, which means 48 addresses are left in reserve. The first address in this range is 14.24.74.208. The last address is 14.24.74.255. We don’t know about the prefix length yet. Figure 18.23 shows the configuration of blocks. We have shown the first address in each block.

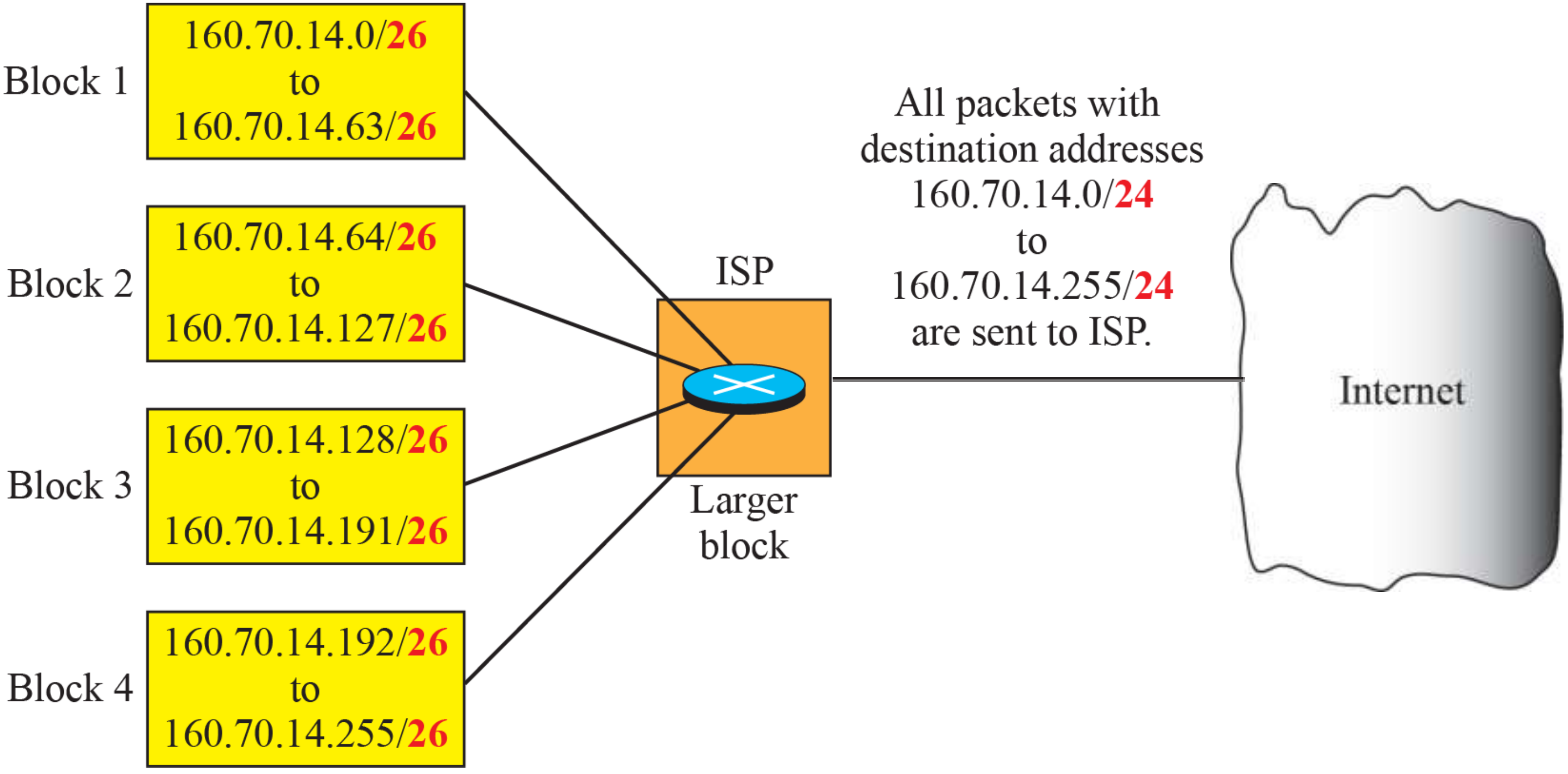
Figure 23: Solution to Example 4.5



Example 6

Figure 24 shows how four small blocks of addresses are assigned to four organizations by an ISP. The ISP combines these four blocks into one single block and advertises the larger block to the rest of the world. Any packet destined for this larger block should be sent to this ISP. It is the responsibility of the ISP to forward the packet to the appropriate organization. This is similar to routing we can find in a postal network. All packages coming from outside a country are sent first to the capital and then distributed to the corresponding destination.

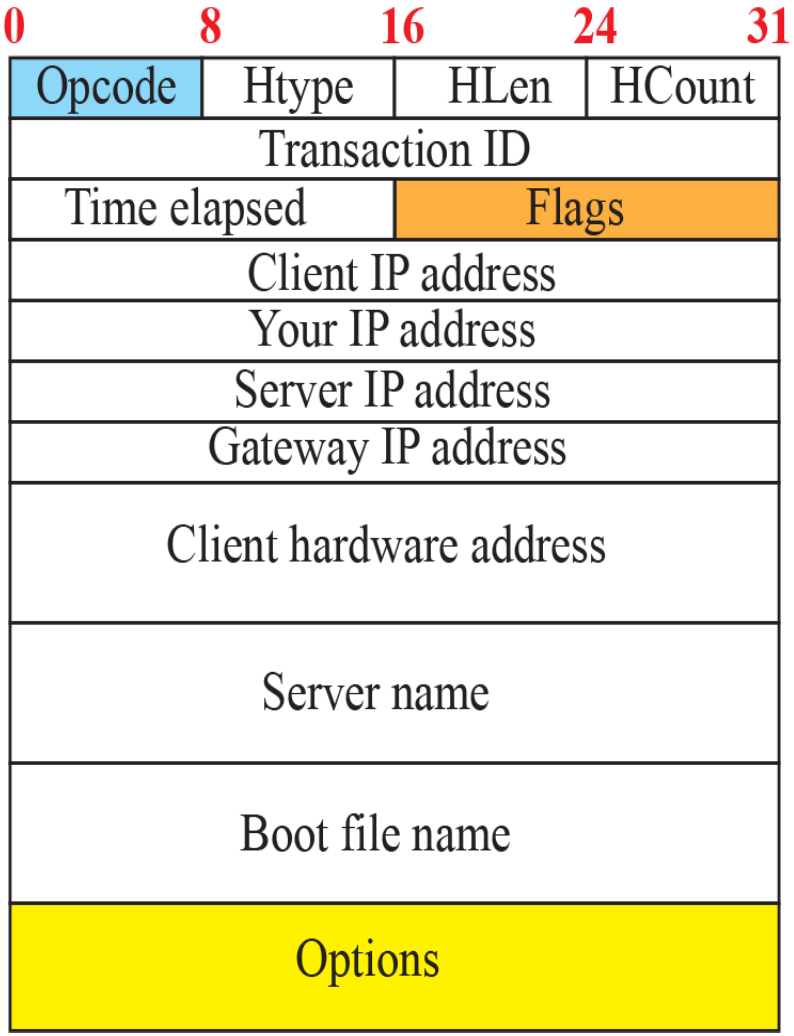
Figure 24: Example of address aggregation



4.4 DHCP

After a block of addresses are assigned to an organization, the network administration can manually assign addresses to the individual hosts or routers. However, 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.

Figure 25: *DHCP message format*



Fields:

Opcode: Operation code, request (1) or reply (2)

Htype: Hardware type (Ethernet, ...)

HLen: Lengh of hardware address

HCount: Maximum number of hops the packet can travel

Transaction ID: An integer set by client and repeated by the server

Time elapsed: The number of seconds since the client started to boot

Flags: First bit defines unicast (0) or multicast (1); other 15 bits not used

Client IP address: Set to 0 if the client does not know it

Your IP address: The client IP address sent by the server

Server IP address: A broadcast IP address if client does not know it

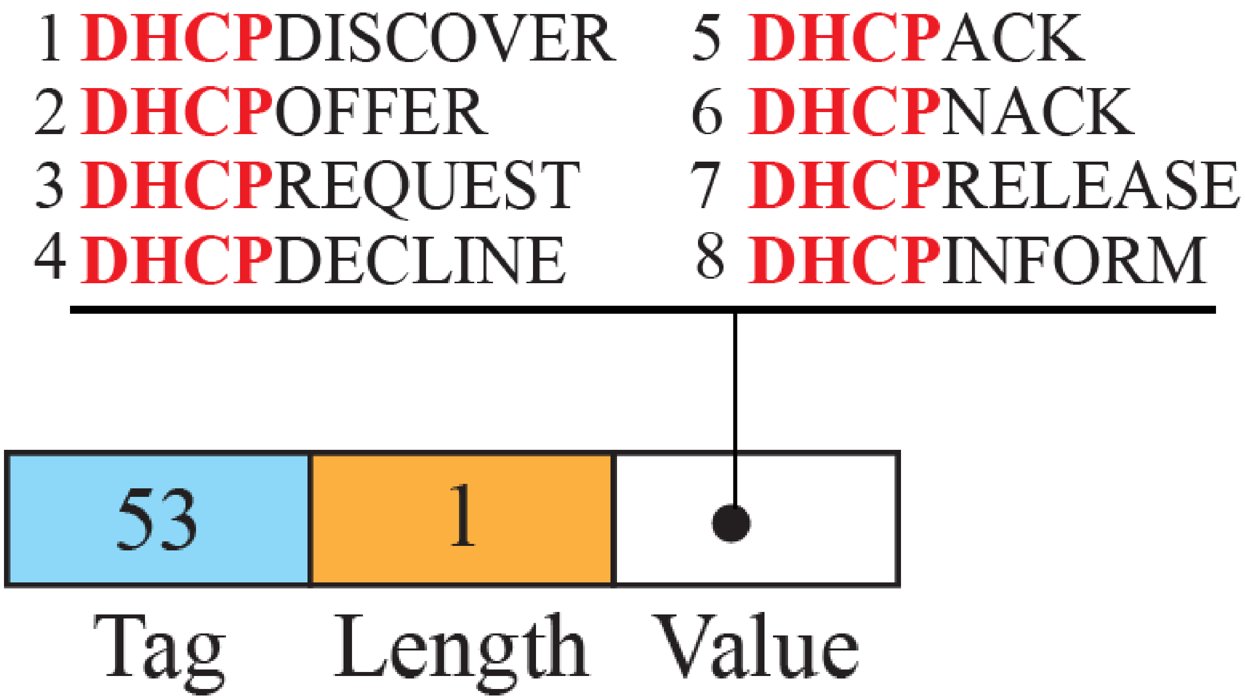
Gateway IP address: The address of default router

Server name: A 64-byte domain name of the server

Boot file name: A 128-byte file name holding extra information

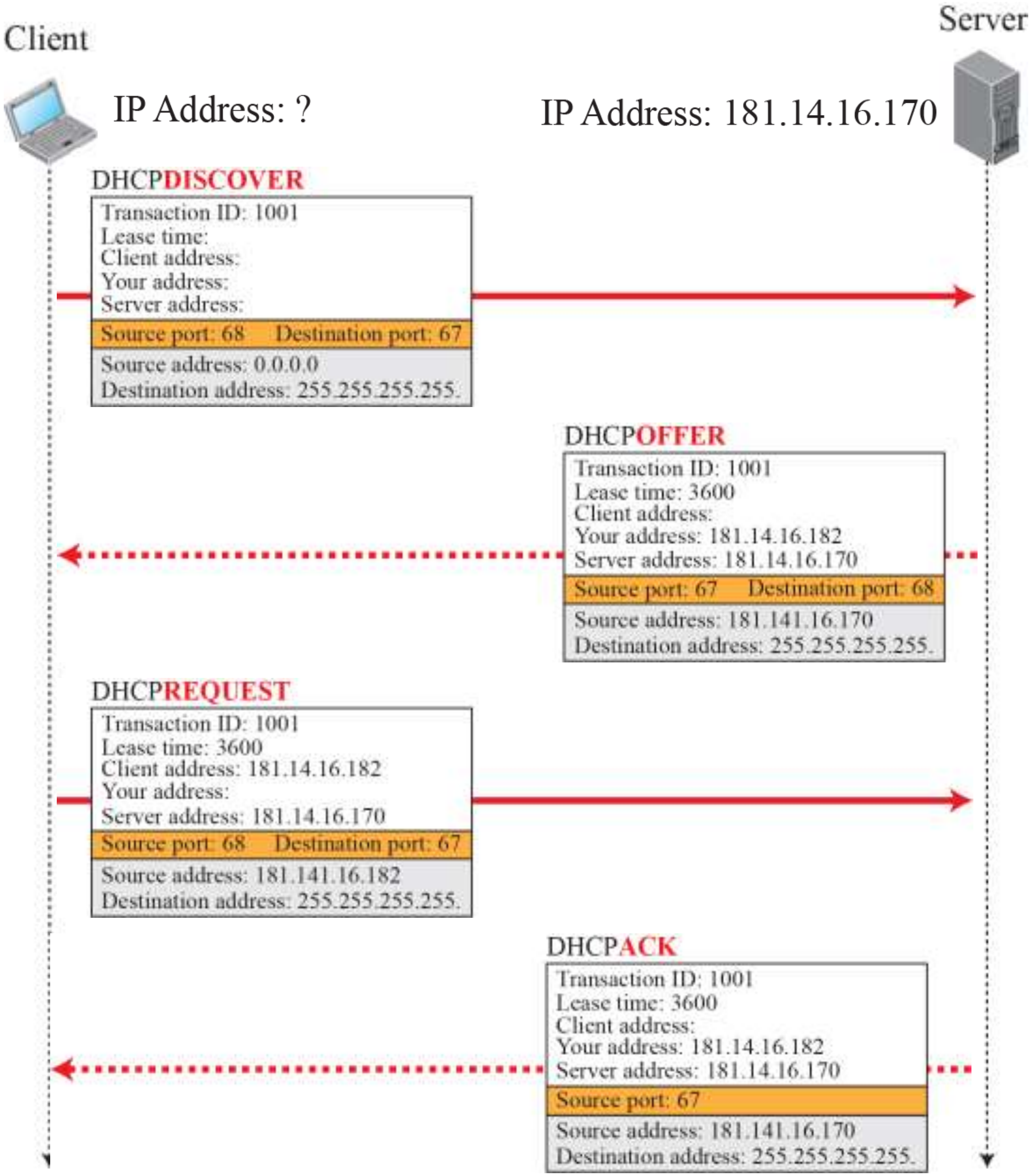
Options: A 64-byte field with dual purpose described in text

Figure 26: Option format



1 DHCPDISCOVER
2 DHCPOFFER
3 DHCPREQUEST
4 DHCPDECLINE
5 DHCPACK
6 DHCPNACK
7 DHCPRELEASE
8 DHCPINFORM

Figure 27: Operation of DHCP



Client

IP Address: ?

Server

IP Address: 181.14.16.170

DHCPDISCOVER

Transaction ID: 1001
Lease time:
Client address:
Your address:
Server address:
Source port: 68 Destination port: 67
Source address: 0.0.0.0
Destination address: 255.255.255.255.

DHCPOFFER

Transaction ID: 1001
Lease time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67 Destination port: 68
Source address: 181.141.16.170
Destination address: 255.255.255.255.

DHCPREQUEST

Transaction ID: 1001
Lease time: 3600
Client address: 181.14.16.182
Your address:
Server address: 181.14.16.170
Source port: 68 Destination port: 67
Source address: 181.141.16.182
Destination address: 255.255.255.255.

DHCPACK

Transaction ID: 1001
Lease time: 3600
Client address:
Your address: 181.14.16.182
Server address: 181.14.16.170
Source port: 67
Source address: 181.141.16.170
Destination address: 255.255.255.255.

Legend

Application
UDP
IP

Note:
Only partial information is given.

4.5 NAT

In most situations, only a portion of computers in a small network need access to the Internet simultaneously.

A technology that can provide the mapping between the private and universal addresses, and at the same time support virtual private networks, is Network Address Translation (NAT).

The technology allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world.

Figure 29: NAT

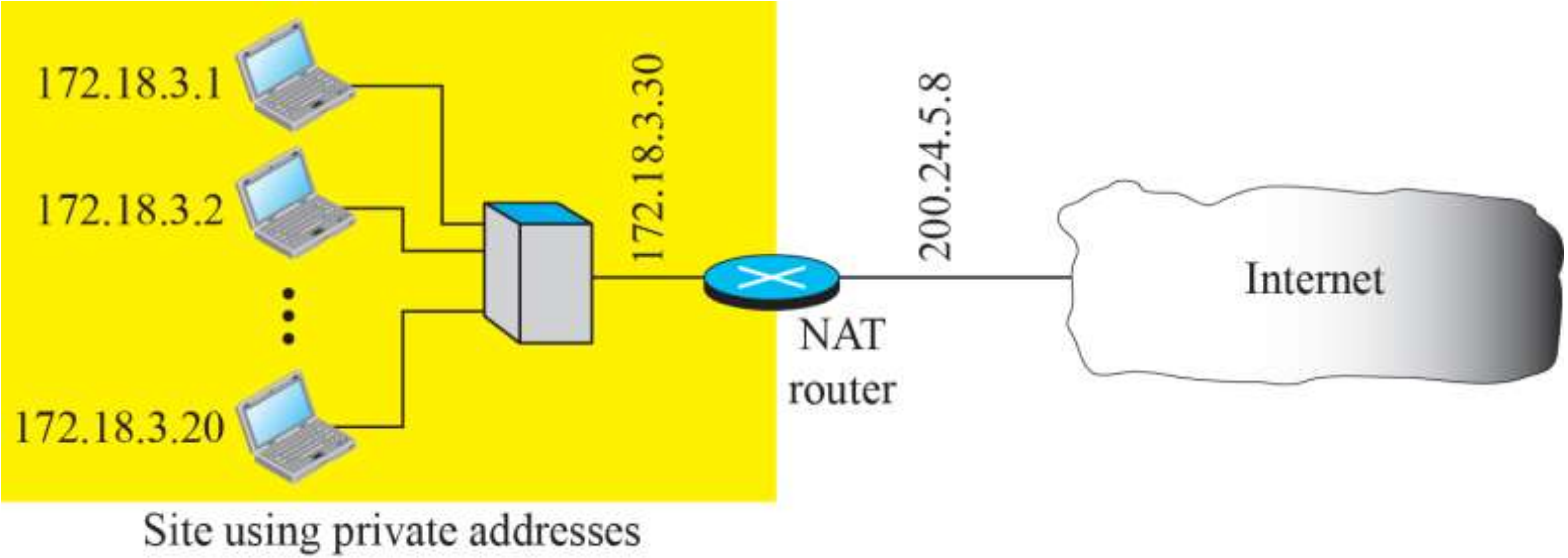


Figure 30: *Address translation*

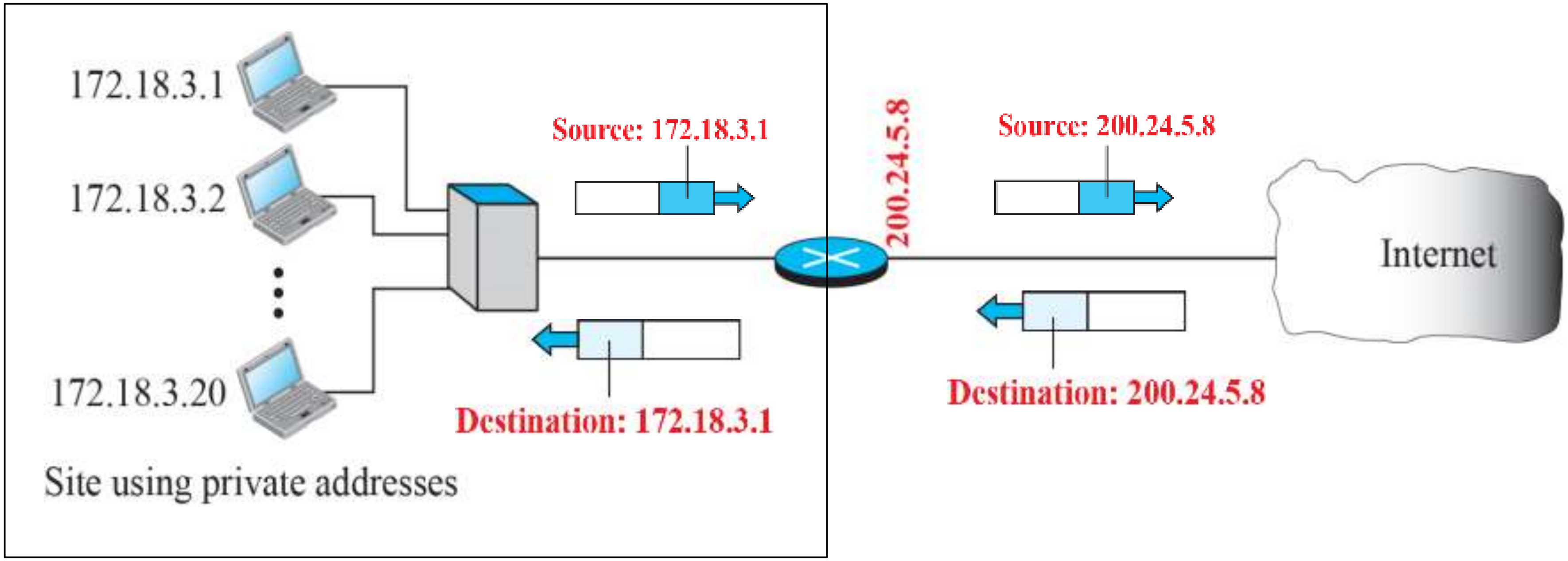


Figure 31: Translation

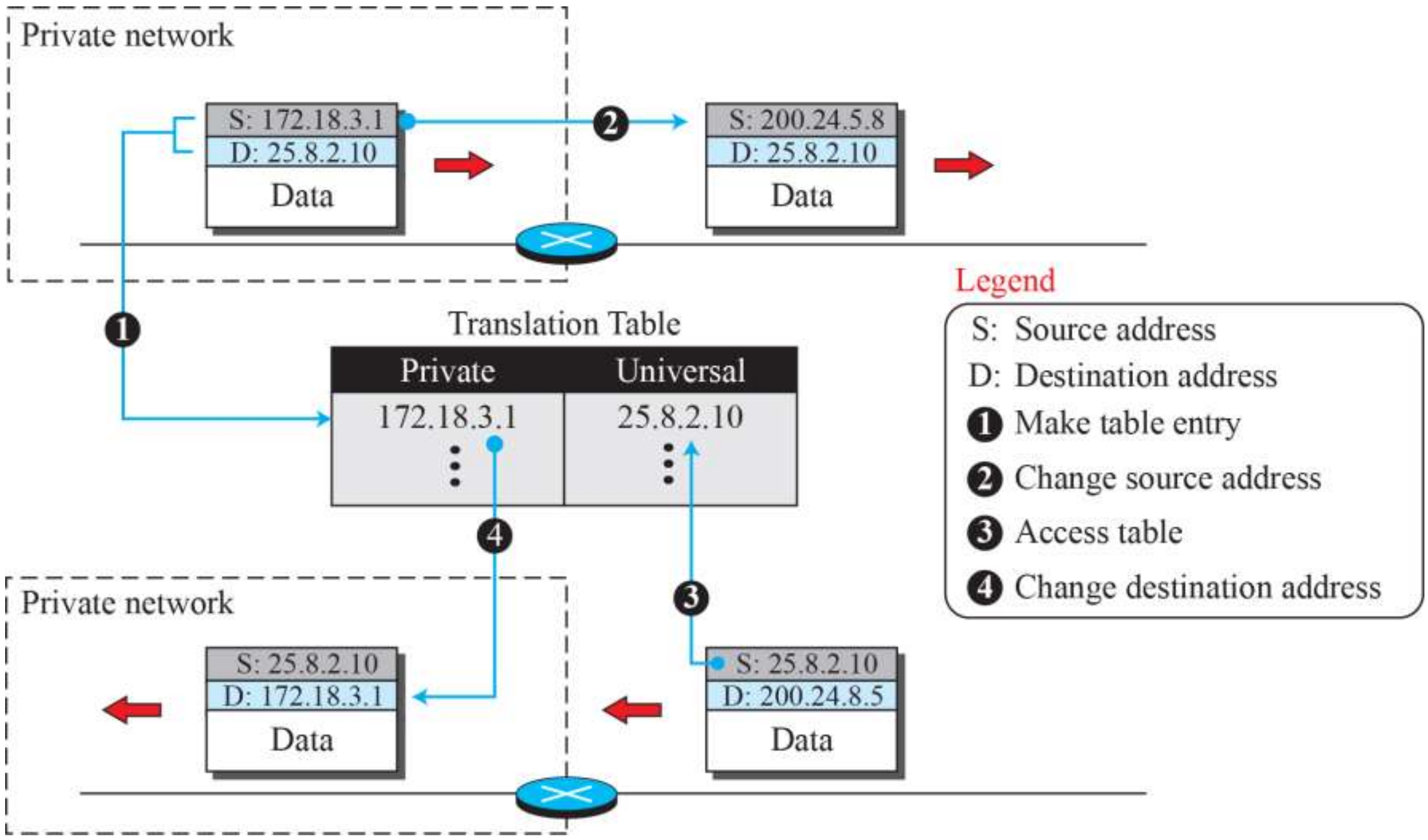
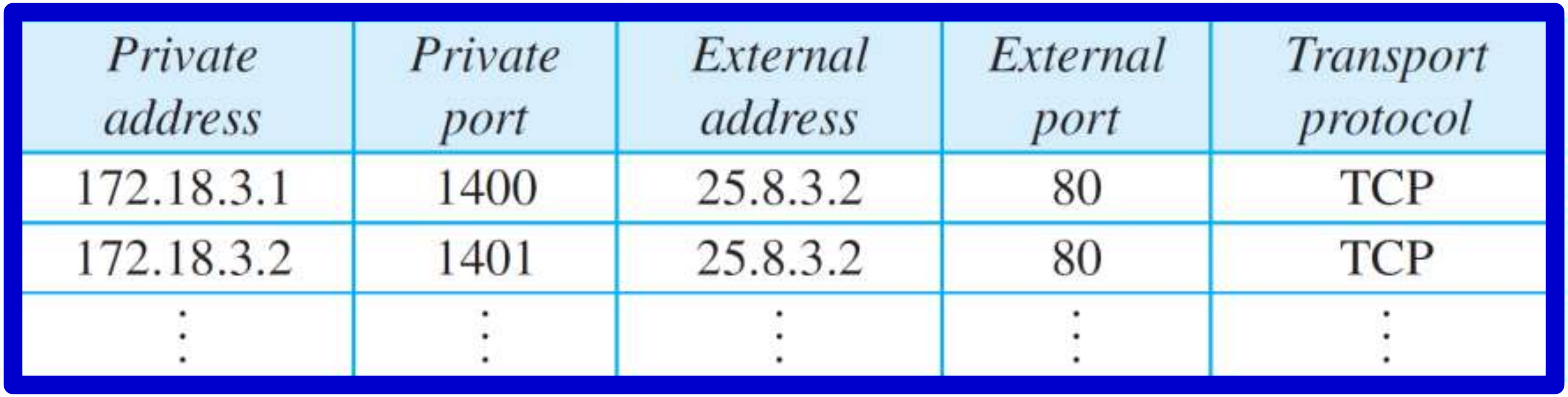


Table 1: Five-column translation table



Private address	*Private port*	*External address*	*External port*	*Transport protocol*
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
⋮	⋮	⋮	⋮	⋮