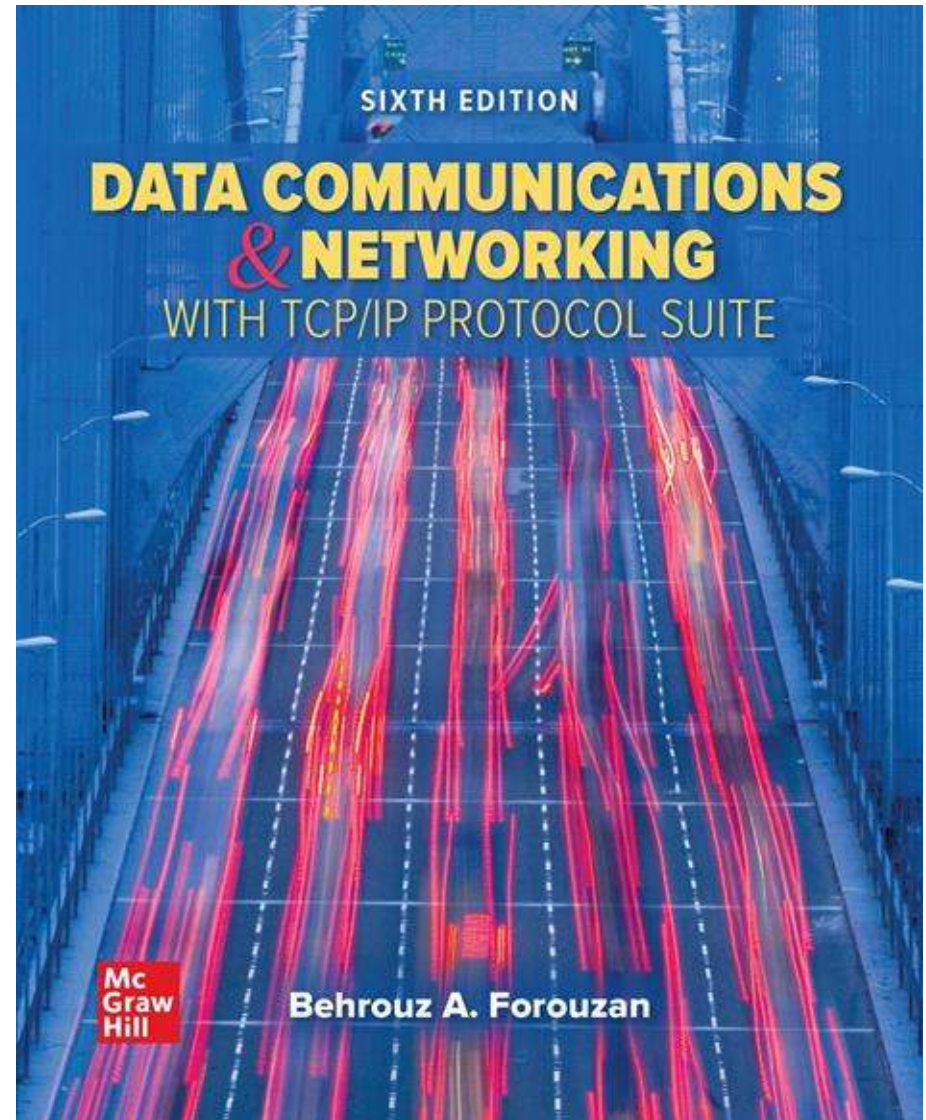


Chapter 07

Network Layer: Data Transfer

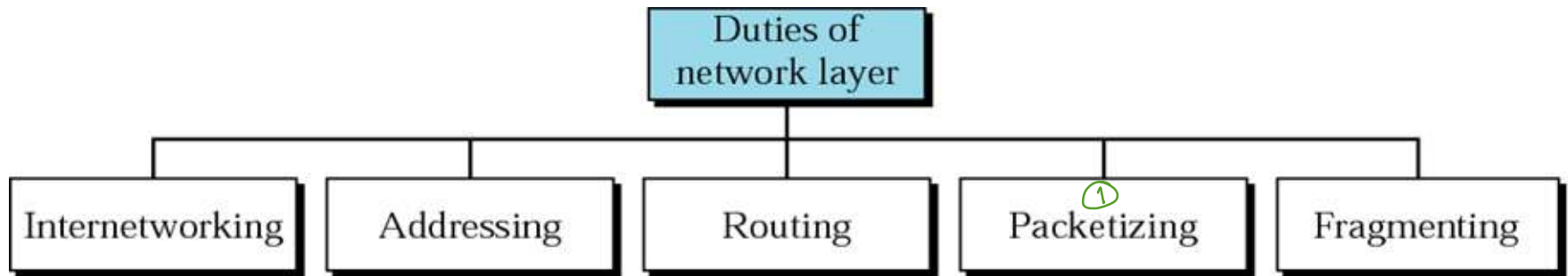
- Data Communications and Networking, With TCP/IP protocol suite Sixth Edition
- Behrouz A. Forouzan



Chapter 7: Outline

- **7.1 Services**
- **7.2 Packet Switching**
- **7.4 Internet Protocol V4**

Network layer duties



Packetizing : similar to encapsulation

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 ^{important data} 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 ^{similar to amazon} postal office, which is responsible for delivery of packages from a sender to a receiver without changing or using the contents.

Includes:

- ① Sender/receiver
- ② Stamp
- ③ Actual contents being sent

Routing and Forwarding



Routing: Finding the best path (route) by running routing protocols to fill a decision-making table (called routing table).

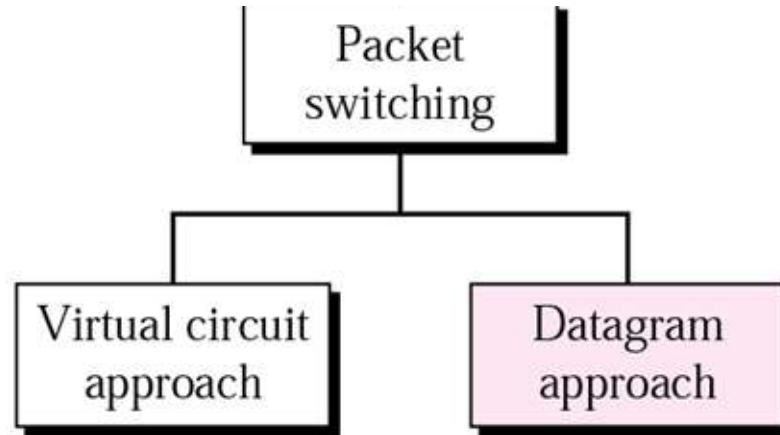
Forwarding: The action applied by the router when it receives a packet at one of its interfaces. It will decide from which other interface the packet should be sent.

PACKET SWITCHING

router higher level than switch
↳ act as switch

From the discussion of routing and forwarding in the previous section, we infer that a kind of switching occurs at the network layer. A router, in fact, is a switch that creates a connection between an input port and an output port (or a set of output ports), just as an electrical switch connects the input to the output to let electricity flow.

SWITCHING



Packet switching –

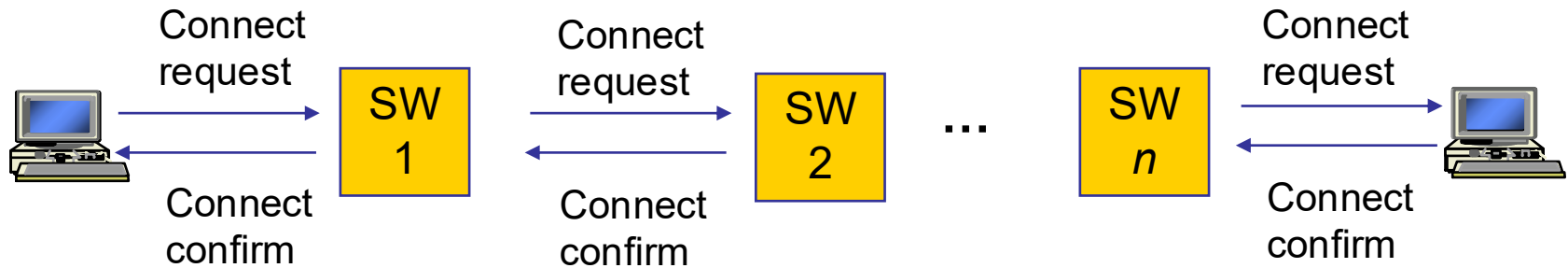
Virtual-Circuit Approach

best path for data, virtually define as my path

*In a connection-oriented service (also called **virtual-circuit** approach), there is a relationship between all packets belonging to a message. Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams. After connection setup, the datagrams can all follow the same path. In this type of service, not only must the packet contain the source and destination addresses, it must also contain a flow label, a **virtual circuit identifier** that defines the virtual path the packet should follow.*

Virtual circuit Setup

Parameters such as buffer, bandwidth, delay requirements were set in every switch along the path during setup



Question: why called virtual-circuit?

Because resources, e.g., switches, buffers and lines, are **shared** by packets from multiple connections.

Figure: *A virtual-circuit packet-switched network*

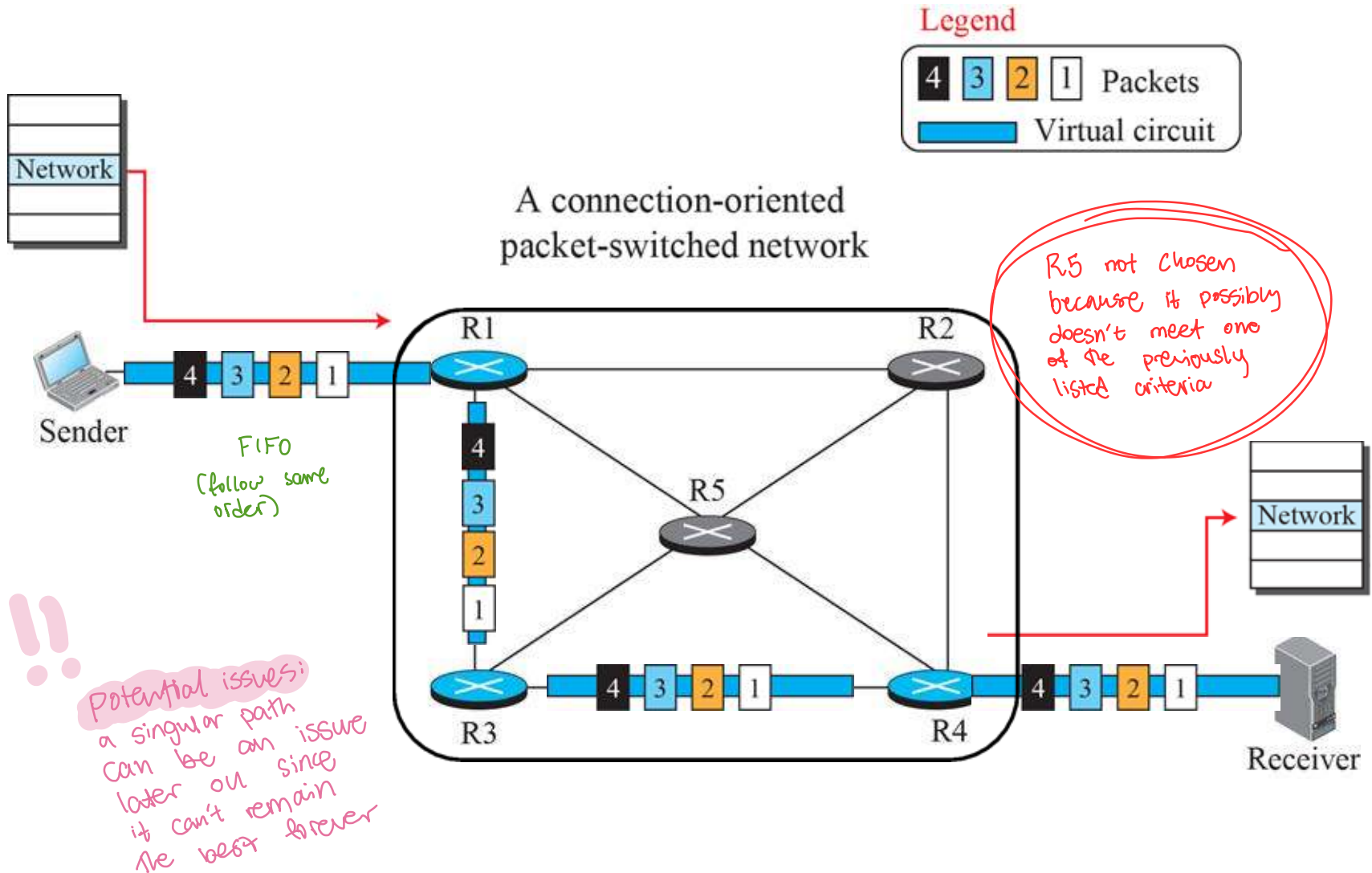


Figure : Flow of one packet in an established virtual circuit

online resources for practice

must know to fill table

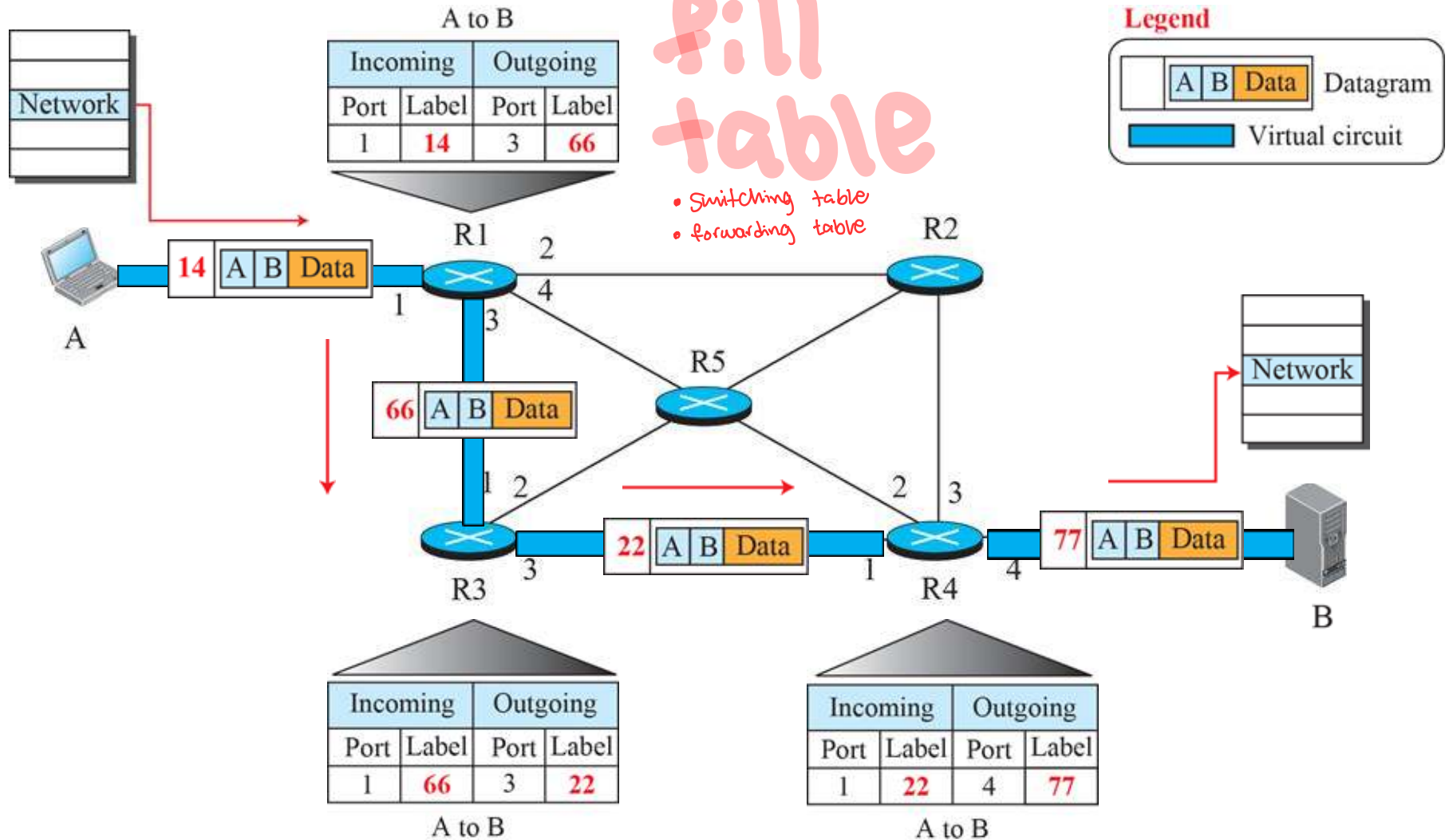
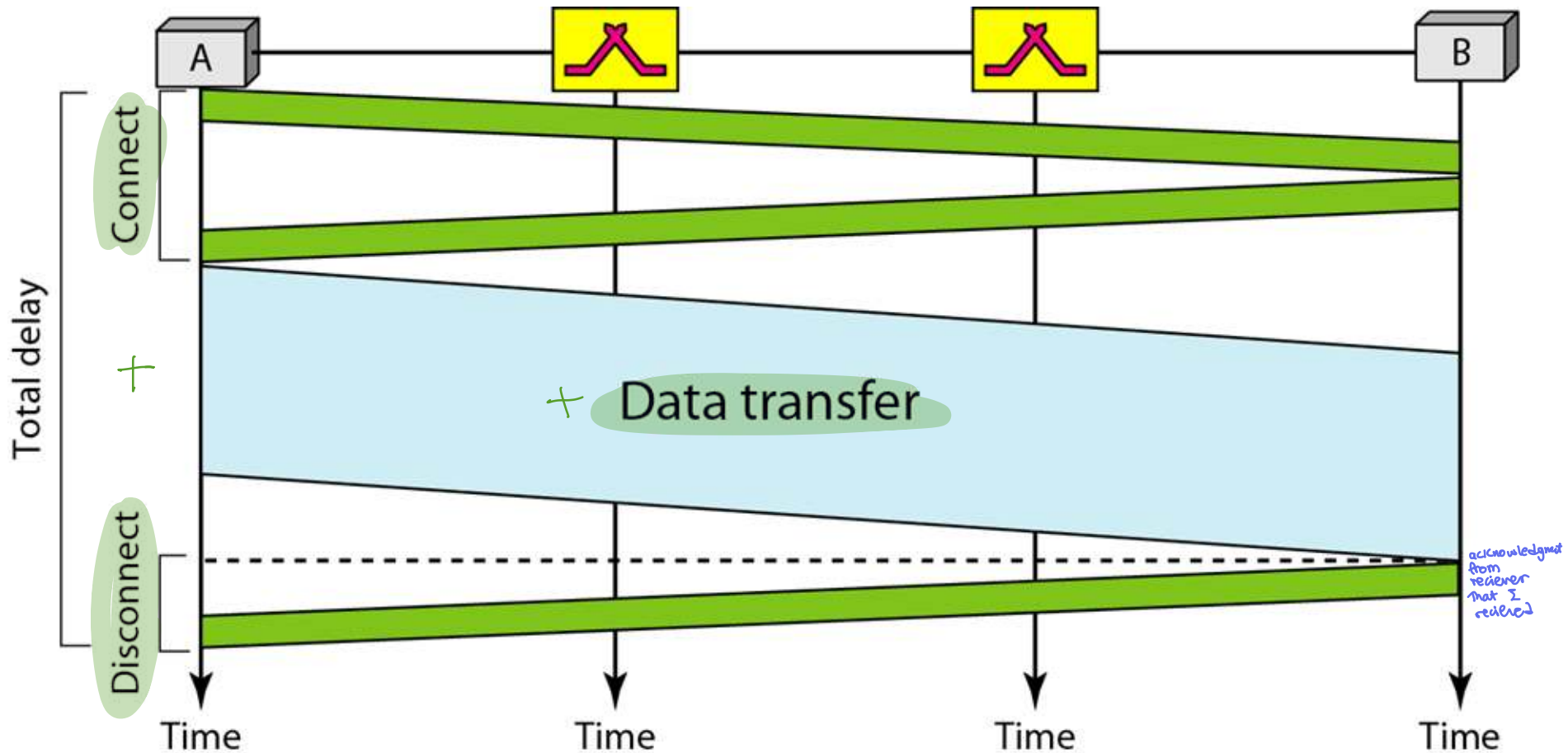


Figure: *Delay in a circuit-switched network*

Another delay type can be asked about



Packet switching –

Datagram Approach

more flexible

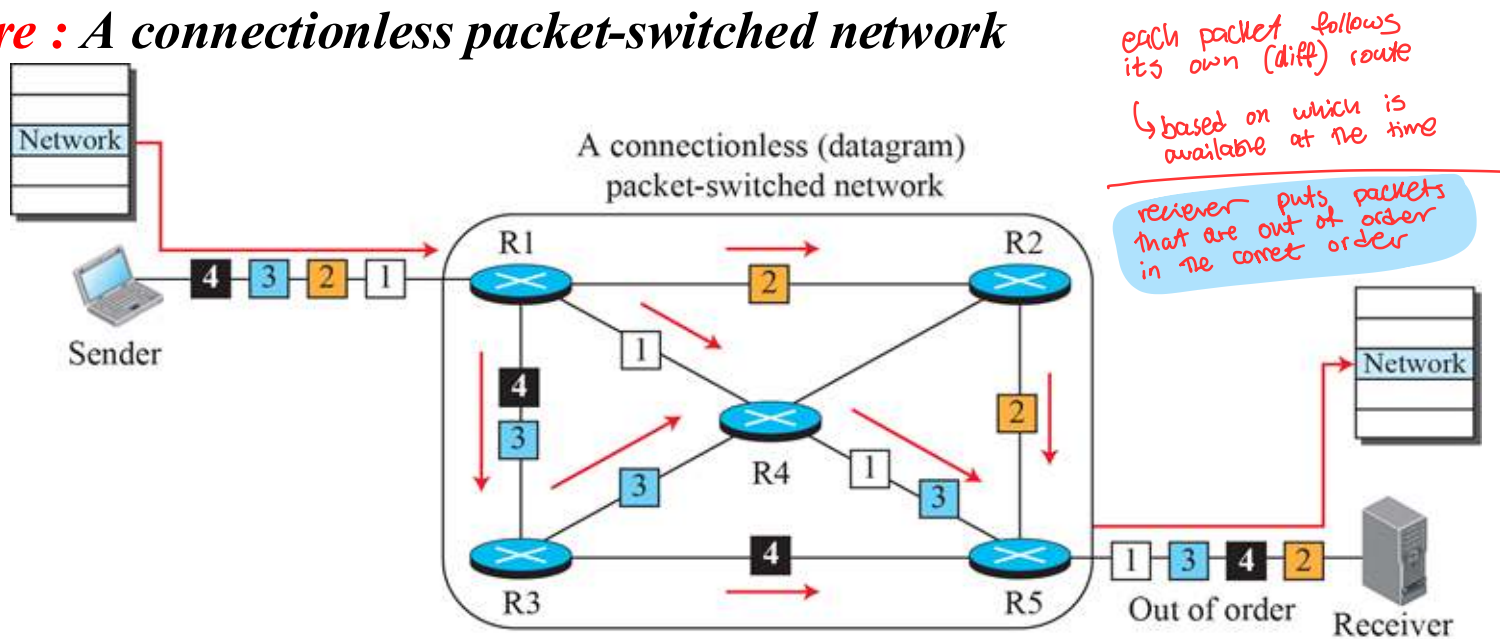
When the Internet started, to make it simple, the network layer was designed to provide a connectionless service in which the network-layer protocol treats each packet independently, with each packet having no relationship to any other packet. The idea was that the network layer is only responsible for delivery of packets from the source to the destination. In this approach, the packets in a message may or may not travel the same path to their destination.



Note:

*Communication at the network layer
in the Internet is connectionless.*

Figure : A connectionless packet-switched network



Connectionless service : **No handshaking**, each packet is sent and routed independently and can follow different paths to reach to the destination.

The full address of the source and destination must be attached to each packet. !!!

- **No setup delay** Advantage!!
- Packets are not guaranteed to arrive in the order they were sent
- **Robust**: If a router crashes only packets inside the router will be lost, other packets can follow other path
- **Used in the Internet**

on the other hand, other kind of delay
time and must find another route
that works instead

Must repeat
• handshake
• find path again

Figure: *Delay in a datagram network*

little waiting time

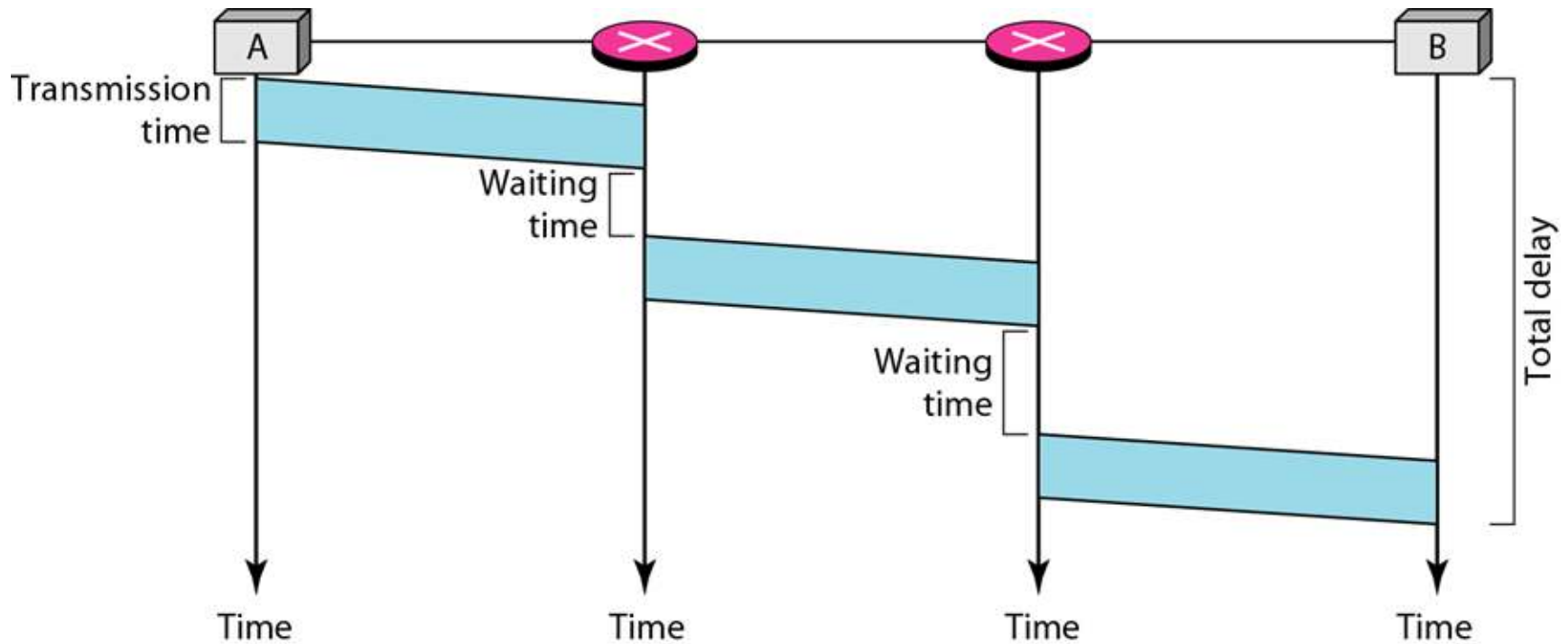
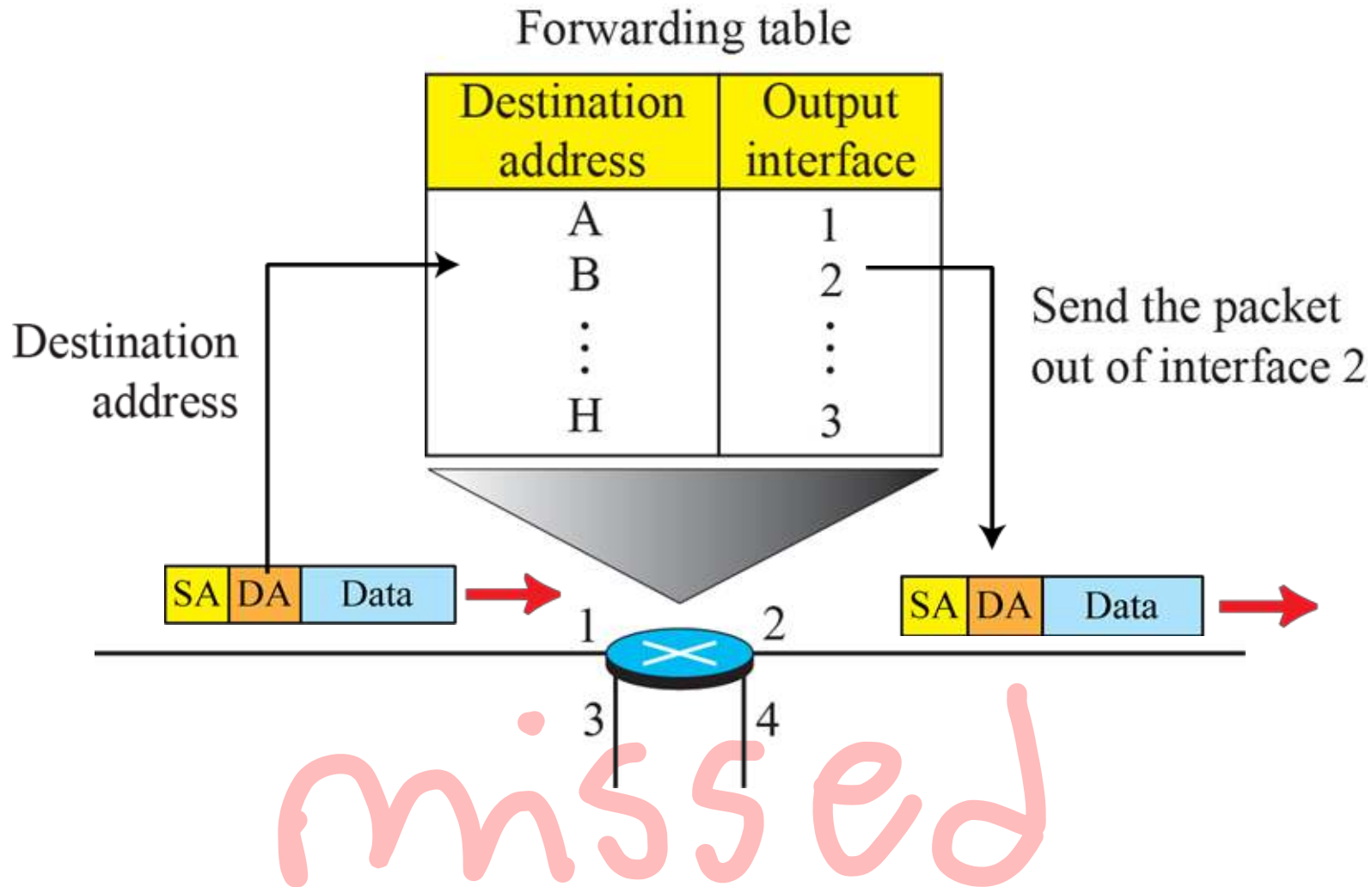


Figure : *Forwarding process in a router when used in a connectionless network*



Addressing

- The address in the network layer of the TCP/IP model is called Internet Address or IP address
- An IP address is a 32-bit address
- The IP addresses are **unique** (each **connection** has a different address) and universal (must be accepted by any host wants to connect to the internet).
- Consists of 4 octets (bytes)
- Network IP addresses are managed by a nonprofit organization called ICANN (**International Corporation for Assigned Names and Numbers**) to avoid conflicts.
 - Assigns addresses to **regional Authorities** which **assign numbers to ISPs**
 - Assigns and manages DNS (Domain Name System)

Note

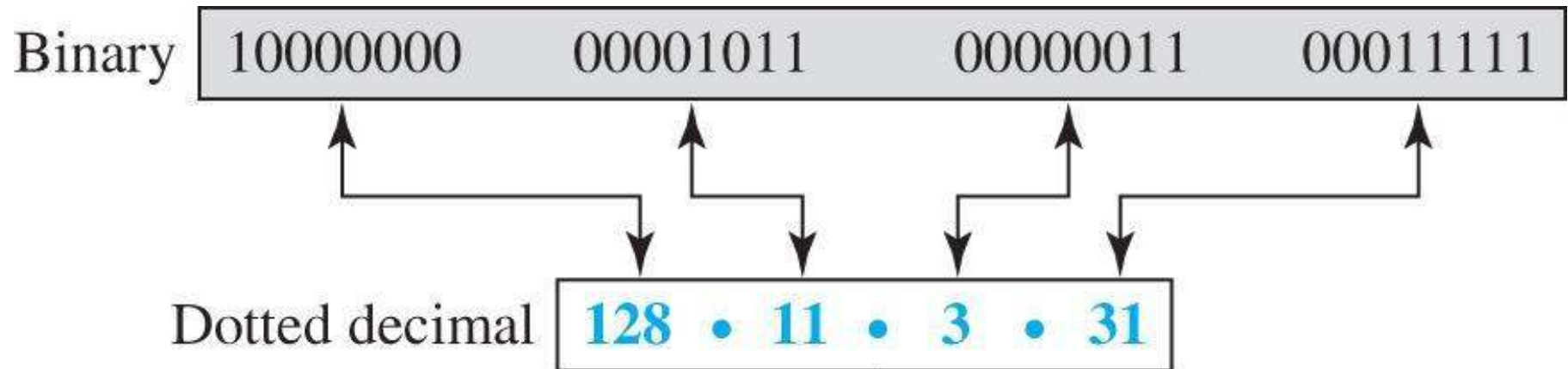
The address space of IPv4 is

2^{32}

or

4,294,967,296.

Figure 7.4 different notations in IPv4 addressing



Example 1

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

a. 10000001 00001011 00001011 11101111

b. 11111001 10011011 11111011 00001111

Solution

We replace each group of 8 bits with its equivalent decimal number (see Appendix B) and add dots for separation:

a. 129.11.11.239

b. 249.155.251.15

Example 2

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

a. 111.56.45.78

b. 75.45.34.78

Solution

We replace each decimal number with its binary equivalent (see Appendix B):

a. 01101111 00111000 00101101 01001110

b. 01001011 00101101 00100010 01001110

Example

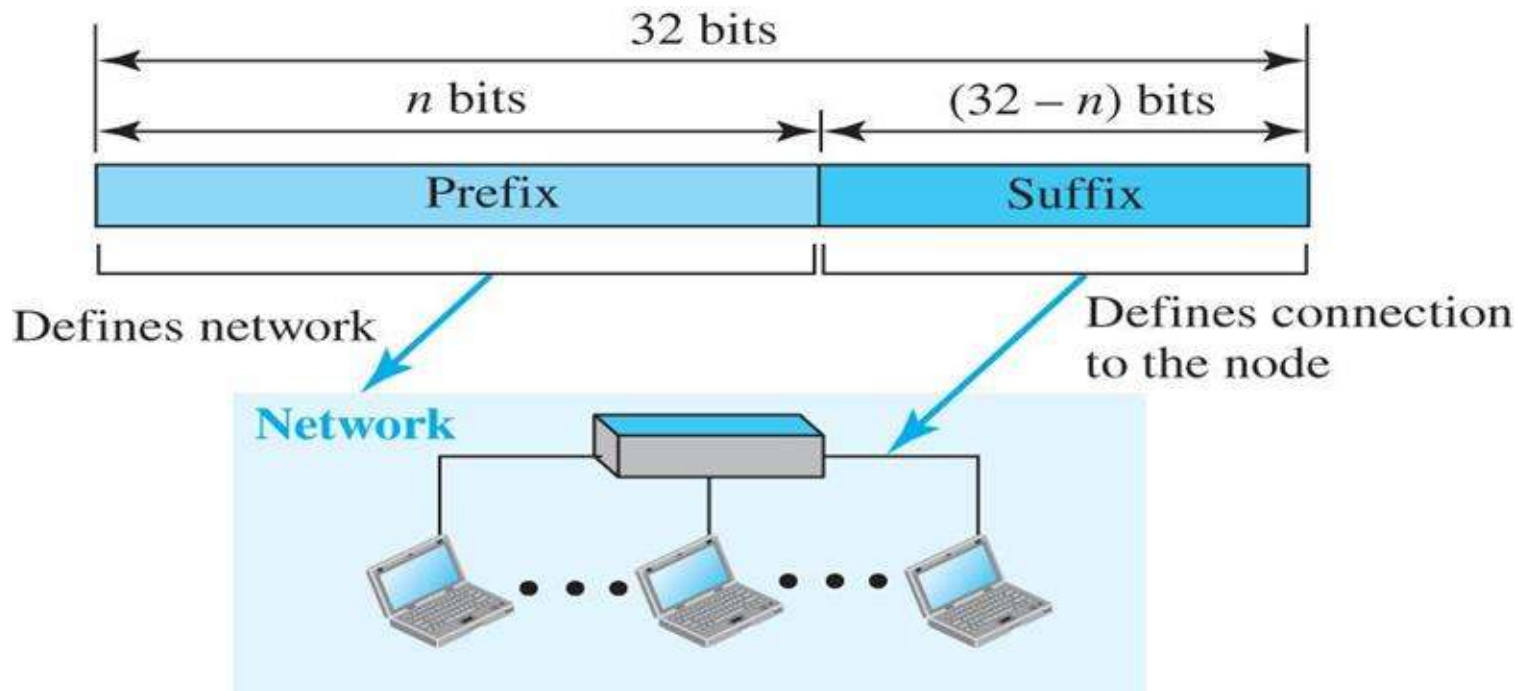
Find the error, if any, in the following IP address:

75.45.301.14

Solution

In dotted-decimal notation, each number is less than or equal to 255; 301 is outside this range.

Figure 7.5 Hierarchy in addressing



Network + Host: Complete IP address

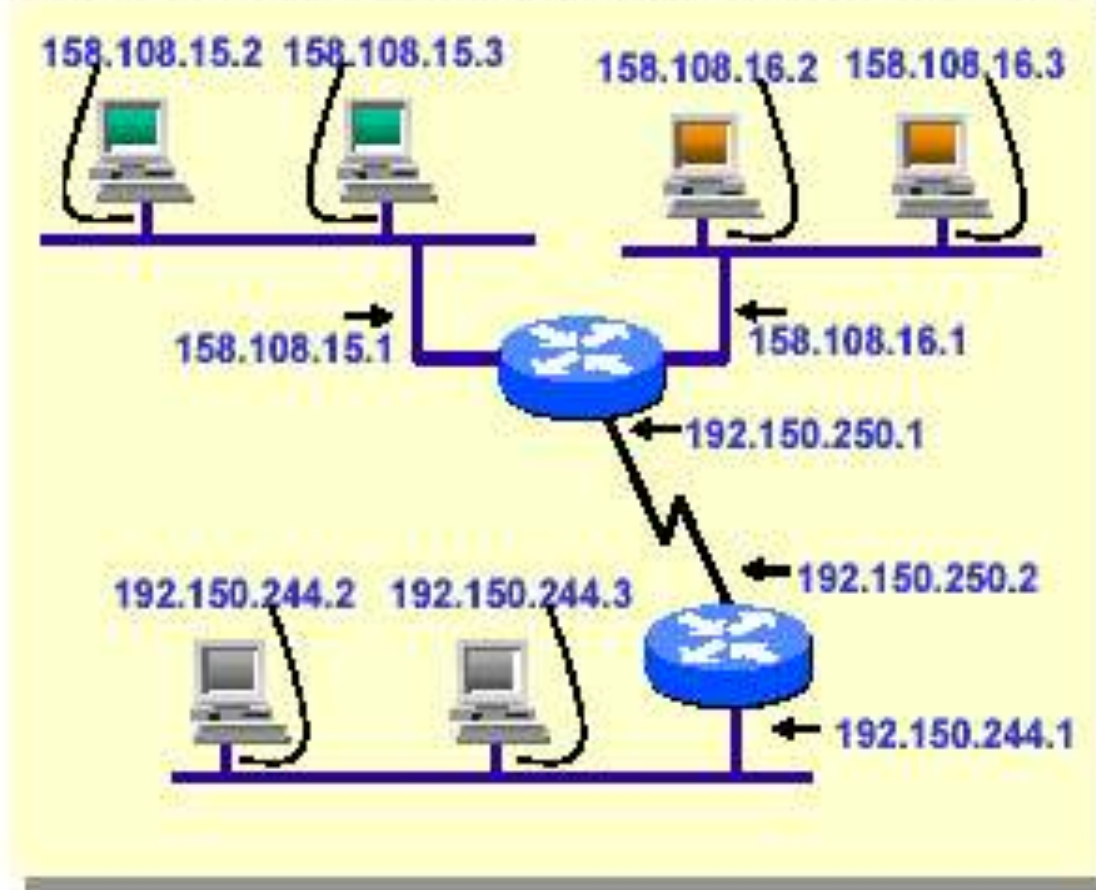
Network Address: Host part set to 0

Network (block) ID: identifies the network to which the host is connected

Host ID: identifies the interface of the network connection to the host *not the host itself*

IP Address with router

- An IP address is associated with an interface not a machine





Note:

In classful addressing, the address space is divided into five classes: A, B, C, D, and E.

Finding the classes in binary and dotted-decimal notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0-127			
Class B	128-191			
Class C	192-223			
Class D	224-239			
Class E	240-255			

Handwritten notes:
- Red arrow pointing to Class A: *memorize*
- Blue bracket over Class A and B: *network*
- Blue bracket over Class C, D, and E: *host : $8 \times 3 = 24$ are used*

b. Dotted-decimal notation

Classful Addressing

create
table
with
class, etc..

■ Class A

- Range in decimal 0 - 127
- Start with binary 0
- Address 0.x.x.x is reserved (0.0.0.0 default route)
- (127) block reserved for **loopback**
- Number of complete IP addresses in **each block** is $2^{24}=16777216 - 2$ (all zeros host - **network address**, and all ones - **broadcast address**)
- Valid Range 1.x.x.x to 126.x.x.x (126 valid blocks)
- All allocated

■ Class B

- Start with binary 10
- Range 128.x.x.x to 191.x.x.x
- $2^{14}=16384$ blocks (network addresses)
- Number of addresses in each block is $2^{16}=65536 - 2$ (all zeros host, and all ones)
- All allocated

compute address
convert
give network address → given figure
find class

Classful Addressing

- Class C
 - Start with binary 110
 - Range 192.x.x.x to 223.x.x.x ↗ Class C
 - $2^{21}=2097152$ blocks (network addresses)
 - Number of addresses in each block is $256 - 2$ (all zeros host, and all ones) class
 - Nearly all allocated
- Class D
 - Multicast addresses
 - No network/host hierarchy

Private addresses

	<i>Range</i>		<i>Total</i>
class A 10.0.0.0 network address	to	10.255.255.255 reserved for broadcast	2^{24}
class B 172.16.0.0	to	172. 31 ¹⁶ .255.255	2^{20}
class C 192.168. 15 ¹³ .0 host	to	192.168.255.255	2^{16}

Figure: Finding the address class

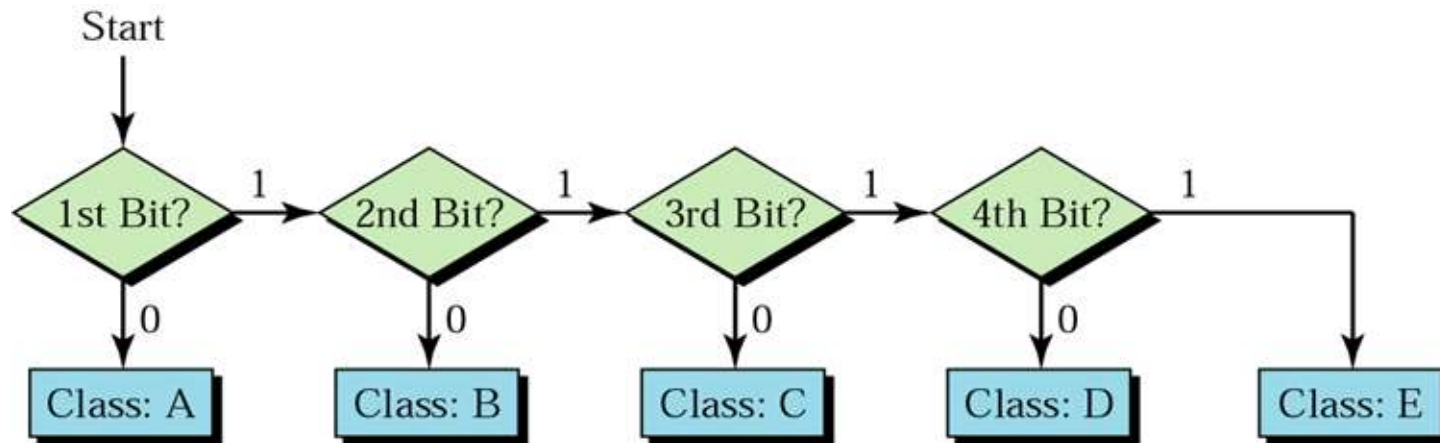


Figure 7.6 Occupation of the address space in classful addressing

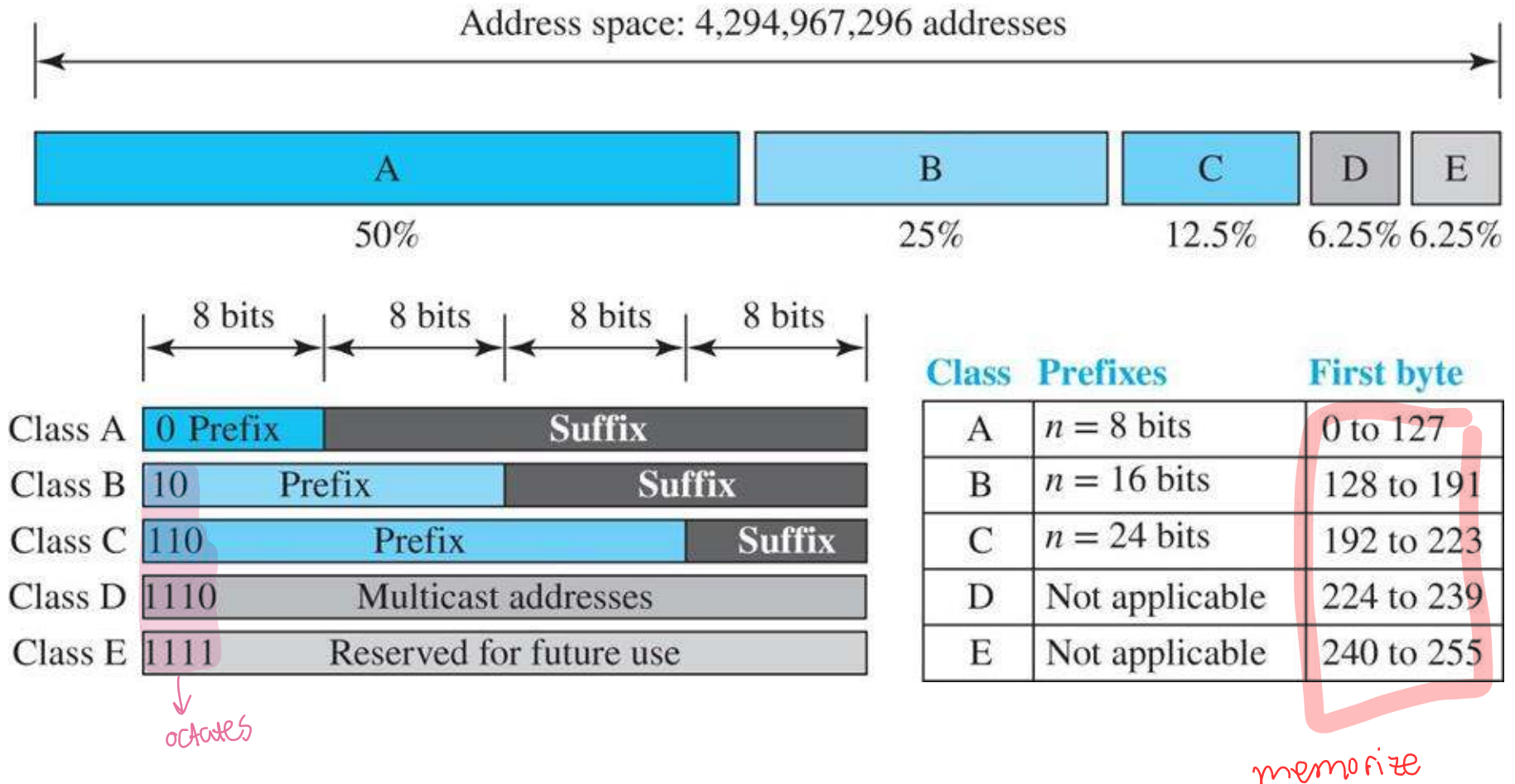
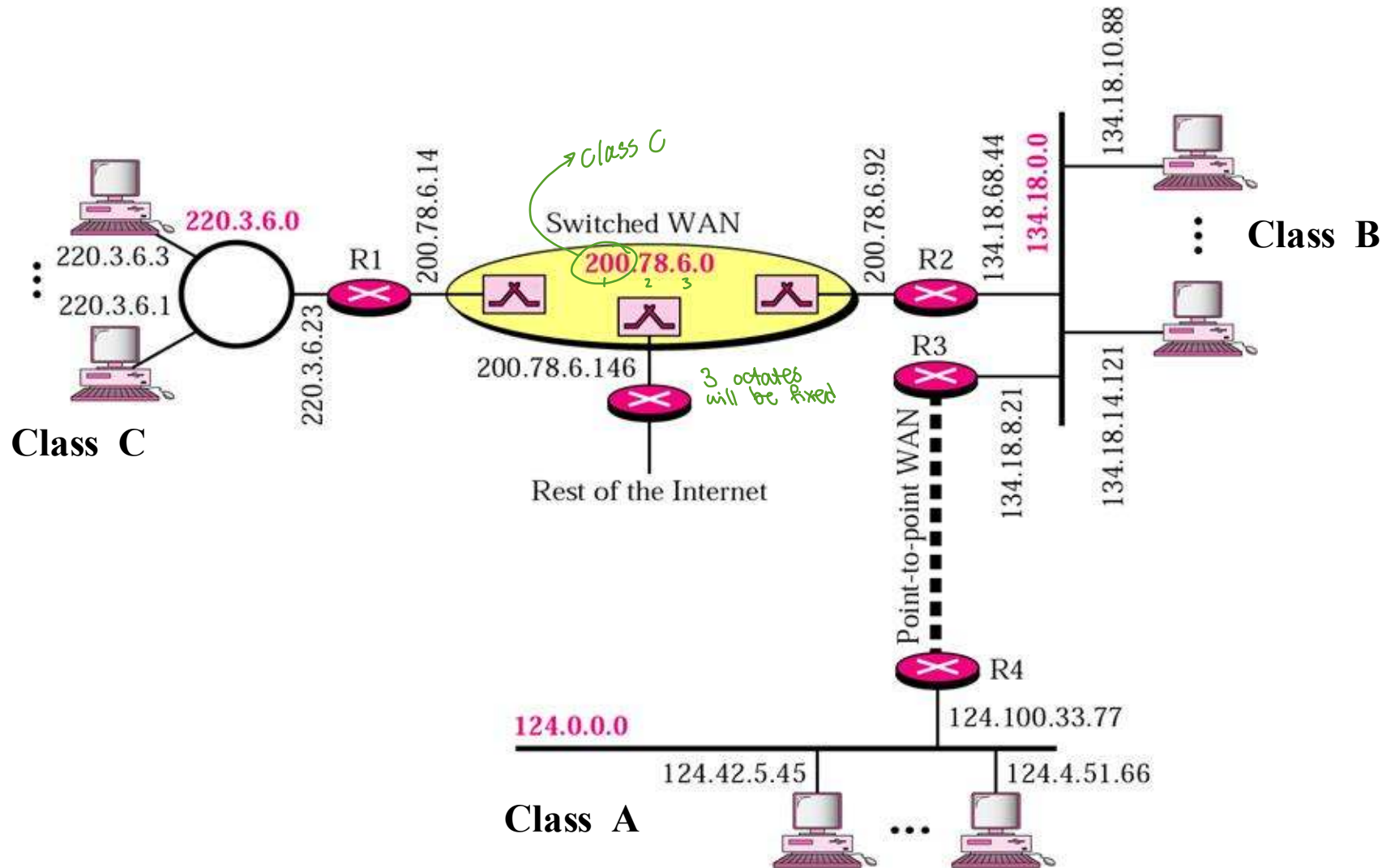


Figure : Sample internet



Broadcast in IPv4

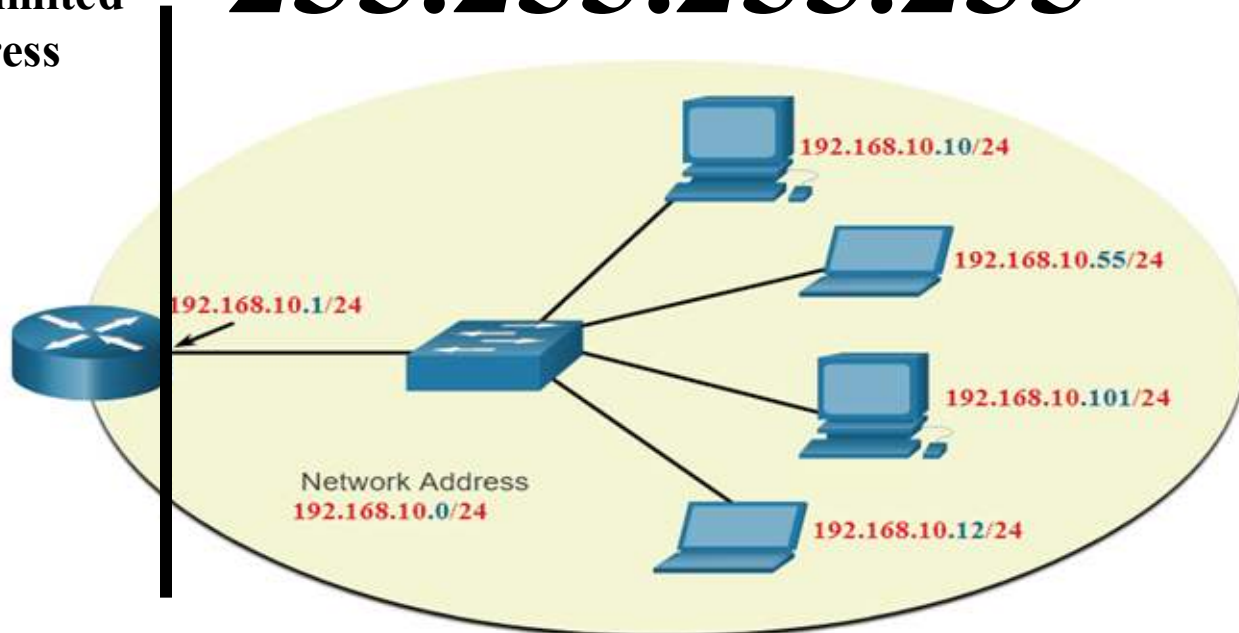
■ Limited Broadcast Address

- Broadcast address for a message to be received by all nodes within the same network as the source device
- Routers do not forward a message that has limited broadcast address as destination address (Routers isolate broadcast domains)

Denial of service

**Routers stop Limited
broadcast address**

255.255.255.255



Broadcast in IPv4

■ Directed Broadcast address

- Broadcast address for a message that is directed to ALL nodes in a specific network different from the source device network
- It has the net id and all ones in binary in the host portion

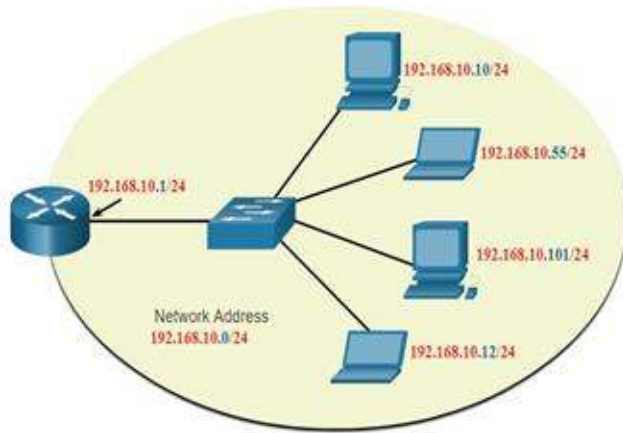
Net ID	All ones in binary
--------	--------------------

- Will be forwarded by routers
- Once reach to the addressed network, it will be converted by the receiving router to limited broadcast (255.255.255.255)
- It is usually blocked as it can be used for denial of service attacks

Network, Host, and Broadcast Addresses

Within each **network there** are **three types** of IP addresses:

- Network address
- Host addresses
- **Directed Broadcast** address



**Directed
Broadcast**

	Network Portion			Host Portion	Host Bits
Subnet mask 255.255.255.0 or /24	255	255	255	0	
	11111111	11111111	11111111	00000000	
Network address 192.168.10.0 or /24	192	168	10	0	All 0s
	11000000	10100000	00001010	00000000	
First address 192.168.10.1 or /24	192	168	10	1	All 0s and a 1
	11000000	10100000	00001010	00000001	
Last address 192.168.10.254 or /24	192	168	10	254	All 1s and a 0
	11000000	10100000	00001010	11111110	
Broadcast address 192.168.10.255 or /24	192	168	10	255	All 1s
	11000000	10100000	00001010	11111111	



Example 3

How to find class

Find the class of each address:

- a. 00000001 00001011 00001011 11101111 → decimal
- b. 11110011 10011011 11111011 00001111

Solution

See the procedure in Figure 19.11.

- a. The first bit is 0; this is a class A address.
- b. The first 4 bits are 1s; this is a class E address.

Example 4

Find the class of each address:

- a. **227.12.14.87**
- b. **252.5.15.111**
- c. **134.11.78.56**

Solution

- a. The first byte is 227 (between 224 and 239); the class is D.
- b. The first byte is 252 (between 240 and 255); the class is E.
- c. The first byte is 134 (between 128 and 191); the class is B.



Note:

In classful addressing, the network address is the one that is assigned to the organization.

Subnet Mask

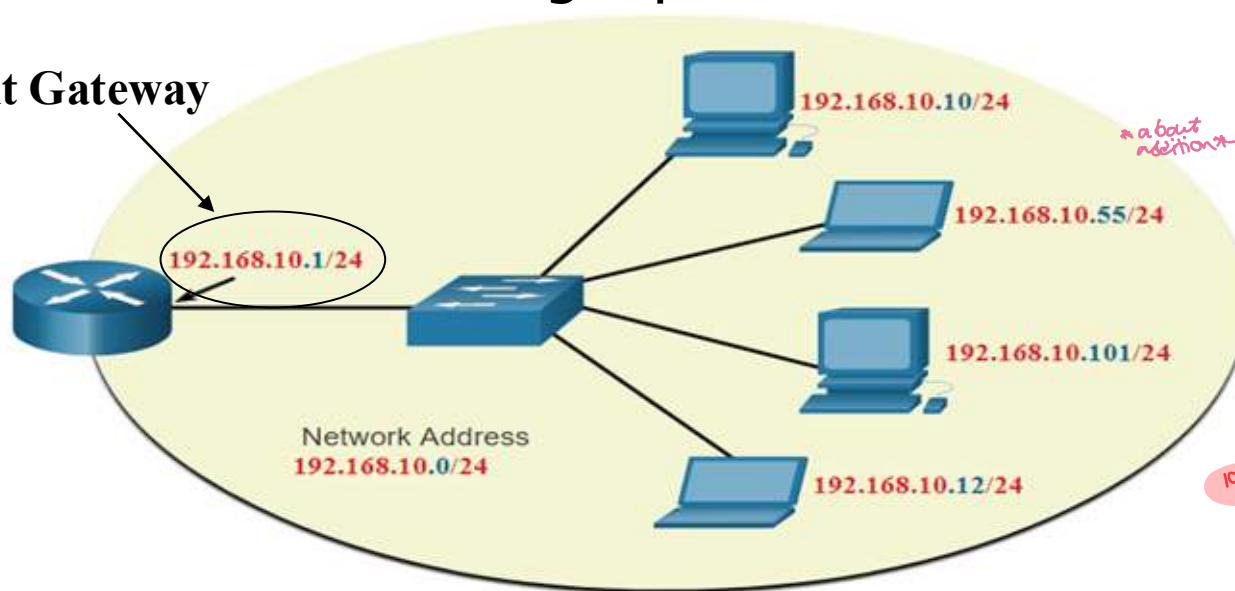
- Why we need subnet address? **See the next two slides**
- What is the difference between subnet mask and default (class) mask?
- **Class (Default) mask is used with classful addressing and subnet mask is used with classless (network address is defined by the mask not by the class)**
- What is the valid length of subnet address?
- **It should be larger than the default mask of the class of the IP address and smaller than /30.**
- How to use the subnet mask to find the subnet address?
- **Just do bitwise AND between the IP address and the subnet mask. If the mask has 255 just write the corresponding number in the IP address as is. If it the mask has 0, then write 0. Otherwise, convert both numbers in the mask and the IP to binary and do bitwise AND then convert the result to decimal.**

last before vacation

Why network address is needed?

Case 1: A device is sending a packet

Default Gateway



define source & destination address

search starts by network

if it were 1/16
192.168.0.0

pay attention to slash notation

192.168.10.1/24
8 8 8 8

about addition → 24

reserved for my network & remaining for host

Network address
192.168.10.0

if want to broadcast (send to all connected devices)

1-254
255

192.168.10.255
2⁸ 2⁸ 2⁸ 2⁸
Sum = 255

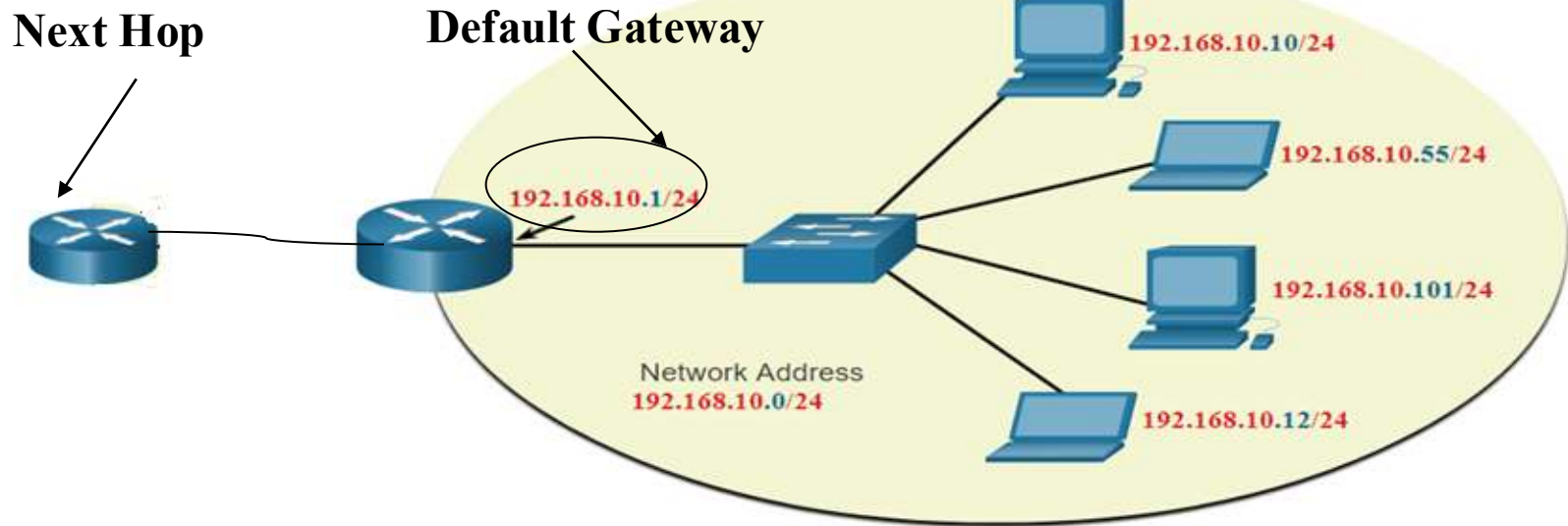
network broadcast reserved
anything between host

- For a **sending device**, network layer needs the network address for the destination to check if the destination is connected to the **same network** as the sender or to **another network**.
- If the destination is connected to **the same network**, then network layer will give the data link layer the packet to deliver it.
- If the destination is NOT connected to the same network, then network layer will ask data link layer to send it to a Router to be delivered (**The default Gateway**).

Why network address is needed?

Case 2: A router receiving a packet to be forwarded

Next lecture:
You can have
net within a net
↳ subnet



- The routing table in routers is mostly arranged by network addresses not by complete (host) addresses.
- Router needs to get the network address of the destination so that it searches for it in the routing table to determine to which next router (**next hop**) the packet should be forwarded to in order to be delivered to the destination.

Example 5

class A
8

convert to 0



Given the address 23.56.7.91, find the network address.

Solution

The class is A. Only the first byte defines the netid. We can find the network address by replacing the hostid bytes (56.7.91) with 0s. Therefore, the network address is 23.0.0.0.

Example 6

class B

Given the address 132.6.17.85, find the network address.

Solution

The class is B. The first 2 bytes defines the netid. We can find the network address by replacing the hostid bytes (17.85) with 0s. Therefore, the network address is 132.6.0.0.

Example 7

class A
↓

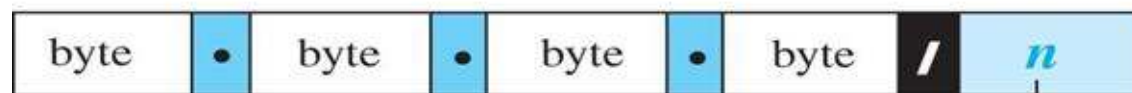
Given the network address 17.0.0.0, find the class.

Solution

The class is A because the netid is only 1 byte.

Figure 7.8 Slash notation

- Classful is NOT used nowadays.
- Currently, Classless Addressing is used where classes are NOT used any more when addresses are distributed.
- This was a solution to the huge need for more addresses and the large shortage of IPv4 addresses.
- By doing this. IPv4 are properly distributed and saved. ISPs are given a large range of addresses and then can subdivide the addresses into different subnets. (This is called subnetting)
- In classless addressing, we refer to the network mask as subnet mask and to Network address as Subnet address



Examples:

⁸12.24.76.8/⁸
⁸23.14.67.92/¹²
⁸220.8.24.255/²⁵

Use the picture rose
made

Table : Default classful masks

Class	In Binary	In Dotted-Decimal	Using Slash
A	<i>network address</i> 11111111 00000000 <i>host addresses</i> 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

- The mask has ones in for all bits that belong to the network ID and zeros for all bits that belong to the host ID.
- Slash notation represents the mask by counting the number of ones in the decimal mask after converting it to binary. For example, /16, it means the size of the network ID is 16 bits.

Converting From Slash to Decimal Notation

Subnet Mask /12				
Binary	11111111	11110000	00000000	00000000
Decimal	255	240	0	0

Subnet Mask /18				
Binary	11111111	11111111	11000000	00000000
Decimal	255	255	192	0

Subnet Mask /26				
Binary	11111111	11111111	11111111	11000000
Decimal	255	255	255	192

Subnet Mask /30				
Binary	11111111	11111111	11111111	11111100
Decimal	255	255	255	252

Binary to Decimal Conversion

Binary	Decimal
10000000	128
11000000	192
11100000	224
11110000	240
11111000	248
11111100	252
11111110	254
11111111	255

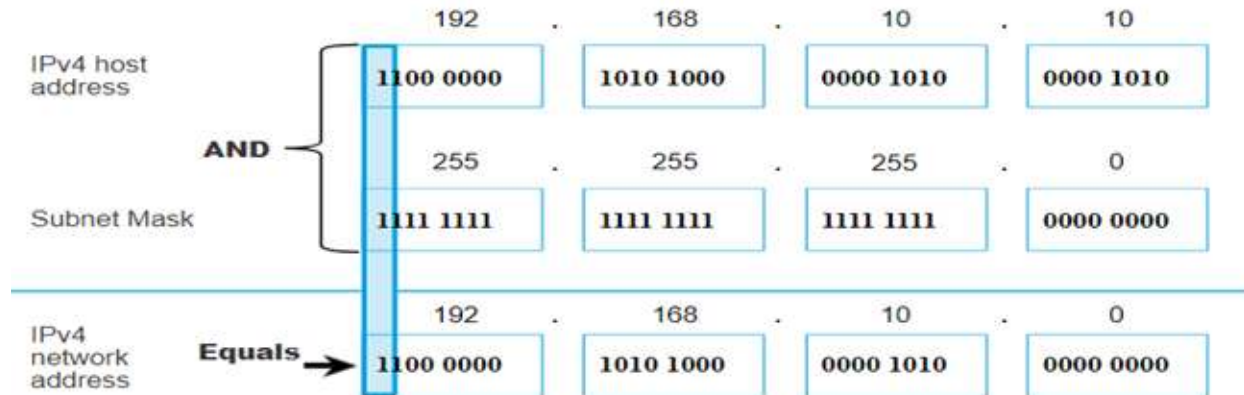
Determining the Subnet Address: Logical AND with Mask

A logical AND Boolean operation is used in determining the subnet address.

1 AND 1 = 1, 0 AND 1 = 0, 1 AND 0 = 0, 0 AND 0 = 0

To identify the subnet address, the host IPv4 address is logically ANDed, bit by bit, with the subnet mask to identify the subnet address.

Mask used to find subnet/network address



What is the subnet address of the following IP address

172.16.200.100 /19.

IP address	172								.	16								.	200								.	100							
Binary	1	0	1	0	1	1	0	0	.	0	0	0	1	0	0	0	0	.	1	1	0	0	1	0	0	0	.	0	1	1	0	0	1	0	0
Subnet Mask	255								.	255								.	224								.	0							
Binary	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	0	0	0	0	0	.	0	0	0	0	0	0	0	0
IP AND MASK	1	0	1	0	1	1	0	0	.	0	0	0	1	0	0	0	0	.	1	1	0	0	0	0	0	0	.	0	0	0	0	0	0	0	0
Subnet Address	172								.	16								.	192								.	0							
Decimal									.									.									.								

What is the subnet address of the following IP address

193.1.2.129 /26.

IP address	193								.	1								.	2								.	129							
Binary	1	1	0	0	0	0	0	1	.	0	0	0	0	0	0	0	1	.	0	0	0	0	0	0	1	0	.	1	0	0	0	0	0	0	1
Subnet Mask	255								.	255								.	255								.	192							
Binary	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	1	1	1	1	1	1	.	1	1	0	0	0	0	0	0
IP AND MASK	1	1	0	0	0	0	0	1	.	0	0	0	0	0	0	0	1	.	0	0	0	0	0	0	1	0	.	1	0	0	0	0	0	0	0
Subnet Address	193								.	1								.	2								.	128							
Decimal									.									.									.								

192.168.10.45/28
255.255.255.240

AND operation

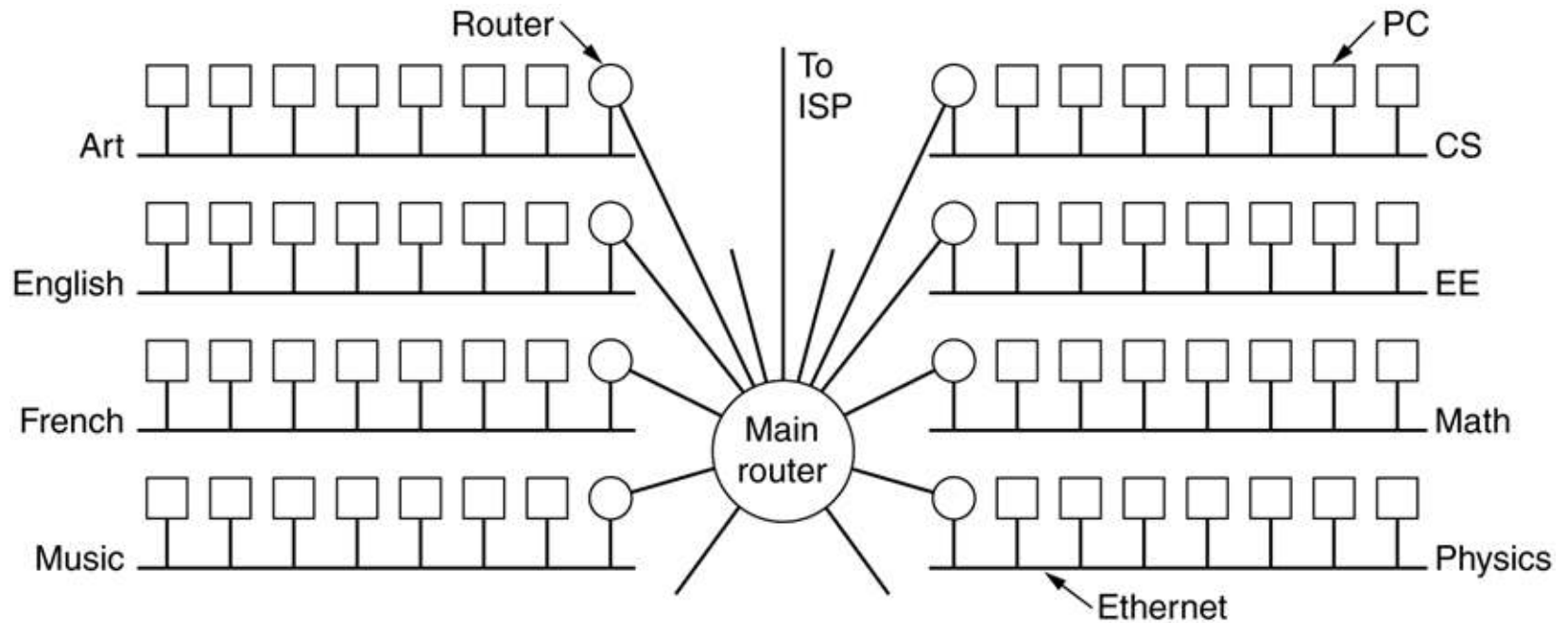
11000000 10010000 00001010 00100000

↓ binary

192.168.10.32

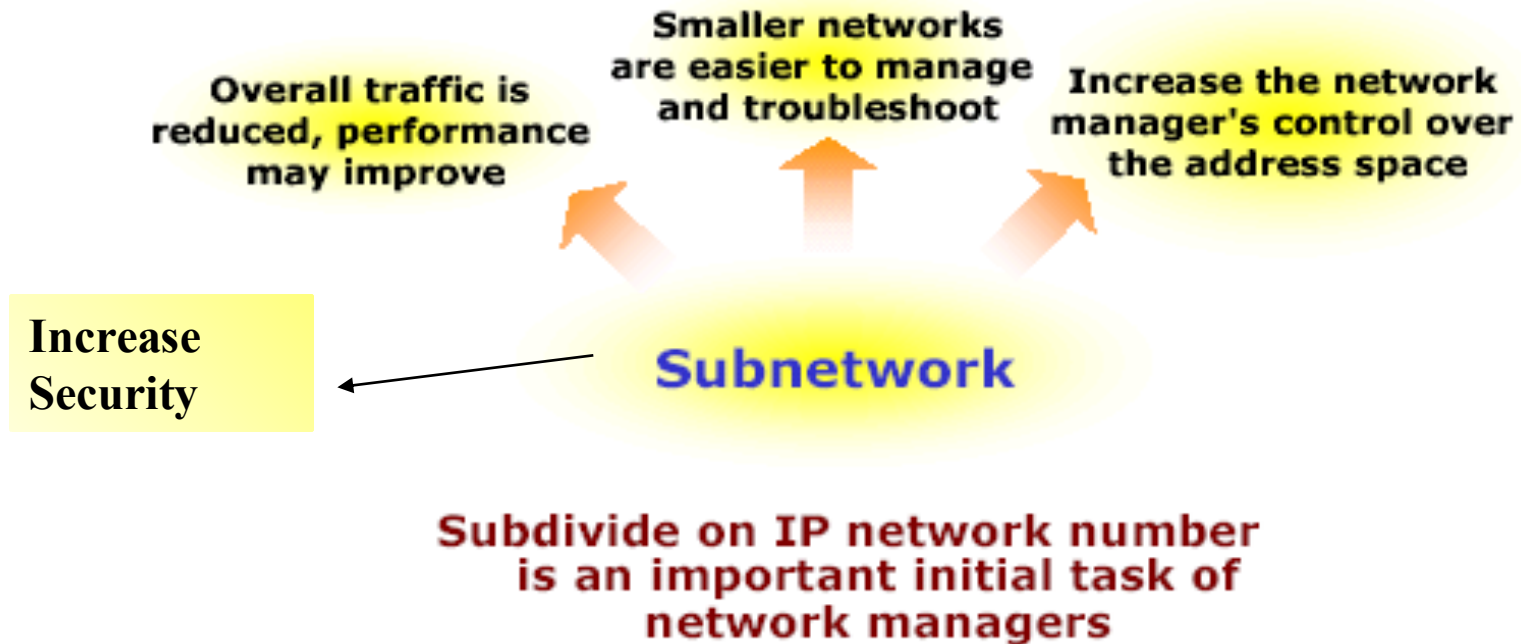
172.25.210.3/22

Subnetting



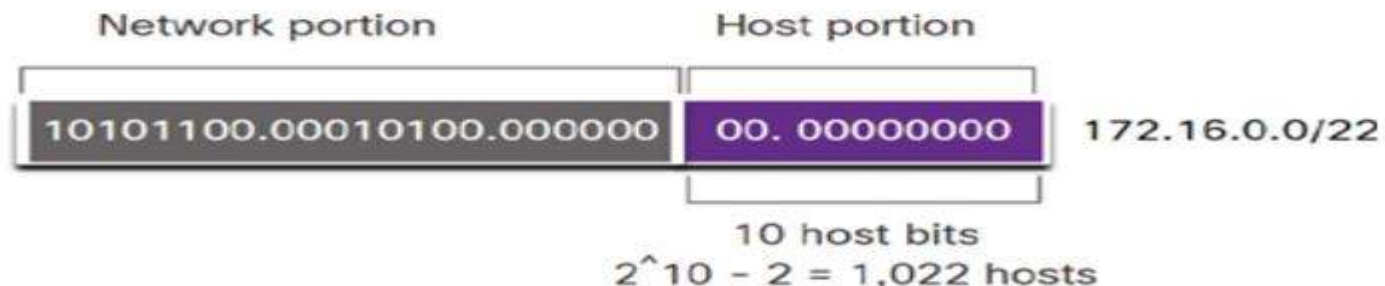
A campus network consisting of LANs for various departments.

Subnetwork benefits



Subnetting

- Dividing the network into several smaller groups called (**subnets**) with each group having its own **subnet IP address**
- Site looks to rest of internet like **single network** and routers outside the organization route the packet based on the main Network address
- Local routers route within subnetted network using subnet address
- **Host portion** of address partitioned into **subnet number** (most significant part) and **host number** (least significant part)
- In this case, IP address will have **3 levels** (Main network, subnet, host)
- **Subnet mask** is a 32-bit consists of zeros and ones that indicates which bits of the IP address are subnet number and which are host number
- Subnet mask when **ANDed** with the IP address it gives the subnetwork address



Subnetting steps

- Given the desired number of subnets and the original classfull network address
 1. Subtract 1 from number of needed subnets ✓
 2. Convert the result of step 1 to binary ✓
 3. Count number of bits obtained in 2 ✓
 4. To obtain the subnet mask, Add the result in 3 to the default mask for the original network. ✓
 5. To write the different subnets:
 1. Write the weight $2^{\text{position number}}$ of the first non-zero bit in the subnet mask starting from the rightmost octet ✓
 2. The first subnet is the original network address with the subnet mask
 3. The next subnet is the original network address after adding the weight, obtained in (2), to the value of the first non-zero octet in original network address from the right
 4. Keep adding the weight to the last obtained subnet to obtain the next subnet address
 5. Stop when the result exceeds 255

limit for no devices
ip address can hold

Class question

Subnetting Scenario

Org classful network address: 192.168.1.0 (class C)

mask $\rightarrow$ class C
255.255.255.0
8 bits 8 bits 8 bits (all ones)
00000000 111 00000
 $2^7 + 2^6 + 2^5 = 224$
 $2^5 = 32$ options

mask becomes 255.255.255.224

No subnets = $2^{\text{subnet mask length} - \text{classful mask length}}$

from step 3 to 2

Most / subnets = $2^{32 - \text{subnet mask length} - 2}$

gives immediately

Solving

Find the subnet addresses for IP address 200.175.0.0, class B, 20 subnets

mask $\rightarrow$ class B
255.255.0.0
8 8

- ① $20 - 1 = 19$
- ② $19 \rightarrow$ 10011000
 $2^7 + 2^3 + 2^4 = 152$
- ③ $2^7 + 2^3 + 2^4 = 152$
- ④ 255.255.152.152
- ⑤ $2^4 = 16$
- ⑥

192.168.1.0 /24

Subnetted to 8 subnets – 5 subnets are used and 3 for future expansion

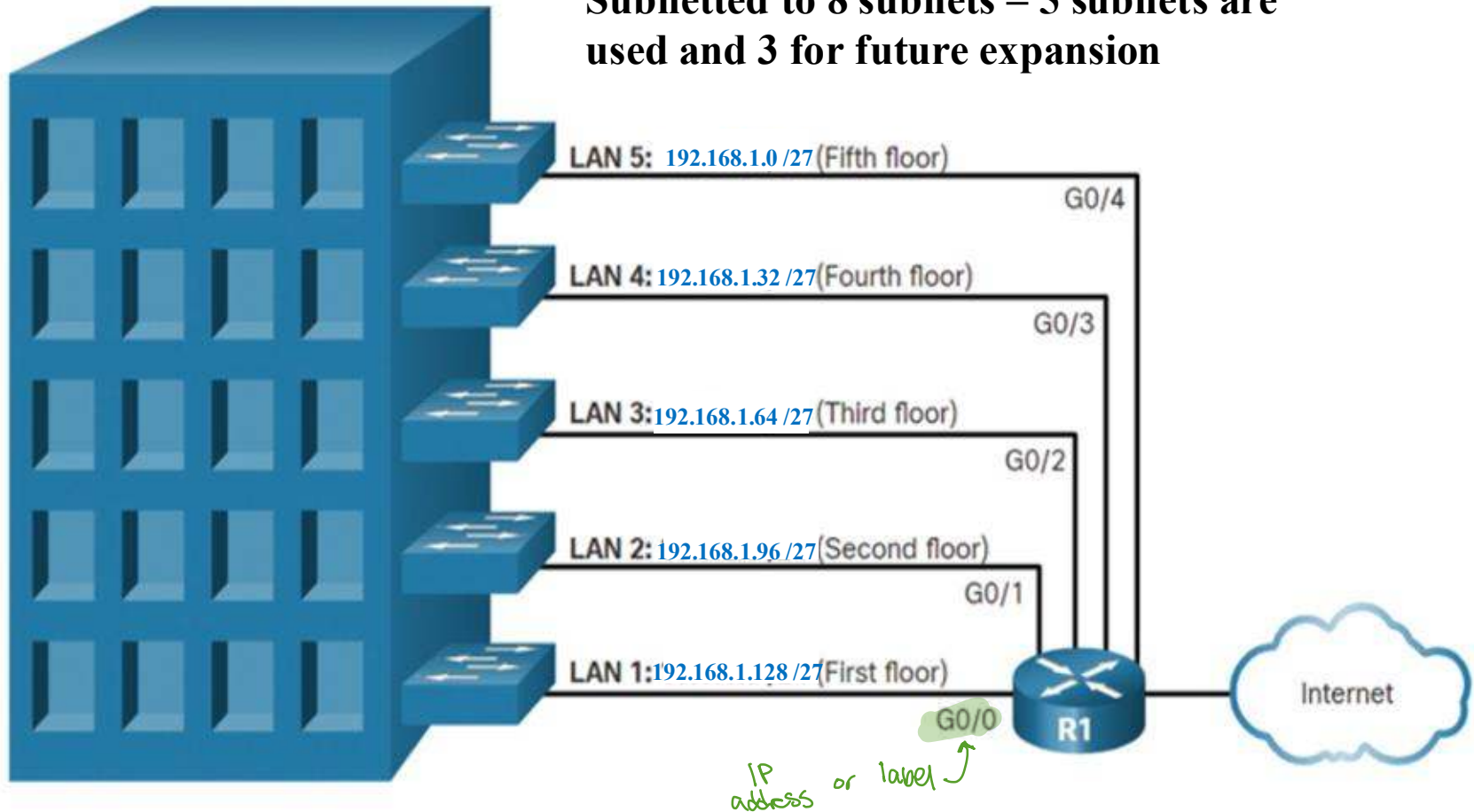
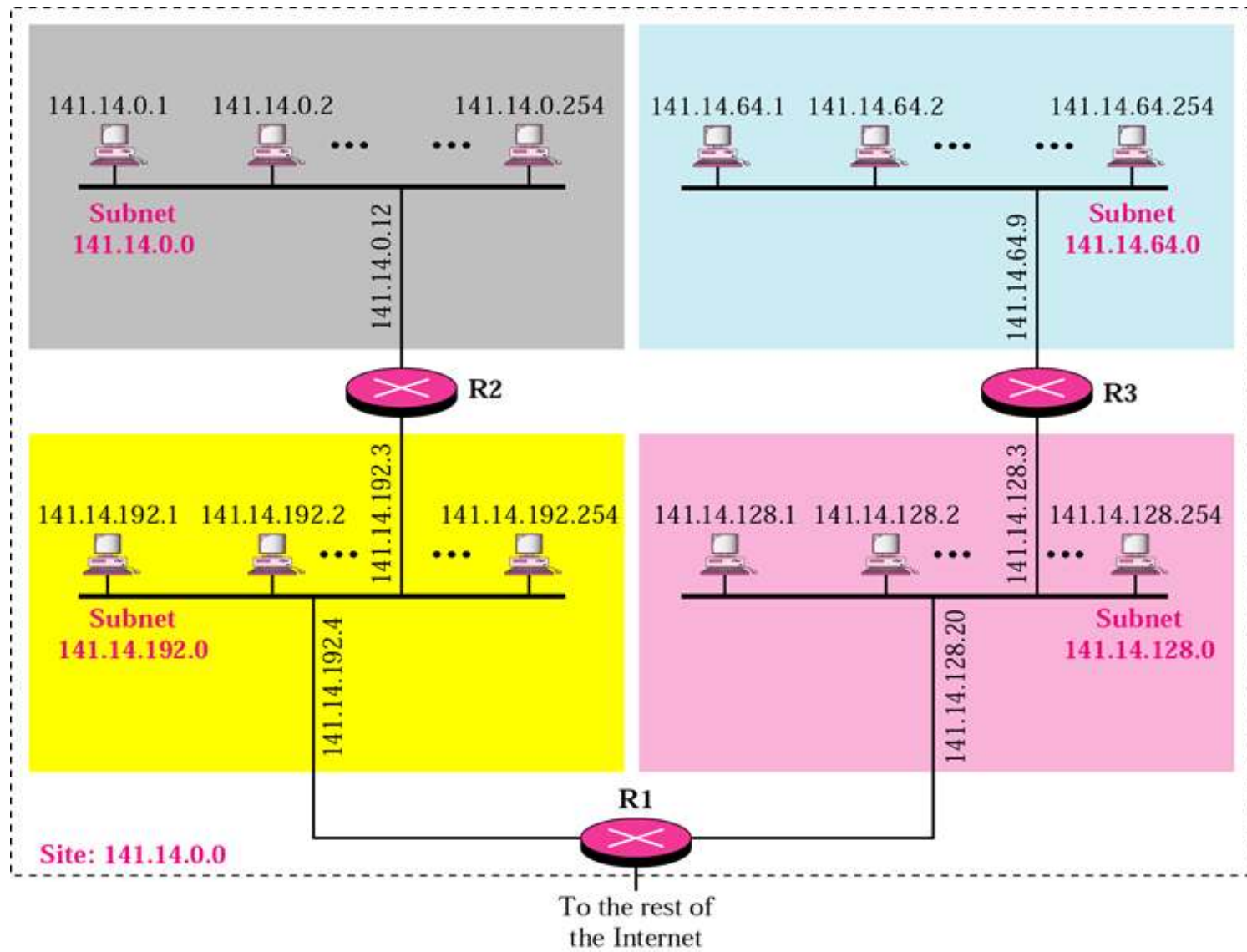


Figure: A network with three levels of hierarchy (subnetted)



**Routers will use subnet mask 255.255.192.0
or /18**

Determining number of subnets and number of hosts per subnet

- Given the classful and the subnet mask
- Number of subnets produced by this subnet mask is

$$2^{(\text{subnet mask length} - \text{classful mask length})}$$

- Number of hosts per subnet is

$$2^{(32 - \text{subnet mask length})} - 2$$

Note: 2 is subtracted from number of hosts because the first address in the block is the network address and the last address is the broadcast. These two addresses can't be assigned to a host.

Obtaining Host IP Address

- Once a network administrator in an organization obtained a block of addresses from its ISP, it can then assign individual IP addresses to the host and router interfaces
- The follow four IP configurations should be done on any host connected to the network:
 - IP Address from the correct subnet
 - Subnet Mask
 - Default Gateway IP address (Default gateway is a router interface that is connected to the same subnet as the other end devices)
 - Domain name Server IP address
- The above IP configurations can be assigned to interfaces in two ways:
 - **Manual configuration:** IP address is stored manually by the administrator in a configuration file
 - What about a **diskless** computer? Or **first time booted** computer with a disk?
 - What about if the computer **has moved from one subnet to another**?
 - Solution is using a protocol called **Dynamic Host Configuration Protocol (DHCP)**

Dynamic Host Configuration Protocol (DHCP)

■ Dynamic Host Configuration Protocol (DHCP)

changing rapidly

- Application layer protocol that provide **IP address, subnet mask, IP address of a gateway router, and IP address of DNS server** *dynamically* to a host or to a diskless computer
- DHCP server keeps **two databases** (static IP addresses and dynamic IP database which has unused temporary Addresses (IP address Pool).)
- **Static IP addresses database** maps **physical addresses (MAC)** to **permanent IP addresses (used for diskless workstations)**
- When a host **requests** an address DHCP will **look into the static database** first.
- If no address match is found, DHCP will **select the dynamic IP database**. DHCP will assign a **Temporary Address**: selected address from a **pool of free** addresses and assign it to the host
- **Leasing**: DHCP server assigns an IP address for a host for a specific **period of time** in order not to waste IP addresses
 - After the period **expires**, host must **return** the IP address or **renew** the lease.

renting it

ARP

Anytime a node has an IP packet to send to another node in a link, it has the IP address of the receiving node.

must know the jumps between layers

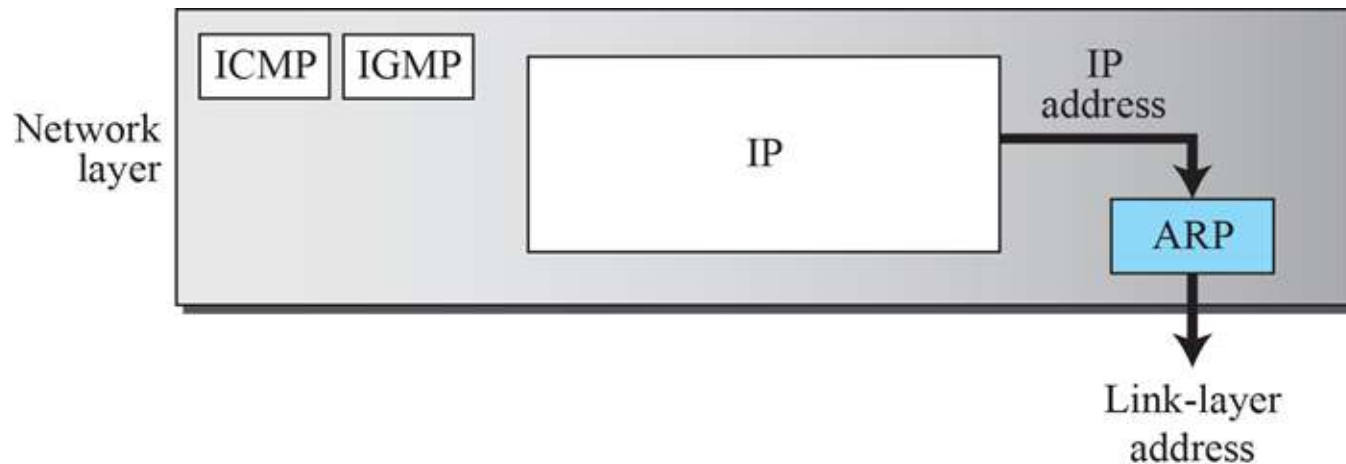
However, the IP address of the next node is not helpful in moving **a frame** through a link; we need the link-layer address of the next node.

This is the time when the **Address Resolution Protocol** (ARP) becomes helpful.

Address Resolution Protocol (ARP)

- ARP is a network layer protocol that translates between **Internet IP address** and **MAC sublayer (layer-2) address**

links both MAC & IP address



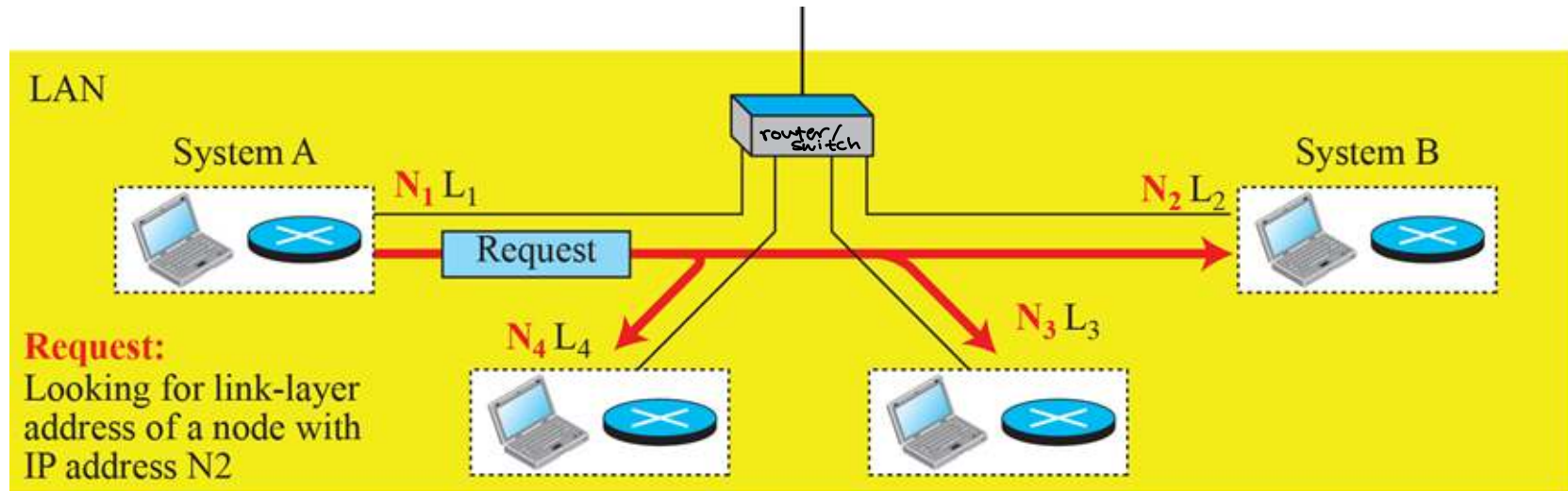
understand
slide after

Note

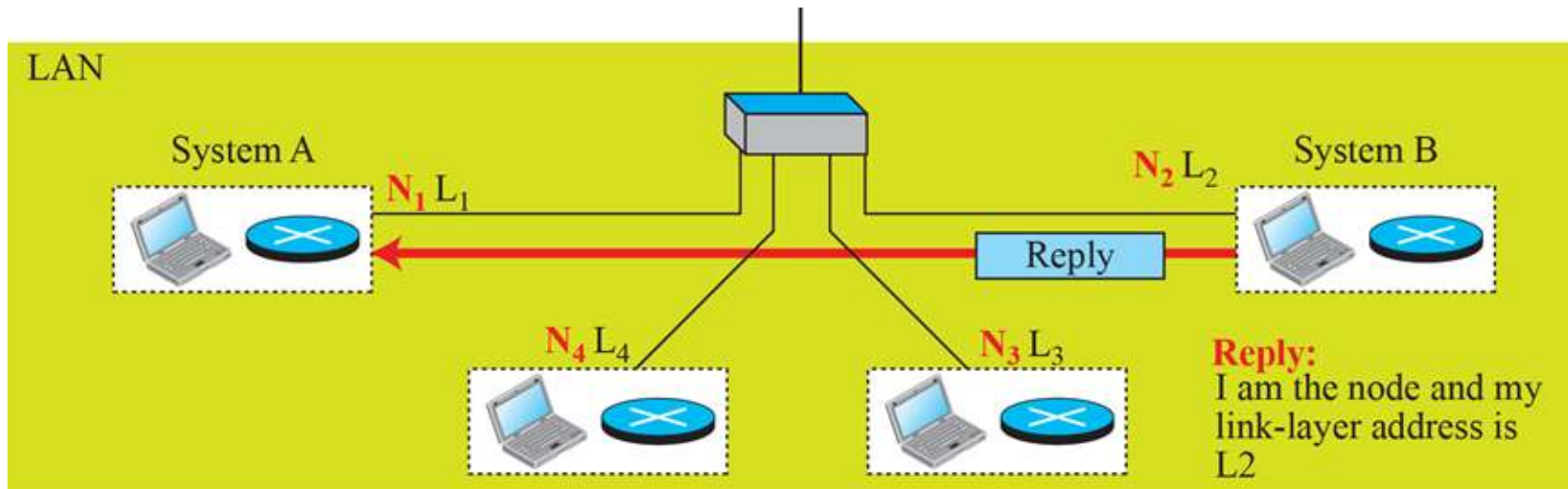
**An ARP request is broadcast;
an ARP reply is unicast.**

then come
back

Figure : ARP operation



a. ARP request is broadcast



b. ARP reply is unicast

Encapsulation of ARP packet

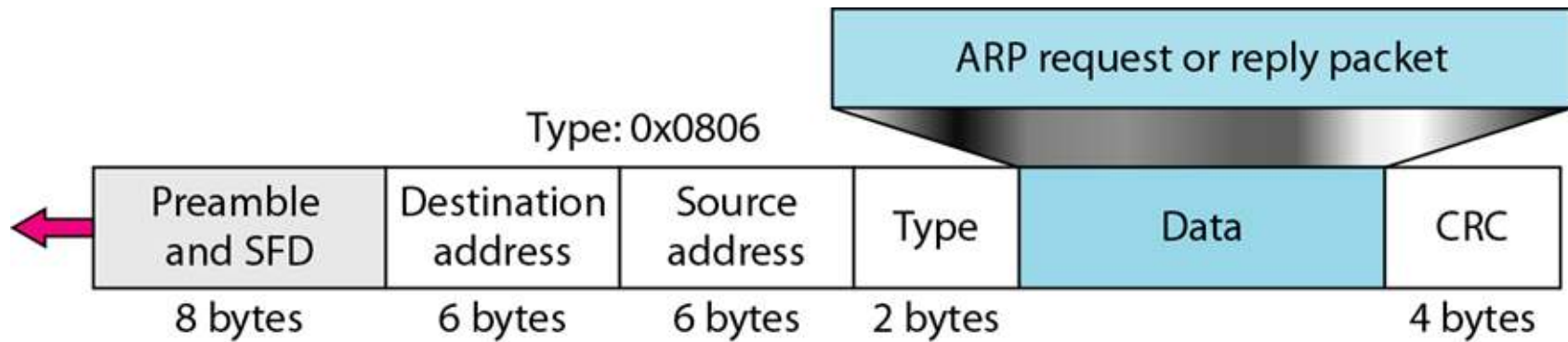
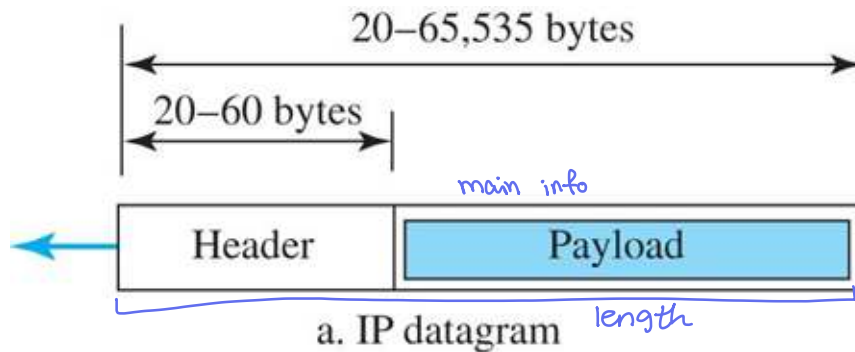


Figure 7.13 IP datagram

look at next then come back

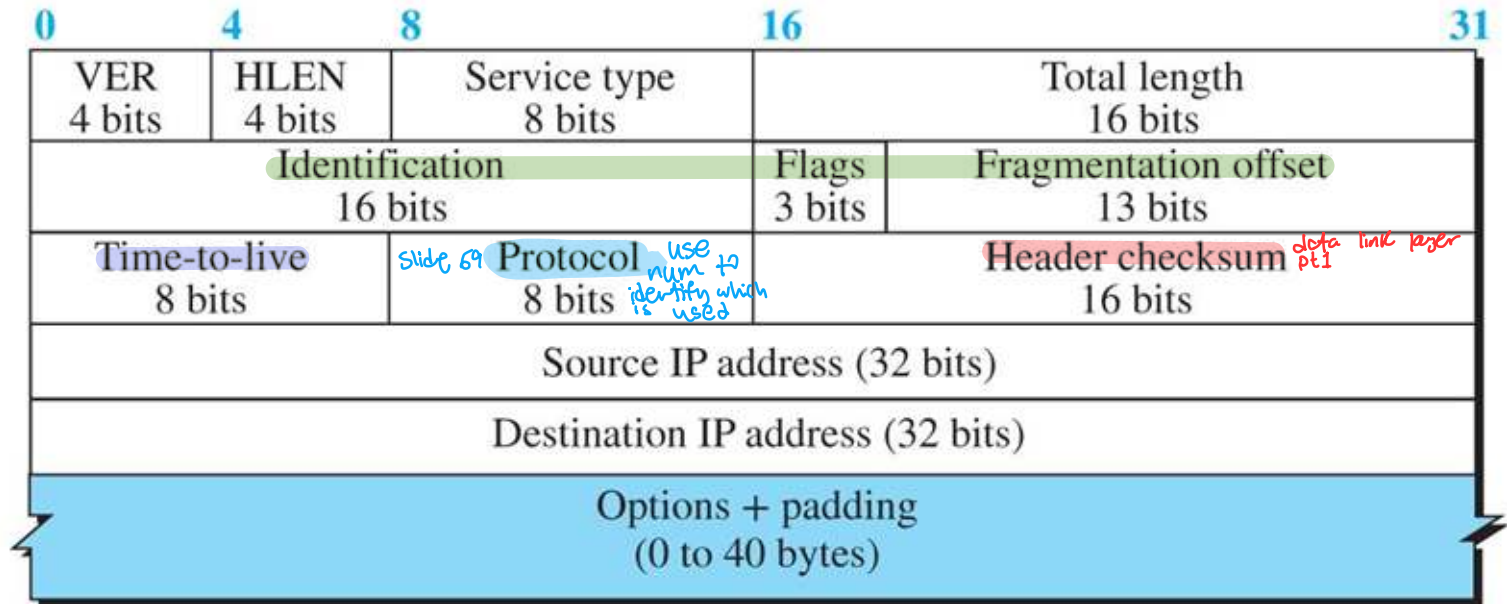


Legend

VER: version number
HLEN: header length
byte: 8 bits

Flags

	D	M
--	---	---



b. Header format

- Access the text alternative for slide images.

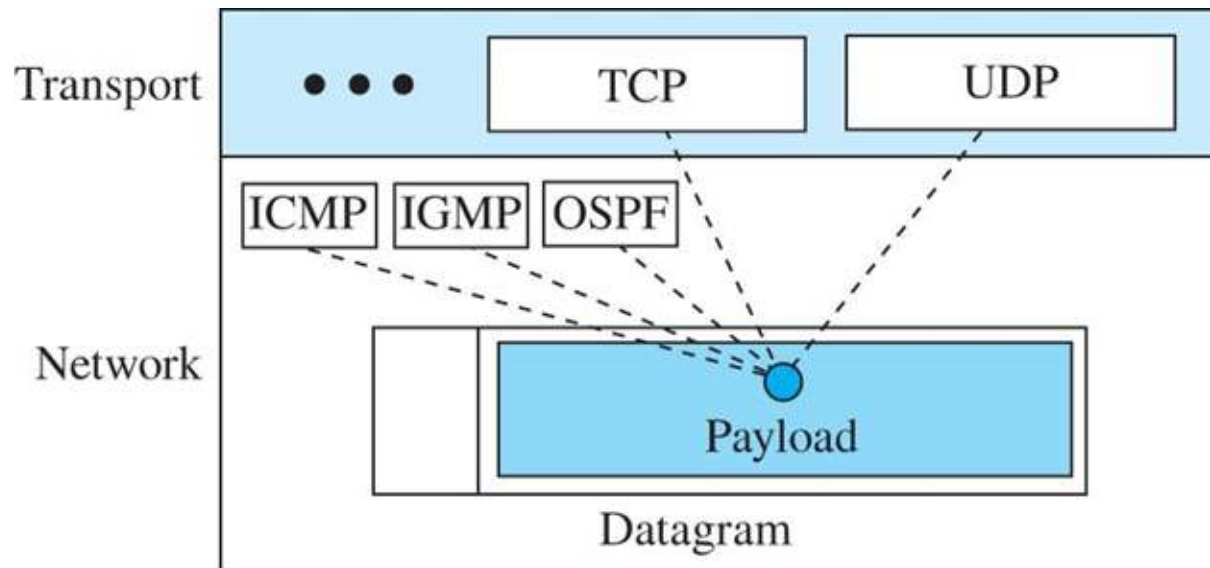
IPv4 datagram fields

- Minimum Header length is 20 bytes without options.
- Total length: total length of the packet: header + data. The Maximum = 65535 bytes
- Identification, flags, and offset used for **fragmentation and reassembly at the destination**.
- Packet can be **fragmented at any node between the source and the destination** but reassembly is done **ONLY at the destination** node.
- **Time to Live (TTL)** is used to prevent lost packets from circulating between routers forever (loops). This field is set to certain value depending on the device operating system. Each router will **decrement this field by one** and **check the value**. If the value is zero the packet will be **dropped**.
don't occupy if not used
- **Protocol**: contains a code for what is being carried in the data field. At the destination the network layer will use the Protocol field to deliver the data to the right destination (TCP or UDP or Routing protocols)
if message lost, destroyed
- **Header checksum** used for checking if there is error in the header only. The checksum is recomputed at each router between the source and the destination.

Figure 7.14 The value of the protocol field

- Protocol field determines to which of the Transport layer and Network layer protocols) the data in the network packet should be delivered to.
- Each protocol is given a value as shown below in the table.
- The source will insert the corresponding value in the protocol field
- The destination network layer will use the value to deliver the data to the right protocol

going up/down or in/out?



id for protocol
Some protocol values

ICMP	01
IGMP	02
TCP	06
UDP	17
OSPF	89

Fragmentation

divide data into smaller units
decapsulating data

- A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel. For example, if a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

MTUs for some networks

<i>Protocol</i>	<i>MTU</i>
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

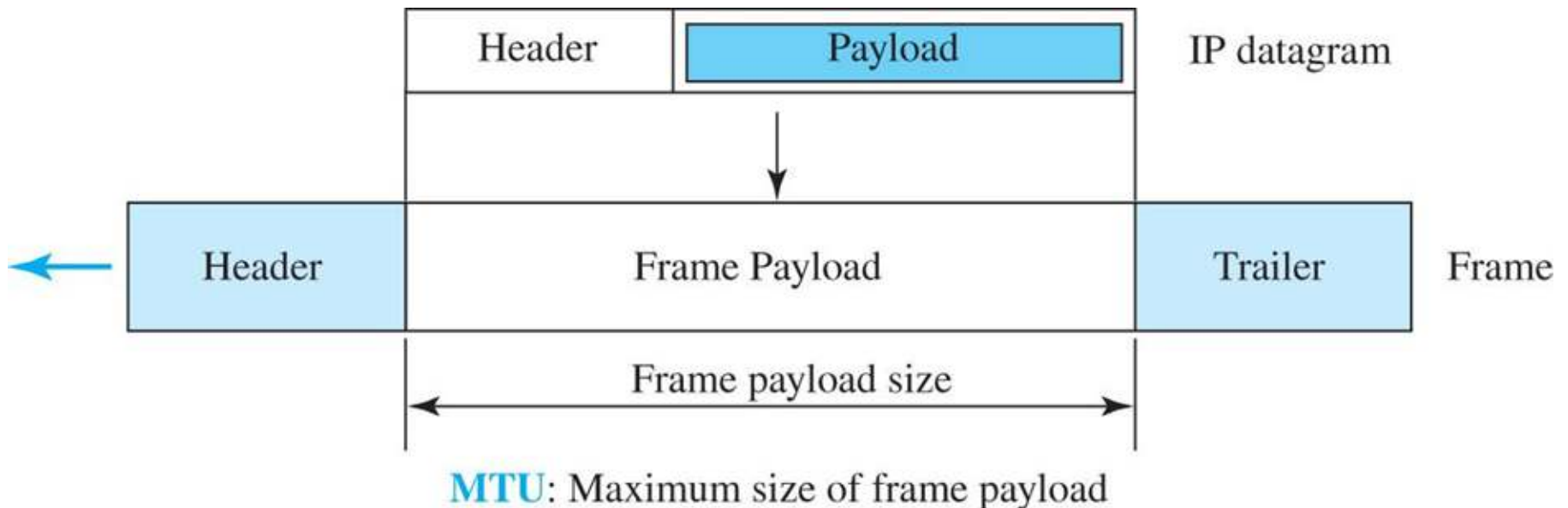
definition

Maximum Transfer Unit

Mostest thing to send between slides



- Each link-layer protocol has its own frame format.
- One of the features of each format is the maximum transfer size (MTU) which puts a limit on the maximum data size that can be encapsulated in a frame
- The network layer packet size must be less than the maximum size

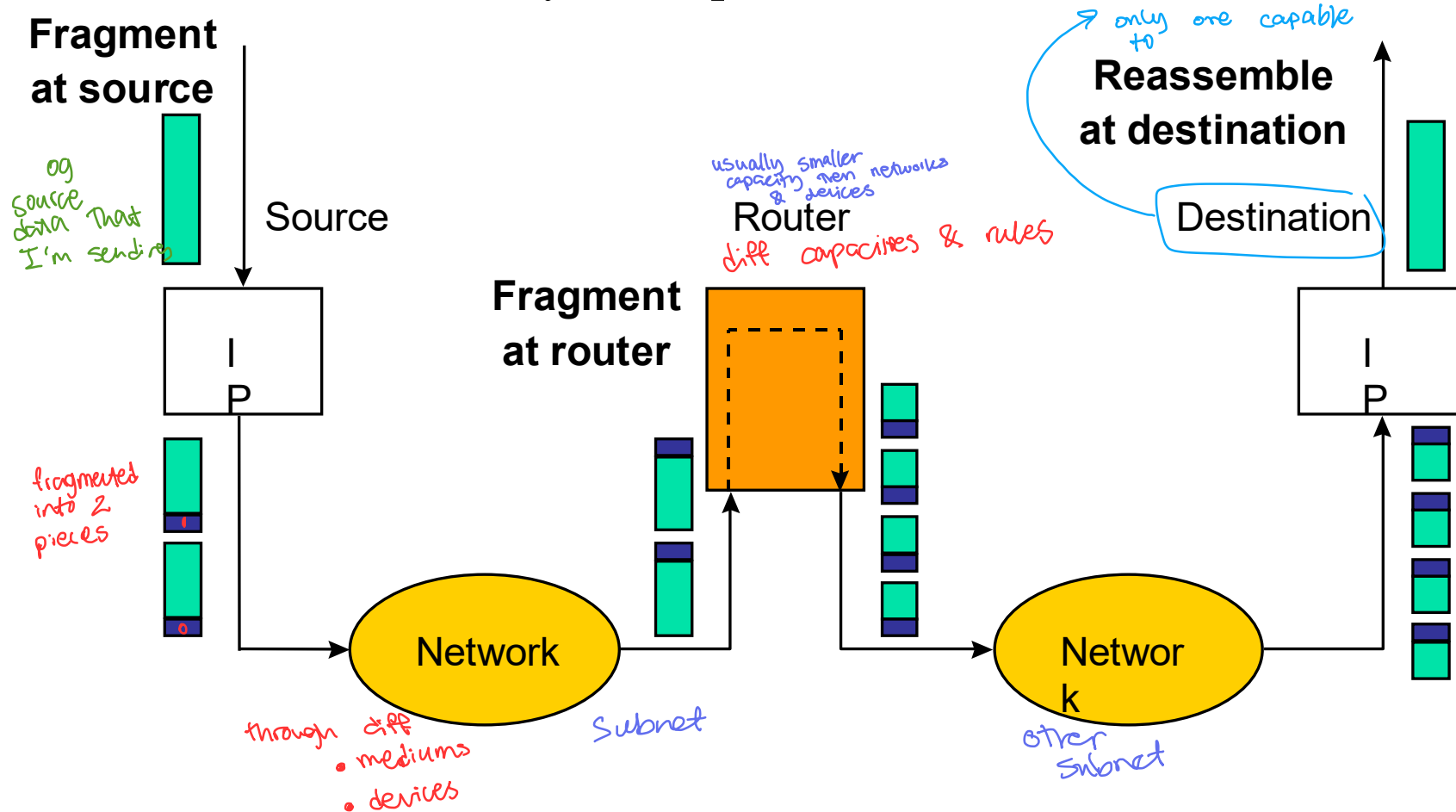


Fragmentation

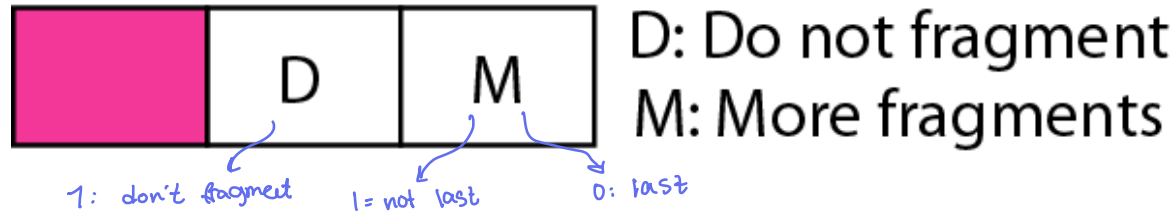
A datagram can travel through different networks. Each router decapsulates the IP datagram from the frame it receives, processes it, and then encapsulates it in another frame. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel. For example, if a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

Fragmentation and Reassembly

- Fragmentation takes place at the sender and routers
- Reassembly takes place at the receiver **ONLY**.



Flags used in fragmentation

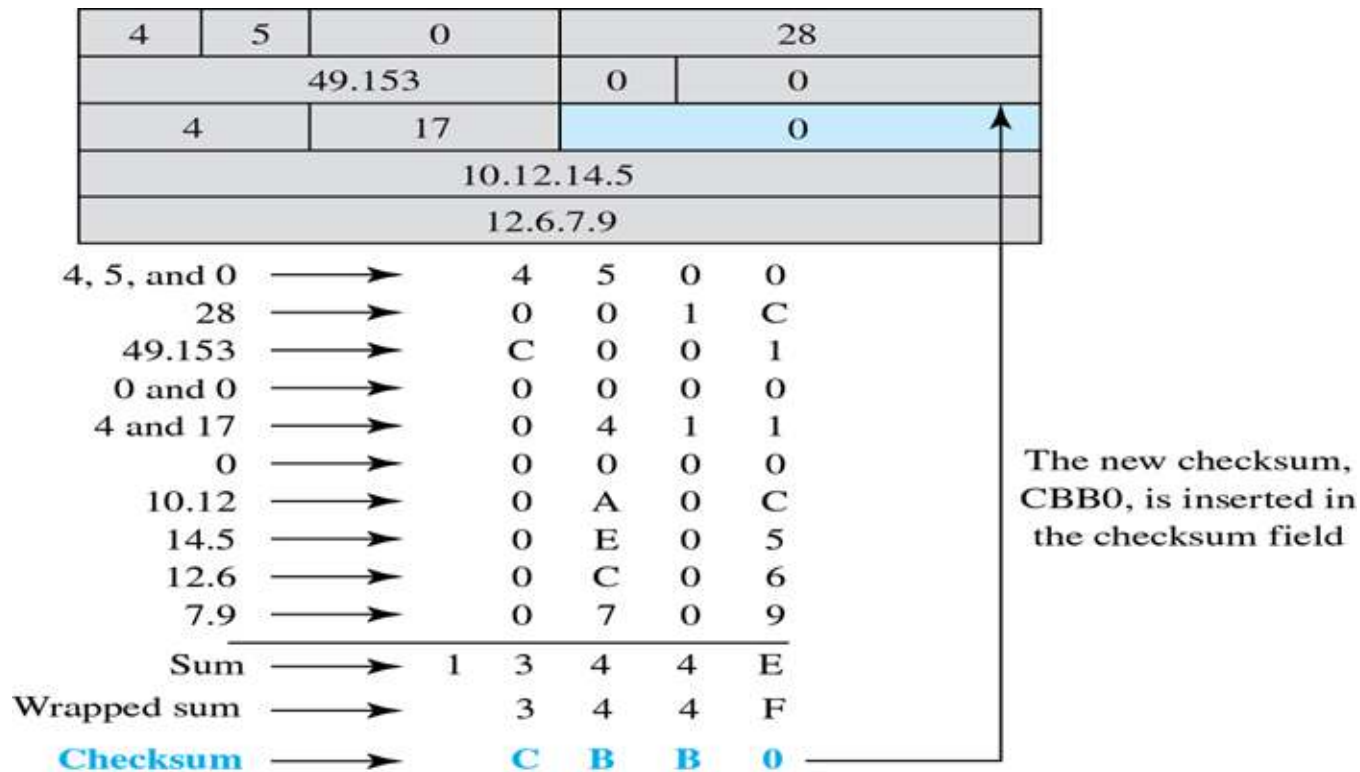


act as true and false {
M=1 means the packet is **not the last fragment**
M=0 means the packet is **the last fragment**
D=1 means **Do not fragment** the packet
deal with it as is or drop it

If the packet arrives to a router with Do not fragment flag equals '1' and the router has to forward the packet but its size is larger than the link MTU, the router will drop the packet

Figure 7.15 Example of checksum calculation

- Header checksum used for checking if there is error in **the header only**.
- If it detects error, the packet will be dropped.
- The checksum is recomputed at each router between the source and the destination because there are fields in the header that must be updated every time the packet arrives to intermediate node such as (TTL value)



Network Address Translation (NAT)

- NAT: is A technology that can provide the mapping between the private (local) and Public (global) IP addresses
- NAT: The technology allows a site to use a set of **private addresses** for internal communication and a set of **global (Public) Internet** addresses (at least one) for communication with the rest of the world.

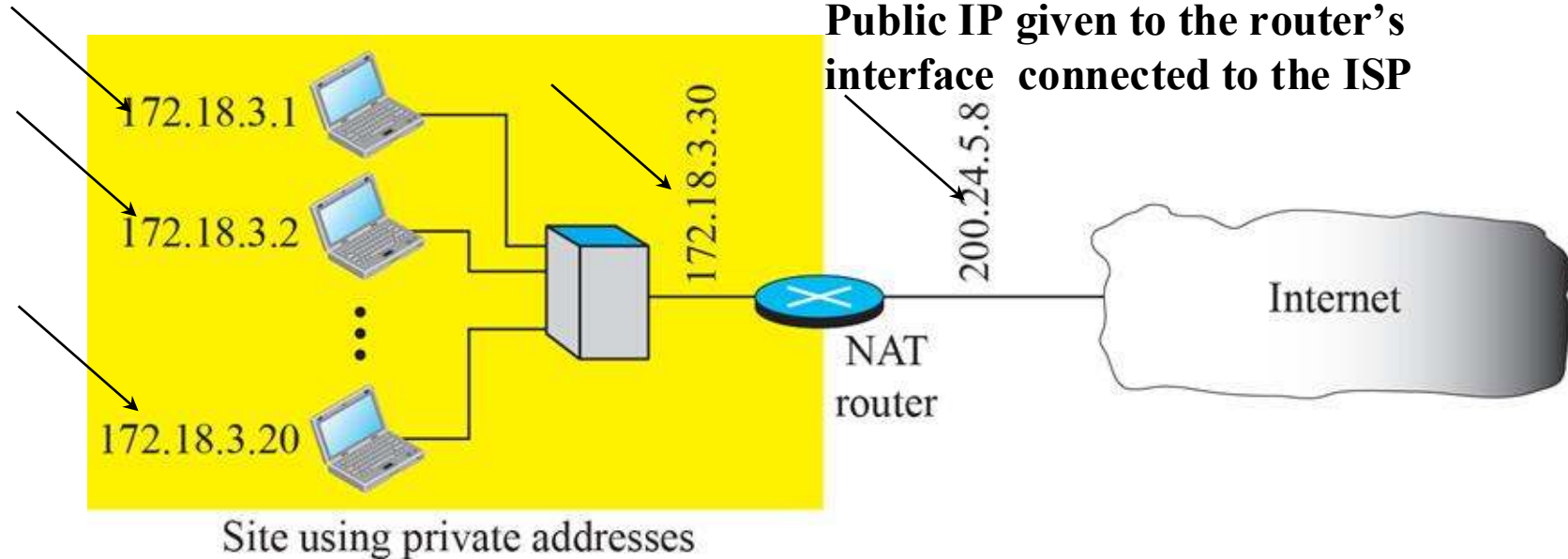
Network Address Translation (NAT)

- How To save IP addresses;
 - For business customers and many home users (ADSL), they want to stay **connected continuously** □ each user must have its own IP address □ total number of IP number an ISP can provide will not be enough to cover all customers (for example, class B block can support 65536 only)
- Solution is using NAT enabled router
- NAT: is A technology that can provide the mapping between the private (local) and Public (global) IP addresses
- NAT: The technology allows a site to use a set of **private (local) addresses** for internal communication and a set of **global (Public) Internet** addresses (at least one) for communication with the rest of the world.

Private IP addresses

<i>Range</i>			<i>Total</i>
10.0.0.0	to	10.255.255.255	2^{24}
172.16.0.0	to	172.31.255.255	2^{20}
192.168.0.0	to	192.168.255.255	2^{16}

Private IPs



Site using private addresses

Figure : Address translation

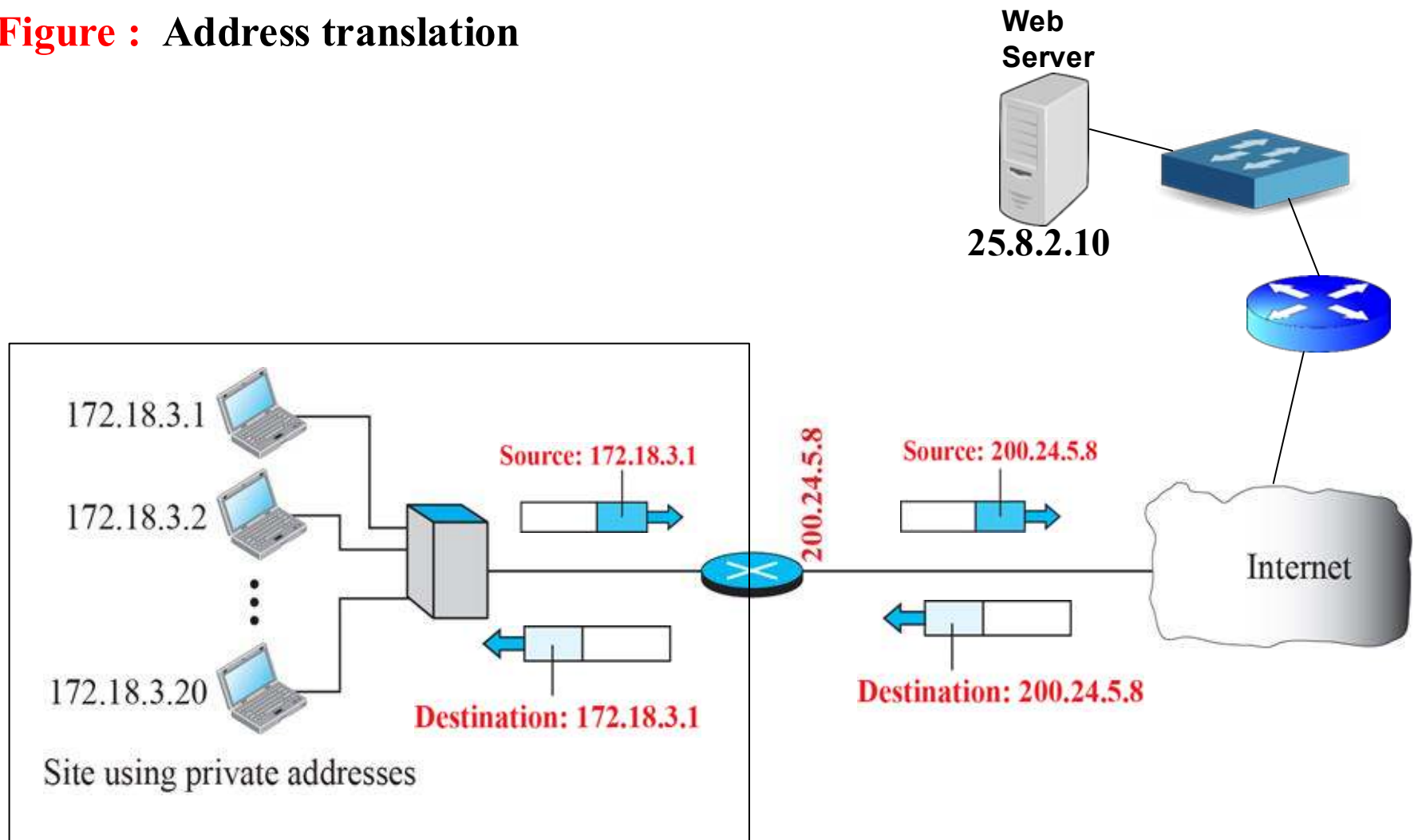
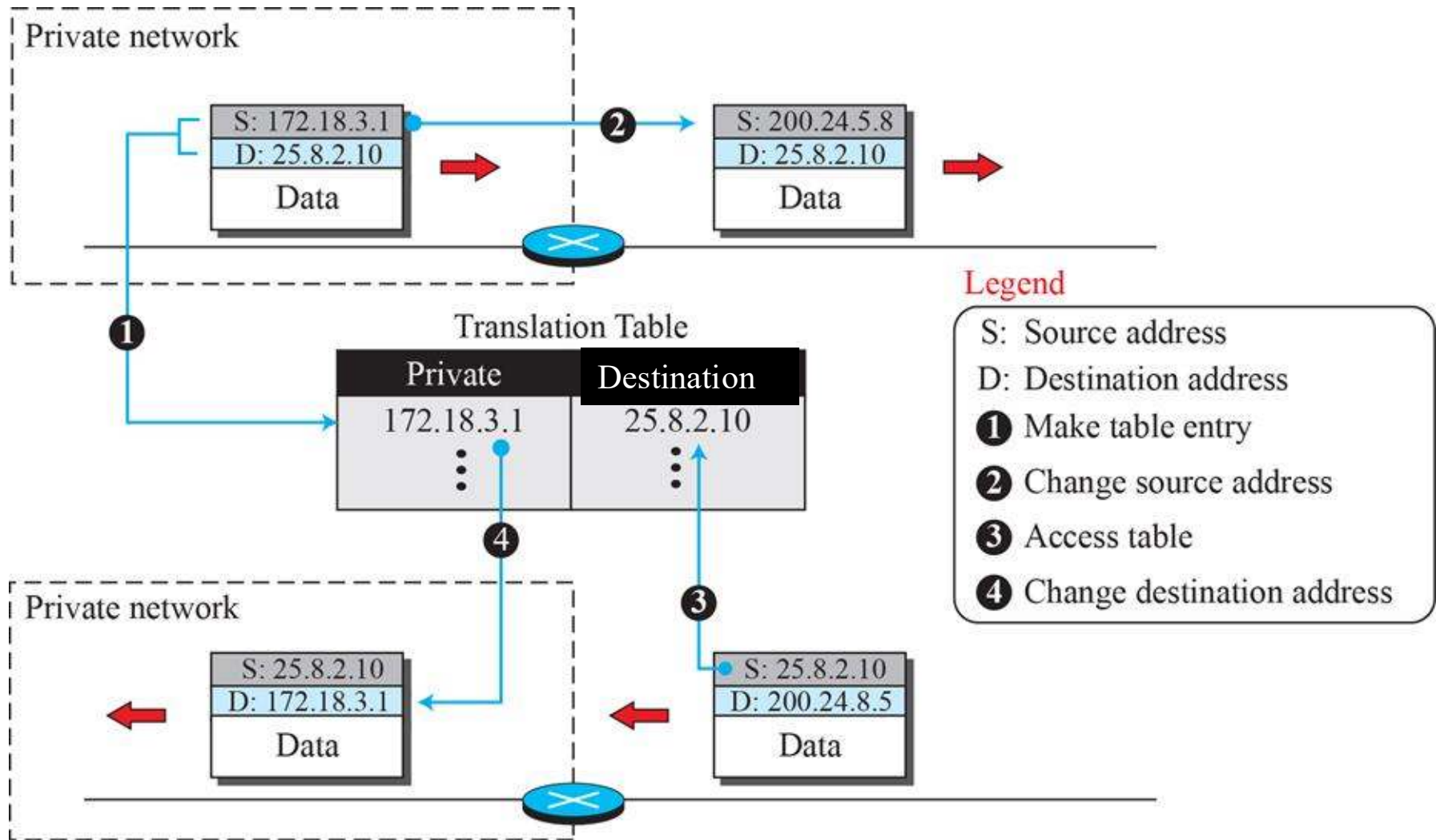


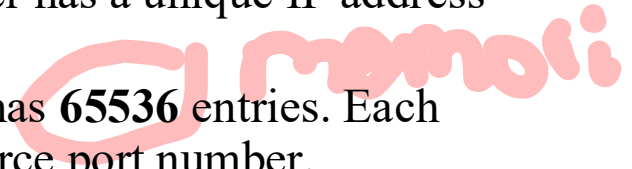
Figure : Translation



Network Address Translation (NAT)

- How does it work?

- A company is connected to the ISP through a router with NAT software (router is called NAT enabled router). The router has a unique IP address given to the company by the ISP
- NAT router maintains a **translation table** that has **65536** entries. Each row has **four fields**: Private source address, source port number, destination address, NAT port number (should be unique)
- Every machine within a company has a unique IP address selected from the set of **private addresses** usually (10.x.y.z)
- If a computer inside the company want to connect to a computer outside the network, such as a Web server, the NAT router receives the packet from the computer
- **NAT will NOT allow more than one host to contact same destination**



Advantages of using NAT

- No need to be allocated range of global addresses from ISP: just one global IP address is used for all devices □ **save IP address**
- can change addresses of devices in local network without notifying outside world
- can change ISP without changing addresses of devices in local network
- Can be used as firewall. A computer on an external network **cannot connect to your computer** unless your computer has initiated the contact. You can browse the Internet and connect to a site, and even download a file; but somebody else cannot use your IP address to connect to a port on your computer. (** Internet routers do not recognize and forward packets with private destination IP addresses)