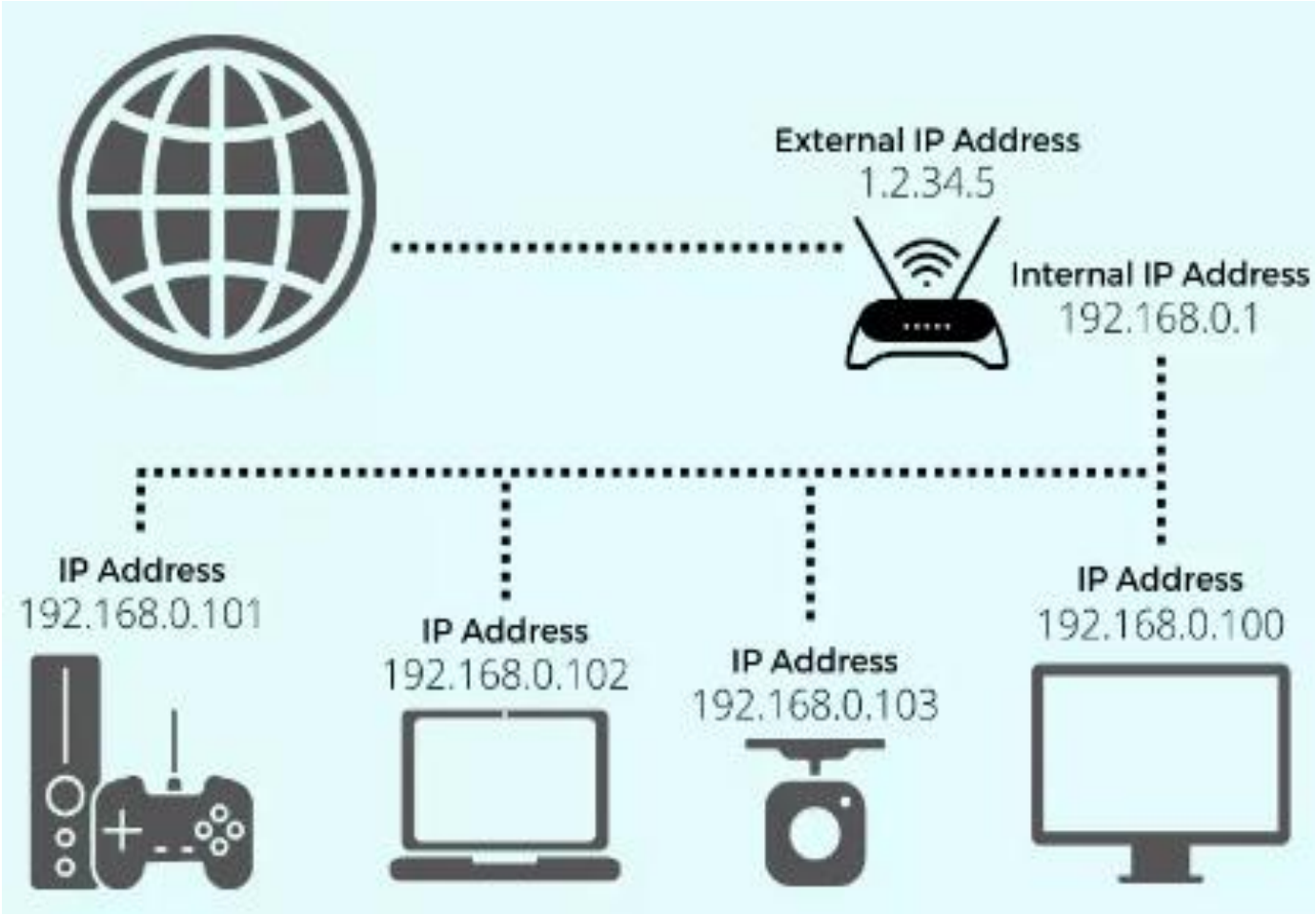
Unit II
ADDRESSING



CLR 2: Produce knowledge in IP addressing

CO 2: Construct the network using Addressing schemes

TOPICS

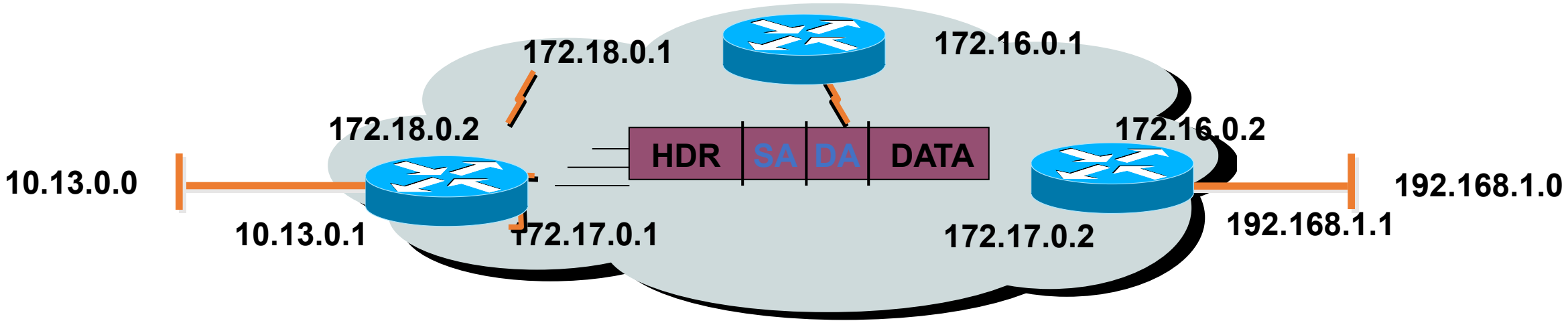
- Introduction
- IPv4 Addressing
- Address Space
- Classful addressing
- Subnet Mask - FLSM
- Classless addressing – VLSM
- NAT – Super netting
- Network Devices – Hup, Repeater, Switch, bridges, Gates, Router

Resources:

Behrouz A. Forouzan, “Data Communication & Networking”, 5th edition, 2010.
William Stallings, Data and Computer Communications”, 9th edition, 2010.

IP Addressing

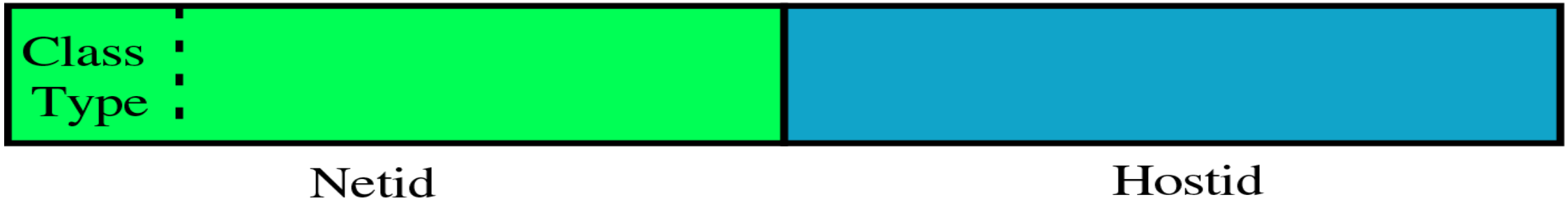
Introduction to TCP/IP Addresses



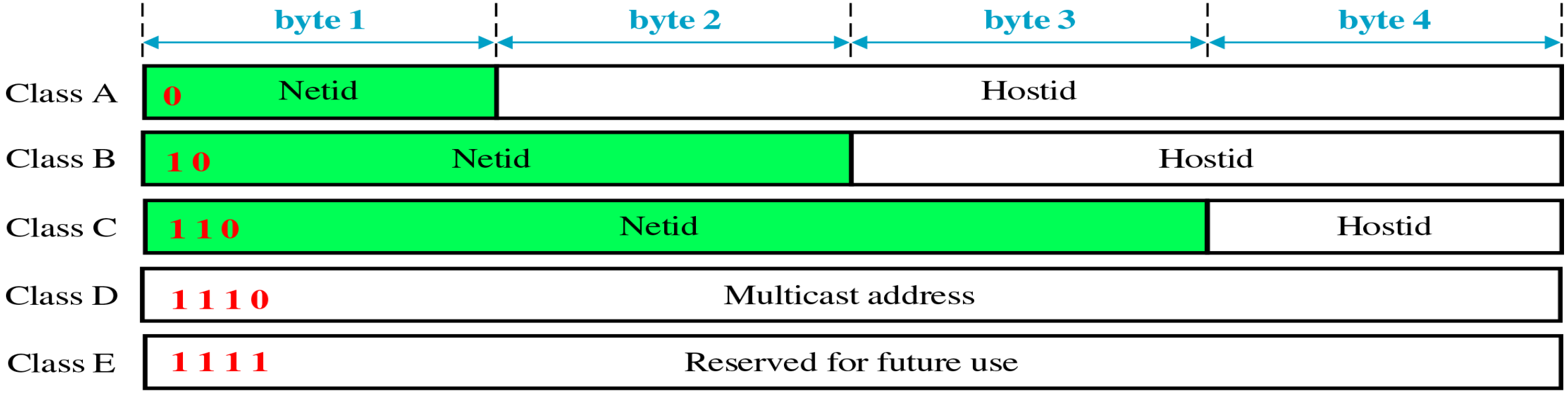
- Unique addressing allows communication between end stations
- Path choice is based on location

Internet Address

An Internet address is made of four bytes (32 bits) that define a host's connection to a network.



Internet Classes



IP Addresses in Decimal Notation

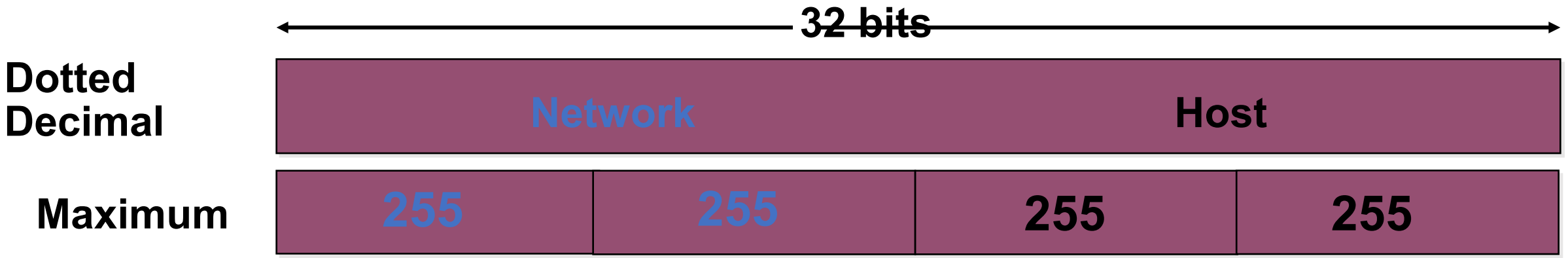
10000000 00001011 00000011 00011111

128.11.3.31

Class Ranges of Internet Addresses

	From	To
Class A	0.0.0.0 Netid Hostid	127.255.255.255 Netid Hostid
Class B	128.0.0.0 Netid Hostid	191.255.255.255 Netid Hostid
Class C	192.0.0.0 Netid Hostid	223.255.255.255 Netid Hostid
Class D	224.0.0.0 Group address	239.255.255.255 Group address
Class E	240.0.0.0 Undefined	255.255.255.255 Undefined

IP Addressing



IP Addressing

SRM INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

32 bits

Dotted Decimal	Network		Host	
Maximum	255	255	255	255
	1 – 8	9 – 16	17 – 24	25 – 32
Binary	11111111	11111111	11111111	11111111
	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1	128 64 32 16 8 4 2 1
Example Decimal	172	16	122	204
Example Binary	10101100	00010000	01111010	11001100

IP Address Classes

	8 bits	8 bits	8 bits	8 bits
•Class A:	Network	Host	Host	Host
•Class B:	Network	Network	Host	Host
•Class C:	Network	Network	Network	Host

•Class D: Multicast

•Class E: Research

Unicast, Multicast, and Reserved Addresses

- Unicast address – identifies a specific device
- Multicast address – identifies a host belongs to a group or groups (used only as a destination address)
- Reserved addresses – class E addresses; only used in special cases

Class A Addresses

- Numerically the lowest
- Use only one byte to identify the class type and netid
- Three bytes are available for hostid numbers
- 127 possible class A networks with a maximum of 16,777,214 computers on each network
- Designed for large organizations with a large number of hosts or routers
- Many addresses are wasted

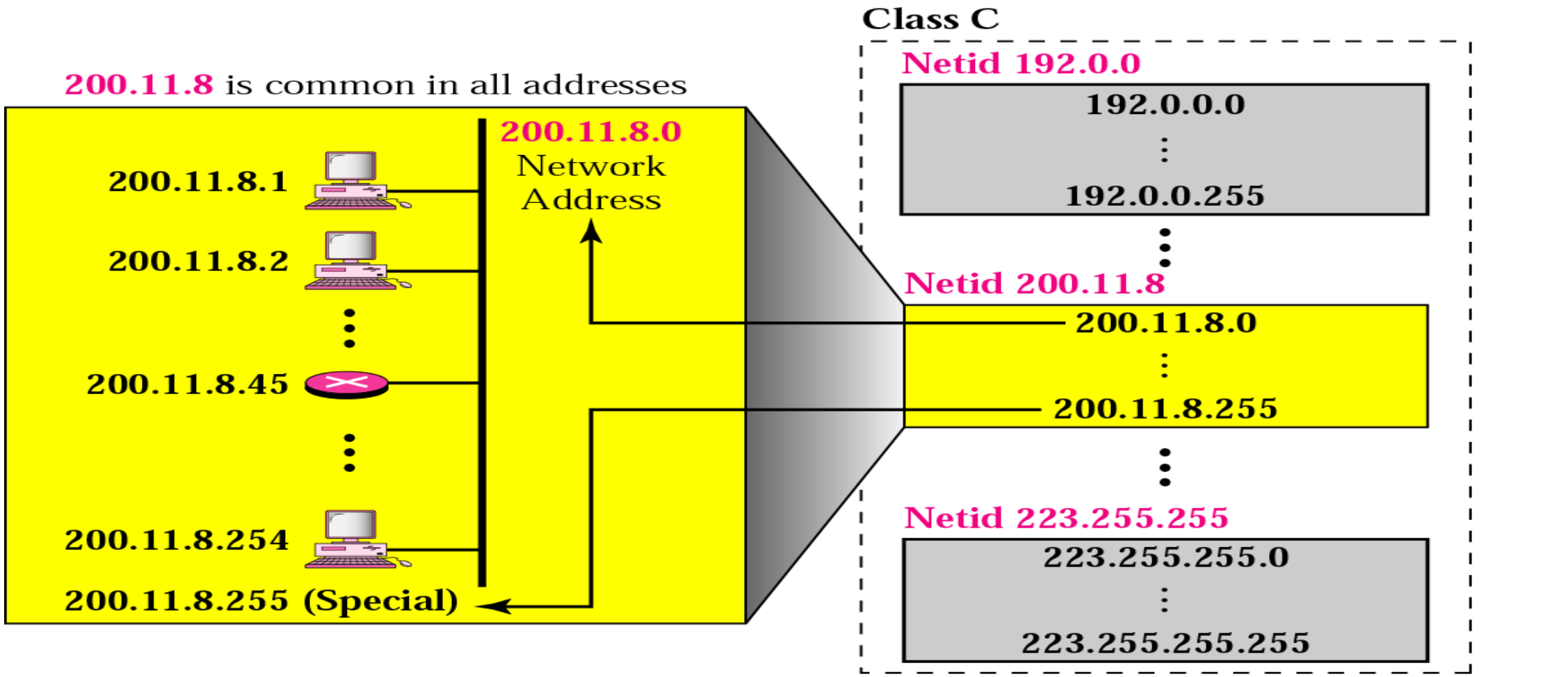
Class B Addresses

- First two octets are the network number and the last two octets are the host number
- 16,382 possible blocks for assignment to organizations with a maximum of 65,534 computers on each network
- Designed for mid-size organizations that may have tens of thousands of hosts or routers
- Many addresses are wasted

Class C Addresses

- The first three octets are the network number and the last octet is the host number
- 2,096,896 blocks for assignment to organizations
- First three bytes (netid) are the same
- Each block only contains 256 addresses, which may be smaller than what many organizations need

Blocks in Class C



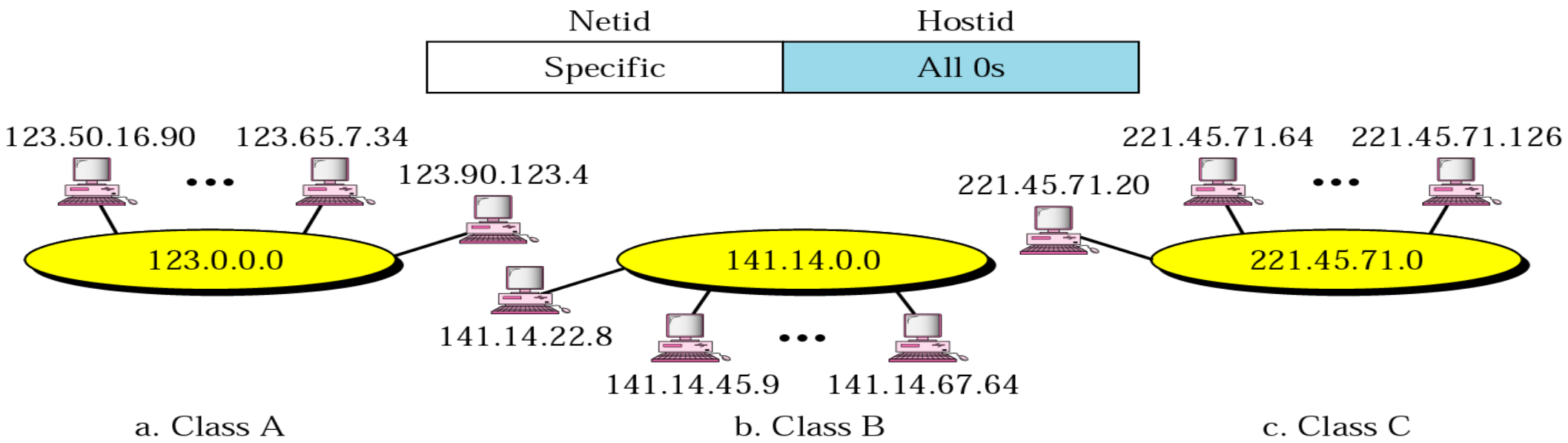
2,097,152 blocks: 256 addresses in each block

Class D and Class E Addresses

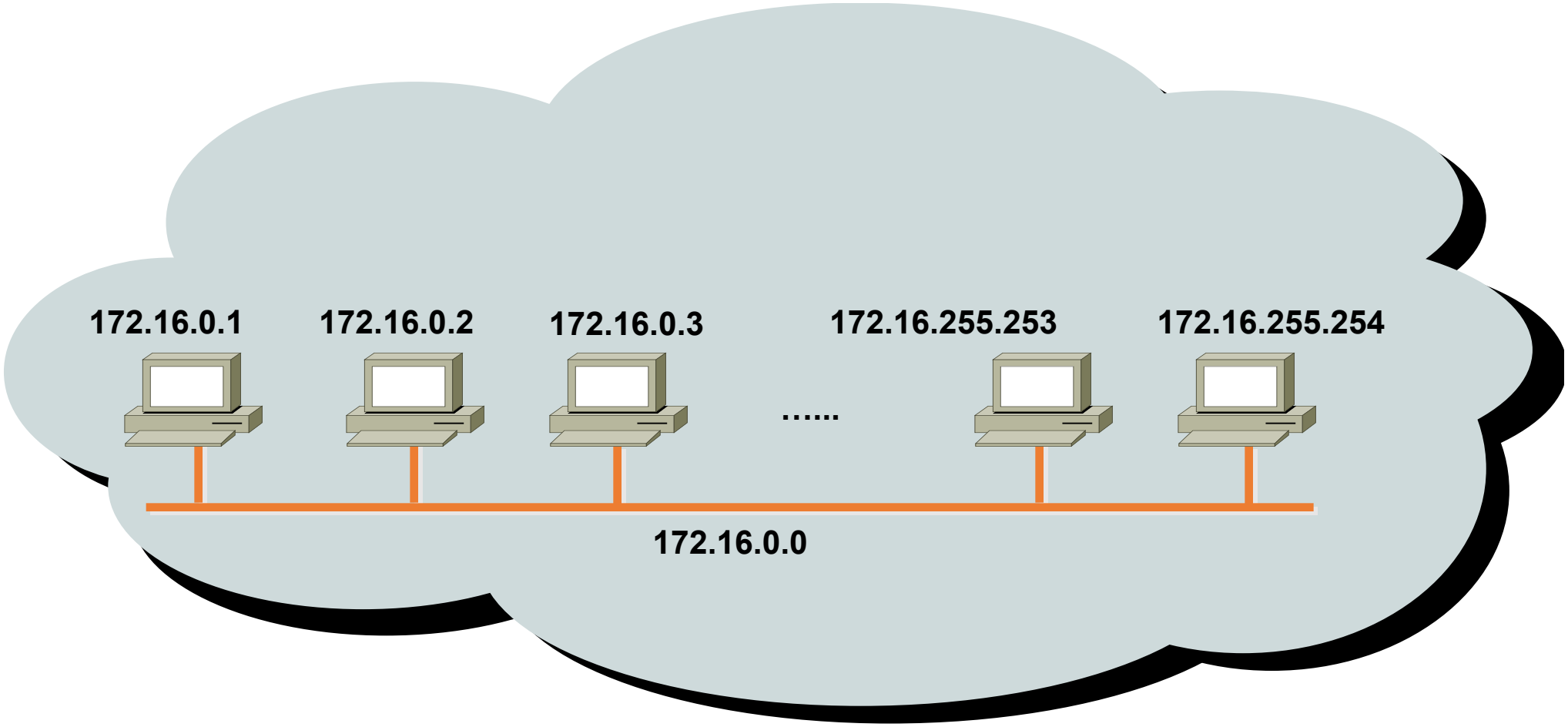
- Class D – reserved for multicast addresses
  - **Multicasting** – transmission method which allows copies of a single packet to be sent to a selected group of receivers
- Class E – reserved for future use

Network Address

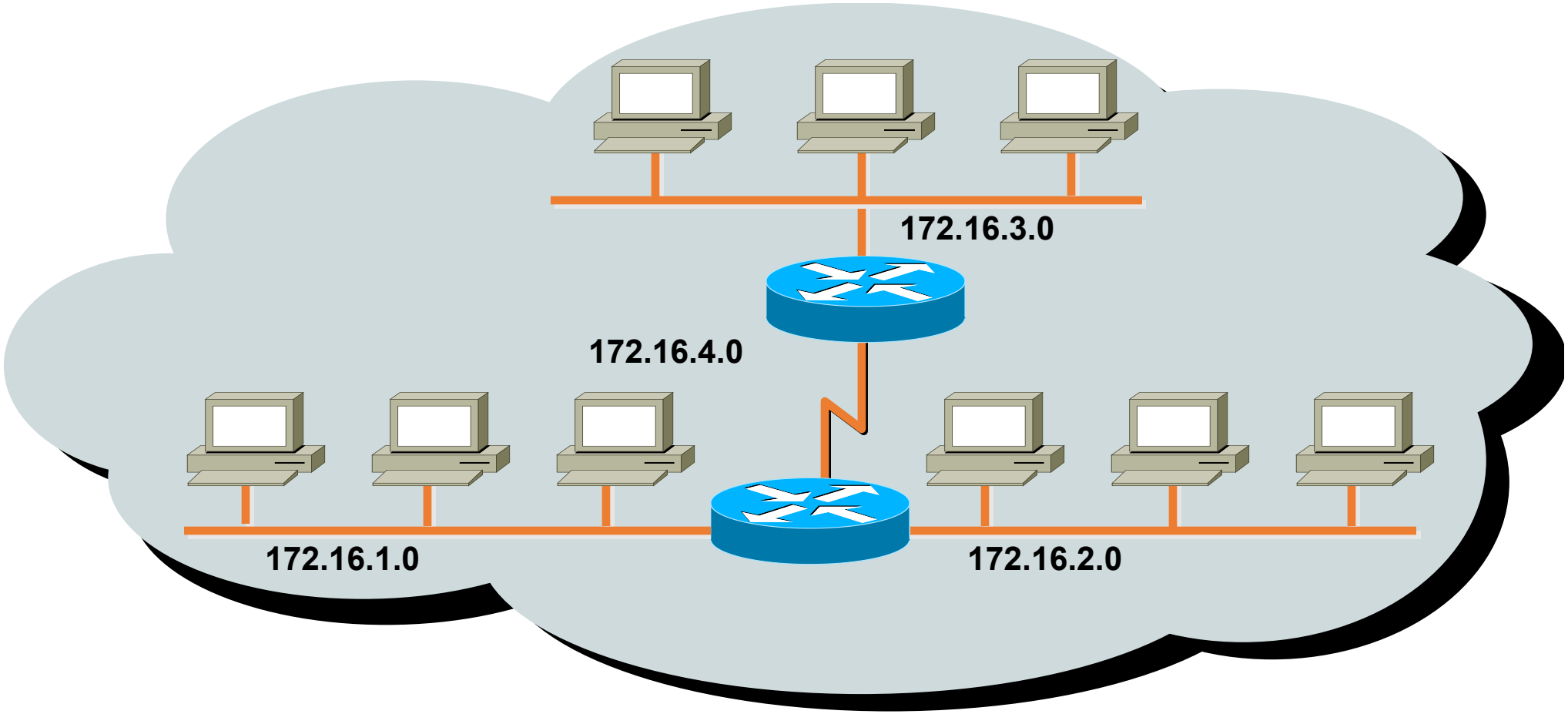
- First address in the block, assigned to the organization
- Defines the network itself and cannot be assigned to a host
- Has both netid and hostid, with 0s for the hostid
- Defines the network to the rest of the Internet



Addressing without Subnets



Addressing with Subnets



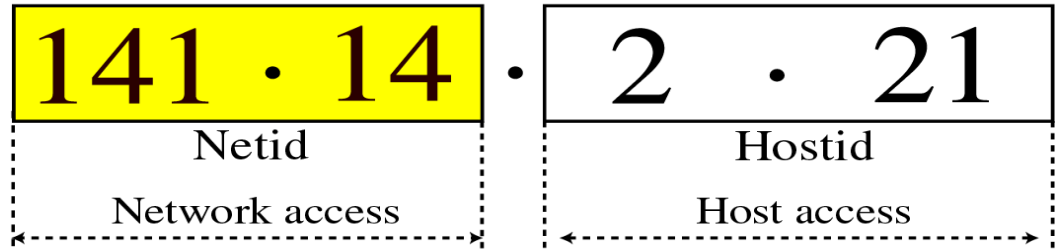
Network 172.16.0.0

Subnetting

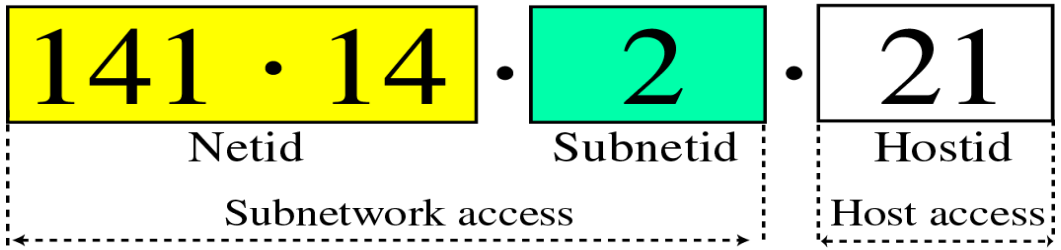
- IP addressing is hierarchical
- First reach a device through its network id (netid)
- Then reach the host itself using the second portion (hostid)
- Since an organization may not have enough address, subnetting may be used to divide the network into smaller networks or **sub-networks**

Contd..

- Sub-netting creates an intermediate level of hierarchy
- IP datagram routing then involves three steps:
  - Delivery to the site,
  - Delivery to the sub-network, and
  - Delivery to the host



a. Without subnetting



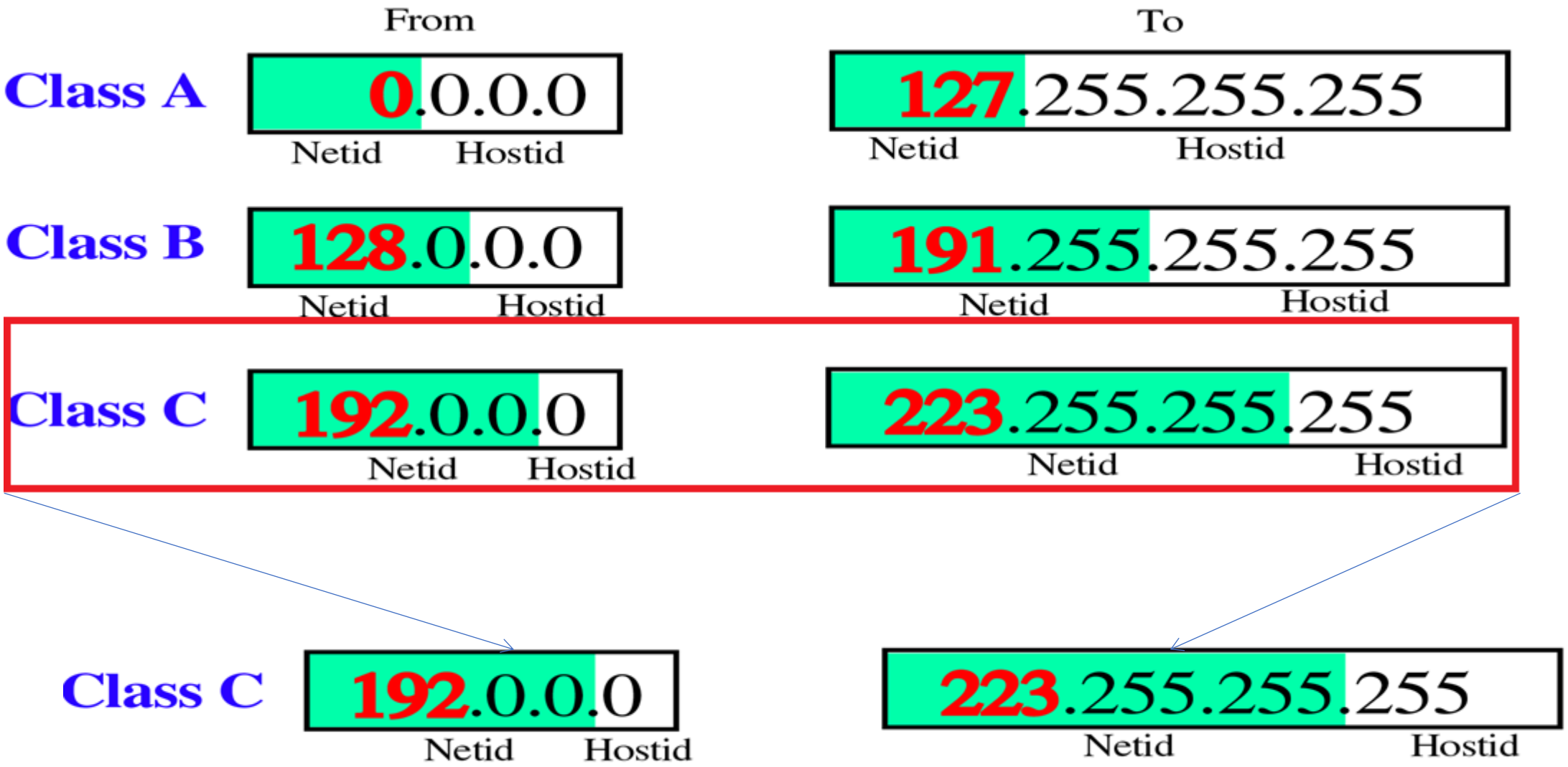
b. With subnetting

Class C Subnets

Class C IP addresses are normally assigned to a very small size network because it can only have 254 hosts in a network. Given below is a list of all possible combination of subnetted Class B IP address

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	1	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.255.240	4	16	14
29	255.255.255.248	5	32	6
30	255.255.255.252	6	64	2

“C- Class Addressing”



Sub-netting "C- Class Addressing"

C- Class IP address

192	168	10	0 to 255

192	168	10	0	11000000	10101000	00001010	00000000
192	168	10	1	11000000	10101000	00001010	00000001
192	168	10	2	11000000	10101000	00001010	00000010
⋮				⋮			
192	168	10	255	11000000	10101000	00001010	11111111

Default Subnet Mask

- Class A – 255.0.0.0
- Class B – 255.255.0.0
- Class C – 255.255.255.0

Masking

- Extracts the address of the physical network from an IP address
- Used by routers inside the organization

a. Without subnetting

b. With subnetting

Sub-netting "C- Class Addressing"

IP address	192	168	10	35	11000000	10101000	00001010	00100011
Subnet Mask	255	255	255	0	11111111	11111111	11111111	00000000
AND operation					11000000	10101000	00001010	00000000
Subnet ID - Binary					11000000	10101000	00001010	00000000
Subnet ID - Decimal	192	168	10	0				

Sub-netting "C- Class Addressing"

IP address	192	168	10	35	11000000	10101000	00001010	00100011
Subnet Mask	255	255	255	128	11111111	11111111	11111111	10000000
AND operation					11000000	10101000	00001010	00000000
Subnet ID - Binary					11000000	10101000	00001010	00000000
Subnet ID - Decimal	192	168	10	0				

Sub-netting "C- Class Addressing"

IP address	192	168	10	132	11000000	10101000	00001010	10000100
Subnet Mask	255	255	255	128	11111111	11111111	11111111	10000000
AND operation					11000000	10101000	00001010	10000000
Subnet ID - Binary					11000000	10101000	00001010	10000000
Subnet ID - Decimal	192	168	10	128				

Sub-netting "C- Class Addressing"

IP address

192	168	10	35

11000000	10101000	00001010	00100011

Subnet Mask

255	255	255	192

11111111	11111111	11111111	11000000

AND operation

11000000	10101000	00001010	00000000

Subnet ID - Decimal

192	168	10	0

Sub-netting "C- Class Addressing"

IP address

192	168	10	75

11000000	10101000	00001010	01001011

Subnet Mask

255	255	255	192

11111111	11111111	11111111	11000000

AND operation

11000000	10101000	00001010	01000000

Subnet ID - Decimal

192	168	10	64

Sub-netting "C- Class Addressing"

IP address

192	168	10	137

11000000	10101000	00001010	10001001

Subnet Mask

255	255	255	192

11111111	11111111	11111111	11000000

AND operation

11000000	10101000	00001010	10000000

Subnet ID - Decimal

192	168	10	128

Sub-netting "C- Class Addressing"

IP address

192	168	10	199

11000000	10101000	00001010	11000111

Subnet Mask

255	255	255	192

11111111	11111111	11111111	11000000

AND operation

11000000	10101000	00001010	11000000

Subnet ID - Decimal

192	168	10	192

Subnet Mask

255	255	255	192

Subnet ID - 1	**192.168.10.0**	Subnet work Identification	**00**	**000000**
	192.168.10.1 **to** 192.168.10.62	**62 Valid IP address**	**00**	**000001 to 111110**
	192.168.10.63	Broadcast Address	**00**	**111111**
Subnet ID - 2	192.168.10.64	Subnet work Identification	**01**	000000
	192.168.10.65 **to** 192.168.10.126	**62 Valid IP address**	**01**	**000001 to 111110**
	192.168.10.127	Broadcast Address	**01**	**111111**
Subnet ID - 3	192.168.10.128	Subnet work Identification	**10**	000000
	192.168.10.129 **to** 192.168.10.190	**62 Valid IP address**	**10**	**000001 to 111110**
	192.168.10.191	Broadcast Address	**10**	**111111**
Subnet ID - 4	192.168.10.192	Subnet work Identification	**11**	000000
	192.168.10.193 **to** 192.168.10.254	**62 Valid IP address**	**11**	**000001 to 111110**
	192.168.10.255	Broadcast Address	**11**	**111111**

Sub-netting "C- Class Addressing"

Subnet Mask

255	255	255	128	11111111	11111111	11111111	1 0000000

180	10	0	0	11000000	10101000	00001010	00000000
192	168	10	1	11000000	10101000	00001010	00000001

IP address

192	168	10	35	11000000	10101000	00001010	00100011
192	168	10	126	11111111	11111111	11111111	01111110
192	168	10	127	11111111	11111111	11111111	01111111
192	168	10	128	11111111	11111111	11111111	10000000
192	168	10	129	11000000	10101000	00001010	10000001
192	168	10	254	11000000	10101000	00001010	11111110
192	168	10	255	11000000	10101000	00001010	11111111

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

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

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

a. 129.11.11.239

b. 193.131.27.255

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

a. 111.56.45.78

b. 221.34.7.82

Solution

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

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

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

a. 111.56.045.78

b. 221.34.7.8.20

c. 75.45.301.14

d. 11100010.23.14.67

Solution

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

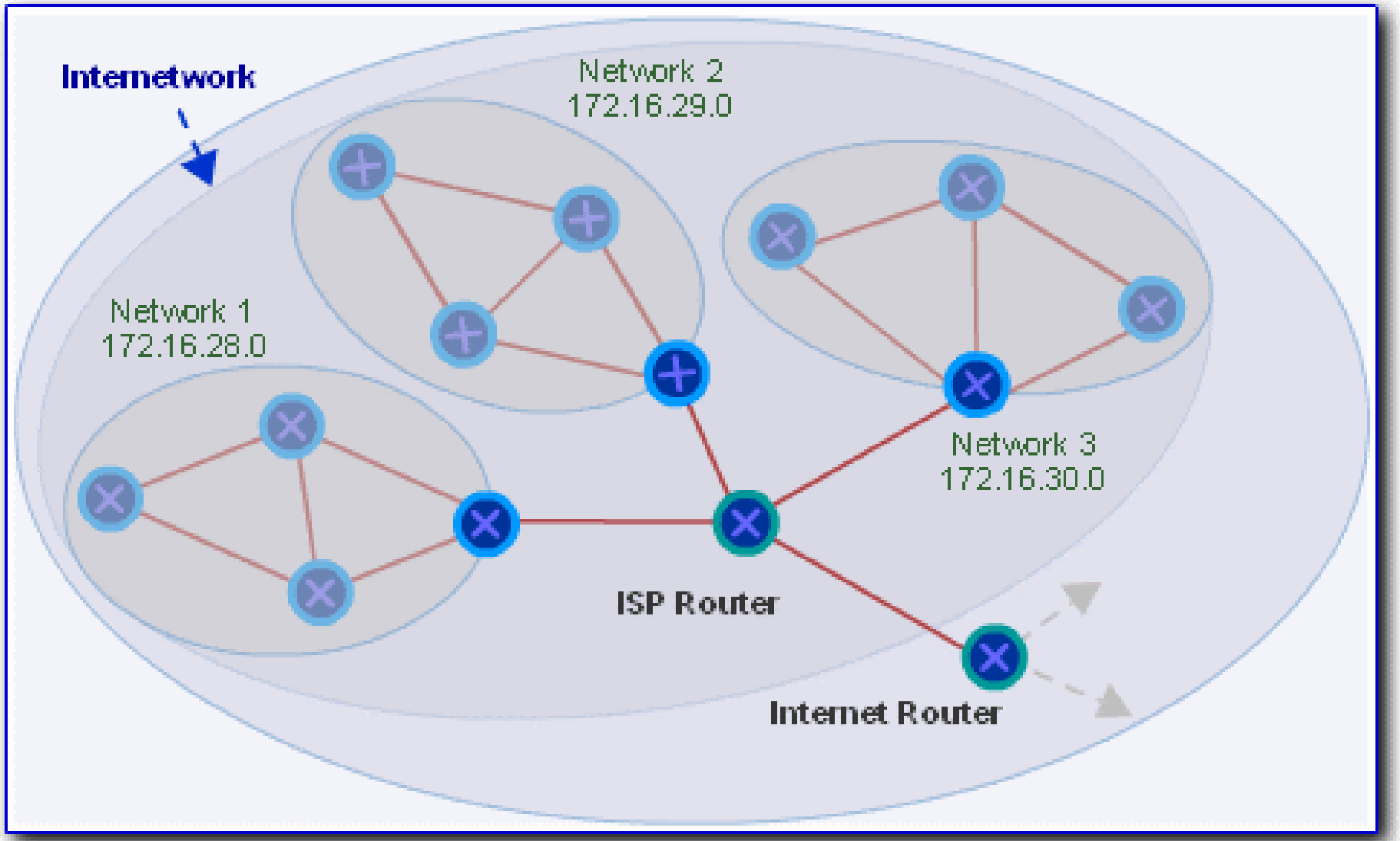
b. There can be no more than four numbers.

c. Each number needs to be less than or equal to 255.

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

Supernetting

- Class C blocks have a maximum number of 256 addresses
- Supernetting allows an organization to combine several class C blocks to create a larger range of addresses


Internetwork
Network 2
172.16.29.0
Network 1
172.16.28.0
Network 3
172.16.30.0
ISP Router
Internet Router

Supernetting in Network Layer

- **Supernetting** is the opposite of ***Subnetting***. In subnetting, a single big network is divided into multiple smaller subnetworks.
- In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.
- Supernetting is mainly used in Route Summarization, where routes to multiple networks with similar network prefixes are combined into a single routing entry, with the routing entry pointing to a Super network, encompassing all the networks.
- This in turn significantly reduces the size of routing tables and also the size of routing updates exchanged by routing protocols.

Supernetting in Network Layer

- More specifically,
- When multiple networks are combined to form a bigger network, it is termed as super-netting
- Super netting is used in route aggregation to reduce the size of routing tables and routing table updates
- There are some points which should be kept in mind while supernetting:
- All the Networks should be contiguous.
- The block size of every networks should be equal and must be in form of 2^n.
- First Network id should be exactly divisible by whole size of supernet.
- **Example –** Suppose 4 small networks of class C:

Supernetting in Network Layer

- **Example –** Suppose 4 small networks of class C:
- 200.1.0.0,
- 200.1.1.0,
- 200.1.2.0,
- 200.1.3.0

- Build a bigger network which have a single Network Id

Explanation – Before Super-netting routing table will be look like as:

Network Id	Subnet Mask	Interface
200.1.0.0	255.255.255.0	A
200.1.1.0	255.255.255.0	B
200.1.2.0	255.255.255.0	C
200.1.3.0	255.255.255.0	D

First, lets check whether three condition are satisfied or not:

- **Contiguous:** You can easily see that all network are contiguous all having size 256 hosts.
  Range of first Network from 200.1.0.0 to 200.1.0.255. If you add 1 in last IP address of first network that is 200.1.0.255 + 0.0.0.1, you will get the next network id that is 200.1.1.0. Similarly, check that all network are contiguous.
- **Equal size of all network:** As all networks are of class C, so all of the have a size of 256 which in turn equal to 2^8.

- **First IP address exactly divisible by total size:** When a binary number is divided by 2^n then last n bits are the remainder.
- Hence in order to prove that first IP address is exactly divisible by while size of Supernet Network.
- You can check that if last n v=bits are 0 or not. In given example first IP is 200.1.0.0 and whole size of supernet is $4*2^8 = 2^{10}$.
- If last 10 bits of first IP address are zero then IP will be divisible.
- Last 10 bits of first IP address are zero (highlighted by green color).
  - So 3rd condition is also satisfied.
- Therefore, you can join all these 4 networks and can make a Supernet. New Supernet Id will be 200.1.0.0.

Advantages & Disadvantages of Super-netting

- **Advantages of Supernetting –**
- Control and reduce network traffic
- Helpful to solve the problem of lacking IP addresses
- Minimizes the routing table
- **Disadvantages of Supernetting –**
  - It cannot cover different area of network when combined
  - All the networks should be in same class and all IP should be contiguous

Problems & Exercises - 1

- You have been allocated a class A network address of **29.0.0.0**. You need to create at least 20 networks and each network will support a maximum of 160 hosts. Would the following two subnet masks Work?
- **255.255.0.0** and or **255.255.255.0**

Problems & Exercises - 2

- You have been allocated a class B network address of 135.1.0.0 and and need to create 4 subnets each with around 200 hosts what is the easiest mask to use to satisfy the criteria?

Problems & Exercises - 3

- You have been allocated a class C network address of 211.1.1.0 and are using the default subnet mask of 255.255.255.0 how may hosts can you have?

Problems & Exercises - 4

- Subnet the Class C IP Address 195.1.1.0 So that you have 10 subnets each with a maximum 12 hosts on each subnet. List the Address on host 1 on subnet 0,1,2,3,10

Problems & Exercises - 5

- Subnet the Class C IP Address 205.11.2.0 so that you have 30 subnets.
- What is the subnet mask for the maximum number of hosts?
- How many hosts can each subnet have?
- What is the IP address of host 3 on subnet 2 ?

Problems & Exercises - 6

- Subnet the Class C IP Address 195.1.1.0 So that you have at least 2 subnets each subnet must have room for 48 hosts .
- What are the two possible subnet masks?

Problems & Exercises - 7

- Given the subnet Mask **255.255.255.192** What is the host address and subnet of the following IP address 197.1.2.67.

Classless Addressing

- Addressing mechanism in which the IP address space is not divided into classes
- Block ranges are variable, as long as they are a power of 2 (2, 4, 8,…)
- Masking is also used as well as subnetting
- Requires a different routing scheme, discussed later

Note

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

Find the class of each address.

a. 00000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

c. 14.23.120.8

d. 252.5.15.111

Solution

a. The first bit is 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 byte is 14; the class is A.

d. The first byte is 252; the class is E.

Note

In classful addressing, a large part of the available addresses were wasted.

Note

Classful addressing, which is almost obsolete, is replaced with classless addressing.

IP Sub-netting from CIDR Notation

Sub-netting from CIDR Notation

192.168.60.55 /20

Network ID				

Broadcast ID				

Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /20

11111111	**11111111**	**11110000**	**00000000**

192.168.60.55 /20 → Conversion → **Subnet Mask : 255.255. 240.0**

Sub-netting from CIDR Notation

192.168.60.55 /20

Network ID	**192**	**168**		

Broadcast ID	**192**	**168**		

Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /20

11111111	**11111111**	**11110000**	**00000000**

Focus

Conversion

192.168.60.55 /20 → **Subnet Mask : 255.255. 240.0**

Sub-netting from CIDR Notation

192.168.60.55 /20

Network ID	192	168		0
Broadcast ID	192	168		255
Usable IP's				

128	64	32	16	8	4	2	1

CIDR Notation : xxx.xxx.xxx.xxx /20

11111111	11111111	11110000	00000000

Focus

Conversion

192.168.60.55 /20 → **Subnet Mask : 255.255. 240.0**

Sub-netting from CIDR Notation

192.168.60.55 /20

Network ID	192	168		0
Broadcast ID	192	168		255
Usable IP's				

128	64	32	16	8	4	2	1

CIDR Notation : xxx.xxx.xxx.xxx /20

60

XXXXXXXX	XXXXXXXX	00111100	XXXXXXXX
11111111	11111111	11110000	00000000

Sub-netting from CIDR Notation

192.168.60.55 /20

Network ID	192	168		0
Broadcast ID	192	168		255
Usable IP's				

128	64	32	16	8	4	2	1

CIDR Notation : xxx.xxx.xxx.xxx /20

60

XXXXXXXX	XXXXXXXX	00111100	XXXXXXXX
11111111	11111111	11110000	00000000
AND Operation Result		00110000	

Sub-netting from CIDR Notation

192.168.60.55 /20

Network ID	**192**	**168**	**48**	**0**
Broadcast ID	**192**	**168**		**255**
Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

AND Operation Result			**00110000**	

Sub-netting from CIDR Notation

192.168.60.55 /20

Network ID	**192**	**168**	**48**	**0**
Broadcast ID	**192**	**168**	**63**	**255**
Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

(48 + 16) -1 = 63

AND Operation Result			**00110000**	
	11111111	**11111111**	**11110000**	**00000000**

Focus

Sub-netting from CIDR Notation

192.168.60.55 /20

Network ID	**192**	**168**	**48**	**0**

Broadcast ID	**192**	**168**	**63**	**255**

Usable IP's	**192.168.48.1**	**TO**	**192.168.63.254**

Example - 2

Sub-netting from CIDR Notation

172.10.85.60 /22

Network ID				

Broadcast ID				

Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /22

11111111	**11111111**	**11111100**	**00000000**

172.10.85.60 /22 → Conversion → **Subnet Mask : 255.255. 252.0**

Sub-netting from CIDR Notation

172.10.85.60 /22

Network ID	**172**	**10**		

Broadcast ID	**172**	**10**		

Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /22

11111111	**11111111**	**11111100**	**00000000**

Focus

172.10.85.60 /22 → **Conversion** → **Subnet Mask : 255.255. 252.0**

Sub-netting from CIDR Notation

172.10.85.60 /22

Network ID	**172**	**10**		**0**

Broadcast ID	**172**	**10**		**255**

Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /22

11111111	**11111111**	**11111100**	**00000000**

Focus

Conversion

172.10.85.60 /22 → **Subnet Mask : 255.255. 252.0**

Sub-netting from CIDR Notation

172.10.85.60 /22

Network ID	**172**	**10**		**0**
Broadcast ID	**172**	**10**		**255**
Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /22

XXXXXXXX	**XXXXXXXX**	**01010101**	**XXXXXXXX**
11111111	**11111111**	**11111100**	**00000000**

Focus

Sub-netting from CIDR Notation

172.10.85.60 /22

Network ID	**172**	**10**		**0**
Broadcast ID	**172**	**10**		**255**
Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /22

XXXXXXXX	**XXXXXXXX**	**01010101**	**XXXXXXXX**
		11111100	
AND Operation Result		**01010100**	

Sub-netting from CIDR Notation

172.10.85.60 /22

Network ID	**172**	**10**	**84**	**0**
Broadcast ID	**172**	**10**		**255**
Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /22

XXXXXXXX	**XXXXXXXX**	**01010101**	**XXXXXXXX**
		11111100	
AND Operation Result		**01010100**	

Sub-netting from CIDR Notation

172.10.85.60 /22

Network ID	**172**	**10**	**84**	**0**
Broadcast ID	**172**	**10**		**255**
Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /22

XXXXXXXX	**XXXXXXXX**	**01010101**	**XXXXXXXX**
		11111100	

(84 + 4) -1 = 87

Last Bit for above

Sub-netting from CIDR Notation

172.10.85.60 /22

Network ID	**172**	**10**	**84**	**0**
Broadcast ID	**172**	**10**	**87**	**255**
Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /22

XXXXXXXX	**XXXXXXXX**	**01010101**	**XXXXXXXX**
		11111100	

(84 + 4) -1 = 87

Last Bit for above

Sub-netting from CIDR Notation

172.10.85.60 /22

Network ID	**172**	**10**	**84**	**0**

Broadcast ID	**172**	**10**	**87**	**255**

Usable IP's	**172.10.84.1**	**to**	**172.10.87.254**

Example - 3

Sub-netting from CIDR Notation

172.10.60.16 /29

Network ID				

Broadcast ID				

Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /29

11111111	**11111111**	**11111111**	**11111000**

Sub-netting from CIDR Notation

172.10.60.16 /29

Network ID	**172**	**10**	**60**	

Broadcast ID	**172**	**10**	**60**	

Usable IP's				

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

CIDR Notation : xxx.xxx.xxx.xxx /29

11111111	**11111111**	**11111111**	**11111000**

Sub-netting from CIDR Notation

172.10.60.16 /29

Network ID	172	10	60	

Broadcast ID	172	10	60	

Usable IP's		TO	

128	64	32	16	8	4	2	1

CIDR Notation : xxx.xxx.xxx.xxx /29

XXXXXXXX	XXXXXXXX	XXXXXXXX	00010000
11111111	11111111	11111111	11111000

Sub-netting from CIDR Notation

172.10.60.16 /29

Network ID	172	10	60	

Broadcast ID	172	10	60	

Usable IP's		TO	

128	64	32	16	8	4	2	1

CIDR Notation : xxx.xxx.xxx.xxx /29

XXXXXXXX	XXXXXXXX	XXXXXXXX	00010000
11111111	11111111	11111111	11111000

AND Operation Result				0001000

Sub-netting from CIDR Notation

172.10.60.16 /29

Network ID	**172**	**10**	**60**	

Broadcast ID	**172**	**10**	**60**	

Usable IP's		**TO**	

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

AND Operation Result				**0001000**

Sub-netting from CIDR Notation

172.10.60.16 /29

Network ID	**172**	**10**	**60**	**16**

Broadcast ID	**172**	**10**	**60**	

Usable IP's		**TO**	

128	**64**	**32**	**16**	**8**	**4**	**2**	**1**

AND Operation Result				**0001000**

Sub-netting from CIDR Notation

172.10.60.16 /29

Network ID	172	10	60	16

Broadcast ID	172	10	60	

Usable IP's		TO	

128	64	32	16	8	4	2	1

CIDR Notation : xxx.xxx.xxx.xxx /29

XXXXXXXX	XXXXXXXX	XXXXXXXX	00010000
11111111	11111111	11111111	11111000

(16 +8)-1 =23

Sub-netting from CIDR Notation

172.10.60.16 /29

Network ID	172	10	60	16
Broadcast ID	172	10	60	23
Usable IP's		TO		

128	64	32	16	8	4	2	1

CIDR Notation : xxx.xxx.xxx.xxx /29

XXXXXXXX	XXXXXXXX	XXXXXXXX	00010000
11111111	11111111	11111111	11111000

(16 +8)-1 =23

Sub-netting from CIDR Notation

172.10.60.16 /29

Network ID	**172**	**10**	**60**	**16**

Broadcast ID	**172**	**10**	**60**	**23**

Usable IP's	**172.10.60.17**	**TO**	**172.10.60.22**

Private IPv4 Addresses (RFC 1918)

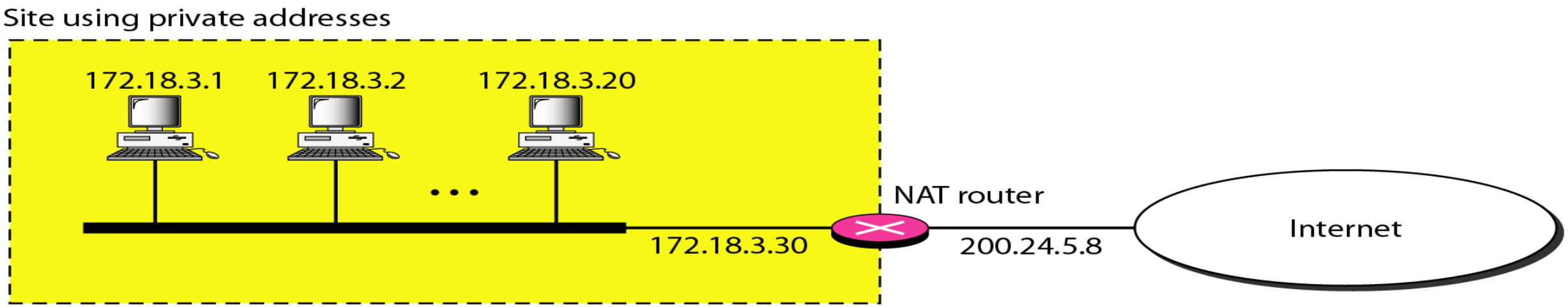
- IPv4 doesn't provide enough addresses for all devices that need an IP address in the modern world.
- The long-term solution is to switch to IPv6.
- There are three main short-term solutions:
  1) CIDR
  2) Private IPv4 addresses
  3) NAT
- RFC 1918 specifies the following IPv4 address ranges as private:

10.0.0.0/8 (10.0.0.0 to 10.255.255.255) → Class A

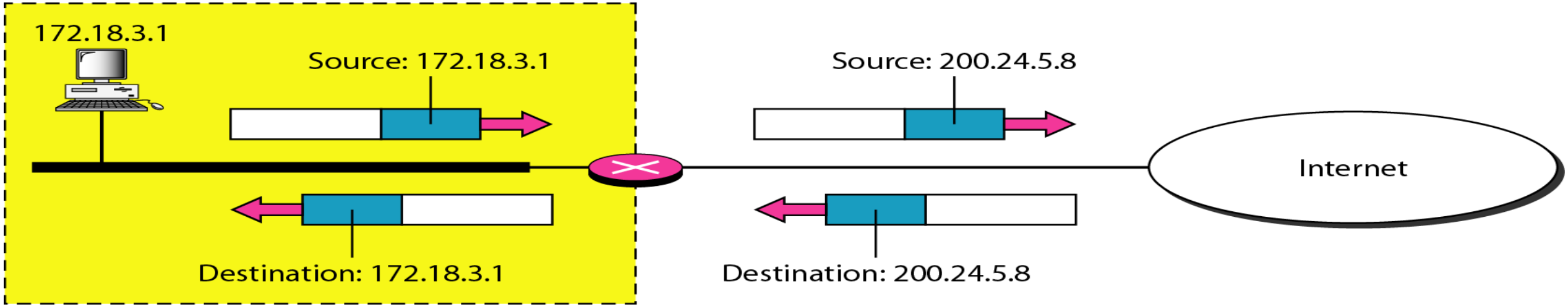
172.16.0.0/12 (172.16.0.0 to 172.31.255.255) → Class B

192.168.0.0/16 (192.168.0.0 to 192.168.255.255) → Class C

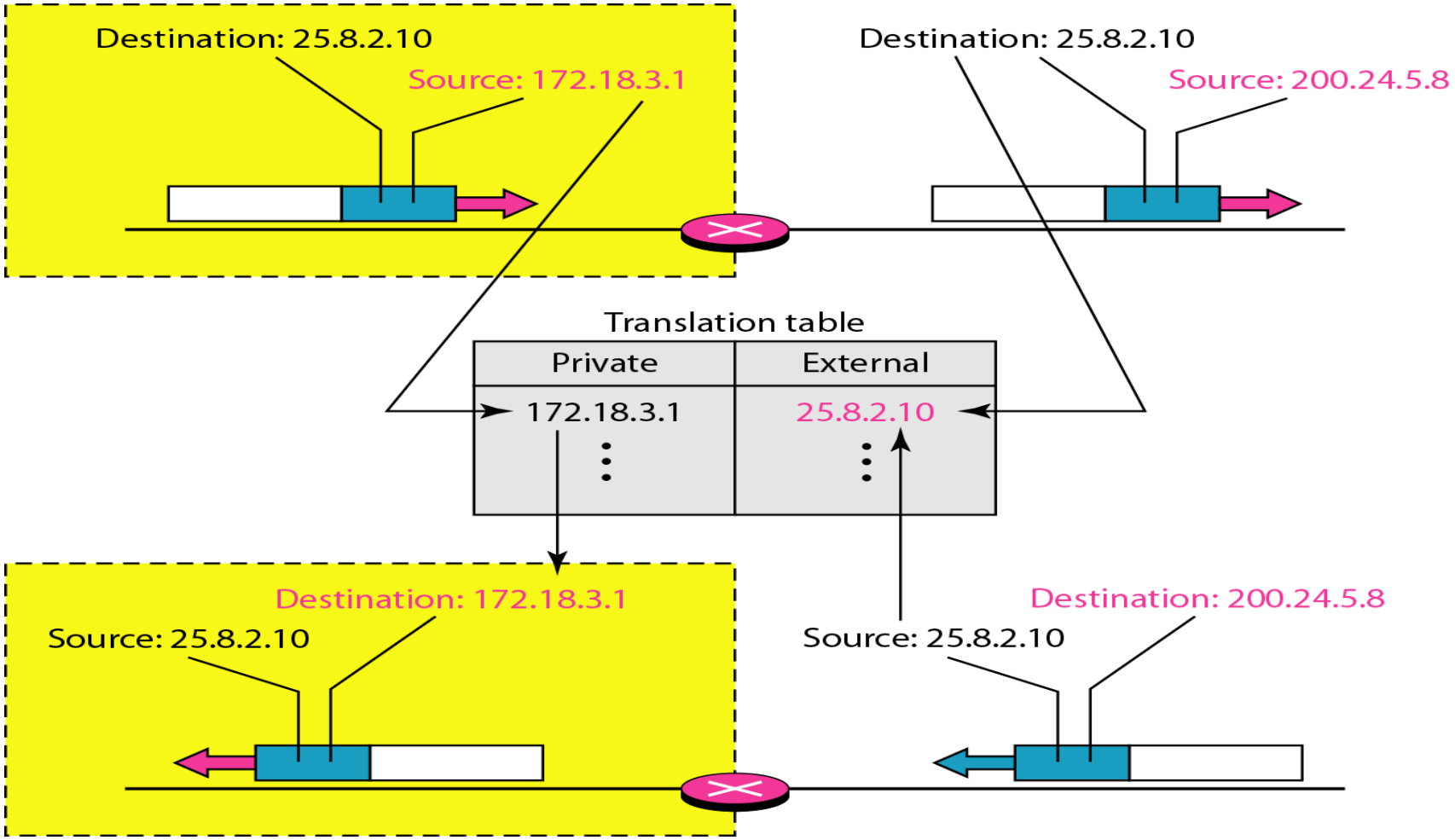
A NAT implementation



Addresses in a NAT



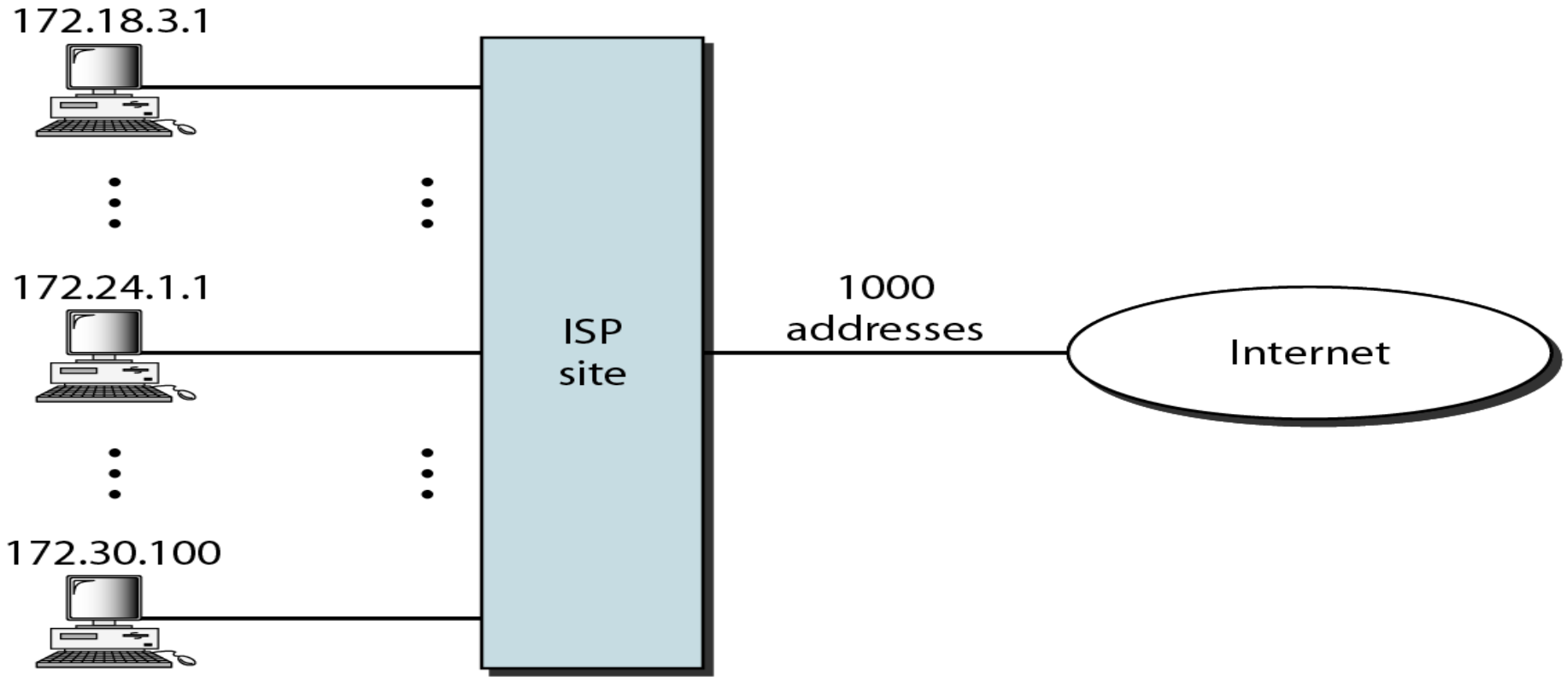
NAT address translation



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
. . .	. . .	. . .	. . .	. . .

An ISP and NAT



NETWORK DEVICES

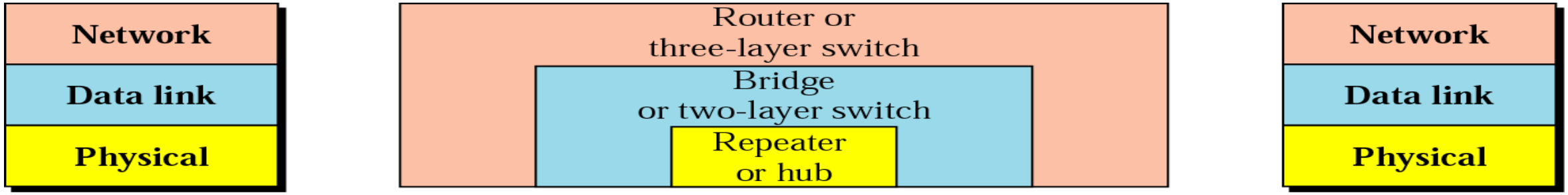
Introduction

- LAN may need to cover more distance than the media can handle effectively, or
- Number of stations may be too great for efficient frame delivery or management of the network
- An *internetwork* or *internet* is two or more networks connected for exchanging resources
- Common devices used: repeaters, bridges, routers and gateways

Connecting Devices

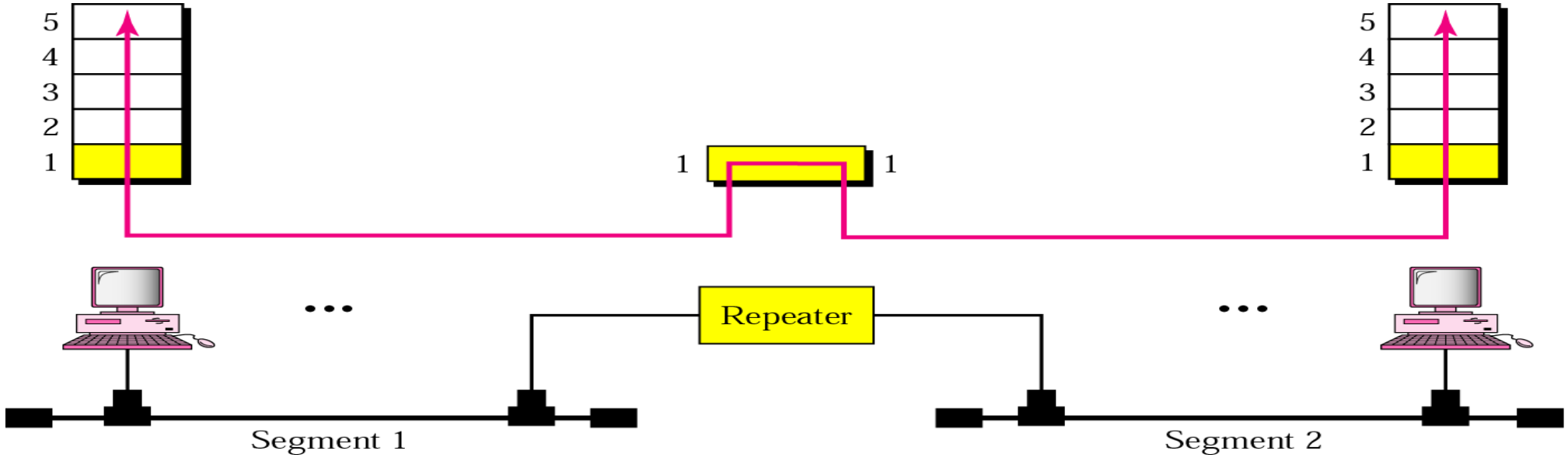
- Five types:
  - Repeaters
  - Hubs
  - Bridges
  - Routers, and three-layer switches
- Repeaters and hubs – layer one of Internet model
- Bridges and two-layer switches – first two layers
- Routers and three-layer switches – first three layers

Connecting Devices



Repeaters

- Operate only in physical layer
- Connects two segments of the same LAN
- Both segments must be of the same protocol
- Only forwards frames; does not filter

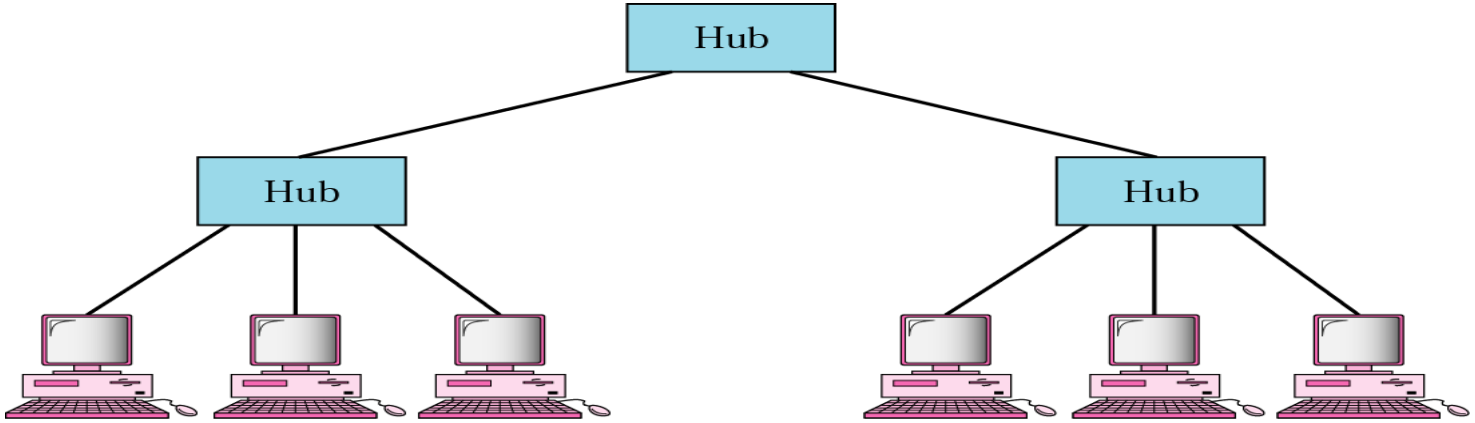


Repeaters

- Solves attenuation issues by extending the physical length of the network
- Receives signal before too weak or corrupted, regenerates the original pattern, sends a refreshed copy
- Positioned so signal reaches it *before* any noise changes the meaning of the bits
- Does not amplify; creates a copy, bit for bit, at the original strength

Hubs

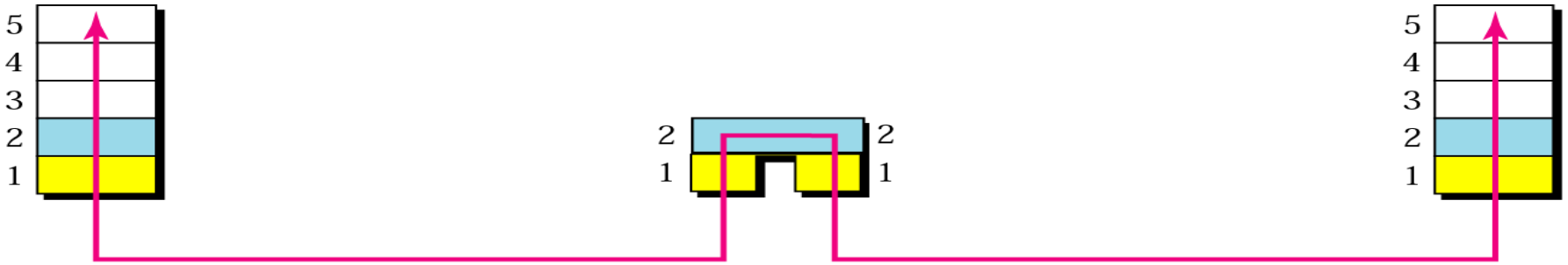
- Actually a multiport repeater
- Connects stations in a physical star topology
- Also may create multiple levels of hierarchy to remove length limitation of 10Base-T



Bridges

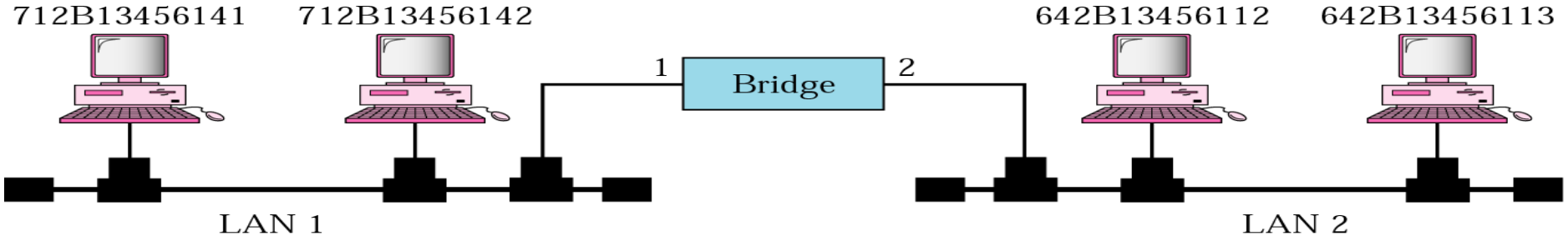
- Operate in both physical and data link layers
- Used to divide a network into smaller segments
- May also relay frames between separate LANs
- Keeps traffic from each segment separate; useful for controlling congestion and provides isolation, as well as security
- Checks address of frame and only forwards to segment to which address belongs

Bridges

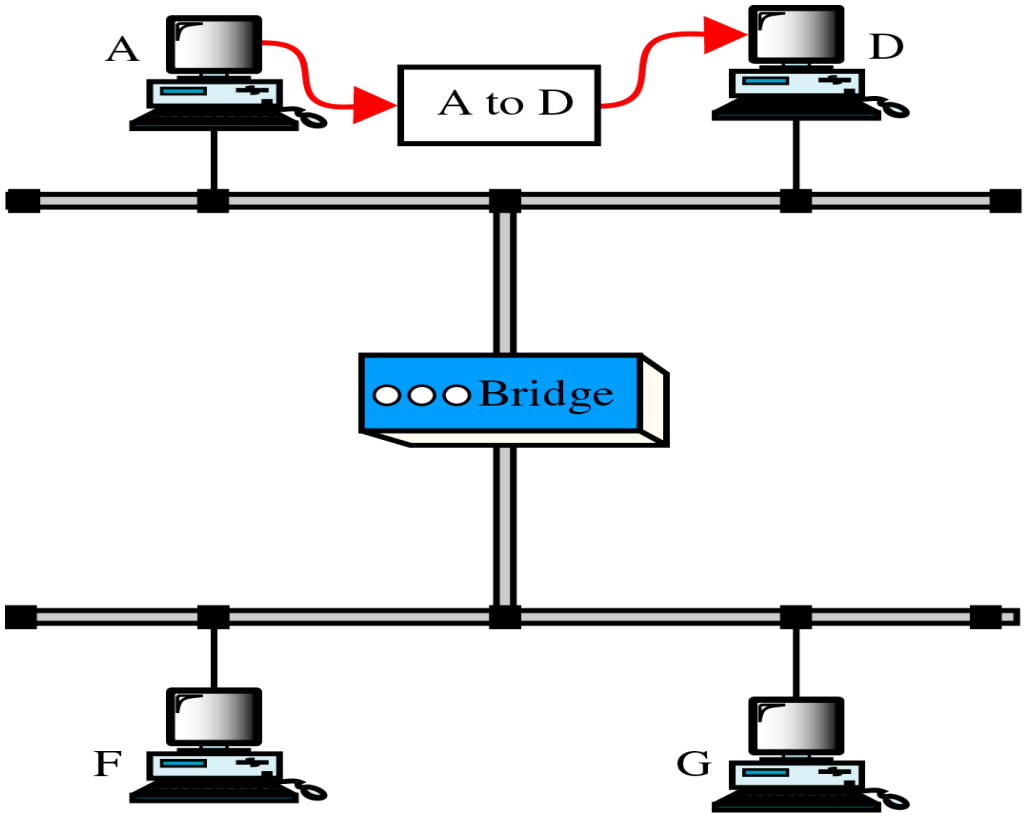


Address	Port
712B13456141	1
712B13456142	1
642B13456112	2
642B13456113	2

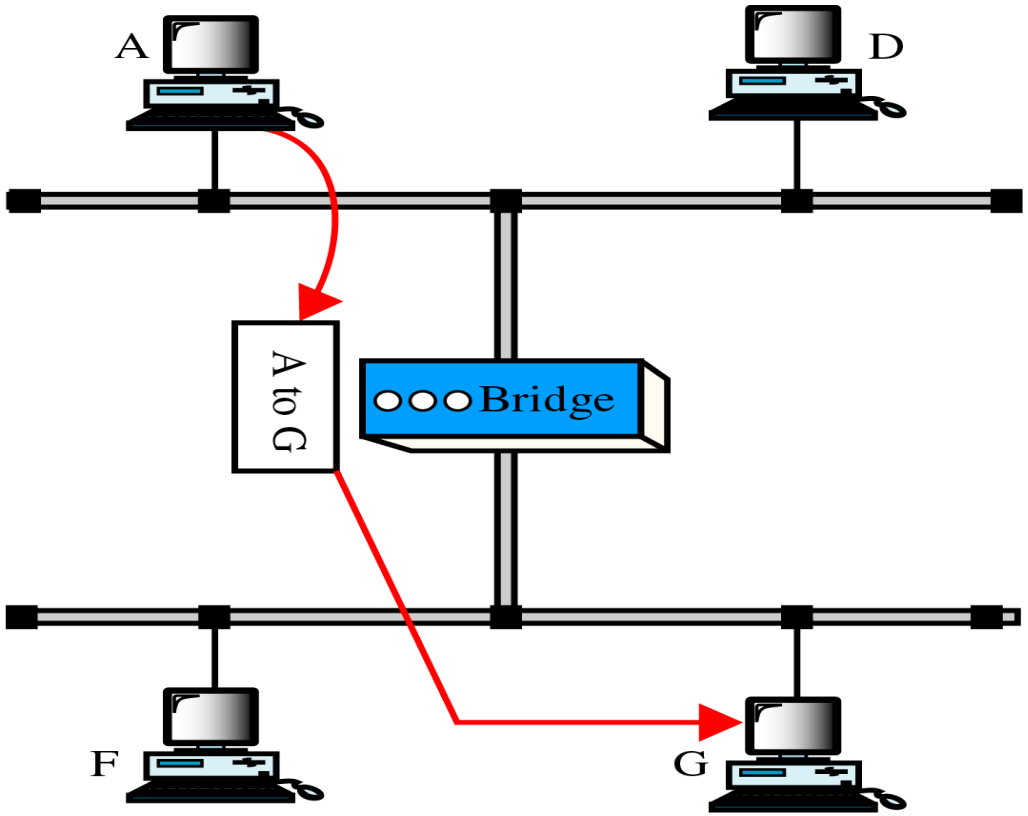
Bridge Table



Function of a Bridge



a. A packet from A to D

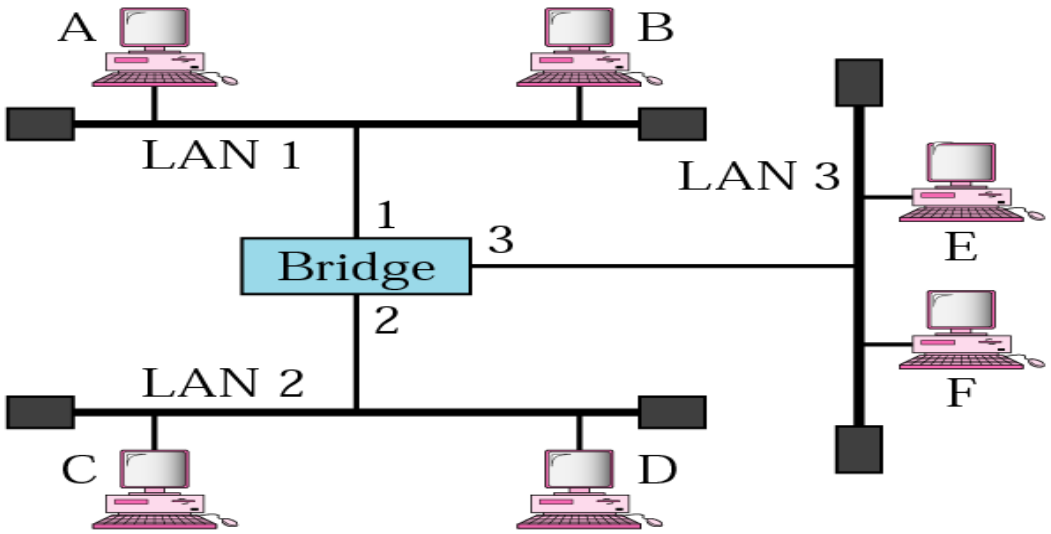


b. A packet from A to G

Transparent Bridges & Learning Bridges

- Builds table by examining destination and source address of each packet it receives
- Learning bridges
  - If address not recognized, packet is relayed to all stations
  - Stations respond and bridge updates routing table with segment and station ID info
  - Changes on the network are updated as they occur

Learning Bridges



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

Address	Port
A	1
E	3

c. After E sends a frame to A

Address	Port
A	1
E	3
B	1

d. After B sends a frame to C

Spanning Tree

- Redundant bridges may be installed to provide reliability
- To prevent infinite looping of packets between bridges, a spanning tree algorithm is used to identify any redundant paths
- Path with lowest cost will be identified and used as the primary route that communications will be routed through; in the event of blocking or bridge failure, secondary routes may be used

Source Routing

- Sender of packet defines bridges and routes that packet should take
- Complete path of bridge IDs and destination address is defined *within* the frame
- Bridge routing table is not used
- Designed to be used with Token Ring LANs

Issues with Bridges Connecting Different LANs

- Frame format – differences in frame structure, fields used (e.g. Ethernet to Token Ring).
- Payload size – size of data encapsulated in the frame may differ.
- Data rates – differences in data rates supported by different protocols; buffering may be necessary.
- Address bit order – differs between protocols.
- Other – differences in handling ACKs, collisions, priority, security, multimedia support, etc.

Two-Layer Switch

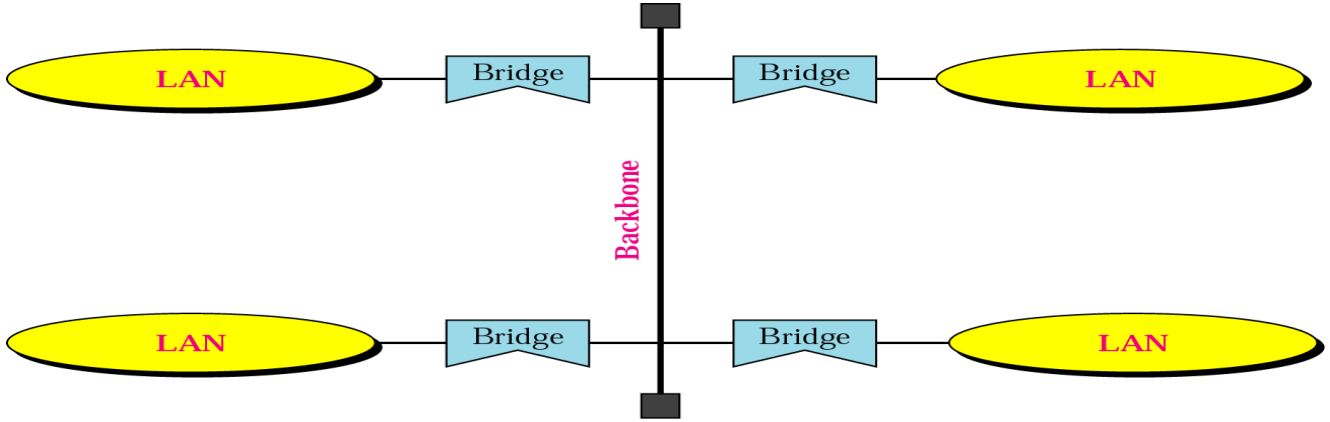
- Performs at the physical and data link layer
- A bridge with many ports designed for faster performance
- Allocates unique port to each station
- No competing traffic
- Routers and three-layer switches covered later

Backbone Networks

- Allows several LANs to be connected
- No station is directly connected to the backbone
- Stations are part of a LAN and the backbone is a LAN itself

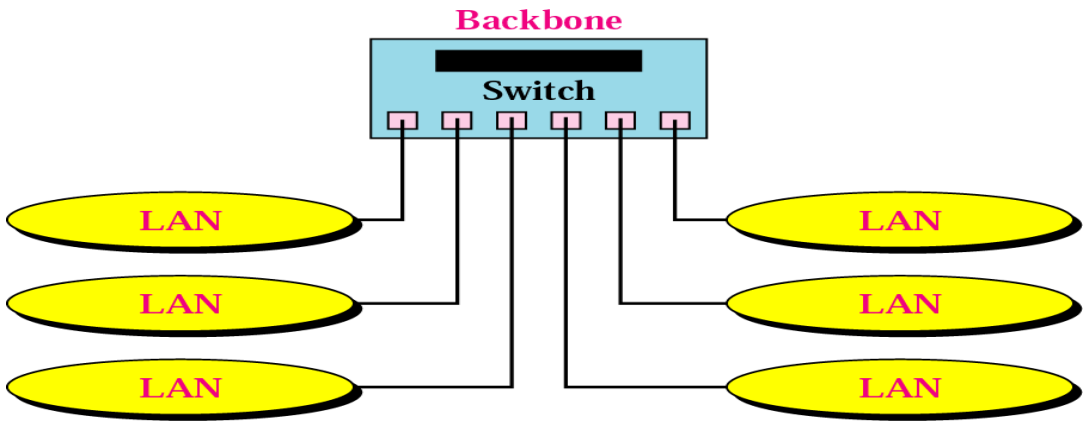
Bus Backbone

- Topology is a bus
- Used in networks such as 10Base5 or 10Base2
- Normally used to connect different buildings or to connect multiple floors within a single building



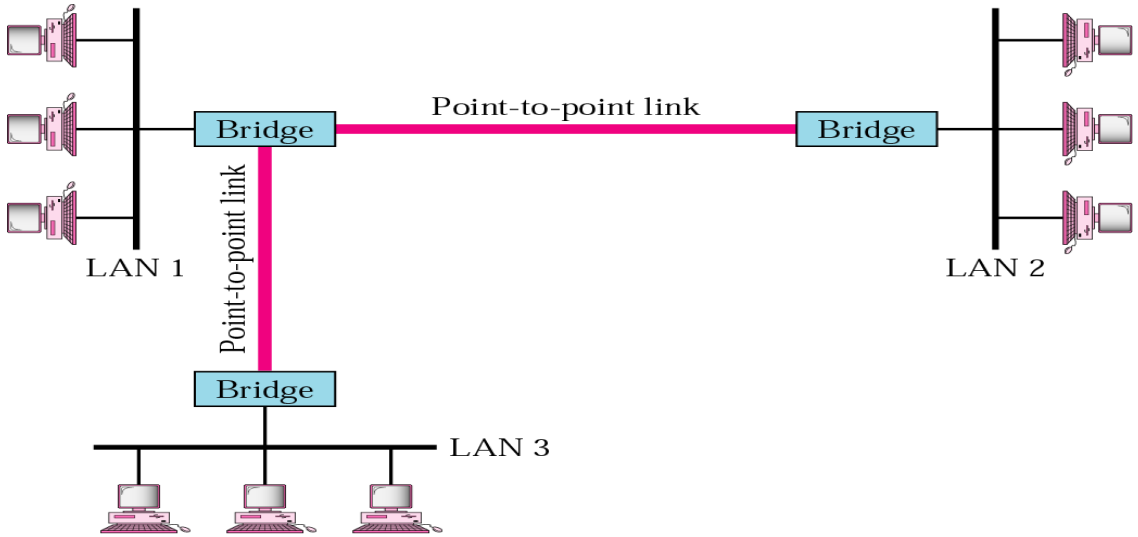
Star Backbone

- Collapsed or switched backbone
- Backbone is just one switch that connects LANs
- Used as distribution backbone inside a building



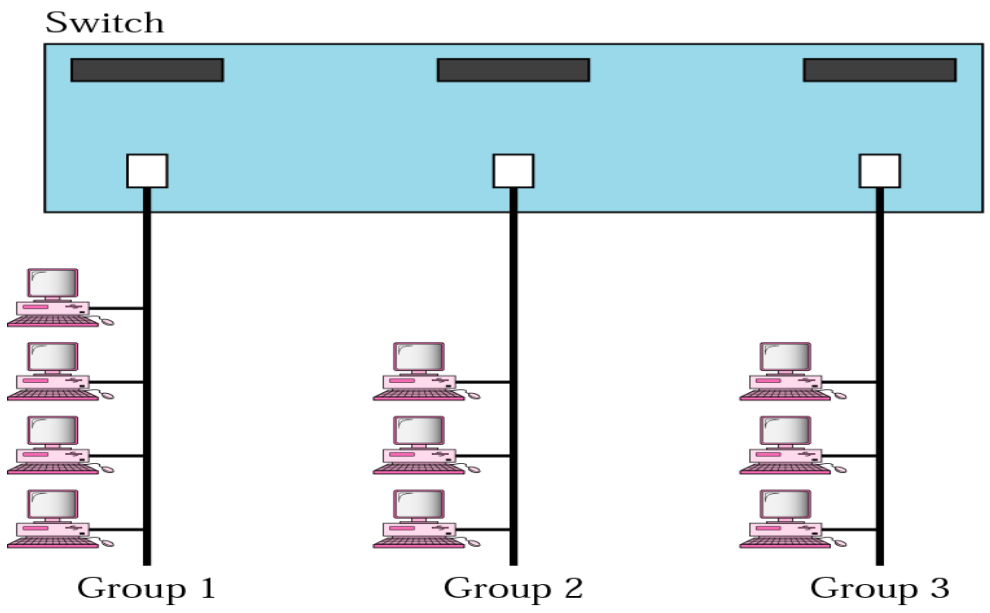
Connecting Remote LANs

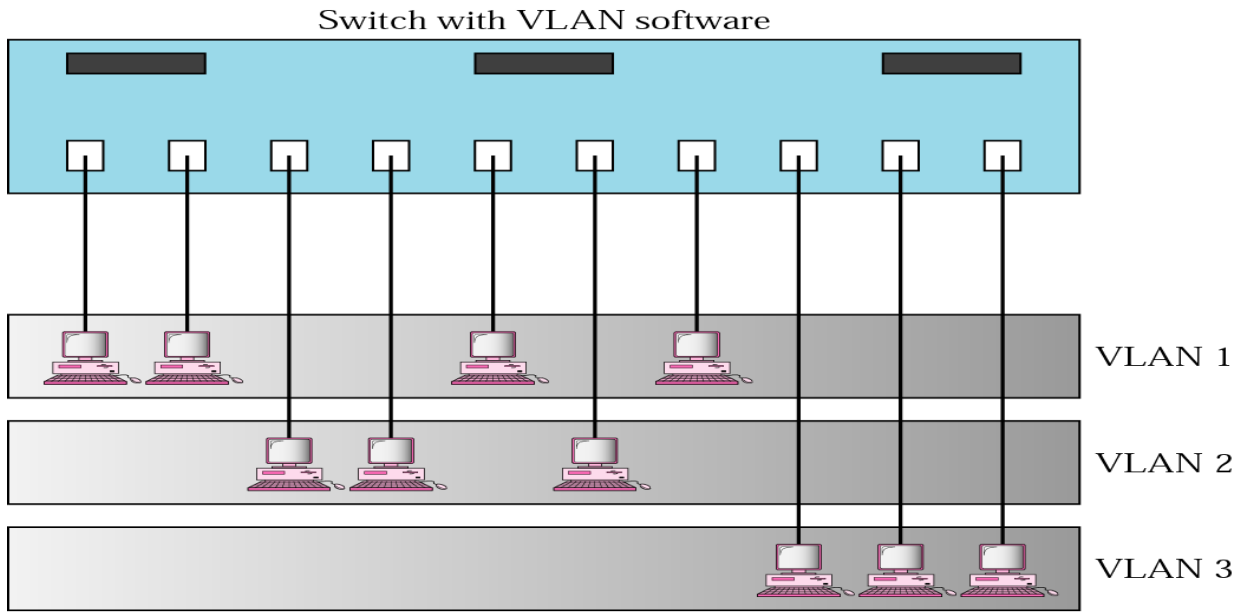
- Remote bridges acting as connecting devices to connect LANs and point-to-point networks, such as leased telephone lines or ADSL lines



Virtual LANs

- Local area network configured by software, not by physical wiring

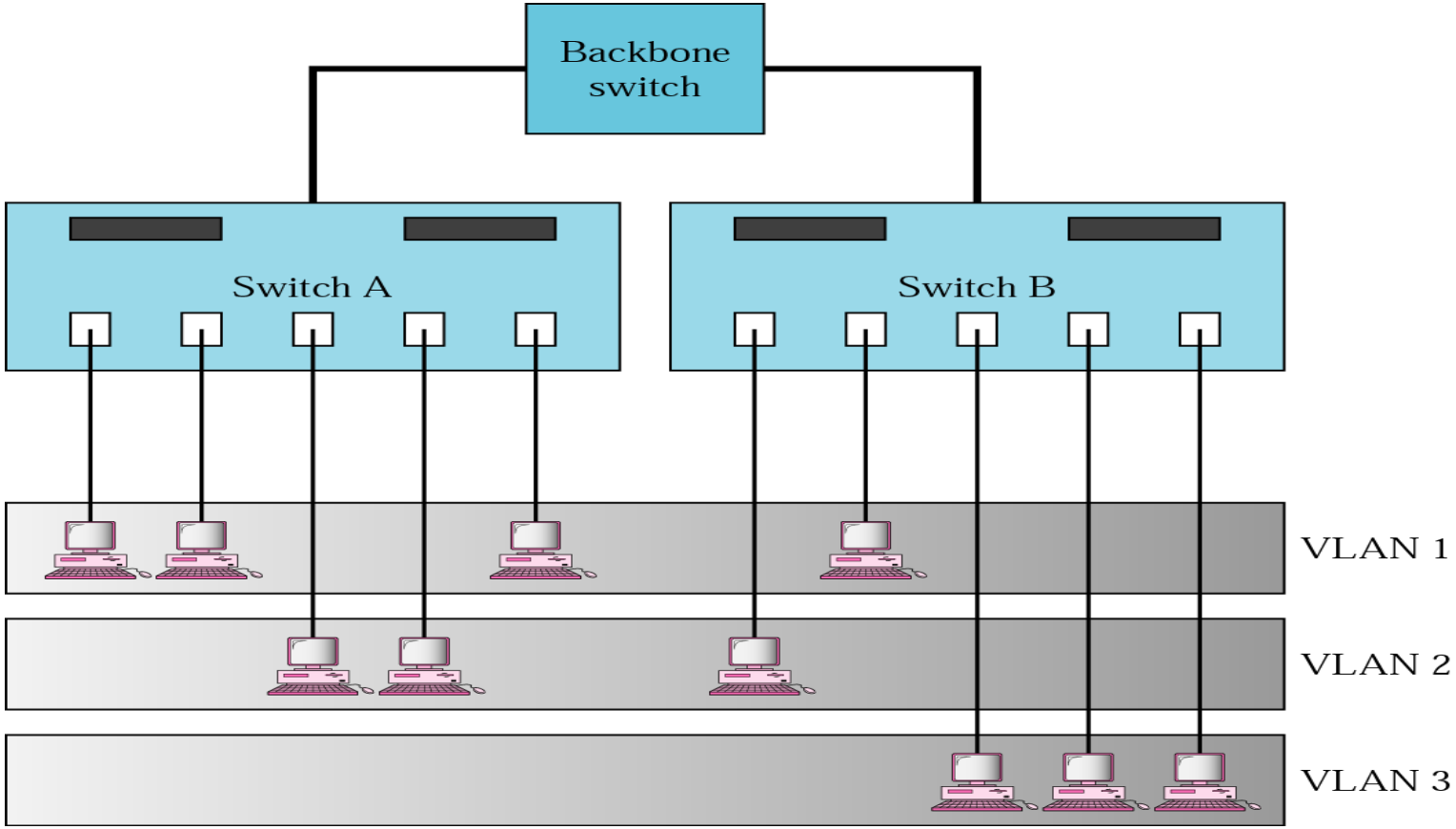




Virtual LANs

- Divides a LAN into logical, instead of physical, segments
- No need to change a physical configuration if changes in workgroups are necessary
- Even allows grouping of stations connected to different switches in a VLAN
- Supports broadcast domains, just as if stations belong to the same physical segment

Switches in a VLAN Backbone



VLAN Membership

- May be classified by
  - Switch port numbers
  - MAC addresses
  - IP addresses
  - IP multicast addresses
  - Combination of two or more

VLAN Configuration

- Manual – network admin manually assigns stations to VLANs at setup and in migration
- Automatic – stations are automatically connected and disconnected based on criteria defined by admin
- Semiautomatic – initialization may be done manually, with migrations automatically

Communication Between Switches

- Must know which station belongs to which VLAN as well as membership of stations connected to other switches
- Tables may be updated by broadcast frames and may be periodically sent amongst switches
- Frame tagging may be used to define the destination VLAN
- TDM may be used to segment channels for each VLAN

Advantages of VLANs

- Cost and time reduction in moving stations from one group to another
- Creation of virtual workgroups
- Security

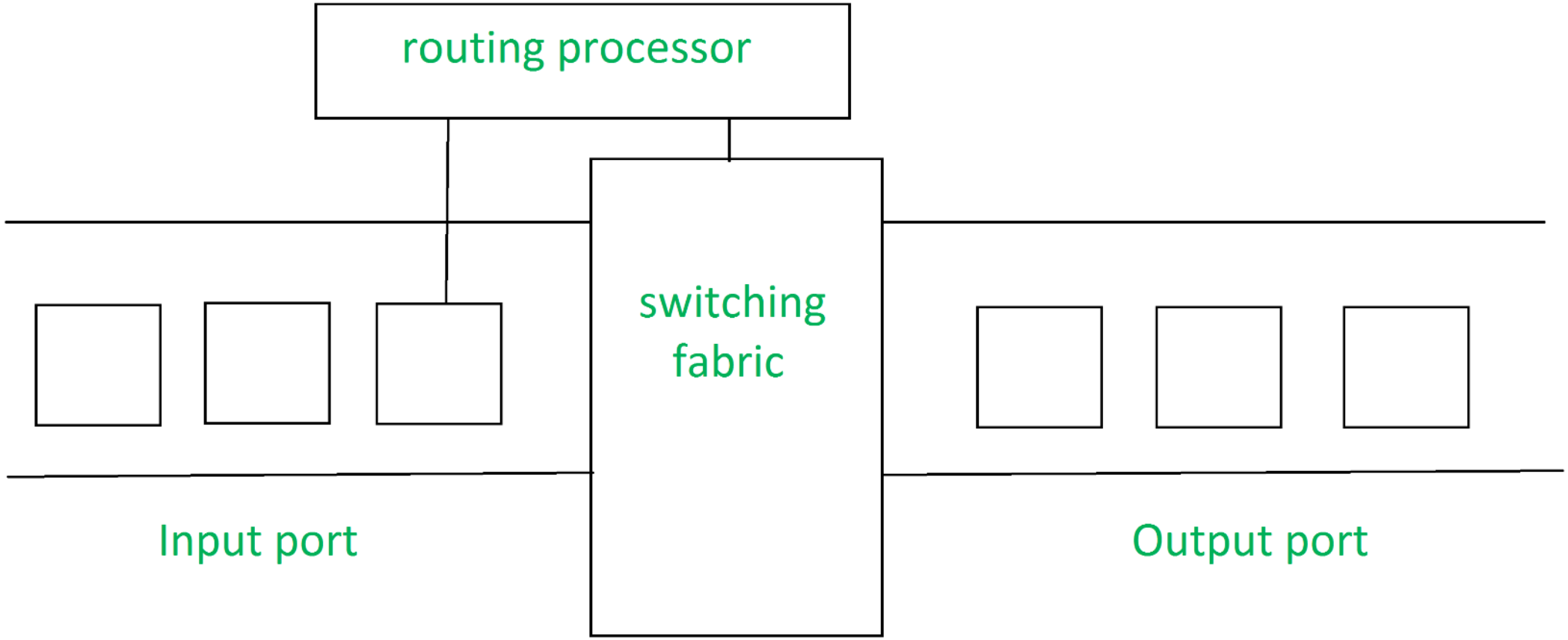
Router

- A **Router** is a networking device that forwards data packets between computer network.
  - Let us understand this by a very general example, suppose you search for *www.google.com* in your web browser then this will be a request which will be sent from your system to the google`s server to serve that webpage, now your request which is nothing but a stream of packets don`t just go the google`s server straightaway they go through a series of networking devices known as router which accepts this packets and forwards them to correct path and hence it reaches to the destination server.

Functions of a Router

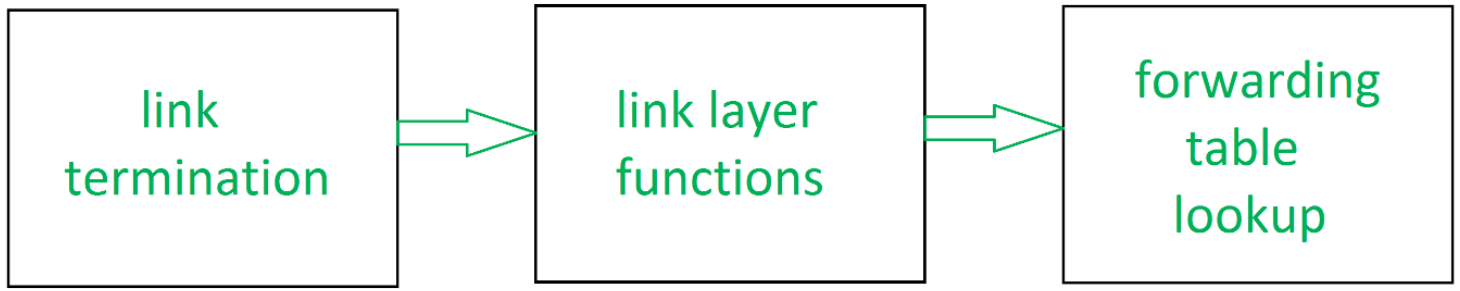
- The router basically performs two major functions:
- **Forwarding**
  - Router receives the packets from its input ports, checks it header, performs some basic functions like checking checksum and then looks upto the routing table to find the appropriate output port to dump the packets onto, and forwards the packets onto that output port.
- **Routing**
  - Routing is the process by which the router ascertains what is the best path for the packet to reach the destination, It maintains a routing table which is made using different algorithms by the router only.

Architecture of a Router



Input Port

- This is the interface by which packets are admitted into the router, it performs sevral key functions as terminating the physical link at router, this is done by the leftmost part in the below diagram, the middle part does the work of interoperating with the link layer like decapsulation, in the last part of the input port the forwarding table is looked up and is used to determine the appropriate output port based on the destination address.



Input port

Switching Fabric

- This is the heart of the Router, It connects the input ports with the output ports. It is kind of a network inside a networking device. The switching fabric can be implemented in a number of ways some of the prominent ones are:
- **Switching via memory:**
  - In this we have a processor which copies the packet from input ports and sends it to the appropriate output port. It works as a traditional cpu with input and output ports acting as input and output devices
- **Switching via bus:**
  - In this implementation we have a bus which connects all the input ports to all the output ports. On receiving a packet and determining which ouput port it must be delivered to, the input port puts a particular token on the packet and transfers it to the bus. All output ports are able to see the packets but it will be delivered to the output port whose token has been put in, the token is then scrapped off by that output port and the packet is forwarded
- **Switching via interconnection network:**
  - This is a more sophisticated network, here instead of a single bus we use 2N bus to connect n input ports to n output ports.

Output Port

- This is the segment from which packets are transmitted out of the router.
- The output port looks at its queuing buffers (when more than one packets have to be transmitted through the same output port queuing buffers are formed) and takes packets, does link layer functions and finally transmits the packets to outgoing link

Routing Processor

- It executes the routing protocols, it works like a traditional CPU.
- It employs various routing algorithm like link-state algorithm, distance-vector algorithm etc. to prepare the forwarding table, which is looked up to determine the forwarding table.

Features of Routers

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- In order to prepare or refresh the routing table, routers share information among each other.
- Routers provide protection against broadcast storms.
- Routers are more expensive than other networking devices like hubs,bridges and switches.
- Routers are manufactured by some popular companies like –
  - Cisco
  - D-Link
  - HP
  - 3Com
  - Juniper
  - Nortel

Routing Table

- The functioning of a router depends largely upon the routing table stored in it.
- The routing table stores the available routes for all destinations.
- The router consults the routing table to determine the optimal route through which the data packets can be sent.
  - A routing table typically contains the following entities –
  - IP addresses and subnet mask of the nodes in the network
  - IP addresses of the routers in the network
  - Interface information among the network devices and channels

Types of Routing tables

- **Static Routing Table**
  - Here, the routes are fed manually and are not refreshed automatically.
  - It is suitable for small networks containing 2-3 routers.
- **Dynamic Routing Table**
  - Here, the router communicates with other routers using routing protocols to determine the available routes.
  - It is suited for larger networks having large number of routers.

Routers - Variety

- A variety of routers are available depending upon their usages. The main types of routers are –
- **Wireless Router** – They provide Wi-Fi connection Wi-Fi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.
- **Broadband Routers** – They are used to connect to the Internet through telephone and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
- **Core Routers** – They can route data packets within a given network, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.

Routers - Variety

- **Edge Routers** – They are low-capacity routers placed at the periphery of the networks. They connect the internal network to the external networks, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.

- **Brouters** – Brouters are specialised routers that can provide the functionalities of bridges as well. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

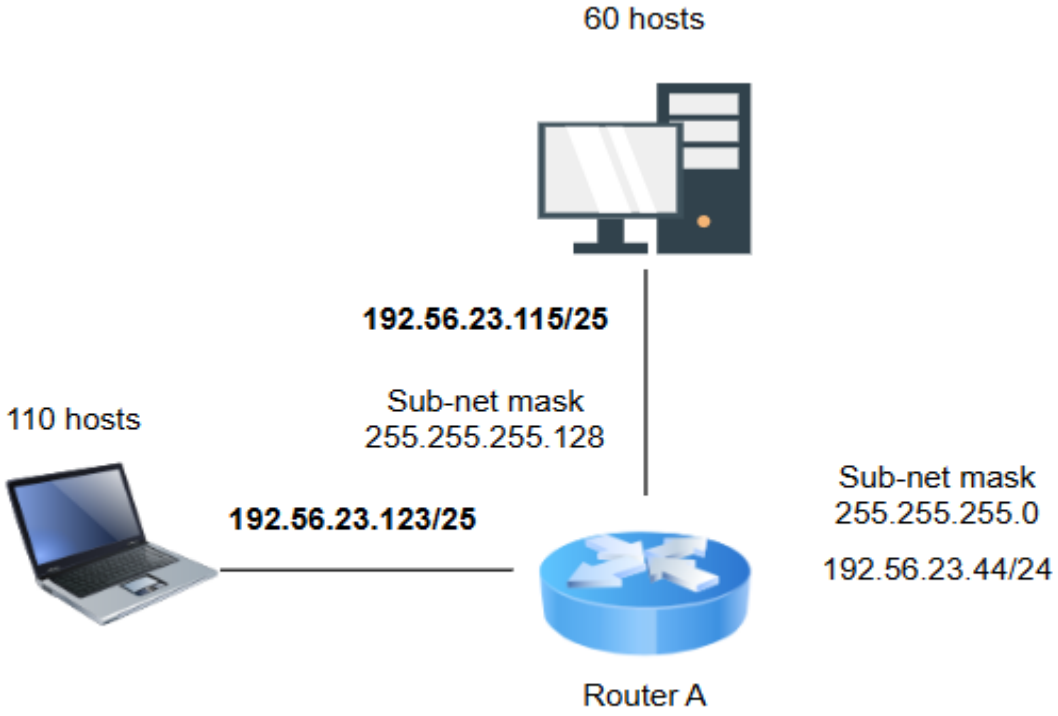
FLSM Vs. VLSM

For subnetting an IP, we use two approaches:

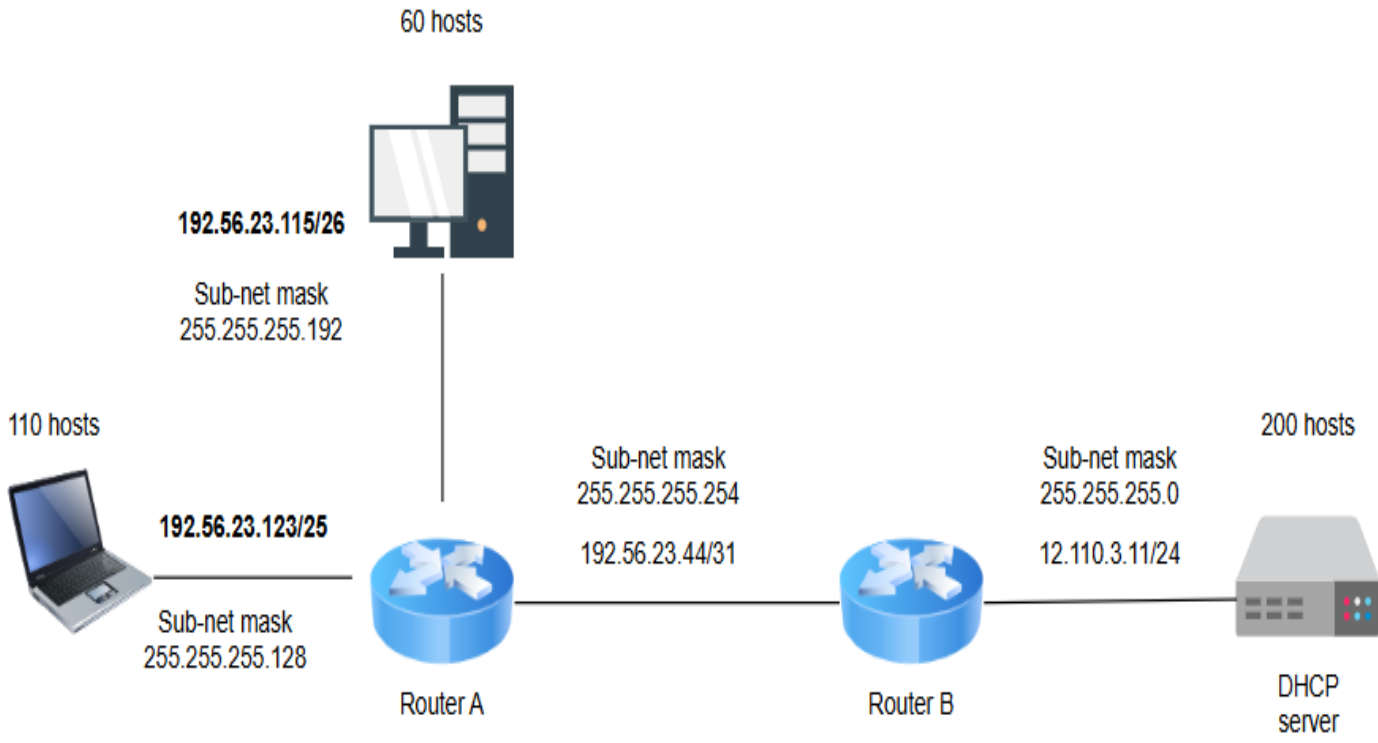
- Fixed length subnet mask (FLSM)
- Variable length subnet mask (VLSM)

- **Fixed-length subnet mask (FLSM)** is a subnet deployment strategy in which a block of IP addresses is split into several subnets of identical length. It is also known as classful subnetting.
- **Variable-length subnet mask (VLSM)** refers to a strategy that allows all the subnetworks to have variable sizes. Network administrators can use VLSM subnetting to divide an IP address space into subnets of various lengths and assign them based on the needs of the network. It is also called classless subnetting.

FLSM Vs. VLSM



Fixed-length subnet masking in a network



The variable-length subnet mask in a network

FLSM Vs. VLSM

Attributes	FLSM	VLSM
Sub-net size	Equal	Variable
Sub-net mask	Same	Different
Number of Hosts	Equal	Variable
Configuration	Easy and simple	Complex
IP addresses wastage	More	Less
Efficiency	Less	More
Routing Protocols	Supports classful and classless	Supports classless
Applications	Suitable for private IP addresses	Suitable for public IP addresses

Advantages of VLSM over FLSM

- More efficient network utilization
- Greater flexibility
- Better scalability
- Improved network performance
- Reduced network management overhead

Disadvantages

- Complexity
- Increased management overhead
- Potential for fragmentation
- Compatibility issues
- Security vulnerabilities & Higher Cost
- Configuration errors

Unit 2 Ends