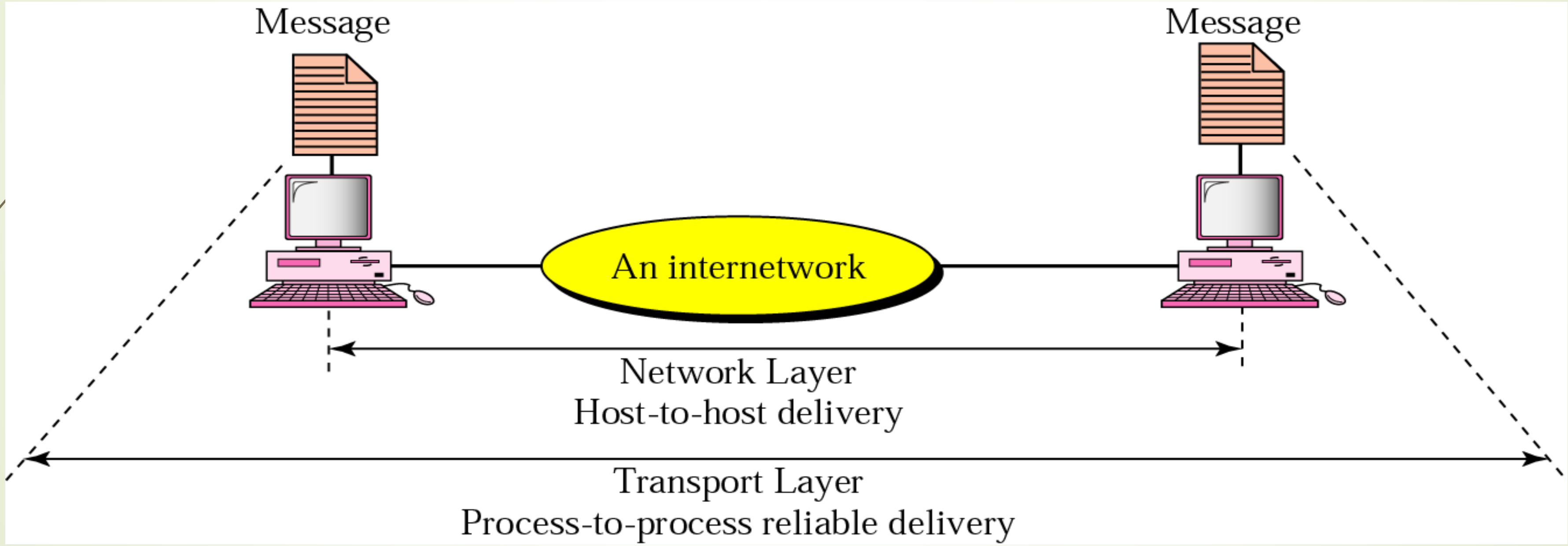
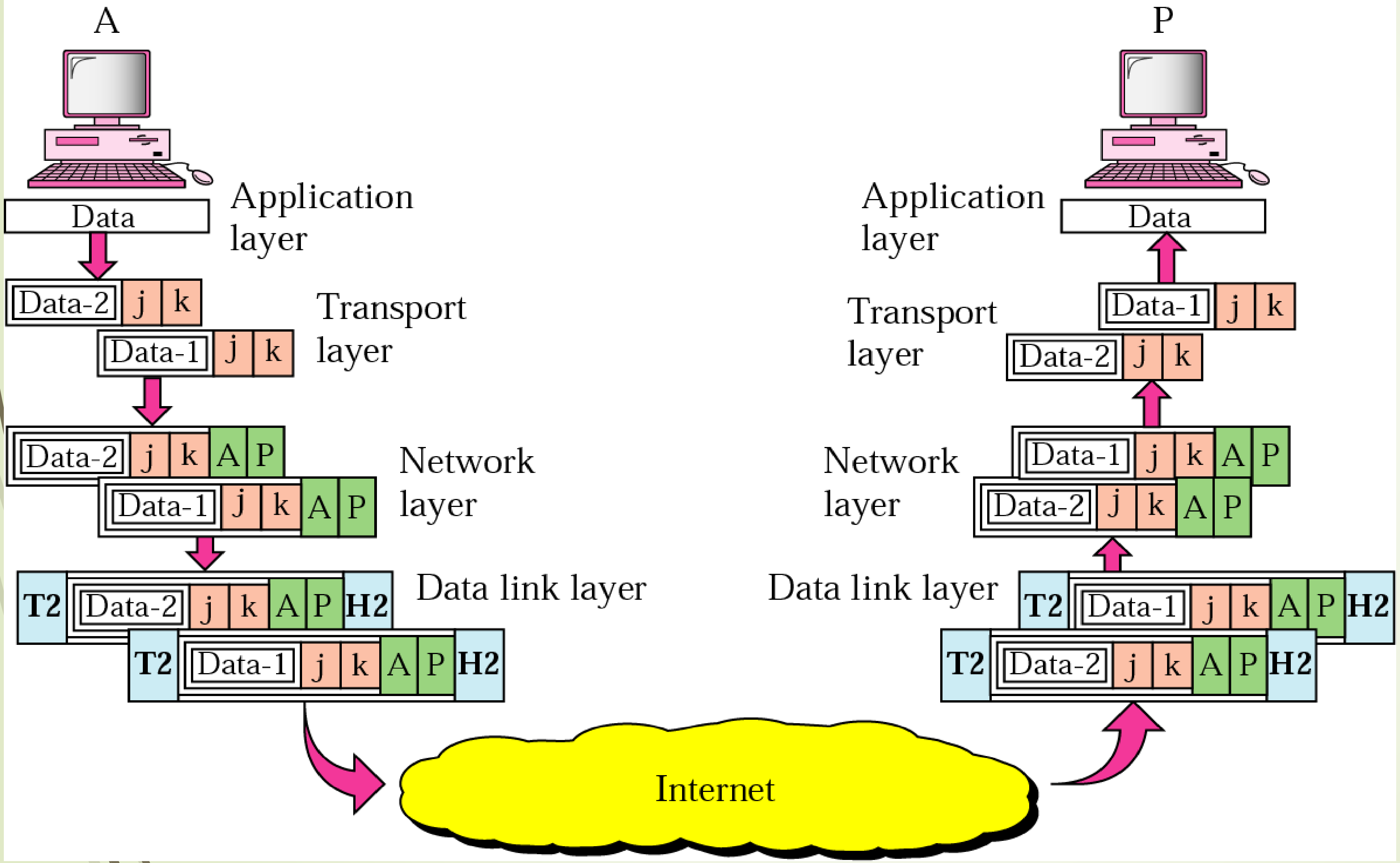
Network Addressing

MAC
IP
Port / Socket


Message
Message
An internetwork
Network Layer
Host-to-host delivery
Transport Layer
Process-to-process reliable delivery

Transport layer communication



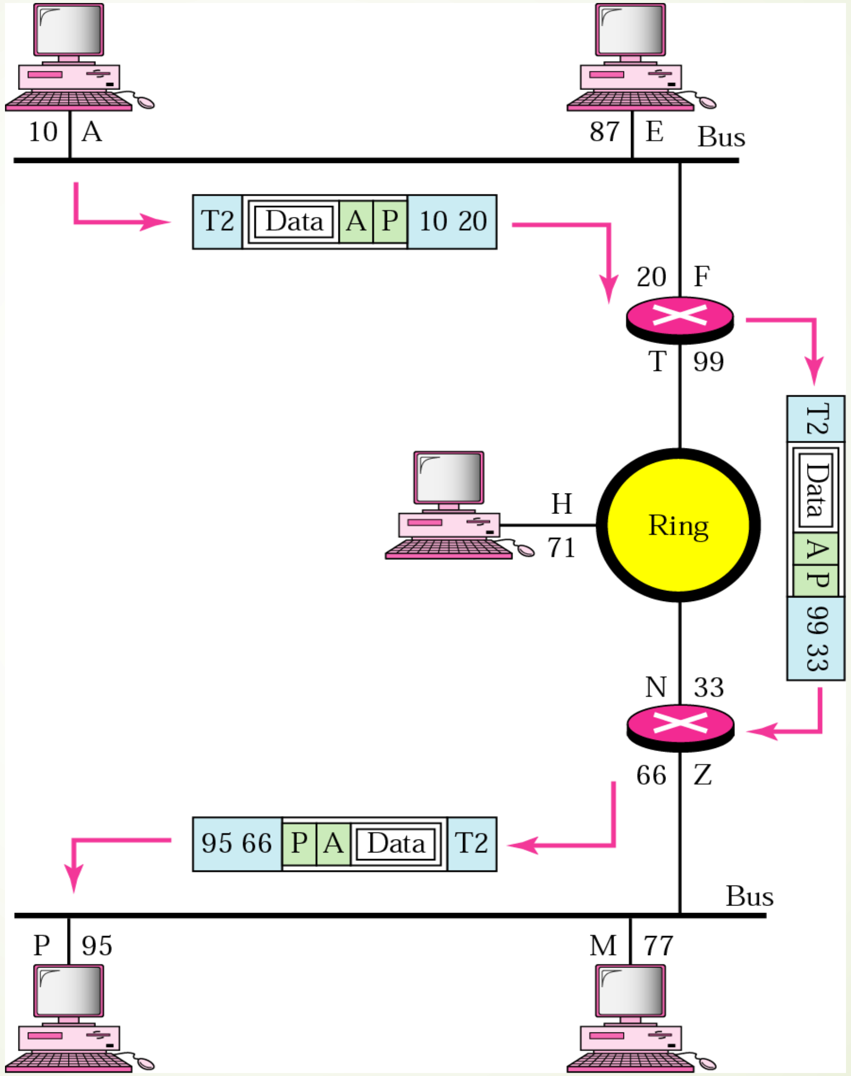
Data coming from the upper layers have **port addresses** j and k

- **j** is the address of the **sending process,**
- **k** is the address of **the receiving process).**

Since the data size is larger than the network layer can handle, the data are split into two packets, each packet retaining the port addresses (**j and k**).

Then in the network layer, network addresses (A and P) **IP address** are added to each packet.

H2 contains **MAC address**



10
A
87
E
Bus
T2
Data
A
P
10 20
20
F
T
99
T2
Data
A
P
99 33
H
71
Ring
N
33
66
Z
95 66
P
A
Data
T2
Bus
P
95
M
77

Difference between MAC Address and IP Address

- Both MAC Address and IP Address are used to uniquely defines a device on the internet.
  - NIC Card's Manufacturer provides the MAC Address
  - Internet Service Provider provides IP Address.
- The main difference between MAC and IP address is that,
  - MAC Address is used to ensure the physical address of computer. It uniquely identifies the devices on a network.
  - IP address are used to uniquely identifies the connection of network with that device take part in a network.

S.NO	MAC ADDRESS	IP ADDRESS
1.	MAC Address stands for Media Access Control Address.	IP Address stands for Internet Protocol Address.
2.	MAC Address is a six bytes hexadecimal address.	IP Address is either four bytes (IPv4) or 16 bytes (IPv6) address.
3.	A device attached with MAC Address can retrieve by ARP protocol.	A device attached with IP Address can retrieve by RARP protocol.
4.	NIC Card's Manufacturer provides the MAC Address.	Internet Service Provider provides IP Address.
5.	MAC Address is used to ensure the physical address of computer.	IP Address is the logical address of the computer.
6.	MAC Address operates in the data link layer.	IP Address operates in the network layer.
7.	MAC Address helps in simply identifying the device.	IP Address identifies the connection of the device on the network.
8.	MAC Address of computer cannot be changed with time and environment.	IP Address modifies with the time and environment.
9.	MAC Address can't be found easily by third party.	IP Address can be found by third party.

Difference between IP address and Port Number

1. **IP address :**

- An Internet Protocol address (IP address) is the logical address of our network hardware by which other devices identify it in a network. IP address uniquely identifies a specific interface on the network. Each device that is connected to internet an IP address is assigned to it for its unique identification.
  - Addresses in IPv4 are 32-bits long example, `12.244.233.165`
  - And Addresses in IPv6 are 128-bits example, `2001:0db8:0000:0000:0000:ff00:0042:7879`

2. **Port Number :**

- The service access point identifiers (SAPIs) used at the transport layer by the transmission control protocol (TCP) and the user datagram protocol (UDP) are called **port** numbers or **socket** numbers
- **Port** number is the part of the addressing information used to identify the senders and receivers of messages in computer networking.
- Different **port** numbers are used to determine what protocol incoming traffic should be directed to.
- **Port** number identifies a specific process to which an Internet or other network message is to be forwarded when it arrives at a server.
- **Ports** are identified for each protocol and It is considered as a communication endpoint.
- **Port** numbers are 16-bit binary values (decimal: 0–65 535) which are assigned by IANA according to the following scheme:
  - 0 to 1023 are restricted port numbers are as they are used by well-known protocol services.
  - 1024 to 49151 are registered port numbers means it can be registered to specific protocols by software corporations
  - 49152 to 65536 are used as private ports means they can be used by anybody.

https://www.geeksforgeeks.org/difference-between-ip-address-and-port-number/?ref=rp

SERIAL NO	IP ADDRESS	PORT NUMBER
01.	Internet Protocol address (IP address) used to identify a host in network.	Port number is used to identify a processes/services on your system
02.	IPv4 is of 32 bits (4 bytes) size and for IPv6 is 128 bits (16 bytes).	The Port number is 16 bits numbers.
03.	IP address is the address of the layer-3 IP protocol.	Port number is the address of the layer-4 protocols.
04.	IP address is provided by admin of system or network administrator.	Port number for application is provided by kernel of Operating System.
05.	ipconfig command can be used to find IP address .	**netstat command** can be used to find Network Statistics Including Available TCP Ports.
06.	IP address identify a host/computer on a computer network.	Port numbers are logical interfaces used by communication protocols.
07.	192.168.0.2, 172.16.0.2 are some of IP address examples.	80 for HTTP, 123 for NTP, 67 and 68 for DHCP traffic, 22 for SSH etc.

TCP (transmission control protocol) UDP (user datagram protocol) **port numbers**

UDP / TCP port number	TCP or UDP as carriage protocol	Application protocol or service
21	**TCP**	FTP (file transfer protocol)
22	**TCP**	SSH (secure shell) remote login protocol and secure forwarding protocol
23	**TCP**	Telnet
25	**TCP**	SMTP (simple mail transfer protocol)
53	**TCP/UDP**	DNS (domain names service)
67	**UDP**	BOOTP (bootstrap protocol) / DHCP (dynamic host configuration protocol) server
69	**UDP**	TFTP (trivial file transfer protocol)
80	**TCP**	Worldwide web HTTP (hypertext transfer protocol)
111	**UDP**	Sun remote procedure call (RPC)
137	**UDP**	NetBIOS name service
161	**UDP**	SNMP (simple network management protocol)
179	**TCP**	BGP (border gateway protocol)
194	**TCP**	IRC (Internet relay chat)
213	**UDP**	Novell IPX (internetwork packet exchange)
443	**TCP**	HTTPS (secure hypertext transfer protocol)
512	**TCP**	Rsh (BSD— Berkeley software distribution) remote shell
513	**TCP**	RLOGIN

Difference between Socket and Port?

- Both **Socket** and **Port** are the terms used in Transport Layer.
- A **port** is a logical construct assigned to **network processes** so that they can be identified within the system.
- A **socket** is a combination of **port** and **IP address**.
- An incoming packet has a port number which is used to identify the process that needs to consume the packet.
- The lowest numbered 1024 port numbers are used for the most commonly used services.
- These ports are called the well-known ports. Higher-numbered ports are available for general use by applications and are known as ephemeral ports

MAC (medium access control) address

- The MAC (medium access control) address used in LANs (local area networks) has 48-bits IEEE unique identifier (also called the MAC address or hardware address).
- The **first three bytes** of the address (most significant bit values) comprise the organisation unique identifier (OUI) of the equipment or network interface card (NIC) manufacturer
- The **last three bytes** are a number unique to each individual piece of hardware. This value is 'burned into' the equipment at its time of manufacture.
- Values appear in the source and destination MAC address fields of the MAC-header
- Ex:
  - 00-10-E3-42-A8-BC is an example of a MAC address.
  - The first 6 hexadecimal digits (3 bytes)
  - the other 6 digits (3 bytes) define the host.

MAC address types

- UNICAST – identify a single destination
- BROADCAST – identify all the computers link in the network address FF-FF-FF-FF-FF-FF
- MULTICAST – identify group of computers (it is not often use)

OUI –Organizational Unique Identifier specify the vendor/manufacturer of the NIC

LAN multicast addresses

NIC Manufacture code

- 00 00 03 SMC
- 00 00 0C CISCO
- 00 00 1B NOVELL
- 00 40 B4 3COM
- 00 AA 00 INTEL
- 10 00 5A IBM
- 08-00-07 Apple
- 08-00-09 HP
- 08-00-2B Compaq

Multicast address	Meaning
01-80-C2-00-00-00	IEEE 802.1d protocol
01-80-C2-00-00-10	IEEE 802.1d All−Bridge−Management
01-00-5E-00-00-01 (224.0.0.1)	All systems on this (IP) subnet
01-00-5E-00-00-02 (224.0.0.2)	All routers on this (IP) subnet
01-00-5E-00-00-05 (224.0.0.5)	All OSPF (open shortest path first) routers
01-00-5E-00-00-06 (224.0.0.6)	All designated OSPF (open shortest path first) routers
01-00-5E-00-00-09 (224.0.0.9)	RIPv2 (routing information protocol) routers
01-00-5E-00-00-0A (224.0.0.10)	IGRP (Cisco interior gateway routing protocol) routers
01-00-5E-00-00-0D (224.0.0.13)	All PIM (protocol independent multicast) routers
01-00-5E-00-01-18 (224.0.1.24)	Microsoft WINS server autodiscovery
01-00-5E-00-01-27 (224.0.1.39)	Cisco PIM rendezvous point announcements
01-00-5E-00-01-28 (224.0.1.40)	Cisco PIM rendezvous point discovery
01-00-5E-00-01-29 (224.0.1.41)	ITU-T H.225 gatekeeper discovery
01-00-5E-00-01-4B (224.0.1.75)	SIP (session initiation protocol) ALL−SIP−Server
01-00-5E-02-7F-FE (224.2.127.254)	SAP (session announcement protocol) announcements
30-00-00-00-00-01	NetBEUI multicast

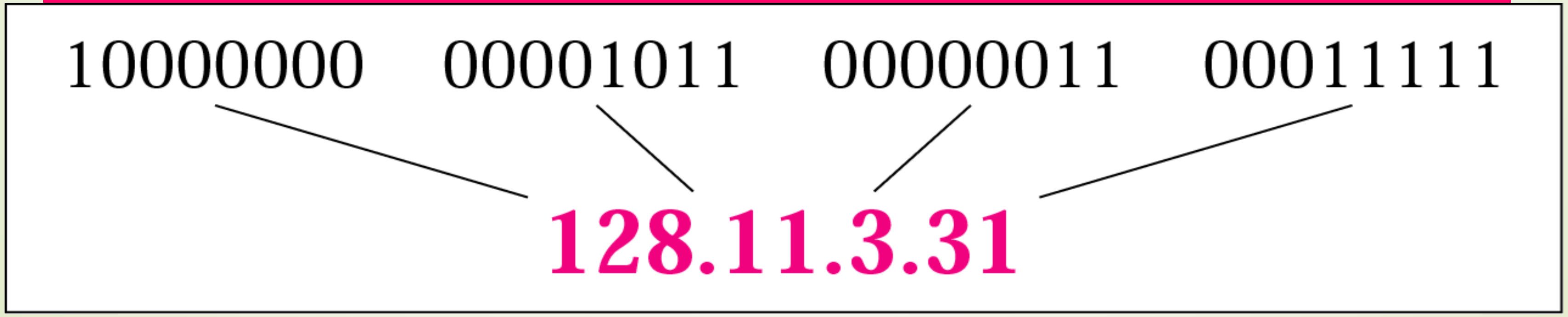
An IP4 address is a 32-bit address.

An IP (Internet Protocol) address

is a unique identifier and universal for a node or host connection on an IP network.

An IP4 address is a 32 bits binary number usually represented as 4 decimal values, each representing 8 bits, in the range 0 to 255 (known as octets) separated by decimal points.

This is known as "dotted decimal" notation.



Example

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 and add dots for separation:

a. 129.11.11.239

b. 249.155.251.15

Example

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 :

a. 01101111 00111000 00101101 01001110
b. 01001011 00101101 00100010 01001110

Every IP address consists of two parts:

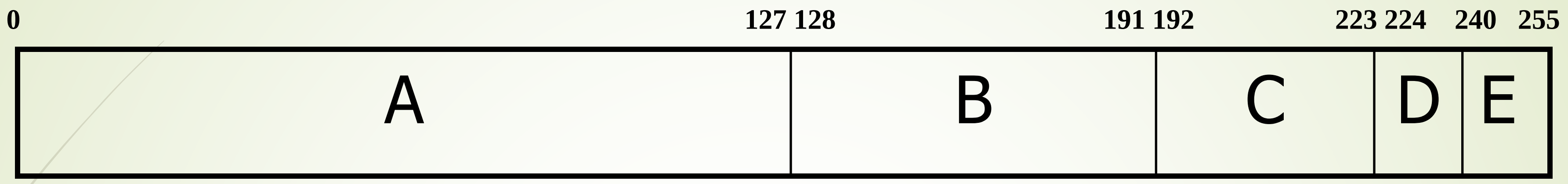
- *one identifying the network*
- *one identifying the node*

The Class of the address and the subnet mask determine:

- *which part belongs to the network address and*
- *which part belongs to the node address.*

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

Finding the class in decimal notation

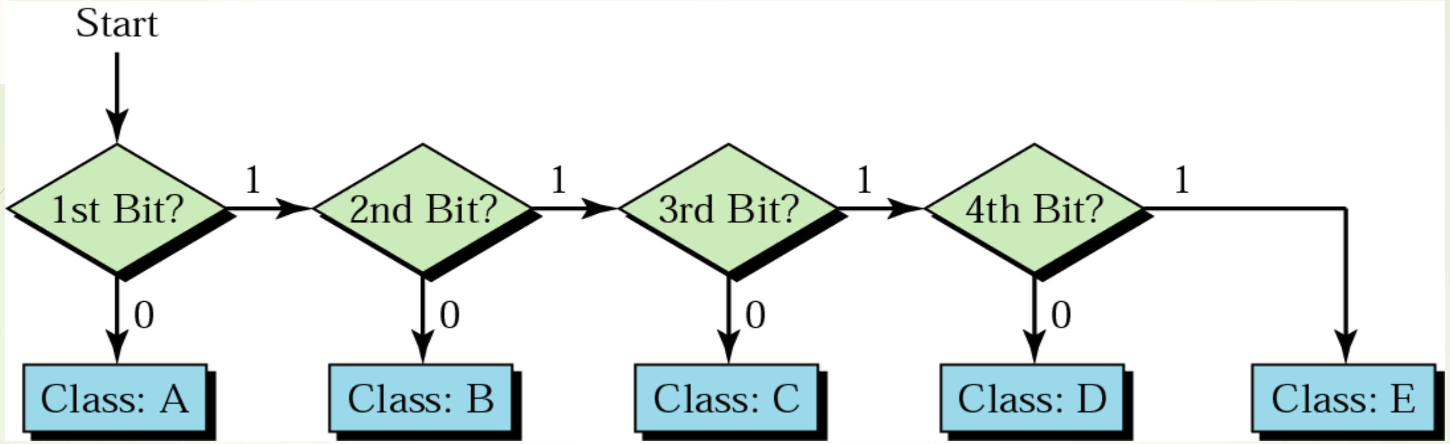


	First byte	Second byte	Third byte	Fourth byte
Class A	**0 to 127**			
Class B	**128 to 191**			
Class C	**192 to 223**			
Class D	**224 to 239**			
Class E	**240 to 255**			

Finding the class in binary notation

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

Finding the address class



Class A addresses begin with 0xxxxxxx, or 1 to 126 decimal.
Class B addresses begin with 10xxxxxx, or 128 to 191 decimal.
Class C addresses begin with 110xxxxx, or 192 to 223 decimal.
Class D addresses begin with 1110xxxx, or 224 to 239 decimal.
Class E addresses begin with 1111xxxx, or 240 to 254 decimal.
Obs:
Addresses beginning with 01111111, or 127 decimal, are reserved for loop back and for internal testing on a local machine.
[You can test this: you should always be able to ping 127.0.0.1, which points to yourself]
Class D addresses are reserved for multicasting.
Class E addresses are reserved for future use. *They should not be used for host addresses.*

Example

Find the class of each address:

a. 00000001 00001011 00001011 11101111

b. 11110011 10011011 11111011 00001111

Solution

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

Find the class of each address:

a. **227**.12.14.87

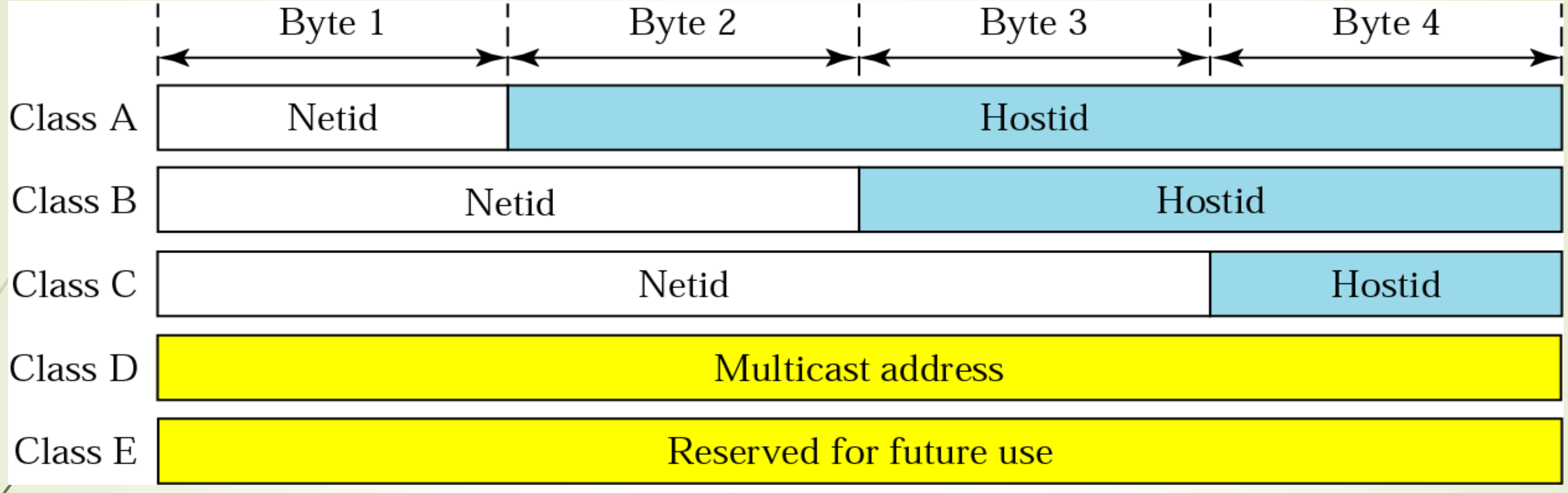
b. **252**.5.15.111

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.

Netid and hostid



Now we can see how the Class determines, by default, which part of the IP address belongs to the network (N) and which part belongs to the node (n).

Class A -- NNNNNNNN.hhhhhhhh.hhhhhhhh.hhhhhhhh

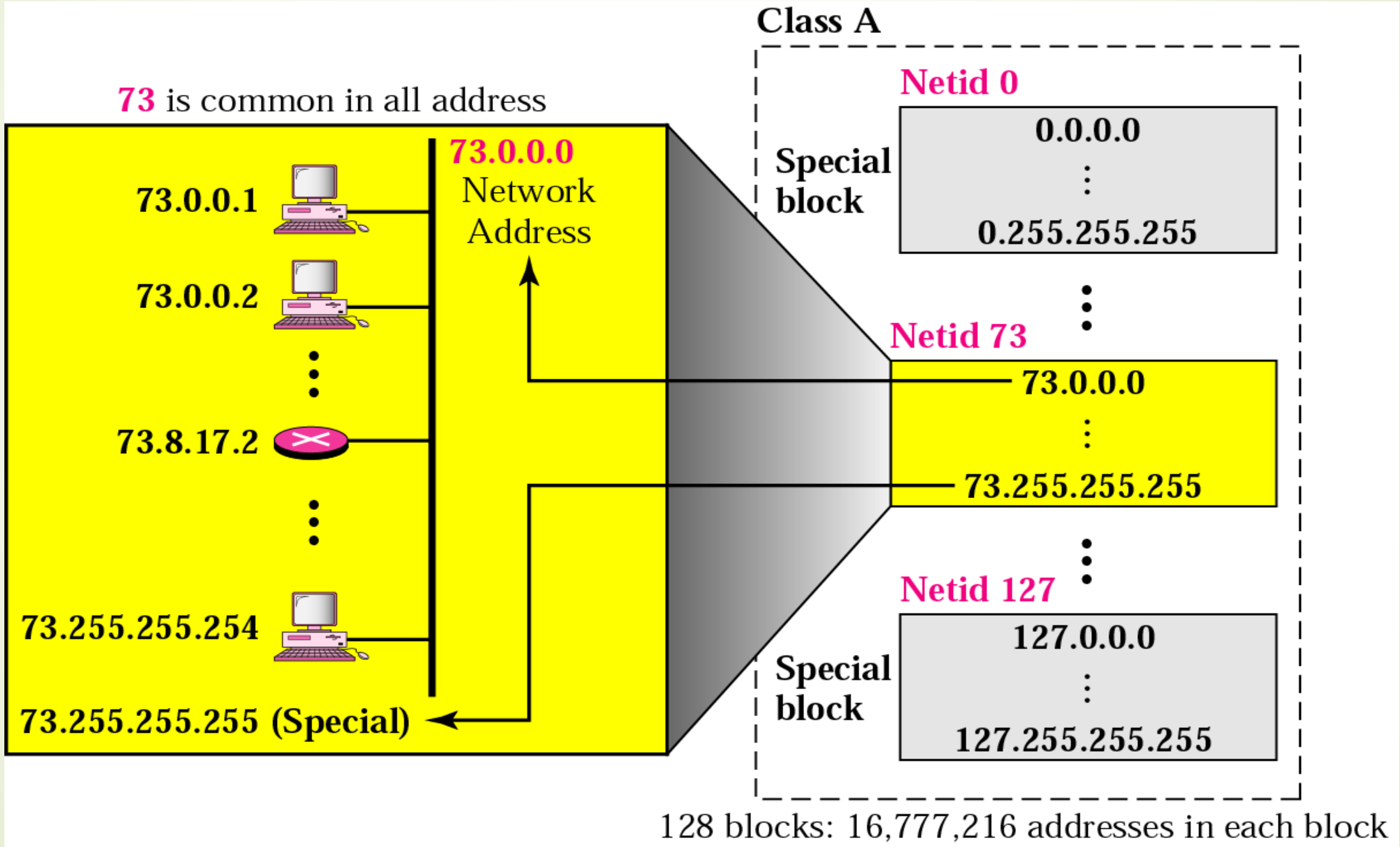
Class B -- NNNNNNNN.NNNNNNNN.hhhhhhhh.hhhhhhhh

Class C -- NNNNNNNN.NNNNNNNN.NNNNNNNN.hhhhhhhh

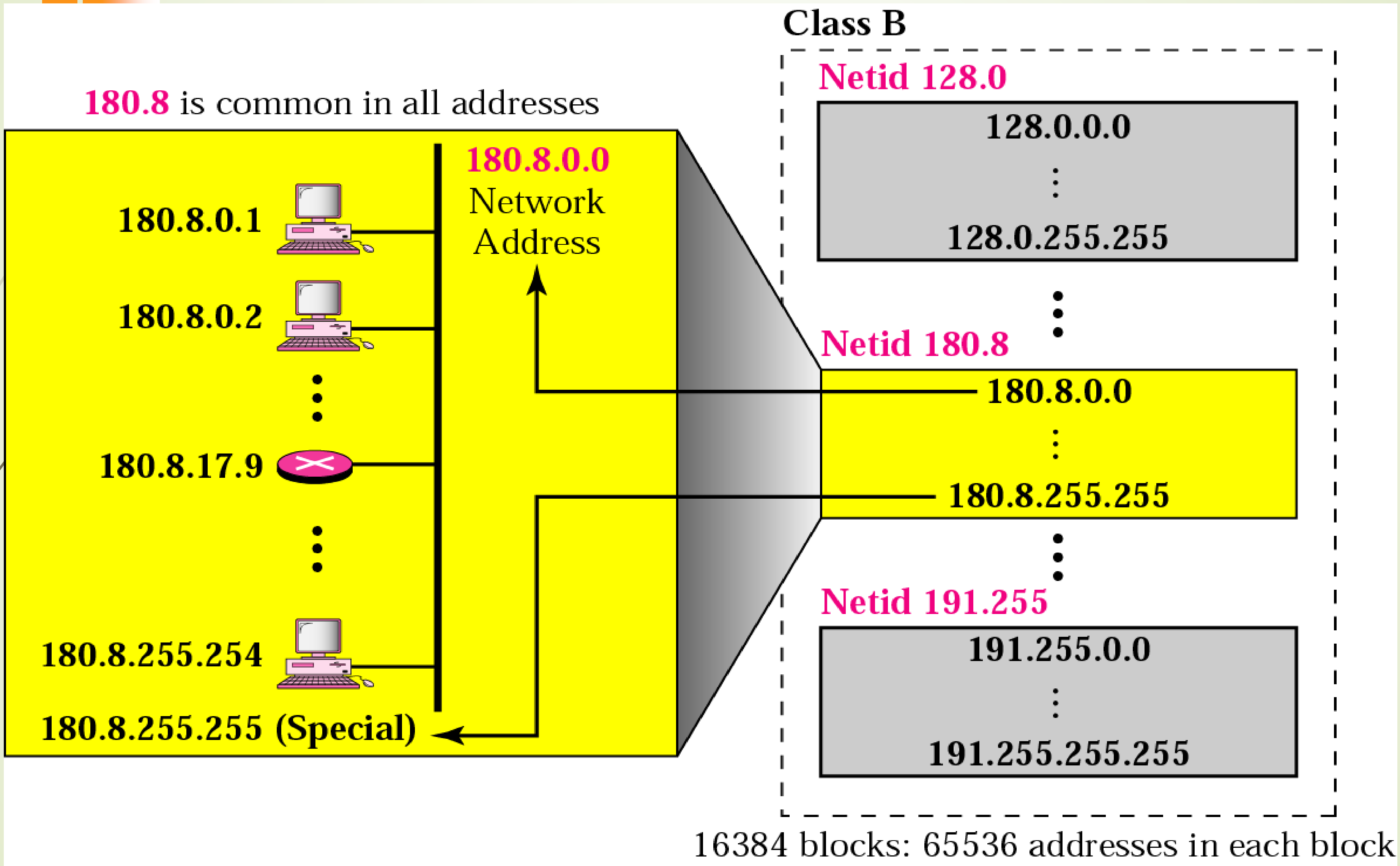
Blocks in class A

Class A is divided into 128 blocks, each block having a different netid.

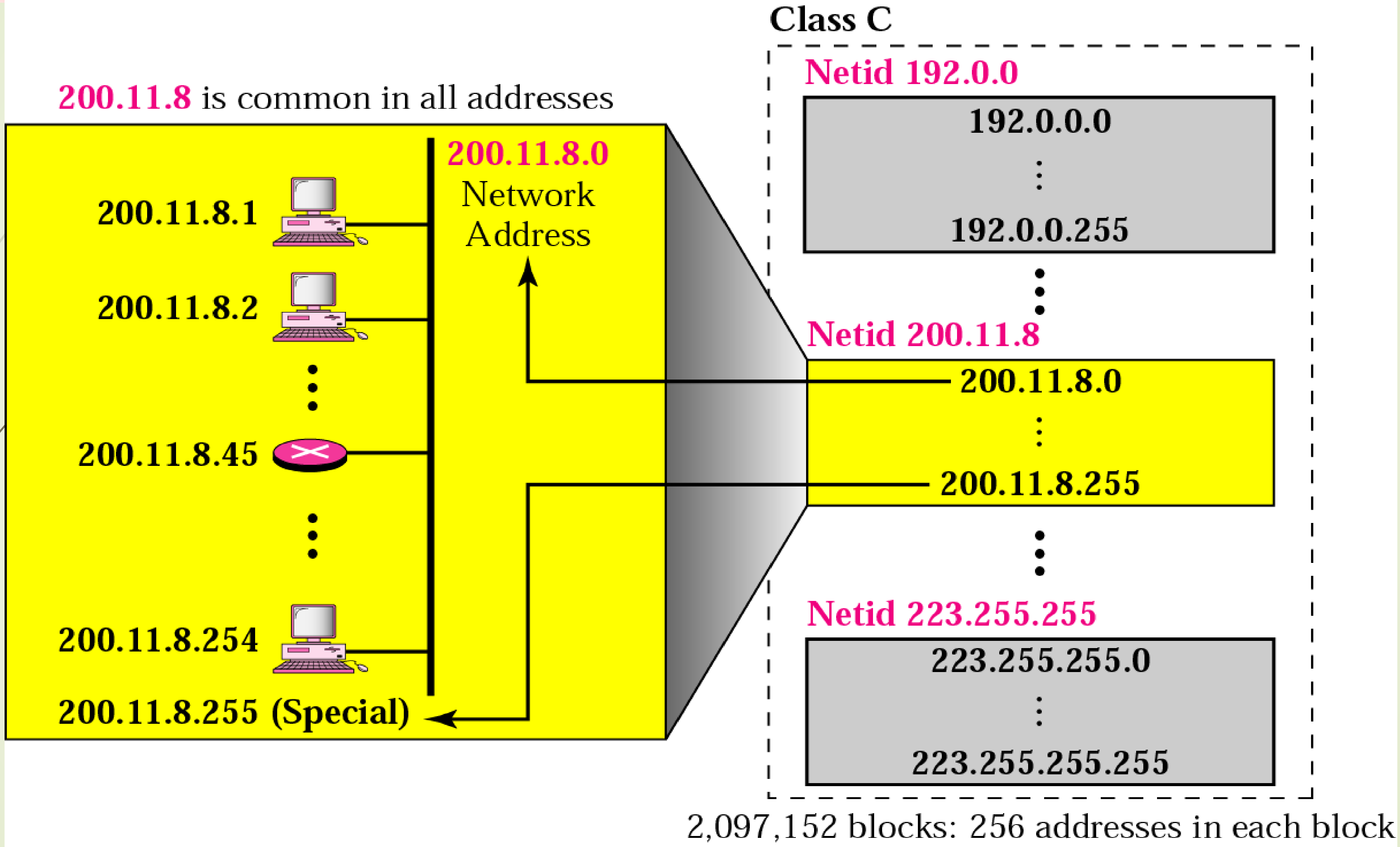
Millions of class A addresses are wasted.



Blocks in class B

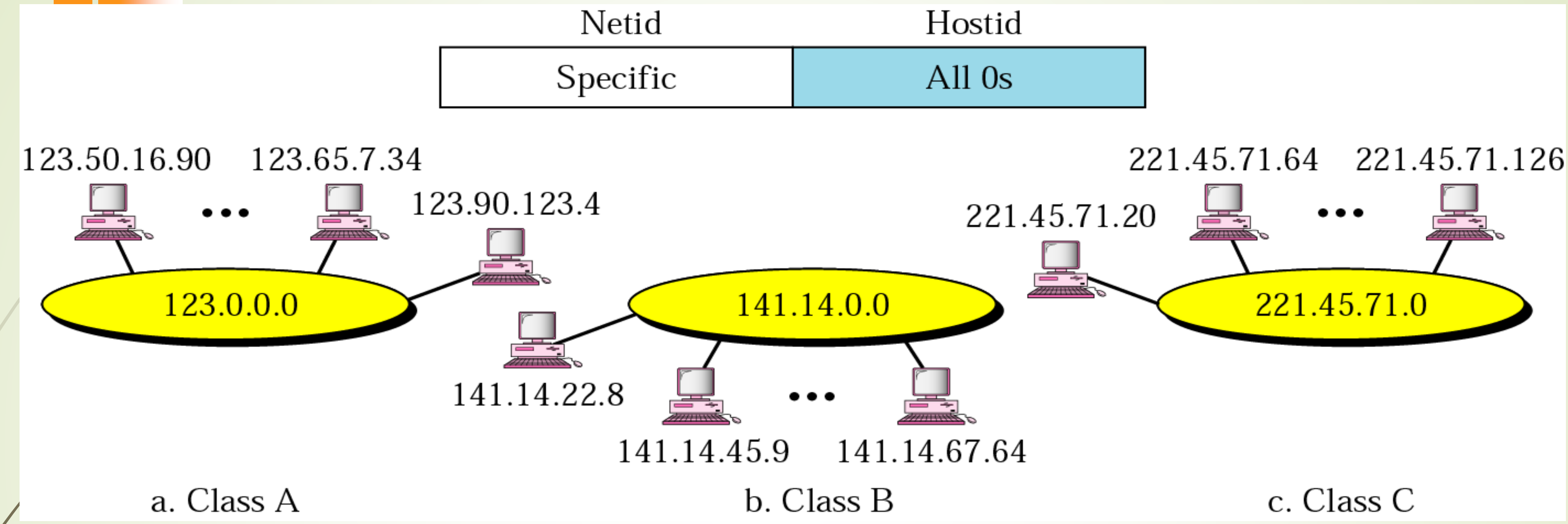


Blocks in class C



The number of addresses in class C is smaller than the needs of most organizations.

Network address



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

*There are reserved three blocks of the IP address space for **private networks**:*

1 * Class A

*Class A network IP address range = **10.0.0.0 - 10.255.255.255***

For one Class A network: Subnet mask = 255.0.0.0

Network address length = 8 bit ; Computer address length = 24 bit

16 * Class B

Class B network IP address range = 172.16.0.0 - 172.16.255.255

...

Class B network IP address range = 172.31.0.0 - 172.31.255.255

For each of the 16 Class B networks: Subnet mask = 255.255.0.0

Network address length = 16 bit ; Computer address length = 16 bit

*Alternatively, 16 * Class B combined*

*Combined Class B networks IP address range = **172.16.0.0 - 172.31.255.255***

For all 16 Class B networks combined: Subnet mask = 255.240.0.0

Network address length = 12 bit ; Computer address length = 20 bit

256 * Class C

Class C network IP address range = 192.168.0.0 - 192.168.0.255

...

Class C network IP address range = 192.168.255.0 - 192.168.255.255

For each of the 256 Class C networks: Subnet mask = 255.255.255.0

Network address = 24 bit ; Computer address = 8 bit

*Alternatively, 256 * Class C combined*

*Combined Class C networks IP address range = **192.168.0.0 - 192.168.255.255***

For all 256 Class C networks combined: Subnet mask = 255.255.0.0

Network address length = 16 bit; Computer address length = 16 bit

Example

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

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

Given the network address 17.0.0.0, find the class.

Solution

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

Windows IP Configuration

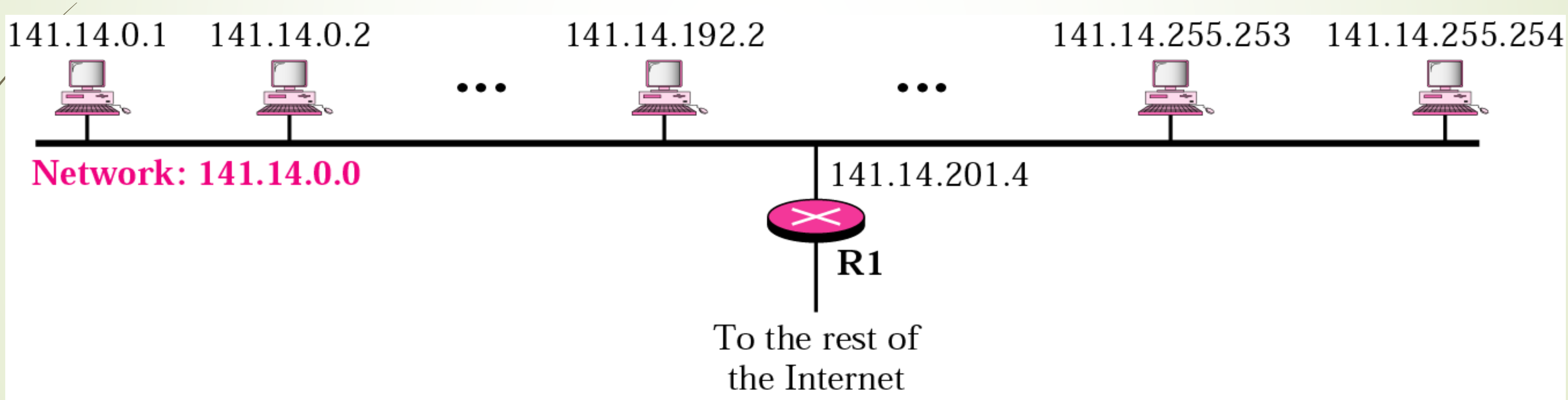
```
        Host Name . . . . . . . . . . . . : computer
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Wireless Network Connection:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless 2200BG Network
 Connection
        Physical Address. . . . . . . . . : 00-15-00-44-2D-2C

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Broadcom NetXtreme Gigabit Ethernet
        Physical Address. . . . . . . . . : 00-14-C2-DF-F2-F4
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.0.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1
        DHCP Server . . . . . . . . . . . : 192.168.0.1
        DNS Servers . . . . . . . . . . . : 192.168.15.1
        Lease Obtained. . . . . . . . . . : 9 decembrie 2006 08:22:01
        Lease Expires . . . . . . . . . . : 12 decembrie 2006 08:22:01

Ethernet adapter VPN:

        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : TAP-Win32 Adapter V8
        Physical Address. . . . . . . . . : 00-FF-41-B3-55-4F
```

A network address is different from a netid.

A network address has both netid and hostid, with 0s for the hostid.

A network with two levels of hierarchy

IP addresses are designed with two levels of hierarchy.



Three level of hierarchy(Sub- netted)

The network needs to be divided into several sub networks

Example :

University has one network address

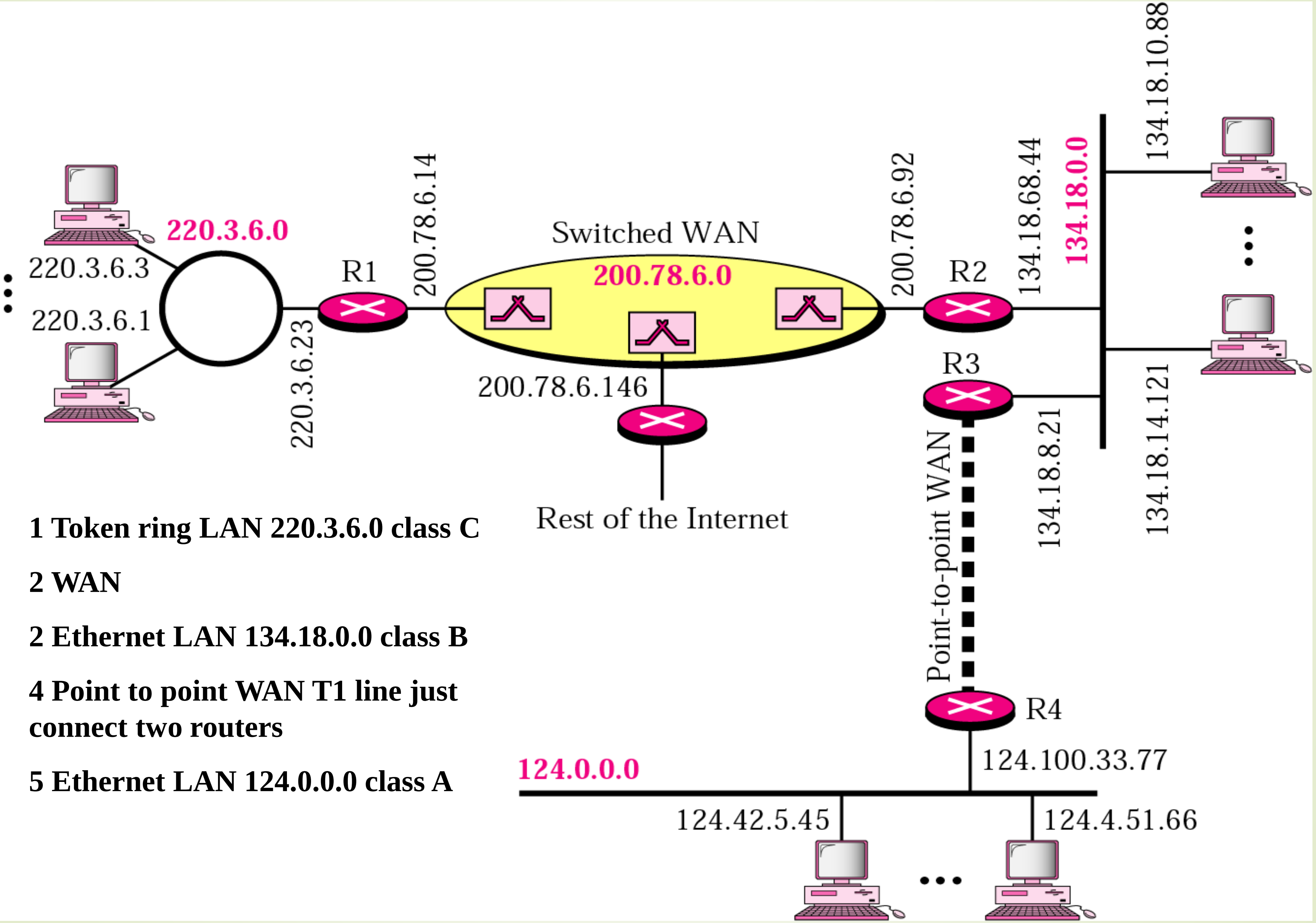
The outside world knows the organization by its network address.

But needs several sub network addresses for different departments

Inside the organization each sub network is recognized by its sub network address

In sub netting, a network is divided into several smaller groups with each sub network having its own sub network address.

Sample internet



1 Token ring LAN 220.3.6.0 class C

2 WAN

2 Ethernet LAN 134.18.0.0 class B

4 Point to point WAN T1 line just connect two routers

5 Ethernet LAN 124.0.0.0 class A

Network address

- Applying a mask to an IP address allows you to identify the **network** and **node** parts of the address.
  - The network bits are represented by the 1s in the mask, and the node bits are represented by the 0s.
  - Performing a bitwise logical AND operation between the IP address and the subnet mask results in the *Network Address* or Number.

For example, using our test IP address and the default Class B subnet mask, we get:

- Class B IP Address
  - 10001100.10110011.11110000.11001000
  - 140.179.240.200
- Default Class B Subnet Mask
  - **11111111.11111111**.00000000.00000000
  - **255.255**.000.000
- Network Address
  - **10001100.10110011**.00000000.00000000
  - **140.179**.000.000

Example

A router outside the organization receives a packet with destination address 190.240.7.91. Show how it finds the network address to route the packet.

Solution

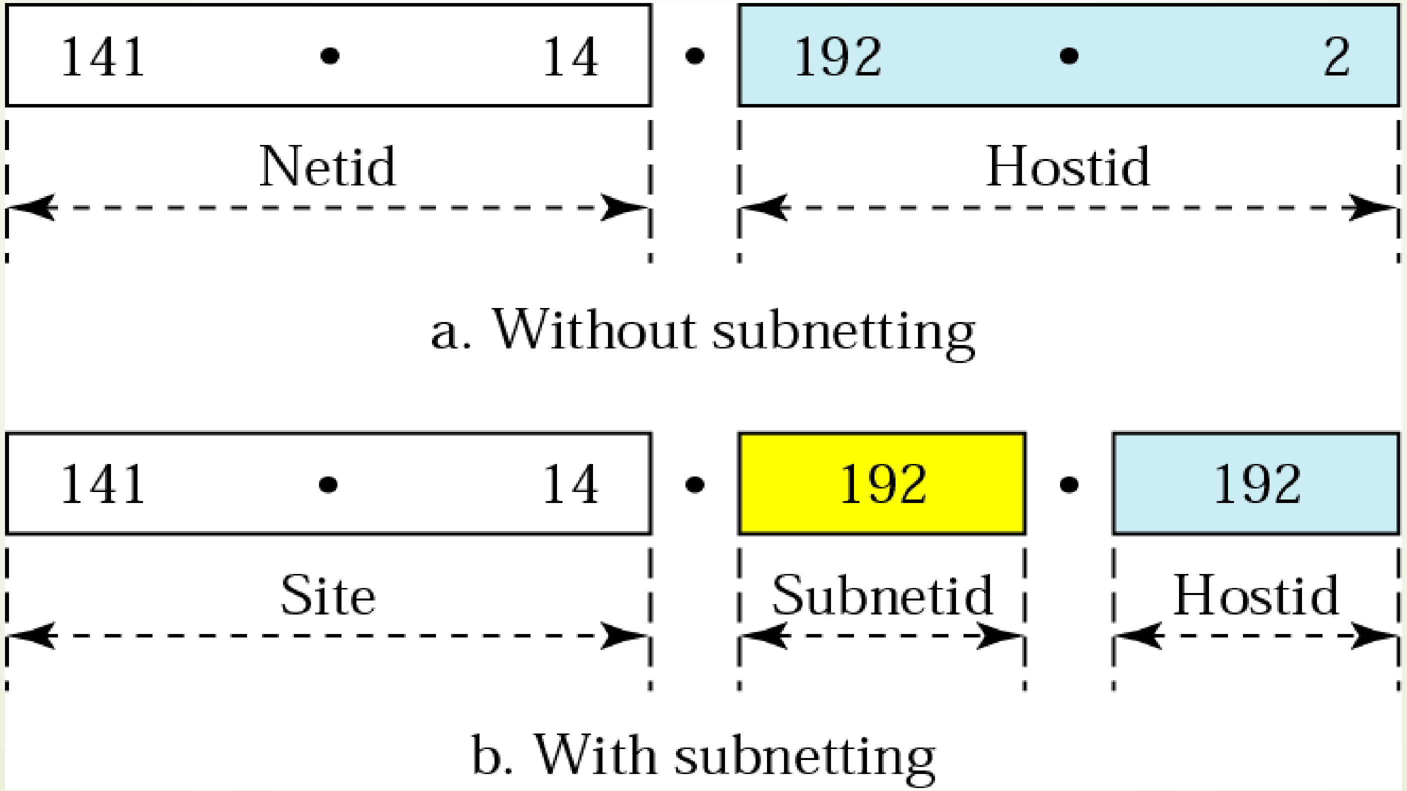
The router follows three steps:

1. The router looks at the first byte of the address to find the class. It is class B.
2. The default mask for class B is **255.255**.0.0. The router ANDs this mask with the address to get **190.240**.0.0.
3. The router looks in its routing table to find out how to route the packet to this destination. Later, we will see what happens if this destination does not exist.

Subnetting

- Subnetting an IP Network can be done for a variety of reasons,
  - including organization,
  - use of different physical media (such as Ethernet, FDDI, WAN, etc.),
  - preservation of address space, and security.
- The most common reason is to control network traffic.
- In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment.
- Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions.
- A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

Addresses in a network with and without sub netting



More Restrictive Subnet Masks

- **Additional bits can be added** to the default subnet mask for a given Class to further subnet, or break down, a network.
  - When a bitwise logical AND operation is performed between the subnet mask and IP address, the result defines the *Subnet Address* (also called the *Network Address* or *Network Number*).
- Initial were some restrictions on the subnet address.
  - ***Node addresses of all "0"s and all "1"s are reserved*** for specifying the local network (when a host does not know its network address) and all hosts on the network (broadcast address), respectively.
  - This also applies to subnets. **A subnet address cannot be all "0"s or all "1"s.** This also implies that a 1 bit subnet mask is not allowed.
  - *This restriction is required because older standards enforced this restriction. Recent standards that allow use of these subnets have superseded these standards, but many "legacy" devices do not support the newer standards.*
- If you are operating in a controlled environment, such as a lab, you can safely use these restricted subnets.

A router inside the organization receives the same packet with destination address **190.240.33.91**

Show how it finds the subnetwork address to route the packet.

255.255.0.0

Default Mask	11111111	11111111	00000000	00000000

16

255.255.224.0

Subnet Mask	11111111	11111111	111	00000	00000000
			3	13	

	190 .	240 .	33 .	91
190.240.33.91	190 .	240 .	0 0 1	00001 . 01011111

The router follows three steps:

1. **The router must know the mask.**
    - **We assume it is /19**
2. **The router applies the mask to the address, 190.240.33.91. The subnet address is 190.240.32.0.**
3. **The router looks in its routing table to find how to route the packet to this destination. Later, we will see what happens if this destination does not exist.**

CIDR -- **C**lassless **I**nter**D**omain **R**outing

- CIDR was invented several years ago to keep the internet from running out of IP addresses.
- The "classful" system of allocating IP addresses can be very wasteful;
  - anyone who could reasonably show a need for more that 254 host addresses was given a Class B address block of 65533 host addresses.
- Even more wasteful were companies and organizations that were allocated Class A address blocks, which contain over 16 Million host addresses!
- Only a tiny percentage of the allocated Class A and Class B address space has ever been actually assigned to a host computer on the Internet.

CIDR notated address

Under CIDR, the subnet mask notation is reduced to a simplified shorthand.

- Instead of spelling out the bits of the subnet mask, it is simply listed as the number of 1s bits that start the mask.
- Example, instead of writing the address and subnet mask as

  192.60.128.0, Subnet Mask 255.255.252.0

  the network address would be written simply as: **192.60.128.0/22**

  which indicates starting address of the network, and number of 1s bits (22) in the network portion of the address.

- If you look at the subnet mask in binary **11111111.11111111.111111**00.00000000, you can easily see how this notation works.

The use of a CIDR notated address is the same as for a Classful address.

Classful addresses can easily be written in CIDR notation :

(Class A = /8, Class B = /16, and Class C = /24)

Note

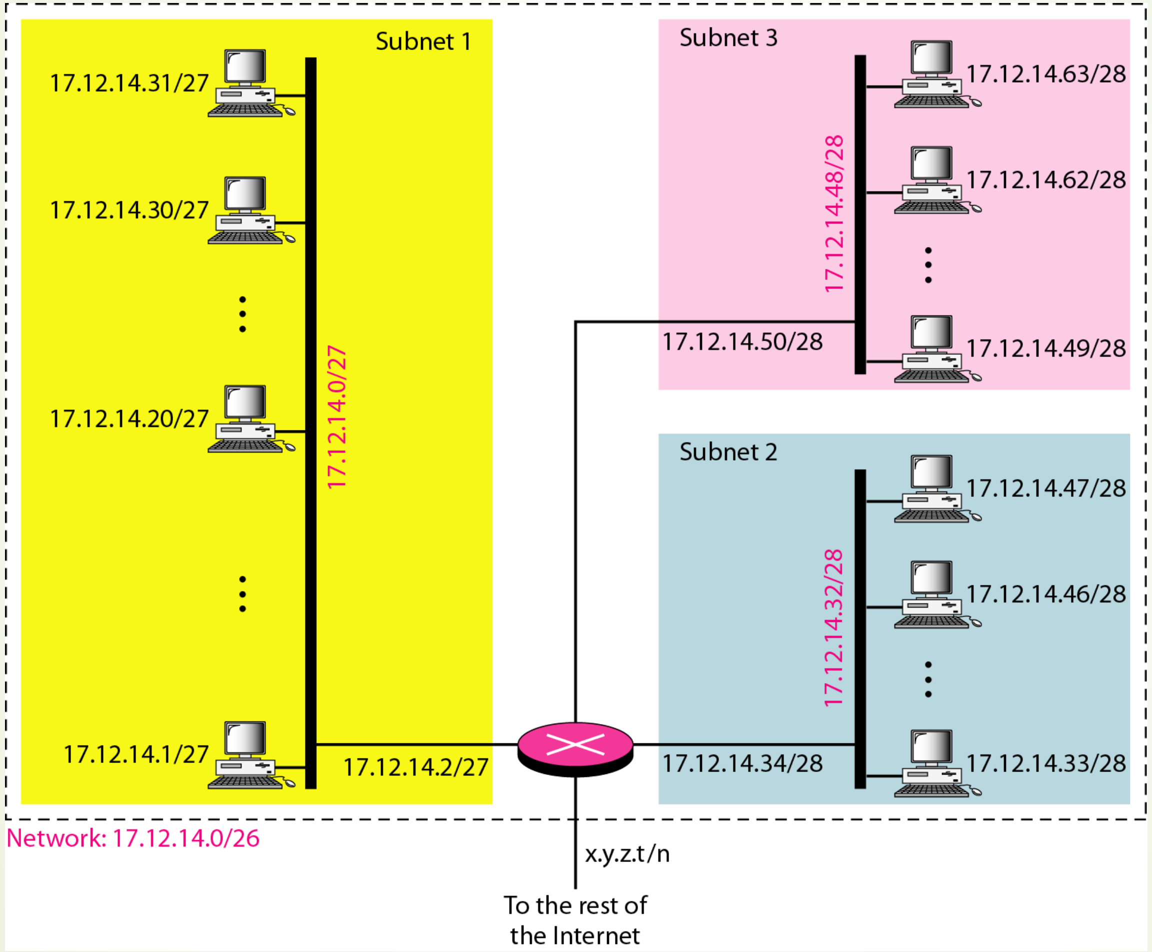
Each address in the block can be considered as a two-level hierarchical structure:
the leftmost *n* bits (prefix) define
the network;
the rightmost 32 − n bits define
the host.

Default masks

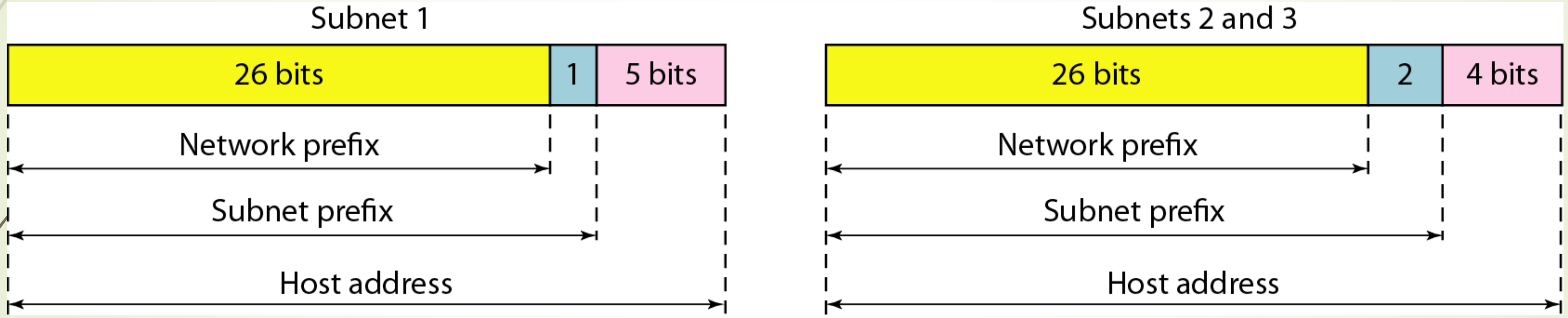
Class	In Binary	In Dotted-Decimal	Using Slash Prefix
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 111111111 11111111 00000000	255.255.255.0	/24

*The **network address** can be found by applying the **default mask** to **any address** in the block (including itself).*
*It **retains the netid** of the block and **sets the hostid to 0s**.*

Configuration and addresses in a subnetted network



Three-level hierarchy in an IPv4 address



Class A 2^24=16,777,216 effective 16,777,214

#bits	SubnetMask	CIDR	#Subnets	#Hosts	Nets*Hosts
2	255.192.0.0	/10	2	4194302	**8388604**
3	255.224.0.0	/11	6	2097150	12582900
4	255.240.0.0	/12	14	1048574	14680036
5	255.248.0.0	/13	30	524286	15728580
6	255.252.0.0	/14	62	262142	16252804
7	255.254.0.0	/15	126	131070	16514820
8	255.255.0.0	/16	254	65534	16645636
9	255.255.128.0	/17	510	32766	16710660
10	255.255.192.0	/18	1022	16382	16742404
11	255.255.224.0	/19	2046	8190	16756740
12	255.255.240.0	/20	4094	4094	**16760836**
13	255.255.248.0	/21	8190	2046	16756740
14	255.255.252.0	/22	16382	1022	16742404
15	255.255.254.0	/23	32766	510	16710660
16	255.255.255.0	/24	65534	254	16645636
17	255.255.255.128	/25	131070	126	16514820
18	255.255.255.192	/26	262142	62	16252804
19	255.255.255.224	/27	524286	30	15728580
20	255.255.255.240	/28	1048574	14	14680036
21	255.255.255.248	/29	2097150	6	12582900
22	255.255.255.252	/30	4194302	2	8388604

Class B 2^16 = 65,536 effective 65,534

# bits	Subnet Mask	CIDR	# Sub Nets	# Hosts	Nets *Hosts
2	255.255.192.0	/18	2	16,382	**32,764**
3	255.255.224.0	/19	6	8,190	49,140
4	255.255.240.0	/20	14	4,094	57,316
5	255.255.248.0	/21	30	2,046	61,380
6	255.255.252.0	/22	62	1,022	63,364
7	255.255.254.0	/23	126	510	64,260
8	255.255.255.0	/24	254	254	**64,516**
9	255.255.255.128	/25	510	126	64,260
10	255.255.255.192	/26	1,022	62	63,364
11	255.255.255.224	/27	2,046	30	61,380
12	255.255.255.240	/28	4,094	14	57,316
13	255.255.255.248	/29	8,190	6	49,140
14	255.255.255.252	/30	16,382	2	32,764

Class C   2^8 =256 effective 254

#bits	SubnetMask	CIDR	#Subnets	#Hosts	Nets*Hosts
2	255.255.255.192	/26	2	62	**124**
3	255.255.255.224	/27	6	30	180
4	255.255.255.240	/28	14	14	**196**
5	255.255.255.248	/29	30	6	180
6	255.255.255.252	/30	62	2	124

Example

- Say you are assigned a Class C network number of **200.133.175.0**
- You want to utilize this network across multiple small groups within an organization. You can do this by subnetting that network with a subnet address.
- We will break this network into **14 subnets** of **14 nodes each**.
- This will limit us to **196 nodes** on the network **instead of the 254** we would have without subnetting, but gives us the advantages of traffic isolation and security.
- To accomplish this, we need to use a subnet mask **4 bits long**.

- Recall that the default Class C subnet mask is
- 255.255.255.0
- 11111111.11111111.11111111.00000000
- Extending this by 4 bits yields a mask of
- 255.255.255.**240**
- 11111111.11111111.11111111.**1111**0000
- **/20**

Example cont'

This gives us 16 possible network numbers, 2 of which cannot be used:

Subnet bits	Network Number	Node Addresses	Broadcast Address
0000	200.133.175.0	Reserved	None
0001	200.133.175.16	17 thru 30	200.133.175.31
0010	200.133.175.32	33 thru 46	200.133.175.47
0011	200.133.175.48	49 thru 62	200.133.175.63
0100	200.133.175.64	65 thru 78	200.133.175.79
0101	200.133.175.80	81 thru 94	200.133.175.95
0110	200.133.175.96	97 thru 110	200.133.175.111
0111	200.133.175.112	113 thru 126	200.133.175.127
1000	200.133.175.128	129 thru 142	200.133.175.143
1001	200.133.175.144	145 thru 158	200.133.175.159
1010	200.133.175.160	161 thru 174	200.133.175.175
1011	200.133.175.176	177 thru 190	200.133.175.191
1100	200.133.175.192	193 thru 206	200.133.175.207
1101	200.133.175.208	209 thru 222	200.133.175.223
1110	200.133.175.224	225 thru 238	200.133.175.239
1111	200.133.175.240	Reserved	None

Example of address allocation by ISP

An ISP is granted a block of addresses starting with 190.100.0.0/16 (65,536 addresses).

The ISP needs to distribute these addresses to three groups of customers as follows:

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

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

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

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

Example (continued)

Solution

Group 1

- ***For this group, each customer needs 256 addresses***
- ***This means that 8 ($\log_2 256$) bits are needed to define each host***
- ***The prefix length is then 32 − 8 = 24.***
- ***The addresses are***

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

Total = 64 × 256 = 16,384

Example

Group 2

- ***For this group, each customer needs 128 addresses.***
- ***This means that 7 ($\log_2 128$) bits are needed to define each host.***
- ***The prefix length is then 32 − 7 = 25.***
- ***The addresses are***

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

Total = 128 × 128 = 16,384

Example 19.10 (continued)

Group 3

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

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

Total = 128 × 64 = 8192

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

The address allocation and distribution by an ISP