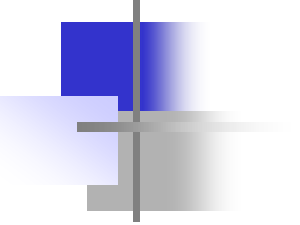
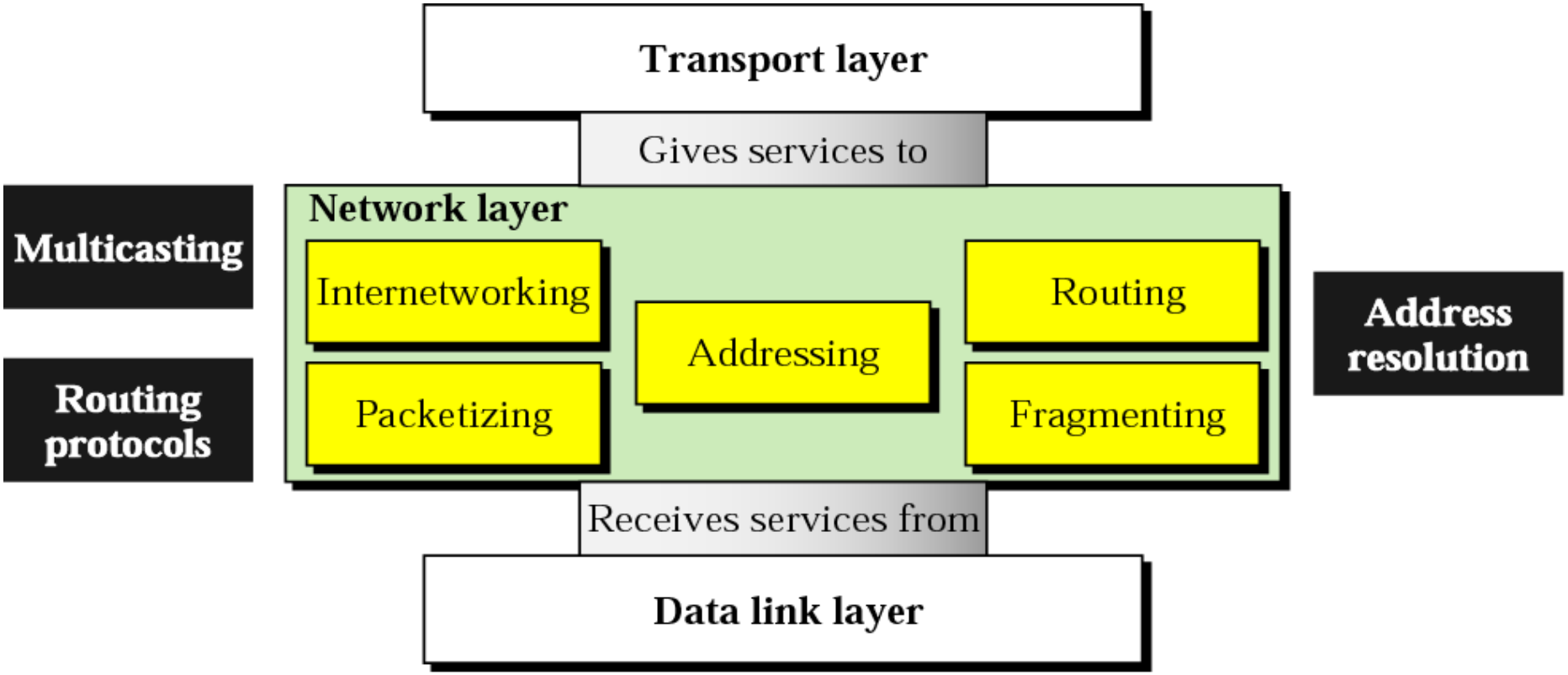


Lecture:
The Network Layer & IP Addressing

Position of network layer



Where is the network layer?

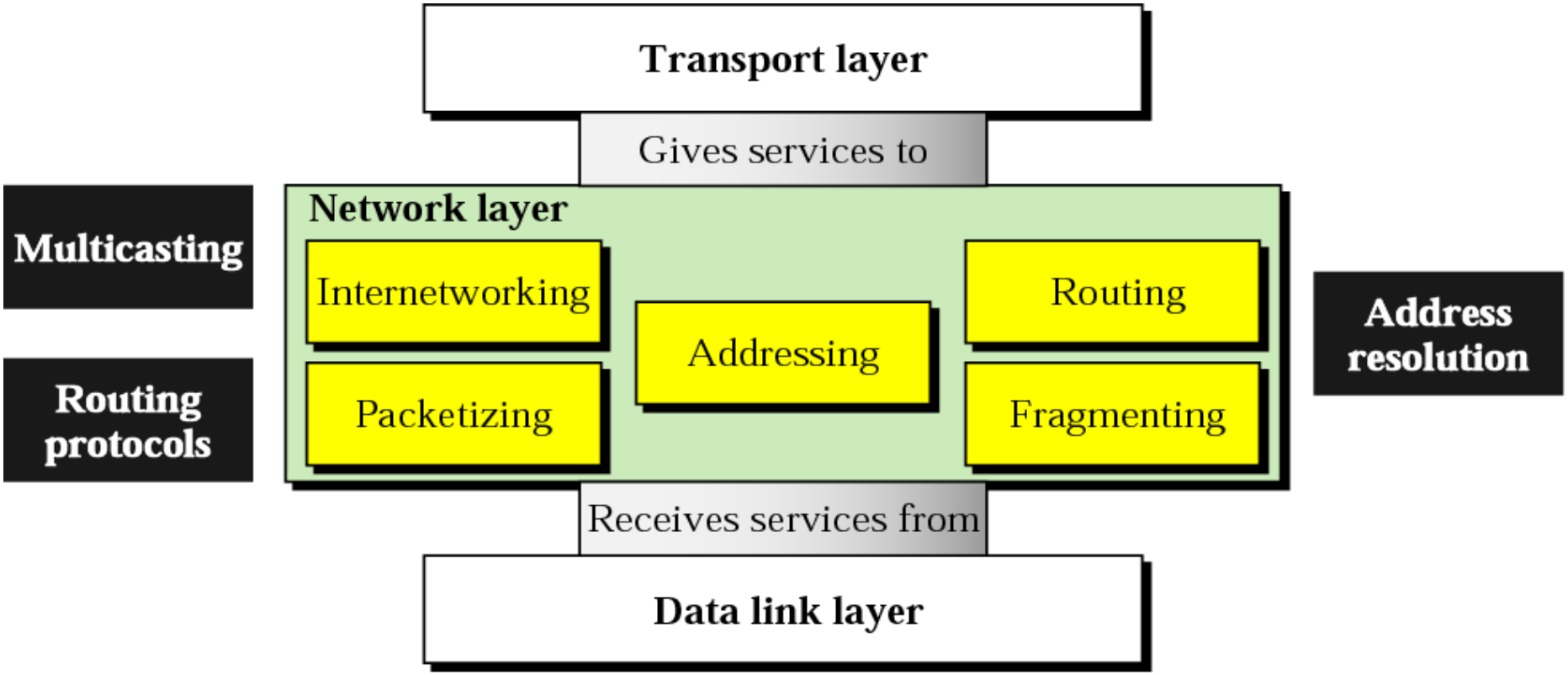
a)There are 7 layers from OSI model and 5 layers from TCP/IP model (as discussed previously!)

b)From OSI, the Network layer rests between the upper layer called the **Transport** layer and the lower layer called the **Data Link** Layer.

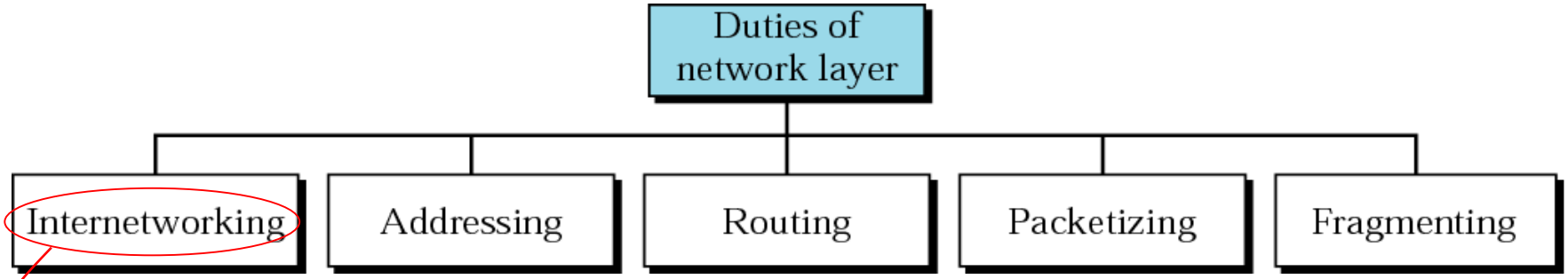
c)From the TCP/IP model, the Network layer is called the ***Internet layer*** and it rests between the upper **Transport** layer and the lower **Host to Network** layer.

Function of Network Layer

Position of network layer



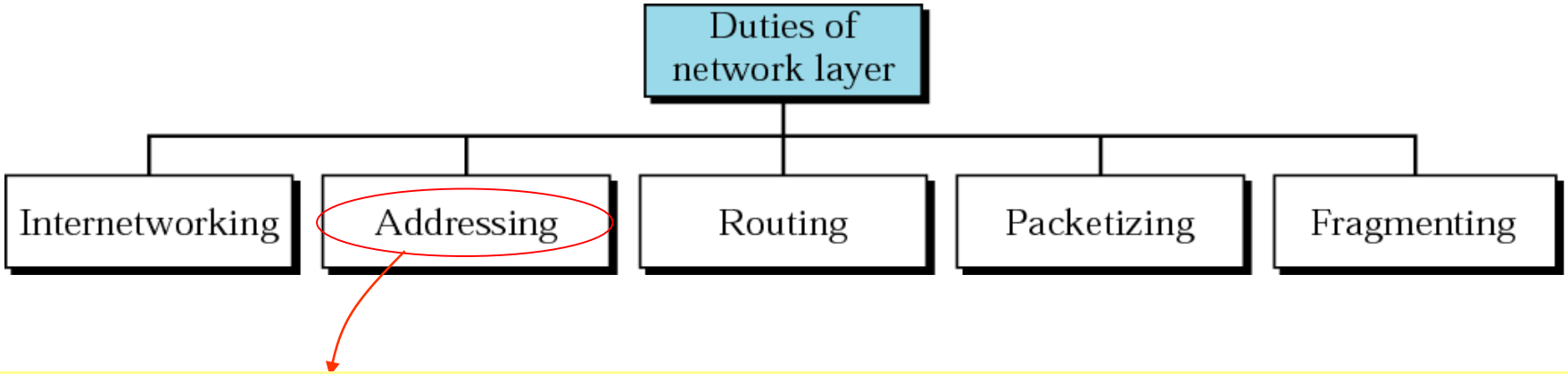
Network layer duties



- The key is interconnecting different networks (various LAN technologies, telephone network, satellite link, ATM networks etc.) and making them look the same to the upper layer; i.e. logical gluing of heterogeneous physical networks together to look like a single network to the Transport & Application layer.

- Additional notes: The transport layer should not be worried about the underlying physical network !

Network layer duties

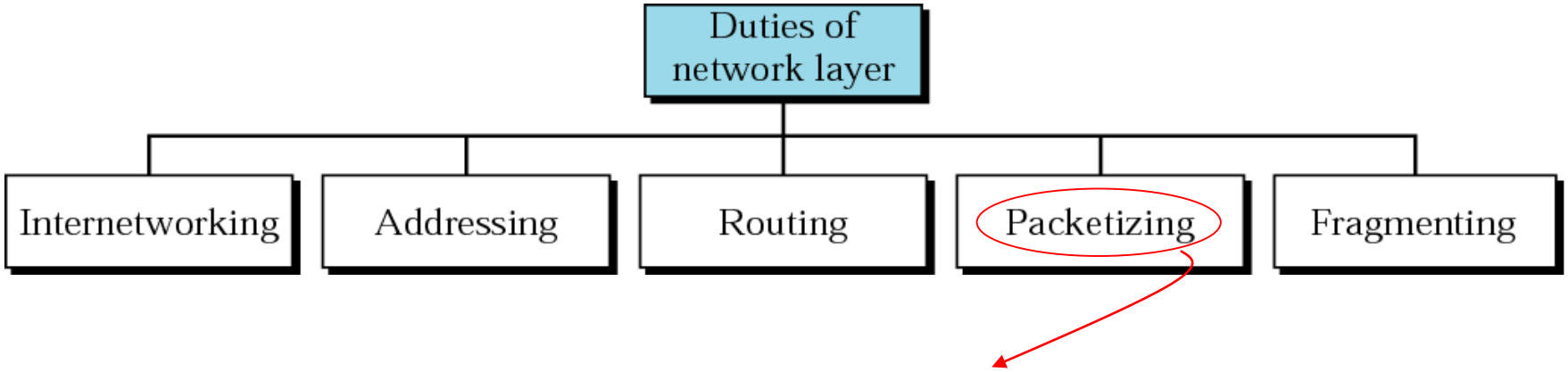


• The addresses must be uniquely and universally define the sole connection of a (host/router/machine/device/user) to the internet. Two devices on the internet can never have the same address. (Address per connection)

Remember, network layer is independent of the data link layer.

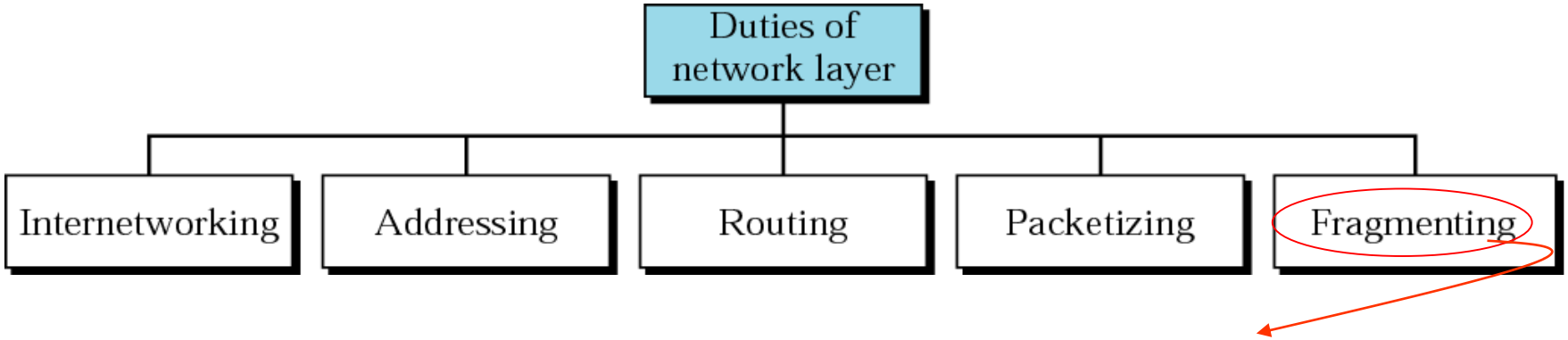
We cannot use the data link layer addresses !! Because these addresses depend on the technology used in the data link layer.

Network layer duties



- Network layer encapsulates packets received from upper layer protocols and makes new packets. (Re-packaging).
- This is a task common to all layers.
- In the Internet model, packetizing is done by network layer protocol called IP – Internetworking Protocol.
- The Protocol Data Units (PDU's) coming from the transport layer must be placed in network-layer packets and sent to the data-link layer.

Network layer duties

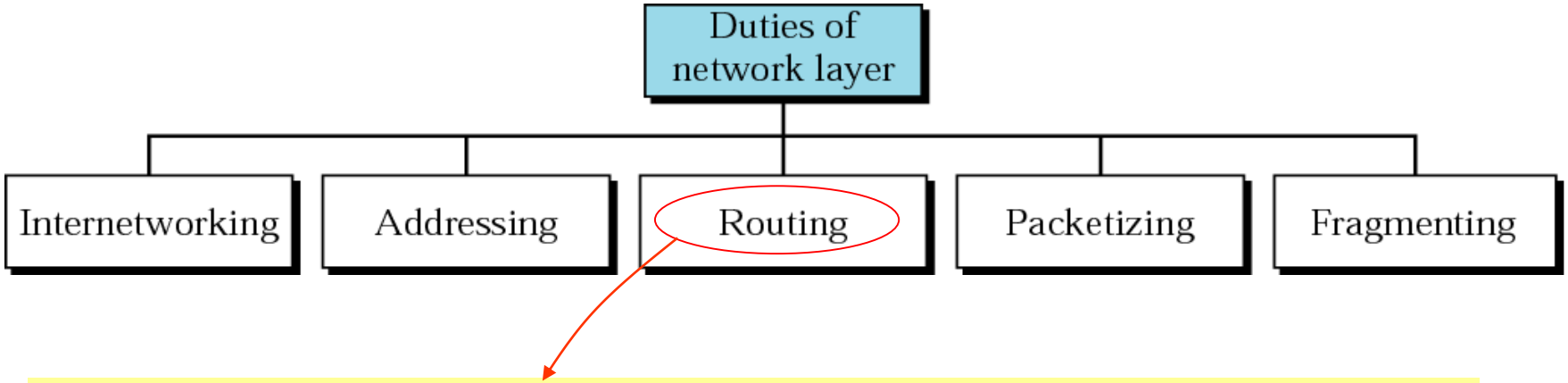


• A packet can travel through different networks. Each router decapsulates the IP datagram from the received frame, processes it and then encapsulates it in another frame. The format & size depend on the physical network.

• Remember, the network layer must be able to operate on top of any data-link layer technology (Ethernet, Fast Ethernet, ATM etc.). All these technologies can handle a different packet length.

• The network layer must be able to fragment transport layer PDUs into smaller units so that they can be transferred over various data-link layer technologies.

Network layer duties

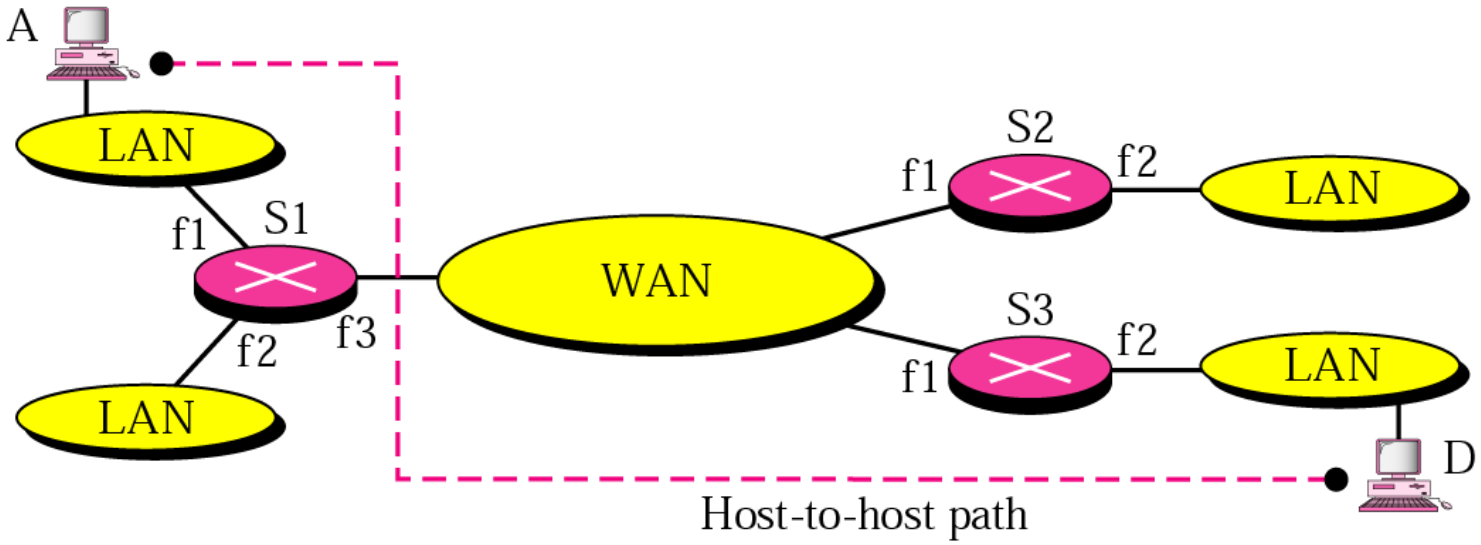


- Now that you have your network layer packet, where do you send it ? Each packet reaches its destination via several routes.
- So, which route is suitable or optimum? Issue of speed, reliability, security etc. (routing algorithm)
- Packet cannot choose the route; the routers connecting the LANs/WANs makes this decision.
- (refer Chap-19 of Forouzan's book).

Internetworking

How can data be exchanged between networks?

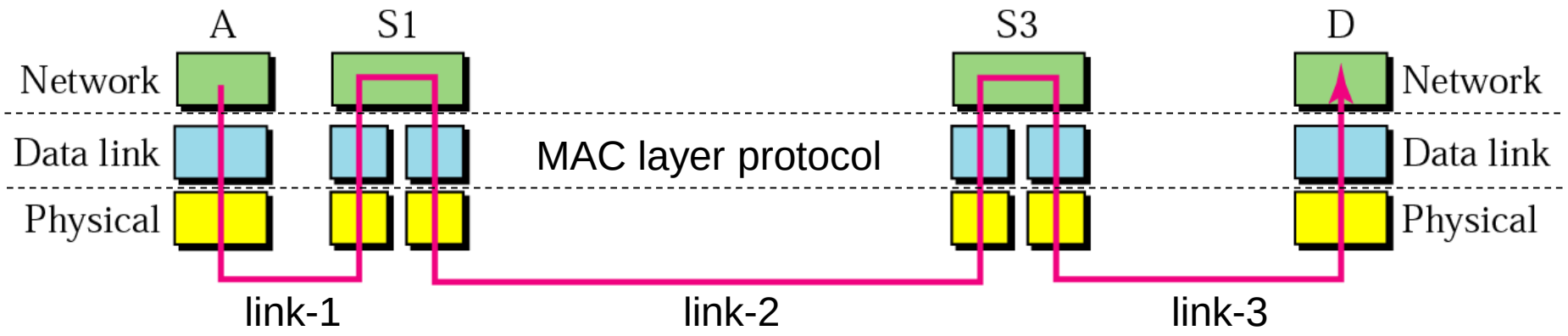
They need to be connected via routers/links to make an internetwork.



- The above internetwork is made of 5 networks: 4 LANs and 1 WAN.

- E.g. If host A needs to send a data packet to host D, the packet needs to go from A to S1, then from S1 to S3, and finally from S3 to D. Therefore the packet passes through 3 links.

Internetworks

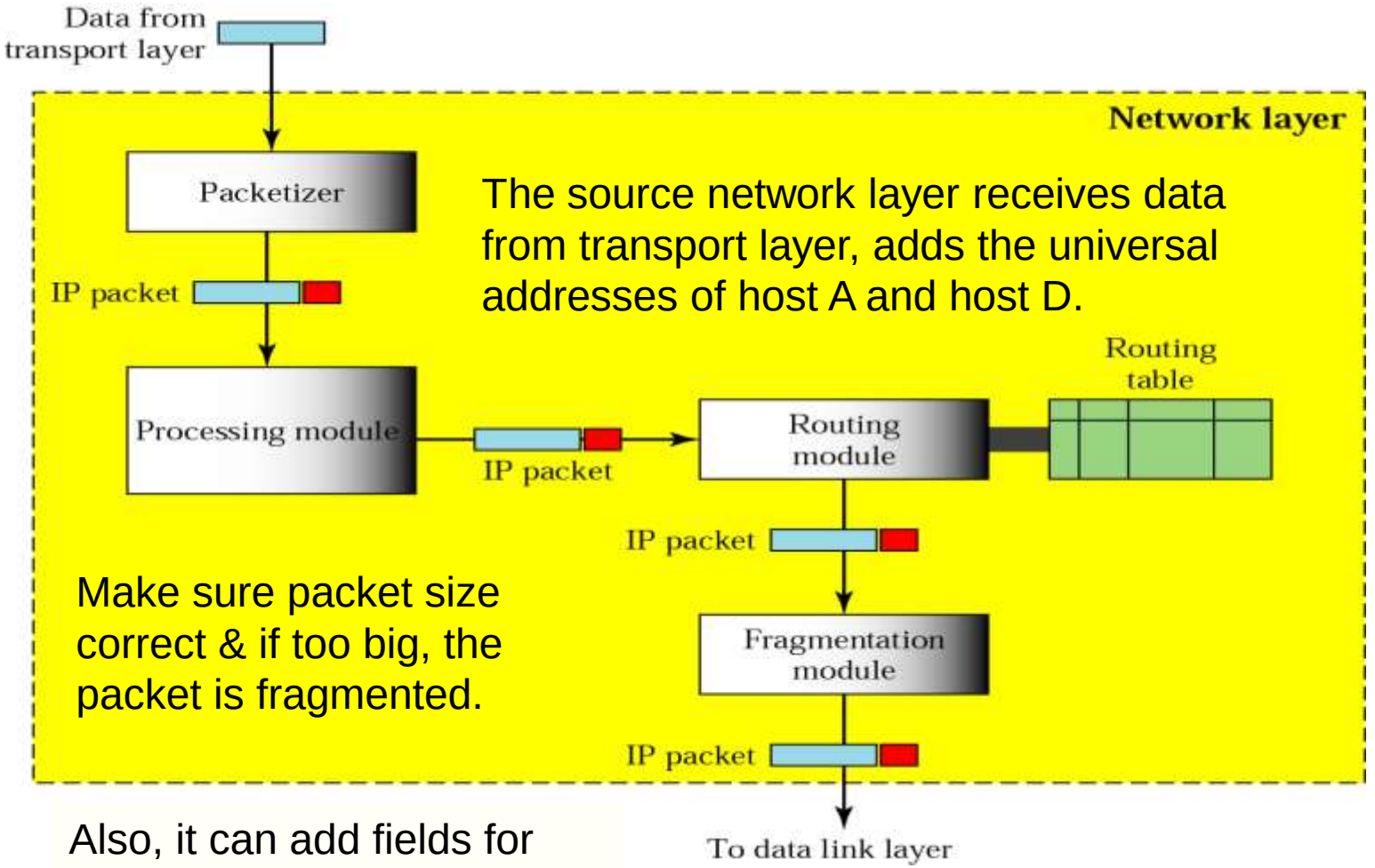


• Problem: how does S1 know that they should send out from f3 after packet arrive at f1 from A? (No provision in data-link layer to help S1 making the decision and the frame only contains the MAC addresses-pair of 1st link)

• To solve the problem of delivery thru several links, the network layer was designed and responsible for host-to-host delivery and for routing the packets thru different routers.

Network layer at the Source

Network layer at source is responsible to create a packet that carrier 2 universal addresses: Destination add. & Source add.



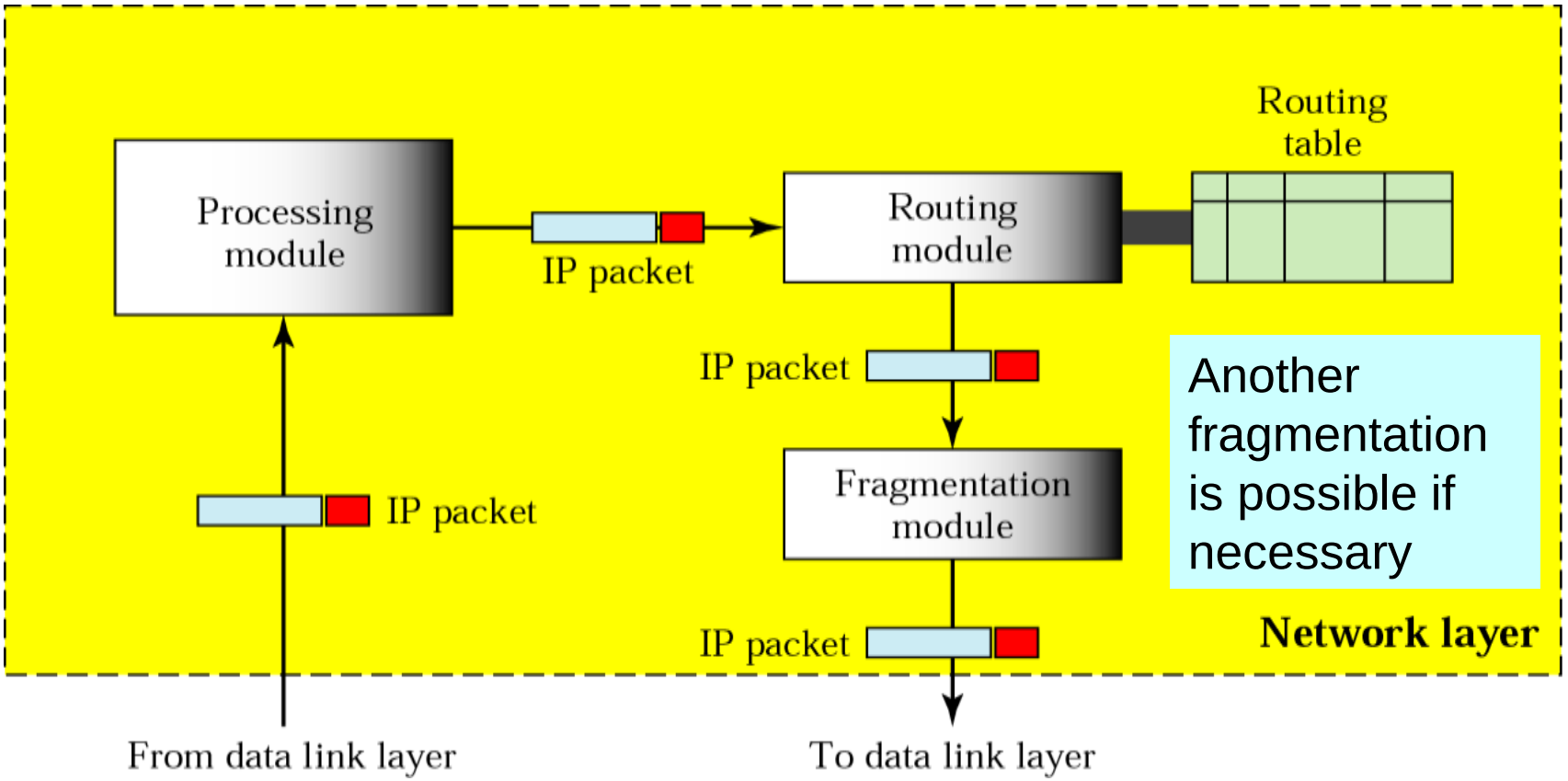
The source network layer receives data from transport layer, adds the universal addresses of host A and host D.

Make sure packet size correct & if too big, the packet is fragmented.

Also, it can add fields for error control.

Network layer at the Router

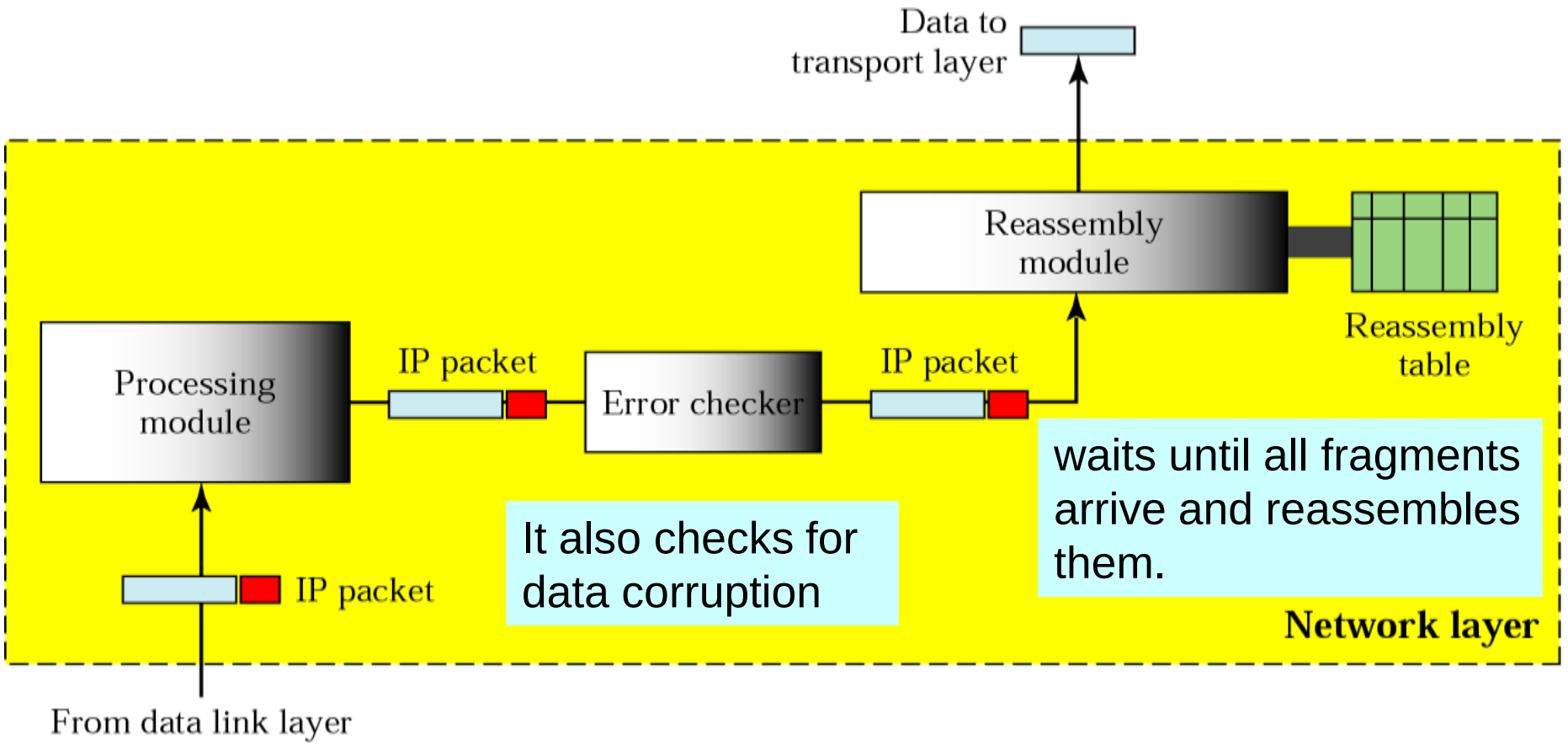
Network layer at the router is responsible for routing the packet.



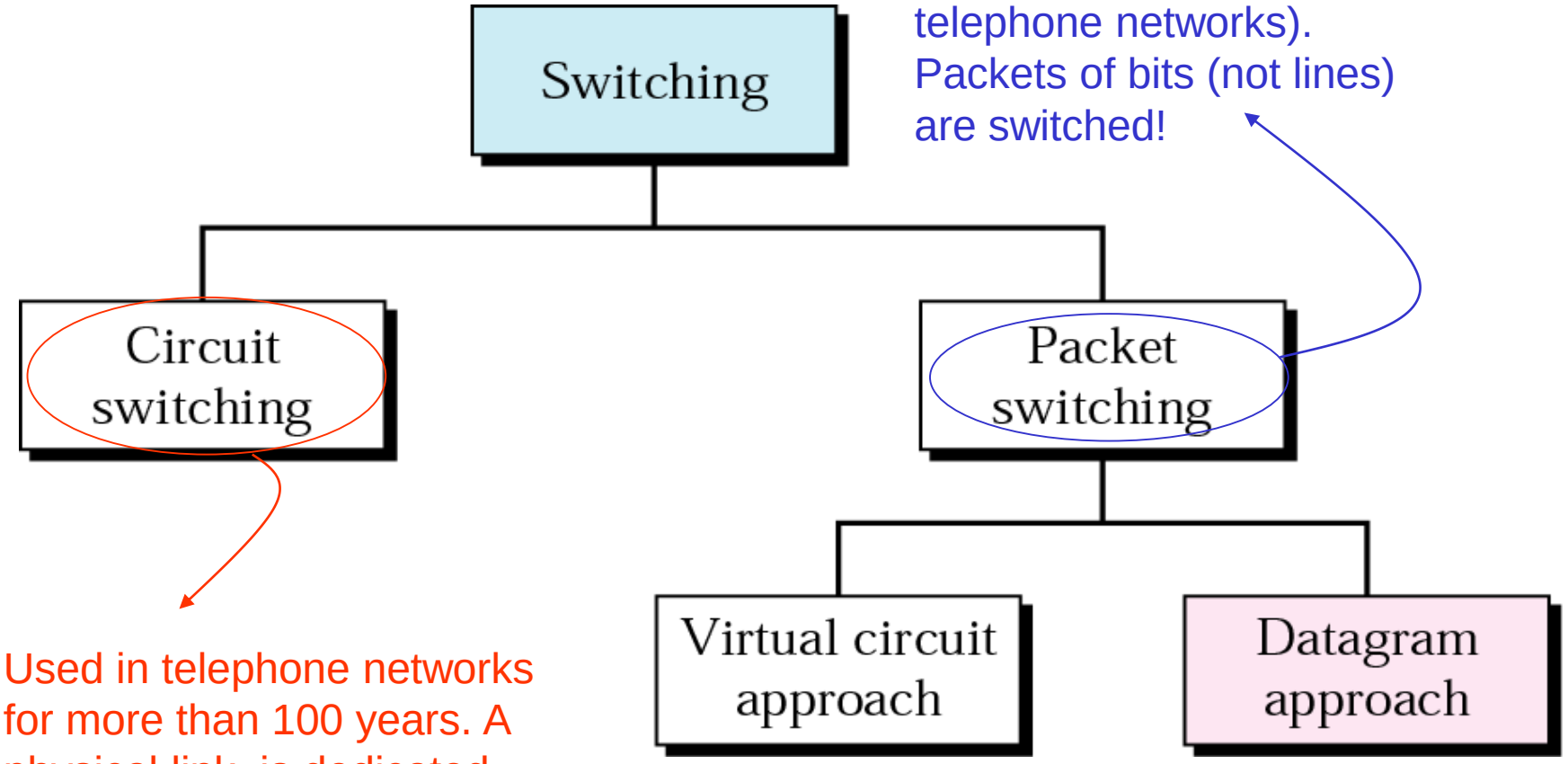
When a packet arrives, the router finds the interface from which the packet must be sent using routing table.

Network layer at the Destination

Network layer at the Destination is responsible for address verification; it makes sure that Destination address on the packet is the same as the address of the receiving host.



Switching/Routing Mechanism



Used in computer networks and (also in modern telephone networks). Packets of bits (not lines) are switched!

Used in telephone networks for more than 100 years. A physical link is dedicated between Source and Destination. Data can be sent as a stream of bits without the need for packetising

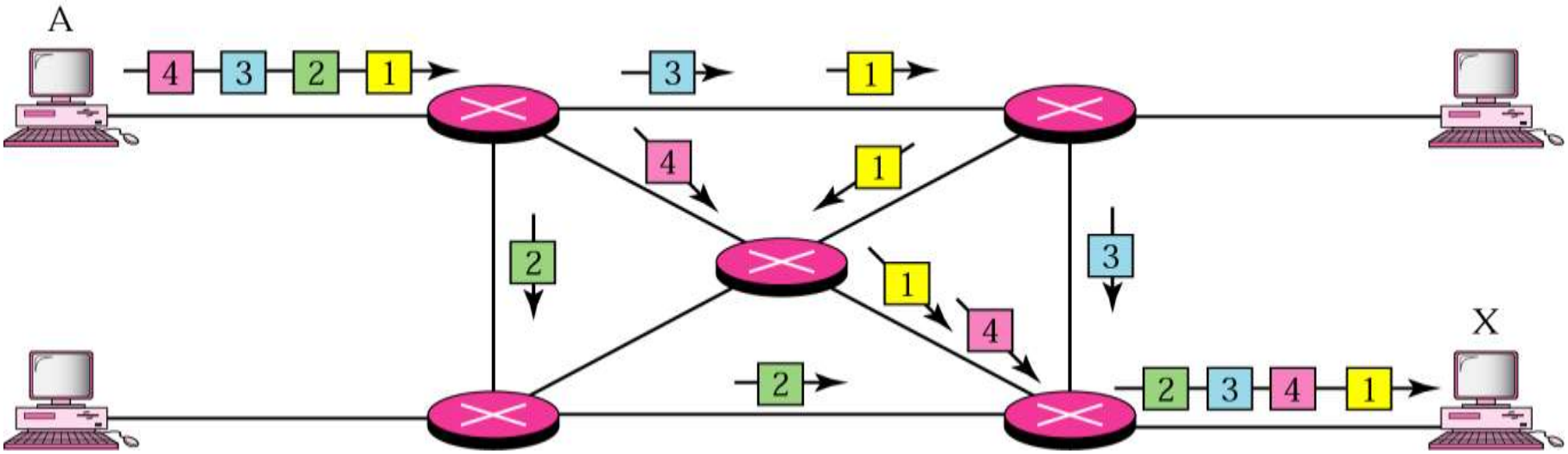
(Also called Connection-oriented networking)

(Also called Connectionless networking)

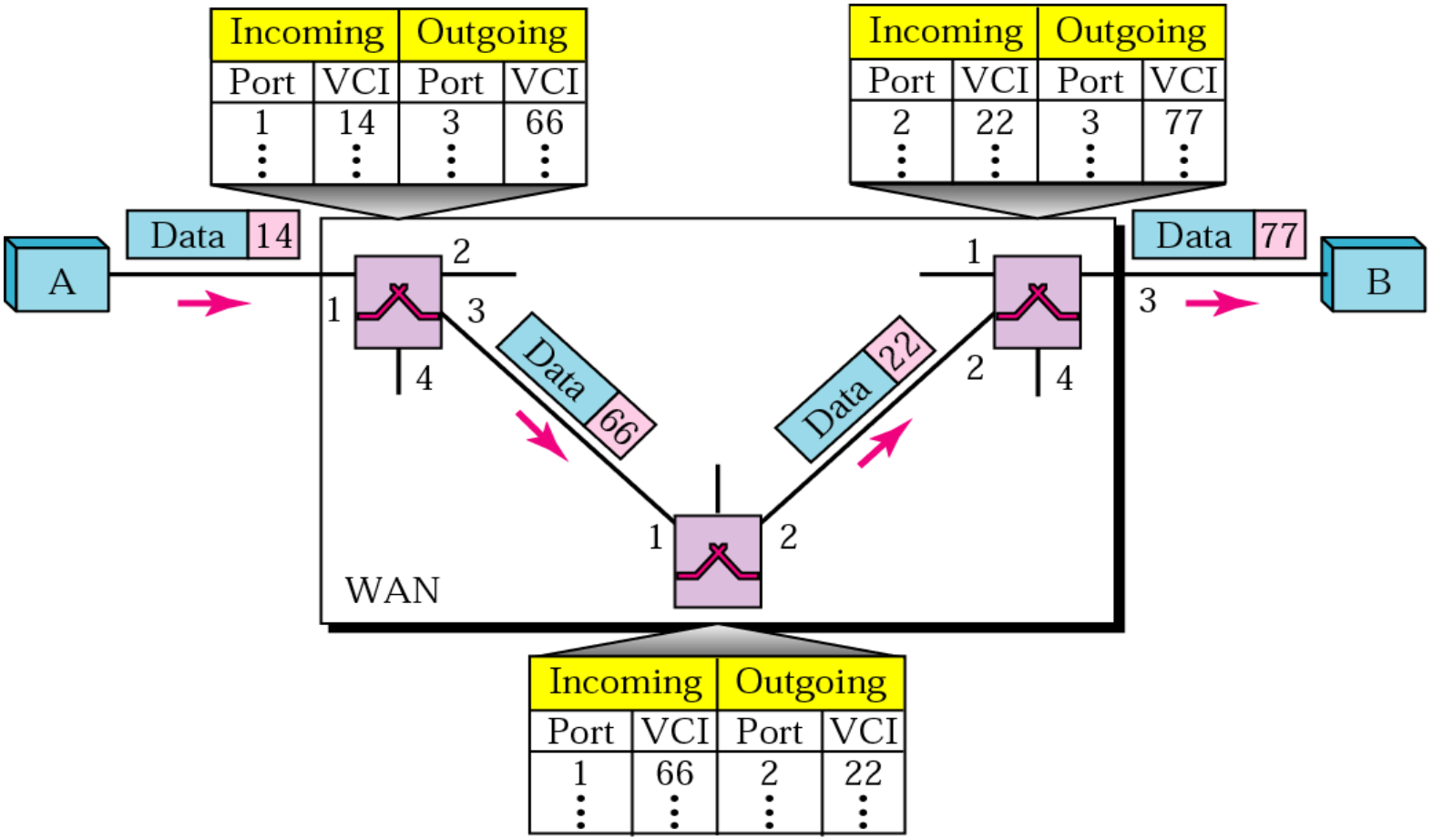
Comparison of Virtual-Circuit and Datagram Approaches

Issue	Datagram subnet	Virtual-circuit subnet
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Datagram approach



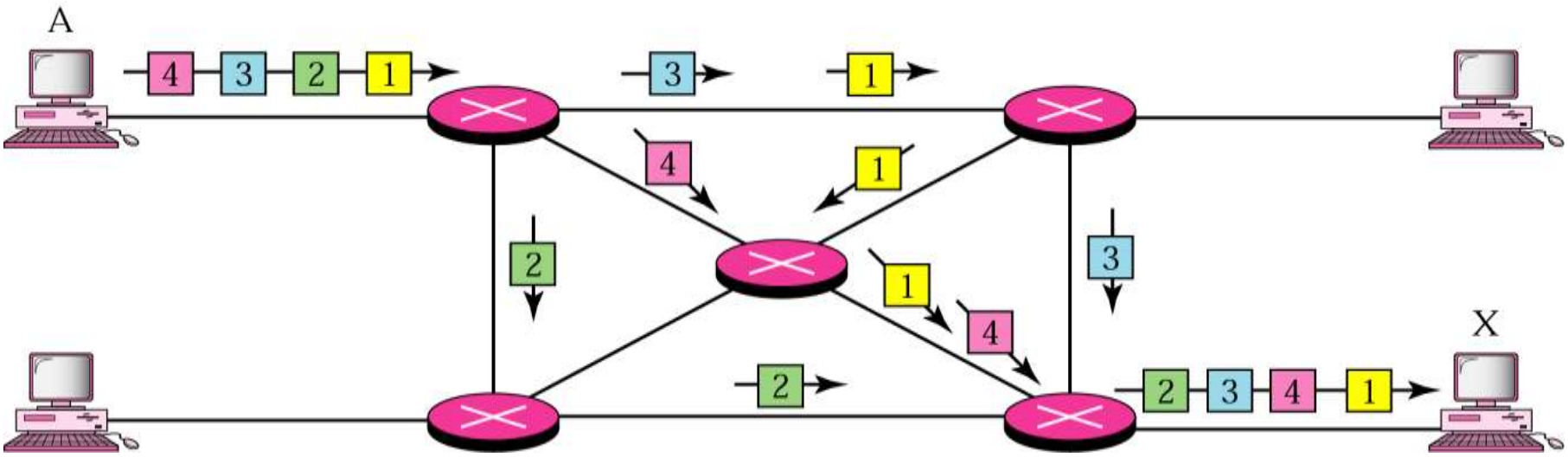
Virtual Circuits approach



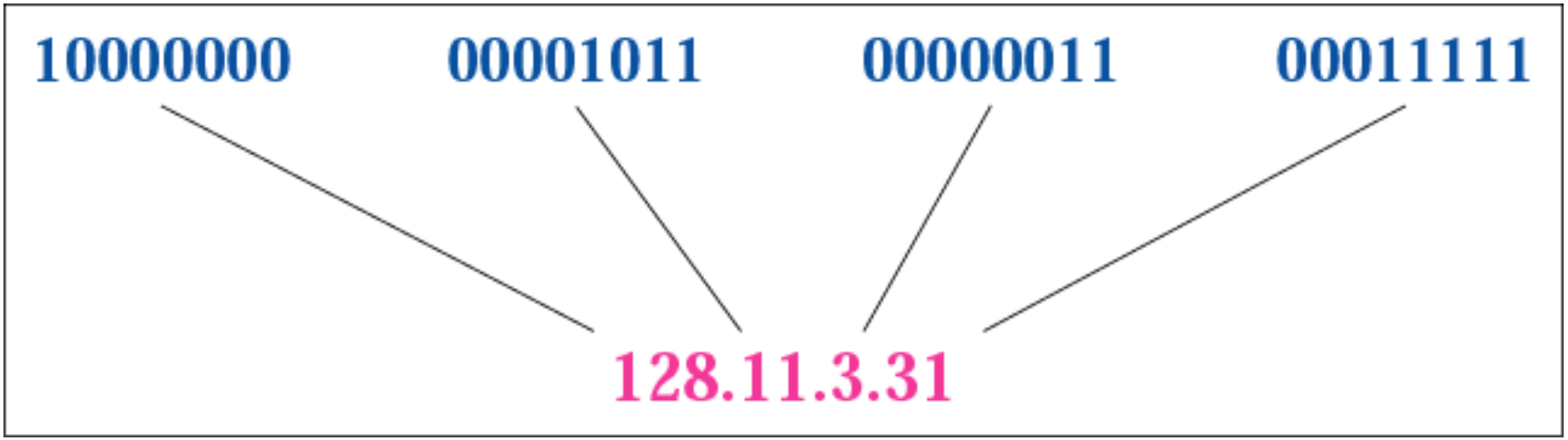
Part A:
Concept of IP Addressing in Network Layer

Internet Protocol (IP)

- IP uses connectionless network-layer protocol.
- IP is based on datagram switching/routing.
- IP is unreliable !!
- Don’t care how, as long as it arrives!!



Relationship of Binary & Dotted-decimal notation



Example

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

10000001 00001011 00001011 11101111

Solution

129.11.11.239

Example

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

111.56.45.78

Solution

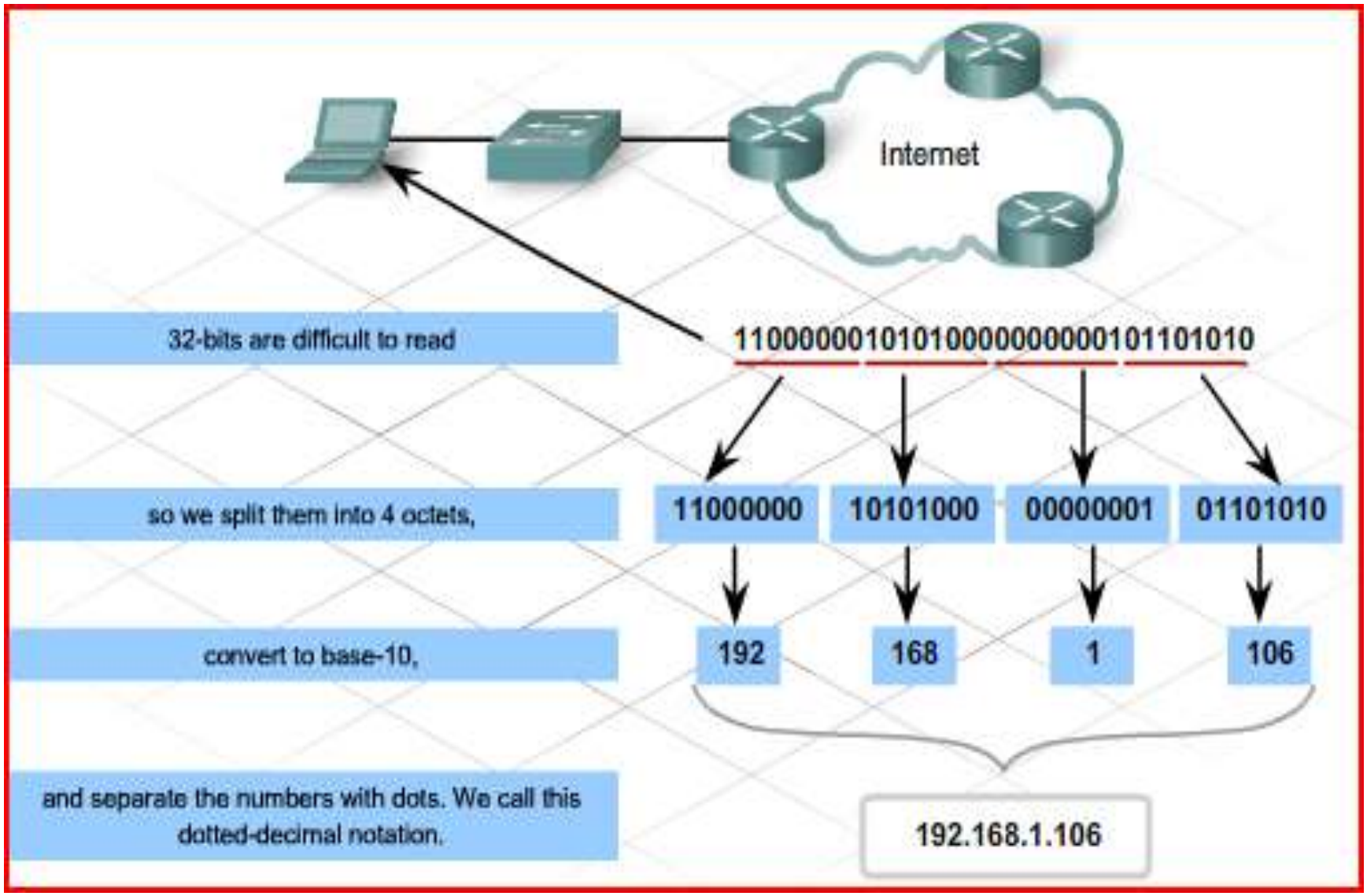
01101111 00111000 00101101 01001110

IP-Addressing

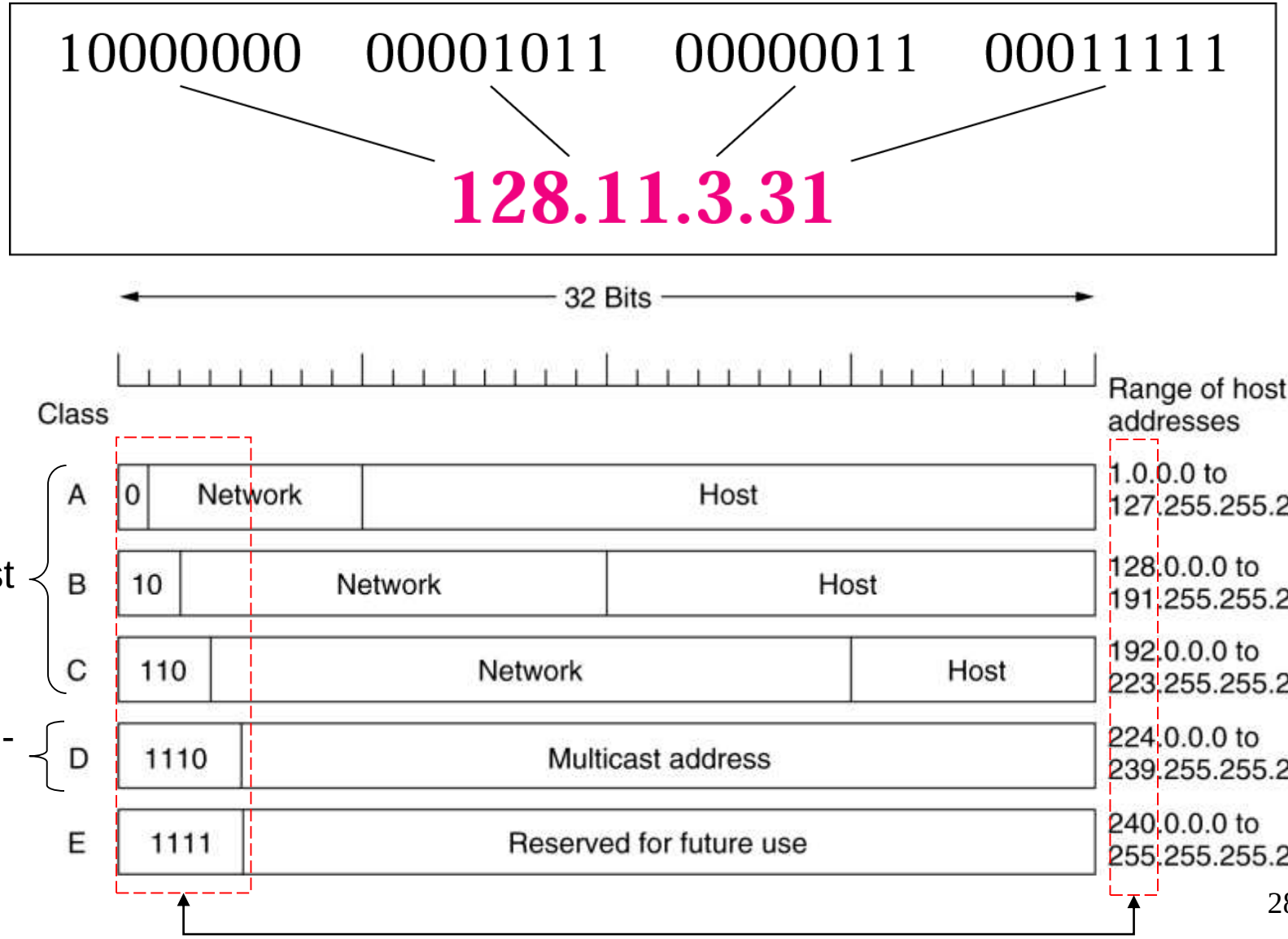
- The general identifier used in network layer to identify each device connected to the Internet is called the Internet address or IP address.
- Two types ID: **Network Address** & **Host Address**.
- In IPv4, an IP address is a 32-bit binary address (4-bytes) that uniquely and universally defines the connection of a host or a router to the Internet. (Universal in the sense that the addressing system must be accepted by any host that wants to be connected to Internet).
- Each IP address is unique and only defines **1** connection to the Internet. Two devices on the internet can never have the same address at the same time. (referring to IP Public addresses).

IP-Addressing

- Two types of IP addressing: **Classful** vs. **Classless**
- When a packet needs to be sent from s host to destination, it needs to pass from one node to the next. The *network layer* provides only host-to-host addressing; the *data-link* layer needs physical MAC addresses for node-to-node delivery.
- Method to map these two addresses: **ARP** – Address Resolution Protocol.


Internet
32-bits are difficult to read
11000000101010000000000101101010
so we split them into 4 octets,
11000000
10101000
00000001
01101010
convert to base-10,
192
168
1
106
and separate the numbers with dots. We call this dotted-decimal notation.
192.168.1.106

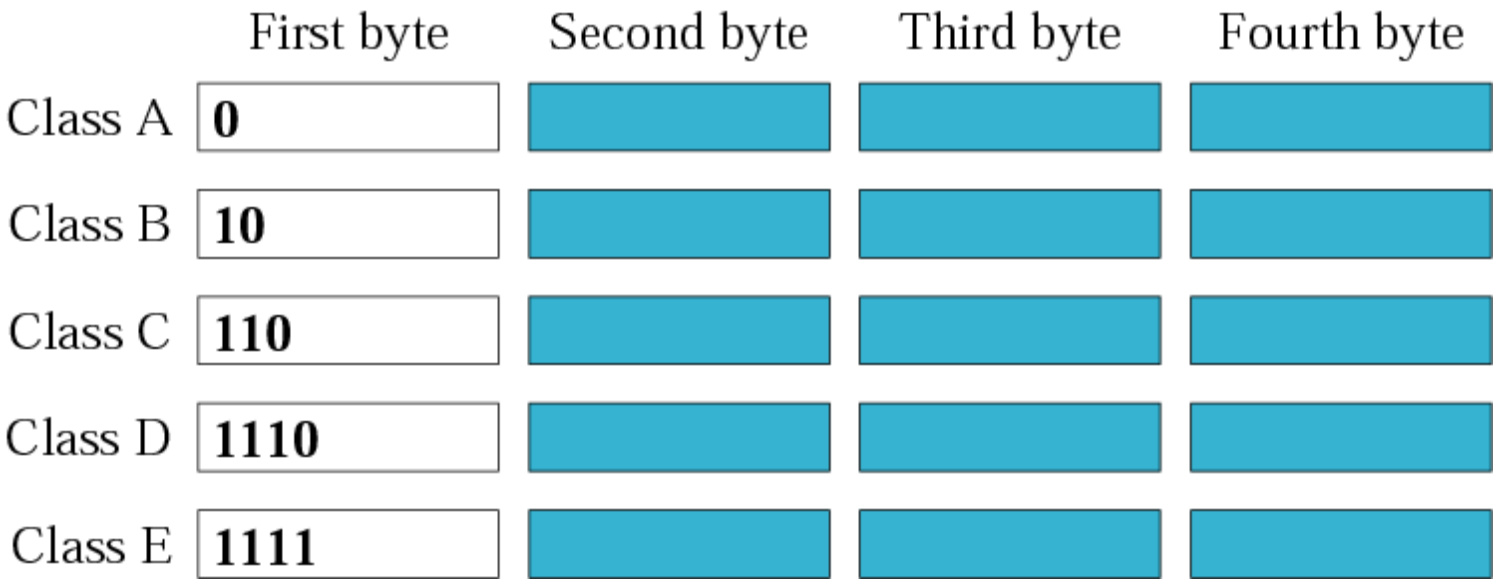
IP Addresses



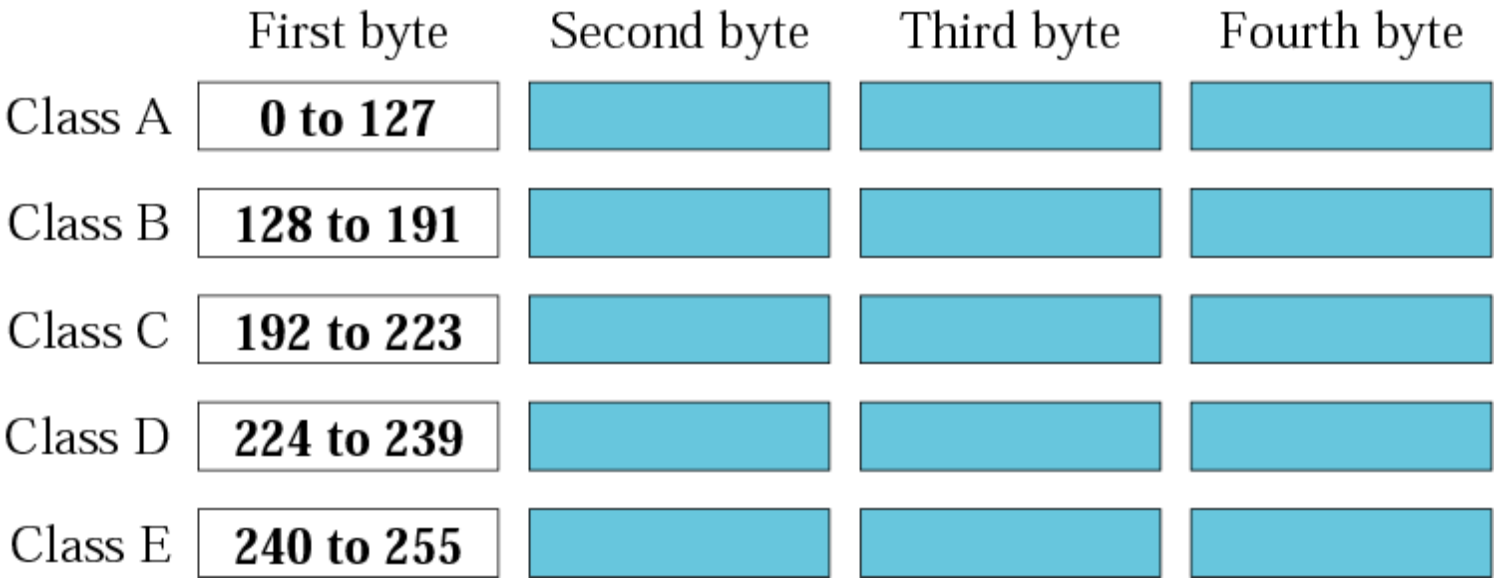
IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits don't change)	Network (N) and Host (H) parts of address	Default subnet mask (decimal and binary)	Numbers of possible networks and hosts per network	Notes and host address range**
A	1 - 127*	00000000 - 01111111	N.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	128 nets (2^7) 16,777,214 hosts per net (2^24-2)	Commercial 1.0.0.1 - 126.255.255.254
B	128 - 191	10000000 - 10111111	N.N.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16,384 nets (2^14) 65,534 hosts per net (2^16-2)	Commercial 128.0.0.1 - 191.255.255.254
C	192 - 223	11000000 - 11011111	N.N.N.H	255.255.255.0 11111111.11111111.11111111.00000000	2,097,152 nets (2^21) 254 hosts per net (2^8-2)	Commercial 192.0.0.1 - 223.255.255.254
D	224- 239	11100000 - 11101111	Not for commerical use as a host			Multicast (reserved) 224.0.0.1 - 239.255.255.254
E	240 - 255	11110000 - 11111111	Not for commerical use as a host			Experimental (reserved) 240.0.0.1 - 255.255.255.255

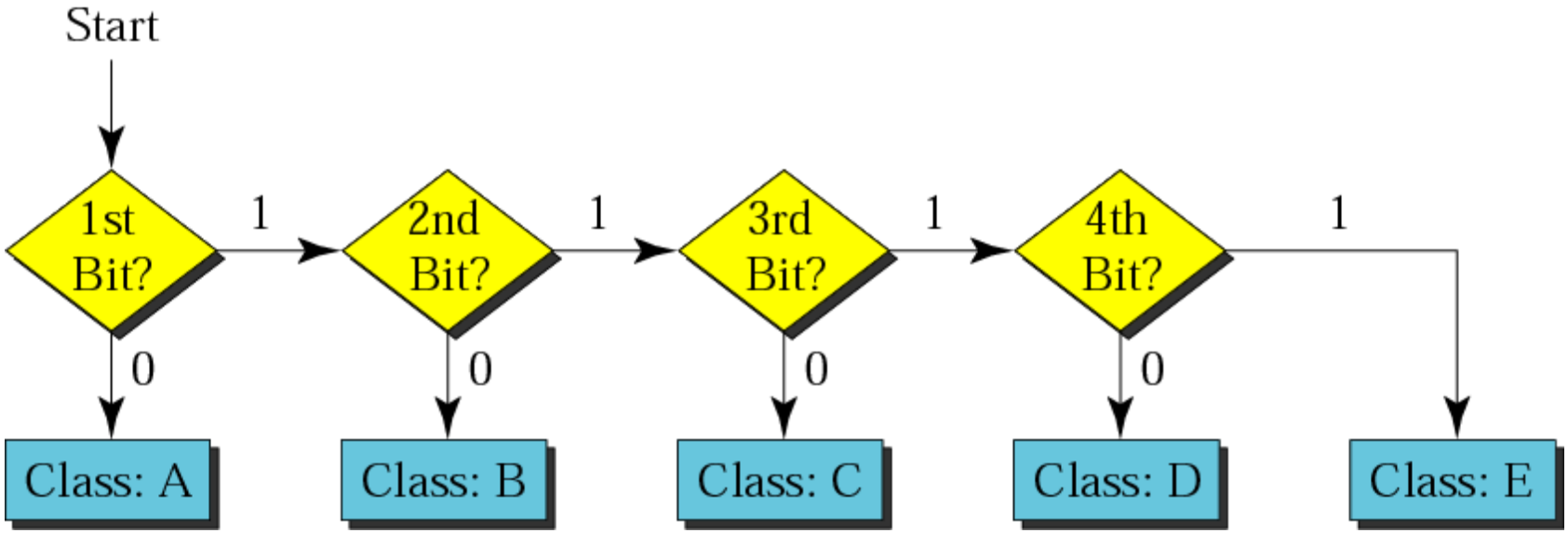
Classful Addressing: Finding the class in binary notation



Classful Addressing: Finding the class in decimal notation

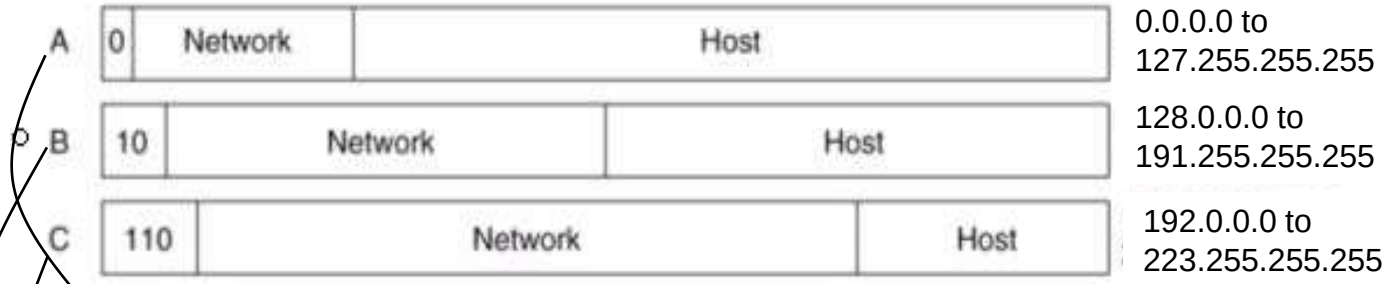


Finding the address class



Classful Addresses

Classful addressing in IP is both inflexible and inefficient !



0.0.0.0 to
127.255.255.255

128.0.0.0 to
191.255.255.255

192.0.0.0 to
223.255.255.255

allows 127 networks and 16 777 214 hosts on each network

7 bits = 2^7 -1: exclude 0.0.0.0

24 bits = 2^{24} -2: exclude 1st and last IP

allows 16384 networks and 65534 hosts on each network

14 bits = 2^{14}

16 bits = 2^{16} -2: exclude 1st and last IP

allows 2 097 152 networks and 254 hosts on each network

21 bits = 2^{21}

8 bits = 2^8 -2: exclude 1st and last IP

Note: In each network, the 1st IP address is the Network Address (e.g. 73.0.0.0) and the last IP address is for special purpose (e.g. 73.255.255.255) .

Classful Addressing

a) Unicast address: one source to one destination; Class A, B & C.

b) Multicast address: one source to a group of destination: only as destination address not source address; Class-D.

c) IP addresses in class A, B, C are divided into different length of:

Network-ID (netid) and Host-ID (hostid)

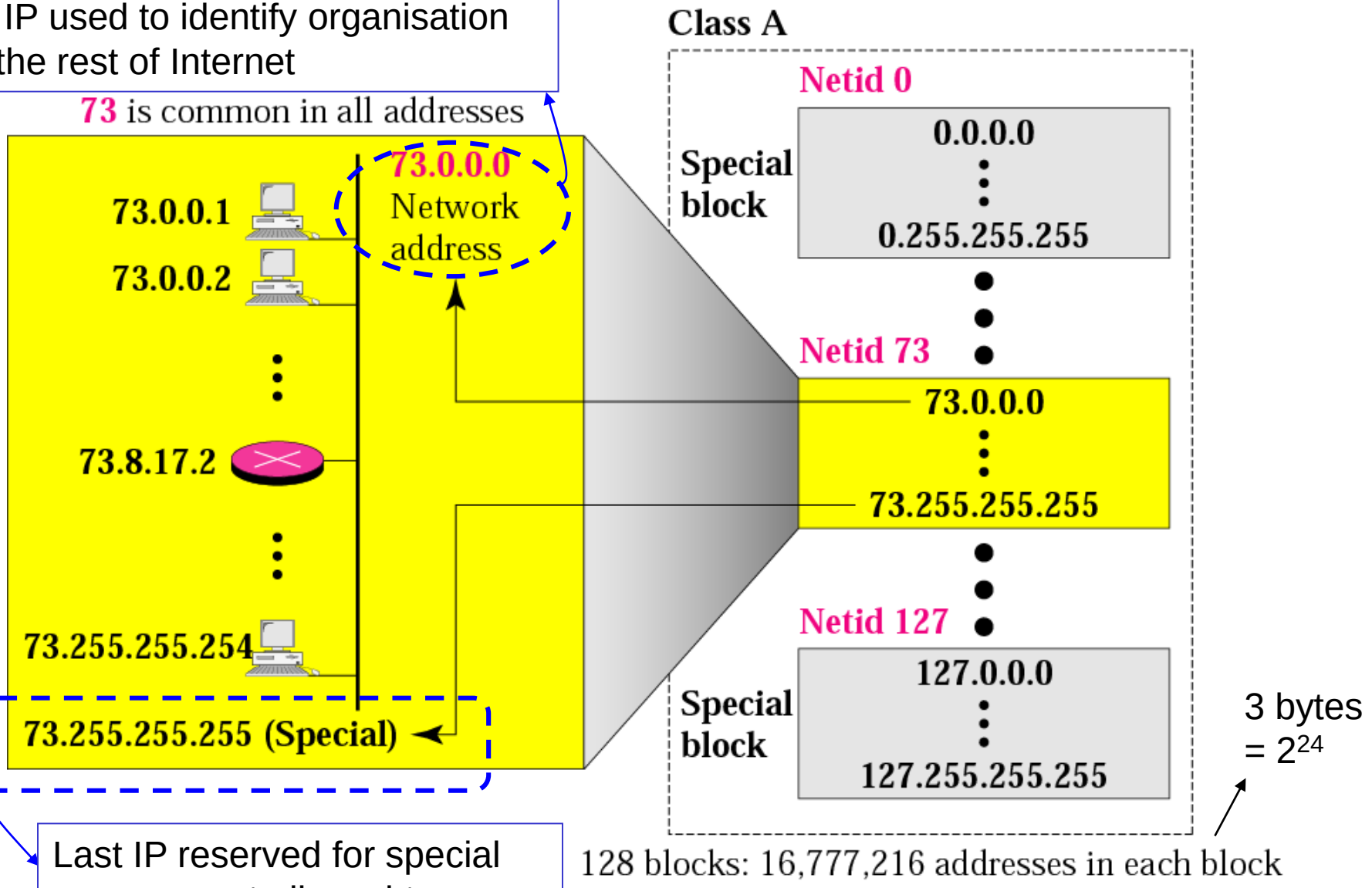
d) Classes and Blocks concept: - for example:

In class-A, 1st block covers from **0**.0.0.0 to **0**.255.255.255 (net-ID 0)
2nd block covers from **1**.0.0.0 to **1**.255.255.255 (net-ID 1)
last block covers from **127**.0.0.0 to **127**.255.255.255 (net-ID 127)

- Note that: block = number of available networks in each class
- One problem with classful addressing is that each class is divided into a fixed number of blocks with fixed size. (read Forouzan's text)
- Plenty of IP addresses wasted!!! in classful addressing method.

128 Blocks in class A

1st IP used to identify organisation to the rest of Internet

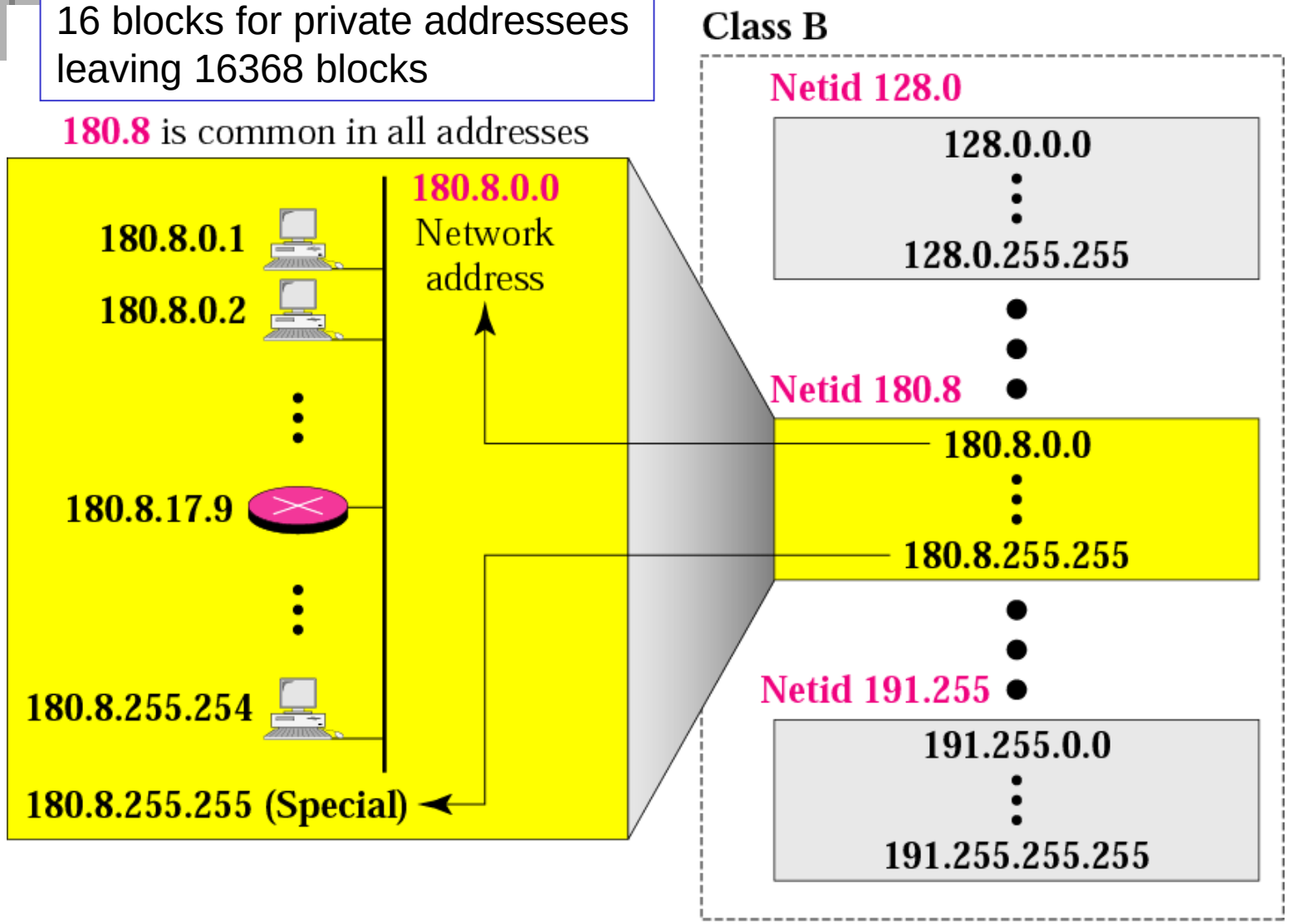


Last IP reserved for special purpose; not allowed to use

Millions of class A addresses are wasted.

16384 Blocks in class B

16 blocks for private addressees leaving 16368 blocks



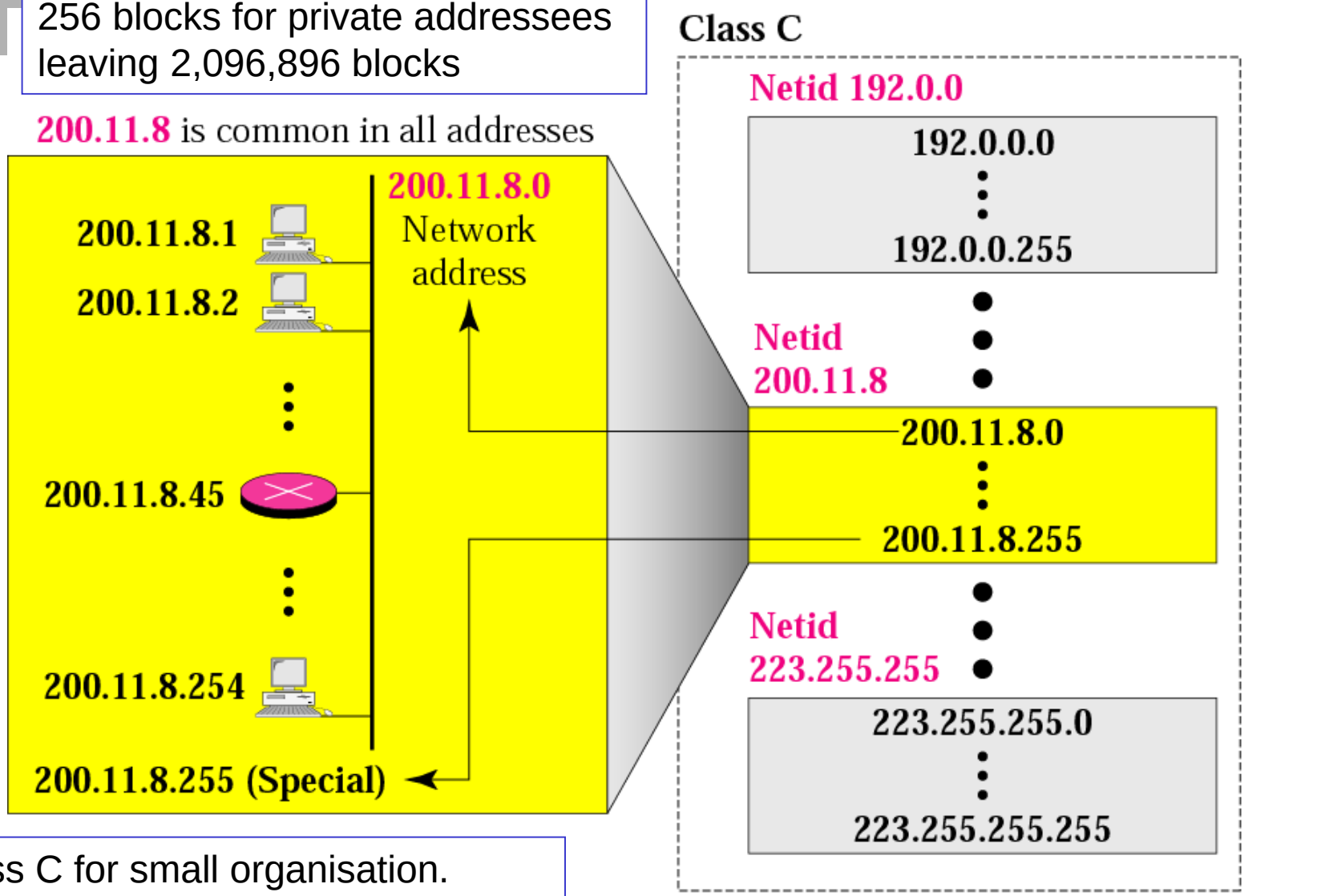
16,384 blocks: 65,536 addresses in each block

Class B for midsize organisation.
16384 organizations are class-B

Many of class B addresses are wasted.

2,097,152 Blocks in class C

256 blocks for private addressees leaving 2,096,896 blocks



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

Class C for small organisation. Limited IP address in each blocks, which is smaller than the needs of most organisations

***Class D** addresses are used for multicasting; there is only one block in this class.*

***Class E** addresses are reserved for special purposes; most of the block is wasted.*

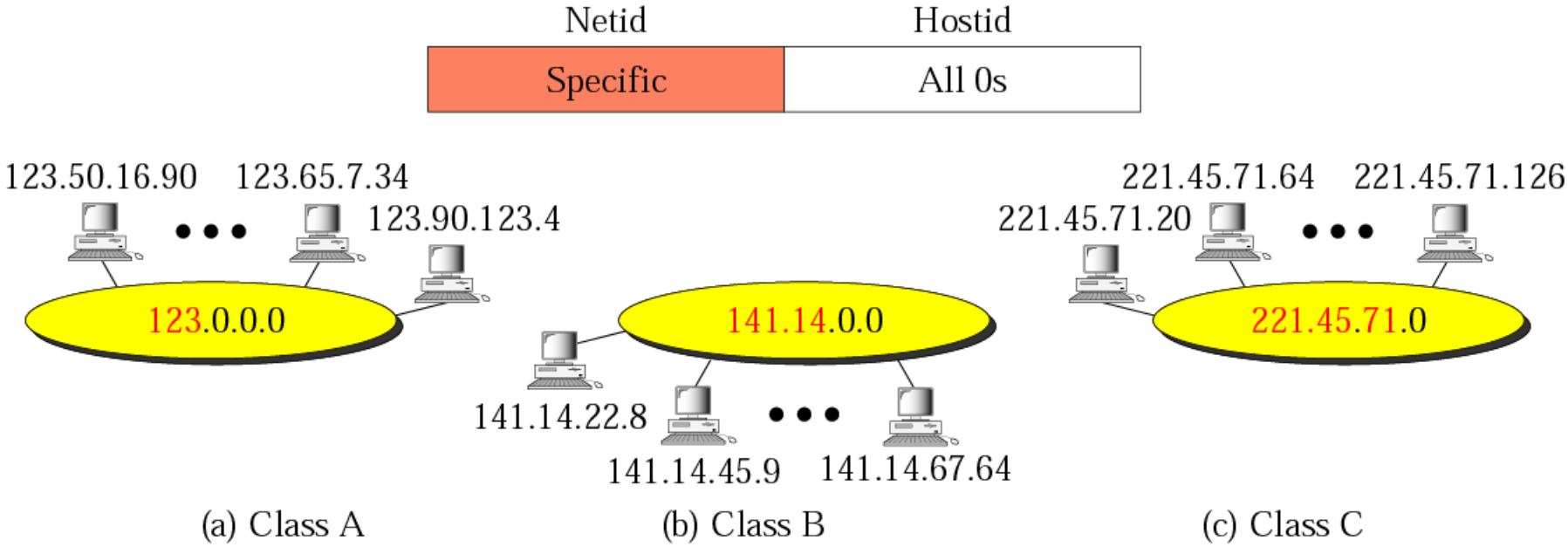
Network Addresses

The network address is the first address.

The network address defines the network to the rest of the Internet.

Given the network address, we can find the class of the address, the block, and the range of the addresses in the block

Network addresses



In classful addressing, the network address (the first address in the block) is the one that is assigned to the organization.

Example

Given the network address 17.0.0.0, find the class, the block, and the range of the addresses.

Solution

The class is A because the first byte is between 0 and 127.
The block has a netid of 17.
The addresses range from 17.0.0.0 to 17.255.255.255.

Example

Given the network address 132.21.0.0, find the class, the block, and the range of the addresses.

Solution

The class is B because the first byte is between 128 and 191.
The block has a netid of 132.21.
The addresses range: 132.21.0.0 to 132.21.255.255.

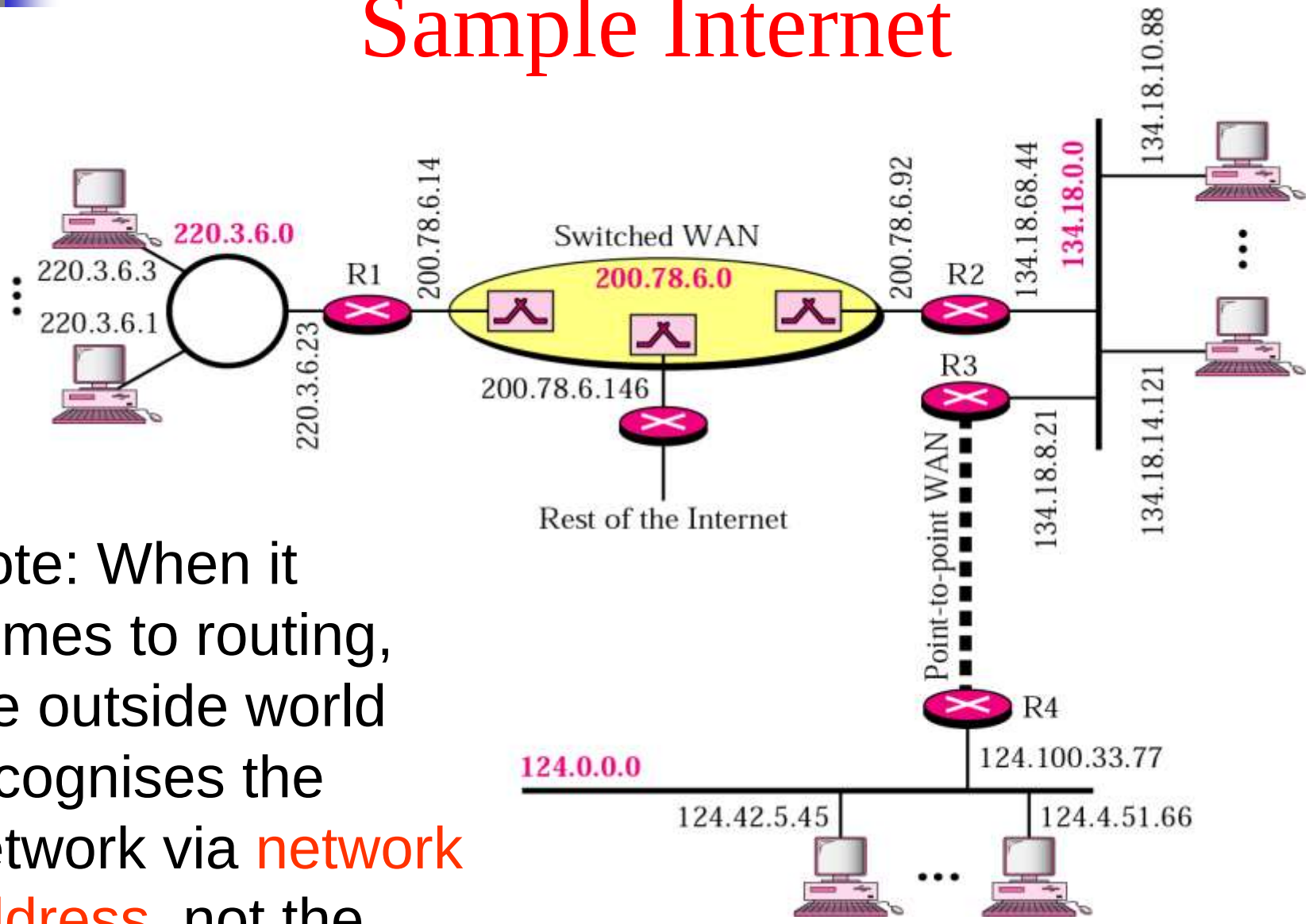
Example

Given the network address 220.34.76.0, find the class, the block, and the range of the addresses.

Solution

The class is C because the first byte is between 192 and 223.
The block has a netid of 220.34.76.
The addresses range from 220.34.76.0 to 220.34.76.255.

Sample Internet



Note: When it comes to routing, the outside world recognises the network via network address, not the individual host-IPs

Network Addresses

*The **network address** is the **beginning address** of each block. It can be found by applying the **default mask** to any of the IP addresses in the block.*

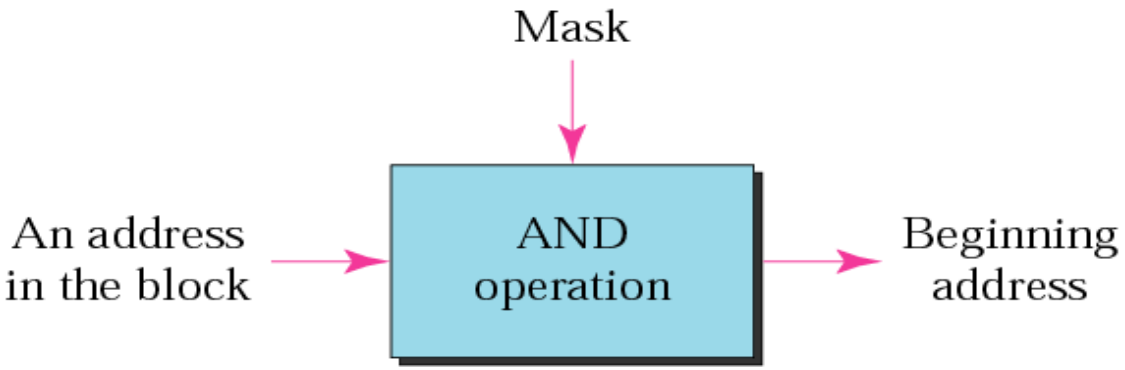
*It retains the **netid** of the block and sets the **hostid** to zero.*

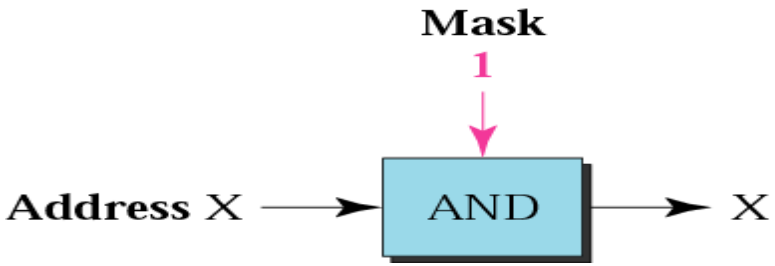
We must not apply the default mask of one class to an address belonging to another class.

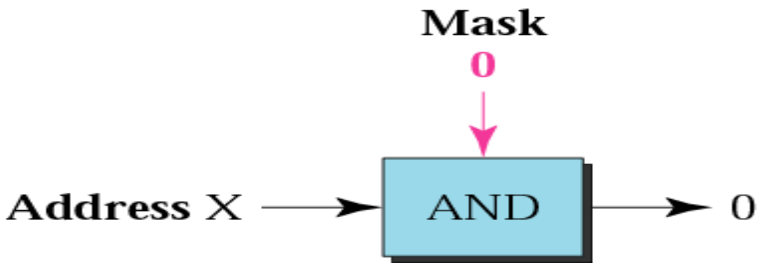
Part B:
Concepts of Subnet & Mask in Network Layer

Mask

A mask is a 32-bit binary number or 4-bytes that gives the first address in the block (the network address) when bitwise ANDed with an address in the block.







Default Mask

Default class A mask is 255.0.0.0

Default class B mask is 255.255.0.0

Default class C mask is 255.255.255.0

Example

Given the address 23.56.7.91 and the default class A mask, find the beginning address (network address).

Solution

The default mask is 255.0.0.0, which means that only the first byte is preserved and the other 3 bytes are set to 0s. The network address is 23.0.0.0.

Example

Given the address 132.6.17.85 and the default class B mask, find network address.

Solution

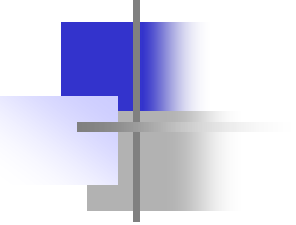
The default mask is 255.255.0.0, which means that the first 2 bytes are preserved and the other 2 bytes are set to 0s. The network address is 132.6.0.0.

Example

Given the address 201.180.56.5 and the class C default mask, find the network address.

Solution

The default mask is 255.255.255.0, which means that the first 3 bytes are preserved and the last byte is set to 0. The network address is 201.180.56.0.



IP-Addressing/Subnetting

a) IP address designed with 2 levels of hierarchy: network-ID & host-ID.

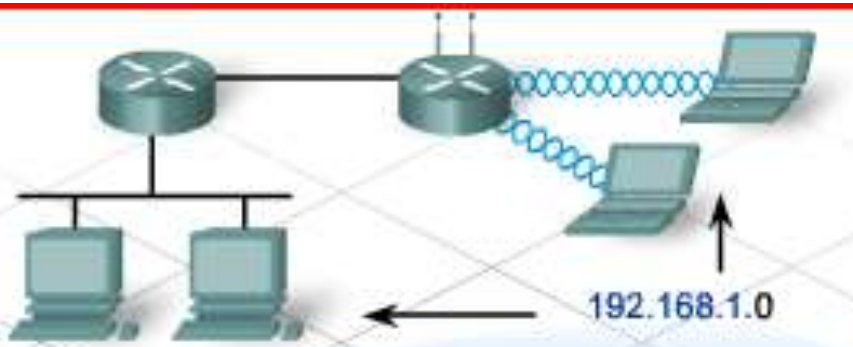
b) However, often organisation needs to assemble the hosts into groups: the network needs to be divided into several subnetworks (subnets); hence requires 3 levels of hierarchy. (netid: subnetid : hostid)

c) The outside world only knows the organisation by its network address. Inside the organisation each sub-network is recognised by its sub-network address.

d) In subnetting, a network is divided into several smaller groups that have its own subnet address depends on the hierarchy of subnetting but still appear as a single network to the rest of the Internet.

e) The question is how a router knows whether it is a network address or a subnet? The key is using the **subnet mask**. (similar to def. mask).

f) Only the network administrator knows about the network address and subnet address but router does not. External router has routing table based on network addresses; Internal router has routing table based on subnetwork addresses.

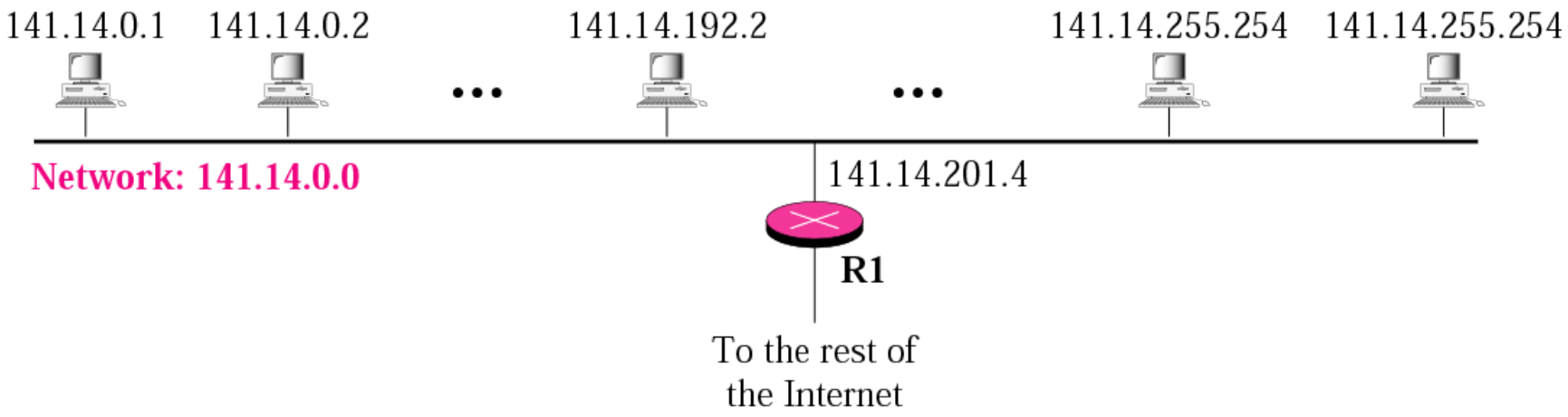


11000000 10101000 00000001 hhhhhhhh

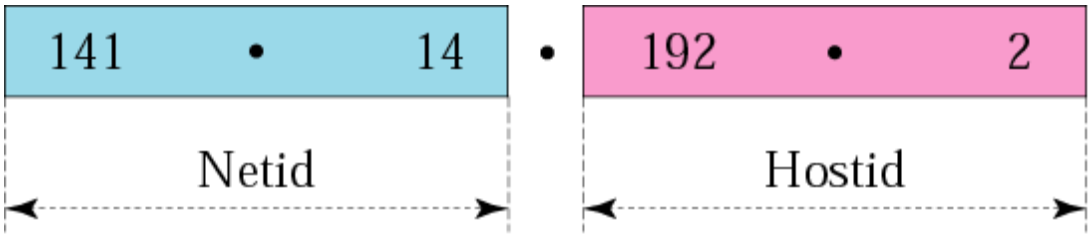
Subnet ID Bits	Host ID Bits	Number of Subnets	Number of Hosts	Bit pattern
0	8	1	254	hhhhhhhh
1	7	2	126	shhhhhhh
2	6	4	62	sshhhhhh
3	5	8	30	sshhhhhh
4	4	16	14	ssshhhhh
5	3	32	6	sssshhh

Our example network has fewer than six hosts in it. If we had to really subnet this network, would we choose to break it into two subnets, or would we choose to break it into the number of subnets that support 6 hosts?

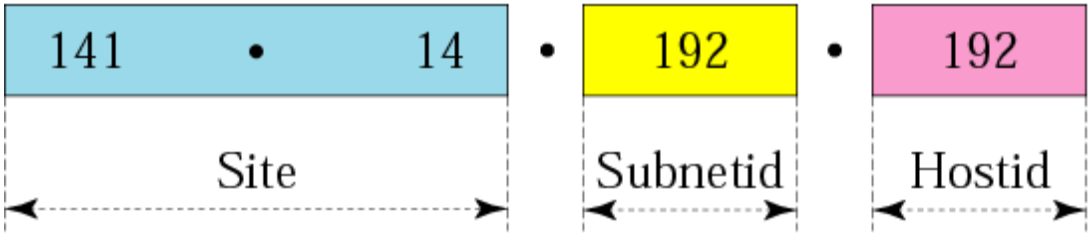
A network with two levels of hierarchy (not subnetted)



Addresses in a network
With and without subnetting



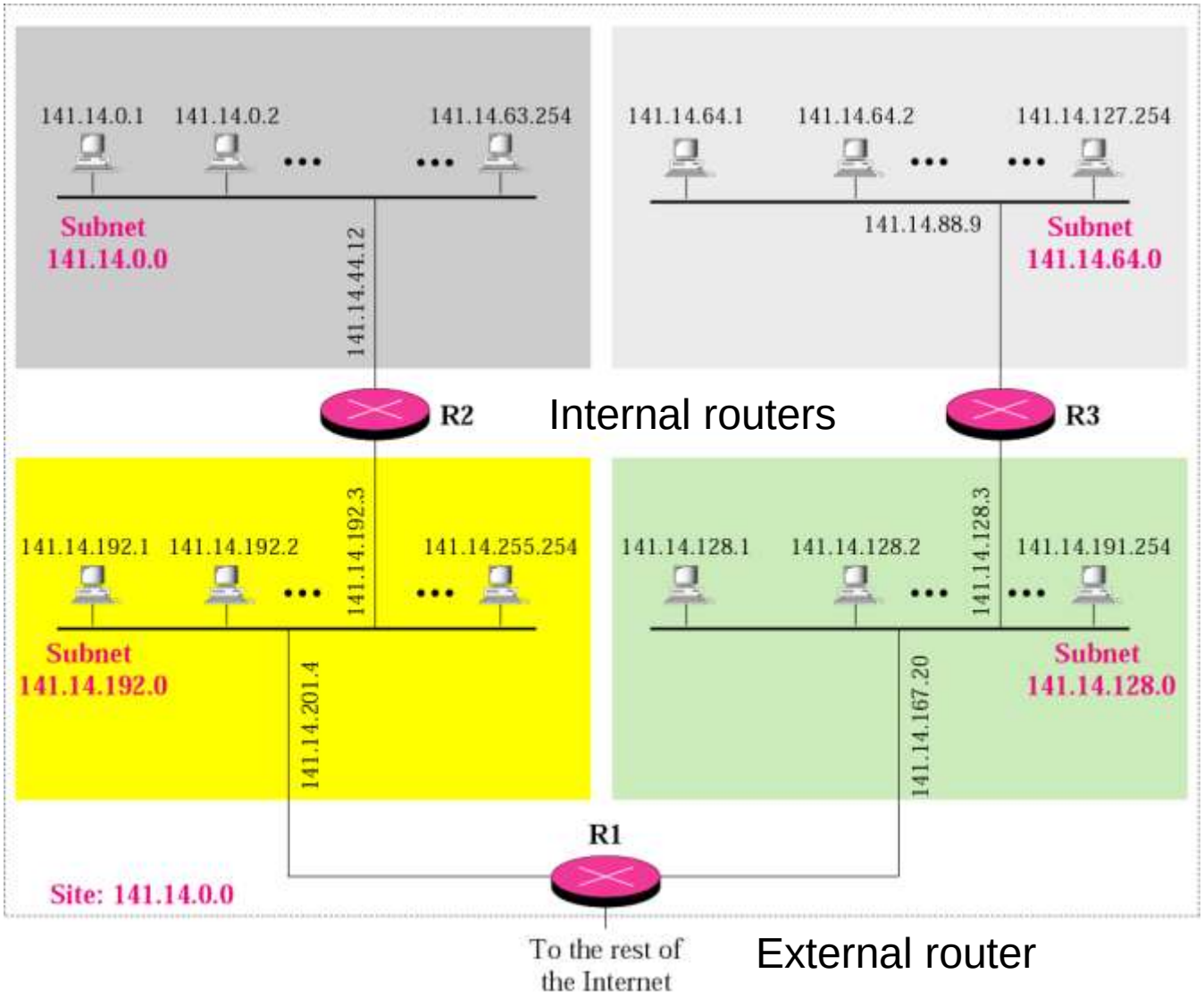
a. Without subnetting



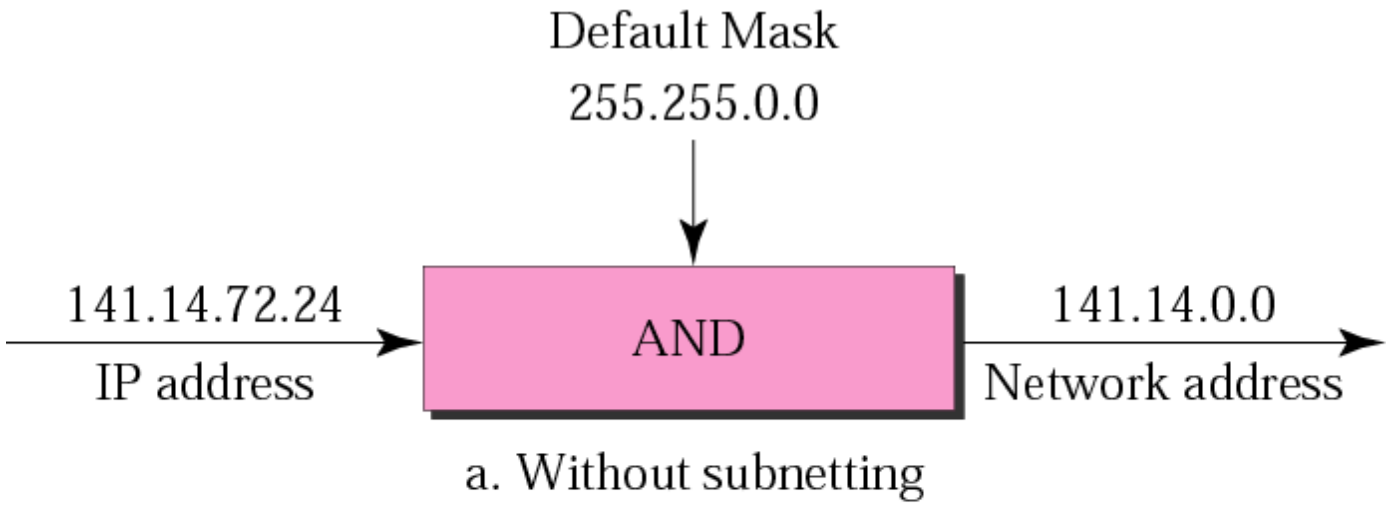
b. With subnetting

Just like telephone system

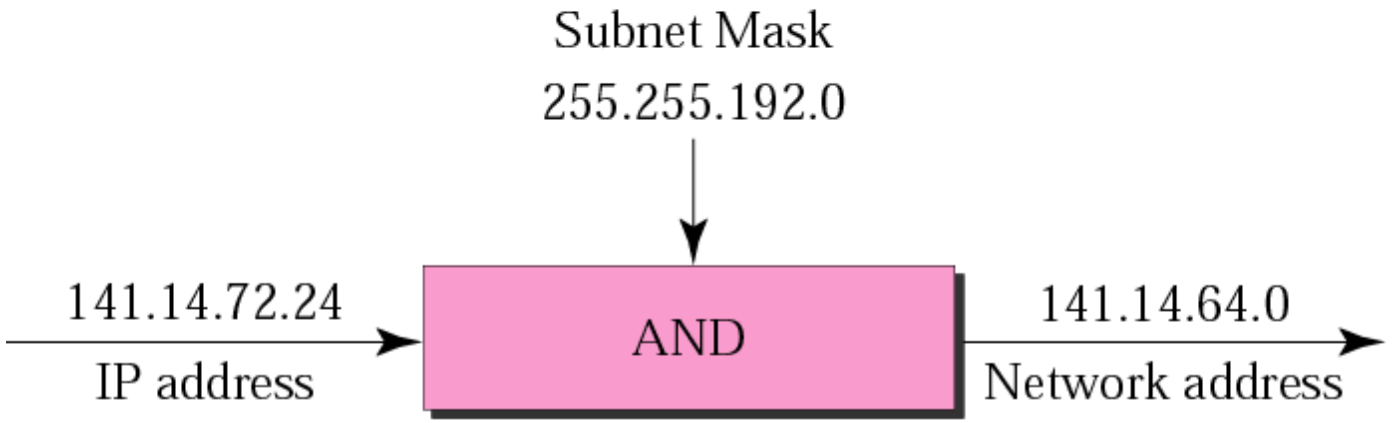
A network with three levels of hierarchy (subnetted)



Default mask and subnet mask



a. Without subnetting



b. With subnetting

Finding the Subnet Address

Given an IP address, we can find the subnet address the same way we found the network address in the previous chapter.

We apply the mask to the address.

We can do this in two ways:
straight or short-cut.

Straight Method

In the straight method, we use binary notation for both the address and the mask and then apply the AND operation to find the subnet address.

Short-Cut Method

** If the byte in the mask is 255, copy the byte in the address.

** If the byte in the mask is 0, replace the byte in the address with 0.

** If the byte in the mask is neither 255 nor 0, we write the mask and the address in binary and apply the AND operation.

Example

What is the sub-network address if the destination address is 200.45.34.56 given that the subnet mask is 255.255.240.0?

Solution

11001000 00101101 00100010 00111000

11111111 11111111 1111**0000** **00000000**

11001000 00101101 0010**0000** **00000000**

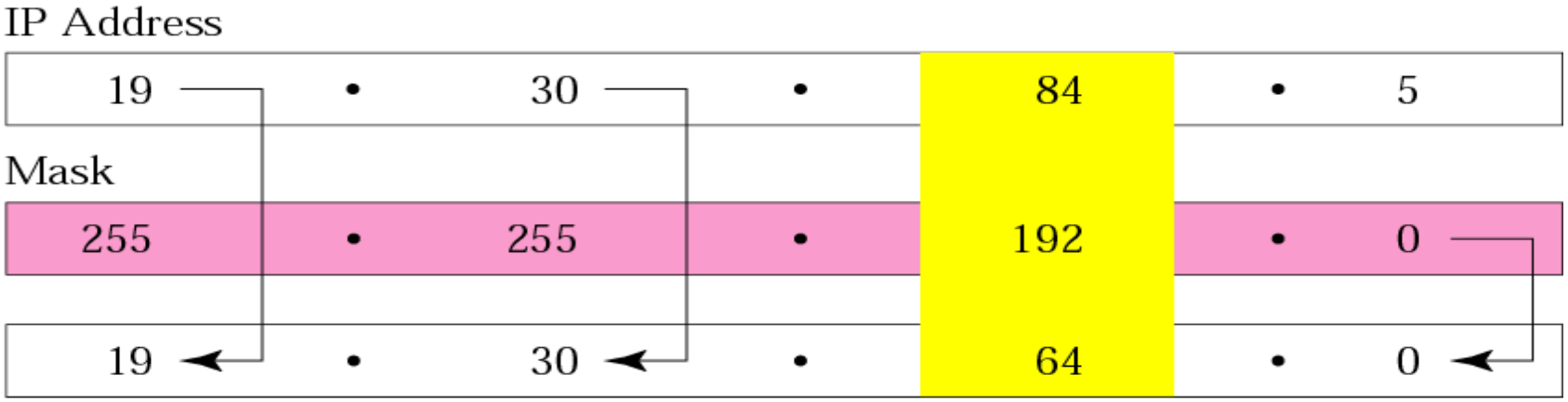
The subnetwork address is **200.45.32.0**.

Example

What is the sub-network address if the destination address is 19.30.80.5 and the mask is 255.255.192.0?

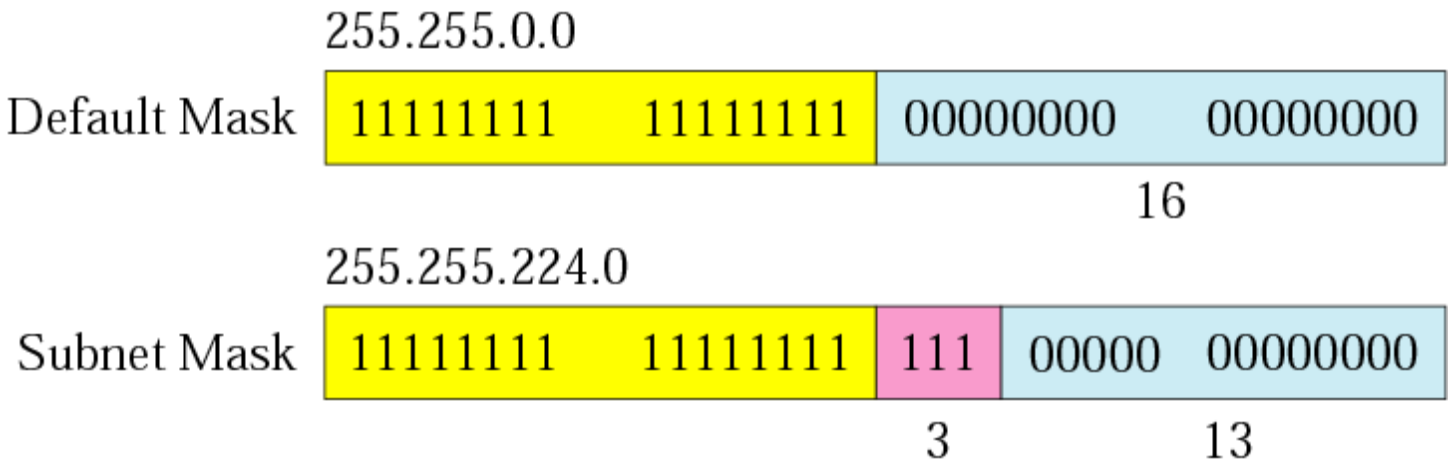
Solution

Answer: Subnet Address = 19.30.64.0



84	0	1	0	1	0	1	0	0
192	1	1	0	0	0	0	0	0
64	0	1	0	0	0	0	0	0

Comparison of a default mask and a subnet mask



Note

The number of subnets must be a power of 2.

Example

A company is granted the site address 201.70.64.0 (class C). The company needs six subnets. Design the subnets.

Solution

The number of 1s in the default mask is 24 (class C).

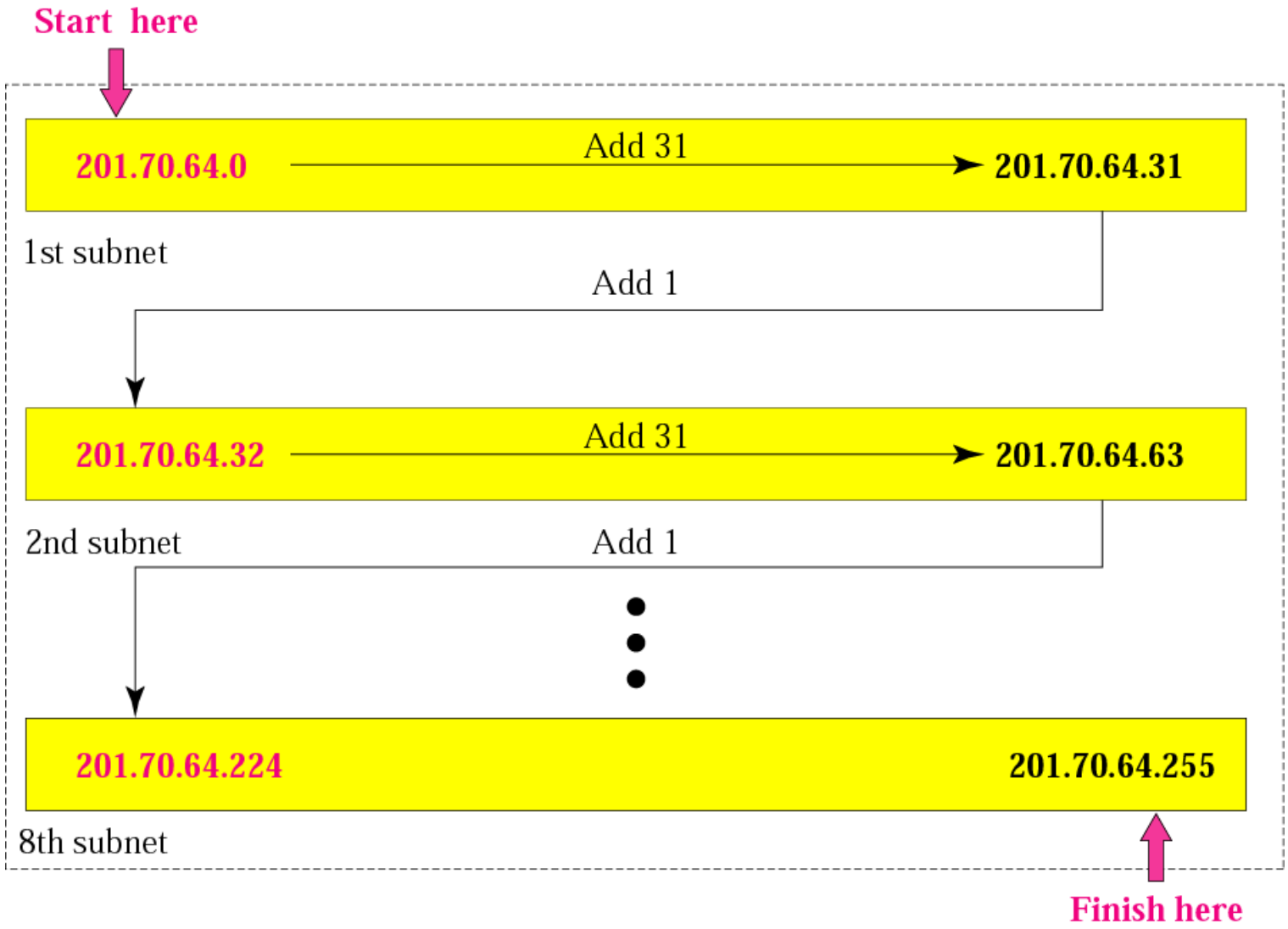
The company needs six subnets. Since 6 is not a power of 2, the next number that is a power of 2 is 8 (2^3). That means up to 8 subnets.

Hence, we need 3 more '1's in the subnet mask = 11111111.11111111.11111111.11100000 or 255.255.255.224

The total number of 1s in the subnet mask is 27 (24 + 3).

Since the total number of 0s is 5 (32 - 27).

The number of addresses in each subnet is 2^5 (5 is the number of 0s) or 32.


Start here
201.70.64.0
Add 31
201.70.64.31
1st subnet
Add 1
201.70.64.32
Add 31
201.70.64.63
2nd subnet
Add 1
201.70.64.224
201.70.64.255
8th subnet
Finish here

Example

A company is granted the site address 181.56.0.0 (class B). The company needs 1000 subnets. Design the subnets.

Solution

The number of 1s in the default mask is 16 (class B).

The company needs 1000 subnets. Since it is not a power of 2, the next number is 1024 (2^{10}). We need 10 more 1s in the subnet mask.

The total number of 1s in the subnet mask is 26 (16 + 10).

The total number of 0s is 6 (32 – 26).

Solution (Continued)

The submask is

11111111 11111111 11111111 11000000

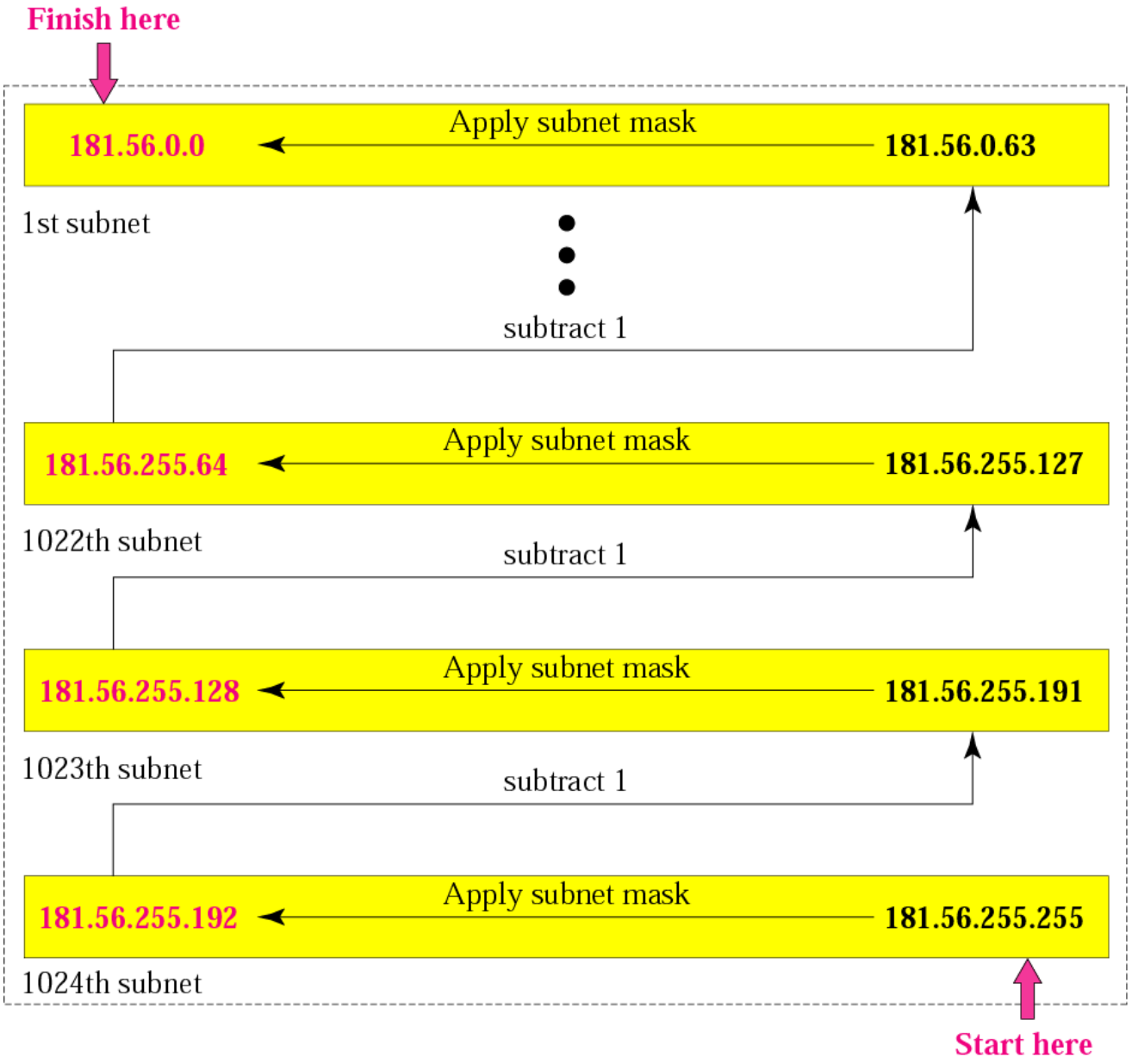
or

255.255.255.192.

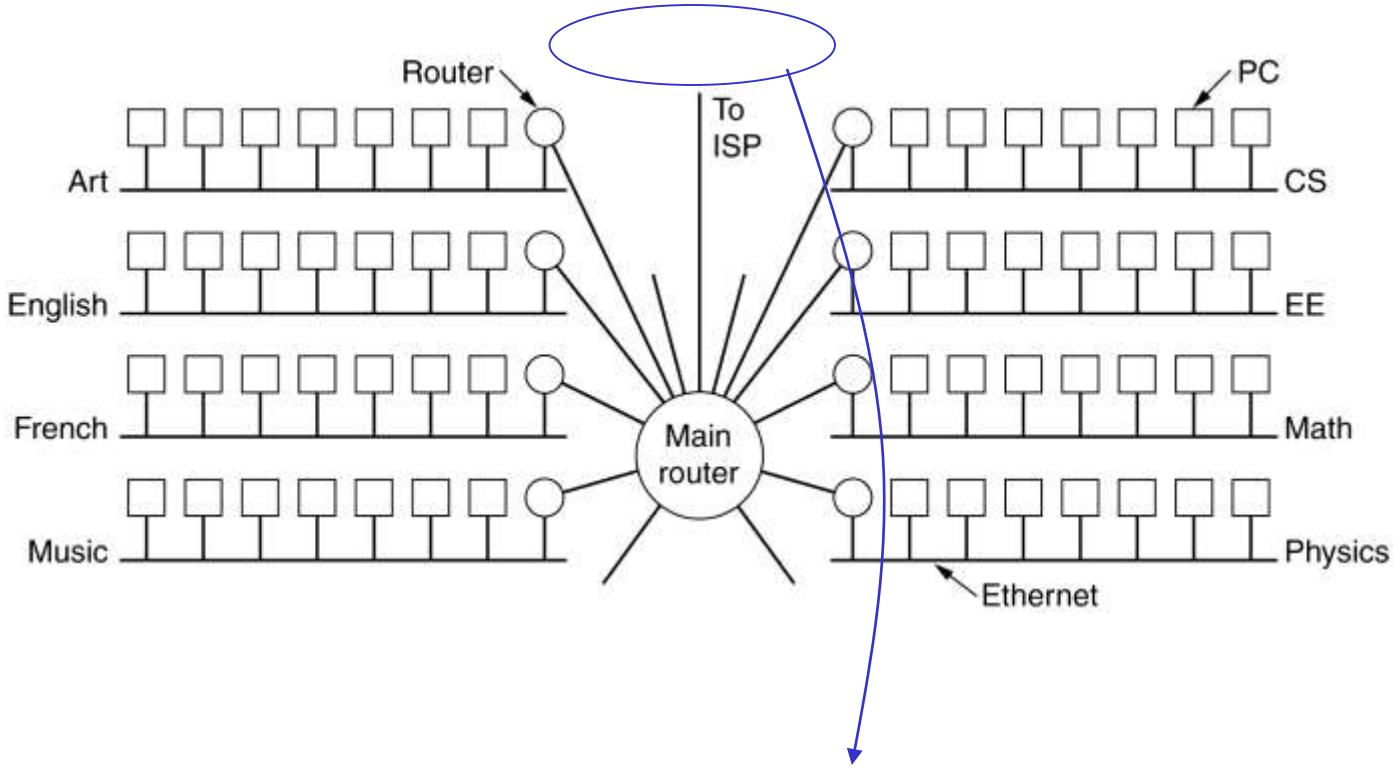
The number of subnets is 1024.

The number of addresses in each subnet is 2^6 (6 is the number of 0s) or 64.

Example


Finish here
181.56.0.0
Apply subnet mask
181.56.0.63
1st subnet
subtract 1
181.56.255.64
Apply subnet mask
181.56.255.127
1022th subnet
subtract 1
181.56.255.128
Apply subnet mask
181.56.255.191
1023th subnet
subtract 1
181.56.255.192
Apply subnet mask
181.56.255.255
1024th subnet
Start here

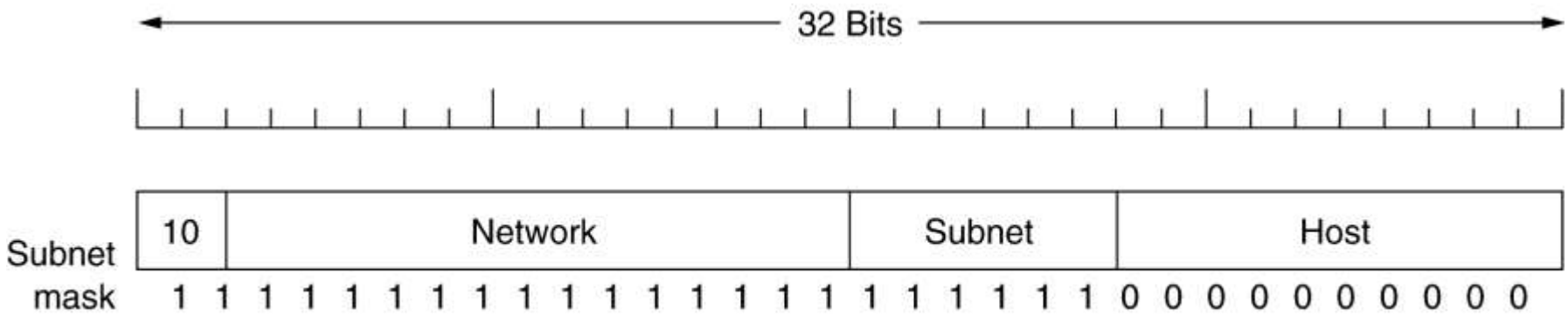
Subnetting in Classful Addresses



10000000 00010100 00000000 00000000

Class B addess	Network Prefix	Host Suffix	
Subnetting with /20 mask	Network Prefix	Subnet ID	Host ID

Subnetting in Classful Addresses



4.1.2 Subnetting a Network

In the original IP address hierarchy, there are two levels: a network and a host. In a classful addressing scheme, the first three leading bit values are used to determine that an IP address is either a Class A, B, or C. When an address is identified by class, the number of bits that make up the network ID and the number of bits that make up the host ID are known. The default subnet masks for the network classes are:

Class A 255.0.0.0

Class B 255.255.0.0

Class C 255.255.255.0

Subdividing a classful network adds a level to the network hierarchy. Now there are three levels: a network, a subnetwork, and a host. How can the subnet mask be modified to indicate the new hierarchical level?

A single Class A, B, or C network address space can be divided into multiple subnetworks by using bits from the host address space to designate the subnet ID. As an example, an organization using a Class C address space has two offices in different buildings. To make the network easier to manage, the network administrators want each location to have a logically separate network. Taking two bits from the host address increases the subnet mask length from the default 24 bits to 26 bits, or 255.255.255.192.

When bits are borrowed from the host portion of the address to identify the subnet, fewer bits are available for individual hosts. If two bits are used for the subnet ID, only six bits are left in the host portion of the address.

Determine the network ID of each IP address.
Enter the binary and decimal values of each octet in the spaces provided.

Host Address	10	253	211	79
Subnet Mask	255	255	255	224
Host Address in binary	00001010	11111101	11010011	01001111
Subnet Mask in binary	11111111	11111111	11111111	11100000
Network Address in binary	00001010	11111101	11010011	01000000
Network Address in decimal	10	253	211	64

4.1.2 Subnetting a Network

With traditional classful subnetting, the same number of host bits is used to designate the subnet ID for all the resulting subnetworks. This type of subnetting always results in a fixed number of subnets and a fixed number of hosts per subnet. For this reason, this is known as fixed-length subnetting.

The decision about how many host bits to use for the subnet ID is a big planning decision. There are two considerations when planning subnets: the number of hosts on each network, and the number of individual local networks needed. The table for the subnet possibilities for the 192.168.1.0 network shows how the selection of a number of bits for the subnet ID affects both the number of possible subnets and the number of hosts that can be in each subnet.

One thing to keep in mind is that in all IPv4 networks, two host addresses are reserved: the all-0s and the all-1s. An address with all 0s in the host portion of the address is an invalid host address and usually refers to the entire network or subnetwork. An address with all 1s in the host portion is used as the local network broadcast address. When a network is subnetted, each subnet contains an all-0s and an all-1s host address that cannot be used for individual host addresses.

Only one network address is available.

192.168.1.0 (/24)	Address:	11000000.10101000.00000001.00000000
255.255.255.0	Mask:	11111111.11111111.11111111.00000000

← Network portion of the address →

Borrow a bit from the host portion

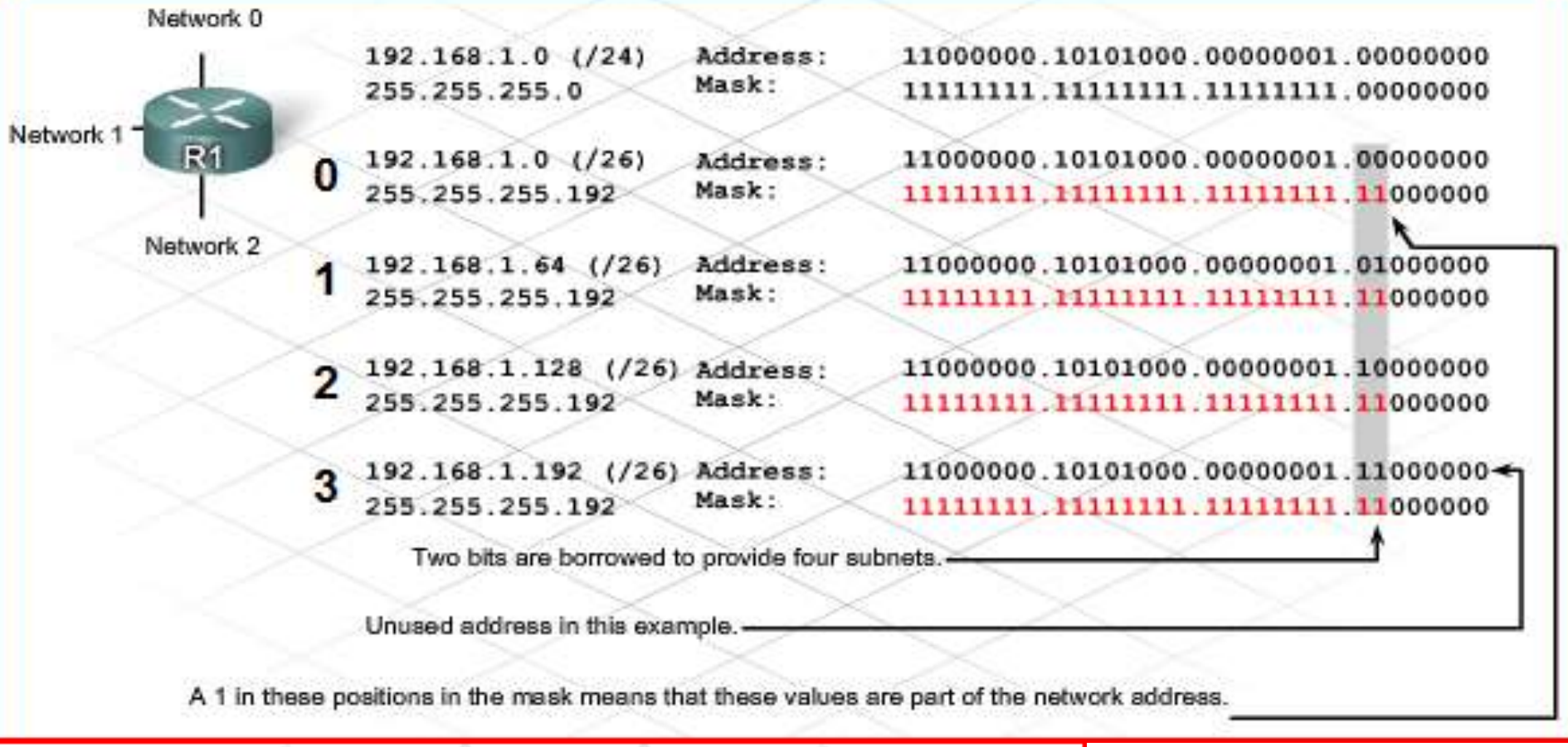
With subnetting, two network addresses are available.

0	192.168.1.0 (/25)	Address:	11000000.10101000.00000001.00000000
	255.255.255.128	Mask:	11111111.11111111.11111111.10000000
1	192.168.1.128 (/25)	Address:	11000000.10101000.00000001.10000000
	255.255.255.128	Mask:	11111111.11111111.11111111.10000000

← Increase the network portion of the address →

Addressing Scheme: Example of 2 networks

Subnet	Network Address	Host range	Broadcast Address
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255



Addressing Scheme: Example of 4 networks

Subnet	Network Address	Host Range	Broadcast Address
0	192.168.1.0/26	192.168.1.1 - 192.168.1.62	192.168.1.63
1	192.168.1.64/26	192.168.1.65 - 192.168.1.126	192.168.1.127
2	192.168.1.128/26	192.168.1.129- 192.168.1.190	192.168.1.191
3	192.168.1.192/26	192.168.1.193 - 192.168.1.254	192.168.1.255

More subnets are available, but fewer addresses are available per subnet.

Part C:
Concept of Classless Addressing in Network Layer

Classless Addressing

a) The idea of Classful addressing has created many problems.

b) Until mid-1990s, a range of addresses meant a block of addresses in class A, B or C.

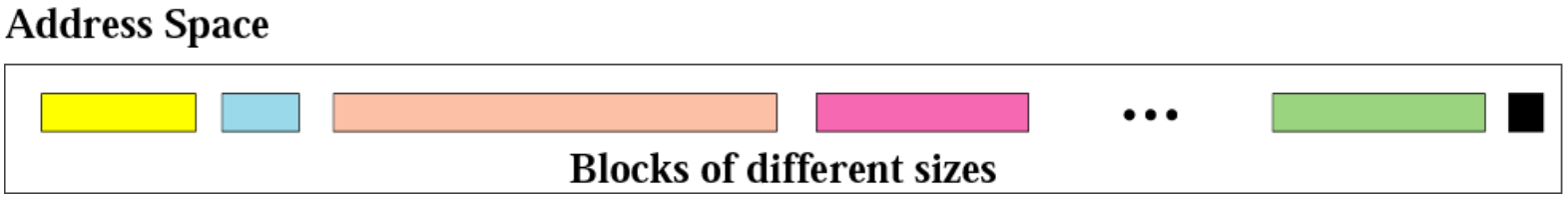
c) The minimum number of addresses granted to an organisation as 256 (class C); the maximum is 16,777,216 (class A).

d) In between these limits, an organisation could have a class B block or several class C blocks. However, the choices were limited.

e) In addition, what about the small business that needed only 16 addresses? Or a household that needed only 2 addresses?

f) Solution: Classless addressing (from 1996)

g) The idea is to have variable-length blocks that belongs to no class.



Classless Addressing Rules:

Number of Addresses in a Block

There is only one condition on the number of addresses in a block; it must be a power of 2 (2, 4, 8, . . .).

For exmaple, a household may be given a block of 2 addresses. A small business may be given 16 addresses. A large organization may be given 1024 addresses.

Classless Addressing Rules:

Beginning Address

The beginning address must be evenly divisible by the number of addresses.

For example, if a block contains 4 addresses, the beginning address must be divisible by 4. If the block has less than 256 addresses, we need to check only the rightmost byte. If it has less than 65,536 addresses, we need to check only the two rightmost bytes, and so on.

Example

Which of the following can be the beginning address of a block that contains 16 addresses?

205.16.37.32
190.16.42.44
17.17.33.80

123.45.24.52

Solution

The address 205.16.37.32 is eligible because .32 is divisible by 16. The address 17.17.33.80 is eligible because 80 is divisible by 16.

Example

Which of the following can be the beginning address of a block that contains 1024 addresses?

205.16.37.32
190.16.42.0
17.17.32.0

123.45.24.52

Solution

To be divisible by 1024, the rightmost byte of an address should be 0 and the second rightmost byte must be divisible by 4 (2 bits of 2nd byte needed). Only the address 17.17.32.0 meets this condition.

Slash notation

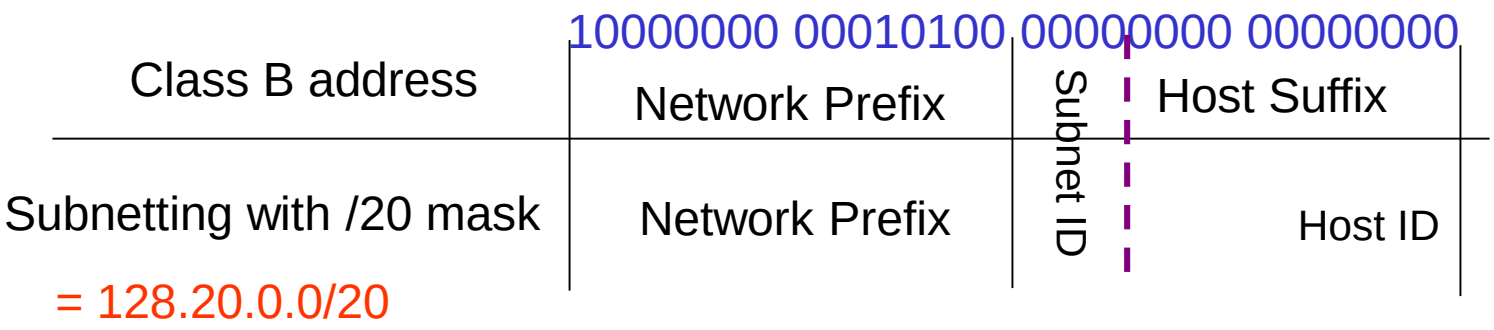
To enable the variable-length blocks, the slash notation is introduced

A.B.C.D/*n*

Slash notation is also called CIDR notation/prefix length represented using '1', as masking.

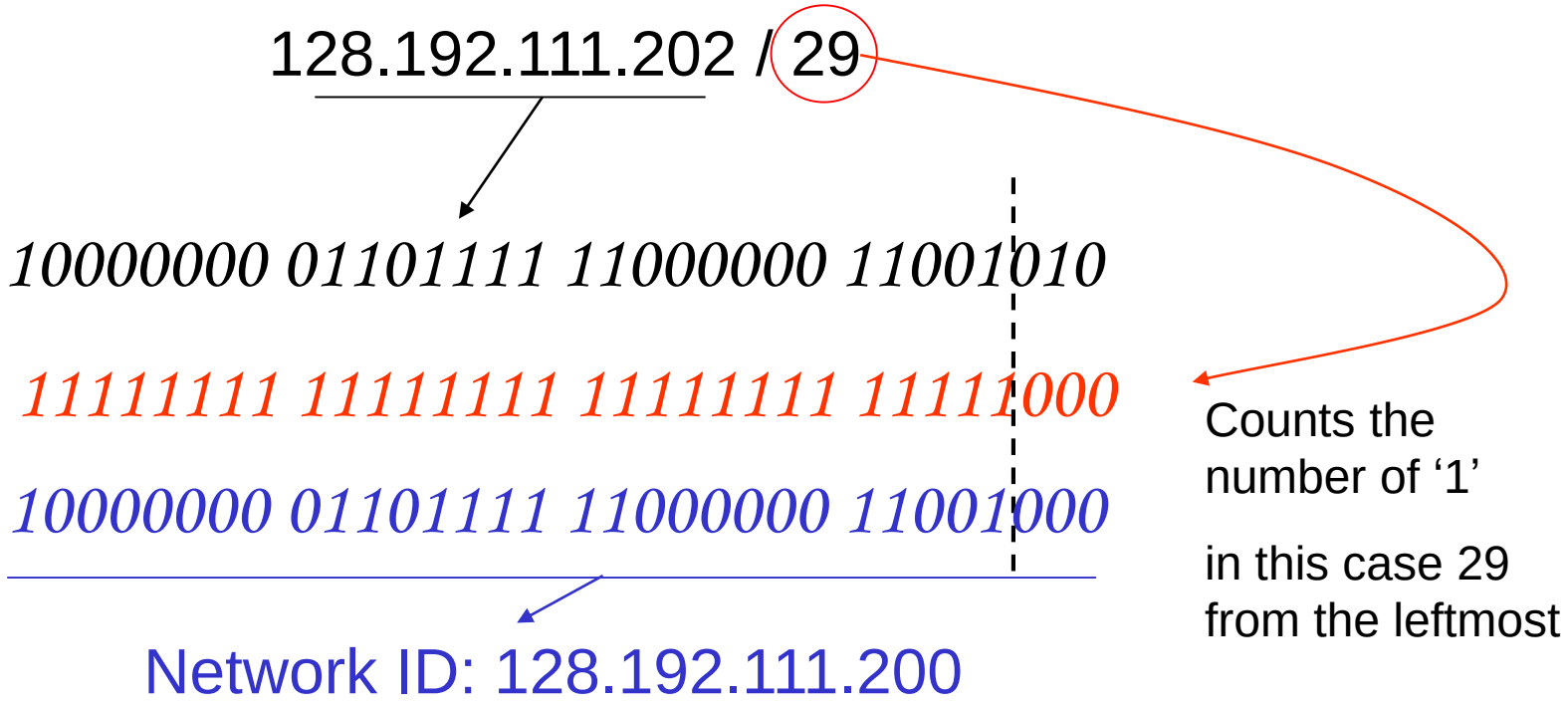
CIDR = Classless InterDomain Routing

*The remaining unmasked '0' is referred to the **suffix length***



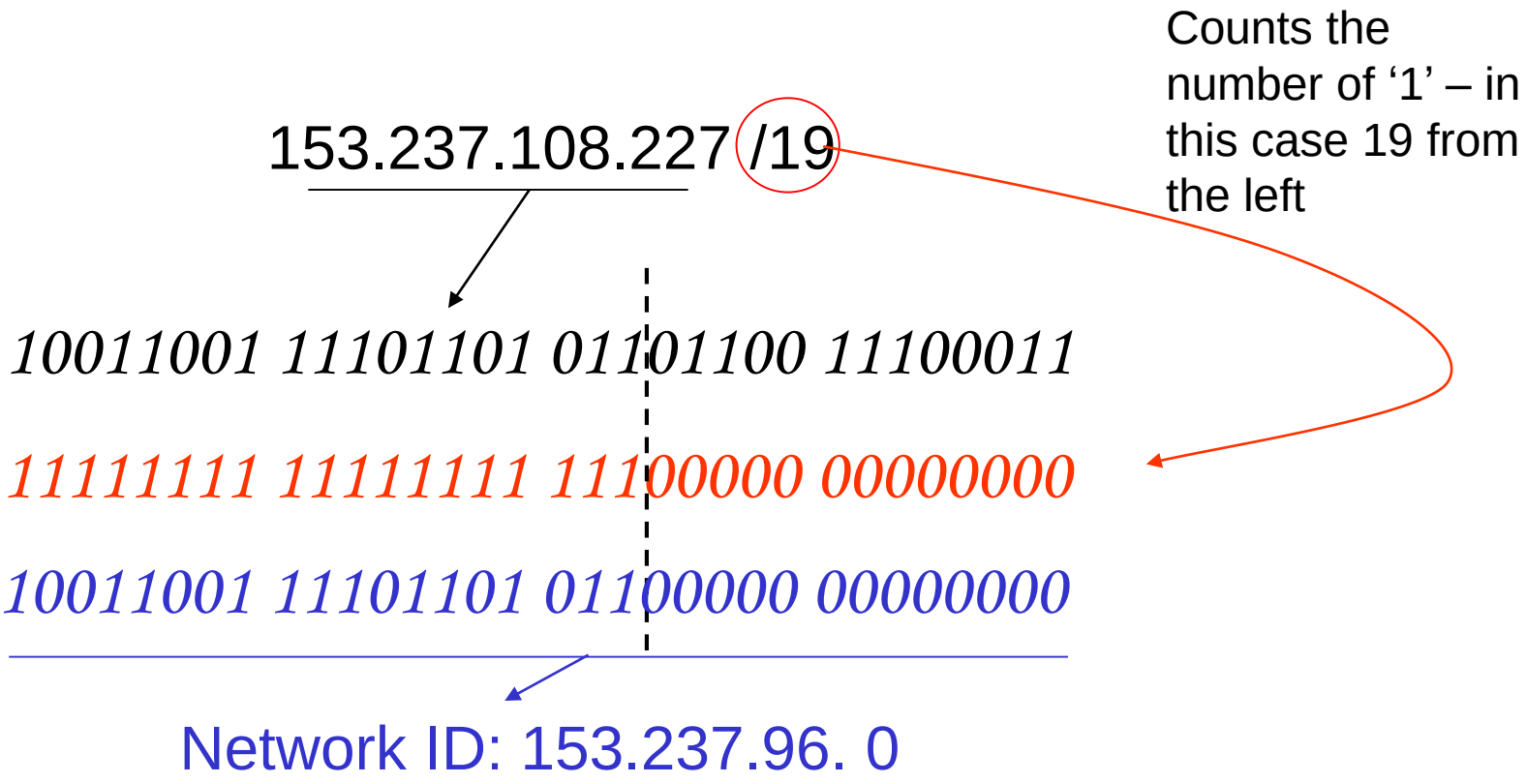
CIDR Addressing in Internet Protocol

CIDR allows each IP address to have a different length of network ID and host ID. In CIDR each IP address is assigned a 32-bit mask to extract the network ID.



The prefix length is 29 and suffix length is 3

CIDR Addressing in Internet Protocol



The prefix length is 19 and suffix length is 13

Example

A small organization is given a block with the beginning address and the prefix length **205.16.37.24/29** (in slash notation). What is the range of the block?

Solution

The beginning address is 205.16.37.24. To find the last address we keep the first 29 bits and change the last 3 bits to 1s.

Beginning: **11001111 00010000 00100101 00011**000
Ending : **11001111 00010000 00100101 00011**111

There are only 8 addresses in this block.

Alternatively, we can argue that the length of the suffix is 32 – 29 or 3. So there are $2^3 = 8$ addresses in this block. If the first address is 205.16.37.24, the last address is 205.16.37.31 (24 + 7 = 31).

A block in classes A, B, and C can easily be represented in slash notation as: A.B.C.D/ *n*
where *n* is either
8 (class A), 16 (class B), or
24 (class C).

Example

What is the network address if one of the addresses is 167.199.170.82/27?

Solution

The prefix length is 27, which means that we must keep the first 27 bits as is and change the remaining bits (5) to 0s. The 5 bits affect only the last byte. The last byte is 01010010. Changing the last 5 bits to 0s, we get 01000000 or 64. The network address is 167.199.170.64/27.

Example

An organization is granted the network address block of 130.34.12.64/26. The organization needs to have four subnets. What are the subnet addresses and their range for each subnet?

Solution

The suffix length is 6 (32-26). This means the total number of addresses in the block is 64 (2^6). If we create four subnets, each subnet will have 16 addresses. Let us first find the subnet prefix (subnet mask). We need four subnets, which means we need to add two more '1's to the site prefix /26. The subnet prefix is then /28.

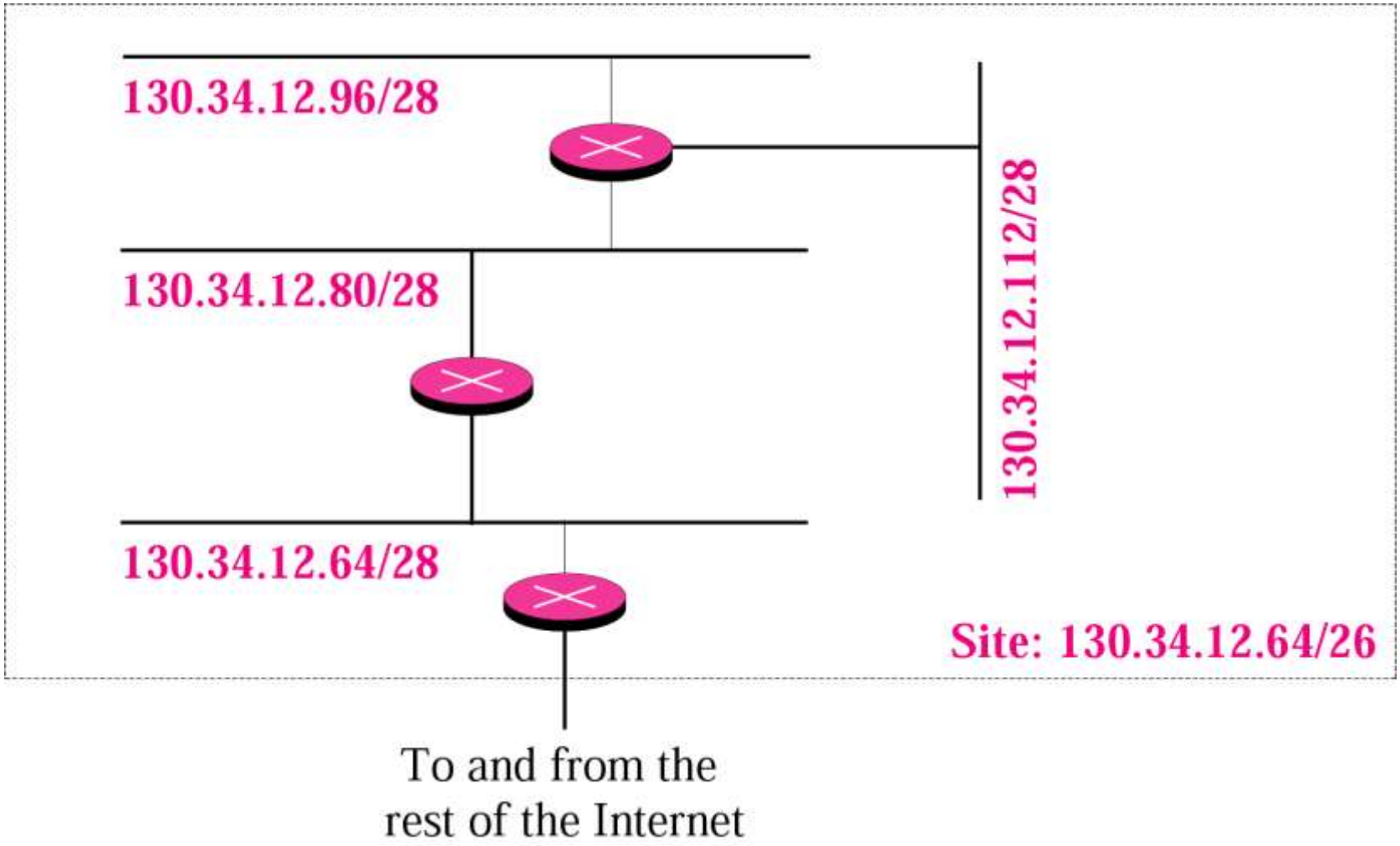
Subnet 1: 130.34.12.64/28 to 130.34.12.79/28.

Subnet 2 : 130.34.12.80/28 to 130.34.12.95/28.

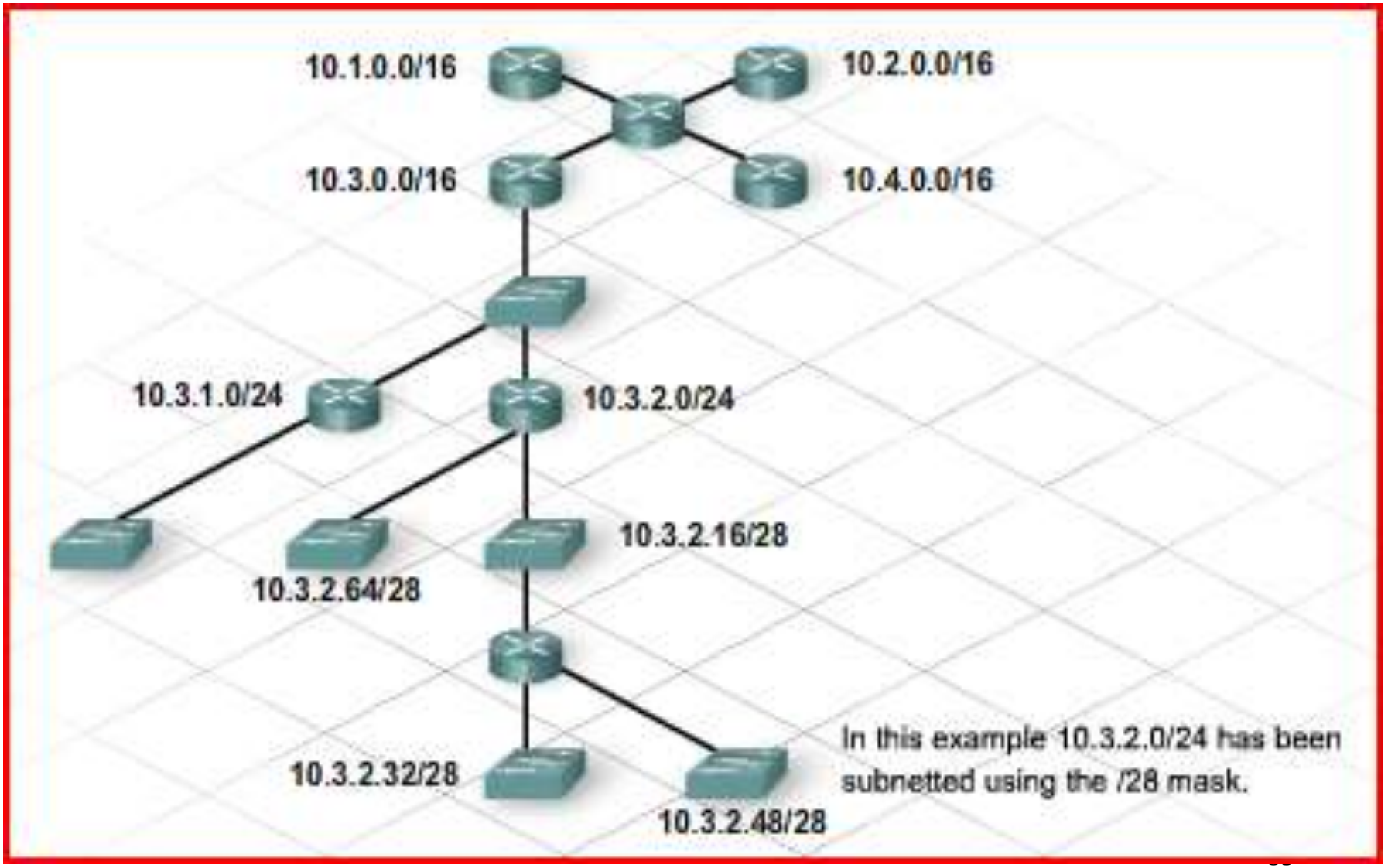
Subnet 3: 130.34.12.96/28 to 130.34.12.111/28.

Subnet 4: 130.34.12.112/28 to 130.34.12.127/28.

Example


130.34.12.96/28
130.34.12.80/28
130.34.12.64/28
130.34.12.112/28
Site: 130.34.12.64/26
To and from the
rest of the Internet

Example


10.1.0.0/16
10.2.0.0/16
10.3.0.0/16
10.4.0.0/16
10.3.1.0/24
10.3.2.0/24
10.3.2.16/28
10.3.2.64/28
10.3.2.32/28
10.3.2.48/28
In this example 10.3.2.0/24 has been subnetted using the /28 mask.

Example

Activity

Determine the /slash format of the subnet mask necessary to accommodate the required number of hosts.

Drag the /slash format to the correct host requirement.

25 hosts	
100 hosts	
1000 hosts	
5 hosts	
45 hosts	
400 hosts	
12 hosts	
2 hosts	

/27 /22 /32 /23 /24 /25 /30 /19 /28 /26 /29

Example

An ISP is granted a block of addresses starting with 190.100.0.0/16. The ISP needs to distribute these addresses to three groups of customers as follows:

1. The first group has 64 customers; each needs 256 addresses.
2. The second group has 128 customers; each needs 128 addresses.
3. The third group has 128 customers; each needs 64 addresses.

Design the subblocks and give the slash notation for each subblock. Find out how many addresses are still available after these allocations.

Solution

Group 1

For this group of 64 customers, each customer needs 256 addresses. This means the suffix length is 8 ($2^8 = 256$). The prefix length is then $32 - 8 = 24$.

01: 190.100.0.0/24 ➔ 190.100.0.255/24

02: 190.100.1.0/24 ➔ 190.100.1.255/24

……..

64: 190.100.63.0/24 ➔ 190.100.63.255/24

Total = $64 \times 256 = 16{,}384$

Solution (Continued)

Group 2

For this group of 128 customers, each customer needs 128 addresses. This means the suffix length is 7 ($2^7 = 128$). The prefix length is then $32 - 7 = 25$. The addresses are:

001: 190.100.64.0/25 ➔ 190.100.64.127/25

002: 190.100.64.128/25 ➔ 190.100.64.255/25

.....

127: 190.100.127.0/25 ➔ 190.100.127.127/25

128: 190.100.127.128/25 ➔ 190.100.127.255/25

Total = $128 \times 128 = 16{,}384$

Solution (Continued)

Group 3

For this group of 128 customers, each customer needs 64 addresses. This means the suffix length is 6 ($2^6 = 64$). The prefix length is then 32 – 6 = 26.

001:190.100.128.0/26 ➔190.100.128.63/26

002:190.100.128.64/26 ➔190.100.128.127/26

……

128:190.100.159.192/26 ➔190.100.159.255/26

Total = 128 × 64 = 8,192

Solution (Continued)

Number of granted addresses: 65,536

Number of allocated addresses: 40,960

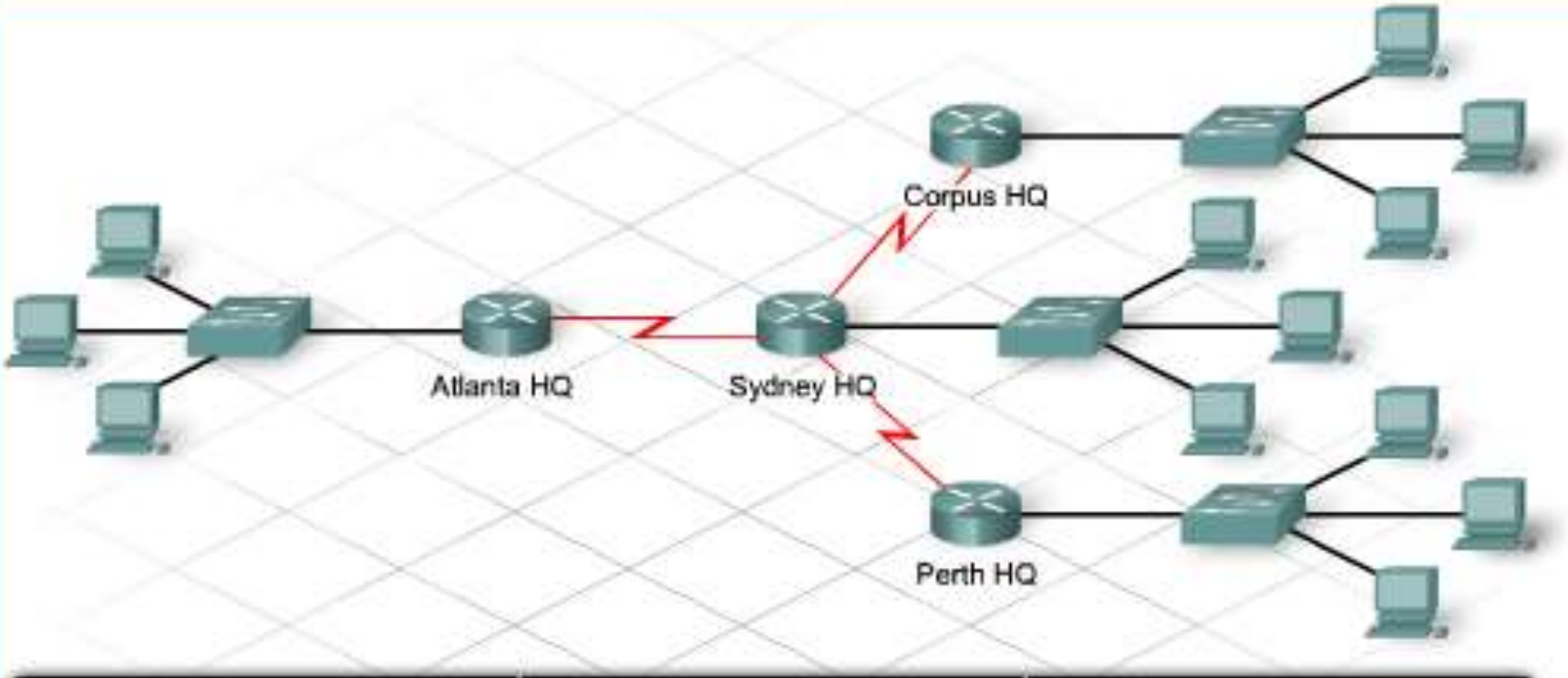
Number of available addresses: 24,576

The available addresses range from:

190.100.160.0 → 190.100.255.255

Total = 96 × 256 = 24,576

Example



Headquarters	Actual Requirements	Total Wasted Addresses
Atlanta HQ	58 host addresses	4 addresses
Perth HQ	26 host addresses	36 addresses
Sydney HQ	10 host addresses	52 addresses
Corpus HQ	10 host addresses	52 addresses
WAN Links	2 host addresses (each)	60 addresses

Example

Name-required addresses	Subnet address	Address range	Broadcast Address	Network/prefix
AtlantaHQ-58	192.168.15.0	.1 - .62	.63	192.168.15.0/26
PerthHQ-28	192.168.15.64	.65 - .94	.95	192.168.15.64/27
SydneyHQ-10	192.168.15.96	.97 - .110	.111	192.168.15.96/28
CorpusHQ-10	192.168.15.112	.113 - .126	.127	192.168.15.112/28
WAN1-2	192.168.15.128	.129 - .130	.131	192.168.15.128/30
WAN2-2	192.168.15.132	.133 - .134	.135	192.168.15.132/30
WAN3-2	192.168.15.136	.137 - .138	.139	192.168.15.136/30

Three point-to-point WAN links require two addresses each.
Use the next available address 192.168.15.128/28.
Borrow 2 more bits with a /30 mask.
This creates subnets: 192.168.15.128, 192.168.15.132, 192.168.15.136.
Use all three subnets, one for each WAN.

Exercise/Tutorial

Activity

Create an IP addressing scheme for the specified requirements.

Fill in the table with appropriate values to complete the IP addressing scheme required.

IP Address: **192.168.5.0/24**

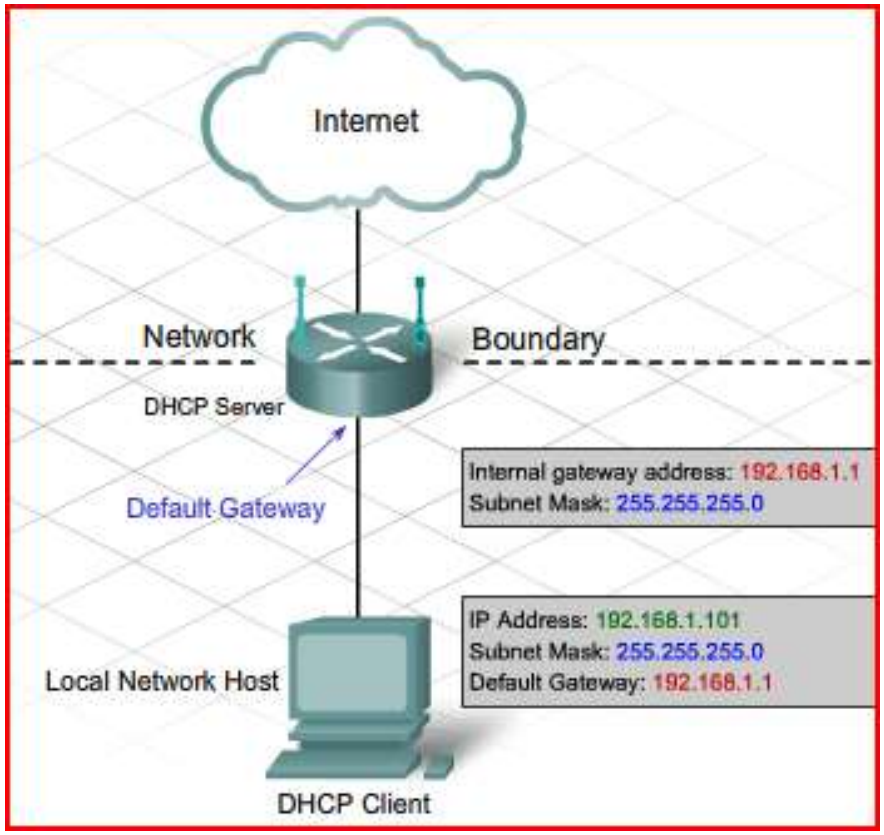
Host Requirements	/Slash	# of hosts	Subnet	Host Range	Broadcast
60	/26	62	192.168.5.0	.1 - .62	.63
30					
25					
10					
2					
2					

Part D:
Concept of Private Address and NAT in Network Layer

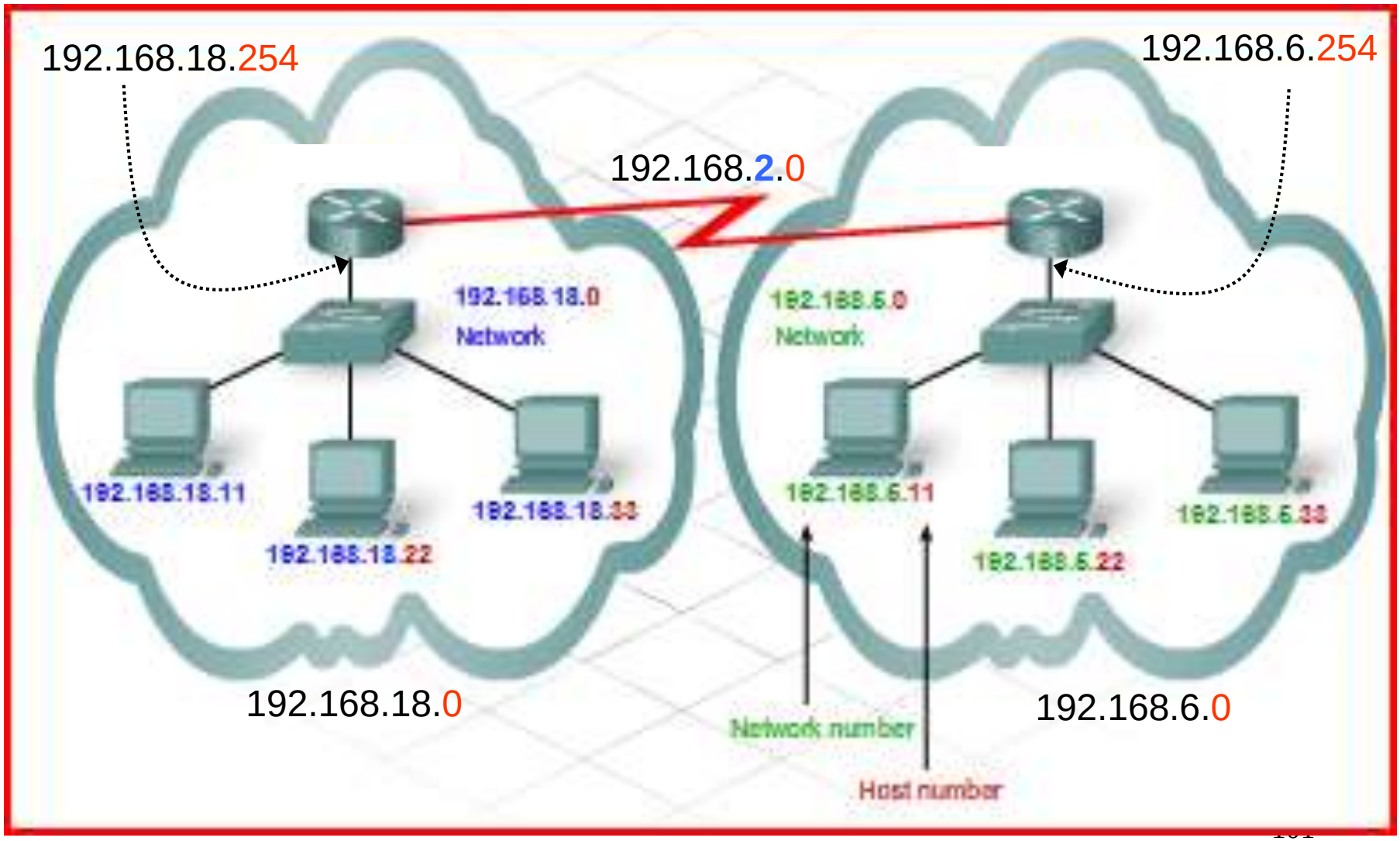
Router - Gateway

a) The router provides a gateway through which hosts on one network can communicate with hosts on different networks.

b) Each interface on a router is connected to a separate network. An IP address assigned to the interface identifies which local network is connected directly to it.



Router - Gateway



Why Private Addresses?

a) All hosts that connect directly to the Internet require a unique public IP address. Due to finite number of 32-bits structure in IPv4 , there is a risk of running out of IP addresses. One solution was to reserve some private addresses for use exclusively inside an organization.

b) This allows hosts within an organization to communicate with one another without the need of a unique public IP address. Therefore, the same set of private addresses can be used by multiple organizations. Private addresses are not routed on the Internet and will be quickly blocked by an ISP router.

c) The use of private addresses can provide a measure of security since they are only visible internally on the local network, and outsiders cannot gain direct access to the private IP addresses.

d) Need Network Address Translation (NAT) Protocol to link the private address to the public address or vice versa.

Private Addresses

Class	Private IP Addresses (RFC 1918)	Default Subnet Mask	Number of Networks	Hosts per Network	Total Hosts
A	10.0.0.0 to 10.255.255.255	255.0.0.0	1	16,777,214	16,777,214
B	172.16.0.0 to 172.31.255.255	255.255.0.0	16	65,534	1,048,544
C	192.168.0.0 to 192.168.255.255	255.255.255.0	256	254	65,024

Advantages of NAT	Disadvantages of NAT
• Public IP address sharing • Transparent to end users • Improved security • LAN expandability or scalability • Local control including ISP connectivity	• Incompatibility with certain applications • Hinders legitimate remote access • Performance reduction caused by increased router processing

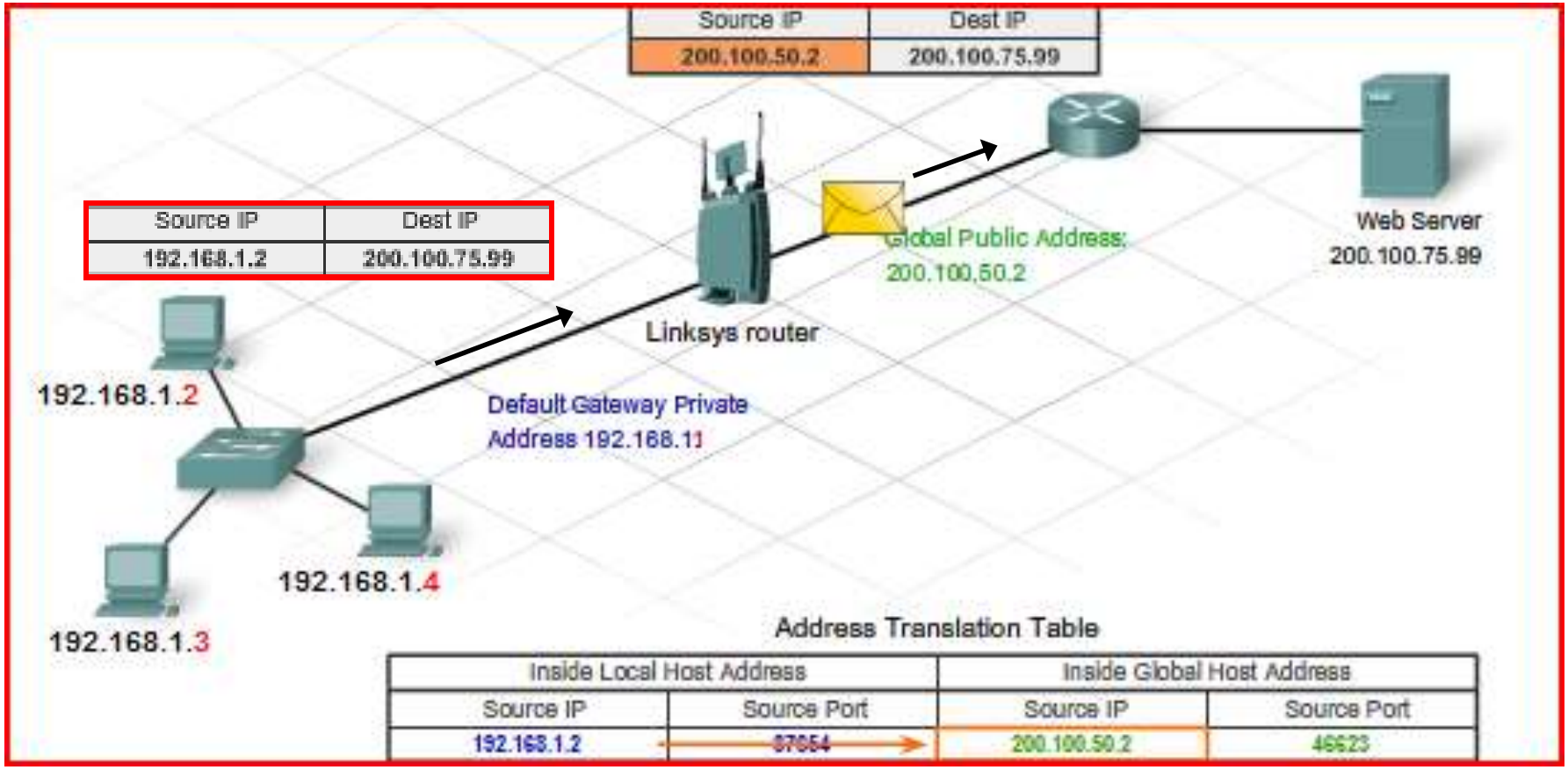
4.2.1 Basic Network Address Translation (NAT)

Routers are required to route between subnets on an internal network, regardless of whether the IP address range is public or private. However, if the address range is private, private networks cannot be routed across the public Internet. Therefore, how do host devices using a private addressing scheme communicate across the Internet? Network Address Translation (NAT) must be enabled on the device connecting the private network to the ISP network.

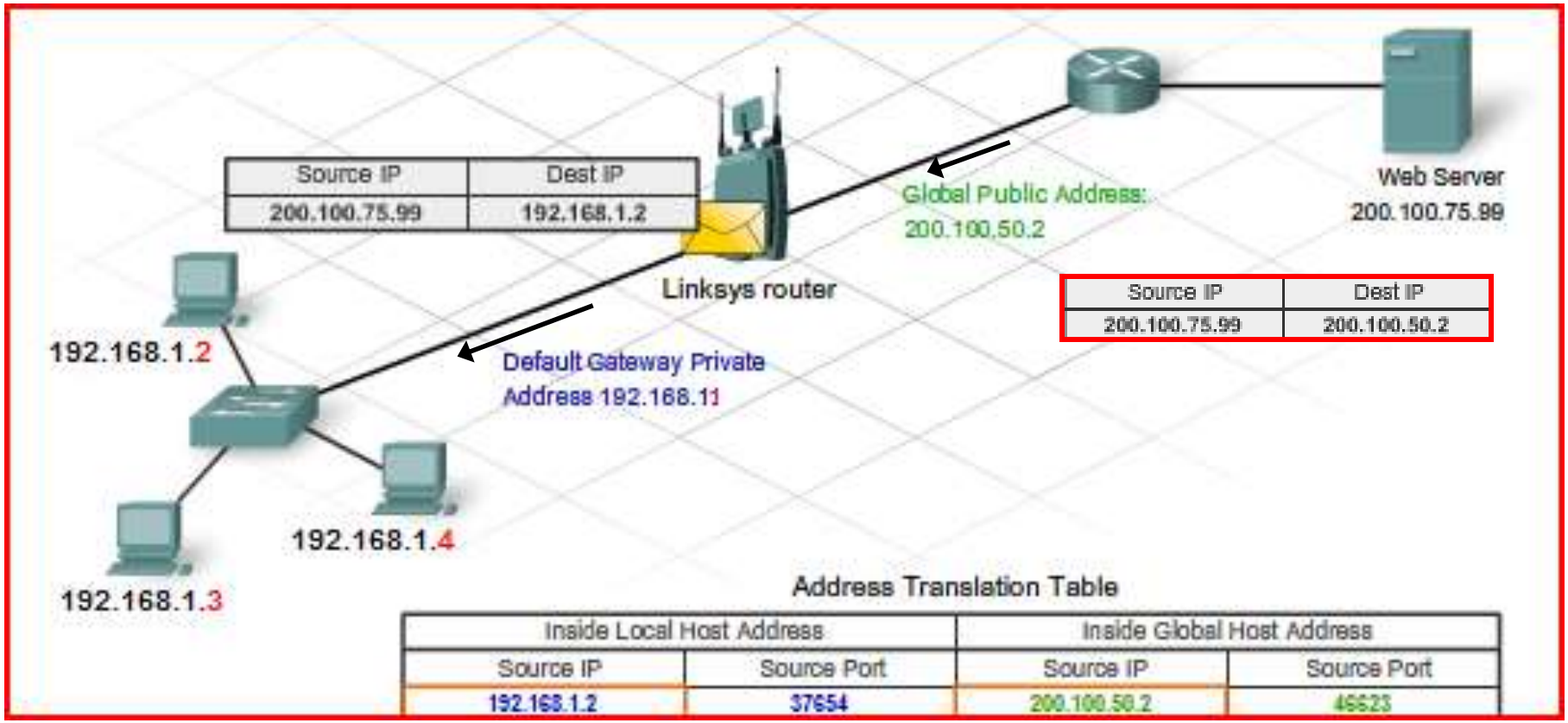
NAT allows a large group of private users to access the Internet by sharing one or more public IP addresses. Address translation is similar to how a telephone system works in a company. As a company adds employees, at some point, they no longer run a public phone line directly to each employee desk. Instead, they use a system that allows the company to assign each employee an extension number. The company can do this because not all employees use the phone at the same time. Using private extension numbers enables the company to purchase a smaller number of external phone lines from the phone company.

NAT works similarly to a company phone system. Saving registered IP addresses is one of the main reasons that NAT was developed. NAT can also provide security to PCs, servers, and networking devices by withholding their actual IP host addresses from direct Internet access.

NAT


Source IP
Dest IP
200.100.50.2
200.100.75.99
Web Server
200.100.75.99
Source IP
Dest IP
192.168.1.2
200.100.75.99
Global Public Address:
200.100.50.2
Linksys router
192.168.1.2
Default Gateway Private
Address 192.168.1.1
192.168.1.4
192.168.1.3
Address Translation Table
Inside Local Host Address
Inside Global Host Address
Source IP
Source Port
Source IP
Source Port
192.168.1.2
87654
200.100.50.2
46623

NAT

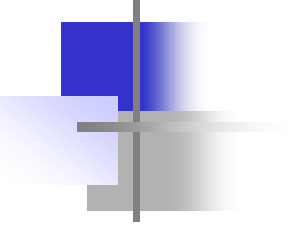

Source IP
Dest IP
200.100.75.99
192.168.1.2
Linksys router
Global Public Address:
200.100.50.2
Web Server
200.100.75.99
Source IP
Dest IP
200.100.75.99
200.100.50.2
192.168.1.2
Default Gateway Private
Address 192.168.11
192.168.1.4
192.168.1.3
Address Translation Table
Inside Local Host Address
Inside Global Host Address
Source IP
Source Port
Source IP
Source Port
192.168.1.2
37654
200.100.50.2
46623

NAT

The main advantages of NAT are that IP addresses can be re-used and many hosts on a single LAN can share globally unique IP addresses. NAT operates transparently and helps shield users of a private network against access from the public domain.

In addition, NAT hides private IP addresses from public networks. The advantage to this is that NAT operates much like an access control list, not allowing outside users to access internal devices. The disadvantage is that additional configurations are required to allow access from legitimate, external users.

Another disadvantage is that NAT has an impact on some applications that have IP addresses in their message payload, because these IP addresses must also be translated. This translation increases load on the router and hinders network performance.



Part E (Extra): Concept of Supernetting in Network Layer

Supernetting

a) Although class A and B addresses are almost depleted, Class C addresses are still available.

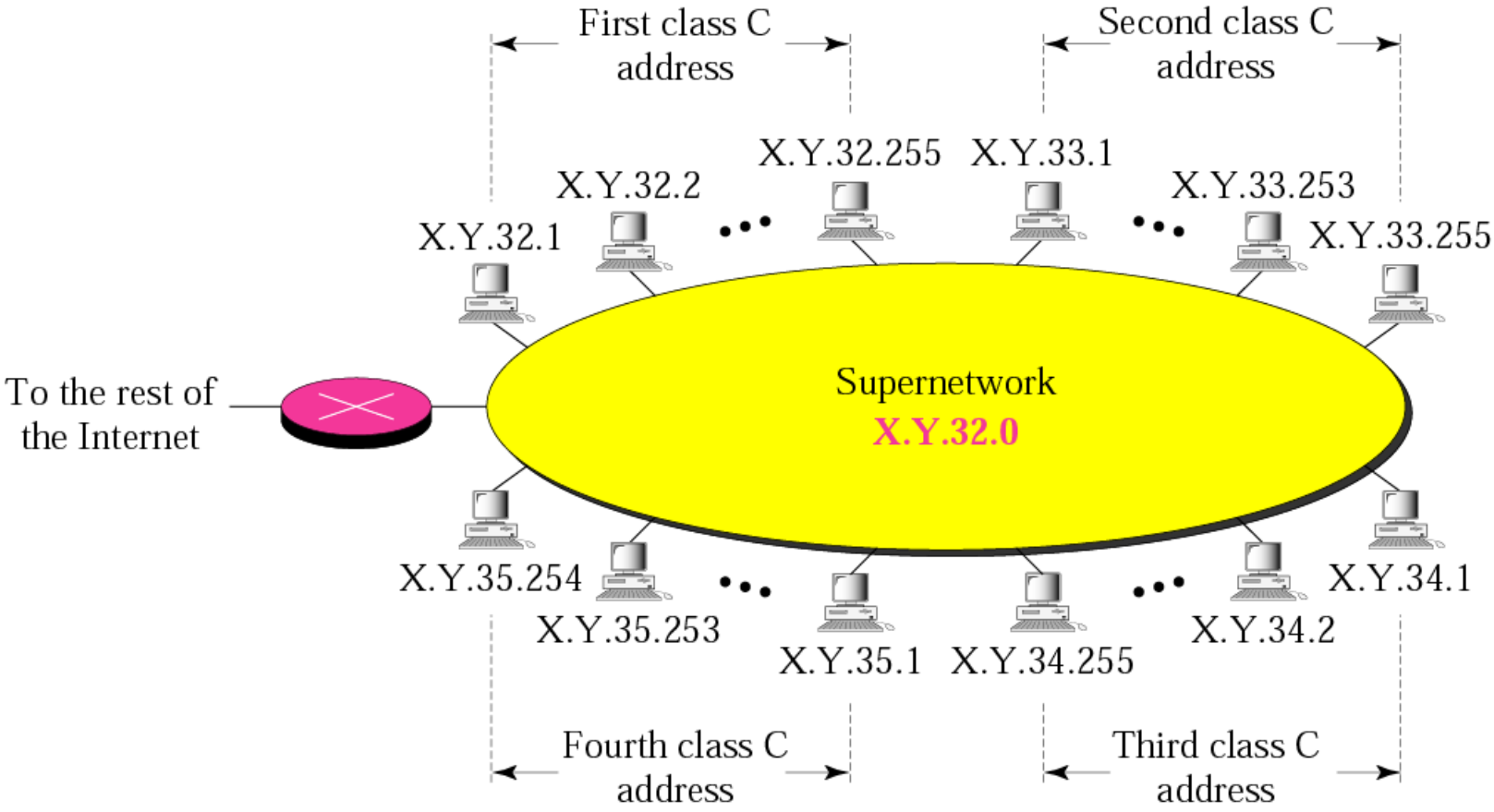
b) However, the size of a class C block with a maximum number of 256 addresses may not satisfy the needs of an organisation.

c) One solution is supernetting.

d) In supernetting, an organisation can combine several calss C blocks to create a large range of addresses.

e) In order words, several networks are combined to create a supernetwork. This is done by applying a set of class C blocks instead of just one.

Example of a Supernetwork



Rules:

** The number of blocks must be a power of 2 i.e: (2, 4, 8, 16, . . .).

** The blocks must be contiguous in the address space (no gaps between the blocks).

** The third (3rd) byte of the first (1st) address in the superblock must be evenly divisible by the number of blocks. In other words, if the number of blocks is *N*, the third byte must be divisible by *N*.

Example

A company needs 600 addresses. Which of the following set of class C blocks can be used to form a supernet for this company?

a. 198.47.32.0 198.47.33.0 198.47.34.0

b. 198.47.32.0 198.47.42.0 198.47.52.0 198.47.62.0

c. 198.47.31.0 198.47.32.0 198.47.33.0 198.47.52.0

d. 198.47.32.0 198.47.33.0 198.47.34.0 198.47.35.0

Solution

a: No, there are only three blocks.

b: No, the blocks are not contiguous.

c: No, 31 in the first block is not divisible by 4.

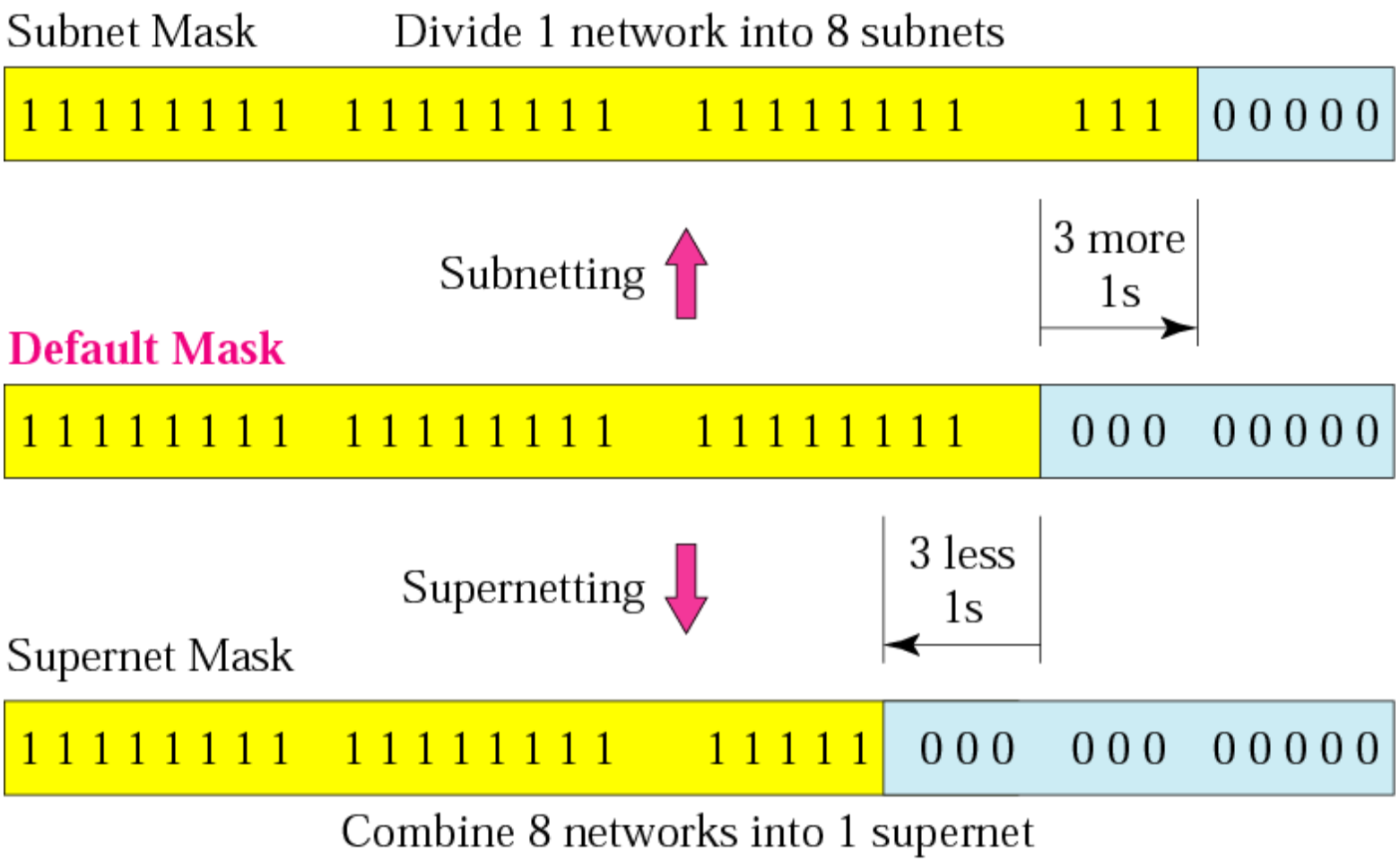
d: Yes, all three requirements are fulfilled.

Vital notes: Supernetting

In subnetting,
we need the first address of the subnet
and the subnet mask to
define the range of addresses.

In supernetting,
we need the first address of the supernet
and the supernet mask to
define the range of addresses.

Comparison of subnet, default, and supernet masks



Example

We need to make a supernetwork out of 16 class C blocks. What is the supernet mask?

Solution

Class C mask is defaulted with 24 of '1' is

11111111 11111111 11111111 00000000

We need 16 blocks. For 16 blocks we need to change four 1s to 0s in the default mask. So the mask is

11111111 11111111 1111**0000** 00000000

or

255.255.240.0

Example

A supernet has a first address of 205.16.32.0 and a supernet mask of 255.255.248.0. A router receives 3 packets with the following destination addresses:

205.16.37.44
205.16.42.56
205.17.33.76

Q: Which packet belongs to the supernet?

Solution

We apply the supernet mask to find the beginning address.

205.16.37.44 AND 255.255.248.0 ➔ 205.16.32.0

205.16.42.56 AND 255.255.248.0 ➔ 205.16.40.0

205.17.33.76 AND 255.255.248.0 ➔ 205.17.32.0

Only the first address belongs to this supernet.

Example

A supernet has a first address of 205.16.32.0 and a supernet mask of 255.255.248.0. How many blocks are in this supernet and what is the range of addresses?

Solution

The supernet has 21 1s. The default mask has 24 1s. Since the difference is 3, there are 2^3 or 8 blocks in this supernet. The blocks are 205.16.32.0 to 205.16.39.0. The first address is 205.16.32.0. The last address is 205.16.39.255.

Part F (Extra):

Idea of Network

LAN - Local Area Network

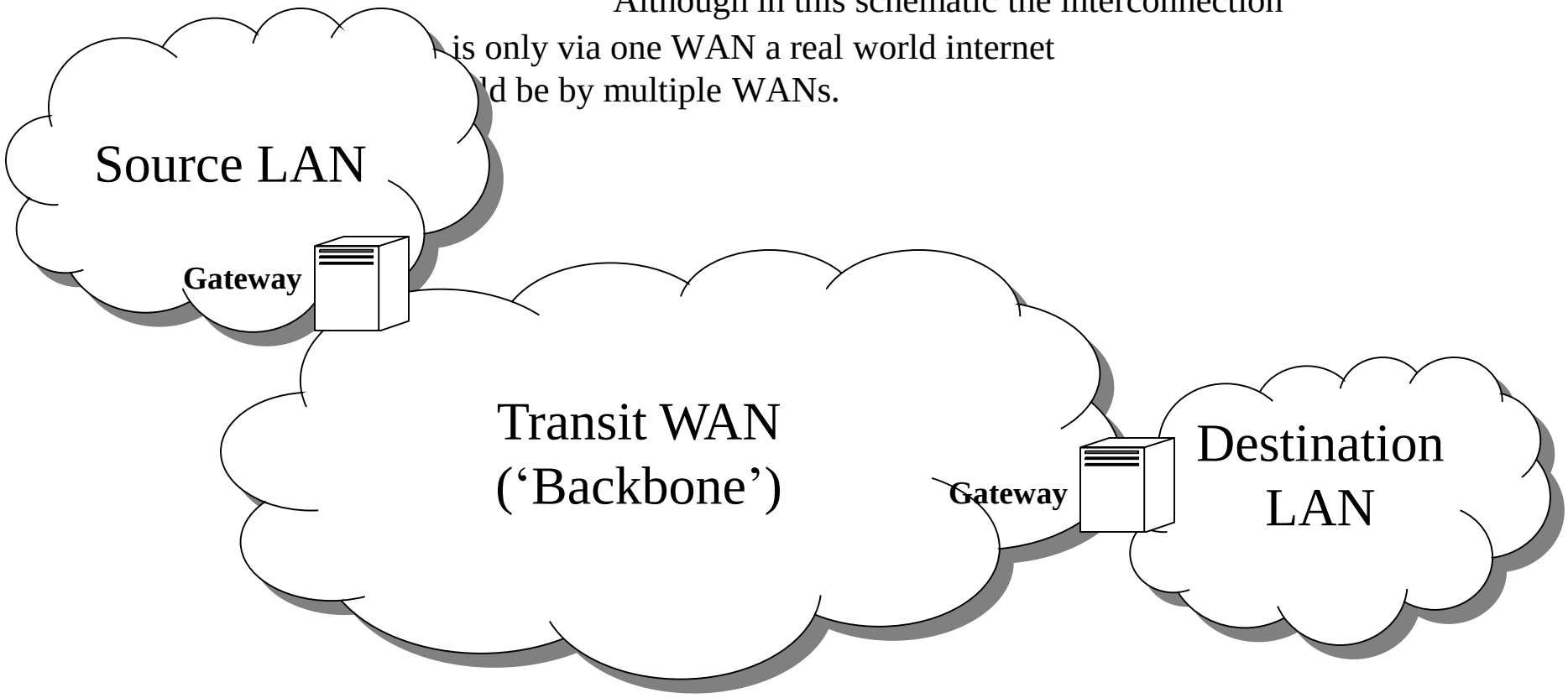
WAN - Wide Area Network

Model of Internetworking delivery

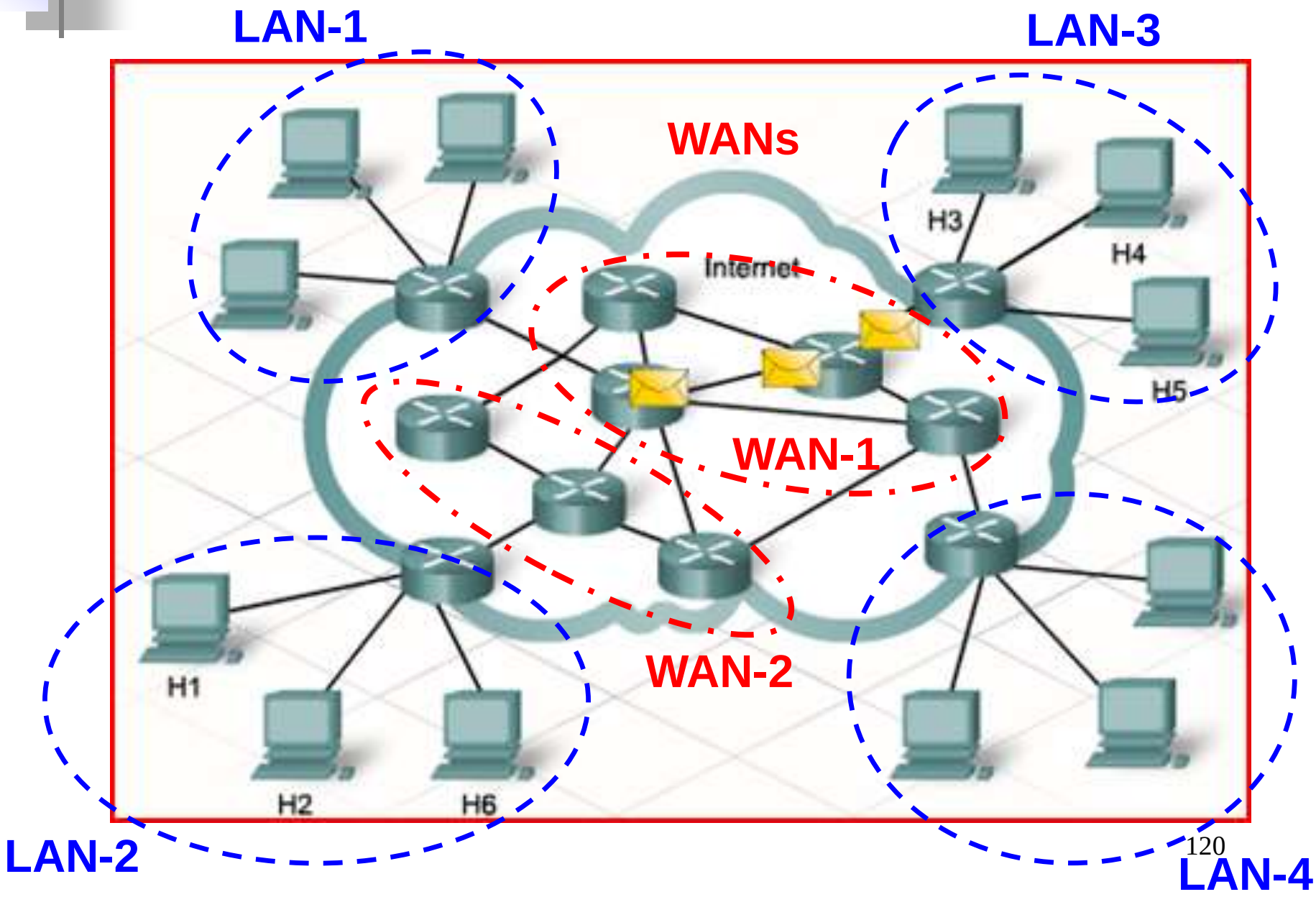
a) Access Networks (LAN based)

b) Interconnection/Transit Networks (WAN based)

Although in this schematic the interconnection
is only via one WAN a real world internet
ld be by multiple WANs.



LANs and WANs



Network Models

WAN - Features

a) Long distance transmission (via serial connection).

b) Typically point to point (PPP) links.

c) Backbones within networks or interconnecting networks.

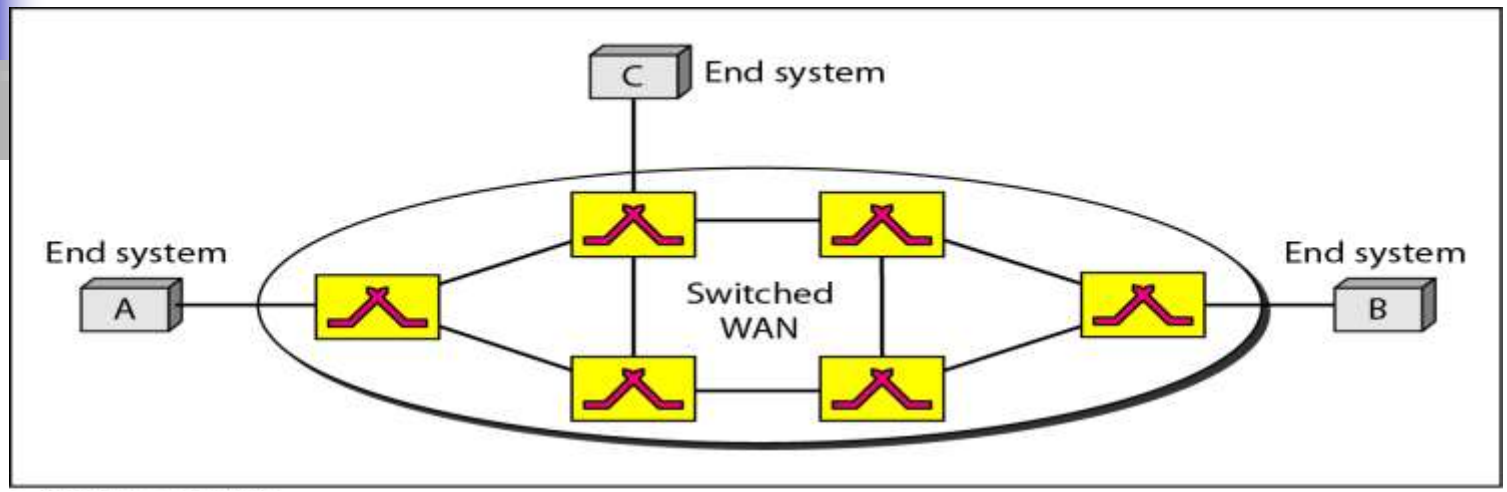
d) WANs can either be circuit switched or packet switched.

- The telephony network (PSTN) is an example of a circuit switched network.

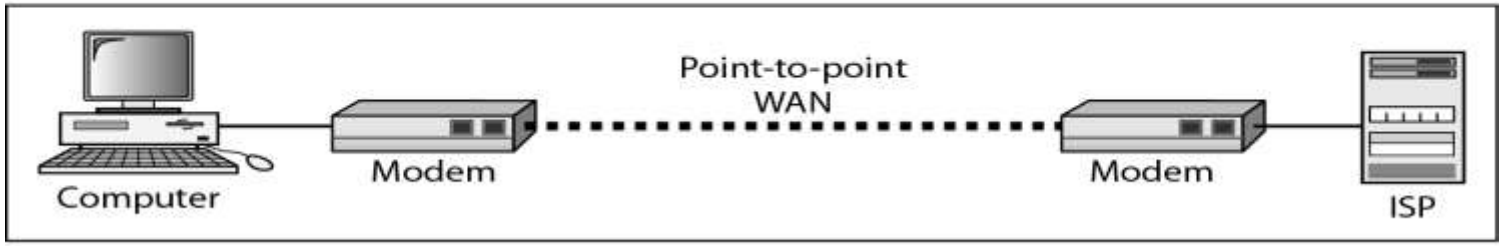
(Voice traffic networking is migrating away from the PSTN to packet switched networks) – not VoIP.

- The Internet is the dominant packet switched network.

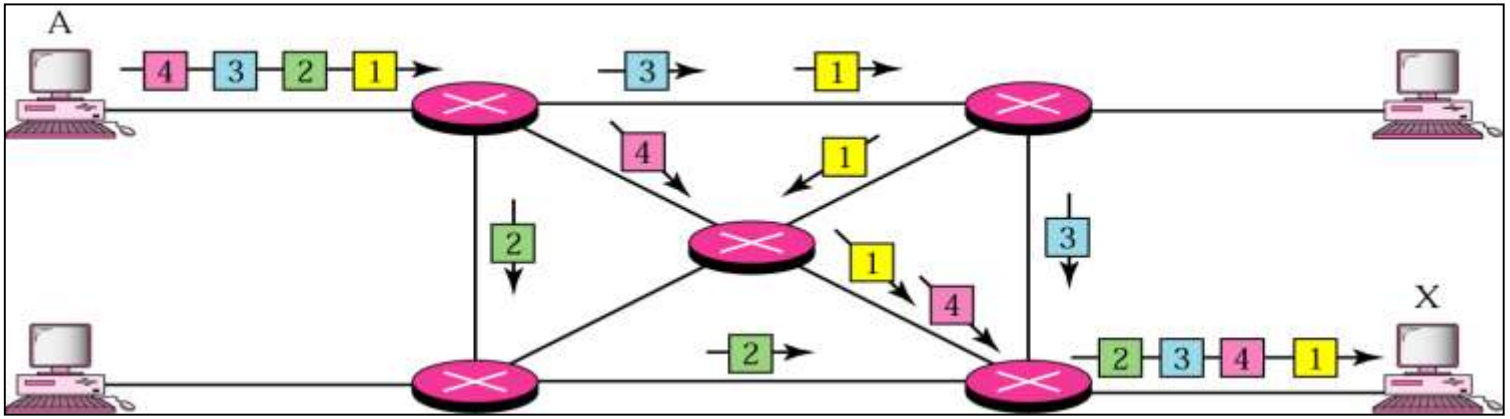
Packet switching comes in two flavours: datagram of which the Internet is the pre-eminent example and virtual circuit of which ATM and frame relay are examples.



a. circuit-switched



b. Point-to-point WAN



c. packet-switched

LAN - Features:

a) Provides connectivity at a local level – within an office, within in a building, within a small campus.

b) Limited coverage distance. (depends on technologies)

c) Utilizes medium access control (MAC) protocols.

d) Operates over shared transmission links. (CSMA/CD or OFDM)

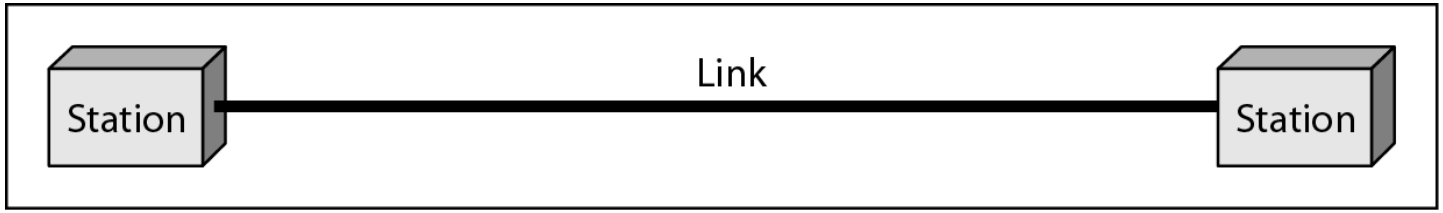
e) Mostly based on Ethernet Technology (Fast-Ethernet interfaces).

f) The Ethernet IEEE802.3 is the pre-eminent wired LAN MAC protocol.

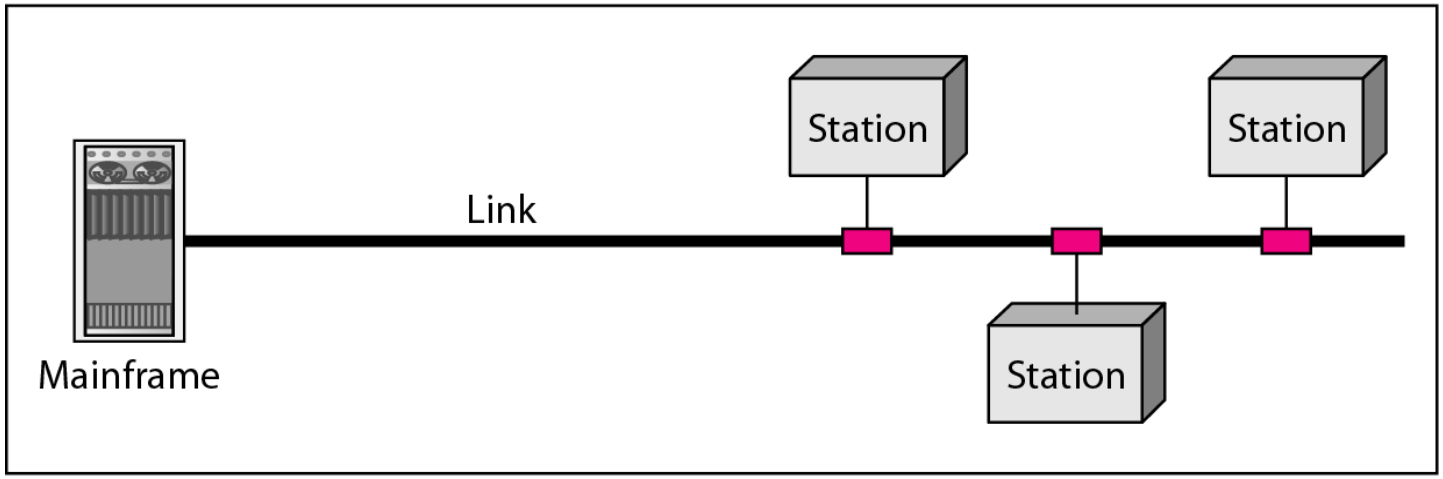
g) The WiFi IEEE802.11x is the pre-eminent wireless LAN MAC protocol.

Types of LAN Structure

Types of connections

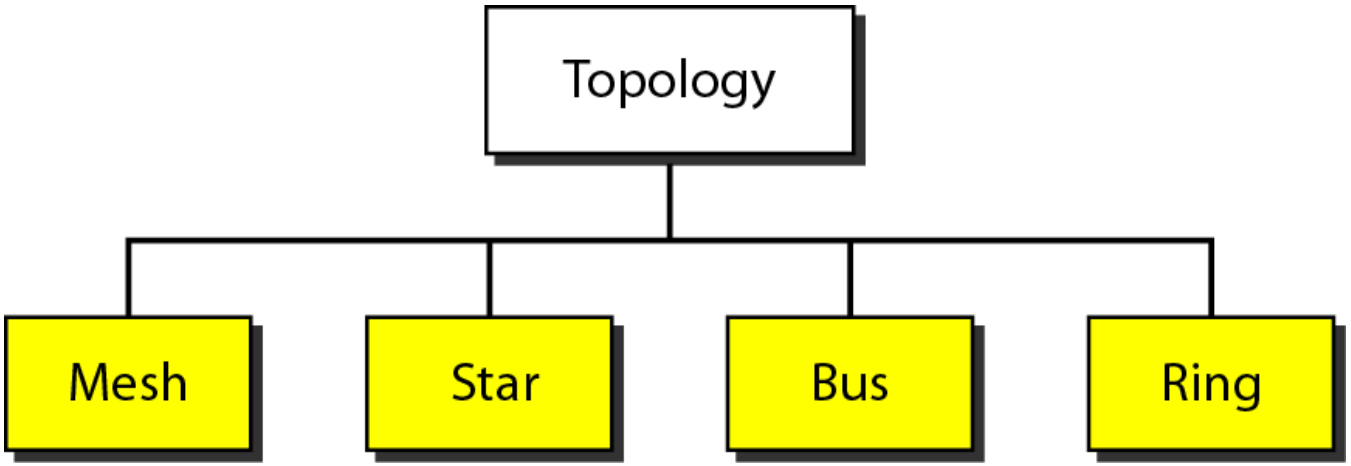


a. Point-to-point



b. Multipoint

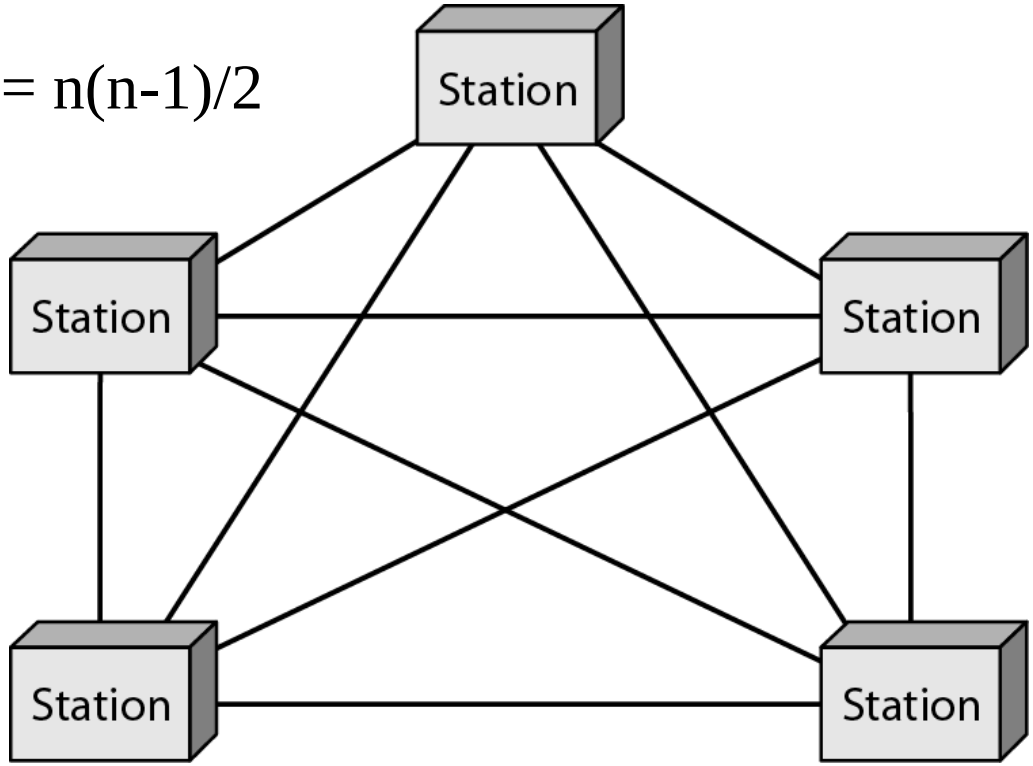
Categories of topology



MESH

A fully connected mesh topology

L = n(n-1)/2



Advantages

No sharing (Dedicated link)

Robust

Secure (Dedicated link)

Easy fault identification

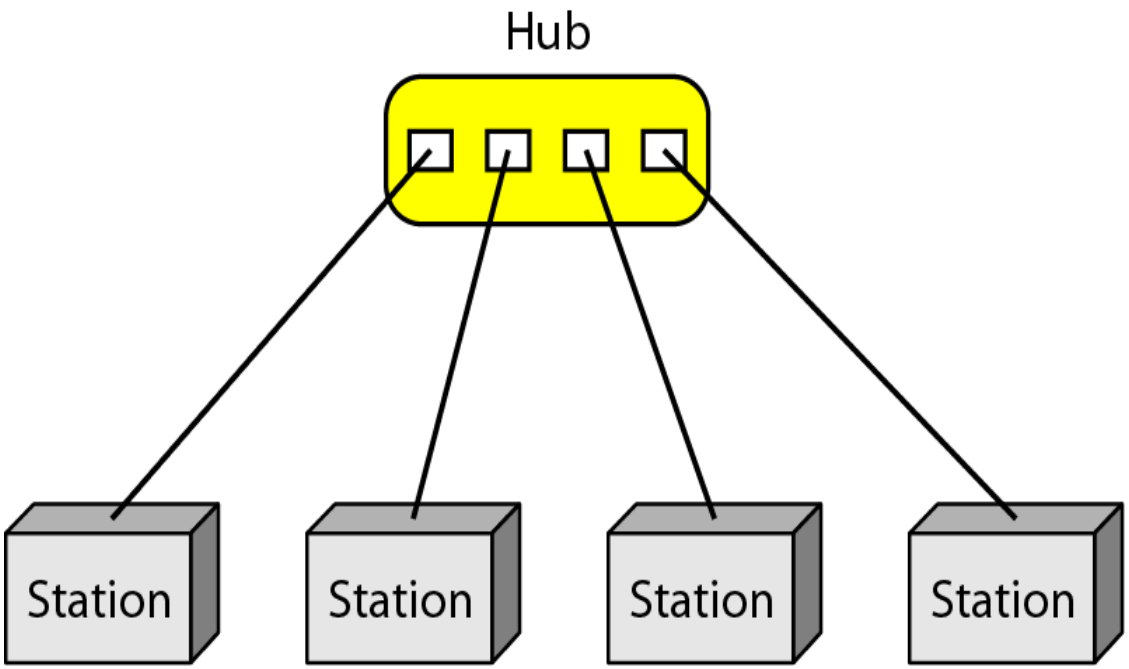
Disadvantages

Complex, Expensive, Bulky

All these are a function of the large amount of cabling needed.

STAR

A star topology connecting four stations



Advantages

Cheaper than mesh (– but more expensive than bus).

Flexible (change only requires the addition or removal of one cable).

Robust in that failure of a cable only results in a single station loosing connectivity.

Easy fault identification

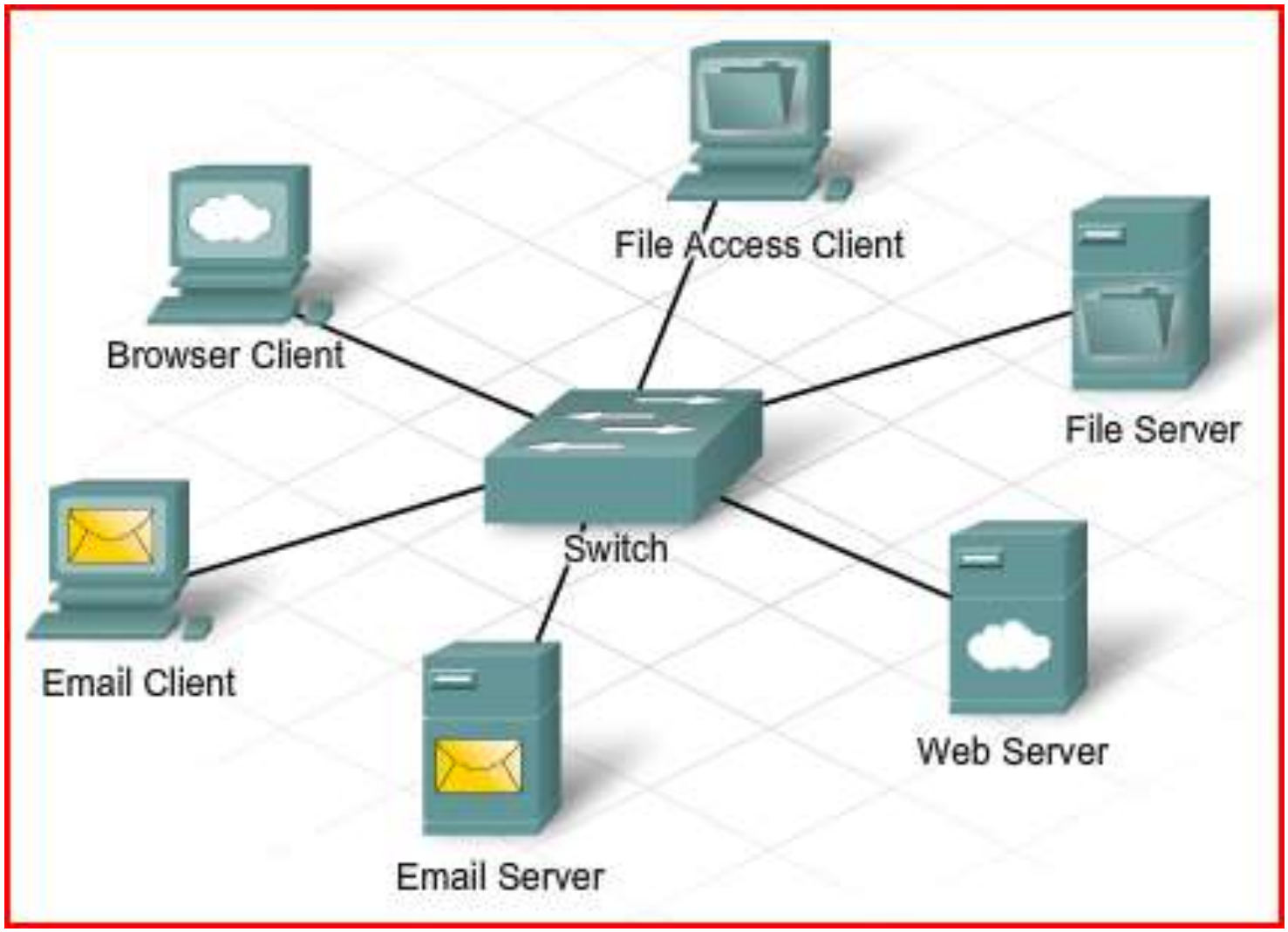
Disadvantages

Single point of failure at the hub.

Less secure.

The STAR can be configured as point to multipoint depending on the nature of the hub but BUS is always a shared multipoint link.

Example of Star Network

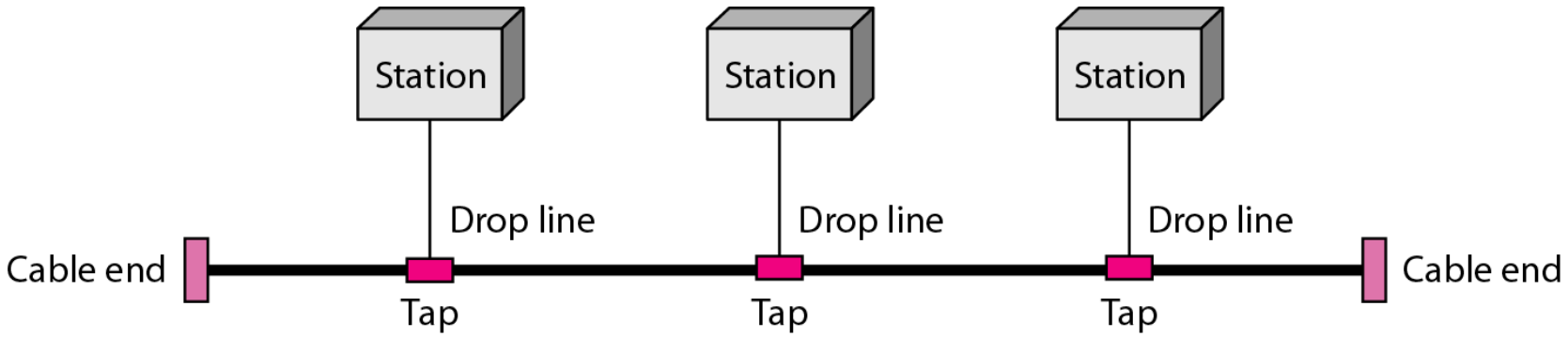


BUS

Advantages — Ease of installation and low cost.

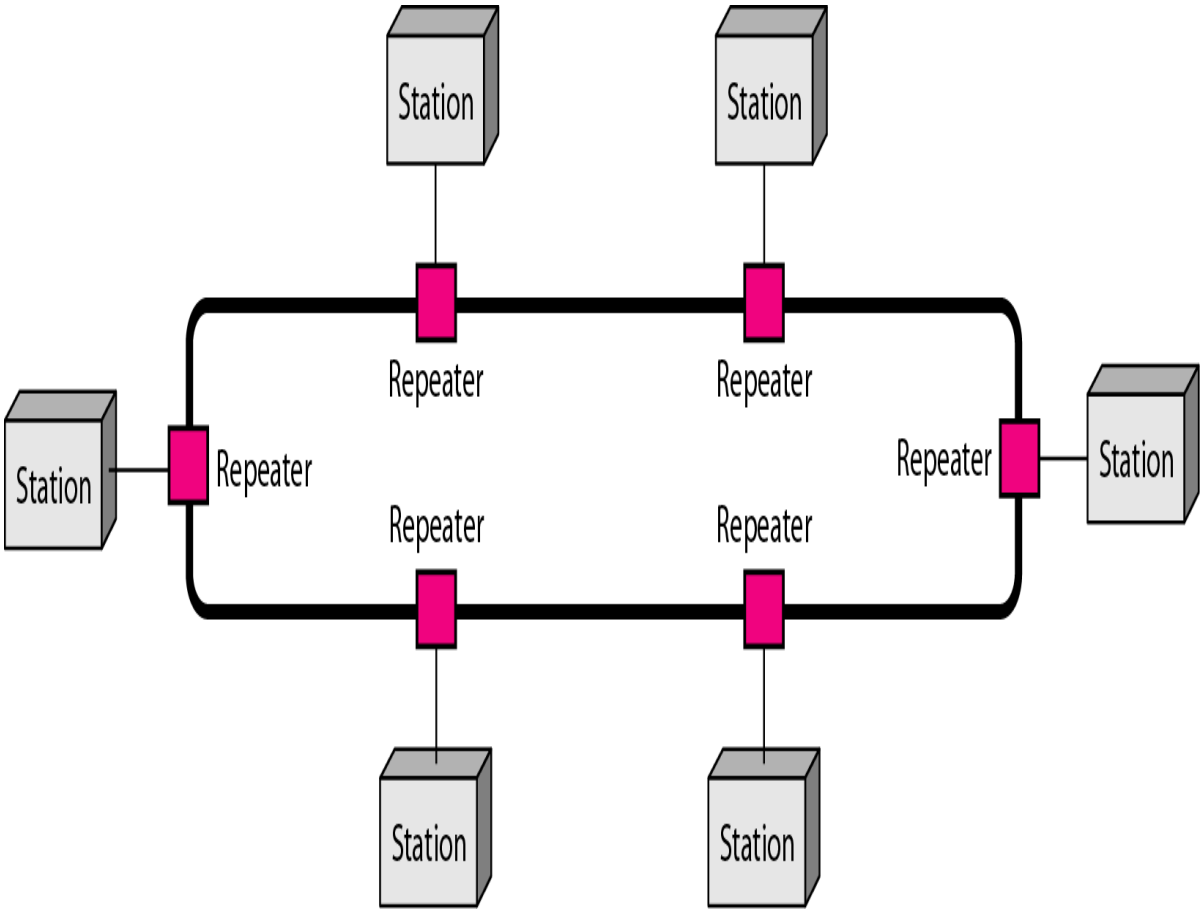
Disadvantages — Performance is very poor under moderate to heavy loading, single point of failure, poor security.

A bus topology



RING

A ring topology



Advantages

Easy to install

Flexible (adding removing stations)

Self monitoring (circulating token)

Disadvantages

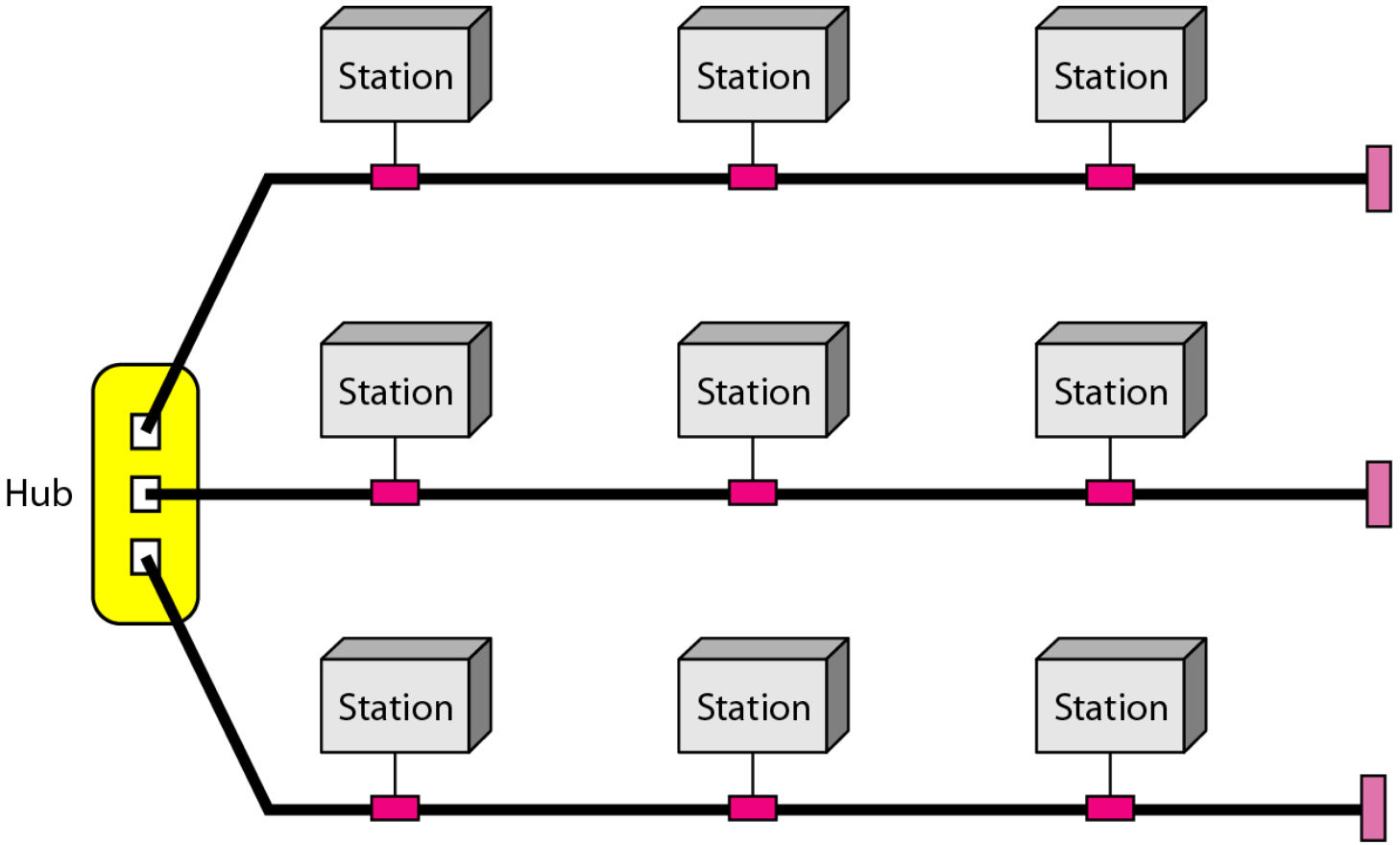
Unidirectional

Single point of failure

Security

TREE

A hybrid topology: a star backbone with three bus networks



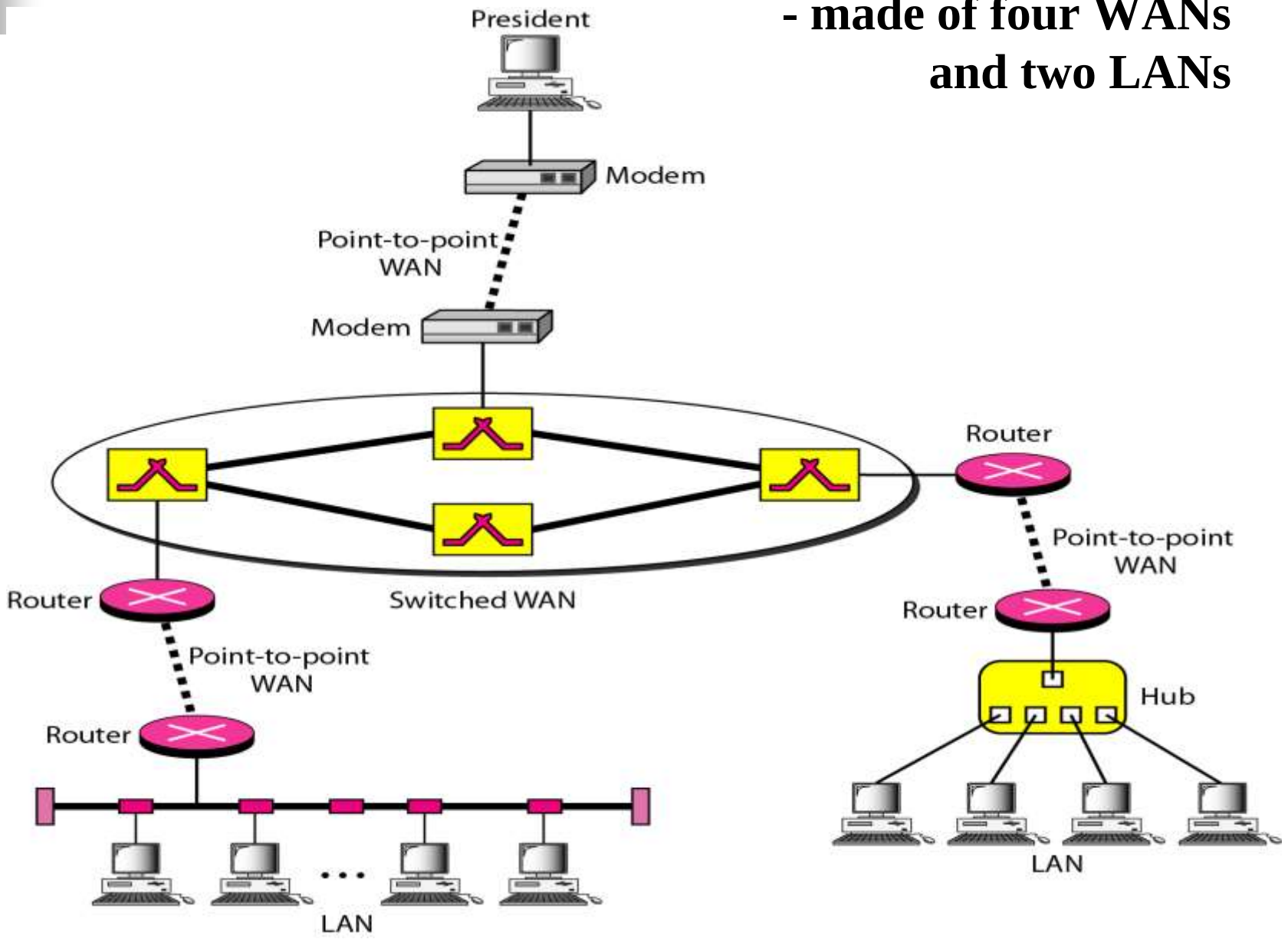
THE INTERNET

Internetworking allows separate networks to exchange data. The Internet connects networks nationally and globally using TCP/IP protocols.

- **The Internet (and the WWW) has revolutionized many aspects of our daily lives.**
- **It has affected the way we do business as well as the way we spend our leisure time.**
- **The Internet is a communication system that has brought a wealth of information to our fingertips and organized it for our use.**

Internetworking schematic

- made of four WANs and two LANs



3.1.1 What is a Network?

There are many types of networks that provide us with different kinds of services. In the course of a day, a person might make a phone call, watch a television show, listen to the radio, look up something on the Internet, or even play a video game with someone in another country. All of these activities depend on robust, reliable networks. Networks provide the ability to connect people and equipment no matter where they are in the world. People use networks without ever thinking about how they work or what it would be like if the networks did not exist.

This picture of the airport illustrates people using networks to share information, use resources and communicate with others. There are multiple types of networks shown in this scene. How many can you find?

Communication technology in the 1990s, and before, required separate, dedicated networks for voice, video and computer data communications. Each of these networks required a different type of device in order to access the network. Telephones, televisions, and computers used specific technologies and different dedicated network structures, to communicate. But what if people want to access all of these network services at the same time, possibly using a single device?

New technologies create a new kind of network that delivers more than a single type of service. Unlike dedicated networks, these new converged networks are capable of delivering voice, video and data services over the same communication channel or network structure.

New products are coming to market that take advantage of the capabilities of converged information networks. People can now watch live video broadcasts on their computers, make a telephone call over the Internet, or search the Internet using a television. Converged networks make this possible.

3.1.3 Basic Network Components

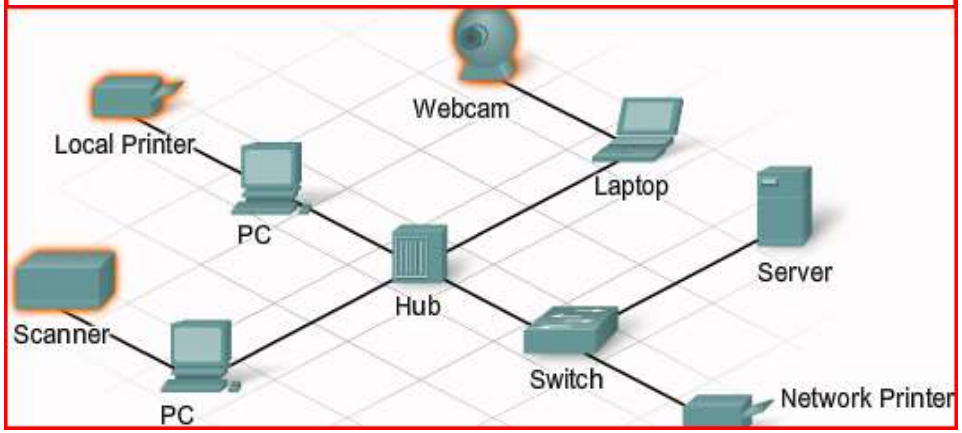
There are many components that can be part of a network, for example personal computers, servers, networking devices, and cabling. These components can be grouped into four main categories:

- Hosts
- Shared peripherals
- Networking devices
- Networking media

The network components that people are most familiar with are hosts and shared peripherals. Hosts are devices that send and receive messages directly across the network.

Shared peripherals are not directly connected to the network, but instead are connected to hosts. The host is then responsible for sharing the peripheral across the network. Hosts have computer software configured to enable people on the network to use the attached peripheral devices.

The network devices, as well as networking media, are used to interconnect hosts.



3.1.5 Peer-to-Peer Networks

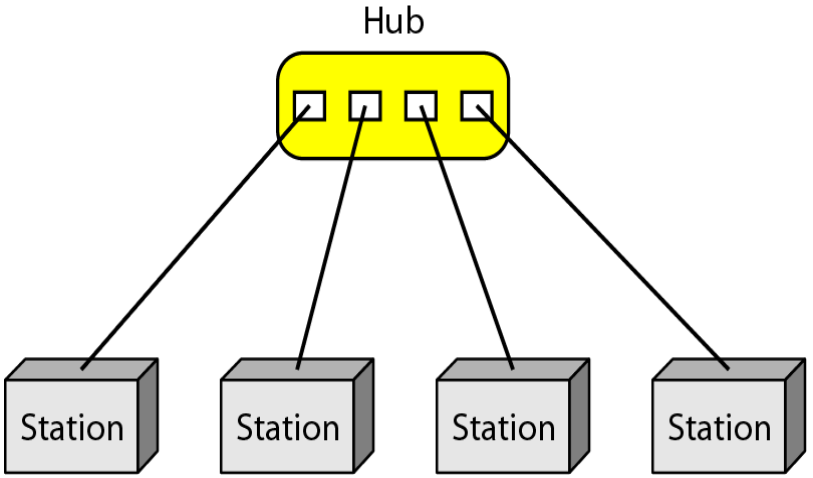
Client and server software usually runs on separate computers, but it is also possible for one computer to carry out both roles at the same time. In small businesses and homes, many computers function as the servers and clients on the network. This type of network is called a peer-to-peer network.

The simplest peer-to-peer network consists of two directly connected computers using a wired or wireless connection.

Multiple PCs can also be connected to create a larger peer-to-peer network but this requires a network device, such as a hub, to interconnect the computers.

The main disadvantage of a peer-to-peer environment is that the performance of a host can be slowed down if it is acting as both a client and a server at the same time.

In larger businesses, due to the potential for high amounts of network traffic, it is often necessary to have dedicated servers to support the number of service requests.



The advantages of peer-to-peer networking:

- Easy to set up
- Less complexity
- Lower cost since network devices and dedicated servers may not be required
- Can be used for simple tasks such as transferring files and sharing printers

The disadvantages of peer-to-peer networking:

- No centralized administration
- Not as secure
- Not scalable
- All devices may act as both clients and servers which can slow their performance

Hierarchical Network

a) A good network structure need to be self-contained.

b) In networking, hierarchical design is used to group devices into multiple networks that are organized in a layered approach. (this layer concept is different from OSI layer)

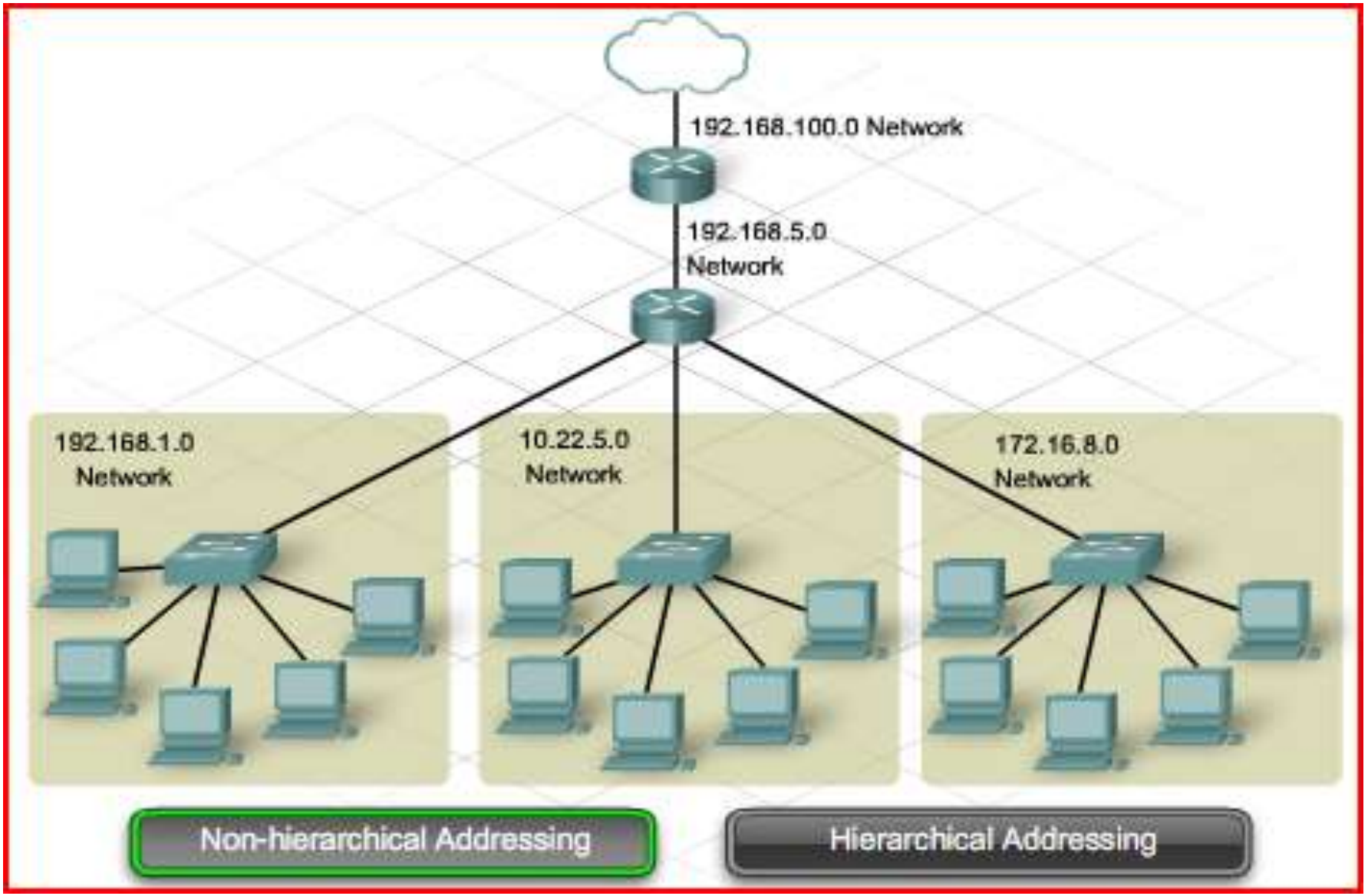
c) It consists of smaller, more manageable groups that allow local traffic to remain local.

d) Only traffic that is destined for other networks is moved to a higher layer.

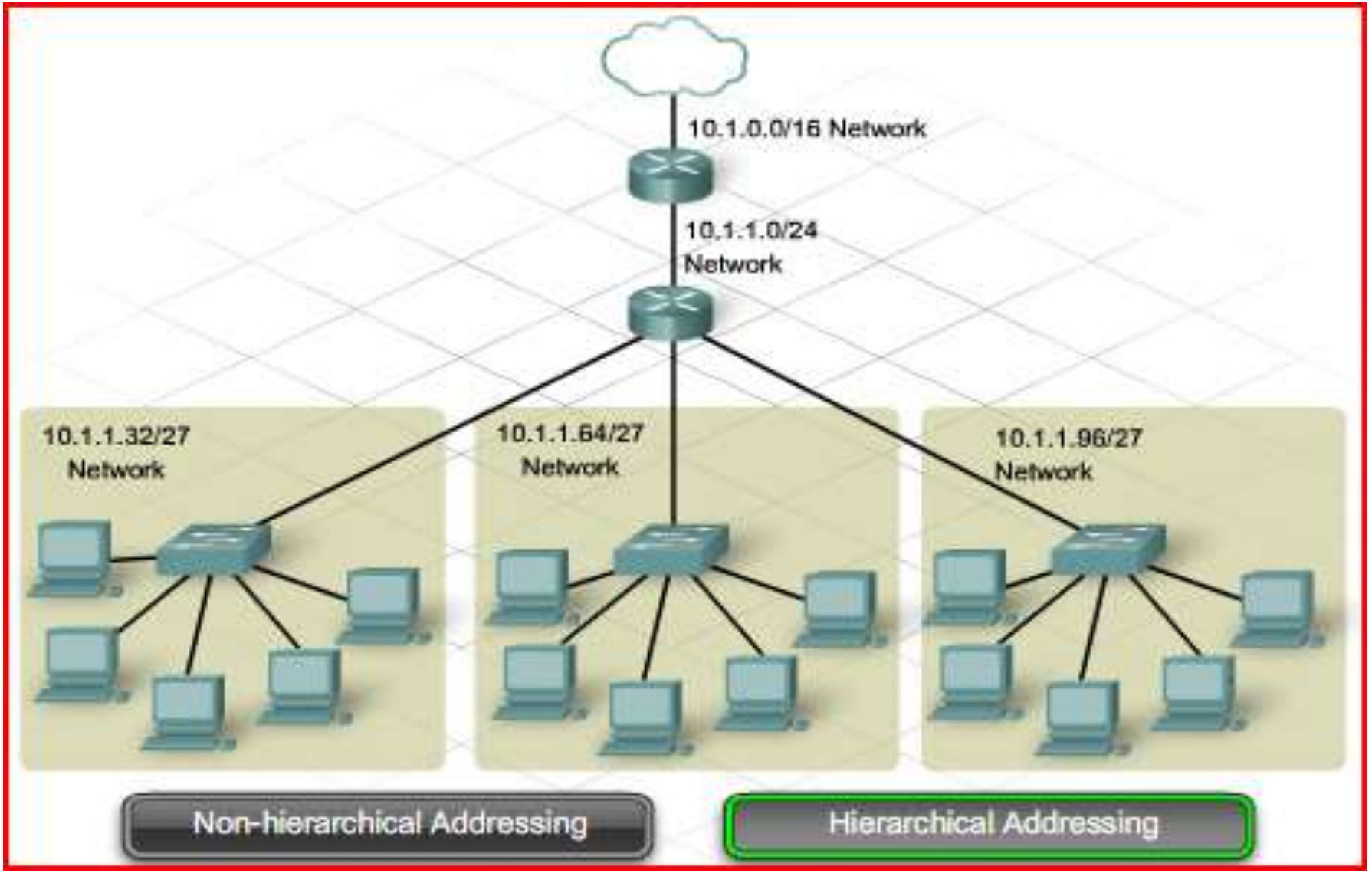
e) A hierarchical, layered design provides optimization of function and increased speed and efficiency.

f) It allows the network to scale as required because additional local networks can be added without impacting the performance of the existing ones.

Non Hierarchical Network



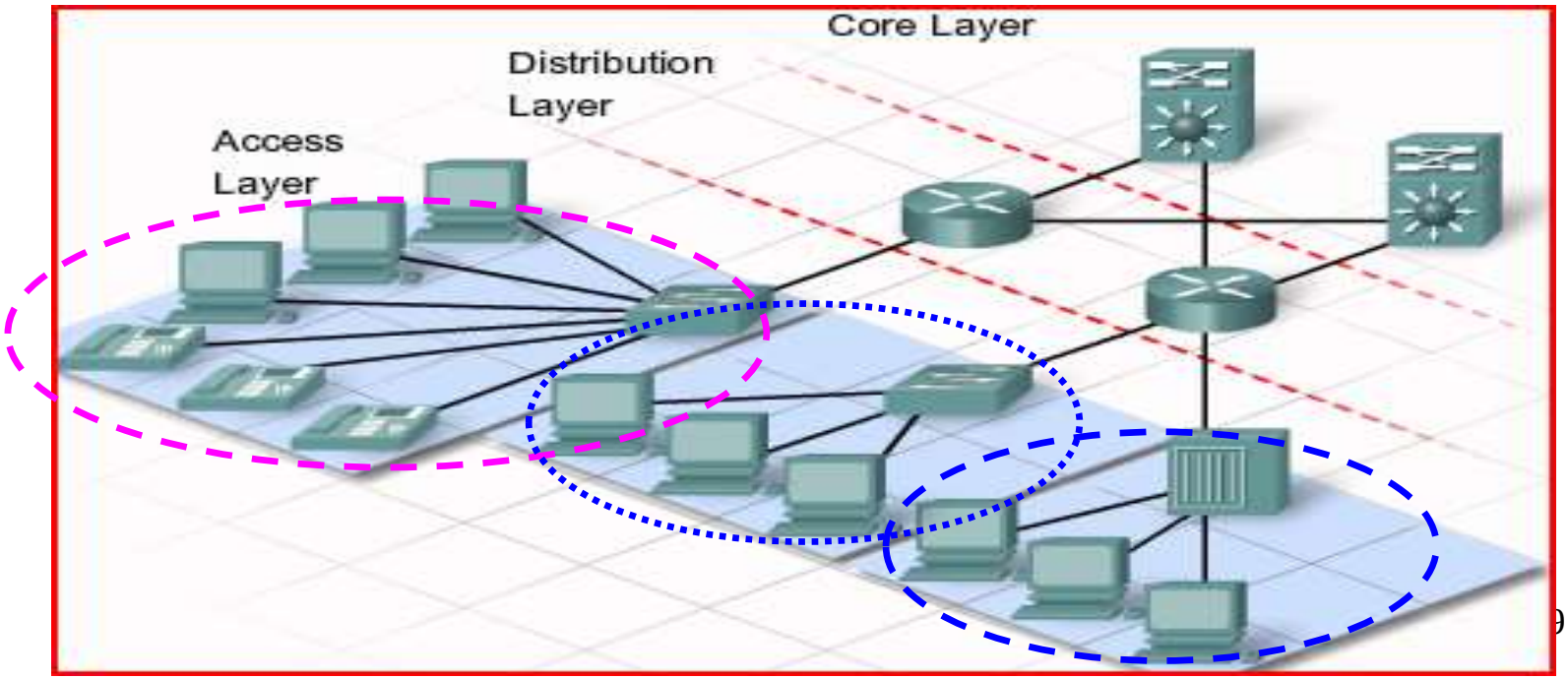
Hierarchical Network



Hierarchical Network

The hierarchical design has three basic layers:

- Access Layer - to provide connections to hosts in a Local Network.
- Distribution Layer - to interconnect various Local Networks.
- Core Layer - a high-speed connection between different Distribution Layer devices.

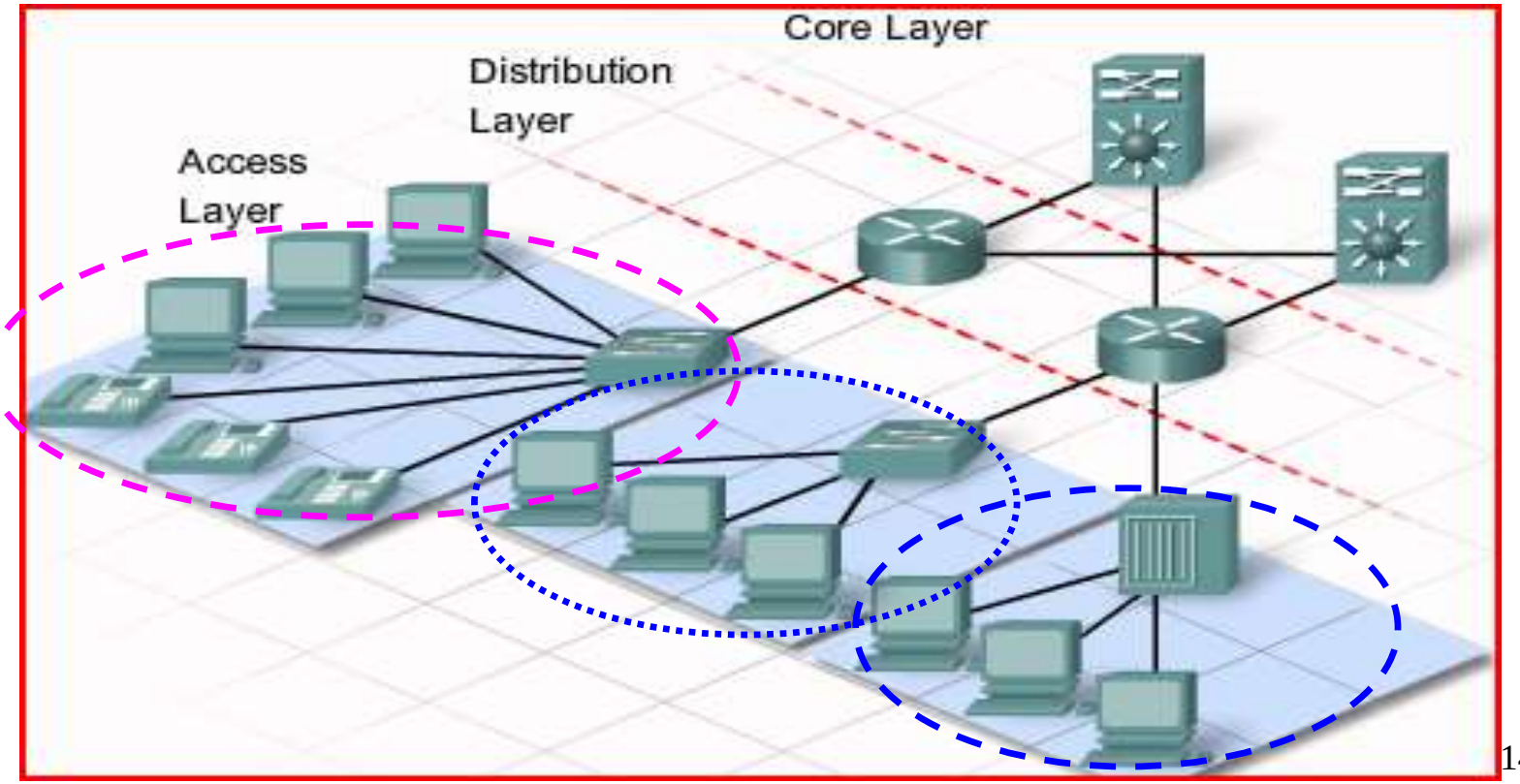


Network Devices in Hierarchical Network

Access Layer – Hubs or Switches (layer-2 device).

Distribution Layer – ISR or Router (layer-3 device).

Core Layer – high-speed Router, WAN devices.



Access Layer

The Access Layer provides a connection point for end user devices to the network and allows multiple hosts to connect to other hosts through a network device, usually a hub or switch. Typically, all devices within a single Access Layer will have the same network portion of the IP address.

If a message is destined for a local host, based on the network portion of the IP address, the message remains local. If it is destined for a different network, it is passed up to the Distribution Layer. Hubs and switches provide the connection to the Distribution Layer devices, usually a router.

Distribution Layer

The Distribution Layer provides a connection point for separate networks and controls the flow of information between the networks. It typically contains more powerful switches than the Access Layer as well as routers for routing between networks. Distribution Layer devices control the type and amount of traffic that flows from the Access Layer to the Core Layer.

Core Layer

The Core Layer is a high-speed backbone layer with redundant (backup) connections. It is responsible for transporting large amounts of data between multiple end networks. Core Layer devices typically include very powerful, high-speed switches and routers. The main goal of the Core Layer is to transport data quickly.

3.4.2 Function of Hubs

A hub is one type of networking device that is installed at the Access Layer of an Ethernet network. Hubs contain multiple ports that are used to connect hosts to the network. Hubs are simple devices that do not have the necessary electronics to decode the messages sent between hosts on the network. Hubs cannot determine which host should get any particular message. A hub simply accepts electronic signals from one port and regenerates (or repeats) the same message out all of the other ports.

3.4.3 Function of Switches

An Ethernet switch is a device that is used at the Access Layer. Like a hub, a switch connects multiple hosts to the network. Unlike a hub, a switch can forward a message to a specific host. When a host sends a message to another host on the switch, the switch accepts and decodes the frames to read the physical (MAC) address portion of the message.

3.5.2 Function of Routers

A router is a networking device that connects a local network to other local networks. At the Distribution Layer of the network, routers direct traffic and perform other functions critical to efficient network operation. Routers, like switches, are able to decode and read the messages that are sent to them. Unlike switches, which only decode (unencapsulate) the frame containing the MAC address information, routers decode the packet that is encapsulated within the frame.

So, what is LAN?

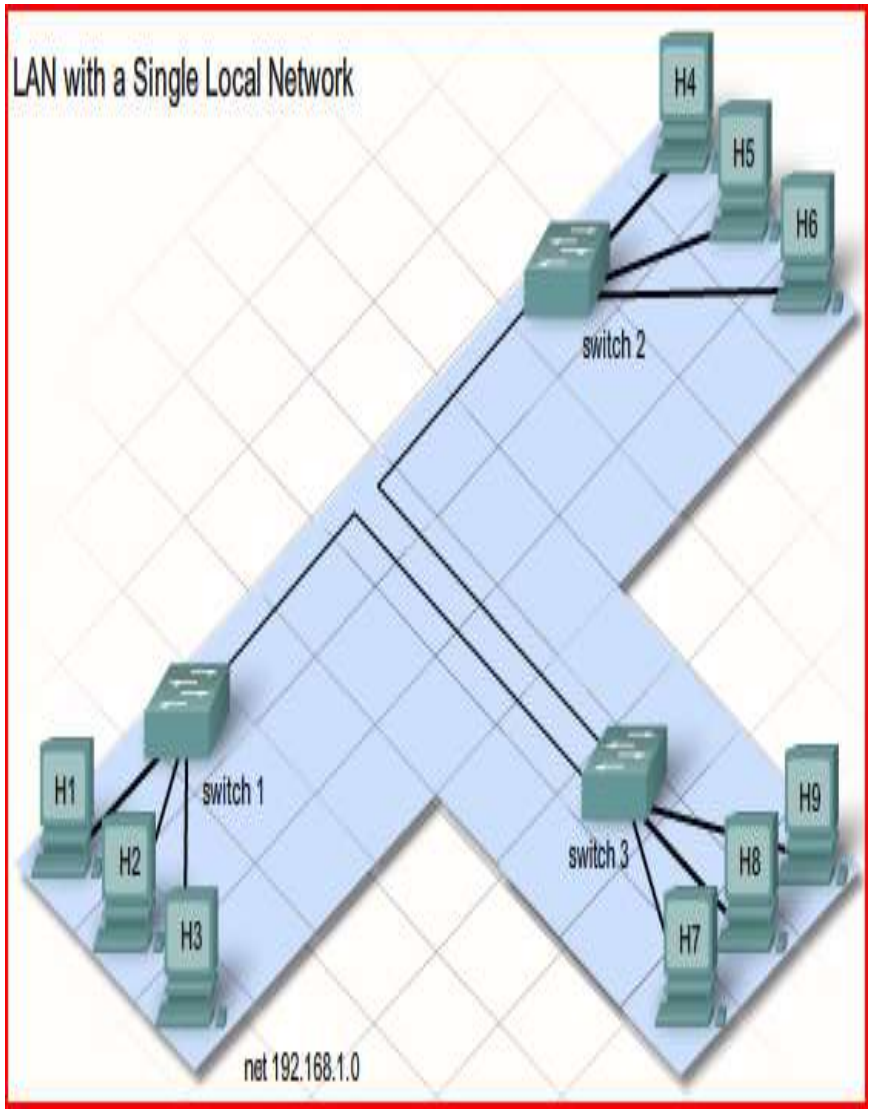
The term Local Area Network (LAN) refers to a local network, or a group of interconnected local networks that are under the same administrative control.

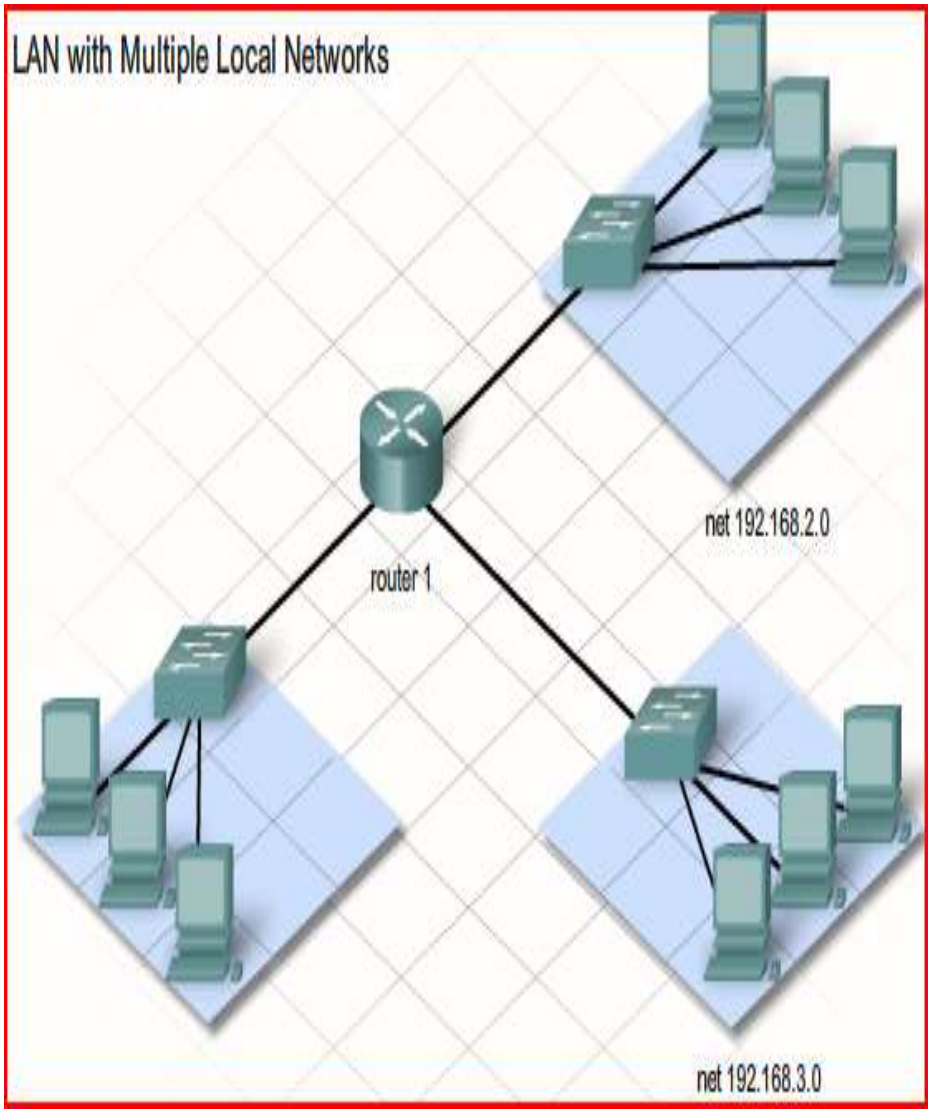
In the early days of networking, LANs were defined as small networks that existed in a single physical location. While LANs can be a single local network installed in a home or small office, the definition of LAN has evolved to include interconnected local networks consisting of many hundreds of hosts, installed in multiple buildings and locations.

The important thing to remember is that all of the local networks within a LAN are under one administrative control. Other common characteristics of LANs are that they typically use Ethernet or wireless protocols, and they support high data rates.

The term Intranet is often used to refer to a private LAN that belongs to an organization, and is designed to be accessible only by the organization's members, employees, or others with authorization.

What is the difference?



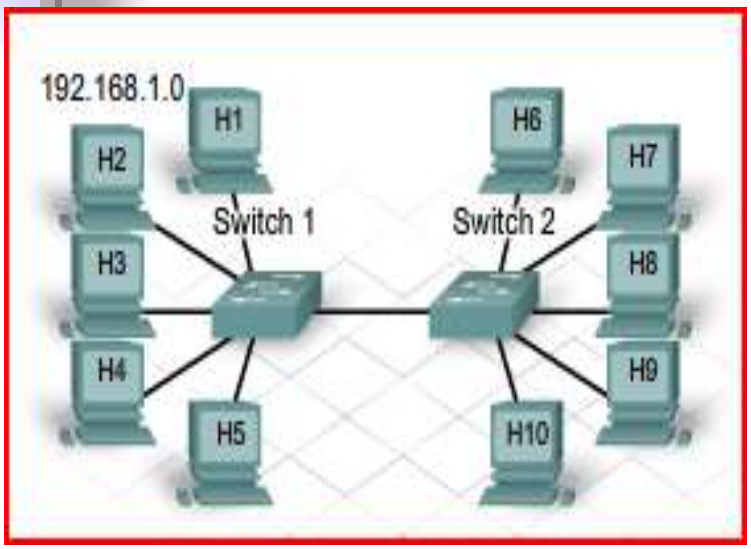


Within a LAN, it is possible to place all hosts on a single local network or divide them up between multiple networks connected by a Distribution Layer. The answer depends on desired results. Placing all hosts on a single local network allows them to be seen by all other hosts. This is because there is one broadcast domain and hosts use ARP to find each other.

In a simple network design it may be beneficial to keep all hosts within a single local network. However, as networks grow in size, increased traffic will decrease network performance and speed. In this case, it may be beneficial to move some hosts onto a remote network.

Placing additional hosts on a remote network will decrease the impact of traffic demands. However, hosts on one network will not be able to communicate with hosts on the other without the use of routing. Routers increase the complexity of the network configuration and can introduce latency, or time delay, on packets sent from one local network to the other.

All hosts in One Local Segment



Placing All Hosts in One Local Network Segment

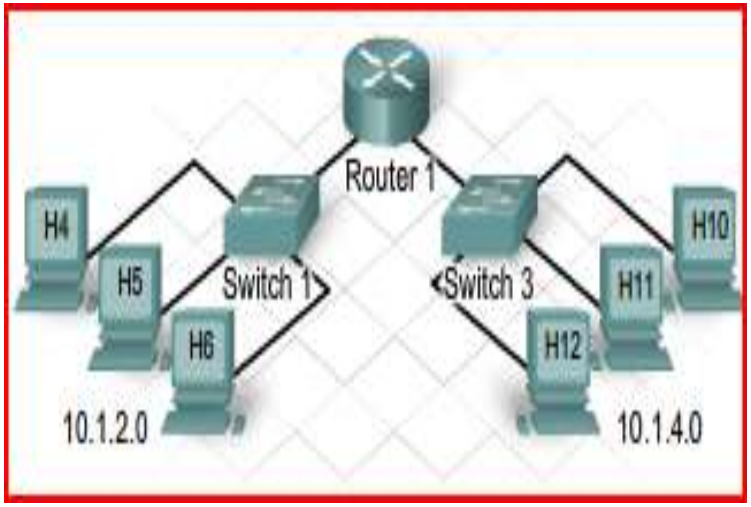
Advantages:

- Appropriate for simpler networks
- Less complexity and lower network cost
- Allows devices to be "seen" by other devices
- Faster data transfer - more direct communication
- Ease of device access

Disadvantages:

- All hosts are in one broadcast domain which causes more traffic on the segment and may slow network performance

Hosts in Remote Segments



Placing Hosts in Remote Network Segments

Advantages:

- More appropriate for larger, more complex networks
- Splits up broadcast domains and decreases traffic
- Can improve performance on each segment
- Makes the machines invisible to those on other local network segments
- Can provide increased security
- Can improve network organization

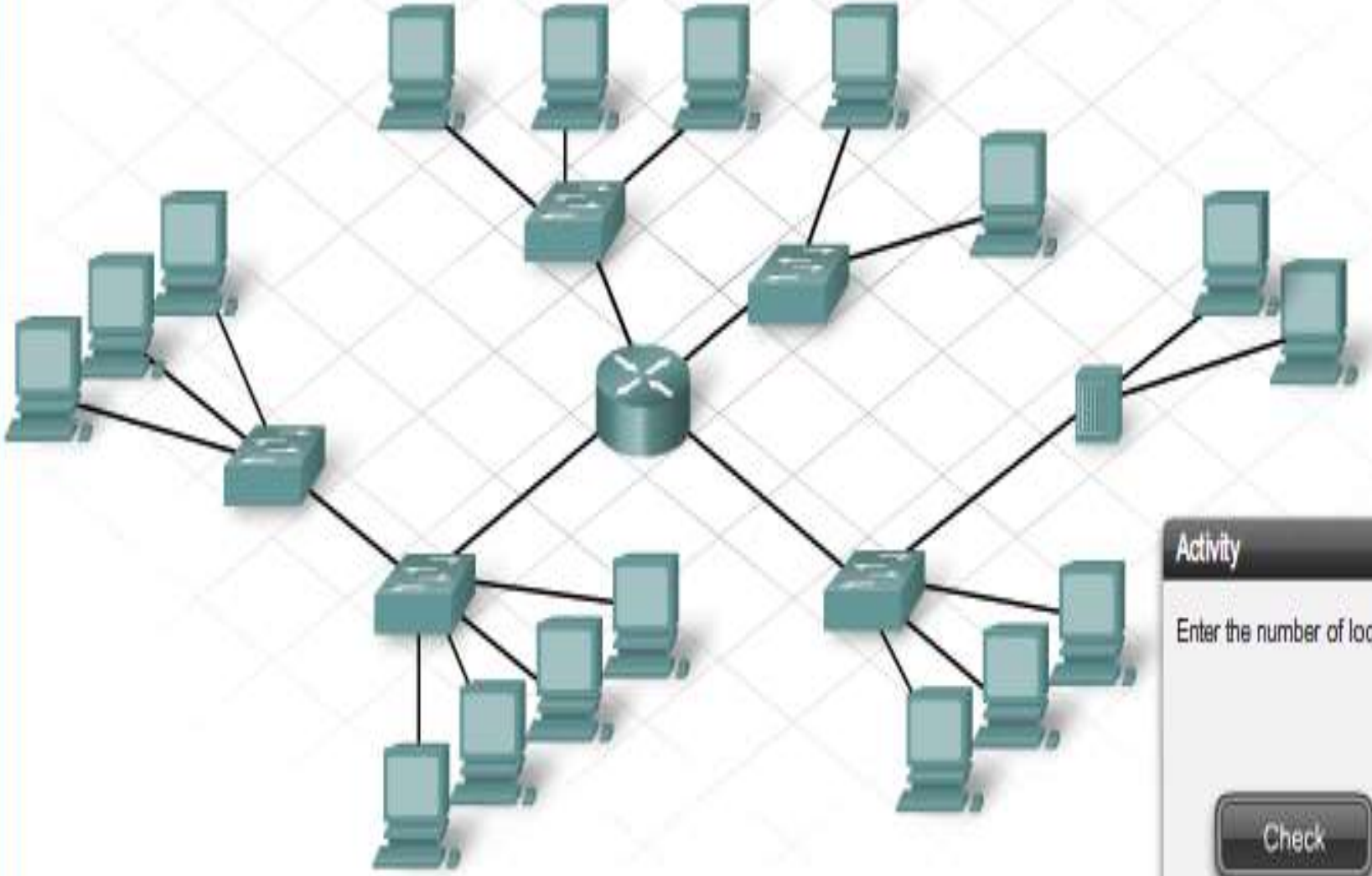
Disadvantages:

- Requires the use of routing (distribution layer)
- Router can slow traffic between segments
- More complexity and expense (requires router)

Activity

Identify the number of local networks within the LAN.

Count the local networks and enter the number in the space provided.



Activity

Enter the number of local networks:

Check Reset

Questions:

a) How many switches can you see?
b) How many hubs?
c) How many routers?
d) Is there a Core-layer in this diagram?
e) From the Access layer, how many individual small local groups are there?
f) From the Distribution layer, how many LANs are there?
g) Is there a peer-to-peer connection?

Network Design and Planning:

- There are many considerations that must be taken into account when planning for a network installation.

- The logical and physical topology maps of the network need to be designed and documented before the networking equipment is purchased and the hosts are connected.

- Some things to consider include:

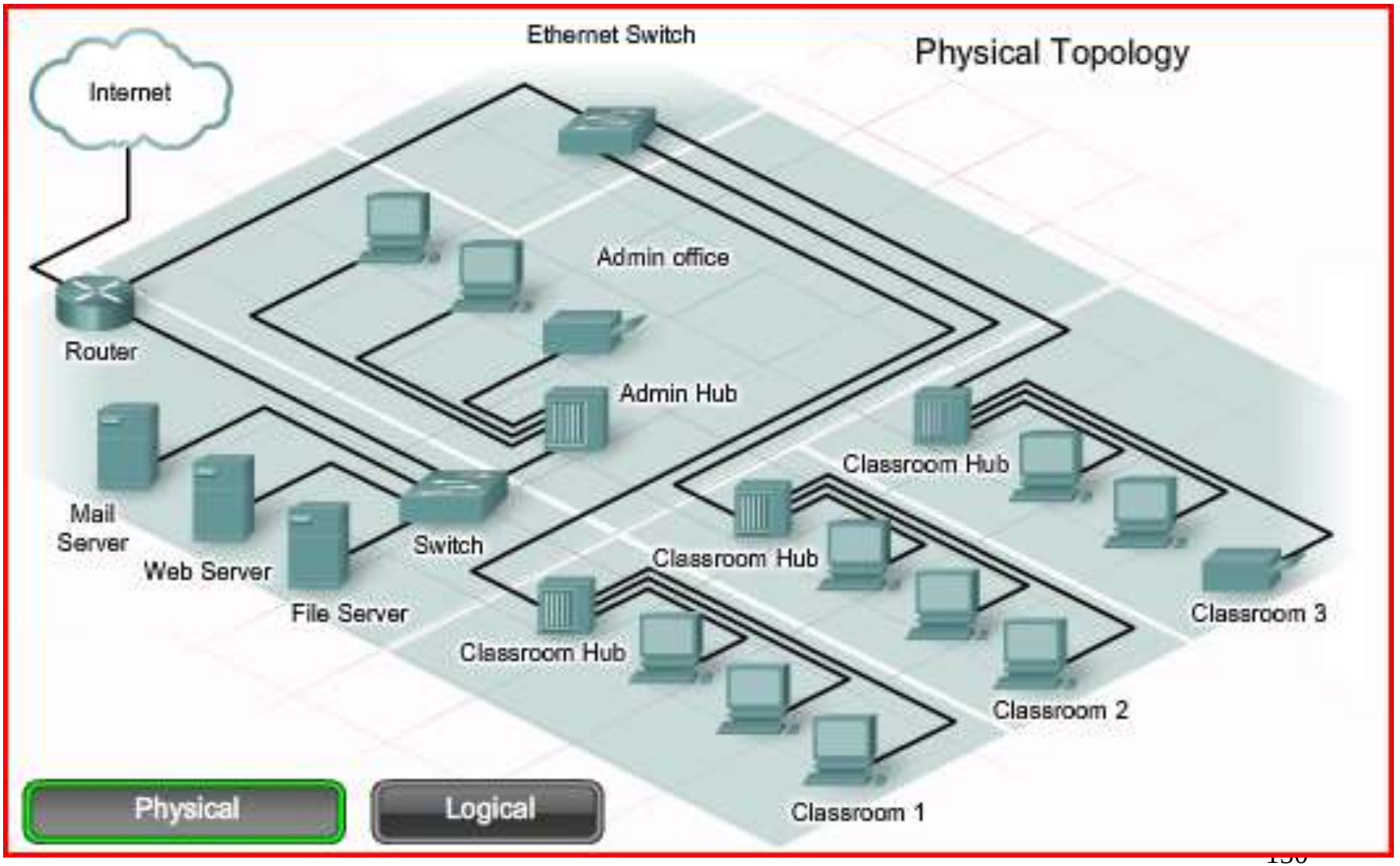
1. Physical environment where the network will be installed:
   - Temperature control: all devices have specific ranges of temperature and humidity requirements for proper operation
   - Availability and placement of power outlets

Network Design and Planning:

2. Physical configuration of the network:
   - Physical location of devices such as routers, switches, and hosts
   - How all devices are interconnected
   - Location and length of all cable runs
   - Hardware configuration of end devices such as hosts and servers

3. Logical configuration of the network:
   - Location and size of broadcast and collision domains
   - IP addressing scheme
   - Naming scheme
   - Sharing configuration
   - Permissions

Physical Layout Planning



Logical Layout Planning