



Lecture 1

INTRODUCTION TO COMPUTER NETWORKS

Dr.Lway Faisal Abdulrazak

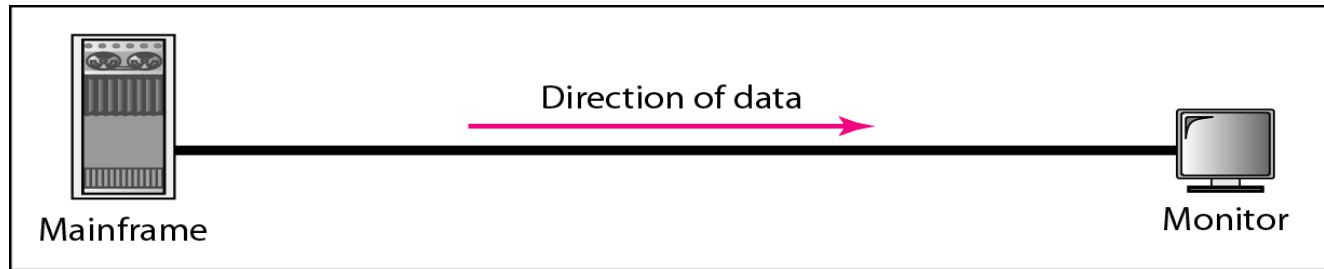
What is a Network?

*A **network** is a set of devices (**nodes**) connected by communication **links**. A node can be a computer, printer, CCTV cameras or any other device capable of sending and/or receiving data generated by other nodes on the network. A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.*

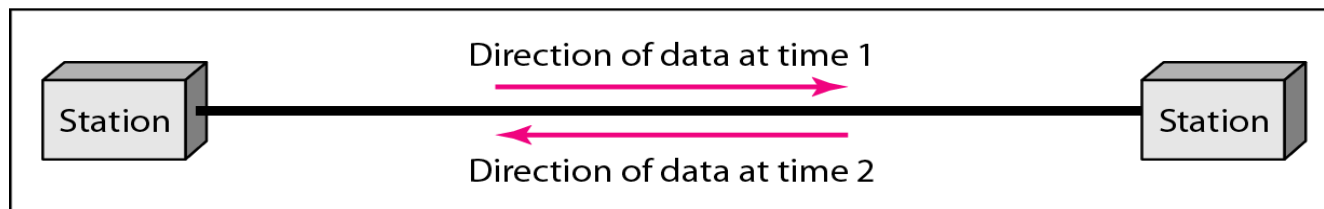
Why we need Networking?

- **Sharing information**
- **Sharing hardware or software.**
- **Centralize administration and support.**

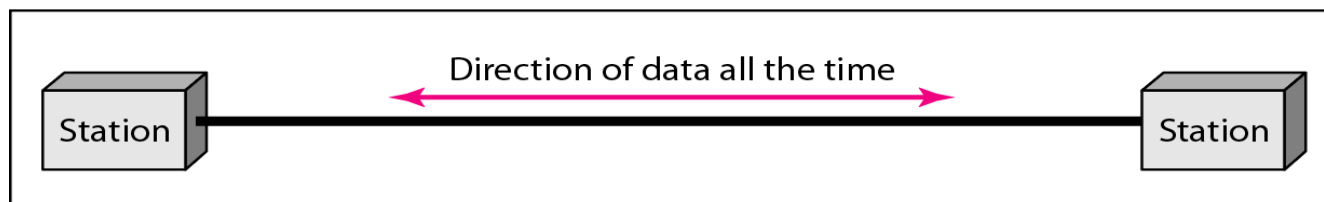
Data flow (simplex, half-duplex, and full-duplex)



a. Simplex



b. Half-duplex



c. Full-duplex

Simplex : one way like radio broadcast, Paging system satellite broadcasting.

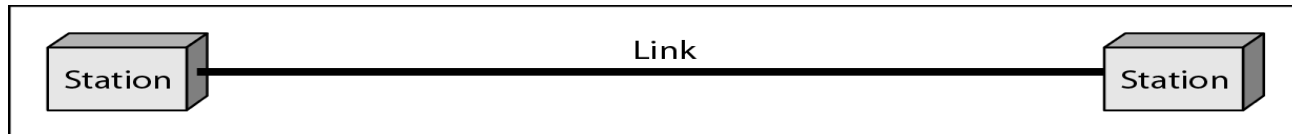
Half-duplex: two-way of communication Like: walky-talky,

Full: like cellular system, Telephone.

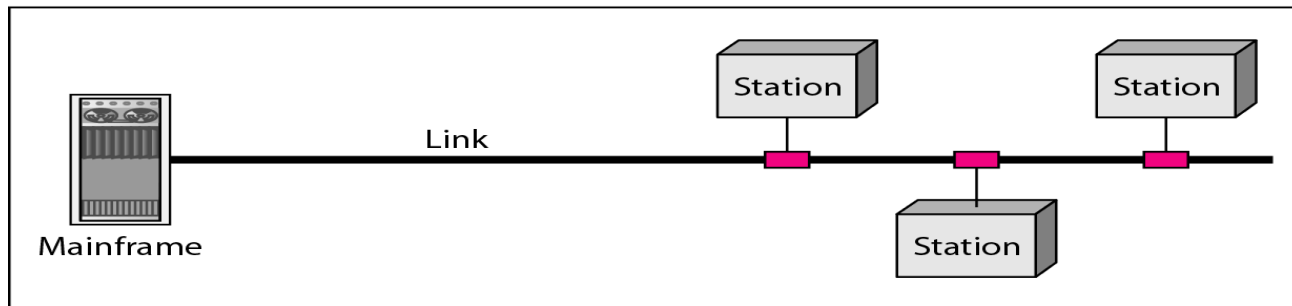
Physical Structures

- **Type of Connection**

- **Point to Point** - single transmitter and receiver
- **Multipoint** - multiple recipients of single transmission



a. Point-to-point



b. Multipoint

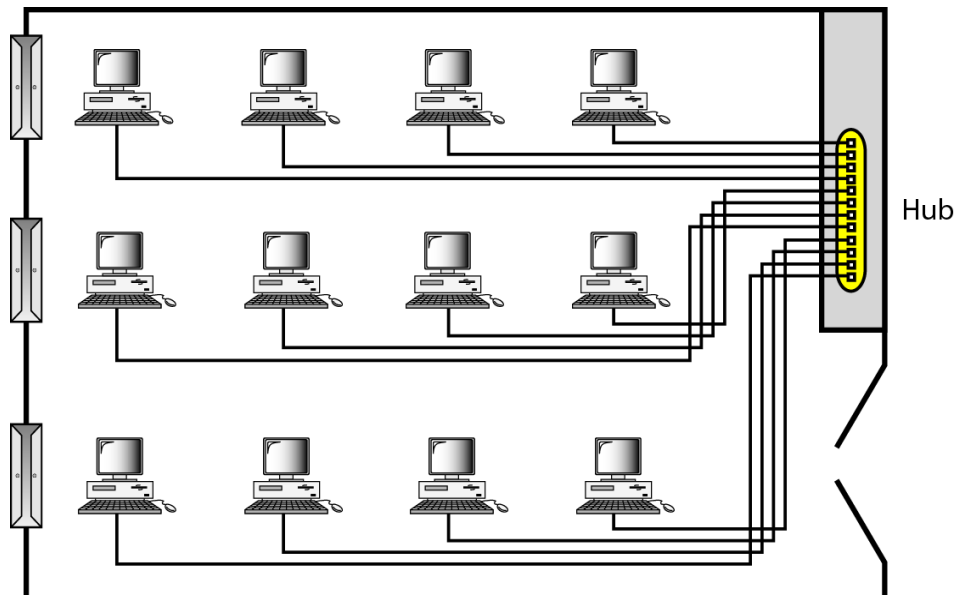
How many kinds of Networks?

- we can classify networks in different ways:
- Based on **network size**: LAN and WAN (and MAN)
- Based on **management method**: Peer-to-peer and Client/Server
- Based on **topology** (connectivity): Bus, Star, Ring ..
- Based on **transmission media**: Wired (UTP, coaxial cables, fiber-optic cables) and Wireless

Network Size

- **Local Area Network (LAN)**

- Small network, short distance suitable for a room, a floor, and building. It is limited by **number of computers** and **distance covered** or serve a department within an organization
- **Examples:** Network inside your home



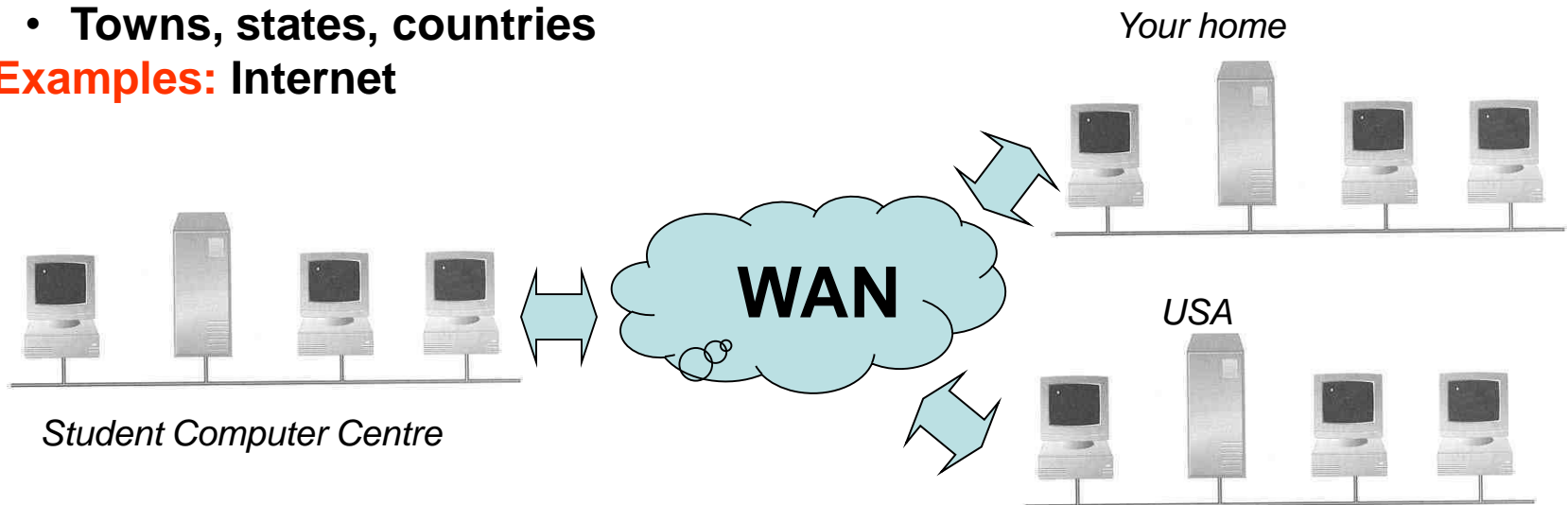
An isolated LAN connecting 12 computers to a hub

Network Size

A **metropolitan area network (MAN)** is a network that interconnects users with computer resources in a geographic area or region larger than that covered by [LAN](#) but smaller than the [WAN](#). The term is applied to the interconnection of networks in a city into a single larger network. It is also used to mean the interconnection of several local area networks by bridging them with [backbone](#) lines.

Wide Area Network (WAN)

- A network that uses long-range **telecommunication links** to connect 2 or more LANs/computers housed in different places far apart.
 - Towns, states, countries
- **Examples:** Internet



Network Size



- **Example WAN technologies:**
 - **ISDN** – Integrated Service Digital Network
 - Basic rate: 192 Kbps Primary rate: 1.544Mbps
 - **T-Carriers** — basically digital phone lines
 - T1: 1.544Mbps T3: 28×T1
 - **Frame relay**
 - Each link offers 1.544Mbps or even higher
 - **ATM** – Asynchronous Transfer Mode
 - Support : 155Mbps or 622Mbps or higher
 - **SONET** – Synchronous Optical Network
 - Basic rate OC1: 51.84Mbps
 - Support OC12 and up to OC192 (9953.28Mbps) or even higher in the future

Peer-to-Peer Networks

- **No hierarchy** among computers \Rightarrow all are equal.
- **No administrator** responsible for the network.



- **Where peer-to-peer network is appropriate:**
 - 10 or less users
 - Security is not an issue
 - Only limited growth in the future

Clients and Servers

- **Network Clients (Workstation)**
 - Computers that request network resources or services
- **Network Servers**
 - Computers that manage and provide network resources and services to clients.
 - Usually have more processing power, memory and hard disk space than clients.
 - Run **Network Operating System** that can manage not only data, but also **users, groups, security, and applications** on the network.
- **Advantages of client/server networks**
 - Enhance security – only administrator can have access to Server.
 - Support more users – difficult to achieve with peer-to-peer networks

Network Topology

• Bus Topology

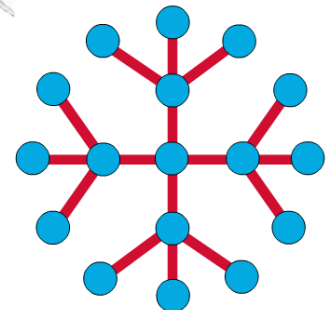
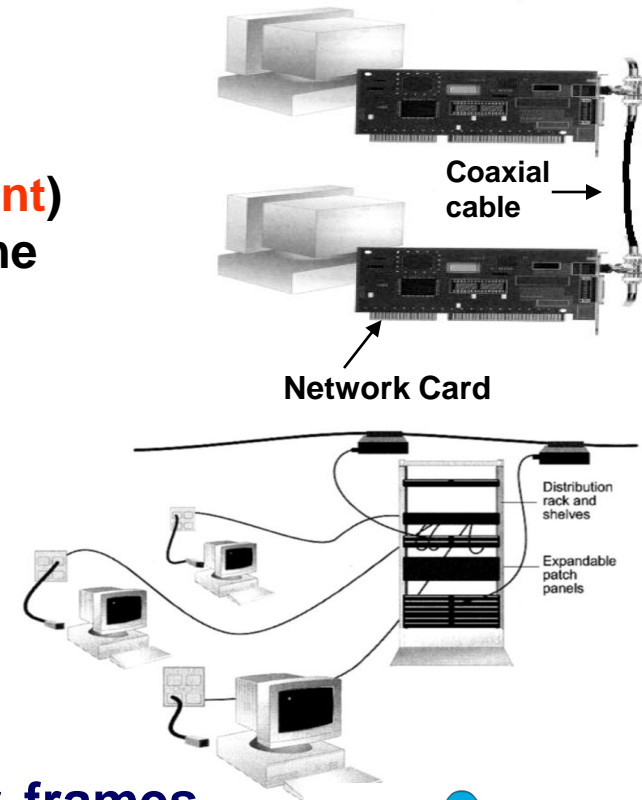
- Simple and low-cost
- A single cable called a **trunk (backbone, segment)**
- Only one computer can send messages at a time

• Star Topology

- Each computer has a cable connected to a single point
- All signals transmission through the hub; **if down, entire network down.**

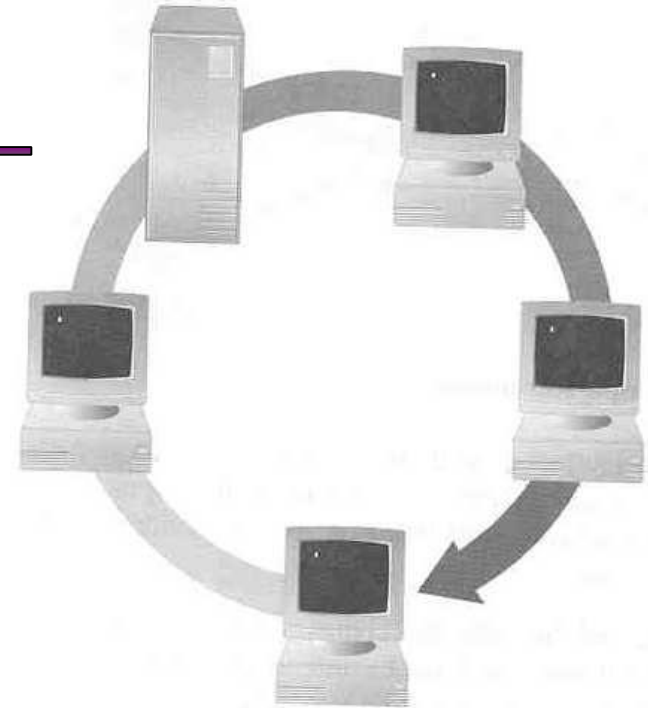
Extended Star or Tree Topology

- When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces the traffic on the wires by sending packets only to the wires of the destination host.



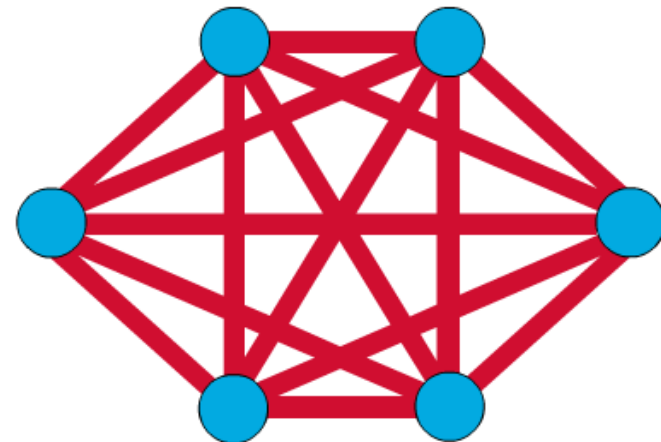
Ring Topology

- Every computer serves as a repeater to boost signals
- Typical way to send data:
 - Difficult to add computers
 - If one computer fails, whole network fails



Mesh Topology

- The mesh topology connects all devices (nodes) to each other for redundancy and fault tolerance.
- Implementing the mesh topology is expensive and difficult.

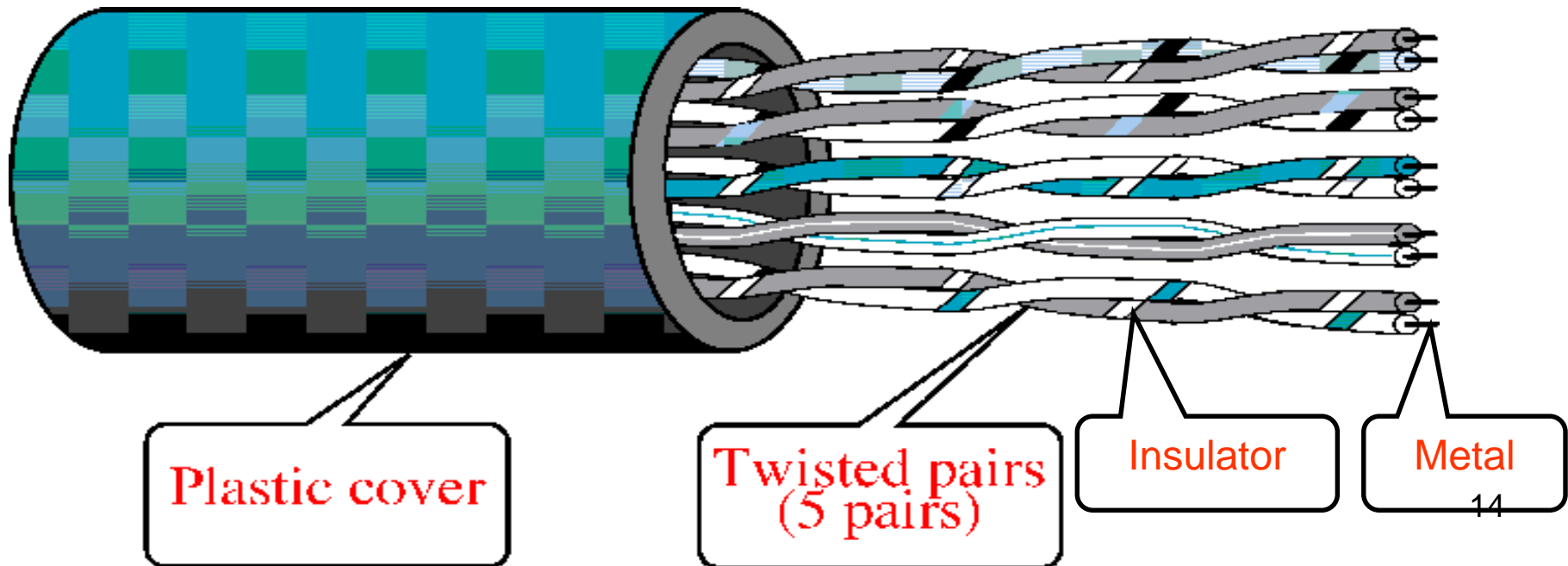


Transmission Media

- **Two main categories:**
 - **Guided** — wires, cables
 - **Unguided** — wireless transmission, e.g. radio, microwave, infrared, sound, sonar
- **We will concentrate on guided media here:**
 - **Twisted-Pair cables:**
 - **Unshielded Twisted-Pair (UTP) cables**
 - **Shielded Twisted-Pair (STP) cables**
 - **Coaxial cables**
 - **Fiber-optic cables**

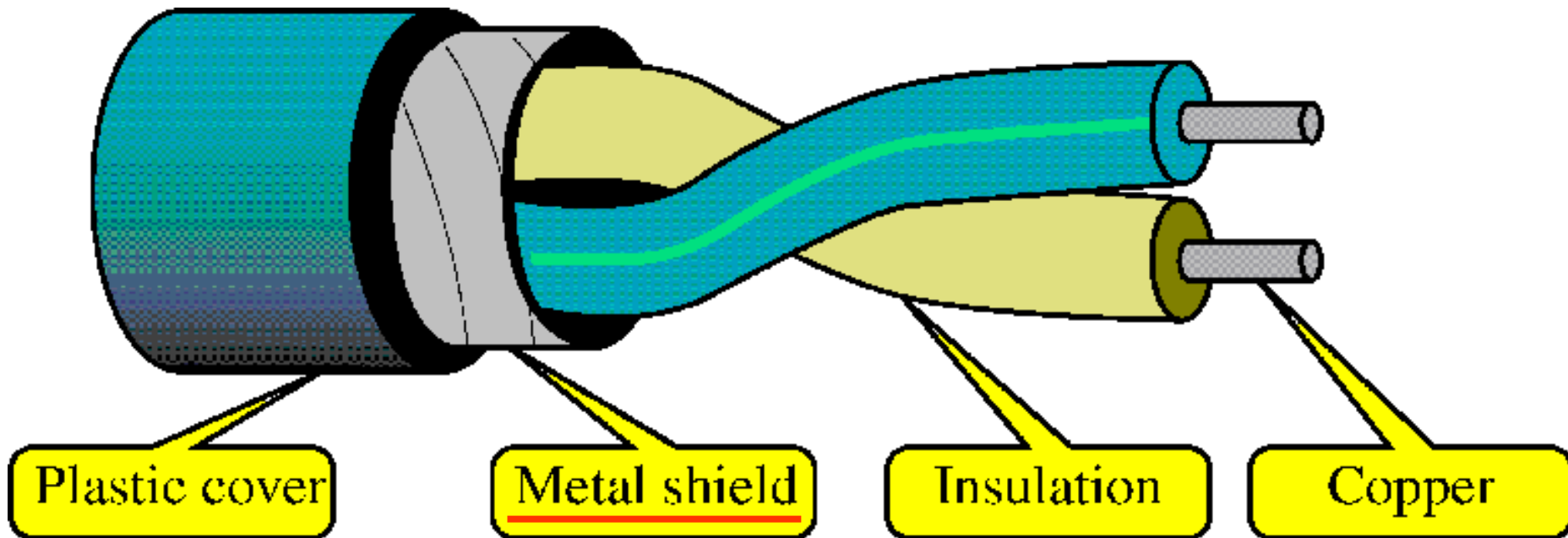
Unshielded Twisted-Pair (UTP)

- Typically wrapped inside a plastic cover (for mechanical protection)
- A sample UTP cable with 5 unshielded twisted pairs of wires



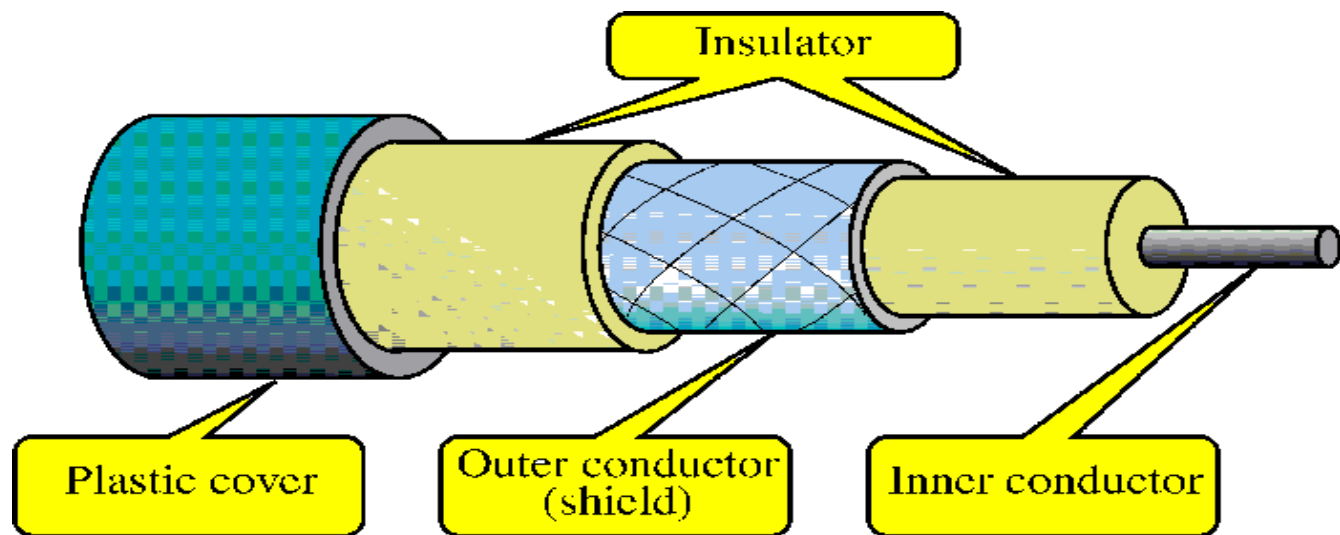
Shielded Twisted-Pair (STP)

- STP cables are similar to UTP cables, except there is a metal foil or braided-metal-mesh cover that encases each pair of insulated wires



Coaxial Cables

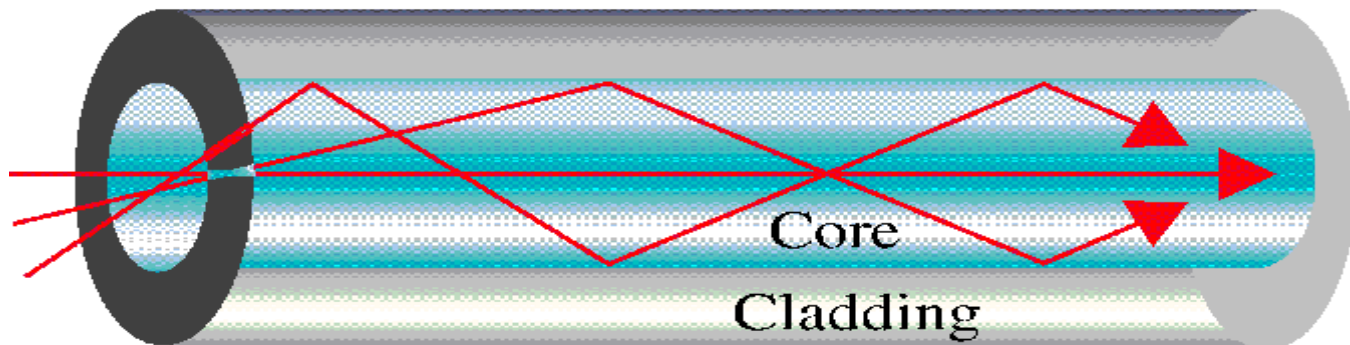
- In general, coaxial cables, or coax, carry signals of 100KHz–500MHz, and speed of up to 10Mbps.
- Outer metallic wrapping serves as a shield against noise.
- Advantage: It is very resistant to Electromagnetic Interference, easy to cut it and adjust the size.
- Disadvantage: not supported by fast Internet standard, more expensive.



Fiber-Optic Cables

- Light travels at $3 \times 10^8 \text{ ms}^{-1}$ in free space and is the fastest possible speed in the Universe
- Light slows down in denser media, e.g. glass
- Refraction occurs at interface, with light bending away from the normal when it enters a less dense medium.
- We have also Diffraction and Reflection.

- An optical fiber consists of a **core** (denser material) and a **cladding** (less dense material).
- Simplest one is Single mode (with single path 10 Microns).
- **Multimode 50-100 Microns** = multiple paths, whereas **step-index** = refractive index follows a step-function profile (i.e. an abrupt change of refractive index between the **core** and the **cladding**).
- Light bounces back and forth along the core.
- Common light sources: LEDs and lasers



Advantages and Disadvantages

- 😊 Noise resistance — external light is blocked by outer jacket
- 😊 Less signal attenuation — a signal can run for miles without regeneration (currently, the lowest measured loss is about ~4% or 0.16dB per km)
- 😊 Higher bandwidth — currently, limits on data rates come from the signal generation/reception technology, not the fiber itself
- 😞 Cost — Optical fibers are expensive
- 😞 Installation/maintenance — any crack in the core will degrade the signal, and all connections must be perfectly aligned

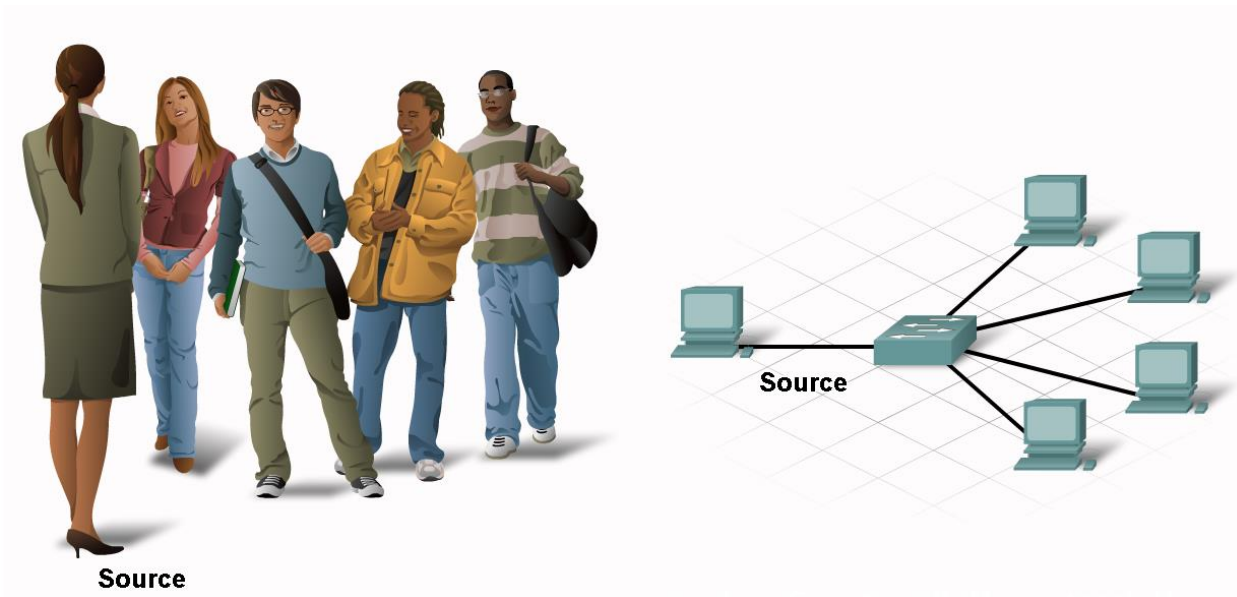
Communication Protocols

Message Patterns

Unicast – single destination

Multicast – same message to a group

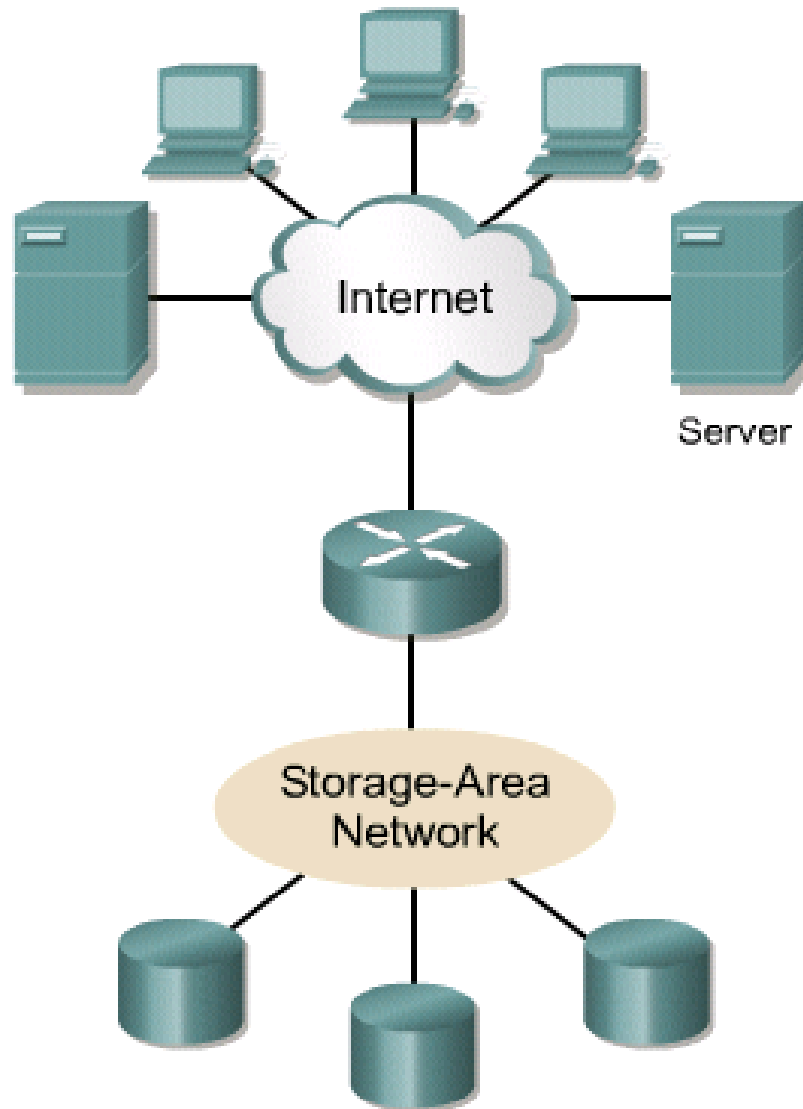
Broadcast – all hosts need to receive the message



Storage-Area Networks (SANs)

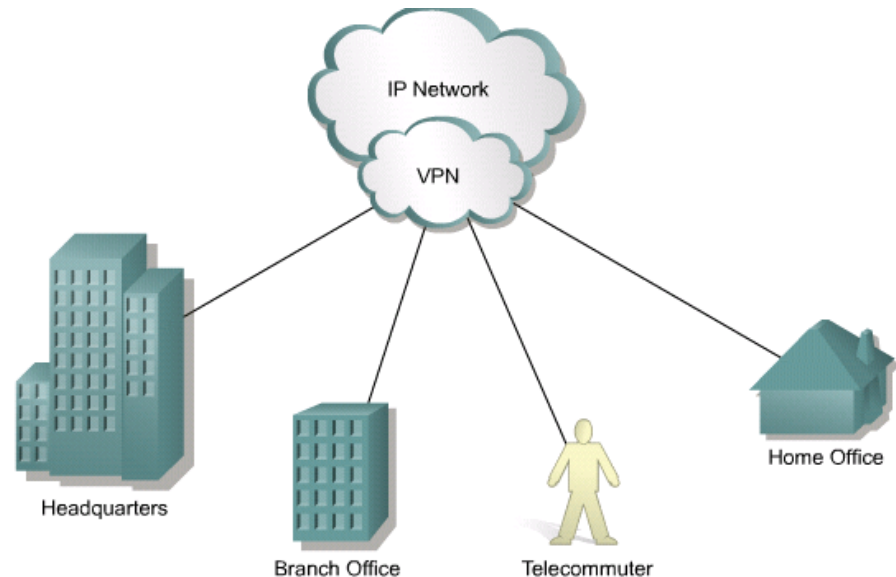
- A SAN is a dedicated, high-performance network used to move data between servers and storage resources.
- Separate, dedicated network, that avoids any traffic conflict between clients and servers
- SANs offer the following features:
 - **Performance** – allows concurrent access of disk or tape arrays by two or more servers at high speeds
 - **Availability** – have disaster tolerance built in, because data can be mirrored using a SAN up to 10km or 6.2 miles away.
 - **Scalability** – Like a LAN/WAN, it can use a variety of technologies. This allows easy relocation of backup data, operations, file migration, and data replication between systems.

SAN



Virtual private network (VPN)

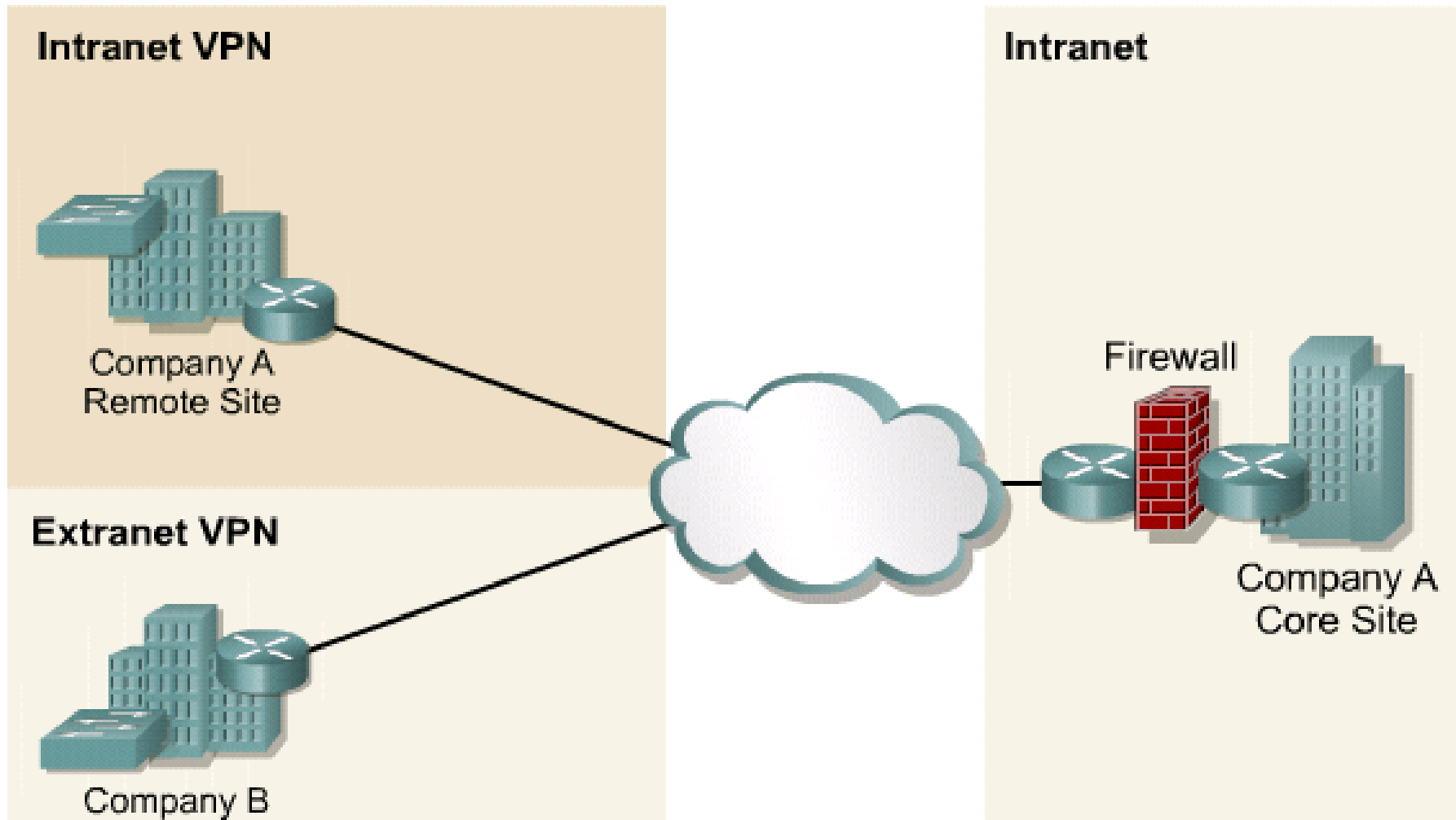
- A VPN is a private network that is constructed within a public network such as the Internet.
- It offers secure, reliable connectivity over a shared public network infrastructure such as the Internet.
- A telecommuter can access the network of the company through the Internet by building a secure tunnel between the telecommuter's PC and a VPN router in the company



Benefits of VPNs

- Three main types of VPNs:
 - **Access VPNs** – provide remote access to a mobile worker and a SOHO to the hq of the Intranet or Extranet over a shared infrastructure.
 - **Intranet VPNs** – link regional and remote offices to the hq of the internal network over a shared infrastructure using *dedicated connections*. They allow access only to the employees of the enterprise.
 - **Extranet VPNs** – link business partners to the hq of the network over a shared infrastructure using *dedicated connections*. They allow access to users outside the enterprise

Intranets and extranets



Importance of bandwidth

- Bandwidth is the amount of information that can flow through a network connection in a given period of time.
- **Bandwidth is finite**
 - the bandwidth of a modem is limited to about 56 kbps by both the physical properties of twisted-pair phone wires and by modem technology
- **Bandwidth is not free**
 - For WAN connections bandwidth is purchased from a service provider
- A key factor in analyzing network performance and designing new networks
- The demand for bandwidth is ever increasing

Measurement

- In digital systems, the basic unit of bandwidth is bits per second (bps)
- The actual bandwidth of a network is determined by a combination of the physical media and the technologies chosen for signaling and detecting network signals

Typical Media	Maximum Theoretical Bandwidth	Maximum Theoretical Distance
50-Ohm Coaxial Cable (10BASE2 Ethernet; Thinnet)	10 Mbps	185 m
50-Ohm Coaxial Cable (10BASE5 Ethernet; Thicknet)	10 Mbps	500 m
Category 5 Unshielded Twisted Pair (UTP) (10BASE-T Ethernet)	10 Mbps	100 m
Category 5 Unshielded Twisted Pair (UTP) (100BASE-TX Ethernet)	100 Mbps	100 m
Category 5 Unshielded Twisted Pair (UTP) (1000BASE-TX Ethernet)	1000 Mbps	100 m
Multimode Optical Fiber (62.5/125mm) (100BASE-FX Ethernet)	100 Mbps	2000 m
Multimode Optical Fiber (62.5/125mm) (1000BASE-SX Ethernet)	1000 Mbps	220 m
Multimode Optical Fiber (50/125mm) (1000BASE-SX Ethernet)	1000 Mbps	550 m

Limitations

- Bandwidth is limited by a number of factors
 - Media
 - Network devices
 - Physics
- Each have their own limiting factors
- Actual bandwidth of a network is determined by a combination of the physical media and the technologies chosen for signaling and detecting network signals

Throughput

- Throughput is the actual, measured, bandwidth, at a specific time of day, using specific internet routes, while downloading a specific file. The throughput is often far less than the maximum bandwidth
- Factors that determine throughput:
 - Internetworking devices
 - Type of data being transferred
 - Network topology
 - Number of users on the network
 - User computer
 - Server computer

Data transfer calculation

Best Download

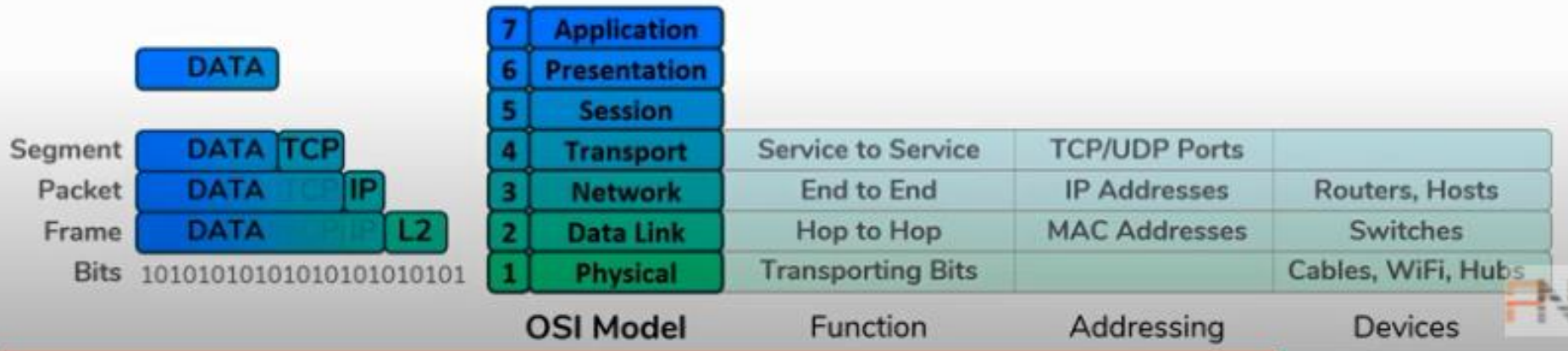
$$T = \frac{S}{BW}$$

Typical Download

$$T = \frac{S}{P}$$

BW	Maximum theoretical bandwidth of the "slowest link" between the source host and the destination host (measured in bits per second)
P	Actual throughput at the moment of transfer (measured in bits per second)
T	Time for file transfer to occur (measured in seconds)
S	File size in bits

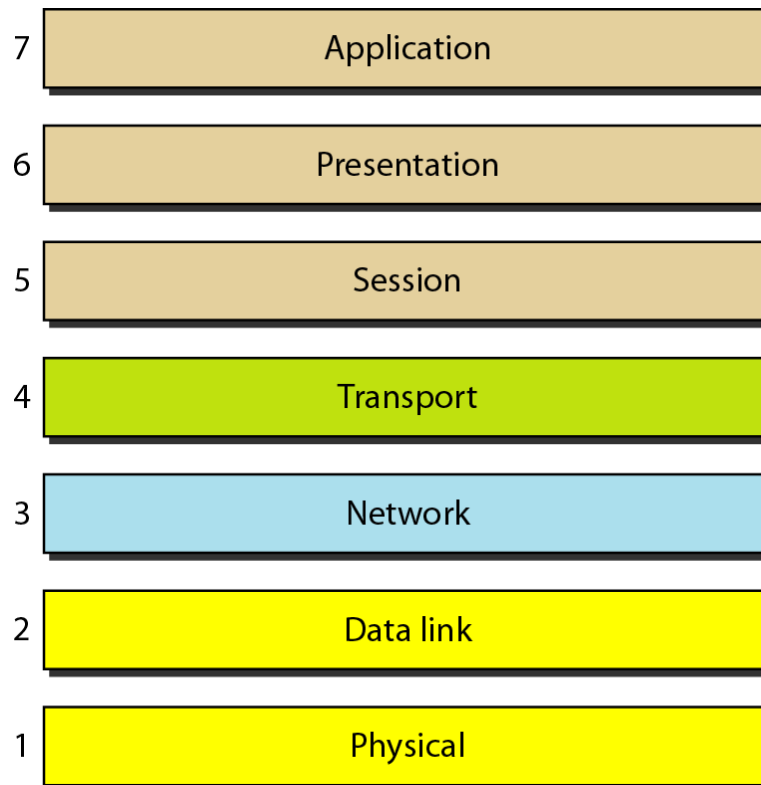
Network Models



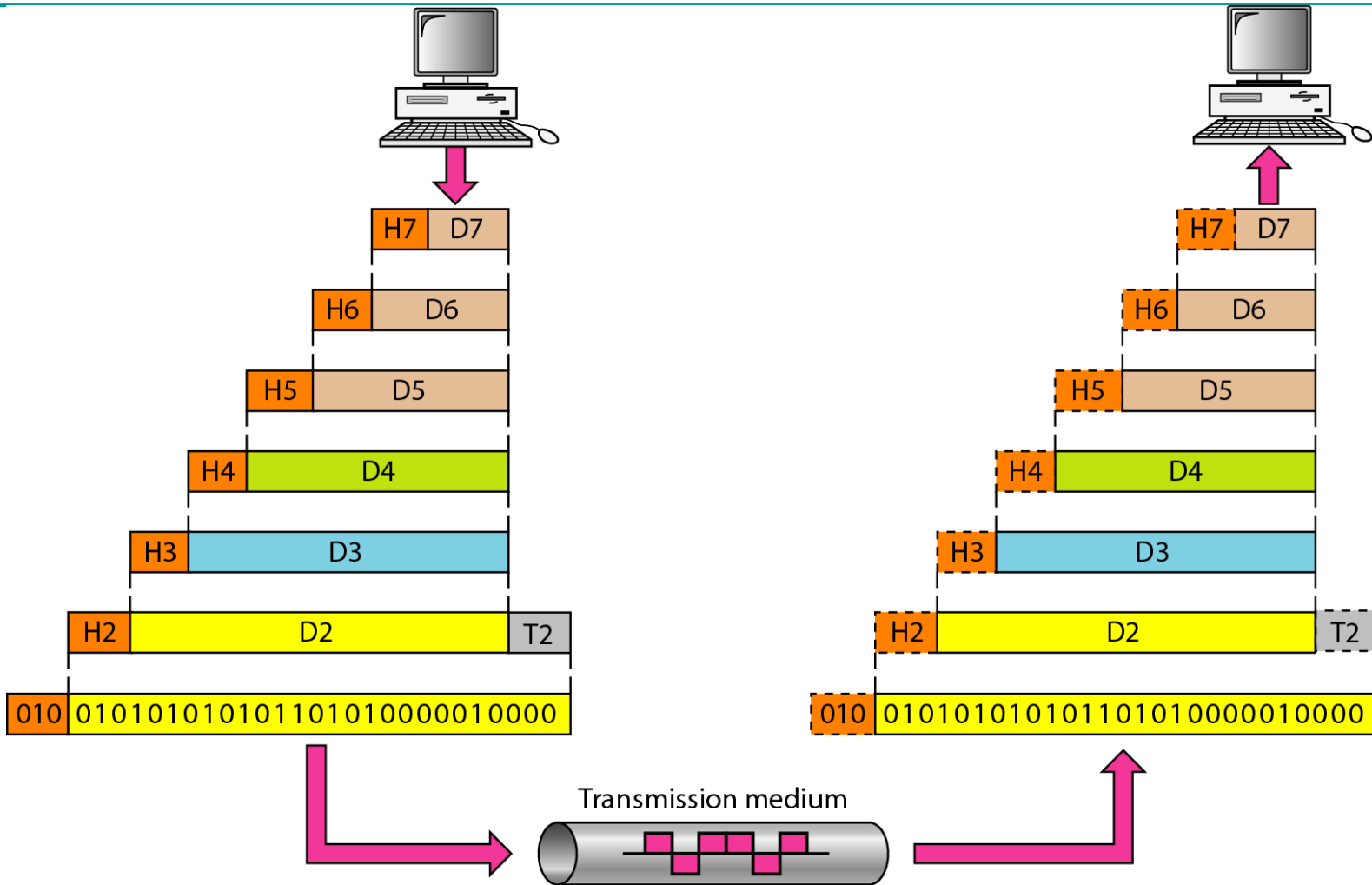
THE OSI MODEL

Established in 1947, the International Standards Organization (ISO). An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.

Seven layers of the OSI model



An exchange using the OSI model

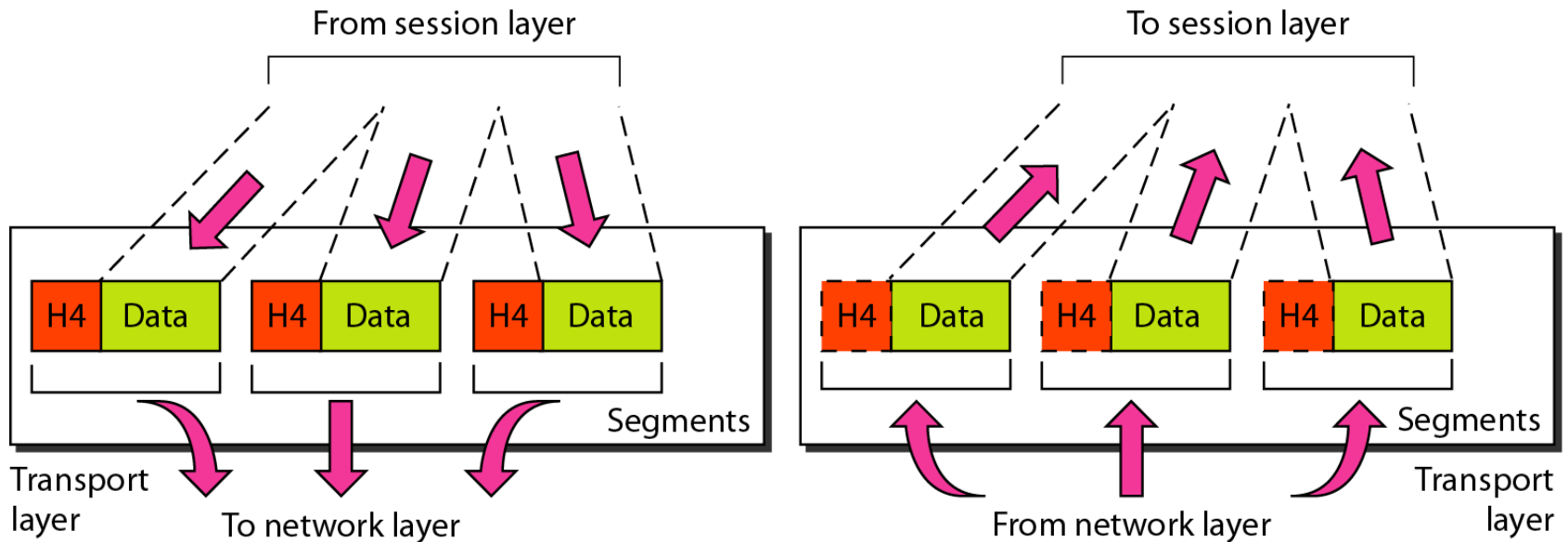


The data link layer is responsible for moving frames from one hop (node) to the next.

Network layer:

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Transport layer:

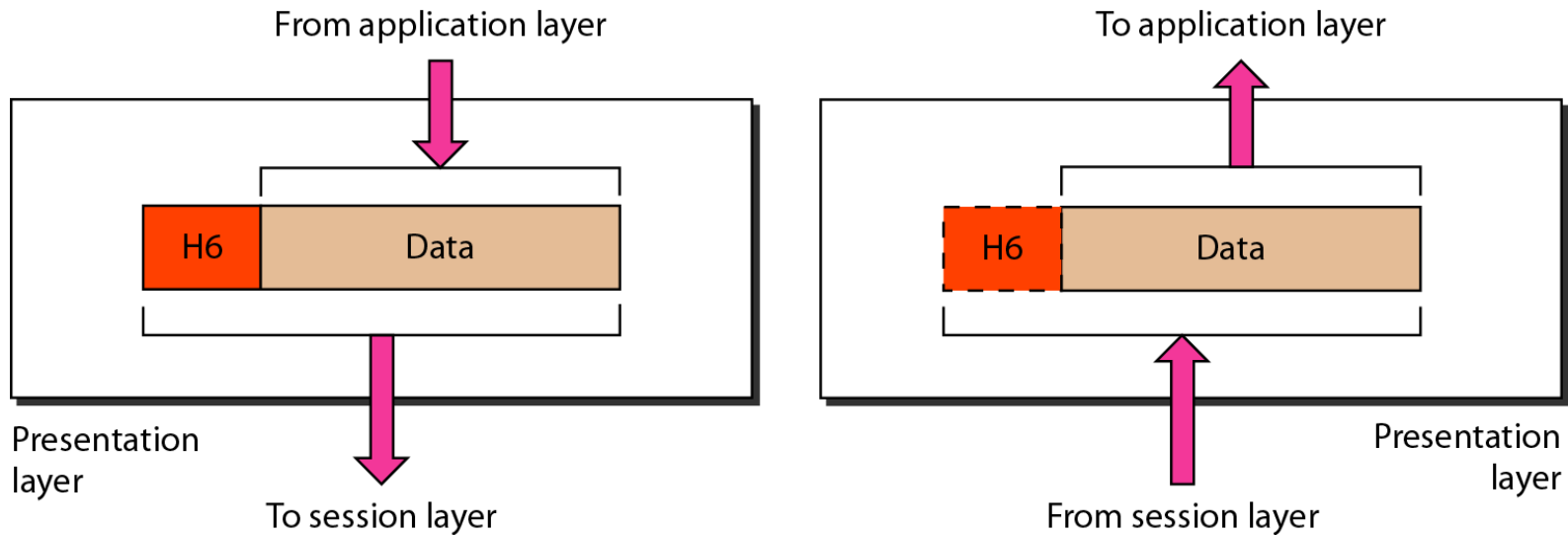


The transport layer is responsible for the delivery of a message from one process to another.

Session layer:

The session layer is responsible for dialog control and synchronization.

Presentation layer:

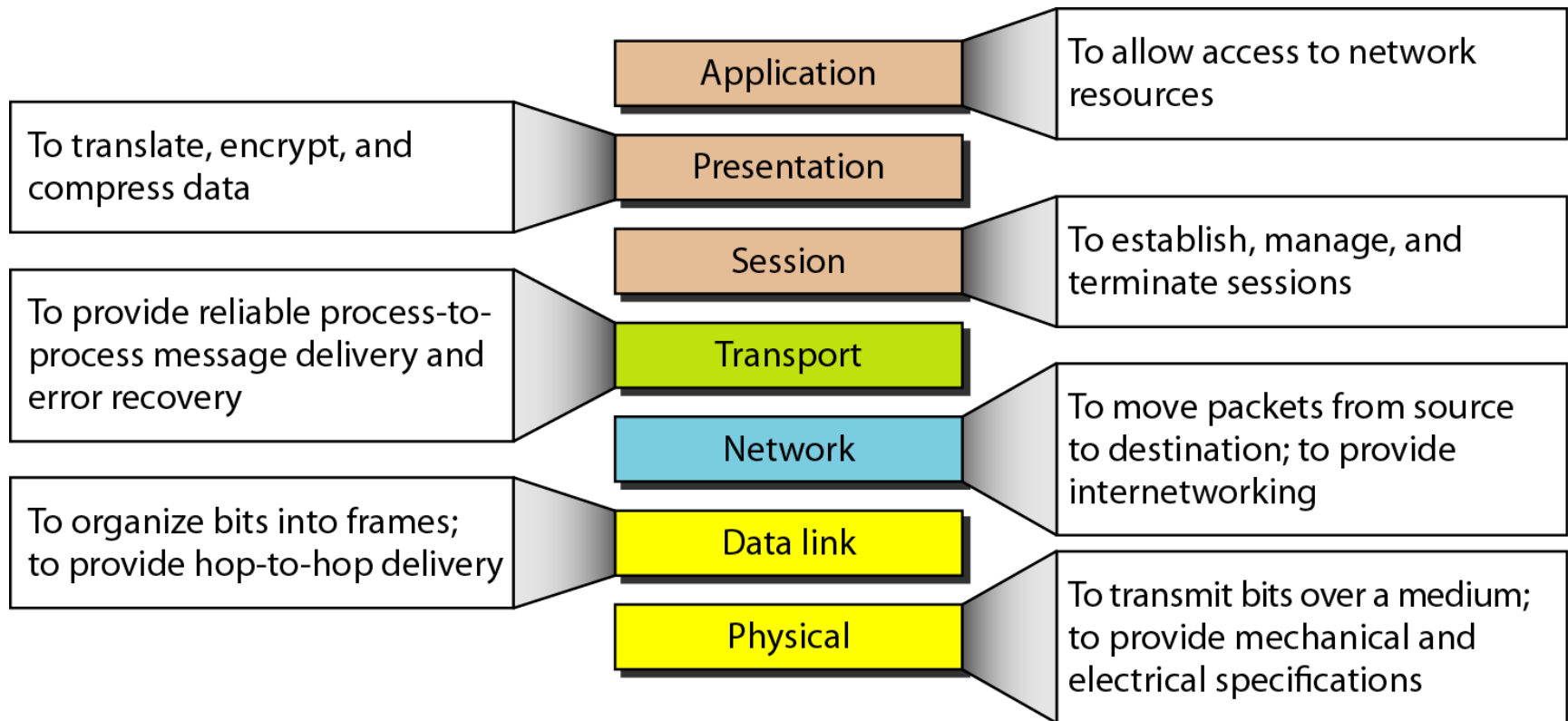


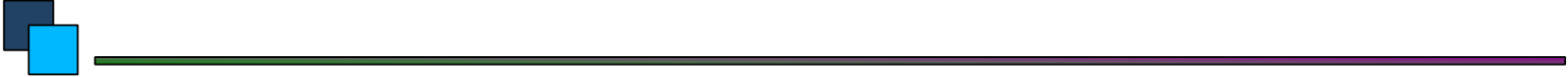
The presentation layer is responsible for translation, compression, and encryption.

Application layer:

The application layer is responsible for providing services to the user.

Summary of layers





TCP/IP

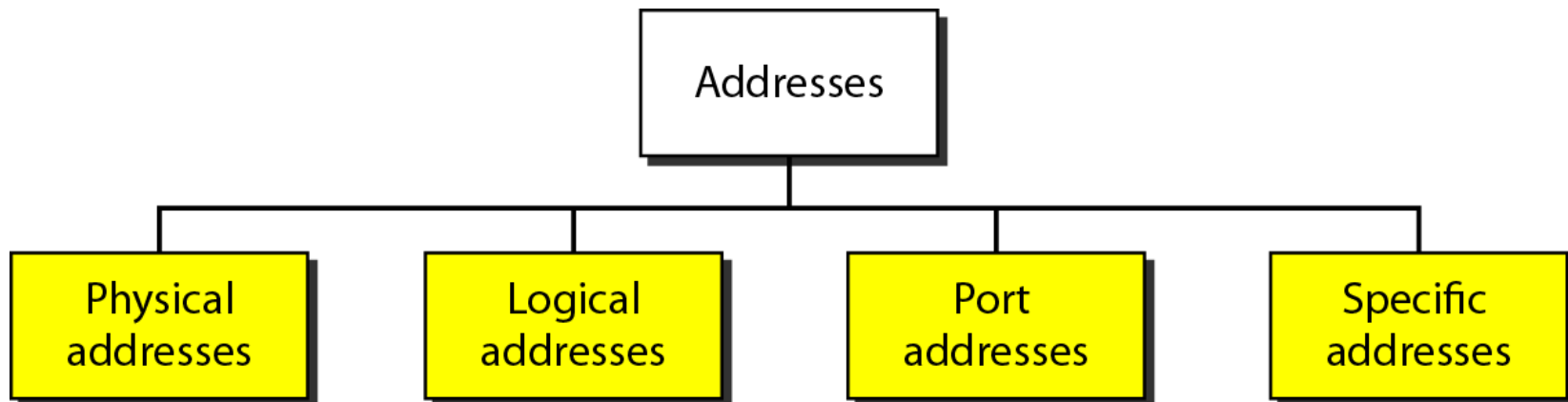
Dr. Lway Faisal

TCP/IP PROTOCOL SUITE

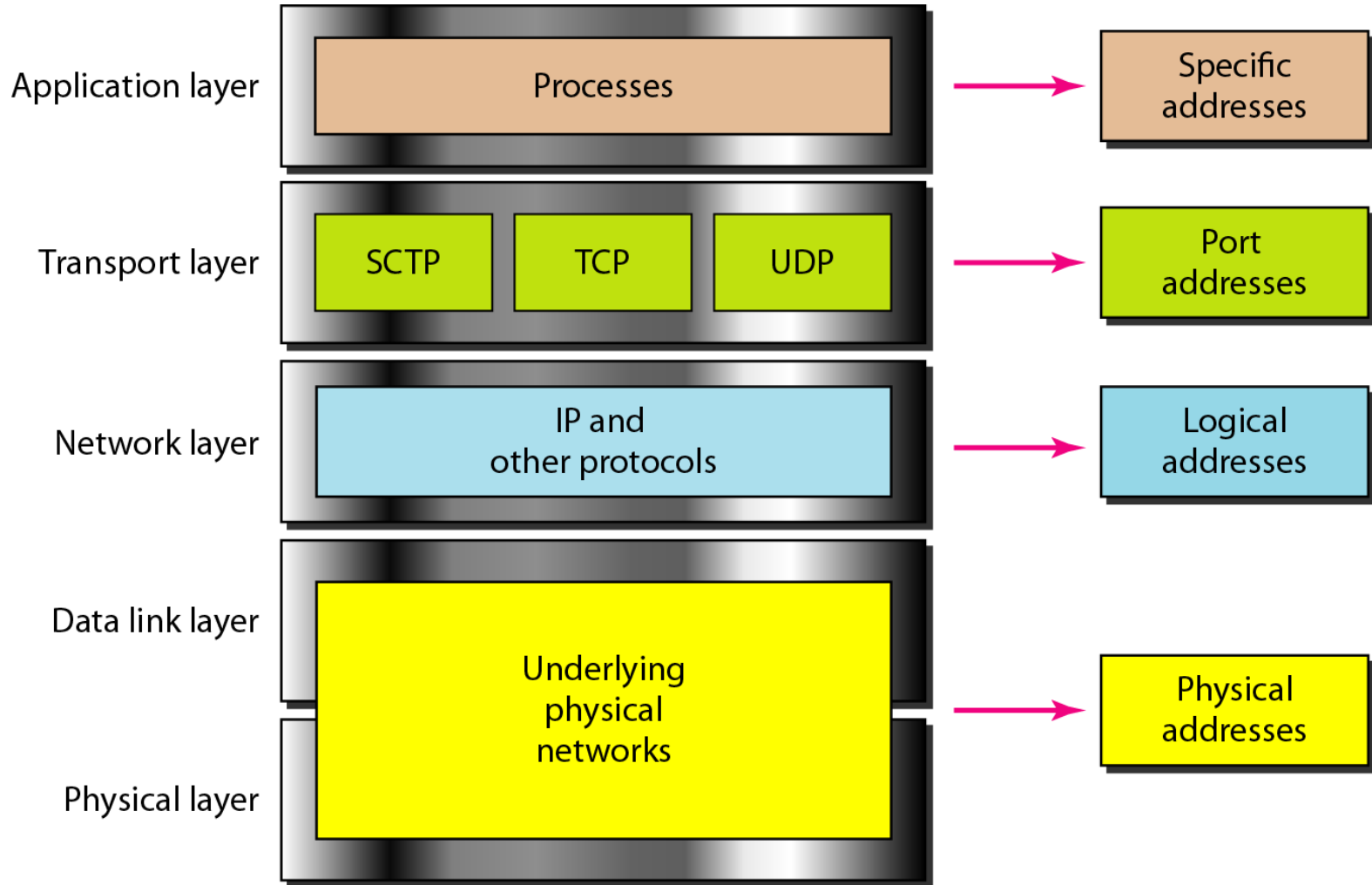
When TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers: *physical*, *data link*, *network*, *transport*, and *application*.

ADDRESSING

Four levels of addresses are used in an internet employing the TCP/IP protocols: *physical*, *logical*, *port*, and *specific*.



Relationship of layers and addresses in TCP/IP



Physical Address

- *Physical address or (hardware Address), or MAC address.*
- *Each node has a unique MAC Address: Globally identifier that burned into your RAM of your network interface card.*
- *MAC Address assigned by manufacturer , each factory has a block of address assigned by IEEE.*
- *No two networks in the world have the same Address.*
- *local-area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below:*


07:01:02:01:2C:4B

A 6-byte (12 hexadecimal digits) physical address.



Network Layer: Logical Addressing

Dr. Lway Faisal



An IP address (Internet Protocol Address) or (logical Address) is a unique address that devices use it in order to communicate with each other.

IP addresses are managed and created by the Internet Assigned Numbers Authority (**IANA**).

IP have two versions:

1. IPv4 is 32bits
2. IPv6 is 128bits

The network layer is responsible for the delivery of individual packets from the source host to the destination host.

IPv4 ADDRESSES

An IPv4 address is 32 bits long, are unique and universal.

A protocol IPv4 has an address space. An **address space** is the total number of addresses used by the protocol. If a protocol uses N bits to define an address, the address space is 2^N .

IPv4 uses 32-bit addresses, which means that the address space is 2^{32} or 4,294,967,296 (more than 4 billion). This means that, theoretically, if there were no restrictions, more than 4 billion devices could be connected to the Internet.

Notations

There are two prevalent notations to show an IPv4 address: **binary notation** and **dotted-decimal notation**.

Binary Notation

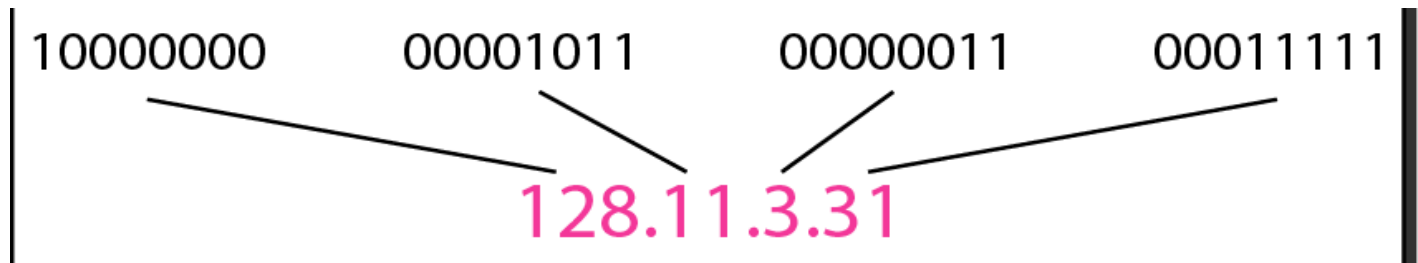
In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. Example: 01110101 10010101 00011101 00000010

00000000.00000000.00000000.00000000

11111111.11111111.11111111.11111111

Dotted-Decimal Notation

To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. Example:



Note that because each byte (octet) is 8 bits, each number in dotted-decimal notation is a value ranging from 0 to 255.

Example 2.1

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

a. 10000001 00001011 00001011 11101111

b. 11000001 10000011 00011011 11111111

Solution

We replace each group of 8 bits with its equivalent decimal number and add dots for separation.

a. 129.11.11.239

b. 193.131.27.255

Example 2.2

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

a. 111.56.45.78

b. 221.34.7.82

Solution

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

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Example 2.3

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

- a. 111.56.045.78
- b. 221.34.7.8.20
- c. 75.45.301.14
- d. 11100010.23.14.67

Solution

- a. There must be no leading zero (045).**
- b. There can be no more than four numbers.**
- c. Each number needs to be less than or equal to 255.**
- d. A mixture of binary notation and dotted-decimal notation is not allowed.**

Classful Addressing

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

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

a. Binary notation

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

b. Dotted-decimal notation

Finding the classes in binary and dotted-decimal notation

Example 2.4

Find the class of each address?

- a. 00000001 00001011 00001011 11101111
- b. 11000001 10000011 00011011 11111111
- c. 14.23.120.8
- d. 252.5.15.111

Solution

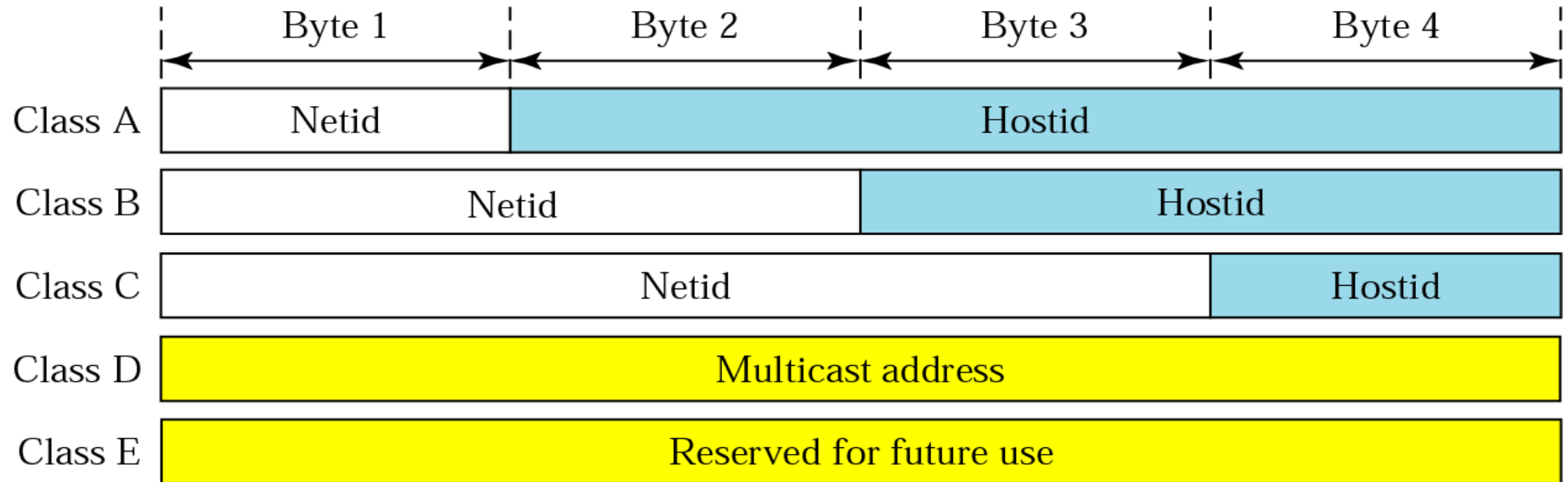
- a. The first bit is 0. This is a **class A** address.
- b. The first 2 bits are 1; the third bit is 0. This is a **class C** address.
- c. The first byte is 14; the **class is A**.
- d. The first byte is 252; the **class is E**.

Anatomy of an IP Address

- The IP address consists of two components:
- **First component** is the network portion of the address, consisting of the network bits.
- **Second component** is the host portion of the address, consisting of the host bits. They consist of the remaining bits not included with the network bits. **The part of an IP address that identifies a host.**



IP Address Classes



IP Address Classes

Class	Leading Bits	Size of Network Number Bit field	Size of Rest Bit field	Number of Networks	Addresses per Network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Mask or Default Mask

The masks for classes A, B, and C are shown in Table below
The concept does not apply to classes D and E.

The mask can help us to find the Net ID and the Host ID. For

<i>Class</i>	<i>Binary</i>	<i>Dotted-Decimal</i>	<i>CIDR</i>
A	11111111 00000000 00000000 00000000	255.0.0.0	/8
B	11111111 11111111 00000000 00000000	255.255.0.0	/16
C	11111111 11111111 11111111 00000000	255.255.255.0	/24

Subnetting

If an organization was granted a large block in class A or B, it could **divide** the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbors.

Supernetting:

A several networks are **combined** to create a super network.

Address Depletion

Yet the number of devices on the Internet is much less than the 2^{32} address space. We have run out of class A and B addresses, and a class C block is too small for most midsize organizations. *One solution that has alleviated the problem is the idea of classless addressing.*

Classful addressing: An IPv4 addressing mechanism in which the IP address space is divided into 5 classes: A, B, C, D, and E. Each class occupies some part of the whole address space.

Classless addressing: An addressing mechanism in which the IP address space is not divided into classes.

Classless Addressing

To overcome address depletion and give more organizations access to the Internet, classless addressing was designed and implemented. In this scheme.

Address Blocks

In classless addressing, when an entity, needs to be connected to the Internet, it is granted a **block** (**range**) of addresses. The **size of the block** (the **number of addresses**) **varies based on the nature and size of the entity**.

An ISP, as the Internet service provider, may be given thousands or hundreds of thousands based on the number of customers it may serve.

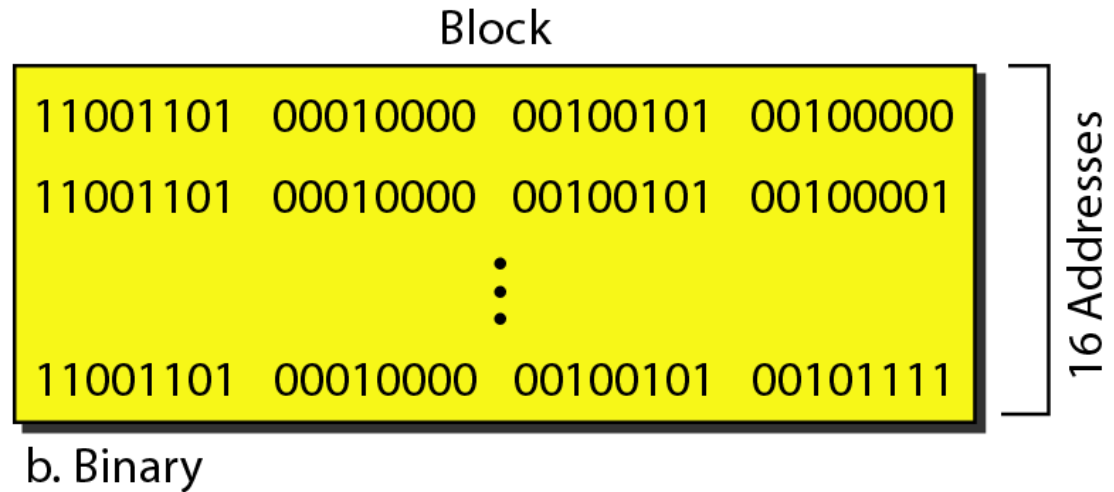
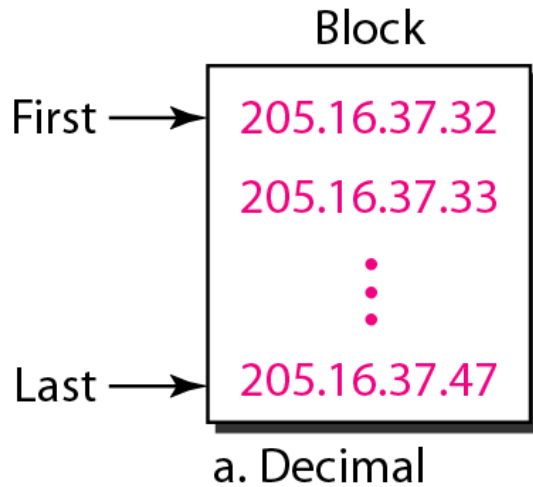
Restriction

To simplify the handling of addresses, the Internet authorities impose **three restrictions on classless address blocks**:

1. The addresses in a block must be contiguous, one after another.
2. The number of addresses in a block must be a power of 2 (1, 2,4,8,.etc)
3. The first address must be evenly divisible by the number of addresses.

Example

Figure 2.3 shows a block of addresses, in both binary and dotted-decimal notation, granted to a small business that needs 16 addresses.



We can see that the restrictions are applied to this block: The addresses are contiguous. The number of addresses is a power of 2 ($16 = 2^4$), and the first address is divisible by 16.

The address and the $/n$ notation completely define the whole block (the first address, the last address, and the number of addresses).

First Address The first address in the block can be found by setting the $32 - n$ rightmost bits in the binary notation of the address to 0s.

Example

A block of addresses is granted to a small organization. We know that one of the addresses is **205.16.37.39/28**. **What is the first address in the block?**

Solution

The binary representation of the given address is

11001101 00010000 00100101 00100 111

If we set 32–28 rightmost bits to 0, we get

11001101 00010000 00100101 00100000

or

205.16.37.32/28

Last Address

The last address in the block can be found by setting the $32 - n$ rightmost bits in the binary notation of the address to 1s.

The last address in the block can be found by setting the **rightmost** : $32 - n$ bits to **1s**.

Example

Find the last address for the block.

205.16.37.39/28

Solution

The binary representation of the given address is

11001101 00010000 00100101 00100111

If we set $32 - 28$ rightmost bits to 1, we get

11001101 00010000 00100101 0010**1111**

or

205.16.37.47

Number of Addresses

The number of addresses in the block can be found by using the formula : 2^{32-n}

Example

Find the number of addresses in Example 6.6.

205.16.37.39/28

Solution

The value of n is 28, which means that number of addresses is 2^{32-28} or 16.

205.16.37.32 → 205.16.37.47

Example

Another way to find the **first address**, the **last address**, and the **number of addresses** is to represent the mask as a 32bit binary (or 8-digit hexadecimal) number. This is particularly useful when we are writing a program to find these pieces of information. Ex: The **205.16.37.39/28** , /28 can be represented as **(Mask Definition)**

11111111 11111111 11111111 11110000

(twenty-eight 1s and four 0s).

Find

- a. The first address**
- b. The last address**
- c. The number of addresses.**

Solution

- a. The first address can be found by ANDing the given addresses with the mask. ANDing here is done bit by bit. The result of ANDing 2 bits is 1 if both bits are 1s; the result is 0 otherwise.

Address:	11001101	00010000	00100101	00100111
Mask:	11111111	11111111	11111111	11110000
First address:	11001101	00010000	00100101	00100000

205.16.37.32



- b.** The last address can be found by ORing the given addresses with the complement of the mask. ORing here is done bit by bit. The result of ORing 2 bits is 0 if both bits are 0s; the result is 1 otherwise. The complement of a number is found by changing each 1 to 0 and each 0 to 1.

Address:	11001101	00010000	00100101	00100111
Mask complement:	00000000	00000000	00000000	00001111
Last address:	11001101	00010000	00100101	00101111

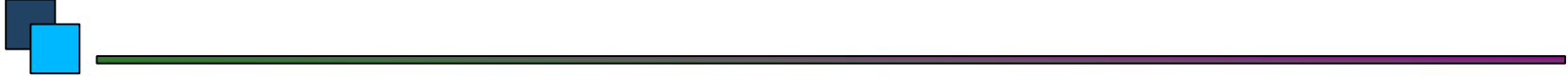
205.16.37.47



- c. The number of addresses can be found by complementing the mask, interpreting it as a decimal number, and adding 1 to it.

Mask complement: 00000000 00000000 00000000 00001111

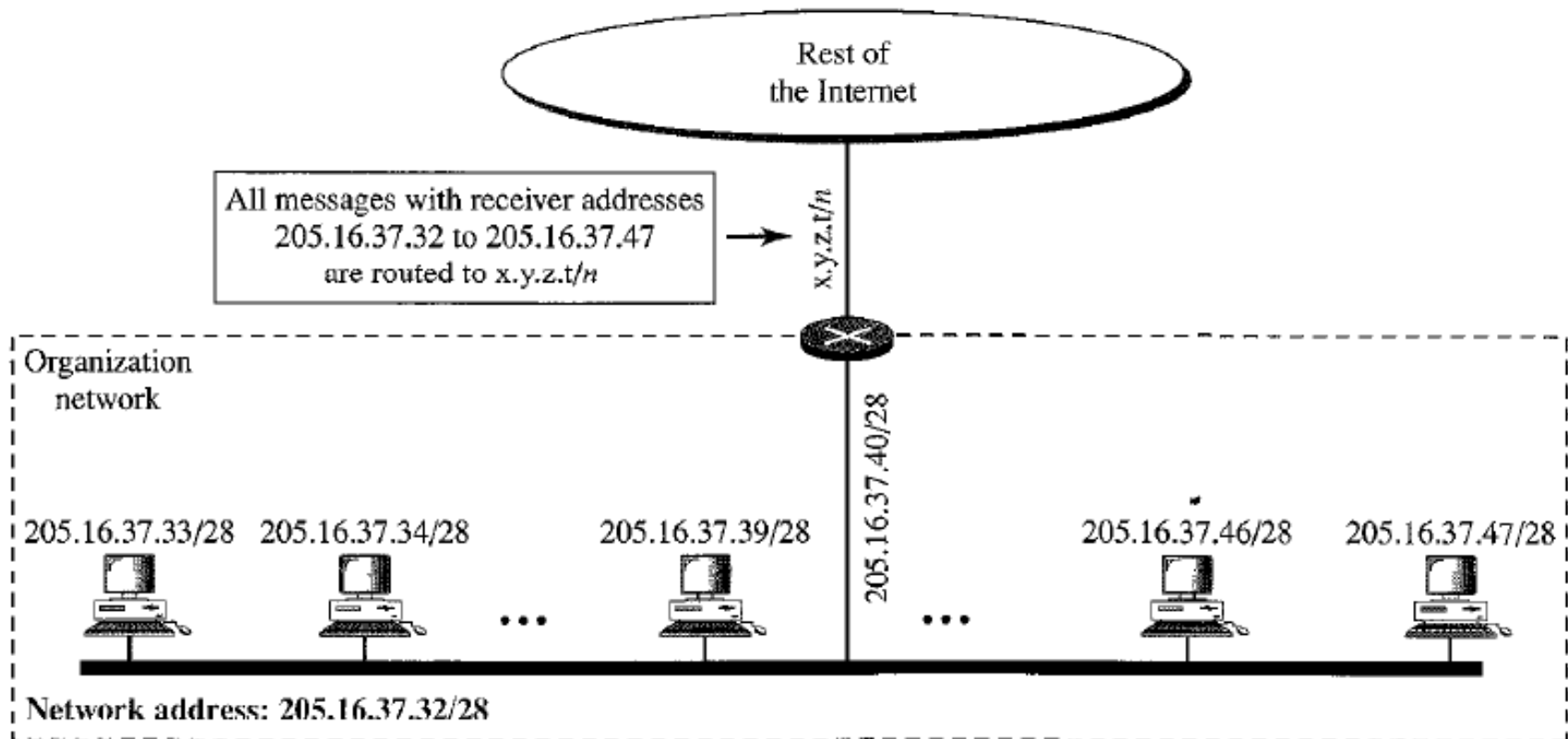
Number of addresses: $15 + 1 = 16$



Chapter 2 Part 2

Network Layer: Logical Addressing- Subnetting

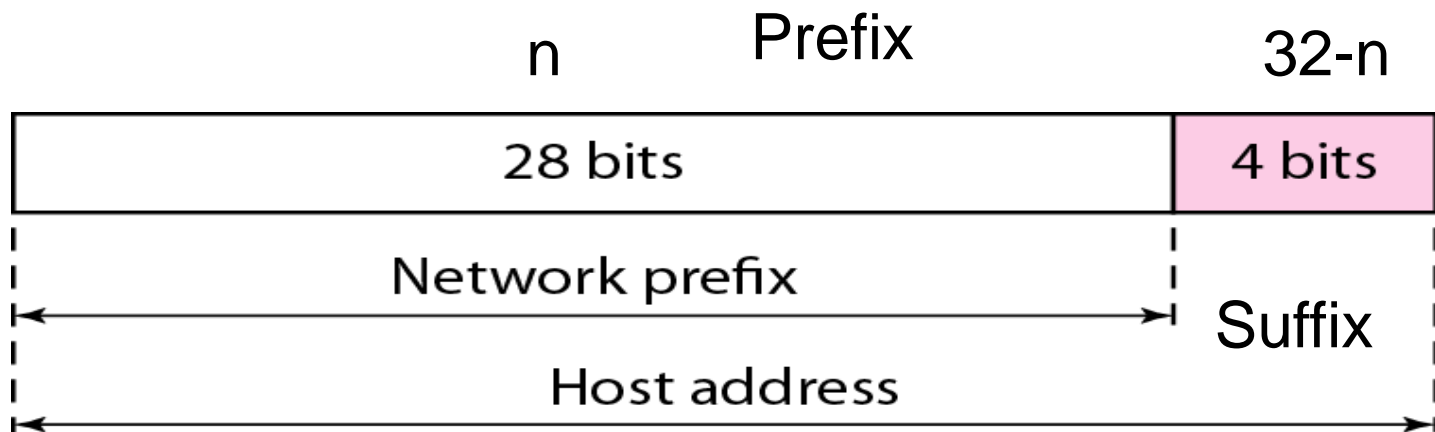
Network Addresses



The first address in a block is normally not assigned to any device; it is used as the network address that represents the organization to the rest of the world.

Two-Level Hierarchy: No Subnetting

An IP address can define only two levels of hierarchy when not subnetted. The n leftmost bits of the address $x.y.z.t/n$ define the network; the $32 - n$ rightmost bits define the particular host to the network. The part of the address that defines the network is called the prefix; the part that defines the host is called the suffix.



Three-Levels of Hierarchy: Subnetting

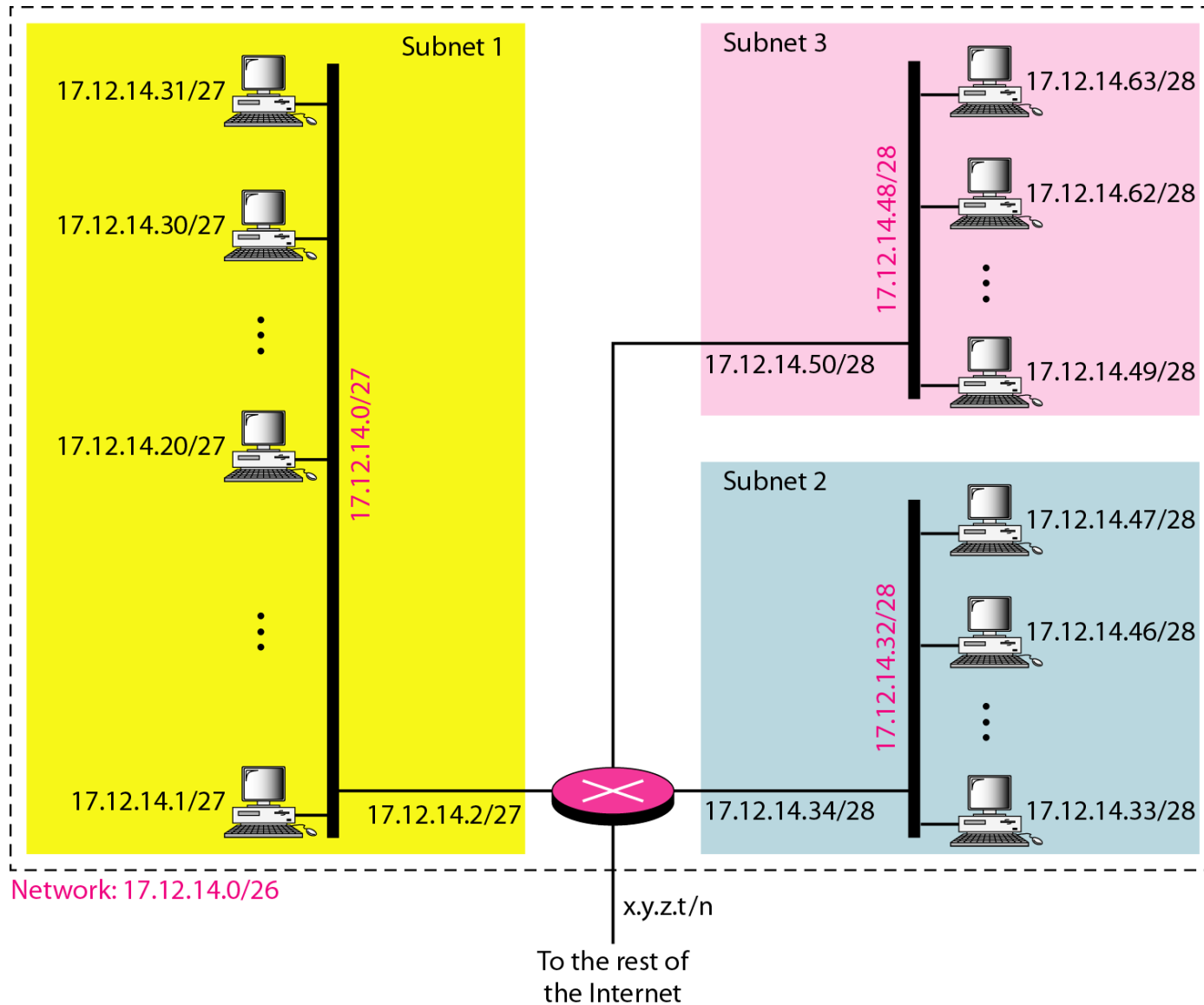
An organization that is granted a large block of addresses may want to create clusters of networks (called subnets) and **divide the addresses between the different subnets**.

The organization, however, needs to create small sub blocks of addresses, each assigned to specific subnets. The organization has its own mask; each subnet must also have its own.

As an example, suppose an organization is given the block 17.12.14.0/26, which contains 64 addresses. The organization has three offices and needs to divide the addresses into three sub blocks of 32, 16, and 16 addresses. We can find the new masks by using the following arguments:

1. Suppose the mask for the first subnet is n_1 , then 2^{32-n_1} must be 32, which means that $n_1 = 27$.
2. Suppose the mask for the second subnet is n_2 , then 2^{32-n_2} must be 16, which means that $n_2 = 28$.
3. Suppose the mask for the third subnet is n_3 , then 2^{32-n_3} must be 16, which means that $n_3 = 28$.

Configuration and addresses in a subnetted network



Let us check to see if we can find the subnet addresses from one of the addresses in the subnet.

a. In subnet 1, the address 17.12.14.29/27 can give us the subnet address if we use the mask /27 because
Host: 00010001. 00001100. 00001110. 00011101
Mask: 11111111 11111111 11111111 11100000 /27 (AND)
Subnet: 00010001 00001100 00001110 00000000
(17.12.14.0)

b. In subnet 2, the address 17.12.14.45/28 can give us the subnet address if we use the mask /28 because
Host: 00010001 00001100 00001110 00101101
Mask: 11111111 11111111 11111111 11110000 /28 (AND)
Subnet: 00010001 00001100 00001110 00100000
(17.12.14.32)

c. **In subnet 3**, the address 17.12.14.50/28 can give us the subnet address if we use the mask /28 because

Host: 00010001 00001100 00001110 00110010
 Mask: 11111111 11111111 11111111 11110000 /28 (AND)
 Subnet: 00010001 00001100 00001110 00110000
 (17.12.14.48)

We can say that through subnetting, we have three levels of hierarchy.

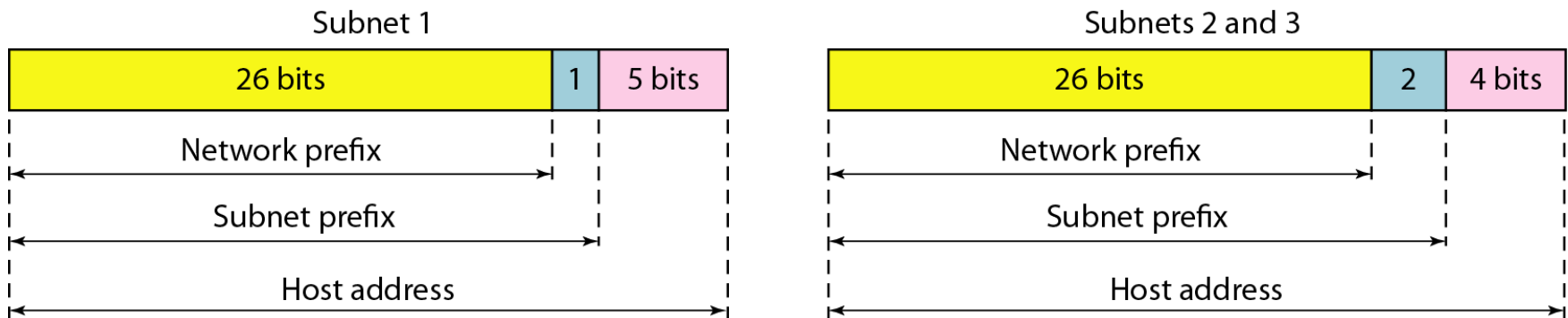
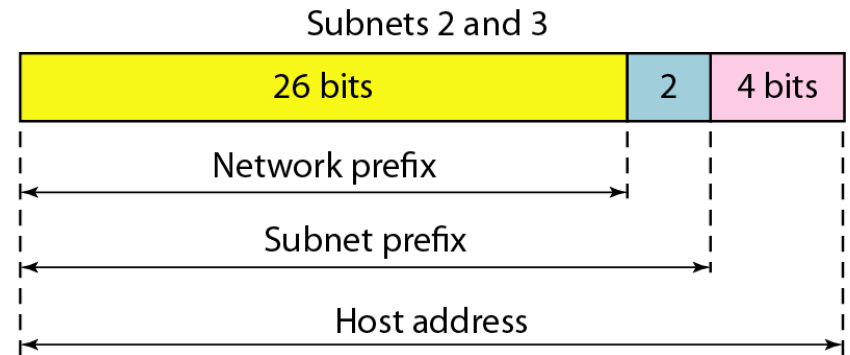
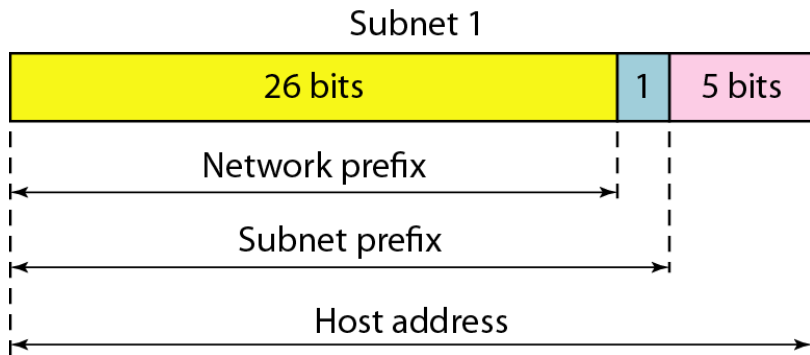


Figure 2.8 *Three-level hierarchy in an IPv4 address*

Q/Analyze three – level of hierarchy as shown below for this network address 17.12.14.0/26 and draw the network diagram?



More Levels of Hierarchy

Large Block → Divide into → Small Blocks → Divide into → Sub Blocks → Customers

National ISP → Regional ISP → Local ISP → Organization → Several Sub nets.

Address Allocation

How are the blocks allocated? The ultimate responsibility of address allocation is given to a global authority called the *Internet Corporation for Assigned Names and Numbers* (ICANN). However, ICANN does not normally allocate addresses to individual organizations. It assigns a large block of addresses to an ISP. Each ISP, in turn, divides its assigned block into smaller sub blocks and grants the sub blocks to its customers.

ICANN → National ISP → Regional ISP → Local ISP → Organization → Several Sub nets.

Example

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 sub blocks and find out how many addresses are still available after these allocations?

Solution

Figure below shows the situation.

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

<i>1st Customer:</i>	<i>190.100.0.0/24</i>	<i>190.100.0.255/24</i>
<i>2nd Customer:</i>	<i>190.100.1.0/24</i>	<i>190.100.1.255/24</i>
<i>...</i>		
<i>64th Customer:</i>	<i>190.100.63.0/24</i>	<i>190.100.63.255/24</i>
<i>Total = $64 \times 256 = 16,384$</i>		

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

<i>1st Customer:</i>	<i>190.100.64.0/25</i>	<i>190.100.64.127/25</i>
<i>2nd Customer:</i>	<i>190.100.64.128/25</i>	<i>190.100.64.255/25</i>
<i>...</i>		
<i>128th Customer:</i>	<i>190.100.127.128/25</i>	<i>190.100.127.255/25</i>
<i>Total = 128 × 128 = 16,384</i>		

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

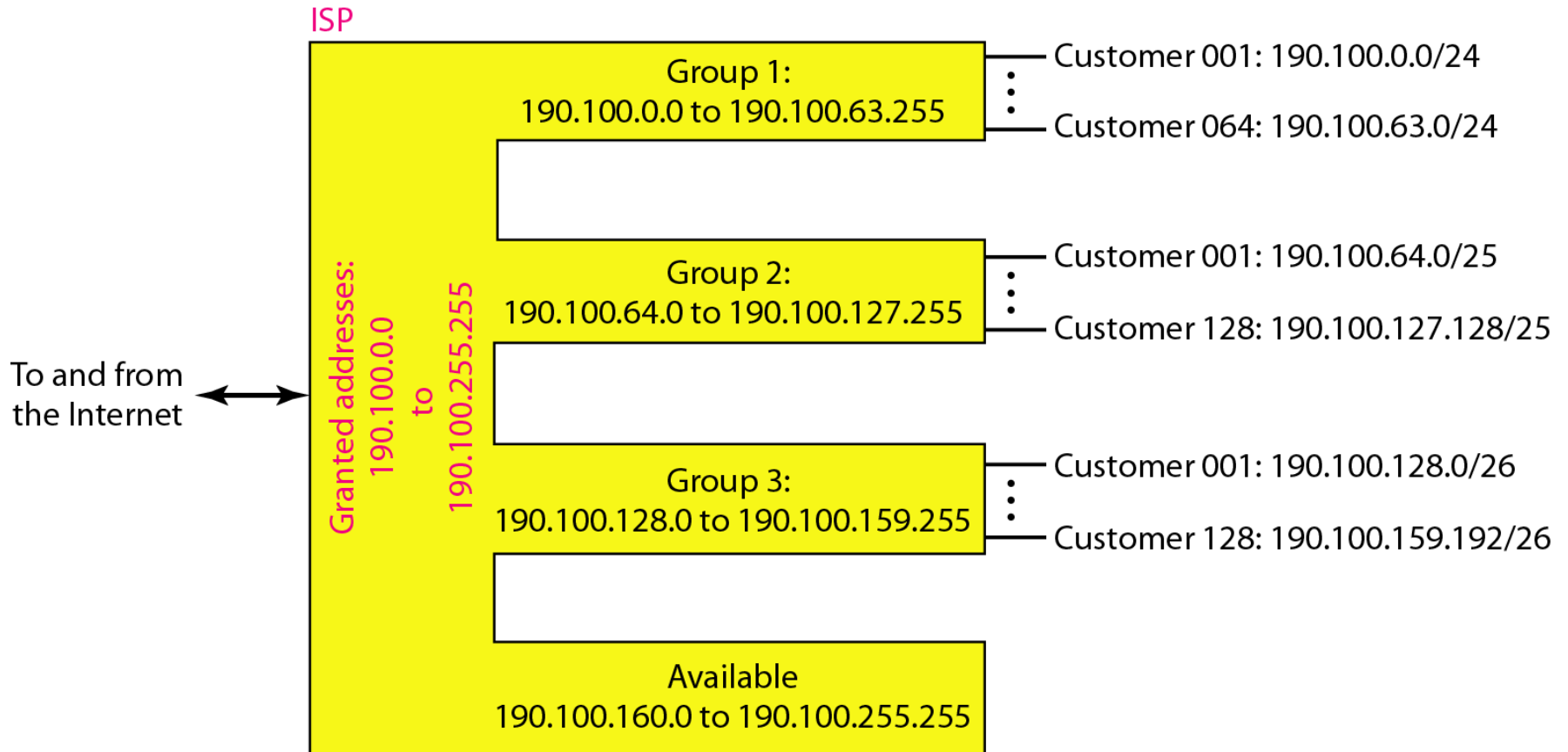
<i>1st Customer:</i>	<i>190.100.128.0/26</i>	<i>190.100.128.63/26</i>
<i>2nd Customer:</i>	<i>190.100.128.64/26</i>	<i>190.100.128.127/26</i>
<i>...</i>		
<i>128th Customer:</i>	<i>190.100.159.192/26</i>	<i>190.100.159.255/26</i>
<i>Total = $128 \times 64 = 8192$</i>		

Number of granted addresses to the ISP: 65,536

Number of allocated addresses by the ISP: 40,960

Number of available addresses: 24,576

An example of address allocation and distribution by an ISP



Network Address Translation (NAT)

A technology that allows a private network to use a set of **private addresses** for internal communication and a set of **global Internet addresses** for external communication.

It provides a **mapping** between **internal IP addresses** and officially assigned **external addresses**.

The Internet authorities have reserved three sets of addresses as private addresses, shown below:

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