Computer networks

- Level: Fourth Year
- Lecturer: Asst. Prof. Dr. Awos Kh. Ali
- Lab Software: Cisco Packet tracer
- Lab assistant: L. Huda Basim Hamid

شبكات

Introduction to Computer Networking

Computer networks
Asst. Prof. Dr. Awos Kh. Ali
Lab assistant: L. Huda Basim Hamid

(Class 1)

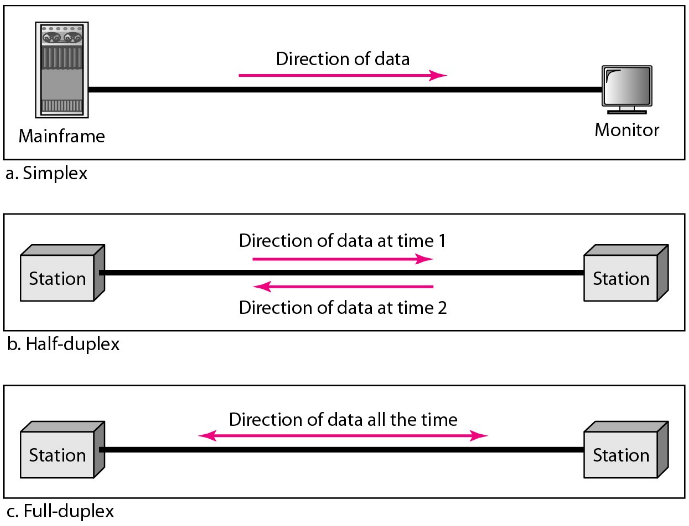
What is Computer Network?

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, 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)


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

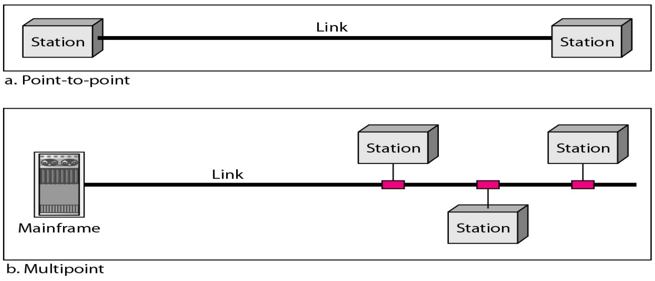
a. Simplex

b. Half-duplex

c. Full-duplex

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

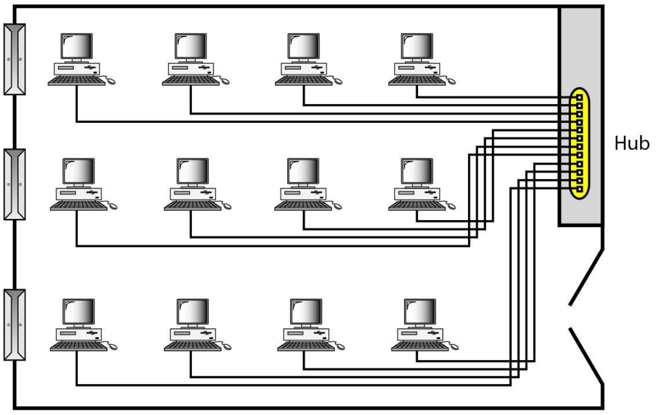
:

:

LAN and WAN

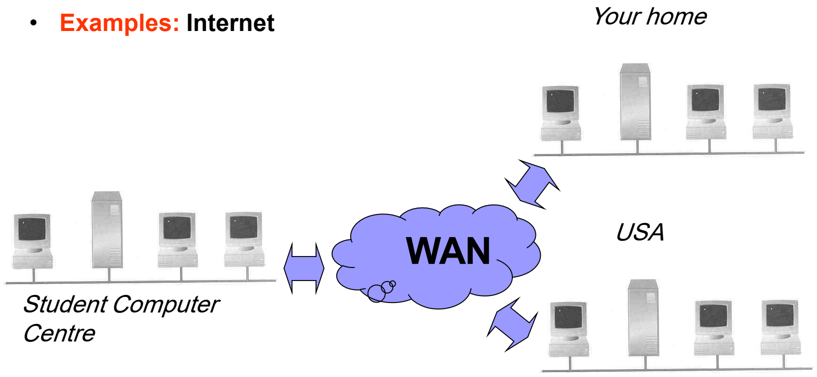
- **Local Area Network (LAN)**
  - **Small network, short distance**
    - **A room, a floor, a building**
    - **Limited by number of computers and distance covered**
    - **Serve a department within an organization**
  - **Examples:**
    - **Network inside the Student Computer Room**
    - **Network inside your home**

Figure . *An isolated LAN connecting 12 computers to a hub in a closet*

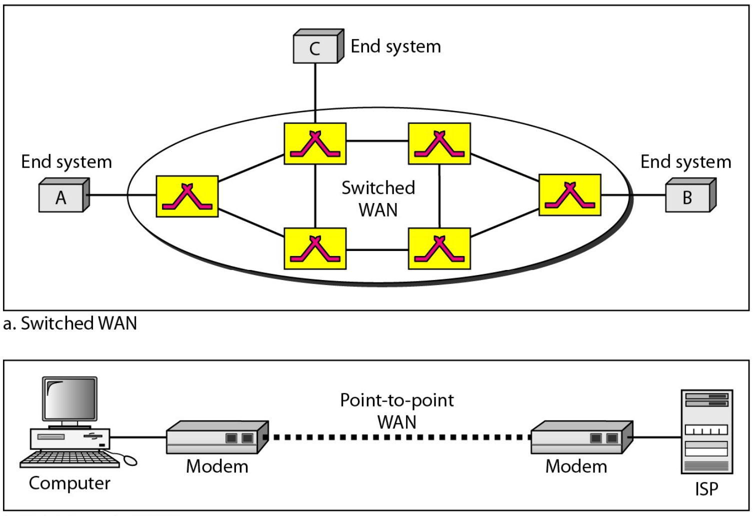


• Wide Area Network (WAN)

- 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

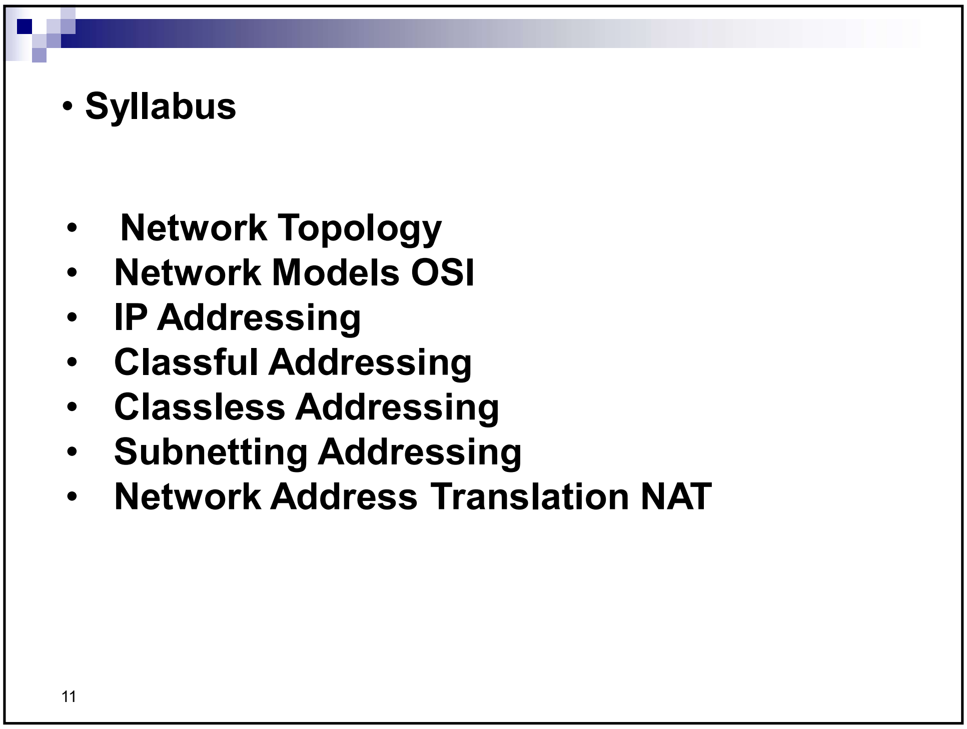


WANs: a switched WAN and a point-to-point WAN



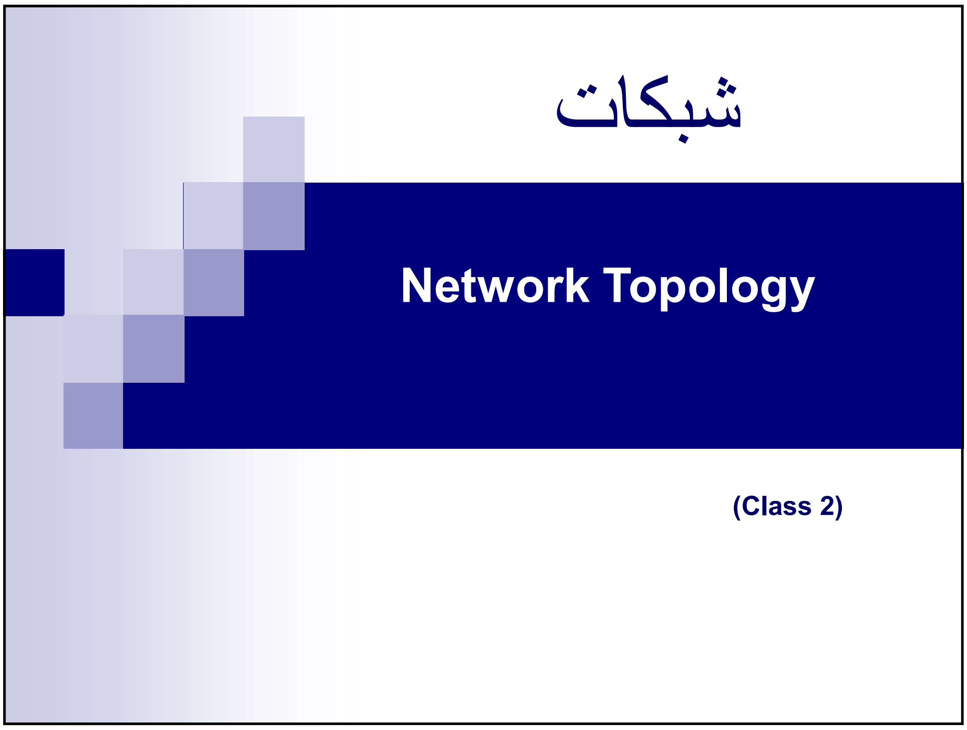
a. Switched WAN

b. Point-to-point WAN



- Syllabus

- Network Topology
- Network Models OSI
- IP Addressing
- Classful Addressing
- Classless Addressing
- Subnetting Addressing
- Network Address Translation NAT



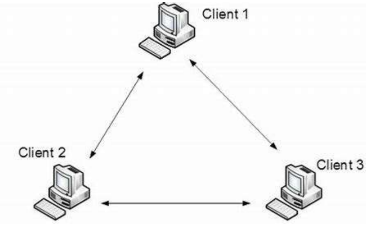
شبكات

Network Topology

(Class 2)

Peer-to-Peer Networks

- No hierarchy among computers ⇒ all are equal.
- لا يوجد تدرج بين الاجهزة – الكل متساوية
- No administrator responsible for the network.
- لا يوجد جهة معينة تدير الشبكة – الكل يساهم في الادارة
- Host in a P2P network Provide and Consume Services. اي عنصر داخل الشبكة ممكن ان ينتج ويستهلك خدمات



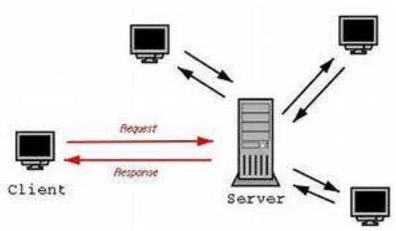
Peer-to-peer

- Advantages of peer-to-peer networks:
  - Low cost كلفة قليلة
  - Simple to configure سهولة في التشكيل
  - User has full accessibility of the computer ممكن للمستخدمين الوصول الكامل للكومبيوتر
- Disadvantages of peer-to-peer networks:
  - Difficult to uphold security policy عدم توفر الامنية الكاملة
  - Difficult to handle uneven loading عدم السيطرة على البيانات الكبيرة
  - Not Scalable: غير قابل للتوسيع
  - Difficult to control, صعوبة في الادارة. لان كل مستخدم هو بحد ذاتة مدير because every user is a network administrator.
- Where peer-to-peer network is appropriate:
  - 10 or less users عندما يكون العدد اقل من 10 مستخدمين
  - Security is not an issue عندما تكون الامنية غير مهمة

Clients and Servers

- Network Clients (Workstation)
  - Computers that request network resources or services
  - الاجهزة التي تطلب خدمات او موارد
- Network Servers
  - Computers that manage and provide network resources and services to clients الاجهزة التي تزود الخدمات و الموارد للمستخدمين
    - Usually have more processing power, memory and hard disk space than clientsعادتا تملك معالجات قوية وذاكرة عالية و سعة خزن كبيرة
    - Run Network Operating System that can manage not only data, but also users, groups, security, and applications on the network (Linux or Windows server) تعمل على انظمة تشغيل عالية الجودة و مختلفة عن الاجهزة العادية لتكون قادرة على توفير الامنية و ادارة المستخدمين و المجاميع

- Advantages of client/server networks
  - Facilitate resource sharing – سهولة في مشاركة المصادر
  - Facilitate system backupسهولة في تامين نسخ احتياطي للنظام
  - Enhance security – only administrator can have access to Server
  - امنية عالية – بسبب وجود مدير واحد مخول للتحكم بالشبكة
  - Support more users – difficult to achieve with peer-to-peer networks دعم عدد كبير من المستخدمين
- Disadvantages of client/server networks
  - High cost for Servers كلفة عالية
  - Need expert to configure the network تحتاج خبراء للعمل والصيانه على تلك الشبكات

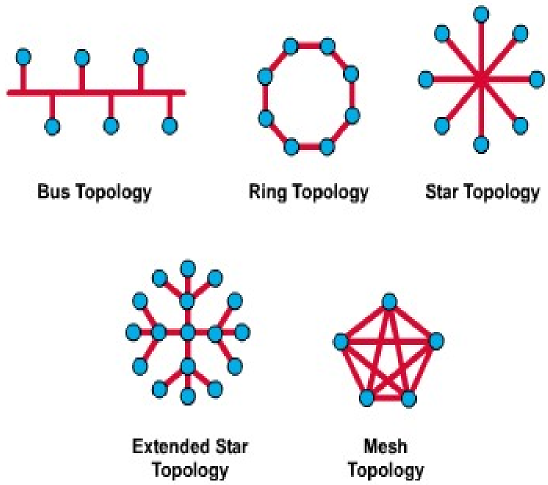


1

Specialized Servers

- **Type of specialized servers**
  - Application Servers (Facebook)
  - Communication Servers
  - Fax Servers
  - Mail Servers
  - Web Servers
  - File & Print Servers

Network Topology



Peer-to-Peer (P2P) vs. Client-Server Networks

1.**Architecture**:
   1. **P2P**: Decentralized; all devices (peers) act as both clients and servers, sharing resources directly.
   2. **Client-Server**: Centralized; dedicated servers manage resources, and clients request services from these servers.

2.**Resource Management**:
   1. **P2P**: Resources (files, processing power) are distributed across peers.
   2. **Client-Server**: Resources are stored and managed centrally on the server.

3.**Scalability**:
   1. **P2P**: Limited scalability for large networks due to direct peer dependencies.
   2. **Client-Server**: Highly scalable, as servers can handle increased client demands.

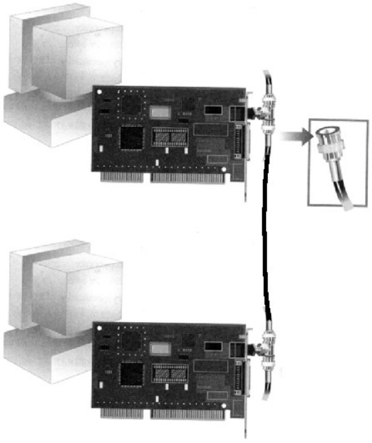
5. **Security**:
   1. **P2P**: Less secure (peer-dependent, no centralized control).
   2. **Client-Server**: More secure (centralized authentication, access controls).

6.**Cost**:
   1. **P2P**: Lower cost (no dedicated server infrastructure).
   2. **Client-Server**: Higher cost (server setup, maintenance).

7.**Reliability**:
   1. **P2P**: Resilient (no single point of failure).
   2. **Client-Server**: Server failure disrupts the entire network.

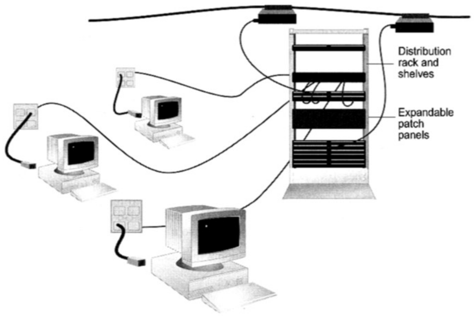
8.**Use Cases**:
   1. **P2P**: File sharing (e.g., BitTorrent), small networks.
   2. **Client-Server**: Enterprise systems, web services (e.g., email, databases).

- **Bus Topology**
  - **Simple and low-cost بسيط و ذو كلفة قليلة**
  - **A single cable called a trunk تحتوي على كيبل واحد يدعى**
  - **Only one computer can send messages at a time فقط جهاز واحد ممكن ان يرسل في المرة الواحدة**



21

- **Star Topology**
  - **Each computer has a cable connected to a single point كل جهاز في الشبكة متصل بنقطة المركز**
  - **More cabling, hence higher cost يحتاج الى توصيلات كثيرة اذن كلفة عالية**
  - **All signals transmission through the hub; if down, entire network down كل البيانات تمر عبر نقطة المركز – اي فشل في تلك النقطة سوف يؤدي الى فشل الشبكة كاملا**



22

Ring Topology

- A **ring topology** is a type of network topology in which each device (or node) is connected to exactly two other devices, forming a closed loop or "ring" structure. The data travels in one or both directions around the ring, passing through each node until it reaches its destination. This topology is used in various local area networks (LANs) and wide area networks (WANs).

Key Characteristics of Ring Topology:

- **Circular Layout**: Each node in the network is connected to exactly two other nodes, creating a closed loop. The last node connects back to the first node, forming a ring.
- **Data Transmission**: Data is sent in a specific direction, either clockwise or counterclockwise, around the ring. In a bidirectional ring (known as a "dual ring"), data can travel in both directions, which provides redundancy(التكرار في ارسال البيانات) in case of a failure.
- **Token Passing**: A common protocol used in ring topology is **token passing**. A "token" is a special data packet that circulates around the network. Only the node holding the token can send data, reducing the chances of data collisions. Once the data is transmitted, the token is passed to the next node.

Ring Topology

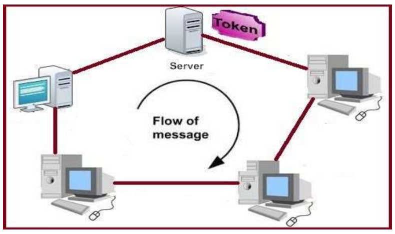
Reliability and Fault Tolerance:

Unidirectional Ring: If a link or node in the ring fails, the entire network can be disrupted because there is no alternate path for the data to travel.

Bidirectional Ring: In a dual-ring topology, if a failure occurs, the network can continue operating because data can flow in the opposite direction.

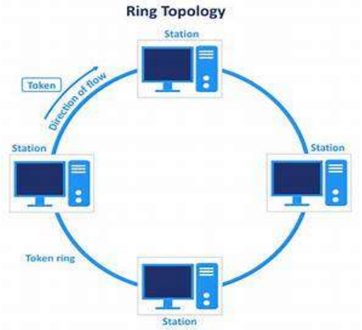
Advantages of Ring Topology:

- **Equal Access**: All nodes have equal opportunity to send data because of the token-passing mechanism.
- **Predictable Performance**: Data collisions are minimized since only one node can transmit at a time.
- **Simpler Cabling**: Only two connections per device are needed (one to each adjacent node).



Disadvantages of Ring Topology:

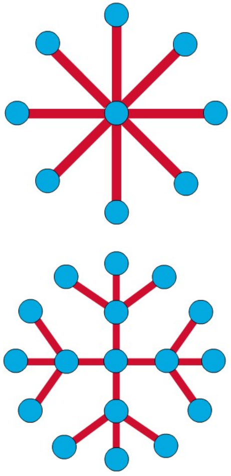
Single Point of Failure (for Unidirectional Rings): A break in the ring can disable the entire network unless it's a dual ring topology.
Latency Increases with Distance: Since data must pass through each node to reach its destination, the time it takes for data to travel increases as more nodes are added.
Complex Troubleshooting: Identifying the point of failure can be more complex compared to other topologies like star.



Star & Tree Topology

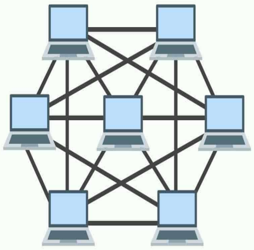
- **The star topology is the most commonly used architecture in Ethernet LANs.** بنية النجمة هو الاكثر استخداما في الوقت الحالي في الشبكات المحلية

- **Larger networks use the extended star topology also called 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.** الشبكات الكبيرة تسمة بالشجرة وهي عبارة عن مجموعة من شبكات النجمة متصلة مع بعضها عن طريق اجهزة اخرة



Mesh Topology

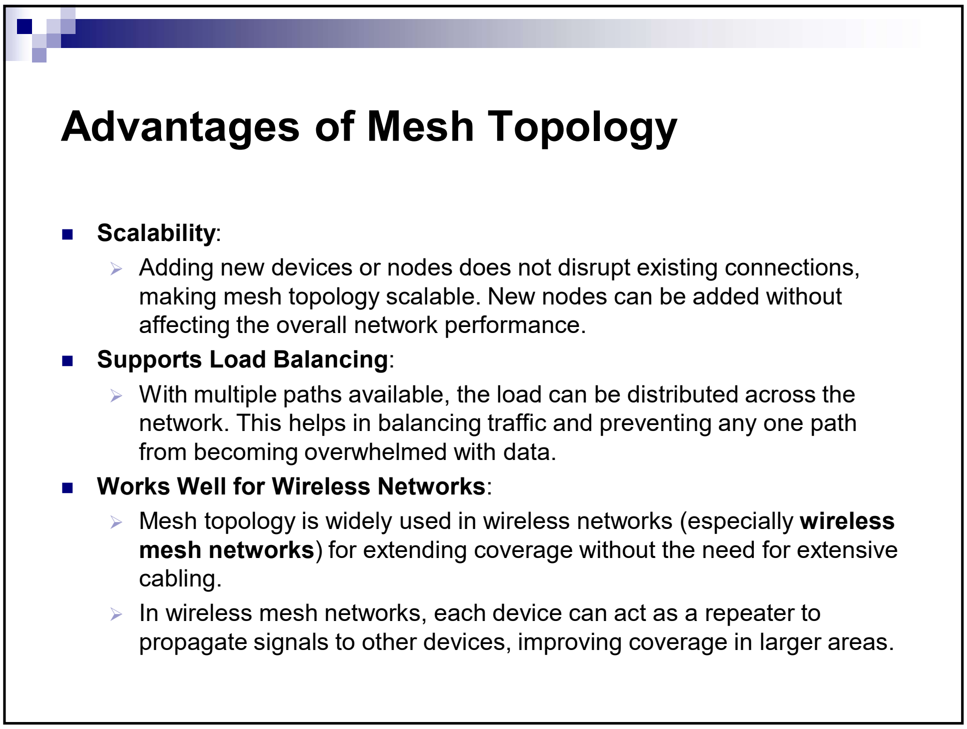
- Mesh topology is a type of network configuration where each node (or device) is connected to every other node in the network. This setup ensures that there are multiple pathways for data to travel between nodes, which increases the reliability and redundancy of the network. Mesh topology can be classified into two types:
  - **Full Mesh**: Every node is directly connected to every other node, providing the highest level of redundancy but requiring a large number of connections as the network grows.
  - **Partial Mesh**: Only some nodes are connected to multiple others, reducing the number of connections but still offering improved redundancy compared to other topologies like star or bus.



Full Mesh Topology

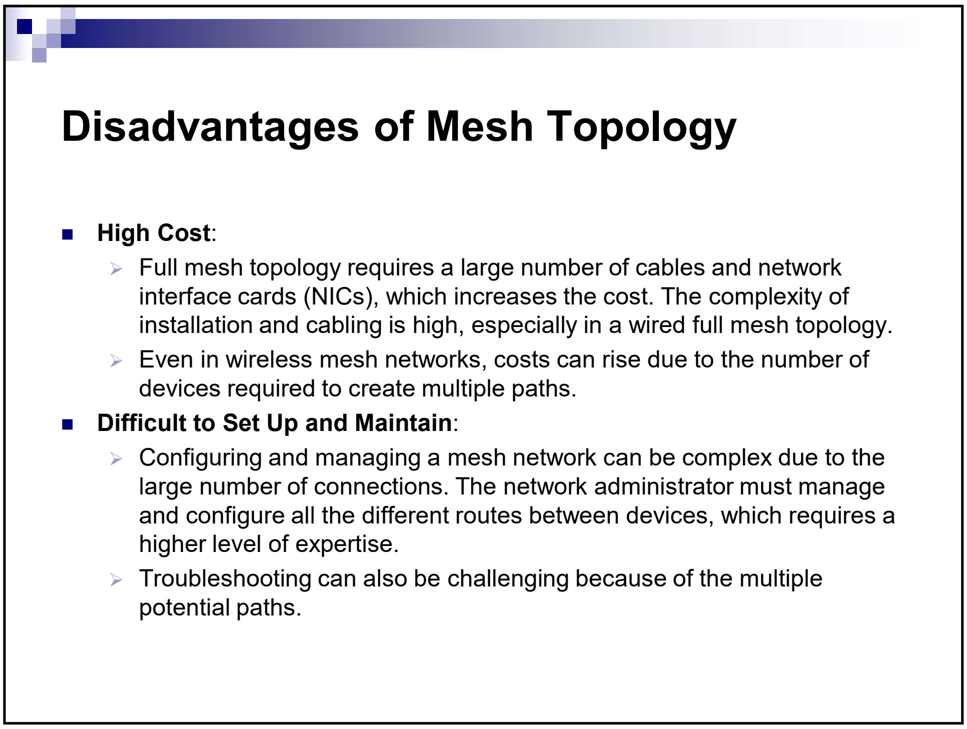
Advantages of Mesh Topology

- **High Fault Tolerance:**
  - In a full mesh topology, every device is connected to every other device. This means that if one connection or node fails, the data can still find alternate paths to reach its destination.
  - Even in a partial mesh, multiple redundant paths exist, improving reliability.
- **Data is Reliable and Secure**:
  - Mesh topology can provide more secure communication, as data travels through multiple routes, and it's harder for attackers to intercept.
  - Data packets can be sent through different paths simultaneously, enhancing data reliability.
- **No Traffic Congestion**:
  - Since multiple routes are available for data transmission, network congestion is minimized. Each node has a dedicated connection to other nodes, so bottlenecks are less likely.



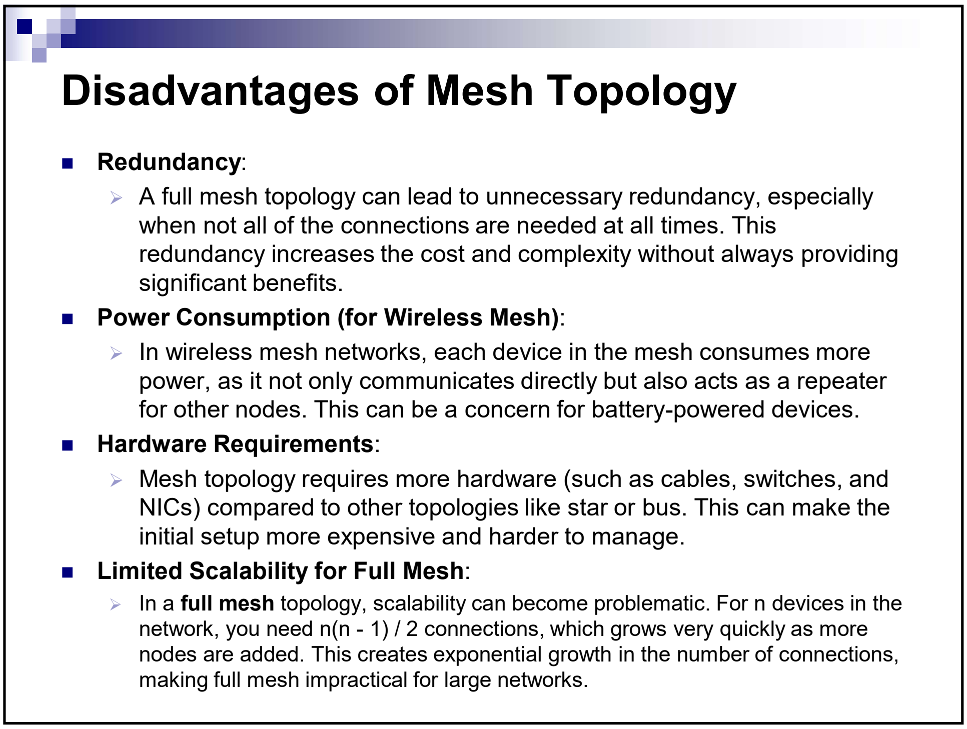
Advantages of Mesh Topology

- **Scalability**:
  - Adding new devices or nodes does not disrupt existing connections, making mesh topology scalable. New nodes can be added without affecting the overall network performance.
- **Supports Load Balancing**:
  - With multiple paths available, the load can be distributed across the network. This helps in balancing traffic and preventing any one path from becoming overwhelmed with data.
- **Works Well for Wireless Networks**:
  - Mesh topology is widely used in wireless networks (especially **wireless mesh networks**) for extending coverage without the need for extensive cabling.
  - In wireless mesh networks, each device can act as a repeater to propagate signals to other devices, improving coverage in larger areas.



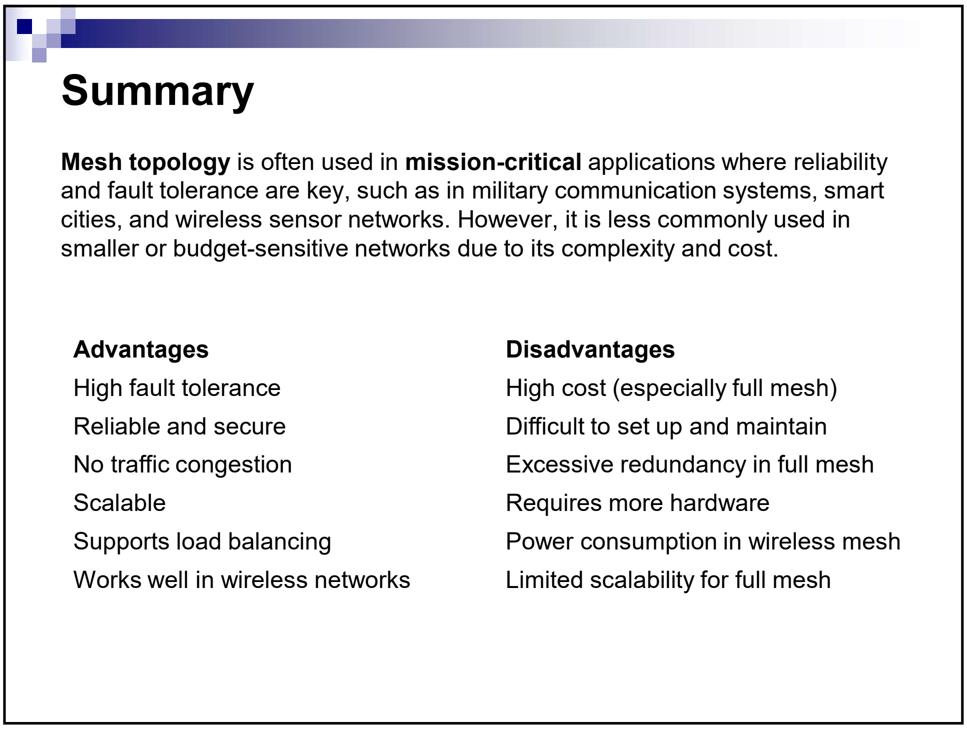
Disadvantages of Mesh Topology

- **High Cost**:
  - Full mesh topology requires a large number of cables and network interface cards (NICs), which increases the cost. The complexity of installation and cabling is high, especially in a wired full mesh topology.
  - Even in wireless mesh networks, costs can rise due to the number of devices required to create multiple paths.
- **Difficult to Set Up and Maintain**:
  - Configuring and managing a mesh network can be complex due to the large number of connections. The network administrator must manage and configure all the different routes between devices, which requires a higher level of expertise.
  - Troubleshooting can also be challenging because of the multiple potential paths.



Disadvantages of Mesh Topology

- **Redundancy**:
  - A full mesh topology can lead to unnecessary redundancy, especially when not all of the connections are needed at all times. This redundancy increases the cost and complexity without always providing significant benefits.
- **Power Consumption (for Wireless Mesh)**:
  - In wireless mesh networks, each device in the mesh consumes more power, as it not only communicates directly but also acts as a repeater for other nodes. This can be a concern for battery-powered devices.
- **Hardware Requirements**:
  - Mesh topology requires more hardware (such as cables, switches, and NICs) compared to other topologies like star or bus. This can make the initial setup more expensive and harder to manage.
- **Limited Scalability for Full Mesh**:
  - In a **full mesh** topology, scalability can become problematic. For n devices in the network, you need n(n - 1) / 2 connections, which grows very quickly as more nodes are added. This creates exponential growth in the number of connections, making full mesh impractical for large networks.



Summary

Mesh topology is often used in **mission-critical** applications where reliability and fault tolerance are key, such as in military communication systems, smart cities, and wireless sensor networks. However, it is less commonly used in smaller or budget-sensitive networks due to its complexity and cost.

Advantages	**Disadvantages**
High fault tolerance	High cost (especially full mesh)
Reliable and secure	Difficult to set up and maintain
No traffic congestion	Excessive redundancy in full mesh
Scalable	Requires more hardware
Supports load balancing	Power consumption in wireless mesh
Works well in wireless networks	Limited scalability for full mesh

شبكات

Network Models OSI

(Class 3)

THE OSI MODEL

The OSI (Open Systems Interconnection) model is a conceptual framework used to understand and implement computer networking by dividing it into 7 layers. Each layer has a specific function in the process of data communication:. It was first introduced in the late 1970s.

Seven layers of the OSI model

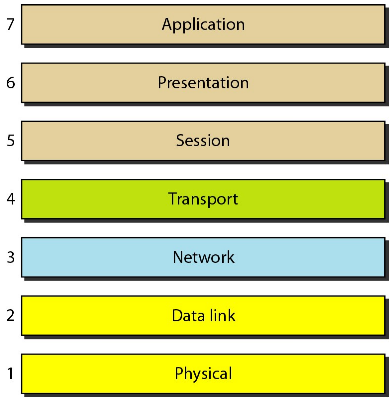
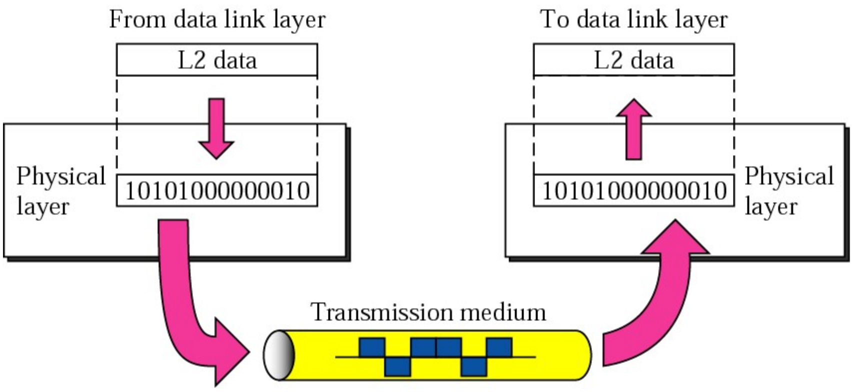


Figure 2-4

Physical Layer



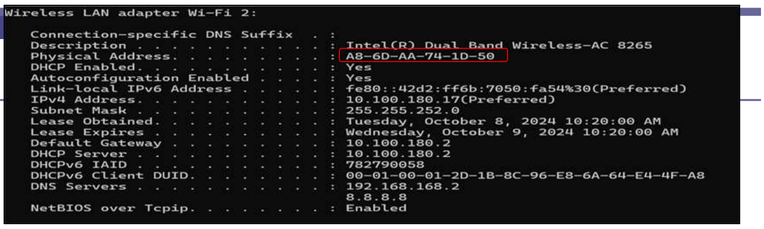
Physical Layer (Layer 1): This is the lowest layer, responsible for the transmission of raw bitstreams over a physical medium, like cables, radio waves, or optical fibers. It deals with the physical connection between devices and the electrical, mechanical, and procedural characteristics required for communication.

An exchange using the OSI model

Network	
Data Link	**LLC Sublayer**
	MAC Sublayer
Physical	

Data Link Layer (Layer 2): The Data Link Layer in the OSI model is divided into two sublayers: **MAC (Media Access Control)** and **LLC (Logical Link Control)**. Each sub-layer has specific roles that contribute to data transmission over a network. Here's how they work:.

Command prompt-> ipconfig/all



```
Wireless LAN adapter Wi-Fi 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Dual Band Wireless-AC 8265
   Physical Address. . . . . . . . . : A8-6D-AA-74-1D-50
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::42d2:ff6b:7050:fa54%30(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.100.180.17(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.252.0
   Lease Obtained. . . . . . . . . . : Tuesday, October 8, 2024 10:20:00 AM
   Lease Expires . . . . . . . . . . : Wednesday, October 9, 2024 10:20:00 AM
   Default Gateway . . . . . . . . . : 10.100.180.2
   DHCP Server . . . . . . . . . . . : 10.100.180.2
   DHCPv6 IAID . . . . . . . . . . . : 782790058
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-1B-8C-96-E8-6A-64-E4-4F-A8
   DNS Servers . . . . . . . . . . . : 192.168.168.2
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

A. MAC (Media Access Control) Sublayer

Function: The MAC sublayer is responsible for controlling how devices on a network access and transmit data over the physical medium. It ensures that data frames are placed onto the transmission media in an orderly way, avoiding collisions when multiple devices try to communicate at the same time.

Key Tasks:

- **Addressing:** MAC uses unique hardware addresses (MAC addresses) to identify devices on a local network. Each network interface card (NIC) has a unique MAC address used for communication.
- **Access Control:** It determines when a device is allowed to send data and when to wait, using protocols like CSMA/CD (Carrier Sense Multiple Access with Collision Detection) in wired Ethernet or CSMA/CA (Collision Avoidance) in wireless networks.
- **Frame Handling:** The MAC sublayer takes data from the LLC sublayer, encapsulates it into data frames, and sends it to the Physical Layer for transmission.

- **Ensuring Hop-by-Hop Data Delivery:** MAC handles hop-by-hop delivery by controlling how data frames are transmitted between directly connected devices on the same network segment, using MAC addresses to ensure that each frame reaches its next immediate destination. It ensures orderly communication and collision avoidance, guiding data from one network node to another within the local network before passing it up to higher layers for further processing.

B. LLC (Logical Link Control) Sublayer

Function: The LLC sublayer acts as an interface between the network layer above it and the MAC sublayer below it. It manages data flow and error-checking functions to ensure reliable data communication.

Key Tasks:

Error Detection and Correction: LLC provides error-checking mechanisms to detect any data transmission errors and take corrective actions. While it doesn't correct the errors directly, it detects them so the data can be retransmitted.

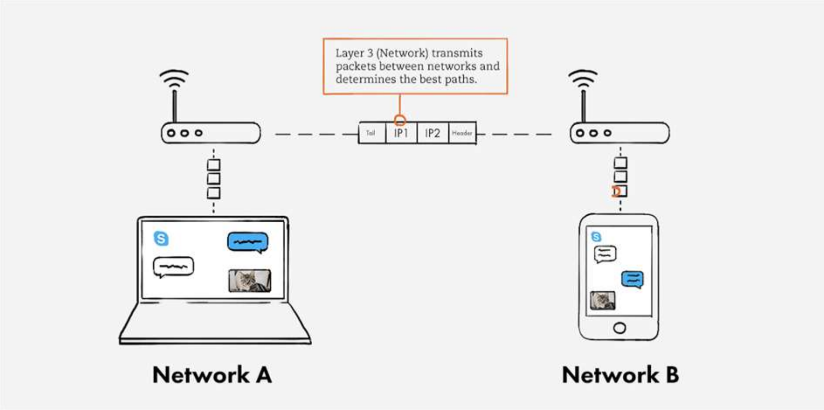
Flow Control: The LLC sublayer manages the rate of data transmission to prevent a fast sender from overwhelming a slow receiver, ensuring a smooth communication process.

Multiplexing: It supports the handling of multiple network protocols over the same network medium, allowing higher-layer protocols to communicate through different logical paths.

Together, these two sublayers allow reliable and orderly communication between devices in a network, with the LLC focusing on error handling and flow control, while the MAC controls how data is actually transmitted onto the physical medium.

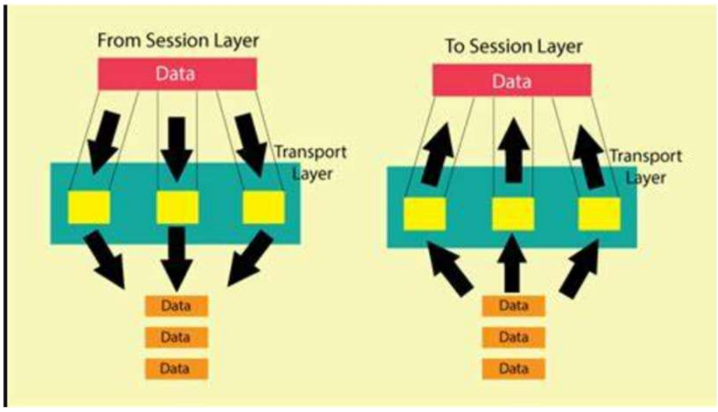
Network layer:

Network Layer (Layer 3): This layer is responsible for data routing, switching, and determining the best path for data transmission. It uses logical addressing (IP addresses) to direct data packets from the ***source*** to ***destination*** across multiple networks.

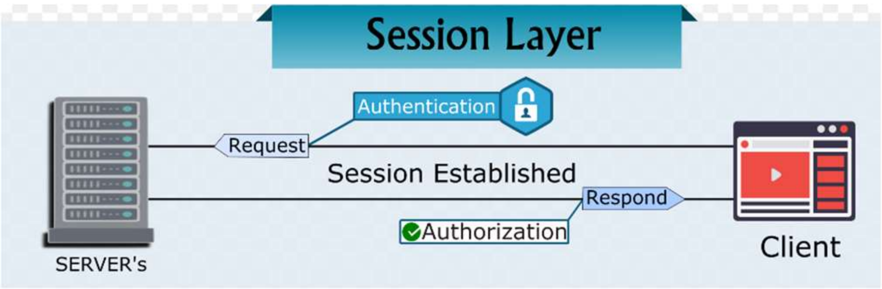


Layer 3 (Network) transmits packets between networks and determines the best paths.

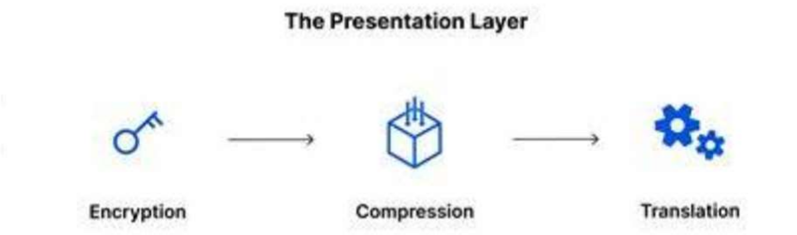
Transport Layer (Layer 4): The transport layer ensures the reliable transmission of data between devices. It manages end-to-end communication, error correction, and data flow control, using protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).



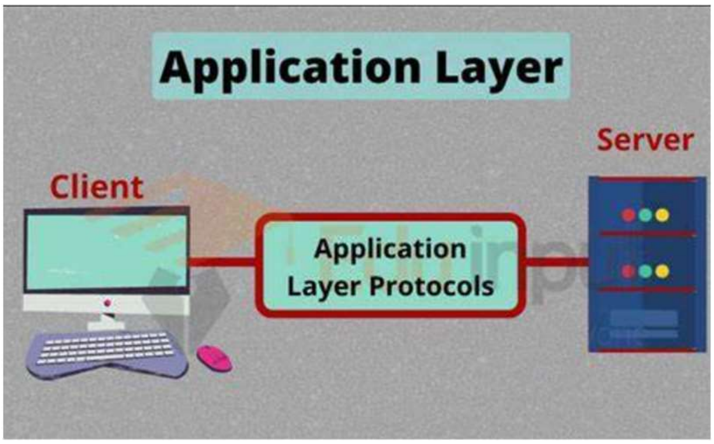
Session Layer (Layer 5): This layer establishes, manages, and terminates communication sessions between two devices. It coordinates the dialogue between the systems and keeps the data separate from other sessions.



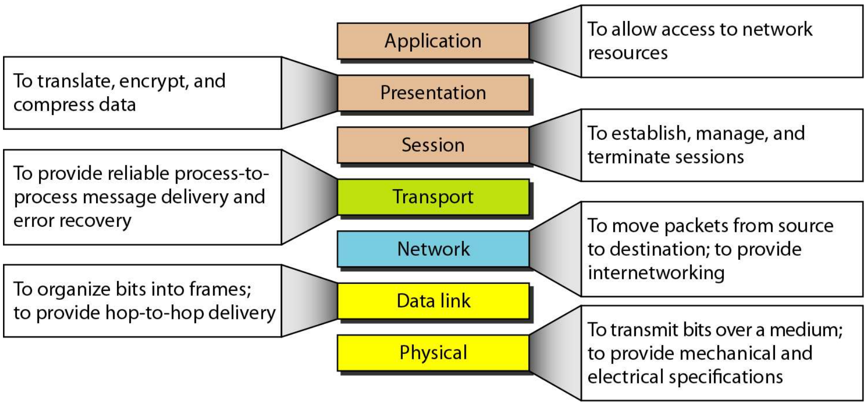
Presentation Layer (Layer 6): The presentation layer translates data into a format that the application layer can understand. It handles data encryption, decryption, compression, and conversion to ensure that data is presented in a readable form.



Application Layer (Layer 7): The topmost layer interacts directly with the user and provides network services to applications. It includes protocols like HTTP, FTP, SMTP, and DNS, facilitating user access to network resources and data exchange.



Summary of layers



To allow access to network resources

To translate, encrypt, and compress data

To establish, manage, and terminate sessions

To provide reliable process-to-process message delivery and error recovery

To move packets from source to destination; to provide internetworking

To organize bits into frames; to provide hop-to-hop delivery

To transmit bits over a medium; to provide mechanical and electrical specifications

Summary of layers

To allow access to network resources

To translate, encrypt, and compress data

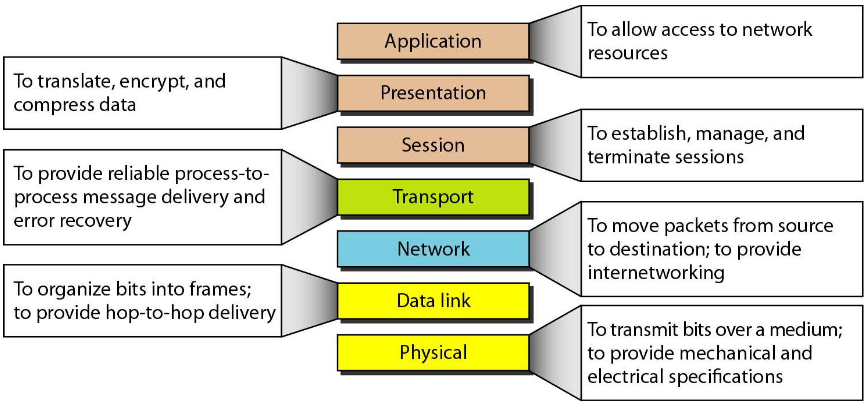
To establish, manage, and terminate sessions

To provide reliable process-to-process message delivery and error recovery

To move packets from source to destination; to provide internetworking

To organize bits into frames; to provide hop-to-hop delivery

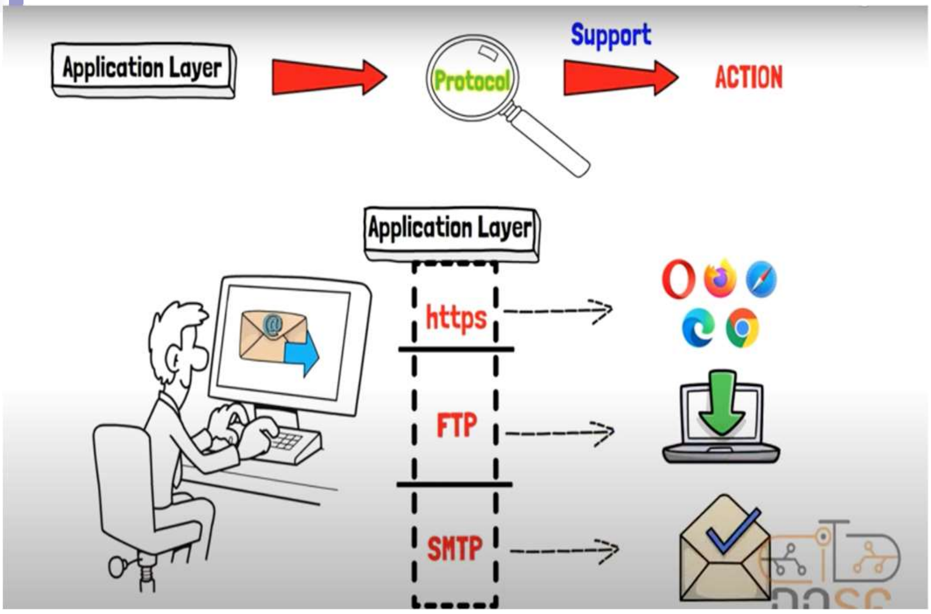
To transmit bits over a medium; to provide mechanical and electrical specifications

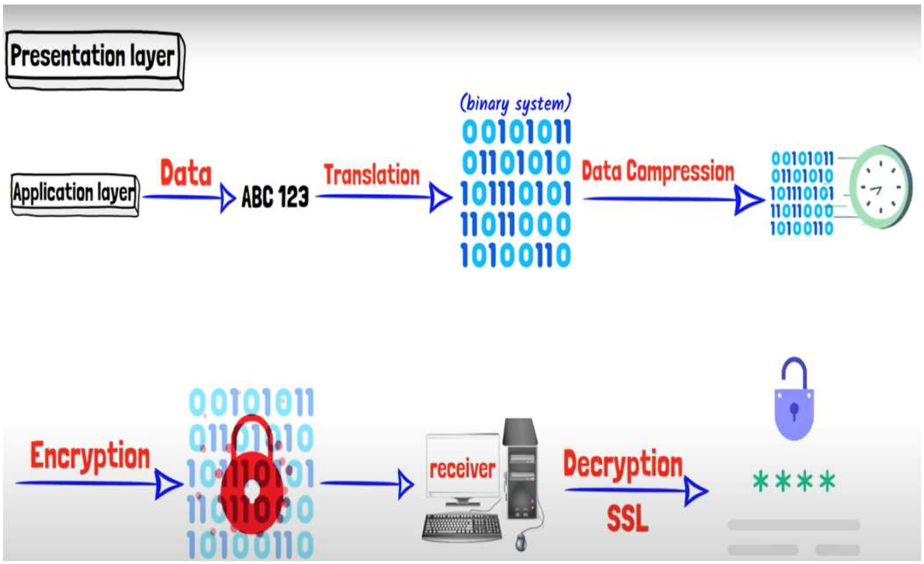


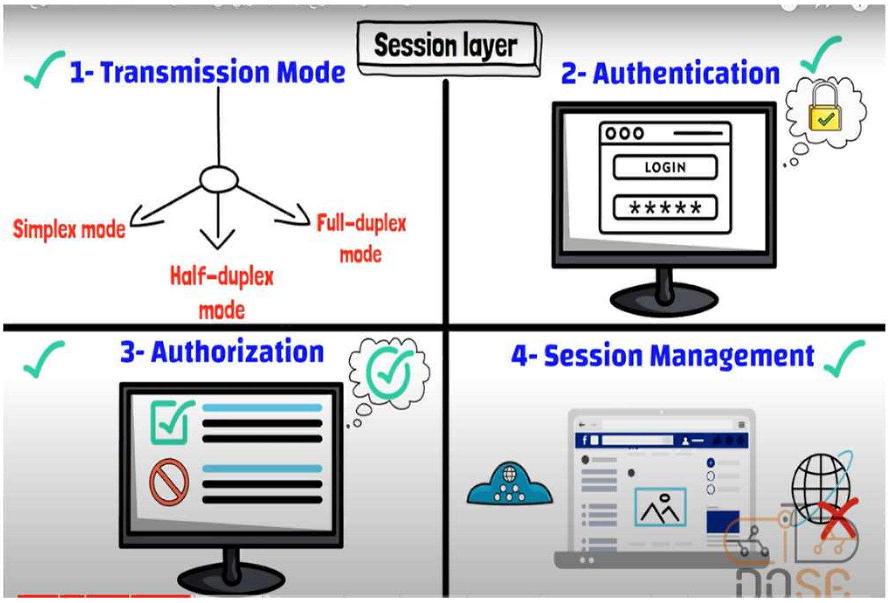
Application, Presentation and Session layers are software layers

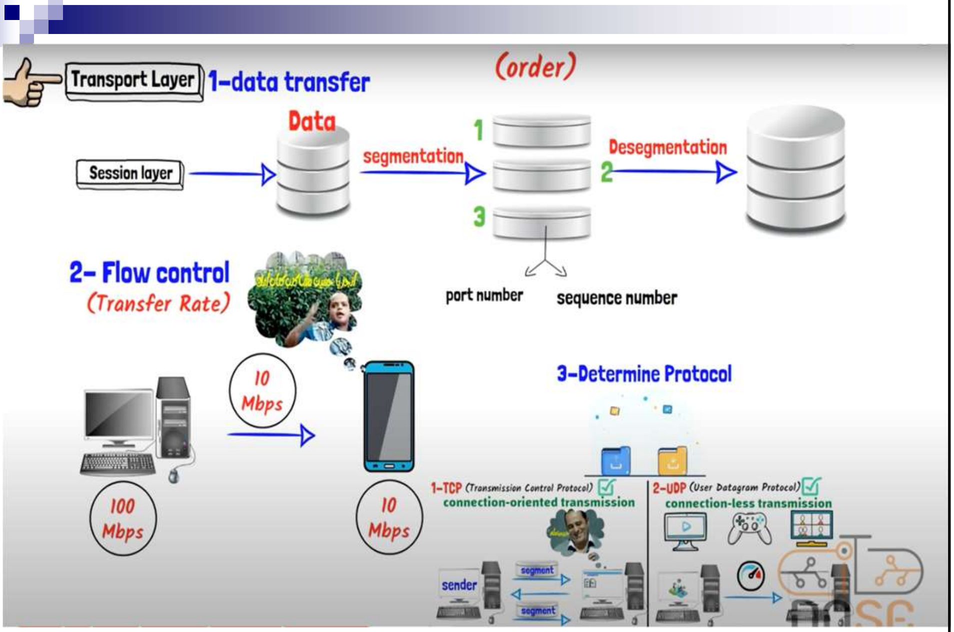
Application layer protocol

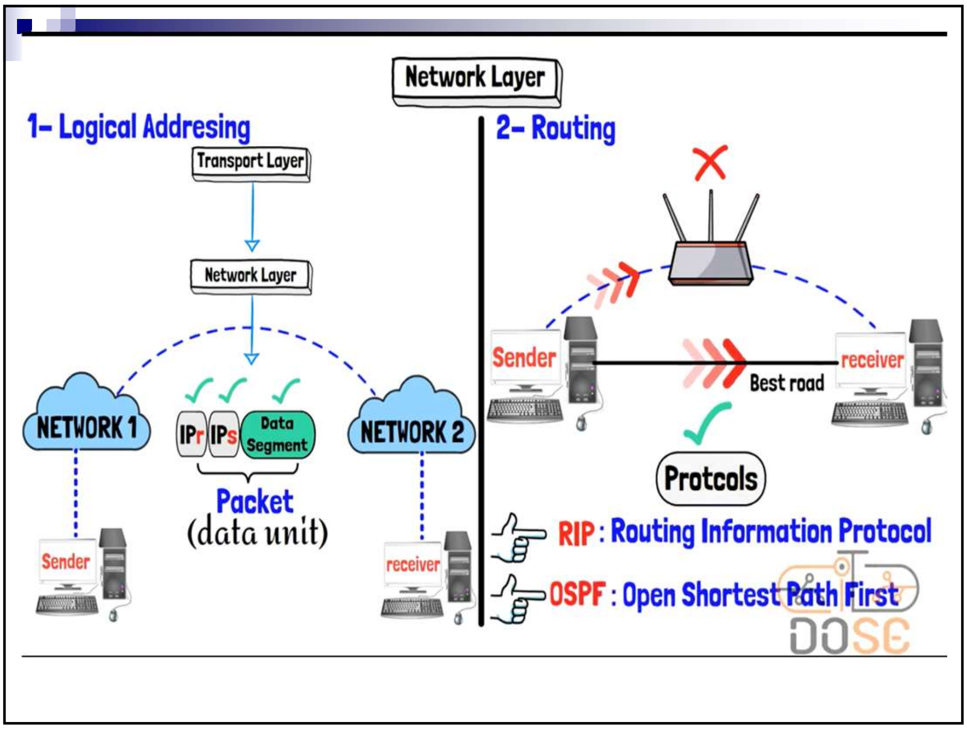
- https or https for web browsing
- File Transport Protocol (FTP) for file downloading and transferring
- Simple Mail Transfer Protocol(SMTP) for email


Application Layer
Protocol
Support
ACTION
Application Layer
https
FTP
SMTP


Presentation layer
Application layer
Data
ABC 123
Translation
(binary system)
00101011
01101010
101110101
11011000
10100110
Data Compression
00101011
01101010
101110101
11011000
10100110
Encryption
receiver
Decryption
SSL
****


Session layer
1- Transmission Mode
Simplex mode
Half-duplex mode
Full-duplex mode
2- Authentication
LOGIN
*****
3- Authorization
4- Session Management


Transport Layer
1-data transfer
(order)
Session layer
Data
segmentation
1
2
3
Desegmentation
port number
sequence number
2- Flow control
(Transfer Rate)
10 Mbps
100 Mbps
10 Mbps
3-Determine Protocol
1-TCP (Transmission Control Protocol)
connection-oriented transmission
2-UDP (User Datagram Protocol)
connection-less transmission
sender
segment
segment



Network Layer

1- Logical Addresing

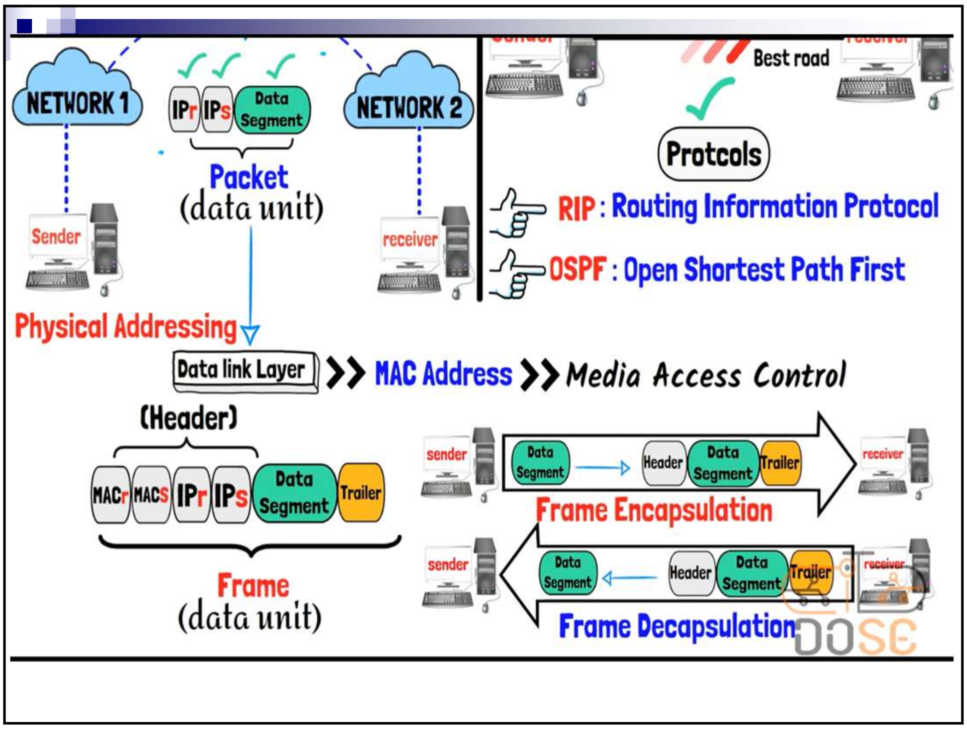
Packet
(data unit)

2- Routing

Protcols

RIP : Routing Information Protocol

OSPF : Open Shortest Path First



Packet
(data unit)

Protcols

RIP : Routing Information Protocol

OSPF : Open Shortest Path First

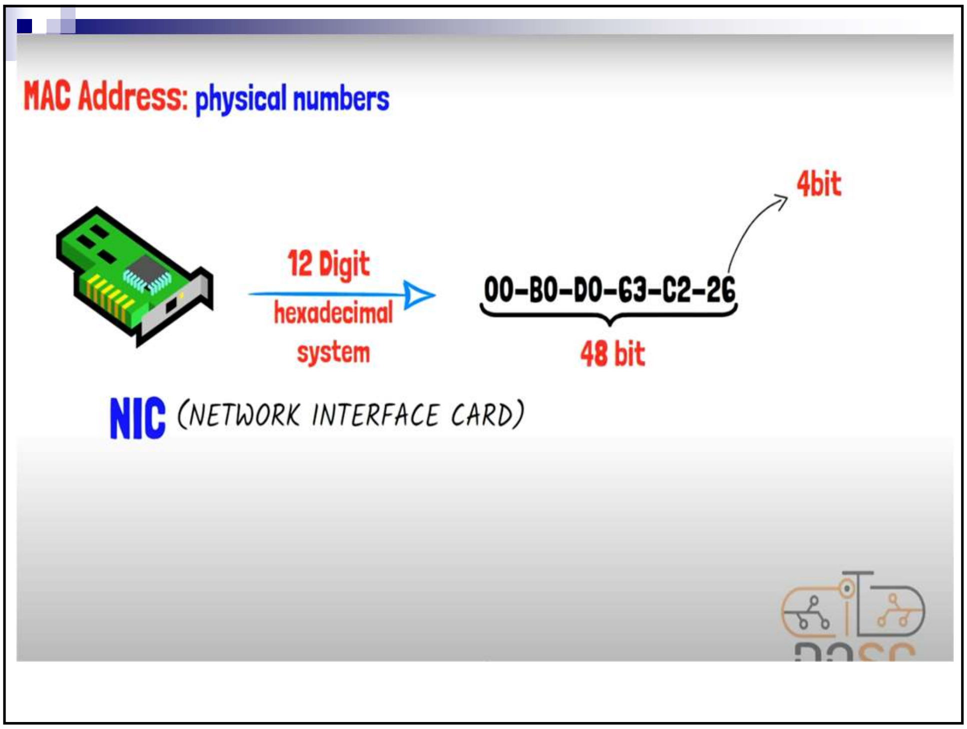
Physical Addressing

Data link Layer >> MAC Address >> *Media Access Control*

Frame
(data unit)

Frame Encapsulation

Frame Decapsulation



MAC Address: physical numbers

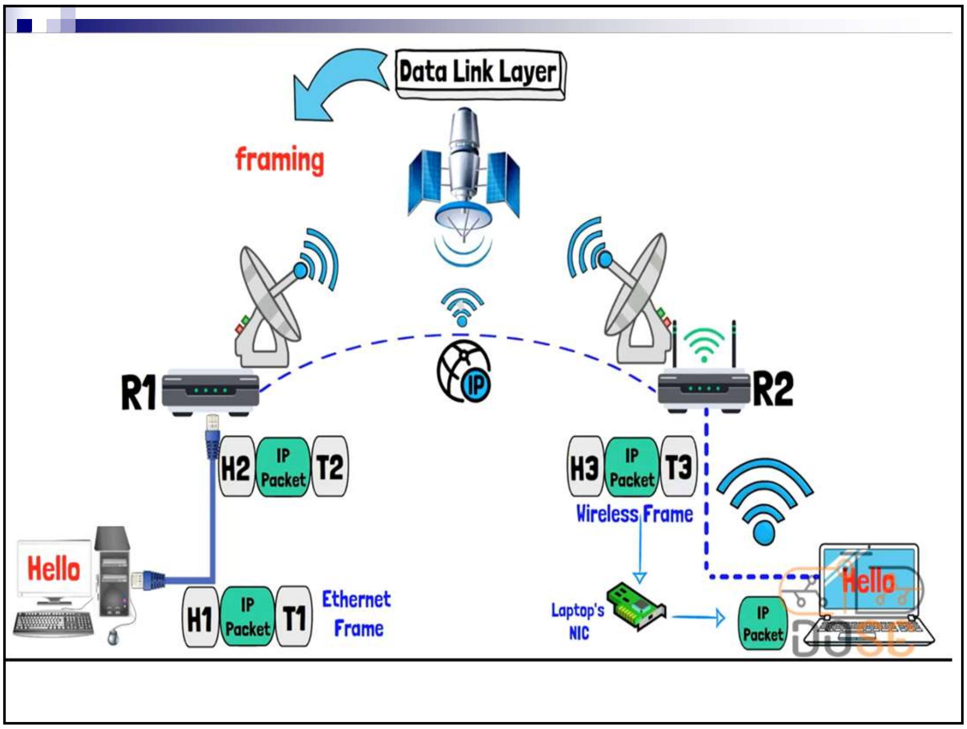
12 Digit hexadecimal system

00-B0-D0-63-C2-26

4bit

48 bit

NIC (NETWORK INTERFACE CARD)



Data Link Layer

framing

R1

R2

Hello

H1 IP Packet T1 Ethernet Frame

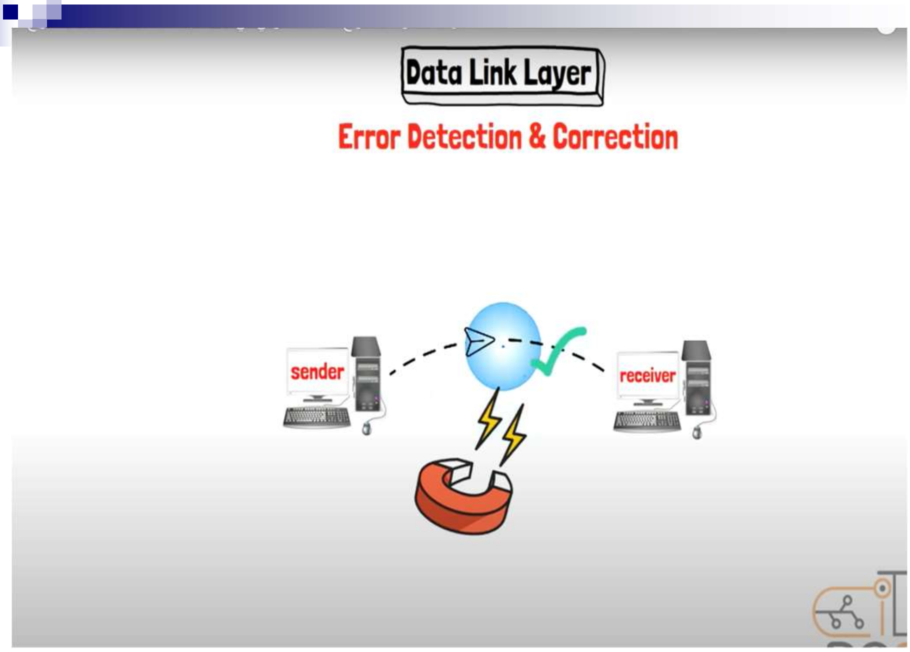
H2 IP Packet T2

H3 IP Packet T3 Wireless Frame

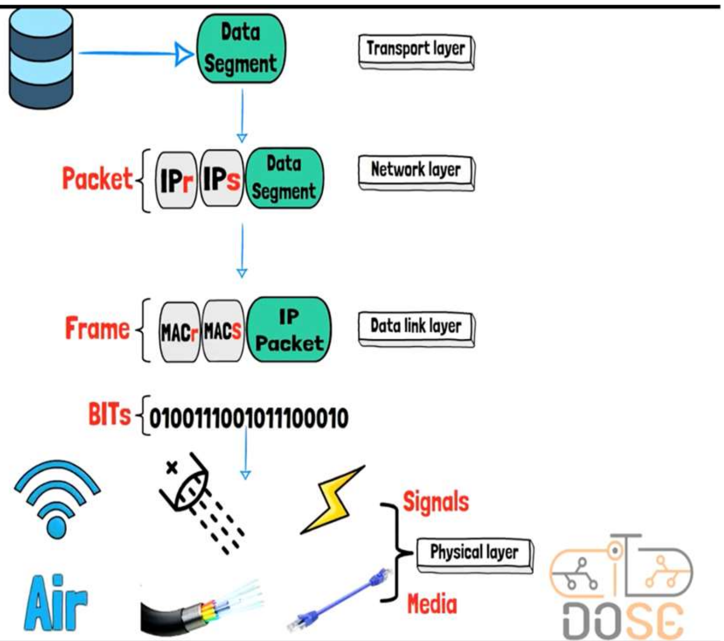
Laptop's NIC

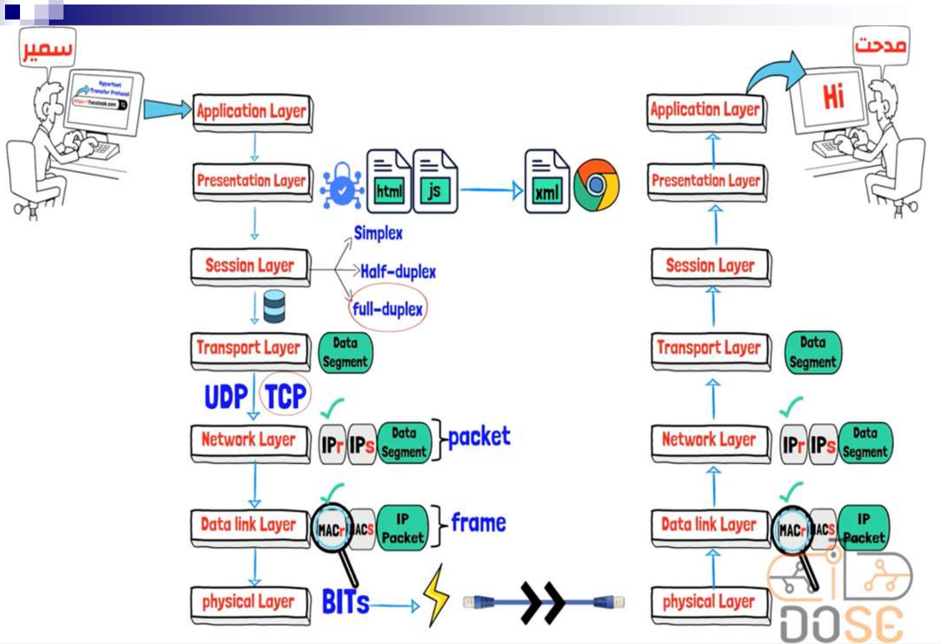
IP Packet

Hello



Physical Layer





شبكات

Network Addressing

(Class 4)

TCP/IP Model

The TCP/IP model is a fundamental framework for computer networking. It stands for Transmission Control Protocol/Internet Protocol, which are the core protocols of the Internet. This model defines how data is transmitted over networks, ensuring reliable communication between devices. It consists of four layers:

- Network access Layer (Data link and Physical),
- Network Layer.
- Transport Layer.
- Application Layer.

Each layer has specific functions that help manage different aspects of network communication, making it essential for understanding and working with modern networks.

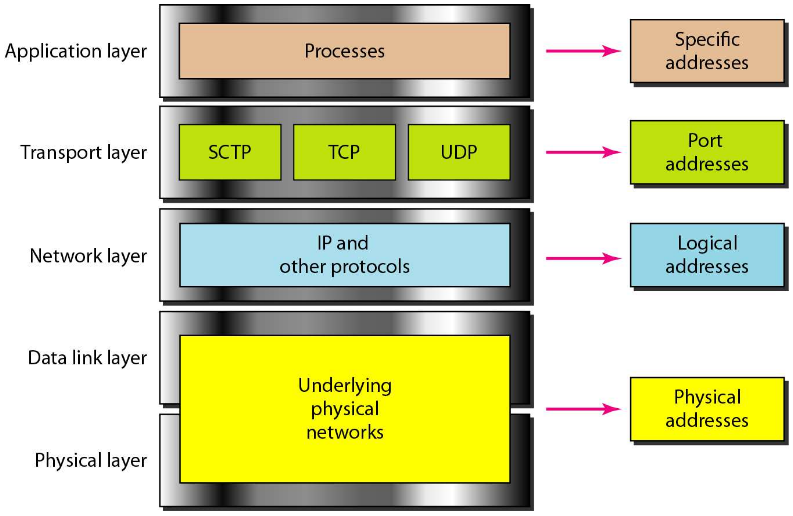
TCP/IP Model

Feature	**OSI Model**	**TCP/IP Model**
Number of Layers	7	4 (or 5)
Layers Included	Physical, Data Link, Network, Transport, Session, Presentation, Application	Network Access, Network, Transport, Application
Development Focus	Conceptual and general networking model	Protocol-driven model (TCP, IP)
Layer Separation	Strict	More flexible
Real-World Use	Rare, mostly for teaching	Widely used, standard for internet
Creator	ISO	U.S. Department of Defense

TCP/IP Model

In practice, the TCP/IP model is more commonly used, but the OSI model remains useful as a framework for understanding how different networking protocols relate to one another.

TCP/IP Layers



Application layer

Transport layer

Network layer

Data link layer

Physical layer

Processes

SCTP

TCP

UDP

IP and other protocols

Underlying physical networks

Specific addresses

Port addresses

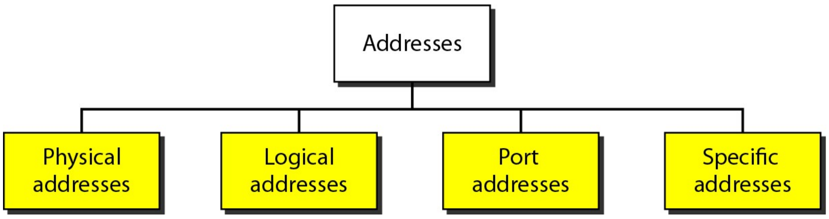
Logical addresses

Physical addresses

TCP/IP PROTOCOL SUITE

ADDRESSING

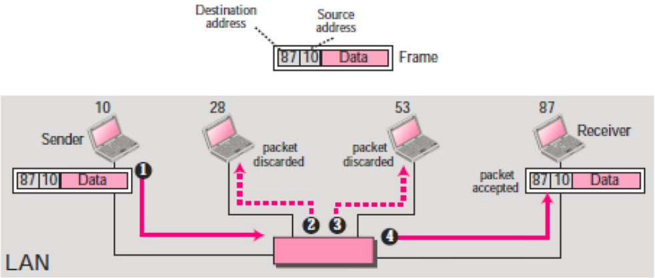
Four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.



Physical Address

- *Physical address or (hardware Address), or Media Address Control MAC address.*
- *Each node has a unique MAC Address: Globally identifier that burned into your RAM of your network interface card.* كل جهاز يحتوي على عنوان الماك معرف بشكل فريد مسجل على ذاكرة بطاقة الشبكة
- *MAC Address assigned by manufacturer , each factory has a block of address assigned by IEEE.* عنوان الماك محدد من قبل الشركة المصنعة لذلك كل مصنع لدية سلسة من العناوين المحجوزة من قبل مؤسسة 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.

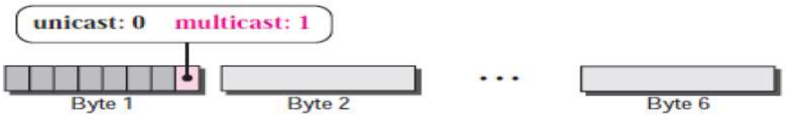


Note that in most data link protocols, the destination address 87 in this case, comes before the source address (10 in this case). The frame is propagated through the LAN. Each station with a physical address other than 87 drops the frame because the destination address in the frame does not match its own physical address. The intended destination computer, however, finds a match between the destination address in the frame and its own physical address. The frame is checked, the header and trailer are dropped, and the data part is decapsulated and delivered to the upper layer.

Unicast, Multicast, and Broadcast Physical Addresses

Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network). Some networks support all three addresses.

A source address is always a unicast address—the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast. The least significant bit of the first byte defines the type of address.



Q: Define the type of the following destination addresses:

1. 4A:30:10:21:10:1A 4A = 01001010

2. 47:20:1B:2E:08:EE 47 = 01000111

3. FF:FF:FF:FF:FF:FF FF = 11111111

Network Layer:
Logical Addressing

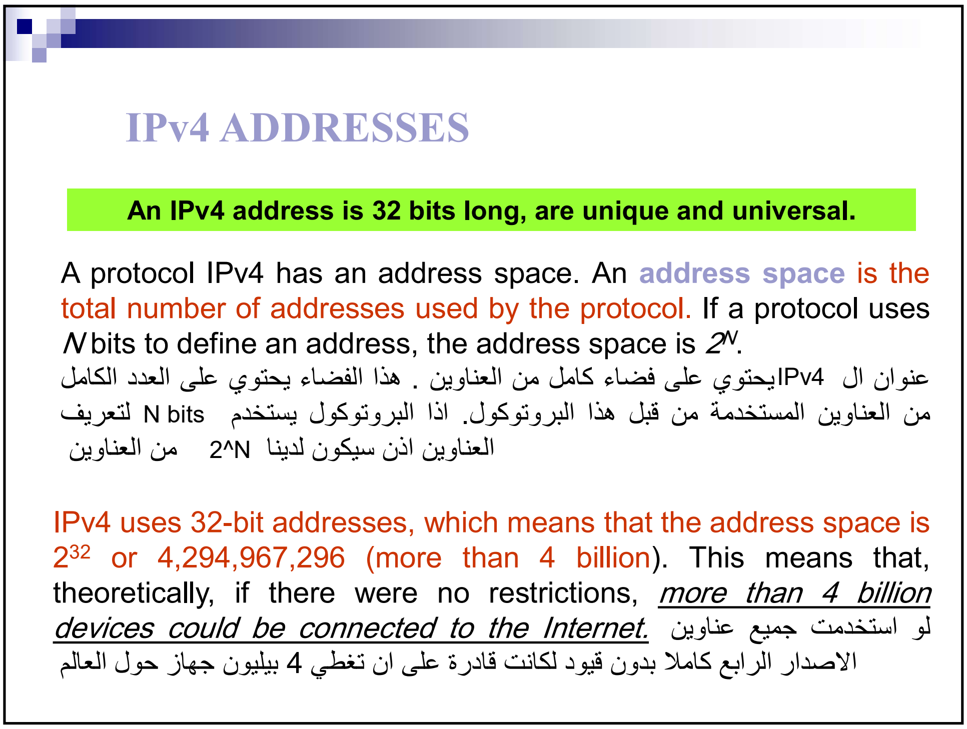
An IP address (Internet Protocol Address) or (logical Address) is a unique address that devices use it in order to communicate with each other. العنوان المنطقي يكون بشكل عنوان منفرد لكل جهاز لغرض الاتصال مع الاجهزة الاخرى

IP addresses are managed and created by the Internet Assigned Numbers Authority (**IANA**). تنشيء و تدار IPsكل عناوين من قبل مؤسسة 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.



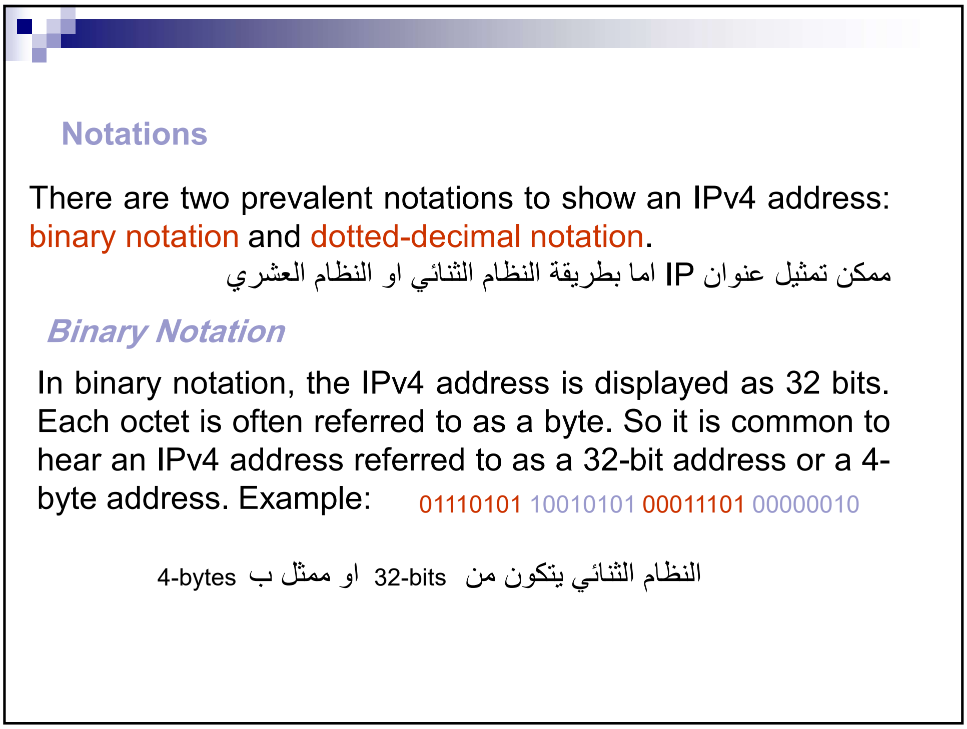
IPv4 ADDRESSES

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.

عنوان ال IPv4يحتوي على فضاء كامل من العناوين . هذا الفضاء يحتوي على العدد الكامل من العناوين المستخدمة من قبل هذا البروتوكول. اذا البروتوكول يستخدم N bits لتعريف العناوين اذن سيكون لدينا 2^N من العناوين

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.* لو استخدمت جميع عناوين الاصدار الرابع كاملا بدون قيود لكانت قادرة على ان تغطي 4 بيليون جهاز حول العالم



Notations

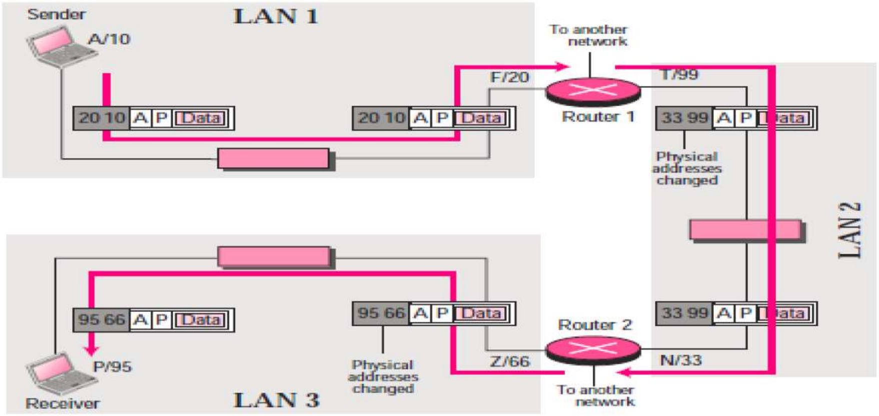
There are two prevalent notations to show an IPv4 address: binary notation and dotted-decimal notation.

ممكن تمثيل عنوان IP اما بطريقة النظام الثنائي او النظام العشري

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

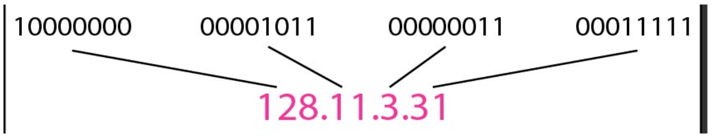
النظام الثنائي يتكون من 32-bits او ممثل ب 4-bytes



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:

لكي يكون عنوان IP اكثر اختصارا و سهل القراءة لذلك يكتب بشكل نظام عشري
مقسم على اربعة اقسام معزولة بنقطة



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

- 0. 0. 0. 0 …….> 0.0.0.1….>0.0.0.2…>0.0.0.255
- 0.0.1.0..>0.0.1.1…>0.0.1.2…>0.0.1.255
- 0.0.2.0 -→ 0.0.2.255
- 0.0.3.0
- 0.0.255.255
- 0.1.0.0 ---→ 255.255.255.255

Example 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

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

a. 111.56.45.78

b. 221.34.7.82

Solution

We replace each decimal number with its binary equivalent.

a. 01101111 00111000 00101101 01001110

b. 11011101 00100010 00000111 01010010

Example 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). لا يجوز ان يسبق العدد بصفر

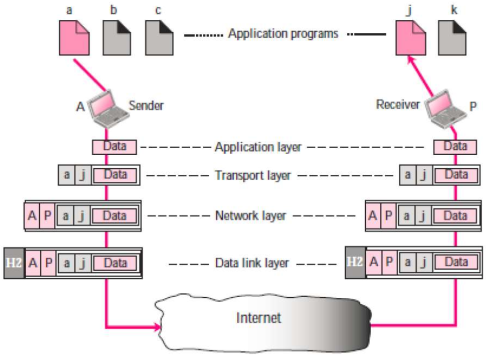
b. There can be no more than four numbers. لا يمكن ان يكون اكثر من 4 ارقام

c. Each number needs to be less than or equal to 255. اي رقم لا يتجاوز ال 255

d. A mixture of binary notation and dotted-decimal notation is not allowed. لا يمكن الخلط بين اكثر من نظامين في ان واحد

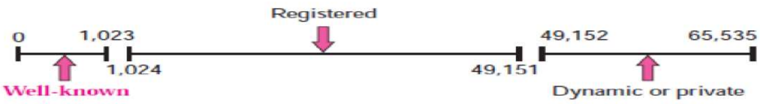
Port Address

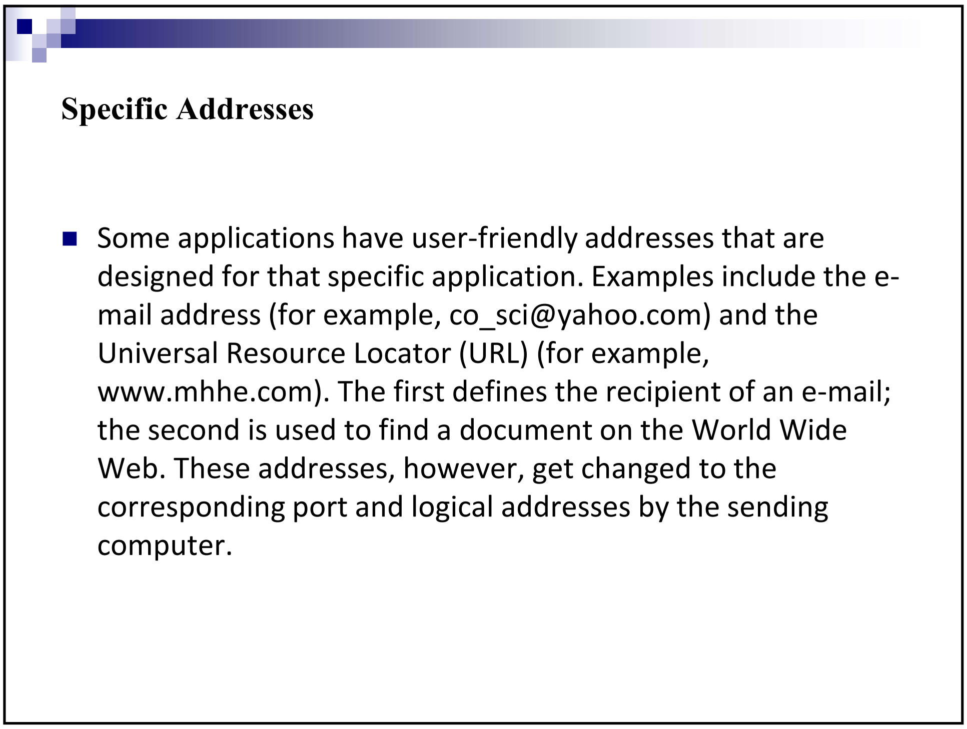
- A port address is a 16-bit address represented by one decimal number>
- The following Figure shows two computers communicating via the Internet. The sending computer is running three processes at this time with port addresses **a**, **b**, and **c**. The receiving computer is running two processes at this time with port addresses **j** and **k**. Process **a** in the sending computer needs to communicate with process **j** in the receiving computer. Note that although both computers are using the same application, FTP, for example, the port addresses are different because one is a client program and the other is a server program.



*ICANN Ranges (*Internet Corporation for Assigned Names and Numbers)

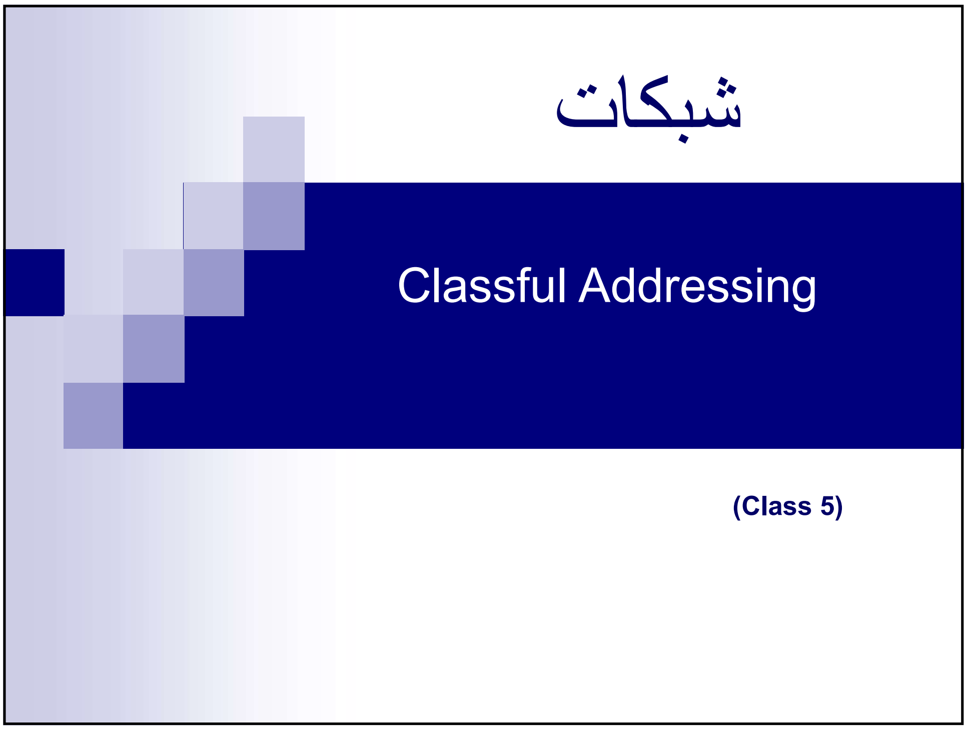
- ICANN has divided the port numbers into three ranges: well-known, registered, and dynamic (or private)
- **Well-known ports:** The ports ranging from 0 to 1,023 are assigned and controlled by ICANN
- **Registered ports:** The ports ranging from 1,024 to 49,151 are not assigned or controlled by ICANN. They can only be registered with ICANN to prevent duplication.
- **Dynamic ports:** The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used as temporary or private port numbers. The original recommendation was that the ephemeral port numbers for clients be chosen from this range. However, most systems do not follow this recommendation.





Specific Addresses

- Some applications have user-friendly addresses that are designed for that specific application. Examples include the e-mail address (for example, co_sci@yahoo.com) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.



شبكات

Classful Addressing

(Class 5)

Classful Addressing

- An **IP address** is an address that has information about how to reach a specific host, especially outside the LAN. An IP address is a 32-bit unique address having an address space of 2^{32}.
- **Classful IP addressing** is a way of organizing and managing IP addresses, which are used to identify devices on a network. Think of IP addresses like street addresses for houses; each device on a network needs its unique address to communicate with other devices.

Need For Classful Addressing

- Initially in 1980's IP address was divided into two fixed part i.e., NID(Network ID) = 8bit, and HID(Host ID) = 24bit. So there are 2^8 that is 256 total network are created and 2^{24} that is 16M Host per network.
- There are one 256 Networks and even a small organization must buy 16M computer(Host) to purchase one network. That's why we need classfull addressing.

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

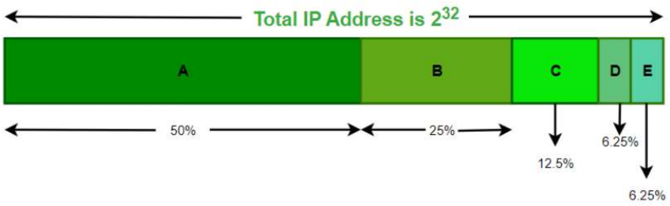
	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191	🟨		
Class C	192–223	🟨	🟨	
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

Finding the classes in binary and dotted-decimal notation

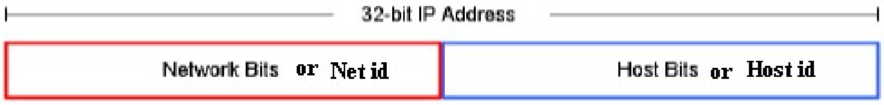
- IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and Regional Internet Registries(RIR).
- While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Occupation of The Address Space In Classful Addressing



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.

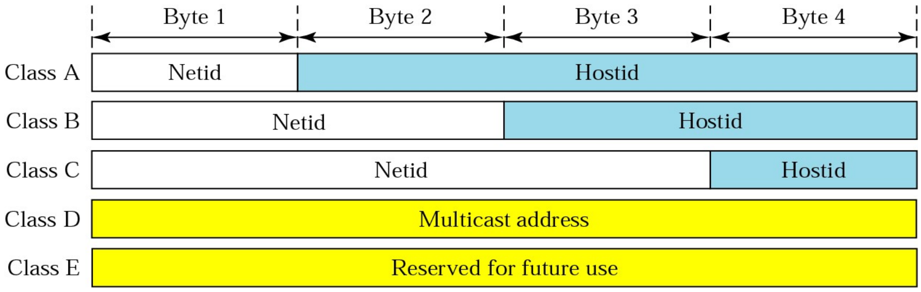


32-bit IP Address

Network Bits or Net id

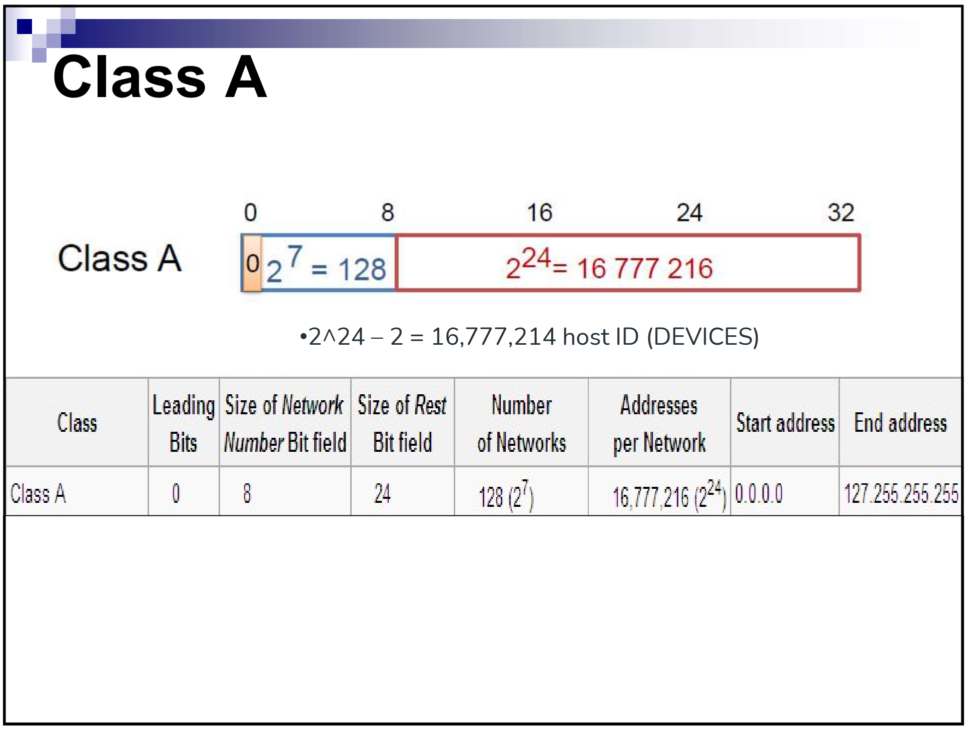
Host Bits or Host id

IP Address Classes



	Byte 1	Byte 2	Byte 3	Byte 4
Class A	Netid	Hostid		
Class B	Netid		Hostid	
Class C	Netid			Hostid
Class D	Multicast address			
Class E	Reserved for future use			

- IP addresses are globally managed **by Internet Assigned Numbers Authority(IANA) and Regional Internet Registries(RIR)**.
- While finding the total number of host IP addresses, **2** IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the ***network number*** and whereas the last IP address is reserved for ***broadcast IP***.



Class A

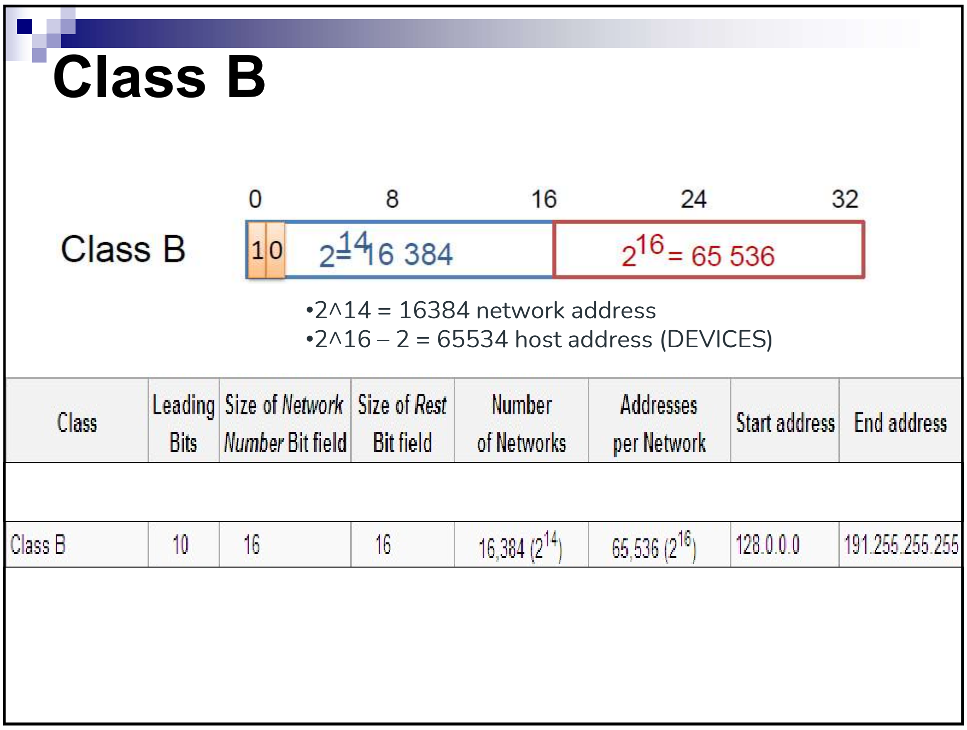
Class A

0 8 16 24 32

0 2^{7} = 128 | 2^{24}= 16 777 216

•2^24 – 2 = 16,777,214 host ID (DEVICES)

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

Class B

0 8 16 24 32

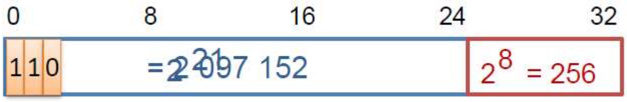
1 0 2^{14}=16 384 | 2^{16}= 65 536

•2^14 = 16384 network address
•2^16 – 2 = 65534 host address (DEVICES)

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 B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255

Class C

Class C

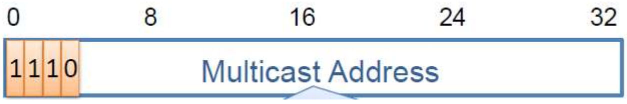


- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

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 C	110	24	8	2,097,152 (2^{21})	256 (2^{8})	192.0.0.0	223.255.255.255

Class D

Class D

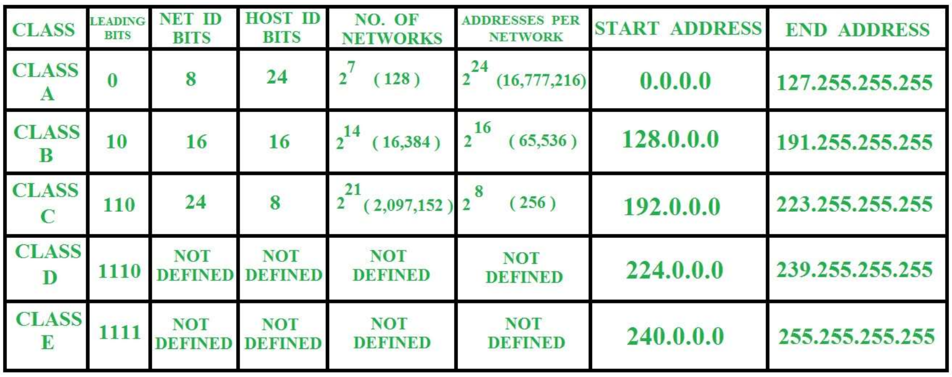


Class	Leading Bits	Size of *Network Number* Bit field	Size of *Rest* Bit field	Number of Networks	Addresses per Network	Start address	End address
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255

Class E

- IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E range from 240.0.0.0 – 255.255.255.255. This class doesn't have any subnet mask. The higher-order bits of the first octet of class E are always set to 1111.

Summary



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7 (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^8 (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Example

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
e. 192.168.0.0
f. 172.16.0.1

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.***

Problems with Classful Addressing

- The problem with this classful addressing method is that millions of class A addresses are wasted.
- Many of the class B addresses are wasted.
- The number of addresses available in class C is so small that it cannot cater to the needs of organizations.
- Class D addresses are used for multicast routing and are therefore available as a single block only.
- Class E addresses are reserved.

Since there are these problems, Classful networking was replaced by Classless Inter-Domain Routing (CIDR) in 1993. We will be discussing Classless addressing in the next lecture

شبكات

Subnetting Addressing

(Class 8)

By
Asst. prof. Dr. Awos Kh. Ali

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.

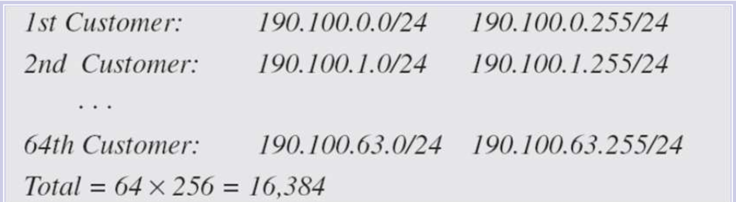
Design the sub blocks and find out how many addresses are still available after these allocations?

Solution

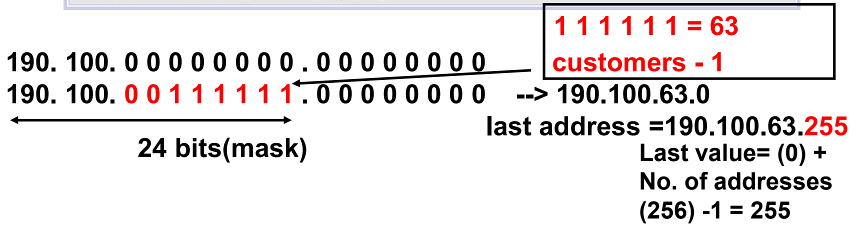
Figure below shows the situation.

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



1st Customer:	*190.100.0.0/24*	*190.100.0.255/24*
2nd Customer:	*190.100.1.0/24*	*190.100.1.255/24*
. . .		
64th Customer:	*190.100.63.0/24*	*190.100.63.255/24*
Total = 64 × 256 = 16,384		



1 1 1 1 1 1 = 63
customers - 1

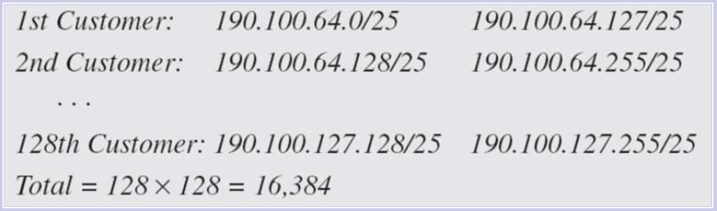
190. 100. 0 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0
190. 100. 0 0 1 1 1 1 1 1 . 0 0 0 0 0 0 0 0 --> 190.100.63.0

24 bits(mask)

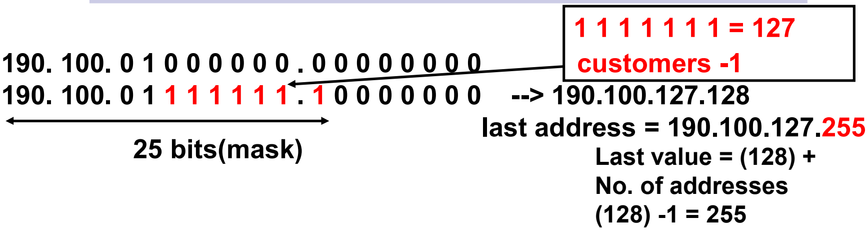
last address =190.100.63.255
Last value= (0) +
No. of addresses
(256) -1 = 255

Group 2

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



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



1 1 1 1 1 1 1 = 127
customers -1

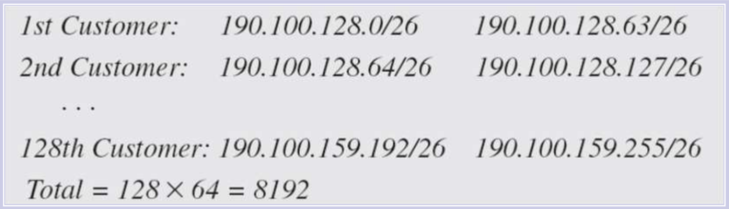
190. 100. 0 1 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0
190. 100. 0 1 1 1 1 1 1 1 . 1 0 0 0 0 0 0 0 --> 190.100.127.128
last address = 190.100.127.255

25 bits(mask)

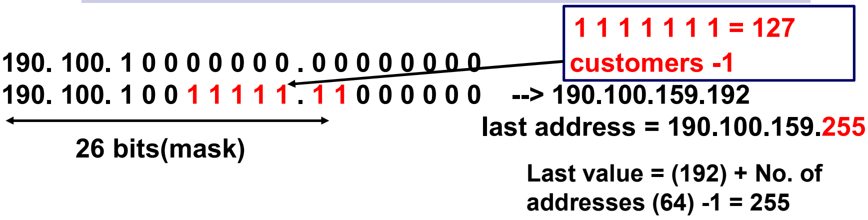
Last value = (128) +
No. of addresses
(128) -1 = 255

Group 3

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



1st Customer:	*190.100.128.0/26*	*190.100.128.63/26*
2nd Customer:	*190.100.128.64/26*	*190.100.128.127/26*
. . .		
128th Customer:	*190.100.159.192/26*	*190.100.159.255/26*
Total = 128 × 64 = 8192		



1 1 1 1 1 1 1 = 127
customers -1

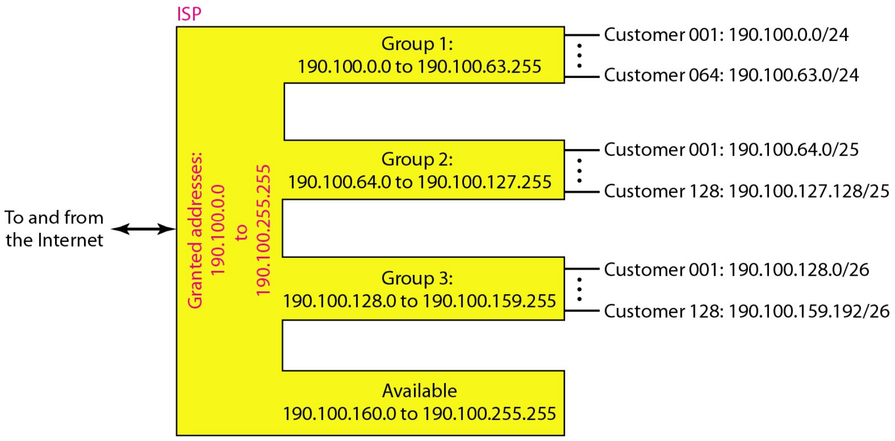
190. 100. 1 0 0 0 0 0 0 0 . 0 0 0 0 0 0 0 0
190. 100. 1 0 0 1 1 1 1 1 . 1 1 0 0 0 0 0 0 --> 190.100.159.192
last address = 190.100.159.255

26 bits(mask)

Last value = (192) + No. of
addresses (64) -1 = 255

An example of address allocation and distribution by an ISP

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



ISP

To and from the Internet

Granted addresses: 190.100.0.0 to 190.100.255.255

Group 1: 190.100.0.0 to 190.100.63.255

Customer 001: 190.100.0.0/24

Customer 064: 190.100.63.0/24

Group 2: 190.100.64.0 to 190.100.127.255

Customer 001: 190.100.64.0/25

Customer 128: 190.100.127.128/25

Group 3: 190.100.128.0 to 190.100.159.255

Customer 001: 190.100.128.0/26

Customer 128: 190.100.159.192/26

Available 190.100.160.0 to 190.100.255.255

- **H.W.: An ISP is granted a block of addresses starting with 187.97.0.0/16 (65,536 addresses). The ISP needs to distribute**

these addresses to three groups of customers as follows:

- **The first group has 128 customers; each needs 64 addresses.**
- **The second group has 128 customers; each needs 128 addresses**
- **The third group has 64 customers; each needs 256 addresses.**