Advanced Networks

Dr. Sara Hebal

Assistant professor

Computer sciences department

Faculty of sciences

Ferhat Abbas Setif university 1

Algeria

Email: sara.hebal@univ-setif.dz

1.0 March 2026

Attribution - NonCommercial : http://creativecommons.org/licenses/by-nc/4.0/fr/

Table of contents

Objectives 3

Introduction 4

I - Requirements 5

II - Quiz : Pre-test 6

III - Introduction to Computer Networks 8

1. Chapter Objectives 8
2. What is a Network? 8
3. Fundamental Objectives of Computer Networks....9
4. Network Components 9
5. Networks Classification....9
   - 5.1. Based on Communication Pattern (transmission techniques)....10
   - 5.2. Based on Geographical Scope (distance covered) 10
   - 5.3. Based on Host role 11
   - 5.4. Based on Fields of application 12
   - 5.5. Based on Mobility....12
6. Networking Models....13
7. Quiz....15

IV - IP Addressing & Dynamic Routing 17

1. Chapter Objectives 17
2. Introduction....17
3. Internet Protocol (IP)....18
   - 3.1. IPv4 Packet Header 19
   - 3.2. IP Address 20
   - 3.3. IP Address Classes....22
   - 3.4. IP Address Subnetting....22
   - 3.5. Classless Inter-Domain Routing CIDR....23
4. Dynamique Routing....24
5. Quiz....27

V - Bibliography 29

Objectives

By the end of this course, students will be able to:

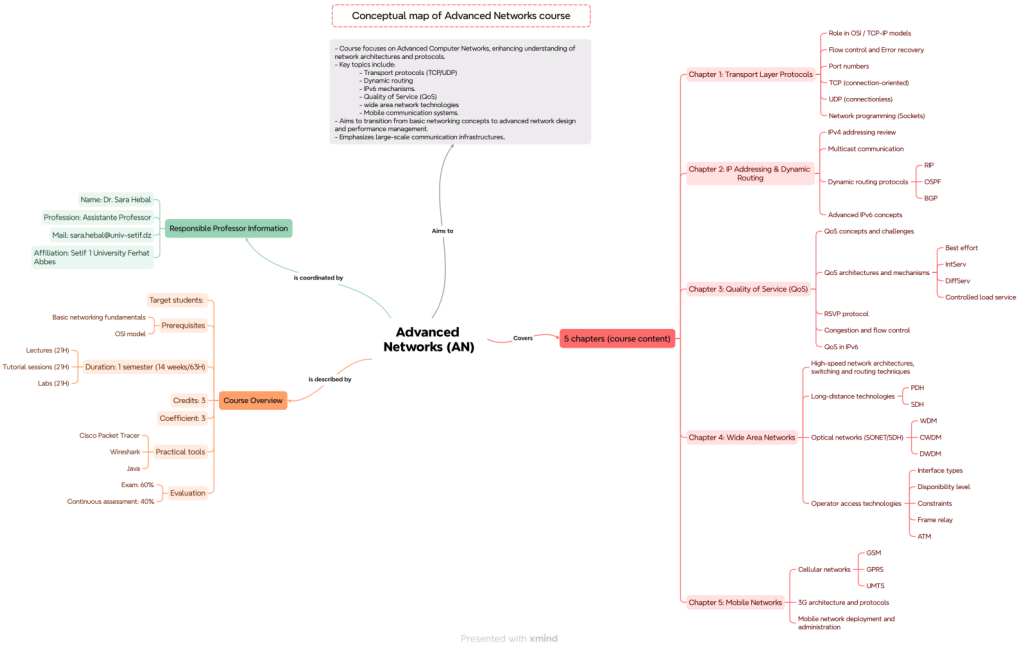
- Explain core networking concepts, including network architectures, components, topologies, and the OSI/TCP-IP models.
- Analyze and apply IP addressing schemes and routing mechanisms, including IPv4/IPv6 and dynamic routing protocols.
- Evaluate the behavior and performance of transport protocols (TCP and UDP), including connection management, flow control, and reliability.
- Assess QoS mechanisms and select appropriate strategies to ensure network performance under different traffic conditions.
- Describe and analyze WAN technologies and architectures, including MPLS and optical networks.
- Explain the architecture and functioning of mobile communication systems (GSM, UMTS, 3G/4G).

Introduction

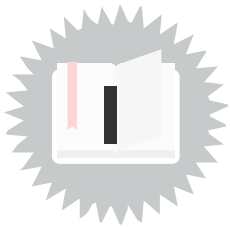
Modern computer networks form the backbone of today's digital world, enabling communication, data exchange, and service delivery across local and global infrastructures. This course on Advanced Computer Networks builds upon fundamental networking concepts to provide a deeper understanding of how complex communication systems operate and are managed.

The course begins with a review of essential concepts, including network components, architectures, and reference models such as OSI and TCP/IP. It then focuses on key layers of network communication, particularly the network and transport layers, exploring addressing mechanisms, routing strategies, and transport protocols.

In addition, the course introduces advanced topics such as Quality of Service (QoS), wide-area network (WAN) technologies, and mobile communication systems. Emphasis is placed on both theoretical understanding and practical application, enabling students to analyze network behavior, configure network services, and evaluate performance in real-world scenarios.



Requirements



Before starting this course, students should have the following basic competencies:

- Be comfortable using a computer, including file management and basic software tools.
- Have introductory knowledge of computer science concepts from a previous course or equivalent background.
- Be familiar with the basics of operating systems, especially command-line usage.
- Understand elementary mathematical ideas such as binary numbers and simple algebraic operations.
- Have general awareness of Internet usage and how data is exchanged over networks.
- Possess introductory knowledge of computer networks, including the concept of IP addresses (IPv4) and basic communication between devices.
- Be able to understand simple technical explanations and follow structured problem-solving steps.

Note: Key foundational networking concepts will be briefly reviewed at the beginning of the course to ensure a common starting level for all students

Quiz : Pre-test



Quiz

What is the most efficient way to organize a project containing documents, images, and code files?

- Keep all files in the desktop folder
- Store all files in a single directory
- Separate files into structured folders by type
- Rename all files with random names for uniqueness

Quiz

Describe the steps you would take to move a file from one folder to another using a file manager.

Quiz

Which option best defines an algorithm?

- A programming language used to build applications
- A sequence of instructions designed to solve a problem
- A hardware component that processes data
- A network communication protocol

Quiz

Which environment represents a command-line interface?

- Windows Explorer
- Terminal / Command Prompt
- Desktop icons
- Web browser

Quiz

A command-line interface allows users to interact with a computer by entering commands through a text-based environment.

- True
- False

Quiz

Write one basic command used in a terminal and explain its function.

Quiz

Which of the following are valid binary numbers?

- [ ] 10101
- [ ] 10201
- [ ] 11100

Quiz

What happens when you send data over the Internet?

- ○ It is sent as one complete block without changes
- ○ It is divided into small packets for transmission
- ○ It is stored in the router permanently
- ○ It is converted into a physical signal only at the destination

Quiz

Which of the following are valid IPv4 addresses?

- [ ] 192.168.1.10
- [ ] 10.0.0.300
- [ ] 172.16.5.4
- [ ] 255.255.255.255

Quiz

Which of the following are Internet services?

- [ ] Email
- [ ] File Transfer (FTP)
- [ ] Offline text editor
- [ ] Web browsing

Introduction to Computer Networks



1. Chapter Objectives

By the end of this chapter, the student will be able to:

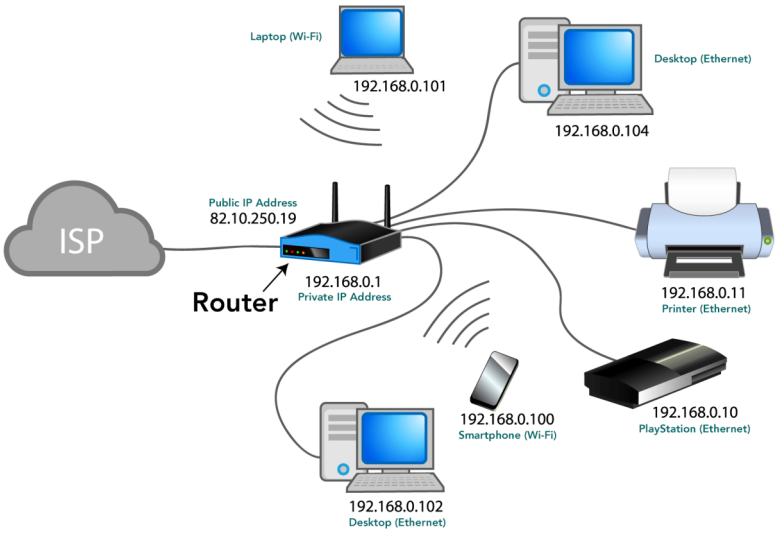
- Define the fundamental concepts of computer networks and their components.
- Classify different types of networks and network topologies.
- Differentiate between the OSI and TCP/IP reference models.

2. What is a Network?

Definition

A computer network is a set of interconnected autonomous devices that communicate and share resources using standardized rules called communication protocols.

- A network could be as large as the Internet or as small as your two computers at home, sharing files and printers
- Two computers are interconnected if they are capable of exchanging information.



Warning

- Autonomy excludes master/slave-type systems.
- A system composed of one unit that controls several slave units is not a network

3. Fundamental Objectives of Computer Networks

- **Data Communication:** efficient and reliable information exchange between geographically distributed entities (email, video conferencing platforms).
- **Resource Sharing:** hardware, software, storage
- **Increase collaboration:** collaborative engineering platforms
- **Reliability and Fault Tolerance:** backup systems.
- **Scalability:** ability to grow without redesign Cost Optimization
- **Distributed Processing:** Distributed databases, cloud computing platforms and Parallel AI model training
- **Mobility and Remote Access:** access resources from different locations and enable devices to remain connected while moving.

Example

AI platforms, IoT ecosystems, cloud computing, and financial systems are examples of modern infrastructures that are essentially network-dependent.

4. Network Components

1. **End Devices (Hosts)**
    - Computers / Workstations
    - Smartphones / Tablets
    - Servers (Web, DNS, Database)
    - IoT Devices (sensors, cameras)
2. **Intermediate Devices**
    - Routers
    - Hubs
    - Switches
    - Access Points
    - Firewalls
3. **Communication Media**
    - Copper cables
    - Fiber Optical cables
    - Wireless channels

5. Networks Classification

Networks lack a standard classification and are typically categorized by various criteria:

- Communication Pattern (transmission techniques)
- Geographical scope (distance covered)
- Host role
- Fields of application

- Mobility

5.1. Based on Communication Pattern (transmission techniques)

Broadcast Networks

- Shared communication medium
- All connected devices receive the transmitted frame Each message contains its destination address
- Devices check upon reception to determine if they should process the message or disregard it.
- A broadcast network allows a message to be sent to all devices in the network.
    - **Limited broadcast:** broadcast in the same network
    - **Direct broadcast:** broadcast from a device to all devides in another network
- Medium access control required (one at a time)
- Typical Topology: Bus topology

Note

In some networks, a message can be sent only to a selected group of devices. This type of transmission is known as Multicasting.

- one-to-many (not all)

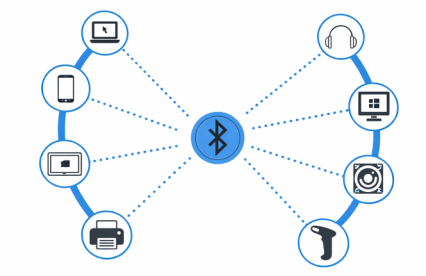
Point-to-Point Networks

- Dedicated link between two devices
- No shared medium
- Data is only delivered to the designated receiver.
- Data is typically forwarded by intermediate devices from source to destination, with routing algorithms determining the optimal path when multiple paths are available.
- Often full-duplex
- Common in WANs
- Typical Topology: Mesh topology

5.2. Based on Geographical Scope (distance covered)

Personal Area Network (PAN)

- Short-range network (few meters 1-10m)
- Centered around one person that links their devices
- Use wireless technologies (Bluetooth, NFC, ZigBee)
- Low data rate

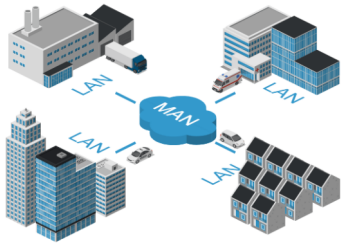


Local Area Network (LAN)



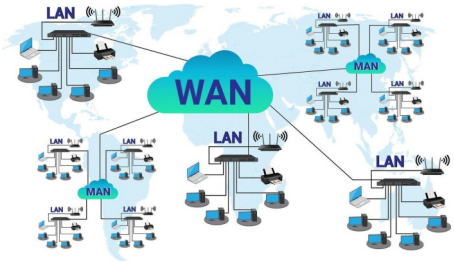
- Interconnects devices within a limited geographical area, such as a building or campus
- Several kilometres, typically use wired connection efficient communication & data transfer, high data rate, Low latency

Metropolitan Area Network (MAN)



- Covers a wider geographical area than a LAN
- Connects multiple sites across a metropolitan area (city or a large campus)
- Several kilometers to tens of kilometers, High data rate

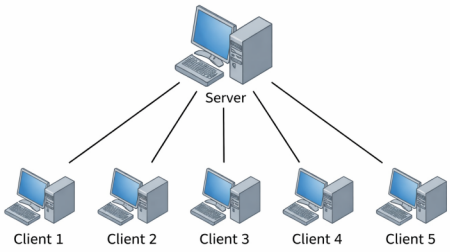
Wide Area Network (WAN)



- Connects networks over large geographic areas (LANs, MANs)
- Mesh topology
- Point-to-Point links
- Global connectivity & High scalability

5.3. Based on Host role

Client-server Network

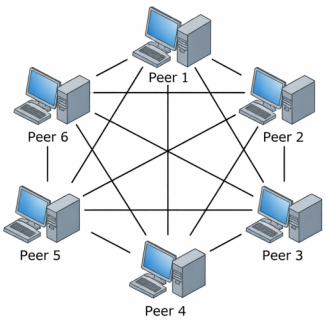


- Centralizes services on dedicated servers
- Clients send requests to the servers
- Servers provide services to clients
- Centralized control
- High scalability
- Easier management
- Security control

Warning

- Single point of failure (without redundancy)

Peer-to-Peer Network (P2P)



- A device can be a client or a server
- Decentralized architecture
- Distributed resource sharing
- Easy to set up
- Less complex
- Lower cost for simple tasks & small networks

Warning

- Not as secure
- Not scalable
- Slower performance

5.4. Based on Fields of application

Networks are designed differently depending on their operational domain.

- **Telecommunication Networks:** used for voice communication (2G, 3G, 4G, 5G,etc)
- **Home networks:** used for communication in houses and apartments (TVs, Mobiles, heating system, lighting system . . .)
- **Offices networks:** used for data communication within a company, university or administration, for exchanging information or sharing resources (documents, printers . . .)
- **Industrial networks:** used to exchange data between control systems in an industrial setup
- **Military networks:** used by military command systems

5.5. Based on Mobility

Wired Network

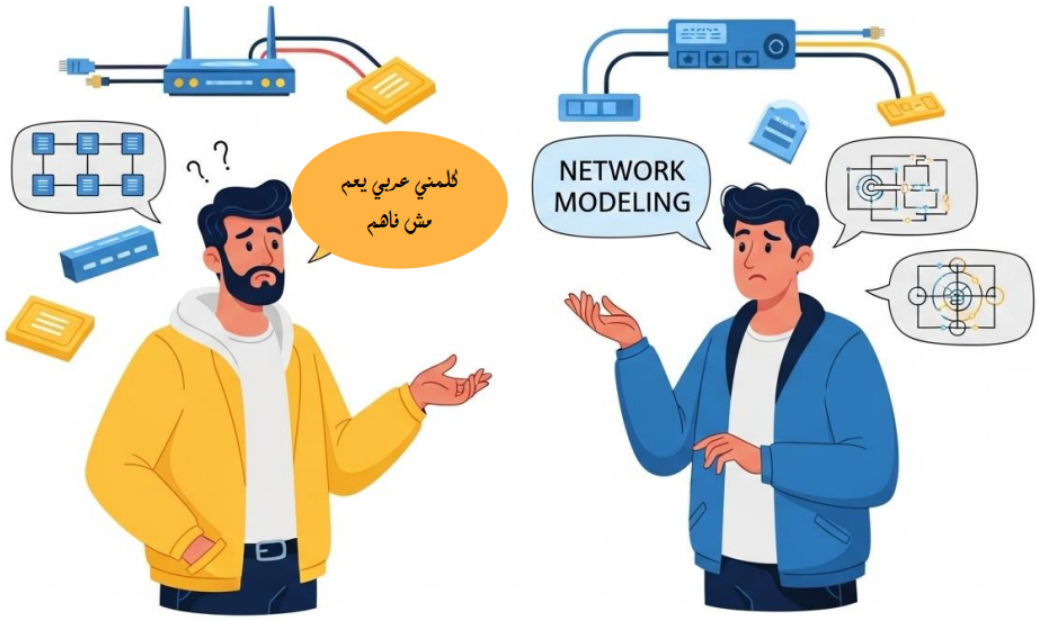
- Wired infrastructure (use cables to connect equipment to the network)
- Minimal mobility
- Predictable topology

Wireless Network

- Radio-based transmission (use antennas to send and receive data)
- Supports device movement while maintaining communication continuity.
- Two categories
    - Networks with infrastructure (those networks using access points)
    - Ad hoc networks

6. Networking Models

How can computers from different organizations communicate with each other despite using different systems and technologies?



Netwoking models *Definition*

Categorise and provide a structure for Network Protocols and Standards

Networking protocols *Definition*

Are a set of rules defining how network devices and software should work to connect and communicate to a network

Note

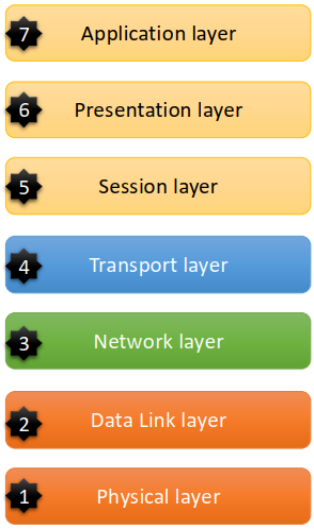
In the beginning the development of networks was chaotic.

- Each vendor had its own proprietary solution.
- The bad part was that one vendor's solution was not compatible with another vendor's solution.

This is where the idea for the standardized networking models such as OSI-model was born, having a layered approach to networks our hardware vendors would design hardware for the network, and others could develop software for the application layer.

Using an open model which everyone agrees on means we can build networks that are compatible with each other.

OSI (Open System Interconnection) Model



- A conceptual architecture that standardizes the functions of a telecommunications or computer system into seven layers
- Each layer has a number, name, functions and communicates with the layers directly above and below it
- The first four layers are important for networking, while the upper three layers are important for applications.

- The seven layers of this model, from the lowest (Layer 1) to the highest (Layer 7), are as follows:
  1. **Physical Layer**
     - Define physical characteristics of the used medium (voltage, connectors, . . .)
     - Convert digital bits to electrical or radio signals (encoding)
     - Bit transmission
  2. **Data Link Layer**
     - Provides node-to-node connectivity and data transfer
     - Define how data is formatted for transmission over a physical media
     - Error detection
     - Physical addressing
     - Two sublayers
       - **Logical Link Control (LLC)**
       - **Media Access Control (MAC)**
  3. **Network Layer**
     - Provide connectivity between end hosts in different networks
     - Logical addressing (IP)
     - Data routing and forwarding (routing protocols) between devices on different networks
  4. **Transport Layer**
     - Ensures reliable end-to-end communication
     - Split large data into smaller segments and handling error detection and correction
     - The most common transport layer protocols are:
       - **TCP (Transmission Control Protocol)** for reliable communications
       - **UDP (User Datagram Protocol)** for connectionless communications
  5. **Session Layer**

- Establishes, maintains and terminates sessions or connections between applications on different devices
- Provides synchronization and control mechanisms to ensure orderly data exchange

6. **Presentation Layer**
   - Translates data between the application layer data and lower layers into appropriate format
   - Data encryption, decryption, compression and formatting
7. **Application Layer**
   - The closest layer to the user interacting directly with end-user applications (web browser)
   - It provides network services directly to end-users or applications, and includes protocols such as HTTP, FTP, SMTP

7. Quiz

Quiz

Which of the following are **functions/objectives** of computer networks?

- ☐ Resource sharing
- ☐ Data encryption
- ☐ Communication between devices
- ☐ Centralized processing

Quiz

Which statement best describes a computer network topology?

- ○ The physical and logical arrangement of devices in a network
- ○ The type of operating system used in devices
- ○ The physical arrangement of devices in a network

Quiz

Differentiate between LAN and WAN in terms of scope and performance.

Quiz

Explain why the TCP/IP model is more widely used than the OSI model in real-world networks.

Quiz

Which of the following are advantages of layered network models (OSI/TCP-IP)?

- ☐ Simplifies troubleshooting
- ☐ Makes systems independent of hardware changes
- ☐ Removes the need for protocols

- ☐ Standardizes communication

Quiz

Which of the following are true characteristics of a LAN?

- ☐ High data transfer rate
- ☐ Covers a large geographical area
- ☐ Low latency communication
- ☐ Usually privately managed

IP Addressing & Dynamic Routing



1. Chapter Objectives

By the end of this chapter, the student will be able to:

- Interpret IPv4 and IPv6 addressing and its structure.
- Explain the basic principles of packet routing in IP networks.
- Identify major dynamic routing protocols such as RIP, OSPF, and BGP.

2. Introduction

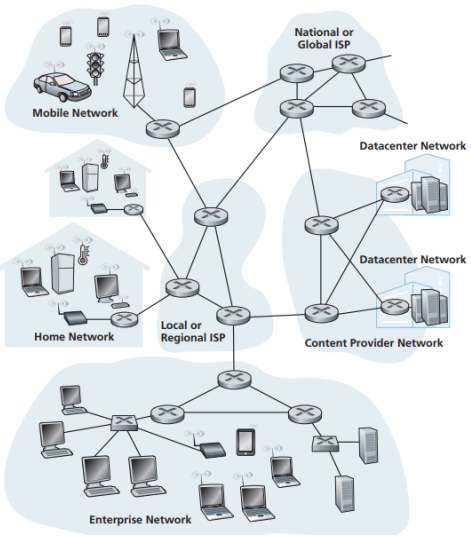
Assume that a student at Setif University sends an email to his friend in Algiers using 4G mobile data. Which networks are involved?

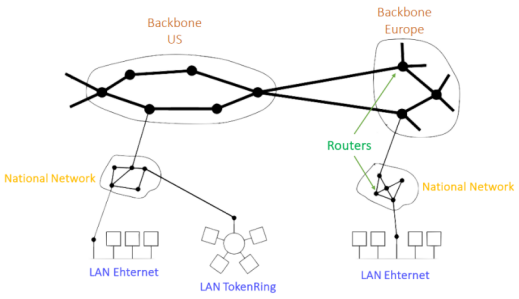
- **University LAN (Ethernet) or WLAN (Wi-Fi):** the packet is sent from the student's laptop to the default gateway (university router).
- **ISP network (fiber backbone):** The university router is connected to a national Internet Service Provider, for example Algérie Télécom
- **Mobile operator network (4G/5G):** The packet's destination address is associated with an Algiers 4G subscriber. Thus, the packet is forwarded to the Mobile Operator Network (e.g., Djezzy, Ooredoo, or Mobilis) by the backbone.
- **4G Radio Access:** The mobile operator transmits the packet to the nearest 4G base station, which then transfers it over the air (by radio waves) to the friend's smartphone in Algiers.

Despite using various devices, protocols, speeds, technologies, and transmission mediums, these networks work together to offer seamless communication. We refer to these networks as **heterogeneous networks.**

When two or more heterogeneous networks are interconnected, they form an **inter-network** or a **network of networks (Internet)**

- The global network that connects several local, regional, and national networks is called the **Internet**.
- It connects billions of computing devices around the world.
- The Internet is a **global network of infrastructures**, and these infrastructures are organized in **different hierarchical levels.**





- **Backbone networks** are at the pinnacle of the Internet structure, employing extremely high-bandwidth links and powerful routers.
- **Regional or national networks** are at the intermediate level, typically handled by telecom operators such as Algérie Télécom, Ooredoo, and Mobilis.
- At the lowest level are **local networks** (access networks, such as those found in homes, businesses, universities, and other organizations.



How do these heterogeneous networks actually cooperate and communicate?

- **The network layer Internet Protocol (IP)**

3. Internet Protocol (IP)

Definition

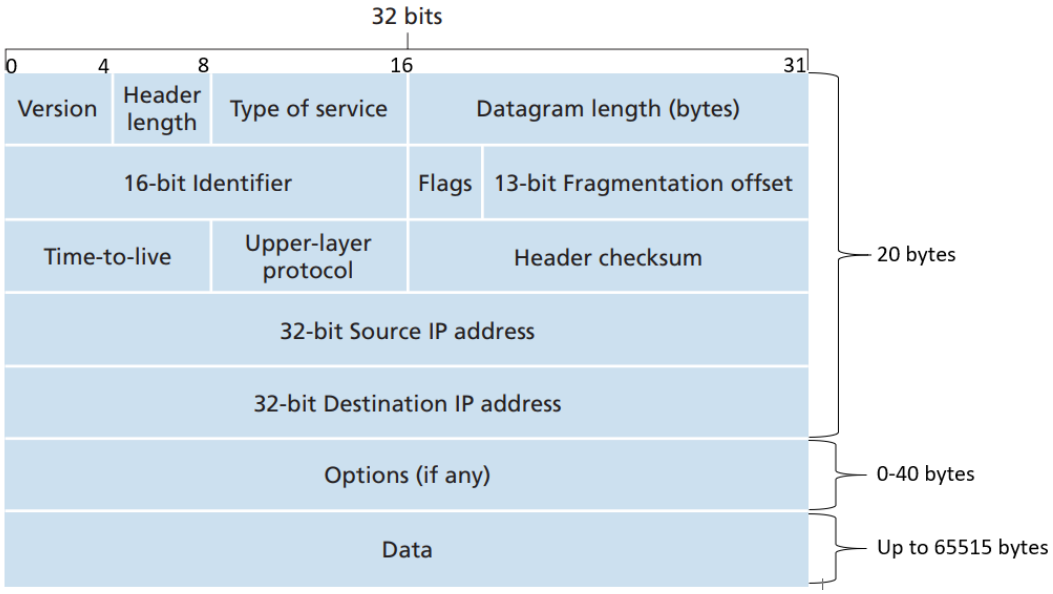
- Internet Protocol (IP), the network layer protocol, serves as the glue that holds together the whole Internet.
- It provides **logical addressing** and **best-effort delivery of packets** from their source to their destination.
- It may be described as:
  - **Connectionless:** does not establish a connection with the destination device before sending the packet. No control information needed (synchronizations, acknowledgements,. . .)
  - **Best effort:** does not guarantee reliable delivery (No guarantee of delivery, order, delay, duplication)

- **Media independent:** does not depend on the physical transmission medium type. There are two IP versions in use today: IPv4 and IPv6

- IP transmits data in small units known as **packets or datagrams,** which consist of two parts: a header field and a data field.

3.1. IPv4 Packet Header

- IPv4 is the primary and most widely used communication protocol for the network layer
- The IPv4 packet header:
  - Ensures proper packet delivery to the destination
  - Contains vital information for network layer processing in various fields Its information is used by all layer 3 devices that handle the packets
- The header consists of a fixed 20-byte part and an optional variable-length part



- **Version:** these 4 bits specify the IP protocol version of the created packet, either **IPv4** the current version or **IPv6** the new version.
- **Header length:** utilizes 4 bits to indicate the position of the payload (Data) due to the potential variable number of options included in the header.
- **Type of service:** this field allows a machine to specify the type of routing required in the form of: delay, bandwidth and reliability
- **Datagram length:** refers to the total size of the IP datagram, including both header and data, measured in bytes. The field is 16 bits long, allowing a theoretical maximum size of 65,535 bytes.
- **Identifier, flags, fragmentation offset:** represents **IP fragmentation**, which involves breaking large IP datagrams into smaller ones for independent forwarding. It includes three key fields: the 16-bit Identifier, which indicates the packet a fragment belongs to (with all fragments sharing the same value); the 3-bit Flags, which include **DF (Don't Fragment)** to prevent fragmentation and **MF (More Fragments)** to indicate that there are additional fragments; and the Fragment offset, which specifies the fragment's position in the original packet.
- **Time-to-live (TTL):** is a field in packets that prevents them from circulating indefinitely in a network. Its value decreases by one with each router processing; if it reaches zero, the router must discard the packet.
- **Protocol:** specifies the transport protocol, such as TCP or UDP, for the network layer to assign to the packet.

- **Header checksum:** serves to identify errors within the header alone. It is important to recalculate the checksum with each jump, as at least one field will have changed, specifically the lifetime, which is decremented by one.
- **Source and destination IP address:** indicate the IP address of the source and destination network interfaces.
- **Options:** allow an IP header to be extended include services not defined in the original version

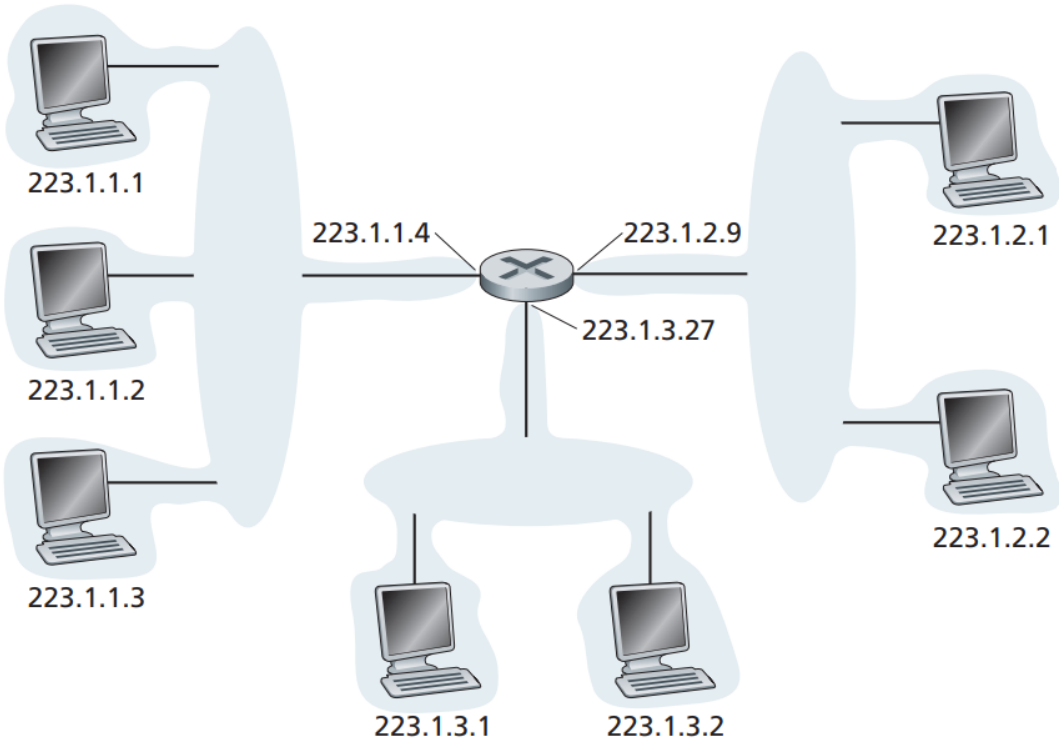
3.2. IP Address

- To uniquely identify devices on the network, **IP addresses** are needed.
- Every host and router on the Internet network has a **unique IP address**; two devices in the same network cannot have the same IP address.
- An IP address is encoded in **32 bits** and consists of two **variable-length parts,** the **network part (Network_id)** and the **host (device) part (Host_id)**.

Warning

A host typically has one network interface, whereas a router has multiple interfaces, each connected to a different network. **Each interface**, whether on a host or a router, **is assigned its own IP address**, meaning that **an IP address is specifically associated with the interface, not the host or router itself.**

Devices connected to multiple networks possess distinct IP addresses for each network, meaning **each device has a separate IP address for every network card.**



Simple Network Example with IP Addressing

- A network is a range of addresses.
- All devices within a network share the **same Network_id** while **possessing distinct Host_id.**

Definition

- The IP address is **32-bit divided** in 4 blocks of 8 bits (4 bytes), usually represented in binary form.

$$\underbrace{\underbrace{11000000}_{1^{st}\text{ byte}} . \underbrace{10101000}_{2^{nd}\text{ byte}} . \underbrace{01100100}_{3^{rd}\text{ byte}} . \underbrace{00000001}_{4^{th}\text{ byte}}}_{32\text{ bits}}$$

- IP addresses are displayed in **dotted decimal notation**, where each of the four bytes is represented in decimal form **(0 to 255)**, separated by dots.

$$\underbrace{11000000}_{192} . \underbrace{10101000}_{168} . \underbrace{01100100}_{100} . \underbrace{00000001}_{1}$$

- **Network_id:** tell us to which "network" the IP address will belong
- **Host_id:** uniquely identifies the network device

$$\underbrace{\underbrace{11000000}_{192} . \underbrace{10101000}_{168} . \underbrace{01100100}_{100}}_{\text{Network_id}} . \underbrace{\underbrace{00000001}_{1}}_{\text{Host_id}}$$

- IP addresses span from 0.0.0.0 to 255.255.255.255, with certain addresses reserved for special purposes and unavailable for general assignment.

What is the rationale behind the first 3 bytes denoting the Network_id and the final byte indicating the Host_id?

The Mask

Definition

- Also called the **Subnet Mask**
- Which bits belong to the network and which bits belong to the host
- All the bits of the **Network_id** are set to **1**.
- All the bits of the **Host_id** are set to **0**.
- Expressed in **dotted-decimal** and **prefix**

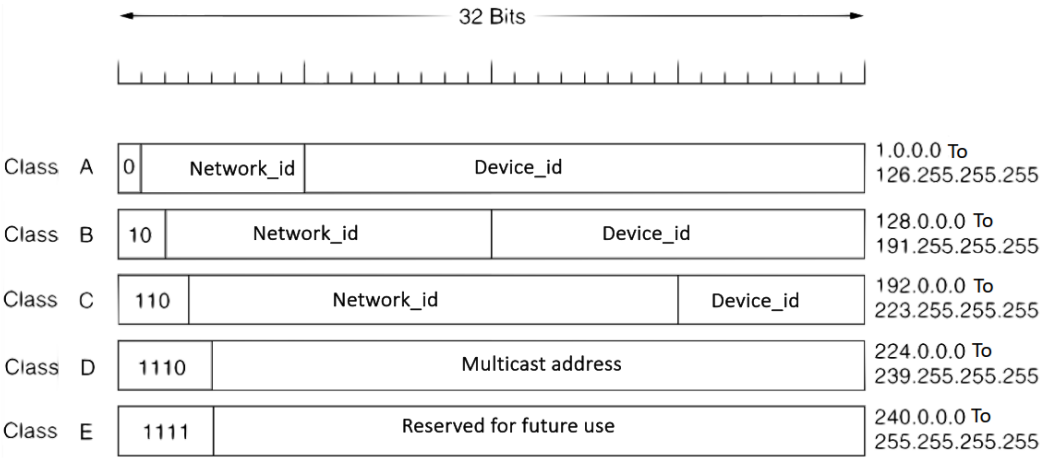
$$\text{The Host IP address: } \underbrace{192 . 168 . 100}_{\text{Network_id}} . \underbrace{1}_{\text{Host_id}}$$

$$\text{The Mask (dotted-decimal): } \underbrace{\underbrace{11111111}_{255} . \underbrace{11111111}_{255} . \underbrace{11111111}_{255}}_{\text{Network_id}} . \underbrace{\underbrace{00000000}_{0}}_{\text{Host_id}}$$

$$\text{The Mask (prefix): } /24$$

3.3. IP Address Classes

- To better understand how IP addresses are organized, they are classified into different categories known as IPv4 address classes.



- Each class of IPv4 address comes with a predefined subnet mask known as the **default mask**.
  - Class A: 255.0.0.0
  - Class B: 255.255.0.0
  - Class C: 255.255.255.0

Warning

In classful IPv4 addressing, networks were categorized into fixed classes (A, B, and C) with specific sizes, which resulted in **inefficient IP address usage** as organizations received either an excess of unused addresses or insufficient addresses for their requirements.

Method

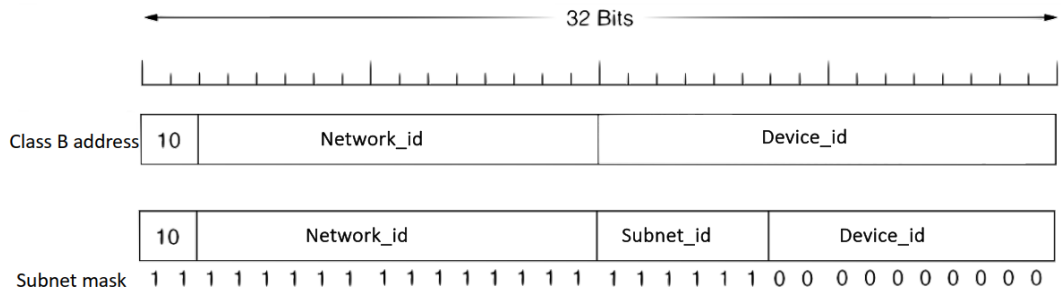
To address these limitations, a more flexible approach called **subnetting** was introduced, which allows the division of networks intosmaller, more manageables parts

3.4. IP Address Subnetting

What Is Subnetting?

Definition

- Subnetting is the process of dividing one IP block into multiple smaller logical networks without requesting new addresses from the ISP.
- An IP address with subnetting concept is formed:
  - **Network_id:** the network identifier; the number of bits varies according to the IP class.
  - **Subnet_id:** the Subnet identifier with n bits size
  - **Host_id:** is the Host identifier; the **number of HostID bits = 32 – (number of NetID bits + n)**



Note

- The creation of subnets reduces the size of routing tables. For example, a router on subnet N doesn't need to know the addresses of devices on other subnets.
- All it needs to do is perform a logical AND between the received packet address and the subnet mask in order to choose an output port.

Warning

Classful IPv4 utilized fixed default masks (A, B, C), leading to inefficient address allocation as large blocks were assigned unnecessarily. This caused rapid address depletion and poor utilization, exacerbated by the increasing size of routing tables due to the growing Internet.

Method

To mitigate address depletion and enhance Internet access for organizations, a classless addressing system termed **CIDR (Classless Inter-Domain Routing)** was implemented.

3.5. Classless Inter-Domain Routing CIDR

Classless Inter-Domain Routing — **Definition**

- An IP addressing system
- Addresses are allocated in **blocks of variable size.**
- It uses a slash (/) followed by a number to highlight the network part of an address, instead of using a subnet mask

```
a.b.c.d / n
```

- **n** = number of network prefix bits
- **32 - p** = number of host bits

```
EX: 128.7.192.0 / 19
```

- Binary representation:

$$\underbrace{10000000.00000111.110}_{\text{Network_id (19 } bits\text{)}}\underbrace{00000.00000000}_{\text{Host_id (13 } bits\text{)}}$$

4. Dynamique Routing

Which layer of the OSI model is accountable for transmitting packets to a destination when a computer delivers data to another computer on a different network?

- The Network Layer is responsible for **moving packets** from a sending host to a receiving host across multiple networks.
- It **determines the route or path taken by packets** as they flow from a sender to a receiver
- It acts as a carrier, akin to a postal service, ensuring packages are delivered from a sender to a receiver without altering their contents.
- To direct data packets across networks two important functions of the network layer can be identified: **Forwarding** and **Routing**.

Forwarding *Definition*

- Is the process by which a **router transmits a packet from one input interface to the designated output interface**.
- This action is executed quickly upon the packet's arrival at the router.
- It uses a decision-making tool, the **forwarding or routing table**, to guide its actions.
- The forwarding decision is based on **packet header information, particularly the destination address**, which helps the router identify the **correct output interface in the forwarding table.**
- In unicast routing, the router forwards packets to a single network (interface), while in multicast routing, it sends them to multiple networks (interfaces).

Routing *Definition*

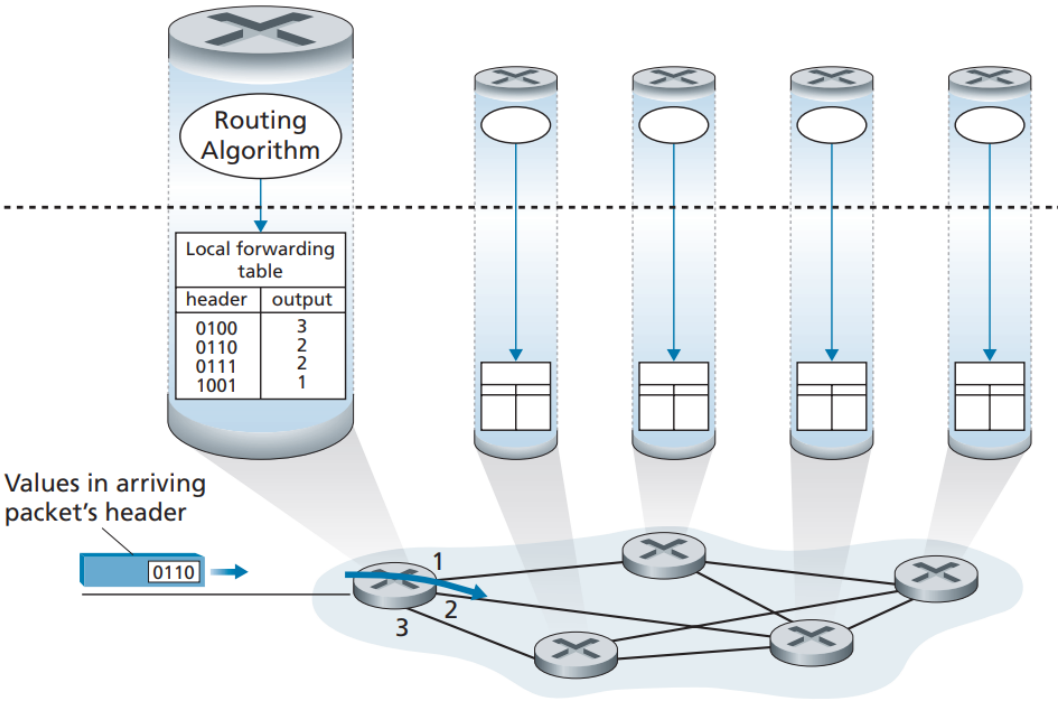
The network layer moves packets from a source to a destination across networks.

It determines the path for packet movement through a process called routing.

Routing is the process of **selecting the optimal path (best route)** between source and destination that the packet should take over the network.

Routers utilize **routing algorithms** to compute the best route.

These algorithms construct **routing tables** (or **forwarding tables**)



Warning



In network communications, a packet can traverse multiple routes from its source to its destination. The key question is how to determine the optimal route for the packet to follow?

Routing algorithms

Definition

- The routing algorithm is part of the network layer software.
- It determines the output line (interface) for transmitting incoming packets. Method employed by routers to identify the best path for packets to traverse from a source to a destination.
- The best path is the path that has the least cost
- The algorithm computed paths are utilized to create and update the routers' routing tables.
- In networks using datagrams, routing decisions are made for each packet, as routes may change.
- In networks using virtual circuits, routing decisions are made only when a new circuit is set up, allowing packets to follow an established route thereafter. Routing algorithms are categorized primarily into two classes:
    - **Non-adaptive routing algorithms :**
        - Nonadaptive algorithms make routing decisions without considering current topology or traffic conditions.
        - Routes from S to D are precomputed offline (before network starts operating) and downloaded to routers upon network boot-up
        - This process is known as static routing.

- **Adaptive routing algorithms:**
  - Routers modify their routing decisions to adapt to changes in network topology and traffic
  - To find the best route, the algorithms use a metric. This may be, for example, the distance to be covered, the number of hops or the time needed to cross the network Routers exchange routing information and dynamically update their routing tables.
  - This capability is the reason they are referred to as dynamic routing algorithms.
  - Several routing algorithms exist, including:
    - Distance-vector routing
    - Link-state routing

Distance vector routing

- Today's computer networks predominantly utilize adaptive routing algorithms (dynamic), with distance-vector routing and link-state routing being the most common types.
- The distance vector refers to the distance (vector) between neighboring nodes and the routing refers to the established route
- It is known as the distributed Bellman-Ford routing algorithm. It was the original routing algorithm for ARPANET and has been utilized in the Internet as RIP (Routing Information Protocol).
- The distance vector routing algorithm employs a separate table for each router, detailing the best-known distance and the output for each destination known as the distance vector.

Destination Network	Distance cost (metric value)	Next hop
A	0	-
B	1	B
C	∞	-

- Metrics used to measure the distance can include hop counts, transmission time, or other measurements.
- Each router is required to know the distance to its neighboring routers.
- Every Ts seconds, routers transmit their distance vector lists to all neighboring routers
- After obtaining a distance vector from each neighboring router , the router x calculates the cost to reach a destination y by applying the Bellman–Ford formula
- The router calculates the total cost for each destination through all its neighbors and selects the path with the minimum total cost.
- The routing table is updated accordingly.

Link state routing

- Proposed to overcome the limitation of Distance-Vector Routing algorithm, providing faster and more accurate routing decisions.
- Link State Routing is a routing algorithm that enables each router to build a complete map of the network topology.
- With this global view, routers can compute the shortest paths to all destinations.
- The link state reflects its characteristics, particularly the cost associated with that link.
- Links with lower costs are prioritized over those with higher costs.
- A link with a cost of ∞ is deemed broken or nonexistent

- The main steps of the Link-State routing algorithm are:

  1 Discover neighbors:

  - Each router identifies its directly connected routers.
  - This process is initiated by sending special HELLO messages on each interface.
  - The router learns the identity and addresses of its neighbors from the responses it receives.

  2 Measure link costs

  - The router evaluates the cost of the link to each neighbor.
  - Cost can signify delay, bandwidth, or another routing metric.
  - Typically, the router calculates the round-trip time (RTT) of packets and divides it by two to estimate link delay.

  3 Build Link-State Packets (LSPs)

  Each router creates a packet with collected information.

  The packet generally contains: the router ID, the list of neighboring routers, and the cost of each link

  This packet reflects the state of the router's links.

  LSPs are generated at regular intervals or in response to specific events like a line or neighbor status change.

  4 Flood the LSPs throughout the network

  - Each router uses flooding to distribute LSPs to all routers in the network.
  - Flooding guarantees that all routers acquire the same topology information.
  - Following this exchange, all routers create an identical Link-State Database (LSDB) that reflects the complete network topology

  5 Compute the shortest paths using Dijkstra's algorithm

  - Each router uses the LSDB to construct a network graph.
  - Dijkstra's shortest path algorithm is employed to determine the least-cost path to all destinations.
  - The outcome is a Shortest Path Tree (SPT), which is utilized to formulate the router's routing table

5. Quiz

Quiz

Which protocol is primarily used for inter-domain routing on the Internet?

- ○ RIP
- ○ OSPF
- ○ BGP

Quiz

Which of the following are characteristics of dynamic routing protocols?

- [ ] Automatic route updates
- [ ] Manual configuration only
- [ ] Adaptation to network changes
- [ ] No need for routing tables

Quiz

What is the main difference between RIP and OSPF?

Quiz

CIDR uses fixed network classes such as Class A, Class B, and Class C.

- ○ True
- ○ False

Quiz

Which routing protocol is based on the distance-vector algorithm?

- ○ OSPF
- ○ BGP
- ○ RIP

Quiz

Which characteristics apply to distance-vector routing protocols?

- [ ] Periodic exchange of routing tables
- [ ] Knowledge of full network topology
- [ ] se of hop count as a metric
- [ ] Slow convergence in large networks

Bibliography



- Tanenbaum, A. S., Feamster, N., Wetherall, D. J., Computer Networks, 6th Edition, Pearson,2021.
- Kurose, J. F., Ross, K. W., Computer Networking: A Top-Down Approach, 8th Edition, Pearson, 2021.
- Comer, D. E., Internetworking with TCP/IP, Volume 1: Principles, Protocols, and Architecture, 6th Edition, Pearson Education, 2014.
- Stallings, W., High-Speed Networks and Internets: Performance and Quality of Service, 2nd Edition, Prentice Hall, 2002.