CHAPTER 1: ACCESS NETWORK FUNDAMENTALS

Lesson 1.1: Introduction to Access Networks

Lesson Objectives

By the end of this lesson, learners should be able to:

- Understand what an **access network** is
- Explain the **role of access networks** in computer networking
- Identify a **wired access network architecture**
- Understand the **enterprise access layer design**
- Relate access networks to **real-world situations**

1. What Is an Access Network?

Simple Explanation

An **access network** is the part of a computer network that **connects end devices** (like computers, phones, and printers) **to the main network**.

It is the **first point of connection** for users.

Real-World Analogy

Think of a **house and a road system**:

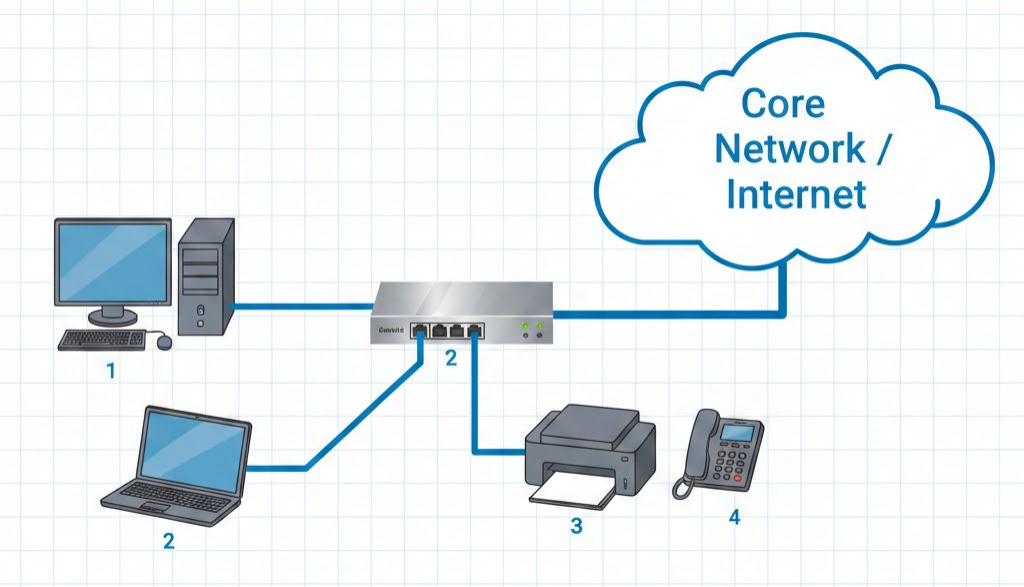
- Your **house** = computer or phone
- Your **driveway** = access network
- The **main road/highway** = larger network (internet or core network)

Without the driveway, your house cannot reach the main road.

Formal Definition (Simple)

An **access network** is the network that connects user devices to the rest of the network.

Figure 1.1: Access Network Concept



This diagram shows a **basic local area network (LAN)** connected to the **Internet**:

- **1 – Desktop computer**: A wired workstation connected to the network.
- **2 – Switch**: The central device that connects all local devices and forwards data between them.
- **2 – Laptop**: Another end device connected to the switch.
- **3 – Network printer**: Shared printer accessible by all devices on the LAN.
- **4 – IP phone**: A VoIP phone using the same network for voice communication.
- **Core Network / Internet**: Provides external connectivity (internet and other remote services).

2. Role of an Access Network

What Does an Access Network Do?

The access network:

- Connects users to the network
- Allows devices to send and receive data
- Controls who can access the network
- Provides security and organization

Examples

- Office computers connecting to a switch
- School computer lab network
- Home devices connecting to a router

Why It Is Important

Without an access network:

- Users cannot communicate
- Internet access is impossible
- Network control and security are lost

3. Wired Access Network Architecture

Simple Explanation

A **wired access network** uses **cables** (usually Ethernet cables) to connect devices.

Most offices, schools, and labs use wired access networks because they are:

- Faster
- More stable
- More secure

Main Components

- **End Devices** – PCs, printers, IP phones
- **Access Switch** – central device that connects all end devices
- **Ethernet Cables** – physical connections

Real-World Analogy

Think of a **power extension board**:

- Devices plug into the extension board
- The extension board connects them to power
- The switch does the same for network data

4. Enterprise Access Layer Design

What Is an Enterprise Network?

An **enterprise network** is a network used by:

- Companies

- Universities
- Hospitals
- Government offices

Access Layer Explained Simply

The **access layer** is the **lowest layer** of an enterprise network.

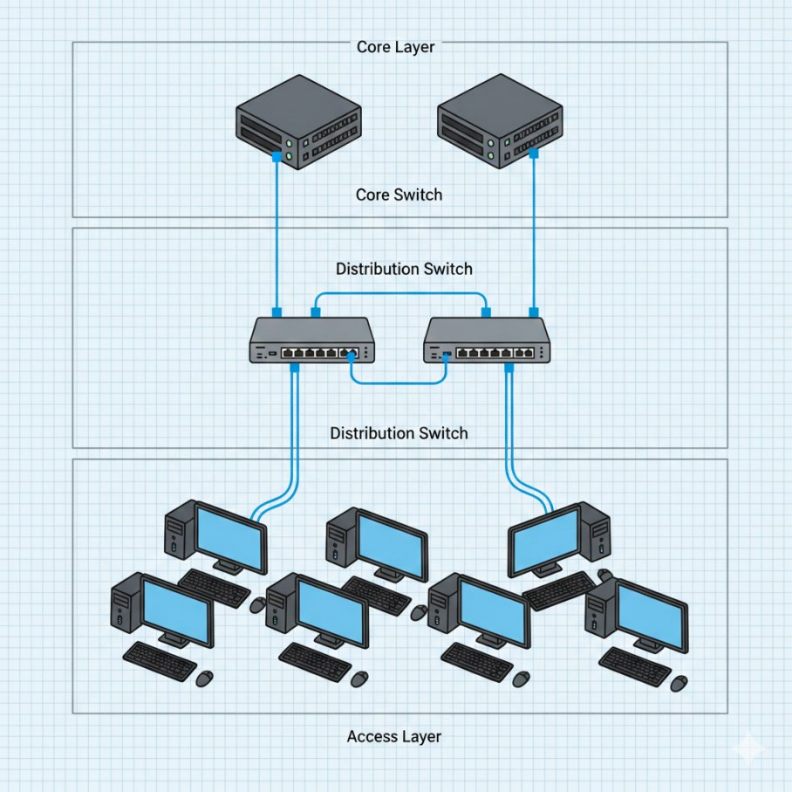
It is where:

- Users connect
- Devices are authenticated
- Basic security is applied

Typical Devices at the Access Layer

- Access switches
- Wireless access points
- IP phones

Figure 1.3: Enterprise Network Layers



Why the Access Layer Is Important

- It is the **first contact point** for users
- Problems here affect many users
- Proper design improves performance and security

5. Key Terms and Definitions

Term	Simple Definition
Access Network	Connects users to the network
End Device	A device used by a user (PC, phone, printer)
Switch	A device that connects multiple devices in a network
Ethernet Cable	Cable used for wired network connections
Access Layer	Network layer where users connect

6. Short Example

Office Scenario

- 20 employees use desktop computers
- All computers connect to one access switch
- The switch connects to the company's main network

➞ This setup is an **access network**.

7. Tools Connection

- **Cisco Packet Tracer**
  - Used to **design and simulate** access networks
- **Wireshark**
  - Used to **observe data traffic** in access networks

Lesson 1.2: Ethernet Switching Basics

Lesson Objectives

By the end of this lesson, learners should be able to:

- Understand what an **Ethernet switch** does
- Explain **MAC address learning**
- Describe **frame forwarding and filtering**
- Understand the meaning of **broadcast domains**
- Relate switching concepts to real-world examples

1. What Is Ethernet Switching?

Simple Explanation

Ethernet switching is the process of **sending data** from one device to another **inside a local network** using a **switch**.

A switch helps devices **communicate efficiently** without confusion.

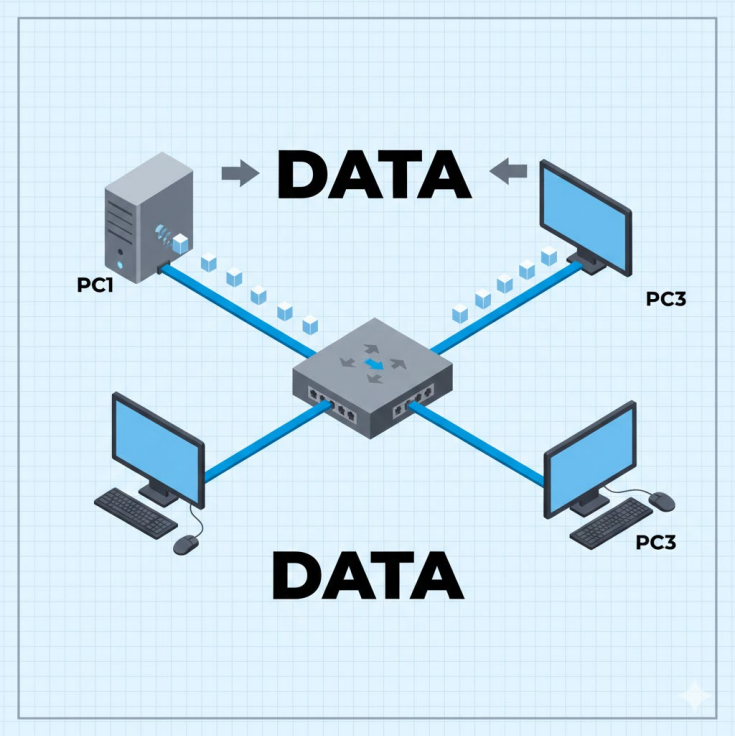
Real-World Analogy

Think of a **school mailroom**:

- Each classroom has a room number
- The mailroom reads the number on the envelope
- Mail is sent only to the correct classroom

➞ A switch does the same thing with data.

Figure 1.4: Basic Ethernet Switching



2. MAC Address Learning

What Is a MAC Address?

A **MAC address** is a **unique physical address** assigned to every network device.

- It looks like: `00:1A:2B:3C:4D:5E`
- It is **permanent** and **unique**

When a device sends data:

- The switch **reads the sender's MAC address**
- The switch **remembers** which port the device is connected to
- This information is stored in a **MAC address table**

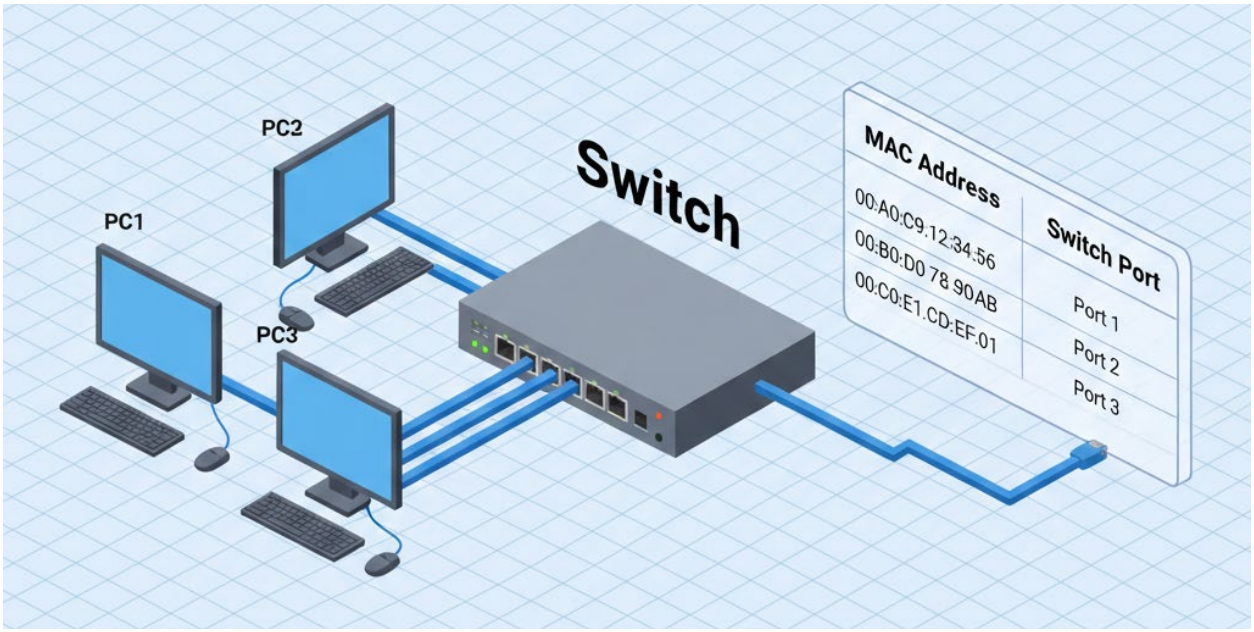
Real-World Analogy

Think of a **phone contact list**:

- Name = device
- Phone number = MAC address
- Once saved, you know who is calling

Figure 1.5: MAC Address Learning

Show a switch with a table beside it listing MAC addresses and corresponding switch ports.



Why MAC Learning Is Important

- Reduces unnecessary traffic
- Makes communication faster
- Helps the switch send data correctly

3. Frame Forwarding and Filtering

What Is a Frame?

A **frame** is a small unit of data sent over an Ethernet network.

It contains:

- Source MAC address
- Destination MAC address
- Actual data

Frame Forwarding

If the switch **knows** the destination MAC address:

- It sends the frame **only to the correct port**

Frame Filtering

If the frame is **not meant** for a port:

- The switch **does not send** it to that port

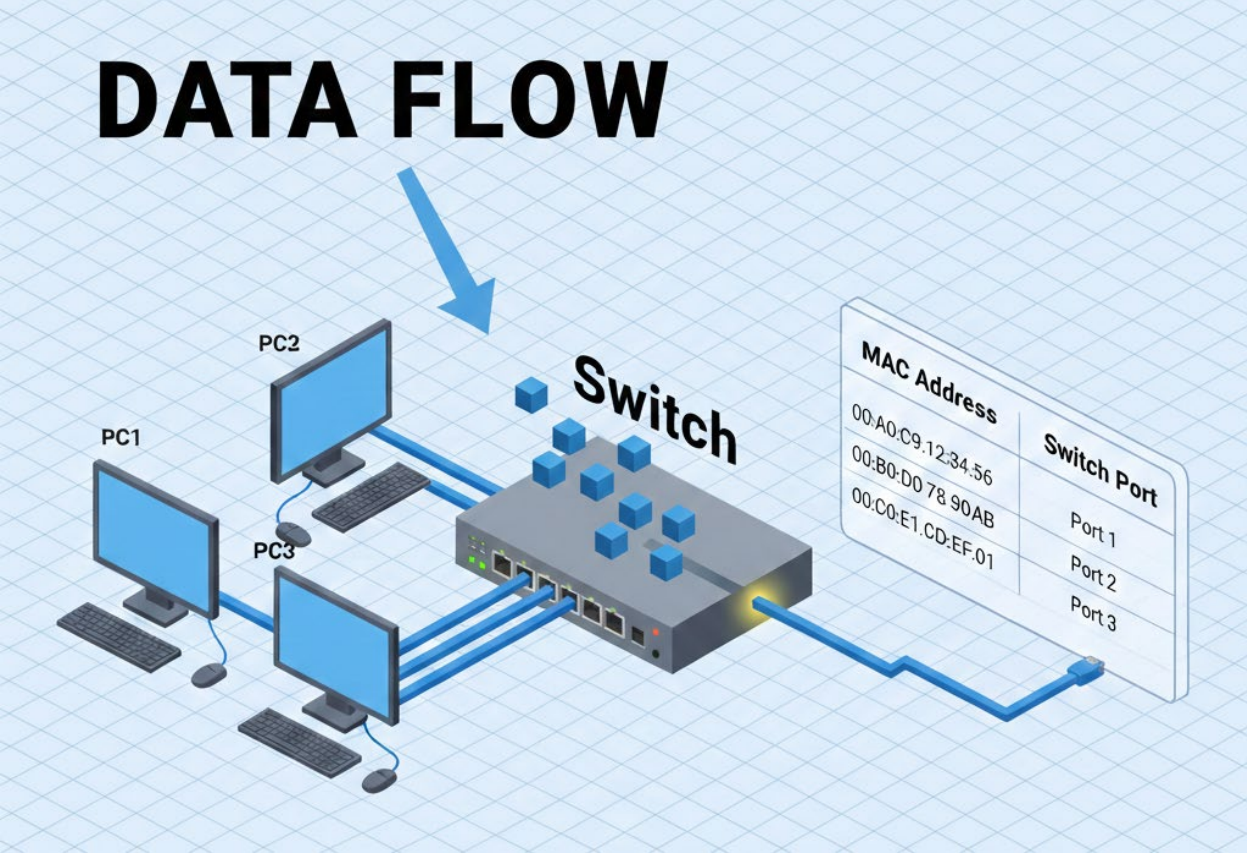
Real-World Analogy

Think of a **delivery rider**:

- If the address is known → deliver directly
- Do not visit other houses unnecessarily

Figure 1.6: Frame Forwarding and Filtering

Show one PC sending data to another. Highlight only one outgoing port from the switch.



4. Broadcast Domains

What Is a Broadcast?

A **broadcast** is a message sent to **all devices** in a network.

Example:

- “Who has this IP address?”

Broadcast Domain

A **broadcast domain** is a group of devices that **receive broadcast messages**.

Key Point

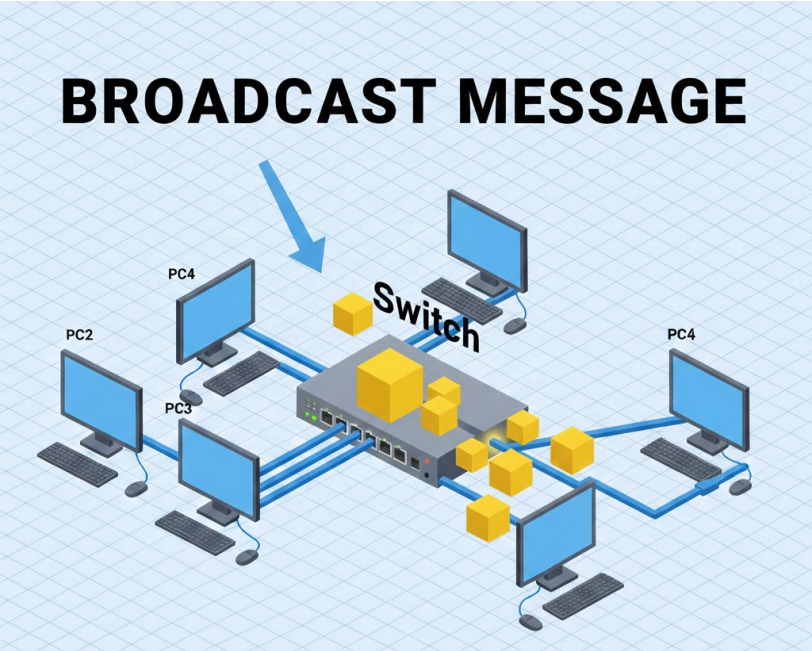
All devices connected to a switch are in the same broadcast domain by default.

Real-World Analogy

Think of a **classroom announcement**:

- Everyone in the class hears it
- Students in other classrooms do not

Figure 1.7: Broadcast Domain



Why Broadcast Domains Matter

- Too many broadcasts can slow down a network
- Networks must be divided to improve performance
- VLANs help reduce broadcast domains (next lesson)

5. Key Terms and Definitions

Term	Simple Definition
Switch	A device that connects network devices
MAC Address	Unique physical address of a device
Frame	Data unit used in Ethernet networks
Forwarding	Sending data to the correct port
Filtering	Blocking data from unnecessary ports
Broadcast	Message sent to all devices
Broadcast Domain	Area where broadcasts are received

6. Short Example

Small Office Example

- PC1 sends data to PC2
- Switch checks MAC table
- Data goes only to PC2
- Other PCs do not receive it

➞ This is **efficient Ethernet switching**

7. Tools Connection

- **Cisco Packet Tracer**
  - Visualize switches, ports, and MAC tables
- **Wireshark**
  - Capture and view Ethernet frames and broadcasts

Lesson 1.3: Virtual LANs (VLANs)

Lesson Objectives

By the end of this lesson, learners should be able to:

- Understand what a **VLAN** is
- Explain the **benefits of VLANs**
- Differentiate between **access ports** and **trunk ports**
- Understand **VLAN segmentation**
- See how VLANs improve network performance and security

1. What Is a VLAN?

Simple Explanation

A **VLAN (Virtual Local Area Network)** is a way to **divide one physical network** into **multiple logical networks**.

Even if devices are connected to the **same switch**, VLANs allow them to act as if they are on **separate networks**.

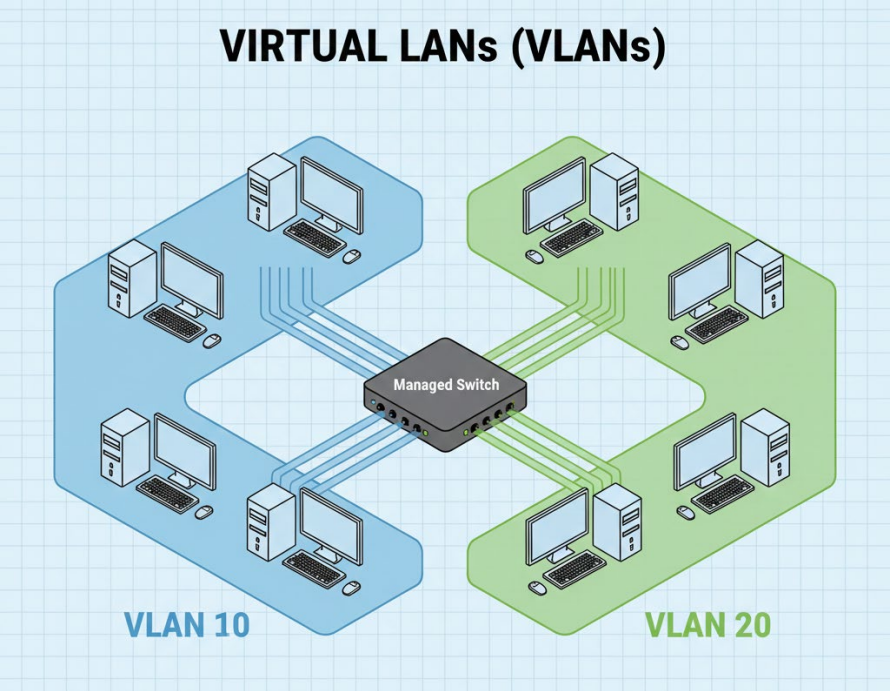
Real-World Analogy

Think of a **building with many offices**:

- Same building
- Different departments
- Each department works separately

➞ VLANs separate users **without needing new switches**.

Figure 1.8: VLAN Concept



2. Why Do We Use VLANs? (Benefits)

Main Benefits

1. **Reduce Broadcast Traffic**
   - Broadcasts stay inside the VLAN
2. **Improve Security**
   - Users in different VLANs cannot communicate directly
3. **Better Network Organization**
   - Group users by department, not location
4. **Improved Performance**
   - Less unnecessary traffic

Real-World Example

- HR department → VLAN 10
- Finance department → VLAN 20
- IT department → VLAN 30

Each department uses the **same switch** but stays **separate**.

3. Access Ports and Trunk Ports

3.1 Access Ports

Simple Explanation

An **access port** connects **end devices** (PCs, printers).

- Carries **only one VLAN**
- Common on user devices

Real-World Analogy

Think of a **single-lane road**:

- One direction
- One type of traffic

3.2 Trunk Ports

A **trunk port** connects **network devices** (switch to switch).

- Carries **multiple VLANs**
- Uses VLAN tags to separate traffic

Real-World Analogy

Think of a **multi-lane highway**:

- Many lanes
- Different types of vehicles

4. VLAN Segmentation

Simple Explanation

VLAN segmentation means **dividing users into groups** using VLANs.

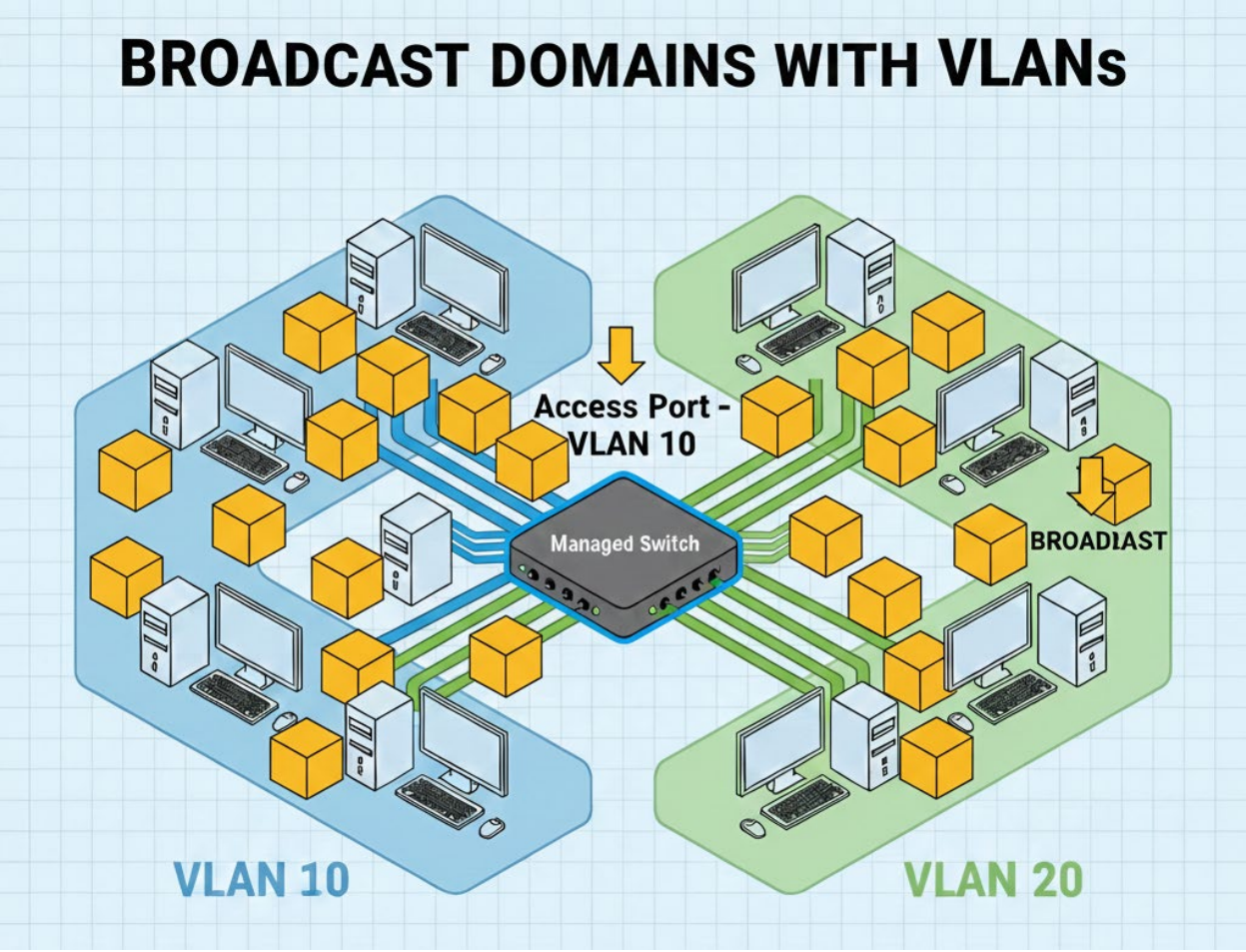
Devices in **different VLANs**:

- Do NOT receive each other's broadcasts
- Cannot communicate **unless routing is used**

Why VLAN Segmentation Is Important

- Improves security
- Reduces network congestion
- Makes troubleshooting easier

Figure 1.11: VLAN Segmentation



5. Key Terms and Definitions

Term	Simple Definition
VLAN	Logical separation of a network
VLAN ID	Number used to identify a VLAN
Access Port	Switch port for end devices
Trunk Port	Switch port carrying multiple VLANs
VLAN Segmentation	Dividing network using VLANs
Broadcast Domain	Area where broadcasts are shared

6. Short Example

Office Scenario

- One switch with 24 ports
- Ports 1–10 → VLAN 10 (HR)
- Ports 11–20 → VLAN 20 (Finance)

Even though everyone uses the same switch:

➞ HR and Finance are **logically separated**

7. Tools Connection (Conceptual)

- **Cisco Packet Tracer**
  - Create VLANs and assign ports
- **Wireshark**
  - Observe VLAN tags in frames

Mini Project 1

Design and Simulate a Small Office Access Network with VLANs

Project Objectives

By the end of this mini project, learners will be able to:

- Design a **small office access network**
- Create and configure **VLANs**
- Assign **access ports** to VLANs
- Verify VLAN isolation using **ping**
- Understand how VLANs separate traffic
- Use **Cisco Packet Tracer** confidently

Project Scenario

A small office has **two departments**:

- **HR Department**
- **Finance Department**

Both departments:

- Use the **same switch**
- Must be **logically separated** for security
- Should not communicate directly

Network Requirements

Department	VLAN ID	Devices
HR	VLAN 10	2 PCs
Finance	VLAN 20	2 PCs

Devices to Use (Packet Tracer)

- 1 × **Cisco 2960 Switch**
- 4 × **PCs**
- 4 × **Copper Straight-Through cables**

Step 1: Open Cisco Packet Tracer

1. Launch **Cisco Packet Tracer**
2. Click **File → New**

Step 2: Add Network Devices

Add a Switch

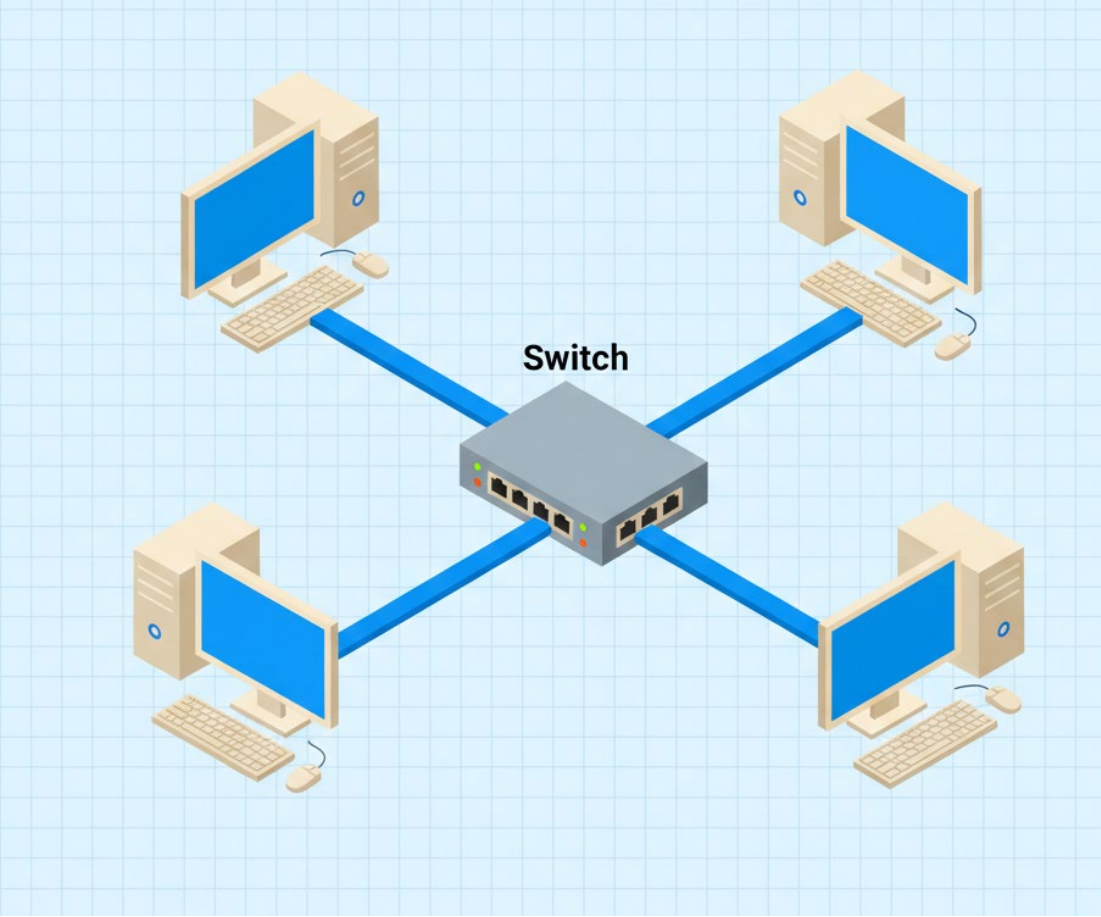
1. Click **Network Devices**
2. Click **Switches**
3. Drag **2960 Switch** to the workspace

Add PCs

1. Click **End Devices**
2. Drag **4 PCs** to the workspace
3. Rename PCs:
    - PC-HR-1
    - PC-HR-2
    - PC-FIN-1
    - PC-FIN-2

Figure MP-1: Physical Network Layout

One switch in the center with four PCs connected using Ethernet cables.



Step 3: Connect Devices

1. Select **Copper Straight-Through Cable**
2. Connect:
    - PC-HR-1 → Switch Fa0/1
    - PC-HR-2 → Switch Fa0/2
    - PC-FIN-1 → Switch Fa0/3
    - PC-FIN-2 → Switch Fa0/4

Wait until **green lights** appear.

Step 4: Configure IP Addresses

HR PCs (VLAN 10)

PC	IP Address	Subnet Mask
PC-HR-1	192.168.10.2	255.255.255.0
PC-HR-2	192.168.10.3	255.255.255.0

Finance PCs (VLAN 20)

PC	IP Address	Subnet Mask
PC-FIN-1	192.168.20.2	255.255.255.0
PC-FIN-2	192.168.20.3	255.255.255.0

How to Set IP Address

1. Click PC
2. Desktop → IP Configuration
3. Enter IP and Subnet Mask

(Leave Default Gateway empty)

Step 5: Create VLANs on the Switch

1. Click the **Switch**
2. Go to **CLI**
3. Press **Enter**

Enter Configuration Mode

```
enable
configure terminal
```

Create VLAN 10 (HR)

```
vlan 10
name HR
exit
```

Create VLAN 20 (Finance)

```
vlan 20
name FINANCE
exit
```

Step 6: Assign Access Ports to VLANs

Assign HR Ports (Fa0/1–Fa0/2)

```
interface range fa0/1 - 2
switchport mode access
switchport access vlan 10
exit
```

Assign Finance Ports (Fa0/3–Fa0/4)

```
interface range fa0/3 - 4
switchport mode access
switchport access vlan 20
exit
```

Step 7: Verify VLAN Configuration

Check VLANs

```
show vlan brief
```

You should see:

- Fa0/1–Fa0/2 → VLAN 10
- Fa0/3–Fa0/4 → VLAN 20

Step 8: Test Network Connectivity

Test Same VLAN Communication

1. Open **PC-HR-1**
2. Command Prompt:

```
ping 192.168.10.3
```

✔ Ping **SUCCESS**

Test Different VLAN Communication

From **PC-HR-1**:

```
ping 192.168.20.2
```

✖ Ping **FAILS**

➡ This proves VLAN isolation is working.

Step 9: Observe Traffic Conceptually

- Switch to **Simulation Mode**
- Send a ping
- Observe traffic staying **within the VLAN**