People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Ibn Khaldoun University of Tiaret - Algeria
Faculty of Mathematics and Computer Sciences,
Department of Computer Sciences

---------- * ----------

Operator Network Technologies

---- Course ----

Addressed to :

1st Year Master's Degree-Networks and Telecommunications

Prepared by :

Dr. KHERICI Cheikh.

Examined by :

1. **Dr. MERATI Medjeded** – Ibn Khaldoun University of Tiaret.
2. **Pr.** KHALFI Mohammed Fethi– Djillali Liabès University of Sidi Bel Abbes.

Academic year : 2025 – 2026.

A propos :

Operator networks today constitute the critical infrastructure upon which the global digital economy depends. From high-speed Internet access to 5G mobile services, including FR, ATM, MPLS networks, optical transport, and network function virtualization, these complex architectures ensure connectivity for billions of users and connected devices.

This course handout, entitled "Operator Network Technologies," has been designed for 1st year Master's students in Networks and Telecommunications, as well as for future Telecommunications engineers seeking to acquire an in-depth understanding of the technologies used in modern operator networks. It aims to provide both the essential theoretical foundations and a practical perspective on architectures, protocols, and performance mechanisms.

This document covers in particular :

- The hierarchical architecture of operator networks (Access, Aggregation, Core)
- Wide Area Network (WAN) technologies: X.25, FR, ATM, IP/MPLS, and operator VPNs
- Routing protocols (OSPF, IS-IS, BGP)
- Access network technologies :
    - Wired local loop topology.
    - The concept of NRA/NRO.
    - Points of mutualization.
    - Connection to the aggregation (collection) network.

Special attention is given to analytical aspects and dimensioning mechanisms, enabling students to understand not only how these technologies operate, but also the performance, reliability, and scalability constraints specific to operator environments.

Each chapter is structured progressively, incorporating:

- Theoretical reminders.
- Explanatory diagrams.
- Detailed examples.
- Advanced-level solved exercises.
- Mathematical analyses where necessary.

The primary objective of this course handout is to bridge the gap between traditional academic knowledge of computer networks and the reality of large-scale operator infrastructures.

We hope that this material will serve as an effective pedagogical tool, promoting both scientific rigor and a practical understanding of the technologies shaping modern networks.

Table of Contents

Chapter I : Wide Area Networks WAN.

1. Definition of WANs 8
2. Positioning of WANs within the overall architecture 8
3. Historical evolution of WAN technologies 9
4. Fundamental Characteristics of WANs 9
5. General Architecture of a WAN 10
6. Types of WAN connections 11
7. Performance parameters of a WAN 12
8. Equipment and devices of WAN networks 13
9. Types of circuits 17
   9.1. Point-to-point circuit (P2P) : 17
   9.2. Virtual circuit : 18
10. Network topology 19
11. WAN connection options 23
   11.1. Private WAN Infrastructure : 24
   11.2. Public WAN Infrastructure : 24
12. Security in WANs 24
13. Conclusion 25
14. Quiz 25
1. Introduction 28
2. HDLC Protocol 29
   2.1. Characteristics of HDLC : 29
   2.2. HDLC frame structure 30
   2.3. HDLC Operation : 33
   2.4. HDLC configuration in Cisco Packet Tracer : 36
   2.5. Different Versions of the HDLC Protocol : 36
3. Conclusion : 37
4. Exercise to do : 37
1. Introduction 40
2. PPP Protocol 40
   2.1. Definition 40
3. Conclusion 43
4. Quiz 43

Chapter II : Protocols : X.25 an Frame Relay.

1. Introduction 47
2. Definition 47
1. Switched Virtual Circuit (SVC) 53
2. Permanent Virtual Circuit (PVC) 53
3. Advantages of X.25 networks : 57
4. Main uses of X.25 networks : 57
5. X.25 in a few figures : 58
6. Example of X.25 configuration in Cisco Packet Tracer : 58
7. Conclusion 58
8. Exercise to be done : 59
1. Introduction 62
2. Definition 62
3. Functioning 63
4. Different Frame Relay topologies 64
5. Advantages 66
6. Virtual Circuits 66
7. Data-Link Connection Identifier (DLCI) 68
8. Local Management Interface (LMI) 68
10. DLCI Addressing 71
11. Frame Relay in a few figures 74
12. Conclusion 75
13. Quiz with solution 75

Chapter III : ATM Networks and MPLS Protocol.

1. Introduction 79
2. Definition 79
3. ATM Cells 79
4. Addressing in ATM Networks 80
5. Types of Links 83
6. Layered Architecture 83
7. ATM Model 84
8. Components of ATM 86
1. UNI (User-to-Network Interface) 87
2. NNI (Node-to-Node Interface) 88

3. NNI Format of ATM Cell....88
4. UNI Format of ATM Cell....89
5. Example of congestion....90
9. Classes of Service (CoS)....92
10. Advantages....93
11. Conclusion....93
12. Exercise....93
1. Introduction....96
2. Definition....96
3. MPLS Objectives....97
4. MPLS Labels....97
5. MPLS Devices....98
6. Label processing....101
7. Label Distribution....101
8. MPLS Operations....102
9. MPLS Principles....103
10. Routing....104
10.1. Implicit Routing LDP....104
10.2. Explicit Routing....106
11. MPLS-L2 VPN....107
12. MPLS-L3VPN....109
13. MPLS/TE (Traffic Engineering)....110
14. Applications....111
15. Conclusion....112
17. Exercise with solution....112
Chapter IV : Access Network Technologies.
1. Introduction....116
2. Definition....116
3. Local loop technologies....116
3.1. FTTx Technologies....117
3.2. High-Speed Access Networks....117
3.3. Telephone Local Loop....119
3.4. Optical Local Loop....119
4. NRA/NRO....120

4.1. NRA core of ADSL network 120
4.2. Optical Connection Node (NRO) 122
5. Distribution Point (PM) in FTTH Networks 124
5.1. Introduction 124
5.2. Definition 124
6. Backhaul Network Connection 126
6.1. Introduction 126
6.2. Definition 127
6.3. Role in FTTH Architecture 127
6.4. Main Components of the Aggregation Connection 127
6.5. Topology of the Aggregation Network 128
6.8. Quality of Service (QoS) 128
6.9. Advantages of a Well-Designed Aggregation Network 129
7. Conclusion 129
8. Exercises 130
Bibliographie 132

Chapter I

Wide Area Networks WAN

Unit 1 : Introduction to Wide Area Networks (WANs).

Chapter Objectives :

- At the end of this chapter, the student will be able to:
- Define a Wide Area Network (WAN) and distinguish it from a LAN.
- Identify the main historical and modern WAN technologies.
- Understand WAN architectures and topologies.
- Analyze the performance parameters of a Wide Area Network.
- Place WANs within the context of service provider networks.

Topics Covered :

- Definition of WANs.
- Difference between LAN / MAN / WAN.
- WAN architectures.
- Main WAN technologies.
- Components of a WAN.
- WAN protocols.
- Transmission modes.

1. Definition of WANs

A Wide Area Network (WAN) is a telecommunications infrastructure that enables the interconnection of local area networks (LANs) or remote devices over large geographical areas (city, country, continent, or worldwide).

Unlike local area networks :

- A WAN covers large distances.
- It generally relies on service provider infrastructures.
- It involves long-distance transmission technologies.
- It introduces greater constraints in terms of latency and reliability.

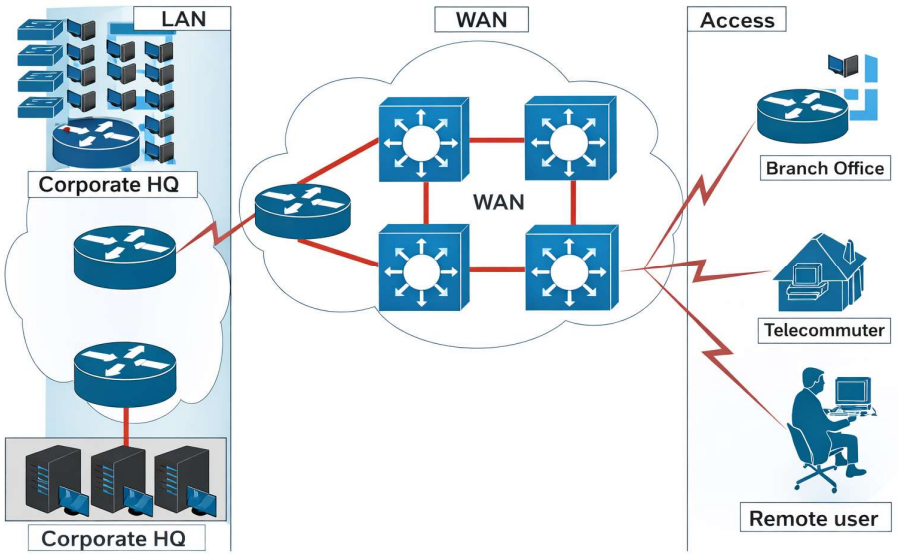


Fig.1 : WAN Network Architecture.

2. Positioning of WANs within the overall architecture

WANs (Wide Area Networks) are positioned as the overarching connectivity layer that links geographically dispersed Local Area Networks (LANs) such as branches, data centers, and cloud resources together. Operating at the edge of organizational networks, they span large distances (cities, countries, or globally), utilizing service provider infrastructure.

Key Aspects of WAN Positioning in Architecture :

- **Inter-site Connectivity:** WANs sit between LANs, bridging disparate locations (e.g., corporate HQ to branch offices).

- **Edge Router Positioning:** WAN connections typically terminate on edge routers (or SD-WAN appliances) at the network perimeter, separating the internal LAN infrastructure from the external service provider network.
- **Multi-layer Hierarchy:** They reside "above" the LAN within the network architecture, facilitating communication across large distances. This includes traditional private links (MPLS) or public internet links to connect, manage, and secure data flow.
- **Hybrid Architecture:** Modern WAN architecture increasingly blends traditional corporate WANs with cloud-connected internet to optimize traffic to both centralized data centers and SaaS applications.

WANs ensure that LAN traffic can securely and efficiently reach remote locations, acting as the bridge for data exchange and resource sharing on a wide scale.

Example of inter-site interconnection :

Site A (Algiers) ——— WAN ——— Site B (Paris)

3. Historical evolution of WAN technologies

Wide Area Network technologies have evolved from 1950s military analog, leased-line systems to modern, software-defined, cloud-based architectures. The journey progressed through packet switching (1970s), Frame Relay (1990s), and MPLS (2000s), shifting from rigid, expensive dedicated circuits to flexible, cost-effective SD-WAN that optimizes network performance across varied, secure transport links.

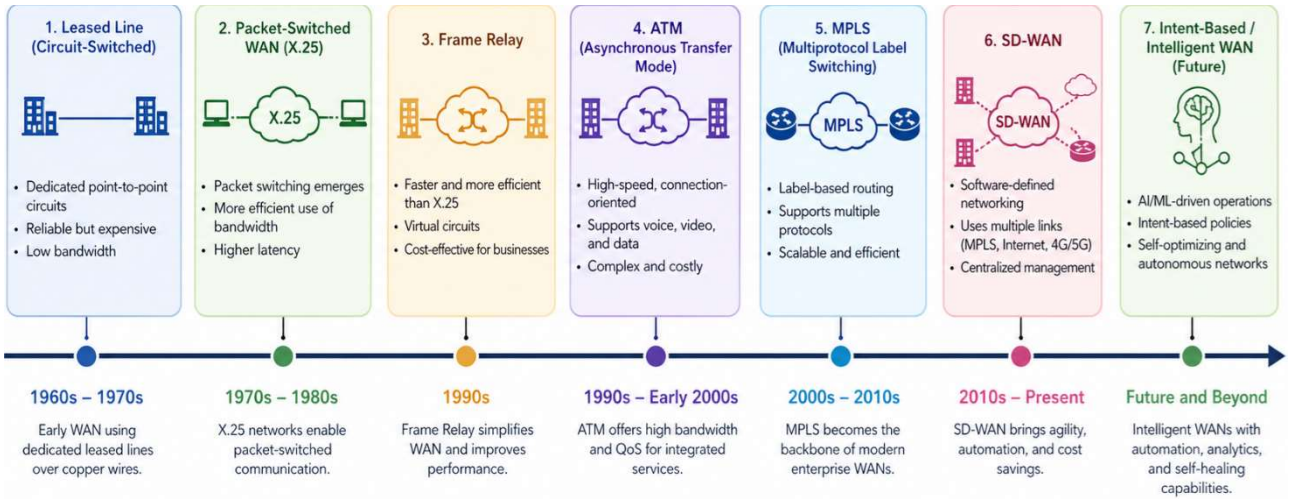


Fig.2 : Evolution of WAN technologies.

4. Fundamental Characteristics of WANs

Wide Area Networks (WANs) are characterized by their ability to cover large geographic areas, connecting devices and networks across cities, countries, or even

continents. They rely on a combination of public and private infrastructure, such as leased lines, satellites, and the Internet, to enable communication between distant locations. Compared to Local Area Networks (LANs), WANs generally have lower data transfer rates and higher latency due to the long distances involved. They also require complex management systems, including advanced routing and monitoring tools, to ensure efficient operation. To maintain reliability, WANs often incorporate redundancy and failover mechanisms. Additionally, they support a variety of technologies, such as MPLS, SD-WAN, VPNs, and older systems like Frame Relay and ATM. Finally, WANs tend to be more costly to deploy and maintain, largely due to their dependence on service providers and extensive infrastructure.

5. General Architecture of a WAN

A Wide Area Network (WAN) connects multiple Local Area Networks (LANs) across large geographic areas using service provider infrastructure.

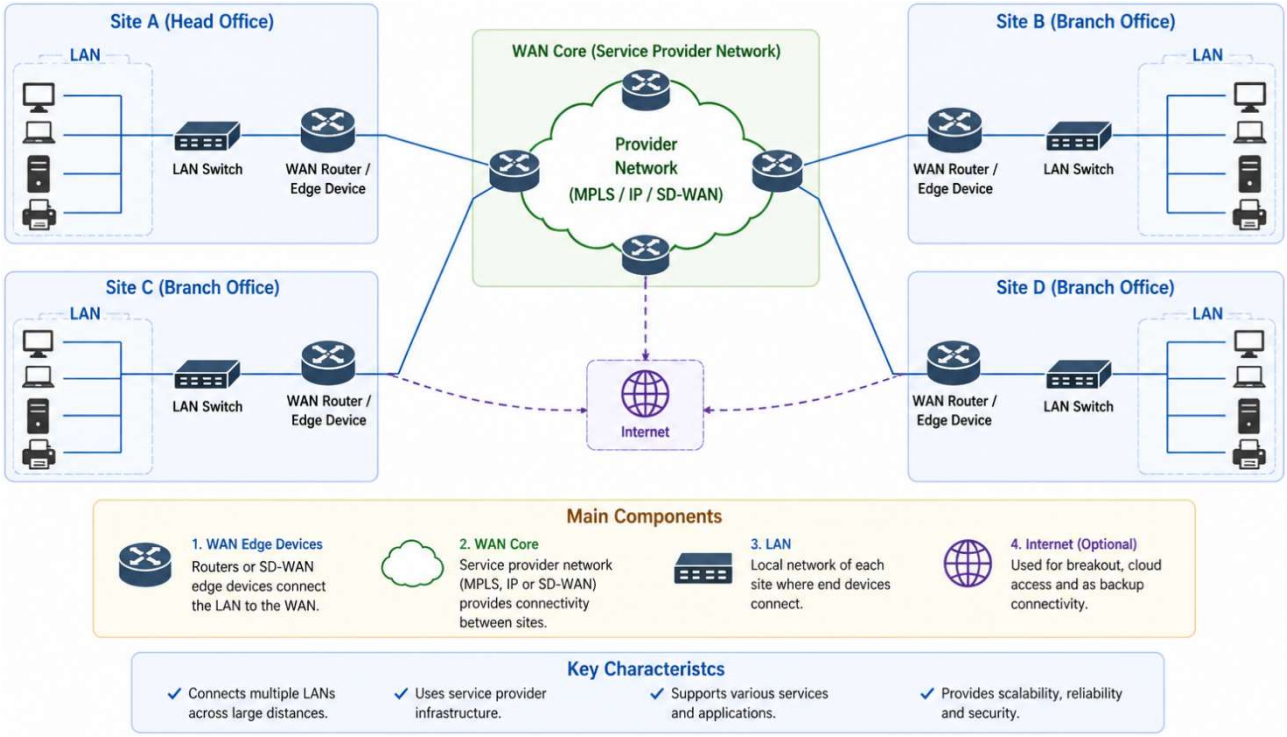


Fig.3 : General Architecture of a WAN.

Main Components :

1. **LAN (Local Area Network)**
   - Internal network within a site (office, campus, branch).
   - Includes devices like PCs, servers, printers, and switches.
2. **WAN Edge Devices (Routers / SD-WAN Devices)**
   - Connect the local LAN to the WAN.
   - Responsible for routing, security, and traffic management.
3. **WAN Core (Service Provider Network)**
   - The backbone that interconnects sites.

- Technologies used: MPLS, IP, SD-WAN.
- Managed by telecom/service providers.

4. **Communication Links**
   - Physical or wireless connections (fiber, leased lines, 4G/5G, satellite).
5. **Internet (Optional)**
   - Used for cloud access, backup links, or hybrid WAN designs.

How It Works :

- Each site has a LAN connected to a WAN router.
- Routers send traffic into the WAN core network.
- The provider network routes data between distant sites.
- Traffic reaches the destination site and is delivered to its LAN.

Key Characteristics :

- Covers large geographic areas.
- Connects multiple remote locations.
- Scalable and flexible.
- Supports multiple services (voice, data, video).
- Can be private (MPLS) or public (Internet-based).

6. Types of WAN connections

6.1 Leased Lines

- Dedicated point-to-point connection.
- Guaranteed bandwidth.
- High reliability.
- High cost.

6.2 Packet-Switched Networks

- **X.25**
  - Connection-oriented.
  - Strong error control.
- **Frame Relay**
  - Simplification of X.25.
  - Reduced overhead.
- **ATM**
  - Transmission in fixed-size cells (53 bytes).
  - Advanced QoS support.
- **MPLS**
  - Label switching.

- Support for carrier (provider) VPNs.
- Traffic engineering.

6.3 Internet with VPN

- Use of the public network.
- IPsec tunnel.
- Reduced cost.
- Fewer performance guarantees.

6.4 SD-WAN (Software Defined WAN)

- Software overlay.
- Multi-link connectivity (MPLS + Internet + 4G/5G).
- Dynamic path selection.

7. Performance parameters of a WAN

7.1 Bandwidth

Bandwidth in a WAN refers to the maximum amount of data that can be transmitted over a network link in a given period of time. It is typically measured in bits per second (bps), such as Mbps (Megabits per second) or Gbps (Gigabits per second).

7.2 Latency

Latency in a WAN refers to the time delay it takes for data to travel from the source to the destination across the network. It is usually measured in milliseconds (ms) and represents how quickly a packet moves through the network. In simple terms, latency is the waiting time between sending a request and receiving a response.

In WAN networks, latency can be affected by several factors :

- ✓ Distance between locations (longer distance = higher latency).
- ✓ Transmission medium (fiber, satellite, etc.).
- ✓ Network congestion.
- ✓ Routing and switching delays.

Note well : Low latency means faster communication (better performance), while high latency can cause delays, lag, or poor user experience especially for real-time applications like video calls or online gaming.

$$\text{Latency} = \frac{\text{Distance}}{\text{Propagation Speed}}$$

Total Latency = Propagation Delay + Transmission Delay + Processing Delay + Queuing Delay

7.3 Jitter

Jitter in a network refers to the variation in the delay (latency) of data packets over time. Instead of packets arriving at a constant, steady rate, jitter occurs when they arrive irregularly some faster, some slower than expected.

In WAN networks, jitter is mainly caused by:

- ✓ Network congestion.
- ✓ Route changes.
- ✓ Packet queuing variations.

High jitter can lead to poor quality in real-time applications such as VoIP calls, video conferencing, and online streaming, causing effects like audio distortion, delays, or interruptions.

7.4 Bit Error Rate (BER)

The ratio of the number of bits received in error to the total number of bits transmitted over a given period of time.

$$\text{BER} = \frac{\text{Number of erroneous bits}}{\text{Total number of transmitted bits}}$$

7.5 Availability

The ability of the network to remain operational, accessible, and usable over time, with minimal downtime.

- ➢ **Key points :**
  - ✓ Expressed as a percentage (e.g., 99.9%, 99.99% uptime)
  - ✓ Depends on factors like:
    - o Redundancy (backup links, failover systems).
    - o Network design.
    - o Hardware/software reliability.
    - o Maintenance and monitoring.
  - ✓ High availability means very little interruption, even in case of failures.
- ➢ **Example :**

A WAN with 99.99% availability allows only about 52 minutes of downtime per year.

Availability = how often your WAN is working and accessible when needed.

8. Equipment and devices of WAN networks

Equipment and devices of WAN networks refer to the hardware components used to establish, manage, and maintain communication over large geographic areas. These devices enable data transmission between different locations, such as cities, countries, or continents.

They include networking hardware responsible for routing, switching, security, and connectivity across long distances. Common examples are routers, modems, switches, multiplexers, firewalls, and WAN optimization devices.

In essence, WAN equipment ensures reliable, efficient, and secure data exchange between remote networks and users.

8.1. Routing and Traffic Management Devices

- **Routers**
  - ✓ Core devices in WANs.
  - ✓ Direct data packets between different networks (LAN ↔ WAN ↔ Internet).
  - ✓ Use routing protocols (e.g., OSPF, BGP) to choose the best path.
  - ✓ Example : Connecting a company's branch offices across cities.
- **Layer 3 Switches**
  - ✓ Combine switching and routing functions.
  - ✓ Used in large enterprise WANs for efficient internal routing.

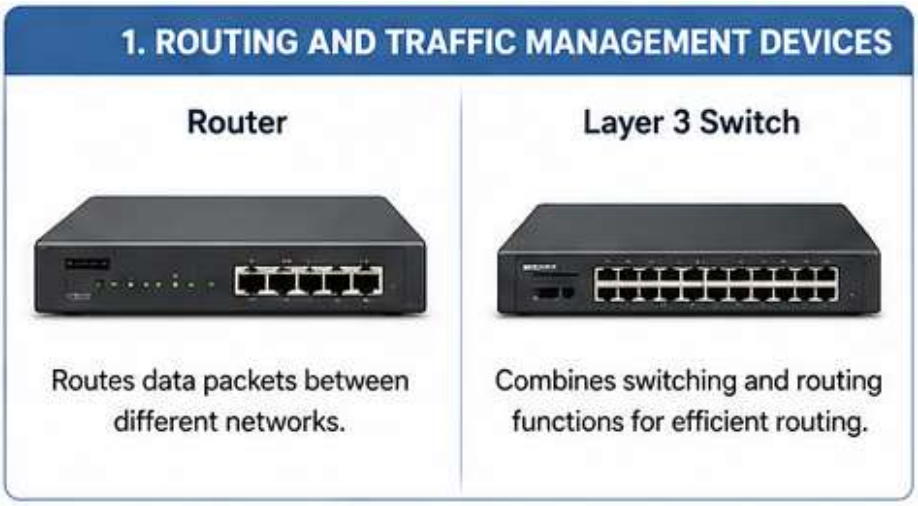


Fig.4 : Routing and Traffic Management Devices.

8.2. Communication and Access Devices

- **Modems (Modulator-Demodulator)**
  - ✓ Convert digital signals to analog (and vice versa).
  - ✓ Used in DSL, cable, or older WAN connections.
  - ✓ Enable communication over telephone or cable lines.
- **CSU/DSU (Channel Service Unit / Data Service Unit)**
  - ✓ Interface between routers and digital WAN lines (like leased lines).
  - ✓ Ensures proper signal formatting and transmission.
- **Access Servers**
  - ✓ Provide remote users access to the WAN.
  - ✓ Often used for VPN or dial-in connections.



Fig.5 : Communication and Access Devices.

8.3. Switching and Data Transport Devices

- **Multiplexers (MUX)**
  - ✓ Combine multiple signals into one transmission channel.
  - ✓ Improve bandwidth efficiency.
  - ✓ Types: TDM (Time Division Multiplexing), FDM (Frequency Division).
- **WAN Switches**
  - ✓ Used in technologies like Frame Relay, ATM, MPLS.
  - ✓ Forward data based on virtual circuits or labels instead of MAC addresses.

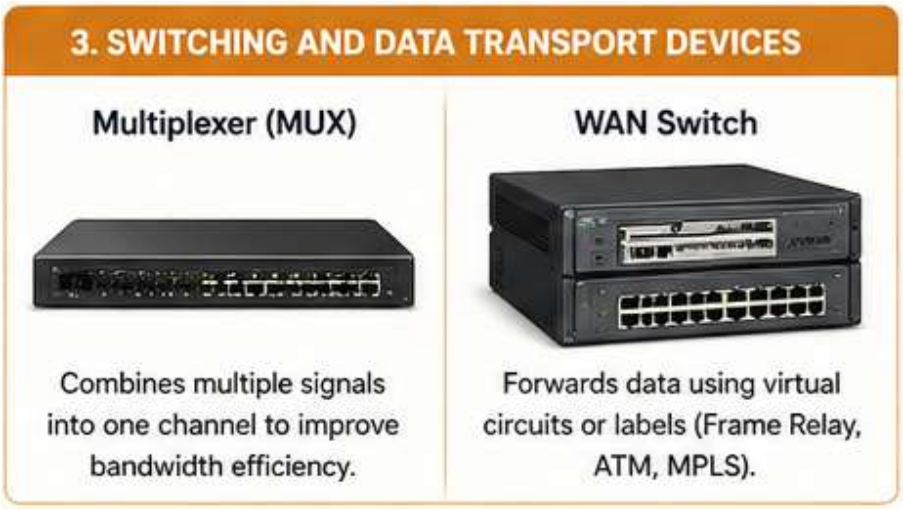


Fig.6 : Switching and Data Transport Devices.

8.4. Security Devices

- **Firewalls**
  - ✓ Protect WAN networks from unauthorized access.
  - ✓ Filter traffic based on rules (IP, ports, protocols).
- **VPN Gateways**
  - ✓ Create secure tunnels over public networks (Internet).

- ✓ Encrypt data between remote sites or users.

➢ **Intrusion Detection/Prevention Systems (IDS/IPS)**

- ✓ Monitor network traffic for suspicious activity.
- ✓ Prevent cyberattacks in real time.



Fig.7 : Security Devices.

8.5. Optimization and Performance Devices

➢ **WAN Optimization Controllers (WOC)**

- ✓ Improve WAN performance.
- ✓ Reduce latency and bandwidth usage.
- ✓ Use techniques like compression, caching, and traffic shaping.

➢ **Load Balancers**

- ✓ Distribute network traffic across multiple links or servers.
- ✓ Improve availability and performance.



Fig.8 : Optimization and Performance Devices.

8.6. Transmission Media and Interfaces

➢ **Network Interface Cards (NICs)**

- ✓ Enable devices to connect to WAN links.

➢ **Transmission Media**

- ✓ Fiber optic cables (high speed, long distance)
- ✓ Satellite links (remote areas)
- ✓ Microwave links (wireless WAN)

- ✓ Copper lines (DSL, legacy systems)

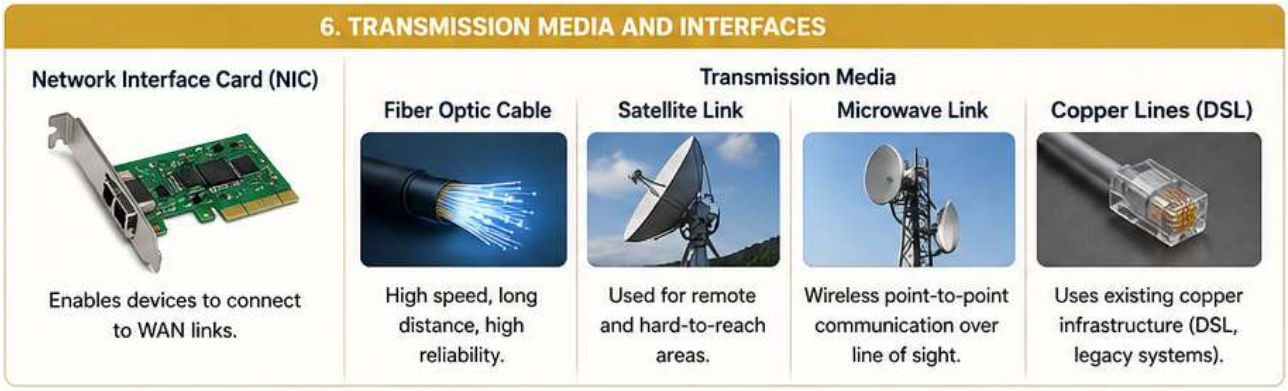


Fig.9 : Transmission Media and Interfaces.

8.7. Modern WAN Devices

- ➢ **SD-WAN Appliances**
  - ✓ Software-defined WAN devices.
  - ✓ Centralized control of network traffic.
  - ✓ Use multiple connections (Internet, LTE, MPLS).
  - ✓ Improve flexibility and reduce cost.
- ➢ **Edge Devices**
  - ✓ Located at the boundary of networks.
  - ✓ Connect local networks to WAN services (cloud, internet).

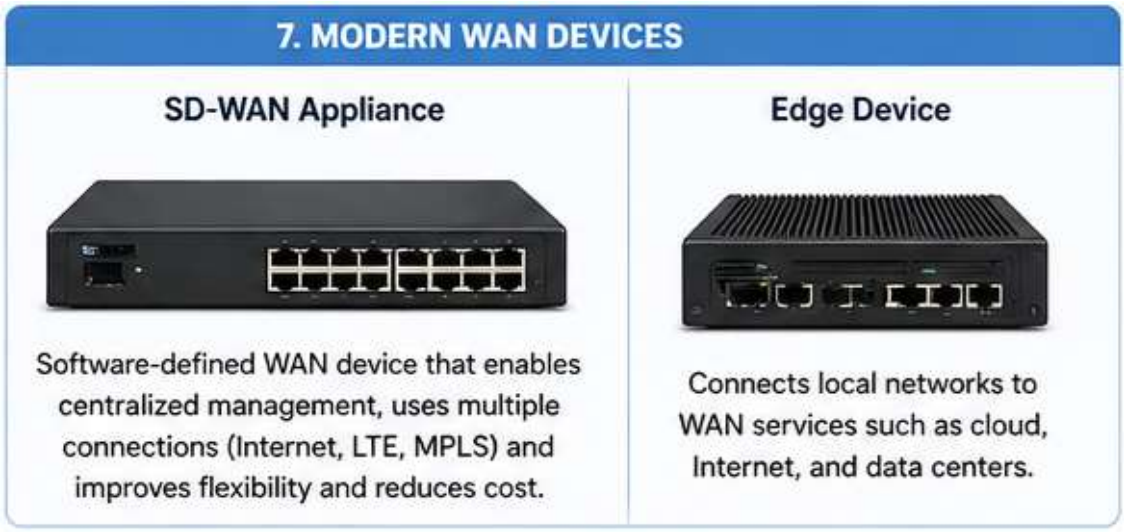


Fig.10 : Modern WAN Devices.

9. Types of circuits

9.1. Point-to-point circuit (P2P) :

A point-to-point circuit in a WAN is a dedicated communication link that directly connects two locations or devices without sharing the connection with others.
In simple terms, it is a private line between two endpoints.

Key characteristics:

- **Dedicated connection:** The entire bandwidth is reserved for the two connected sites.
- **Reliable and secure:** Since no other users share the link, performance is consistent and data is more secure.
- **Fixed path:** Data travels along a single, predefined route.
- **Higher cost:** Typically more expensive than shared network solutions because the infrastructure is reserved exclusively.



Fig.11 : A point-to-point ISDN circuit.

Characteristics :

- Expensive.
- Better quality of service (2 Mb/s) compared to older 56 kb/s modems.

9.2. Virtual circuit :

A virtual circuit in WAN (Wide Area Network) is a logical connection established between two devices, even though the data may travel through multiple physical paths in the network.

Unlike a dedicated physical circuit, a virtual circuit:

- Does not use a fixed physical path.
- Is created by the network using packet-switching technologies (Frame Relay, ATM, or X.25).
- Appears to the user as a continuous, dedicated connection.

Key points :

- Data packets follow a predefined logical path.
- Packets usually arrive in order.
- The network maintains state information about the connection.
- It is more efficient and cost-effective than leased lines.

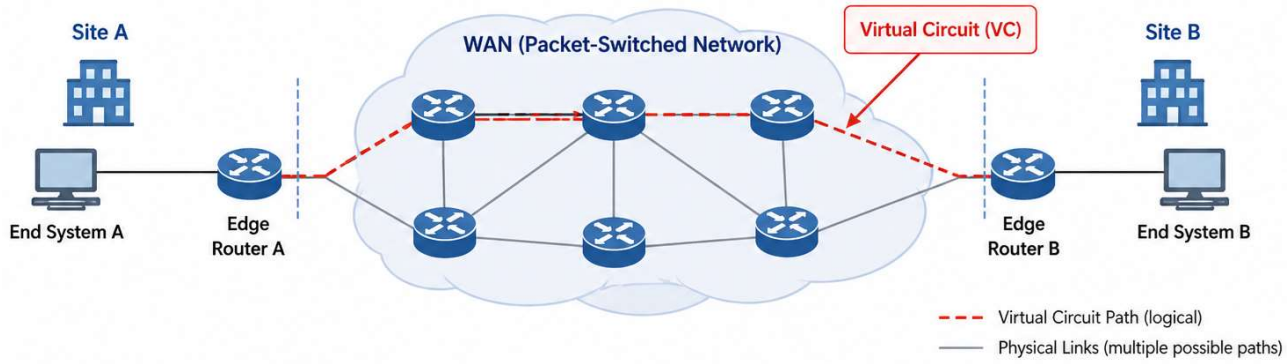


Fig.12 : Virtual circuit (VC).

10. Network topology

Network topology refers to the physical or logical arrangement of devices (nodes) and connections (links) in a network. It describes how computers, routers, and other devices are interconnected and how data flows between them. Topology plays an important role in determining the performance, reliability, and scalability of a network.

10.1. Bus Topology

In a bus topology, all devices are connected to a single central cable called the backbone. Data is transmitted along this cable, and all devices receive the signal, but only the intended device processes it.

- Simple and inexpensive to install
- Requires less cable.
- However, if the backbone fails, the entire network stops.

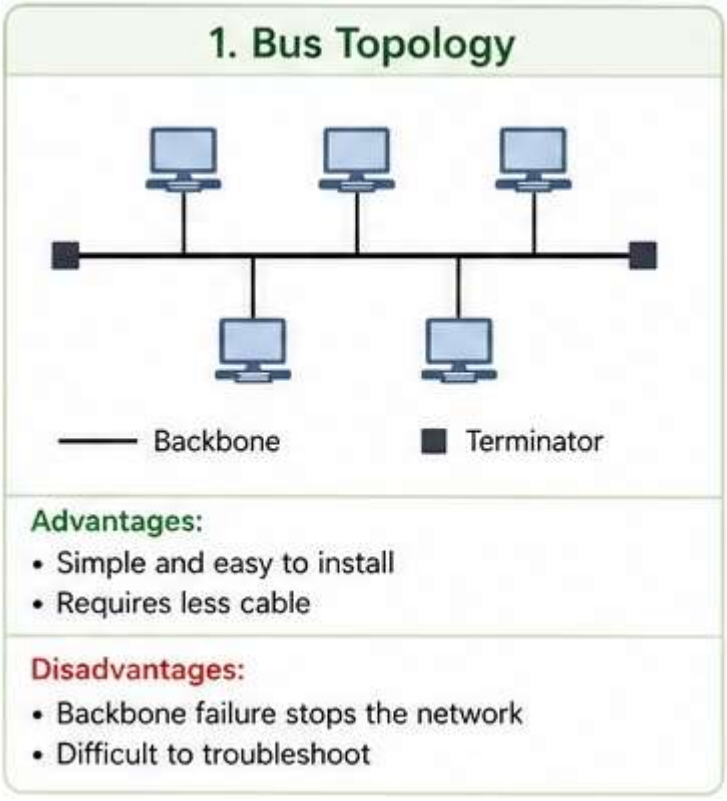


Fig.13 : Bus Topology.

10.2. Star Topology

In a star topology, all devices are connected to a central hub or switch. Each device has its own dedicated connection to the central device.

- Easy to install and manage.
- Failure of one device does not affect others.
- But if the central hub fails, the whole network is down.

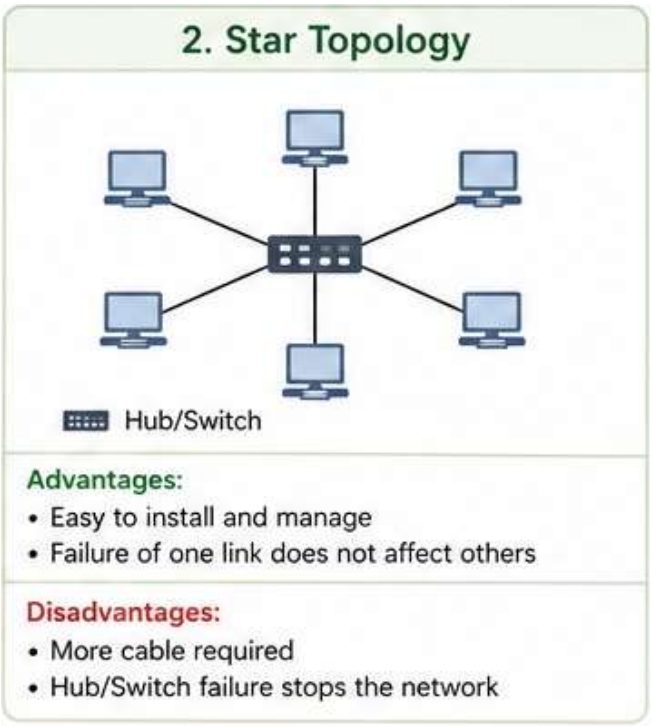


Fig.14 : Star Topology.

10.3. Ring Topology

In a ring topology, each device is connected to two others, forming a circular path. Data travels in one direction around the ring.

- No data collisions.
- Predictable performance.
- However, failure of one node can disrupt the entire network.

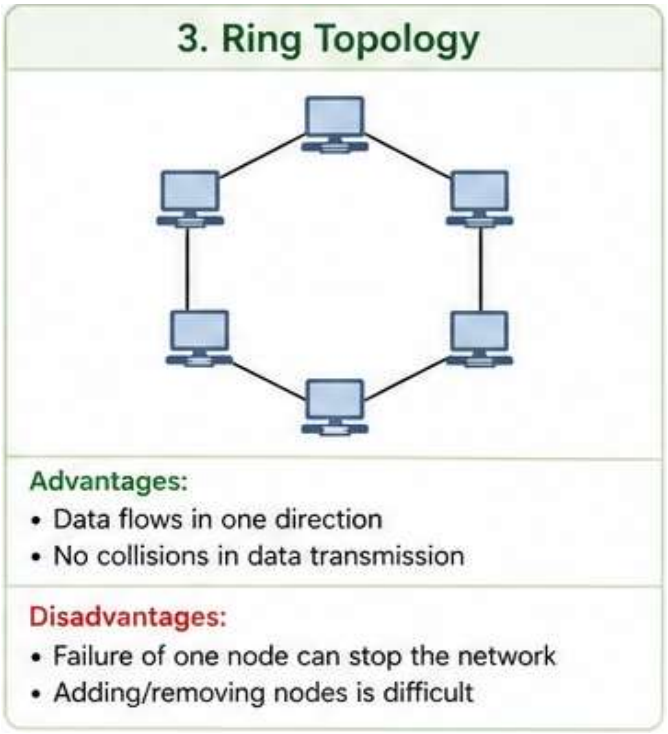


Fig.15 : Ring Topology.

10.4. Mesh Topology

In a mesh topology, devices are interconnected with multiple paths between them.

- Highly reliable and fault-tolerant.
- Data can take multiple routes.
- Expensive and complex to install.

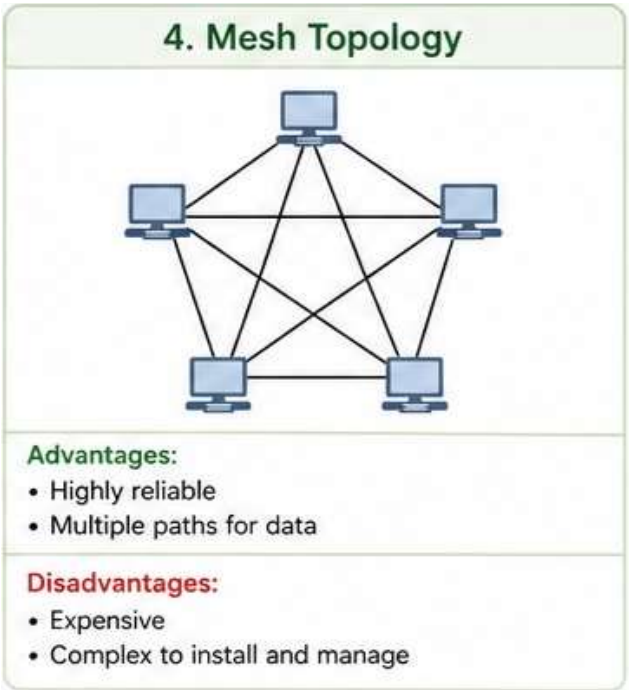


Fig.16 : Mesh Topology.

10.5. Tree Topology

Tree topology is a combination of bus and star topologies, forming a hierarchical structure.

- Scalable and easy to manage.
- Suitable for large networks.
- Backbone failure can affect many devices.

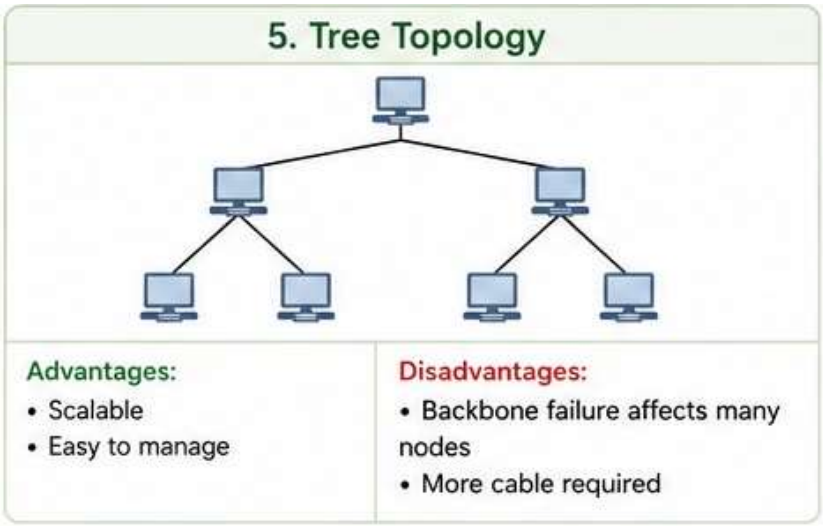


Fig.17 : Tree Topology.

10.6. Hybrid Topology

Hybrid topology combines two or more different topologies (e.g., star + ring).

- Flexible and scalable.
- Can optimize performance.
- Complex design and costly.

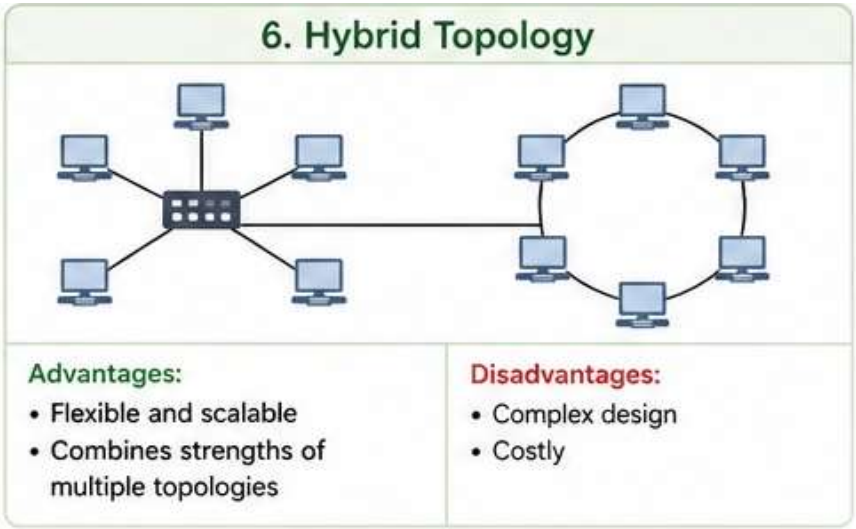


Fig.18 : Hybrid Topology.

10.7. Point-to-Point Topology

This is the simplest topology, where two devices are directly connected.

- Simple and fast communication.
- High performance.

- Not scalable (only connects two devices).

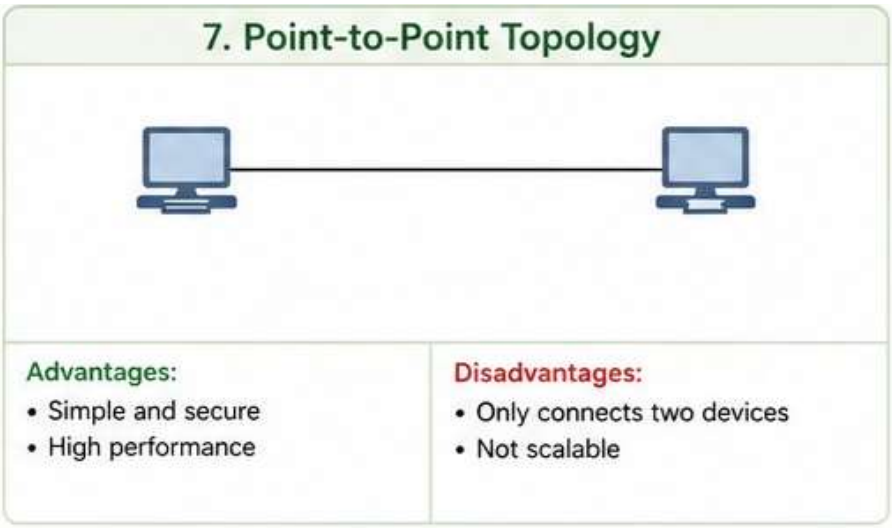


Fig.19 : Point-to-Point Topology.

11. WAN connection options

Service providers have various connection options available for WAN access to connect the local loop to the enterprise edge.

These WAN access options differ in terms of technology, speed, and cost. Each of these options has well-defined advantages and disadvantages.

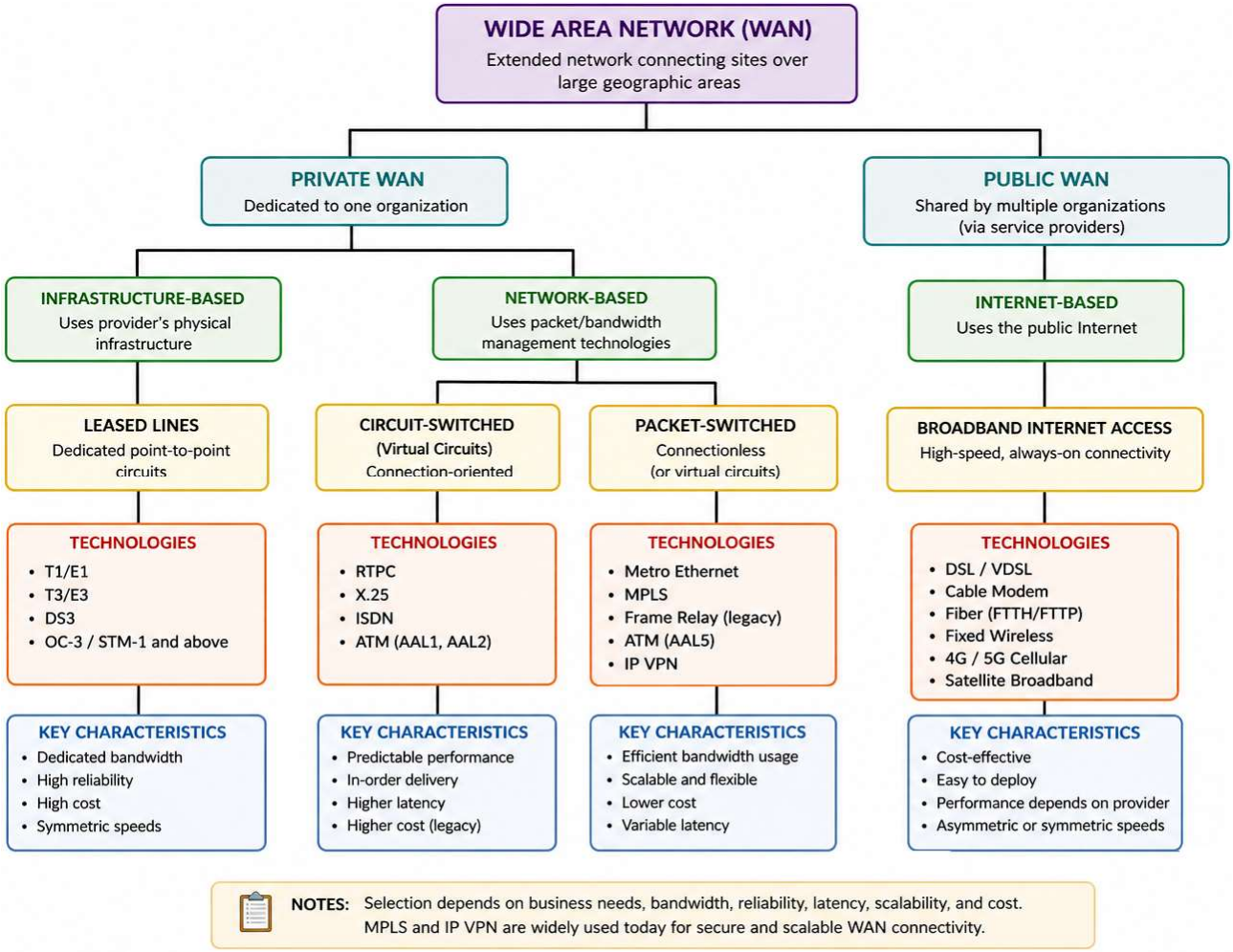


Fig.20 : WAN connection options.

11.1. Private WAN Infrastructure :

Service providers can offer dedicated point-to-point leased lines, circuit-switched connections such as PSTN or ISDN, and packet-switched connections such as Ethernet WAN, ATM, or Frame Relay.

11.2. Public WAN Infrastructure :

Service providers can offer high-speed Internet access through Digital Subscriber Line (DSL) and satellite access. Broadband connection options are generally used to connect small offices and remote workers to a corporate site via the Internet.

Data transfer between enterprise sites over a public WAN infrastructure must be secured using VPN networks.

The topology in Fig.21 illustrates some of these WAN access technologies.

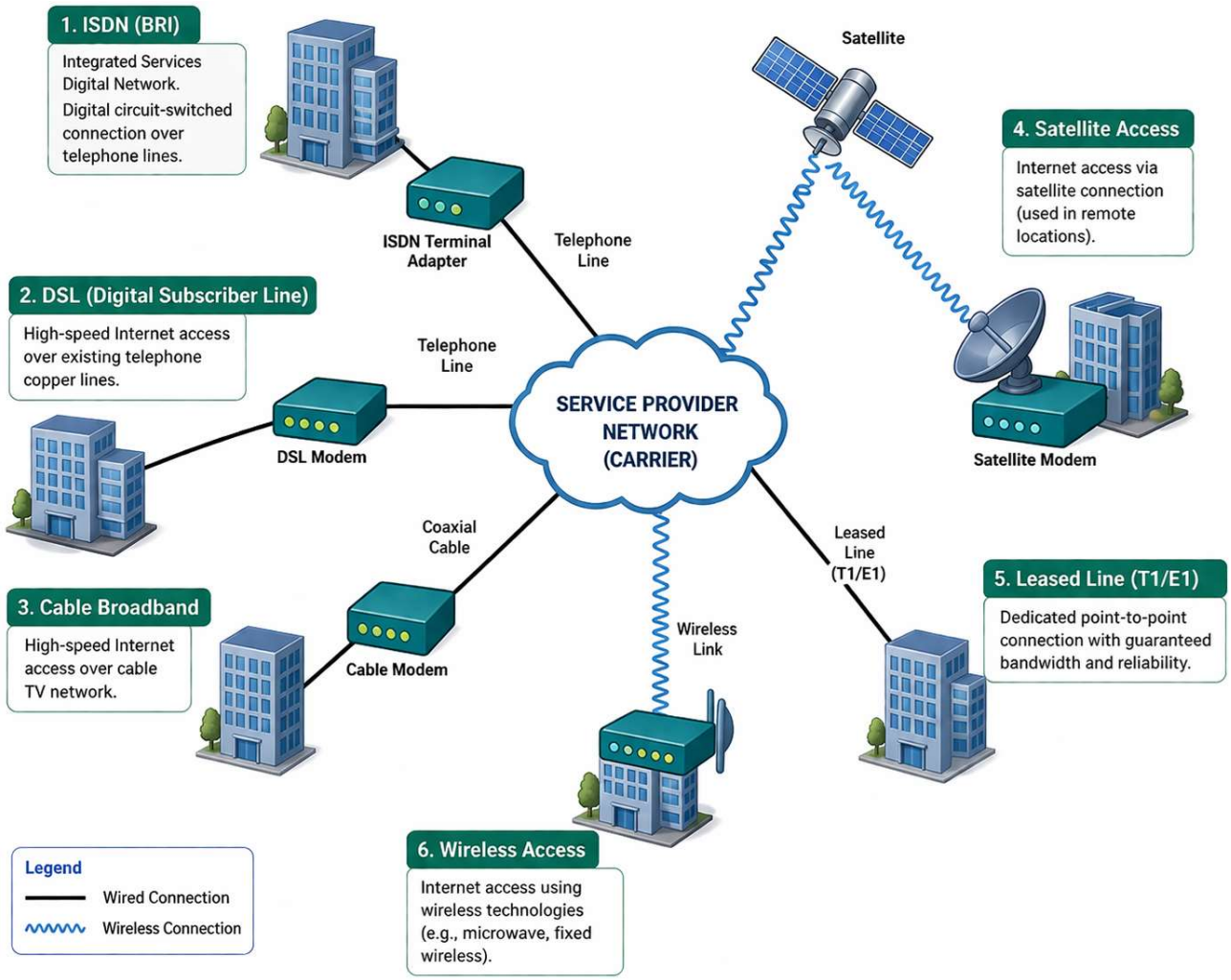


Fig.21. : WAN access technologies.

12. Security in WANs

Security in WANs (Wide Area Networks) refers to the set of policies, technologies, and mechanisms used to protect data, devices, and communications across geographically distributed networks.

Because WANs often use public or shared infrastructure (like the Internet), they are more exposed to threats such as unauthorized access, data interception, and cyberattacks.

Key aspects of WAN security:

- **Confidentiality**: Ensuring that data is accessible only to authorized users (e.g., encryption).
- **Integrity**: Protecting data from being altered during transmission.
- **Authentication**: Verifying the identity of users and devices.
- **Availability**: Ensuring network services remain accessible and reliable.

Common WAN security technologies:

- **VPN (Virtual Private Network)**: Encrypts data over public networks.
- **Firewalls**: Control incoming and outgoing traffic.
- **IPsec (Internet Protocol Security)**: Secures IP communications.
- **Encryption protocols (SSL/TLS)**: Protect data in transit.
- **Access control mechanisms**: Restrict unauthorized access.

13. Conclusion

Wide Area Networks (WANs) represent a fundamental component of modern communication infrastructures. Their evolution, from X.25 to SD-WAN, reflects the continuous improvement of physical media and the growing demands for performance, reliability, and flexibility.

In the following chapters, we will explore specific WAN technologies in greater depth, with a focus on their internal mechanisms, analytical performance, and applications in service provider networks.

14. Quiz

Q1 : WAN Technology Selection

A company has : Headquarters and 10 branch offices.

- Needs high reliability and QoS for voice/video.
- Wants to reduce cost compared to leased lines.

👉 Which WAN technology is most suitable ? Justify your answer ?

Key1 : WAN Technology Selection

The best choice is MPLS (Multi Protocol Label Switching).

👉 Explanation :

- Provides QoS support ⟶ ideal for voice/video.
- More cost-effective than leased lines.
- Highly reliable and scalable.
- Supports multiple sites efficiently.

Q2 : Virtual Circuit vs Leased Line

Compare :

- Virtual Circuit (Frame Relay / ATM).
- Leased Line.

👉 Which is more efficient and why?

Key2 : Virtual Circuit vs Leased Line

Virtual circuits are more efficient and cost-effective, while leased lines are more reliable.

👉 Explanation :

Feature	Virtual Circuit	Leased Line
Cost	Lower	High
Path	Logical	Dedicated
Efficiency	High (shared)	Low (dedicated)
Reliability	Medium	Very High

Q3 : WAN Security Scenario

A company connects remote offices via the Internet.

👉 What security solution should be used? Why?

Key3 : WAN Security Scenario

Use a VPN (Virtual Private Network).

👉 Explanation :

- Encrypts data ⟶ ensures confidentiality.
- Protects against interception and attacks.
- Creates a secure tunnel over public WAN.

Unit 2 : HDLC Protocols.

Unit Objectives :

- Understand the role of data link layer protocols.
- Explain how HDLC ensures reliable communication.
- Describe how PPP establishes and manages point-to-point connections.
- Compare HDLC vs PPP.
- Understand error detection and flow control mechanisms.
- Analyze frame structure and operation.

Topics Covered :

- Functions of the data link layer.
- Framing, error control, flow control.

1. Introduction

Modern communication networks rely heavily on reliable data transmission mechanisms. At the Data Link Layer, protocols such as HDLC and PPP ensure proper framing, error detection, and flow control over point-to-point links.

This study aims to analyze and compare these two protocols in both theoretical and practical contexts.

Review of Data Link Layer Functions

- Ensures reliable data transfer over a physical link.
- Controls access to the physical medium.
- Uses @MAC addresses (Switching level).
- Detects bit errors using the Frame Check Sequence (FCS) field and ensures synchronization.
- Provides ordered frame delivery.
- Performs flow control.

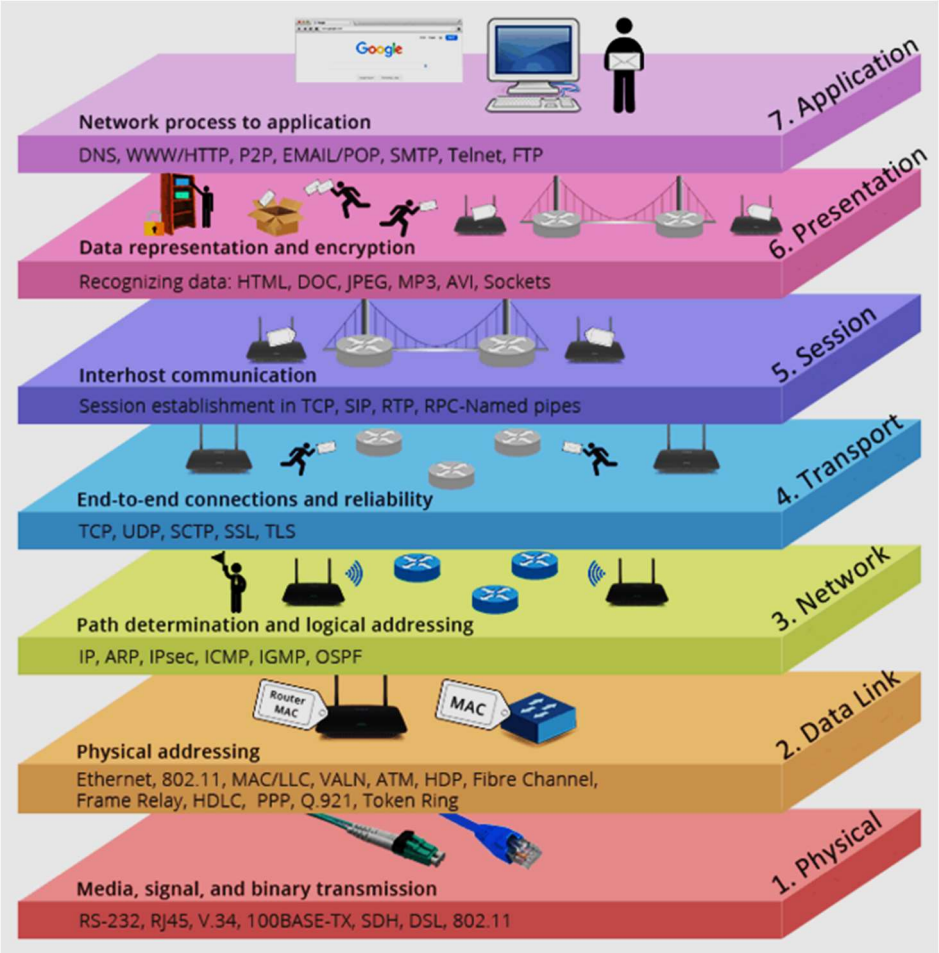


Fig.22. : 7 layers of OSI model.

Note well : LLC : Logical Link Control : Ensures the multiplexing of protocols operating above the data link layer, and provides data link addressing and control, as well as flow control, acknowledgment, and error correction.

2. HDLC Protocol

HDLC, for High-Level Data Link Control, is a bit-oriented communication protocol, standardized by the ISO. It allows the reliable transmission of data over synchronous links.

HDLC is a point-to-point (P2P) protocol of level 2 (link layer) of the OSI model, derived from SDLC (Synchronous Data Link Control).

Its purpose is to :

- Define a mechanism to delimit frames of different types, by adding an error control « FCS ».

It is historically used in WAN networks to connect two network equipment, for example two routers.

2.1. Characteristics of HDLC :

- Reliable delivery (using I-frames).
- Full-duplex communication.
- Flow control.
- Use of physical clocks to synchronize frame transmission.
- Connection-oriented or connectionless operation.

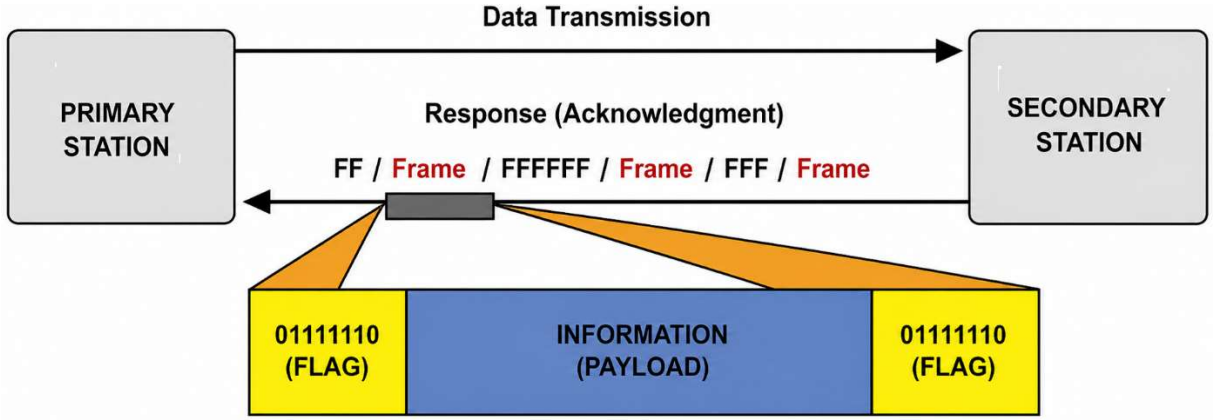


Fig.23. : HDLC Link.

HDLC protocol uses in-band signaling. In this context, three types of frames are distinguished:

- **Information Frame (I-frame) :** ensures data transmission.
- **Supervisory Frame (S-frame) :** provides flow control (acknowledgment).
- **Unnumbered Frames (U-frame) :** manage and supervise the link (control/signaling frames).

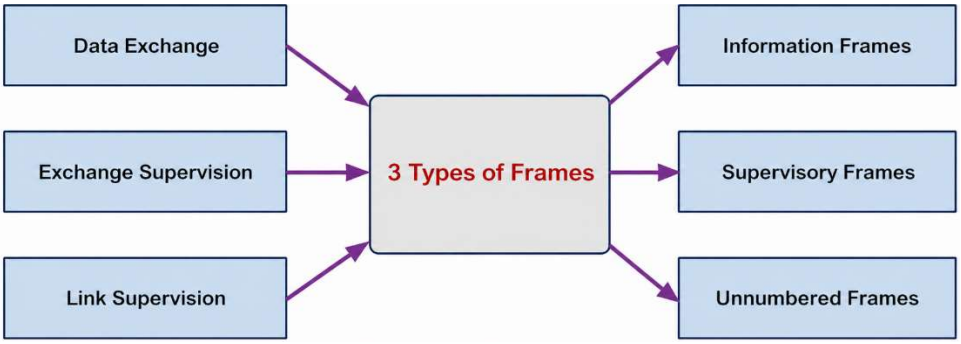


Fig.24. : Functions and corresponding frames of HDLC.

2.2. HDLC frame structure

The transfer unit of HDLC is the **frame**; each frame is delimited by a specific character called the flag.

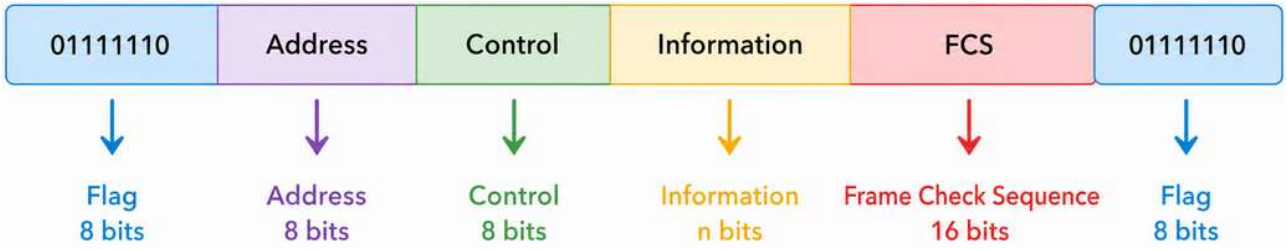


Fig.25. : General structure of the HDLC frame.

a) Flag :

Is a frame delimiter for synchronization. Its value for HDLC is:

- 01111110 (binary).
- 7E (hexadecimal).

Remarks :

- HDLC frames can be sent one after another; in this case, the ending flag of the first frame can be shared and serve as the starting flag for the next frame.
- The flag maintains synchronization between frames during idle periods (when no frames are being transmitted).
- What should be done if the data contains the same bit sequence (data = ...01111110...)?

Solution :

- Add a 0 after every sequence of five consecutive 1s (11111) at the sender side.

Example :

- ✓ Message to send: 011111011111011111111.
- ✓ Message sent: 0111110011111010111110111 (add a stuffing bit).

Therefore, the receiver must remove a 0 after every sequence: 11111.

This method is called: **"transparency"**.

b) Address :

The address field identifies the secondary station in the case of a multipoint link.

- In a command, it represents the destination station.
- In a response, it represents the transmitting station.
- In the case of a point-to-point link, it is not taken into account.

Example :

✓ In the PPP protocol, address = FF (broadcast address).

c) Control :

Three types of frames are distinguished : Information frame (I), Supervisory frame (S), and Unnumbered frame (U).

The following table shows the different values of the control field corresponding to the different types of frames.

Frame Type	Control Field (bits)							
I Frames *(Information frames)*	0	N(s)			P/F	N(r)		
S Frames *(Supervisory frames)*	1	0	S	S	P/F	N(r)		
U Frames *(Unnumbered frames)*	1	1	U	U	P/F	U	U	U

Table.1 : Different types of frames.

❖ **In the information frame format I :**

- Ns is the number of the current frame (modulo 8 or 128).
- Nr is the number of the expected information frame; it acknowledges all frames with numbers less than Nr (modulo 8 or 128).

The P/F bit stands for Poll/Final (Request to transmit / End). It is considered set when its value is 1.

- P if the frame is a command.
- F if the frame is a response.

In the balanced mode of the protocol **LAP-B (Link Access Procedure Balanced):** both ends are primary ; they can send commands.

- In a command: request for an immediate response.
- In a response: reply to the request for an immediate response.

Note : Issuing a command (P = 1) requires an immediate response (F = 1).

❖ **In the supervision frame S :**

The supervision frame is used to monitor data exchange. Four subtypes of supervision frames can be distinguished, i.e., depending on the value of the two S bits.

Frame Type	Sub-Type	Control Field (Command)							
S Frame	RR	1	0	0	0	P/F	N_r	N_r	N_r
	RNR	1	0	1	0	P/F	N_r	N_r	N_r
	REJ	1	0	0	1	P/F	N_r	N_r	N_r
	SREJ	1	0	1	1	P/F	N_r	N_r	N_r

Table.2 : Sub-Type S Frame.

- **RR (Receive Ready)** = 00:
  - ✓ Confirms the reception of data frames with sequence number < Nr.
  - ✓ Sent to indicate that the receiver is ready to receive subsequent frames, or to acknowledge frame Nr when there is no data to send.
- **RNR (Receive Not Ready)** = 10:
  - ✓ Confirms the reception of data frames with sequence number < Nr.
  - ✓ Requests a temporary stop of transmission from the sender.
- **REJ (Reject)** = 01:
  - ✓ Confirms the reception of data frames with sequence number < Nr.
  - ✓ Requests retransmission of frames with sequence number ≥ Nr.
- **SREJ (Selective Reject)** = 11:
  - ✓ Confirms the reception of data frames with sequence number < Nr.
  - ✓ Requests retransmission of the frame with sequence number = Nr.

Example :

- ✓ I(3,5,P) = 00111101: this is a command for an information frame with Ns = 3 and Nr = 5.
- ✓ REJ(4,F) = 10011100: this is a response indicating rejection, requesting retransmission starting from frame number 4.

❖ **In the Unnumbered frame U :**

The Unnumbered frame is used for connection management (establishment, termination, selection of a response mode, etc.). Several types are distinguished depending on the value of the U bits :

Type	Subtype	P/F	Control Field (command)							
U frame	SABM	Command	1	1	1	1	P	1	0	0
	SABME		1	1	1	1	P	1	1	0
	DISC		1	1	0	0	P	0	1	0
	UA	Response	1	1	0	0	F	1	1	0
	FRMR		1	1	1	0	F	0	0	1
	DM		1	1	1	1	F	0	0	0

Table.3 : Sub-Type U Frame.

- **Unnumbered command frame** (Primary ⟶ Secondary) **:**
  - **Connection establishment :**
    - ✓ **SABM** (Set Asynchronous Balanced Mode) **:** normal format (modulo 8).
    - ✓ **SABME** (Set Asynchronous Balanced Mode Extended) **:** extended format (modulo 128).
  - **Connection release :**
    - ✓ **DISC** (Disconnection) **:** connection release.
- **Unnumbered response frame** (Secondary ⟶ Primary) **:**
  - **Acknowledgment of an unnumbered frame :**
    - ✓ **UA** (Unnumbered Acknowledgment) **:** acknowledgment of an unnumbered frame.
  - **Error recovery :**
    - ✓ **FRMR** (Frame Reject) **:** frame rejection.
  - **Connection released indication frame :**
    - ✓ **DM** (Disconnected Mode) **:** the terminal is disconnected.

d) Data :

This optional variable-length field contains the data to be transmitted. The number of bits to be sent does not have to be a multiple of 8: since this field does not need to be byte-aligned, it is not necessary to add padding bits at the end.

e) FCS (Frame Check Sequence) :

It is a code added after the data to detect possible transmission errors. It is usually encoded on 16 bits, but it can also be encoded on 32 bits.

This sequence corresponds to the CRC calculated over the Address + Control + Information fields using the generator polynomial $x^{16}+x^{12}+x^5+1$. The CRC, computed at the transmitter, is verified at the receiver.

2.3. HDLC Operation :

2.3.1. Connection Establishment and Release :

When the link is in the logically disconnected state (fig. 26), the primary station requests the establishment of a connection by sending unnumbered (U) frames of type SABM (Asynchronous Balanced Mode or LAP-B, Link Access Protocol Balanced). The P bit is set to 1 (it could also have been set to 0).

If the secondary station accepts the connection, it responds with an unnumbered UA frame. The F bit in the response is set to the same value as the P bit.

The link is then established, and information exchange can begin.

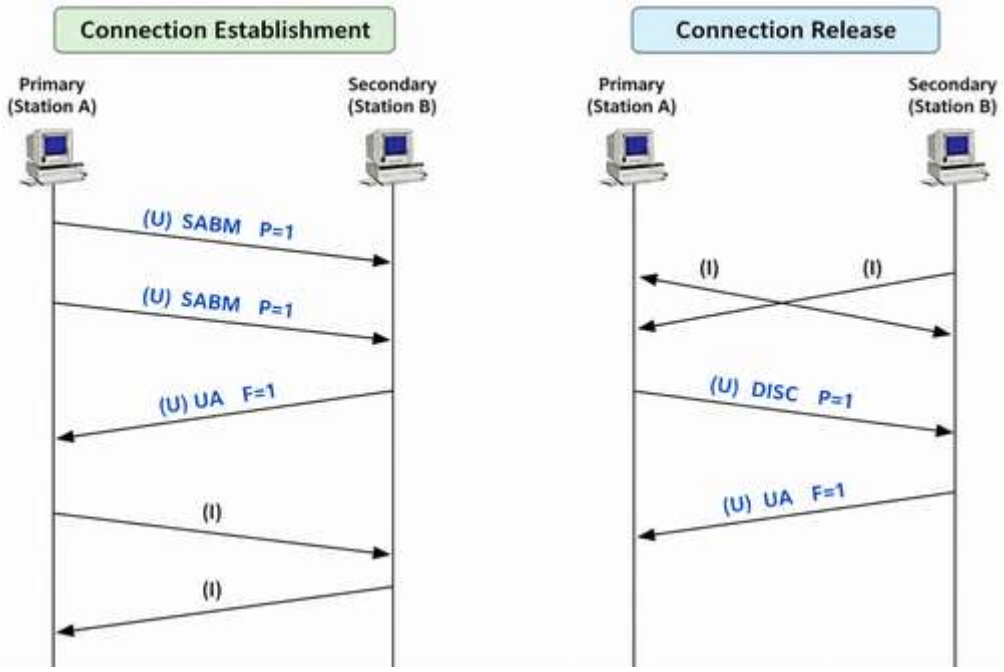


Fig.26. : HDLC Connection Management.

The link is in the logically connected state. The primary station sends a disconnection request DISC (fig. 26); the P bit may be set to either 1 or 0.

The secondary station acknowledges with a UA frame, and the value of the F bit matches that of the P bit in the DISC frame.

The link is then terminated. The exchange of flags continues to maintain synchronization as long as the physical link is not broken.

2.3.2. Timeout Management :

Two timers (fig. 27) are managed by the communicating entities :

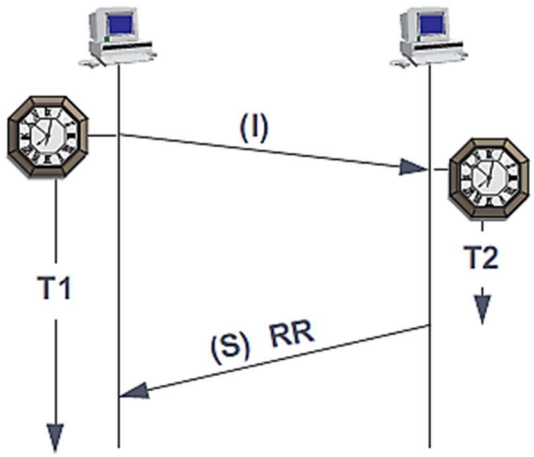


Fig.27. : Timeout Management.

❖ **Retransmission timer (T1 or RTO – Retransmission Time Out) :**

For each transmitted frame, the sender initializes the T1 timer. If this timer (or guard time) expires and the sender has not received an information or acknowledgment frame from its peer, it retransmits the frame assumed to be lost.

❖ **Acknowledgment timer (T2) :**

This corresponds to the maximum delay after which the receiver, if it has no data to send, must send an acknowledgment to its peer.

2.3.3. Flow Control Management :

In Fig. 28, machine B rejects the excess frame and informs A of its temporary inability to accept new data. It sends an S-frame RNR (Receive Not Ready) with the counter Nr set to the number of the received and rejected frame.

Machine A takes this request into account and periodically polls (every T1) machine B, both to indicate its presence and to request the resumption of transmission using an S-frame RR (Receive Ready), with the P bit set to 1.

When B is ready to resume reception, it signals this to the sender by acknowledging with an S-frame RR. The Nr counter contains the number from which retransmission should resume. Since A had set the P bit to 1, B's response is sent with the F bit set to 1.

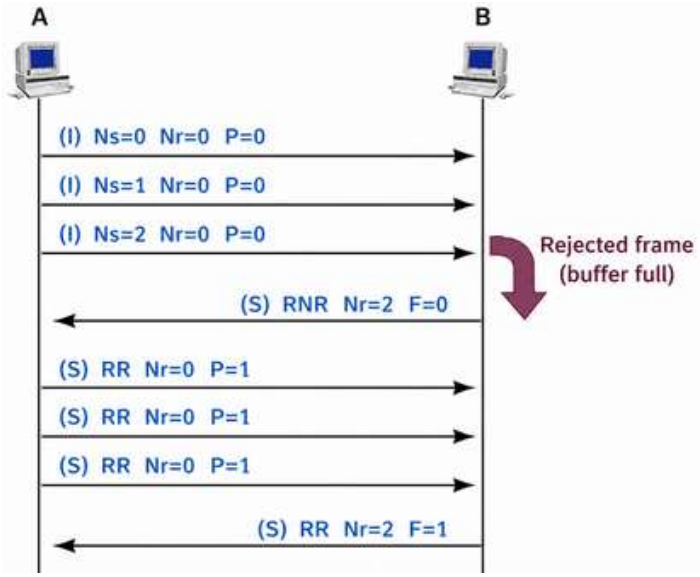
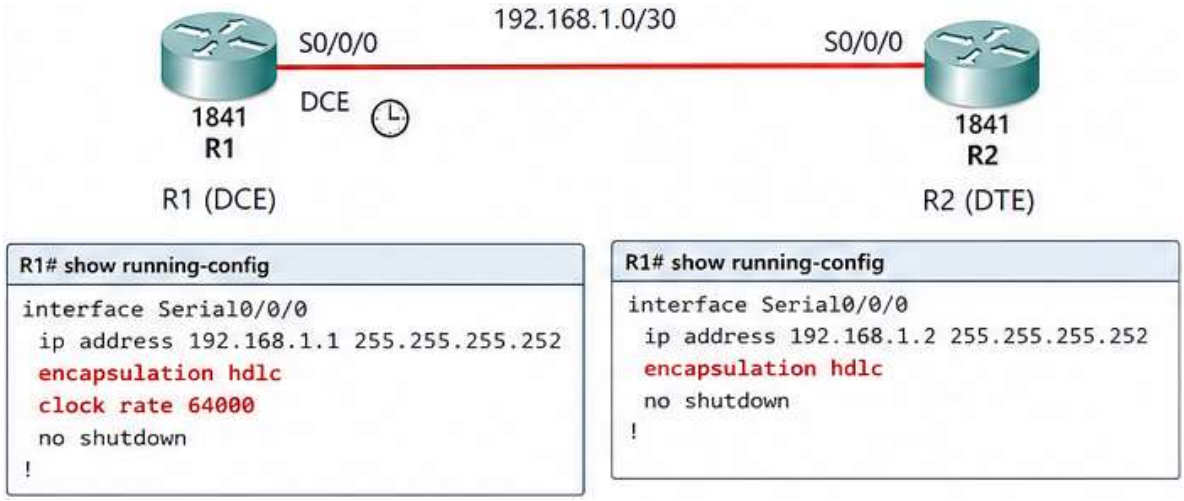


Fig.28. : Flow Control Management.

2.4. HDLC configuration in Cisco Packet Tracer :



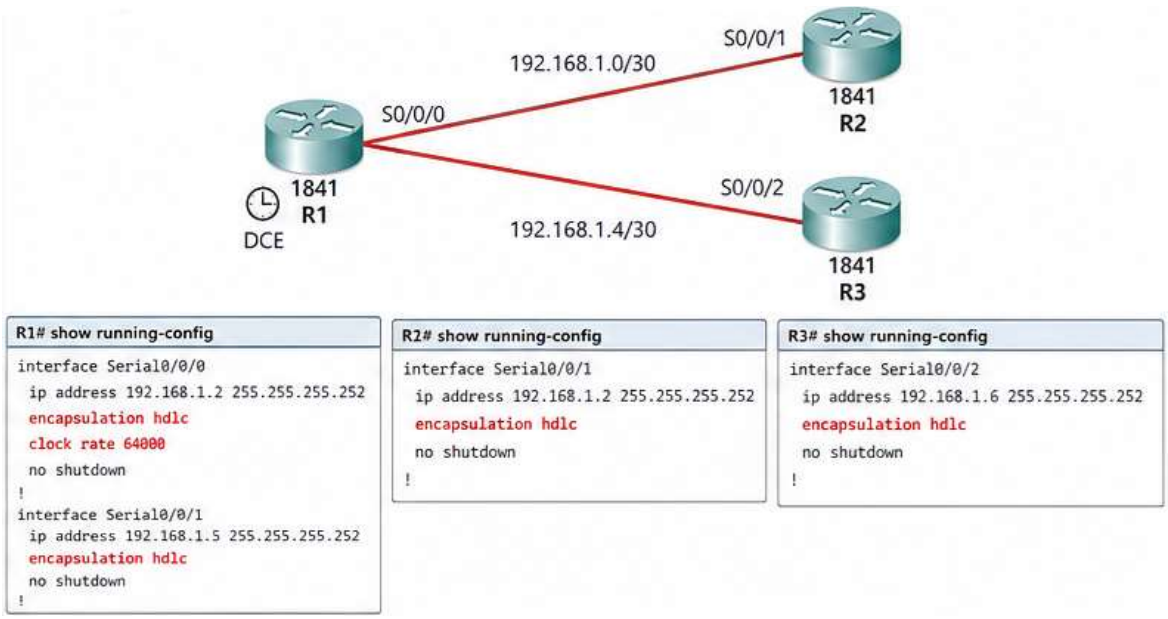


Fig.29. : HDLC configuration P2P and P2MP.

2.5. Different Versions of the HDLC Protocol :

Standardized in 1976 (CCITT and ISO), HDLC inspired many variants :

- **LAP mode** (Link Access Protocol) **:** operates with polling from a single endpoint: the primary.
- **LAP-B mode** (B for Balanced) **:** in this type of link, there is no predefined primary; each station can act as a primary.
- **LAP-D mode** (D for D-channel) **:** this protocol, similar to LAP-B, is used in digital networks (ISDN).
- **LAP-M mode** (M for Modem) **:** derived from LAP-D, it is implemented for PC–host computer connections ; this protocol is used in modems compliant with V.42 and V.42bis recommendations.
- **LAP-X mode :** a half-duplex mode derived from LAP-D, used in Telex.
- **LAP-F mode :** Frame Relay, ITU-T Q.931 or I.451.
- **LAP-Dm mode :** used for GSM radio links.

3. Conclusion :

In its LAP-B version, HDLC has been widely used in X.25 networks (e.g., Transpac). In this context, error control and flow control are performed on a point-to-point basis, that is, between adjacent nodes. While this approach ensures reliable data transmission, it can significantly degrade overall performance due to repeated control mechanisms at each hop.

With the evolution of network technologies, particularly the introduction of optical fiber transmission media have become much more reliable, with lower error rates. This improvement has made it possible to simplify communication protocols such as HDLC.

Furthermore, establishing dedicated point-to-point links between information systems can be costly relative to their actual usage time. Therefore, beyond protocol considerations or multi-protocol environments, it becomes relevant to explore whether a single link can be shared simultaneously by multiple communicating entities. This concept is known as resource sharing or traffic concentration, and it represents an important evolution in optimizing network efficiency.

4. Exercise to do :

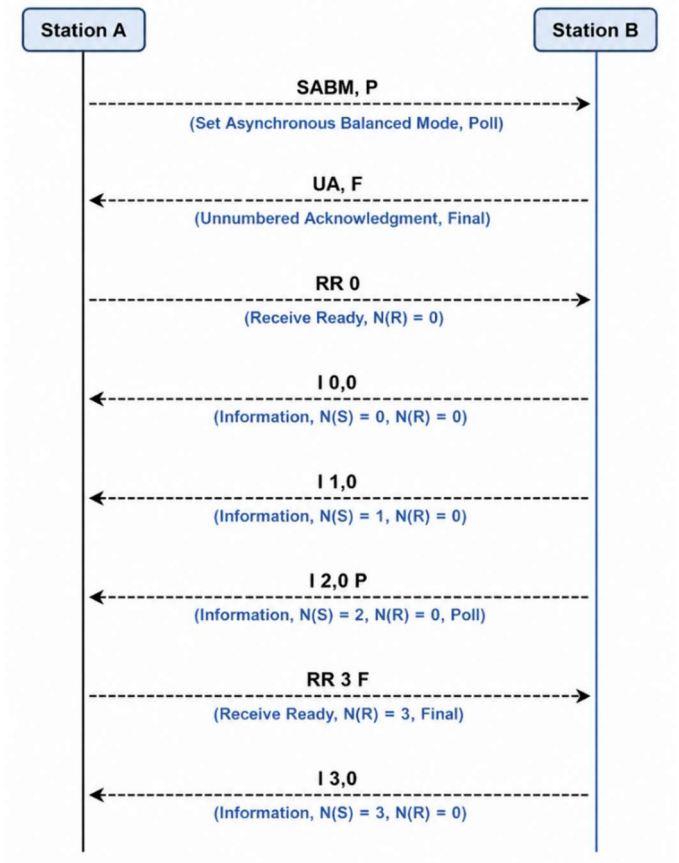
Consider a data link between two stations A and B using the HDLC protocol. The sequence below arrives at station B:

S = 01111110000000100010100111011111010011111000010101100111110000101000111111001111110011111100000001010001001001011101111101010111111 0.

1. How many frames are present in this sequence?
2. Break down this sequence and identify (name) each field.
3. Draw the exchange diagram between the two stations.

Solution :

- **Frame 1:**
  Address: 00000010
  Control: 00101001
  Interpretation:
  0-------- ⟶ I-frame
  -**010**---- ⟶ N(S) = 2
  ------**1**--- ⟶ P (Poll bit)
  --------**001** ⟶ N(R) = 1
  Data: 1101111110011111 0001010
  FCS: 1001111100010100
- **Frame 2:**
  Address: 00000010
  Control: 10001001
  Interpretation:
  10------- ⟶ S-frame
  ---**00**---- ⟶ type RR (Receive Ready)
  ------**1**--- ⟶ F (Final bit)
  --------**001** ⟶ N(R) = 1
  Data: no data
  FCS: 0010111011111101
- **Exchange Diagram**



Unit 3 : PPP (Point-to-Point) Protocols

Unit Objectives :

- Understand the role of data link layer protocols.
- Describe how PPP establishes and manages point-to-point connections.
- Compare HDLC vs PPP.
- Understand error detection and flow control mechanisms.
- Analyze frame structure and operation.

Topics Covered :

- Functions of the data link layer.
- Framing, error control, flow control.

1. Introduction

The Point-to-Point Protocol (PPP) is a data link layer (Layer 2) communication protocol used to establish a direct connection between two network nodes. It is widely used for transmitting data over serial links, such as telephone lines, fiber optic cables, or satellite connections.

PPP was designed to be a more advanced and flexible alternative to older protocols like HDLC. It supports multiple network layer protocols, including IP, IPX, and AppleTalk, making it highly versatile in different networking environments.

2. PPP Protocol

2.1. Definition

PPP provides a standard method for :

- Encapsulating network layer protocols (like IP).
- Establishing and configuring the connection.
- Authenticating the communicating devices.
- Ensuring reliable data transmission.

It is widely used in WAN (Wide Area Network) connections, especially between routers and for internet access technologies like PPPoE (PPP over Ethernet).

The PPP protocol relies on three components :

- Datagram encapsulation
- Link control using LCP (Link Control Protocol):
  ➤ Used to establish a point-to-point connection.
- Network layer control using NCP (Network Control Protocol):
  ➤ Used to initialize different upper-layer protocols (PPP, IP, etc.).

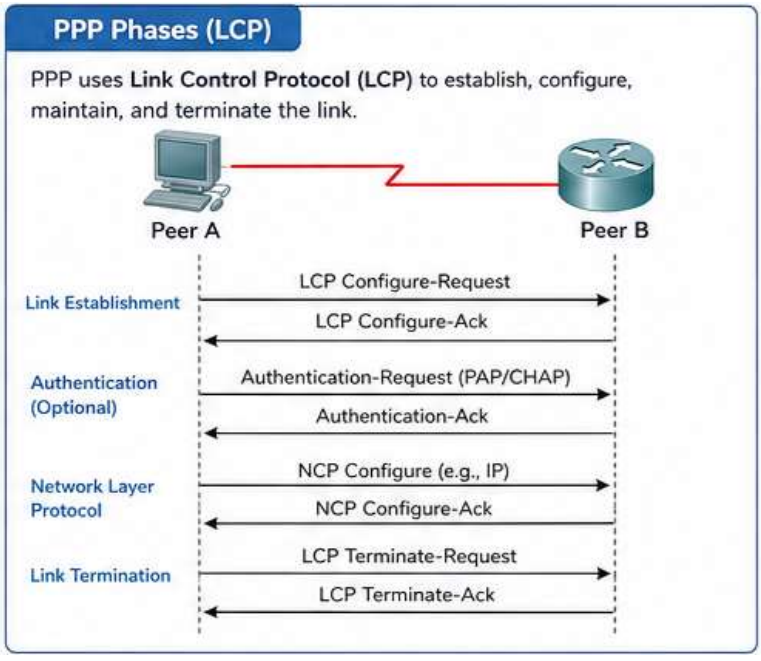


Fig.30. : PPP Phases (LCP).

Additionally, PPP offers features like :

- Error detection.
- Link quality monitoring.
- Compression support.

Because of its reliability and security features, PPP is commonly used in:

- Dial-up internet connections.
- WAN links between routers.
- VPN connections (in some implementations like PPPoE).

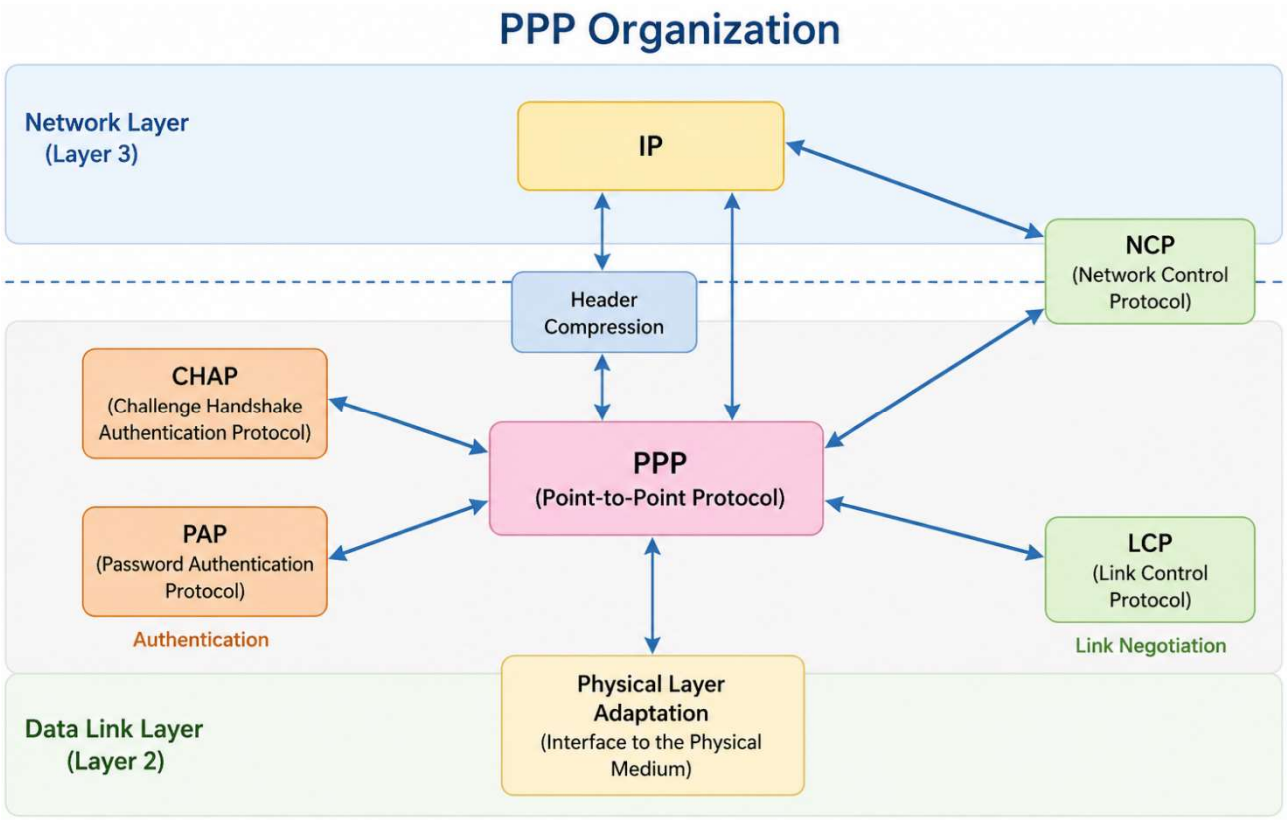


Fig.31. : PPP Organisation.

➢ **Advantages :**

The PPP protocol provides better link management compared to HDLC because:

- It supports authentication mechanisms such as :

  ➤ **PAP :** The username and password are transmitted in clear text over the line.

  ➤ **CHAP :** The username and password are transmitted in encrypted form over the line.
- It allows link aggregation (known as PPP Multilink).
- It supports data compression.

- It is widely used for Internet connections for individuals, either directly based on HDLC (dial-up connections) or encapsulated (for example PPPoX, used in ADSL and cable connections).

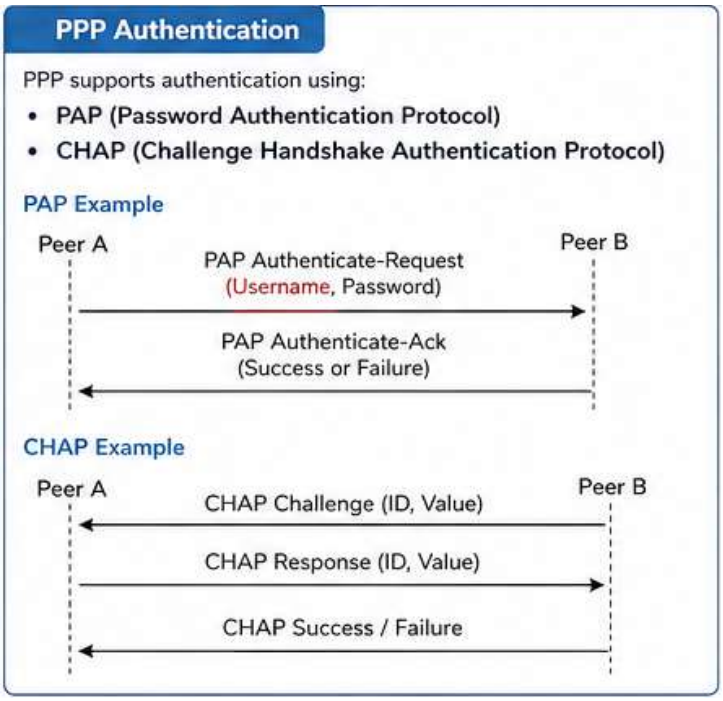


Fig.32. : PPP Authentication.

➢ **PPP Frame Format :**

A PPP frame is an HDLC frame to which a protocol field is added for encapsulating upper-layer protocols.

- The Flags and the FCS are the same as in HDLC.
- The Address field is always set to 11111111 to indicate that the frame should be accepted by the intended receiver.
- The Control field is always set to 00000011 to indicate that the frames are of the unnumbered type.
- Protocol field : specifies the upper-layer protocol to which the packet will be delivered (PPP-LCP, IP, IPCP, etc.).

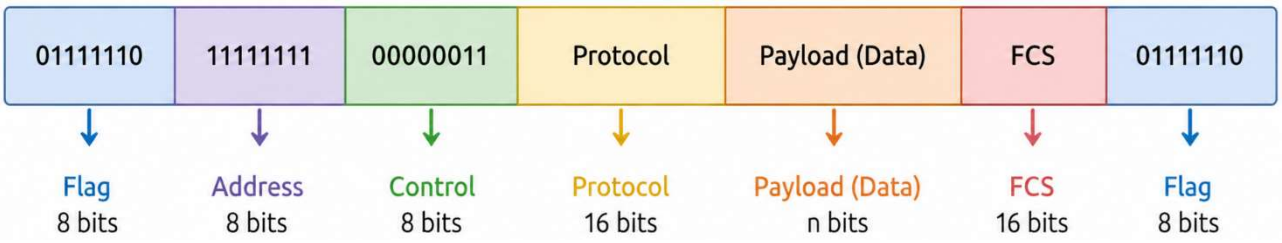


Fig.33. : PPP Frame Format.

➢ **HDLC vs PPP :**

Feature	HDLC	PPP
Type	Cisco proprietary (default)	Open standard
Layer	Data Link Layer (Layer 2)	Data Link Layer (Layer 2)
Authentication	✗ Not supported	✓ PAP, CHAP supported
Multiprotocol Support	✗ Limited (mainly IP)	✓ Supports multiple protocols
Error Detection	✓ Yes (FCS)	✓ Yes (FCS)
Compression	✗ No	✓ Yes
Configuration	Simple	More flexible
Compatibility	Cisco devices only (by default)	Works across vendors
Overhead	Lower	Slightly higher
Security	✗ No	✓ Yes (with authentication)

Table.4 : HDLC vs PPP.

3. Conclusion

PPP is a reliable data link layer protocol used for point-to-point communication. It offers better security, flexibility, and support for multiple protocols compared to HDLC. With features like authentication, LCP, and NCP, PPP ensures secure and efficient data transmission and is widely used in modern WAN networks despite slightly higher overhead.

4. Quiz

Q1 : Establishing, configuring and testing.

☞ Which PPP component is responsible for establishing, configuring, and testing the data link connection ?

a) NCP.
b) LCP.
c) PAP.
d) FCS.

Key1 : Establishing, configuring and testing.

☞ b) LCP.

Q2 : Authentication protocols.

☞ Which of the following authentication protocols is considered more secure in PPP ?

a) PAP.
b) CHAP.
c) HDLC.
d) ARP.

Key2 : Authentication protocols.

☞ b) CHAP.

Q3 : Role of NCP in PPP.

☞ What is the primary role of NCP in PPP ?

a) Encrypt data.
b) Detect errors.
c) Configure network layer protocols.
d) Manage physical connections.

Key3 : Role of NCP in PPP.

☞ c) Configure network layer protocols.

Q4 : Protocol field.

☞ In PPP, what does the value 0xC021 in the Protocol field represent ?

a) IP.
b) IPCP.
c) LCP.
d) CHAP.

Key4 : Protocol field.

☞ c) LCP.

Chapter II

Protocols :

X25 and Frame Relay

Unit 1 : X.25 Protocol.

Chapter Objectives :

After completing this chapter, you will be able to :

- Understand the fundamentals of packet-switched networks.
- Explain the operation of the X.25 protocol.
- Identify the main components and layers of X.25.
- Understand the concept of virtual circuits.
- Describe how Frame Relay works and its advantages over X.25.
- Compare X.25 and Frame Relay protocols.
- Understand key terms such as PVC (Permanent Virtual Circuit) and DLCI (Data Link Connection Identifier).
- Analyze the role of these protocols in WAN technologies.

Topics Covered :

- This chapter introduces packet-switched networks and explains two important WAN protocols : X.25 and Frame Relay.
- It begins with the basics of packet switching and how it differs from circuit switching. Then, it covers the X.25 protocol, including its layered architecture, use of virtual circuits, and strong error control mechanisms.
- Next, the chapter highlights the limitations of X.25, such as high overhead and low speed.
- The focus then shifts to Frame Relay, a faster and more efficient protocol with reduced error control and lower overhead. Key concepts like DLCI, PVC, and congestion control mechanisms are explained.
- Finally, the chapter compares X.25 and Frame Relay, showing their differences in performance and complexity, and discusses their role in the evolution of modern WAN technologies.

1. Introduction

X.25 is a packet-switched network protocol developed in the 1970s by the International Telecommunication Union (ITU-T). It was designed to provide reliable data communication over long-distance networks, especially when transmission lines were prone to errors.

X.25 operates across the first three layers of the OSI model :

- Physical Layer.
- Data Link Layer.
- Network Layer.

One of its main features is the use of virtual circuits, which establish a logical path between two devices before data transmission begins. These circuits can be :

- SVC (Switched Virtual Circuits) – temporary connections
- PVC (Permanent Virtual Circuits) – fixed, always-available connections

X.25 is known for its strong error detection and correction mechanisms, ensuring reliable data delivery even on unreliable networks. However, this reliability comes at the cost of high overhead and lower performance.

Although X.25 has largely been replaced by more efficient technologies like Frame Relay, MPLS, and modern IP networks, it played a crucial role in the development of early Wide Area Networks (WANs).

2. Definition

X.25 is a packet-switched network protocol that operates at the physical, data link, and network layers of the OSI model. It is designed to enable reliable data communication between devices over long-distance networks by using virtual circuits and strong error detection and correction mechanisms.

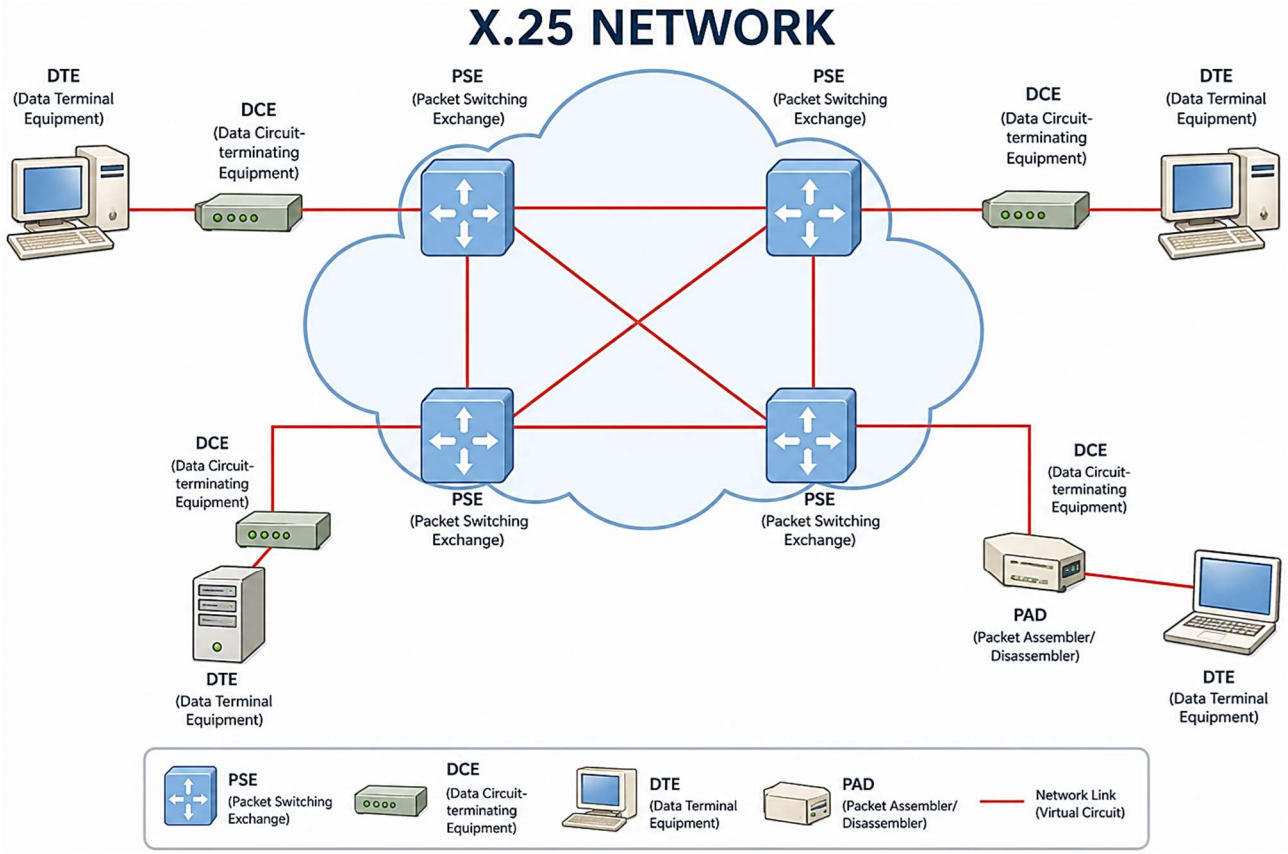


Fig.34. : X25 network architecture.

In 1976, the ITU-T published the X.25 recommendations, describing the interface between a DTE (Data Terminal Equipment) and a DCE (Data Circuit Terminating Equipment), specifying layers 1, 2, and 3.

- ETTD = DTE (Data Terminal Equipment).
- ETCD = DCE (Data Circuit Equipment).

The three layers defined by the ITU-T:

- X.25 Layer 3.
- X.25 Layer 2, a subset of the HDLC standard: LAP-B.
- X.25 Layer 1, standard X.21.

The X.25 protocol uses packet switching, and its objectives are to :

- Standardize the transport network.
- Interconnect different networks.
- Optimize the use of communication lines.
- Increase communication security.
- Reduce telecommunication costs.

- **Note well :** It is a full-duplex protocol that uses error control and correction procedures.

3.1. Physical level

Packet-switched networks can offer one or more of the following physical interfaces :

- **ITU-T Recommendation X.21: "Access via a circuit-switched network." :**

ITU-T Recommendation X.21 is a standard that defines the physical interface for connecting Data Terminal Equipment (DTE) to Data Circuit-terminating Equipment (DCE) over a circuit-switched network.

It specifies:

- Electrical characteristics.
- Functional procedures.
- Signal exchange between devices.

X.21 is mainly used at the physical layer (Layer 1) of the OSI model and enables reliable communication setup over digital circuit-switched networks.

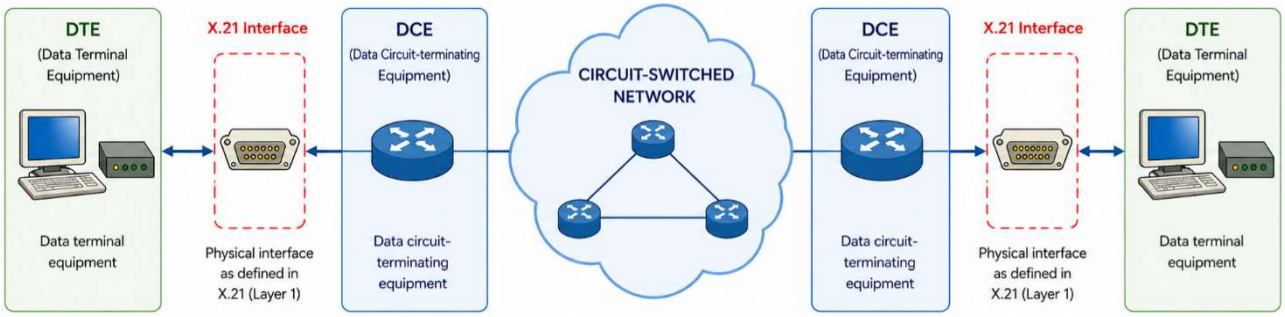


Fig.35. : Access via a circuit-switched network.

- **ITU-T Recommendation X.21 bis : "Access via leased line (dedicated link)" :**

ITU-T Recommendation X.21 bis defines a physical interface that allows Data Terminal Equipment (DTE) to connect to Data Circuit-terminating Equipment (DCE) over a leased line (dedicated link) instead of a circuit-switched network.

Unlike X.21, which is used for circuit-switched access, X.21 bis is designed for permanent, point-to-point connections that are always available.

It specifies:

- Electrical and mechanical characteristics.
- Signal exchange procedures.
- Interface standards for reliable communication.



Fig.36. : Access via leased line.

- **ITU-T Recommendations of the V series : "Access via switched network" :**

The ITU-T V-Series Recommendations define standards for data communication over switched networks, particularly the public switched telephone network (PSTN).

These recommendations specify how Data Terminal Equipment (DTE) communicates over analog telephone lines using devices such as modems.

They cover:

- Signal modulation and demodulation techniques.
- Data transmission speeds.
- Interface and control procedures.
- Error detection and correction methods.

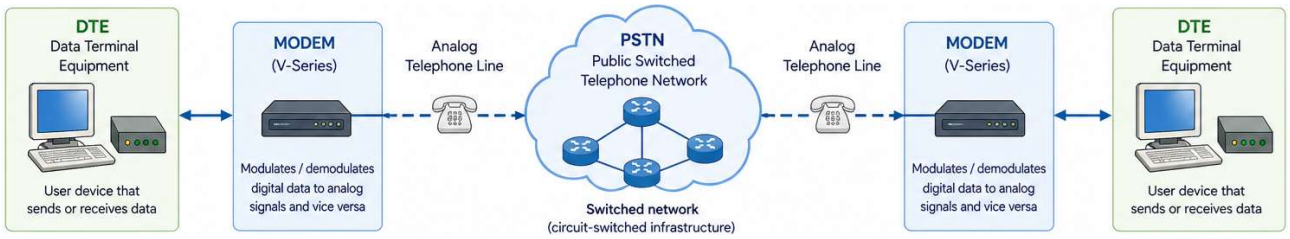


Fig.37. : Access via switched network.

CCITT Recommendation	Data Rate (bit/s)	Type of Modulation	Modulation Speed (symbols/s)	Operation (Mode of Operation)
V.21	300	Frequency	300	Full Duplex
V.22	600 / 1200	Phase	600	FD
V.22 bis	1200 / 2400	Phase	600	FD
V.23	600 / 1200	Frequency	600 / 1200	Half Duplex
V.26	2400	Phase	1200	FD
V.26 bis	1200 / 2400	Phase	1200	HD
V.27	4000	Phase	1600	FD or HD
V.27 bis	2400 / 4800	Phase	1200 / 1600	FD or HD
V.29	4800 / 9600	Phase / Amplitude	4800 / 9600	FD
V.32	4800 / 9600	Phase / Amplitude	2400	FD
V.32 bis	Up to 14,400	Phase / Amplitude	3200	FD
V.34	Up to 28,800	Phase / Amplitude	3200	FD

Table.5 : ITU-T Recommendations of the V series.

- **ITU-T Recommendation X.31: "Access via ISDN network (Integrated Services Digital Network)" :**

ITU-T Recommendation X.31 defines how data communication networks (such as X.25 packet-switched networks) can be accessed through an ISDN (Integrated Services Digital Network).

It specifies:

- The procedures for connecting Data Terminal Equipment (DTE) to packet-switched networks via ISDN
- The integration of packet switching (X.25) with digital circuit-switched services (ISDN)
- Signaling and interface methods for reliable data transmission over ISDN

X.31 enables users to access packet-switched services using the digital infrastructure of ISDN, combining the advantages of both technologies.

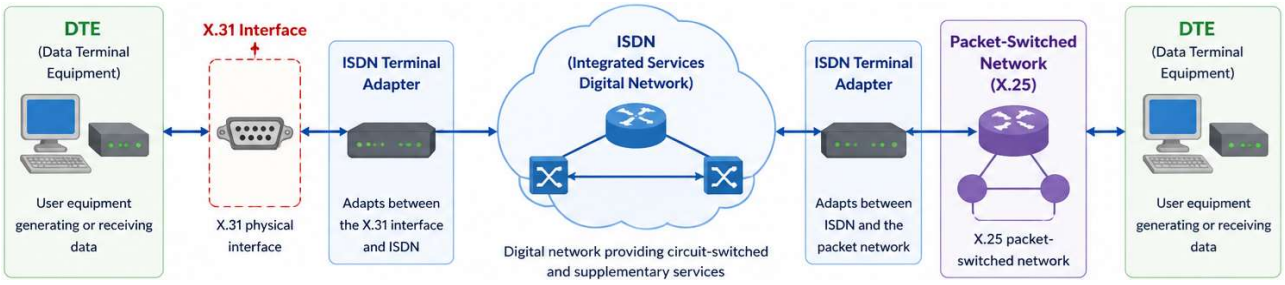


Fig.38. : Access via ISDN network.

3.2. Frame level

X.25 uses the LAP-B (Link Access Procedure Balanced) version of the HDLC (High-Level Data Link Control) protocol.

HDLC implements several concepts such as: acknowledgment, non-acknowledgment, data numbering, acknowledgment numbering, anticipation (pipelining), sliding window, grouped acknowledgments, supervision timer, connection, disconnection, window closure, synchronization, etc.

These concepts are reflected by the addition of control bytes at the beginning of the frame, called protocol bytes, which define the type of frame and its content (I-frames, S-frames, and U-frames).

The frame level corresponds to the data link layer of the OSI reference model.

Two types of procedures can be used at this level :

- Single-link procedure (identical to the LAP-B mode of the HDLC protocol).
- Multi-link procedure (using multiple physical media).

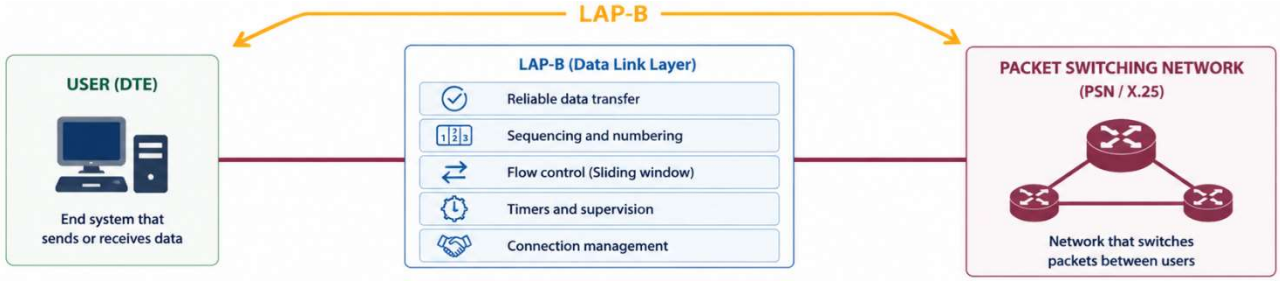


Fig.39. : Access via LAP-B.

The objective of the frame level is to:

- Protect against transmission errors.
- Provide overall flow control at the user-network interface.

3.3. Packet level

The objective of the packet level is to:

- Provide interconnection between two network users through a virtual circuit (VC).
- Allow a user to open (create) multiple virtual circuits, enabling the management of multiple simultaneous communications (multiplexing).

a. Virtual circuit management :

- A virtual circuit consists of establishing communication between two users.

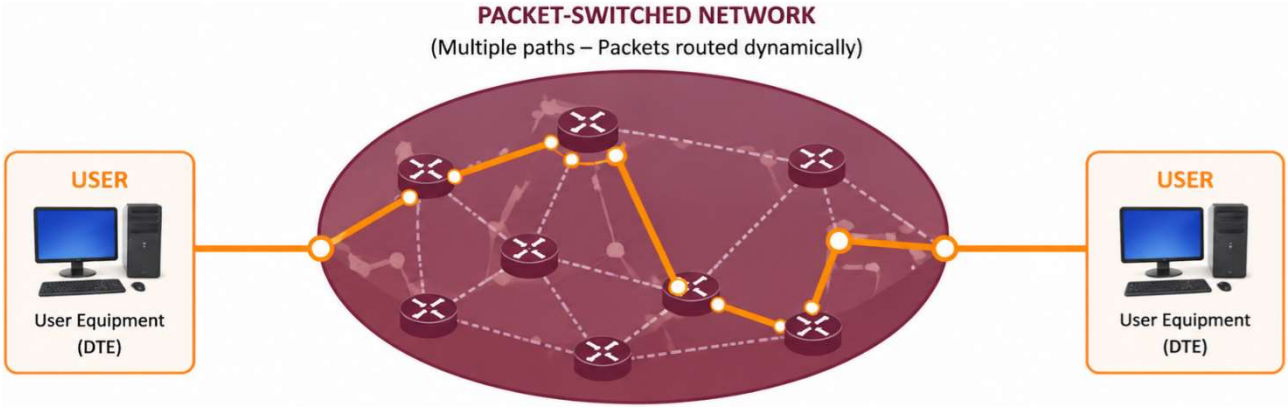


Fig.40. : Virtual circuit management.

b. Types of virtual circuits :

- In the X.25 protocol, communication between two devices is established using virtual circuits, which are logical connections created within the packet-switched network. There are two main types :

1. Switched Virtual Circuit (SVC)

A Switched Virtual Circuit is a temporary connection established only when needed.

- Characteristics:
  - Created dynamically before data transmission
  - Requires a call setup phase
  - Released after communication ends
  - Similar to a telephone call
- Phases:
  - Call setup
  - Data transfer
  - Call clearing

2. Permanent Virtual Circuit (PVC)

A Permanent Virtual Circuit is a pre-established, always available connection.

- Characteristics:
  - Configured in advance by the network provider.
  - No call setup required.
  - Always ready for data transmission.
  - Used for frequent.

Here is the English translation:

The packet level manages the virtual circuits established by the user with remote devices by ensuring:

- The establishment and release of switched virtual circuits.

- The transfer of data in the form of packets.
- Control of data transmission.
- Error management.

c. Logical channel :

To allow the simultaneous coexistence of multiple virtual communications, communication identifiers called Logical Channel Numbers (LCN) are used.

A Logical Channel Number (LCN) is assigned to each permanent virtual circuit (PVC) when the subscription is established.

In the case of a switched communication (SVC), the logical channel number is assigned during the virtual circuit setup phase.

- In theory, X.25 supports up to 4096 virtual channels (VCs).
- In practice, 256 logical channels are supported by equipment.

The format of X.25 Layer 3 packets is as follows :

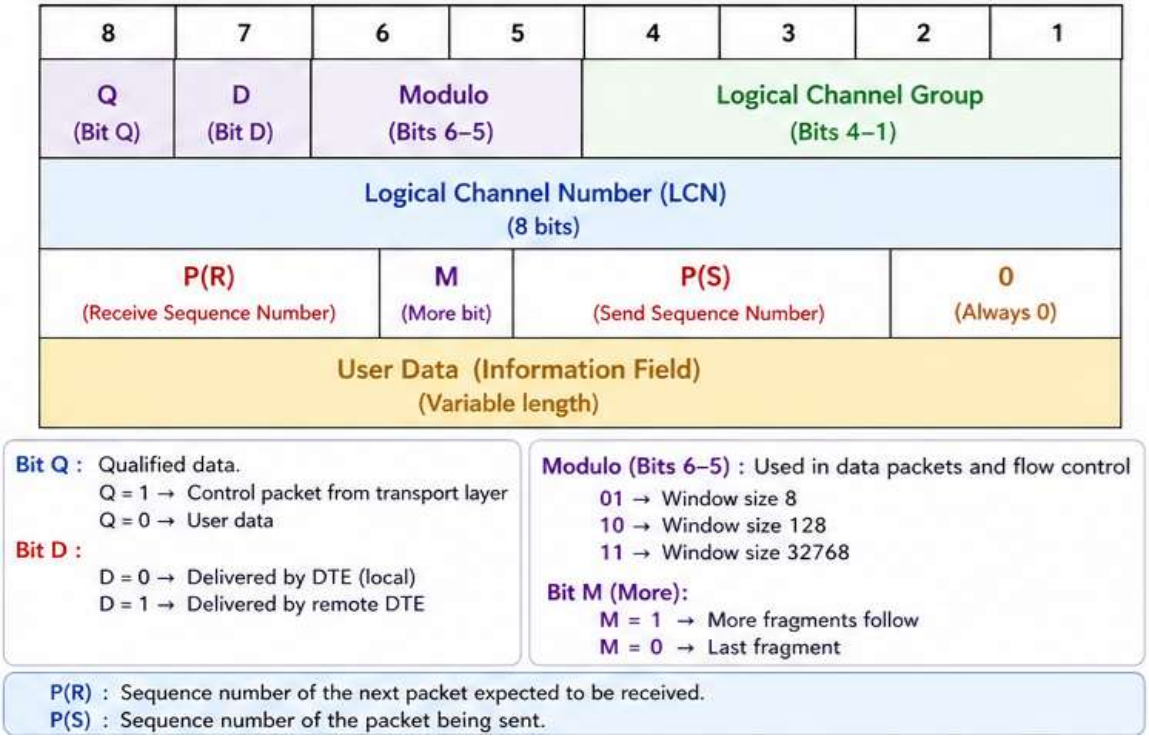


Table.6 : X.25 Layer 3 Packet.

Packet Type	Packet Identifier (7 bits)							CM (1 bit)
	P	P	P	M	S	S	S	
Data	P	P	P	M	S	S	S	0
Call Request	0	0	0	0	1	0	1	1
Call Accepted	0	0	0	0	1	1	1	1
Clear Request	0	0	0	1	0	0	1	1
Clear Confirmation	0	0	0	1	0	1	1	1
Interrupt	0	0	1	0	0	0	1	1
Interrupt Confirmation	0	0	1	0	0	1	1	1
RR (Receive Ready)	P	P	P	0	0	0	0	1
RNR (Receive Not Ready)	P	P	P	0	0	1	0	1
REJ (Reject)	P	P	P	0	1	0	0	1
Reset Request	0	0	0	1	1	0	1	1
Reset Confirmation	0	0	0	1	1	1	1	1
Restart Request	1	1	1	1	1	1	0	1
Restart Confirmation	1	1	1	1	1	1	1	1
Diagnostic	1	1	1	1	0	0	0	1

Table.7 : Packet Identifier Field.

CM Bit:

- Data packet ⟶ CM = 0.
- Control packet ⟶ CM = 1.

PACKET TYPE		PACKET IDENTIFIER (7 BITS)							CM (1 BIT)
FROM DTE TO DCE (ETCD → ETTD)	FROM DCE TO DTE (ETTD → ETCD)	P	P	P	M	S	S	S	
		8	7	6	5	4	3	2	1
CALL ESTABLISHMENT AND RELEASE									
Incoming Call	Call	0	0	0	0	1	0	1	1
Call Established	Call Accepted	0	0	0	0	1	1	1	1
Clear Indication	Clear Request	0	0	0	1	0	0	1	1
Clear Confirmation by DCE	Clear Confirmation by DTE	0	0	0	1	0	1	1	1
DATA AND INTERRUPT									
Data from DTE	Data from DTE	X	X	X	X	X	X	X	0
Interrupt by DTE	Interrupt by DTE	0	0	1	0	0	0	1	1
Interrupt Confirmation by DCE	Interrupt Confirmation by DCE	0	0	1	0	0	1	1	1
FLOW CONTROL AND RESET									
RR (Receive Ready) – Modulo 8	RR (Receive Ready) – Modulo 8	X	X	X	0	0	0	0	1
RR (Receive Ready) – Modulo 128	RR (Receive Ready) – Modulo 128	0	0	0	0	0	0	0	1
RNR (Receive Not Ready) – Modulo 8	RNR (Receive Not Ready) – Modulo 8	X	X	X	0	0	1	0	1
RNR (Receive Not Ready) – Modulo 128	RNR (Receive Not Ready) – Modulo 128	0	0	0	0	0	1	0	1
REJ (Reject) – Modulo 8	REJ (Reject) – Modulo 8	X	X	X	0	1	0	0	1
REJ (Reject) – Modulo 128	REJ (Reject) – Modulo 128	0	0	0	0	1	0	0	1
Reset Indication	Reset Request	0	0	0	1	1	0	1	1
Reset Confirmation	Reset Confirmation	0	0	0	1	1	1	1	1
RESTART									
Restart Indication	Restart Request	1	1	1	1	1	1	0	1
Restart Confirmation	Restart Confirmation	1	1	1	1	1	1	1	1
DIAGNOSTIC									
Diagnostic	Diagnostic	1	1	1	1	0	0	0	1
REGISTRATION (OPTIONAL)									
Registration Confirmation	Registration Request	1	1	1	1	0	0	1	1

Table.8 : Global Packet Identifier Field.

X.25 PACKET LAYER (NAP / PLP)

- The Packet level (NAP: Network Access Protocol or PLP: Packet Layer Protocol): operates according to the same logic, with specialized packets.
- The NAP (or X25 PLP) defines 3 categories of packets:

1 COMMAND PACKETS

To open the line, establish and release Virtual Circuits:

- ✓ RESTART : Open : reset the PHYSICAL line (cuts off all VCs on this line !!)
- ✓ CALL Request : call packet : establishment of 1 VC.
- ✓ CALL Accepted : Call confirmation, establishment of the VC.
- ✓ CLEAR Request : request to release (close) the VC, or refusal to accept an incoming call.
- ✓ CLEAR Confirmed : confirmation of release (close) of the VC.

NOTE: All of the above applies only to switched VCs; permanent VCs remain open.

2 SUPERVISORY PACKETS

To manage flow control and acknowledgments.

- ✓ RR : Receive Ready, RNR : Receive Not Ready, REJ : Reject Packet.

NOTE: These packets have only a local value (from one X.25 switch to another) and not end-to-end !!!!

3 DATA PACKETS

- ✓ Carry user information in numbered packets, and also carry acknowledgments.

Abbreviations:
NAP : Network Access Protocol
PLP : Packet Layer Protocol
VC : Virtual Circuit
CV : Circuit Virtuel
RR : Receive Ready
RNR : Receive Not Ready
REJ : Reject Packet

Table.9 : X.25 Packet Layer (NAP/PLP).

d. Flow control :

- Allows a receiver to limit the rate at which a sender transmits its data packets.

e. Multiplexing :

- Allows a subscriber to establish multiple communications (called virtual circuits) over the same physical medium.

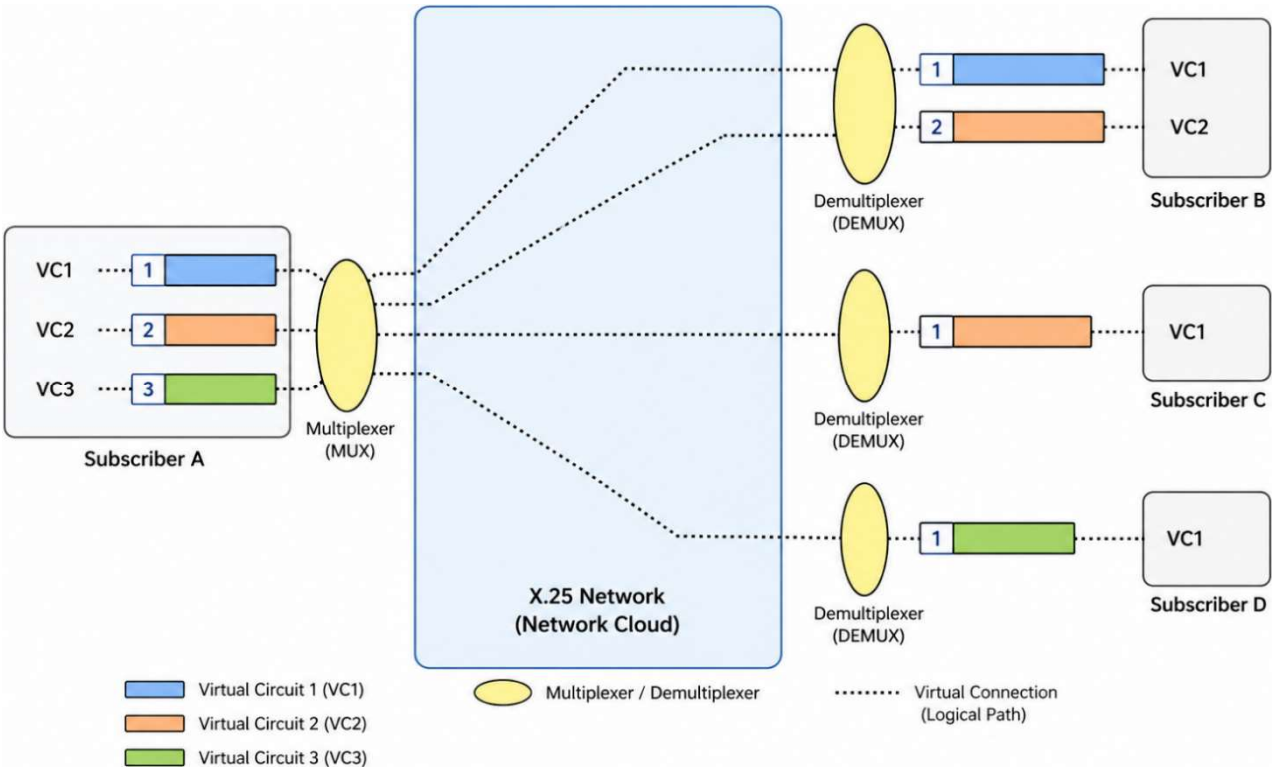


Fig.41. : Multiplexing of VC.

f. Example of X.25 connection :

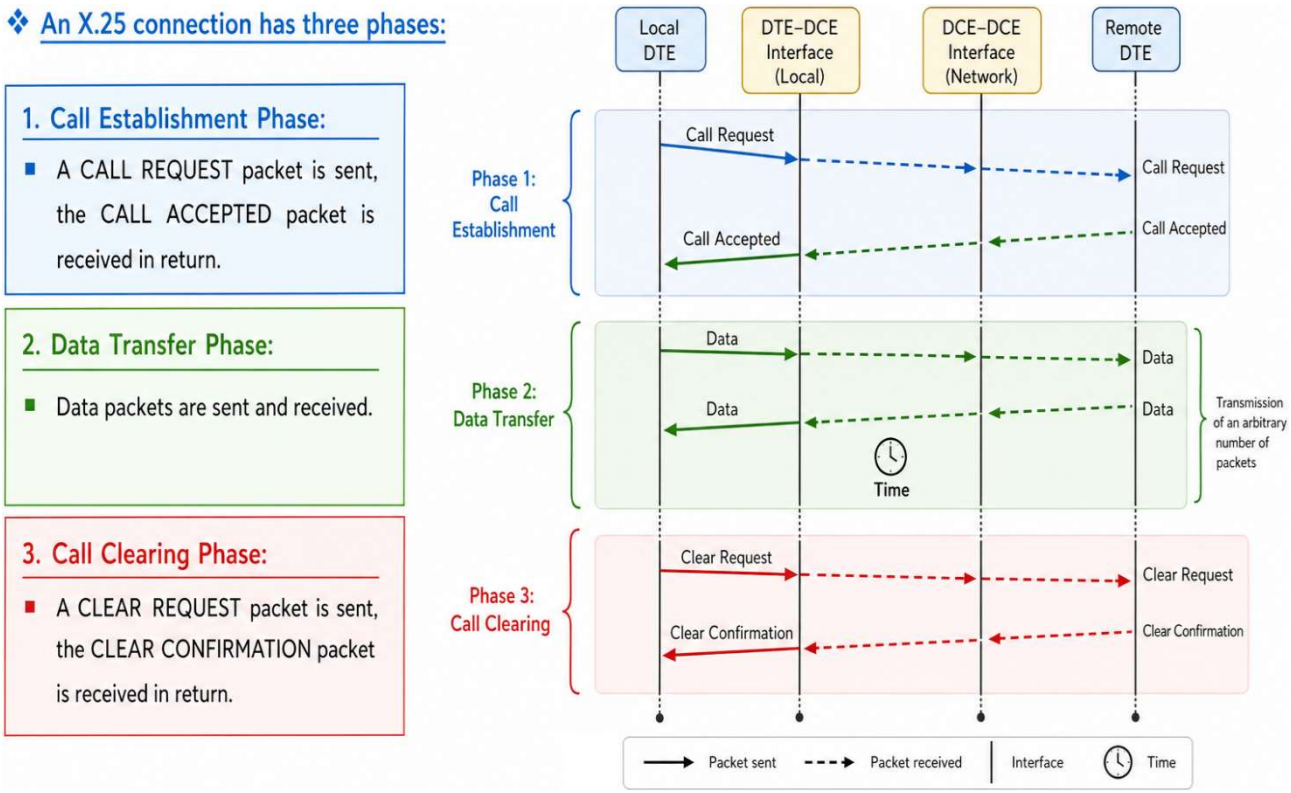


Fig.42. : Three phases of X.25 connection.

3. Advantages of X.25 networks :

- Very significant increase in the efficiency of transmission channels.
- High protection against transmission errors.
- High network availability.
- Compliance with international standards and connectivity with networks in other countries.
- Reduced costs, independent of distance, mainly based on the volume of data transmitted.

4. Main uses of X.25 networks :

- Conversational (interactive) applications.
- Data entry with delayed transmission.
- Batch processing (teleprocessing).
- Interconnection of computers or networks.

Note :

- The PVC (Permanent Virtual Circuit) is established permanently, which eliminates the connection setup phase and therefore saves time. It is useful when there is regular traffic on the line, but it increases telecom costs.

- The SVC (Switched Virtual Circuit), on the other hand, requires a connection setup phase. During this phase, options are negotiated and a logical channel number is assigned.
- To establish communication, the packet type used is: "CALL REQUEST."

5. **X.25 in a few figures :**
   - Packet size: 128 bytes.
   - Packet window: 2–3.
   - Initial data rate: 4800 / 19200 bps, then 512 Kbps (with X25-2G, up to 2 Mbps).
   - Services offered by TRANSPAC.
   - More than 100,000 access points from 300 bps to 256 Kbps.
   - Setup costs are relatively high (monthly subscription depending on speed, transmission cost based on duration and volume).
6. **Example of X.25 configuration in Cisco Packet Tracer :**

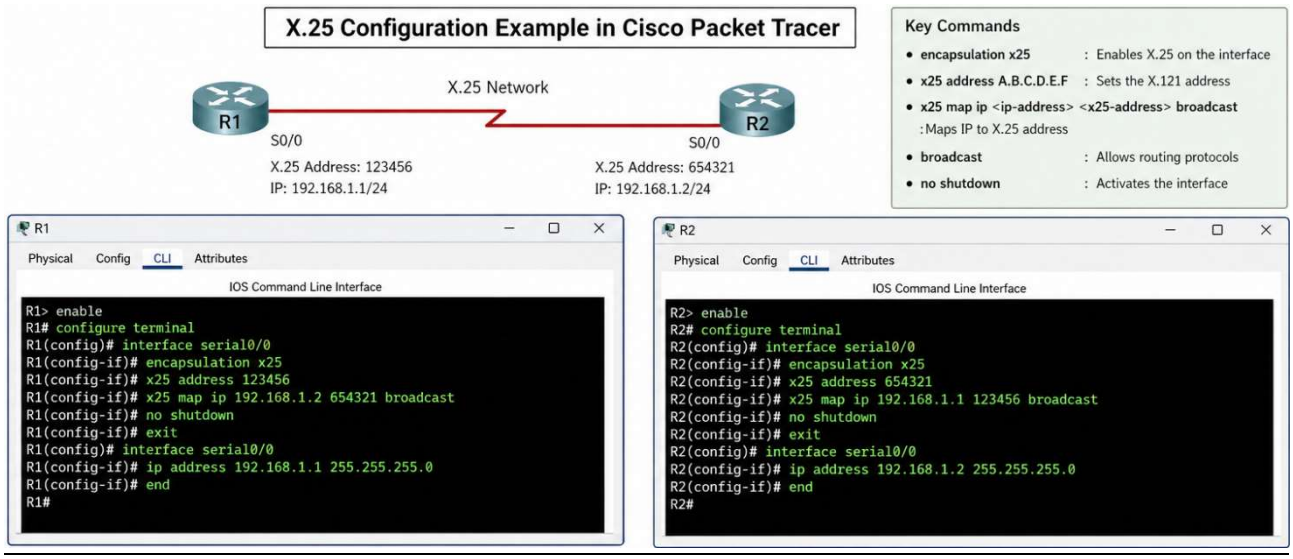


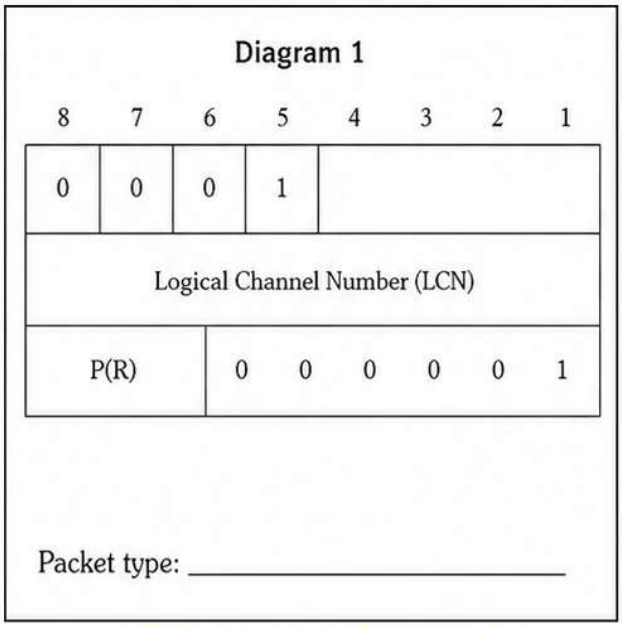
Fig.43. : X.25 configuration in Cisco Packet Tracer.

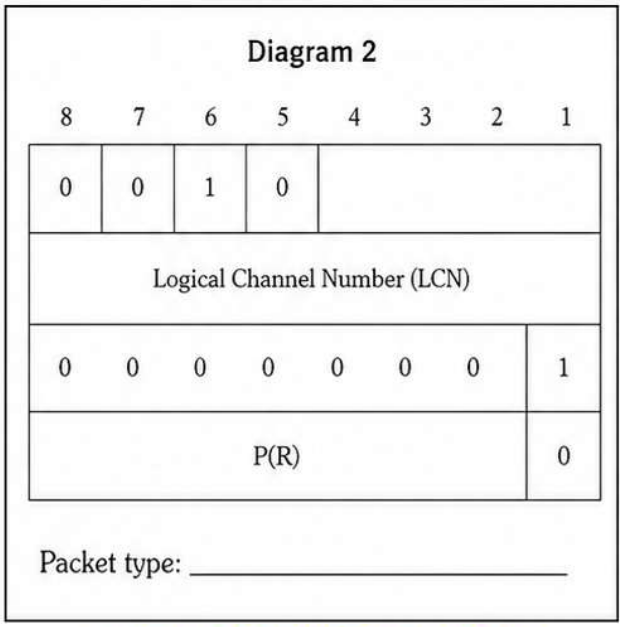
7. **Conclusion**

X.25 was a foundational packet-switching protocol that played a critical role in the early development of data communication networks. Designed to ensure reliable transmission over unreliable analog lines, it introduced concepts such as error correction, flow control, and virtual circuits. While its robust reliability made it widely adopted in the past, its complexity and overhead led to its gradual replacement by faster and more efficient technologies like Frame Relay, ATM, and eventually IP-based networks. Today, X.25 remains largely obsolete, but its influence persists in the evolution of modern networking protocols and the principles of reliable data transmission

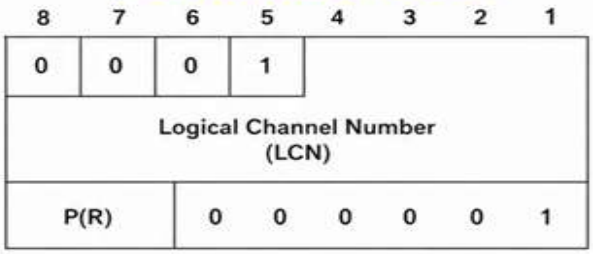
8. Exercise to be done :

- List the types of packets in the X.25 protocol ?



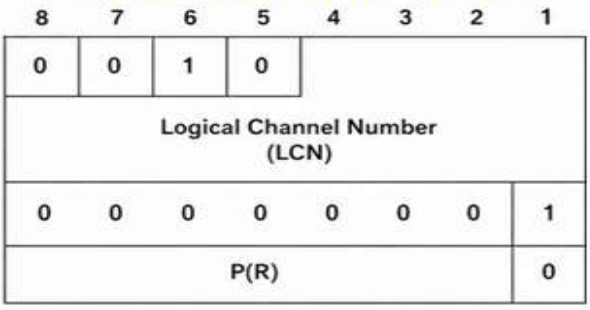


1) CALL REQUEST PACKET

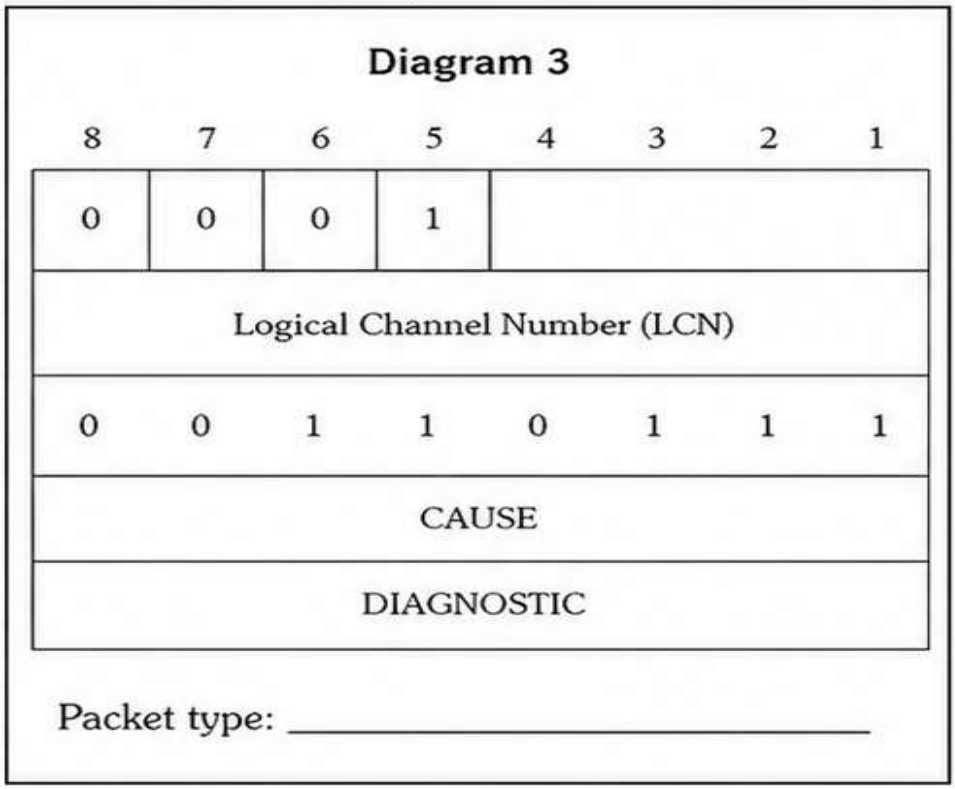


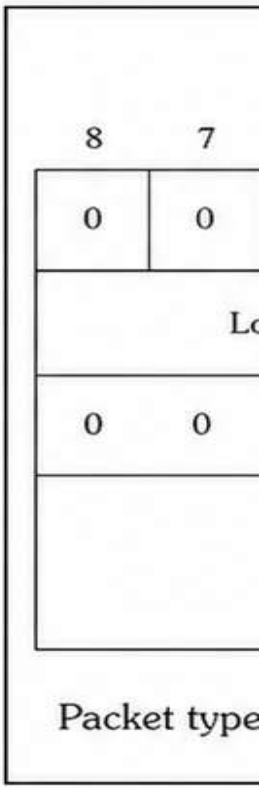
(Sent to request the establishment of a virtual circuit)

2) CALL ACCEPTED PACKET



(Sent in response to CALL REQUEST)





3) CLEAR REQUEST PACKET

8	7	6	5	4	3	2	1
0	0	0	1				
Logical Channel Number (LCN)							
0	0	1	1	0	1	1	1
CAUSE							
DIAGNOSTIC							

(Sent to request the clearing of a virtual circuit)

4) DATA PACKET

8	7	6	5	4	3	2	1
0	0	0	1				
Logical Channel Number (LCN)							
0	0	1	0	0	0	0	1
User Data (1 to 32 octets)							

(Carries user information)

Diagram 5

8	7	6	5	4	3	2	1
0	0	1	0				
Logical Channel Number (LCN)							
0	0	0	0	0	1	0	1
P(R)							0

Packet type: _____

Diagram 6

8	7	6	5	4	3	2	1
0	0	0	1				
Logical Channel Number (LCN)							
0	0	1	0	0	1	1	1

Packet type: _____

5) RR (RECEIVE READY) PACKET

8	7	6	5	4	3	2	1
0	0	1	0				
Logical Channel Number (LCN)							
0	0	0	0	0	1	0	1
P(R)							0

(Positive acknowledgment)

6) REJECT PACKET

8	7	6	5	4	3	2	1
0	0	0	1				
Logical Channel Number (LCN)							
0	0	1	0	0	1	1	1

(Indicates that a packet has been rejected)

Unit 2 : Frame Relay Protocol.

Unit Objectives :

By the end of this unit, you should be able to:

- Understand the concept and architecture of Frame Relay networks.
- Explain how Frame Relay improves over X.25.
- Identify and describe virtual circuits (PVC & SVC).
- Understand the role of Data Link Connection Identifier (DLCI).
- Analyze Frame Relay frame structure and fields.
- Explain congestion control mechanisms (FECN, BECN, DE bits).
- Evaluate advantages, limitations, and applications of Frame Relay.

Topics Covered :

- Introduction : Basics of Frame Relay and its evolution from X.25.
- Architecture : Components like DTE, DCE, and the network cloud.
- Virtual Circuits : PVC (permanent) and SVC (switched) connections.
- Frame Format : Structure of a Frame Relay frame and its fields.
- DLCI : Identifier used to distinguish virtual circuits.
- Congestion Control : Mechanisms like FECN, BECN, and DE.
- Error Handling : Detection only (no correction, relies on upper layers).
- Traffic Management : CIR, burst rates, and bandwidth control.
- Advantages & Limitations : Speed and efficiency vs limited reliability.
- Applications : Used in WANs and enterprise network connections.

1. Introduction

Frame Relay is a high-performance wide area network (WAN) protocol that operates at the data link layer (Layer 2) of the OSI model. It was designed to provide fast and efficient data transmission for intermittent traffic between local area networks (LANs) and between endpoints in a WAN.

Unlike older protocols such as X.25, Frame Relay reduces overhead by eliminating extensive error correction and flow control mechanisms. Instead, it relies on the reliability of modern digital transmission systems, which allows for faster data transfer speeds.

2. Definition

It is a Packet-switching protocol standardized by the ITU-T and ANSI (American National Standards Institute). It was invented by **Eric Scace**, an Engineer at **Sprint International**. Frame Relay is indeed the result of an American initiative.

FR is a Layer 2 protocol (data link layer) of the OSI model. It uses a technique called packet switching, where data is transmitted in units called frames. These frames travel across a shared network infrastructure using virtual circuits, which can be either:

- Permanent Virtual Circuits (PVCs) : Always available connections.
- Switched Virtual Circuits (SVCs) : Temporary connections established when needed.

Each frame contains addressing information known as the Data Link Connection Identifier (DLCI), which helps route the data to its correct destination.

One of the key advantages of Frame Relay is its ability to efficiently handle bursty data traffic, making it suitable for applications that require variable bandwidth. However, with the rise of newer technologies such as MPLS and broadband networks, Frame Relay is now considered largely obsolete.

Its purpose is to:

- Provide error checking.
- Be used for intersite communication (WAN).
- Replace leased lines (which are expensive because they are dedicated to a single client) with a shared Frame Relay "cloud" used by multiple customers.
- Support multi-access networks, similar to LAN protocols.
  - ✓ Multiple devices can be connected to the Frame Relay network.
- Operate as a Non-Broadcast Multi-Access network (NBMA).
  - ✓ It is not possible to send a frame to multiple devices at the same time.

From a technical perspective, it can be seen as:

- A successor to X.25.

- A step toward ATM (Asynchronous Transfer Mode).
- Part of ISDN (Integrated Services Digital Network).

3. Functioning

a) Devices :

Devices connected to a WAN are classified into :

- DTE (Data Terminal Equipment).
- DCE (Data Circuit Equipment).

DTEs are generally end devices located at the edge of the customer network, such as routers or Frame Relay Access Devices (FRADs) :

- ✓ FRAD : a specialized device that provides a connection between a LAN and a Frame Relay WAN.

DCEs are devices located within the core of the network and provide synchronization services between equipment as well as switching functions.

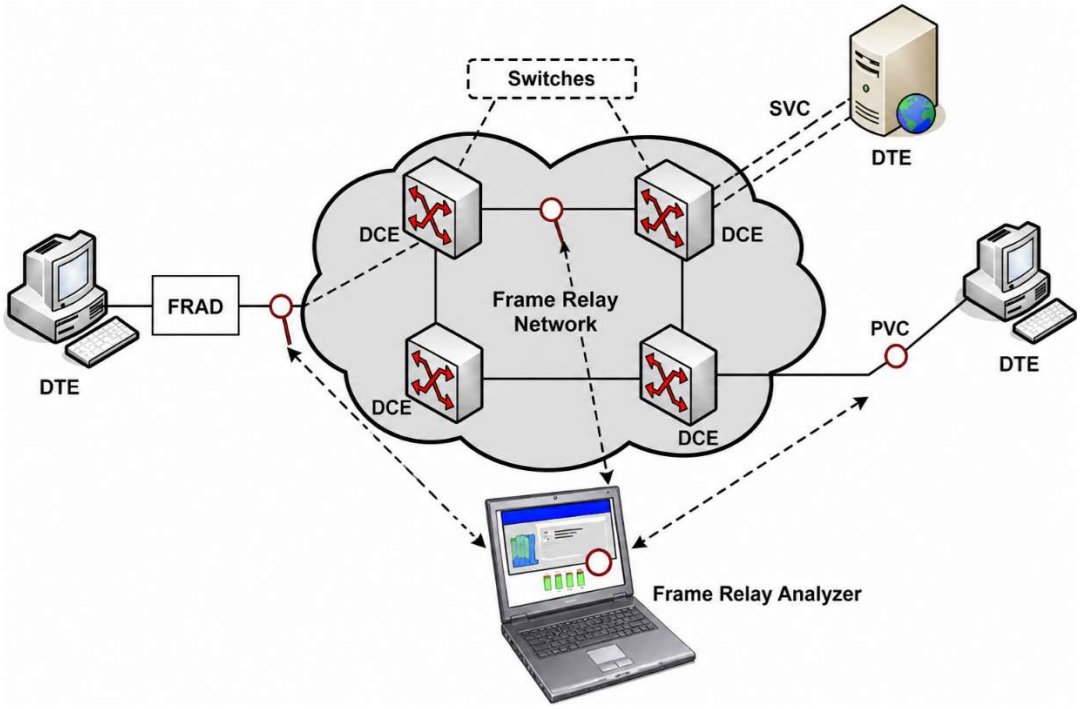


Fig.44. : Frame Relay Architecture.

b) Physical Characteristics :

- DTEs are connected to Frame Relay switches (considered as DCEs) through dedicated lines.
- These links are called access links, over which messages defined by the Local Management Interface (LMI) protocol are periodically transmitted.

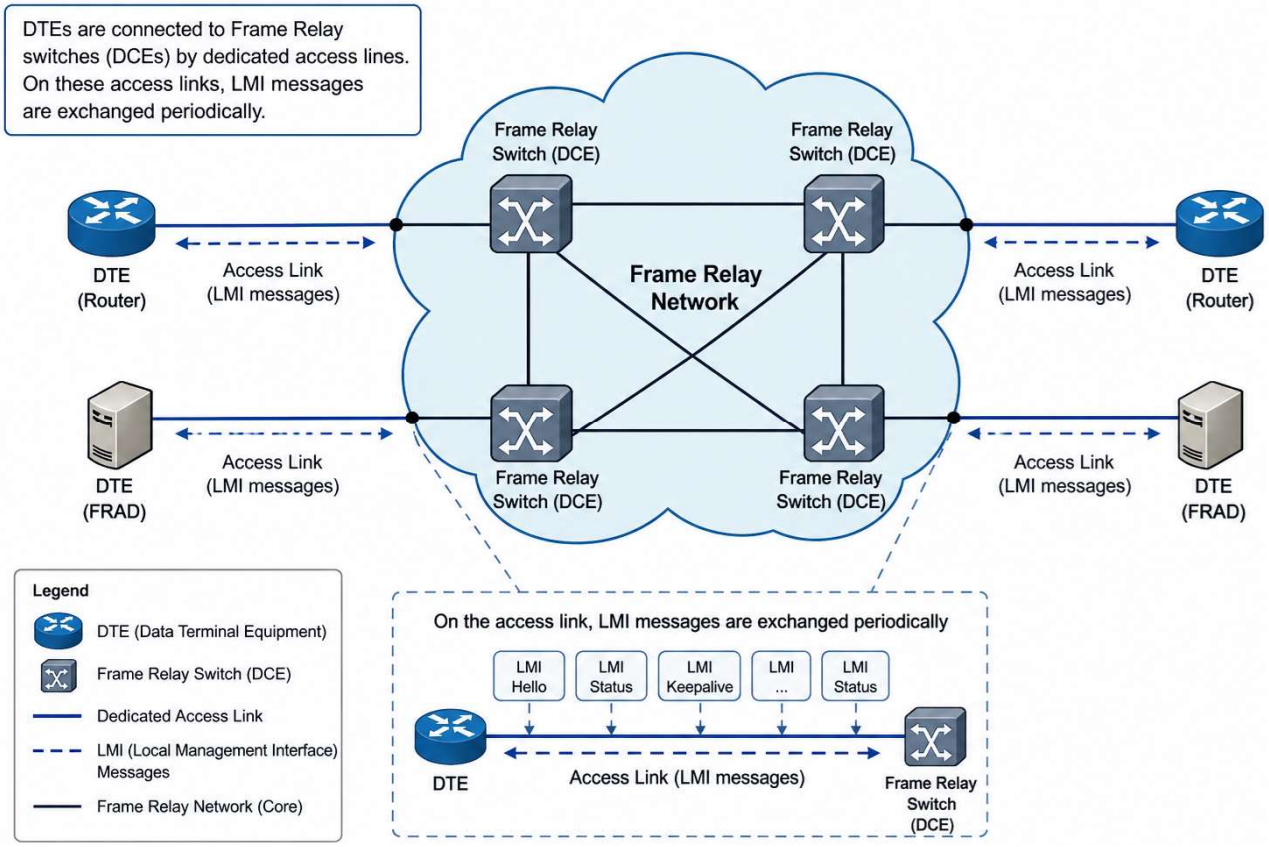


Fig.45. : Physical Characteristics of Frame Relay.

4. Different Frame Relay topologies

Among the topologies used in Frame Relay networks, three types can be distinguished:

a) Hub-and-Spoke topology
b) Full Mesh topology
c) Partial Mesh topology

a) Hub-and-Spoke topology :

In this topology, routers R2, R3, and R4 are connected through virtual circuits PVC1, PVC2, and PVC3 via a central router (Hub).

The number of PVCs used is: **n – 1**.

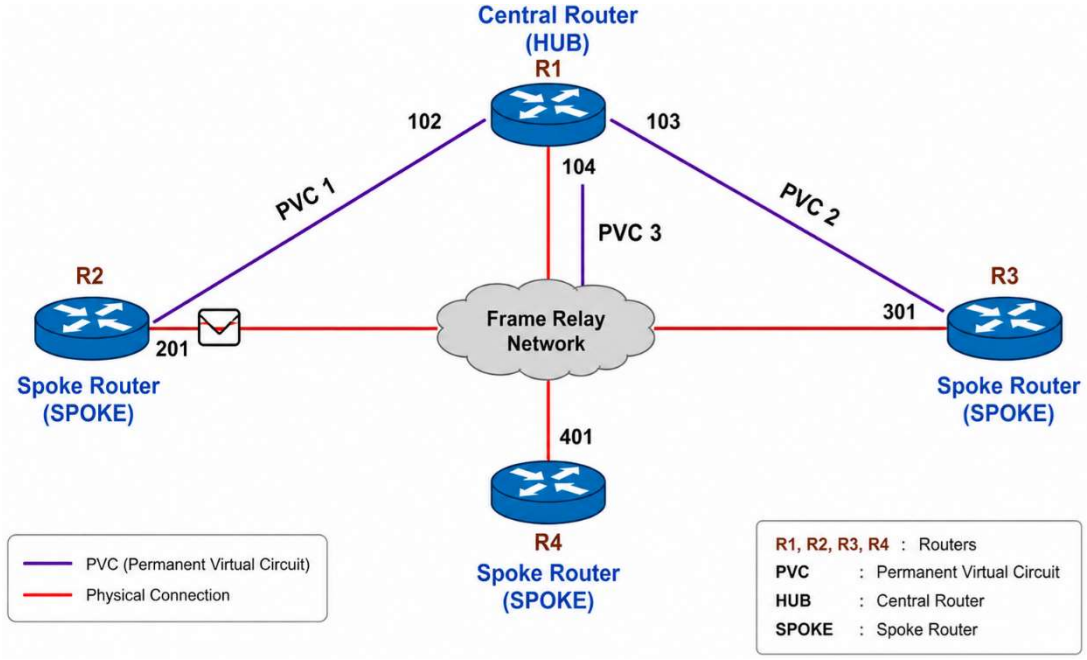


Fig.46. : Hub-and-Spoke topology.

b) Full Mesh topology :

In this topology, the four routers (R1, R2, R3, and R4) are connected by PVC virtual circuits, and the number of PVCs used is: **n × (n – 1) / 2.**

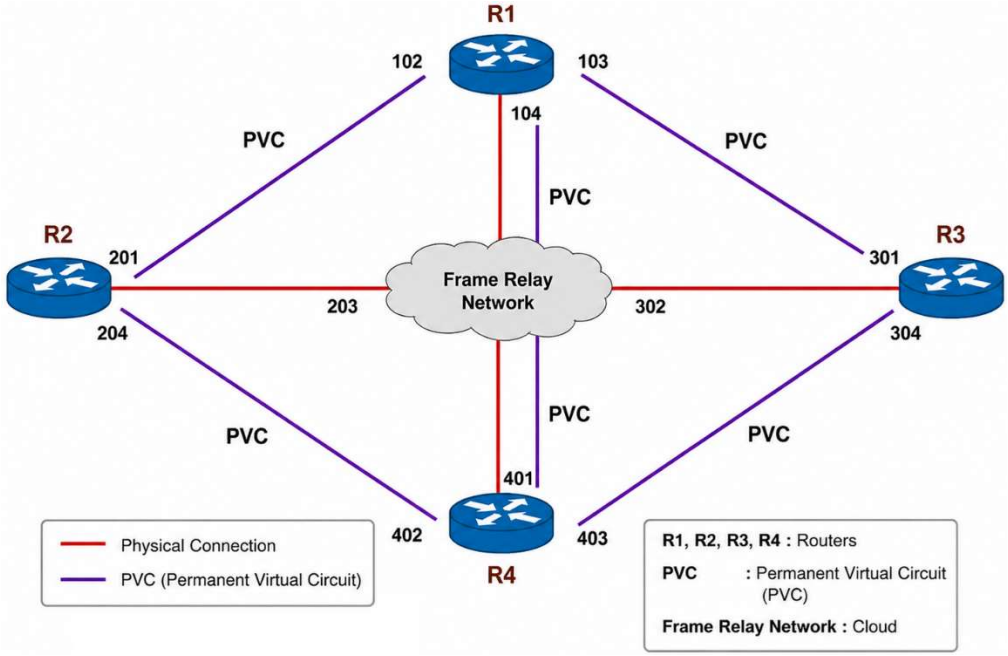


Fig.47. : Full Mesh topology.

c) Partial Mesh topology :

In this topology, router R3 communicates with R4 via router R1.

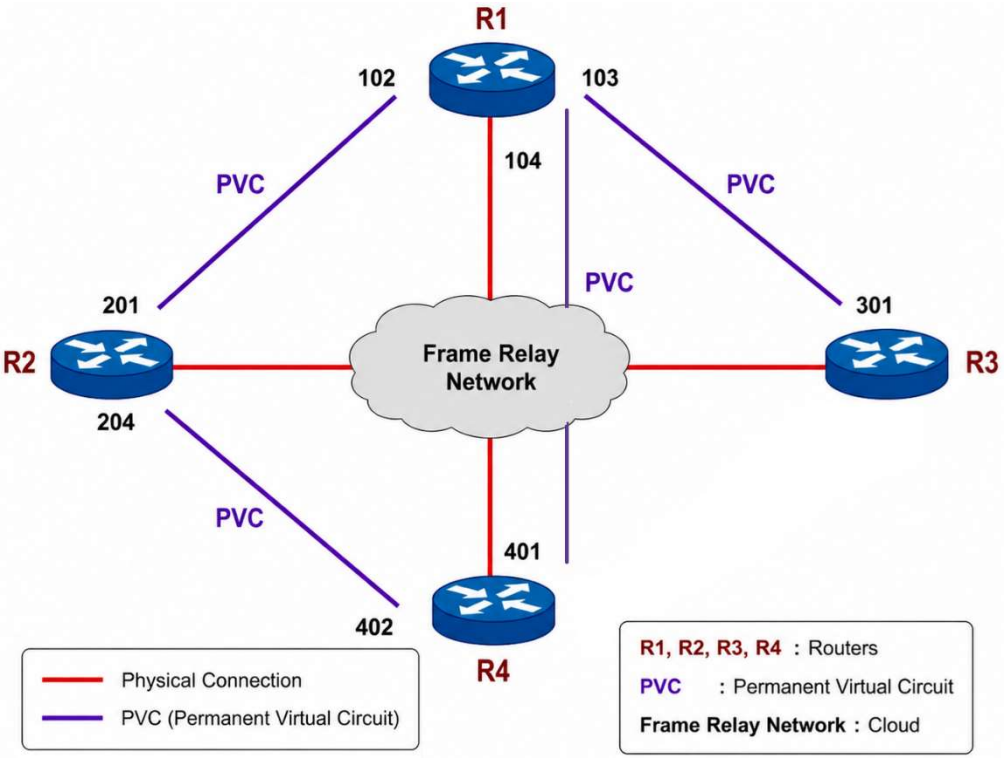


Fig.48. : Partial Mesh topology.

5. Advantages

- The greater the distance covered by a dedicated line, the more expensive the service becomes:
  - ✓ Maintaining a full mesh between all remote sites using this type of line is too costly for most companies.
- Packet-switched networks provide multiplexing of multiple data streams over a single communication link:
  - ✓ Service providers can design more cost-effective networks compared to leased lines.
  - ✓ In this case, packet-switched networks use virtual circuits to route data between users across a shared infrastructure.

6. Virtual Circuits

- A virtual circuit defines a logical path between two endpoints (two Frame Relay DTEs) :
  - ✓ It allows the creation of a point-to-point connection between two devices across a WAN without an actual physical circuit directly connecting them.
- Routers use Data-Link Connection Identifiers (DLCIs) as Frame Relay addresses :
  - ✓ DLCIs identify the virtual circuits (VCs) used to transmit data to the destination.

- There are two types of virtual circuits: PVC and SVC:
  - ✓ PVCs are preconfigured by the service provider when the service is set up.
  - ✓ SVCs are established dynamically at the user's request.

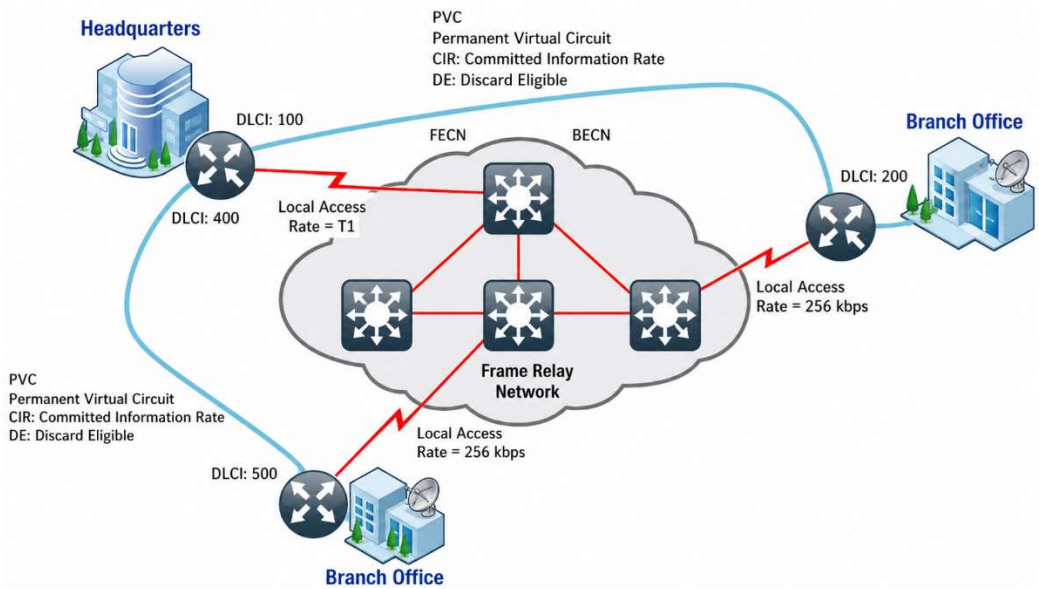


Fig.49. : Virtual Circuits.

- PVC is the most common circuit type in Frame Relay:
  - ✓ Establishes a permanent circuit used for frequent data exchanges between DTEs across a Frame Relay network. These correspond to preconfigured virtual circuits (VCs).
- SVC uses temporary circuits for occasional transfers between DTEs:
  - ✓ Their temporary nature requires setting up the connection and then disconnecting it for each session.
- Each virtual circuit is associated with a connection identifier:
  - ✓ A table is used by the provider to route data to the correct outputs, since identifying only the interface is not sufficient.
  - ✓ In Frame Relay, this identifier is called a Data-Link Connection Identifier (DLCI).

7. Data-Link Connection Identifier (DLCI)

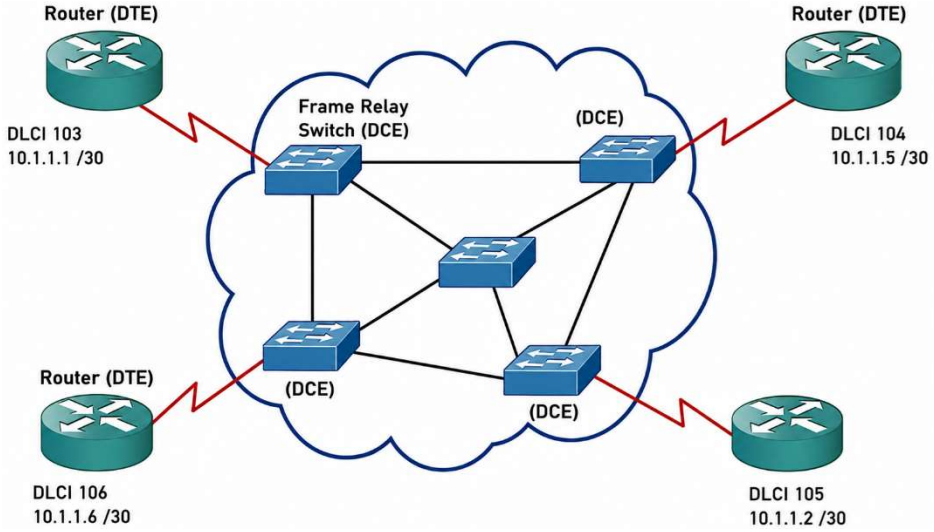


Fig.50. : Data-Link Connection Identifier (DLCI).

DLCIs have a local significance because the identifier refers to the point between the local router and the switch to which it is connected. Devices at the ends of the connection may identify the same virtual circuit using different DLCIs.

Note :

- Multiple VCs (Virtual Circuits) on the same access link are distinguished by their DLCIs.

8. Local Management Interface (LMI)

- LMI is a standard for signaling between a DTE and Frame Relay switches :
  - It is responsible for connection management and maintaining the status between devices.
- It supports the following mechanisms :
  - **Keepalive function** : maintains the connection. In case of access link failure, the absence of keepalive messages indicates that the line is unavailable.
  - **PVC status information** : indicates the existence of new PVCs, removal of existing ones, and integrity information about PVCs.
  - **Global addressing** : provides a global meaning to the addressing system instead of a local one.
- LMIs were developed independently of Frame Relay and implemented earlier. Therefore, there are three types of LMI (Cisco, ITU, ANSI) which are incompatible with each other :
  - Cisco uses DLCI 1023 for messages.
  - ANSI and ITU use DLCI 0.
- Due to the different LMI types, it is recommended to leave the default type on the equipment (DTE and DCE) :

- Thanks to LMI autosensing, the DTE attempts to automatically match the LMI type used by the DCE.

8.1. LMI Message Format :

Field sizes in octets.

1	2	1	1	1	1	variable	2	1
Flag	LMI DLCI 1023	UI	PD	CR	MT	Information	FCS	*Flag*
			LMI Header			Information Field		LMI Trailer

Flag	: Flag (01111110)	**PD**	: Poll/Final bit	**Information**	: Variable-length information field
LMI DLCI 1023	: DLCI used for LMI messages	**CR**	: Command/Response bit	**FCS**	: Frame Check Sequence (CRC)
UI	: Unnumbered Information	**MT**	: Message Type	**Flag**	: Flag (01111110)

Table.9 : LMI Message Format.

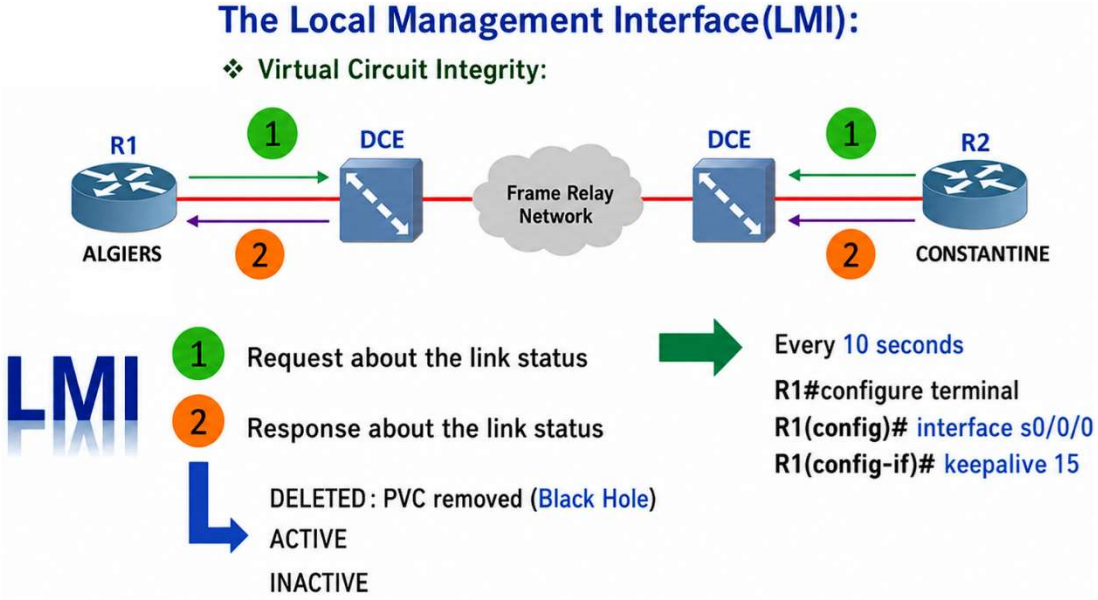


Fig.51. : The Local Management Interface (LMI).

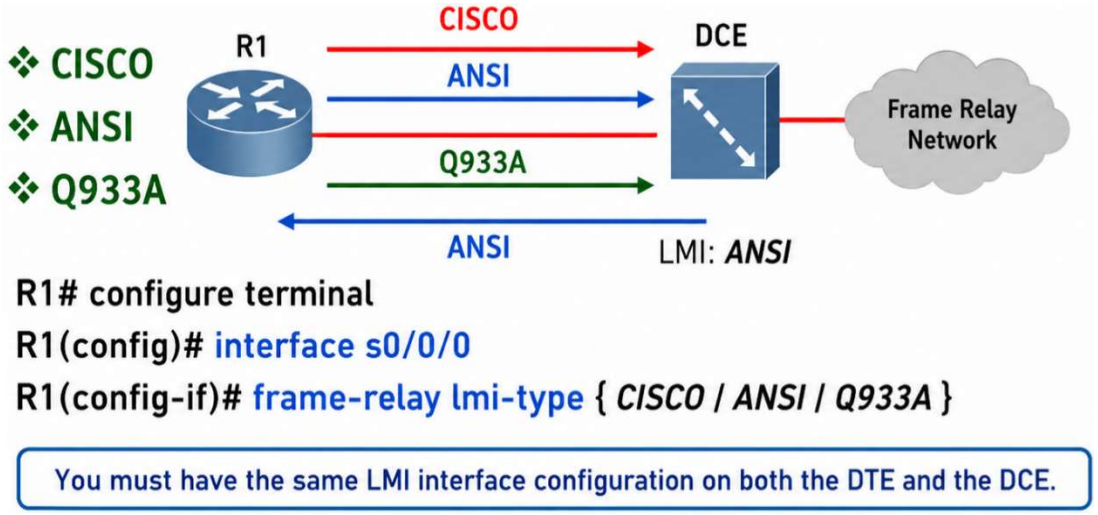


Fig.52. : LMI Type.

9. Frame Format

- Each Layer 3 packet is encapsulated at Layer 2 between a Frame Relay header and trailer.
- These two elements are defined in the specifications of the Link Access Procedure for Frame Bearer Services (LAPF).

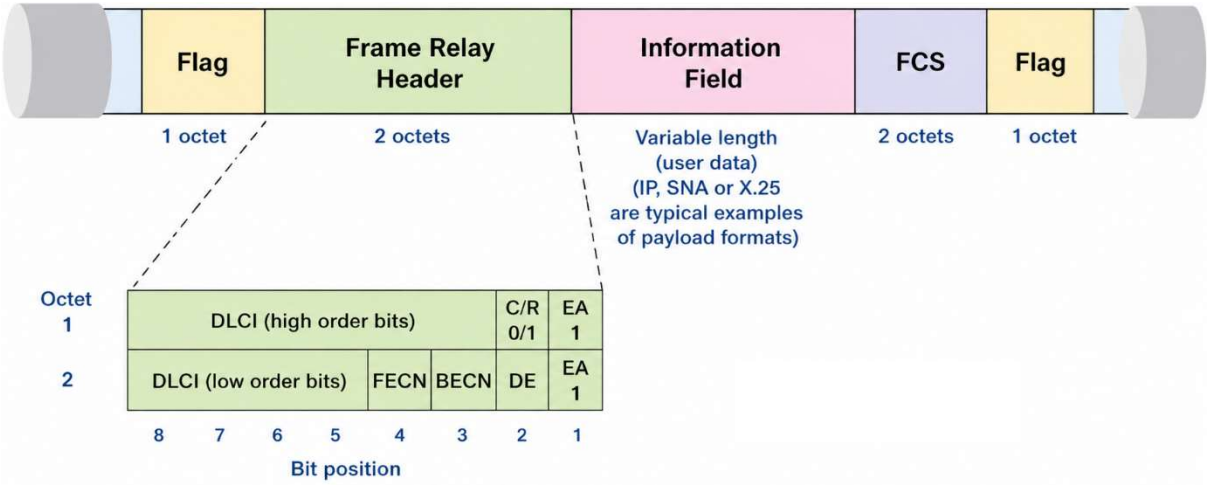


Fig.53. : Typical Frame Format FR.

9.1. Frame Relay header

- **DLCI (Data-Link Connection Identifier):**
  Contains the virtual link identifier = address field (it is included in the addressing part and is used to identify the virtual connection used by the frames).
  - ✓ Possible values range from 0 to 1023.
  - ✓ 0 and 1023 are reserved.
  - ✓ 1 to 15 and 1008 to 1022 are reserved for future use.
  - ✓ 992 to 1007 are reserved for Frame Relay Bearer Services (FRBS) Layer 2 managements.
  - ✓ 16 to 991 are available for user use.
- **FECN (Forward Explicit Congestion Notification) – sender :**
  - ✓ A bit used to indicate that congestion has occurred (the receiving device can notify a higher-layer protocol to take corrective action).
- **BECN (Backward Explicit Congestion Notification) – receiver :**
  - ✓ A bit used to inform a DTE that a congestion avoidance procedure has been initiated (a router receiving such a frame will reduce its transmission rate).
- **C/R (Command / Response) :**
  - ✓ An unused bit indicating whether the frame is a command or a response.
- **D/C = D/L (Core / Control) :**
  - ✓ Indicates whether the last octets contain DLCI bits or control bits (D/C = 0).

- **DE (Discard Eligibility) :**
  - ✓ A bit indicating frames that are eligible to be discarded first in case of congestion.
- **EA (Extended Address) :**
  - ✓ A bit indicating an extension of the addressing field.
- **Data :**
  - ✓ The maximum value is 262 octets (can be less than 1600 octets depending on implementation).
- **FCS (Frame Check Sequence) :**
  - ✓ Used to detect errors at the frame level.

10. DLCI Addressing

- A single DLCI field in the header, instead of two DLCI fields (source and destination).

10.1. Local Significance of the DLCI Field

- Addresses must be unique on the same access link, but not necessarily across the entire Frame Relay WAN.

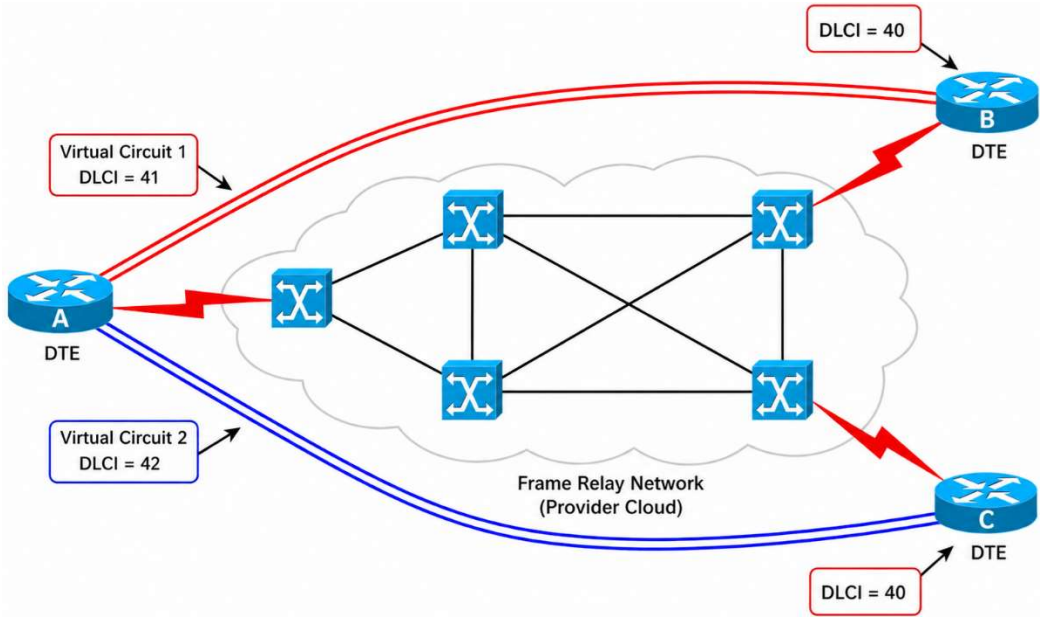


Fig.54. : Local Significance of the DLCI Field.

10.2. Global Significance of the DLCI Field

- The DLCI number is similar to a destination MAC address.
- The sender treats the DLCI field as a destination address by using the global destination DLCI.
- The receiver sees the DLCI field as a source address because it contains the global DLCI of the frame sender.

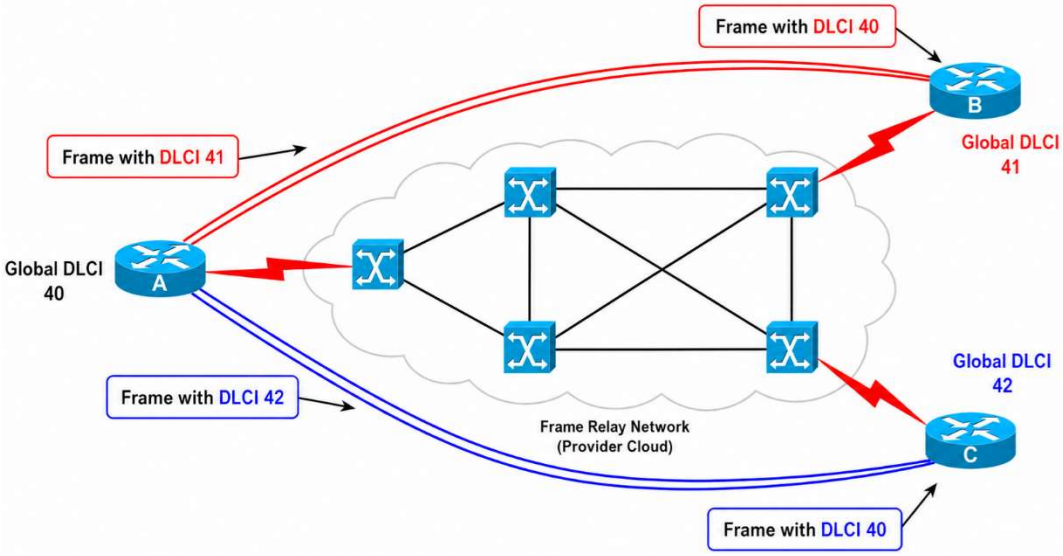


Fig.55. : Global Significance of the DLCI Field.

10.3. Address Mapping

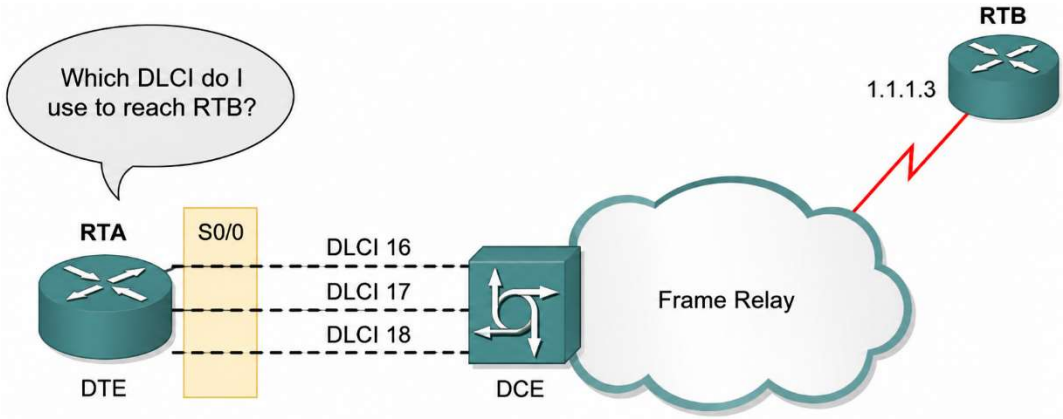


Fig.56. : Address Mapping.

- **Mapping between DLCIs and Layer 3 addresses :**
  Example : the ARP protocol in LANs.
  - ✓ How to establish a mapping between a Frame Relay router's Layer 3 address and the DLCI needed to reach it?
- **Mapping :**
  - ✓ The association established between a next-hop Layer 3 address and the corresponding Layer 2 address (DLCI) used to reach it. Especially important in the context of IP routing.
- **Two methods :**
  - ✓ Manual, using the Frame Relay map command (static configuration).
  - ✓ Dynamic, using Inverse ARP.
- **Inverse ARP :**

Inverse ARP was developed to provide a mechanism for dynamically mapping DLCIs to Layer 3 addresses :

- ✓ It works similarly to ARP in a LAN.
- ✓ In IP networks, ARP is used when a device knows the IP address and wants to find the MAC address.
- ✓ With Inverse ARP, the router knows the Layer 2 address (DLCI) and wants to discover the Layer 3 address.

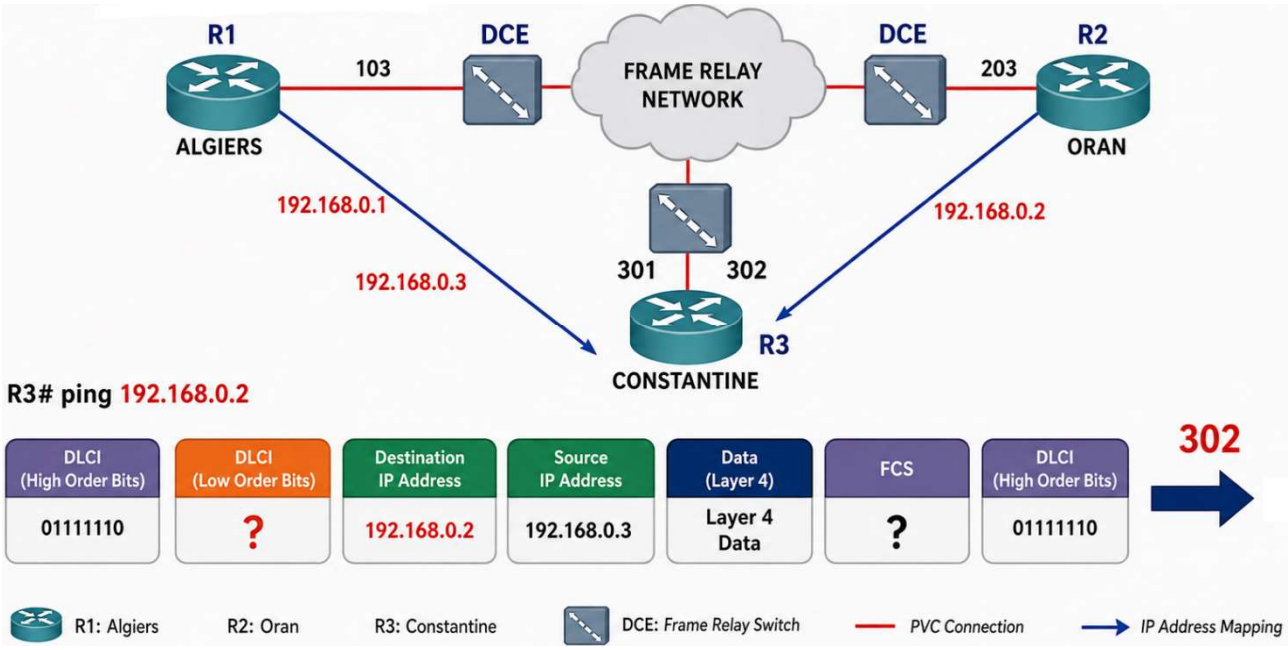
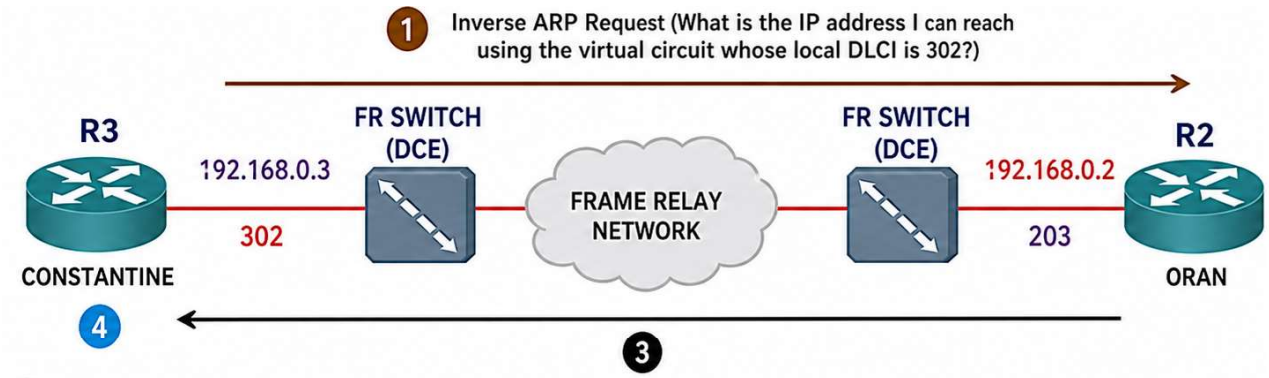


Fig.57. : Address Mapping 1.



1. Inverse ARP Request: What is the IP address I can reach using the virtual circuit whose local DLCI is 302?
2. The request arrives with DLCI 203 and IP address 192.168.0.3. So router R2 adds the mapping 192.168.0.3 : 203
3. Inverse ARP Reply: The IP address is 192.168.0.2
4. Router R3 adds the following mapping 192.168.0.2 : 302

Fig.58. : Address Mapping 2.

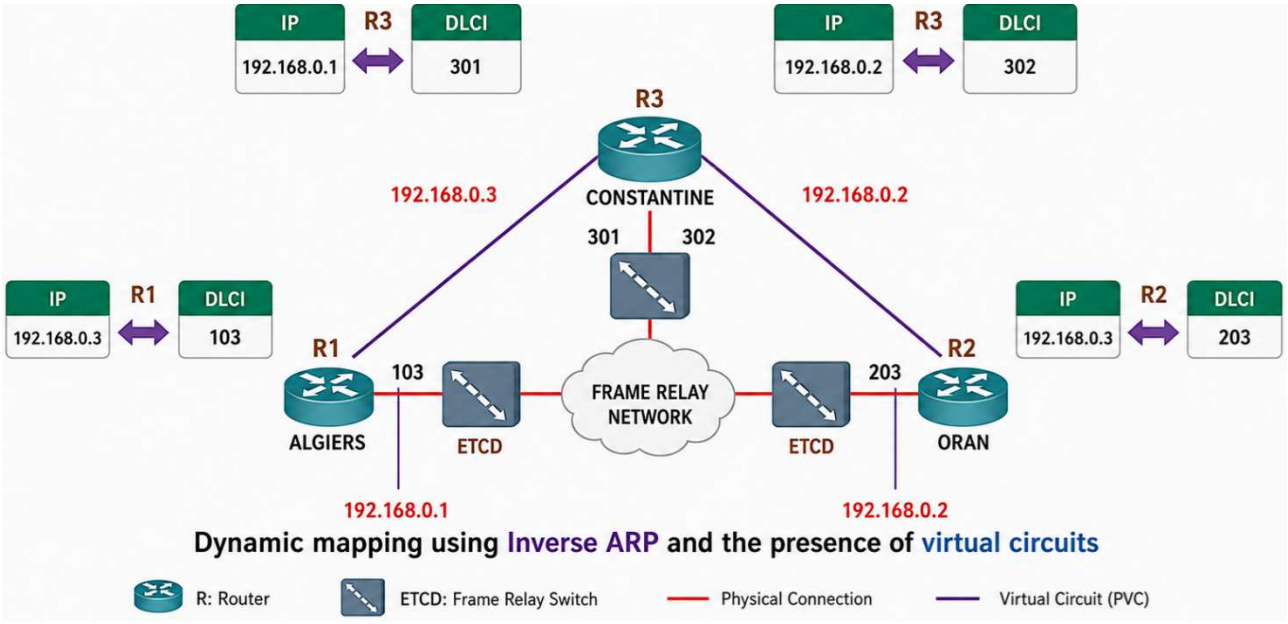


Fig.59. : Address Mapping 3.

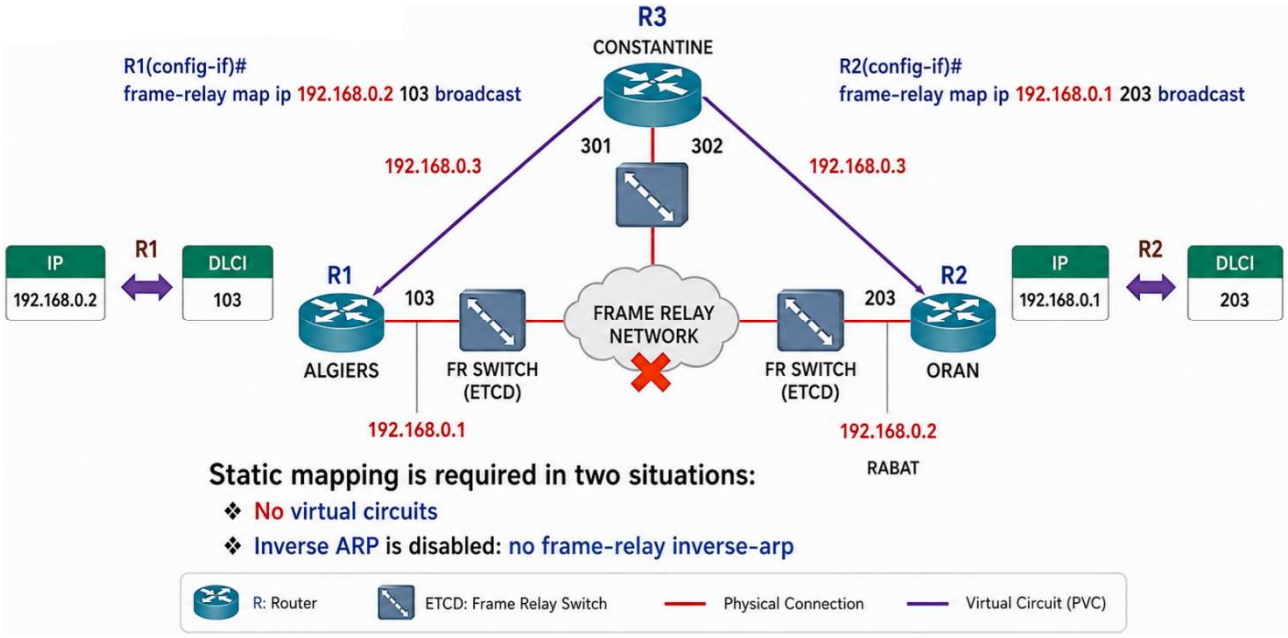


Fig.60. : Address Mapping 4.

11. Frame Relay in a few figures

- Frame size : approximately 1600 octets (bytes).
- Speeds range from 64 Kbps to 2 Mbps (extended up to 44 Mbps).
- Services provided by TRANSPAC.
- More than 1500 connection points.
- Access speeds from 64 Kbps to 2 Mbps.
- CIR (Committed Information Rate) from 4 to 384 Kbps.
- Network availability of 99.99%.
- Average latency of 40 ms and a maximum of 60 ms between two national access points.

- Data transported via Frame Relay costs about twice less than X.25 per megabyte.
- Switching times are 5 to 10 times faster than X.25.

12. Conclusion

X.25 offerings and products are gradually disappearing from catalogs. This suggests that Frame Relay is likely to prevail certainly compared to X.25, because its implementation as a replacement for X.25 networks is not very complex. It manages bandwidth dynamically, and transit times are almost cut in half compared to X.25.

However, Frame Relay does not yet fully meet all user needs. Multimedia and video applications require very high bandwidth, which only very fast switching technologies can provide. This is why many are turning their attention to ATM, although it still needs to prove itself. In the meantime, Frame Relay still has its place but for how long ?

13. Quiz with solution

1. **Which protocols can be encapsulated by Frame Relay? (Choose 4 correct answers).**
   a. Novell IPX.
   b. DECnet.
   c. AppleTalk.
   d. SNA.
   e. IP.
   f. SNMP.
   g. AAL.
2. **Which bits must be set in data frames so that a device reduces the data flow to or from a Frame Relay switch? (Choose one answer).**
   a. Window bits.
   b. ECN bits.
   c. DE bits.
   d. EIR bits.
   e. CIR bits.
3. **Why are full mesh topologies rarely used in large Frame Relay networks? (Choose one answer).**
   a. The number of required links becomes prohibitive.
   b. The slowdown in transmission speed is inversely proportional to the square of the number of links.
   c. They require additional interfaces because each interface supports only 10 virtual circuits.
   d. They require additional hardware to implement the mesh.
   e. Additional virtual circuits reduce access link speeds.
4. **Which data link layer protocol is used to transport frames over a Frame Relay link? (Choose one answer).**
   a. LAPF.
   b. HDLC.
   c. Frame Relay.
   d. LAPD.

e. PPP.

5. **The Frame Relay protocol performs static bandwidth allocation.**
   - ✓ False: X.
   - ✓ True: ……..

6. **What is the role of the Status Enquiry PDU (LMI signaling)? (Choose one answer).**
   a. Activate a tunnel configured in IPv6.
   b. Destroy a frame.
   c. Reset an active PVC.
   d. Request the status of a Frame Relay PVC.

Chapter III

ATM Networks & MPLS Protocol.

Unit 1 : ATM Networks.

Chapter Objectives :

By the end of this chapter, you should be able to :

- Understand the basic concepts of ATM (Asynchronous Transfer Mode) and MPLS (Multiprotocol Label Switching).
- Explain how ATM uses fixed-size cells and supports high-speed data transmission.
- Describe the architecture and components of ATM networks (switches, virtual paths, virtual channels).
- Understand the concept of Quality of Service (QoS) in ATM.
- Explain how MPLS improves packet forwarding using labels instead of IP lookups.
- Differentiate between ATM, Frame Relay, and MPLS technologies.
- Understand the advantages and limitations of ATM and MPLS.
- Identify real-world use cases for MPLS in modern networks.

Topics Covered :

- Introduction to ATM (Asynchronous Transfer Mode).
- Definition and characteristics.
- Evolution of ATM.
- ATM switches and interfaces.
- ATM Cell Structure.
- Virtual Circuits in ATM.
- Quality of Service (QoS) in ATM.
- Traffic classes (CBR, VBR, ABR, UBR).
- Traffic shaping and congestion control.
- Introduction to MPLS (Multiprotocol Label Switching).
- Basic concepts.
- Label switching mechanism.
- MPLS Architecture.
- MPLS Labels and Forwarding.
- Forwarding Equivalence Class (FEC).
- MPLS vs Traditional IP Routing.
- VPNs.
- Traffic Engineering (TE).

1. Introduction

ATM networks were a major step forward in networking, offering high-speed, reliable communication with guaranteed performance. Although largely obsolete today, the concepts of QoS and traffic management introduced by ATM are still widely used in modern networking technologies.

2. Definition

ATM (Asynchronous Transfer Mode) technology is a relatively recent technology that enables high-speed network access. It supports the transmission of data, voice, and video while guaranteeing a minimum bandwidth for each connection.

- ATM technology is used in LAN, MAN, and WAN networks.
- ATM technology was developed by CENT (Centre for Studies of France Télécom) in the early 1980s to improve data transport over the public network.
- ATM operates at Layer 2 (Data Link layer) of the OSI model (Fig.61).

2. Data Link	Token Ring • Token Bus • ARINC 429 • ATM • AFDX • Bitnet • CAN • Ethernet • FDDI • Frame Relay • HDLC • ISO/IEC 13239 (I^2C) • IEEE 802.3ad (LACP) • IEEE 802.1aq (SPB) • LLC • LocalTalk • MIL-STD-1553 • PPP • STP • Wi-Fi • X.21

Fig.61. : Data Link Layer protocols.

3. ATM Cells

ATM cells have a fixed length, which simplifies multiplexing and switching. This enables switching speeds of several Mbps. ATM allows any type of information to be converted into small, fixed-length cells.

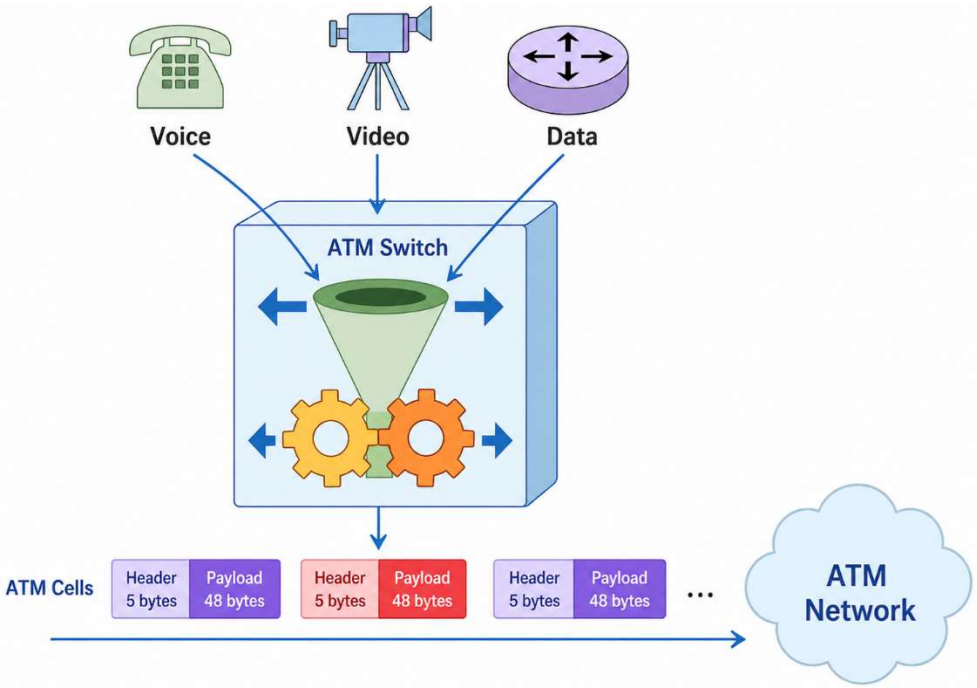


Fig.62. : Conversion of information into Cells.

The size of an ATM cell is fixed at 53 bytes, which makes it possible to : Improve the multiplexing of data over voice. A connection is defined by its path (VPI : Virtual Path Identifier) and its channel (VCI : Virtual Channel Identifier). Large nation-wide networks use ATM for transporting voice, video, and data.

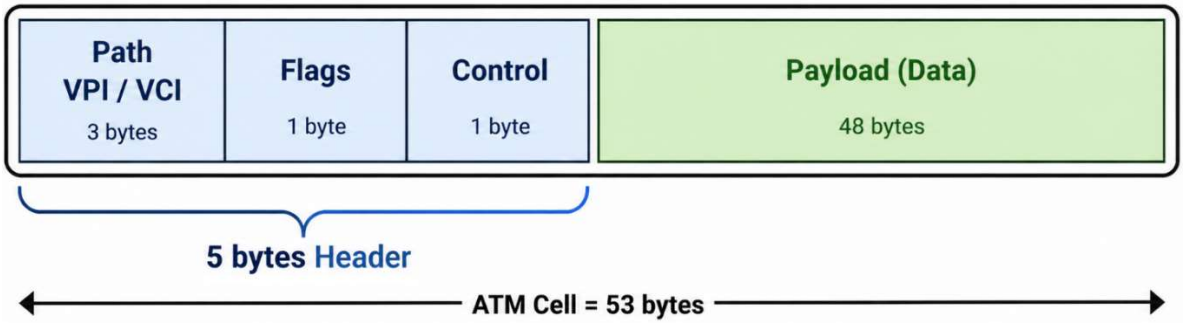


Fig.63. : ATM Cell.

4. Addressing in ATM Networks

The ATM network internally uses an addressing system that identifies virtual paths in order to ensure optimal switching performance. ATM implements a two-level addressing technique internally :

- VCI : (Virtual Channel Identifier).
- VPI : (Virtual Path Identifier).

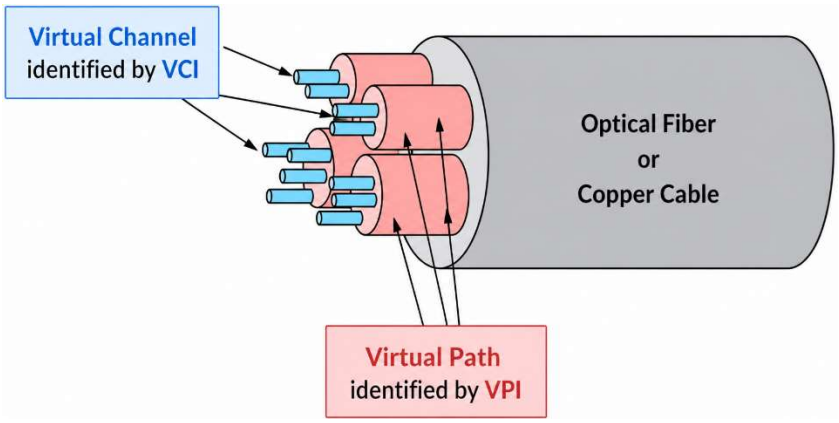


Fig.64. : Addressing in ATM Networks.

a) VCI (Virtual Channel Identifier) :

The first level identifies the virtual path (channel). The VCI is a semi-permanent connection that is established with each call.

b) VPI (Virtual Path Identifier) :

The second level groups together a set of virtual channels that share the same destination (intermediate switch) into a virtual path. The VPI is a semi-permanent connection controlled by the network.

Note :

VPIs help reduce the size of routing tables in switches because each virtual channel no longer needs to be routed individually; instead, the virtual path is routed. This allows faster address processing and reduces routing table size.

Some switches route only VPIs; these are called **cross-connects.**

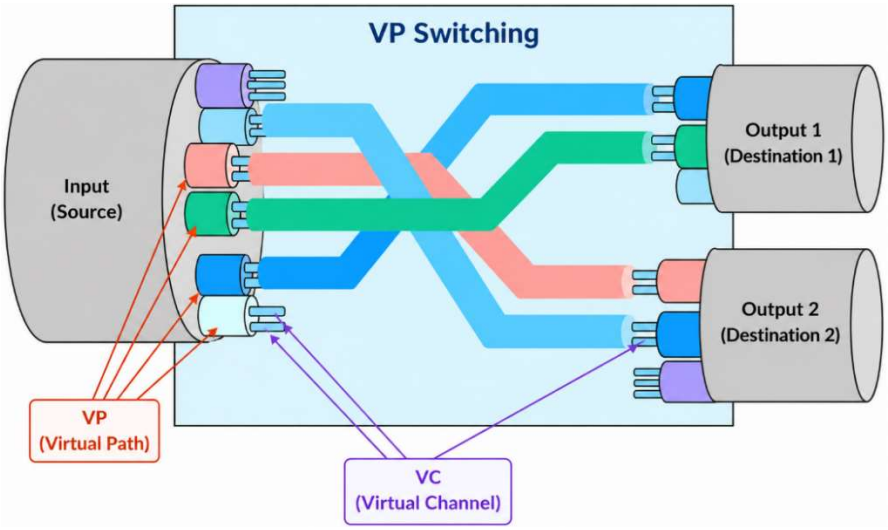


Fig.65. : VP Switching.

Example of VP Switching :

In this example, all VCs reach the same destination, so it is not necessary for the ATM network to examine all VPI/VCI fields.

The ATM network switches the cells based on the VP number, regardless of the VC number.

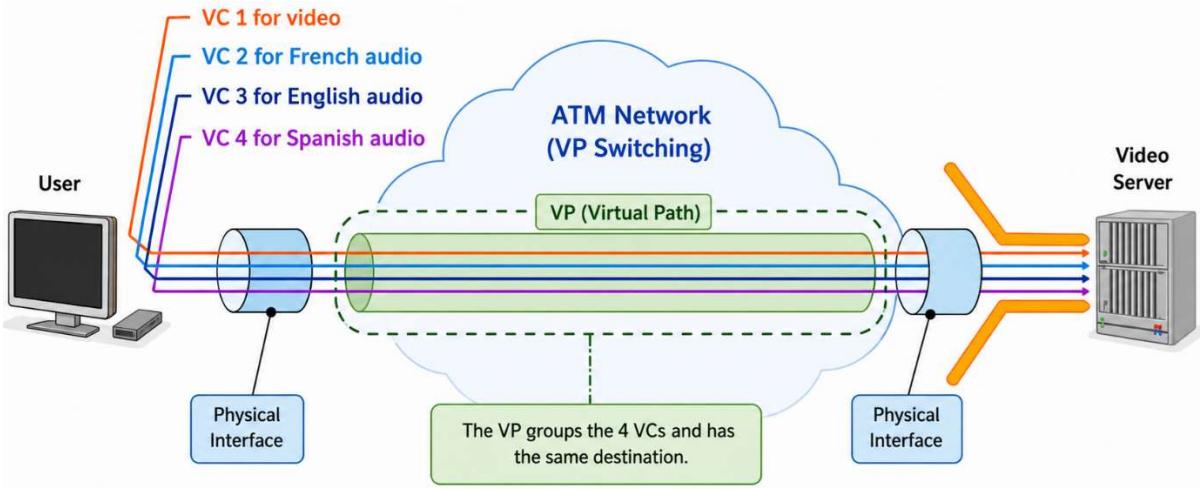


Fig.66. : Example of VP Switching.

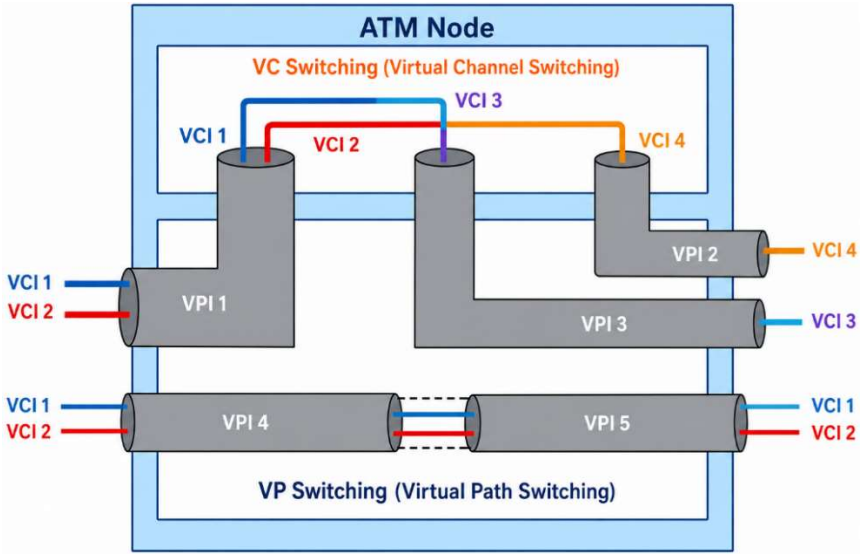


Fig.67. : VP/VC Switching.

Example of VP/VC Switching Multiplexing :

Here, VP connections are established within the ATM network between each service provider and the multiplexer.

When a new user connection needs to be set up, it is sufficient to establish, only at the multiplexer, a connection on a VP/VC corresponding to the chosen service provider.

It is no longer necessary to involve ATM network operators to establish each user connection.

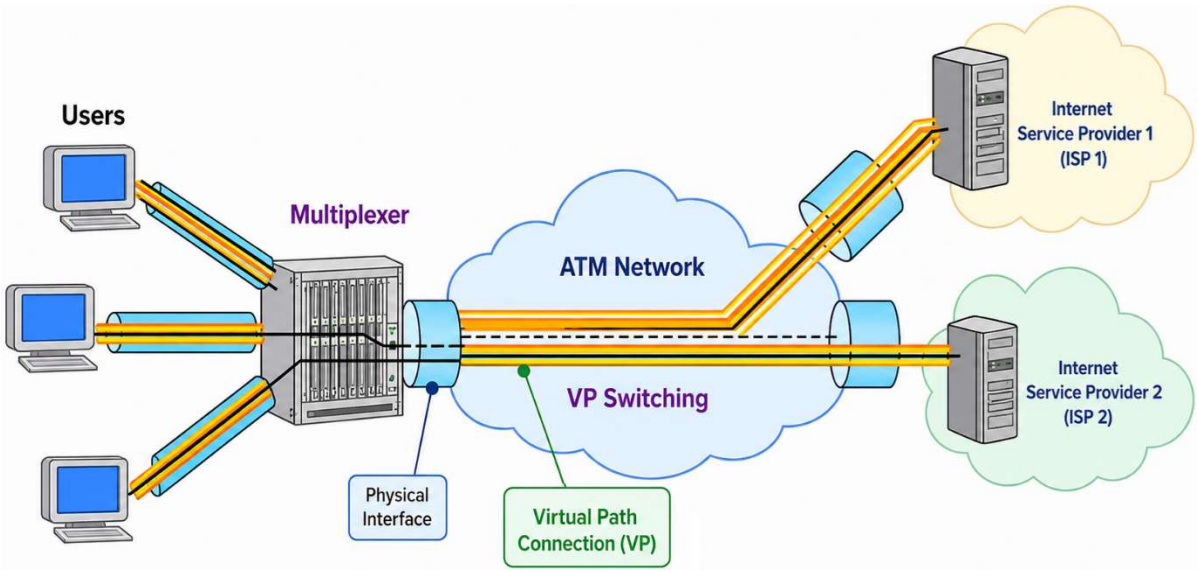


Fig.68. : Example of VP/VC Switching Multiplexing.

a) Cell Identification :

Each ATM cell header contains a dual virtual connection identifier : a Virtual Path Identifier (VPI) and a Virtual Channel Identifier (VCI).

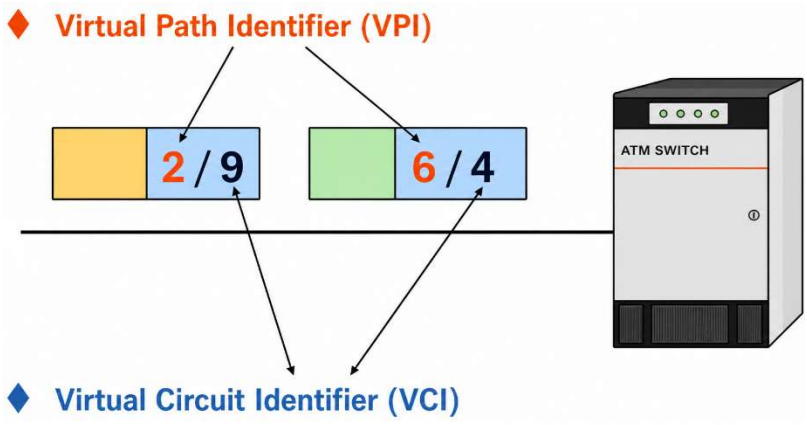


Fig.69. : Cell Identification.

b) ATM Cell Switching :

ATM cell switching is performed using a table that contains an input port number and an input VPI/VCI, as well as an output port number and an output VPI/VCI.

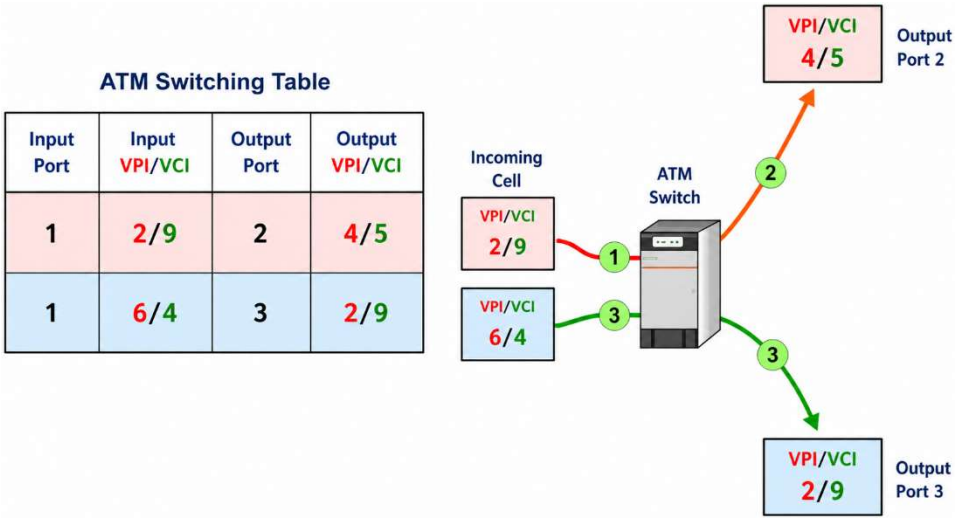


Fig.70. : ATM Cell Switching.

5. Types of Links

The connections supported by ATM technology are of two types :

- Point-to-point (P2P) connections.
- Point-to-multipoint (P2MP) connections.

The ATM network is said to be connection-oriented; for each transmission request, a virtual circuit is established that meets the desired Quality of Service (QoS). This virtual circuit can be permanent or temporary.

6. Layered Architecture

ATM consists of three layers :

- The physical layer, which adapts cells to the physical transmission system used.
- The ATM layer, which handles the switching and multiplexing of cells.

- The AAL (ATM Adaptation Layer), which adapts data units from higher-level protocols to the ATM layer.

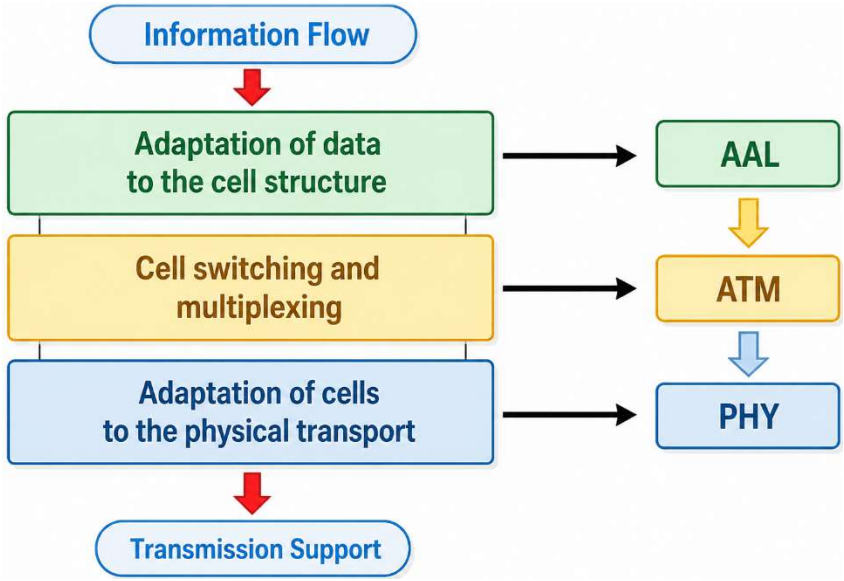


Fig.71. : Layered Architecture.

7. ATM Model

ATM technology is described using a relatively sophisticated model, which includes:

- Three horizontal layers corresponding to the first three levels of the OSI model.
- Three successive vertical planes that handle the different aspects of ATM.

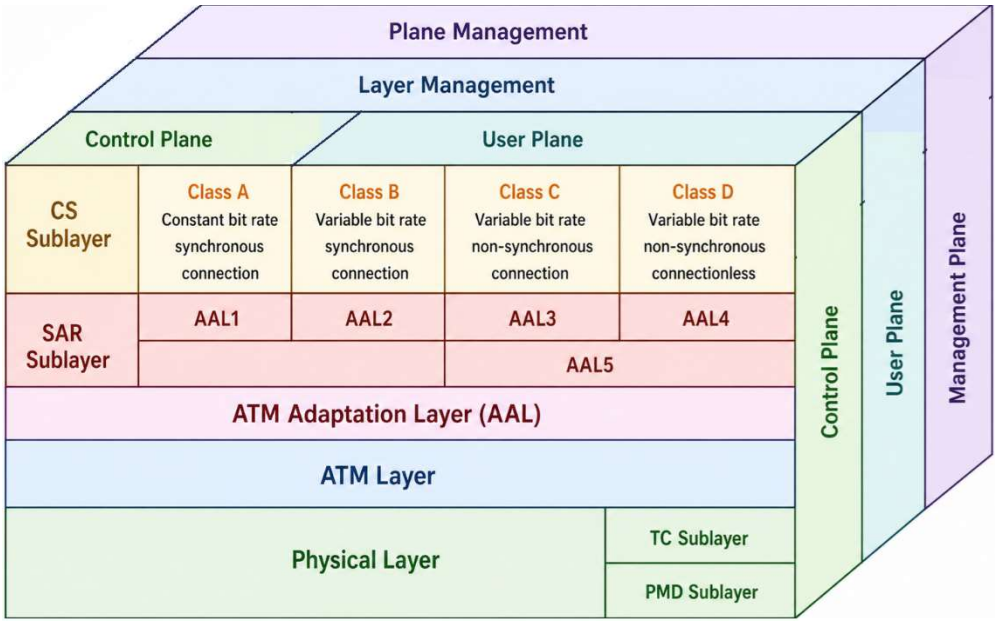


Fig.72. : ATM Model.

a) The different planes of the model :

➢ **User plane :**

Corresponds to the routing function provided by ATM to a higher-level protocol.

- **Control plane :**

  Corresponds to the internal ATM mechanisms, such as :

  - Signaling required for :
    - ✓ Connection establishment.
    - ✓ Connection maintenance.
    - ✓ Connection release .
- **Management planes :**

  Provide performance management, enabling the user plane to deliver the required services. They use specific cells (OAM cells – Operation And Maintenance cells).

b) The different layers :

- **Physical layer :**

  Responsible for providing the ATM layer with a cell transport service. It is divided into two sublayers:
- **TC sublayer (Transmission Convergence):**

  Ensures rate adaptation, data control, and cell delineation.
- **PM sublayer (Physical Medium):**

  Provides access to the physical medium and manages synchronization mechanisms.

c) ATM layer :

The ATM layer is responsible for:

- Routing cells within the network.
- Performing multiplexing and demultiplexing of cells.
- Adding and removing headers.
- Flow control (GFC) at the UNI (User-Network Interface).
- Rate adaptation by inserting and removing idle cells.

- **Congestion control :**
  - An ATM network is a queue-based network and may experience congestion
  - Three mechanisms are used to prevent or resolve congestion :
    1. Selection of cells to be discarded.
    2. Connection admission control.
    3. Source rate control.

d) AAL layer (ATM Adaptation Layer) :

Ensures that user applications receive the required Quality of Service (QoS). Five AAL types have been defined (AAL1, AAL2, AAL3, AAL4, and AAL5). They are divided into two sublayers :

- **SAR sublayer (Segmentation And Reassembly) :**

Segments and reassembles cells for higher layers.

- **CS sublayer (Convergence Sublayer) :**

  Ensures clock synchronization between the application and the transmission system.

- **Defined AAL types :**
  - AAL1 : Supports Class A applications (constant bit rate video and voice).
  - AAL2 : Supports Class B applications (variable bit rate video and audio).
  - AAL3/4 : Suitable for reliable data transfer.
  - AAL5 : Optimized for data transport.

Specific Adaptations for the Different AAL Layers in ATM Networks

AAL Type	Supported Traffic Class	Connection Type	Service Type	Data Unit from Higher Layer	AAL Service Provided
AAL1	Class A (Constant Bit Rate)	Connection-oriented (Synchronous)	CBR (Constant Bit Rate)	Fixed-size data (e.g., video, voice frames)	• Timing recovery • Cell payload mapping • Minimal overhead
AAL2	Class B (Variable Bit Rate)	Connection-oriented (Synchronous)	VBR (Variable Bit Rate)	Variable-size data (e.g., compressed video, audio)	• Timing recovery • Cell payload mapping • Supports variable rate sources
AAL3/4	Class C (Variable Bit Rate)	Connection-oriented (Non-synchronous)	Reliable Data Transfer	Packets (e.g., X.25, Frame Relay, TCP/IP)	• Segmentation and reassembly • Error control • Reliable data transfer
AAL5	Class D (Variable Bit Rate, Connectionless)	Connectionless (Non-synchronous)	Data Transfer (Connectionless)	Packets (e.g., IP datagrams, User data)	• Segmentation and reassembly • Multiplexing/demultiplexing • Minimal overhead
Summary	Traffic Class Supported	Connection Mode	Typical Service	Example of Higher Layer Data Unit	Main Functions

Table.10 : AAL types.

8. Components of ATM

The following figure shows the different components that make up the ATM network.

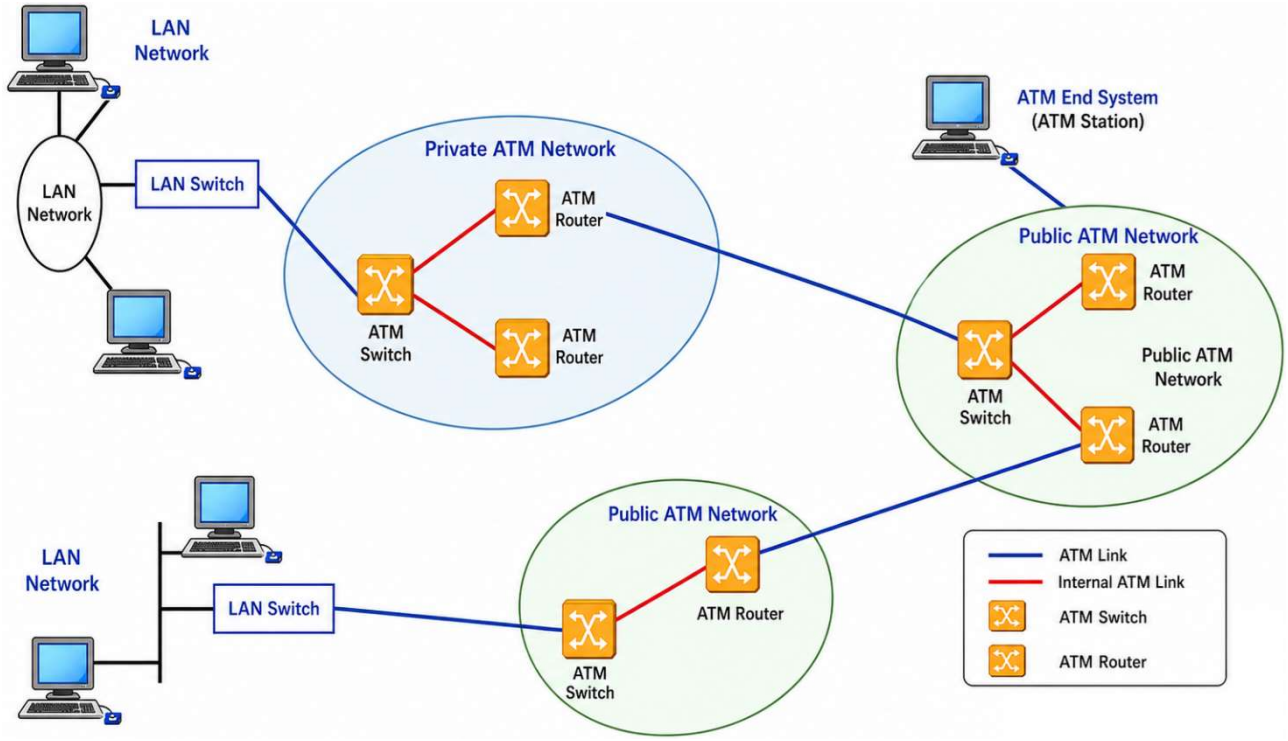


Fig.73. : Components of ATM.

a) ATM Network Interface Card :

An ATM network interface card connects a LAN station to an ATM switch. The ATM interface converts the data generated by the station into cells that are transmitted to a LAN ATM switch.

b) LAN Switch :

A LAN switch provides interconnection between traditional local area networks such as Ethernet or Token Ring and the ATM network. It supports at least two types of interfaces: an ATM interface and a LAN interface.

c) ATM Switch :

An ATM switch is a multiport switch where each port is connected to an ATM device. It forms the basic infrastructure of an ATM network. It routes cells from an input port to an output port.

d) ATM Cell :

- **Network interface :**

  Two families of frames are distinguished, depending on the type of network interface used.

  1. **UNI (User-to-Network Interface)**

     UNI is an interface between a private end device and an ATM switch (private UNI). The connection of a private ATM network to a public network is also called a public UNI.

2. NNI (Node-to-Node Interface)

NNI is an interface between two switches. Two types of NNI exist :

- **Private NNI**, which describes the interface between local switches within an enterprise.
- **Public NNI**, which describes the interface between switches in public ATM networks.

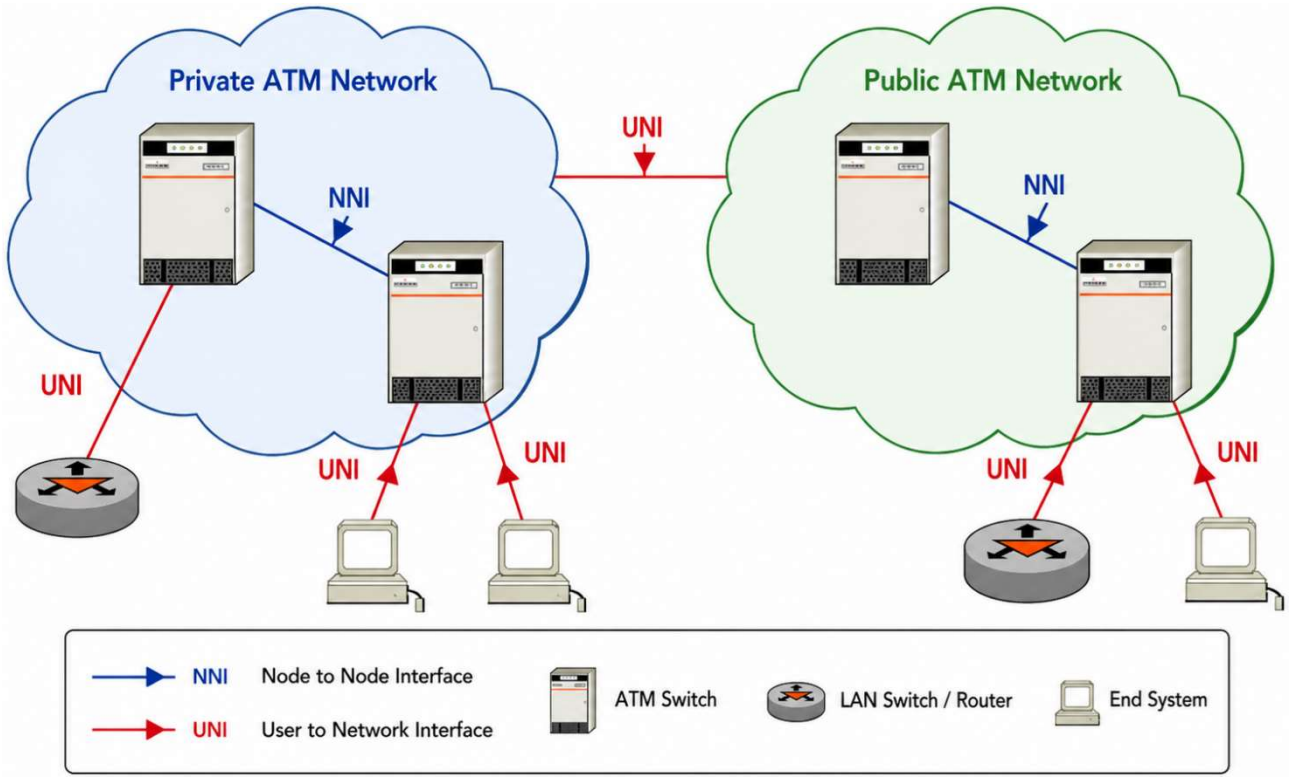


Fig.74. : Network interface of ATM.

3. NNI Format of ATM Cell

The header of an ATM cell in NNI format contains two address fields: the VPI field encoded on 12 bits and the VCI field encoded on 16 bits.

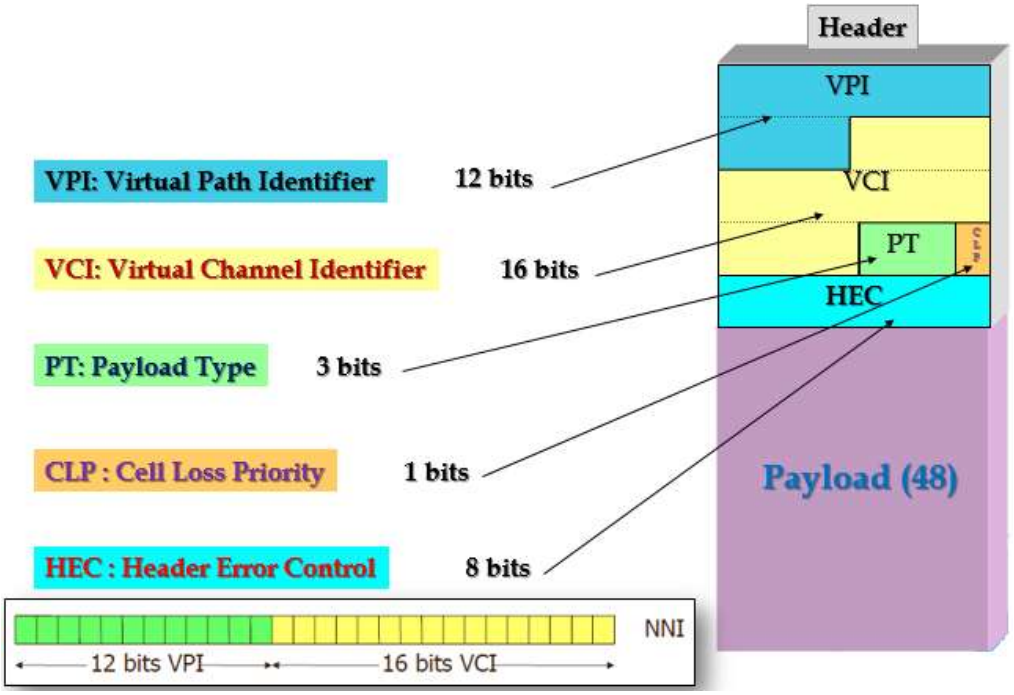


Fig.75. : NNI Format of ATM Cell.

4. UNI Format of ATM Cell

The header of an ATM cell in UNI format contains two address fields: the VPI field encoded on 8 bits and the VCI field encoded on 16 bits, along with a flow control field (GFC) encoded on 4 bits.

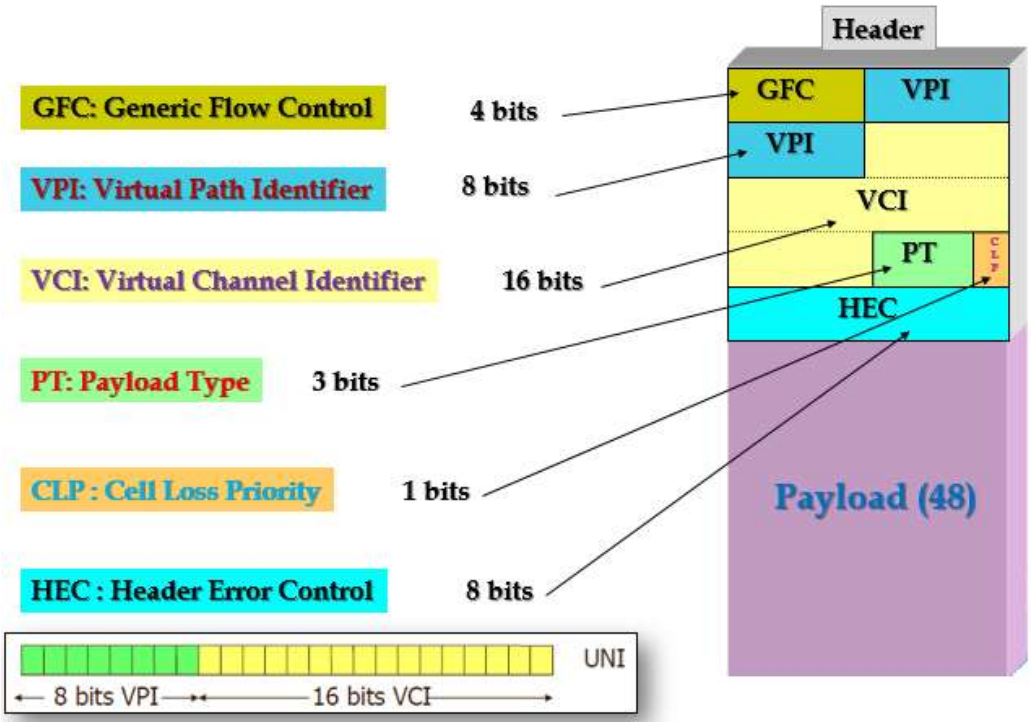


Fig.76. : UNI Format of ATM Cell.

- **Generic Flow Control (GFC) :**
  - ✓ The GFC field (4 bits) is used for UNI Cells.
  - ✓ It enables flow control.

- **Payload Type (PT) :**

  Two types of data are transmitted over the network :

  - ✓ User originated data.
  - ✓ Network internal data (signaling, maintenance, etc.).

  The PT field therefore indicates the type of payload contained in the data field.

- **Cell Loss Priority (CLP) :**
  - ✓ Enables congestion management.
  - ✓ Indicates which cells should be discarded first during congestion.
  - ✓ CLP = 1: Indicates that the cell has low priority.
  - ✓ CLP = 0: Indicates that the cell has high priority.

5. Example of congestion

In this example, the access switch of a user may set the CLP bit to 1 when the user sends cells at a rate higher than that specified in the contract.

The network then allows other switches to discard these cells in case of congestion. In this case, the network will give priority to dropping cells marked as less important.

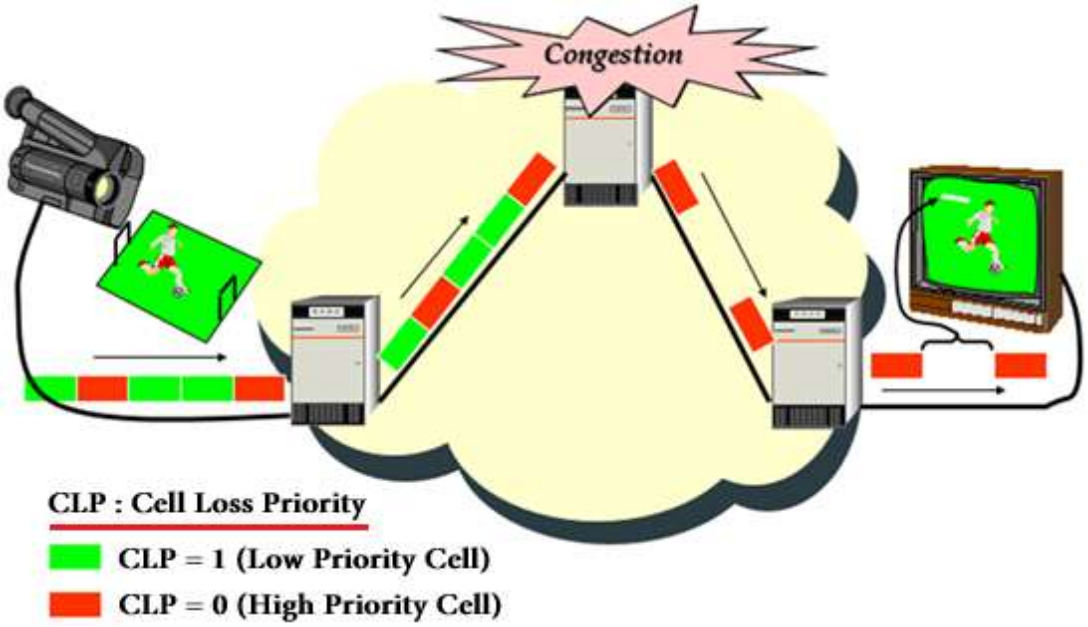


Fig.77. : Example of congestion.

- **Header Error Control (HEC) :**
  - ✓ Assures error detection and correction.
  - ✓ In case of an uncorrected error (i.e., more than one bit), the cell is discarded.
  - ✓ Ensures the cell delineation function (cell boundaries).

The following table shows the error indications during ATM cell transmission.

No errors	Cell transmitted
1-bit error	Cell corrected and transmitted
Error greater than 1 bit	Cell discarded

Table.11 : Error indications during ATM Cell transmission.

6. Operation of the layers

6.1. Physical Layer :

- ✓ The PDH mode (Plesiochronous Digital Hierarchy).
- ✓ The SDH mode (Synchronous Digital Hierarchy).
- ✓ The cell mode (used in private infrastructures or local area networks).
- ✓ Rate adaptation (through insertion or removal of empty cells) is performed by the TC (Transmission Convergence) sublayer.
- ✓ The PM (Physical Medium) sublayer ensures encoding, bit alignment, synchronization, and electrical and optoelectrical adaptation to the medium.
- ✓ The data rate provided for the ATM layer is 135.63 Mbit/s.

a) ATM 155 Framed Mode :

- ATM 155 Mbit/s in framed mode was defined to operate over multimode optical fiber and Category 5 twisted pair.
- The frame consists of 27 cells, one of which is reserved for signaling.
- The 5-byte ATM cell header (Header) of the PL-OH (Physical Layer Overhead) is replaced by 5 symbols used for decoding synchronization.

b) ATM 25 :

- It enables the connection of multimedia workstations and operates over twisted pairs with a maximum length of 100 m, with a nominal data rate of 25.6 Mbit/s.

c) ATM 100 :

- ATM 100 Mbit/s was defined to operate over the FDDI network.

7. Standardized data rates at the UNI interface :

The following table shows the standardized data rates at the UNI interface.

Plesiochronous Access

Network Access	Bit Rate (Mbit/s)	Medium	Distance (m)	UNI Type
E1	2.048	Twisted pairs	-	Public
T1	1.544	Twisted pairs	-	Public
nT1	n × 1.544	Twisted pairs	-	Public
nE1	n × 2.048	Twisted pairs	-	Public

Cell Mode Access

Network Access	Bit Rate (Mbit/s)	Medium	Distance (m)	UNI Type
ATM 25	25.6	UTP Cat 3 & 5	100	Private
ATM 155	155.5	Multimode fiber	2000	Private
ATM 155	155.5	STP	100	Private

Synchronous Access

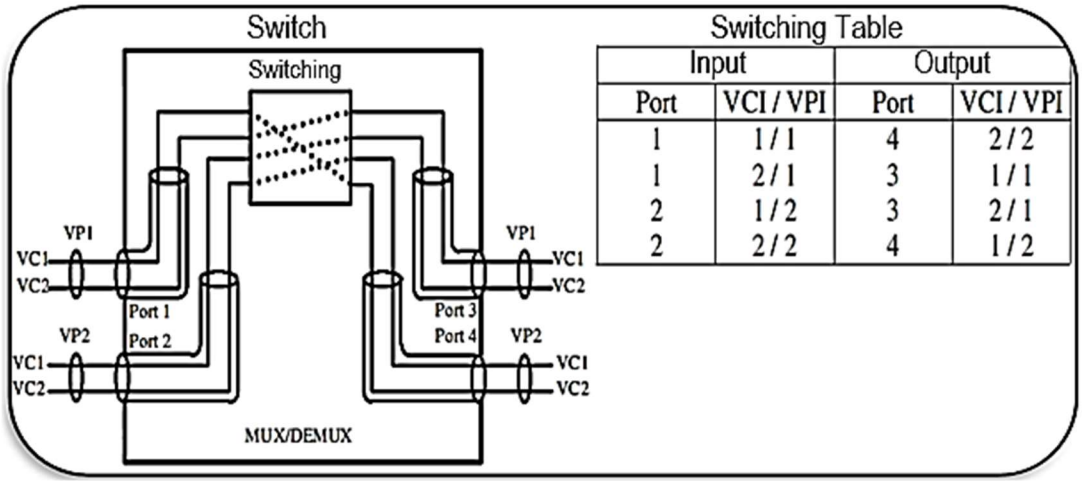
Network Access	Bit Rate (Mbit/s)	Medium	Distance (m)	UNI Type
STS-1	51.48	Single-mode fiber	15000	Public
STS-3	155.52	UTP Cat 3 & 5	100	Private
STS-3	155.52	Optical fiber	15000	Public/Private
STS-3	155.52	Coaxial	150	Private
STS-12	622.08	Single-mode fiber	15000	Public/Private

Table.12 : Standardized data rates at the UNI interface.

8. Structure of ATM Switches

We distinguish two types of ATM switches : a time switch and a space switch.

a) Time switch :



Switching Table

Input		Output	
Port	VCI / VPI	Port	VCI / VPI
1	1 / 1	4	2 / 2
1	2 / 1	3	1 / 1
2	1 / 2	3	2 / 1
2	2 / 2	4	1 / 2

Fig.78. : Time switch.

b) Space switch :

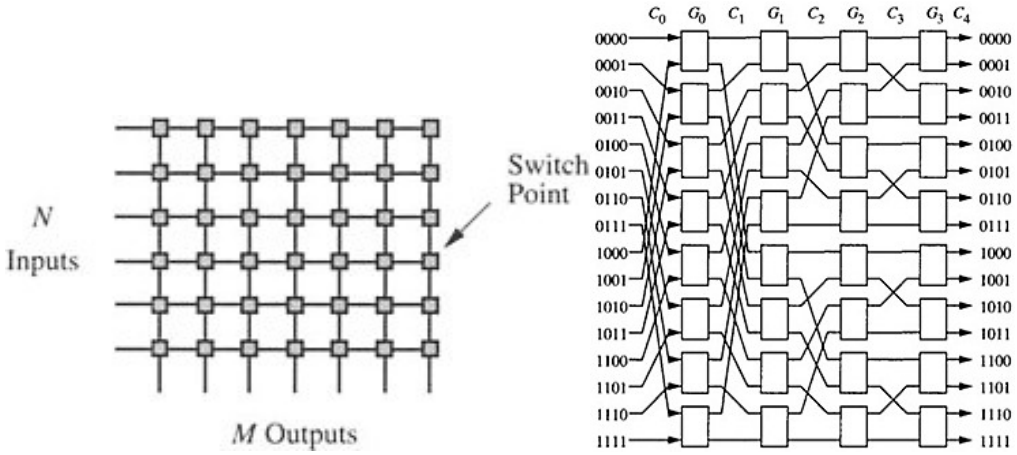


Fig.79. : Space switch.

9. Classes of Service (CoS)

ATM defines five service classes (CoS) :

Service	Name	Characteristic	Applications
CBR	Constant Bit Rate	Constant Bit Rate Isochronous stream	Uncompressed voice and video
VBR-rt	Variable Bit Rate real time	Variable bit rate (VBR) Isochronous stream	Compressed audio and video applications
VBR-nrt	Variable Bit Rate non real time	Variable bit rate but predictable	Transactional application
ABR	Available Bit Rate	Sporadic bit rate without time constraint	Local Area Network Interconnection
UBR	Unspecified Bit Rate	Unspecified Traffic	Messaging, Remote backup.

Table.13 : Classes of Service (CoS).

10. Advantages

Among the advantages of ATM networks, we find :

- ATM enables more efficient use of WAN links.
- True dynamic multiplexing during transmission.
- Asynchronous transfer mode.
- Prevents the transmission medium from remaining idle for a certain period of time.
- ATM carries all types of traffic over all distances and regardless of the transmission medium (twisted pairs, optical fiber, and wireless).
- Operates at very high bit rates (Gb/s).
- Guarantees QoS for each user.
- Switching technique : Cell switching.

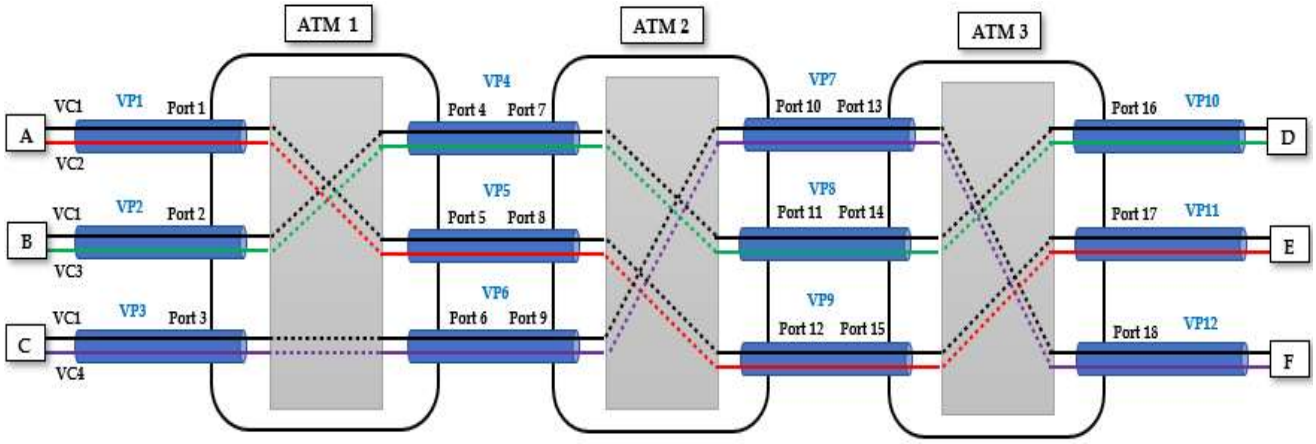
11. Conclusion

Asynchronous Transfer Mode (ATM) is a high-performance networking technology designed to efficiently transport various types of traffic such as voice, video, and data over the same infrastructure. Its cell-based switching mechanism ensures fast and predictable transmission with low delay, making it suitable for real-time and multimedia applications. ATM provides dynamic bandwidth allocation and supports very high data rates while maintaining Quality of Service (QoS) for different users. Although it has been largely replaced in modern core networks by IP-based technologies, ATM played a fundamental role in the evolution of broadband and high-speed communication systems.

12. Exercise

The following diagram represents a private ATM network in which 6 stations are connected through 3 nodes. Nodes 1 and 3 are VPI/VCI switches, while node 2 is a cross-connect (switching fabric).

1. Construct the switching tables for the 3 nodes for the following Virtual Circuits :
   - A – E
   - B – D
   - C – F



VC	ATM1				ATM2				ATM3			
	Input		Output		Input		Output		Input		Output	
	Port	VPI/VCI	Port	VPI/VCI	Port	VPI/VCI	Port	VPI/VCI	Port	VPI/VCI	Port	VPI/VCI
…	…	…	…	…	…	…	…	…	…	…	…	…

12.1. Solution :

VC	ATM1				ATM2				ATM3			
	Input		Output		Input		Output		Input		Output	
	Port	VPI/VCI	Port	VPI/VCI	Port	VPI	Port	VPI	Port	VPI/VCI	Port	VPI/VCI
1	1	1/1	5	5/1	8	5	12	9	15	9/1	17	11/1
	1	1/2	5	5/2	8	5	12	9	15	9/2	17	11/2
2	2	2/1	4	4/1	7	4	11	8	14	8/1	16	10/1
	2	2/3	4	4/3	7	4	11	8	14	8/3	16	10/3
3	3	3/1	6	6/1	9	6	10	7	13	7/1	18	12/1
	3	3/4	6	6/4	9	6	10	7	13	7/4	18	12/4

Unit 2 : MPLS Protocol.

Unit Objectives :

By the end of this chapter, you should be able to :

- Understand the basic concepts of MPLS (Multiprotocol Label Switching).
- Explain how MPLS improves packet forwarding using labels instead of IP lookups.
- MPLS technologies.
- Understand the advantages and limitations of MPLS.
- Identify real-world use cases for MPLS in modern networks.

Topics Covered :

- Introduction to MPLS (Multiprotocol Label Switching).
- Basic concepts.
- Label switching mechanism.
- MPLS Architecture.
- MPLS Labels and Forwarding.
- Forwarding Equivalence Class (FEC).
- MPLS vs Traditional IP Routing.
- VPNs.
- Traffic Engineering (TE).

1. Introduction

The emergence of high-speed internet access for everyone, everywhere, has simplified access to services and knowledge, representing a real improvement in the way we live today. This context of exponential internet growth implies the need to build increasingly larger, faster, and more secure networks.

The idea of the MPLS protocol (Multi-Protocol Label Switching) is to label each packet when it enters a network ; routing through the network is then performed based on a label forwarding table or a Label Forwarding Information Base (LFIB). However, it is important to understand that MPLS still relies on standard routing protocols such as OSPF, EIGRP, or BGP.

2. Definition

MPLS (Multi-Protocol Label Switching) is a transmission protocol that sends information in a labeled manner. The set of information contains a label that allows the content to be identified. This enables faster and more secure data transfer.

The MPLS protocol uses its own routing mechanism based on assigning a label to each packet. This allows packets to be routed while optimizing the transition between Layer 2 and Layer 3 of the OSI model.

Its main role is to combine IP routing concepts at Layer 3 with Layer 2 switching mechanisms such as those implemented in ATM or Frame Relay.

- **MPLS enables :**
  - Improve the performance/cost ratio of routing equipment.
  - Improve routing efficiency (especially for large networks).
  - Enrich routing services.
  - MPLS can be extended to multiple protocols (IPv6, IPX, AppleTalk, etc.).
  - Packet forwarding at Layer 3.
  - Handles switching in connection-oriented mode (based on labels).
  - MPLS can be considered as an interface that provides IP with a connection-oriented mode and uses Layer 2 services (PPP, ATM, Ethernet, Frame Relay, SDH, etc.).
  - Ensure a smooth transition toward the optical Internet.

Remark : The switching tables are computed from information provided by IP routing protocols as well as control protocols.

The goal is to combine the power of Layer 2 switching with the flexibility of Layer 3 routing. Schematically, it can be represented as being located between Layer 2 (data link) and Layer 3 (network).

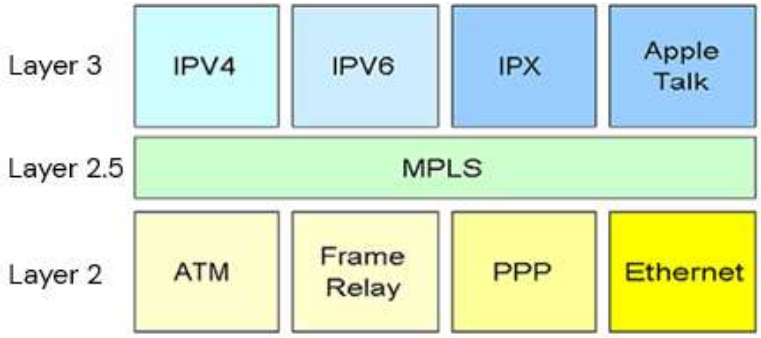


Fig.80. : MPLS Layer.

3. MPLS Objectives

One of the initial objectives was:

- To increase the speed of datagram processing across all intermediate devices.
- IP/ATM integration.
- Creation of VPNs (Virtual Private Networks).
- Flexibility: ability to use multiple media, namely ATM, Frame Relay (FR), Ethernet, PPP, SDH, etc.
- Multicast routing.
- Facilitate the use of optical networks by operating directly over WDM (Wavelength Division Multiplexing).

4. MPLS Labels

MPLS works by dividing traffic (data) into discrete units that are processed separately. IP units are packets, ATM units are cells, and Frame Relay units are frames.

A label has local significance between two adjacent Label Switching Routers (LSRs) and maps the traffic flow between the upstream LSR and the downstream LSR. At each hop along the LSP (Label Switched Path), a label is used to look up routing information (next hop, outgoing link, encapsulation, queuing and scheduling) and to determine the actions to be performed on the label : push, swap, or pop.

The following figure describes the implementation of labels in different technologies such as ATM, Frame Relay, PPP, Ethernet, and HDLC.

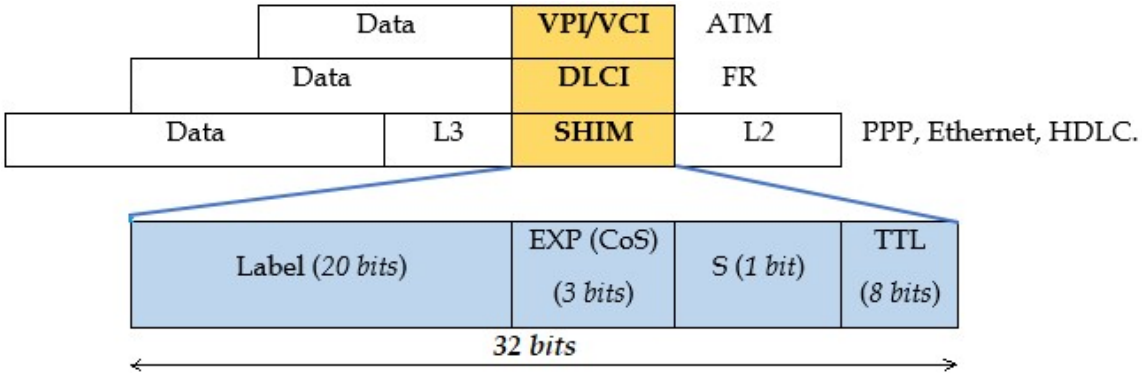


Fig.81. : Implementation of labels in different technologies.

For Ethernet networks, a field called the Shim header has been introduced between Layer 2 and Layer 3.

- It is 32 bits long and acts as a local identifier for a FEC (Forwarding Equivalence Class).
- 20 bits contain the label, a 3-bit field called Class of Service (CoS) currently used for QoS.
- One bit S indicates whether there is a label stack, and a final field.
- An 8-bit TTL (same meaning as in IP).

Label stacking makes it possible, in particular, to associate multiple service contracts with a flow as it traverses the MPLS network.

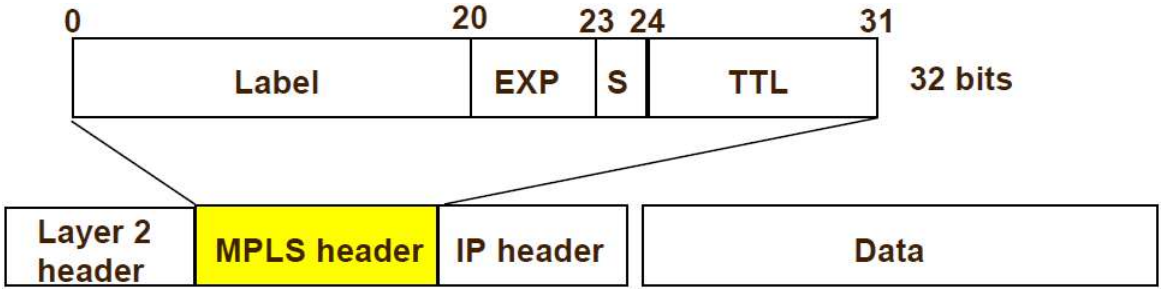


Fig.82. : MPLS Packet Format.

- Label: 20 bits – Used to configure the LSP (Label Switched Path).
- EXP: 3 bits – Experimental – used to prioritize traffic.
- S: 1 bit – Stack (indicates the bottom of the label stack).
- TTL: 8 bits – Time-To-Live (lifetime).

Remark :

- Labels are only relevant between adjacent nodes.
- The label stack allows chaining to provide extended service support. This is one of the main advantages of MPLS technology.
- Inner and outer labels are generally used in VPN services.

5. MPLS Devices

MPLS uses Label Switched Paths (LSPs) for Layer 2 forwarding. The path is configured using signaling protocols such as the Label Distribution Protocol (LDP) and routing protocols.

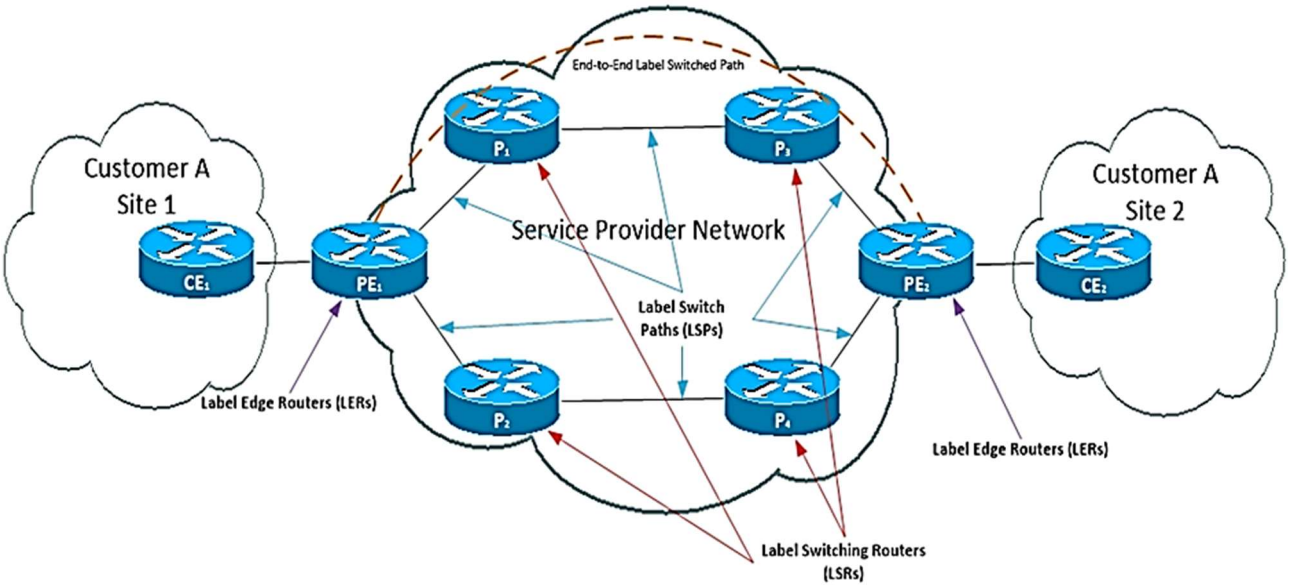


Fig.83. : MPLS Devices.

5.1. Label Edge Router (LER)

- Examines incoming IP packets and assigns them to a FEC (Forwarding Equivalence Class).
- Generates an MPLS header and assigns an initial label.
- Ingress and egress.
- Last hop in the operator's network before connection to the customer.
- Performs routing toward the customer and internal label switching within the operator's network.
- Performs label imposition (push) and label removal (pop).
- Requires end-to-end connectivity between PE routers (Label Switched Path). PE-to-PE must establish peering (MP-BGP) using loopback addresses.
- Creates label-switched paths within the operator's network.

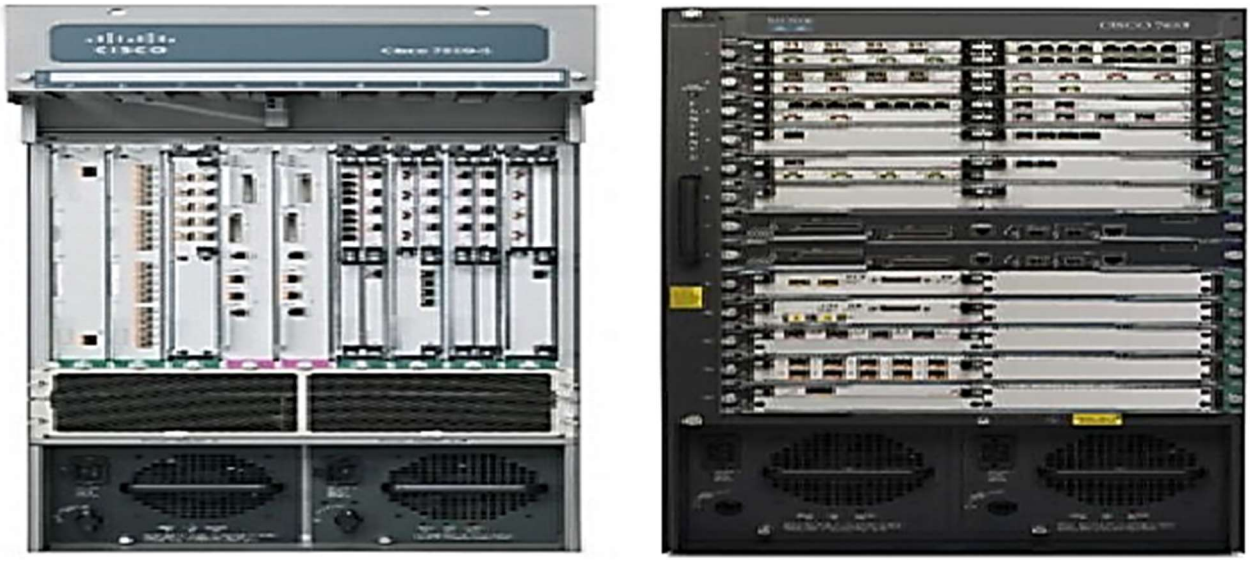


Fig.84 : Label Edge Router (LER).

5.2. Label Switch Router (LSR)

- Forwards MPLS packets using label swapping.
- Performs table lookup in the Label Information Base (LIB).
- Label-switching router devices in the operator's core network.
- Executes the label swapping function.
- Switches packets based on MPLS labels.
- Creates label-switched paths.



Fig.85. : Label Switch Router (LSR).

5.3. Label Switch Path (LSP)

- Path used for configuring the MPLS network via a signaling protocol (LDP).
- LSPs are unidirectional, roughly equivalent to virtual circuits (VCs).
- LSP setup is based on FEC criteria.
- The LSP may differ from the IGP path.

5.4. Customer Edge (CE)

- Does not support MPLS.
- Runs standard routing processes and protocols.
- Last hop in the customer network before connecting to the transport network.

5.5. Label Distribution Protocol (LDP)

- It is a protocol used by the control plane to exchange labels (between adjacent routers).
- Associates a set of destinations with each LSP.
- Packets can be assigned to an LSP based on the combination of destination address and application type.
- Updates different routing tables (FIB and LFIB).
- Combines the destination address and the source address.

5.6. Penultimate Hop Popping (PHP)

- It is an optimization technique that prevents the egress LER from performing a double lookup in the routing table and in the LFIB (Label Forwarding Information Base).

6. Label processing

6.1. Push

- Adds a new label on top of the packet.
- The TTL, stack, and CoS fields are derived from the IP packet header.
- Can be performed on an existing stack of MPLS packet labels.

6.2. Pop

- Remove the label.
- The TTL is copied from the label to the IP header.
- The IP packet is forwarded as a native IP packet.

6.3. Swap

- Replaces the label at the top of the label stack with a new label.
- The TTL, stack, and CoS fields are copied from the previous label.

6.4. Multiple Push

- Addition of multiple labels (up to 3).

6.5. Swap and Push

- Replaces the existing top of the label stack with a new label, then pushes another new label on top.
- Used when an LDP-signaled LSP transits through a core signaled by RSVP (Resource Reservation Protocol) - TE.

7. Label Distribution

The MPLS architecture does not rely on a single signaling method for label distribution. Various label exchange schemes include :

- LDP : maps unicast destinations to labels ; it is the most commonly used method.
- RSVP (Resource Reservation Protocol) and CR-LDP (Constraint-Based Label Distribution Protocol) : used for Traffic Engineering (TE) and resource reservation.
- Protocol Independent Multicast (PIM) : used for mapping multicast state labels.
- Border Gateway Protocol (BGP) : used for external label mapping (VPNs).

7.1. Label Assignment Mode

- DoD : Downstream on Demand.
- DU : Downstream Unsolicited.

7.2. Mode de contrôle des étiquettes

- Managed.
- Independent.

7.3. Mode de maintien des étiquettes

- Liberal retention mode : when a label is received, if there is no route for the corresponding FEC, the label is kept for later use.
- Conservative mode : when a label is received, if there is no route for the corresponding FEC, the label is discarded.

8. MPLS Operations

When a packet arrives in an MPLS network (1). Depending on the FEC (Forwarding Equivalent Class) to which the packet belongs, the Ingess Node looks up its switch table (2) and assigns a label to the packet (3), and passes it to the next LSR (4).

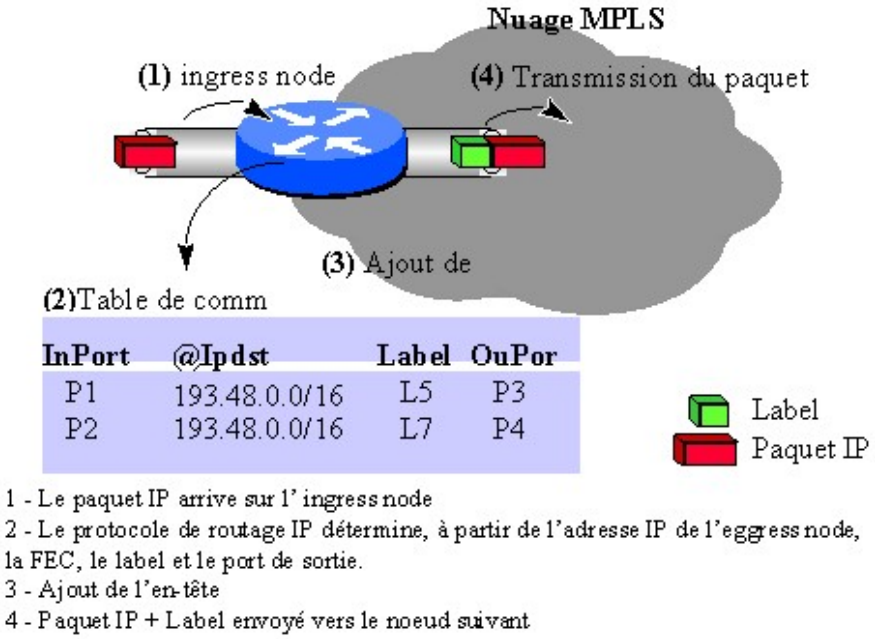


Fig.86. : Arrival of a Packet at the Ingress Node.

When an MPLS packet arrives at an internal LSR (1) within the MPLS cloud, the routing protocol running on this device determines, in the Label Information Base (LIB), the next label to be applied to the packet so that it reaches its destination (2). The device then updates the MPLS header (label swapping and updating the TTL field and the S bit) (3), before forwarding it to the next node (LSR or egress node) (4). It should be noted that on an internal LSR, the network layer routing protocol is never used.

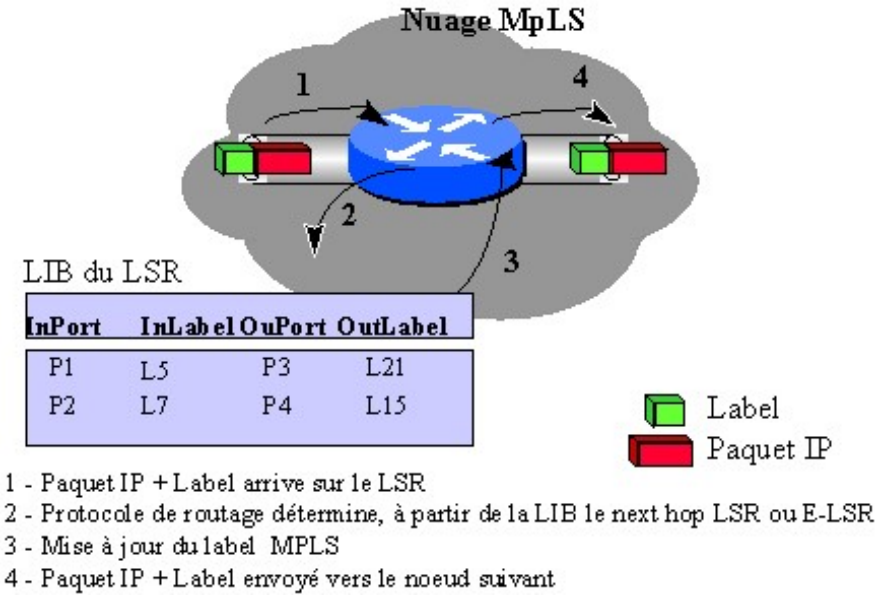


Fig.87. : Label on LSR.

Finally, once the MPLS packet arrives at the egress node (1), the device removes all MPLS information (2) and forwards it to the network layer.

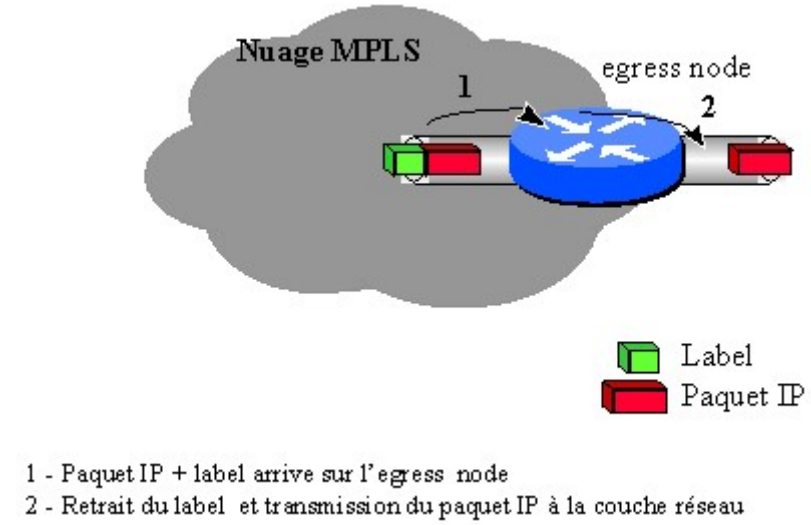


Fig.88. : Label removal at the egress node.

9. MPLS Principles

Based on label swapping, a simple forwarding mechanism enables new control models and new applications. At an LSR (Label Switching Router) within the MPLS cloud, label swapping is performed by analyzing an incoming label, which is then replaced with an outgoing label and finally forwarded to the next hop. Labels are imposed on packets only once at the edge of the MPLS network at the Ingress E-LSR (Edge Label Switching Router), where a computation is performed on the datagram in order to assign it a specific label. What is important here is that this computation is performed only once. The first time a datagram of a flow arrives at an Ingress E-LSR, this label is removed at the other end by the Egress E-LSR. The mechanism is therefore as follows : the Ingress LSR (E-LSR) receives IP packets, classifies them, assigns a label

to them, and forwards the labeled packets into the MPLS cloud. Based solely on labels, the LSRs within the MPLS cloud switch labeled packets until they reach the Egress LSR, which removes the labels and forwards the packets to their final destination.

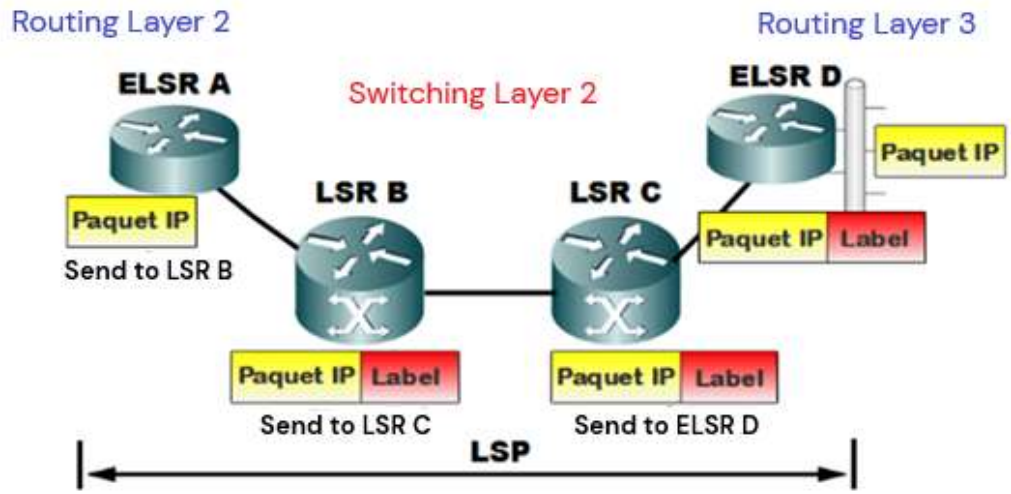


Fig.89. : Labels Switching.

The assignment of labels to packets depends on groups or flow classes called FECs (Forwarding Equivalence Classes). Packets belonging to the same FEC are processed in the same way. The path established by MPLS, called LSP (Label Switched Path), is used by all datagrams of this flow. The label is inserted between Layer 2 and the Layer 3 header (in a packet-based environment), or within the VPI/VCI field (in ATM networks). The LSR switch within the MPLS cloud simply reads the labels, applies the appropriate services, and forwards the packets based on the labels. This MPLS lookup-and-forwarding scheme provides the ability to precisely control routing based on source and destination addresses, thereby facilitating the introduction of new IP services. An MPLS flow is considered a Layer 2.5 flow, positioned between Layer 2 and Layer 3 of the OSI model.

10. Routing

Two types of routing can be distinguished : implicit and explicit distribution.

10.1. Implicit Routing LDP

The implicit distribution of labels to LSRs is performed using the LDP (Label Distribution Protocol). LDP defines a set of procedures and messages used by LSRs to inform each other about the mapping between labels and flows. Labels are assigned according to a “hop-by-hop” path defined by the IGP (Interior Gateway Protocol) within the network. Each node must therefore run a Layer 3 routing protocol, and routing decisions are made independently at each node.

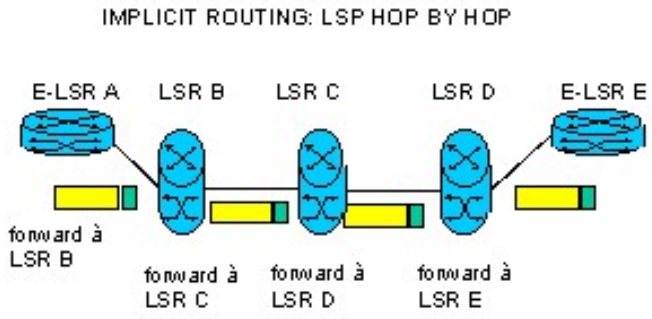


Fig.90. : Implicit routing.

LDP is bidirectional and enables the dynamic discovery of adjacent nodes through Hello messages exchanged via UDP. Once the two nodes have discovered each other, they establish a TCP session that acts as a reliable transport mechanism for session establishment messages, label advertisement messages, and notification messages.

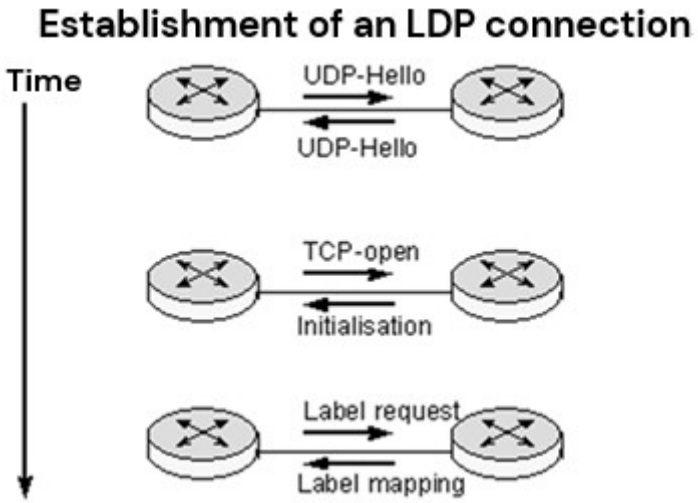


Fig.91. : Establishment of LDP connection.

- **LDP supports the following specifications :**
  - Labels are assigned to an upstream node based on information contained in the routing table:
    - ✓ 3 FECs (Forwarding Equivalence Classes) are defined; it is possible to map a label either to a traffic flow, an IP address prefix, or a router ID. The traffic flow receives the same forwarding treatment according to the label associated with it.
  - An LDP session can be established between two LSRs that are directly or indirectly connected.
  - There are two label retention modes: "conservative" or "liberal". In conservative mode, only the label corresponding to the best next hop is

retained. In liberal mode, all labels advertised by adjacent LSRs for a given flow are retained. This mode enables fast rerouting in case of failure, since alternative labels are immediately available.

10.2. Explicit Routing

Explicit routing is the MPLS solution for Traffic Engineering (TE), whose objectives are as follows :

- Efficiently use network resources.
- Avoid congestion hotspots by distributing traffic across the entire network (the shortest path is often overused).

Today, MPLS is emerging as a new Traffic Engineering mechanism by offering greater IP routing flexibility (bandwidth, QoS, etc.) through Explicit Routing. In this case, the LSP is no longer determined at each hop as in Implicit Routing : instead, the ingress node selects the end-to-end path.

At core LSRs, only the MPLS label is examined (not the IP datagram header).

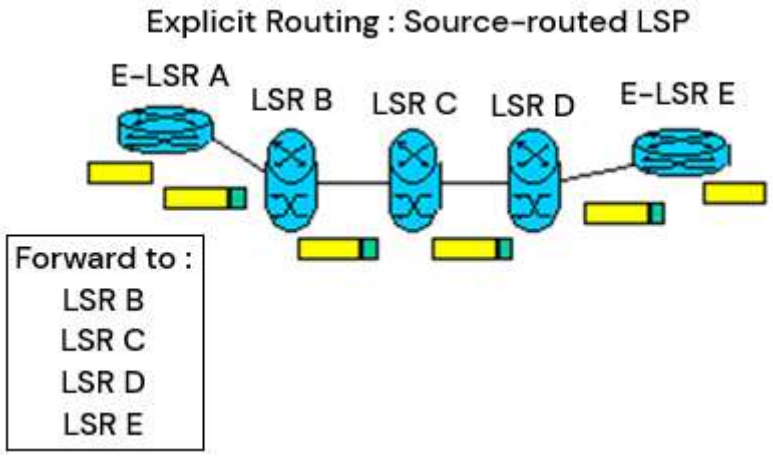


Fig.92. : Explicit Routing.

Explicit routing allows an operator to perform Traffic Engineering by imposing constraints on traffic flows from the source point to the destination point. Thus, routes other than the shortest path can be used. The network determines the path itself by following the steps below :

- Knowledge of the network state : topology, actual link bandwidth, used bandwidth, and remaining bandwidth.
- Calculation of a path that satisfies the specified constraints.
- Establishment of the ER-LSP (Explicitly Routed Label Switched Path). The source knows the complete path from the ingress node to the egress node, and it specifies the LSRs within the LSP.
- Monitoring the status of the LSPs.
- Re-optimization of the LSPs whenever necessary.

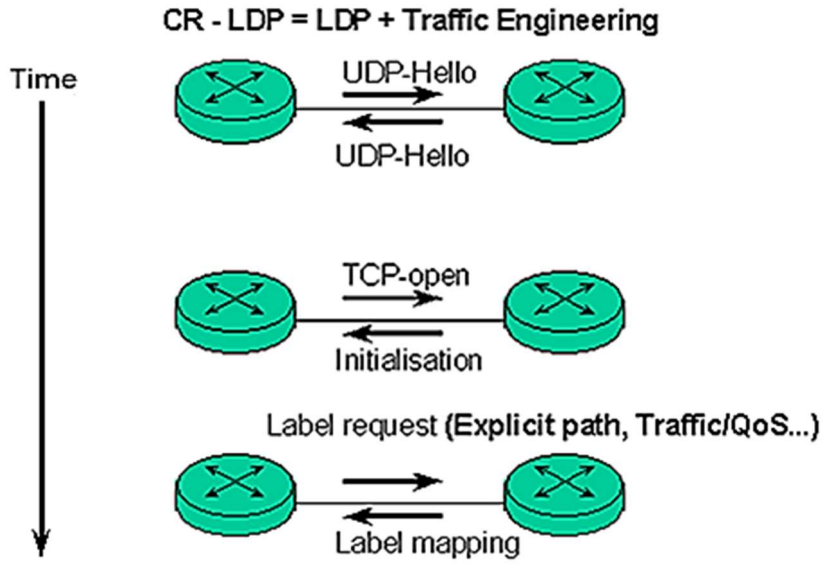


Fig.93. : LDP + Traffic Engineering.

11. MPLS-L2 VPN

Explicit routing enables an operator to perform Traffic Engineering by imposing constraints on traffic flows from the source point to the destination point. Thus, routes other than the shortest path can be used. The network determines the path itself by following the steps below :

- Knowledge of the network state : topology, actual link bandwidth, used bandwidth, and remaining bandwidth.
- Calculation of a path that satisfies the specified constraints.
- Establishment of the ER-LSP (Explicitly Routed Label Switched Path). The source knows the complete path from the ingress node to the egress node, and it specifies the LSRs within the LSP.
- Monitoring of the LSP status.
- Re-optimization of LSPs whenever necessary.

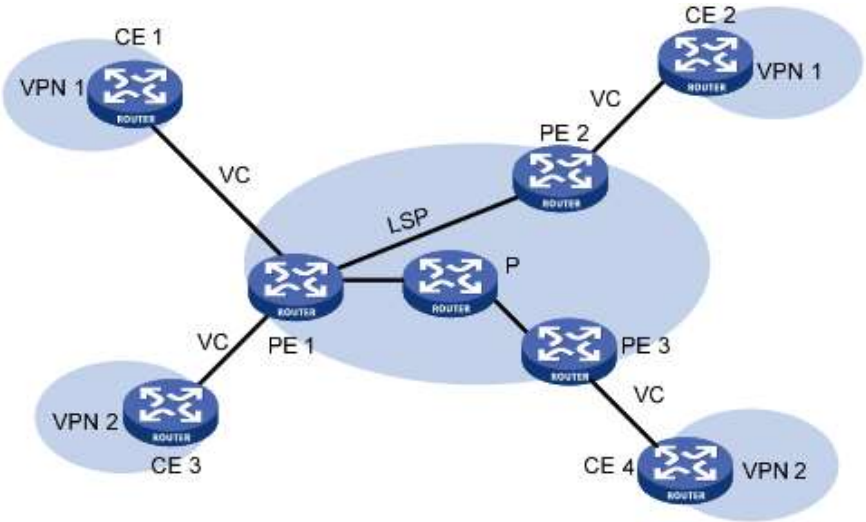


Fig.94. : MPLS L2VPN network.

11.1. Comparison with a Traditional VPN

Traditional VPNs based on Asynchronous Transfer Mode (ATM) or Frame Relay (FR) are very popular. They share the network infrastructure of service providers. However, they present certain inherent drawbacks :

- Dependence on dedicated media : To provide both ATM-based VPN services and FR-based VPN services, operators must deploy two separate infrastructures across the entire service coverage area : one ATM infrastructure and one FR infrastructure. Obviously, the cost is very high, and the infrastructures are not used efficiently.
- Complex deployment : To add a site to an existing VPN, it is necessary to modify the configurations of all edge nodes connected to the VPN site.

MPLS Layer 2 VPN (MPLS L2VPN) was developed as a solution to overcome the above disadvantages.

11.2. Comparison with a MPLS L3VPN

Compared with MPLS L3VPN, MPLS L2VPN offers the following advantages :

- High scalability. MPLS L2VPN establishes only Layer 2 connections. It does not involve user routing information. This significantly reduces the load on Provider Edge (PE) devices, as well as the load on the entire service provider network, enabling operators to support more VPNs and serve more users.
- Guaranteed reliability and security of private routing information. Since no user routing information is involved, MPLS L2VPN does not attempt to obtain or process user routing information, ensuring the security of the user's VPN routing information.
- Support for multiple network layer protocols, such as IP, IPX, and SNA.

11.3. Basic Concepts

In MPLS L2VPN, the concepts and principles of CE, PE, and P are the same as those of MPLS L3VPN :

- **Customer Edge (CE) device :** A CE resides on the customer network and has one or more interfaces directly connected to the service provider's network. It may be a router, a switch, or a host. It cannot "detect" the existence of a VPN, nor does it need to support MPLS.
- **Provider Edge (PE) device :** A PE resides on the service provider's network and connects one or more CEs to the network. In an MPLS network, all VPN processing takes place on the PE devices.

- **Provider (P) device :** A P device is a backbone device in the service provider's network. It is not directly connected to any CE. It only needs to support basic MPLS forwarding capabilities.

MPLS L2VPN uses label stacks to implement transparent transmission of user packets across the MPLS network.

- The outer label, also called the tunnel label, is used to forward packets from one PE to another.
- The inner label, also called the VC (Virtual Circuit) label, is used to identify different connections between VPNs.
- Upon receiving packets, a PE determines to which CE the packets should be forwarded according to the virtual circuit labels.

11.4. MPLS L2VPN Implementation

MPLS L2VPN can be implemented using one of the following methods:

1. **Circuit Cross Connect (CCC) and Static Virtual Circuit (SVC) :**
   Two methods for implementing MPLS L2VPN by statically configuring VC labels.
2. **Martini :**
   A method for establishing point-to-point connections to implement MPLS L2VPN. It uses the Label Distribution Protocol (LDP) as the signaling protocol to exchange VC labels.
3. **Kompella :**
   A CE-to-CE mode for implementing MPLS L2VPN over an MPLS network. It uses Multiprotocol BGP as the signaling protocol to advertise Layer 2 reachability information and VC labels.

12. MPLS-L3VPN

MPLS L3VPN is a type of L3VPN technology based on PE for service provider VPN solutions. It uses BGP to advertise VPN routes and uses MPLS to forward VPN packets across service provider backbones. MPLS L3VPN is widely used because it offers flexible networking modes, excellent scalability, and practical support for MPLS QoS and MPLS TE.

The MPLS L3VPN model consists of the following device types :

- **Customer Edge (CE) device :**
  A CE resides in the customer network and has one or more interfaces directly connected to the service provider's networks. It can be a router, switch, or host. It is not aware of the VPN and does not need to support MPLS.

- **Provider Edge (PE) device :**

  A PE resides in the service provider network and connects one or more CEs to the network. In an MPLS network, all VPN processing occurs on the PEs.

- **Provider (P) device :**

  A P device is a core router within the service provider network. It is not directly connected to a CE. It only needs to support basic MPLS forwarding capability.

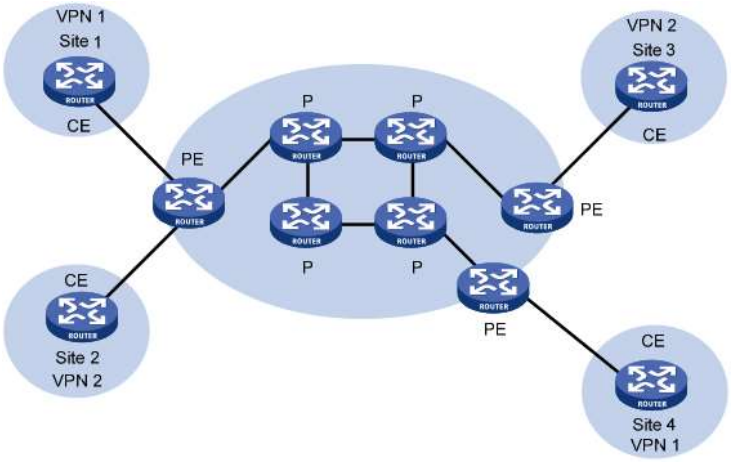


Fig.95. : MPLS L3VPN network.

CE and PE devices define the boundary between service providers and customers.

A CE is usually a router. Once a CE establishes contact with a directly connected PE, it advertises its VPN routes to the PE and learns remote VPN routes from the PE.

A CE and a PE use BGP/IGP to exchange routing information. Static routes can also be configured between them. Once a PE has learned VPN routing information from a CE, it uses BGP to exchange VPN routing information with other PEs. A PE keeps routing information only for directly connected VPNs, rather than all VPN routing information in the provider's network. A P router maintains only routes to PE routers. It does not need to know any VPN routing information. When VPN traffic passes through the MPLS backbone, the ingress PE acts as the ingress LSR, the egress PE acts as the egress LSR, while P routers function as transit LSRs.

13. MPLS/TE (Traffic Engineering)

Traffic Engineering (TE) is one of the main applications of MPLS. It allows load distribution across the entire network by establishing explicitly routed paths (Explicit Routing) and controlling traffic distribution over different links in order to avoid underutilization of certain part of the network. By default, MPLS builds LSPs based on routing information and follows the "shortest path" selected by the IGP routing protocol. This often leads to overused or underused links. MPLS/TE is used to create LSPs that diverge from the "shortest path". CR-LDP and RSVP-TE are used to establish these LSPs. MPLS/TE supports automatic LSP generation but also allows explicit specification of the path the LSP must follow. CR-LDP and RSVP-TE further allow

associating Quality of Service (QoS) characteristics with paths and making LSP establishment dependent on resource availability in intermediate devices. MPLS/TE enables advanced load balancing and differentiated routing functions based on information contained in the packet header or the ingress interface. To achieve this, one or more alternative paths can be created for a given FEC, and the route selection can be made based on additional information such as IP header fields, packet origin, link utilization state, etc. Thus, Traffic Engineering allows mapping traffic flows to the physical network topology. It provides the ability to divert traffic away from the IGP-computed "shortest path" and route it through less utilized paths. The goal of Traffic Engineering is to balance traffic load across different links or routers in the network so that none of these components is overused or underused. This allows an ISP to fully exploit its network infrastructure.

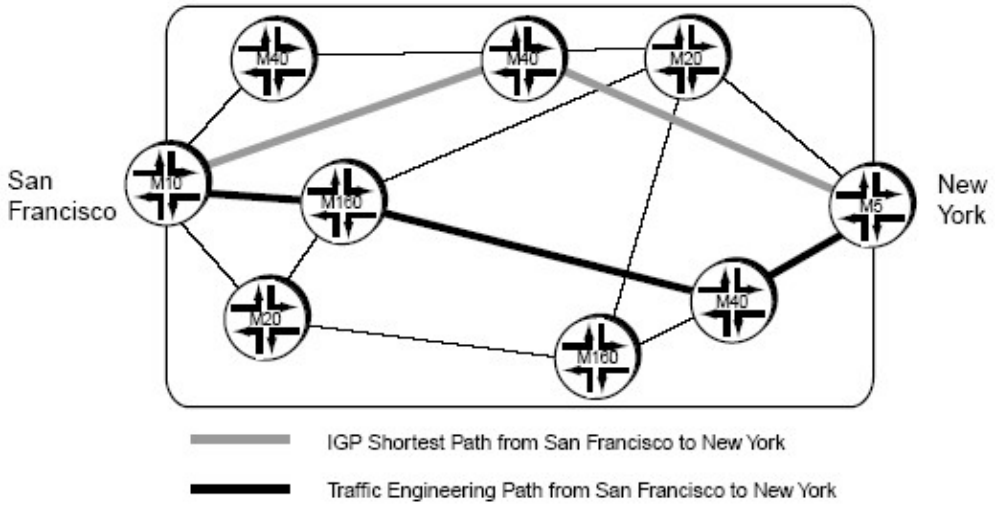


Fig.96. : MPLS/TE Traffic Engineering.

An algorithm (modified Dijkstra) calculates the best path based on the requested constraints, using topology information received from the routing protocol (IGP + its TE extension), such as bandwidth information (maximum physical bandwidth, maximum reservable bandwidth, availability per service class), link identification, TE metrics, and attributes.

14. Applications

The most common applications of MPLS are as follows :

- Traffic Engineering (TE) is enabled by MPLS mechanisms that allow traffic to be directed along a specific path.
- Guaranteed bandwidth provides a high-value improvement compared to traditional traffic engineering mechanisms.
- MPLS allows service providers to allocate bandwidth and guaranteed channels.
- Fast rerouting enables very rapid recovery after a link or node failure.

- MPLS Virtual Private Networks significantly simplify service deployment compared to traditional IP VPNs.
- The MPLS Class of Service (CoS) function ensures that important traffic is treated with the appropriate priority across the network and that latency requirements are met.

15. Conclusion

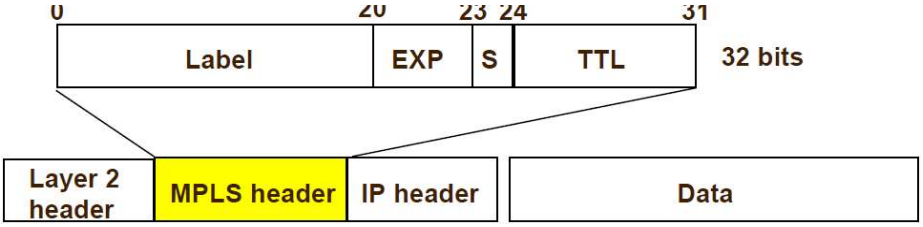
MPLS therefore enables better traffic management across the network by relying on traffic classification and label switching mechanisms. The need to optimize performance, resources, and traffic flows in operational networks has led to the concept of Traffic Engineering (TE).

In MPLS networks, the use of the RSVP-TE protocol helps meet these requirements. Thanks to its advanced capabilities for traffic optimization, management, and routing, combined with error detection, RSVP-TE provides essential complementarity within an MPLS network alongside Quality of Service (QoS) and Traffic Engineering.

16. Exercise with solution

1. **What does MPLS represent ?**
   - MPLS (Multi-Protocol Label Switching) is a packet-switching technology based on labels to make forwarding decisions. With MPLS, the analysis of the Layer 3 header is performed only once, which speeds up processing in the core of the network.
2. **What is the role of Traffic Engineering ?**
   - Traffic Engineering refers to the set of techniques applied to control and regulate traffic distribution within a network. It addresses the optimization of network resources.
3. **What applications does MPLS provide ?**
   - Virtual Private Networking (VPN).
   - Traffic Engineering (TE): controlling and regulating traffic distribution in a network.
   - Quality of Service (QoS).
   - Any Transport over MPLS (AToM).
4. **In your opinion, which routing protocol is used by MPLS ?**
   - None. However, path establishment using LDP relies on OSPF or IS-IS routing tables.
5. **If we map MPLS to the OSI model, at which layer does it operate ?**
   - Layer 2.5.
6. **Why is there a difference between edge routers and core routers ?**
   - Yes. Core routers only handle MPLS switching, while edge routers handle MPLS as well as IP, ATM, Frame Relay, and Ethernet (adaptation and encapsulation of packets/frames into MPLS packets).
7. **What do FEC and LDP mean in MPLS ?**
   - Label Distribution Protocol (LDP): a protocol that defines procedures and messages by which a Label Switching Router (LSR) informs another LSR of label bindings it has made. LDP is used to establish label-switched paths across a network by mapping network-layer routing information directly onto data-link layer switched paths.
   - Forwarding Equivalence Class (FEC): a term used in MPLS to describe a set of packets with similar and/or identical characteristics that are forwarded in the same way.

8. **What is the relationship between MPLS and DiffServ ?**
   - MPLS uses DiffServ marking.
9. **Which protocol and port does LDP use ?**
   - TCP, port 646.
10. **What is a label? What is the format of an MPLS header ?**
    - A label is a 20-bit integer with local significance.
    - The MPLS header format is as follows :



    - Label: 20 bits – Used to configure the LSP (Label Switched Path).
    - EXP: 3 bits – Experimental – used to prioritize traffic.
    - S: 1 bit – Stack (stack indicator).
    - TTL: 8 bits – Time-To-Live (lifetime).

    Note : Labels only concern adjacent nodes.
11. **What does "Layer 2 VPN" represent ?**
    - Layer 2 VPNs allow service providers to deliver Layer 2 services such as Frame Relay, ATM, and Ethernet between customer sites over an IP/MPLS backbone.

Chapter IV

Access technologies.

(Wired Local Loop Topology, NRA/NRO, Distribution Point (PM), Backhaul Network Connection)

Unit 1 : Access technologies :

(Wired Local Loop Topology, NRA/NRO, Distribution Point (PM), Backhaul Network Connection).

Unit Objectives :

By the end of this chapter, you should be able to :

- Learning Objectives.
- Understand Access Network Fundamentals.
- Analyze Wired Local Loop Topologies.
- Understand NRA/NRO Access Nodes.
- Explain the transition from DSL-based NRA architectures to fiber-based NRO architectures.
- Study Distribution Point (PM).
- Explain fiber splitting and subscriber distribution mechanisms.
- Understand Backhaul Network Connection.
- Analyze Integrated Access Architecture.

Topics Covered :

- Definition of access technologies.
- Evolution of access networks.
- Local loop fundamentals.
- Copper access topology.
- Fiber access topology.
- Network architecture models.
- NRA/NRO architecture.
- DSLAM operation.
- OLT deployment.
- Migration from xDSL to FTTH.
- PM architecture.
- Fiber distribution cabinets.
- Operator mutualization.
- Metro and backhaul architecture.

1. Introduction

A telecommunications operator's access network—often called the local loop, subscriber loop, or last-mile network, is the part of the operator infrastructure that connects end users (residential, enterprise, or mobile sites) to the operator's core network. Historically, this loop was built using copper pairs for traditional telephone services, but modern operator networks now integrate fiber, coaxial cable, wireless access, and hybrid infrastructures to support broadband, voice, video, and data services.

The local loop plays a critical role because it represents the interface between customer premises and the operator's transport infrastructure. It typically starts at the customer equipment (telephone, modem, router, or optical network terminal) and extends to a central office, street cabinet, or aggregation node where traffic is concentrated before entering metropolitan or core networks.

2. Definition

The local loop refers to all the resources and facilities implemented by an operator to collect and transport users' traffic. A more restrictive definition limits the use of the term local loop to only the subscriber access cable connecting the user to the network. For historical reasons, the infrastructure of the local loop network corresponds to that originally deployed for the distribution of voice services. Today, this infrastructure is shared between access to voice networks and access to data networks.

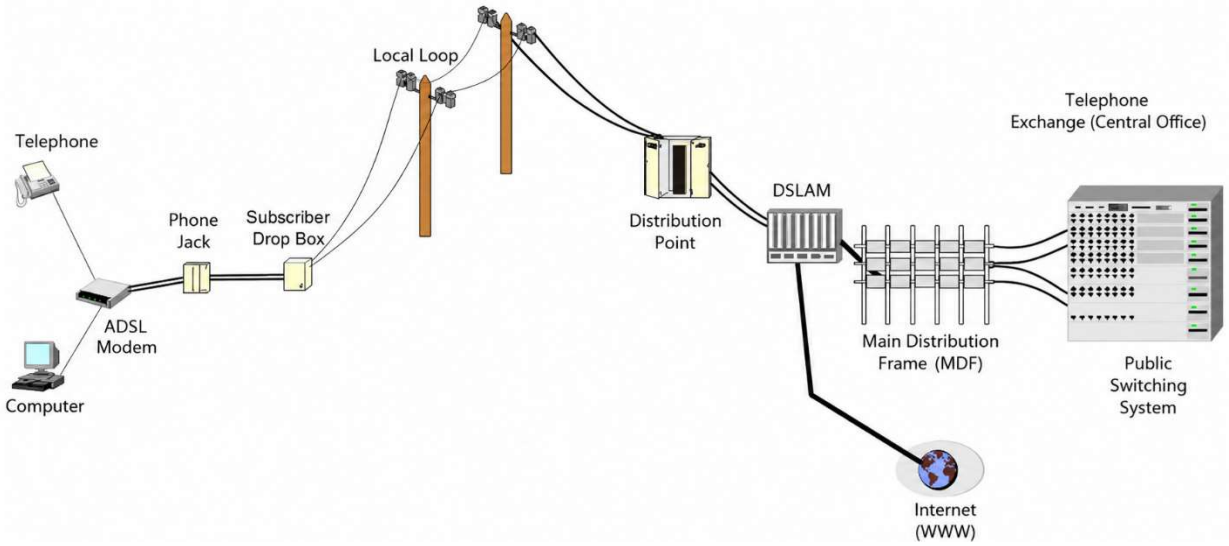


Fig.97 : Local Loop.

3. Local loop technologies

Several local loop technologies used to connect customers to high-speed Internet networks coexist :

- ✓ Cable networks, historically introduced for the first time by cable TV providers ; this technology is mainly deployed in urban areas. Cable networks make it possible to offer subscriptions ranging from 100 Mbit/s to 400 Mbit/s. The transmission media traditionally used are existing coaxial cables, which

carry traffic to a nearby optical node. The investment required to deploy a cable connection is significantly lower than that of FTTx, especially in homes already equipped with cable television infrastructure.

- ✓ Optical fiber, such as FTTH (Fiber To The Home) or more generally FTTx, is the preferred technology for very high-speed broadband. Several technologies coexist under this designation, depending on the point in the network where the conversion from optical to electrical signals takes place, each supporting different transmission speeds.



Fig.98. : FTTx Technologies.

3.1. FTTx Technologies

Among optical access networks, we find :

1. FTTN : Fiber To The Neighbourhood.
2. FTTC : Fiber To The Curb.
3. FTTS : Fiber To The Street.
4. FTTN : Fiber To The Node.
5. FTTB : Fiber To The Building.
6. FTTCab : Fiber To The Cab.
7. FTTP : Fiber To The Premises.
8. FTTH : Fiber To The Home.
9. FTTO : Fibre To the office.
10. FTTLA : Fiber To The Last Amplifier.

3.2. High-Speed Access Networks

3.2.1. General Overview

In large metropolitan areas, the distribution of video content has widely relied on optical fiber, which is the ideal medium for broadband transmissions. Bringing optical

fiber directly to the subscriber (FTTH, Fiber To The Home) appears to be the ideal solution, but it is too expensive.

Therefore, distribution to the end user is generally carried out using copper cable from a shared distribution point located in the building (FTTB, Fiber To The Building) or closer to a group of houses (FTTC, Fiber To The Cabinet).

However, this approach requires infrastructure work that can only be economically justified in large metropolitan areas. Given the existing installed base, the idea of reusing the entire telephone distribution network to provide every subscriber of the residential or business switched telephone network with high-speed access over a simple telephone line has led to the development of new technologies aimed at making.

3.2.2. DSL Techniques

The voice service bandwidth is limited to 4 kHz; however, the actual bandwidth of the twisted pair exceeds 1 MHz. ADSL technology (Asymmetric Digital Subscriber Line), while preserving the bandwidth required for telephone service, provides high-speed access to the end user. ADSL shares the available bandwidth between the voice service (0 to 4 kHz) and two simplex data channels: the so-called upstream (Up), offering a bandwidth from 32 to 640 kbit/s, and the downstream (Down), providing a data rate from 1.5 to 8.2 Mbit/s. Access to the operator's broadband network via the telephone line requires the installation of a specific device at the user's premises that ensures channel separation: the splitter (voice separator), or POTS coupler (Plain Old Telephone Service), and the ADSL modem. The splitter is generally integrated into the modem. The modem provides access via Ethernet, USB, or ATM interfaces.

On the operator side, the DSLAM (Digital Subscriber Line Access Multiplexer) is a statistical multiplexer that provides the interface between user connections and the operator's broadband network.

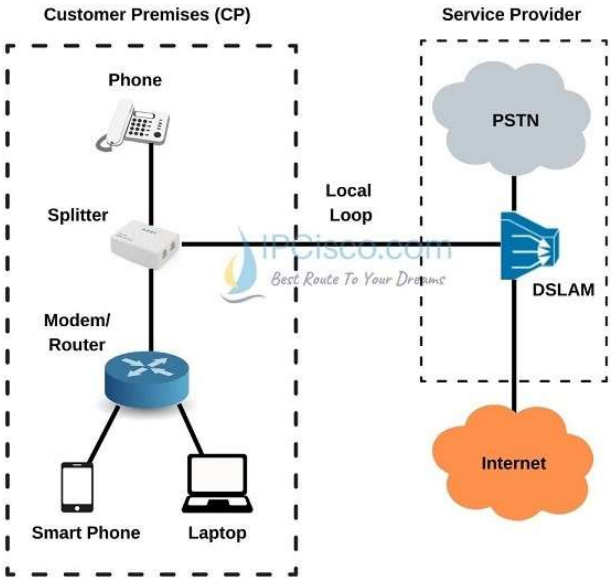


Fig.99. : DSL Techniques.

ADSL is standardized by ANSI and ETSI. However, given the investments required to deploy an ADSL network, manufacturers and operators have formed a working group, the UAWG (Universal ADSL Working Group), to define a simplified version. ADSL G.Lite integrates the splitter (channel separator) into a self-configuring (Plug and Play) modem, limits the data rates to 1.5 Mbit/s in the upstream direction and to 512 kbit/s in the downstream direction by reducing the number of sub-channels.

Type	Description	Data Rate Upstream Data Rate	Max Downstream Data Rate	Max Reach	POTS Support
HDSL	High Bit Rate - DSL	1.54Mbps	1.54Mbps	3650mtrs	No
ADSL	Asymmetric - DSL	800Kbps	8Mbps	5500mtrs	Yes
SDSL	Symmetric - DSL	2.3Mbps	2.3Mbps	6700mtrs	No
VDSL	Very High Bit Rate - DSL	16Mbps	52Mbps	1200mtrs	Yes
VDSL2	Very High Bit Rate - DSL (2nd Generation)	100Mbps	100Mbps	<1500mtrs	Yes

Table.14. : xDSL Techniques.

3.3. Telephone Local Loop

The local loop is the part of the telephone line (copper pairs) extending from the telephone operator's distribution frame to the subscriber's telephone socket. Physically, it consists of all the urban cables that can be seen in the streets, underground cables, as well as the pair of wires reaching the end user's premises.

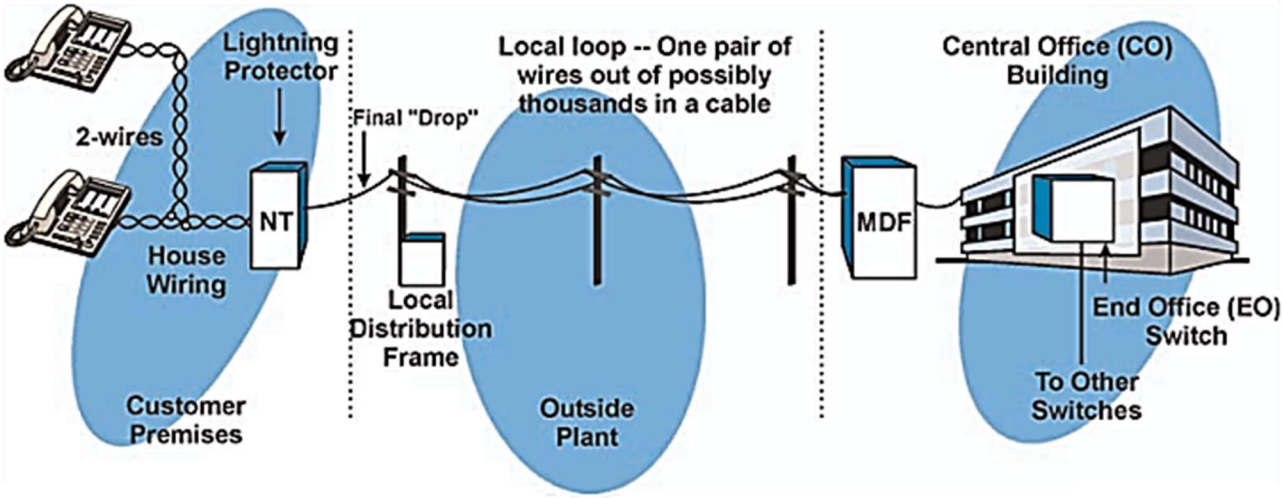


Fig.100. : Telephone Local Loop.

3.4. Optical Local Loop

The optical local loop enables very high-speed Internet access (typically equal to or greater than 100 Mbit/s); it may consist of end-to-end optical fibers (FTTH) or a combination of fiber optics and terminations using coaxial cable or copper twisted pairs.

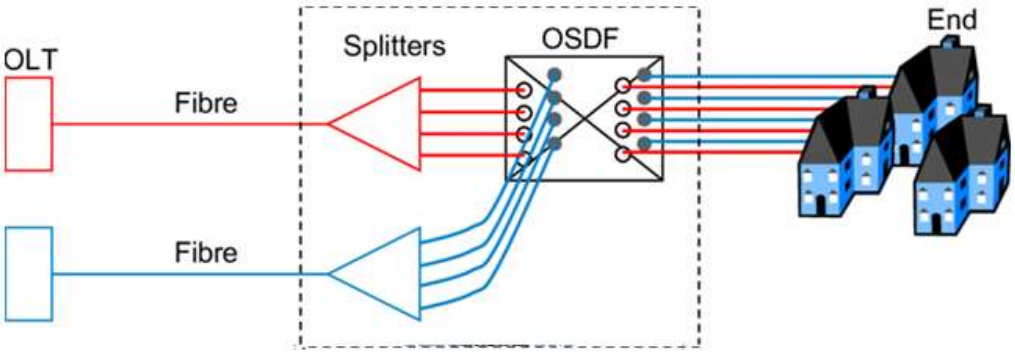


Fig.101. : Optical Local Loop.

4. NRA/NRO

The NRA (Subscriber Connection Node) is a secure technical facility that has been granted access to the core of a distribution frame (telephone exchange). It provides detailed insight into the operation of the network that connects ADSL subscribers to their service providers.

4.1. NRA core of ADSL network

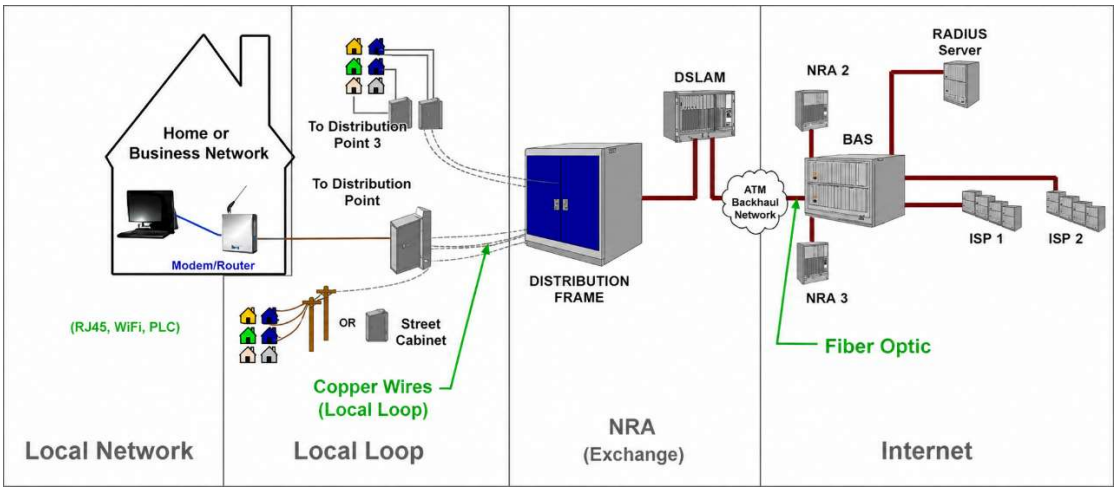


Fig.102. : NRA core of ADSL network.

The NRAs are the telephone exchanges of the telecom operator in which subscribers' telephone lines terminate, regardless of their ADSL internet service provider. Today, there are nearly 88 NRAs distributed across the entire territory of the Wilaya of Tiaret (Algérie Télécom). Previously dedicated only to the public switched telephone network (PSTN), NRAs (or telephone exchanges) are now essential for Internet users subscribed to ADSL services.

a) The distribution frame :

It is an important component of the NRA, since it is here that the first sorting of subscribers' lines takes place. The copper pairs are therefore organized and routed to be connected to the respective DSLAMs of the service providers corresponding to each line.



Fig.103. : The distribution frame.

b) The copper pair

xDSL technologies, such as ADSL or HDSL, all rely on the use of the copper pair used for telephone services. It is over this copper wire, which runs from your wall socket to the telecommunications operator's facilities, that voice signals (telephony) and digital IP signals (Internet) are transmitted. Your line is therefore connected from your home to a street cabinet, then to a distribution node that groups together several lines from the same neighborhood, for example. It then continues to the Algeria Telecom exchange, where all the copper pairs of the area are connected. This part of the network is called the "local loop".

c) DSLAM (Digital Subscriber Line Access Multiplexer)

The NRA itself is composed of several parts. On one side, there is the Algérie Télécom distribution frame, and on the other side, a co-location room where all the DSLAMs of the internet service providers are gathered. In reality, DSLAMs hide equipment that acts as an interface between subscriber lines and the operator's network to which they belong (the Algérie Télécom operator).



Fig.104. : DSLAM.

The DSLAM manages both voice traffic and data traffic (IP data). It is also the final stage for the copper pair. Once concentrated in the DSLAM, the data is separated by type (voice, internet, TV) and then sent over the provider's fiber optic network to be routed toward its own infrastructure.

d) Unbundling Room (Co-location Room)

The unbundling room is a space reserved for alternative operators, where all the DSLAMs of each operator are located. This is where technicians connect your copper lines to your operator's fiber optic network.

At the heart of this secured room, you will find:

- Electrical cabinets,
- Backup batteries,
- Patch cords connecting the lines to the DSLAMs,
- Fiber optic cables linking the DSLAMs to the different networks.



Fig.105. : Unbundling room (Co-location Room).

Unbundling rooms are generally small in size and, given the high density of electrical equipment, the ambient temperature is close to 30°C.

4.2. Optical Connection Node (NRO)

The Optical Connection Node (NRO) is, in a fiber-to-the-home (FTTH) access network, the location where the subscriber lines of the same neighborhood or city converge. It can be compared to the NRA (Subscriber Connection Node) of the copper local loop.

The main components of an NRO are:

- Uninterruptible power supplies (UPS).
- Backup batteries.
- Air conditioning system.
- Fiber optic cables.

- Optical subscriber distribution frame.
- Optical network switches (so-called Optical Switches).
- Optical patch cords.

➢ **Concept :**

The concept is similar to that of the NRA, with some differences. The term Optical Connection Node is defined by ARCEP. On November 18, 2011, ARCEP published a summary of responses to its public consultation on FTTH network deployment costs, which addresses both the Subscriber Connection Node (NRA) and the Optical Branching Point (PBO).

The NRO occupies about 100 m². It also supports FTTH services.

The Optical Line Terminal (OLT) replaces the DSLAM. It connects the Internet Service Provider's customers to the operator's network via a 10 Gbit/s optical link. An NRO serving 24,000 customers can occupy only 20 m².



Fig.106. : Optical Connection Node.

Note :

By using FTTH-GPON technology, the telecom operator optimizes the occupancy of underground ducts in the streets.

GPON : Gigabit Passive Optical Network.



Fig.107. : FTTH-GPON.

5. Distribution Point (PM) in FTTH Networks

5.1. Introduction

In fiber-to-the-home (FTTH) architectures, the Distribution Point (PM) (French: Point de Mutualisation) is a key infrastructure element that enables the sharing of the optical access network between multiple operators.

It plays a central role in the last segment of the fiber access network, where operator infrastructure meets the building or neighborhood distribution network.

5.2. Definition

The Distribution Point (PM) is a technical location in a shared FTTH network where:

- Optical fibers from subscribers (via the building operator).
- are interconnected with fibers from commercial Internet service providers (ISPs).

This interconnection allows multiple operators to serve the same end users using a shared passive infrastructure.

5.3. Role of Distribution Point

The PM ensures :

- Fiber sharing (network mutualization) between operators.
- Flexibility of connection for subscribers.
- Access competition between different ISPs.
- Management of last-mile fiber distribution.

5.4. Architecture Position in FTTH Network

Typical FTTH hierarchy :

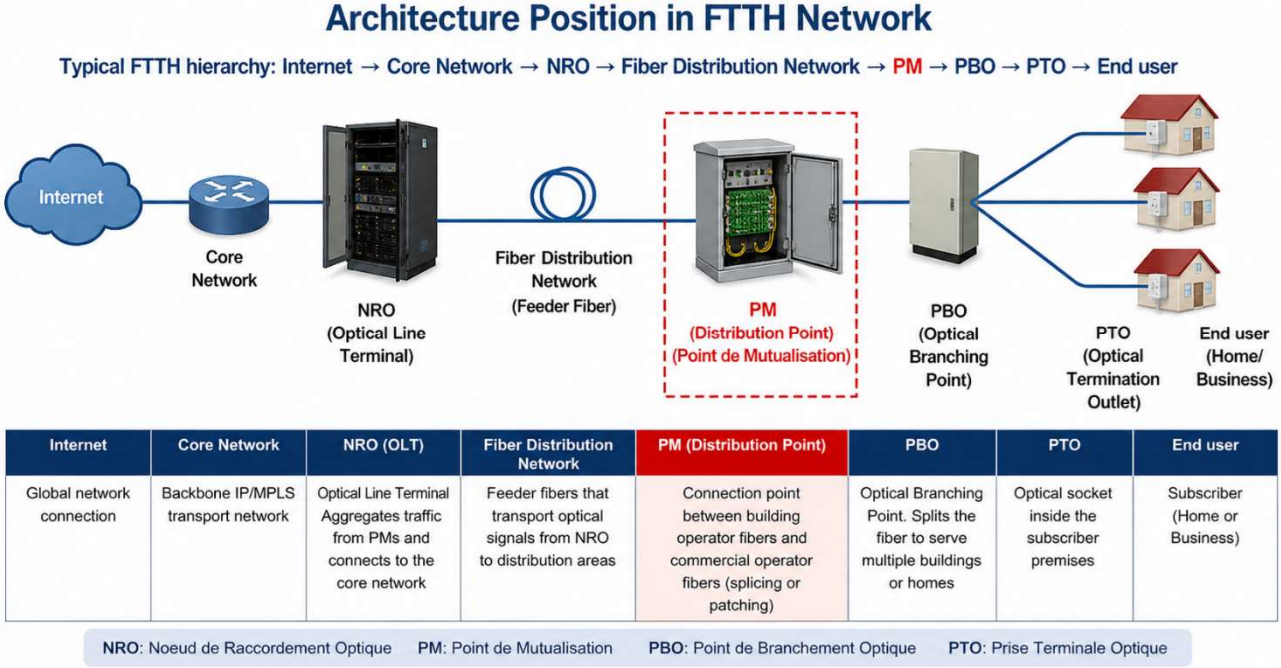


Fig.108. : Architecture Position in FTTH Network.

5.5. Types of Connections at the PM

At the PM, connections can be made using :

- **Fiber Splicing**
  - Permanent connection.
  - Low loss.
  - Used for stable network design.
- **Patch Panel (Brassage)**
  - Flexible connection using patch cords.
  - Allows easier reconfiguration.
  - Common in operator-managed PMs.

5.6. Physical Implementation

A PM is usually installed in:

- Street cabinets.
- Technical rooms in buildings.
- Underground chambers.
- Outdoor shelters (weather-protected).

5.7. Main Components of a PM

- Optical distribution frames (ODF).
- Fiber splice trays.
- Patch panels.
- Optical connectors (SC/APC, LC, etc.).
- Cable management systems.

5.8. Types of PM

- **Outdoor PM**
  - Located in street cabinets.
  - Covers a neighborhood or street area.
- **Indoor PM**
  - Located inside buildings.
  - Used in dense urban FTTH deployments.

5.9. Importance of the PM in FTTH

- Enables multi-operator competition.
- Simplifies fiber deployment.
- Reduces infrastructure duplication.
- Facilitates customer migration between ISPs.
- Improves network scalability.

5.10. Advantages and Limitations

- **Advantages**
  - Efficient infrastructure sharing.
  - Faster deployment of FTTH services.
  - Flexible operator management.
- **Limitations**
  - Requires precise fiber management.
  - Risk of congestion in poorly designed PMs.
  - Maintenance complexity in large deployments.

6. Backhaul Network Connection

6.1. Introduction

In modern telecommunications networks (FTTH, mobile, and enterprise networks), the aggregation network (also called the backhaul network) plays a key role in transporting traffic from access networks (users) toward the core network.

The connection to the aggregation network refers to how access equipment (such as Optical Line Terminals, DSLAMs, or base stations) is interconnected to higher-level transport infrastructure that carries data to service providers and the Internet backbone.

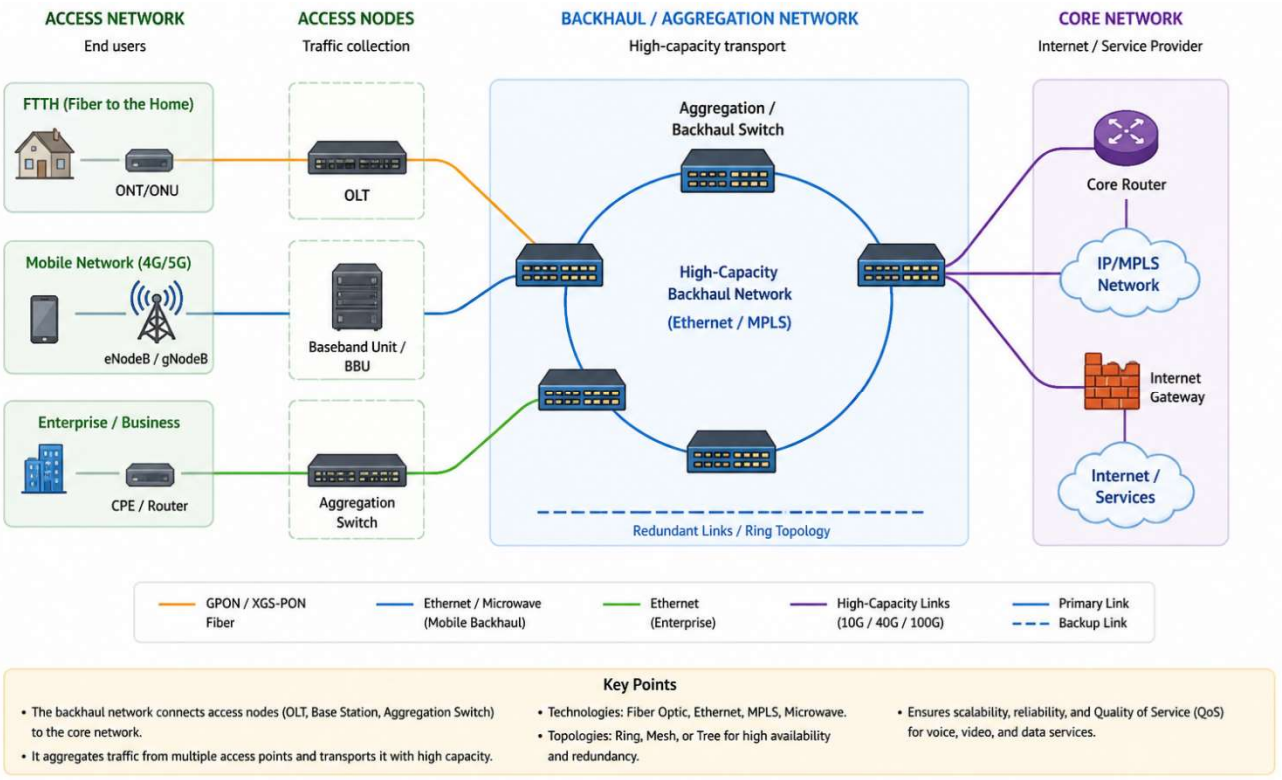


Fig.109. : Backhaul Network Connection.

6.2. Definition

The aggregation network is an intermediate layer between : Access network (users: FTTH subscribers, mobile users, enterprises) ; Core network (Internet backbone, service providers, data centers).

Its main function is to:

- Collect traffic from multiple access nodes.
- Aggregate (combine) it efficiently.
- Forward it to the core network with optimized bandwidth usage.

6.3. Role in FTTH Architecture

In a typical FTTH (Fiber To The Home) architecture :

- ONTs/ONUs (at user side).
- are connected to ODN (Optical Distribution Network).
- then to OLT (Optical Line Terminal).
- and finally to the aggregation/backhaul network.

This connection is essential for transporting broadband services like Internet, IPTV, and VoIP.

6.4. Main Components of the Aggregation Connection

➢ **Access Nodes**

- OLT (Optical Line Terminal).
- DSLAM (Digital Subscriber Line Access Multiplexer).
- Mobile Base Stations (eNodeB / gNodeB).

- **Aggregation Switches/Routers**
  - Layer 2/Layer 3 switches.
  - IP/MPLS routers.
  - Ethernet aggregation switches.
- **Transport Technologies**
  - Optical Fiber (main medium).
  - Ethernet (10G/40G/100G links).
  - MPLS (Multi-Protocol Label Switching).
  - WDM (Wavelength Division Multiplexing).

6.5. Topology of the Aggregation Network

Common topologies include:

- Tree topology (most common in FTTH).
- Ring topology (high resilience).
- Mesh topology (high redundancy in core areas).

Ring topology is widely used to ensure:

- Fault tolerance.
- Automatic traffic rerouting

6.6. Connection Process (How traffic is aggregated)

- User data is generated at access network (FTTH, mobile, etc.).
- Traffic is collected at access nodes (OLT, DSLAM).
- Traffic is multiplexed and aggregated.
- Data is transported via high-capacity links.
- Aggregation routers forward traffic to the core network.

6.7. Key Protocols Used

- Ethernet (Layer 2 transport).
- MPLS (traffic engineering, QoS).
- IP (routing).
- VLAN tagging (traffic separation).
- GPON/XG-PON protocols (in access segment).

6.8. Quality of Service (QoS)

In aggregation networks, QoS is critical to ensure:

- IPTV streaming without delay.
- VoIP with low latency.
- Internet data stability.

Mechanisms include:

- Traffic prioritization.
- Bandwidth allocation.

- Congestion control.

6.9. Advantages of a Well-Designed Aggregation Network

- Efficient bandwidth usage.
- Reduced congestion.
- Scalability for future growth (5G, IoT, FTTH expansion).
- High reliability and redundancy.
- Better service quality for users.

7. Conclusion

Modern fixed access networks are built on a hierarchical and highly optimized architecture that ensures scalability, service quality, and efficient traffic aggregation from end users to the core network. The key components—Backhaul Network Connection, Distribution Point (PM), NRA/NRO access nodes, and the Integrated Architecture layer—form a coherent end-to-end ecosystem that supports the transition from legacy copper systems to high-capacity fiber infrastructures.

The NRA/NRO (Access Nodes) represent the strategic aggregation points of the access network. The NRA, traditionally associated with DSL technologies, has progressively evolved toward the NRO in FTTH architectures, where optical line terminals (OLT) aggregate and manage large volumes of subscriber traffic. This evolution reflects the shift from electrical to optical access, enabling higher bandwidth, reduced attenuation, and improved service reliability.

At an intermediate level, the Distribution Point (PM) plays a crucial role in fiber unbundling and last-stage distribution. It acts as a flexible optical branching node, enabling multiple operators to access shared passive infrastructure while ensuring fair resource allocation and physical separation of subscriber fibers. The PM is therefore essential in supporting competition and modular network expansion in FTTH deployments.

Above this layer, the Backhaul Network Connection ensures the transport of aggregated traffic from access nodes (NRO/OLT) toward the core IP/MPLS network. It is a critical performance domain where capacity, latency, jitter, and resilience must be tightly controlled. Technologies such as DWDM optical transport, MPLS traffic engineering, and high-capacity fiber links are fundamental to guarantee end-to-end QoS, especially with the rise of 5G, cloud services, and real-time applications.

Finally, the Integrated Architecture unifies these layers into a structured end-to-end model:

- Access layer (ONU/ONT ⟶ PM).

- Aggregation layer (PM ⟶ NRO/NRA).
- Transport layer (Backhaul network).
- Core network (IP/MPLS backbone).

This integration ensures seamless data flow, scalable bandwidth provisioning, and efficient network management, while enabling operators to support massive broadband demand, multi-service delivery (triple/quad play), and future-ready infrastructures.

8. Exercises

1. Backhaul Network Connection

➢ Q1. In a modern FTTH architecture, the backhaul network primarily connects :

- ONT to customer devices.
- Distribution Point (PM) to end users.
- NRO to the core IP/MPLS network.
- ONU to ONT inside the home.

Explanation :
The backhaul carries aggregated traffic from the NRO (or OLT sites) toward the core network (IP/MPLS backbone).

➢ Q2. Which technology is MOST commonly used for high-capacity backhaul in dense urban FTTH deployments ?

- DSL copper pairs.
- Microwave point-to-point only.
- Optical fiber with WDM or DWDM.
- Satellite links.

Explanation :
Fiber with WDM/DWDM is used for scalable multi-terabit backhaul.

➢ Q3. A key QoS requirement in backhaul networks is:

- Low optical attenuation only.
- High latency variation tolerance.
- Deterministic latency and jitter control.
- Maximum number of subscribers per ONU.

Explanation:
Backhaul must ensure stable latency and low jitter, especially for 5G/VoIP.

2. Distribution Point (PM)

➢ Q1. The PM in FTTH architecture is best described as :

- A customer modem termination point.
- A fiber aggregation node between operator and subscribers.
- A core IP routing switc.
- A microwave relay station

Explanation:
The PM is where multiple subscriber fibers are aggregated and made available to operators.

- Q2. In multi-operator FTTH architecture, the PM mainly ensures:
  - A. Encryption of user traffic.
  - Physical separation of home routers.
  - Fiber unbundling between operators.
  - Power supply to ONT devices

  Explanation:
  The PM enables local loop unbundling (LLU) in FTTH networks.
- Q3. Which statement about PM placement is TRUE?
  - Always located inside the central office.
  - Always installed in the subscriber home.
  - Can be located in buildings, street cabinets, or underground chambers.
  - Exists only in backbone networks.

  Explanation:
  PM is a flexible physical node depending on FTTH topology (P2P, GPON, etc.).

3. NRA / NRO (Access Nodes)

- Q1. The NRO (Nœud de Raccordement Optique) is equivalent to:
  - A customer router.
  - A central fiber distribution hub / OLT site.
  - A Wi-Fi access point.
  - A satellite gateway.

  Explanation:
  The NRO is the main optical access node hosting OLT equipment.
- Q2. The main function of the NRA (Noeud de Raccordement Abonnés) in legacy networks is :
  - Optical signal amplification in backbone.
  - DSL subscriber aggregation point.
  - Cloud data processing node.
  - Mobile base station controller.

  Explanation:
  The NRA is historically used in copper DSL networks to aggregate subscribers.
- Q3. Which evolution correctly describes the transition from NRA to NRO?
  - Copper network ⟶ Satellite network.
  - DSL aggregation ⟶ Fiber optic access aggregation.
  - Wireless LAN ⟶ Ethernet LAN.
  - IP network ⟶ Analog network.

  Explanation:
  NRA (DSL) ⟶ replaced by NRO in FTTH fiber-based access networks.

4. Integrated Architecture

- Q1. In a complete FTTH architecture, the correct traffic flow is:
  - Core ⟶ PM ⟶ ONU ⟶ NRO.
  - ONU ⟶ PM ⟶ NRO ⟶ Backhaul ⟶ Core Network.
  - PM ⟶ ONU ⟶ Core ⟶ Backhaul.
  - NRO ⟶ ONU ⟶ PM ⟶ Internet.

  Explanation:
  Correct hierarchy:
  ONU ⟶ PM ⟶ NRO ⟶ Backhaul ⟶ Core Network
- Q2. Which element is responsible for splitting fiber towards multiple subscribers?
  - OLT.
  - Splitter inside PM.
  - Core router.
  - IP gateway.

  Explanation:
  Optical splitters in the PM distribute a single fiber into multiple drops.
- Q3. A major technical constraint in backhaul dimensioning is:
  - Number of Wi-Fi users.
  - Optical fiber color coding.
  - Traffic aggregation from multiple PMs and NROs.
  - Customer billing system.

  Explanation:
  Backhaul must scale according to aggregated traffic from many access nodes.

Bibliographie

- A. S. Tanenbaum, Computer Networks, Pearson.
- W. Stallings, Data and Computer Communications, Pearson.
- ITU-T Recommendations (X.25, ATM).
- RFCs IETF (MPLS, BGP, IPsec).
- Mas-Machuca, C., et al. (2023). Optical Networks and Interconnects.
- Olzak, T. (2016). FTTx Networks: Technology Implementation and Operation. Morgan Kaufmann.