DEMOCRATIC AND POPULAR REPUBLIC OF ALGERIA
MINISTERY OF HIGHT EDUCATION AND SCIENTIFIC RESEARCHES

University of Ibn Khaldoun - Tiaret

THESIS

posted to :

MATHEMATICS AND COMPUTER SCIENCE
FACULTY COMPUTER SCIENCE DEPARTMENT

For the graduation of:

MASTER

Specialty: [Networks and Telecommunications (RT)]

presented by :

[BENSATTALAH ABDELKADER]

On the subject :

Comparison And Performance Evaluation Of ATM, FR And MPLS Wide Area Networks

Publicly supported on 07/13/2021 in Tiaret in front of the jury composed of:

Mr MEGHAZI Elhadj	MAA	Tiaret University	President
Mr Mostefaoui sid Ahmed Mokhtar	MCB	Tiaret University	Examiner
Mr Mostefaoui Kadda	MAA	Tiaret University	Supervisor

2020-2021

Gratitude

First we would like to thank God Almighty, Most Merciful, Most Merciful, who gave us strength and patience to accomplish this humble work.

Thank you very much to my father and mother who are the wings of the bird that I fly in the world. I wish them long life, health and wellness.

Secondly, I would like to thank Mr. **KADDA MOSTEFAOUI**, the supervisor of my memorandum, for his assistance and encouragement, and express my appreciation for his contribution to this study. His knowledge and explanation of procedures was crucial to my ability to complete this project using appropriate and supported research methods. I would also like to thank Mr. lARBI BEGHANI very much for his valuable and unforgettable advice and assistance in providing valuable information that you cannot find in people of high morals. I wish him A beautiful journey in appreciation of the study.

I would also like to thank Mr. SALIM BOUZIAN, who gave me a helping hand.

We also extend our sincere thanks to the members of the jury, **Mr SID_AHMED** MOKHTAR **MOSTEFAOUI** and **Mr.H.MEGHAZI**, who devoted their time to judge this humble work and we were honored to attend them, and who contributed to extending a helping hand to us during the study, you may find from us an expression of our gratitude and respect.

We also extend our thanks to all the professors and administrative staff who helped us during this undergraduate course, and finally we would like to thank our colleagues from the class of 2020-2021

We wish them a successful future

BENSATTALAH ABDELKADER

Dedication

I dedicate my dissertation work to my family , my father and mother.

and to my wife and son Iyad Abdul Basit, may God prolong his life

A special feeling of gratitude words of encouragement and push for tenacity .

I also dedicate this dissertation to my many friends, I will always appreciate all they have done,ather all to helping me develop my technology skills,

To everyone who participated directly or indirectly in my and helped me through difficult times.

To all my friends from closest to furthest.

BENSATTALAH ABDELKADER

Abstract

There are two categories of computer networks: local area network (LAN) and wide area network (WAN). To avoid bandwidth problems in the local network, we need to find a good visualization in a large-scale network that is often called a group of networks that are placed in many companies and organizations, and this type of network uses the hierarchical model. Several protocols are used for WAN such as: ATM, MPLS and Frame-relay. The first uses ATDM multiplexing and "cell switching", and the second uses "label switching". Both of them provide a lot of class of services to the users. The advantage of ATM and Frame-relay is the good performance in real-time transmission. But according to the analysis, we find that MPLS works with the famous "IP network" to build the path that packets take to reach the destination node. To connect two companies of "Local Area Network", MPLS is the best solution if we don't need many real-time transmissions, because it has good performance in throughput and high quality.

ملخص

هناك فئتان من شبكات الكمبيوتر: الشبكة المحلية (LAN) والشبكة الواسعة (WAN). لتجنب مشاكل النطاق الترددي في الشبكة المحلية ، نحتاج إلى إيجاد تصور جيد في شبكة واسعة النطاق غالبًا ما يتم استدعاؤها كمجموعة من الشبكات التي يتم وضعها في العديد من الشركات و المؤسسات ، ويستخدم هذا النوع من الشبكات النموذج الهرمي. يتم استخدام العديد من البروتوكولات لشبكة WAN مثل ATM: و MPLS و Frame-relay. الأول يستخدم تعدد إرسال ATDMو "تبديل الخلية" ، والثاني يستخدم "تبديل التسمية". كلاهم يوفر الكثير من فئة الخدمات للمستخدمين. ميزة ATMو Frame-relay هي الأداء الجيد في النقل في الوقت الفعلي. ولكن حسب التحليل نجد ان MPLS تعمل مع "شبكة IP" الشهيرة لبناء المسار الذي تسلكه الحزم للوصول إلى العقدة الوجهة. لربط شركتين من "شبكة المنطقة المحلية" ، فإن MPLS هي الحل الأفضل إذا لم نكن بحاجة إلى العديد من عمليات النقل في الوقت الفعلي ، لأنها تتمتع بأداء جيد في الإنتاجية و اعطاء جودة عالية.

RESUME

Il existe deux catégories de réseaux informatiques : les réseaux locaux (LAN) et les réseaux étendus (WAN). Pour éviter les problèmes de bande passante dans le réseau local, nous devons trouver une bonne visualisation dans un réseau à grande échelle qui est souvent appelé un groupe de réseaux qui sont placés dans de nombreuses entreprises et organisations, et ce type de réseau utilise le modèle hiérarchique. Plusieurs protocoles sont utilisés pour le WAN tels que : ATM, MPLS et Frame-relay. La première utilise le multiplexage ATDM et la "commutation de cellules", et la seconde utilise la "commutation d'étiquettes". Les deux fournissent beaucoup de classe de services aux utilisateurs. L'avantage de l'ATM et du Frame-relay est la bonne performance de la transmission en temps réel. Mais selon l'analyse, nous constatons que MPLS fonctionne avec le fameux "réseau IP" pour construire le chemin que les paquets empruntent pour atteindre le nœud de destination. Pour connecter deux entreprises de "Local Area Network", MPLS est la meilleure solution si nous n'avons pas besoin de beaucoup de transmissions en temps réel, car il a de bonnes performances en termes de débit et de haute qualité.

index

Figure list

ACRONYMS

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BIA	Burned In Address
BNC	Bayonet Nut Connector
BPDU	Bridge Protocol Data Unit
CBR	Constant Bit Rate
CCITT	International Telegraph and Telephone Consultative Committee
CDV	Cell Delay Variation
CIDR	Classless InterDomain-Routing
CEN	Carrier Ethernet Network
CER	**Cell Error Ratio**
CIR	Commited Information Rate
CLP	Cell Loss Priority
CLR	Cell Loss Ratio
CoS	Class of Service
CR-LDP	Contraint based-Routing LDP
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CS-PDU	Convergence Sublayer PDU
CTD	Cell Transfert Delay
CU	Currently Unused
CRC	cyclical redundancy check
CVDT	**Cell Variation Delay Tolerance**
DAN	Departemental Area Network
DARPA	Defense Advanced Research Projects Agency
DBR	Deterministe Bit Rate
DNS	Domain Name System
DE	Discard Eligibility
DTN	Disruptive Tolerance Network
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DLCI	Data Link Connection Identifier
DoD	Departement of Defense
DoS	Deny of Service
DCE	Data circuit-terminating equipment
DTE	Data terminal equipment
DSCP	Diffserv Code Point
DSL	Digital Subscriber Loop
EA	Extended Address

EGP	Exterior Gateway Protocol
EIR	Excess Information Rate
ELSR	Egress LSR
ETCD	Equipement Terminaison de Circuit de Donnés
ETTD	Equipement Terminal de Traitement de Données
EXP	Experimental
FCS	Frame Check Sequence
FECN	Forward Explicit Congestion Notification
FIFO	First In First Out
FR	Frame Relay
FTP	File Transfert Protocol
GFC	Generic Flow Control
GNS3	Graphical Network Simulator
GSM	Global System for Mobile
HDLC	High-level Data Link Control
HEC	Header Error Control
HTTP	Hyper Text Transfert Protocol
HTTPS	Hyper Text Transfert Protocol Secure
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIS	Internet Information Services
ILSR	Ingress LSR
IOS	Internetwork Operating System
ILD	injection laser diode
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ISDN	Integrated Service Digital Network
ISIS	Intermediate System to Intermediate System
ITU	International Telecommunication Union
LAN	Local Area Network
LAP-B	Link Access Protocol Balanced
LAP-D	Link Access Protocol on the D-channel
LAP-F	Link Access Protocol Frame
LDP	Label Distribution Protocol
LED	light emitting diodes
LER	Label Edge Router
LIB	Label Information Base
LLC	Logical Link Control
LMI	Local management Interface

LSFT	Label Switching Forwarding Table
LSP	Label Switch Path
LSR	Label Switch Router
MAC	Medium Access Control
MAN	Metropolitan Area Network
MBGP	MPLS Border Gateway Protocol
MBS	Maximum Brust Size
MCR	**Minimum** Cell Rate
MIC	Modulation par Impulsion Codée
MPLS	MultiProtocol Label Switching
MPLS-TE	MPLS Traffic Engineering
MSTP	Multiple Spanning Tree Protocol
NIC	network interface card
NGN	Next Generation Network
NNI	Network Node Interface
OAM	Operating And Maintenance
OSI	Open System Interconnection
OSPF	Open Shortest Path First
PABX	Private Automatic Branch eXchange
PCI	Protocol Control Information
PCR	Peak Cell Rate
PDU	Protocol Data Unit
PHB	Per-Hop Behaviour
PMD	Physical Medium Dependantsublayer
PME	Petites et MoyennesEntreprise
PMI	Physical Medium Independent sublayer
PPP	Point to Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PT	Playload Type
PTI	Playload Type Identifier
PVC	Permanent Virtual Circuit
PVST	Pre Vlan Spanning Tree
PSN	packet-switched network
QoS	Quality of Service
RFC	Request For Comment
RIP	Routing Information Protocol
RNIS	Reseau Numérique à Integration de Service
RSTP	Rapid STP
RSVP-TE	ReSerVation Protocol-Traffic Engineering
RPC	Remote procedure call protocol
RTC	RéseauTéléphoniqueCommuté
SAP	Service Access Point
SP	Switch Path
SAR	Segmentation And Reassembly

SBR	Statistical Bit Rate
SCP	Session Control Protocol
SCR	Sustainable Cell Rate
SDP	Session Description Protocol
SDU	Service Data Unit
SDH	Synchronous Digital Hierarchy
SMTP	Simple Mail Transfert Protocol
SNR	Signal to Noise Ratio
SONET	Synchronous Optical Network
STA	Spanning-Tree Algorithm
STP	Spanning-Tree Protocol
SVC	Switched virtual circuit
SONET	Synchronous Optical Network
TCP	Transmission Control Protocol
TLV	Type Length Value
ToS	Type of Service
TTL	Time To Live
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UTP	Unshielded twisted-pair
UMTS	Universal Mobile Telecommunications System
UNI	User Network Interface
VBR	Variable Bit Rate
VBR-rt/nrt	Variable Bit Rate real time/no real time
VCI	Virtual Circuit Identifier
VLAN	Virtual Local Area Network
VPI	Virtual Path Identifier
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

GENERAL INTRODUCTION

In the early days of information and communication technologies, telecommunications were represented only by telephones and telegraphs because of the limited integration of electronic components and the lack of control over radio wave propagation technologies. Since then, the people have always sought to emit more information to ever more distant destinations through the air and increasingly rational means. This race towards new technologies in the field of telecommunications has seen the advent of digital systems supplanting analog systems. Examples include the replacement of Morse codes by voice communication, mechanical machines by electronic machines such as computers.

The objective is always the same, introduce new technological discoveries into everyday life in order to improve the quality of connection of people and reduce further the distance of them, today Telecommunication and computer technology became common means that are increasingly found in homes and became common and indispensable tools in the daily work of people.

The network is one of the technologies that has been enhanced by this development in communications and computing, where all efforts are rewarded: the effort to migrate to the digital system, efforts to detect and correct transmission errors, and efforts to transmit speech to the side of the data. In this vast area, the main problem for users remains the same: How can we find a network that does not waste information and delivers better quality service? This aims to find a solution to this problem. Taking a practical example provides a more realistic view of the problem, and what network can be used to send high quality data in a certain amount of time. This means improving the means of communication, whether in the local area network (LAN) or in the wide area network (WAN).

The title of my thesis defense is: **“Comparing and Evaluating the Performance of ATM, FR and MPLS Wide Networks”.**

we will insist on the quality of service, The first chapter provides an overview of the network, ranging from transmission media to dynamic routing, Then, we will go into the details concerning the local network by proposing different configurations of a network.

In Chapter 2, WAN working techniques will be explained in their method and how to improve data transfer in ATM cell switching, MPLS naming switch, frame relay (FR), and the comparison between them.

As for the last chapter, it will be an application aspect of the network operation, we project the network from LAN to the wide area network WAN , we will compare the three different configurations ATM, MPLS FR, to give the best and the optimum one in the operator network, all through the GNS3 simulator and "Windows" devices. Analyzing the packet by "Wireshark" .

CHAPTER 1

GENERALITIES ABOUT NETWORKS AND ROUTING

I GENERAL INFORMATION ABOUT NETWORKS AND ROUTING

I.1 INTRODUCTION

In this first part of the discussion, we will focus on a set of basic definitions in the network that communicate with each other in order to share resources in the network. For more performance, the way these resources are shared must be improved, either in the physical or in the Logical part. This is the same goal that led to the digitalization of the transmission , it also encouraged engineers to search for the best transmission medium and to find the most appropriate software solution to make the most of the physical equipment. This chapter provides an overview of the network: While talking about generalities, we will go into details about critical points in this area, without losing sight of our goal of solving network problems. The concept of transmission medium will be explained first, then comes the model OSI and TCP / IP: the two software architectures that summarize all types of communication between entities.

I.2 Transmission Supports

Transmission support is a communication channel that carries the information from the sender to the receiver. Data is transmitted through the electromagnetic signals, The main functionality of the transmission media is to carry the information in the form of bits through LAN (Local Area Network). It is a physical path between transmitter and receiver in data communication.

In a copper-based network, the bits are in the form of electrical signals, In a fibre based network, the bits are in the form of light pulses, In OSI (Open System Interconnection) phase, transmission media supports the Layer 1. Therefore, it is considered to be as a Layer 1 component, The electrical signals can be sent through the copper wire, fibre optics, atmosphere, water, and vacuum. The characteristics and quality of data transmission are determined by the characteristics of medium and signal, Transmission media has two types , wired media and wireless media. In wired media, medium characteristics are more important, whereas, in wireless media, signal characteristics are more important.

Different transmission media have different properties such as bandwidth, delay, cost and ease of installation and maintenance, it is available in the lowest layer of the OSI reference model, i.e., Physical layer, Some factors need to be considered for designing the transmission media. [30]

I.2.1 Characteristics Of A Support

Several criteria are common to all types of media. Depending on these criteria and the quality of service we want to have, we opt for the transmission medium that appears to us to be the best. These characteristics are: the bandwidth, the noise in the medium and its capacity.

A good transmission medium should provide communication with good quality at long distance. [26]

- For voice communication, quality of communication is determined by the voice quality.

- For data communication, however, the quality of communication is mainly determined by the effective data rate of communication.

I.2.1.1 Bandwidth

Bandwidth describes the maximum data transfer rate of a network or Internet connection, it measures how much data can be sent over a specific connection in a given amount of time. For example, a gigabit Ethernet connection has a bandwidth of 1,000 Mbps (125 megabytes per second). An Internet connection via cable modem may provide 25 Mbps of bandwidth.

While bandwidth is used to describe network speeds, it does not measure how fast bits of data move from one location to another, Since data packets travel over electronic or fiber optic cables, the speed of each bit transferred is negligible. Instead, bandwidth measures how much data can flow through a specific connection at one time.

When visualizing bandwidth, it may help to think of a network connection as a tube and each bit of data as a grain of sand. If you pour a large amount of sand into a skinny tube, it will take a long time for the sand to flow through it. If you pour the same amount of sand through a wide tube, the sand will finish flowing through the tube much faster. Similarly, a download will finish much faster when you have a high-bandwidth connection rather than a low-bandwidth connection.

Data often flows over multiple network connections, which means the connection with the smallest bandwidth acts as a bottleneck, Generally, the Internet backbone and connections between servers have the most bandwidth, so they rarely serve as bottlenecks. Instead, the most common Internet bottleneck is your connection to your ISP.

It also refers to a range of frequencies used to transmit a signal, This type of bandwidth is measured in hertz and is often referenced in signal processing applications. [26]

I.2.1.2 Noise And Distortion

Various sources of noise affect the media according to their type: interference, crosstalk phenomenon, environmental disturbances,…. The signals are therefore distorted and this can induce a decoding error, can the receiver confuse the amplitude of a "1" with that of a "0".

Interference, noise along with other causes of signal distortion such as inter symbol interference and inter modulation products constitute unwanted but ubiquitous aspects of any radio mobile radio system whether frequencies are reused or not. When two transmitters, located within the same geographical area for the purpose of achieving higher spectrum efficiency, are assigned identical carrier frequency as is the case of simulcast system or in two geographically distinct areas separated by a distance of cellular systems, co channel interference results. The desired and the interfering signals may travel to the receiver via the same or different paths; in the latter case the two signals fade independently with or without identical distributions. The impact of co-channel interference on the system performance is in the form of degradation in the signal to interference plus noise. The impact is either worsening of the symbol error or outage probability. [13]

I.2.1.3 Capacity

Capacity measures the amount of information carried per unit of time. It is limited and is specific to each type of media. Shannon's theorem expresses the maximum limit of the capacitance in bits per second. Cap_{max}, from a transmission medium. [13]

The signal-to-noise ratio is important in the transmission of digital data because it sets the upper bound on the achievable data rate. Shannon’s result is that the maximum channel capacity, in bits per second, obeys the equation

$Cap_{max=}$ W log_2 (1 + SNR)

signal-to-noise ratio (SNR, or S/N),10 which is the ratio of the power in a signal to the power contained in the noise that is present at a particular point in the transmission. Typically, this ratio is measured at a receiver, because it is at this point that an attempt is made to process the signal and recover the data. For convenience, this ratio is often reported in decibels : [13]

$$\mathrm{SNR_{dB}} = 10 \log_{10} \frac{\text{signal power}}{\text{noise power}}$$

This expresses the amount, in decibels, that the intended signal exceeds the noise level. A high SNR will mean a high-quality signal and a low number of required intermediate repeaters.

I.2.2 The types Of transmission supports

- **Conducted Or Guided Media** : Use a conductor such as a wire or a fiber optic cable to move the signal from sender to receiver**.**
- **Wireless Or Unguided Media**: Use radio waves of different frequencies and do not need a wire or cable conductor to transmit signals**.**

I.2.2.1 Guided Transmission Supports

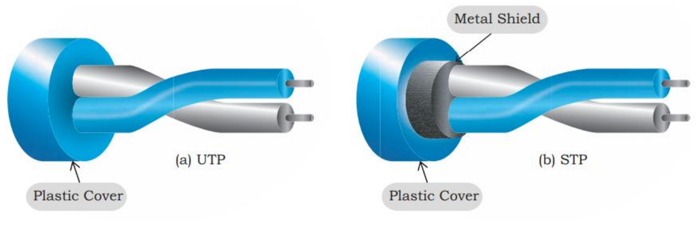
Guided media includes everything that 'guides' the transmission. That usually takes the form of some sort of a wire. Usually copper, but can also be an optical fibre.

Transmission capacity depends on the distance and on whether the medium is point-to-point or multipoint.

Examples: - twisted pair wires - coaxial cables - optical fiber[01]

1- Twisted Pair Wires : A transmission medium consisting of pairs of twisted copper wires arranged in a regular spiral pattern to minimize the electromagnetic interference between adjacent pairs Often used at customer facilities and also over distances to carry voice as well as data communications Low frequency transmission medium We can transmit 1 Mbps over short distances (less than 100m). (**Figure 1)**

Each of the twisted pairs act as a single communication link. The use of twisted configuration minimises the effect of electrical interference from similar pairs close by. Twisted pairs are less expensive and most commonly used in telephone lines and LANs. These cables are of two types: Unshielded twisted-pair (UTP) and Shielded twisted-pair (STP), as shown in **(Figure 1.2)**



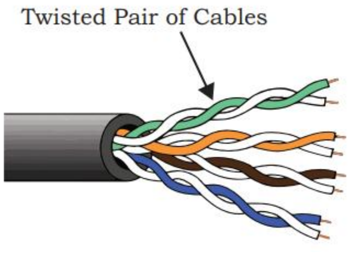


Figure 1.2: UTP Cable and STP Cable

Figure 1: Twisted pair of cables

- **Twisted Pair Advantages**

  - Inexpensive and readily available.

  -Flexible and light weight.

  -Easy to work with and install Twisted Pair .

- **Disadvantages**

  - Susceptibility to interference and noise.

  - Attenuation problem .

  - For analog, repeaters needed every 5-6km .

  - For digital, repeaters needed every 2-3km.

  - Relatively low bandwidth (3000Hz)

- **Applications**

  -They are used in telephone lines to provide voice and data channels.

  -Local area networks, such as 10 Base-T and 100 Base-T also use twisted-pair cables.

  -They are mainly used to transmit analog signals, but they can be used for digital signals.

2- Coaxial Cable (or Coax): In its simplest form, coaxial consists of a core made of solid copper surrounded by insulation, a braided metal shielding, and an outer cover. A transmission medium consisting of thickly insulated copper wire, which can transmit a large volume of data than twisted wire**.(Figure 2,2.1)** [01]

- **Coax Advantages**

- Higher bandwidth.

- 400 to 600Mhz.

- up to 10,800 voice conversations.

- Much less susceptible to interference than twisted pair.

- **Coax Disadvantages**

-High attenuation rate makes it expensive over long distance.

-Bulky.

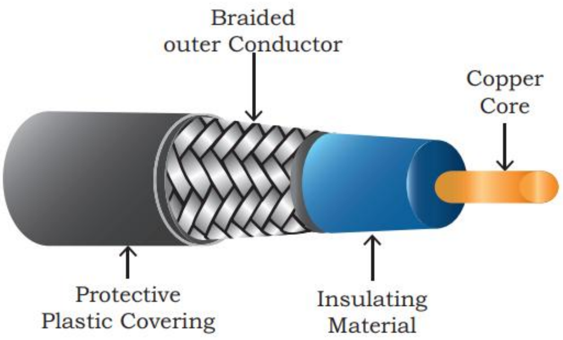


Figure 2.1: Coaxial Cable

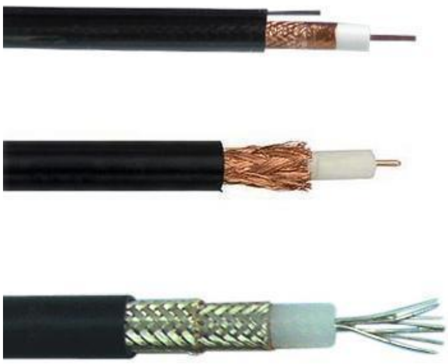


Figure 2: Coaxial Cable

- **Applications**
  -It is used in cable TV networks.
  -It is used in traditional Ethernet LANs.

3- Fiber Optic Cable

The optical fiber cable carries data as light, which travels inside a thin fiber of glass **(Figure 3).** Optic fiber uses refraction to direct the light through the media. A thin transparent strand of glass at the centre is covered with a layer of less dense glass called cladding. This whole arrangement is covered with an outer jacket made of PVC or Teflon. Such types of cables are usually used in backbone networks. These cables are of light weight and have higher bandwidth which means higher data transfer rate. Signals can travel longer distances and electromagnetic noise cannot affect the cable. However, optic fibers are expensive and unidirectional. Two cables are required for full duplex communication, relatively new transmission medium used by telephone companies in place of long-distance trunk lines. Also used by private companies in implementing local data communications networks. In most networks fiber-optic cable is used as the high-speed backbone, and twisted wire and coaxial cable are used to connect the backbone to individual devices. [13]

Optical fiber consists of a glass core, surrounded by a glass cladding with slightly lower refractive index, Require a light source with injection laser diode (ILD) or light emitting diodes (LED). **(Figure 3.1)**

- **Fiber Optic Advantages**
  - Greater capacity (bandwidth of up to 2 Gbps).
  - Smaller size and lighter weight.
  - Lower attenuation.
  - immunity to environmental interference.
  - highly secure due to tap difficulty and lack of signal radiation. [13]
- **Fiber Optic Disadvantages**
  - expensive over short distance.
  - requires highly skilled installers.
  - adding additional nodes is difficult.

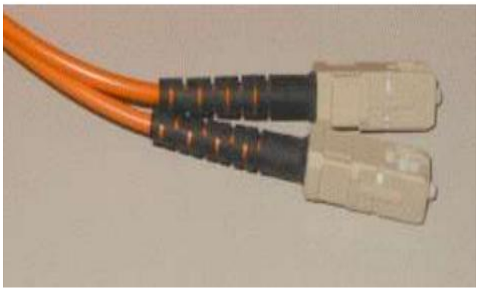


Figure 3: Fiber optic cable

- **Applications The Fiber Optic**

  - cable is often found in backbone networks because its bandwidth is cost effective.

  - Used in TV companies.

  -LAN such as 100 Base-FX Network. [13]

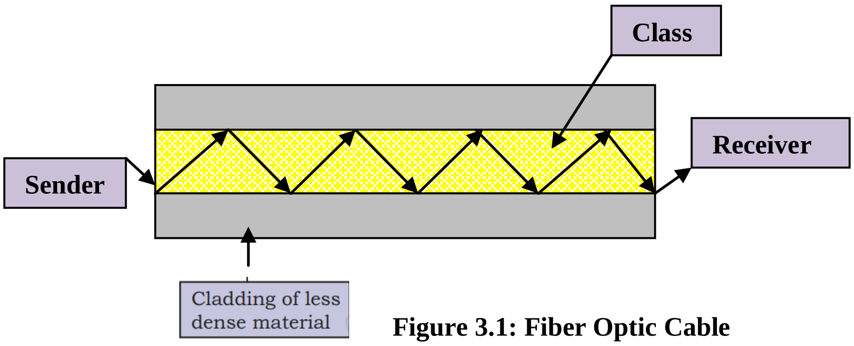


Figure 3.1: Fiber Optic Cable

I.2.2.2 Wireless (Unguided Media) Transmission

- transmission and reception are achieved by means of an antenna.
- directional ν transmitting antenna puts out focused beam.
- transmitter and receiver must be aligned omnidirectional.
- signal spreads out in all directions .
- can be received by many antennas

Examples : terrestrial microwave- satellite microwave…[16]

a-Microwaves

-Electromagnetic waves having frequency between 1 and 300 GHz are called as Micro waves.

-Micro waves are unidirectional.

-Microwave propagation is line of sight.

-Very high frequency Micro waves can not penetrate walls.

-The microwave band is relatively wide, almost 299 GHz[16]

b-Terrestrial Microwave

-Used for long-distance telephone service.

-Uses radio frequency spectrum, from 2 to 40 Ghz.

-Parabolic dish transmitter, mounted high.

-Used by common carriers as well as private networks.

-Requires unobstructed line of sight between source and receiver.

-Curvature of the earth requires stations (repeaters) ~30 miles apart.

c-Satellite Microwave

- a microwave relay station in space.

- can relay signals over long distances.

- geostationary satellites.

-remain above the equator at a height of 22,300 miles (geosynchronous orbit).

-travel around the earth in exactly the time the earth takes to rotate. [16]

- **Applications**
- They are used in Cellular phones.
- They are used in satellite networks.
- They are used in wireless LANs.

I.3 Layered architectures

Layered architecture patterns are n-tiered patterns where the components are organized in horizontal layers. This is the traditional method for designing most software and is meant to be self-independent. This means that all the components are interconnected but do not depend on each other. [25]

Architecture is kind of an overloaded term, so we should probably dig deeper into what the term really means in the context of layers. The main idea behind Layered Architecture is a separation of concerns – as we said already, we want to avoid mixing domain or database code with the UI stuff, etc. The actual idea of separating a project into layers suggests that this separation of concerns should be achieved by source code organization. This means that apart from some guidance to what concerns we should separate, the Layered Architecture tells us nothing else about the design and implementation of the project. This implies that we should complement it with some other architectural processes, such as some upfront design, daily design sessions, or even full-blown Domain-Driven Design. Whichever option we choose doesn't matter, at least for the sake of layering, but we need to remember: Layered Architecture gives us nothing apart from a guideline on how to organize the source code. [25]

I.3.1 Definition

A communication architecture is an abstract representation of the flow of information and concepts used within any network. An architectural model is characterized by the number of layers that constitute it. Layering considers a system as logically composed of a set of n ordered subsystems. Adjacent subsystems communicate through their common interface. A layer is a component of the architecture which performs a well-defined function and contributes to the proper functioning of the network. [25]

The basic elements of layered architecture are services, protocols, and interfaces.

a-Service: It is a set of actions that a layer provides to the higher layer.

b-Protocol: It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.

c-Interface: It is a way through which the message is transferred from one layer to another layer.

I.3.2 Principles

Layer (i) requests one or more services from layer (i-1) using primitives which are divided into 4 types: request, indication, response and confirmation. The stages of communication between two layers are as follows:

- Layer (i + 1) sends SDU (i) data units to layer (i).

- Layer (i) adds to the SDUs (i) protocol control information called PCI (i) or 'Protocol Control Information". This step is called encapsulation.

- The set [PCI (i); SDU (i)] therefore constitutes PDU (i) which is also SDU (i-1) and it will be provided at layer (i-1).

Relationship between the Protocol Data Unit (PDU) and Service Data Unit (SDU)

To understand the relationship between this data, consider the following diagram of data being passed down from the upper layers to the lower layers during transmission of data from a sender to a receiver. **(figure 4)**

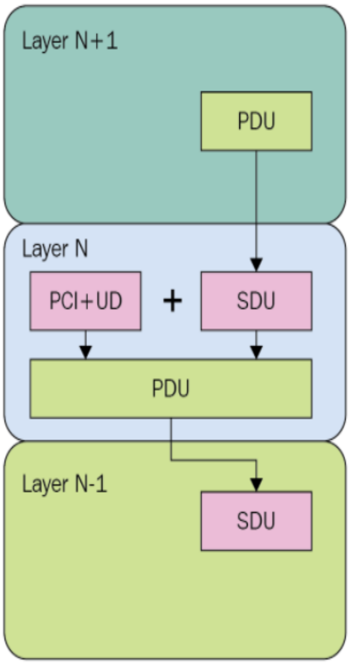


Figure 4: Layered architecture

Data is passed down from a higher Layer N+1 to the current Layer N and becomes an SDU at the current layer. Layer N then adds its bits of PCI and UD (if present), and combines all of this data into a new PDU, which is to be passed down again to the lower Layer N-1 to become a new SDU at that lower layer. This process is termed encapsulation, as each SDU is encapsulated . [25]

I.4 THE OSI MODEL

I.4.1 The History Of OSI

In the late 1970s, two projects began independently, with the same goal: to define a unifying standard for the architecture of networking systems. One was administered by the International Organization for Standardization (ISO), while the other was undertaken by the International Telegraph and Telephone Consultative Committee, or CCITT (the abbreviation is from the French version of the name). These two international standards bodies each developed a document that defined similar networking models. [12]

In 1983, these two documents were merged together to form a standard called The Basic Reference Model for Open Systems Interconnection. That's a mouthful, so the standard is usually referred to as the Open Systems Interconnection Reference Model, the OSI Reference Model, or even just the OSI Model. It was published in 1984 by both the ISO, as standard ISO 7498, and the renamed CCITT (now called the Telecommunications Standardization Sector of the International Telecommunication Union or ITU-T) as standard X.200. (Incidentally, isn't the new name for the CCITT much catchier than the old one? Just rolls off the old tongue, doesn't it.

However, things didn't quite work out as planned. The rise in popularity of the Internet and its TCP/IP protocols met the OSI suite head on, and in a nutshell, TCP/IP won. Some of the OSI protocols were implemented, but as a whole, the OSI protocols lost out to TCP/IP when the Internet started to grow.

The OSI model itself, however, found a home as a device for explaining the operation of not just the OSI protocols, but networking in general terms. It was used widely as an educational tool—much as I use it myself in this Guide—and also to help describe interactions between the components of other protocol suites and even hardware devices. While most technologies were not designed specifically to meet the dictates of the OSI model, many are described in terms of how they fit into its layers. This includes networking protocols, software applications, and even different types of hardware devices, such as switches and routers. The model is also useful to those who develop software and hardware products, by helping to make clear the roles performed by each of the components in a networking system. [12]

1.4.2 Definition The OSI

The Open Systems Interconnection (OSI) Reference Model is a conceptual framework that describes functions of the networking or telecommunication system independently from the underlying technology infrastructure. It divides data communication into seven abstraction layers and standardizes protocols into appropriate groups of networking functionality to ensure interoperability within the communication system regardless of the technology type, vendor, and model.

The OSI model was originally developed to facilitate interoperability between vendors and to define clear standards for network communication. However, the older TCP/IP model remains the ubiquitous reference framework for Internet communications today. [12]

I.4.3 Functions Of The OSI Layers

There are the seven OSI layers, Each layer has different functions.(**Figure 5)**

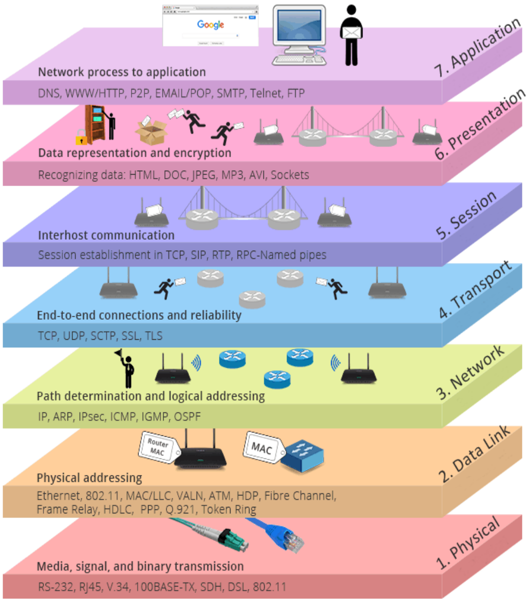

Google
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
2. Data Link
Router MAC
MAC
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

Figure 5 : OSI Layers

1- Physical Layer

Starting at the bottom layer of the OSI Model is the Physical Layer. The Physical Layer specifies the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, FR, RS232,MPLS and ATM are protocols with physical layer components. [11]

It addresses the physical characteristics of the network. This includes the types of cables used to connect everything together. The types of connectors used, how long the cables can be, and so on. For example, the Ethernet standard for 100BaseT cable specifies the electrical characteristics of the twisted-pair cables, the size and shape of the connectors, the maximum length of the cables.

The Physical Layer also specifies the electrical characteristics of the signals used to transmit data over cables from one network node to another. There is not any particular meaning to the signals other than what the binary characteristics of what a ‘0’ or a ‘1’ looks like. The OSI model upper layers will assign meanings to the bits transmitted at the Physical Layer. [12]

2- Data Link Layer

The Data Link Layer is where we start to give meaning or intelligence to what we are going to send over the network. The protocols on the Data Link Layer resolve such matters as the size of a packet to send, a way to address each packet to be delivered so that it gets to the intended receiver, and a way to insure that no more than one node tries to send a packet to the receiver at the same time.

The Data Link Layer provides for error detection and correction to make sure that the data sent is the same as the data that was received. If an error is not correctable, the data-link standard needs to specify how the node is to be told of the error so that it can retransmit the data that was in error.

Each node (Network Interface Card - NIC)has an address at the Data Link layer called the Media Access Control address commonly referred to as the MAC Address. This is the actual hardware address, which is assigned by the manufacturer of the device. You can find the MAC Address of your device by opening a command window and running the ‘ipconfig /all’ command. [12]

3- Network Layer

The third layer of the OSI model organizes and transmits data between multiple networks.

The network layer is responsible for routing the data via the best physical path based on a range of factors including network characteristics, best available path, traffic controls, congestion of data packets, and priority of service, among others. The network layer implements logical addressing for data packets to distinguish between the source and destination networks.

Other functions include encapsulation and fragmentation, congestion controls, and error handling. The outgoing data is divided into packets and incoming data is reassembled into information that is consumable at a higher application level. Network layer hardware includes routes, bridge routers, 3-layer switches, and protocols such as Internet (IPv4) Protocol version 4 and Internet Protocol version 6 (IPv6).

4- Transport Layer

The fourth layer of the OSI model ensures complete and reliable delivery of data packets.

- The transport layer provides mechanisms such as error control, flow control, and congestion control to keep track of the data packets, check for errors and duplication, and resend the information that fails delivery. It involves the service-point addressing function to ensure that the packet is sent in response to a specific process (via a port address).
- Packet Segmentation and reassembly ensure that the data is divided and sequentially sent to the destination where it is rechecked for integrity and accuracy based on the receiving sequence.

Common protocols include the Transmission Control Protocol (TCP) for connection-oriented data transmission and User Datagram Protocol (UDP) for connectionless data transmission. [12]

5- Session Layer

As the first of three layers that deal with the software level, the session layer manages sessions between servers to coordinate communication. Session refers to any interactive data exchange between two entities within a network. Common examples include HTTPS sessions that allow Internet users to visit and browse websites for a specific time period. The Session Layer is responsible for a range of functions including opening, closing, and re-establishing session activities, authentication and authorization of communication between specific apps and servers, identifying full-duplex or half-duplex operations, and synchronizing data streams.

Common Session Layer protocols include:

- Remote procedure call protocol (RPC)
- Point-to-Point Tunneling Protocol (PPTP)
- Session Control Protocol (SCP)
- Session Description Protocol (SDP), as described here

6-Presentation Layer

The sixth layer of the OSI model converts data formats between applications and the networks. Responsibilities of the presentation layer include:

- Data conversion
- Character code translation
- Data compression
- Encryption and decryption

The presentation layer, also called the syntax layer, maps the semantics and syntax of the data such that the received information is consumable for every distinct network entity. For example, the data we transfer from our encryption-based communication app is formatted and encrypted at this layer before it is sent across the network. [12]

At the receiving end, the data is decrypted and formatted into text or media information as originally intended. The presentation layer also serializes complex information into transportable formats. The data streams are then deserialized and reassembled into original object format at the destination.

7-Application Layer

The application layer concerns the networking processes at the application level. This layer interacts directly with end-users to provide support for email, network data sharing, file transfers, and directory services, among other distributed information services. The upper most layer of the OSI model identifies networking entities to facilitate networking requests by end-user requests, determines resource availability, synchronizes communication, and manages application-specific networking requirements. The application layer also identifies constraints at the application level such as those associated with authentication, privacy, quality of service, networking devices, and data syntax.

Common application layer protocols include:

- File Transfer Protocol (FTP).
- Simple Mail Transfer Protocol (SMTP).
- Domain Name System (DNS). [12]

I.5 The TCP/IP And UDP Models

I.5.1 The TCP/IP Model

I.5.1.1 The History Of TCP/IP

The Defense Advanced Research Projects Agency (DARPA), the research branch of the U.S. Department of Defense (DOD), created the TCP/IP model in the 1970s for use in ARPANET, a wide area network (WAN) that preceded the internet. TCP/IP was originally designed for the UnixOS, and it has been built into all of the OSes that came after it.

The TCP/IP model and its related protocols are now maintained by the Internet Engineering Task Force (IETF). [11]

I.5.1.2 Definition

TCP/IP, or Transmission Control Protocol/Internet Protocol, is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP can also be used as a communications protocol in a private computer network (an intranet or extranet).

The entire IP suite - a set of rules and procedures - is commonly referred to as TCP/IP. TCP and IP are the two main protocols, though others are included in the suite .The TCP/IP protocol suite functions as an abstraction layer between internet applications and the routing/switching fabric.

TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management and is designed to make networks reliable with the ability to recover automatically from the failure of any device on the network. [11]

The two main protocols in the IP suite serve specific functions. TCP defines how applications can create channels of communication across a network. It also manages how a message is assembled into smaller packets before they are then transmitted over the internet and reassembled in the right order at the destination address.

IP defines how to address and route each packet to make sure it reaches the right destination. Each gateway computer on the network checks this IP address to determine where to forward the message.

A subnet mask is what tells a computer, or other network device, what portion of the IP address is used to represent the network and what part is used to represent hosts, or other computers, on the network.

Network address translation (NAT) is the virtualization of IP addresses. NAT helps improve security and decrease the number of IP addresses an organization needs.

-Common TCP/IP protocols include the following: [11]

- **HTTP (Hypertext Transfer Protocol)**, which handles the communication between a web server and a web browser;
- **HTTPS (HTTP Secure)**, which handles secure communication between a web server and a web browser; and
- **FTP (File Transfer Protocol)**, which handles transmission of files between computers.

I.5.1.3 The TCP/IP Layers

TCP/IP functionality is divided into four layers, each of which includes specific protocols: Figure - TCP/IP model**[27]**

1-The Application Layer: provides applications with standardized data exchange. Its protocols include HTTP, FTP, Post Office Protocol 3 (POP3), Simple Mail Transfer Protocol (SMTP) and Simple Network Management Protocol (SNMP). At the application layer, the payload is the actual application data.

2-The Transport Layer: is responsible for maintaining end-to-end communications across the network. TCP handles communications between host s and provides flow control, multiplexing and reliability. The transport protocols include TCP and User Datagram Protocol (UDP), which is sometimes used instead of TCP for special purposes. **[27]**

3-The network layer: also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are IP and Internet Control Message Protocol (ICMP), which is used for error reporting.

4-The Physical Layer: also known as the network interface layer *or* data link layer, consists of protocols that operate only on a link -- the network component that interconnects nodes or hosts in the network. The protocols in this lowest layer include Ethernet for local area networks (LANs) and Address Resolution Protocol (ARP). **[27]**

I.5.1.4 The Similarities Between OSI And TCP/IP Model

The functions performed in each model are also similar because each uses a network layer and transport layer to operate. The TCP/IP and OSI models are each mostly used to transmit data packets. Although they will do so by different means and by different paths, they will still reach their destinations.

-They are both logical models: Both the models are the logical models and having similar architectures as both the models are constructed with the layers.

-They define networking standards: Both the layers have defined standards, and they also provide the framework used for implementing the standards and devices.

-They divide the network communication process in layers: Both models have simplified the troubleshooting process by breaking the complex function into simpler components. [27]

-They provide frameworks for creating and implementing networking standards and devices.

-They enable one manufacturer to make devices and network components that can coexist and work with the devices and components made by other manufacturers.

I.5.1.5 The Differences Between OSI And TCP/IP - figure 6

The differences between the TCP/IP model and the OSI model include the following:

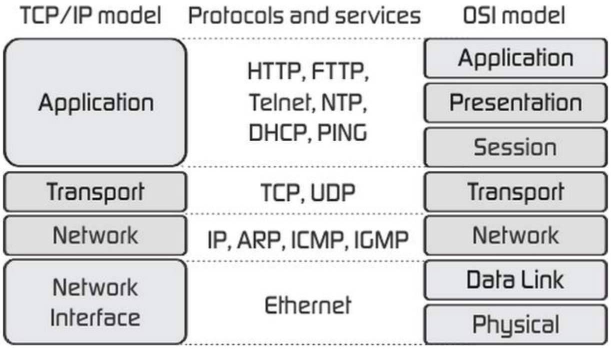


figure 6: TCP/IP vs OSI

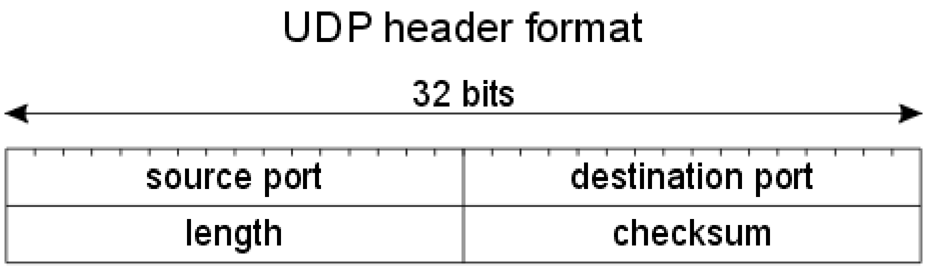
- TCP/IP uses just one layer (application) to define the functionalities of the upper layers, while OSI uses three layers (application, presentation and session).
- TCP/IP uses one layer (link) to define the functionalities of the bottom layers, while OSI uses two layers (physical and data link).
- TCP/IP uses the internet layer to define the routing standards and protocols, while OSI uses the network layer.
- The TCP/IP header size is 20 bytes, while the OSI header is 5 bytes.
- TCP/IP is a protocol-oriented standard, whereas OSI is a generic model based on the functionalities of each layer.
- TCP/IP follows a horizontal approach, while OSI follows a vertical approach.
- In TCP/IP, the protocols were developed first, and then the model was developed. In OSI, the model was developed first, and then the protocols in each layer were developed.
- TCP/IP helps establish a connection between different types of computers, whereas OSI helps standardize routers, switches, motherboards and other hardware. [27]

I.6 The UDP Model

In addition to TCP, there is one other transport-level protocol that is in common use as part of the TCP/IP protocol suite: the User Datagram Protocol (UDP). [29]

UDP does not guarantee delivery, preservation of sequence, or protection against duplication. UDP enables a procedure to send messages to other procedures with a minimum of protocol mechanism. Some transaction-oriented applications make use of UDP; one example is SNMP (Simple Network Management Protocol), the standard network management protocol for TCP/IP networks. Because it is connectionless, UDP has very little to do. Essentially, it adds a port addressing capability to IP.

This is best seen by examining the UDP header, UDP also includes a checksum to verify that no error occurs in the data; the use of the checksum is optional. [29]



UDP header format

32 bits

source port	destination port
length	checksum

I.6.1 UDP header

Destination port number, Identifies the receiver's port and is required, if the client is the destination host an ephemeral port number. if the destination host is the server a well-known port number ,Length , Specifies the length in bytes of the entire datagram: header and data , The minimum length is 8 bytes = the length of the header.

I.7 TYPES OF NETWORK: LAN, MAN AND WAN

I.7.1 The Local Area Network (LAN)

Is a communication network that interconnects a variety of data communicating devices within a small geographic area and broadcasts data at high data transfer rates with very low error rates , its use has become widespread in commercial and academic environments Data Communications and Computer Networks.

Whether you are in a company, or in an administrative office, you can only interconnect equipment through a local network. This term is widely used to designate the interconnection in a building or more generally in an area of a few kilo meters in diameter. Often known by the acronym LAN (Local Area Network), local networks have become essential to any business. Indeed, this network makes it possible to interconnect workstations, printers, storage disks and video equipment. In addition, the way to set it up is a freedom of the one who wants to set it up. Nevertheless, organizations have developed standards to have more or less uniform LAN architectures. [27]

I.7.1.1 Primary Function Of Local Area Networks

To provide access to hardware and software resources that will allow users to perform one or more of the following activities: – File serving • A large storage disk drive acts as a central storage repository – Print serving • Providing the authorization to access a particular printer, accept and queue print jobs, and providing a user access to the print queue to perform administrative duties – Video transfers • High-speed LANs are capable of supporting video image and live video transfers Data Communications and Computer Networks.

LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can’t be accessed outside.

LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps. [27]

I.7.1.2 LAN Topologies (Networking)

I.7.1.2.1 Topology

is the physical and logical arrangement of a network. The physical arrangement of the network refers to how the workstations, servers, and other equipment are joined together with cables and connectors. The logical arrangement of a network refers to how the workstations, servers, and other equipment relate to each other in terms of traffic flow. There are three primary LAN topologies: linear bus, ring, and star. Another network topology is hierarchical in nature, which may incorporate elements of the bus, ring, and star. The appropriate physical and logical topology for a LAN is determined by reliability and cost objectives as well as by the connectivity requirements of users. [27]

I.7.1.2.2 Physical Network Topology

is the placement of the various components of a network and the different connectors usually represent the physical network cables, and the nodes represents usually the physical network devices (like switches): which may incorporate elements of the bus, ring, and star. [12]

1- Bus Topology

In a linear bus topology stations are arranged along a single length of cable, which can be extended at either end or at both ends to accommodate more nodes (**Figure 7**). The network consists of coaxial cable, such as the RG-58 A/U cable used with 10Base2 Ethernet LANs. The nodes are attached to the cable with a BNC (Bayonet Nut Connector) T-connector , the stem of which attaches to the network interface card (NIC). A BNC barrel connector attaches cable segments and a BNC terminator connector caps the cable ends. Of course, twisted pair wiring is most often used for Ethernet LANs, in which case RJ45 connectors provide the connections between devices. [12]

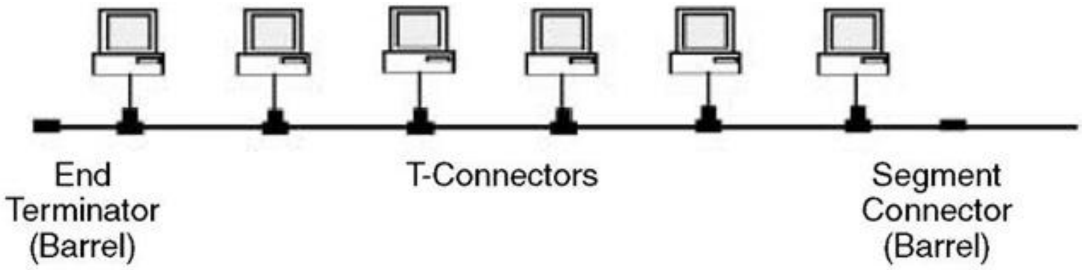


Figure 7: Bus Topology

A linear bus network can be further extended. For example, a tree topology is actually a complex linear bus in which the cable branches at either or both ends, but offers only one transmission path between any two stations.

2- Ring Topology

In a ring topology, nodes are arranged along the transmission path so data passes through each successive station before returning to its point of origin. As its name implies, the ring topology consists of nodes that form a closed circle. [12] **(Figure 8)**

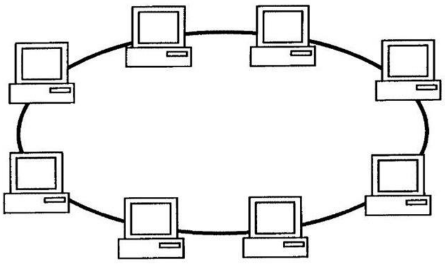


Figure 8: Ring Topology

3- Star Topology

The star topology is the most widely implemented network design in use today, but it is not without its shortcomings. Because all devices connect to a centralized hub, this creates a single point of failure for the network. If the hub fails, any device connected to it will not be able to access the network. Because of the number of cables required and the need for network devices, the cost of a star network is often higher than other topologies.[12] **(Figure 9)**

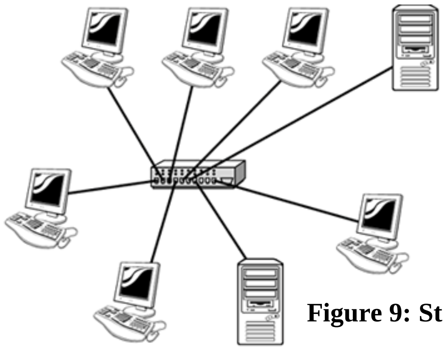


Figure 9: Star Topology

I.7.1.2.3 Advantages And Disadvantages Of Local Area Networks:

1- Advantages:

Ability to share hardware and software resources Individual workstation might survive network failure Component and system evolution are possible Support for heterogeneous forms of hardware and software – Access to other LANs and WANs– Private ownership – Secure transfers at high speeds with low error rates Data Communications and Computer Networks. [12]

2- Disadvantages :

Equipment and support can be costly Level of maintenance continues to grow Private ownership? Some types of hardware may not interoperate Just because a LAN can support two different kinds of packages does not mean their data can interchange easily – LAN is only as strong as its weakest link, and there are many links Data Communications and Computer Networks.

I.7.2 The Metropolitan Area Network (MAN)

MAN or Metropolitan area Network covers a larger area than that of a LAN and smaller area as compared to WAN. It connects two or more computers that are apart but resides in the same or different cities. It covers a large geographical area and may serve as an ISP (Internet Service Provider). MAN is designed for customers who need a high-speed connectivity. Speeds of MAN ranges in terms of Mbps. It's hard to design and maintain a Metropolitan Area Network.

Is a bigger version of LAN that uses similar technology as LAN. It spans over a larger geographical area such as a town or an entire city.

It can be connected using an optical fiber cable as a communication medium. Two or more LAN's can also be connected using routers to create a MAN. When this type of network is created for a specific campus, then it is termed as CAN(Campus Area Network).

A MAN can be either a public or privately owned network. Generally, a telephone exchange line is most commonly used as a communication medium in MAN. The protocols that are used in MAN are RS-232, Frame Relay, ISDN, etc.

MAN can be used for connecting the various offices of the same organization, spread over the whole city. It can be used for communication in various government departments. [28]

I.7.3 The Wide Area Network (WAN)

WAN or Wide Area Network is a computer network that extends over a large geographical area, although it might be confined within the bounds of a state or country. A WAN could be a connection of LAN connecting to other LAN's via telephone lines and radio waves and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive.

There are two types of WAN: Switched WAN and Point-to-Point WAN. WAN is difficult to design and maintain. Similar to a MAN, the fault tolerance of a WAN is less and there is more congestion in the network. A Communication medium used for WAN is PSTN or Satellite Link. Due to long distance transmission, the noise and error tend to be more in WAN.

WAN's data rate is slow about a 10th LAN's speed, since it involves increased distance and increased number of servers and terminals etc. Speeds of WAN ranges from few kilobits per second (Kbps) to megabits per second (Mbps). Propagation delay is one of the biggest problems faced here. Devices used for transmission of data through WAN are: Optic wires, Microwaves and Satellites. Example of a Switched WAN is the asynchronous transfer mode (ATM) network and Point-to-Point WAN is dial-up line that connects a home computer to the Internet. [28]

I.8 Address MAC

MAC address is the physical address, which uniquely identifies each device on a given network. To make communication between two networked devices, we need two addresses: IP address and MAC address. It is assigned to the NIC (Network Interface card) of each device that can be connected to the internet, It consists of 48 bits, the first 24 of which designate the manufacturer number and the last 24 are the serial numbers of the network card

It stands for Media Access Control, and also known as Physical address, hardware address, or BIA (Burned In Address).(Figure 10) [28]

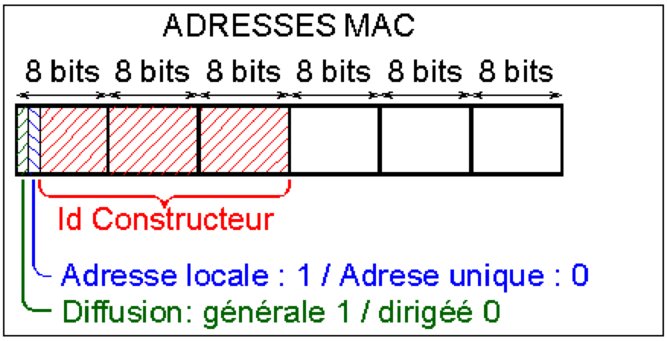

ADRESSES MAC
8 bits 8 bits 8 bits 8 bits 8 bits 8 bits
Id Constructeur
Adresse locale : 1 / Adrese unique : 0
Diffusion: générale 1 / dirigéé 0

Figure 10: Format of a MAC address

It is globally unique; it means two devices cannot have the same MAC address. It is represented in a hexadecimal format on each device, such as 00:0a:95:9d:67:16.

MAC Addresses are unique 48-bits hardware number of a computer, which is embedded into network card (known as Network Interface Card) during the time of manufacturing. MAC Address is also known as Physical Address of a network device. In IEEE 802 standard, Data Link Layer is divided into two sublayers .

- Logical Link Control(LLC) Sublayer.
- Media Access Control(MAC) Sublayer. [28]

I.8.1 Characteristic Of MAC address

Here, are some important characteristic of MAC address:

- TCP/IP networks can use MAC addresses in the communication.
- It helps you to Identify a specific NIC in a computer on a network.
- Network devices cannot efficiently route traffic using MAC addresses.
- Not provide information about physical or logical network configuration.

I.8.2 Benefits Of Using MAC Address:

- It provides a secure way to find senders or receivers in the network.
- MAC address helps you to prevent unwanted network access.
- MAC address is a unique number; hence it can be used to track the device.
- Wi-Fi networks at the airport use the MAC address of a specific device to identify it. [28]

I.9 Network Topologies

Network topology is the arrangement of the different network elements of a communication network, usually represented with a graph.

Network topology is an application of graph theory in which different network devices are mode led as nodes and the connections between the devices are mode led as links or lines between the nodes, There are usually two different types of network topologies: **[16]**

- **Physical network topology**: is the placement of the various components of a network and the different connectors usually represent the physical network cables, and the nodes represents usually the physical network devices (like switches).
- **Logical Network Topology**: illustrates, at a higher level, how data flows within a network.

I.10 Support Access Technique

The access technique is used to share the bandwidth of the medium and to order and harmonize the communication between the devices. There are two types: the random technique and the deterministic technique.

I.10.1 Aloha Method

Aloha, also called the Aloha method, refers to a simple communications scheme in which each source (transmitter) in a network sends data whenever there is a frame to send. If the frame successfully reaches the destination (receiver), the next frame is sent. If the frame fails to be received at the destination, it is sent again. This protocol was originally developed at the University of Hawaii for use with satellite communication systems in the Pacific.

In a wireless broadcast system or a half-duplex two-way link, Aloha works perfectly. But as networks become more complex, for example in an Ethernet system involving multiple sources and destinations that share a common data path, trouble occurs because data frames collide (conflict). The heavier the communications volume, the worse the collision problems become. The result is degradation of system efficiency, because when two frames collide, the data contained in both frames is lost.

To minimize the number of collisions, thereby optimizing network efficiency and increasing the number of subscribers that can use a given network, a scheme called slotted Aloha was developed. This system employs signals called beacons that are sent at precise intervals and tell each source when the channel is clear to send a frame. [16]

I.10.2 The CSMA/CD

Carrier Sense Multiple Access with Collision Detection (CSMA/CD): is a network protocol for carrier transmission that operates in the Medium Access Control (MAC) layer. It senses or listens whether the shared channel for transmission is busy or not, and defers transmissions until the channel is free. The collision detection technology detects collisions by sensing transmissions from other stations. On detection of a collision, the station stops transmitting, sends a jam signal, and then waits for a random time interval before retransmission. [16]

I.11 ETHERNET AND IEEE 802.3 STANDARD

Ethernet was developed by Xerox Corporation’s Palo Alto Research Center (PARC) in the 1970s,Ethernet was the technological basis for the IEEE 802.3 specification, which was initially released in 1980. Shortly thereafter, Digital Equipment Corporation, Intel Corporation, and Xerox Corporation jointly developed and released an Ethernet specification (Version 2.0) that is substantially compatible with IEEE 802.3. Together, Ethernet and IEEE 802.3 currently maintain the greatest market share of any local-area network (LAN) protocol. Today, the term Ethernet is often used to refer to all carrier sense multiple access/collision detection (CSMA/CD) LANs that generally conform to Ethernet specifications, including IEEE 802.3.When it was developed, Ethernet was designed to fill the middle ground between long-distance, low-speed networks and specialized, computer-room networks carrying data at high speeds for very limited distances. Ethernet is well suited to applications where a local communication medium must carry sporadic, occasionally heavy traffic at high peak data rates. [08]

I.12 THE TOKEN RING: THE IEEE 802.5 STANDARD

Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition. A token is a special frame of 3 bytes that circulates along the ring of stations. A station can send data frames only if it holds a token. The tokens are released on successful receipt of the data frame. [02]

Although IBM is usually considered to be the founder of the Token-Ring LAN standard, it was actually patented by Dr. Olaf Solderblum in Sweden in 1967. IBM obtained the technology from Dr. Solderblum and, with the assistance of Texas Instruments, developed the chipset technology and guidelines.

IBM released the technology to the IEEE, whose 802.5 subcommittee developed and released the 4Mbps Token-Ring standard in 1985. The IEEE 802.5 specification defines the MAC sub layer and the Physical layer specification, using the 802.2 specification at the LLC layer for protocol identification. [02]

I.13 WLAN AND 802.11 STANDARDS

WLAN or Wireless LAN refers to a wireless local area network. The constraints in the development of such a technology are to find free frequencies and also to take into account the different disadvantages of radio signals. The 802.11 standards were developed by the IEEE for wireless (Wi-Fi) networks; it uses the CSMA/CA or CSMA with Collision Avoidance access technique to avoid collisions. It achieves theoretical speeds of 54 Mbps, or even 600 Mbps for 802.11n. [08]

I.13.1 CSMA / CA Or (CSMA)

CSMA stands for Carrier Sense Multiple Access with Collision Avoidance. It means that it is a network protocol that uses to avoid a collision rather than allowing it to occur, and it does not deal with the recovery of packets after a collision. It is similar to the CSMA CD protocol that operates in the media access control layer. In CSMA CA, whenever a station sends a data frame to a channel, it checks whether it is in use. If the shared channel is busy, the station waits until the channel enters idle mode. Hence, we can say that it reduces the chances of collisions and makes better use of the medium to send data packets more efficiently. [08]

I.14 The IP Network

The IP address is, in turn, one of the cornerstones of the Internet Protocol. Information is transmitted over the network in discrete chunks called packets; each packet is mostly made up of whatever data the sender is trying to communicate, but also includes a header, consisting of metadata about that packet.

The daily of most of us is dominated by IP or Internet Protocol, this evocative name which means Internet Protocol: which says "Internet" says IP. This protocol has had incomparable success and its implementation has allowed the technology to develop. [01] We often talk about an all-IP NGN network, 4G and its “All over IP”, telephony over IP or VoIP, IP-TV, IP cameras and many others. This layer 3 protocol, therefore at the network level, has been the heart of the Internet since it is used to identify each of the web servers that users have requested. It was defined in RFC 791. [01]

I.14.1 Address Format

here are two versions of IP addresses: IPv4 and IPv6, and they have different formats, the major difference between them being that it's possible to create vastly more unique IPv6 addresses (2128) than IPv4 addresses (232).

That's thanks to the format they use. IPv4 addresses are written in four parts separated by dots like this:45.48.241.198

Each part written in conventional Base 10 numerals represents an eight-bit binary number from 0 to 255,Each of these four numbers separated by dots is written in standard decimal notation. But computers fundamentally deal with numbers in binary (using just zeroes and ones, and each of the numbers in an IPv4 address represents an 8-bit binary number, which means that none of them can be higher than 255 (111111 in binary).

It's quite likely that you've seen IP addresses like that one before since they've been around since 1983. The newer version of the protocol, IPv6, is slowly displacing IPv4, and its addressing looks like this:2620:cc:8000:1c82:544c:cc2e:f2fa:5a9b. [01]

Note that instead of four numbers, there are eight, and they're separated by colons rather than commas. And yes, they are all numbers. There are letters in there because IPv6 addresses are written in hexadecimal (Base 16) notation, which means 16 different symbols are required to uniquely represent Base 10 numbers 1-16. The ones used are numerals 0-9 plus letters A-F. Each of these numbers represents a 16-bit binary number, and the difference between that the 8-bit components of an IPv4 address is the main reason for IPv6's existence. [01]

I.14.2 IP Class

Now that we've looked at what an IP address is, the next thing to consider is IP classes, as these are essential for understanding how subnets work.

Say you're trying to find one particular IP address, or organize IP addresses on your network. This would be an impossible task without some kind of system. IP addresses are divided into numerical sections to help you find what you're looking for more quickly. These sections are called classes. IP addresses are divided into three classes: A, B, and C.

- **Class A:** IP addresses are those between 0.0.0.0 and 127.255.255.255.
- **Class B:** IP addresses are those between 128.0.0.0 and 191.255.255.255.
- **Class C:** IP addresses are those between 192.0.0.0 and 223.255.255.255. [01]

I.14.3 Subnetting And Subnet Masks

Every device has an IP address with two pieces: the client or host address and the server or network address. IP addresses are either configured by a DHCP server or manually configured (static IP addresses). The subnet mask splits the IP address into the host and network addresses, thereby defining which part of the IP address belongs to the device and which part belongs to the network.

The device called a gateway or default gateway connects local devices to other networks. This means that when a local device wants to send information to a device at an IP address on another network, it first sends its packets to the gateway, which then forwards the data on to its destination outside of the local network.

I.14.4 The IP Datagram

Datagram is a combination of the words data and telegram. Therefore, it is a message containing data that is sent from location to another. A datagram is similar to a packet, but does not require confirmation that it has been received. This makes datagrams ideal for streaming services, where the constant flow of data is more important than 100% accuracy.

The IP datagram is the one that transports data at the IP level, with the source and destination addresses, It includes a few header and data bytes, its maximum size is 64 KB. IP does not guarantee data reliability, it just has the role of routing the data to the destination. Arrived at the router, the datagram is routed to the optimal route that the router found by looking in the destination address field. [01]

I.15 ADDRESS RESOLUTION PROTOCOL (ARP)

Most of the computer programs/applications use logical address (IP address) to send/receive messages, however the actual communication happens over the physical address (MAC address) i.e from layer 2 of OSI model. So our mission is to get the destination MAC address which helps in communicating with other devices. This is where ARP comes into the picture, its functionality is to translate IP address to physical address.

The important terms associated with ARP are : [07]

ARP Cache: After resolving MAC address, the ARP sends it to the source where it stores in a table for future reference. The subsequent communications can use the MAC address from the table ARP Cache Timeout: It indicates the time for which the MAC address in the ARP cache can reside ARP request: This is nothing but broadcasting a packet over the network to validate whether we came across destination MAC address or not.

-The physical address of the sender.

-The IP address of the sender.

-The physical address of the receiver is FF:FF:FF:FF:FF:FF or 1's.

-The IP address of the receiver

-ARP response-reply: It is the MAC address response that the source receives from the destination which aids in further communication of the data. [07]

I.16 ROUTING

To reach another network different from our own local network, we need equipment that can guide you to the desired path. The router is designed primarily for this. It is a node which has the specificity of connecting with several different networks because it has more than one network card and therefore has an address. The router is a level 3 device that works with IP addresses. With each packet received, it looks for the destination address and looks in its routing table, then routes the packet to the appropriate path. [27]

I.16.1 Types Of Routing

To perform this function, the router uses certain routing algorithms and protocols. Routing can be classified into three categories: Static Routing-Default Routing- Dynamic Routing . **(Figure 11)** [27]

I.16.1.1 Default Routing

- Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
- Default Routing is used when networks deal with the single exit point.
- It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
- When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table. [27]

I.16.1.2 Static Routing

-Static Routing is also known as Non adaptive Routing.
- It is a technique in which the administrator manually adds the routes in a routing table.
-A Router can send the packets for the destination along the route defined by the administrator.

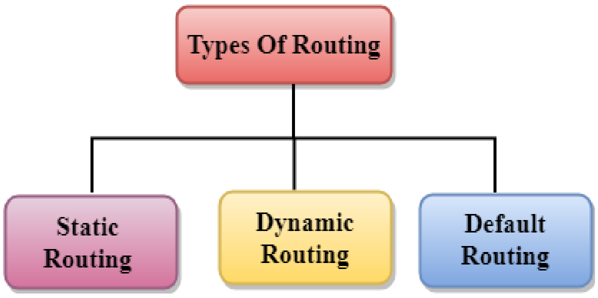


Figure 11: Types of Routing

-In this technique, routing decisions are not made based on the condition or topology of the networks.

➢ **Advantages Of Static Routing**

Following are the advantages of Static Routing:

- No Overhead: It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
- Bandwidth: It has not bandwidth usage between the routers.
- Security: It provides security as the system administrator is allowed only to have control over the routing to a particular network. [27]

➢ **Disadvantages of Static Routing:**

Following are the disadvantages of Static Routing:

- For a large network, it becomes a very difficult task to add each route manually to the routing table.
- The system administrator should have a good knowledge of a topology as he has to add each route manually.

I.16.1.3 Dynamic Routing

- It is also known as Adaptive Routing.
- It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
- Dynamic protocols are used to discover the new routes to reach the destination.
- In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
- If any route goes down, then the automatic adjustment will be made to reach the destination.

The Dynamic protocol should have the following features:

- All the routers must have the same dynamic routing protocol in order to exchange the routes.
- If the router discovers any change in the condition or topology, then router broadcast this information to all other routers. [27]

➢ **Advantages of Dynamic Routing:**

- It is easier to configure.
- It is more effective in selecting the best route in response to the changes in the condition or topology.

➢ **Disadvantages of Dynamic Routing:**

- It is more expensive in terms of CPU and bandwidth usage.
- It is less secure as compared to default and static routing. [27]

I.17 CONCLUSIN

The network is a major advance in the technologies of our time, and all efforts of the past decades have resulted in more performance. Primarily, improving support is very important to get better quality service. After support, the layer architecture also allows for a solution to get the best performance, and there are two architectural models: OSI and TCP / IP on which the network technologies depend. Next, we talked about the different types of standards in networks with an emphasis on architecture, IP was explained in the last part by focusing on data and routing fines, and we can see distance vector protocols like RIP and link state protocols like OSPF. In this chapter, we have presented the network in its generality. Although we have summarized local networks, it is imperative to know how to improve them, which is within our goal. The next chapter will explain a study about the WAN network and how to improve the management of technologies and resources within the network, so we will study the network and the three technologies (FR.ATM. MPLS) that we will rely on in our paperwork and compare between them in terms of transferring information and providing high-quality service.

CHAPTER 2

EXTENDED NETWORKS

II .DATA TRANSMISSION AND NETWORK CAPACITY REQUIREMENTS

Momentous changes in the way organizations do business and process information have been driven by changes in networking technology and at the same time have driven those changes. It is hard to separate chicken and egg in this field. Similarly, the use of the Internet by both businesses and individuals reflects this cyclic dependency: the availability of new image-based services on the Internet (i.e., the Web) has resulted in an increase in the total number of users and the traffic volume generated by each user. This, in turn, has resulted in a need to increase the speed and efficiency of the Internet. On the other hand, it is only such increased speed that makes the use of Web-based applications palatable to the end user. **[17]**

In this section, we survey some of the end-user factors that fit into this equation. We begin with the need for high-speed LANs in the business environment, because this need has appeared first and has forced the pace of networking development. Then we look at business WAN requirements.

II.1 WIDE AREA NETWORK (WAN)

II.1 Introduction

Is a computer communications network that spans cities, countries, and the globe, generally using telephone lines and satellite links, The Internet connects multiple WANs.

As data across the world continues to proliferate at breakneck speed, network providers of various sizes (from LAN to WAN) are beginning to see a strain on what their networks can support. This has resulted in new forms of data optimization to increase data collection, reduce bandwidths and consolidate servers, among other things.

As WANs are so expansive, modern organizations have been eager for a more optimized version of a WAN connection. Software-defined WANs (SD-WANs) is one solution organizations are beginning to turn to, as it can help alleviate serious traffic issues in the sharing and spreading of data information.

SD-WANs use smart software that can monitor the performance of different WAN connections and then appropriately allocate the data into the right connection for the type of traffic users need.

For example, an organization may have many different forms of WAN telecommunications — from emails and conference calls to data sharing and dedicated server networks — and SD-WANs typically help alleviate the strain from all these connections by choosing the appropriate channel to funnel the data through. [17]

Data demands will continue to grow exponentially over the coming decades, so more advanced forms of WAN connections may continue to be developed. Even now, NASA is working on creating an interplanetary internet for future exploration, and it is currently using a disruptive tolerance network (DTN) for the International Space Station. The biggest concern will be addressing the speed of data transfer, as the greater the distance between two servers, the longer it will take for data to get from point A to point B. [17]

WANs have become an essential part of human communication and business relations, and as the world continues to grow, WANs may change and develop new forms of technology in time, as well.

II.1.1 Definition

A wide area network (WAN) is a data network, usually used for connecting computers, that spans a wide geographical area. WANs can be used to connect cities, states, or even countries. WANs are often used by larger corporations or organizations to facilitate the exchange of data, and in a wide variety of industries corporations with facilities at multiple locations have embraced WANs. Increasingly, however, even small businesses are utilizing WANs as a way of increasing their communications capabilities. [17]

It is a large network of information that is not tied to a single location, WANs can facilitate communication, the sharing of information and much more between devices from around the world through a WAN provider.

WANs can be vital for international businesses, but they are also essential for everyday use, as the internet is considered the largest WAN in the world.

wide area networks are a form of telecommunication networks that can connect devices from multiple locations and across the globe. WANs are the largest and most expansive forms of computer networks available to date.

For international organizations, WANs allow them to carry out their essential daily functions without delay. Employees from anywhere can use a business’s WAN to share data, communicate with coworkers or simply stay connected to the greater data resource center for that organization. Certified network professionals help organizations maintain their internal wide area network, as well as other critical IT infrastructure. [17]

II.1.2 Purpose Of a WAN Connection

If WAN connections didn’t exist, organizations would be isolated to restricted areas or specific geographic regions. LANs would allow organizations to work within their building, but growth to outside areas — either different cities or even different countries — would not be possible because the associated infrastructure would be cost prohibitive for most organizations.

As organizations grow and become international, WANs allow them to communicate between branches, share information and stay connected. When employees travel for work, WANs allow them to access the information they need to do their job. WANs also help organizations share information with customers, as well as partner organizations, such as B2B clients or customers. [06]

However, WANs also provide an essential service to the public. Students at universities might rely on WANs to access library databases or university research. And every day, people rely on WANs to communicate, bank, shop and more. [06]

II.1.3 TYPES OF WAN TECHNOLOGIES NETWORKS

II.1.3.1 Circuit Switching

In a circuit-switching network, a dedicated communications path is established between two stations through the nodes of the network. That path is a connected sequence of physical links between nodes. On each link, a logical channel is dedicated to the connection. Data generated by the source station are transmitted along the dedicated path as rapidly as possible. At each node, incoming data are routed or switched to the appropriate outgoing channel without delay. The most common example of circuit switching is the telephone network. [06]

II.1.3.2 Packet Switching

Packet switching is a method of data transmission in which a message is broken into several parts, called packets, that are sent independently, in triplicate, over whatever route is optimum for each packet, and reassembled at the destination. Each packet contains a piece part, called the payload, and an identifying header that includes destination and reassembly information. The packets are sent in triplicate to check for packet corruption. Every packet is verified in a process that compares and confirms that at least two copies match. When verification fails, a request is made for the packet to be re-sent. [06]

II.1.3.3 TCP/IP Protocol Suite

TCP/IP is a protocol suite of foundational communication protocols used to interconnect network devices on today's Internet and other computer/device networks. TCP/IP stands for Transmission Control Protocol/Internet Protocol. [11]

II.1.3.4 Router

A router is a networking device typically used to interconnect LANs to form a wide area network (WAN) and as such is referred to as a WAN device. IP routers use IP addresses to determine where to forward packets. An IP address is a numeric label assigned to each connected network device. [11]

II.1.3.5 Overlay Network

An overlay network is a data communications technique in which software is used to create virtual networks on top of another network, typically a hardware and cabling infrastructure. This is often done to support applications or security capabilities not available on the underlying network.

II.1.3.6 Packet Over SONET/SDH (PoS)

Packet over SONET is a communication protocol used primarily for WAN transport. It defines how point-to-point links communicate when using optical fiber and SONET (Synchronous Optical Network) or SDH (Synchronous Digital Hierarchy) communication protocols. [11]

II.1.3.7 Frame Relay (FR)

Frame Relay is a technology for transmitting data between LANs or endpoints of a WAN. It specifies the physical and data-link layers of digital telecommunications channels using a packet switching methodology.

II.1.3.8 ATM (Asynchronous Transfer Mode)

ATM (Asynchronous Transfer Mode) is a switching technique common in early data networks, which has been largely superseded by IP-based technologies. ATM uses asynchronous time-division multiplexing to encode data into small, fixed-sized cells. By contrast, today's IP-based Ethernet technology uses variable packet sizes for data. [11]

II.1.3.9 MPLS (Multiprotocol Label Switching)

is a virtual private network built on top of a provider’s Multiprotocol Label Switching Network to provide Layer 2 or Layer 3 VPN data networking services. Multiprotocol and tagging capabilities of MPLS connect remote sites into a common type of data communication network. the configurations available include site to site, multipoint, and meshed networks. Customer data is partitioned from each other, keeping it private across the provider’s infrastructure. Data partitioning is created using MPLS tags rather than encryption.

II.1.4 NETWORK QOS

We might wish to treat different traffic. some applications. such as voice and video, are delay sensitive but loss insensitive. Others, such as file transfer and electronic mail, are delay insensitive but loss sensitive The control and visibility provided by QoS enables WAN ,service providers to offer carefully tailored grades of service differentiation to their customers, uses in various technologies, including Frame Relay, Asynchronous Transfer Mode (ATM), MPLS, Ethernet and 802.1 networks, SONET, and IP-routed networks that may use any or all of these underlying technologies. Primary goals of QoS include dedicated bandwidth, QoS technologies provide the elemental building blocks that will be used for future business applications in WAN, This chapter outlines the features and benefits of the QoS (required by some real-time and interactive traffic), Coexistence of mission-critical applications— QoS technologies make certain that your.

WAN is used efficiently by mission-critical applications that are most important to your business, and that other applications using the link get their fair service without interfering with mission-critical traffic. [01]

Foundation for a fully integrated network in the future: implementing Cisco QoS technologies in your network now is a good first step toward the fully integrated multimedia network needed in the near future.

II.4.1 Basic QoS Architecture (Figure 12)

- QoS within a single network element (for example, queuing, scheduling, and traffic shaping tools).
- QoS signaling techniques for coordinating QoS from end to end between network elements. [01]

- QoS policy, management, and accounting functions to control and administer end-to-end traffic.

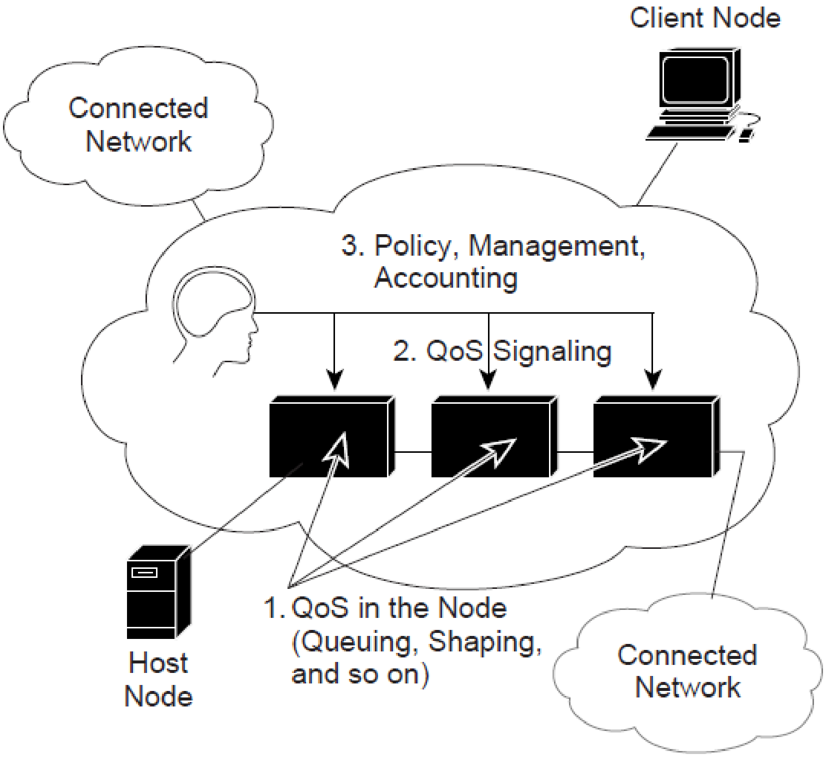

Client Node
Connected Network
3. Policy, Management, Accounting
2. QoS Signaling
1. QoS in the Node (Queuing, Shaping, and so on)
Host Node
Connected Network

Figure 12: A basic QoS Architecture

II.1.4.2 QoS Levels

Service levels refer to the actual end-to-end QoS capabilities, meaning the ability of a network to deliver service needed by specific network traffic from end to end or edge to edge, The services differ in their level of "QoS strictness," which describes how tightly the service can be bound by specific bandwidth, delay, jitter, and loss characteristics.

There three levels of end-to-end QoS are best-effort service, differentiated service, and guaranteed service. [01] (**Figure 13**)

- **Best-effort service**: Also known as lack of QoS, best-effort service is basic connectivity with no guarantees.
- **Differentiated service (also called soft QoS):**Some traffic is treated better than the rest (faster handling, more bandwidth on average, lower loss rate on average). This is a statistical preference, not a hard and fast guarantee.
- **Guaranteed service (also called hard QoS):**An absolute reservation of network resources for specific traffic. [01]

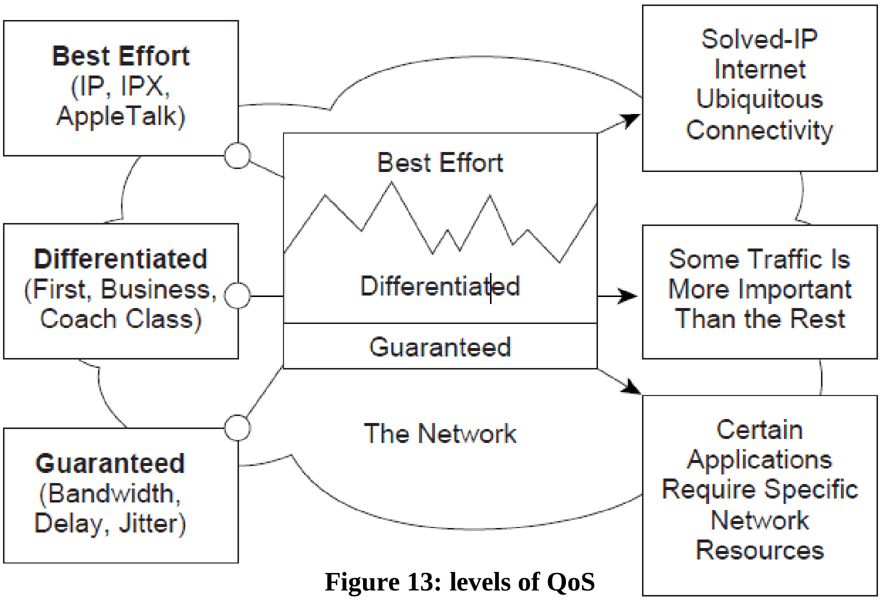


Figure 13: levels of QoS

II.2 The WAN technologies

In the first part of this paperwork we talked about WAN and several technologies, but we took only three types of uses for WAN networks that public and private corporate customers depend on and designed for a variety of use cases that affect virtually every aspect of modern life and private lines, to connect cities. The main in different locations, multi-protocol switching (FR, ATM ,MPLS), virtual private networks (VPNs), wireless (cellular) networks and the Internet. The distributed network and the sites they connect to can be a few miles away, halfway or around the world. In any organization, the purposes of a WAN can include connecting branch offices or even individual remote workers to a headquarters or data center in order to share company resources and connections. [09]

A key design issue that must be confronted both with data networks, such as packet-switching, frame relay, and ATM networks, and also with internets, is that of congestion control. The phenomenon of congestion is a complex one, as is the subject of congestion control. In very general terms, congestion occurs when the number of packets being transmitted through a network begins to approach the packet-handling capacity of the network. The objective of congestion control is to maintain the number of packets within the network below the level at which performance falls off dramatically. Which we will describe in detail below:

II.2.1 FRAME RELAY (FR) NETWORK

II.2.1.1 The Frame Relay Development

In 1990, four vendors - StrataCom, Digital Equipment Corporation, Cisco Systems and Northern Telecom - collaborated on developing a specification called the Frame Relay Specification with Extensions. This document introduced a Local management Interface (LMI) to provide control procedures for permanent virtual circuits (PVCs).

before that it was part of the ISDN standards. Since that time there has been much debate, disagreement, and controversy over the nature of the benefits of this new communications protocol. Many claims have been made as to its capabilities in various situations from data networking (taking over from X25) through LAN interconnection, across WAN, even to the realms of passing voice and video information. However the reality is somewhat removed from many of the claims and the applicability of frame relay is very closely tied into the application and the networking infrastructure. [10]

II.2.1.2 Definition

Frame Relay is a standardized wide area network technology that specifies the physical and data link layers of digital telecommunications channels using a packet switching methodology, The frame relay service uses either a permanent or switched virtual circuit to set the connection and enable the transfer of bit from source to the destination at a fair speed in an affordable cost.

Is a high-performance WAN protocol that operates at the physical and data link layers of the OSI reference model. Frame Relay originally was designed for use across Integrated Services Digital Network (ISDN) interfaces. Today, it is used over a variety of other network interfaces as well. Frame Relay is an example of a packet-switched technology. Packet-switched networks enable end stations to dynamically share the network medium and the available bandwidth. The following two techniques are used in packet-switching technology:

- Variable-length packets
- Statistical multiplexing

1.Variable-length packets are used for more efficient and flexible data transfers. These packets are switched between the various segments in the network until the destination is reached.

2. Statistical multiplexing techniques control network access in a packet-switched network.

The advantage of this technique is that it accommodates more flexibility and more efficient use of bandwidth. Most of today’s popular LANs, such as Ethernet and Token Ring, are packet-switched networks.

is a technology for transmitting data between LANs or endpoints of a WAN. It specifies the physical and data-link layers of digital telecommunications channels using a packet switching methodology, Each frame contains all necessary information for routing it to its destination. Frame Relay's original purpose was to transport data across telecom carriers' ISDN infrastructure, but it's used today in many other networking contexts. [10]

II.2.1.3 Characteristics Of Frame Relay

- Frame Relay service is a service that supports the transport of data.

- Frame relay is a connectionless service, meaning that each data packet passing through the network contains -address information.

-Frame relay is a service that is provided with a variety of speeds from 56 Kbs up to 25 Mbs.

-Even though the most used speeds for the service are currently 56 Kbs and 1.544 Mbs Frames are variable in length and goes up to 4,096 bytes Frame Relay is considered to be a Broadband ISDN service One of the unique facets of frame relay service is that the service supports variable size data packets. [10]

II.2.1.4 Frame Relay Role And Function

II.2.1.4.1 The Role Of Frame Relay

Frame relay has an important role to play in providing elastic bandwidth communication in support of distributed applications, and modern client/server LAN-to-LAN systems in particular. It also forms an important step in the direction to full multimedia ATM networking. The bandwidth requirements for emerging data applications such as client/server based transaction processing, image and graphics transmission as well as distributed database systems are very different from those used in earlier applications. These modern applications all process large volumes of data, transmit intermittent high speed bursts and are intolerant of long delays. To satisfy the requirements of these applications, the bandwidth management system in LAN-to-WAN and LAN-to-LAN networking must offer access to high bandwidth on demand, direct connectivity to all other points in the network and consumption only of bandwidth actually needed. This tutorial discusses a range of background, technical, design and operational issues by examining. [10]

II.2.1.4.2 The Function Of Frame Relay

Frame relay is used to transfer the data in the form of packets, with the help of the data link layer. Here, a unique identifier DLCI (Data link connection identifier) identifies the virtual connection which is referred to as ports. The frame relay basically connects two DTE devices by using a DCE device. The DTE devices connected to the frame relay is assigned with a port to make each remote connection unique. It can create two types of circuits, PVC (Permanent virtual circuit) and SVC (Switched virtual circuit).

The former type of virtual circuit, PVC comprised of two operational states, data transfer and idle. In the data transfer state, the transferring of data occurs within the DTE devices across the virtual circuit. In the idle state, the data transfer does not occur even if the connection within the DTE devices is active.

The latter SVC type establishes the transient connection which could prevail until the data transfer takes place. It includes various operations such as call set up, data transfer, idle and call termination. In the call set up, termination operation the connection is established and terminated between the two DTE devices, and other operations are similar to PVC operation. [10]

II.2.1.5 Frame Relay Devices

Devices attached to a Frame Relay WAN fall into the following two general categories:

- Data terminal equipment (DTE) .
- Data circuit-terminating equipment (DCE) .

DTEs generally are considered to be terminating equipment for a specific network and typically are located on the premises of a customer. In fact, they may be owned by the customer. Examples of DTE devices are terminals, personal computers, routers, and bridges.

DCEs are carrier-owned internetworking devices. The purpose of DCE equipment is to provide clocking and switching services in a network, which are the devices that actually transmit data through the WAN. [10]

The connection between a DTE device and a DCE device consists of both a physical layer component and a link layer component. The physical component defines the mechanical, electrical, functional, and procedural specifications for the connection between the devices. One of the most commonly used physical layer interface specifications is the recommended standard (RS)-232 specification. The link layer component defines the protocol that establishes the connection between the DTE device, such as a router, and the DCE device, such as a switch.

II.2.1.6 Virtual Circuits

Frame Relay is a virtual circuit network, so it doesn’t use physical addresses to define the DTEs connected to the network. Frame Relay provides connection-oriented data link layer communication. This means that a defined communication exists between each pair of devices and that these connections are associated with a connection identifier. However, virtual circuit identifiers in Frame relay operate at the data link layer, in contrast with X.25, where they operate at the network layer. This service is implemented by using a Frame Relay virtual circuit, which is a logical connection created between two data terminal equipment (DTE) devices across a Frame Relay packet-switched network (PSN). [10]

A virtual circuit can pass through any number of intermediate DCE devices (switches) located within the Frame Relay PSN. Before going into the details of DLCI let us first have a look at the two types of Frame Relay Circuits, namely: switched virtual circuits (SVC) and permanent virtual circuits (PVC).

II.2.1.6.1 Switched Virtual Circuits

Switched virtual circuits (SVCs) are temporary connections used in situations requiring only sporadic data transfer between DTE devices across the Frame Relay network. A communication session across an SVC consists of the following four operational states:

- **Call setup**:The virtual circuit between two Frame Relay DTE devices is established.
- **Data transfer**: Data is transmitted between the DTE devices over the virtual circuit.
- **Idle**: The connection between DTE devices is still active, but no data is transferred. If an SVC remains in an idle state for a defined period of time, the call can be terminated.
- **Call termination**: The virtual circuit between DTE devices is terminated. After the virtual circuit is terminated, the DTE devices must establish a new SVC if there is additional data to be exchanged. It is expected that SVCs will be established, maintained, and terminated using the same signaling protocols used in ISDN. [10]

II.2.1.6.2 Permanent Virtual Circuits

Permanent virtual circuits (PVCs) are permanently established connections that are used for frequent and consistent data transfers between DTE devices across the Frame Relay network. Communication across PVC does not require the call setup and termination states that are used with SVCs. PVCs always operate in one of the following two operational states:

Data transfer: Data is transmitted between the DTE devices over the virtual circuit.

Idle: The connection between DTE devices is active, but no data is transferred. Unlike SVCs, PVCs will not be terminated under any circumstances when in an idle state[10]. DTE devices can begin transferring data whenever they are ready because the circuit is permanently established.

II.2.1.7 Frame Relay Layers

Frame Relay has only two layers, namely Physical layer and Data Link layer. And as compared to other layer of packet switching network such as X.25, frame relay has only 1.5 layers whereas X.25 has 2 layers. Frame Relay eliminates all network layer functions and a portion of conventional data-link layer functions. [10]

II.2.1.7.1 Physical layer

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

-It supports ANSI standards. [10]

-No specific protocol is defined for the physical layer. The user can use any protocol which is recognized by ANSI.

This layer plays with most of the network's physical connections—wireless transmission, cabling, cabling standards and types, connectors and types, network interface cards, as per network requirements. The functions of the physical layer are :

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex. [10]

II.2.1.7.2 Data Link layer

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address. Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.

The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address. The functions of the data Link layer are[10] :

1. **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time. [10]

II.2.1.8 QoS Of Frame Relay

In a shared network, it is necessary to "meter" the traffic entering into and transiting the elements that comprise the network infrastructure. When a connection is made to a Frame Relay network, characteristics are established that provide for a Committed Information Rate, a Maximum Burst Rate, and Burst values ('commit' and 'exceed') that govern the proportion of Frame Relay resources consumed by traffic over that connection. The Committed Information Rate (CIR) specifies the projected demand on the network for transport resources. It reflects a moving average value, which is approached over time using the Burst commit (Bc) and Burst-exceed (Be) rates. The combination of values allows for the efficient use of the network from both Provider and a Customer perspective. This provided a mechanism for efficient allocation of resources, but as Frame networks enjoyed increasing subscription, an enforcement mechanism was required in the event of saturation. [10]

II.2.1.9 Advantages And Disadvantages Of Frame Relay

II.2.1.9.1 Advantages Of Frame Relay

➨It offers higher speeds. This is because of no error detection is incorporated and hence overhead is less. It offers high throughput compare to X.25.

➨The bandwidth can be allocated dynamically as per need.

➨The network overhead is less due to incorporation of congestion control mechanism. Streamlined communication process

➨It allows bursty data which do not have fixed data rate.

➨It operates at layer-1 (physical) and layer-2 (data link). Hence it is easy to integrate with devices having layer-3 (i.e. network) layer functionalities.

➨It allows frame size of 9000 bytes which is enough for all the LAN frame types.

➨It is less expensive compare to traditional WAN networks.

➨It offers guaranteed throughput and delay.

➨It provides secured connection as it is difficult to break into PVCs between the sites.

➨Frame relay operates at a high speed (1.544 Mbps to 44.376 Mbps). [10]

II.2.1.9.2 Disadvantages Of Frame Relay

➨The flow control and error control is not available in frame relay. This should be taken care by upper layer protocols. Packets having errors are simply discarded.

➨Packets incur additional delay with every node they pass through, Frames are delivered unreliably.

➨It involves data overhead and processing overhead with every packet. It does not provide the acknowledgement of received packets.

➨It allows variable length frames and hence may create varying delays for different users.

➨Due to varying delay, it is not suitable to send sensitive data like real time voice or video. Packets may not be delivered in the same sequence as that at the sending end.

➨It can operate at 44.376 Mbps and hence it is not suitable for protocols requiring higher data rates.

➨It is more expensive compare to internet service. [10]

II.2.2 ATM NETWORK

II.2.2.1 The ATM network development

Asynchronous Transfer Mode (ATM) networking had its origins as a switching and multiplexing technology suitable for the design of high capacity switches. The essential features of ATM are a fixed-length packet (called a cell), which is switched based on a virtual circuit identifier in the cell header. End-hosts request that the network set up a virtual circuit via a signaling (control) protocol that allows them to specify the desired quality of service.

For a period of time in the early to mid 1990’s, investment and research on ATM exploded, based on an expectation that ATM would revolutionize networking. For telecom providers, ATM promised to unify a number of disparate networks (voice, private line, data) on a single switching network. The fixed cell size fit well with designs for large self-routing switch fabrics suitable for the construction of very high-capacity switches. ATM’s proponents anticipated that ATM would be ubiquitous, and that end-to-end quality of service would enable an entirely new class of network applications to be built. [15]

The reality today is far different. ATM is used today to provide Virtual Private Network (VPN) services to businesses, consisting primarily of point-to-point virtual circuits connecting customer sites.

also provides the underpinnings of Digital Subscriber Loop (DSL) services, which are growing rapidly. In DSL access networks, ATM enables local exchange carriers to switch subscriber traffic to different Internet Service Providers. ATM is also used as the core network infrastructure for large Frame Relay networks and for some IP networks. While these uses of ATM are important and should be viewed as a mark of success for ATM technology, there is a perception in the network research community that ATM “failed.” Indeed, when compared with the grandiose visions that many of its proponents had, ATM was not as successful as it might have been. [15]

II.2.2.2 Definition

Is a connection-oriented technology in the sense that before two systems on the network can communicate, they should inform all intermediate switches about their service requirements and traffic parameters. This is similar to the telephone networks where a fixed path is set up from the calling party to the receiving party. In ATM networks, each connection is called a virtual circuit or virtual channel (VC), because it also allows the capacity of each link to be shared by connections using that link on a demand basis rather than by fixed allocations. The connections allow the network to guarantee the quality of service (QoS) by limiting the number of VCs. Typically, a user declares key service requirements at the time of connection setup, declares the traffic parameters, and may agree to control these parameters dynamically as demanded by the network. [15]

Quality of service per virtual circuit is provided through admission control and switch scheduling algorithms, allowing delay-constrained traffic, such as voice and circuit-emulated TDM traffic, to share a single network infrastructure with bursty data traffic. The cell size was kept small to support low delay for voice (although introducing enough delay that echo cancellation is needed).

II.2.2.3 Principle Characteristics of ATM

- The ATM standard defines a full suite of communication protocols, from the transport layer all the way down through the physical layer.
- It uses packet switching with fixed length packets of 53 bytes. In ATM jargon these packets are called cells. Each cell has 5 bytes of header and 48 bytes of "payload". The fixed length cells and simple headers have facilitated high-speed switching.
- ATM uses virtual circuits (VCs). In ATM jargon, virtual circuits are called virtual channels. The ATM header includes a field for the virtual channel number, which is called the virtual channel identifier (VCI) in ATM jargon. As discussed in Section 1.3, packet switches use the VCI to route cells towards their destinations; ATM switches also perform VCI translation. [04]
- ATM provides no retransmissions on a link-by-link basis. If a switch detects an error in an ATM cell, it attempts to correct the error using error correcting codes. If it cannot correct the error, it drops the cell and does not ask the preceding switch to retransmit the cell.
- ATM provides congestion control on an end-to-end basis. That is, the transmission of ATM cells is not directly regulated by the switches in times of congestion. However, the network switches themselves do provide feedback to a sending end system to help it regulate its transmission rate when the network becomes congested.
- ATM can run over just about any physical layer. It often runs over fiber optics using the SONET standard at speeds of 155.52 Mbps, 622 Mbps and higher. [15]

II.2.2.4 ATM Cells

II.2.2.4.1 Definition

ATM cells are standardized- length size of 53 bytes to enable faster switching than is possible on networks using variable-packet sizes (such as Ethernet) [3]. It is much easier to design a device to quickly switch a fixed-length packet than to design a device to switch a variable-length packet. (Switching a fixed-length packet is easier because the device knows in advance the exact length of the packet and can anticipate the exact moment at which the last portion of the packet will be received. With variable-length packets, the device must examine each packet for length information.) Using fixed-length cells also makes it possible to control and allocate ATM bandwidth more effectively, making support for different quality of service (QoS) levels for ATM possible. [3]

ATM cells is the basic data unit of the ATM (Asynchronous Transfer Mode) protocol. Cells contain identifiers known as VCI (Virtual Channel Identifier) and VPI (Virtual Path Identifier) to associate the cells with a logical data stream. Each cell consists of a 5 byte header and 48 bytes of payload. The cells are small in order to facilitate low processing delay and so high speed transmission.

II.2.2.4.2 Header Of An ATM Cell

Header - 5 octets reserved for:- Routing (GFC), Addressing (VPI, VCI, PTI), Flow control (CLP, HEC) [3]**.** (**Figure 14**).

- **Generic Flow Control (GFC)** : four bits that control traffic flow between the ATM network and terminal equipment. These are gatekeeper bits that do not travel with the cells across the ATM network, but are used to establish connections with end user equipment. Additionally, GFC bits:

  - Manage access conflicts .
  - giving each user fair access to the ATM network.
  - Ensure proper Quality of Service is allotted each user.
  - Support up to 100 users on each UNI.[3]

- **VCI (Virtual circuit identifier):** is the most fundamental unit in the ATM network, while the virtual path connection is a collection of virtual channel connections. Further, a set of virtual path connection makes up a transmission path.

- **VPI (Virtual path identifier):**The VPI field employs the virtual values to switch the cells between the ATM networks such as the routing. The UNI interface contains 8 bits for the VPI field which allows 256 virtual path identifiers. While NNI interface format can have 12 bits in the VPI fields and that allow 4,095 virtual path identifiers. On the other hand, the VCI field is used to perform switching for the end users and has a 16-bit value for both UNI and NNI interface formats. This field permits to get 65,536 virtual channels. [3]

- **Payload Type Identifier (PTI**) : three bits that identify the cell as carrying information for the user or as carrying service information.

- **Cell Loss Priority (CLP)** : one bit that determines if a cell can be discarded if the network becomes too congested. 0=keep, 1=discard.

- **Header Error Control (HEC**) : 8 bits that do cyclical redundancy checks on the first four header octets. The HEC ensures multiple bit error detection and single bit error correction. [3]

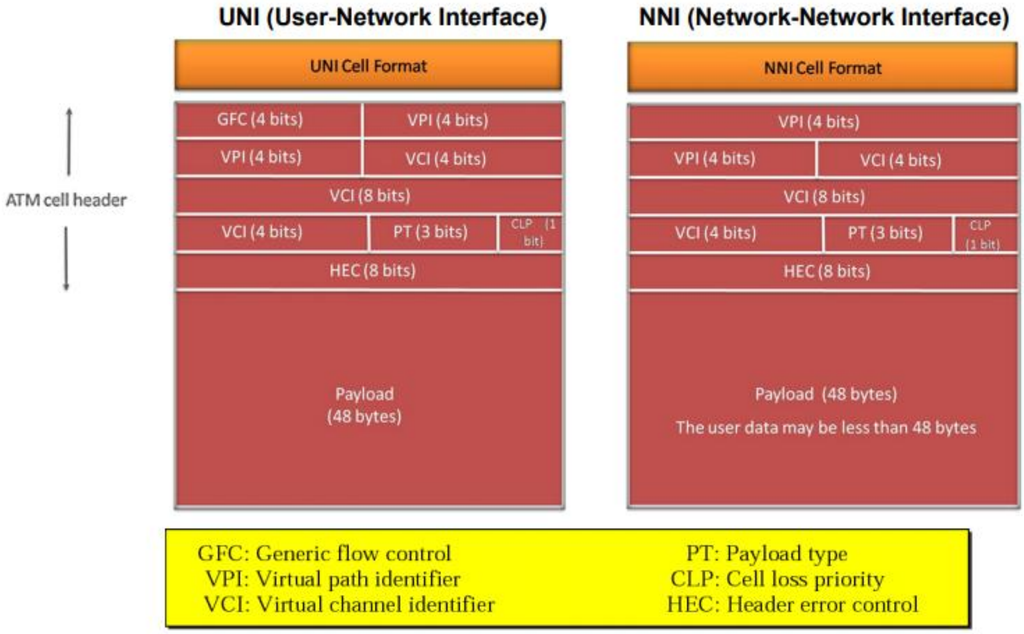


Figure 14: ATM Cells

The functions of information stored in the 5-byte header of an ATM cell include the following:

- Providing information about the physical layer transmission method being used.
- Providing flow control to enable a steady flow of cell traffic and to reduce cell jitter.
- Specifying virtual path or channel identification numbers so that multiplexed cells belonging to the same ATM connection can be distinguished from cell s belonging to other ATM connections, and so that cells can be switched to their intended destination.
- Specifying the nature of the payload contained in the cell—that is, whether it contains actual user data or ATM cell-management information.
- Specifying the priority of the cell to determine whether the cell can be dropped in congested traffic conditions.
- Providing error checking by means of an 8-bit field containing cyclical redundancy check (CRC) information for the header itself. [3]

II.2.2.4.3 Payload For ATM Cells

This is the result of a trade-off between larger 64-byte payloads that contain more data but take longer to package and unpackage, and are therefore not suitable for real-time transmissions such as voice or multimedia – and shorter 32-byte payloads that provide better real-time transmission but are inefficient for larger amounts of data. By compromising at a 48-byte payload size, ATM has good transmission capabilities for both voice and data communication, providing efficient packet transfer with low latency. 48 octets reserved for voice, video, audio and data (user or service). [3]

II.2.2.5 The Function Of Cells ATM

There are two kinds of interfaces in ATM. An interface that connects two or more networks, called Network to Network Interface (NNI) and an interface to connect the user to the network, called User to Network Interface (UNI) . It is envisioned that the ATM network service providers may offer several types of interfaces to their networks. One interface that is likely to be popular with companies that build routers and bridges for local area networks is a Frame based interface. One or more of the IEEE 802.X or FDDI frames may be supported at the UNI, with frame to ATM cell conversion and reassembly being done inside the UNI at the source and destination end points respectively. Thus a gateway host on a local area network might directly connect its Ethernet, token ring, or other LAN/MAN interface to the UNI, and thus bridge two widely separated LANs with an ATM backbone network. This will preserve the existing investment in these standards and equipments, and enable a gradual transition of the ATM networks into the market place. [23]

II.2.2.5.1 User Network Interface (UNI)

The term User Network Interface (UNI) can be defined as a physical demarcation edge between the responsibility of the service provider and the responsibility of the service subscriber. It is quite different from the Network to Network Interface (NNI) which defines a similar interface between provider networks. The network which provides the Ethernet services is known as Carrier Ethernet Network (CEN). In telecommunications, a User Network Interface is a point between ATM end users and a private ATM switch. It can also represent the interface between a private ATM switch and the public carrier ATM network.

Typically, an ATM network will require a network management agent or proxy to be running at every UNI which can communicate and exchange administrative messages with the user attachments at the UNI for connection setup, tear down, and flow control of the payload using some standard signalling protocol. A direct user attachment at the UNI is likely to cost more and be more complex, than a user attachment to something which in turns interfaces to the UNI. [23]

II.2.2.5.2 network-to-network interface (NNI)

A network-to-network interface (NNI) is a physical interface that connects two or more networks and defines inter signaling and management processes. It enables the linking of networks using signaling, Internet Protocol (IP) or Asynchronous Transfer Mode (ATM) networks. Is also known as a network node interface (NNI).

A NNI is used to provide the interconnection between two or more service providers or connecting service providers with an organizational network. It usually connects two or more P routers. [23]

II.2.2.6 ATM Protocol Reference Model

The ATM protocol reference model is based on standards developed by the ITU, Communication from higher layers is adapted to the lower ATM layers, which in turn pass the information onto the physical layer for transmission over a selected physical medium, ATM functionality corresponds to the physical layer and part of the data link layer of the OSI reference model.

The protocol reference model is divided into three layers: the ATM adaptation layer (AAL), the ATM layer, and the physical layer [3] (Figure 15).

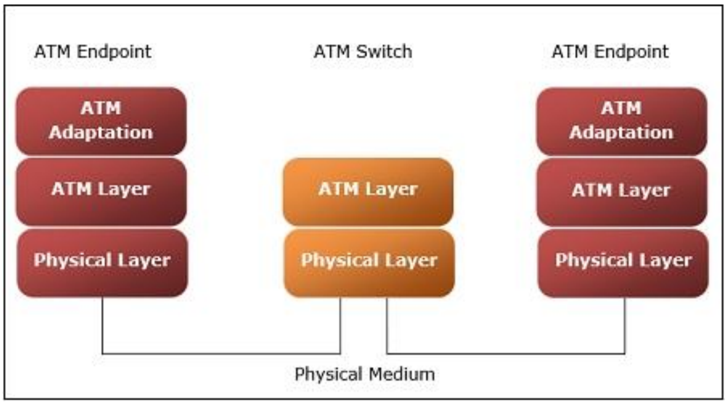


Figure 15: ATM Protocol Structure

II.2.2.6.1 The ATM Adaptation Layer (AAL)

This layer corresponds to network layer of OSI model. It provides facilities to the existing packet switched networks to connect to ATM network and use its services. It accepts the data and converts them into fixed sized segments. The transmissions can be of fixed or variable data rate. This layer has two sub layers − Convergence sub layer and Segmentation and Reassembly sub layer . [3]

Some networks that need AAL services are Gigabit Ethernet, IP, Frame Relay, SONET/SDH and UMTS/Wireless.

This is following diagram illustrates the function of AAL. (Figure 16)

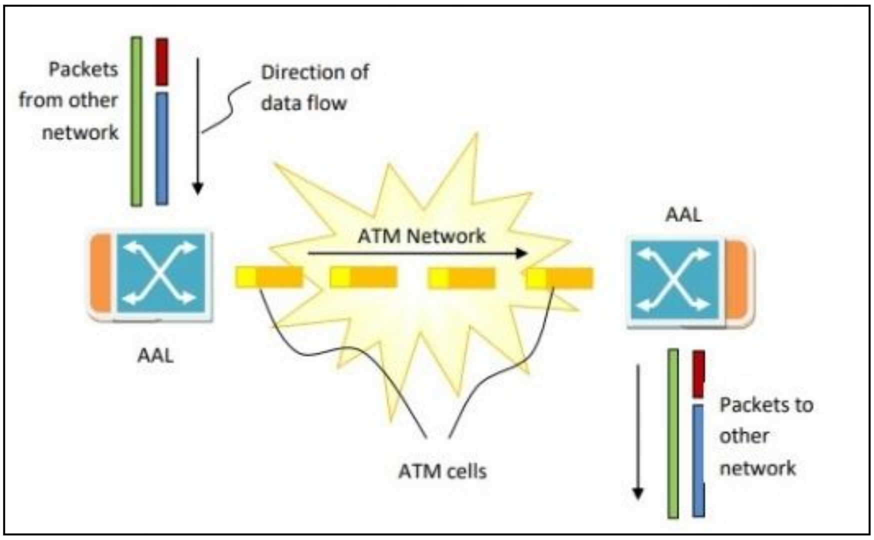


Figure 16: diagram illustrates the function of AAL

II.2.2.6.2 ATM Layer

This layer is comparable to data link layer of OSI model. It accepts the 48 byte segments from the upper layer, adds a 5 byte header to each segment and converts into 53 byte cells. This layer is responsible for routing of each cell, traffic management, multiplexing and switching. [3]

Operations in the ATM Layer are independent of Physical Layer operations, and are not affected if an ATM cell is running on fiber, twisted pair, or other media type. The ATM Layer is organized into the following four major functions.

1. **Cell Muxing and Demuxing:** This function is responsible for multiplexing cells from various virtual connections at the originating point, and demultiplexing them at the terminating endpoint.

2. **VPI/VCI Processing:** This function is responsible for processing the labels and identifiers in a cell header at each ATM node. ATM virtual connections are created and identified by a virtual path identifier (VPI) and a virtual channel identifier (VCI).

3. **Cell Header Processing:** This function creates the cell header at the originating point, interprets, and translates it at the terminating endpoint. The virtual path endpoint (VPE)/VCI data may be translated to a service access point (SAP) at the receiving node.

4. **Generic Flow Control:** This function is responsible for creating the generic flow control field in the ATM header at the originating point, and acting upon it at the receiving endpoint. [3]

II.2.2.6.3 Physical Layer

This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.

This layer corresponds to physical layer of OSI model. At this layer, the cells are converted into bit streams and transmitted over the physical medium. This layer has two sub layers: PMD sub layer (Physical Medium Dependent) and TC (Transmission Convergence) sub layer.

The Physical Layer is responsible for bit transfer and reception, and bit synchronization. It contains two sub-layers, the Physical Medium (PM) Sub-layer, and the Transmission Convergence (TC) Sub-layer. PM functions are dependent on the nature of the medium making the connection, while the TC Sub-layer is responsible for conventional physical layer operations that are not medium dependent. TC is responsible for the following five functional capabilities. [3]

1. **Transmission Frame Generation and Recovery:** This function is responsible for the generation and recovery of certain protocol data units (PDUs), which are called frames in B-ISDN.

2. **Transmission Frame Adaptation:** This function is responsible for placing and extracting the cell into and out of the Physical Layer frame. The exact operation depends on the type of frame that is used at the physical layer.

3. **Cell Delineation:** This function is responsible for originating an endpoint to define the cell boundaries in order for the receiving endpoint to recover all cells.

4. **Cell Header Processing:** This function is responsible for generating a header error control (HEC) field at the originating point, and processing it at the terminating endpoint to determine if the cell header was damaged during transmission.

5. **Cell Rate Decoupling:** This function inserts idle cells at the sending end and extracts them at the receiving end in order to adapt to the physical level of bandwidth capacity. [3]

II.2.2.7 ATM protocol architecture

The asynchronous transfer mode (ATM) protocol architecture is designed to support the transfer of data with a range of guarantees for quality of service. The user data is divided into small, fixed-length packets, called cells, and transported over virtual connections. ATM operates over high data rate physical circuits, and the simple structure of ATM cells allows switching to be performed in hardware, which improves the speed and efficiency of ATM switches. [15]

(Figure 17) shows the reference model for ATM. The first thing to notice is that, as well as layers, the model has planes. The functions for transferring user data are located in the user plane; the functions associated with the control of connections are located in the control plane; and the co-ordination functions associated with the layers and planes are located in the management planes. [15]

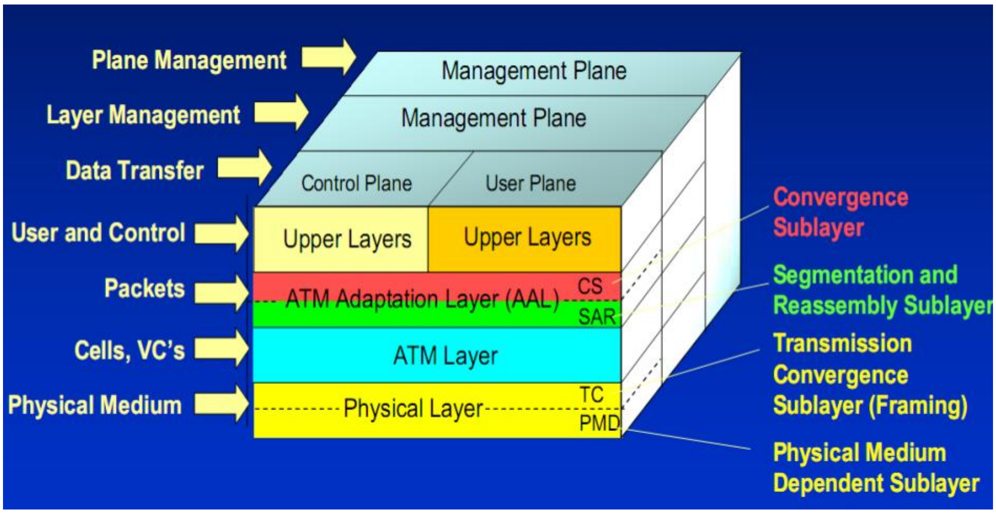


Figure 17: ATM reference model

The three-dimensional representation of the ATM protocol architecture is intended to portray the relationship between the different types of protocol. The horizontal layers indicate the encapsulation of protocols through levels of abstraction as one layer is built on top of another, whereas the vertical planes indicate the functions that require co-ordination of the actions taken by different layers. An advantage of dividing the functions into control and user planes is that it introduces a degree of independence in the definition of the functions: the protocols for transferring user data (user plane) are separated from the protocols for controlling connections (control plane). [15]

- **Control**: The main function of this plane is to produce and manage the signalling request.
- **User**: This plane handles the transfer of the data.
- **Management**: Layer related functions such as failure detection, problems regarding protocols are governed by this plane. It also involves the functions related to the complete system.
- **ATM endpoints** – It contains ATM network interface adaptor. Examples of endpoints are workstations, routers, CODECs, LAN switches, etc.

- **ATM switch −**It transmits cells through the ATM networks. It accepts the incoming cells from ATM endpoints (UNI) or another switch (NNI), updates cell header and retransmits cell towards destination. [15]

II.2.2.8 QUALITY OF SERVICE (QOS) PARAMETERS

ATM monitors Quality of Service (QOS) parameters such as cell loss, delay, and delay variation, incurred by the cells belonging to the connection in an ATM network. QOS parameters can be either specified explicitly by the user or implicitly associated with specific service requests. A limited number of specific QOS classes are becoming standardized in practice.

Future applications are expected to require increasingly higher bandwidth and generate a heterogeneous mix of network traffic. Existing networks cannot provide the transport facilities to efficiently support a diversity of traffic with various service requirements. ATM is potentially capable of supporting all classes of traffic such as (voice, video, data) in one transmission and switching fabric technology. It promises to provide greater integration of capabilities and services, increased and more flexible access to the network, and more efficient and economical service. [14]

- Quality of Service (QoS**)** is a type of Networking Technology that can guarantee a specific level of output for a specific connection, path, or type of traffic. QoS mechanisms provide control on both quality and availability of bandwidth whereas another network provides only a best-effort delivery.
- QoS feature is used when there is traffic congestion in-network, it gives priority to certain real-time media. A high level of QoS is used while transmitting real-time multimedia to eliminate latency and dropouts. Asynchronous Transfer Mode (ATM) is a networking technology that uses a certain level of QoS in data transmission.
- The Quality of Service in ATM is based on following: Classes, User-related attributes, and Network-related attributes. [14]

II.2.2.8.1 The ATM Service Classes

The ATM Forum defines four service classes that are explained below .

1. Constant Bit Rate (CBR): CBR is mainly for users who want real-time audio or video services. The service provided by a dedicated line. For example, T line is similar to CBR class service.

2. Variable Bit Rate (VBR) :VBR class is divided into two sub classes

2.1 Real-time (VBR-RT): The users who need real-time transmission services like audio and video and they also use compression techniques to create a variable bit rate, they use VBR-RT service class.

2.2 Non-real Time (VBR-NRT) : The users who do not need real-time transmission services but they use compression techniques to create a variable bit rate, then they use VBR-NRT service class. [14]

3. Available Bit Rate (ABR) :ABR is used to deliver cells at a specific minimum rate and if more network capacity is available, then minimum rate can be exceeded. ABR is very much suitable for applications that have high traffic. [14]

4. Unspecified Bit Rate (UBR) :UBR class and it is a best-effort delivery service that does not guarantee anything.

II.2.2.8.2 The ATM user related Attributes

ATM defines two sets of attributes and User-related attribute is one of them. They are those type attributes that define at what speed user wants to transmit data. These are negotiated during time of contract between a network and a customer. The following are some user-related attributes [14]

1. Sustained Cell Rate (SCR):SCR is average cell rate over a long time interval. The original cell rate can be less or greater than value of SCR, but average must be equal to or less than value of SCR.

2. Peak Cell Rate (PCR) :PCR is defined as maximum cell rate of sender. As long as SCR is maintained, cell rate of user can reach this peak value.

3. Minimum Cell Rate (MCR) :MCR defines minimum cell rate acceptable to sender. For example, if MCR is 50,000, network must guarantee that sender can send at least 50,000 cells per second.

4. Cell Variation Delay Tolerance (CVDT) :CVDT is a measure of the variation in cell transmission times. Let’s take an example if value of CVDT is 8 ns, this signifies that difference between minimum and maximum delays in delivering the cells should not be greater then 8 ns. [14]

II.2.2.8.3 Network-Related Attributes

The attributes that are used to define different characteristics of network are known as Network-related attributes. The following are some network-related attributes

1. Cell Loss Ratio (CLR) :CLR defines the fraction of cells lost (or delivered so late that they are considered lost) during transmission. For example, if sender sends 100 cells and one of them is lost, CLR is CLR = 1/100

2. Cell Transfer Delay (CTD) : The average time taken by a cell for traveling from source to destination is known as Cell transfer delay. The maximum CTD and minimum CTD are also considered attributes.

3. Cell Delay Variation (CDV) :CDV is difference between CTD maximum and CTD minimum.

4. Cell Error Ratio (CER) :CER defines fraction of cells delivered in error. [15]

II.2.2.9 Advantages And Disadvantages Of ATM

II.2.2.9.1 Advantages Of The ATM

- It provides the dynamic bandwidth that is particularly suited for bursty traffic.
- Since all data are encoded into identical cells, data transmission is simple, uniform and predictable.
- Uniform packet size ensures that mixed traffic is handled efficiently.
- Small sized header reduces packet overload, thus ensuring effective bandwidth usage.
- ATM networks are scalable both in size and speed.
- ATM supports voice, video and data allowing multimedia and mixed services over a single network. [15]

- It can easily interface with the existing network such as PSTN, ISDN. It can be used over SONET/SDH.
- Seamless integration with the different types of networks (LAN, MAN and WAN).
- Effective utilization of the network resources.
- It is less susceptible to the noise degradation.
- Provides large bandwidth.
- supports the broadest range of burstiness, delay tolerance and loss performance through the implementation of multiple QoS classes. [14]

II.2.2.9.2 Disadvantages Of The ATM

- Cost of switching devices is higher.
- Overhead generated by the cell header is more.
- ATM QoS mechanism is quite complex.
- flexible to efficiency's expense, at present, for any one application it is usually possible to find a more optimized technology.
- cost, although it will decrease with time.
- new customer premises hardware and software are required.
- competition from other technologies -100 Mbps FDDI, 100 Mbps Ethernet and fast Ethernet. [15]

II.2.2.10 CONCLUDING REMARKS

From these definitions, we found that ATMs provide a common flexible transmission capacity for a wide range of services with widely varying traffic patterns and can be used on different transportation modes operating at widely varying rates. ATM adaptation functions are provided to accommodate the data formats and operating characteristics of specific services.

II.2.3 MULTIPROTOCOL LABEL SWITCHING (MPLS)

II.2.3.1 Development Of MPLS

Multiprotocol label switching (MPLS) is a technique for speeding up network connections that was first developed in the 1990s. The public Internet functions by forwarding packets from one router to the next until the packets reach their destination. MLPS, on the other hand, sends packets along predetermined network paths. Ideally, the result is that routers spend less time deciding where to forward each packet, and packets take the same path every time. [19]

The Internet Engineering Task Force (IETF) and the ATM Forum specified several solutions to transport IP packets over Asynchronous Transfer Mode (ATM) networks, including Classical IP over ATM, LAN Emulation over ATM, and Multiprotocol over ATM. All of these followed a network overlay model where IP was put over ATM, and each of them retained their own control procedures. Concurrently, several vendors proposed alternative solutions that sought a tighter integration of IP and ATM in some cases, or simply to forward packets at very high speeds based on fixed-length labels à la ATM, but without cells. [19]

The Internet Engineering Task Force (IETF) MPLS working group was formed on 1997 and the first MPLS RFCs had its release on 2001. RFC 3031 specifies MPLS architecture and RFC 3032 specifies its label stack encoding. Label switching allows a device to do the same router operations with performance of ATM switch. ATM switches and label lookups are faster than a conventional IP routing.

The Multiprotocol Label Switching (MPLS) architecture, tandardized by the IETF in 2001 [3], follows this general approach. Packets labeled with MPLS can be encapsulated over different layer 2 protocols, including Ethernet, Point-to-Point Protocol (PPP), With advancement in packet switching, MPLS overcomes ATM setbacks with less overhead and connection-oriented services for frames with varying length. This also provides the advantage of maintaining traffic engineering and out-of-band control. Thus Frame Relay and ATM are less in need for installing large-scale networks, as MPLS performance is far superior to previous ones. [19]

II.2.3.2 Definition

Multiprotocol Label Switching (MPLS) is data forwarding technology that increases the speed and controls the flow of network traffic. With MPLS, data is directed through a path via labels instead of requiring complex lookups in a routing table at every stop, Scalable and protocol independent, this technique works with Internet Protocol (IP) .

When data enters a traditional IP network, it moves among network nodes based on long network addresses. With this method, each router on which a data packet lands must make its own decision, based on routing tables, about the packet’s next stop on the network. MPLS, on the other hand, assigns a label to each packet to send it along a predetermined path, the first router to receive a packet determines the packet's entire route upfront, the identity of which is quickly conveyed to subsequent routers using a label in the packet header.

Multi-Protocol Label Switching(MPLS) is a method of switching packets using labels instead of IP addresses or Layer 3 information. It is protocol-agnostic and speeds up packet forwarding and routing. Back when MPLS was first introduced, it showed a considerable boost in speed and took substantial load off networks by laying off IP address inspection. Today, MPLS is used not only to facilitate higher speed requirements but to develop advanced and augmented applications and services over the existing network infrastructure. [19]

II.2.3.3 MPLS Overview and Architecture

MPLS has the capacity to develop both Layer 2 and Layer 3 MPLS VPNs. Additional advantages of MPLS are traffic engineering, utilization of one unified network infrastructure, optimal traffic flow and, better IP over ATM integration. MPLS 4 is the innovation utilized by all Internet Service Providers (ISPs) in their core or backbone networks for packet forwarding.

Packets can move independently, from the network algorithms of Interior Gateway Protocol (IGP) protocols, using manually configured routes. Paths built up in a MPLS network are called Label Switched Path (LSP). Each MPLS enabled router is called Label Switching Router (LSR). Redirection is typically in view of the parcel header containing the numerical estimation of the label. An MPLS label switch path is one-way and is within a single autonomous system (Autonomous System - AS) or domain. Approaches to build up MPLS LSP are: [21]

- ✓ **Dynamically**: Dynamic LSP is built up automatically by the signalling protocol. Only the edge router (ingress router) is set up with the data required to establish paths.

- ✓ **Statically**: In this case, the administrator chooses how to forward the traffic, and what labels are utilized to distinguish resource distribution. Static LSPs expend less resources, do not require signalling protocol and don't need to store data about their state. The disadvantage is that it has to be done manually and errors may be done while configuring them. Additionally, a single device failure causes complete traffic loss. [21]

Any Label Switching Router (LSR) can handle the MPLS header and the actions associated. LSR can be of different types: input (ingress), intermediate (transit), penultimate (penultimate) or output (egress), as shown in (Figure 18)

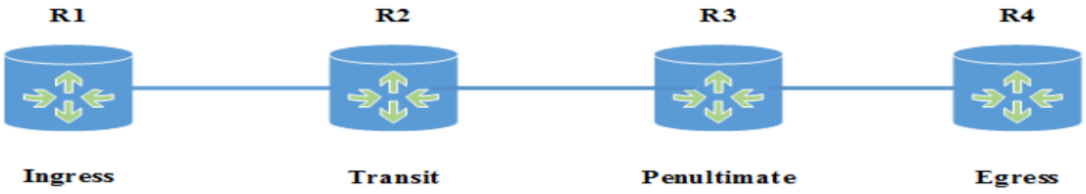


Figure 18: MPLS router types

II.2.3.3.1 Typical MPLS network [20] Figure 19

1. **In the LSR of type ingress** : the client IPv4 packet is encapsulated with an MPLS header. Packets are then forwarded to the egress router through the relating LSPs. Each LSP requires ingress router and just one router can be ingress for one LSP.

2.**The Transit LSR (intermediary router)** : is placed between the ingress LSR and the egress LSR. One path may contain from 0 to 253 such devices. Operations performed by the transit LSR include:

- ➢ Reading the value of the label of a received packet.
- ➢ Accessing the MPLS forwarding table to find the output for a given input label.
- ➢ Label switching is utilized to forward the input label to the output label.
- ➢ The value of the Time-To-Live (TTL) field is decremented.
- ➢ The packet is forwarded to the next router along the path.
- ➢ During this operation the data in the IP header is never utilized.

3.The penultimate LSR :is the last router before the egress LSR. Typically, its task is to remove the MPLS label from the data packet. This process is named penultimate hop popping. It supports network scalability and reduces the load on the egress router. Its tasks include:

- ➢ Determines the next and final router.
- ➢ Removes the stack of labels.
- ➢ Decreases the value of the TTL field by "1".
- ➢ Forwards the packet based on the label. [21]

4.The Egress LSR (output router) : is the definitive router for an LSP. It gets packets from the penultimate node and compares the IPv4 address with its routing table. Then redirects the packet to the next hop. Each LSP must have egress router and only one router can be egress for a given LSP . [21]

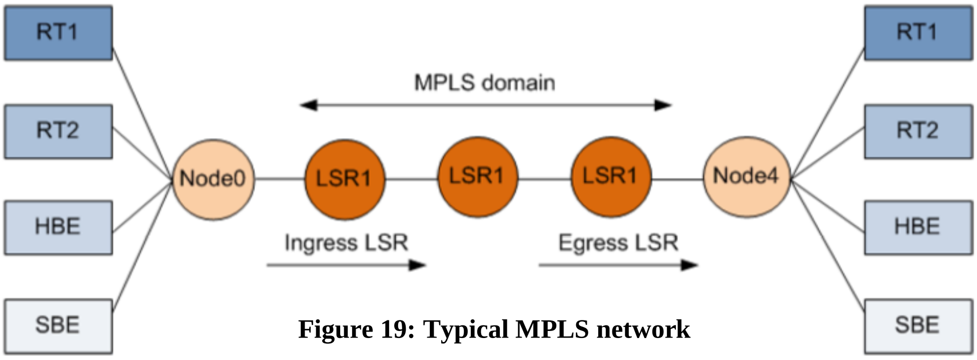


Figure 19: Typical MPLS network

Redirection of packets in MPLS backbone network depends on the labels that are set by the LSRs. The designation of the MPLS labels is done manually or automatically. Nodes exchange data about the compliance between the labels for the set up LSPs. An MPLS label is a short fixed length physically set up identifier. [21]

II.2.3.3.2 Virtual Private Network

A Virtual Private Network (VPN) is a technology that helps to create a private network across a public network (e.g., the Internet), collection of virtual links which logically interconnect the different network components over a physical network and also is a network in which information is transmitted using cryptographic and authentication algorithms. It is virtual since there is no real physical connection between the sites. A VPN uses shared public telecom infrastructure, such as the Internet, to provide secure access to remote offices and users in a cheaper way than an owned or leased line. The virtual private network is mainly used to establish connections between different corporate branches or remote activities when using less secure network lines. With the help of data encryption, a network inside the Internet, for example, can only be accessed by those who have the necessary addresses and passwords. [21]

One of the most capability of MPLS is to possibility to build Virtual Private Networks (VPNs). MPLS has the capability to construct both Layer 2 and Layer 3 MPLS VPNs. Both types of VPNs have their own merits and demerits. VPNs became popular during past two decades because of the evolution of related technologies. Primarily, the implementation cost of virtual networks had dropped drastically as a result of the availability of low-cost network equipment and communication systems .

II.2.3.3.3 MPLS Layer 2 VPNs

In this approach, the customer network and the service provider network are separated and no exchange of paths between the CE and PE routers is done. The division between the client and the service provider simplifies the implementation of the VPN. MPLS L2VPNs offer services to transport the layer-2 frames from one client site to another. This approach is completely transparent to the CE devices. Working with layer-2 frames allows the ISP to provide services that are independent from layer-3 protocols. Layer 2 VPNs requires not router equipment, and traffic is tagged with a MAC address instead of an IP address. Since it works at a lower layer, the latency is lower compared to a 6 layer 3 based solution. Also, it is easy to deploy since it does not require any specific configuration, like a device in a LAN. [19]

As a layer 2 protocol it also has some disadvantages. Layer 2 networks are susceptible to broadcast storms. Services are difficult to monitor since the service provider has no visibility.

II.2.3.3.4 MPLS Layer 3 VPN

A MPLS Layer 3 VPN contains a provider router, a provider edge router and a CE router. At each customer site, one or more CE routers connect to one or more PE routers. A client network is a combination of VPN sites at various geographical areas. Each VPN Site is associated with carrier networks through the CE router, and CE gets to PE by means of single or double connections and interconnects VPN sites at various areas by means of carrier networks. [19]

MPLS L3VPN can allocate different sites of a client to various VPNs to allocate one office to a few VPNs or isolate services for VPN shared to get to. Also, routing information from one customer is completely separated from other customers and tunnelled over the service provider MPLS network. MPLS L3VPN has strong client isolation flexibility to meet the prerequisites of various clients in flexible networking and service security. In the Layer 3, the service provider will be involved in routing with the customer. The customer will run appropriate IGP protocols, such as BGP, OSPF, EIGRP or any different routing protocol with the service provider .

Routing scenarios can sometimes be complex, however, an any-to-any topology where any customer device can connect directly to the L3 MPLS VPN it is the most common case. Data is encapsulated with MPLS labels to ensure proper tunnelling and de-multiplexing via the core and enterprise traffic .

MPLS Layer 3 VPN builds a peer-to-peer VPN with customer sites (See Figure 3). It forms Layer 3 relations with service provider routers. Labels are added to customer IP routes when they enter from Customer Edge (CE) routers to Provider Edge (PE) routers. All forwarding is finished utilizing label switching with MPLS within service provider network and labels are removed when sending traffic from Provider Edge to Customer Edge routers.

MPLS L3VPN utilizes GRE/IP tunnel and MPLS tunnel. A tunnel isolates a client route from a provider router. Provider router is just related to a public network route rather and not to a client router. Tunnel management is complex for GRE with a weak protocol support. An IP network not supporting MPLS can transport VPN service through a GRE/IP tunnel to avoid the upgrade to put a cost pressure on the whole network. [19]

II.2.3.4 ROUTING PROTOCOLS

There are many different ways to transmit data in networks, in this scenario I am going to design and implement a sample configuration base of a MPLS Layer 2 (for one customer) and Layer 3 (for two customers) VPN with three different protocols for each customer, namely Border Gateway Protocol (BGP), Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).The idea behind it to compare and analyse them together and see how they compare in terms of performance and configurability. [24]

II .2.3.4.1 Open Shortest Path First (OSPF)

It First routing protocol, always seeks the fastest route to reach its destination. Routers that are on an OSPF network will always check the status of other routers that they have access to and send messages to each other whenever necessary. [05] Using this mechanism, routers will understand the status of other routers in the network and understand whether a router is online. One of the features that OSPF offers to us is that routers, in addition to finding the fastest and closest route 10 to reach the destination, also notice all possible routes and routes for passing the packet from origin to destination. In such a case, there is the ability to implement Load Balancing on the routers so that information packets can be divided into different parts and shipped to different destinations on different routes. OSPF is commonly used in medium to medium sized networks and is commonly used in large networks for less frequent protocols. [24]

II.2.3.4.2 Border Gateway Protocol (BGP)

MPLS can be used to efficiently exchange routes using the Border Gateway Protocol (BGP). You can read more about BGP here. BGP can be deployed at the edge of a network with an MPLS core. MPLS provides end to end transport for BGP routes. The PEs in the provider network using MPLS BGP use the Multiprotocol-Border Gateway Protocol (MP-BGP) to dynamically communicate with each other. This MPLS BGP model enhances the efficiency and scalability of routing/forwarding features of the underlying network infrastructure. [05]

Is used in large networks. For example, Internet uses the BGP routing protocol. BGP can also be used for internal networks. BGP can also be used in an internal network, as a single autonomous system. The main differences between OSPF and BGP routing protocols are as follows

- BGP works on very large networks with more than one Autonomous System, while OSPF is an intermediate protocol.
- BGP is used on the Internet, but OSPF is on the internal network.
- BGP has more complexity than OSPF. [05]

was designed to allow routers, called gateways in the standard, in different autonomous systems (ASs) to cooperate in the exchange of routing information. The protocol operates in terms of messages, which are sent over TCP connections. The current version of BGP is known as BGP-4

Three functional procedures are involved in BGP:

- Neighbor acquisition
- Neighbor reachability
- Network reachability

(Figure 20) illustrates the formats of all of the BGP messages.

Each message begins with a 19-octet header containing three fields, as indicated by the shaded portion of each message in the figure: [05]

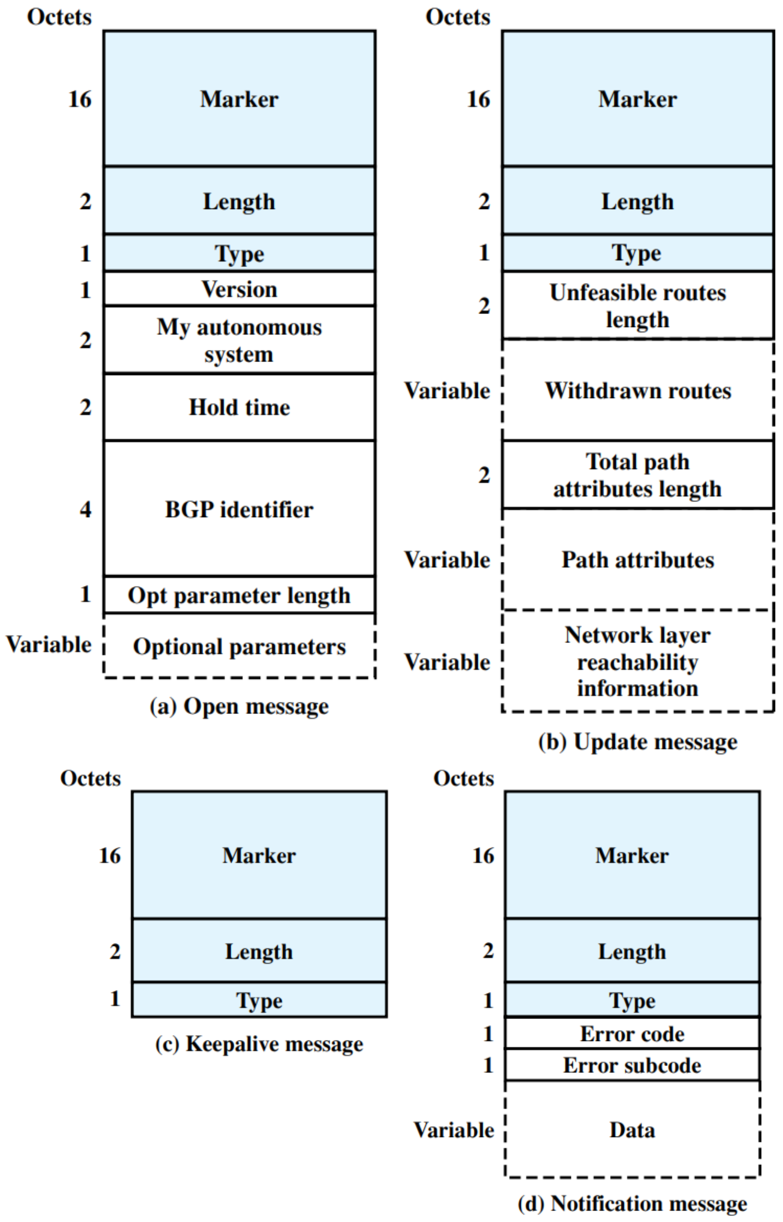


Figure 20: BGP Message Formats

- **Marker**: Reserved for authentication. The sender may insert a value in this field that would be used as part of an authentication mechanism to enable the recipient to verify the identity of the sender.
- **Length**: Length of message in octets.
- **Type**: **Type of message**: Open, Update, Notification, Keepalive. To acquire a neighbor, a router first opens a TCP connection to the neighbor router of interest. It then sends an Open message. This message identifies the AS to which the sender belongs and provides the IP address of the router. It also includes a Hold Time parameter, which indicates the number of seconds that the sender proposes for the value of the Hold Timer. If the recipient is prepared to open a neighbor relationship, it calculates a value of Hold Timer that is the minimum of its Hold Time and the Hold Time in the Open message. [05] This calculated value is the maximum

number of seconds that may elapse between the receipt of successive Keepalive and/or Update messages by the sender.

The Keepalive message consists simply of the header. Each router issues these messages to each of its peers often enough to prevent the Hold Timer from expiring.

The Update message communicates two types of information:

- Information about a single route through the internet. This information is available to be added to the database of any recipient router. [05]
- A list of routes previously advertised by this router that are being withdrawn.

II.2.3.4.3 The Routing Information Protocol (RIP)

The Routing Information Protocol (RIP) protocol is one of the oldest distance vector routing protocols that uses the hop count parameter as a metric. The RIP protocol exchanges information with its closest neighbours, which is a set of known purposes for participating routers. [33]

A RIP router broadcasts routing information to its directly connected networks every 30 seconds. It receives updates from neighboring RIP routers every 30 seconds and uses the information contained in these updates to maintain the routing table. If an update has not been received from a neighboring RIP router in 180 seconds, a RIP router assumes that the neighboring RIP router is down, sets all routes through that router to a metric of 16 (infinity), and stops using those routes when routing IP packets. If an update has still not been received from the neighboring RIP router after another 120 seconds, the RIP router deletes from the routing table all of the routes through that neighboring RIP router.

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520. [33]

You can use RIP to configure the hosts as part of a RIP network. This type of routing requires little maintenance and also automatically reconfigures routing tables when your network changes or network communication stops. RIPv2 was added to the IBM product so you can send and receive RIP packets to update routes throughout your network. [33]

II.2.3.4.3.1 Features of RIP

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbor routers. This is also known as Routing on rum ours. [33]

II.2.3.5 Network Topology

II.2.3.5.1 MPLS VPN

there are three P (Provider) routers and two PE (Provider Edge)routers (**Figure 21**). The IGP protocol is used in order to advertise their subnets to the Routers of the Core network between them (such as directly connected networks and Loopback IP addresses) is the OSPF (Open Shortest Path First). Next the MPLS protocol was activated in all the Core Routers of the network, where each router using the LDP protocol exchanges labels corresponding to each subnet. [18]

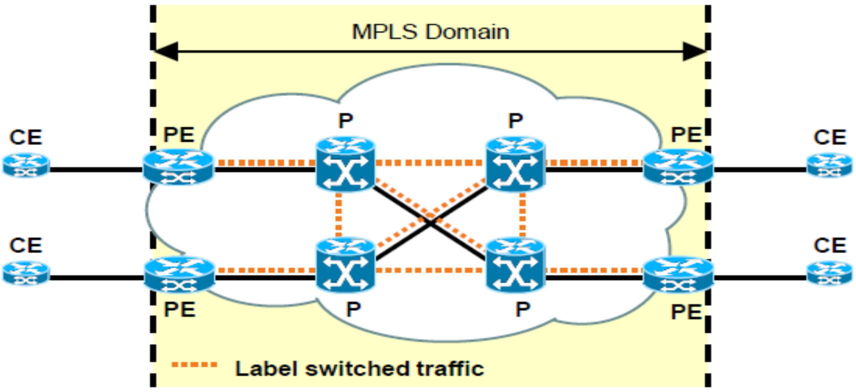


Figure 21: MPLS VPN

- **(P) -** (Provider) router - label switching router - core router (LSR) Switches MPLS-labeled packets
- **(PE)-** (Provider Edge) router = edge router (LSR) -Imposes and removes MPLS labels
- **(CE)-** (Customer Edge) router Connects customer network to MPLS network.

A typical MPLS VPN model consists of Provider Edge(PE) routers, Provider(P) routers, Customer Edge(CE) routers and Customer(C) routers. The PE and CE are directly connected at Layer 3. In the service provider's network, all PE and P routers run MPLS VPN as a service. They are equipped to send and receive packets with MPLS labels and take routing decisions accordingly. Therefore, routing and forwarding is carried out with the help of Label Switch Paths(LSPs). Customer networks run Layer 3 routing protocols internally. CE routers need not run MPLS. [18]

The CE from Customer Network 1 sends a packet to the provider network's ingress PE which adds two labels to the incoming packet.

1. VPN label - to specify corresponding egress PE router that is the packet receiver.
2. MPLS label - to route the packet using MPLS.

At every router hop in the LSP, the MPLS label is read and swapped with the next hop's MPLS label. The router that is second to last in the LSP pops the MPLS label off and forwards the packet to the intended egress PE based on the address enclosed in the VPN label.

The egress PE uses IP routing at Layer 3 to forward the packet to the CE router of Customer Network 2. [18]

It is vital that P routers in the provider network do not receive a packet with just the VPN label. They are not configured to handle such a packet, thereby resulting in its drop.

- There are six principal tasks to achieve an MPLS VPN up and running:

1. Enable MPLS on the provider backbone.
2. Create VRFs and assign routed interfaces to them.
3. Configure OSPF between the PE routers.
4. Configure OSPF between each PE router and its attached CE routers for Layer3.
5. Configure RIP between each PE router and its attached CE routers
for Layer2. [18]
6. Enable route redistribution between the customer sites and the backbone.

II.2.3.5.2 MPLS Label and Label Encapsulation

The MPLS layer (Figure 22) lies between layer 2 and 3 of the model in the Data Link and the Network Layer. That's why it is also known as 2.5 layer protocol or "shim" protocol.

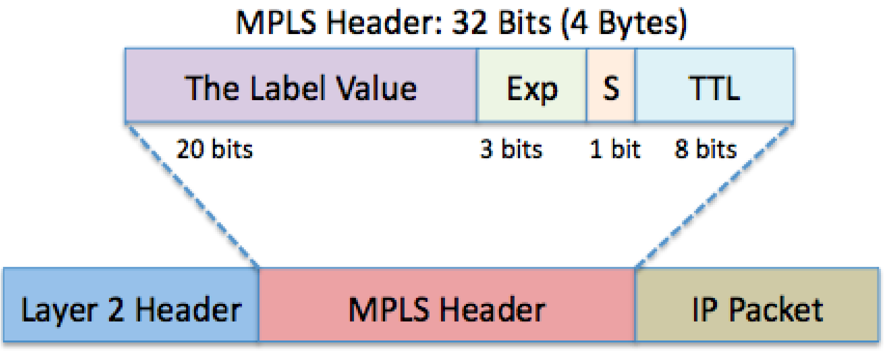


Figure 22: MPLS Label

The MPLS header is of 32 bits. It contains the following information: [31]

1. **Label**: The label field is of 20 bits, hence the label could take values from 0 to 2^20–1, or 1,048,575. However, the first 16 label values ie from 0 to 15 are exempted from normal use as they have a special meaning.

2. **Experimental(Exp):** The three bits are reserved as experimental bits. They are used for Quality of Service(QoS).

3. **Bottom of Stack(BoS):** A network packet can have more than one MPLS labels which are stacked one over another. To ensure which MPLS label is at the bottom of stack we have a BoS field which is of 1 bit. The bit is high (ie value 1) only when that particular label is at the bottom of the stack otherwise its value remains 0. [31]

4. **Time to Live (TTL):** The last 8 bits are used for Time to Live(TTL). This TTL has the same function as the TTL present in the IP header. Its value is simply decreased by 1 at each hop. The job of TTL is to avoid the packet being stuck in the network by discarding the packet if its value becomes zero. [31]

II.2.3.5.3 Basic MPLS Forwarding Operations

figure 23 show Labels are being used to establish End-to-End Connectivity

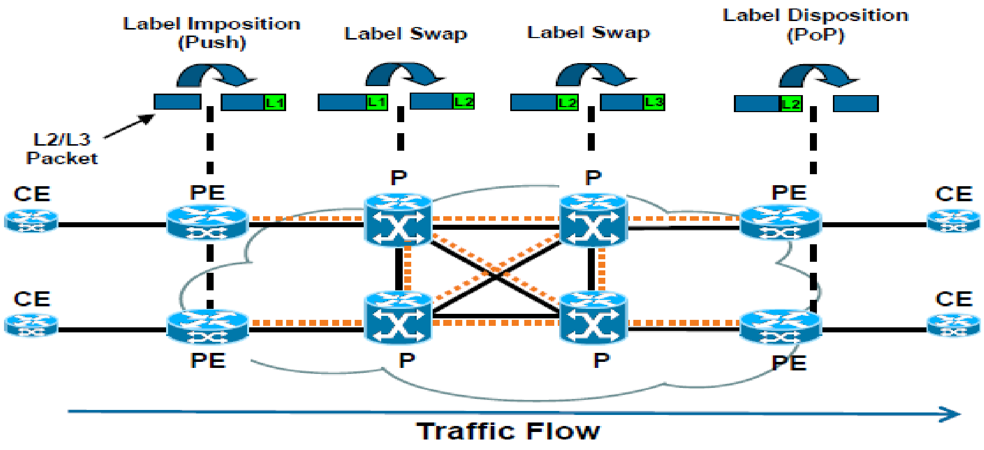


Figure 23: Basic MPLS Forwarding Operations

- ✓ **Label imposition (PUSH)**
  – By ingress PE router; classify and label packets.
  – Based on Forwarding Equivalence Class (FEC).
- ✓ **Label swapping or switching (SWAP)**
  – By P router; forward packets using labels; indicates service class & destination.
- ✓ **Label disposition (POP)**
  – By egress PE router; remove label and forward original packet to destination CE [22]

II.2.3.6 Quality of Service Assurance in MPLS

One of the most important features of the MPLS technology is that it can significantly improve network performance and increase the efficiency of quality of service (QoS) support mechanisms. MPLS offers multiple service classes, each associated with different types of traffic. The QoS assurance in MPLS networks is closely related to the usage of an MPLS label. RFC 3031 defines a label as “a short fixed length physically contiguous identifier which is used to identify a Forwarding Equivalence Class (FEC), usually of local significance.” The label makes possible to decouple routing from the forwarding paradigm. The label is an identifier assigned to a packet that tells the network where the packet should be sent. It is located at a header called the Shim header. The 32 bit long Shim header resides between the layer 2 and layer 3 headers. Besides the label itself it also contains other fields, like an experimental Exp field, the indicator of the bottom of the stack called S-bit and the Time to Live (TTL) field. The structure of the MPLS Shim header is shown in **Figure 24.** [31]

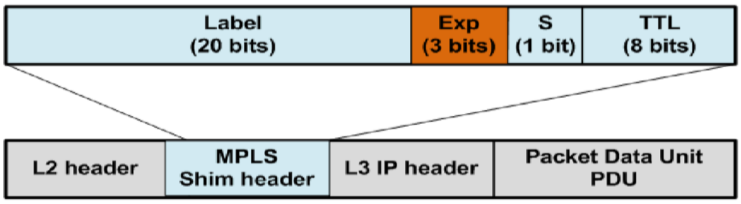


Figure 24: The structure of the MPLS Shim header

From the point of view of QoS assurance the 3-bit Exp field is especially important because in most MPLS implementations it is used to hold a QoS indicator. Often the copy of the IP precedence bits of the encapsulated IP packet is stored here. If the Exp bits are used to indicate the differentiated packet treatment than the LSP is called E-LSP indicating that the LSR will use these bits for packet scheduling and policing. [31]

II.2.3.6.1 Evaluation of QoS assurance in MPLS Network

Although the mechanism of Differentiated Services (DiffServ) is presently the most wide spread QoS support technology for IP-based networks the MPLS can be a preferable alternative in many data networks. In contrast to DiffServ MPLS also controls packet forwarding and due to this feature it is able to use different paths for distinguished traffic classes. There are various types of network services with different requirements on transmission parameters. [31] For example, MPLS can assign faster network path with lower delay to the real-time video flow and a more reliable path to the traffic-flows of classical data services. In this way the application requirements can be better satisfied. To evaluate the behaviour of the MPLS mechanism with QoS assurance a simulation model had been built in

Network Simulator version 2 (NS-2) environment. For this purpose the classical NS-2 environment was extended with the MPLS Network Simulator (MNS) tool and with additional modules for label switching, constraint based routing label distribution protocol (CR-LDP) and class- based queuing (CBQ) scheduling. [31]

II.2.3.7 Summary

MPLS provides a step-change improvement in the scalability and ease of provisioning of VPNs over IP networks. It also offers enhanced CoS support to allow SPs to offer differentiated service levels.

By leveraging these MPLS facilities, SPs can offer highly cost-effective and competitive VPN solutions to their customers and maximize bandwidth usage across the core network.

LSP tunnels provide the encapsulation mechanism for VPN traffic. Automatic methods for determining VPN routes allow the configuration complexity of an MPLS VPN to scale linearly (order(n)) with the number of sites in the VPN, as opposed to geometric (order(n2)) scaling for other IP-tunneling VPN solutions. Best scalability of peer discovery is achieved by overlaying the VPN peer and route discovery using a routing protocol or by use of a directory.

VPN traffic can be multiplexed onto common outer LSP tunnels in order that the number of tunnels scales according to the number of SP edge routers rather than the much larger number of VPN sites serviced by these routers. This avoids the scalability problems seen in some ATM or Frame Relay VPN solutions by reducing the problem to order(m) where m is the number of LSRs providing access to n VPN sites, and m n. Outer LSP tunnels can also be provisioned for different CoS ranges, allowing SPs to customize the way VPN traffic is treated in the network core to match the service levels they wish to make available to customers. This can be combined with bandwidth reservations for certain CoS ranges or particular dedicated LSP tunnels for a specific customer if required by their SLA.

In the short-term, RFC 2547 provides an efficient VPN implementation model. Longer-term, a Virtual Router (VR) based implementation is likely to provide easier management of very complex VPN topologies. In the interests of having a single implementation and management model, SPs may also come to use VRs for smaller VPNs despite its lack of efficiency in that case.

The benefits of using MPLS for VPNs will be magnified if SPs have a choice of interoperable multivendor equipment that supports the VPN solutions. Standardization efforts are under way in the IETF MPLS Working Group for the technologies required for such solutions. The main challenge over the coming months will be to whittle down the number of different possible approaches for VPN membership determination and VPN/CoS multiplexing to a few generally applicable solutions to maximize interoperability.

in the last chapter, we will take these results to be tested on field by simulating the three of them (FR, ATM and MPLS) on **GNS3** and tracking each one by itself on **WIRESHARK**.

CHAPTER 3
COMPARING AND EVALUATING IN ATM,FR,MPLS

III.COMPARING AND EVALUATING IN ATM,FR,MPLS

III.1 INTRODUCTION

We will realize the three solutions for the wide area network, namely ATM, FR and MPLS in order to compare these three techniques and thus find the best solution for the users and the operator. In order to find the best evaluation and performance in the practical side of this work, we will use virtual operating systems on the VM program as if it were for peripheral devices, which is "Windows 7" and "Windows Server 2008",and windows 8 we use Wireshark which gives us the capture results that were studied on the GNS3 simulation software.

We will conduct a practical study of these techniques using GNS3 simulator, which will give us the results and analyzes of a large-scale network application process as it is on the ground even though it is a virtual simulation of the network

III.2 Presentation of the simulator GNS3(The Graphical Network Simulator)

III.2.1 Introduction

The network engineers, administrators, and students had to build labs with physical hardware or rent time on a rack. Both options can be expensive and inconvenient, and they limit the network designs available to you. Software simulation programs such as RouterSim and Boson NetSim have been around for a long time, too, but these limited applications merely simulate the commands of Cisco IOS. Cisco Education does offer cheaper virtualized rack rental, based on Cisco IOS on Unix (IOU), but it allows you to practice on only specific preconfigured network configurations. It also requires that you have an active Internet connection to access the labs. Cisco also offers a product named Virtual Internet Routing Lab (VIRL) that's similar to GNS3, but it requires an annual fee, limits the number of objects you can use in your labs, and uses only simulated Cisco operating systems.

GNS3 is a cross-platform graphical network simulator that runs on Microsoft Windows, OS X, and Linux, and it's the collaborative effort of some super-talented, industrialstrength nerds—folks such as Christophe Fillot, Jeremy Grossmann, and Julien Duponchelle, just to name a few. Fillot is the creator of the MIPS processor emulation program (Dynamips) that allows you to run Cisco's router operating system, and Grossmann is the creator of GNS3. He took Dynamips and integrated it, along with other open source software, into an easy-to-use graphical user interface. Duponchelle assists with coding GNS3, and his contributions have helped to advance the software. GNS3 lets you design and test virtual networks on your PC, including (but not limited to) Cisco IOS, Juniper, MikroTik, Arista, and Vyatta networks, and it's commonly used by students who need hands-on experience with Cisco IOS routing and switching while studying for the Cisco Certified Network Associate (CCNA) and Cisco Certified Network Professional . [33]

III.2.2 Definition

GNS3 is a Graphical Network Simulator that allows emulation of complex networks. You may be familiar with VMWare or Virtual PC that are used to emulate various operating systems in a virtual environment. These programs allow you to run operating systems such as Windows XP or Ubuntu Linux in a virtual environment on your computer. GNS3 allows the same type of emulation using Cisco Internetwork Operating Systems. It allows you to run a Cisco IOS in a virtual environment on your computer. GNS3 is a graphical front end to a product called Dynagen. Dynamips is the core program that allows IOS emulation. Dynagen runs on top of Dynamips to create a more user friendly, text-based environment. A user may create network topologies using simple Windows ini-type files with Dynagen running on top of Dynamips. GNS3 takes this a step further by providing a graphical environment.

III.2.3 Characteristics Of GNS3

GNS3 does not take the place of a real router, but is meant to be a tool for learning and testing in a lab environment. GNS3 allows the emulation of Cisco IOSs on your Windows or Linux based computer. Emulation is possible for a long list of router platforms and PIX firewalls. Using an EtherSwitch card in a router, switching platforms may also be emulated to the degree of the card's supported functionality. This means that GNS3 is an invaluable tool for preparing for Cisco certifications such as CCNA and CCNP.In addition, GNS3 is an open source, free program for you to use. However, due to licensing restrictions, you will have to provide your own Cisco IOSs to use with GNS3. Also, GNS3 will provide around 1,000 packets per second throughput in a virtual environment. A normal router will provide a hundred to a thousand times greater throughput. [33]

III.2.4 installation GNS3

The requirements for running GNS3 are largely determined by the operating system you're installing on, the model and number of routers you want to use in your projects, and whether you integrate external programs like VMware ,QEMU or VirtualBox into your designs. Most computers purchased in the last few years should be able to run this base installation without a hitch. That said, if you decide to move beyond creating projects using only Cisco routers and incorporate other virtual environments into your GNS3 designs (such as Linux, BSD, ASA, IDS, or Juniper), you'll want as much horsepower as you can get your hands on. The more memory and processing power you have, the better everything will run because programs like QEMU and VirtualBox require RAM to run their guest operating systems, and they compete with your native operating system for CPU time. You'll also need additional disk space to store your guest operating systems. You can visit the GNS3 website to verify the requirements for your operating system, but a good rule of thumb for a simple base install is the following:

It's a whole new way to learn networking. In this chapter, I'll guide you through the process of installing a basic GNS3 system on Microsoft Windows or Mac OS X, or Ubuntu Linux.

A basic installation consists of the GNS3 application and a few helper applications , all prerequisite applications come bundled in the GNS3 installer package, which is available from the GNS3 website (http://www.gns3.com/). When installing on Microsoft Windows or Mac OS X, or Ubuntu Linux , you can download and install GNS3 through a platform-specific package manager or directly from source code. The principles used for installing from source code can be applied to about any. [33]

III.2.4.1 Follow these steps to install GNS3 on Windows:

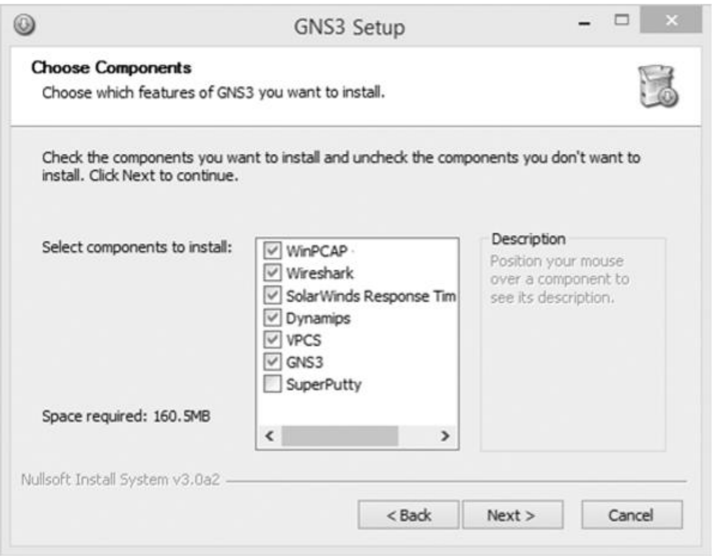
1. Download the GNS3 all-in-one installer from the GNS3 website (http://www.gns3.com/) and launch it to begin installation.

2. Click Next on the Setup Wizard screen, and click I Agree on the License Agreement screen.

3. Select the folder where you want the installer to place a shortcut to the application on the Start Menu, and then click Next. (The default folder is GNS3.)

4. You can then choose the components to include in your installation, as shown in Figure 34.

The default option installs all components to create a fully functional GNS3 system, including Wireshark, VPCS, and QEMU. To save disk space, or if you don't need these added features, uncheck those options. WinPCAP is required for NIO Ethernet cloud connections, and Dynamips is required to create projects using Cisco routers and switches. Make your selections and then click Next. [33]



GNS3 Setup

Choose Components

Choose which features of GNS3 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ WinPCAP
☑ Wireshark
☑ SolarWinds Response Tim
☑ Dynamips
☑ VPCS
☑ GNS3
☐ SuperPutty

Description

Position your mouse over a component to see its description.

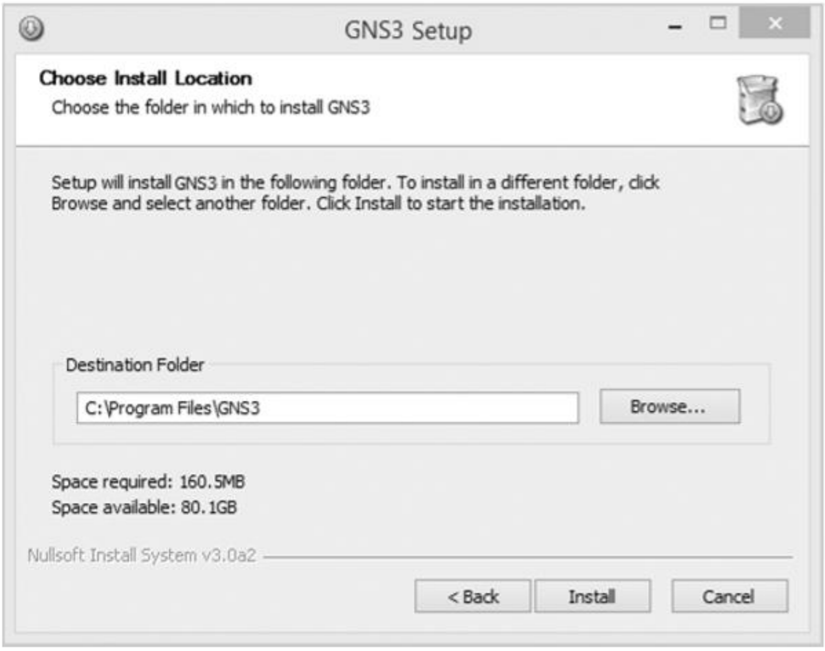
Space required: 160.5MB

Nullsoft Install System v3.0a2

Figure 34: Choosing the GNS3 components to install

5. You should see the Choose Install Location screen, as shown in Figure 35. To install GNS3 to an alternative location, enter the new location in the Destination Folder field and click Install.

6. Continue following all the prompts to complete the installation. I recommend you accept all default settings. [33]



Choose Install Location

Choose the folder in which to install GNS3

Setup will install GNS3 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder

C:\Program Files\GNS3

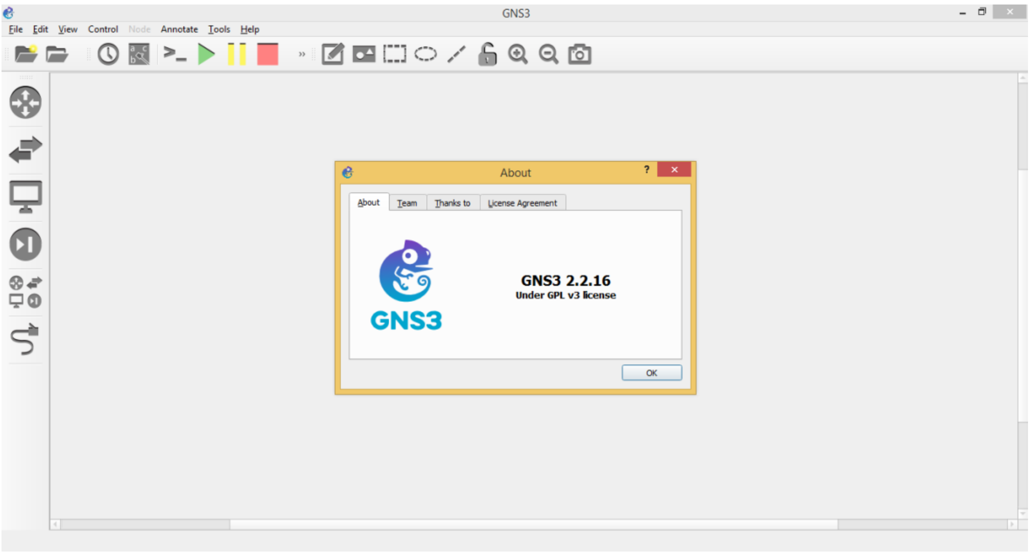
Space required: 160.5MB

Space available: 80.1GB

Nullsoft Install System v3.0a2

Figure 35: Choosing the destination folder location

- Upon completion, GNS3 should place an icon on your desktop


GNS3
File Edit View Control Node Annotate Tools Help
About
About Team Thanks to License Agreement
GNS3
OK

GNS3 2.2.16

Under GPL v3 license

Figure 36: GNS3 an icon on desktop

III 2.4.2 Installing On Ubuntu Linux

GNS3 runs well on many different Linux distributions, but there's an unfortunate lack of documentation for most of them. In this section, I'll strip away the mystery and show you how simple it is to get GNS3 running on a Unixbased platform. I've chosen to cover Ubuntu because it's one of the most commonly used distributions. There are two ways to install GNS3 on Linux. You can install a bundled package through your package manager or you can install from source code. Using a packaged install is quick and easy, but the downside is that you're stuck with whatever version of GNS3 has been ported to your specific platform, which may not be the latest version. [33] This is where a source install comes in handy.

Installing from source requires only a few extra steps and provides you with the latest version of GNS3. Even though I highly recommend installing from source code, we'll cover both methods here.

Installing GNS3 from Packages To install GNS3 using the Advanced Package Tools, open the terminal program and enter the following command: [33]

```
$ sudo apt-get install gns3
```

When prompted, enter your password. The output from this command displays a list of packages that will be installed and shows how much disk space will be used by the installation. The installer prompts you to confirm that this is okay before proceeding. When confirmed, the packages are installed and GNS3 is ready to run. You can start the application from the terminal program by entering gns3 or launching GNS3 from your display manager's application menu. You're now ready to configure GNS3. [33]

Installing GNS3 from Source Code Installing from source code ensures that you get the latest version of GNS3 and is, in my opinion, the best way to install GNS3 on Unix-based systems. No matter which version of Linux you're using, you should be able to use these instructions as a guide to get GNS3 up and running on your system. In the following example, I'll use Ubuntu Linux as a framework, but keep in mind that these instructions can be applied to just about any Unix-based distribution. The primary difference between distributions is the dependencies that are required and how you install them. Be sure to check the GNS3 website for the latest dependency requirements. I've installed GNS3 on Solaris, FreeBSD, OpenBSD, Ubuntu, Mint, OpenSUSE, Fedora, Fuduntu, Debian, Arch, Gentoo, Kali, Netrunner, and PCLinuxOS, so I'm sure you can run it on your system, too! Download and unzip the installation files from the GNS3 website (http://www.gns3.com/).[33]

III.2.5 GNS3 Appliances

An alternative to installing GNS3 on your PC is to use a preconfigured GNS3 appliance. A GNS3 appliance is simply a virtual machine that comes with GNS3 already installed. GNS3 appliances are extremely flexible because they run using an application like VirtualBox or VMware. they are free and runs on most operating systems (including Windows, OS X, Linux, and FreeBSD). [33]

III.3 Wireshark

III.3.1 Definition Of Wireshark

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level and is the de facto standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998. [33]

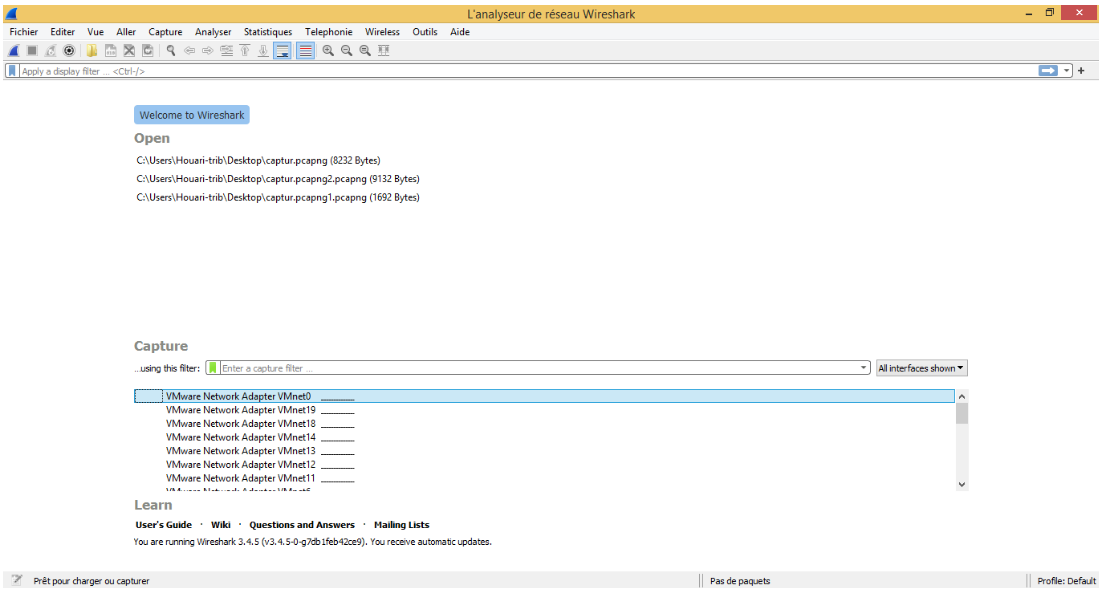
III.3.2 Characteristics Of Wireshark

It is an open source network packet analyzer tool that captures data packets flowing over the wire (network) and presents them in an understandable form. as it can be used under different circumstances such as network troubleshoot, security operations, and learning protocol internals. This one tool does it all with ease, Some of the important benefits of working with Wireshark are: [33]

- Multiple protocol support: Wireshark supports a wide range of protocols ranging from TCP, UDP, and HTTP to advanced protocols such as AppleTalk.

- User friendly interface: Wireshark has an interactive graphical interface that helps in analyzing the packet capture. It also has several advance options such as filtering the packets, exporting packets, and name resolution. [33]

- Live traffic analysis: Wireshark can capture live data flowing on the wire and quickly.



C:\Users\Houari-trib\Desktop\captur.pcapng (8232 Bytes)
C:\Users\Houari-trib\Desktop\captur.pcapng2.pcapng (9132 Bytes)
C:\Users\Houari-trib\Desktop\captur.pcapng1.pcapng (1692 Bytes)

VMware Network Adapter VMnet0
VMware Network Adapter VMnet19
VMware Network Adapter VMnet18
VMware Network Adapter VMnet14
VMware Network Adapter VMnet13
VMware Network Adapter VMnet12
VMware Network Adapter VMnet11

You are running Wireshark 3.4.5 (v3.4.5-0-g7db1feb42ce9). You receive automatic updates.

Prêt pour charger ou capturer | Pas de paquets | Profile: Default

Figure 37:Wireshark Interface

III.4 Equipment used to study this technology

To configure FR, ATM and MPLS in the WAN network using GNS3, we must provide a set of means such as Router, Switch, and computers, and we link them in a LAN and then connect them with each other over a wide area network using the aforementioned technologies and then we analyze and We evaluate the packet that we send from point A to point B and determine the transmission time that it took for this packet to connect through all the routers for each technology, and we compare between them.

III.5 CONFIGURATION FOR (FR, ATM,MPLS) Using GNS3

III.5.1 The Frame Relay extended network solution

III.5.1.1 The Network Topology

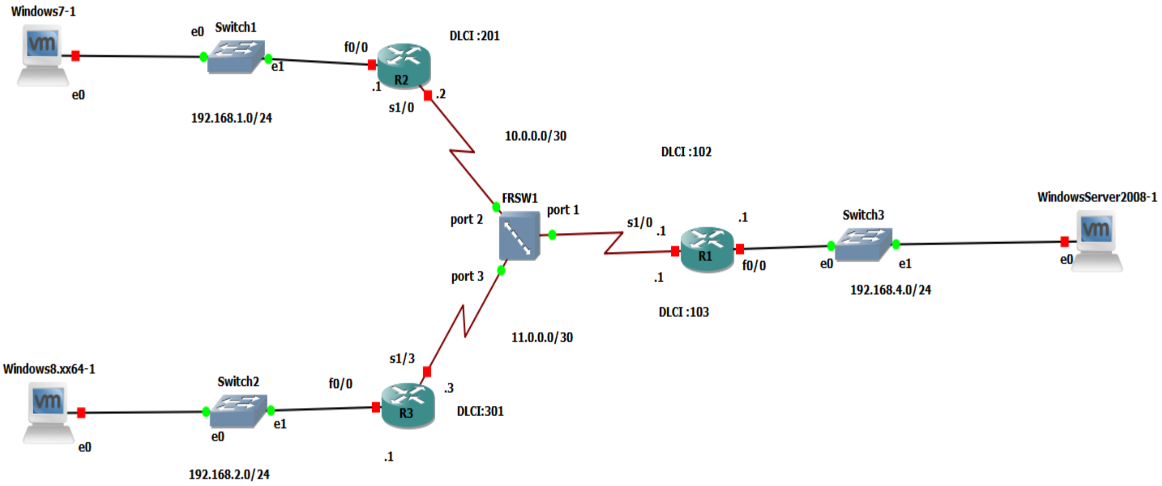


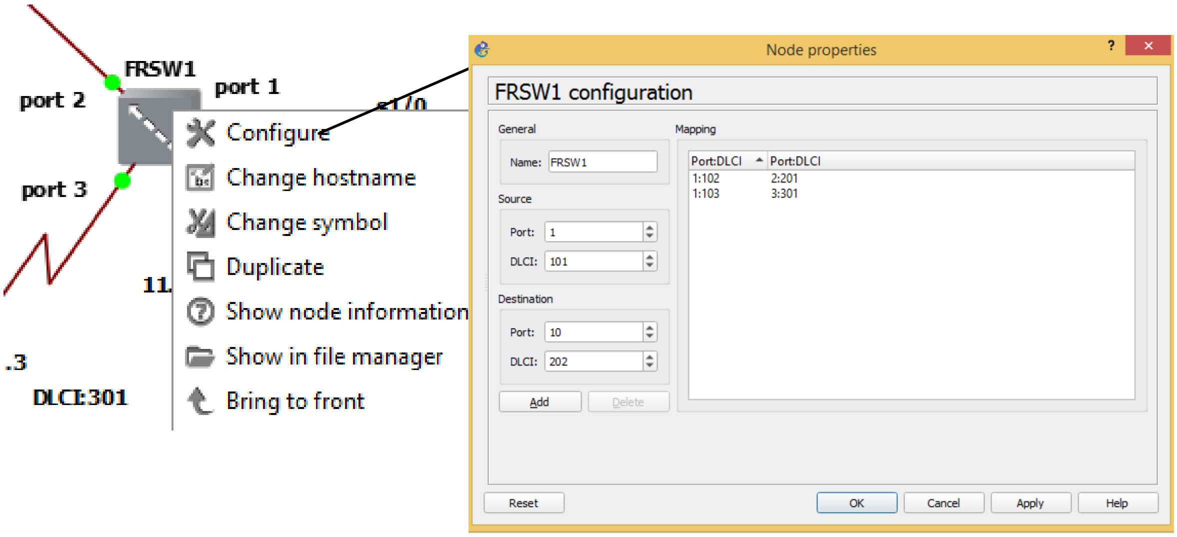
Figure 38:Network Topology Frame Relay

III.5.1.2 The router and Frame-relay Switching Configuration

III.5.1.2.1 basic configuration of Frame-relay Switching

Configure. The selected devices display in (FRSW) the Node properties, in Frame Relay, data link connection identifiers (DLCIs) are used to assign frames to a permanent virtual circuit (PVC) using serial port connections. To configure DLCI to serial port mappings, right-click the Frame Relay switch icon and open the Node configurator. Use the Source and Destination fields to create a mapping and click Add. When you're finished, click Apply and OK to complete the configuration, as shown in Figure 39.

in port 1: DLCI:102-port 1: DLCI:103-port 2: DLCI:201-port 3: DLCI:301



FRSW1 configuration

General

Name: FRSW1

Source

Port: 1

DLCI: 101

Destination

Port: 10

DLCI: 202

Mapping

Port:DLCI	Port:DLCI
1:102	2:201
1:103	3:301

Figure 39: Modifying multiple devices Frame-relay

III.5.1.2The Routers Configuration

```
R1#conf terminal
R1(config)#interface serial 1/0
R1(config-if)#encapsulation frame-relay
R1(config-if)#exit
R1(config)#interface serial 1/0.1 point-to-point
R1(config-subif)#ip address 10.0.0.1 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 102
R1(config-subif)#interface s1/0.103 point-to-point
R1(config-subif)#ip address 11.0.0.1 255.255.255.252
R1(config-subif)#frame-relay interface-dlci 103
R1(config-subif)#end
R1#conf terminal
R1(config)#int s1/0
R1(config-if)#no shut
R1(config-if)#do copy r s
                    configuration OPSF
R1(config)#router ospf 1
R1(config-router)#network 192.168.1.0 0.0.0.255 area 0
R1(config-router)#network 10.0.0.0 0.0.0.3 area 0
R1(config-router)#do copy r s
                configuration interface s0/0
R1(config)#int f0/0
R1(config-if)#ip add 192.168.4.1 255.255.255.0
R1(config-if)#no shut
R1(config-if)#
R1(config-if)#do copy r s

R3#conf t
R3(config)#int s1/3
R3(config-if)#encapsulation frame-relay
R3(config-if)#ip add 11.0.0.3 255.255.255.252
Bad mask /30 for address 11.0.0.3
R3(config-if)#frame-relay interface-dlci 301
R3(config-fr-dlci)#no shut
R3(config-if)#do copy r s
                        configuration OPSF
R3(config)#router ospf 1
R3(config-router)#network 192.168.2.0 0.0.0.255 area 0
R3(config-router)#network 11.0.0.0 0.0.0.3 area 0
R3(config-router)#do copy r s
                       configuration inteface
R3(config)#int f0/0
R3(config-if)#ip add 192.168.1.1 255.255.255.0
R3(config-if)#no shut
R3(config-if)# do copy r s
```

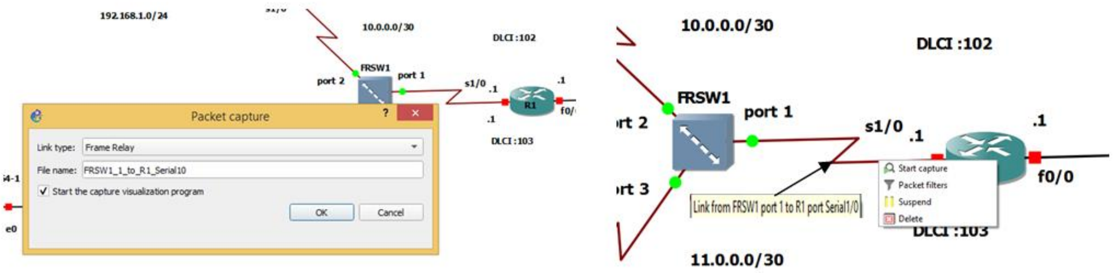
```
R2#conf t
R2(config)#
R2(config)#int s1/0
R2(config-if)#encapsulation frame-relay
R2(config-if)#ip add 10.0.0.2 255.255.255.252
R2(config-if)#frame-relay interface-dlci 201
R2(config-fr-dlci)#no shut
R2(config-if)#do copy r s
                    configuration OPSF
R2#conf t
R2(config)#router ospf 1
R2(config-router)#network 192.168.4.0 0.0.0.255 area 0
R2(config-router)#network 10.0.0.0 0.0.0.3 area 0
R2(config-router)#network 11.0.0.0 0.0.0.3 area 0
R2(config-router)#do copy r s
                  configuration interface
R2(config)#int f0/1
R2(config-if)#ip add 192.168.1.1 255.255.255.0
R2(config-if)#no shut
R2(config-if)#do copy r s
```

III.5.1.2.3 Testing Configuration

```
R2#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/50/96 ms
R2#ping 11.0.0.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 11.0.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/71/96 ms
R1#ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/31/48 ms
R3#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/38/76 ms
```

III.3.1.3.1 Result 1: Use of the network Frame-relay

Figure 40 shows us how to capture analysis in Frame Relay technology, using Wireshark. We right-click on the line linking the Frame Relay switch and the router of the head-company that uses Frame Relay technology and is connected to the second branch, then we click on start capture And upon completion, the following figure 41 shows us the process of packet transmission.



Link type: Frame Relay

File name: FRSW1_1_to_R1_Serial10

☑ Start the capture visualization program

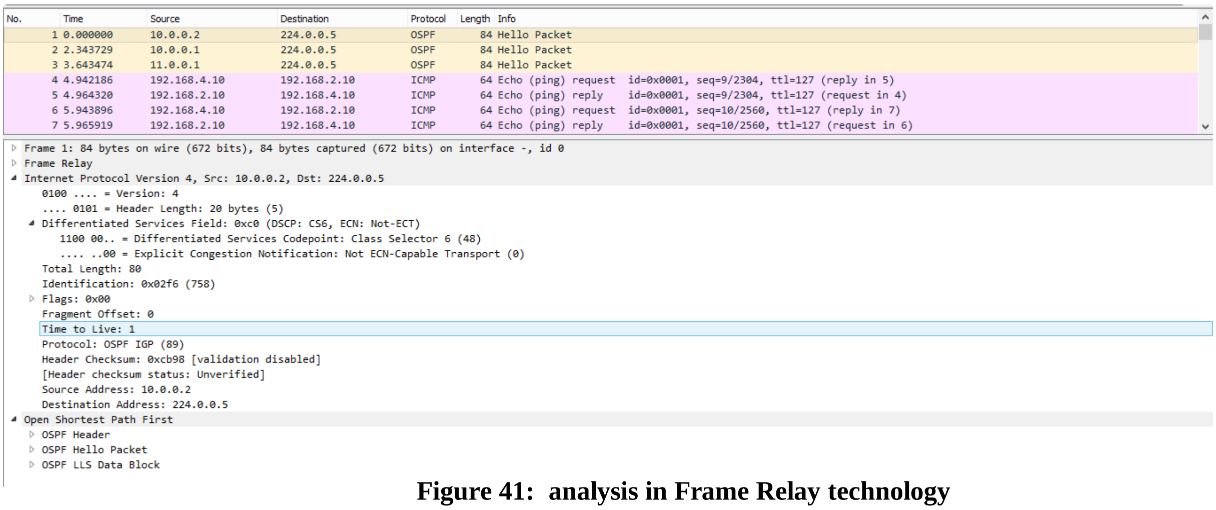
Link from FRSW1 port 1 to R1 port Serial1/0

Figure 40: capture analysis in Frame

III.3.1.3.2 The result of this sensor is :

This simple network is an example of a Frame Relay hub and topology and should give you a good idea of how DLCI mapping works in a Frame Relay network.

In this application side, I will ping from the server that has the address 192.168.4.10 located in the headquarter to the second branch that has the address 192.168.2.10. I will also send a packet and do a capture using Wireshark, and we get the following results shown in the two figures:

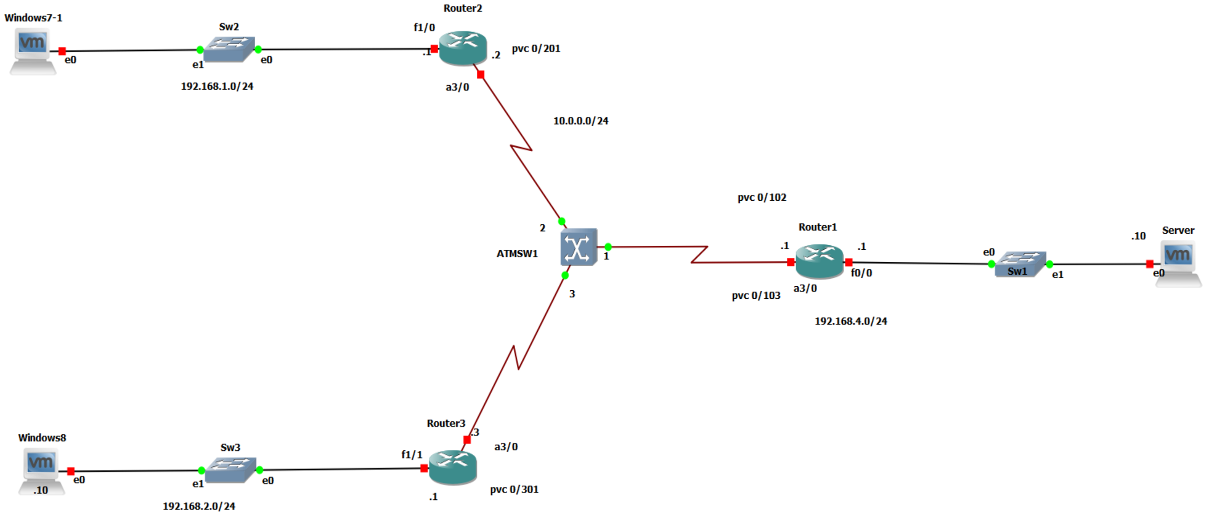


```
No.  Time        Source          Destination     Protocol  Length Info
   1 0.000000    10.0.0.2        224.0.0.5       OSPF        84 Hello Packet
   2 2.343729    10.0.0.1        224.0.0.5       OSPF        84 Hello Packet
   3 3.643474    11.0.0.1        224.0.0.5       OSPF        84 Hello Packet
   4 4.942186    192.168.4.10    192.168.2.10    ICMP        64 Echo (ping) request  id=0x0001, seq=9/2304, ttl=127 (reply in 5)
   5 4.964320    192.168.2.10    192.168.4.10    ICMP        64 Echo (ping) reply    id=0x0001, seq=9/2304, ttl=127 (request in 4)
   6 5.943896    192.168.4.10    192.168.2.10    ICMP        64 Echo (ping) request  id=0x0001, seq=10/2560, ttl=127 (reply in 7)
   7 5.965919    192.168.2.10    192.168.4.10    ICMP        64 Echo (ping) reply    id=0x0001, seq=10/2560, ttl=127 (request in 6)

▷ Frame 1: 84 bytes on wire (672 bits), 84 bytes captured (672 bits) on interface -, id 0
▷ Frame Relay
◢ Internet Protocol Version 4, Src: 10.0.0.2, Dst: 224.0.0.5
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ◢ Differentiated Services Field: 0xc0 (DSCP: CS6, ECN: Not-ECT)
      1100 00.. = Differentiated Services Codepoint: Class Selector 6 (48)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 80
    Identification: 0x02f6 (758)
  ▷ Flags: 0x00
    Fragment Offset: 0
    Time to Live: 1
    Protocol: OSPF IGP (89)
    Header Checksum: 0xcb98 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.0.0.2
    Destination Address: 224.0.0.5
◢ Open Shortest Path First
  ▷ OSPF Header
  ▷ OSPF Hello Packet
  ▷ OSPF LLS Data Block
```

Figure 41: analysis in Frame Relay technology

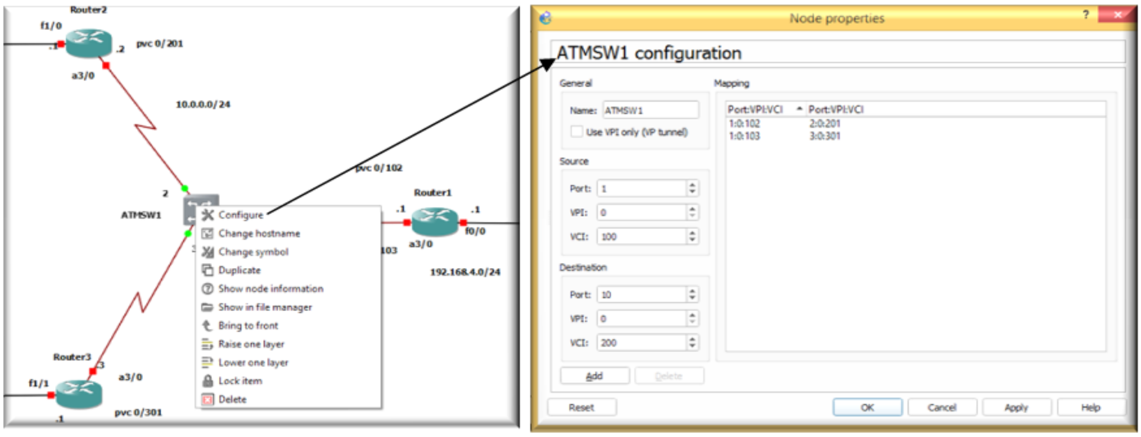
III.5.2 The ATM extended network configuration

III.5.2.1 The Network Topology



III.5.2.2 The router and ATM Configuration

III.5.2.2.1 basic configuration of ATM



ATMSW1 configuration

General

Name: ATMSW1

□ Use VPI only (VP tunnel)

Source

Port: 1

VPI: 0

VCI: 100

Destination

Port: 10

VPI: 0

VCI: 200

Mapping

Port:VPI:VCI	Port:VPI:VCI
1:0:102	2:0:201
1:0:103	3:0:301

Figure 43: Modifying ATM

III.3.2.2.2 basic configuration The Routers

Router (R1)

```
Router1(config)#interface a3/0
Router1(config-if)#no shutdown
Router1(config-if)#interface a3/0.1 multipoint
Router1(config-subif)#ip address 10.0.0.1 255.255.255.0
Router1(config-subif)#pvc 0/102
Router1(config-if-atm-vc)#encapsulation aal5snap
Router1(config-if-atm-vc)#protocol ip 10.0.0.2 broadcast
Router1(config-if-atm-vc)#exit
Router1(config-subif)#pvc 0/103
Router1(config-if-atm-vc)#encapsulation aal5snap
Router1(config-if-atm-vc)#protocol ip 10.0.0.3 broadcast
Router1(config-if-atm-vc)#exit
Router1(config-subif)#exit
Router1(config)#do copy r s
Router1(config)#interface fa0/0
Router1(config-if)#ip address 192.168.4.1 255.255.255.0
Router1(config-if)#no shutdown
Router1(config-if)#exit
Router1(config)#do copy r s
Router1(config)#router rip
Router1(config-router)#version 2
Router1(config-router)#network 192.168.4.0
Router1(config-router)#network 10.0.0.0
Router1(config-router)#no aut
Router1(config-router)#no auto-summary
Router1(config-router)#do copy r s
```

Router (R2)

```
Router2#conf t
Router2(config)#interface a3/0
Router2(config-if)#no shutdown
Router2(config-if)#exit
Router2(config)#interface a3/0.1 point-to-point
Router2(config-subif)#ip address 10.0.0.2 255.255.255.0
Router2(config-subif)#pvc 0/201
Router2(config-if-atm-vc)#encapsulation aal5snap
Router2(config-if-atm-vc)#exit
Router2(config-subif)#do copy r s
Router2(config)#interface f1/0
Router2(config-if)#ip address 192.168.2.1 255.255.255.0
Router2(config-if)#no shutdown
Router2(config-if)#Do copy r s
Router2(config)#router rip
Router2(config-router)#version 2
Router2(config-router)#network 192.168.1.0
Router2(config-router)#network 10.0.0.0
Router2(config-router)#no auto-summary
Router2(config-router)#do copy r s
```

Router (R3)

```
Router3#conf t
Router3(config)#interface a3/0.1 point-to-point
Router3(config-subif)#ip address 10.0.0.3 255.255.255.0
Router3(config-subif)#pvc 0/301
Router3(config-if-atm-vc)#encapsulation aal5snap
Router3(config-if-atm-vc)#end
Router3#conf t
Router3(config)#interface fa1/1
Router3(config-if)#ip address 192.168.2.1 255.255.255.0
Router3(config-if)#no shutdown
Router3(config-if)#do copy r s
Router3(config-if)#end
Router3(config)#conf t
Router3(config)#router rip
Router3(config-router)#version 2
Router3(config-router)#network 192.168.2.0
Router3(config-router)#network 10.0.0.0
Router3(config-router)#no auto-summary
Router3(config-router)#do copy r s
```

III.5.2.2.3 The Testing Configuration

a- Router (2) To Router1 (10.0.0.1) - Router 3 (10.0.0.3)

```
Router2#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!!
```

Success rate is 100 percent (5/5), round-trip min/avg/max = 60/96/144 ms

Router2#ping 10.0.0.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 92/103/140 ms

b- Router 1 To ip R1(10.0.0.2) - ip R3(10.0.0.3)

Router1#ping 10.0.0.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/32/72 ms

Router1#ping 10.0.0.3

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.3, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/32/96 ms

c- Router 3 To ip R1 (10.0.0.1) - ip R2(10.0.0.2)

Router3#ping 10.0.0.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 8/13/32 ms

Router3#ping 10.0.0.2

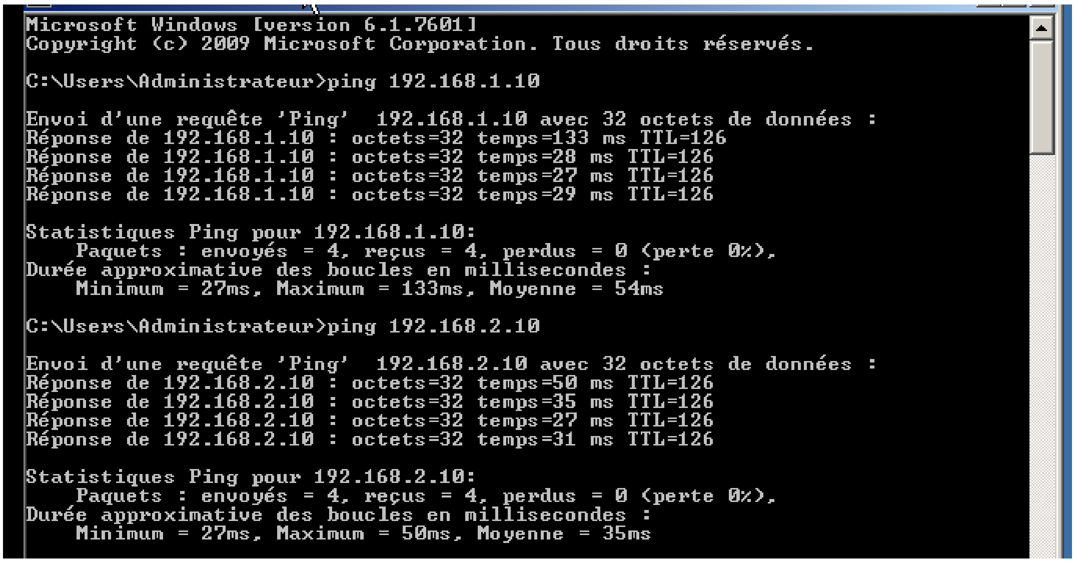
Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 36/40/48 ms

c-Server To ping 192.168.1.10 and ping 192.168.2.10

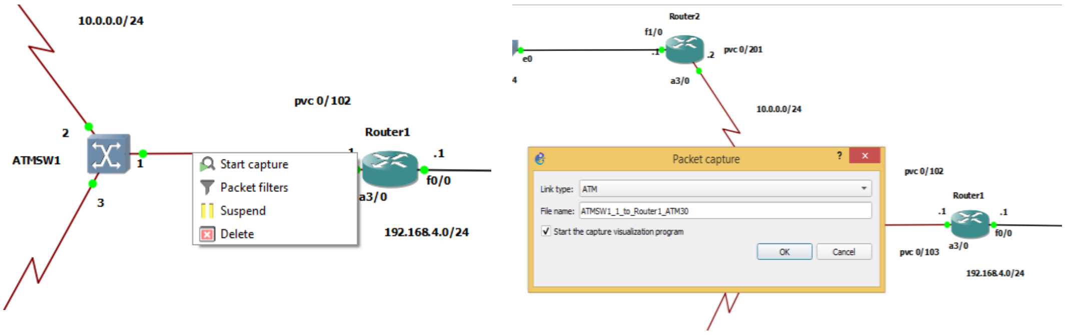


```
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping 192.168.1.10

Envoi d'une requête 'Ping'  192.168.1.10 avec 32 octets de données :
Réponse de 192.168.1.10 : octets=32 temps=133 ms TTL=126
Réponse de 192.168.1.10 : octets=32 temps=28 ms TTL=126
Réponse de 192.168.1.10 : octets=32 temps=27 ms TTL=126
Réponse de 192.168.1.10 : octets=32 temps=29 ms TTL=126

Statistiques Ping pour 192.168.1.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 27ms, Maximum = 133ms, Moyenne = 54ms

C:\Users\Administrateur>ping 192.168.2.10

Envoi d'une requête 'Ping'  192.168.2.10 avec 32 octets de données :
Réponse de 192.168.2.10 : octets=32 temps=50 ms TTL=126
Réponse de 192.168.2.10 : octets=32 temps=35 ms TTL=126
Réponse de 192.168.2.10 : octets=32 temps=27 ms TTL=126
Réponse de 192.168.2.10 : octets=32 temps=31 ms TTL=126

Statistiques Ping pour 192.168.2.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 27ms, Maximum = 50ms, Moyenne = 35ms
```

Figure 44:ping -testing

III.5.2.2.4 Result 2: Use of the ATM network

For an ATM, we have Figure 45 which shows us how to pick up the packet from a HQ and three branches, we send a packet from HQ to its second branch, and then I pick up the packet on Wireshark link a3 / 0 of Router 1 directly.



Link type: ATM

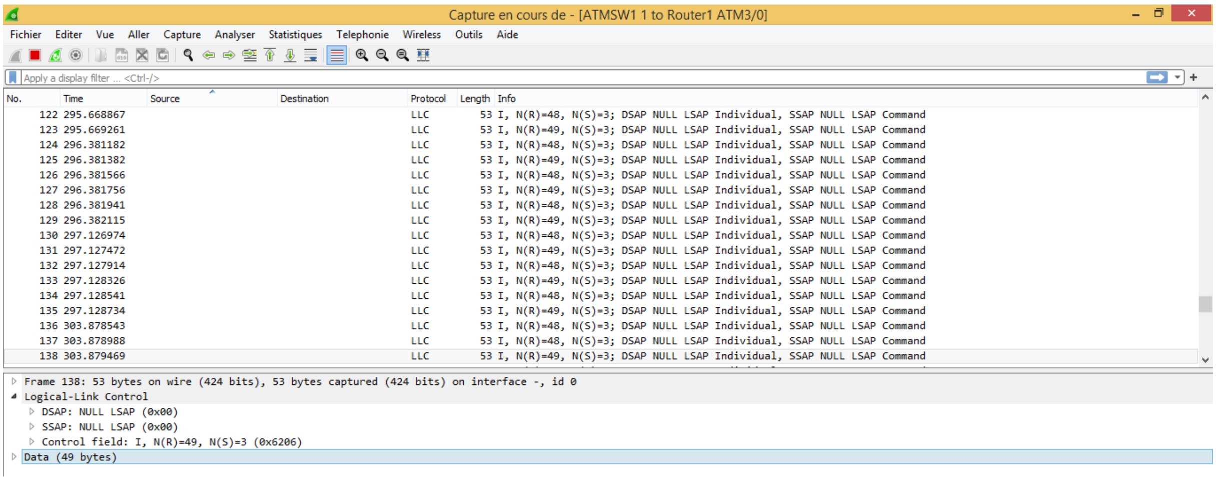
File name: ATMSW1_1_to_Router1_ATM30

☑ Start the capture visualization program

Figure 45: capture ATM network

The result of this sensor is:

I was unable to catch the packet transfer from the headquarters to the second branch and see the reason for this is that Wireshark is not compatible with ATM and the figure 46 below shows that .


Capture en cours de - [ATMSW1 1 to Router1 ATM3/0]
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide
Apply a display filter ... <Ctrl-/>

```
No.     Time        Source        Destination        Protocol  Length  Info
    122 295.668867                                   LLC        53 I, N(R)=48, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    123 295.669261                                   LLC        53 I, N(R)=49, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    124 296.381182                                   LLC        53 I, N(R)=48, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    125 296.381382                                   LLC        53 I, N(R)=49, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    126 296.381566                                   LLC        53 I, N(R)=48, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    127 296.381756                                   LLC        53 I, N(R)=49, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    128 296.381941                                   LLC        53 I, N(R)=48, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    129 296.382115                                   LLC        53 I, N(R)=49, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    130 297.126974                                   LLC        53 I, N(R)=48, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    131 297.127472                                   LLC        53 I, N(R)=49, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    132 297.127914                                   LLC        53 I, N(R)=48, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    133 297.128326                                   LLC        53 I, N(R)=49, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    134 297.128541                                   LLC        53 I, N(R)=48, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    135 297.128734                                   LLC        53 I, N(R)=49, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    136 303.878543                                   LLC        53 I, N(R)=48, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    137 303.878988                                   LLC        53 I, N(R)=48, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
    138 303.879469                                   LLC        53 I, N(R)=49, N(S)=3; DSAP NULL LSAP Individual, SSAP NULL LSAP Command

▷ Frame 138: 53 bytes on wire (424 bits), 53 bytes captured (424 bits) on interface -, id 0
◢ Logical-Link Control
   ▷ DSAP: NULL LSAP (0x00)
   ▷ SSAP: NULL LSAP (0x00)
   ▷ Control field: I, N(R)=49, N(S)=3 (0x6206)
▷ Data (49 bytes)
```

Figure 46: result of this sensor

III.5.3 The MPLS extended network technology

III.5.3.1 The Network Topology

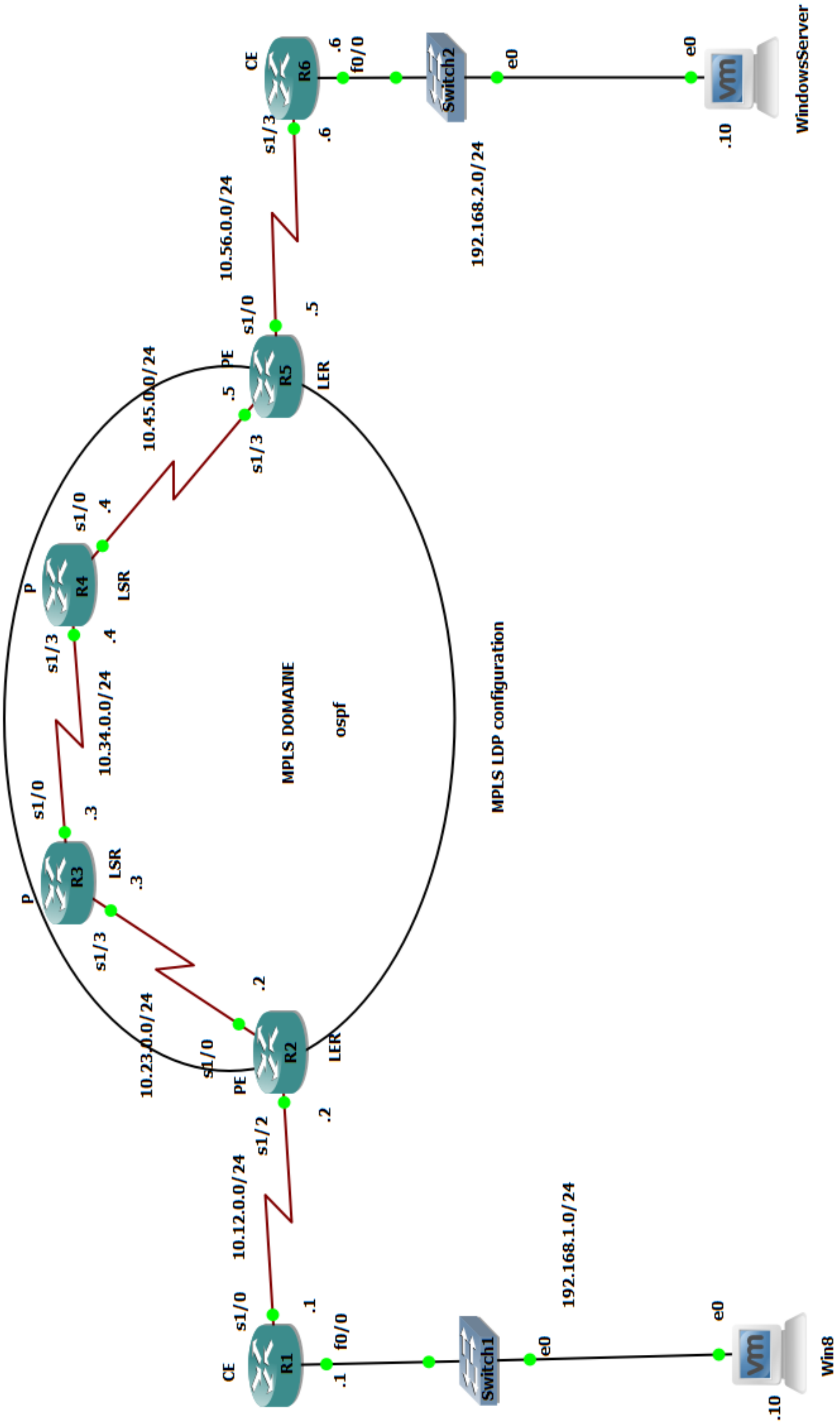


Figure 47: MPLS Network Topology

III.5.3.2 The router and MPLS Configuration

III.5.3.2.1 basic configuration of Router

Router R1

```
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#no ip domain-lookup
R1(config)#int f0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#ip route 0.0.0.0 0.0.0.0 10.12.0.2
R1(config)#do copy r s
R1(config)#int s1/2
R1(config-if)#ip address 10.12.0.1 255.255.255.0
R1(config-if)#no sh
R1(config-if)#exit
R1(config)#do copy r s
```

Router R2

```
R2#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R2(config)#int s1/1
R2(config-if)#ip address 10.12.0.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#ip ospf 1 area 0
R2(config-if)#exit
R2(config)#interface loopback 2
R2(config-if)#ip address 2.2.2.2 255.255.255.255
R2(config-if)#ip ospf 1 area 0
R2(config-if)#exit
R2(config)#int s1/0
R2(config-if)#ip address 10.23.0.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#ip ospf 1 area 0
R2(config-if)#exit
R2(config)#router ospf 1
R2(config-router)#passive-interface s1/2
R2(config-router)#do copy r s
```

Router R3

```
R3#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R3(config)#int s1/3
R3(config-if)#ip address 10.23.0.3 255.255.255.0
R3(config-if)#no sh
R3(config-if)#ip ospf 1 area 0
R3(config-if)#exit
R3(config)#interface loopback 3
R3(config-if)#ip address 3.3.3.3 255.255.255.255
R3(config-if)#ip ospf 1 area 0
R3(config-if)#exit
R3(config)#int s1/0
R3(config-if)#ip address 10.34.0.3 255.255.255.0
R3(config-if)#no sh
R3(config-if)#ip ospf 1 area 0
R3(config-if)#exit
R3(config)#do copy r s
```

Router R6

```
R6# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R6(config)#no ip domain-lookup
R6(config)#int f0/0
R6(config)#ip address 192.168.2.6 255.255.255.0
R6(config)#no sh
R6(config)#exit
R6(config)#ip route 0.0.0.0 0.0.0.0 10.56.0.5
R6(config)#do copy r s
R6(config)#int s1/3
R6(config)#ip address 10.56.0.6 255.255.255.0
R6(config)#no sh
R6(config)#exit
R6(config)#do copy r s
```

Router R5

```
R5#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R5(config)#int s1/3
R5(config-if)#ip address 10.56.0.5 255.255.255.0
R5(config-if)#no sh
R5(config-if)#ip ospf 1 area 0
R5(config-if)#exit
R5(config)#interface loopback 5
R5(config-if)#ip address 5.5.5.5 255.255.255.255
R5(config-if)#ip ospf 1 area 0
R5(config-if)#exit
R5(config)#int s1/1
R5(config-if)#ip address 10.45.0.5 255.255.255.0
R5(config-if)#no sh
R5(config-if)#ip ospf 1 area 0
R5(config-if)#exit
R5(config)#router ospf 1
R5(config-router)#passive-interface s1/0
R5(config-router)#do copy r s
```

Router R4

```
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#int s1/1
R4(config-if)#ip address 10.34.0.4 255.255.255.0
R4(config-if)#no sh
R4(config-if)#ip ospf 1 area 0
R4(config-if)#exit
R4(config)#interface loopback 4
R4(config-if)#ip address 4.4.4.4 255.255.255.255
R4(config-if)#ip ospf 1 area 0
R4(config-if)#exit
R4(config)#int s1/0
R4(config-if)#ip address 10.45.0.4 255.255.255.0
R4(config-if)#no sh
R4(config-if)#ip ospf 1 area 0
R4(config-if)#exit
R4(config)#do copy r s
```

```
R1#traceroute 10.56.0.6
Type escape sequence to abort.
Tracing the route to 10.56.0.6
VRF info: (vrf in name/id, vrf out name/id)
  1 10.12.0.2 96 msec 96 msec 92 msec
  2 10.23.0.3 96 msec 88 msec 96 msec
  3 10.34.0.4 140 msec 140 msec 140 msec
  4 10.45.0.5 184 msec 184 msec 180 msec
  5 10.56.0.6 184 msec 180 msec 184 msec
```

III.5.3.2.2 basic configuration of MPLS

MPLS CONFIGURATION ** R2**

```
R2#conf t
R2(config)#mpls label range 200 299
R2(config)#interface s1/0
R2(config-if)#mpls ip
R2(config-if)#do copy r s
```

MPLS CONFIGURATION ** R3**

```
R3#conf t
R3(config)#mpls label range 300 399
R3(config)#interface s1/3
R3(config)#mpls ip
R3(config)#exit
R3(config)#interface s1/0
R3(config)#mpls ip
do copy r s
```

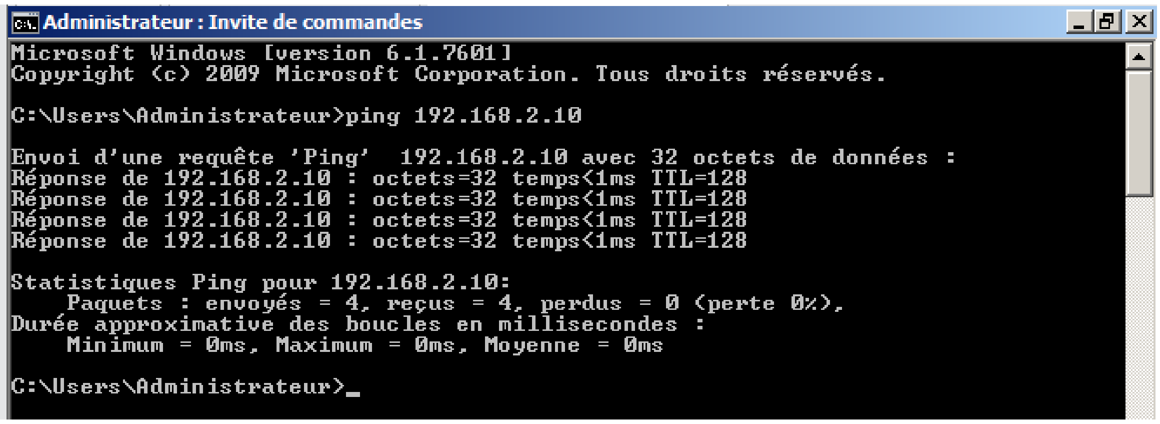
MPLS CONFIGURATION ** R4**

```
R4#conf t
R4(config)#mpls label range 400 499
R4(config)#interface s1/3
R4(config)#mpls ip
R4(config)#exit
R4(config)#interface s1/0
R4(config)#mpls ip
R4(config)#do copy r s
```

MPLS CONFIGURATION ** R5**

```
R5#conf t
R5(config)#mpls label range 500 599
R5(config)#interface s1/3
R5(config)#mpls ip
R5(config)#do copy r s
```

III.5.3.2.3 Testing Configuration Figure:48



```
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping 192.168.2.10

Envoi d'une requête 'Ping'  192.168.2.10 avec 32 octets de données :
Réponse de 192.168.2.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.2.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.2.10 : octets=32 temps<1ms TTL=128
Réponse de 192.168.2.10 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.2.10:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>_
```

figure48:testing Configuration

III.5.3.2.4 Result 3: Use of the MPLS network

in this part, we realized the MPLS topology , I will ping from the server that has the address 192.168.2.10 located in the headquarter to the second branch that has the address 192.168.1.10. I will a capture using Wireshark, and we get the following results shown in the two figures (49- 50)

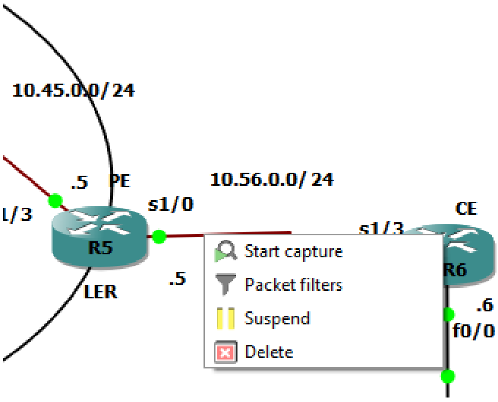
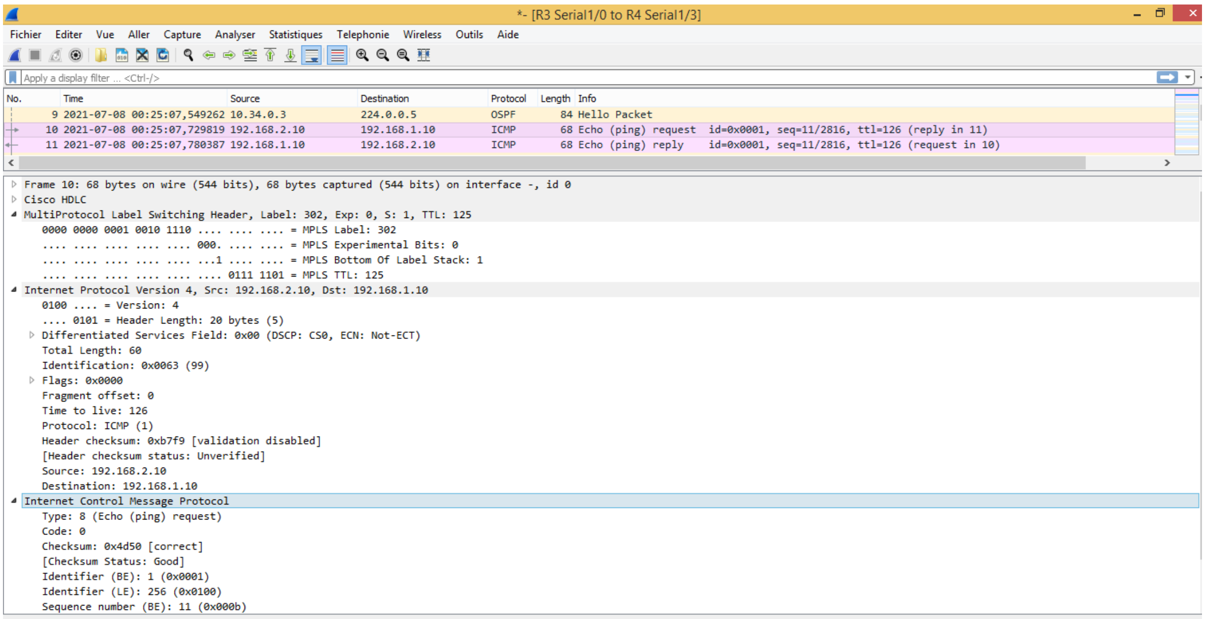


figure 49: capture MPLS



```
No.   Time                        Source        Destination   Protocol Length Info
    9 2021-07-08 00:25:07,549262 10.34.0.3     224.0.0.5     OSPF        84 Hello Packet
   10 2021-07-08 00:25:07,729819 192.168.2.10  192.168.1.10  ICMP        68 Echo (ping) request  id=0x0001, seq=11/2816, ttl=126 (reply in 11)
   11 2021-07-08 00:25:07,780387 192.168.1.10  192.168.2.10  ICMP        68 Echo (ping) reply    id=0x0001, seq=11/2816, ttl=126 (request in 10)
```

```
▷ Frame 10: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface -, id 0
▷ Cisco HDLC
◢ MultiProtocol Label Switching Header, Label: 302, Exp: 0, S: 1, TTL: 125
    0000 0000 0001 0010 1110 .... .... .... = MPLS Label: 302
    .... .... .... .... .... 000. .... .... = MPLS Experimental Bits: 0
    .... .... .... .... .... ...1 .... .... = MPLS Bottom Of Label Stack: 1
    .... .... .... .... .... .... 0111 1101 = MPLS TTL: 125
◢ Internet Protocol Version 4, Src: 192.168.2.10, Dst: 192.168.1.10
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  ▷ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 60
    Identification: 0x0063 (99)
  ▷ Flags: 0x0000
    Fragment offset: 0
    Time to live: 126
    Protocol: ICMP (1)
    Header checksum: 0xb7f9 [validation disabled]
    [Header checksum status: Unverified]
    Source: 192.168.2.10
    Destination: 192.168.1.10
◢ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4d50 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 11 (0x000b)
```

figure 50: Result of This Sensor

III.6 Comparison and performance evaluation

III.6.1 Results interpretation

After we captured the transmission of packets sent through the three technologies ATM.FR.MPLS using Wireshark, we found the following:

Throughput is the amount of information transmitted per unit of time. The MPLS offers a higher speed: the delay of the ATM is caused by the small size of the cells which does not transmit the large volumes of data but it transmits only by 53 bytes, we then have an under-utilization of the band pass-through if there is only one virtual channel in a link.

The packet transfer time reflects latency and jitter. Jitter is defined as the difference between the arrival time of two packets. ATM has a very short transfer time.

A definition for FR to MPLS Network interworking might include a number of requirements such as:

- Mapping fault conditions from the MPLS side to the FR side.
- Automatic configuration of FR PVCs to Label Switched Paths.
- Multiprotocol encapsulation procedures
- Mapping of FR Service Class/Priority to MPLS equivalents.

Key Differences Between Frame Relay and ATM

- The packet size in the frame relay varies while ATM uses a fixed size packet known as a cell.
- ATM produces fewer overheads as compared to the frame relay technology.
- Frame relay is less expensive respective to the ATM.
- ATM is faster than the frame relay.
- ATM provides error and flow control mechanism, whereas the frame relay does not provide it.
- Frame relay is less reliable than the ATM.
- Throughput generated by frame relay is medium. In contrast, ATM has a higher throughput.
- The delay in the frame relay is more. As against, it is less in case of ATM.

III.7 CONCLUSION

MPLS is a protocol that provides and facilitates routing by relying on labels or references compared to a routing table containing many thousands of entries. However, MPLS uses routing protocols to know which path it must take and to find which label to give to a packet to reach its destination. An MPLS network is an independent system consisting of several "switching routers" called Label Switch Router (LSR), which perform the role of a route-finding router and the role of a switch for relaying IP packets. There are two specific types of LSRs: the first is the Ingress LSR also called the LER entry, and it is through it that IP packets pass first and is responsible for mapping the label so that other LSRs know where to take them. The second is LSR or LER exit, which is the last transit by the packet before leaving the network, and therefore is responsible for removing the label so that the IP packet can return to what it was before. traversal of the MPLS network. The meaning of the label is local only and to agree on label numbers, LSR uses label distribution protocols. These protocols use routing tables when calculating routes, and there are several types including LDP, RSVP-TE, MBGP, and CR-LDP. Therefore, MPLS is a network that solves the routing problem, but its largest application is "Traffic Engineering", a type of routing that takes into account network bandwidth and congestion. MPLS is the long-awaited protocol for providing IP with service guarantee provided in ATM and FR, and all I found in this third section is that MPLS technology is the best to use in a wide area network due to the high quality it provides by transferring files at high speed and without errors.

III.8 GENERAL CONCLUSION

The network is a fairly broad field that provides a variety of technologies for its implementation. In this thesis we tried to implement the solutions available to implement a network: from layer 1 to layer 7, from local to extended. To achieve our goals, we first looked at the network as a whole by talking about the generalities and models of the OSI architecture, TCP/IP, the routing protocol, and different types of communication frames. Then, a simplified example of a local network solution was developed: it is a network among the networks of companies, economic or public institutions. It implements a hierarchical model with access, distribution, and core layers. The two networks are LAN and WAN, and the technologies used in WAN are ATM and .FR. MPLS. The first is based on switching cells while the second is based on "label switching".

The Frame Relay technology is very effective due to the simplified mechanism of data routing .And a tight system to control the flow of data and no need for complex control of error handling. The process of joining the Frame Relay network is carried out according to the following steps: Permission is obtained from the service provider, and the service provider assigns DLCI addresses. ATMs offer several types of services adapted to each stream such as audio, file and video. However, its implementation is very complicated because its signals still require a level different from the level of control. For its part, MPLS is trying to emulate ATM in QoS.

The success of MPLS lies in switching its label in close collaboration with IP and Routing Protocol (OSPF) in our case. It does not require another transmission plan because IP routing takes care of it. In the last chapter, the use of GNS3 made it possible to simulate CISCO routers and thus realize the network, which communicates with its local headquarters through a wide area network. The main office consists of the server represented by "Windows Server 2008". It gave us a comparison between MPLS and Frame Relay, knowing that I found it difficult to compare with ATM due to its incompatibility with Wireshark.

and wide area network classification. MPLS offers better throughput but with more latency; On the other hand, ATMs provide lower throughput and such as FR but with excellent real-time performance. Thus, the solution is to use MPLS for interconnection since it is more flexible in terms of IP adaptation and its real-time transmission is still acceptable. However, thanks to its high speed and real-time performance, ATM and FR can compete with MPLS especially in the field of network and capacity for the purpose of high quality in packet transmission. Apart from the practical solution of the company, the solution was determined for the operator by comparing the results of the test. From another point of view, the use of an ATM is an expensive solution and simultaneously with MPLS it is a very good solution, but the cost promises to be high, if not very high.

REFERENCES

[**01**] Armitage, G. Quality of Service in IP Networks. Indianapolis, IN: Macmillan Technical Publishing, 2000.

[**02**] Bouillet, E.; Mitra, D.; and Ramakrishnan, K. “The Structure and Management of Service Level Agreements in Networks.” IEEE Journal on Selected Areas in Communications, May 2002.

[**03**] Bonaventure, O., and Nelissen, J. “Guaranteed Frame Rate: A Better Service for TCP/IP in ATM Networks.” IEEE Network, January/February 2001.

[04] Black, U. ATM Volume I: Foundation for Broadband Networks. Upper Saddle River, NJ: Prentice Hall, 1992.

[**05**] Black, U. IP Routing Protocols: RIP, OSPF, BGP, PNNI & Cisco Routing Protocols. Upper Saddle River, NJ: Prentice Hall, 2000.

[**06**] Bing, B. Wireless Local Area Networks. New York: Wiley, 2002.

[**07**] Cerf, V, and Kahn, R.“A Protocol for Packet Network Interconnection.” IEEE Transactions on Communications, May 1974.

[**08**] Crow, B., et al. “IEEE 802.11 Wireless Local Area Networks.” IEEE Communications Magazine, September 1997.

[**09**] Cohen, J. “Rule Reversal: Old 80/20 LAN Traffic Model is Getting Turned on Its Head.” Network World, December 16, 1996.

[**10**] Harbison, R. “Frame Relay: Technology for Our Time.” LAN Technology, December 1992.

[**11**] Comer, D. Internetworking with TCP/IP, Volume I: Principles, Protocols, and Architecture. Upper Saddle River, NJ: Prentice Hall, 2006.

[**12**] Forouzan, B., and Chung, S.Local Area Networks. New York: McGraw-Hill, 2002.

[**13**] Freeman, R. Fiber-Optic Systems for Telecommunications. New York: Wiley, 2002.

[**14**] Giroux, N., and Ganti, S. Quality of Service in ATM Networks. Upper Saddle River, NJ: Prentice Hall, 1999.

[**15**] Garrett, M. “A Service Architecture for ATM: From Applications to Scheduling.” IEEE Network, May/June 1996.

[**16**] Green, P. “An Introduction to Network Architecture and Protocols.” IEEE Transactions on Communications, April 1980.

[**17**] https://www.edrawsoft.com/wide-area-network.html.

[**18**] ITU-T G.8114. Operation and maintenance mechanisms for T-MPLS layer networks [S]. 2007.

[**19**] ITU-T Rec G.8131.1. Transport MPLS (T-MPLS) layer network protection switching [S]. 2007.

[**20**] ITU-T New Supplement Y.Sup4. Transport requirements for T-MPLS OAM and ITU-T Rec G.8112. Interfaces for the Transport MPLS(T-MPLS) hierarchy [S]. 2006.

[**21**] ITU-T Rec G.8110.1/Y.1370.1. Architecture of Transport MPLS (T-MPLS) layer network [S]. 2006.

[**22**] ITU-T G.8121. Characteristics of transport MPLS equipment functional blocks [S]. 2007.

[**23**] McDysan, D., and Spohn, D. ATM: Theory and Application. New York: McGraw-Hill, 1999.

[**24**] Niven-Jenkins B, BRUNGARD D, BETTS M, et al. MPLS-TP requirements [R]. draft-jenkins-mpls-tp-requirements-01. 2008.

[**25**] network [J]. Telecommunications for Electric Power System, 2009, 30(4): 52-59.

[**26**] Rodriguez, A., et al. TCP/IP Tutorial and Technical Overview. Upper Saddle River: NJ: Prentice Hall, 2002.

[**27**] Regan, P. Local Area Networks. Upper Saddle River, NJ: Prentice Hall, 2004.

[**28**] Schnider, Joel. "SSL VPN Gateways." *Network World*. 12 January 2004

[**29**] Stevens, W. TCP/IP Illustrated, Volume 1: The Protocols. Reading, MA: Addison-Wesley, 1994.

[**30**] Stevens, W. TCP/IP Illustrated, Volume 3: TCP for Transactions, HTTP, NNTP, and the UNIX(R) Domain Protocol. Reading, MA: Addison-Wesley, 1996.

[**31**] WARD D, BETTS M. MPLS architectural considerations for a transport profile [R],

[**32**] Wright, G., and Stevens, W. TCP/IP Illustrated, Volume 2: The Implementation. Reading, MA: Addison-Wesley, 1995.

[**33**] Weston.Jason. Neumann, GNS3 ,Build Virtual,Network Labs Using,Cisco

[**34**] www.ibm.com/docs/en/zvm/7.1?topic=mproute-routing-information-protocol-rip